3isco.ir

CCNA Security

With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats.

FARSHID BABAJANI

09199926216

به نام خدا

کتاب آموزشی

CCNA Security (210-260)

نویسنده:

فرشید باباجانی – آزاده تیشه برسر

زمستان ۱۳۹۸ – تهران

فهرست

مقدمه

دوره‌ی Cisco Certified Network Associate Security یا همان CCNA Security برای ایجاد امنیت مقدماتی در شبکه‌ای که از محصولات سیسکو استفاده می‌کند کاربرد دارد، با داشتن این گواهینامه امنیتی می‌توانید مهارت‌های لازم برای توسعه زیرساخت‌های امنیتی، تشخیص تهدیدات و آسیب پذیری‌ها را کسب کنید.

دوره‌های امنیتی سیسکو شامل دوره‌ی CCNA Security (کارشناس امنیت)، CCNP Security (کارشناس ارشد امنیت) و CCIE Security (دکترای امنیت) است که هر کدام از این دوره‌ها دارای سرفصل‌های جدا و جذابی هستند.

ایجاد امنیت در شبکه کار آسانی نخواهد بود و در هر زمان باید مواظب باشیم که اطلاعات شما افشاء نشود و یا به شبکه شما حمله نشود، ولی شما با ایجاد راه‌حل های امنیتی این تهدیدات را کاهش دهید، برای اینکار نیاز دارید تا تهدیدات را شناسایی و راه‌های جلوگیری از آن را به درستی پیاده‌سازی کنید.

اگر شما امنیت یک شبکه مد نظرتان است باید یک سری از قواعد را پیروی کنید تا با مشکلی مواجع نشوید، این قواعد شامل سه هدف است، محرمانه بودن (Confidentiality)، یکپارچگی (Integrity) و در دسترس بودن (Availability) است که این سه کلمه را به اختصار با نام CIA می‌شناسند، بیشتر مشکلاتی که در بخش امنیت شبکه به وجود می‌آید، زیر مجموعه این سه بخش است و باید سعی کرد دید خود را در این سه زمینه گسترده‌تر کنیم.

در این دوره و در این کتاب با طراحی و پیاده‌سازی سیستم‌های امنیتی مبتنی بر IOSرا با هم فرا خواهیم گرفت و سعی شده است تا اکثر مطالبی که در سرفصل‌های سیسکو بیان شده بررسی و توضیح داده شود.

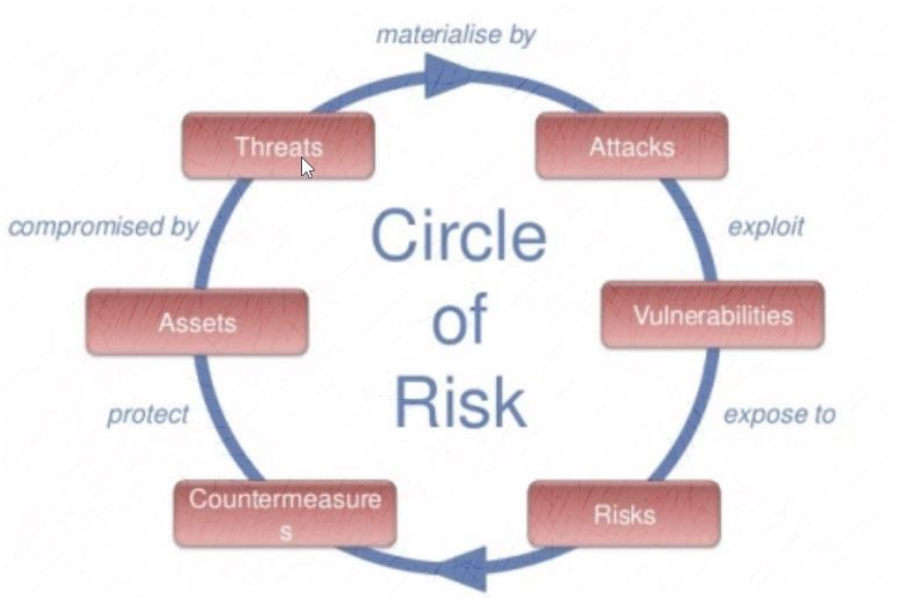
توجه داشته باشید پیش‌نیاز این دوره، دوره‌ی CCNA Route # switch است که کتاب آن به زبان فارسی تهیه شده و از سایت می‌توانید دانلود و مطالعه کنید تا دید شما برای کار با دستگاه‌های سیسکو عمیق‌تر شود.

تقدیم به همسرم

به آن کسی که آفتاب مهرش در قلبم همچنان پا برجاست و هرگز غروب نخواهد کرد، ممنونم به خاطر همه خوبی‌هات...

فصل اول – بررسی شرایط امنیتی

در این قسمت ریسک‌های شبکه را با هم بررسی خواهیم کرد.



- **منابع یا دارایی‌های سازمان (Assets)**

در این بخش باید منابع با ارزش سازمان مشخص شود، که این منابع می‌تواند شامل داده‌ها، برنامه‌ها و سرورها و... باشد.

در زیر جدولی از منابع موجود را مشاهده می‌کنید.:

طبقه‌بندی‌های دولتی	حساس اما غیر طبقه بندی شده(SBU) محرمانه راز فوق سری
طبقه‌بندی بخش خصوصی و عمومی	حساس خصوصی محرمانه
معیارهای طبقه بندی ارزش	سن هزینه جایگزینی طول عمر مفید

- **آسیب پذیری (Vulnerability)**

نقص یا ضعف در طراحی، پیاده‌سازی، بهره‌برداری و مدیریت یک سیستم می‌توانند برای نقض سیاست امنیتی سیستم، مورد سوء استفاده قرار گیرند. اصولاً مهاجمان از آسیب‌پذیری‌هایی که از طریق نرم‌افزار، سخت‌افزار و یا کارمندان به وجود می‌آید می‌توانند به شبکه سازمان حمله کنند، بیشتر سازمان‌های امروزی یک ارزیابی کلی برای شناسایی این آسیب‌پذیری‌ها انجام می‌دهند.

طبقه‌بندی آسیب‌پذیری‌ها به صورت زیر بیان می‌شود:

- Policy flaws (نقص در سیاست سازمان)
- Design errors (طراحی اشتباه)
- Protocol weaknesses (ضعف در پروتکل)
- Misconfiguration (تنظیمات اشتباه)
- Software vulnerabilities (آسیب‌پذیری نرم‌افزار)
- Human factors (عوامل انسانی)
- Malicious software (نرم‌افزارهای مخرب)
- Hardware vulnerabilities (آسیب‌پذیری سخت‌افزاری)
- Physical access to network resources (دسترسی فیزیکی به منابع شبکه)

- **تهدیدات (Threat)**

تهدیدات زمانی رخ می‌دهد که مهاجم در بخش قبلی (**Vulnerability**)، آسیب‌پذیری‌های یک سیستم را شناسایی کند و بتواند از آن طریق به شبکه ما ضربه بزند، یک مثال ساده در این بخش، می‌تواند به اشتراک گذاشتن یک پوشه با دسترسی اشتباه باشد.

- **عامل تهدیدات (Threat agent)**

عامل، کسی است که تهدیدات را به وجود می‌آورد، مثلاً مهاجمی که از ACL یا همان Access List اشتباه استفاده می‌کند می‌تواند عامل تهدید باشد که این عامل‌ها می‌توانند آسیب‌پذیری‌ها را شناسایی و از آنها برای حمله به شبکه استفاده کنند، البته همه عامل‌ها این کار را انجام نمی‌دهند.

- **ریسک (Risk)**

احتمال یک خطر است که توسط یک عامل تعدید (Threat agent) از طریق پیدا کردن یک آسیب‌پذیری در شبکه به وجود می‌آید، کاهش ریسک‌های یک شبکه بسته به سیاست‌هایی دارد که مدیر شبکه پیاده‌سازی می‌کند.

روش‌هایی که در اقدام متقابل می‌توان از آنها استفاده کرد شامل موارد زیر است:

۱- اجرایی (Administrative) که شامل استانداردها، رویه‌ها، دستورالعمل‌ها و سیاست‌های سازمان است که باید به صورت کتبی از همه کاربران تعهد گرفت تا خلاف آن عمل نکنند.

۲- فیزیکی (Physical) شامل کنترل‌های فیزیکی دقیق برای تجهیزات شبکه خود است، مثلاً می‌توانید برای اتاق سرور خود از درب‌های ضد سرقت پیشرفته و نسوز استفاده کنید و یا اینکه برای رک‌های دیواری که در هر طبقه موجود هستند را قفل کنید، طراحی باید به صورتی باشد که کاربران به هیچ قطعه یا سیسمی دسترسی نداشته باشند.

۳- منطقی (Logical) که شامل کنترل‌های منطقی شامل گذرواژه‌ها ، فایروال‌ها ، سیستم‌های پیشگیری از نفوذ، لیست‌های دسترسی ، تونل‌های VPN و... کنترل‌های منطقی اغلب به عنوان فنی گفته می‌شوند، کنترل می‌کند.

- **در معرض قرار گرفتن (Exposure)**

وقتی که به یک پوشه به اشتراک گذاشته شده یک دسترسی اشتباه می‌دهید، آن پوشه در معرض تهدیدات قرار خواهد گرفت و امنیت شرکت را زیر سوال خواهد برد.

- **اقدام متقابل (Countermeasure)**

اقدام متقابل، ریسک‌های یک شبکه را کاهش خواهد داد، برای انجام یک کار در شبکه سه موضوع آسیب‌پذیری، تهدیدات و ریسک باید مورد توجه قرار گیرد تا بتوان اقدام متقابل را برای آنها انجام داد.

فرآیند مدیریت ریسک (Risk Management Process)

فرآیند مدیریت ریسک شامل یک سرس عملیات است که عبارتند از:

- ✓ شناسایی کردن منابع و ارزش‌های سازمان
- ✓ شناسایی تهدیدات
- ✓ شناسایی آسیب‌پذیری
- ✓ تعیین احتمال حمله
- ✓ شناسایی ضربه
- ✓ تعیین ریسک به عنوان ترکیبی از احتمال و تاثیر.

طبقه‌بندی منابع (Asset Classification)

اولین قدم در ارزیابی ریسک‌ها شناسایی منابع و ارزش‌های آن سازمان است، دارایی‌هایی که در یک سازمان وجود دارد مشهود و غیر مشهود است که این دارایی‌های مشهود عبارتند از:

کاربران، کامپیوترها، امکانات و منابع، ولی دارایی‌های غیر مشهود شامل مالکیت معنوی داده‌ها و شهرت سازمانی است.

شناخت تهدیدات شبکه فعلی

تهدیدات امروز به طور مداوم در حال تغییر هستند و تهدیدهای جدیدی ظهور میکند، در این قسمت می‌خواهیم به دسته‌های مختلف تهدیدات شبکه بپردازیم:

۱- مهاجمان نهایی (**Potential Attackers**)

که این مورد اشاره دارد به هکرها، تروریست‌ها، کارکنان ناراضی یک شرکت و...

۲- روش‌های حمله (**Attack Methods**)

یک هکر، به هیچ عنوان دوست ندارد که شناسایی شود، به خاطر همین از روش‌هایی برای مخفی کردن خود استفاده می‌کنند و کارهایی را که در زیر لیست شده است را برای نفوذ به شبکه انجام می‌دهد که شامل:

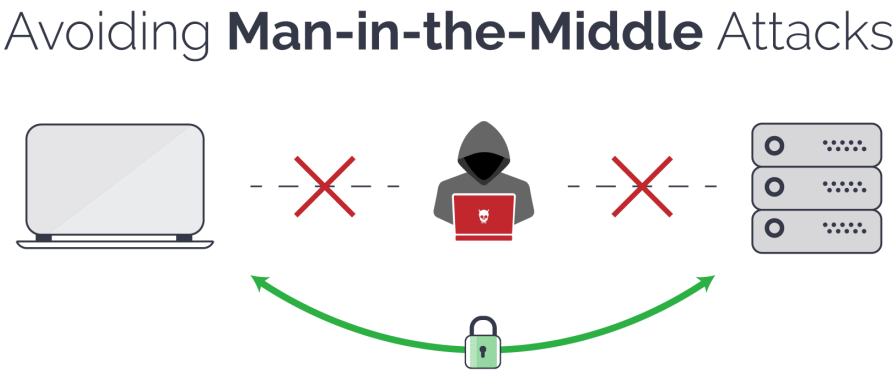
شناسایی (Reconnaissance)	در اولین قدم هکر با استفاده از نرم‌افزار خاصی اقدام به شناسایی آدرس IP و پورت‌های باز شبکه می‌کند تا موارد قابل نفوذ را شناسایی کند.
مهندسی اجتماعی (Social engineering)	یکی از روش‌های ساده برای بدست آوردن اطلاعات یک سازمان است، در این روش هکر با استفاده از کارمندان یک سازمان اقدام به بدست آوردن اطلاعات مهم آن می‌کند، مثلاً می‌تواند با استفاده از ایمیل‌های جعلی از کارمندان اطلاعات بگیرد یا اینکه از فیشینگ کردن وب‌سایت‌های مشخص استفاده کند تا به اطلاعات خود دست پیدا کند.
حداکثر امتیاز (Privilege escalation)	در این روش مهاجم با استفاده از یک کاربر معمولی وارد روتر می‌شود و با استفاده از حملات brute-force شروع به بدست آوردن حداکثر دسترسی می‌کند.
در پشتی (Back doors)	مهاجم بعد از ورود به شبکه اقدام به نصب نرم‌افزارهای مخرب بر روی کلاینت یا سرور می‌کند و بعد از آن در هر زمان می‌تواند به اطلاعات آنها دستگاه دست پیدا کند، مانند نرم‌افزارهای Key-logging که تمام اطلاعات ورودی از کیبورد را ذخیره و به آدرس خاصی ارسال می‌کنند.
اجرای کد (Code execution)	در این روش مهاجم توانایی این را دارد که کدها مورد نظر خود را در سرور سازمان شما اجرا کند که این کار یکی از خطرناکترین حملات است این روش با نام Remote Code Execution یا به اختصار RCE شناخته می‌شود.

۳- راه‌های حمله (**Attack Vector**)

این موضوع را به خاطر داشته باشید فرد مهاجم همیشه از بیرون شرکت به شبکه شما حمله نمی‌کند و شاید کسی از داخل شرکت این کار را انجام دهد، شاید کاربر از سر بی‌اطلاعی بخواهد بر روی موضوع خاصی کنجکاوی کند و همان موضوع باعث شود حملات درب پشتی (Back doors) انجام شود. برای جلوگیری از این روش باید سیاست‌های درست پیاده‌سازی شود.

۴- حمله مرد میانی (**Man-in-the-Middle Attacks**)

حملات مرد میانی با نام Bucket Bridge Attack هم شناخته می‌شوند، در این نوع حمله مهاجم خود را بین دو سیستم قرار می‌دهد و از روش‌های خاصی برای بدست آوردن اطلاعات سیستم‌ها استفاده می‌کند، این کار با هدف شناسایی و دستکاری داده‌ها انجام می‌شود، این حمله می‌تواند در لایه دو و یا لایه سه اتفاق بیفتد، هدف اصلی این کار گوش دادن به اطلاعات ردو بدل شده بین دو منبع است.



۵- سایر روش‌های حمله

کانال پنهان (Covert channel)	در این روش اگر شما به عنوان مدیر شبکه اجازه دسترسی به یک وب‌سایت را در فایروال ببندید، کاربر یا مهاجم با استفاده از VPN و ایجاد تونل در شبکه داخلی باعث می‌شود این سیاست شما را دور بزند.
منطقه قابل اعتماد	در این روش اگر در یک فایروال که دارای سه منطقه است و به منطقه خارجی (outside) آن دسترسی کامل دهید، مهاجم با ورود به سرورهای مستقر در منطقه DMZ می‌تواند به سیستم‌های داخل Inside دسترسی پیدا کند، در مورد مناطق شبکه در فصل ششم به صورت کامل صحبت کردیم.

حملات بی رحمانه با رمز عبور Brute-force) (passwordguessing) (attacks	در این روش مهاجم با استفاده از دیتابیسی از کلمه عبور، تلاش می‌کند رمز عبور سیستم را حدس بزند که البته با ایجاد سیاست، تعداد تلاش برای وارد کردن رمز عبور، این مورد حل می‌شود.
Botnet	در این حمله مهاجم در یک سازمان دارای هزاران سیستم آلوده آماده به کار هست و با استفاده از آنها بدون اطلاع صاحبان شرکت شروع به حمله به یک مقصد مشخص می‌کند که از این طریق می‌توان حملات DDOS را انجام داد.
حملات DoS and DDoS	این نوع حملات زمانی مشخص می‌شوند که ترافیک غیر واقعی و بسیار زیاد بر روی سرور وب‌سایت شما افزایش می‌یابد و این موضوع باعث می‌شود دستگاه‌هایی مانند سوئیچ و روتر با افزایش کارکرد CPU روبرو شوند و باعث از کار افتادن آنها می‌شود در حملات Dos یا denial-of-service مهاجم فقط از طریق یک سیستم شروع به حمله می‌کند ولی در روش پیشرفته‌تر آن یعنی DDoS یا همان distributed denial-of-service از چندین سیستم برای این کار استفاده می‌شود که روش Botnet می‌تواند جز آن باشد.

استفاده از اصول اساسی امنیت در شبکه

در این بخش رویکردهایی برای بهبود شبکه مشخص شده است که می‌تواند از مواردی که در بالا بیان کردیم پیشگیری کند.

محرمانه بودن (Confidentiality)

برای ایجاد یکپارچگی در اطلاعات باید سطح دسترسی را برای افراد مشخص کنید تا از افشای اطلاعات در بیرون سازمان جلوگیری شود، سه اصل؛ شناسایی(Identification)، احراز هویت(Authentication)، مجوز دسترسی(Authorization) می‌تواند شما را در این امر بسیار کمک کند، همه این موارد در ادامه کتاب بررسی خواهد شد.

یکپارچگی (Integrity)

این قسمت از سه مرحله قبل یعنی، شناسایی(Identification)، احراز هویت(Authentication)، مجوز دسترسی(Authorization) اطمینان حاصل پیدا می‌کند، و هدف اصلی آن حفظ یکپارچگی داده‌ها، از جمله داده‌های ذخیره شده در فایل‌ها، پایگاه داده‌ها، سیستم‌ها و شبکه ها است.

در دسترس بودن (Availability)

در دسترس بودن به این معنی است که اطلاعات در زمان و مکان مورد نیاز فقط برای افرادی که مجوز لازم را دارند همیشه در دسترس باشد.

در دو حوزه می‌توان از ویژگی در دسترس بودن خیلی خوب استفاده کرد:

۱- زمانی که حملات گسترده به شبکه انجام شود و شبکه به طور کامل غیرفعال شود، مانند ویروس‌های باجگیر که این روزها شبکه‌های بسیاری را آلوده کردند و در نوع خاصی از آنها هیچ راهی برای برگشت اطلاعات وجود ندارد.
۲- زمانی که بلایای طبیعی رخ دهد.

یکی از راه‌های مهمی که برای در دسترس بودن اطلاعات باید انجام گیرد استفاده از فناوری Raid برای شبکه است تا اطلاعات در سریعترین زمان ممکن در دسترس قرار گیرد.

تعاریف اولیه در امنیت اطلاعات

کمترین امتیاز (Least Privilege)

مفهوم کلی این تعریف در مورد این است که به هر کسی به اندازه‌ی نیازش دسترسی بده، که این موضوع می‌تواند برای یک کاربر باشد و یا یک فرآیند، برای فعال کردن حداقل‌ها، باید سازمان‌ها تمامی کارکردهای کاربران را شناسایی و بر اساس آن دسترسی‌ها را اولویت‌بندی کنند تا کسی بیشتر از نیاز خود به منابع شبکه دسترسی نداشته باشد.

یک سری قوانین سازمانی وجود دارد که از اصل کمترین امتیاز (Least Privilege) حمایت می‌کنند:

۱- تعداد اکانت‌هایی که دارای مجوزهای زیاد در شبکه هستند را محدود کنید.
۲- مدیران شبکه باید از یک اکانت با دسترسی معمولی برای عملیات معمول خود استفاده کنند.
۳- دسترسی‌ها ابزاری محبوب برای مهاجم‌ها هستش که باید دقت لازم در این زمینه را داشته باشیم و آن را محدود کنیم.

دسترسی به هیچ چیز (Access to Nothing)

سعی کنید به صورت پیش‌فرض دسترسی‌ها را برای همه کاربرانی که برای اولین بار به شبکه متصل می‌شوند ببندید، این کار یکی از بهترین عملکردهای امنیتی محسوب خواهد شد که افراد ناشناس نتوانند به راحتی به شبکه دسترسی داشته باشند.

دفاع در عمق (Defense in Depth)

استراتژی دفاع از عمق به این موضوع اشاره دارد که برای ایجاد امنیت باید از چند لایه‌ی امنیتی برای رسیدن به اطلاعات استفاده کرد، یکی از این استراتژی ها استفاده از کنترل دسترسی‌ها در شبکه است.

تفکیک وظایف (Separation of Duties)

برای کاربران باید وظایف مشخص معین شود و هر کسی وظایف مربوط به خود را انجام دهد، با این کار از تقلب در کارها جلوگیری خواهد شد، مثلاً می‌توانیم برای یک کار که قرار است انجام شود دو مدیر تعیین کنیم تا هر دو مجوز آن کار را صادر کنند و با یک نفر آن کار انجام نشود.

چرخش کار (Job Rotation)

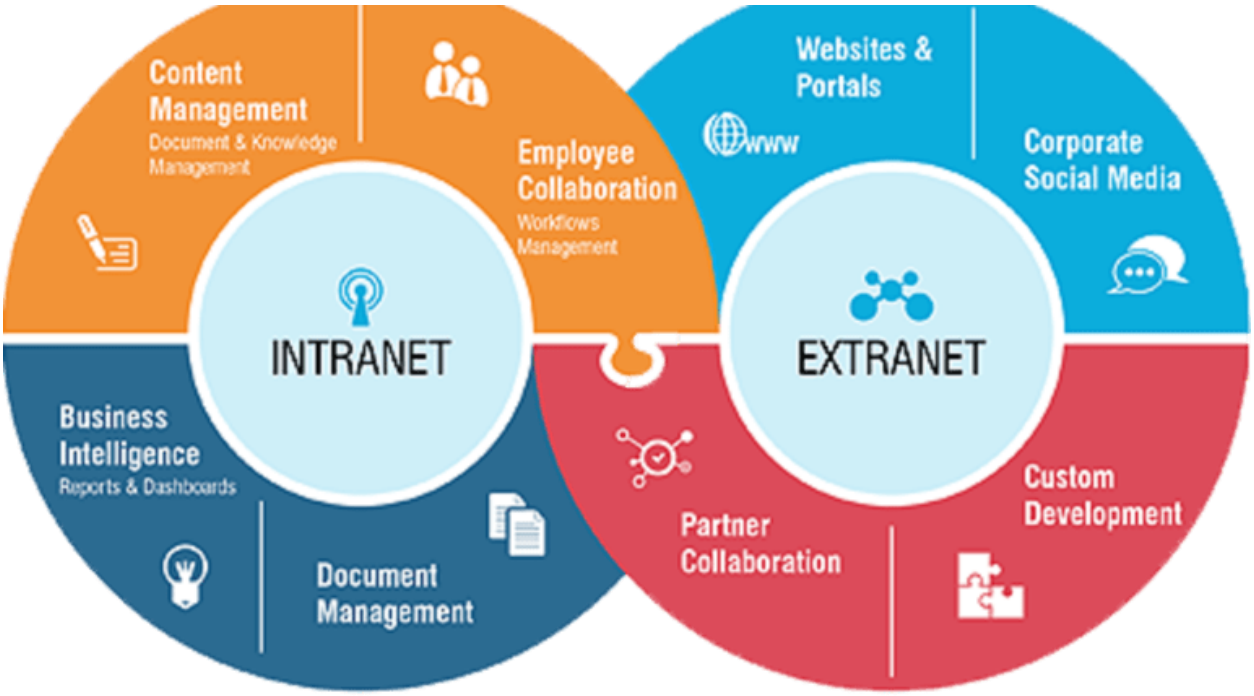
در این بخش باید آموزش‌های لازم داده شود تا از انجام تقلب جلوگیری شود، در چرخش کار باید یک نسخه از اطلاعات شبکه داشته باشیم.

مناطق امنیتی مشترک شبکه (Common Network Security Zones)

DMZ یک زیرشبکه منطقی یا فیزیکی است که اطلاعات شبکه داخلی را به بیرون از سازمان یعنی فضای اینترنت ارسال می‌کند، هدف از یکDMZ ، اضافه کردن یک لایه امنیتی بیشتر به شبکه محلی یک سازمان است؛ یک مهاجم خارجی به جای دیگر قسمت‌های شبکه، تنها به تجهیزاتی که در DMZ هستند دسترسی دارد و با این کار خطرات ناشی از دسترسی غیر مجاز به شبکه اصلی کاهش پیدا خواهد کرد، DMZ فقط و فقط برای جلوگیری از دسترسی افراد به شبکه داخلی (Intranet) و یا همان محلی است و اگر مهاجمی از داخل شبکه بخواهد جاسوسی کند، نمی‌تواند کاری انجام دهد، بهترین راه استفاده از این نوع شبکه‌ها استفاده از یک دستگاه Firewall برای جدا کردن سه شبکه Internet، DMZ و Intranet است که در شکل زیر آن را مشاهده می‌کنید.

بررسی شبکه Interanet

Intranet به شبکه‌ی داخلی اشاره می‌کند که به عنوان یک شبکه خصوصی شناخته می‌شود و در این شبکه می‌توان هر نوع پروتکلی را اجرا و استفاده کرد، در این نوع شبکه‌ها به مانند شبکه اینترنت می‌توانید سرورهای ایمیل، وب، FTP و دیگر پروتکل‌ها را پیاده‌سازی کرد، این نوع شبکه‌های با استفاده از فایروال‌ها محافظت می‌شود و کسی نمی‌توانید بدون اجازه به آن دست پیدا کند.

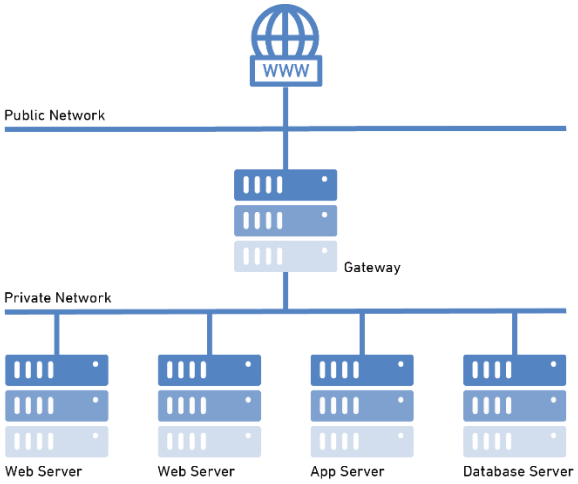


شبکه Extranet

Extranet بخشی از یک شبکه خصوصی است که مدیران شبکه‌ی یک سازمان برای متصل شدن کاربران خارج از سازمان به شبکه از روش‌های امنی استفاده می‌کنند تا کاربران بر روی سیستم خارجی خود مانند سیستم داخل منزل یا جایی دیگر شبکه داخلی آن سازمان را داشته باشند، یکی از روش‌های پیاده‌سازی این نوع شبکه‌ها فعال‌سازی پروتکل VPN است که این کار را با امنیت کامل و سریع انجام می‌دهد.

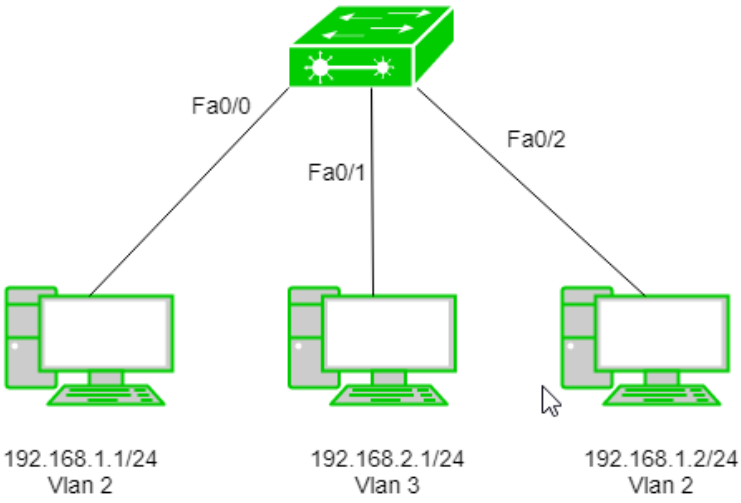
شبکه عمومی و خصوصی (Public and Private)

شبکه‌ی Public یک شبکه‌ی عمومی است که همه افراد می‌توانند به ان دسترسی داشته باشند مانند شبکه‌ی اینترنت که در سرتاسر جهان گسترده شده و امروزه اکثر افراد در این شبکه در حال فعالیت هستند، شبکه‌های Private همان شبکه خصوصی یک سازمان خواهد بود.



شبکه مجازی (Virtual LAN)

Virtual LAN یا VLAN به شبکه‌ای گفته می‌شود که در لایه دو کاربرد دارد و برای ایجاد امنیت در سوئیچ به کار می‌رود، VLAN ها برای جدا کردن پورت‌های سویچ به کار می‌روند، مثلاً می‌خواهید به سرور مالی شرکت فقط و فقط یک سیستم خاص متصل شود، برای این کار آنها را در یک VLAN قرار میدهید، در مورد شبکه VLAN در کتاب CCNA R&S توضیحات لازم را دادم.

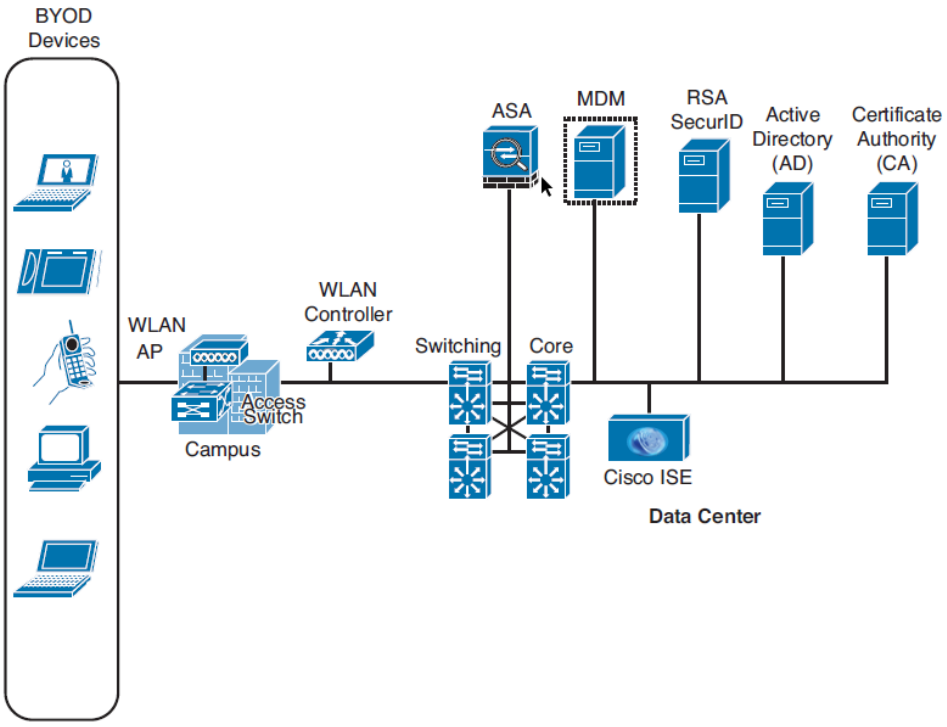


فصل دوم– طراحی شبکه و چشم‌انداز تهدیدات امنیتی

یک شبکه بسته به نوع کار و وسعت آن به انواع مختلفی تقسیم می‌شود که در زیر آنها را بررسی میکنیم.

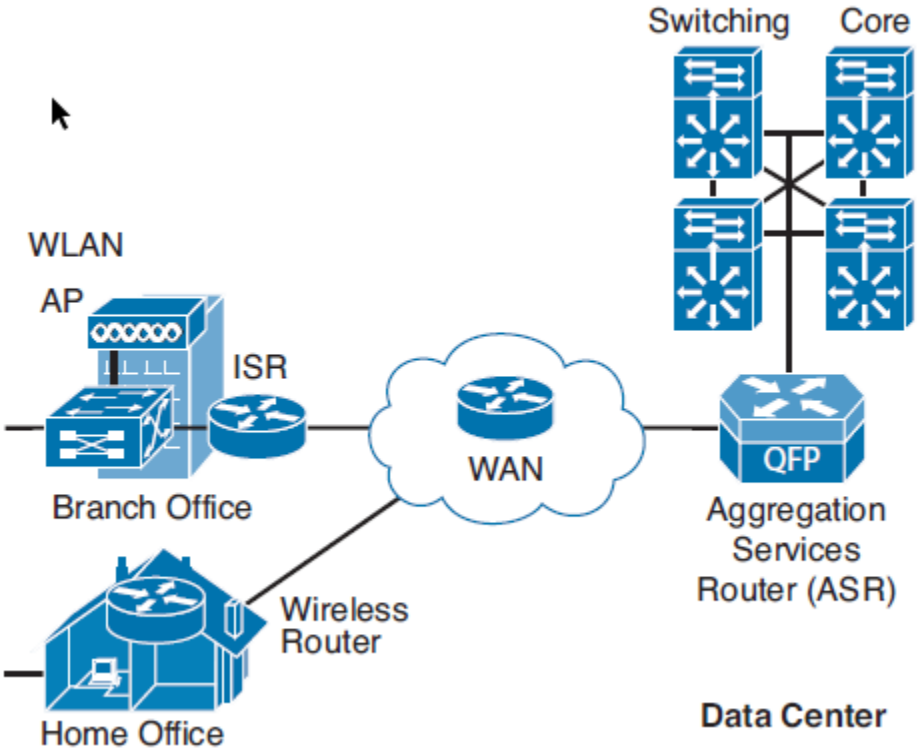
شبکه محوطه دانشگاه یا Campus-Area Network (CAN)

یک محیط دانشگاهی را در نظر بگیرید که دارای چندین دانشکده است و ارتباط بین آنها از طریق Wireless یا Fibr ایجاد شده است، این نوع شبکه طوری طراحی شده‌اند تا به کاربران و یا BYOD Devices خدمات ارائه دهند، BYOD به دستگاه‌های نهایی گفته می‌شود که از خدمات آن شبکه استفاده می‌کنند و در شکل زیر هم مشخص شده است.



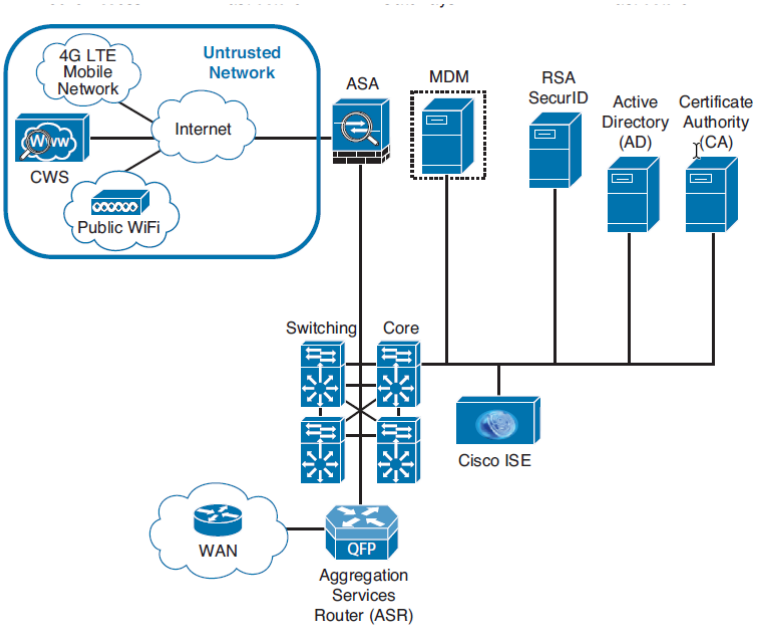
شبکه Wide-Area Network (WAN) یا Cloud

این شبکه با عنوان یک شبکه جهانی شناخته می‌شود که محدودیت جغرافیایی آن بسیار زیاد است و اگر بخواهید از دفتر کار به کارخانه خود متصل شوید این شبکه می‌تواند بسیار مفید باشد، مثال بارز آن شبکه جهانی اینترنت است، در این نوع شبکه‌ها می‌توانید از خاصیت Cloud هم استفاده کنید و در هر مکان و زمانی که هستید می‌توانید به داده‌های سازمان خود دسترسی داشته باشید.



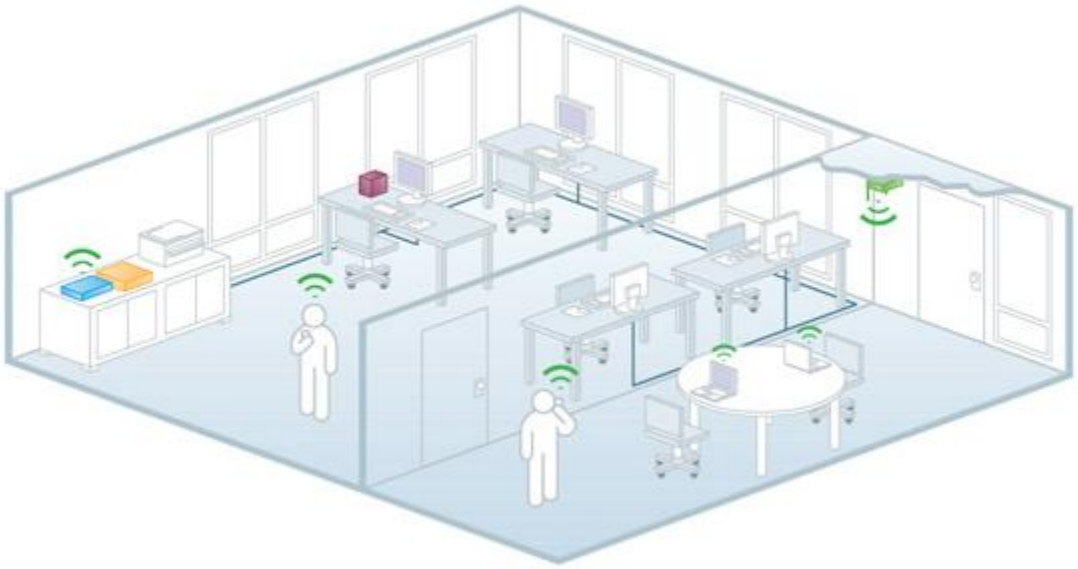
شبکه Data Center

این نوع شبکه‌ها شامل سرورهای عظیم و با تعداد بالا هستند که برای ارائه سرویس‌های تحت وب مانند Host، Email، Virtulization و... کاربرد دارند.



شبکه‌های Small office/Home office

به شبکه‌های با مقیاس کوچک گفته می‌شود که با نام SOHO هم شناخته می‌شود، دراین نوع شبکه‌ها کاربران از طریق مودم‌های شخصی به ISP مورد نظر متصل می‌شوند و از خدمات آن استفاده می‌کنند.



امنیت شبکه برای یک محیط مجازی

به علت گستردگی کار در شبکه‌های بزرگ باید روش‌هایی پیدا کرد تا هزینه‌ها کاهش و امنیت داده‌ها افزایش یابد، به خاطر همین موضوع شرکت‌های بزرگ به سوی مجازی کردن سرورهای فیزیکی روی آوردند، به طور مثال شرکت CISCO بعضی از سیستم‌های خود را مجازی کرده مانند ASAv که همان ASA Virtual است و در همین کتاب هم پیاده‌سازی می‌شود از همین قبیل سیستم‌ها است.

چشم انداز تهدید امنیتی شبکه

تهدیدات امنیتی امروزه بسیار گسترده و پیچیده‌تر شده است، در این قسمت سعی کریدم در مورد انگیزه‌های مهاجمان برای حمله به شبکه، افرادی که مورد حمله قرار می‌گیرند و چگونگی جلوگیری از حملات صحبت کنیم.

انگیزه‌های مهاجمان برای حمله به شبکه شما چیست؟

- مالی (Financial): یکی از مهمترین دلایل اینکه مهاجمان به شبکه‌های مختلف حمله می‌کنند، این است که بتوانند از منابع مالی آن سازمان استفاده کنند، مانند هک کردن سایت‌های بانکی و به سرقت بردن اطلاعات هزاران کاربر و استراخ از آن.

- اختلال (Disruption): در اکثر موارد مهاجم فقط برای ایجاد اختلال در شبکه شروع به هک کردن سایت یا سرور مورد نظر می‌کند؛ که دلایل مختلفی هم دارد، مثلاً کاربر مورد نظر برای اینکه خود را مطرح کند شروع به هک کردن سایت می‌کند و با قرار دادن اطلاعات خود در صفحه سایت خود را مطرح می‌کند.

- ژئوپلیتیک (Geopolitical): در این نوع حملات که به جنگ سایبری معروف است، گروهی از هکرها به سرورها مهم یک کشور حمله می‌کنند تا آنها را از کار بیندازند.

بررسی حملات انکار سرویس

این نوع حملات با نام DOS (Denial-of-Service) و DDOS (Distributed Denial-of-Service) شناخته می‌شود که اصولاً برای از کار انداختن سرور یا سرورها به کار می‌رود، تلاش این نوع حملات برای از کار انداختن سرویس‌های تحت وب مانند هاستینگ و... است که با این کار سایت مورد حمله برای دقایقی یا برای همیشه از کار خواهد افتاد، تفاوت بین حمله DOS با DDOS این است که حمله DOS از طریق یک سیستم انجام می‌شود ولی حمله DDOS که به عنوان حمله توزیع شده شناخته می‌شود با استفاده از چندین سرور انجام می‌گیرد، با این کار روترها، سوئیچ‌ها و دیگر دستگاه‌ها متصل به شبکه با افزایش درخواست‌ها مواجه می‌شوند و همین موضوع باعث می‌شود کارایی CPU افزایش یابد و دستگاه از کار بیفتد.

روش‌های حمله:

۱- تداخل در ارتباط کاربران با شبکه.
۲- ریسیت کردن کانکشن‌های TCP در ارتباط‌ها.
۳- ایجاد تداخل در دستگاه‌های شبکه.
۴- ایجاد اختلال در وضعیت روترها مانند اطلاعات مسیریابی.
۵- مصرف حداکثری منابع مانند پهنای باند، دیسک و...

بررسی روش‌های مهندسی اجتماعی

یکی از بهترین راه‌های ایجاد نفوذ به شبکه سازمان استفاده از منابع انسانی آن است، در این نوع حملات هکرها با استفاده از روش‌هایی، اطلاعات مهم یک سازمان را از کاربران آن بدست می‌آورند، مانند جعل آدرس ایمیل، پنجره‌های Pop-Ip در وب‌سایت‌ها، ساخت وب‌سایت‌های جعلی و از همه مهمتر کلاهبرداری از طریق تلفن است.

چگونه باید در برابر این نوع حملات دفاع کرد:

۱- مدیریت کامل رمزهای عبور با استفاده از سیاست‌ها پیچیدگی رمز عبور و تاریخ انقضاء آن، البته نرم‌افزارهایی مانند ACS می‌توانند بسیار کمک کننده باشند، در مورد ACS در ادامه توضیح جامع خواهیم داد.

۲- استفاده از احراز هویت دوعاملی.

۳- استفاده از آنتی ویروس‌ها و ضدفیشینگ‌ها.

۴- طبقه‌بندی اطلاعات حساس و غیرحساس.

۵- محافظت از زباله‌های اداری که دو ریخته می‌شود.

۶- استفاده از نگهبانان امنیتی برای محافظت از سازمان.

روش های موجود برای شناسایی بدافزار

۱- Packet captures: برای شناسایی بدافزار باید جمع‌آوری، ذخیره و تجزیه و تحلیل بسته‌هایی که در شبکه در حال رد و بدل هستند را انجام دهید، البته به علت حجم بالای اطلاعات پیدا کردن آنها بسیار سخت خواهد بود.

۲- Snort: یک سیستم شناسایی هوشمند است که یک نرم‌افزار منبع باز بوده و توسط شرکت Sourcefire توسعه یافته است و اکنون بخشی از شرکت سیسکو است و در حال حاضر با نام (IPS , IDS) شناخته می‌شود، این سیستم برای جلوگیری از تهدیدات، شناسایی، اجرای سیاست‌های لازم و.... کاربر دارد.

۳- NetFlow: یکی از پروتکل‌های اختصاصی شرکت سیسکو است که آن را برای عیب‌یابی، مانیتورینگ و برای بدست آوردن داده‌های آماری ایجاد کرده است، یکی از مهمترین دلایل استفاده از این سیستم برای جلوگیری از حملاتی است که به شبکه شما انجام می‌شود.

۴- بررسی رویدادهای IPS: دستگاه‌های IPS برای شناسایی حملات کاربرد دارند و بسته‌های عبوری در شبکه را بررسی می‌کنند، از IPS برای ارتباط دو شبکه در دو نقطه مختلف می‌توان استفاده کرد تا Wormها و دیگر ابزارهای مخرب شناسایی شوند.

۵- حفاظت از بدافزار پیشرفته: در این بخش شرکت سیسکو AMP را طراحی کرده که در دستگاه‌های FirePOWER به کار گرفته شده است، این سیستم از نفوذ پیشگیری می‌کند و حتی فایل‌های درون شبکه را هم بررسی می‌کند تا در صورت وجود فایل‌های مخرب و تهدیدها آنها را شناسایی کند.

۶- سیستم جلوگیری از نفوذ نسل بعدی(Cisco FirePOWER (NGIPS : راه‌حل چند لایه محافظت پیشرفته در بازرسی را فراهم می‌کند که این محصول در دستگاه‌های ASA که در ادامه کار بررسی می‌کنیم ارائه می‌شود، در شکل زیر دستگاه فایروال NGIPS سیسکو را مشاهده می‌کنید.

فصل سوم – Network Foundation Protection

NFP یا Network Foundation Protection چارچوبی امنیتی است که توسط سیسکو طراحی شده است تا به طور منطقی کارکردهایی که در شبکه اتفاق می‌افتد را گروه‌بندی کند، در این چارچوب تعدادی از تکنیک‌ها و روش‌های ایمن‌سازی روترها و سوئیچ را با هم ترکیب کرده تا از حملات جلوگیری کنیم.

NFP شامل سه قسمت مجزا است که در زیر آنها را بررسی می‌کنیم:

Management plane

به پروتکل‌ها و ترافیک‌هایی که مدیر شبکه برای متصل شدن به دستگاه‌های شبکه ایجاد می‌کند را Management Plane گفته می‌شود که این ترافیک می‌تواند SSH یا Telnet باشد که مدیر شبکه می‌خواهد از راه دور به دستگاه‌های شبکه متصل شود، البته یک خرابی در Management Plane باعث می‌شود دیگر نتوانیم از راه دور به دستگاه‌ها دسترسی داشته باشیم، به خاطر همین حفظ امنیت آن بسیار مهم است.

Control plane

در این قسمت پروتکل‌های که بین دستگاه‌های شبکه ردو بدل می‌شود مورد بررسی قرار می‌گیرد مانند پیام‌های ARP یا ارسال لیست همسایگی در روترها که برای بروزرسانی روترهای مسیریابی استفاده می‌شود اگر خطا یا اتفاقی در این گروه اتفاق بیفتد دستگاه‌ها توانایی به اشتراک گذاشتن و یادگیری را از دست خواهند داد.

Data plane

به ترافیکی اشاره دارد که توسط کاربر نهایی ایجاد شده است، مثلاً ترافیکی کاربری که یک صفحه را در حال مشاهده است.

وابستگی متقابل

توجه داشته باشید که این سه قسمت با هم در ارتباط هستند، مثلاً اگر در قسمت Control plane خرابی ایجاد شود و ارتباط بین روترها قطع شود مطمئناً در قسمت Data plane ارتباط کاربر با سرور یا وب سایت مورد نظر قطع خواهد شد.

در جدول زیر اقدامات امنیتی را که می‌توانیم در هر سه گروه انجام دهیم را مشاهده می‌کنید:

نام Plane	تمهیدات امنیتی	اهداف حفاظت
Management plane	Authentication, authorization, accounting (AAA)	محافظت از پروتکل NTP با استفاده از Authentication، استفاده از پروتکل‌های رمز نگاری شده SSH / TLS برای ارتباط از راه دور و ...
	Authenticated Network Time Protocol (NTP)	
	Secure Shell (SSH)	
	Secure Sockets Layer/Transport Layer Security (SSL/TLS)	
	Protected syslog	
	Simple Network Management Protocol Version 3 (SNMPv3)	
	Parser views	
Control Plane	Control Plane Policing (CoPP)	به روزرسانی پروتکل‌های مسیریابی و استفاده از Authentication در آن، که این کار باعث می‌شود مهاجم نتواند جدول مسیریابی را دستیابی کند
	Control Plane Protection (CPPr)	
	Authenticated routing protocol updates	
Data plane	Access control lists (ACL)	استفاده از Access List برای محدود کردن ترافیک به ترافیک‌های خاص، استفاده از سیستم‌های شناسایی IPS و به کارگیری zone-base Firewall و ایجاد امنیت در پروتکل STP
	IOS IPS, zone-based firewall	
	Layer 2 controls, such as private VLANs, Spanning Tree Protocol (STP) guards	

در ادامه کار هر سه قسمت DATA plane، Management Plane و Control plane را به طور کامل با هم بررسی می‌کنیم تا دقیقاً اجزا و نحوه کانفیگ انها مشخص شود.

کار با Management plane

در این قسمت می‌خواهیم به تنظیمات اولیه دستگاه‌های شبکه از دید امنیت بپردازیم، هر دستگاه شبکه‌ای که خریداری می‌شود تنظیمات آن به صورت خام و بدون دستکاری افراد دیگر در دسترس مدیر شبکه قرار می‌گیرد و باید بر روی آن راه‌کارهای امنیتی را برای امن نگه داشتن آن پیاده‌سازی کنیم.

طبق آموزش‌های که در کتاب CCNA بنده مطالعه کردید زمانی که یک روتر یا یک سوئیچ سیسکو را تهیه می‌کنید همراه آن یک کابل آبی رنگ که به عنوان کابل کنسول شناخته می‌شود قرار دارد و از طریق آن می‌توانید به دستگاه خود متصل شوید و تنظیمات اولیه آن را انجام دهید ولی اگر توجه کرده باشید هیچ گونه نام کاربری و رمز عبوری از شما درخواست نمی‌شود، اصولاً زمانی که به روتر متصل می‌شوید یک آدرس IP برای آن در نظر میگیرید و بعد از آن یکی از سرویس‌های Telnet و SSH را برای راحتی کار بر روی آن فعال می‌کنید، فعال کردن این نوع سرویس‌ها نیازمند این است که بستر امنیت را در روتر فراهم کنید.

روش‌هایی برای حفظ Managemant Plane

در این قسمت برای اینکه در بخش Managemant Plane بتوانید امنیت اطلاعات را افزایش دهید روش‌هایی را برای بالا بردن امنیت بررسی می‌کنیم:

- **استفاده از رمز عبور قدرتمند**

بدست آورن رمز عبور پیچیده و قدرتمند بسیار سخت است و حدس زدن ان هم آسان نخواهد بود، اصولاً مهاجمان با استفاده از دیکشنری از رمزهای عبور سعی در شکستن قفل دستگاه می‌کنند که اگر چنانچه رمز عبور را ساده قرار دهید مثلاً ۱۲۳٤٥٦ این نوع رمزها به راحتی هک خواهد شد و به خاطر همین همیشه سعی کنید از رمز عبور پیچیده استفاده کنید، روش دیگر حمله به رمز عبور را می‌توان از brute-force هم نام برد که در ادامه کتاب درباره آن صحبت خواهیم کرد.

- **تایید اعتبار کاربر و استفاده از AAA**

برای اینکه امنیت افزایش پیدا کند باید به کاربران سازمان خود یک نام کاربری به همراه رمز عبور اختصاص دهید تا مهاجم برای وورد به دردسر بیفتد، توجه داشته باشید سیستم AAA یا authentication, authorization, and accounting که در ادامه در باره آن بحث خواهیم کرد بسیار می‌تواند در این مورد به

شما کمک کند تا بتوانید تسلط کاملی بر روی کاربران و مجوزهایی که برای آنها صادر می‌کنید داشته باشید.

- **تلاش برای وورد به سیستم**

شما به عنوان مدیر شبکه باید سیساست‌هایی را در قبال کاربرانی که برای وورد به سیستم تلاش می‌کنند داشته باشید، مثلاً باید یک زمانی را در سیستم AAA مشخص کنید که وقتی کاربری با نام کاربری و رمز عبور خود وارد شد و بعد از یک مدت مشخص در پشت سیستم خود قرار نداشت بهتر است آن حساب Logout شود تا با این کار از دستکاری غیر مجاز با آن نام کاربری جلوگیری شود و ی اینکه اگر کسی برای ورود بیشتر از سه بار تلاش کرد ان حساب مسدود شود.

- **کنترل مجوز دسترسی یا RBAC**

همه‌ی مدیران نیاز به دسترسی کامل به همه بخش‌های شبکه را ندارند و باید از طریق سیستم AAA سطح دسترسی آنها را محدود کرد، مثلاً مدیر مالی نیاز به دسترسی به اطلاعات سایر واحدها ندارد پس نباید یک دسترسی کامل برای آن صادر کرد.

- **استفاده از پروتکل‌های مدیریتی رمزنگاری شده**

برای ارتباط کاربران با دستگاه‌های شبکه بهتر است از پروتکل‌های قدرتمند رمزنگاری شده مانند HTTPS و SSH استفاده کرد تا مهاجمان نتوانند با گوش دادن به پیام‌ها به اطلاعات دست پیدا کنند، اگر شما برای دستگاه‌های خود از پروتکل‌های plaintext مانند HTTP یا Telnet استفاده کنید مهاجمان به راحتی می‌توانند به اطلاعات حساس شما دست پیدا کنند البته اگر بخواهید از این دو پروتکل اسفاده کنید سعی کنید یک ارتباط VPN قبل از آن راه‌اندازی کنید تا تمام بسته‌ها رمزنگاری شوند، پس همیشه به این نکته توجه کنید که از بهترین پروتکل‌های رمزنگاری استفاده کنید.

- **ورود به سیستم و نظارت بر روی آن**

در هر شبکه‌ای اگر نظارت بر روی عملکرد دستگاه‌ها و کاربران وجود نداشته باشد، می‌تواند بسیار خطرناک باشد، اگر مهاجمی در تلاش برای نفوذ به دستگاه‌های شبکه شما باشد و شما هم خبری از آن نداشته باشد کمی نگران کننده خواهد بود، بهترین راه برای حل این نوع مشکلات استفاده از سیستم مانیتوریگ بر روی همه دستگاه‌ها و کاربران شبکه است که در این کتاب هم نحوه ایجاد گزارش و ارسال آن به سرورهای Syslog را با هم می‌آموزیم.

- **استفاده از سرویس Network Time Protocol**

در یک شبکه باید تمام دستگاه‌های شبکه دارای یک ساعت مشخص باشند تا زمانی که رویدادی در هر دستگاه ایجاد و به سرور مانیتوریگ ارسال می‌شود دارای زمان و تاریخ درست باشد، این مورد با استفاده از سرویس NTP انجام خواهد شد که باید در سرور مادر راه‌اندازی شود.

توصیه‌هایی برای استفاده از کلمه عبور

- همیشه سعی کنید کلمه عبوری را که برای کاربران در نظر می‌گیرید حداقل دارای هشت کاراکتر باشد.
- کلمه عبور می‌تواند شامل حروف الفبا، ترکیبی از حروف بزرگ و کوچک، نمادها و فضاها باشد، اگر از چنین پسورد پیچیده‌ای در شبکه خود استفاده کنید کار مهاجم برای نفوذ بسیار سخت خواهد بود، استفاده از فضای خالی یا Space در کلمه عبور بسیار می‌تواند کمک کننده باشد.

نکته مهم در استفاده از کمه عبور این است که با اینکه رمز عبور را به صورت پیچیده در نظر میگیرید ولی باید در یک دوره‌ی زمانی مشخص آن را تغییر دهید.

استفاده از AAA برای تأیید کاربران

برای اینکه دسترسی غیر مجاز به شبکه گرفته شود و کاربرانی که اجازه‌ی دسترسی به شبکه را دارند مشخص شوند بهترین راه استفاده از سیستم AAA یا authentication, authorization, and accounting است که در فصل چهارم به طور کامل درباره آن توضیح خواهیم داد.

هدف اصلی AAA این است که چه کسی به چه جایی باید دسترسی داشته باشد و عملکرد آن به چه صورت بوده است یعنی اینکه چه کاربری در چه زمانی وارد شبکه شده است و چه کاری انجام داده است.

حساب‌های کاربری که در AAA ثبت می‌شوند می‌توانند به صورت محلی باشند و یا اینکه از طریق سرویس Active Directory انجام گیرد.

احراز هویت (Authentication)

احراز هویت فرایندی است که توسط آن مشخص می‌شود یک فرد همان کاربر مورد نظر است، برای احراز هویت روش‌های مختلفی وجود دارد که می‌توان به نام کاربری و رمز عبور، کارت‌های هوشمند و... اشاره کرد، معمولاً استفاده از Authenticaion می‌تواند برای دسترسی به کنسول روتر، پورت VTY، Auxiliary و... اشاره کرد.

مجوز دسترسی (Authorization)

در این قسمت بعد از اینکه کاربر مورد نظر از نظر احراز هویت بررسی شد و توانست وارد دستگاه مورد نظر شود باید مجورهای لازم را برای دسترسی به منابع شبکه برای ان تایین کنید، مثلاً می‌توانید مشخص کنید کاربر در یک ساعت مشخص بتواند وارد شبکه شود و یا اینکه برای مدیران مشخص کنید که چه چیزی را می‌توانند ببینند و تغییر دهند.

حسابداری و حسابرسی (Accounting and auditing)

کاربر بعد از انجام دو مرحله بالا شروع به کار در شبکه می‌کند و به مسیرهای مختلفی وارد و عملیات خود را انجام می‌دهد، برای اینکه متوجه شویم کاربر به چه مسیری رفته و چه کاری در چه زمانی انجام داده باشد این سرویس را برای آن فعال کنیم، یکی از سیستم‌های حسابرسی می‌توان به عملیات بانکی اشاره کرد که در ان مقدار پول دریافتی و جزئیات آن به صورت دقیق مشخص شده است.

توجه داشته باشید برای اینکه با سرور AAA ارتباط برقرار کنیم باید از پروتکل‌های خاصی استفاده کنیم که این پروتکل‌ها شامل TACACS+ و RADIUS هستند، پروتکل TACACS+ مختص شرکت سیسکو و دیگری عمومی و در همه دستگاه‌ها اجرا می‌شود، در ادامه برای انجام و پیاده‌سازی این نوع پروتکل‌ها از نرم‌افزار ACS استفاده خواهیم کرد و نحوه کار با آن را می‌آموزیم.

در ادامه کار می‌خواهیم روش‌هایی را برای امن نگه داشتن دستگاه‌های سیسکو انجام دهیم تا از دسترسی افراد غیر مجاز به آنها جلوگیری کنیم.

پیاده‌سازی رمز عبور قوی و پیچیده

قبل از اقدام به هر کاری توجه داشته باشید که در این کتاب از نرم‌افزار مجازی‌سازی GNS3 استفاده شده که در فصل چهارم آن را به صورت کامل نصب و راه‌اندازی کردیم و از آن در کل کتاب استفاده خواهیم کرد.

روش‌های دسترسی و رمزگذاری

برای دسترسی به روتر چندین روش وجود دارد که هرکدام را مورد بررسی قرار می‌دهیم:

پورت Console

این همان پورتی است که از طریق کابل Console (آبی رنگ) به روتر متصل می‌شویم و برای متصل شدن به یک روتر خام به کار می‌رود که هیچ‌گونه تنظیماتی روی آن انجام نشده است، برای رمزنگاری این پورت، باید کارهای زیر را انجام دهیم.

وارد مد global شوید و با دستور Line console 0، وارد پورت کنسول شوید. مانند زیر عمل کنید:

```
R1(config)#line console ?
  <0-0>  First Line number
```

اصولاً روی روترها، یک پورت کنسول وجود دارد که شماره‌ی آن صفر است و می‌خواهیم روی این پورت رمز عبور قوی قرار دهیم، باید به صورت زیر عمل کنیم.

```
R1(config-line)#password AB_@@_@@ba
```

برای این کار، از دستور Password و بعدازآن، از یک کلمه‌ی عبور پیچیده، مانند AB_@@_@@BA استفاده می‌کنیم، همانطور که مشاهده می‌کنید رمز عبوری که برای این منظور در نظر گرفتیم دارای حروف بزرگ و کوچک و علامت اختصاری است.

بعدازاین که رمز را وارد و enter کردیم باید از دستور login استفاده کنیم تا زمانی که می‌خواهیم وارد تنظیمات روتر شویم از ما رمز عبور پرسیده شود، پس به این صورت این دستور را وارد می‌کنیم:

R1(config-line)#**login**

تذکر: اگر شما دستور Login را وارد نکنید، هر رمزی را هم روی روتر فعال کنید، باز برای ورود از شما رمز عبور درخواست نمی‌شود، پس به این نکته توجه کنید.

در حال حاضر با واردکردن این دستورات، روی روتر رمز قرار دادیم و زمانی‌که می‌خواهیم از طریق کابل Console وارد User Mode شویم، از شما رمز درخواست می‌شود.

دستور exec-timeout

زمانی‌که وارد یک مد می‌شوید، اگر مدت‌زمانی با روتر کار نکنید، در هر مدی که هستید، خارج شده و به مد اول، یعنی UserMode برگشت می‌کند، برای جلوگیری از این کار، باید از دستور زیر در پورت consol استفاده کنید، البته پیشنهاد می‌شود برای حفظ امنیت یک زمان مناسب برای آن در نظر بگیرید.

Router(config-line)#**exec-timeout 0 0**

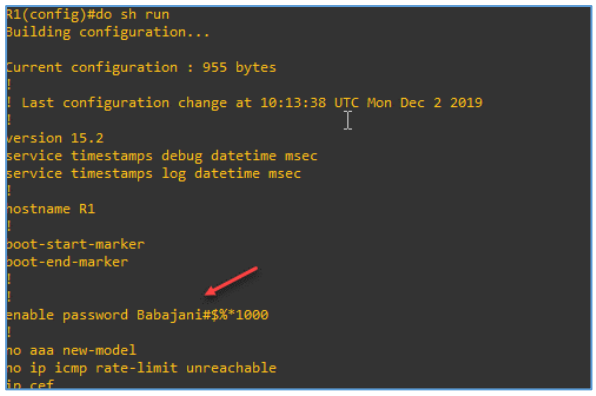
همان‌طور که مشاهده می‌کنید، در این دستور از دو صفر استفاده شده است که اولی برای دقیقه و دومی برای ثانیه است، با صفر کردن هر دو اگر در هر مدی باشید در همان مد ثابت خواهد ماند و خارج نمی‌شود، البته می‌توانید هر زمان که خودتان دوست دارید وارد کنید.

Enable Password

این رمز برای Privileged Mode است. اگر کاربری بخواهد وارد این مد شود از وی پسورد درخواست می‌شود. برای فعال کردن آن، وارد مد Global می‌شویم و دستور زیر را تایپ و بعد enter می‌کنیم.

Router(config)#**enable password Babajani#$%*1000**

رمزهای عبوری که با دستور Enable Password فعال می‌شوند، زیاد نمی‌توانند امن باشند، چون این رمزها به صورت Text Base بوده و با یک فرمان می‌توانید رمز عبور را به دست آورید. برای دیدن رمز عبور از دستور Show Runing-config استفاده کنید، می‌خواهیم با این دستور به شما نشان دهیم که دستور Enable Password زیاد هم امن نیست، این دستور را در مد Privileged وارد کنید.



همان‌طور که مشاهده می‌کنید با واردکردن دستور Show Running-config، رمز عبور واردشده، نمایش داده شد، پس باید کاری کرد که این رمز به صورت Hashing یا کد شده در این قسمت نمایش داده شود تا کسی نتواند این رمز را مشاهده کند .

اول از همه، رمز قبلی را که وارد کردیم، حذف می‌کنیم.

برای حذف هر دستوری که وارد کردیم، باید قبل از آن دستور، از کلمه‌ی No استفاده کنیم تا دستور مورد نظر حذف شود، برای این کار از دستور No enable password استفاده می‌کنیم، بعد از این کار، از دستور enable Secret AB_@@_@@ba استفاده می‌کنیم که رمز عبور را به صورت کد شده درمی‌آورد و برای شما نمایش می‌دهد، بعد از این کار در مد Privileged دستور show Running-config را اجرا کنید، متوجه می‌شوید که رمز عبور password AB_@@_@@ba به صورت کد شده درآمده، مانند رمز زیر:

enable secret 5 1mERr$3HhIgMGBA/9qNmgzccuxv0

تذکر: زمانی‌که Enable Secret فعال است، Enabel Password روی روتر کاربردی ندارد و اگر هر دو دستور را در یک‌زمان فعال کنید، فقط رمز عبوری که با دستور Enable Secret فعال کردیم، جواب می‌دهد.

اگر بخواهید از Password استفاده کنید و رمز آن هم به صورت Hash شده تغییر کند باید از دستور زیر در روتر استفاده کنید:

R1(config)# **service password-encryption**

پورت AUX

این پورت برای ارتباط از راه دور از طریق خط تلفن با روتر استفاده می‌شود که می‌توانیم به روش زیر فعال کنیم و یک رمز عبور پیچیده برای آن در نظر بگیرید.

R1(config)#Line aux 0

R1 (config-line)#password 123

R1 (config-line)#login

این رمز عبور قبل از وارد شدن به User Mode پرسیده می‌شود.

Telnet

برای فعال کردن Telnet باید پورت‌های مجازی Vty را فعال کنیم. Vty مخفف Virtual terminal که از چندین پورت مجازی برای ورود به روتر استفاده می‌کند، مثلاً در روتر ۲۹۱۱ از ۱۵ پورت تشکیل شده است. برای مشاهده این پورت‌ها در مد Global دستور زیر را وارد کنید:

R1(config)#**line vty ?**

<0-15> First Line number

با واردکردن دستور Line Vty و بعدازآن، علامت سؤال به ما تعداد پورت‌های مجازی برای این روتر را نشان می‌دهد که ۱۵ عدد استکه البته در روترهای جدید بسیار بالا است. شما می‌توانید تمام این ۱۵ پورت را فعال کنید که با این کار ۱۵ نفر در یک‌زمان می‌توانند وارد روتر یا سوئیچ شوند.

در اینجا تمام این ۱۵ پورت را انتخاب و همه‌ی آن‌ها را فعال می‌کنیم، و روی همه آن‌ها رمز قرار می‌دهیم:

R1(config)#**line vty 0 15**

R1(config-line)#**pass ###$$$2741652ABCDfVGjjj**

R1(config-line)#**login local**

در قسمت سوم از دستور Login استفاده کردیم که با این دستور به روتر اعلام می‌کنیم که در زمان Telnet رمز عبور را درخواست کن. اگر به جای Login از دستور No Login استفاده کنید، روتر هیچ‌گونه رمزی درخواست نخواهد کرد، پس مواظب این دستور باشید. شما می‌توانید به چند پورت اجازه دسترسی بدهید و به بقیه‌ی پورت‌ها اجازه دسترسی ندهید.

برای تعریف نام کاربری و رمز عبور باید از دستور زیر استفاده کرد، همانطور که مشاهده می‌کنید رمز عبور هم به صورت پیچیده وارد شده و هم نوع آن را Secret در نظر گرفتیم که Secret به این معنا است که رمز عبور شما به صورت Hash شده در Config قابل مشاهده است و کسی نمی‌تواند این رمز عبور را تشخیص دهد.

R1(config)#username babajani secret AB_@@_@@BA

برای اینکه رمز عبور را در Config مشاهده کنیم باید از دستور زیر استفاده کنیم که نتیجه آن هم مشخص است.

R1(config)#**do show run | include username**

username babajani secret 5 1.08t$t9W8awy7EEzk.Zk89.DDn/

با دستور زی می‌توانیم تنظیماتی که برای پورت‌های مورد نظر انجام دادیم را مشاهده کنید.

```
R1(config-line)#do show run | begin line
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 08006E7129393A3732292D
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 password 7 107D08140419110F2C567A7A71
 logging synchronous
 login
 stopbits 1
line vty 0 4
 password 7 03247B2B454C620F0D4A5A4653564F48
 login
line vty 5 15
 password 7 03247B2B454C620F0D4A5A4653564F48
 login
```

ایجاد سطح امتیاز سفارشی برای کاربران

شما می‌توانید به صورت دستی و نه به کمک AAA برای کاربرن خود دسترسی سفارشی ایجاد کنید، به صورت پیش فرض اگر کاربری در User Mode باشد سطح آن یک است و اگر در privileged mode سطح آن پانزده است و شما می‌توانید از یک تا پانزده برای کاربران دسترسی تعریف کنید.

برای تست این موضوع می‌خواهیم دوکاربر ایجاد کنیم که سطح دسترسی آنها متفاوت باشد و مشخص کنیم که آن سطح مورد نظر به چه دستوری دسترسی داشته باشد.

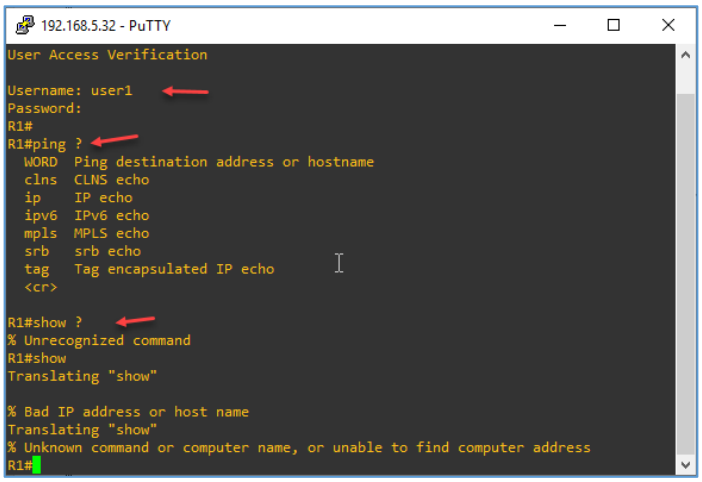
برای تست این موضوع در روتر یا سوئیچ دستورات زیر را وارد کنید، در این دستور دو کاربر با سطح دسترسی 9 و 8 ایجاد شده است.

```
R1(config)#username user1 privilege 8 secret Test@12345
R1(config)#username user2 privilege 9 secret Test@12345
```

بعد از انجام این کار باید مشخص کنیم که در سطح مورد نظر چه دستوری اجازه اجرا را دارد، در دستور زیر مشخص شده است که دستور PING از از سطح ۸ به بعد توانایی اجرا را دارد و دستور Show که خیلی دستور مهمی است از سطح ۹ به بعد، یعنی اگر User1 وارد روتر شود نباید دستور Show را اجرا کند چون در سطح ۹ قرار ندارد.

```
R1(config)#privilege exec level 8 ping
R1(config)#privilege exec level 9 show
```

نکته: توجه داشته باشید برای تست این موضوع باید سرویس Telnet را فعال کنید.



همانطور که مشاهده می‌کنید با کاربر User1 به روتر R1 متصل شدیم، اگر دستور Ping را اجرا کنید بدون مشکل اجرا خواهد شد ولی اما اگر دستور Show که مربوط به سطح ۹ بود را در سطح ۸ اجرا کنید نتیجه‌ای در بر ندارد، از این روش می‌توانید یک سری محدودیت برای سطح‌های مختلف ایجاد کنید.

روش دیگری هم برای فعال‌سازی سطح مورد نظر وجود دارد و آن هم این است که برای آن سطح یک رمز عبور قرار دهیم که دستور آن به صورت زیر است:

R1(config)#**enable secret level 8 Test@12345**

R1(config)#**enable secret level 9 Test@123456**

بعد از تعریف دستور بالا در مد User دستور زیر را وارد کنید، در این دستور به جای ۹ باید سطح مورد نظر خود را وارد کنید و رمز عبوری را که در مرحله قبل ایجاد کردید را وارد کنید.

R1#**enable 9**

Password:

R1#

برای اینکه سطح دسترسی کاربر مورد نظر را به صورت آنلاین مشاهده کنید باید از این دستور استفاده کنید:

R1#**show privilege**

Current privilege level is 9

فعال سازی سرویس SSH و HTTPS

برای فعال سازی پروتکل امن SSH در روتر و سوئیچ سیسکو باید به صورت زیر دستورات را وارد کنید.

در اولین دستور باید یک نام دومین برای روتر خود مشخص کنید، که بهتر است این نام همان نام دومین مورد نظر شما در شبکه داخلی باشد.

R1(config)#ip domain-name 3isco.ir

در ادامه باید یک دسته کلید ایجاد کنید تا زمانی که کلاینت درخواست اتصال می‌دهد این دسته کلید برای آن فعال شود.

R1(config)#crypto key generate rsa

The name for the keys will be: R1.3isco.ir

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

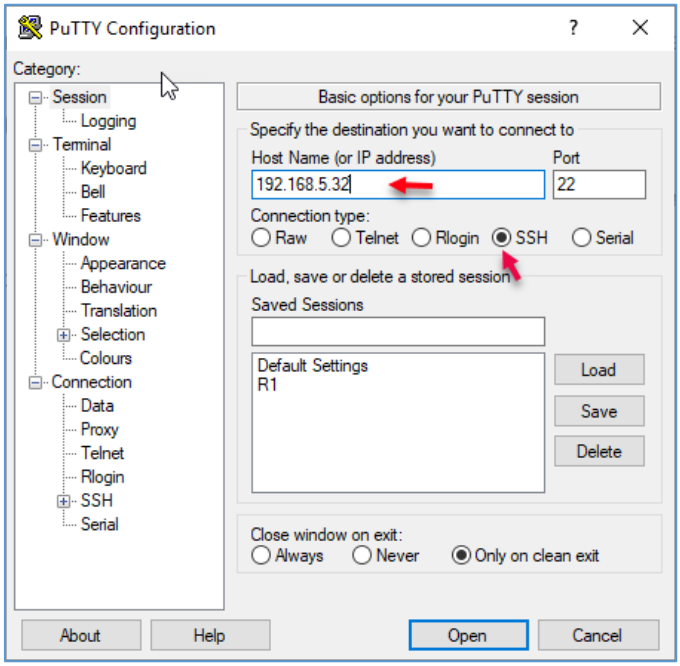
a few minutes.

در این قسمت باید اندازه دسته کلید را مشخص کنید که بهتر است از ۱۰۲٤ استفاده کنید.

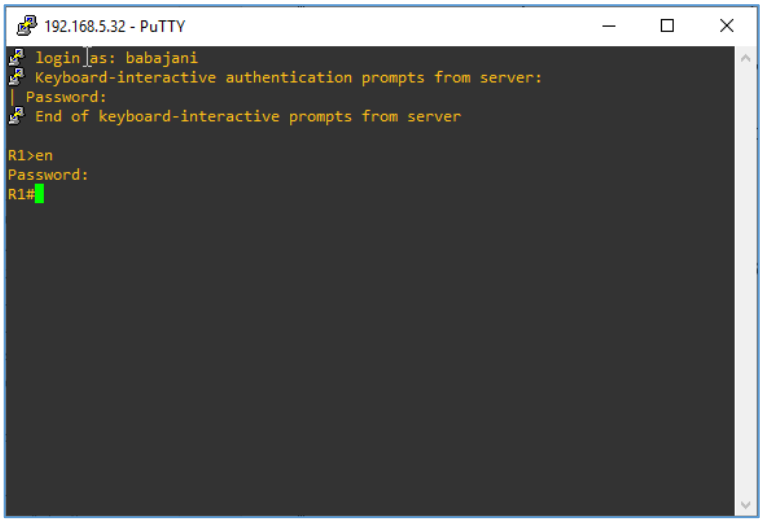
```
How many bits in the modulus [512]: 1024

.Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 2 seconds)
```

در آخر هم یک نام کاربری و رمز عبور برای ورود در نظر می‌گیریم.

```
R1(config)#username babajani secret test@2015
```



با استفاده از نرم‌افزار Putty یا با استفاده از دستور SSH به روتر یا سوئیچ مورد نظر خود از طریق متصل می‌شویم، توجه داشته باشید که در زمان متصل شدن به دستگاه یک دسته کلید مخصوص سیستم شما ایجاد می‌شود که باید بر روی Yes کلیک کنید.



همانطور که مشاهده می‌کنید، از طریق کاربری که ایجاد کردیم توانستیم وارد دستگاه مورد نظر شویم.

به این نکته توجه کنید که Enable Secret را هم باید قبل از این کار فعال کنید.

برای فعال‌سازی سرویس HTTPS هم باید از دستور زیر استفاده کنید:

دستور زیر پروتکل HTTPs را فعال می‌کند.

```
R1(config)#ip http secure-server
٪Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
```

دستور زیر هم دسترسی لازم به روتر را از طریق وب صادر می‌کند.

```
R1(config)#ip http authentication local
```

بررسی Parser View

یکی دیگر از روش‌های اختصاص دستورات به کاربران این است که یک View ایجاد کنیم و دستورات را به آن view اختصاص دهیم و کاربران هم با عضو شدن در آن View می‌توانند از دستورات آن view استفاده کنند و دسترسی لازم را داشته باشند، این روش به نسبت روش قبلی قویتر و بهتر خواهد بود.

اولین کاری که باید انجام دهید این است که بت دستور enable secret یک رمز عبور برای روتر یا سوئیچ خود قرار دهید.

```
R1(config)#enable secret Test@12345
```

در مرحله بعد باید سرویس AAA را با دستور زیر فعال کنیم، در مورد این دستور به صورت کامل در فصل بعد بحث کردیم.

```
R1(config)#aaa new-model
```

وارد مد User شوید و دستور enable view را وارد و رمز عبور مشخص شده را وارد کنید:

```
R1#enable view
Password:
```

بعد از وارد کردن رمز عبور و فشار بر روی Enter شما وارد View Root خواهید شد.

بعد از وارد شدن به view root باید یک view جدید با نام مشخص ایجاد کنیم که دستور آن به صورت زیر است:

R1(config)#**parser view V1**

بعد از وارد شدن اگر یک علامت سوال در جلوی خط قرار دهید و اجرا کنید دستوراتی را که می‌توانیم در view استفاده کنیم را در زیر مشاهده می‌کنید:

R1(config-view)#**?**

View commands:

commands Configure commands for a view

default Set a command to its defaults

exit Exit from view configuration mode

no Negate a command or set its defaults

secret Set a secret for the current view

اولین کاری که باید انجام دهید این است که یک رمز عبور برای View V1 اختصاص دهیم:

R1(config-view)#**secret Test@12345**

بعد از قرار دادن رمز باید با دستور Commands دستوراتی که می‌خواهیم مجوز اجرا را داشته باشند را فعال کنیم، در زیر سه دستور Ping، Show و Configure Terminal مجوز اجرا در VIEW V1 را دارند:

R1(config-view)#**commands exec include ping**

R1(config-view)#**commands exec include show**

R1(config-view)#**commands exec include configure Terminal**

بعد از اجام دستورات بالا حالا می‌توانیم با دستور زیر وارد View V1 شویم:

R1#**enable view V1**

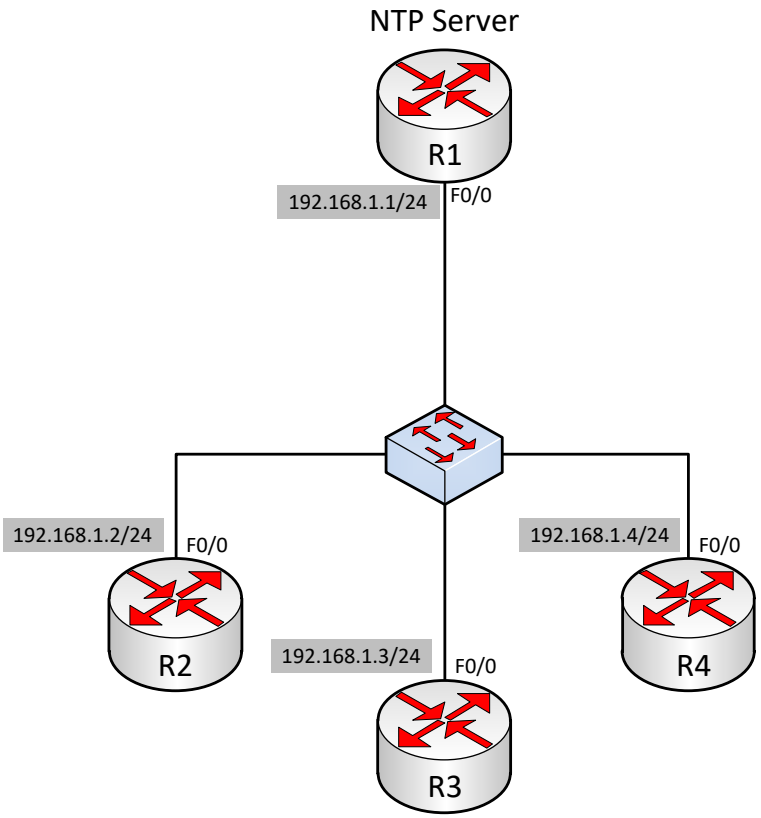
Password:

بعد از وارد کردن رمز وارد View مورد نظر یعنی v1 می‌شوید و اگر از علامت سوال استفاده کنید متوجه خواهید شد چه دستوراتی به لیست اضافه شده است:

```
R1#?

Exec commands:

  configure  Enter configuration mode
  do-exec    Mode-independent "do-exec" prefix support
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  ping       Send echo messages
  show       Show running system information
```

فعال‌سازی سرویس NTP

از آنجا که زمان یک فاکتور بسیار مهم در شبکه است و باید تمام اتفاقاتی که در آن روی می‌دهد باید در زمان و تاریخ مشخص در سیستم ثبت شود به خاطر همین از سرویس NTP برای مشخص کردن زمان دستگاه‌ها استفاده می‌کنیم، با یک مثال این پروتکل را بررسی می‌کنیم:



در این مثال، R1 به عنوان سرور NTP در نظر می‌گیریم و به بقیه‌ی روترها باید از روتر R1، تنظیمات ساعت و تاریخ را دریافت کنند.

وارد روتر R1 شوید و دستورات زیر را وارد کنید:

R1#**clock set 10:15:00 22 nov 2013**

R1#**configure t**

R1#**configure terminal**

R1(config)#**ntp master 1**

R1(config)#**ntp authentication-key 1 md5 saman 123**

در قسمت اول، ساعت و تاریخ روتر را تنظیم کردیم و بعد وارد مد Global شدیم و دستور Ntp Master 1 را وارد کردیم که با این دستور، این روتر را به عنوان روتر سرور برای پروتکل NTP در نظر می‌گیریم. عدد ۱ که در انتهای دستور مشاهده می‌کنید، می‌تواند از ۱ تا ۱۵ و برای مشخص کردن Master مورد نظر باشد و بعدازآن، یک کلید امنیتی تعریف می‌کنیم تا کسی بدون اجازه، زیرمجموعه این سرور نشود.

بعد از مشخص کردن سرور NTP، باید وارد روترهای دیگر شویم و روتر R1 را به عنوان روتر NTP به روترهای دیگر معرفی کنیم:

در روترهای R2,R3,R4 دستورات زیر را وارد کنید:

R5(config)#ntp server 192.168.1.1

R5(config)#ntp authentication-key 1 md5 saman 123

با این دستور، روترها تنظیمات ساعت و تاریخ خود را از سرور، یعنی R1 دریافت می‌کنند. برای مشاهده‌ی این موضوع از دستور زیر استفاده می‌کنیم:

R2#show ntp status

Clock is synchronized, stratum 2, reference is 192.168.1.1

nominal freq is 250.0000 Hz, actual freq is 250.0003 Hz, precision is 2**18

reference time is D639AF96.2C66330A (10:25:26.173 UTC Fri Nov 22 2013)

clock offset is 12.7890 msec, root delay is 43.90 msec

root dispersion is 902.04 msec, peer dispersion is 889.22 msec

همان‌طور که مشاهده می‌کنید، وارد روتر R2 شدیم و از دستور **show ntp status** استفاده کردیم که به ما تاریخ و ساعت مورد نظر را نمایش داد.

فعال‌سازی پروتکل SCP

پروتکل انتقال امن یا همتن SCP که مخفف کلمه Secure Copy Protocol است، روشی است برای انتقال امن فایل‌ها در شبکه این پروتکل از طریق سرویس SSH فایل‌ها را به صورت امن انتقال می‌دهد.

با دستور زیر می‌توانید این پروتکل را بر روی دستگاه‌های خود فعال کنید.

R1# **configure terminal**

R1(config)# **ip scp server enable**

R1(config)# **exit**

توجه داشته باشید که برای استفاده از SCP حتماً باید پروتکل AAA را قبل از آن فعال کنید، در مورد پروتکل AAA در فصل بعد به صورت کامل توضیح دادیم.

فعال‌سازی سرویس SNMP

سرویس SNMP یا همان Simple Network Management Protocol یک پروتکل برای مدیریت بر عملکرد دستگاه‌های شبکه، سرورها و... است، نسخه‌های SNMP از 1 تا 3 وجود دارد، که نسخه‌ی ۳ آن بیشترین امنیت را دارد.

سرویس SNMPv3 دارای سه نوع مدل امنیتی است که در جدول زیر مدل و سطوح امنیتی آن را مشاهده می‌کنید.

سطح	احراز هویت	رمزگذاری	نتیجه کار
noAuthNoPriv	نام کاربری	ندارد	فقط از طریق وارد کردن نام کاربری می‌توانید به اطلاعات دست پیدا کنید که این موضوع بسیار می‌تواند خطرناک باشد.

authNoPriv	الگوریتم MD5 و SHA	No	بر اساس الگوریتم‌های احراز هویت MD5 و SHA تایید اعتبار را ارائه می‌دهد.
authPriv	الگوریتم MD5 و SHA	Data Encryption Standard (DES)	بر اساس الگوریتم‌های احراز هویت MD5 و SHA تایید اعتبار را انجام می‌دهد و علاوه بر این رمزنگاری DES 56 bit را بر اساس استانداردهای CBC-DES و DES-56 ارائه می‌دهد.

برای فعال کردن پروتکل SNMP V3 باید به صورت زیر عمل کنید:

در دستور زیر کلمه 3isco به عنوان گروه معرفی شده است و V3 هم به این معنا است که ورژن snmp استفاده شده برای تنظیم ۳ است در ادامه دستور priv را وارد کنید و اگر بعد از آن از علامت سوال استفاده کنید گزینه‌های مختلفی را مشاهده می‌کنید که هر کدام برای مشاهده حالت خاصی از اطلاعات است، مثلاً گزینه‌ی read برای مشاهده اطلاعات است و نمی‌توانید اطلاعات را تغییر بدهید.

توجه داشته باشد اگر هیچ کدام از گزینه‌ها را انتخاب نکنید به این معنا است که تمام اطلاعات قایل مشاهده است.

```
SW4(config)# snmp-server group 3isco v3 priv?
  access  specify an access-list associated with this group
  context  specify a context to associate these views for the group
  match   context name match criteria
  notify  specify a notify view for the group
  read    specify a read view for the group
```

write specify a write view for the group

پس دستور نهایی به صورت زیر است:

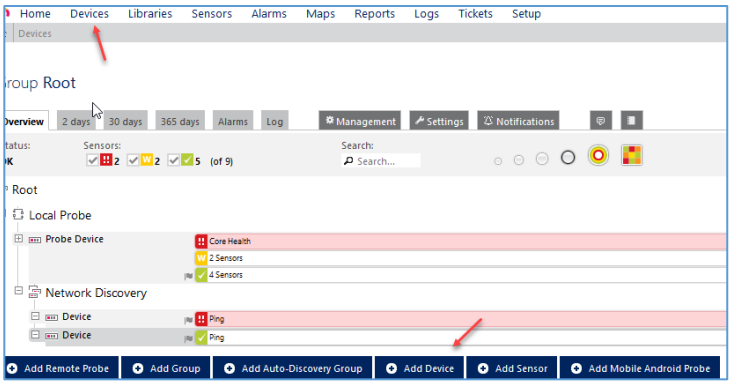
SW4(config)# snmp-server group 3isco v3 priv

دستور نهایی هم به صورت زیر وارد کنید:

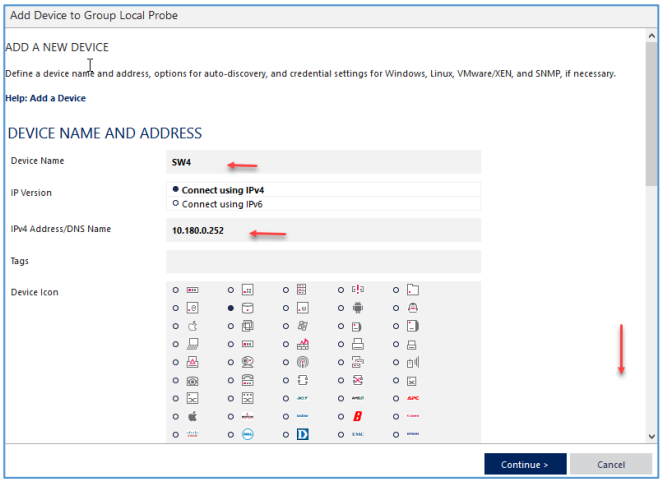
در این دستور یک نام کاربری با عنوان **snmp_user** وارد کنید و به گروهی را که در مرحله قبل اسجاد کردید در این قسمت وارد کنید بعد از آن باید دو پروتکل برای احراز هویت و کد کردن اطلاعات وارد کنید و رمز عبور آنها را وارد کنید، مثلاً در دستور زیر رمز **Test@12345** برای پروتکل **MDP** و رمز **12345@Test** برای پروتکل **des** است.

SW4(config)# snmp-server user User1 3isco v3 auth md5 Test@12345 priv des 12345@Test

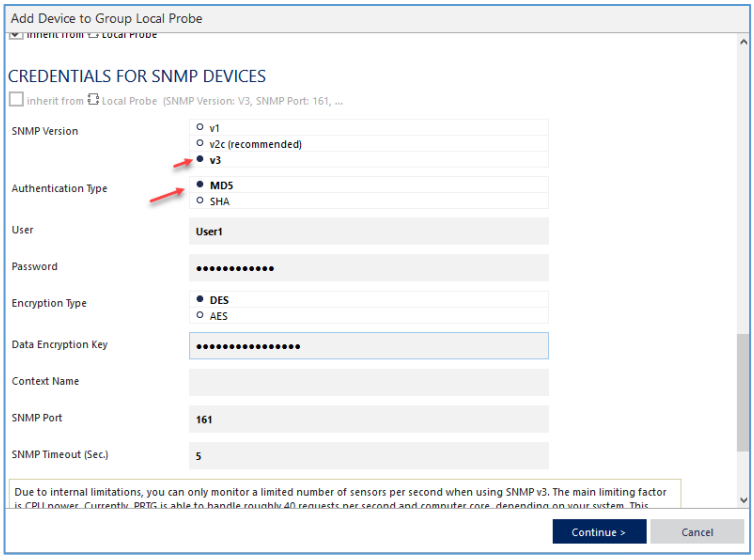
بعد از این کار می‌خواهیم عملکرد این پروتکل را تست بگیریم، برای اینکه بتوانیم از پروتکل **SNMP** استفاده کنیم باید از یک نرم‌افزار مانیتورینگ استفاده کنیم که در اینجا از نرم‌افزار **PRTG** استفاده می‌کنید، توجه داشته باشید آموزش این نرم‌افزار را می‌توانید از کتاب مدیر شبکه ۱، که بنده آن را تالیف کردم مشاهده کنید.



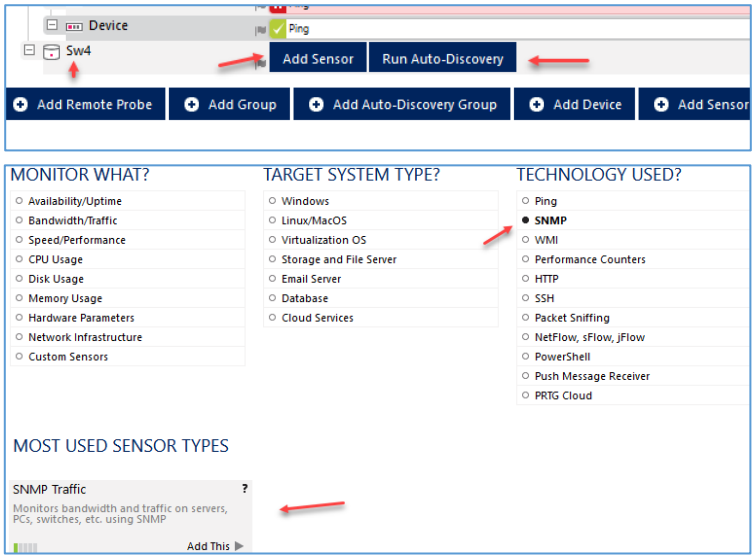
وارد تب **Devices** در نرم‌افزار **PRTG** شوید و برای اضافه کردن دستگاه مورد نظر بر روی **Add Devices** کلیک کنید.



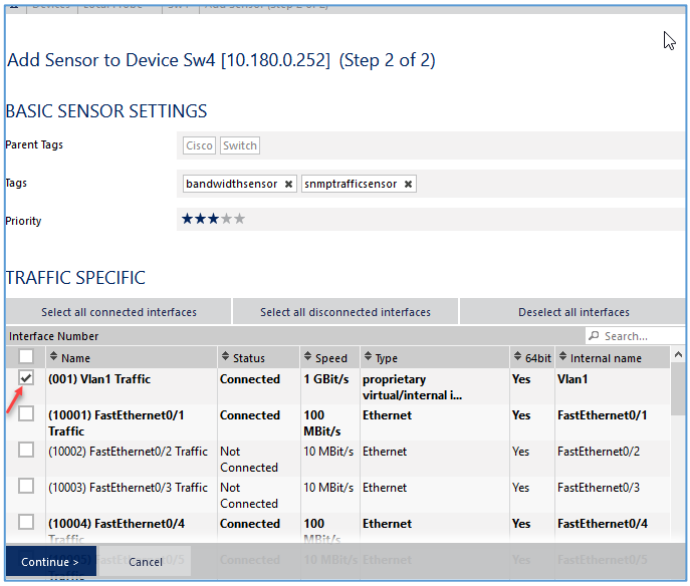
در این صفحه یک نام برای دستگاه خود وارد کنید و در قسمت **IPV4** آدرس سوئیچ یا روتر خود را وارد کنید و صفحه را به پائین اسکرول کنید.



در این صفحه ورژن **SNMP** را **V3** انتخاب کنید و نوع **Authentication** را **MD5** در نظر بگیرید، نام کاربری **User1** را که ایجاد کردید در قسمت **User** وارد کنید و رمز عبور اول که **Test@12345** بوده را وارد کنید و در قسمت **Encryption Type** گزینه‌ی **Des** را انتخاب و رمز **12345@Test** را وارد کنید و بر روی **Continue** کلیک کنید.



بعد از اضافه کردن دستگاه به لیست باید سنسور مورد نظر را برای آن فعال کنید، یا می‌توانید بر روی **Run Auto-Discovery** کلیک کنید که این گزینه به صورت اتوماتیک کارها را انجام می‌دهد یا اینکه بر روی **Add Sensor** کلیک کنید تا شکل رویرو ظاهر شود و در این قسمت گزینه‌ی **SNMP** را انتخاب کنید و بر روی **SNMP Traffic** کلیک کنید.



همانطور که مشاهده می‌کنید لیستی از **interface**ها و **Vlan** را مشاهده می‌کنید که می‌توانید برای مانیتور کردن انها هر کدام را که مایل بودید انتخاب کنید، در تب **Status** هم مشخص شده است که کدام **interface** متصل شده و درحال کار است، بعد از انتخاب بر روی **Continue** کلیک کنید، بعد از این کار می‌توانید نظارت دقیقی بر روی دستگاه خود داشته باشید.

نصب و راه اندازی GNS3 به همراه IOU

GNS3 یکی از بهترین نرم‌افزارهای مجازی سازی برای دستگاه‌های شبکه خصوصاً سیسکو است است که عملکرد خوبی را دارا است، یکی از مهمترین مشکلات GNS3 در گذشته در زمینه‌ی سوئیچ بوده که عملکرد ضعیفی داشته ولی با روی‌کار آمدن نرم‌افزار IOU این ضعف بر طرف شده و مشکلی از این لحاظ وجود ندارد، در این قسمت می‌خواهیم نحوه نصب و راه اندازی نرم‌افزار GNS3 را بررسی کنیم و IOU را به آن متصل کنیم.

برای شروع کار این دو نرم‌افزار را دانلود کنید:

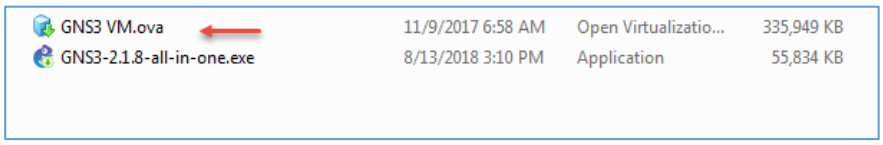
GNS3 Installation

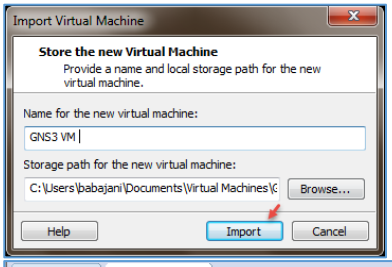
http://p30download.com/fa/entry/56879/

GNS3 VMware Workstation

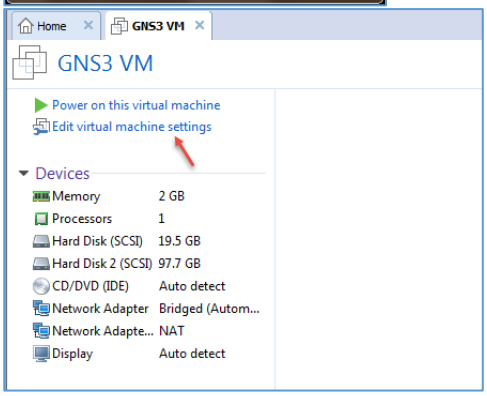
https://github.com/GNS3/gns3-gui/releases/download/v2.1.9/GNS3.VM.VMware.Workstation.2.1.9.zip

نصب GNS3 ساده بوده و نیاز به توضیح خاصی ندارد ولی فایل GNS3 VMware Workstation به صورت یک فایل فشرده با پسوند ova است که با کلیک بر روی آن ماشین مجازی آن بر روی نرم‌افزار VMware Workstation ایجاد خواهد شد، اگر با VMware کار نکردید می‌توانید کتاب آن را از سایت دانلود و مطالعه کنید.

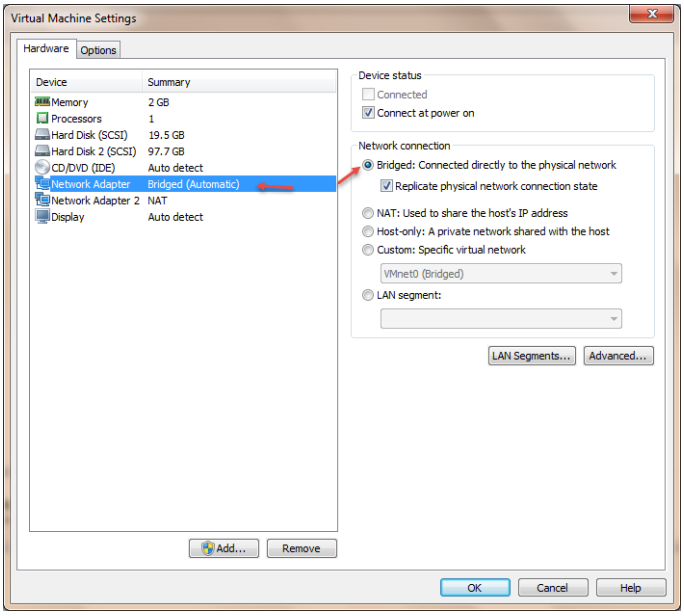




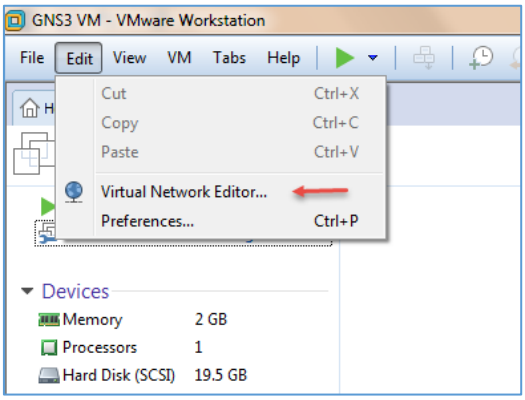
بعد از باز کردن فایل مورد نظر شکل زیر ظاهر خواهد شد که می‌توانید اسم و آدرس ذخیره شدن آن را تغییر دهید و بر روی کلید Import کلیک ککنید تا ماشین مورد نظر ایجاد شود.



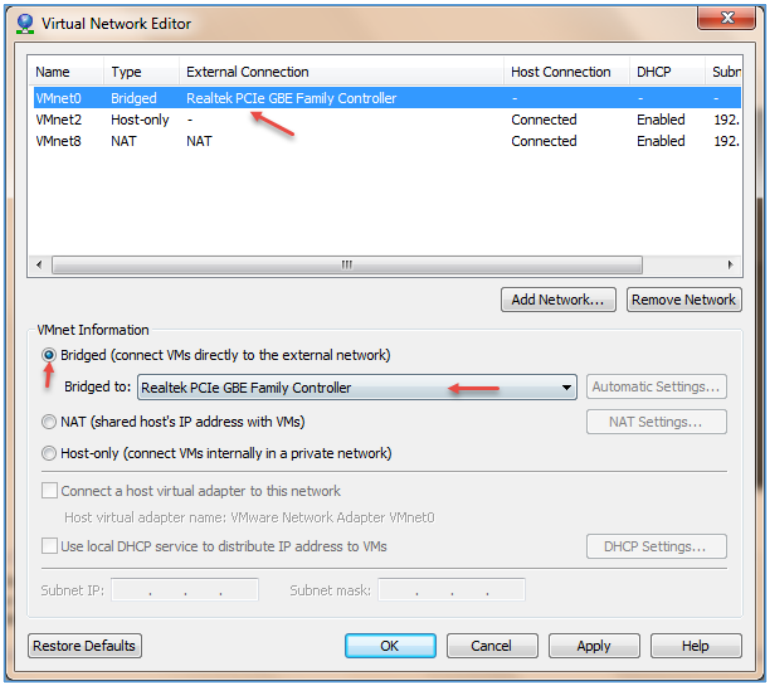
بعد از فعال شدن ماشین برای اینکه تنظیمات خود را بر روی آن اعمال کنید بر روی Edit virtual machine settings که در شکل مشخص شده است کلیک کنید.



در این صفحه می‌توانید مقدار رم و CPU ماشین مورد نظر را برای عملکرد بهتر تغییر دهید که به صورت پیش‌فرض ۲ گیگابایت رم و ۱ هسته CPU به آن اختصاص داده شده است که برای کار ما پاسخگو خواهد بود، در قسمت بعد کارت شبکه مورد نظر را انتخاب کنید و در صفحه باز شده تیک گزینه‌ی Bridged را انتخاب کنید تا این سرور بتواند به شبکه واقعی شما از طریق کارت شبکه اصلی متصل شود.

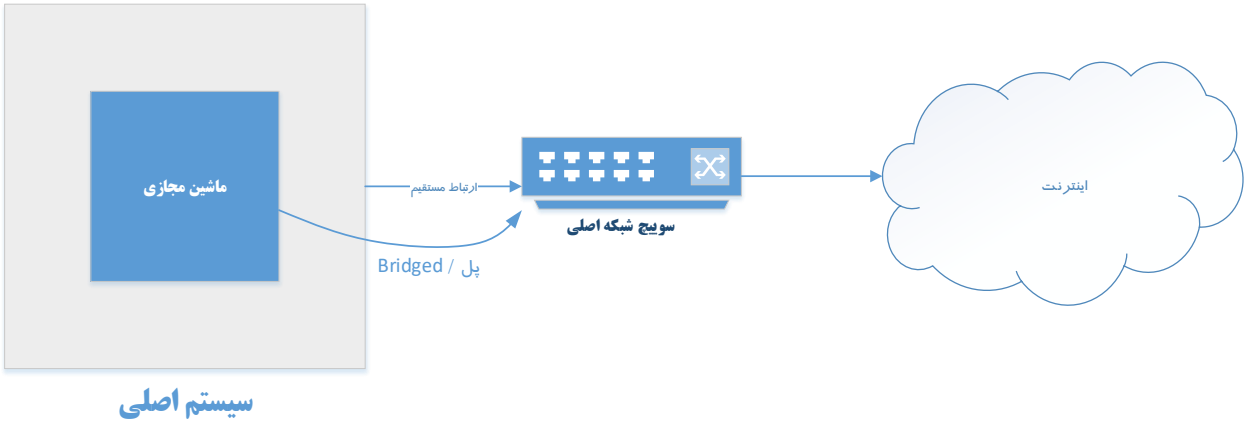


البته برای اینکه تنظیمات مربوط به کارت شبکه‌ها را در نرم‌افزار VMware بررسی کنید باید وارد منوی Edit شوید و گزینه‌ی virtual Network Editor را انتخاب کنید.

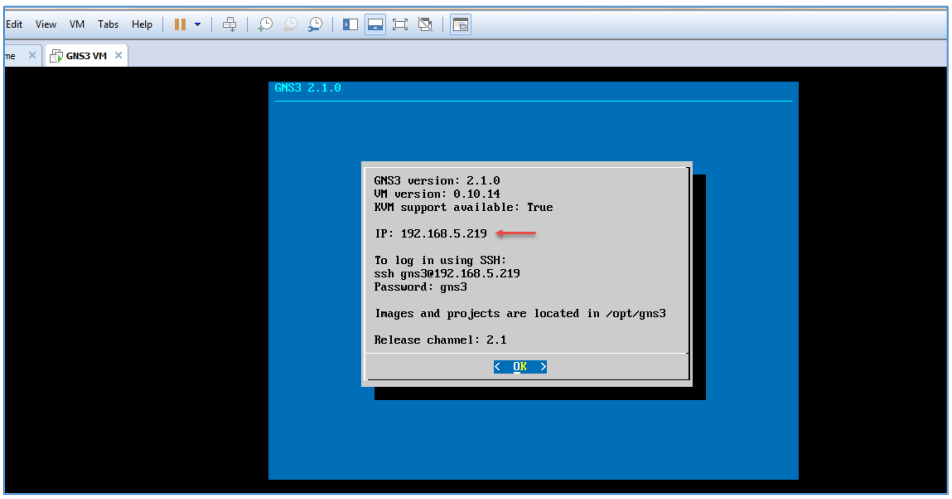


در این صفحه باید کارت شبکه VMnet0 را انتخاب کنید و در پایین صفحه گزینه‌ی Bridged را انتخاب و کارت شبکه واقعی سیستم خود را که به شبکه اصلی شما متصل است انتخاب کنید و ب رروی OK کلیک کنید.

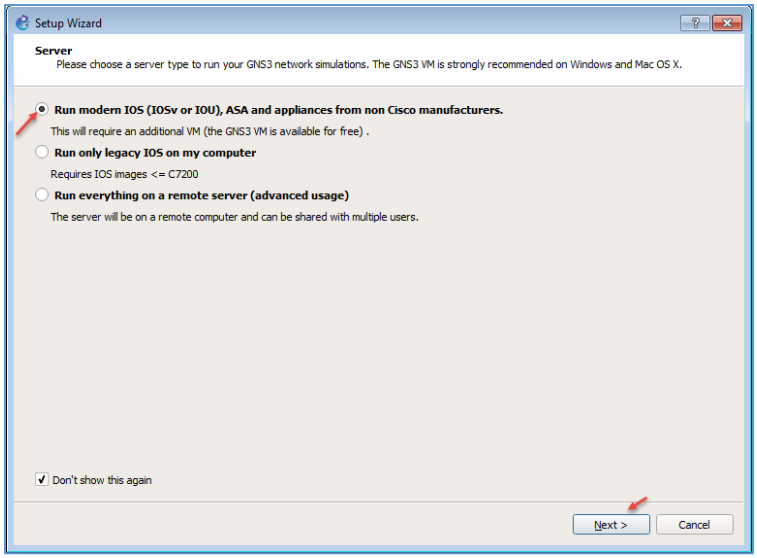
نکته: شما می‌توانید یک شبکه مجازی داشته باشید و از کارت شبکه از نوع Host Only استفاده کنید و نیاز به کارهای بالا نیست.



اگر به شکل بالا که برای شما آماده کردیم توجه کنید مفهوم Bridged را بهتر درک خواهید کرد، ماشین مجازی داخل یک سیستم فیزیکی اصلی است که از طریق کارت شبکه‌ای که آن سیستم به دنیای شبکه اصلی ما متصل است از طریق پل یا همان Bridged به شبکه اصلی متصل می‌شود و می‌تواند مثلاً آدرس IP را از سرویس DHCP دریافت کند.

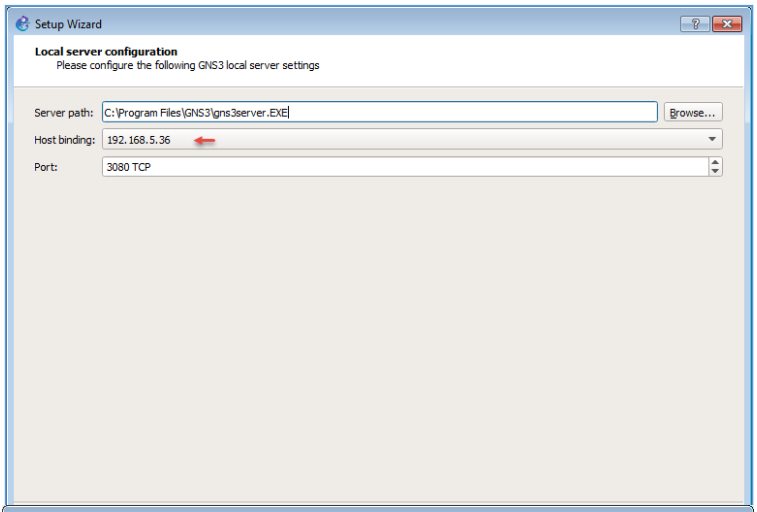


بعد از روشن کرد ماشین و اجرا شدن آن صفحه روبرو برای شما ظاهر خواهد شد که اگر تنظیمات مربوط به کارت شبکه را به درستی انجام داده باشید، آدرس IP به آن اختصاص داده خواهد شد که در این شکل آدرس ۱۹۲.۱۶۸.۵.۲۱۹ به آن داده شده است، در قسمت زیر IP دستورات مربوط به متصل شدن با SSH مشخص شده است که نام کاربر یو رمز عبور آن GNS3 است که در ادامه با آن کار خواهیم کرد، تا اینجا توانستیم نرم‌افزار GNS3 را به همراه ماشین مجازی آن فعال کنیم در ادامه باید سوئیچ لایه دو و سه IOU را به GNS3 اضافه کنیم و از آن در این کتاب استفاده کنیم، پس باید به درستی مطالب بعد را انجام دهید تا مشکلی در این زمینه نداشته باشید.



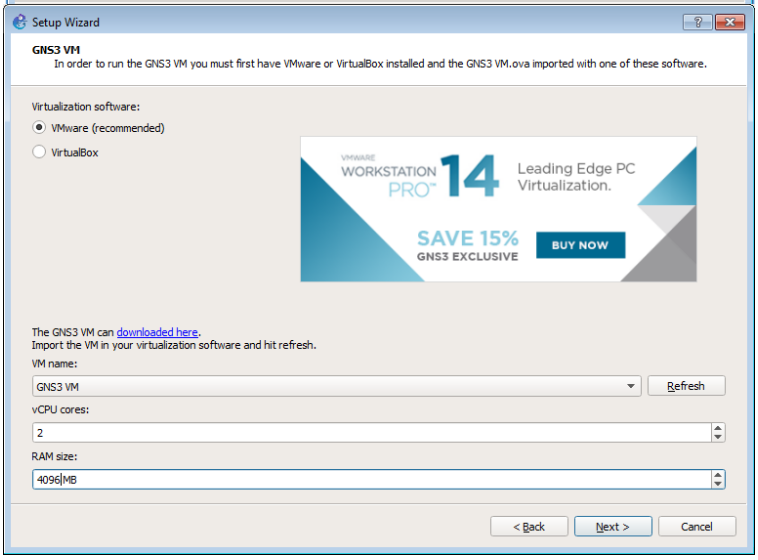
نرم‌افزار GNS3 را اجرا کنید، بعد از اجرا شکل روبرو ظاهر خواهد شد، در این قسمت گزینه‌ی اول را انتخاب و بر روی Next کلیک کنید.

نکته: در بعضی موارد در این قسمت و در ادامه با خطاهای مختلف مواجه خواهید شد که این مشکل‌ها بر می‌گردید به تنظیمات آنتی ویروس و فایروال.

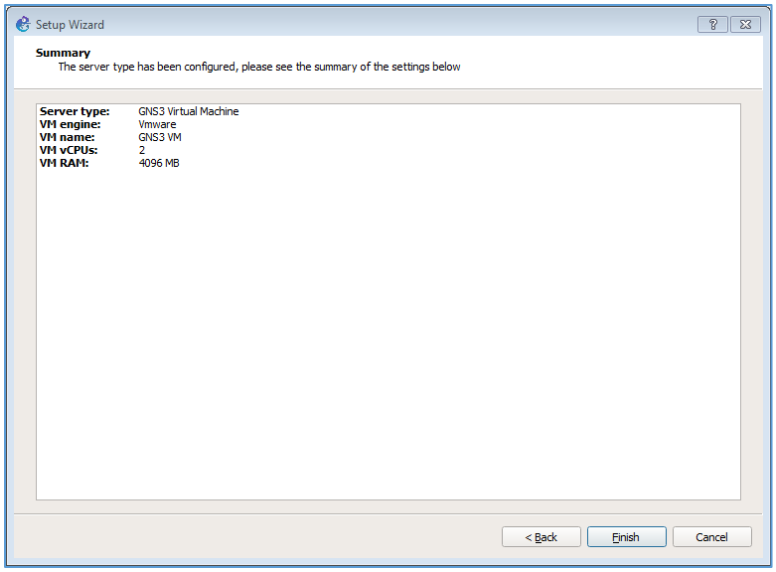


در این صفحه باید آدرس سروری که نرم‌افزار GNS3 بر روی آن نصب شده است را مشخص کنید، توجه داشته باشید که چورت پیش‌فرض برای اتصال ۳۰۸۰ است.

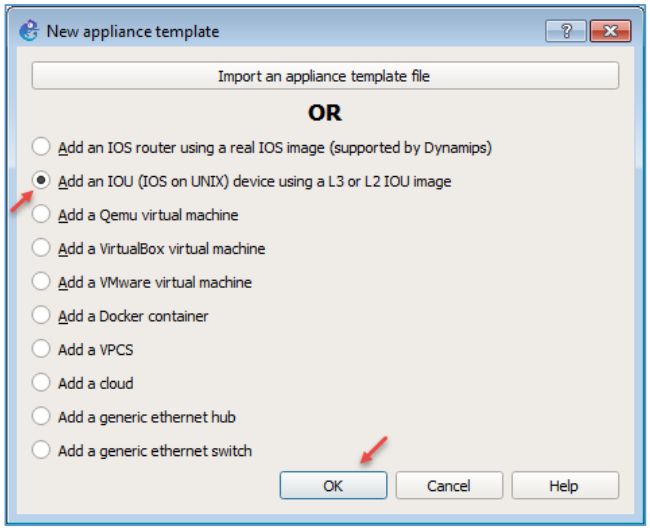
بر روی Next کلیک کنید.



در این قسمت اگر مراحل راه‌اندازی ماشین مجازی را در قسمت قبل انجام داده باشید این قسمت ماشین مورد نظر را به صورت خودکار شناسایی خواهد کرد، مقدار CPU و مقدار رم را مشخص کرده و بر روی Next کلیک کنید.



در این قسمت به ماشین مجازی متصل شدیم و برای ادامه کار بر روی Finish کلیک کنید.

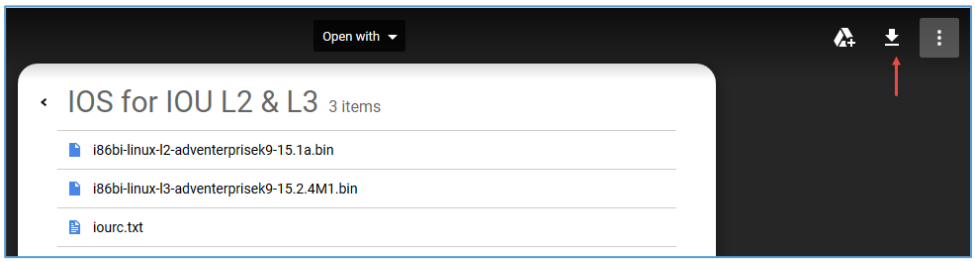


بعد از کلیک بر روی Finish صفحه روبرو ظاهر خواهد شد که باید IOS مربوط به سوئیچ لایه دو و سه را به نرم‌افزار GNS3 اضافه کنیم، برای این کار گزینه‌ی Add an IOU ... را انتخاب کنید و بر روی OK کلیک کنید.

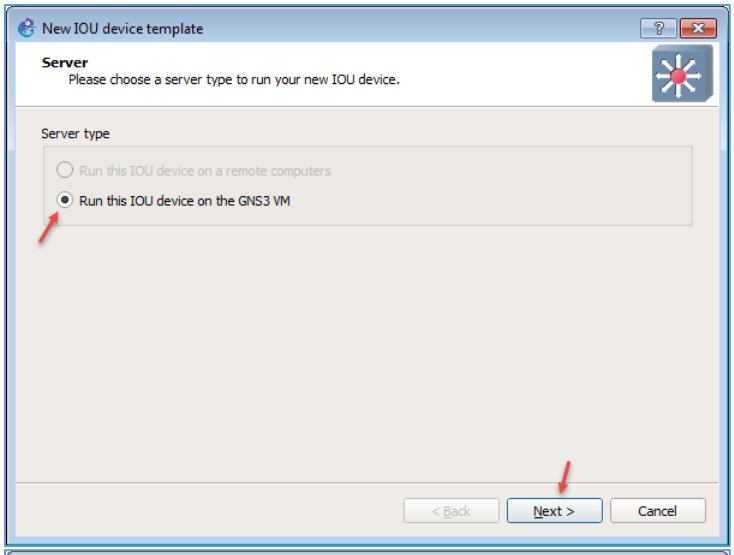
برای استفاده از IOS مربوط به سوئیچ، دو فایل Image مربوط به سوئیچ لایه دو لایه سه را از لینک زیر دانلود کنید:

Switch L2 & L3:

https://drive.google.com/file/d/0B8tSmsEbVQs-bjVXY3VqMFJrc1E/view

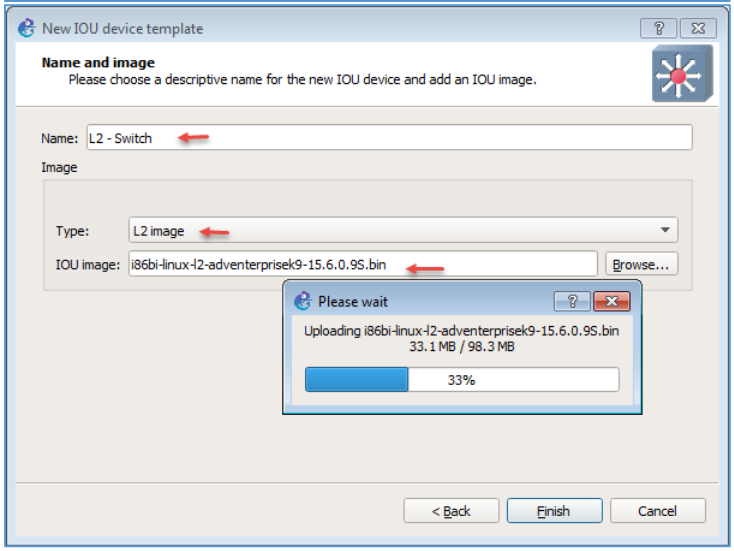


در این صفحه بر روی آیکون دانلود کلیک کنید و هر دو فایل را دریافت کنید.

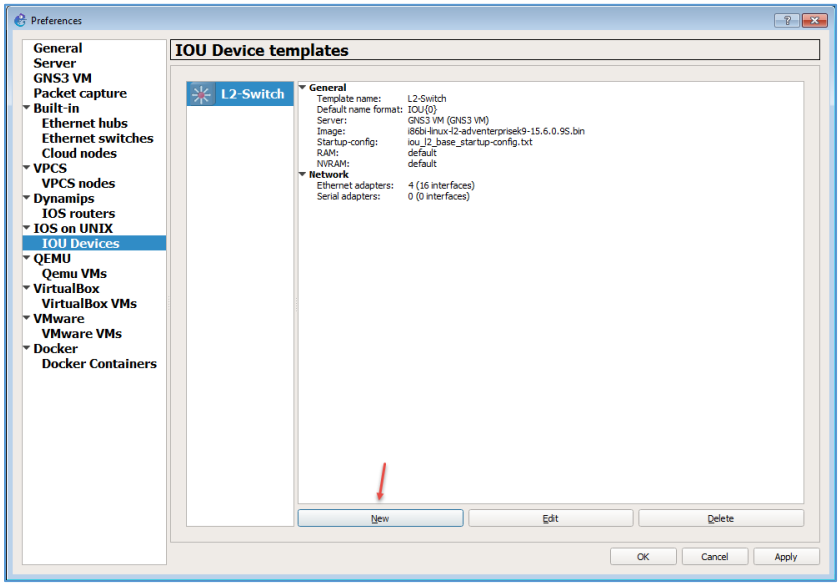


در این قسمت گزینه‌ی GNS3 VM به صورت پیش‌فرض انتخاب شده است.

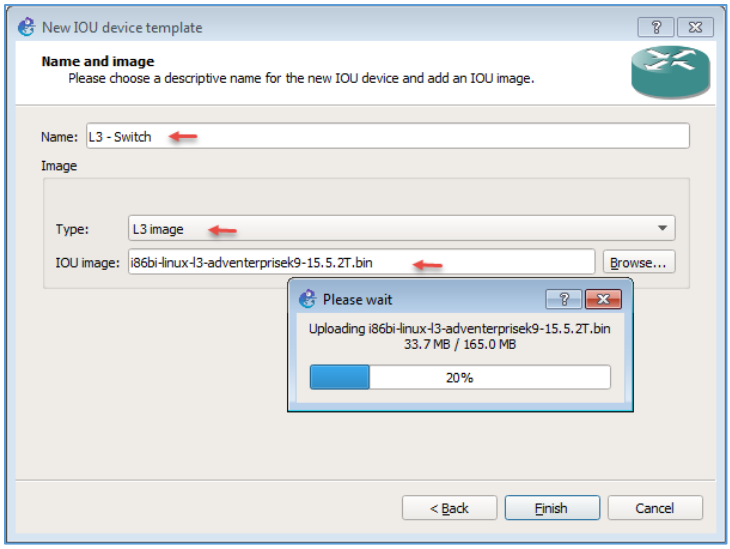
بر روی Next کلیک کنید.



در این صفحه باید دو فایلی که برای سوئیچ سیسکو بوده را به ماشین مجازی معرفی کنید، برای این کار برای سوئیچ لایه دو نام مورد نظر خود را وارد کنید، و در قسمت Type باید گزینه‌ی L2 image را انتخاب کنید و با کلیک بر روی Browse فایل IOS مربوط به آن را انتخاب کنید، با این کار فایل IOS در ماشین مجازی GNS3 آپلود خواهد شد.

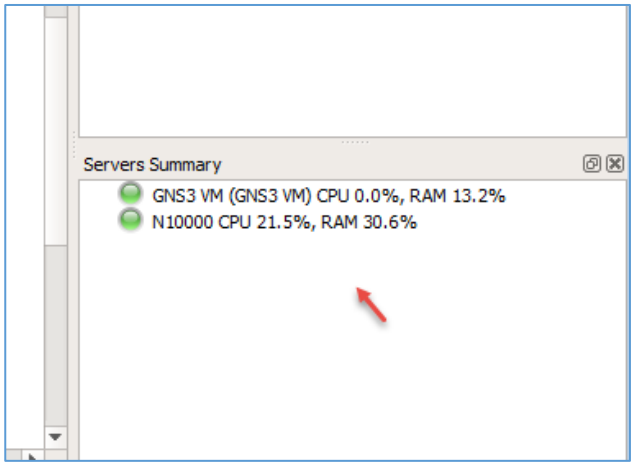


بعد از کلیک بر روی Finish به مانند شکل روبرو سوئیچ لایه دو به لیست مورد نظر اضافه خواهد شد و برای اینکه سوئیچ لایه سه هم به لیست اضافه کنید باید بر روی New کلیک کنید.

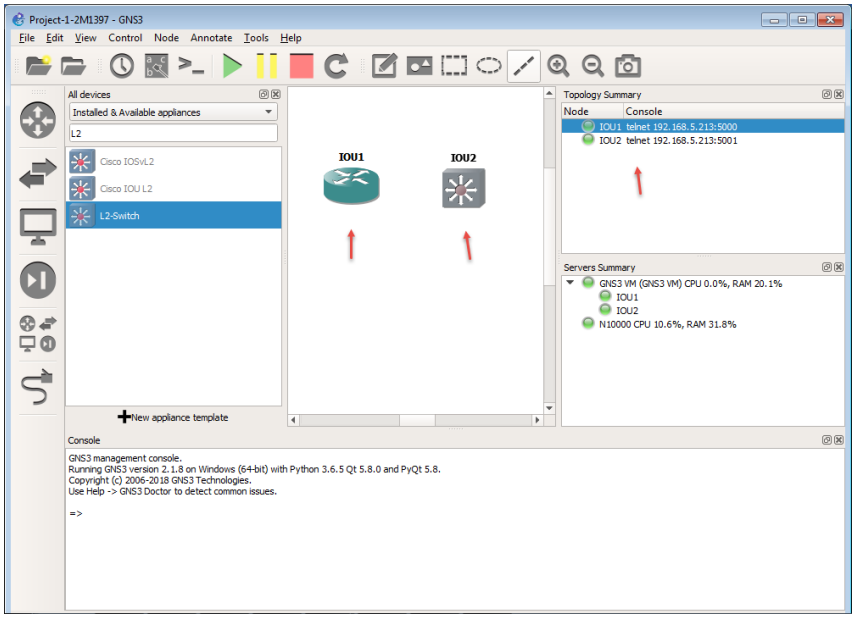


در این صفحه هم نام سوئیچ لایه سه را وارد و فایل IOS آن را به نرم‌افزار معرفی تا در ماشین مجازی آپلود شود.

بعد از اتمام کار بر روی Finish کلیک کنید.



اگر در نرم‌افزار GNS3 به قسمت Servers Summary توجه کنید، هر دو سرور local و سرور مجازی را به همراه مانیتورینگ سخت‌افزاری آن مشاهده می‌کنید که این موضوع نشان دهنده فعال بودن آن‌ها است.



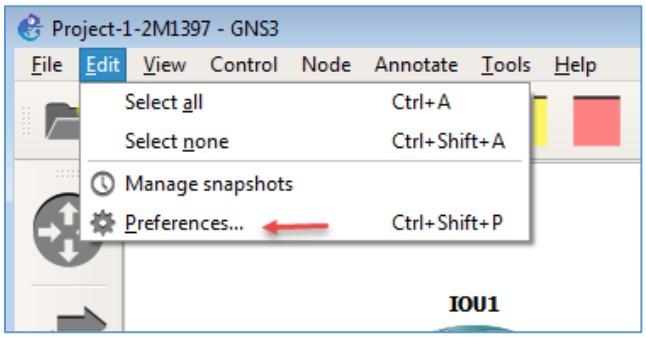
بعد از اتمام مراحل بالا در قسمت Device به مانند شکل سوئیچ مورد نظر خود را که با اسم مشخص شده ایجاد کردید جستجو کنید و آن را کشیده و در صفحه مورد نظر رها کنید و بعد آنها را روشن کنید، همانطور که مشاهده می‌کنید هر دو سوئیچ لایه دو و سه بدون مشکل روشن شده است.

اضافه کردن IOS مربوط به روتر در GNS3

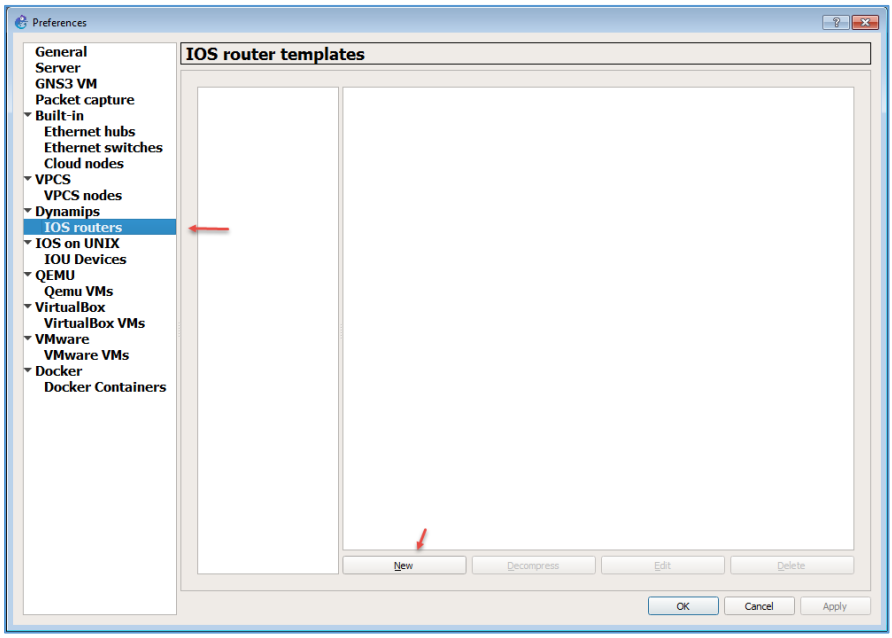
در قسمت قبلی توانستیم، ماشین مجازی راه‌اندازی کنیم و سوئیچ لایه دو و سه را به آن اضافه و به نرم‌افزار اصلی GNS3 اضافه کنیم که همانطور که گفتیم یکی از مشکلات عمده GNS3 در مبحث سوئیچینگ بوده که با این کار مشکلش حل شد و همه دستورات سوئیچ که در ادامه کار خواهیم کرد اجرا خواهد شد، در این قسمت باید IOS مربوط به روتر را هم به نرم‌افزار GNS3 اضافه کنیم، البته نیازی نیست آن را درون ماشین مجازی آپلود کنید، بلکه می‌توانید آن را درون خود نرم‌افزار اصلی آپلود کنید.

برای دانلود IOS 7200 cisco Router می‌توانید از لینک زیر است

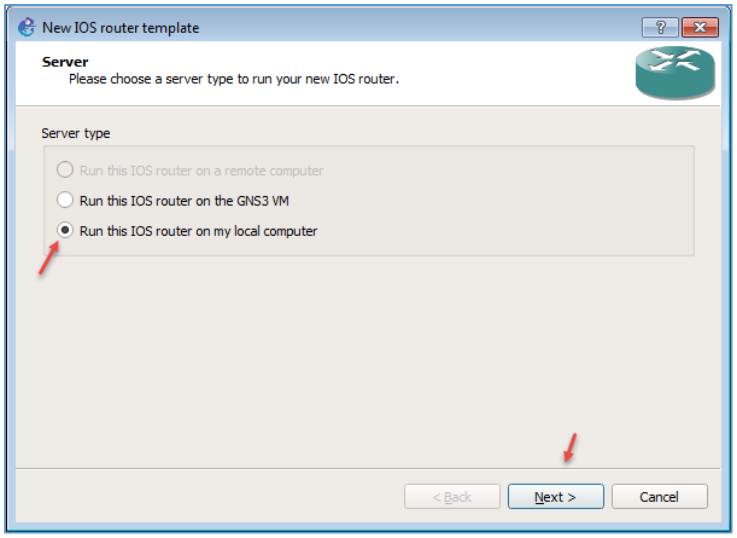
http://ipmanager.ir/r/CISCO/7200/c7200-adventerprisek9-mz.151-4.M.bin



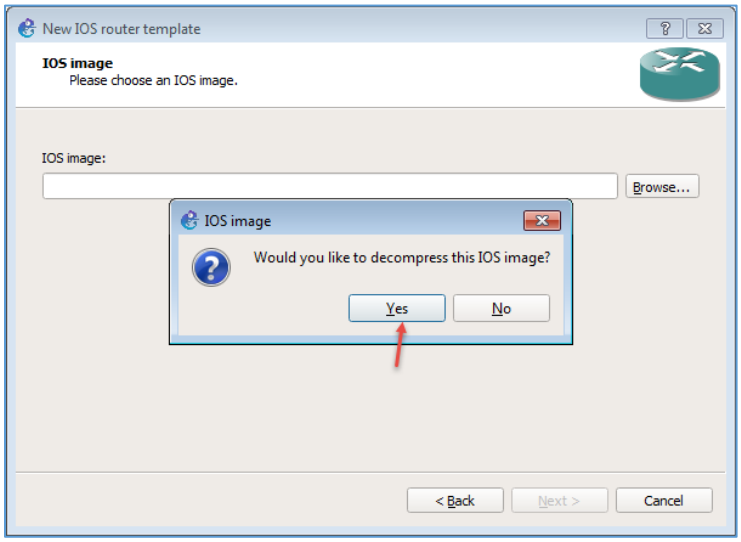
بعد از دانلود IOS مربوط به روتر وارد منوی Edit شوید و بر روی گزینه‌ی Preferences کلیک کنید.



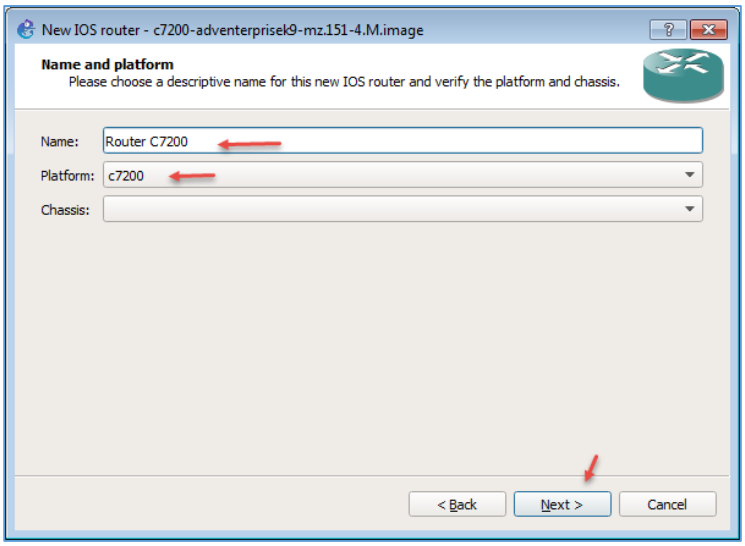
در این صفحه از سمت چپ وارد قسمت IOS Routers شوید و بر روی New کلیک کنید.



در این قسمت برا اینکه IOS را بر روی سیستم اصلی اجرا کنیم گزینه‌ی دوم یعنی Local Computer را انتخاب کنید و بر روی Next کلیک کنید.

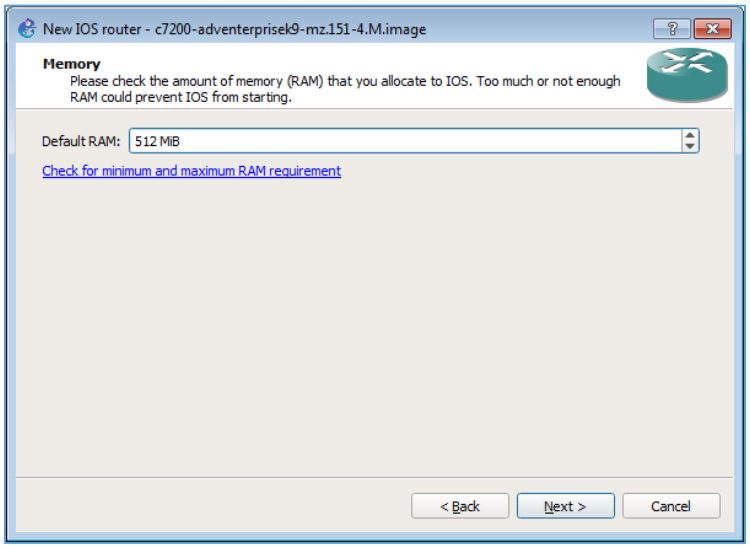


در این صفحه بر روی Browse کلیک کنید و فایل دانلود شده را به آن معرفی و برای اضافه کردن آن به نرم‌افزار بر روی Yes کلیک و بعد بر روی Next کلیک کنید.



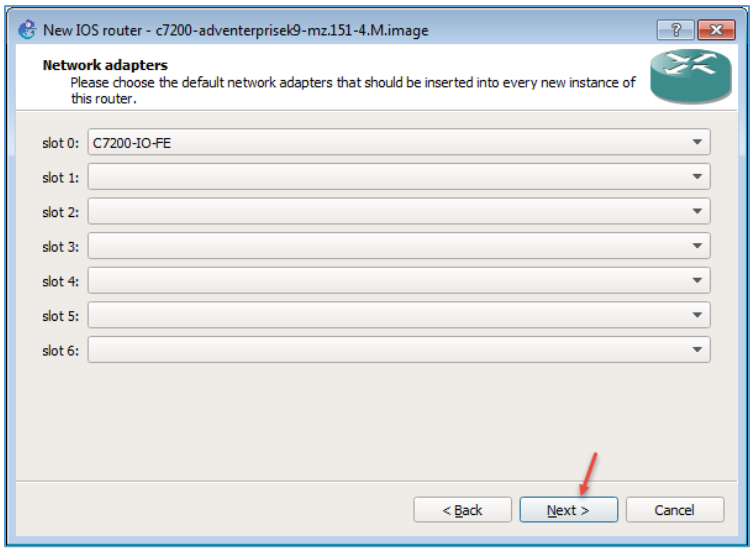
در این قسما باید نام روتر را به دلخواه وارد و در قسمت Platform باید مدل روتر را بر روی C7200 قرار دهید و بر روی Next کلیک کنید.

در این قسمت بر روی Next کلیک کنید.

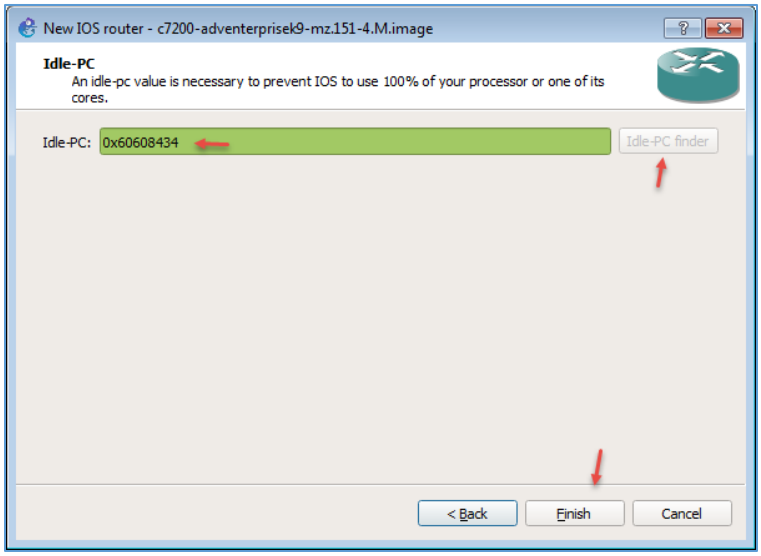


در این قسمت باید Slot مربوط به روتر را انتخاب کنید، که بر روی این Slotها می‌تواند انواع پورت‌ها قرار بگیرد، در حال حاضر Slot پیش‌فرض کفایت می‌کند.

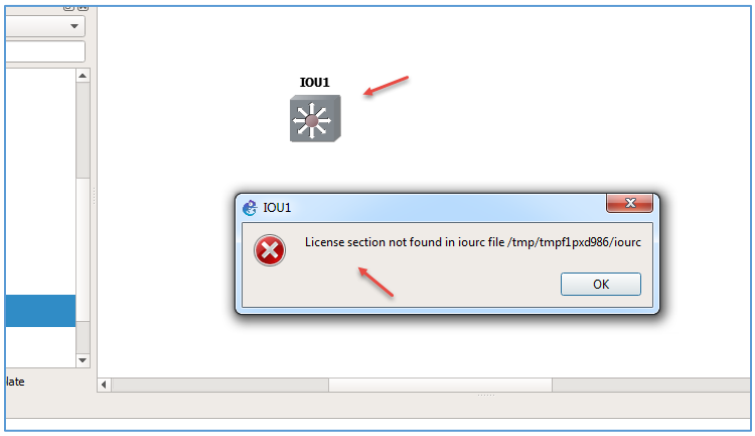
بر روی Next کلیک کنید.



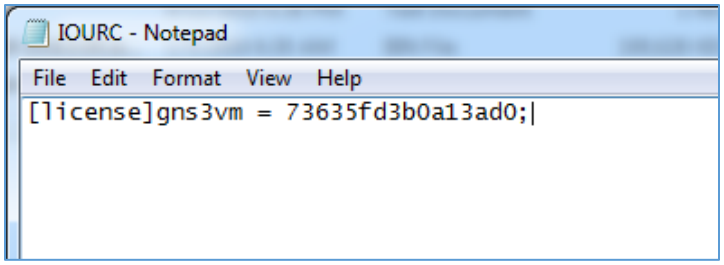
در این قسمت باید برای روتر خود یک Idle-PC مشخص کنید، برای این کار بر روی دکمه Idle-Pc finder کلیک کنید، این موضوع کمک می‌کند که مقدار درگیری سرور بسیار کم شود و مشکلی در کار پیش نیاید، اگر این کار را نکنید CPU کاملاً مشغول خواهد شد.



اضافه کردن لایسنس IOU به نرم‌افزار



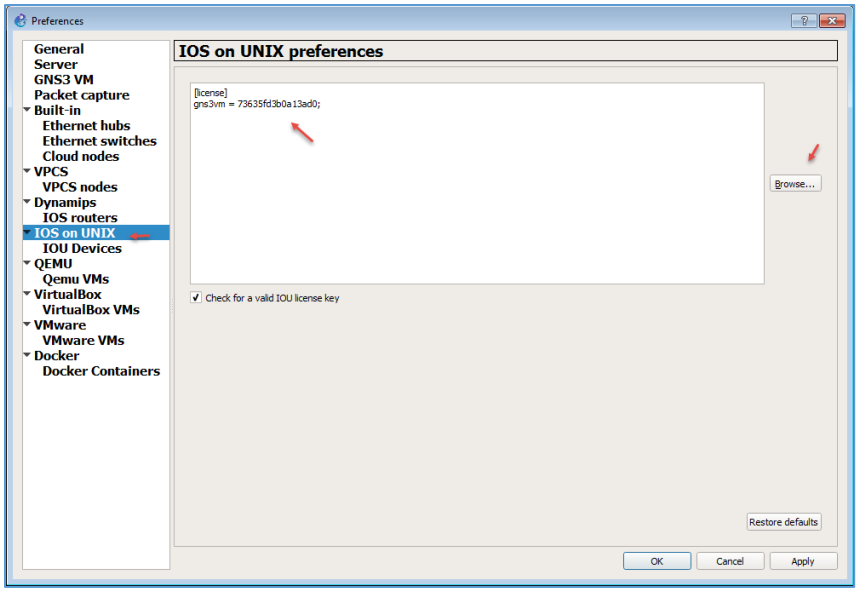
توجه داشته باشید که برای کار با IOU نیاز به لایسنس دارید که باید در GNS3 وارد کنید، اگر چنانچه با خطای روبرو هنگام روشن کردن دستگاه مواجه شدید باید به صورت زیر عمل کنید.



متن زیر را در یک فایل txt وارد و با هر نامی ذخیره کنید:

[license]

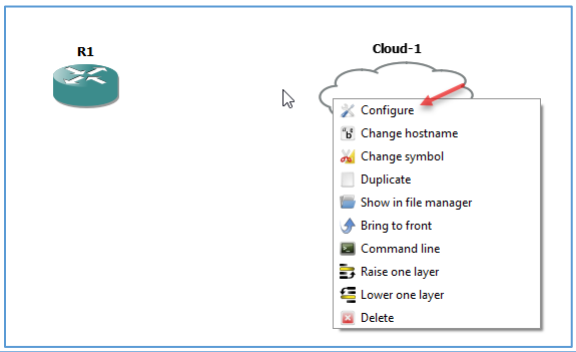
gns3vm = 73635fd3b0a13ad0;



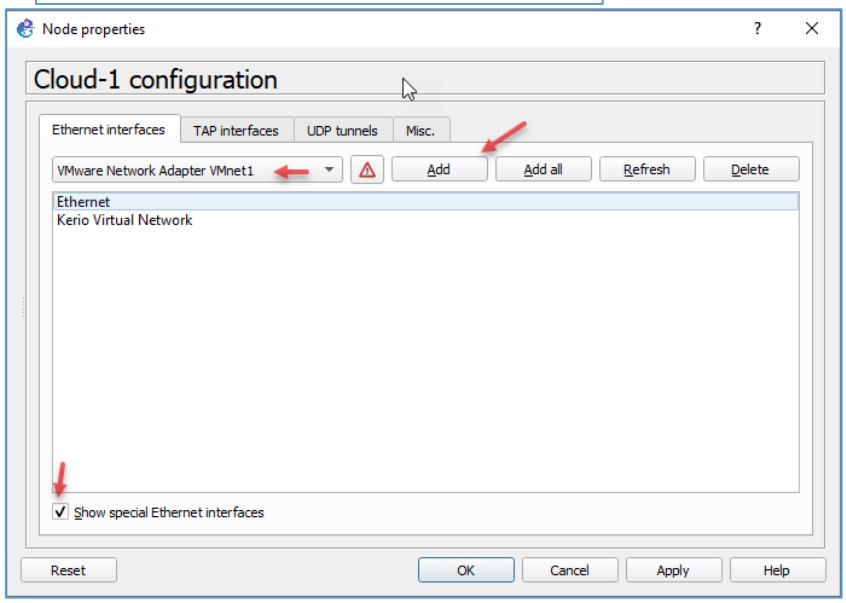
وارد GNS3 شوید و قسمت Preferences را فعال و به قسمت IOS on UNIX مراجعه کنید و در صفحه باز شده بر روی Browse کلیک کنید و فایل TXT مربوط به لایسنس را که ایجاد کردید انتخاب و بر روی ok کلیک کنید، با این کار لایسنس IOU فعال و سوئیچ‌ها فعال خواهند شد.

فعال‌سازی سرویس Log در دستگاه‌های سیسکو

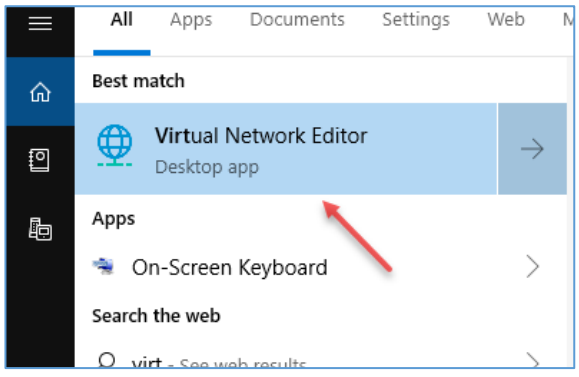
داشتن اطلاعات از رویدادهایی که برای دستگاه‌های شبکه مخصوصاً سوئیچ، روتر، فایروال و... اتفاق می‌افتد بسیار می‌تواند شما را در ارائه گزارش درست و جلوگیری از مشکلات ناشی از آن کمک کند، برای انجام این کار به مانند شکل روبرو یک روتر و یک Cloud را به صفحه اضافه کنید و بر روی آن کلیک راست و گزینه‌ی Configure را انتخاب کنید.

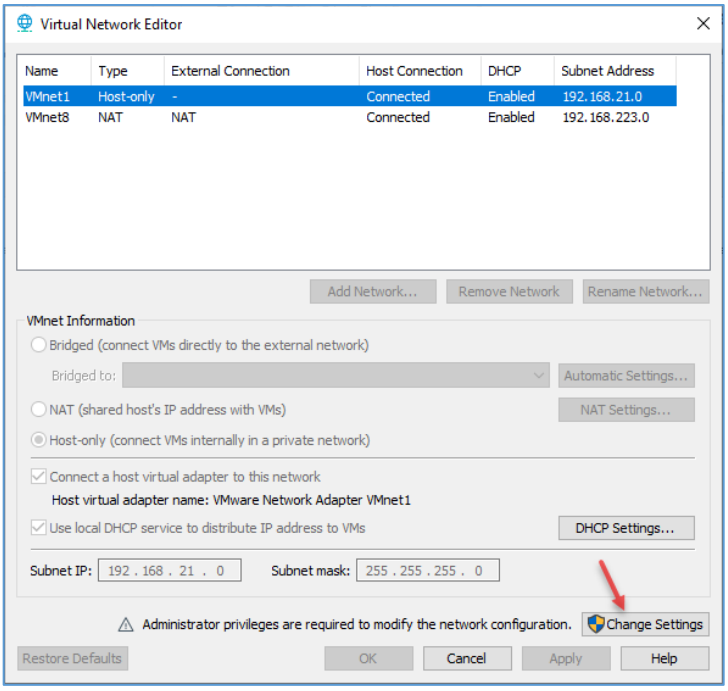


در این صفحه از قسمت پایین آن تیک گزینه‌ی Show special Ethernet interfaces را انتخاب کنید و بعد از لیست کشویی کارت شبکه مجازی VMnet1 را انتخاب کنید، این کارت شبکه مجازی مربوط به VMware است که می‌توانید رنج IP آن را تنظیم کنید، بر روی ok کلیک کنید.

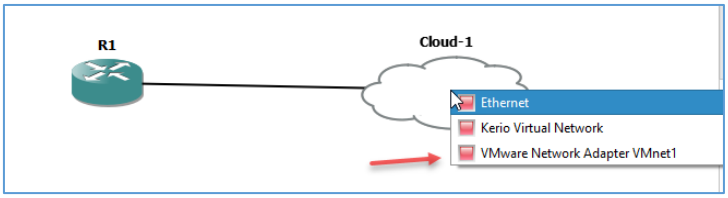


برای اینکه تنظیمات کارت شبکه مجازی را مشاهده کنید بر روی Start کلیک کنید و سرویس Virtual Network Editor را اجرا کنید.





در این صفحه لیست کارت شبکه مجازی خود را مشاهده می‌کنید، برای اینکه بتوانید آدرس مورد نظر خود را وارد کنید و کارت شبکه را ویرایش کنید باید بر روی Change Settings کلیک کنید.



بعد از تنظیم کارت شبکه در زمان اتصال به Cloud می‌توانید نام کارت شبکه مجازی را انتخاب کنید.

برای شروع به روتر R1 آدرس IP می‌دهیم:

```
R1(config)#interface ethernet 0/0
R1 (config-if)#ip addres 192.168.21.6 255.255.255.0
R1 (config-if)#no sh
```

همانطور که مشاهده می‌کنید آدرس 192.168.21.6 به روتر R1 تخصیص داده شده است و پورت آن روشن شده است.

پس تا به اینجا یک روتر با نام R1 به صفحه اضافه کردیم و آدرس آن را ۱۹۲.۱۶۸.۲۱.٦ در نظر گرفتیم و آن را به یک Cloud متصل کردیم که می‌توانیم از سیستم واقعی خود به آن روتر دسترسی داشته باشیم، برا اینکه ادامه کار را بررسی کنیم باید یک نرم‌افزار Syslog Server را دانلود کنیم و بر روی سیستم خود نصب کنیم.

نرم‌افزاری که برای این کار در نظر گرفتیم نرم‌افزار SolarWinds Kiwi Syslog Server است که می‌توانید از اینجا دانلود کنید، بعد از نصب دو آیکون روبرو را مشاهده می‌کنید که یکی برای تحت ویندوز ودیگری برای تحت وب می‌باشد که در ادامه از هر دوی آنها استفاده خواهیم کرد.

در ادامه دوباره وارد روتر شوید و دستور زیر ار اجرا کنید:

```
R1(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

با اجرای دستور logging trap ? گزینه‌های مختلف برای اجرای log گیری به شما نمایش داده خواهد شد که جلوی هر یک از آنها عددی وجود دارد که عنوان آن severity در نظر گرفته شده است، مثلاً گزینه‌ی یک مربوط به logهای Alert است و به همین ترتیب گزینه‌های دیگر، اگر گزینه‌ی یک را انتخاب کنید، فقط و فقط Alert برای سرور Syslog ارسال خواهد شد و گزینه‌های دیگر ارسال نخواهند شد ولی اگر گزینه‌ی هفتم را انتخاب کنید همه‌ی گزینه‌های قبل از آن به سرور Syslog ارسال خواهند شد و نیاز نیست تک تک آنها را در این دستور وارد کنید.

```
R1(config)#logging trap debugging
```

با دستور بالا عملیات Log گیری از سرور با سطح Debugging فعال شده است و ادامه باید اطلاعات را به سرور Syslog ارسال کنیم.

R1(config)#logging source-interface ethernet 0/0

در دستور بالا باید مشخص کنیم که اطلاعات Log را به کدام Interface ارسال کنیم، که در این قسمت Interface شماره 0/0 مشخص شده است که به Cloud متصل است.

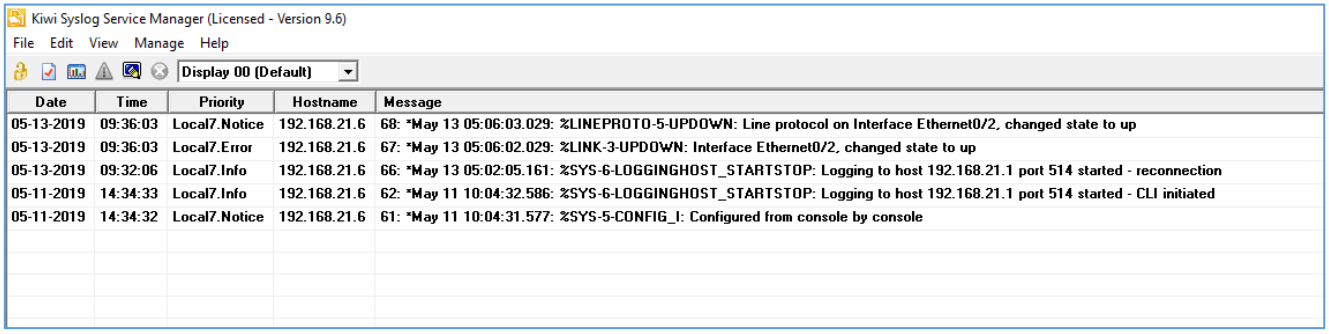
R1(config)#logging on

با دستور logging on سرورو شروع به Log انداختن می‌کنید، یعنی هر کاری که در روتر انجام شود، یک Log برای آن ایجاد خواهد شد.

R1(config)#logging host 192.168.21.1

با این دستور مشخص می‌کنیم، که چه سیستمی به عنوان Syslog سرور است، یعنی نرم‌افزار Syslog سرور بر روی آن نصب شده است که در اینجا آدرس آن ۱۹۲.۱۶۸.۲۱.۱ در نظر گرفته شده است.

حال اگر هر اتفاقی در روتر رخ دهد اطلاعات آن به مانند شکل زیر به نرم‌افزار Kiwi Syslog سرور ارسال خواهد شد.



کار با Control plane

یکی دیگر از قسمت‌های مهم شبکه Control Plane است که به صورت مستقیم مربوط میشود به دستگاه‌های شبکه که باید بار کاری آنها بررسی و آنالیز شود تا با افزایش درخواست‌ها از دستگاه‌های مورد نظر مشکلات سخت‌افزاری برای آن پیش بیاید و اگر هم Control Plane از کار بیفتد هر دو قسمت Managemnet Plane و Data Palen از کار خواهد افتاد.

بررسی CoPP

CoPP یا Control plane policing به روش‌ها و سیاست‌های کنترلی برای حفظ Control Plane اشاره دارد که به صورت کلی بر روی Control Plane اعمال می‌شود.

ترافیک بیش از حد در روتر می‌تواند به مرور زمان بر عملکرد آن تاثیر بگذارد و به خاطر همین باید کارهایی را در رفع مشکل آن پیاده‌سازی کرد.

در زیر روش‌هایی را بررسی می‌کنیم که کارکرد آنها می‌تواند بر روی CPU اثر گذار باشد:

- Access control list (ACL) logging : زمانی که از Access List در سی5است‌های کاری خود استفاده می‌کنید، هر عملی که با این لیست‌ها انجام شود یک Log در دستگاه ثبت خواهد شد که همین موضوع بار CPU را افزایش می‌دهد.
- IP options : پردازش تمام بسته‌های IP با جزئیات آن
- Fragmentation : همانطور که می‌دانید هر بسته‌ی IP در صورت نیاز باید تکه تکه شود و این کار باز هم به CPU نیاز دارد.
- Time-To-Live (TTL) expiry: بسته‌های ICMP که زمانی کمتر یا مساوی یک دارند نیاز به پردازش CPU دارند
- ICMP unreachables : بسته‌هایی که در هنگام مسیریابی غیر قابل دسترس هستند توسط CPU پردازش می‌شوند

- Traffi c requiring an ARP request : مقصدی که ورودی پروتکل ARP برای آنها وجود ندارد باید پردازش شود.
- Non-IP traffic : تمام ترافیک‌های غیر IP توسط CPU پردازش می‌شوند.
- Receive adjacency traffic : به ترافیک‌هایی گفته می‌شود که توسط خود روتر پردازش می‌شود، اگر از دستور Show IP cef استفاده کنید، در شکل روبرو این دستور اجرا شده است و در قسمت Next Hop اگر کلمه‌ی receive را مشاهده کردید به این معنا است که ترافیک توسط خود روتر ایجاد و پردازش شده است.

```
R1#show ip cef
Prefix              Next Hop
0.0.0.0/0           no route
0.0.0.0/8           drop
0.0.0.0/32          receive
127.0.0.0/8         drop
224.0.0.0/4         drop
224.0.0.0/24        receive
240.0.0.0/4         drop
255.255.255.255/32  receive
R1#
```

برای اینکه از Access list استفاده کنید بهتر است از Access List پیشرفته استفاده کنید و نوع سرویس را مشخص کنید تا محدوده Access List محدود به سرویس خاصی شود و بیش از حد از CPU استفاده نکند، در زیر به طور کامل Access list را بررسی و دو مورد Standard و Extended را مورد بررسی قرار می‌دهیم.

کار با Access List

Access control List یا همان Access list برای ایجاد محدودیت و امنیت در شبکه کاربرد دارد، با استفاده از این سرویس می‌توانید بر روی پروتکل‌ها، کلاینت‌ها، سرورها و هر چیزی که در شبکه در حال رد و بدل اطلاعات است محدودیت ایجاد کنید، روتر با استفاده از این لیست‌ها به تجزیه و تحلیل اطلاعات می‌پردازد.

Access List با استفاده از اطلاعات منبع و مقصد مانند شماره پورت، آدرس IP و... محدودیت مورد نظر خود را اعمال کند که در ادامه با این موضوعات کار خواهیم کرد.

این لیست شامل شرط‌هایی است که برای ان تعریف می‌کنیم و زمانی که بر روی یک پورت خاص اعمال شود محدودیت یا دسترسی به منابع خاص را خواهد داد که این موضوع بسیار می‌تواند به امنیت شبکه کمک کند.

با اجرا این سیاست‌ها در شبکه شما خود را به عنوان یک مدیر شبکه با امنیت بالا معرفی خواهید کرد.

در این قسمت لیستی از تعدیدات امنیتی را مشاهده می‌کنید که با استفاده از Access List کم خواهد شد:

- ✓ IP address spoofing, inbound
- ✓ IP address spoofing, outbound
- ✓ Denial of service (DoS) TCP SYN attacks, blocking external attacks
- ✓ DoS TCP SYN attacks, using TCP Intercept
- ✓ DoS smurf attacks
- ✓ Filtering ICMP messages, inbound
- ✓ Filtering ICMP messages, outbound
- ✓ Filtering traceroute

در کل دو نوع Access List در شبکه داریم که با شماره‌های مختلف مشخص شده‌اند.

- Access List استاندارد با شماره‌های ۱ تا ۹۹ و ۱۳۰۰ تا ۱۹۹۹
- Access List پیشرفته با شماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹.

اگر وارد روتر شوید و دستور یر را اجرا کنید لیستی از access list ها را با شماره مشخص شده مشاهده می‌کنید:

```
R1(config)# access-list ?
<1-99> IP extended access list
<100-199> IP extended access list
<1100-1199> Extended 48-bit MAC address access list
<1300-1999> IP standard access list (expanded range)
<200-299> Protocol type-code access list
<2000-2699> IP extended access list (expanded range)
<700-799> 48-bit MAC address access list
compiled Enable IP access-list compilation
dynamic-extended Extend the dynamic ACL absolute timer
rate-limit Simple rate-limit specific access list
```

همانطور که در لیست بالا مشاهده می‌کنید، همه Access List ها با شماره مشخص شده‌اند که هر کدام برای اجرای محدودیت خاصی، کاربرد دارد، برای شروع Access List Standard را با هم بررسی می‌کنیم.

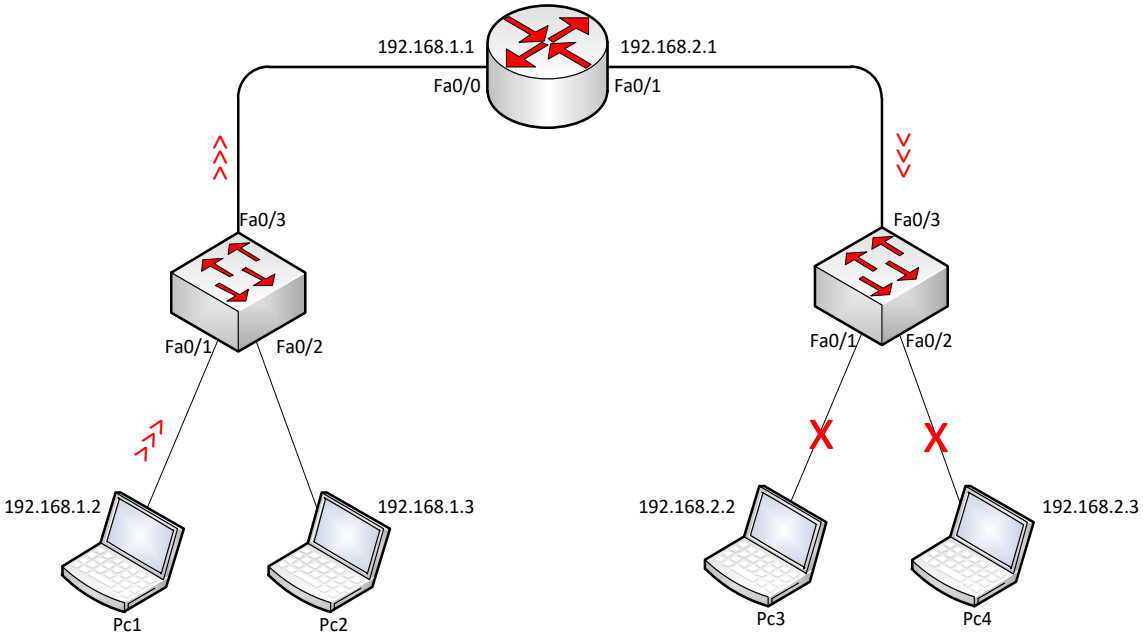
Access List استاندارد:

این نوع از Access List ها از شماره‌های ذکرشده در بالا استفاده می‌کنند و فقط ترافیک‌های مربوط به مبدأ را مورد بررسی قرار می‌دهند. با نحوه‌ی کار این Access List آشنا می‌شویم.

Deny: این دستور در access List برای جلوگیری از دسترسی یک Node خاص به یک شبکه‌ی دیگر است که بسیار پرکاربرد و خطرناک است، به دلیل اینکه با یک اشتباه، نصف یا کل شبکه از کار می‌افتد.

Permit: این دستور ضد دستور Deny است و برای دسترسی به شبکه کاربرد دارد.

در این مثال می‌خواهیم از دسترسی pc1 به Pc3 و Pc4 جلوگیری کنیم.



وارد روتر می‌شویم و دستورات زیر را به ترتیب وارد می‌کنیم:

Router(config)#**ip access-list standard dpc1**

در قسمت اول باید access List را تعریف کنیم؛ هم می‌توانیم با نام و هم می‌توانیم با شماره تعریف کنیم که در این قسمت از نام dpc1 استفاده کردیم. شما می‌توانید هر اسم دیگری در این قسمت قرار دهید و یا از شماره استفاده کنید، اما همیشه سعی کنید از نام استفاده کنید که مدیریت آن آسان باشد.

Router(config-std-nacl)#**deny 192.168.1.2 0.0.0.0**

با این دستور، ip address مربوط به pc1 را Deny می‌کنیم. اگر توجه کنید در قسمت اول، دستور Deny و بعد، ip address مربوط به‌pc1 و بعد از آن که مهم است از Wildcard Mask تأکیدی استفاده کردیم، یعنی استفاده از ٤ تا صفر که تأکید بر Deny کردن همین ip را دارد. اگر wild Card Mask را به صورت 0.0.0.255 وارد کنیم، یعنی تمام ip address ها در رنج 192.168.1.0 فیلتر شود، پس سعی کنید از Wild card Mask تأکیدی استفاده کنید.

Router(config-std-nacl)#**permit any**

بعد از Deny حتماً از Permit استفاده کنید، چون هر زمان که از Deny استفاده می‌کنید، بقیه‌ی شبکه هم deny می‌شود و به خاطر همین از Permit Any استفاده می‌کنیم تا بقیه‌ی شبکه اجازه‌ی دسترسی داشته باشند.

بعد از تعریف کامل access List باید به روتر بگوییم که این فیلترینگ را روی کدام پورت انجام بدهد، پس وارد روتر می‌شویم. اگر توجه کنید می‌خواهیم دسترسی pc1 به pc3 و pc4 جلوگیری کنیم، پس باید در پورت Fa0/1 روتر دستور زیر را وارد کنیم:

Router(config)# int f0/1

Router(config-if)#ip access-group dpc1 out

به دستور توجه کنید، ip Access-group را تعریف و بعد از آن، نام Access List که ایجاد کرده‌ایم را وارد می‌کنیم. گفتیم ترافیک این access List در زمان خروج از اینترفیس فیلتر شود. اگر به جای out، گزینه‌ی in را انتخاب می‌کردید، این بدان معنا بود که شما access List را برای شبکه‌ی 192.168.2.0 نوشتید که این امر اشتباه است و این access list عمل نمی‌کند.

و حالا اگر از pc1 به pc3 و pc4، Ping کنید، با پیام زیر مواجه می‌شوید:

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.

Reply from 192.168.1.1: Destination host unreachable.

Reply from 192.168.1.1: Destination host unreachable.

Reply from 192.168.1.1: Destination host unreachable.

و حالا اگر از طریق pc2 بخواهید pc3 و pc4 را Ping کنید، جواب خواهید گرفت.

PC>**ping 192.168.2.3**

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=127

Reply from 192.168.2.3: bytes=32 time=0ms TTL=127

Reply from 192.168.2.3: bytes=32 time=0ms TTL=127

Reply from 192.168.2.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

برای قرار دادن توضیحات روی یک Access List، باید از دستور Remark استفاده کرد:

Router(config-std-nacl)# remark Access List Deny Pc1

برای مشاهده‌ی این دستور باید وارد Running-config شوید تا این پیام را مشاهده کنید.

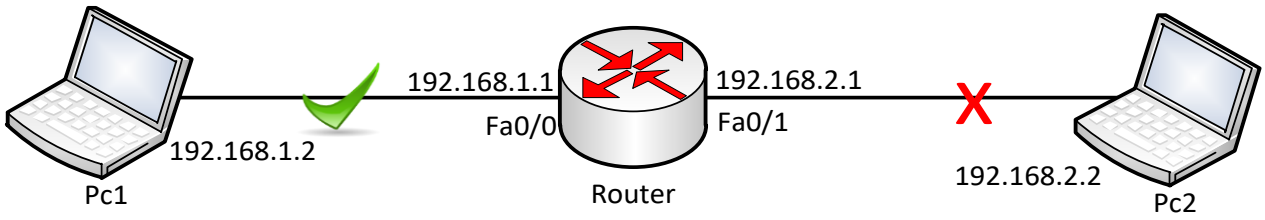
Router# **show Running-Config**

access-list 20 remark Access List Deny Pc1

Access List پیشرفته:

این نوع Access List از شماره‌های ۱۰۰ تا ۱۹۹ و ۲۰۰۰ تا ۲۶۹۹ تشکیل شده است و می‌تواند ترافیک مربوط به مبدأ و مقصد را مورد بررسی قرار دهد، حتی می‌توانید پروتکل‌ها یا برنامه‌های خاص را Deny یا Permit کنید.

مثال۵: در این مثال می‌خواهیم Telnet را روی روتر راه‌اندازی کنیم و accessList بنویسیم که از دسترسی Pc2 به Telnet جلوگیری کند.



وارد روتر می‌شویم و به صورت زیر عمل می‌کنیم:

Router(config)#**ip access-list extended Dpc2tel**

یک access List extended با نام Dpc2tel را ایجاد کردیم که شما می‌توانید به جای این نام از نام دلخواه یا از شماره‌های ذکرشده در قسمت قبل استفاده کنید.

Router(config-ext-nacl)# **deny tcp 192.168.2.0 0.0.0.255 any eq 23**

در این قسمت برای Deny کردن pc2 برای جلوگیری از Telnet، باید از پروتکل Tcp و پورت 23 که مربوط به Telnetاست را Deny کنید. در زیر جدول مربوط به پروتکل‌ها و شماره‌ی پورت‌ها مشخص شده است.

Decimal	Keyword	Description	Protocol
0		Reserved	
1-4		Unassigned	
20	FTP-DATA	FTP (data)	TCP
21	FTP	FTP	TCP
23	TELNET	Terminal connection	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Host name server	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		Unassigned	
160-223		Reserved	
162		FNP	UDP
224-241		Unassigned	
242-251		Unassigned	

Router(config-ext-nacl)# **deny tcp 192.168.2.0 0.0.0.255 any eq 23**

چون در اینجا قرار است که Telnet را برای pc2 ببندیم، از پروتکل TCP طبق جدول و از پورت ۲۳ که مربوط به Telnet است، استفاده می‌کنیم، پس به این صورت بخوانیم که Deny کن، پروتکل TCP را برای شبکه‌ی 192.168.2.0 با Wild Card mask، 0.0.0.255 و با پورت 23 که مربوط به Telnet است.

نکته: بعد از این کار، تمام ترافیک مربوط به شبکه‌ی 192.168.2.0 فیلتر می‌شود، به خاطر این باید از دستور زیر در آخر کار برای Permit دادن به بقیه‌ی شبکه استفاده کرد.

Router(config-ext-nacl)#**permit ip any any**

با این کار، pc2 می‌تواند با روتر ارتباط داشته باشد و فقط پروتکل Telnet بسته شده است. اگر یادتان باشد در access List standard همه‌ی ترافیک مربوط به یک دستگاه فیلتر می‌شد و حق دسترسی به هیچ عنوان نداشت، اما در accesslist Extended این چنین نیست و فقط pc2 نمی‌تواند Telnet کند، اما می‌تواند روتر را ping کند.

در ادامه باید این access List را روی پورت روتر فعال کنیم:

Router(config-if)#**ip access-group Dpc2tel in**

پس این دستور به این صورت خوانده می‌شود که Ip access-group Dpc2tel را بر روی این پورت به صورت ورودی فعال کن، ورودی یعنی این‌که Pc2 در حال ورود به روتر است. اگر از Pc2 به روتر Telnet کنیم، جواب نمی‌دهد.

PC>**telnet 192.168.2.1**

Trying 192.168.2.1 ...

% Connection timed out; remote host not responding

اما اگر به روتر ping کنیم، جواب می‌گیریم:

PC>**ping 192.168.2.1**

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255

Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

Reply from 192.168.2.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.2.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

دستور Show access-lists:

این دستور، تعداد Access List های موجود در روتر را با جزئیات نمایش می‌دهد:

Router(config)#**do sh ip access-list**

Extended IP access list Dpc2tel

دوستان توجه داشته باشید که دستورات به صورت خلاصه‌شده وارد شده است و چون در مد Global هستیم، در اول دستور از do استفاده کردیم.

دستور show access-list:

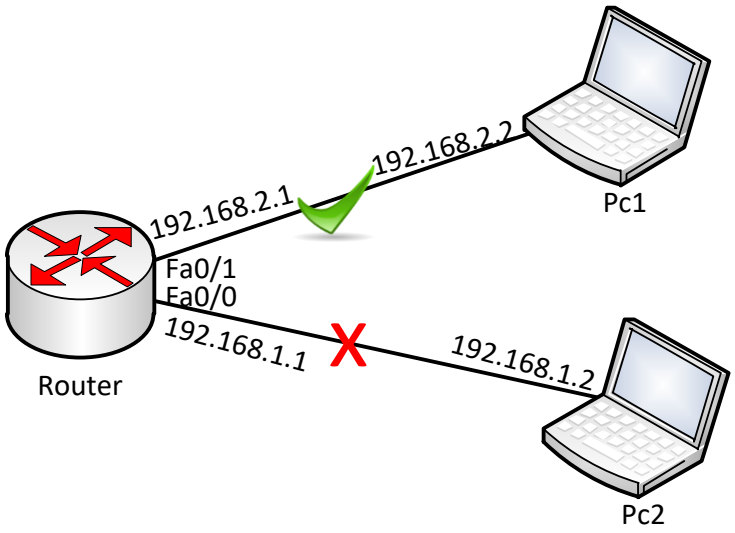
با این دستور می‌توانیم جزئیات یک access-list را مشاهده کنیم:

```
Router#show access-lists Dpc2tel
Extended IP access list Dpc2tel
    deny tcp 192.168.2.0 0.0.0.255 any eq telnet (24 match(es))
    permit ip any any (8 match(es))
```

در ادامه از access-List بسیار استفاده می‌کنیم و این دستور یک دستوراساسی در سیسکو است.

استفاده از Access-List در پورت مجازی VTY:

شما می‌توانید با تعریف یک ACCESS List و فعال کردن آن در پورت Vty به یک ip اجازه‌ی Telnet بدهید یا ندهید. برای انجام این کار به مثال زیر توجه کنید:



مانند شکل بالا، یک روتر و دو pc به صفحه اضافه و به هم متصل کنید و به پورت‌های مورد نظر ip دهید.

وارد روتر شوید و access-List زیر را وارد کنید:

```
Router(config)#ip access-list standard 10
Router(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

در دستورات بالا، یک access-list استاندارد با شماره‌ی ۱۰ تعریف کردیم و بعد از آن به شبکه‌ی 192.168.1.0 اجازه دسترسی دادیم و زمانی که یک Permit برای یک شبکه تعریف می‌کنیم، بقیه‌ی شبکه‌ها Deny می‌شوند.

بعد از ایجاد Access-list، وارد پورت Line Vty می‌شویم و telnet را روی پورت‌ها فعال می‌کنیم:

Router(config)#**line vty 0 15**

Router(config-line)#**password 123**

Router(config-line)#**login**

Router(config-line)#**access-class 10 in**

در دستور اول وارد پورت15 0 VTY می‌شویم و بعد، رمز عبور را بر روی پورت‌ها قرار می‌دهیم، سپس با دستور login می‌گوییم که در زمان telnet شدن، رمز عبور را درخواست کند و بعد از آن، با دستور access-class به این پورت می‌گوییم که در زمان telnet شدن، فقط ip address هایی را قبول کن که access-list 10 می‌گوید.

بعد از اتمام کار، اگر از طریق pc1 به روتر telnet کنید، جواب می‌گیرید، اما از طریق pc2 این امکان وجود ندارد.

بررسی CPPr

CPPr یا Control plane protection به مانند CoPP است با این تفاوت که بر جزئیات کار تمرکز دارد و می‌توانید مشخص کنید چه ترافیکی بررسی شود در زیر سه زیر شاخه در باره این موضوع را مشاهده می‌کنید:

Host subinterface : نشان دهنده‌ی ترافیک‌های عبوری است که مقصد آن خود دستگاه مورد نظر است.

Transit subinterface : ترافیکی که از دستگاه خارج می‌شود و ربطی به خود دستگاه ندارد.

CEF-Exception subinterface : مربوط به یک سری از ترافیک‌های به غیر از IP

بررسی Securing Routing Protocols

به طور پیش فرض دستگاه‌های شبکه اطلاعات جدول مسیریابی را به دیگر همسایه‌های ارسال می‌کنند و احراز هویتی هم بین آنها انجام می‌شود اما این احراز هویت به صورت Clear Text است و اطلاعات در مسیر قابل مشاهده است و به همین طریق مهاجمان می‌توانند آدرس‌های جعلی خود را در شبکه تبلیغ کنند، برای جلوگیری

از این خطر باید احراز هویت را بین دو روتر یا روترها با استفاده از الگوریتم MD5 ایجاد کنیم تا امنیت کار بسیار افزایش پیدا کند و رمزهای که ایجاد می‌کنیم به صورت Hash شده باشند.

فعال‌سازی تأیید اعتبار در به روزرسانی مسیریابی در OSPF

برای اینکه تایید اعتبار را در OSPF راه‌اندازی کنیم یک مثال را به طور کامل با هم بررسی می‌کنیم تا کل کار را متوجه شوید.

پروتکل OSPF(Open Shortest Patch First) یک پروتکل آزاد است و مختص شرکت خاصی نیست و توسط سازمان IETF در سال ۱۹۸۸ نوشته شده است، مانند Eigrp نیست که فقط در روترهای سیسکو قابل اجرا باشد، بلکه در تمام روترهای شرکت‌های مختلف کاربرد دارد.

پس اگر شما در شبکه‌های خود از روترهای مختلف با برندهای مختلف استفاده کنید، نمی‌توانید روی آن‌ها Eigrp اجرا کنید، بلکه فقط باید پروتکل OSPF یا RIP روی آن‌ها run کنید تا بتوانند باهم دیگر ارتباط برقرار کنند.

این پروتکل از مجموعه پروتکل‌های Link state است و زیرمجموعه‌ی پروتکل‌های IGPs است، یعنی داخل یک AS کار می‌کنند.

الگوریتمی که در این پروتکل استفاده می‌شود، Dijkstra است که شبکه را به صورت یک درخت بدون دور در نظر می‌گیرد.

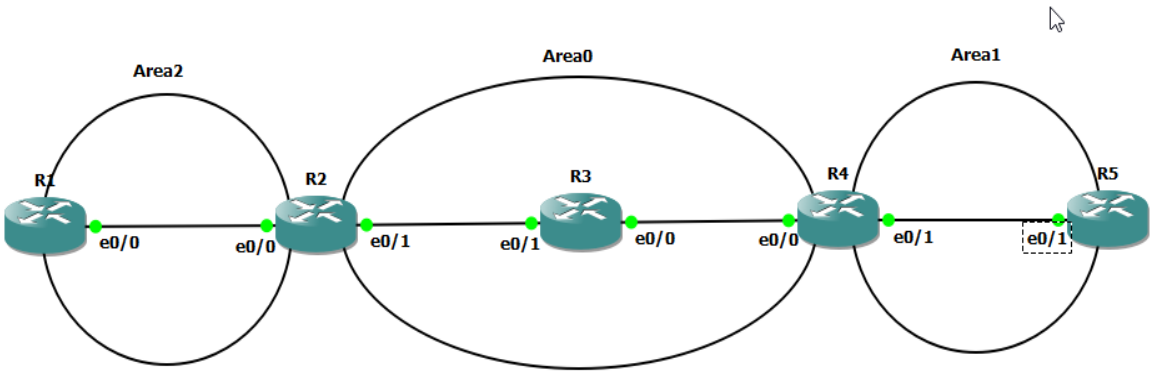
Ospf از جدولی به نام Link-satate Dtabase استفاده می‌کند که کل اطلاعات شبکه یا نقشه‌ی شبکه را برای انتخاب کوتاه‌ترین مسیر در خود ذخیره می‌کند و برای به دست آوردن کوتاه‌ترین مسیر از الگوریتمی به نام SPF استفاده می‌کند و بعد از پیدا شدن مسیر، آن را در جدول دیگری به نام Routing Table ذخیره می‌کند.

OSPF برای ارسال آپدیت از بسته‌هایی به نام LSA (Link-state Advertisement) استفاده می‌کند که اطلاعات جدول خود را به نام Link-state Database به روترهای دیگر ارسال می‌کند.

در مثال زیر، نحوه‌ی راه‌اندازی پروتکل OSPF را بررسی و امنیت را در آن اجرا می‌کنیم.

نکته: در مورد OSPF در کتاب آموزشی CCNA R& S که بنده آن را به نگارش در آوردم توضیحات کاملی دادم که می‌توانید آن را از وب سایت بنده دریافت کنید.

چهار روتر را به لیست اضافه کنید و به صورت زیر به هم متصل کنید، و طبق جدول آدرس IP را در Interface های آن وارد کنید.



	E0/0	E0/1	LoopBack
R1	172.16.1.1/24	--------	150.1.1.1/24
R2	172.16.1.2/24	172.16.2.1/24	150.1.2.2/24
R3	172.16.3.1/24	172.16.2.2/24	150.1.3.3/24
R4	172.16.3.2/24	172.16.4.1/24	150.1.4.4/24
R5	-------	172.16.4.2/24	150.1.5.5/24

بعد از تخصیص IP ها در روتر باید پروتکل OSPF را راه‌اندازی کنیم:

روتر R1 :

Router(config)#**router ospf 20**

تعریف Router OSPF 20 که ۲۰ یک شماره‌ی شناسایی برای این پروتکل است که تأثیری در روند کار ندارد، اما باید تعریف شود.

Router(config-router)#**router-id 150.1.1.1**

در این قسمت باید RID روتر را تعریف کنید که این IP مربوط به اینترفیس LoopBack است، پس بعد از ورود به پروتکل OSPF در درجه‌ی اول RID را تعریف کنید.

Router(config-router)#**network 172.16.1.1 0.0.0.0 area 2**

در این قسمت Network های مربوط به روتر را تعریف می‌کنیم و می‌گوییم که در کدام area قرار دارد، مثلاً در این قسمت، اینترفیس Fa0/0 روتر R1 در Area2 قرار دارد. در تعریف Network، اول خود Ip و بعد، Wild Card MASk مربوط به آن را وارد می‌کنیم که همان‌طور که در مطالب قبلی کتاب گفتیم، سعی کنید به جای Wild Card Mask از چهار صفر استفاده کنید (0.0.0.0).

در بقیه‌ی روترها هم همین کار را انجام دهید:

روتر R2:

Router(config)#router ospf 10

Router(config-router)#router-id 150.1.2.2

Router(config-router)#network 172.16.1.2 0.0.0.0 area 2

Router(config-router)#network 172.16.2.1 0.0.0.0 area 0

روتر R3:

Router(config)#router ospf 10

Router(config-router)#router-id 150.1.3.3

Router(config-router)#net 172.16.2.2 0.0.0.0 area 0

Router(config-router)#net 172.16.3.1 0.0.0.0 area 0

روتر R4:

Router(config)#router ospf 30

Router(config-router)#router-id 150.1.4.4

Router(config-router)#net 172.16.3.2 0.0.0.0 area 0

Router(config-router)#net 172.16.4.1 0.0.0.0 area 1

روتر R5:

Router(config)#router ospf 30

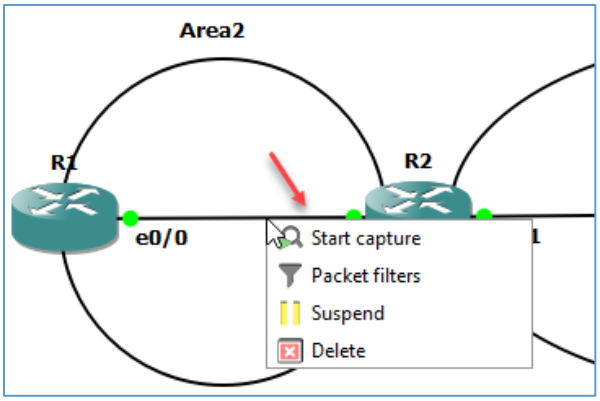
Router(config-router)#router-id 150.1.5.5

Router(config-router)#net 172.16.4.2 0.0.0.0 area 1

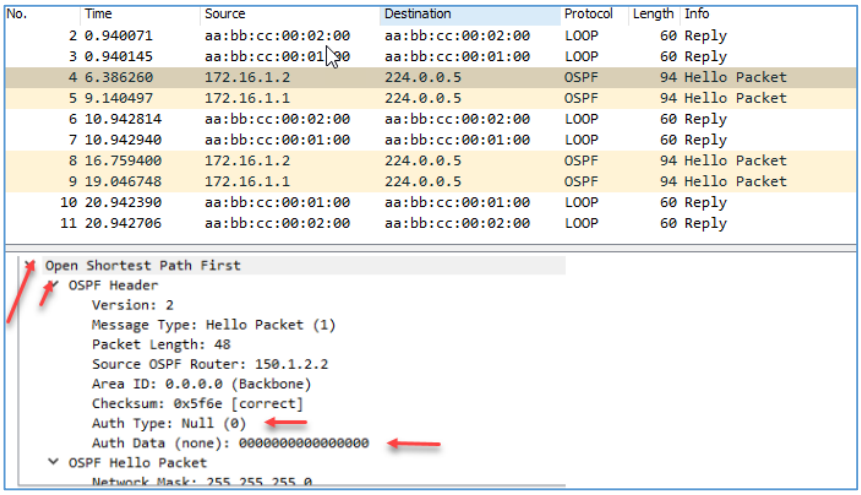
در این قسمت، از طریق فرمان Show Ip Route، نگاهی به جدول روتینگ روتر R1 می‌کنیم و این دستور را در مد Privileged وارد می‌کنیم:

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       150.1.1.0/24 is directly connected, Loopback0
L       150.1.1.1/32 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0
O IA    172.16.2.0/24 [110/20] via 172.16.1.2, 00:03:26, Ethernet0/0
O IA    172.16.3.0/24 [110/30] via 172.16.1.2, 00:02:29, Ethernet0/0
O IA    172.16.4.0/24 [110/40] via 172.16.1.2, 00:01:20, Ethernet0/0
```

همان‌طور که مشاهده می‌کنید، Network هایی که از طریق OSPF یاد گرفته است به صورت O IA نمایش داده است که O IA، بیانگر OSPF inter area است و نشان‌دهنده‌ی این است که این شبکه‌ها را از Area دیگری غیر از area خود یاد گرفته است و اگر یک روتر در area خود چیزی یاد بگیرد، آن را با حرف O ثبت می‌کند.



برای اینکه متوجه شویم امنیت کار چقدر ارزش دارد بر روی خط ارتباطس بین روتر R1 و R2 کلیک راست کنید و گزینه‌ی Start capture را کلیک کنید تا از طریق Wireshark بتوانیم جزئیات کار را مشخص کنیم.



در این تصویر گروتکل‌های OSPF را در تصویر مشاهده می‌کنید، اگر یکی از آنها را انتخاب کنید در قسمت Open Shortest path First و قسمت OSPF Header گزینه‌ی Auth Type برابر Null قرار گرفته که نشان دهنده این است که هیچ گونه امنیتی در این پروتکل لحاظ نشده و مهاجم به راحتی می‌تواند روتر خود را به عنوان یک همسایه جدید به Area مورد نظر اعلام کند و کل جدول مسیریابی را تغییر دهد، برای حل این مشکل باید دستورات امنیتی را بین دو یا چند روتر که در یک یا چند Area هستند اعمال کنیم.

برای مثال می‌خواهیم امنیت را بین روتر R1 و R2 برقرار کنیم که برای این کار باید به صورت زیر عمل کنید:

روتر R1 :

وارد Interface که در Area1 قرار دارد شوید و دستور زیر را وارد کنید:

```
R1(config-if)#int e0/0
```

فعال کردن الگوریتم message-digest با دستور زیر:

```
R1(config-if)#ip ospf authentication message-digest
```

در دستور زیر عدد یک می‌تواند بین 1 تا 65535 متغیر باشد که در اینجا عدد یک را انتخاب می‌کنیم و توجه کنید در روتر روبرو هم باید همین عدد را انتخاب کنید، بعد از ان الگوریتم MD5 و بعد یک رمز عبور پیچیده برای ان در نظر بگیرید.

```
R1(config-if)#ip ospf message-digest-key 1 md5 Test@12345
```

بعد از اجرای دستور بالا وارد OSPF شوید و دستور زیر را وارد کنید:

```
R1(config-if)#router ospf 20
R1(config-router)#area 1 authentication message-digest
```

بعد از اجرای کامل دستورات پیغام زیر را در صفحه مشاهده خواهید کرد که به این نکته اشاره دارد که ارتباط با روتر 150.1.2.2 که همان روتر R2 است قطع شده و دلیل آن هم این است که در R1 الگوریتم و رمز عبور را فعال کردید ولی در روتر R2 انجام ندادید.

```
*Dec  8 07:33:52.175: %OSPF-5-ADJCHG: Process 20, Nbr 150.1.2.2 on Ethernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

روتر R2 :

در روتر R2 هم دستورات زیر را وارد کنید:

```
R2(config-router)#int e0/0
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 Test@12345
R2(config-router)#router ospf 10
R2(config-router)#area 1 authentication message-digest
```

بعد از فعال کردن رمز دوباره ارتباط بین R1 و R2 را با استفاده از نرم‌افزار WireShark ارتباط آنها را بررسی می‌کنیم.

همانطور که در شکل زیر مشاهده می‌کنید قسمت OSPF Header به صورت کامل تغییر کرده است و به صورت کامل رمزنگاری شده است، کلمه Auth Crypt در شکل تایید کننده‌ی این موضوع است.

No.	Time	Source	Destination	Protocol	Length	Info
26	57.881031	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
27	58.791557	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
28	65.960267	172.16.1.1	224.0.0.5	OSPF	134	Hello Packet
29	67.871696	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
30	67.885823	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply
31	68.100145	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
32	74.987446	172.16.1.1	224.0.0.5	OSPF	134	Hello Packet
33	77.246053	172.16.1.2	224.0.0.5	OSPF	134	Hello Packet
34	77.872637	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60	Reply
35	77.886088	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60	Reply

```
Open Shortest Path First
  OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 150.1.2.2
      Area ID: 0.0.0.2
      Checksum: 0x0000 (None)
      Auth Type: Cryptographic (2)
      Auth Crypt Key id: 1
      Auth Crypt Data Length: 16
      Auth Crypt Sequence Number: 1575790762
      Auth Crypt Data: e46745b7e2fcddb07bd0e0e499475622
```

فعال‌سازی امنیت در پروتکل EIGRP

یکی از محبوب‌ترین پروتکل‌ها در دنیای امروز است و فقط روی دستگاه‌های سیسکو کاربرد دارد، یعنی اینکه این پروتکل ساخت سیسکو است و فقط روی ادوات سیسکو کار می‌کند، یکی از پرسرعت‌ترین پروتکل‌ها است که سرعت convergence یا هماهنگی بسیار بالایی دارد.

برای فعال‌سازی امنیت در EIGRP باید دستورات زیر را در روتر وارد کنید:

در دستور زیر یک نام برای دسته کلید خود در نظر بگیرید:

```
R1(config)#key chain profile_key
```

بعد یک ID برای ان مشخص کنید:

```
R1(config-keychain)#key 2122
```

بعد باید رمز عبور را وارد کنید که در ادامه از دسته کلیدی که استفاده کردیم و ایم رمز داخل آن قرار دارد می‌توانیم استفاده کنیم.

```
R1(config-keychain-key)#key-string Test@12345
```

در ادامه وارد Interface مورد نظر شوید و دستورات زیر را وارد کنید:

```
R1(config-keychain-key)#interface fast0/0
```

در دستور زیر عدد ۲۰۰ مربوط به AS پروتکل EIGRP است که روترها برای ارتباط باید از یک شماره‌ی مشخص استفاده کنند.

```
R1(config-if)#ip authentication mode eigrp 200 md5
```

در دستور زیر profile_key همان key chain یا دسته کلیدی است که در بالا تعریف کردیم

```
R1(config-if)#ip authentication key-chain eigrp 200 profile_key
```

شما باید دقیقاً همین دستورات را در روتر یا روترهای دیگر وارد کنید تا بتوانند به صورت امن با هم در ارتباط باشند.

امنیت در پروتکل RIP

این پروتکل یکی از محبوب‌ترین پروتکل‌های روتینگ و یکی از قدیمی‌ترین آن‌ها هم است. این پروتکل زیرمجموعه‌ی پروتکل‌های Distance Vector است و یک پروتکل IGPs است و در داخل یک AS(Autonomous System) کار می‌کند، در این قسمت می‌خواهیم امنیت را در این پروتکل به اجرا درآوریم، فقط به این نکته توجه کنید که راه‌اندازی امنیت فقط در ورژن ۲ پروتکل RIP پشتیبانی می‌شود و در ورژن ۱ این امکان وجود ندارد.

در کل تایید اعتبار به دو صورت Plaintext و MD5 در RIP صورت می‌گیرد که در ورژن 2 این پروتکل به صورت پیش‌فرض Plaintext فعال می‌شود ولی این نوع تایید اعتبار بسیار ضعیف و قابل مشاهده توسط مهاجمان است که باید MD5 را هم فعال کنید که برای این کار باید به صورت زیر عمل کنید.

در دستور زیر یک نام برای دسته کلید خود در نظر بگیرید:

```
R1(config)#key chain profile_key
```

بعد یک ID برای ان مشخص کنید:

```
R1(config-keychain)#key 2122
```

بعد باید رمز عبور را وارد کنید:

```
R1(config-keychain-key)#key-string Test@12345
```

در ادامه وارد Interface مورد نظر شوید و دستورات زیر را وارد کنید:

```
R1(config-keychain-key)#interface fast0/0
```

در دستور زیر عدد احراز هویت MD5 را فعال می‌کنیم:

```
R1(config-if)#ip rip authentication mode md5
```

در دستور زیر profile_key همان key chain یا دسته کلیدی است که در بالا تعریف کردیم و رمز را به آن متصل کردیم:

```
R1(config-if)#ip rip authentication key-chain profile_key
```

شما باید دقیقاً همین دستورات را در روتر یا روترهای دیگر وارد کنید تا در هنگام استفاده از پروتکل RIP به صورت کاملاً امن این کار صورت پذیرد.

نصب و راه‌اندازی نرم‌افزار CCO

هر شرکتی برای اینکه مشتریانش بتوانند راحت‌تر با محصولاتشان کار کنند یک محیط گرافیکی آماده کرده و مشری با چند کلیک و وارد کردن اطلاعات لازم می‌توان دستگاه مورد نظر را تنظیم کند، به خاطر همین موضوع شرکت سیسکو نرم‌افزار Cisco Configuration Professional را برای اینکار ایجاد و معرفی کرده است، در این قسمت می‌خواهیم این نرم‌افزار را با هم نصب و کار با آن را بررسی کنیم.

قبل از هر چیز باید نیازمنی‌های این نرافزار را بر روی سیستم مورد نظر خود نصب کنیم، که برای این منظور باید آخرین ورزن Flash Player و Java بر روی سیستم نصب شود تا بتوانید از این نرم‌افزار استفاده کنید.

برای دانلود نرم‌افزار JAVA Runtime به لینک زیر مراجعه کنید:

https://www.java.com/download/

و برای دانلود نرم‌افزار Flash Player از لینک زیر:

https://get.adobe.com/flashplayer/

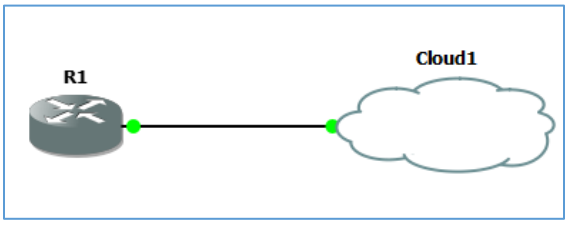
توجه کنید اگر سایت‌های مورد نظر اجازه دسترسی به آدرس‌های داخلی از داخل ایران را ندادن می‌توانید از سایت‌های فارسی استفاده کنید و نرم‌افزارها را دانلود کنید.

بعد از نصب دو پیش‌نیاز بالا می‌توانید از لینک زیر نرم‌افزار Cisco Configuration Professional را دانلود کنید:

https://software.cisco.com/download/home/281795035/type/282159854/release/3.5.2

بد از نصب نرم‌افزار سیستم را یک بار Restart کنید تا تنظیمات به درستی اعمال شود.

قبل از اینکه با نرم‌افزار کار کنیم باید روتر یا سوئیچ خود را به صورتی تنظیم کنیم که بشود از طریق این نرم‌افزار به تنظیمات دستگاه مورد نظر دست پیدا کرد.



برای اینکه یک روتر را به صورت مجازی تست بگیریم آن را به نرم‌افزار GNS3 اضافه می‌کنیم و یک Cloud هم به آ ن متصل می‌کنیم تا بتوانیم از شبکه خودمان به آن متصل شد.

در مرحله اول یک نام کاربری و رمز عبور در روتر تعریف می‌کنیم که سطح دسترسی آن ۱۵ باشد.

R1#**config terminal**

R1(config)#**username admin privilege 15 secret Test@12345**

در مرحله دوم باید سرویس HTTP و HTTPS را برای دسترسی نرم‌افزار به روتر فعال کرد.

R1(config)#**ip http server**

R1(config)#**ip http secure-server**

٪Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 2 seconds)

در مرحله سوم باید به روتر اعلام کرد که نام کاربری را از دیتابیس داخلی دریافت کند.

R1(config)#**ip http authentication local**

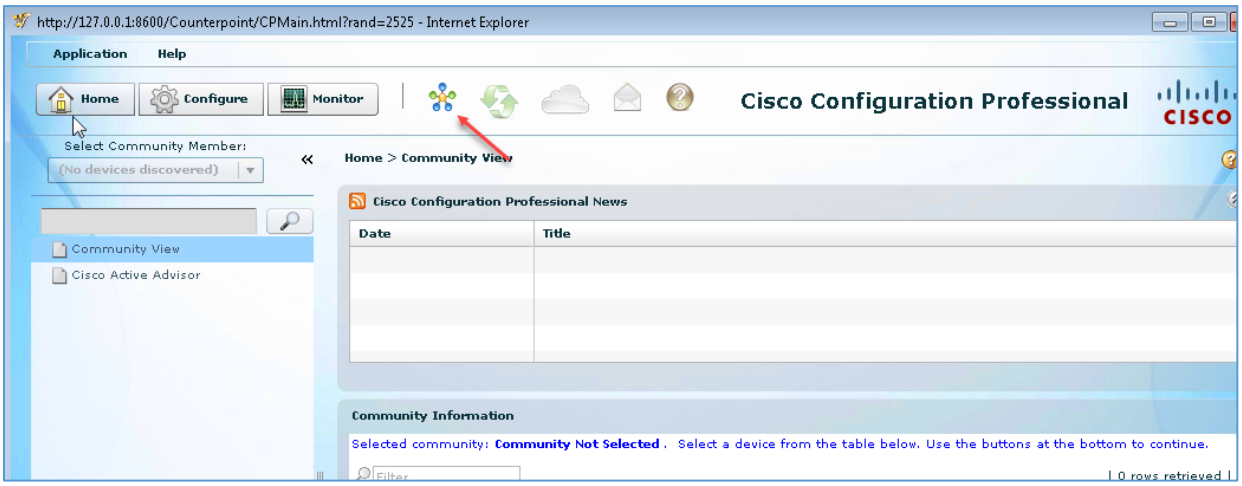
در مرحله آخر هم یک آدرس IP برای روتر در نظر می‌گیرم و پورت مورد نظر را روشن می‌کنیم.

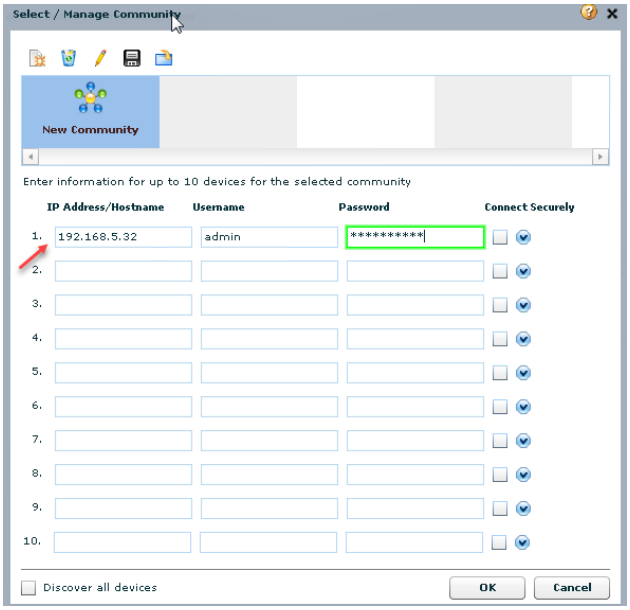
R1(config)#**int fastEthernet 0/0**

R1(config-if)#**ip address 192.168.5.32 255.255.255.0**

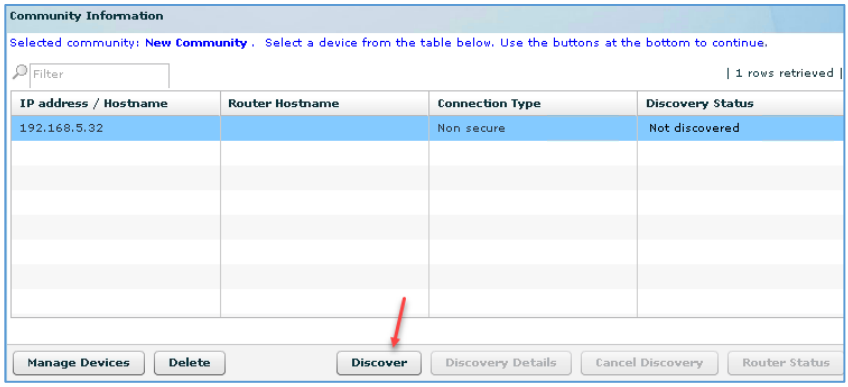
R1(config-if)#**no sh**

بعد از دانلود و نصب نرم‌افزار آن را اجرا کنید و به مانند شکل روبرو بر روی آیکون Manage Community کلیک کنید.



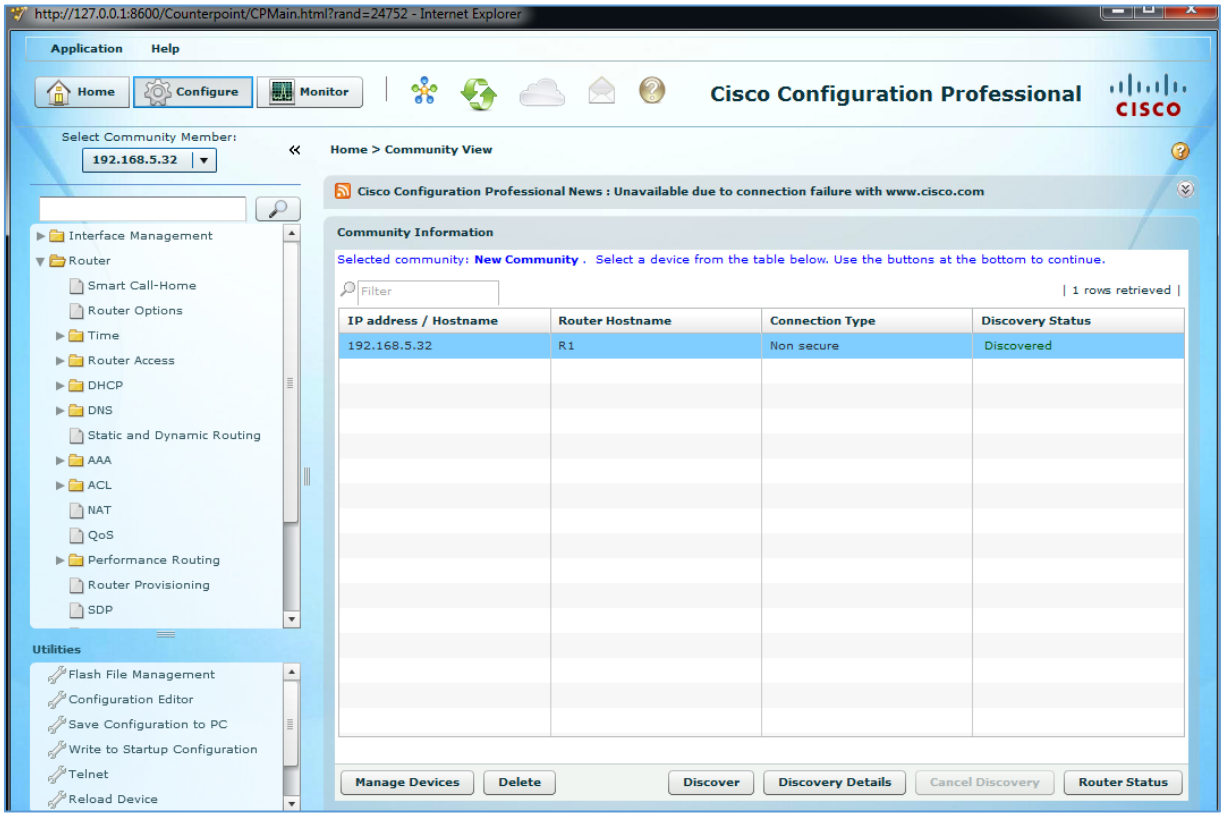


و در شکل باز شده باشد آدرس IP، نام کاربری، رمز عبور و نوع ارتباط HTTP یا HTTPS را با روتر مشخص کنید، نوع ارتباط پیش‌فرض HTTP است که اگر تیک گزینه‌ی Connect Security را انتخاب کنید ارتباط به صورت HTTPS خواهد بود.



در شکل زیر بعد از اضافه شدن روتر مورد نظر باید بر روی Discover کلیک کنید تا اطلاعات کامل روبرت بر روی نرم‌افزار Load شود.

برای اینکه تنظیمات و دستورات مورد نظر خود را بر روی روتر اعمال کنید باید به مانند شکل زیر وارد تب Configure شوید و گزینه‌ی مورد نظر خود را از لیست سمت چپ انتخاب کنید.



فصل چهارم – کار با ACS سیسکو

ACS مخفف کلمه‌ی Access Control Server است که کار آن بررسی هویت (Authentication) ، بررسی دسترسی‌ها (Authorization) و بررسی رویدادها (Accounting) است و مخفف کلمه‌ی معروف AAA است که از سه کلمه‌بالایی ایجاد شده است.

این نرم‌افزار در نوع خود یکی از قدرتمندترین نرم‌افزارها است و مختص شرکت سیسکو است، از طریق این نرم‌افزار می‌توانید همه دستگاه های موجود در شبکه را زیر مجموعه آن قرار دهید تا بتوانند اطلاعات کاربری و تایید هویت خودشان را از این سرور دریافت کنند تا از این طریق بتوانیم بر همه‌ی دستگاه‌ها شبکه مدیریت داشته باشیم.

یکی از ویژگی‌های این نرم‌افزار متصل شدن به سرویس Active Directory برای مدیریت کاربران است، زمانی که در این سرویس کاربری را تعریف می‌کنید، اطلاعات جدید به سرور ACS ارسال می‌شود و بعد می‌توانید به راحتی با آن نام کاربری وارد دستگاه یا نرم‌افزار مورد نظر شوید.

با استفاده از این نرم‌افزار مدیر شبکه می‌تواند پیچیده‌ترین سیاست‌ها یا همان Policy را برای کاربران و دستگاه‌های شبکه خود به راحتی ایجاد کند، این می‌تواند یکی از ویژگی‌های قدرتمند این نرم‌افزار باشد، یکی دیگر از ویژگی‌های این نرم‌افزار ارائه پکیج‌های آپدیت است که برای آن آماده و در سایت سیسکو قرار داده می‌شود، در ادامه کار، نحوه آپدیت کردن این نرم‌افزار را بررسی خواهیم کرد، البته آخرین تاریخ بروزرسانی نرم‌افزار طبق این لینک، در تاریخ August 31, 2022 به پایان خواهد رسید و بعد از آن شرکت سیسکو هیچ آپدیتی برای آن منتشر نخواهد کرد، البته سیسکو راه‌حل جایگزین آن را هم با ارائه نرم‌افزار ISE یا همان Identity Services Engine معرفی کرد که یک نسل جدیدتر از ACS است و در این کتاب بررسی خواهد شد.

برای شروع کار به آدرس زیر مراجعه و نرم‌افزار ACS را دانلود کنید:

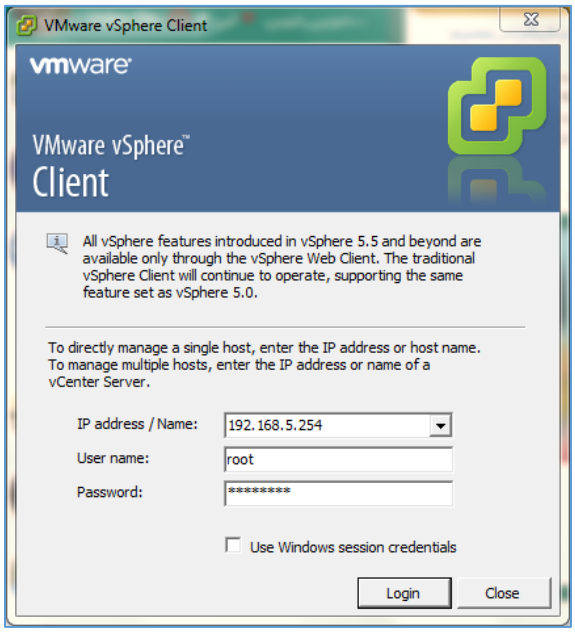
https://hellodigi.ir/other-hellodigi/download/1208-acs-v5-8-1-4.html

توجه داشته باشید برای نصب این نرم‌افزار می‌توانید از یک سیستم واقعی و یا از یک سیستم مجازی استفاده کنید که هر کدام باید مقدار سخت‌افزار مورد نیاز را که در لیست زیر مشاهده می‌کنید پشتیبانی کنند:

مقدار سخت‌افزار مورد نیاز برای راه اندازی ACS

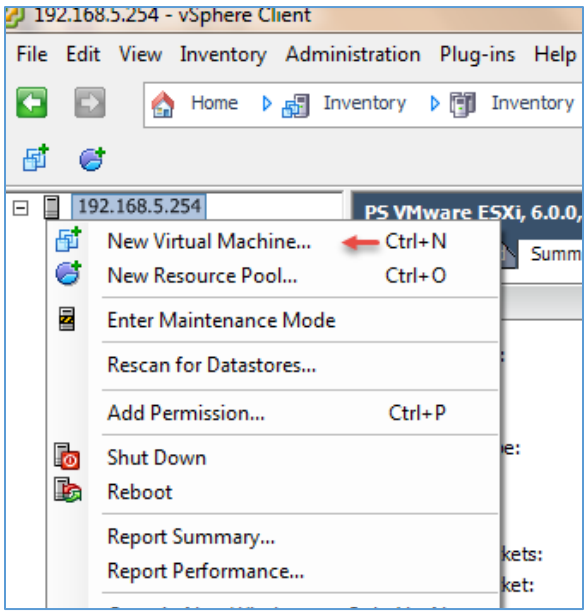
نوع سخت‌افزار	حداقل نیازمندی
CPU	2 CPUs (dual CPU, Xeon, Core2 Duo or 2 single CPUs) 2 GHz CPU speed
Memory	4 GB
Hard Disk	A minimum of 60 GB is required Maximum storage is up to 750 G.
NIC (Network Interface Card)	1 Gb dedicated NIC interface
Hypervisor	VMware ESXi 5.5 VMware ESXi 5.5 Update 1 VMware ESXi 5.5 Update 2 VMware ESXi 5.5 Update 3 VMware ESXi 6.0 Update 2

همان‌طور که در جدول بالا مشاهده می‌کنید، سخت‌افزار قدرتمندی برای اجرای نرم‌افزار ACS نیاز ندارید و با یک سیستم معمولی و یا ماشین مجازی می‌توانید این سرور را راه‌اندازی کنید، هارد دیسکی که برای این سرور در نظر می‌گیرد حداقل باید ۶۰ گیگابایت فضا داشته باشد تا دیتابیس‌ها بتوانند درآن ذخیره شوند، البته اگر می‌خواهید از Log دیتابیس هم استفاده کنید باید فضای هارد دیسک شما حداقل ۵۰۰ گیگابایت باشد.

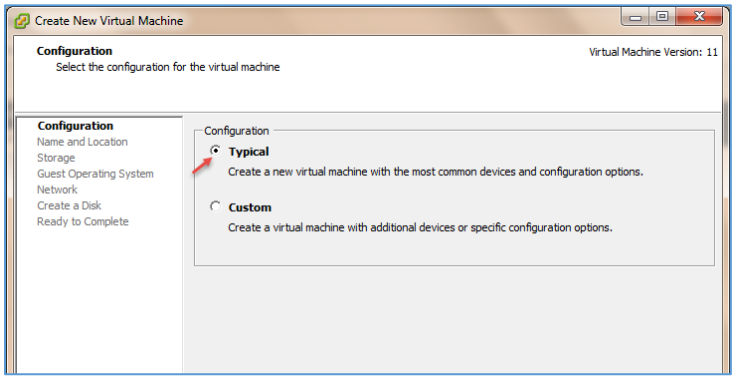


در این کتاب برای راه‌اندازی این نرم‌افزار از سرور ESXI استفاده کردیم که البته شما می‌توانید از نرم‌افزار VMware Workstation هم برای این کار استفاده کنید، توجه داشته باشید که آموزش نرم‌افزار VMware در کتاب « VMware Systems» موجود است و می‌توانید از طریق سایت آن را دانلود و مطالعه کنید.

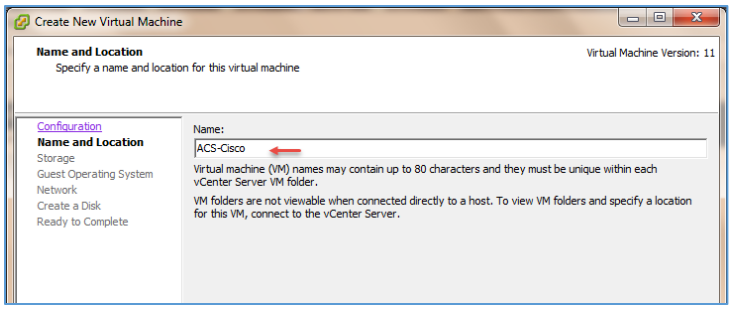
برای متصل شدن به سرور ESXi از نرم‌افزار VMware Vsphere استفاده می‌کنیم و به مانند شکل روبرو به آن متصل می‌شویم.



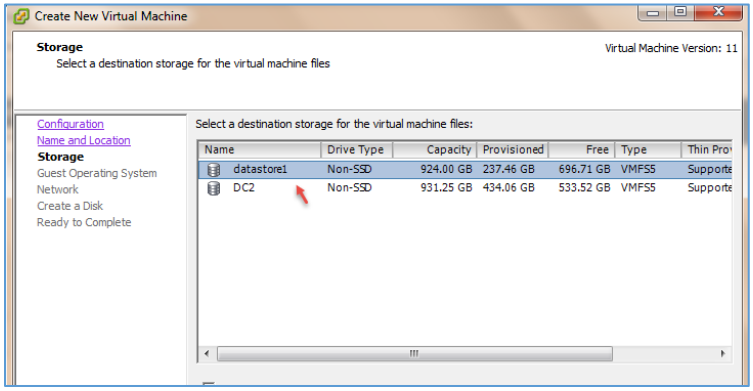
بعد از ورود به سرور بر روی آدرس سرور کلیک راست کنید و گزینه‌ی New Virtual Machine را انتخاب کنید.



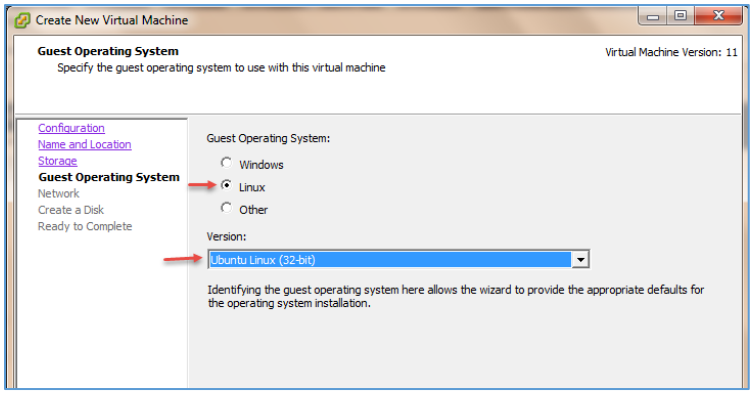
برای راه‌اندازی سریعتر، گزینه‌ی Typical را انتخاب و بر روی Next کلیک کنید.



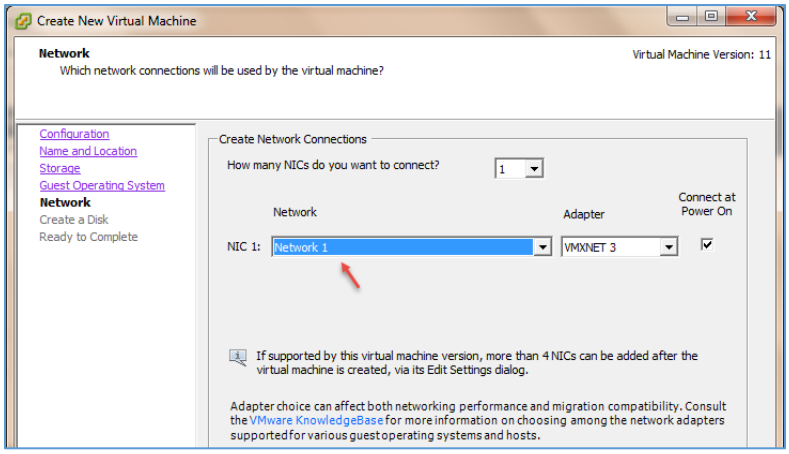
در این صفحه نام مورد نظر خود را برای این ماشین مجازی وارد و بر روی Next کلیک کنید.



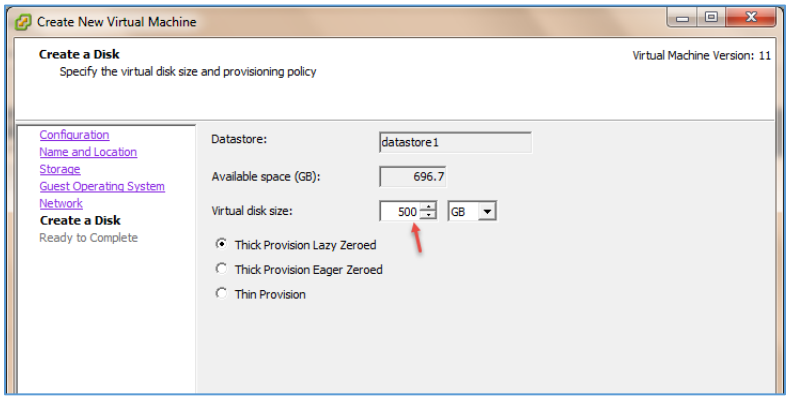
در این صفحه باید محل ذخیره ماشین بر روی هارد دیسک سرور را مشخص کنید که در اینجا هارد یا DataStore را انتخاب می‌کنیم که فضای کافی برای این ماشین داشته باشد.



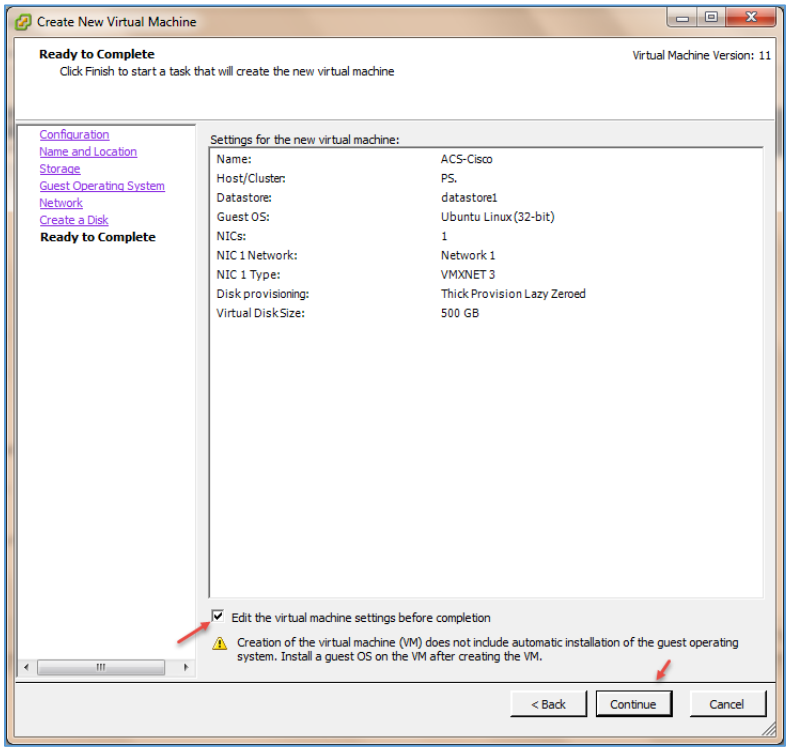
در این قسمت باید سیستم‌عامل لینوکس را انتخاب کنید، به خاطر اینکه، ACS بر پایه لینوکس پیاده سازی شده است، در قسمت ورژن هم Ubuntu Linux (32 bit) را انتخاب کنید و بر روی Next کلیک کنید.



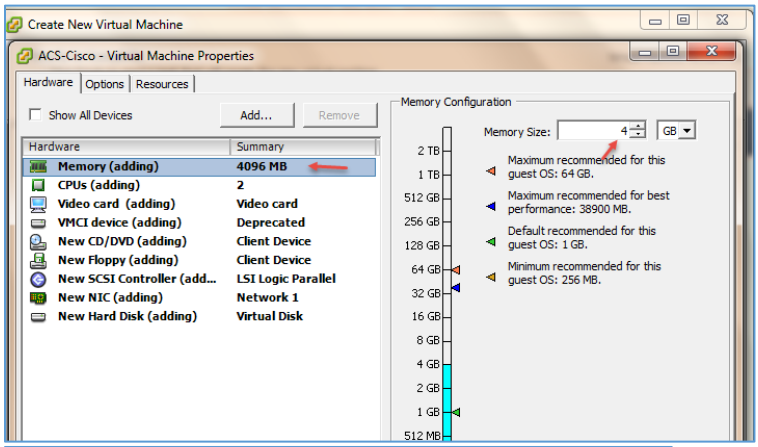
در این قسمت، کارت شبکه مربوط به سرور را انتخاب و بر روی Next کلیک کنید.



در این قسمت باید مقدار هارد دیسک را مشخص کنید که همانطور که قبلاً بیان کردیم باید حداقل ۵۰۰ گیگابایت فضا برای آن در نظر بگیرید.

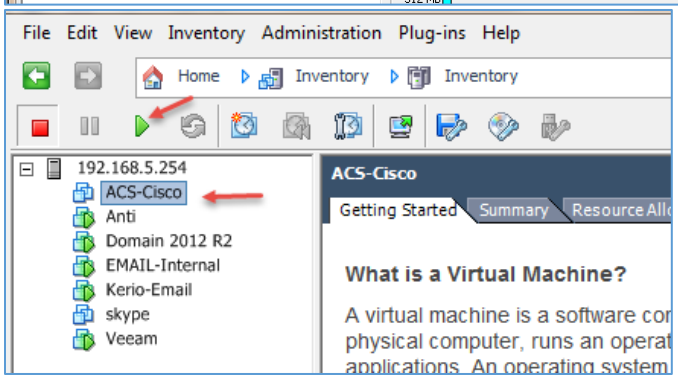


در این صفحه اطلاعات ماشین مجازی خود را مشاهده می‌کنید، تیک گزینه‌ی Edit The... را انتخاب و بر روی Continue کلیک کنید.

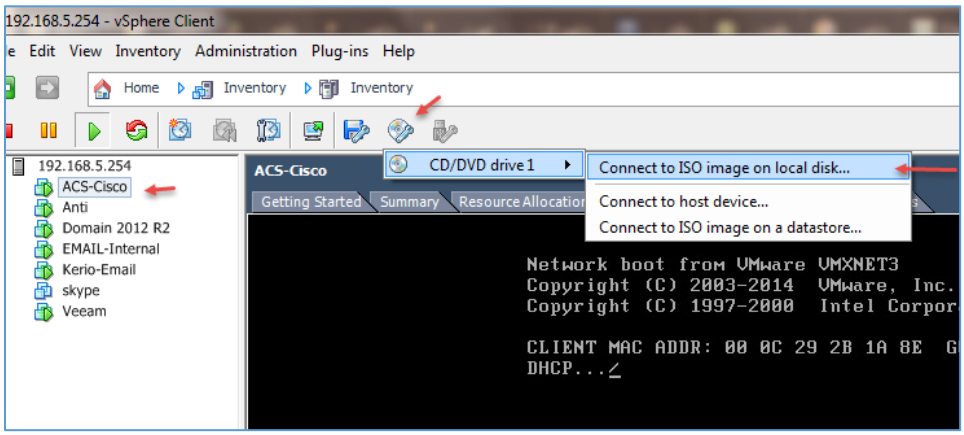


در صفحه تنظیمات ماشین مجازی مقدار رم را به ٤ گیگابایت تغییر دهید و مقدار هسته CPU را ۲ در نظر بگیرید.

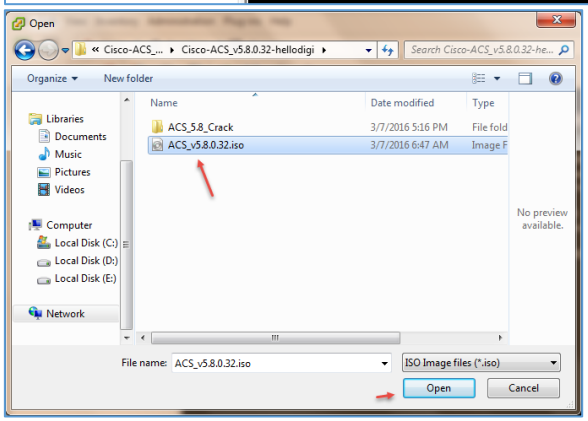
با این کار ماشین مورد نظر ایجاد و برای نصب ACS آماده شده است.



به مانند شکل بعد از ایجاد ماشین مورد نظر بر روی آیکون Power On کلیک کنید تا ماشین مورد نظر روشن شود، البته باید بعد از روشن شدن ماشین فایل ACS را به آن معرفی کنیم.

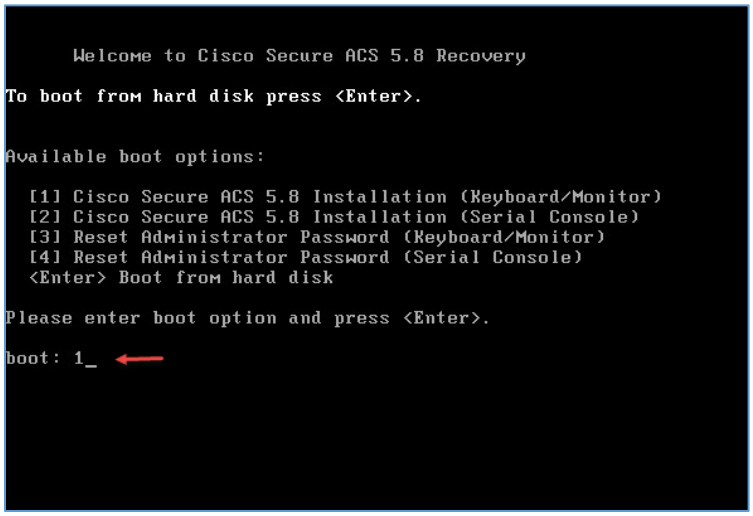


ماشین مورد نظر را انتخاب کنید و از ابزار بالای آن بر روی Connect کلیک کنید و گزینه‌ی اول را انتخاب کنید.

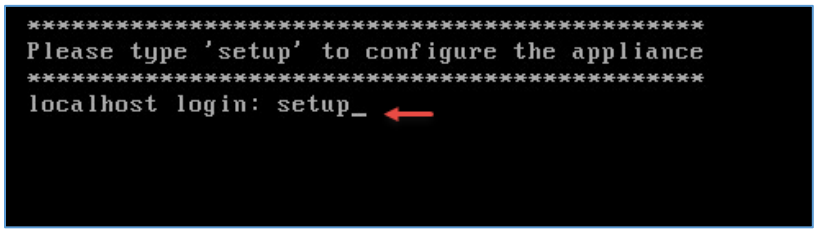


در این قسمت باید فایل با پسوند ISO را انتخاب و بر روی Open کلیک کنید.

همان‌طور که مشاهده می‌کنید فایل ACS اجرا شده است و چند گزینه برای شما به نمایش گذاشته شده است، برای شروع کار و نصب نرم‌افزار، شماره‌ی یک را وارد و بر روی Enter فشار دهید.



بعد از نصب صفحه Login ظاهر خواهد شد و برای شروع کار باید کلمه Setup را وارد کنید.



بعد از وارد کردن کلمه‌ی Setup سوالاتی از شما پرسیده خواهد شد که جدول آن به صورت زیر خواهد بود.

دستور	پیش فرض	شرایط	توضیحات
Host Name	*localhost*	اولین حرف باید یک کاراکتر ASCII باشد. حداقل ۳ و حداکثر ۱۵ کلمه می‌باشد. اولین حروف باید یک حرف باشد و حروف‌های معتبر A-Z و ۰-۹ و - است.	نام میزبان یا دستگاه مورد نظر را وارد کنید.
IPV4	چیزی وارد نشده	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵	وارد کردن آدرس IP
IPv4 Netmask	چیزی وارد نشده	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵	وارد کردن Subnet مربوطه
IPv4 Gateway	چیزی وارد نشده	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵	آدرس Gateway یا همان روتر را وارد کنید

Domain Name	چیزی وارد نشده	نیاز به وارد کردن IP نیست و باید نام وارد شود	نام دومین خود را وارد کنید
IPv4 Primary Name Server Address	چیزی وارد نشده	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵	آدرس DNS سرور خود را وارد کنید
Add another nameserver	چیزی وارد نشده	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵	آدرس DNS سرور دیگری را که در شبکه دارید وارد کنید
NTP Server	time.nist.gov	آدرس مجاز بین ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵ وارد و یا اینکه نام سرور را وارد کنید.	نام دومین یا ip آن را وارد کنید
Timezone	UTC	باید یک منطقه زمانی درست را وارد کنید.	منطقه زمانی معتبر را وارد کنید
SSH Service	چیزی وارد نشده		برای فعال‌سازی سرویس SSH باید Y را وارد کنید
Username	admin	به صورت پیش‌فرض اگر چیزی در این قسمت وارد نکنید نام کاربری Admin است، ولی می‌توانید آن را تغییر دهید تعداد حروف باید بین ۳ تا ۸ کاراکتر باشد و حروه A-Z و 0-9 قابل قبول است	نام کاربری را وارد کنید
Admin Password	چیزی وارد نشده	به صورت پیش‌فرض رمز عبوری برای نام کاربری Admin وارد نشده است و شما باید رمز عبور را وارد کنید. رمز عبور باید حداقل ٦ کاراکتر و به صورت پیچیده باشد.	رمز عبور را وارد کنید.

	لطفاً این رمز عبور را در جای مناسب حفظ کنید، چون راه دیگری برای دسترسی به سرور ندارد. توجه داشته باشید که در صورتی که رمز عبور خود را فراموش کردید، باید از طریق DVD مربوط به ACS آن را برگردانید.		

همانطور که مشاهده کردید تمام دستورات با جزئیات آن در جدول بالا بررسی شد، در این قسمت می‌خواهیم به صورت عملی این کار را انجام دهیم.

localhost login: **setup**

Enter hostname []: **ACS-Center**

Enter IP address []: **192.168.5.22**

Enter IP default netmask []: **255.255.255.0**

Enter IP default gateway []: **192.168.5.35**

Enter default DNS domain []: **int.net**

Enter primary nameserver []: **192.168.5.100**

Add secondary nameserver? Y/N: **N**

Add primary NTP server [time.nist.gov]: **192.168.5.100**

Add secondary NTP server? Y/N: **N**

Enter system timezone [UTC:]

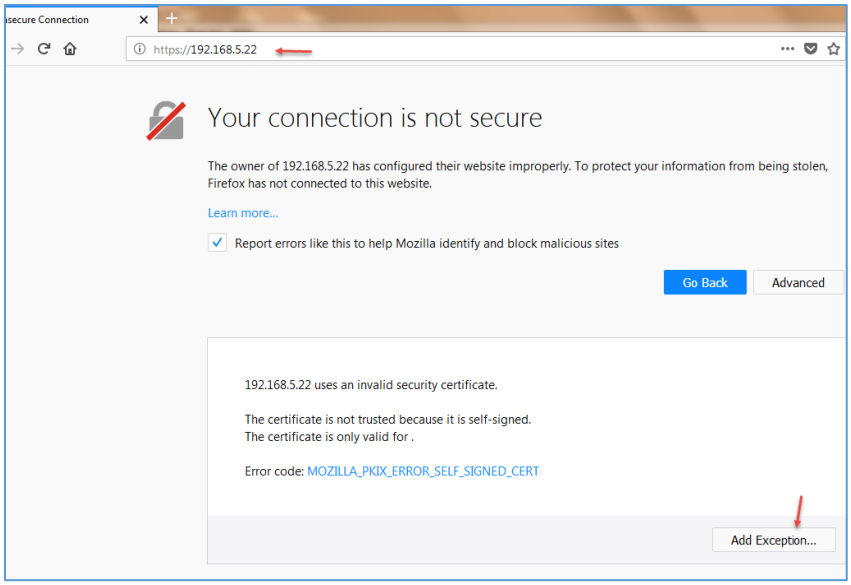
Enable SSH service? Y/N [N]: **y**

Enter username [admin]: **Root**

Enter password: **Test@12345**

Enter password again: **Test@12345**

با وارد کردن اطلاعات بالا سرور مورد نظر تنظیمات را دریافت و ذخیره می‌کند و بعد از آن سرور Restart خواهد شد.



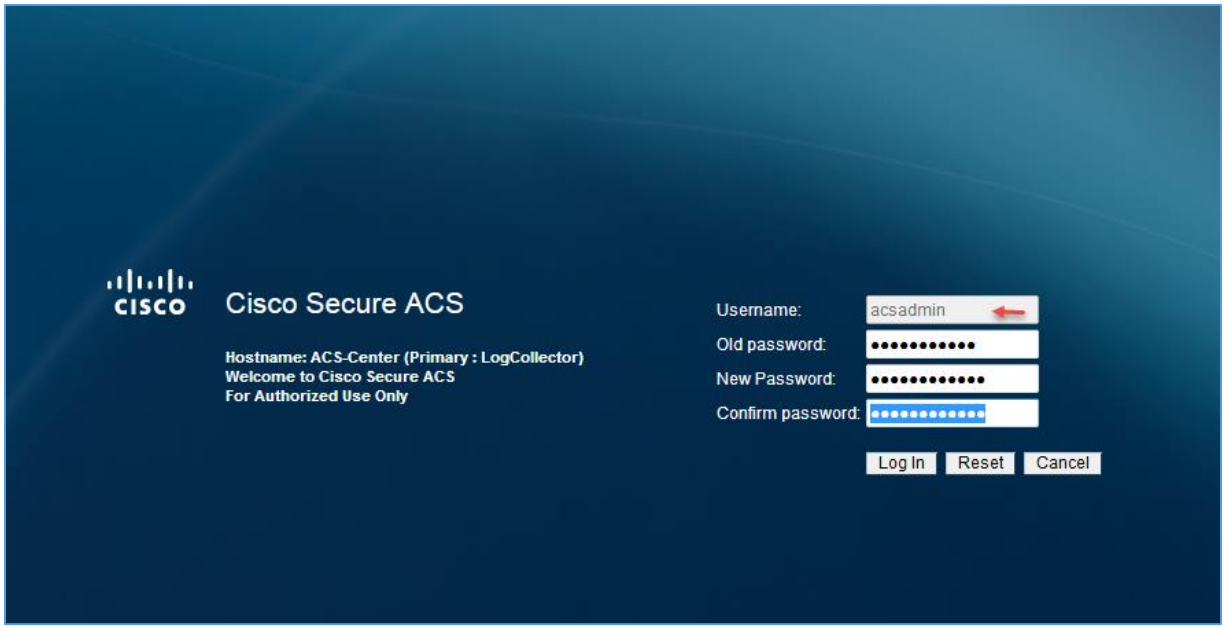
بعد از نصب نرم‌افزار ACS باید وارد مرورگر شوید و آدرس آن را به صورت https وارد کنید، به خاطر اینکه از گواهینامه معتبر استفاده نمی‌کنید، با اخطار روبرو مواجه خواهید شد که باید بر روی Add Exception کلیک کنید، البته بهترین عملکرد ACS را می‌توانید با Internet Explorer تجربه کنید.

بعد از باز شدن صفحه Login باید نام کاربری و رمز عبور پیش‌فرض را وارد کنید.

نام کاربری: acsadmin

رمز عبور: default

بعد از وارد کردن از شما رمز عبور جدید درخواست می‌شود که باید به صورت پیچیده به مانند Test@12345

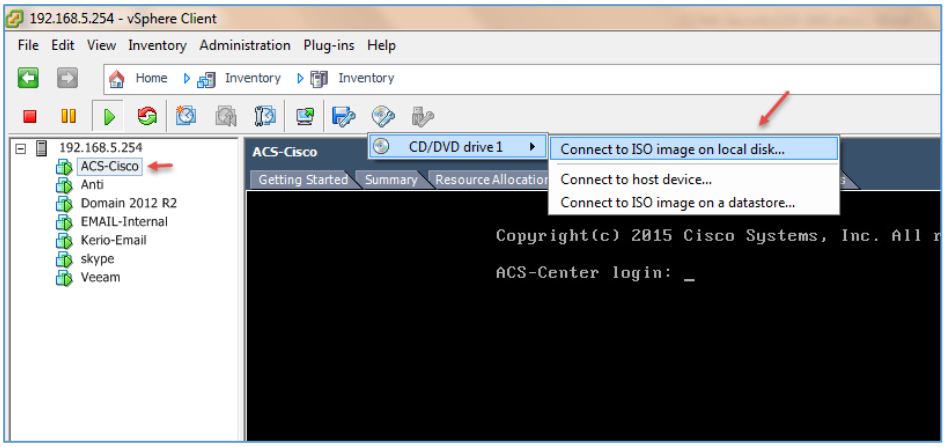


وارد کنید وبر روی Log in کلیک کنید، بعد از کلیک بر روی Login دوباره از شما برای ورود نام کاربری و رمز عبور جدید درخواست می‌کند که باید وارد کنید تا وارد صفحه مدیریتی شوید.

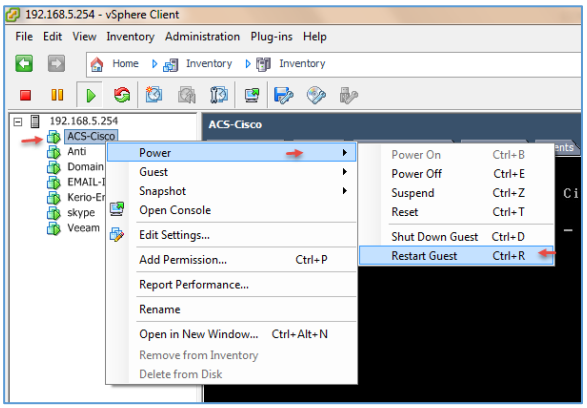
در این صفحه از شما لایسنس درخواست می‌شود که باید بر روی Browse کلیک و لایسنس نرم‌افزار ACS را انتخاب کنید، متاسفانه در ایران همه چیز کرک شده و لایسنس این نرم‌افزار هم به صورت کرک شده موجود است.

برای کرک کردن این نرم‌افزار راه‌های متفاوتی وجود داره که در این قسمت یکی از آنها را انجام خواهیم داد.

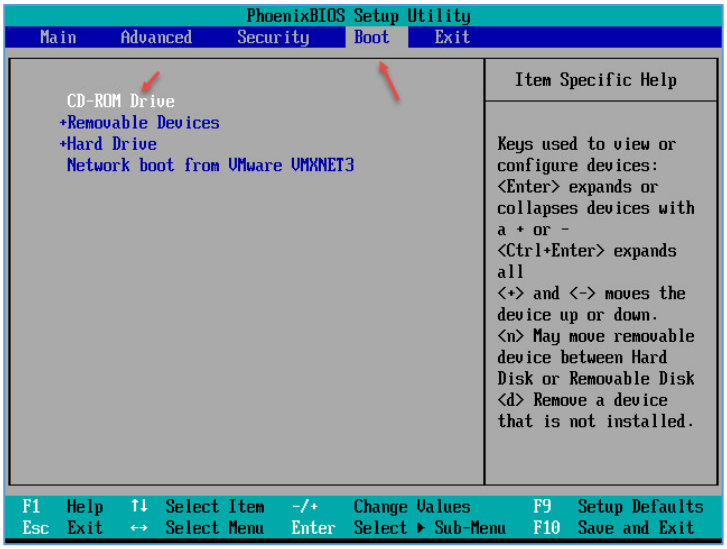
برای کرک کردن این نرم‌افزار نیاز به یک سیستم‌عامل لینوکس داریم که به صورت Live آن را اجرا کنیم و پوشه‌های مربوط به ACS را دستکاری کنیم، برای این کار می‌توانیم از لینوکس Ubuntu یا Kali یا هر سیستم عامل لینوکسی دیگری استفاده کنیم، در این قسمت از سیستم عامل Kali استفاده می‌کنیم.



برای شروع وارد سرور ESXi می‌شویم و ماشین مورد نظر را از لیست انتخاب و به مانند شکل بر روی گزینه‌ی مورد نظر کلیک کنید تا بتوانید فایل ISO مربوط به لینوکس Kali



را به ماشین مجازی اضافه کنید، بعد از انجام کار بالا به مانند شکل روبرو بر روی ماشین مجازی کلیک راست کنید و از قسمت Power گزینه‌ی Restart Guest را انتخاب کنید تا به صورت نرم‌افزاری سرور Restart شوید.

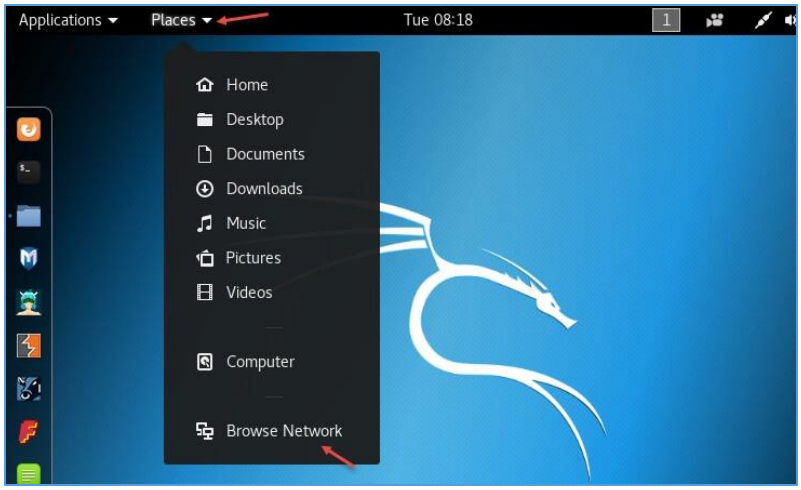


بعد از Restart شدن دکمه F2 را از صفحه کلید انتخاب کنید تا وارد تنظیمات Setup شوید، بعد از ورود وارد تب Boot شوید و گزینه‌ی CD-Rom Drive را با کلید + و – به بالای لیست ارجاع دهید و بعد کلید F10 را فشار دهید و گزینه‌ی YES را انتخاب کنید تا تنظیمات ذخیره شود و ماشین Restart شود.

بعد از انجام این کار فایل ISO مربوط به لینوکس Kali اجرا خواهد شد.

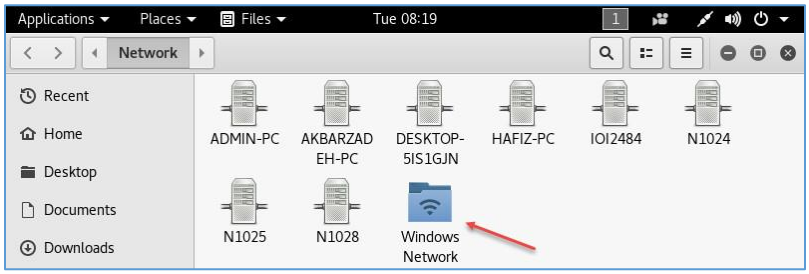
همانطور که مشاهده می‌کنید، صفحه بوت مربوط به Kali را مشاهده می‌کنید، گزینه‌ی Live را انتخاب کنید تا لینوکس بدون نصب و بر روی فایل مورد نظر اجرا شود.

صفحه اول لینوکس Kali را مشاهده می‌کنید، برای اینکه کار کرک را انجام دهیم باید فایل لایسنس کرک شده را وارد لینوکس کنید و در مسیر فایل ACS که در درایو است کپی کنید، برای انتقال فایل به Kali باید فایل مورد نظر را در شبکه Share کنید و آن را بر روی Kali قرار دهید.

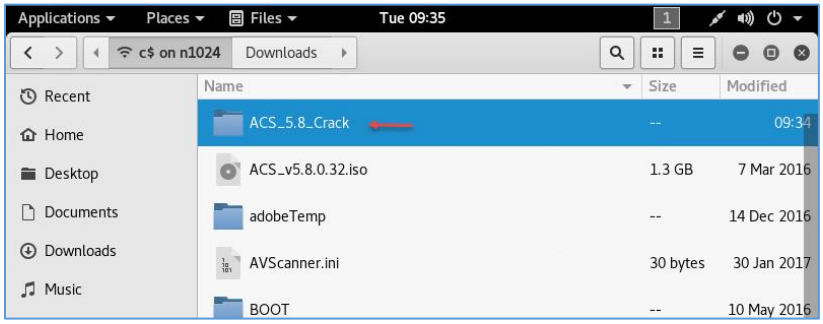


به مانند شکل روبرو از منوی Places گزینه‌ی Browse را انتخاب کنید.

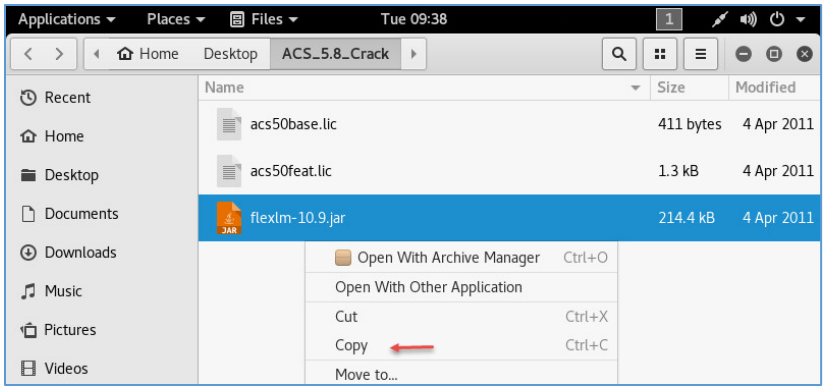
نکته: می‌توانید فایل لایسنس را در یک فایل ISO قرار دهید و آن را به ماشین ACS متصل کنید و از طریق KALI به راحتی آن را باز کنید.



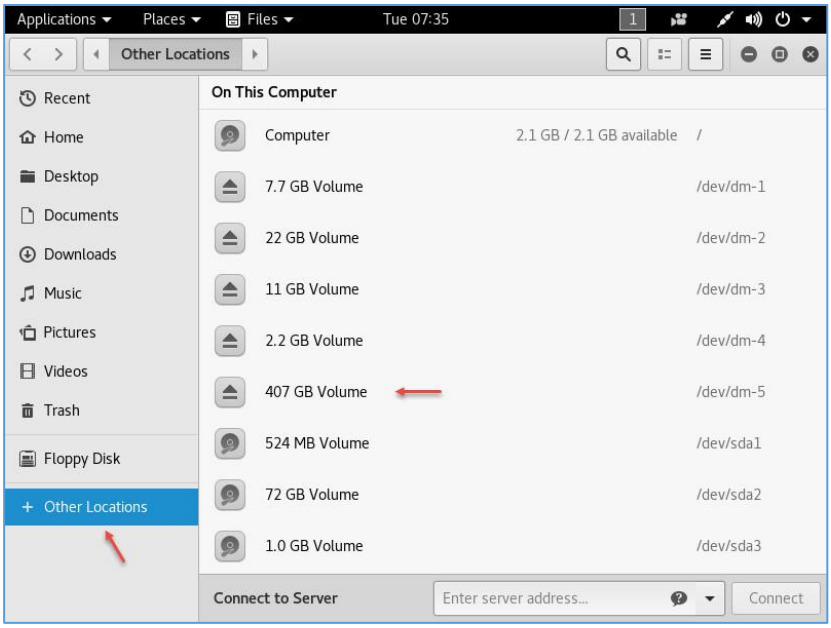
در این صفحه سیستم‌های در دسترس را مشاهده می‌کنید، اگر سیستم خود را در لیست مشاهده نمی‌کنید می‌توانید بر روی Windows Network کلیک کنید و وارد سیستم خود شوید.



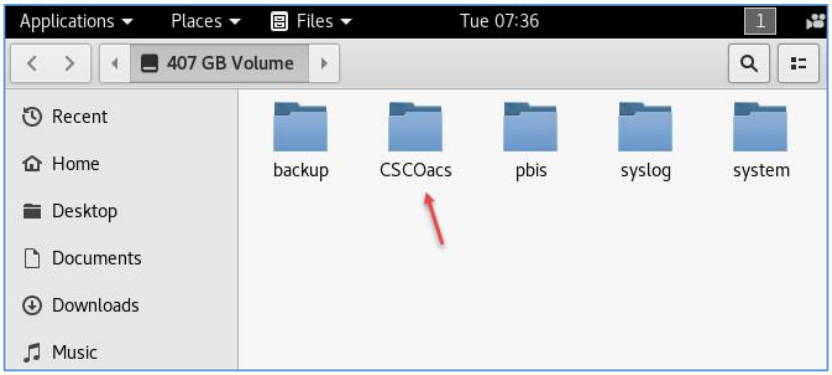
همان‌طور که مشاهده می‌کنید پوشه کرک از طریق شبکه در دسترس قرار گرفته است و برای استفاده از آن شما باید آن را کپی و در Desktop ذخیره کنید تا ادامه کار را با هم انجام دهیم.



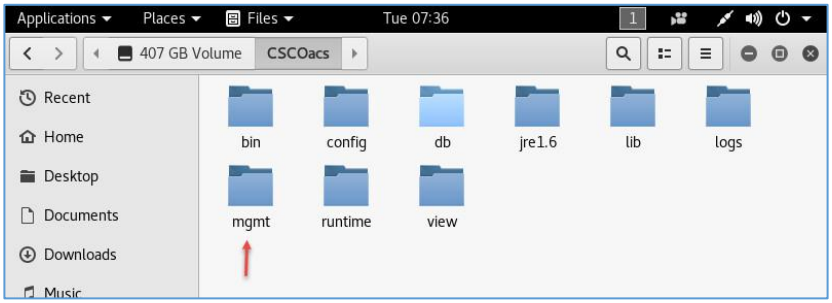
وارد پوشه مورد نظر شوید و بر روی فایل flexlm-10.9.jar کلیک راست کنید و گزینه‌ی کپی را انتخاب کنید.



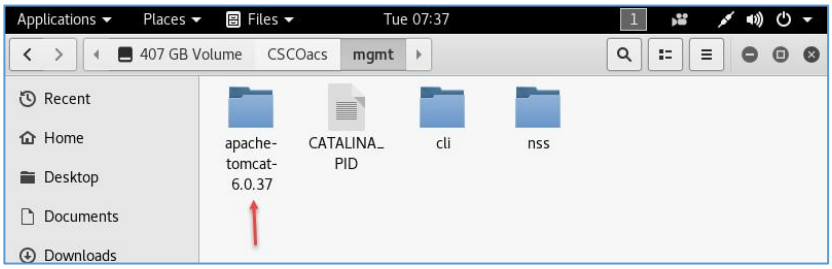
بعد از Copy از فایل مورد نظر باید وارد پوشه مربوط به نرم‌افزار ACS شوید و این فایل را با فایل اصلی جایگزین کنید، برای این کار از سمت چپ بر روی Other Location کلیک کنید، در این صفحه چندین هارد دیسک را مشاهده می‌کنید که باید بررسی کنید که فایل ACS در کدام درایو قرار دارد، در این سیستم فایل مورد نظر در درایو dm-5 وجود دارد بر روی آن دو بار کلیک کنید.



در این صفحه باید وارد پوشه CSCOacs شوید که مربوط به نرم‌افزار ACS است.

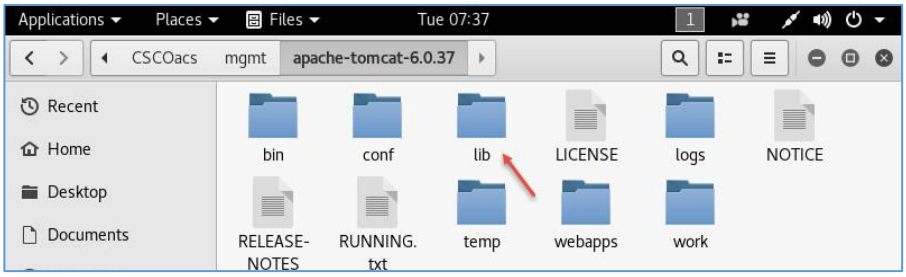


در این صفحه وارد پوشه mgmt شوید.

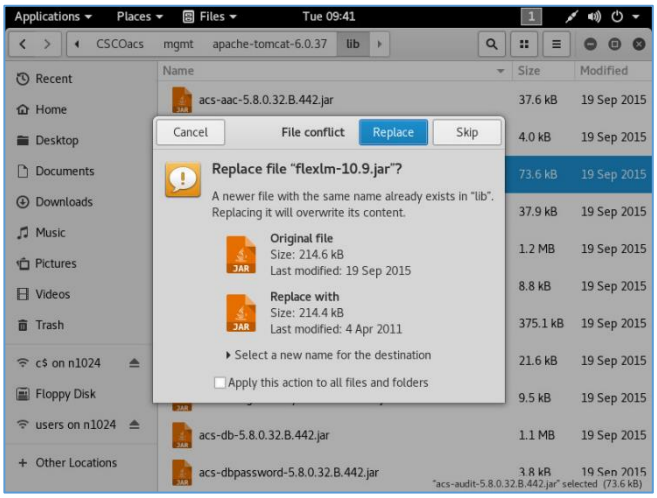


وارد پوشه Apach-tomcat-6.0.37 شوید.

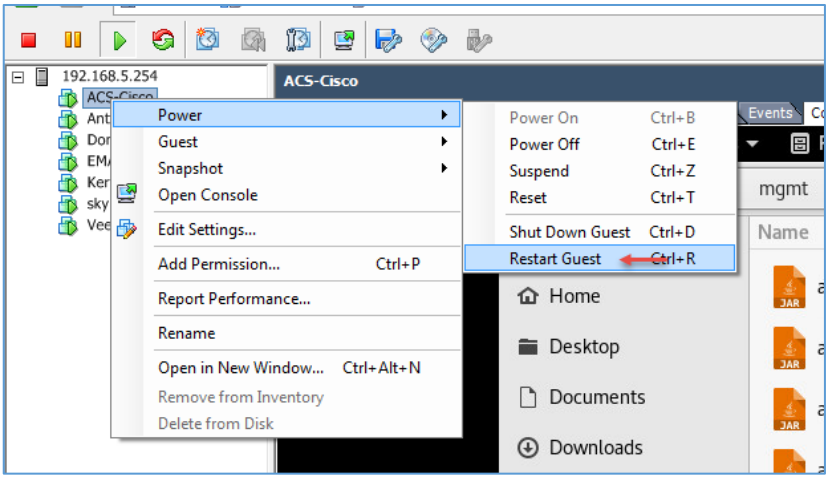
وارد پوشه lib شوید.



در پوشه lib با کلید ترکیبی CTRL + V فایل مورد نظر را Past کنید که بعد از این کار شکل روبرو ظاهر خواهد شد و از شما سوال می‌کند که آیا مایلید فایل جدید را با فایل قبلی جایگزین کنم که با کلیک بر روی دکمه Replace این کار انجام خواهد شد.

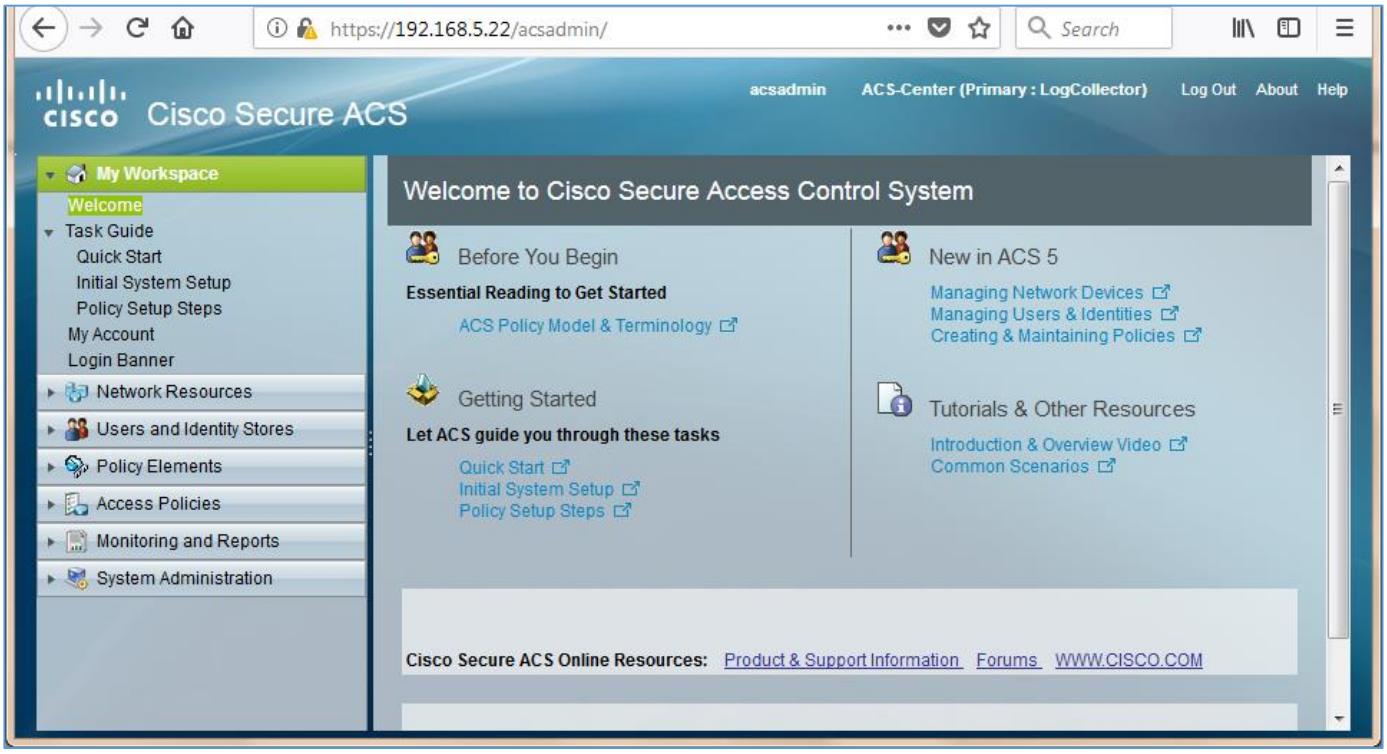


بعد از انجام مراحل بالا بر روی سرور ACS کلیک راست و از قسمت Power گزینه‌ی Restart Guest را انتخاب کنید، با این کار کرک نرم‌افزار انجام می‌شود و شما باید وارد صفحه وب نرم‌افزار ACS شوید و دوباره لایسنس را اضافه کنید.



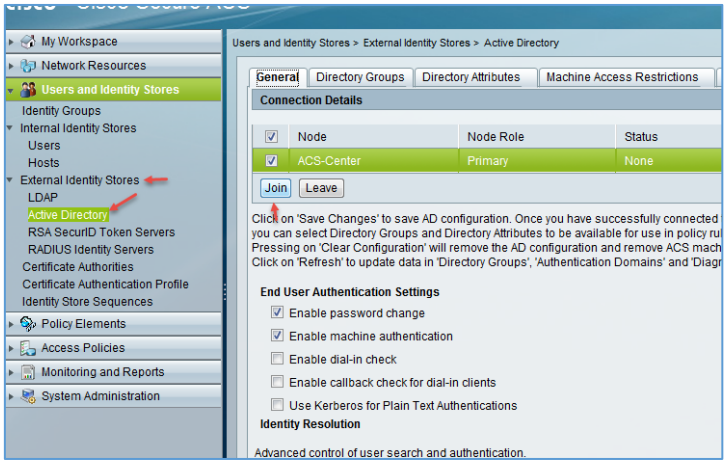
دوباره لایسنس نرم‌افزار را Add کنید و بر روی Install کلیک کنید با این کار به درستی لایسنس مورد نظر به نرم‌افزار اضافه خواهد شد.

همان‌طور که در تصویر زیر مشاهده می‌کنید نرم‌افزار به درستی اجرا شده است و باید ادامه کار را با این نرم‌افزار انجام دهیم.

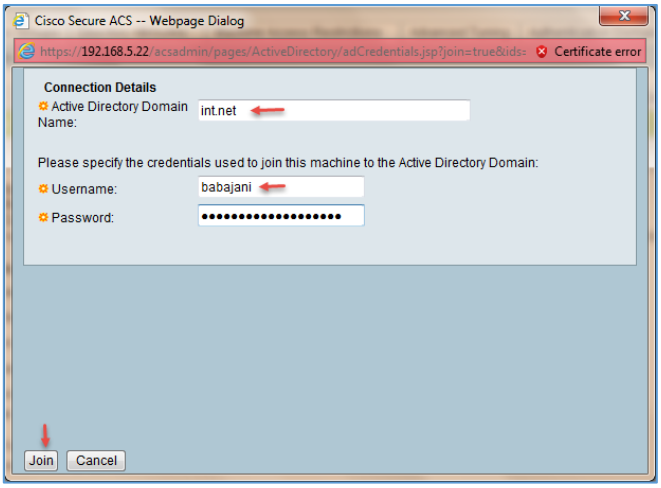


متصل کردن ACS به Active Directory

یکی از ویژگی‌های مهم نرم‌افزار ACS متصل شدن به سرویس Active Directory است که می‌توانید با این کار دستگاه‌های شبکه خود را از طریق کاربر موجود در Active Directory مدیریت کنید، در این قسمت می‌خواهیم از طریق نرم‌افزار ACS به سرویس Active Directory در شبکه متصل شویم.

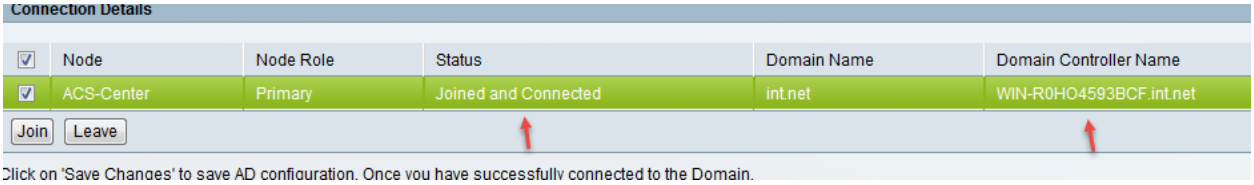


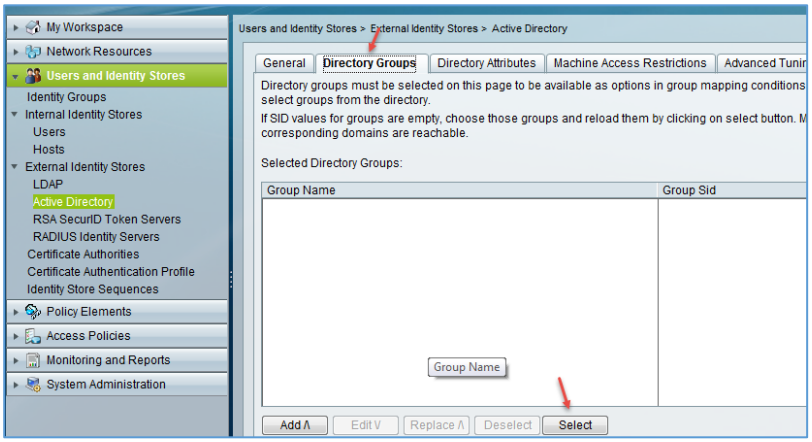
در این صفحه از سمت چپ بر روی External identity Stores کلیک کنید و گزینه‌ی Active Directory را انتخاب و در صفحه باز شده بر روی Join کلیک کنید.



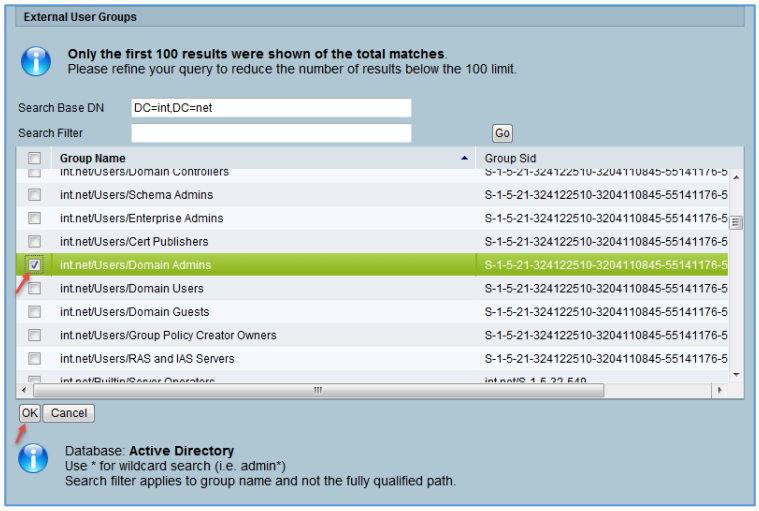
در این قسمت نام دومین خود را وارد کنید و در قسمت Username باید نام کاربری مربوط به دومین خود را که دسترسی‌های لازم را دارا است را وارد کنید و بر روی Join کلیک کنید، با این کار سرور ACS عضو دومین int.net خواهد شد.

همانطور که در شکل زیر مشاهده می‌کنید، سرور ACS که با نام ACS-Center است عضو دومین int.net شده است و نام دومین کنترلر در شکل مشخص شده است.





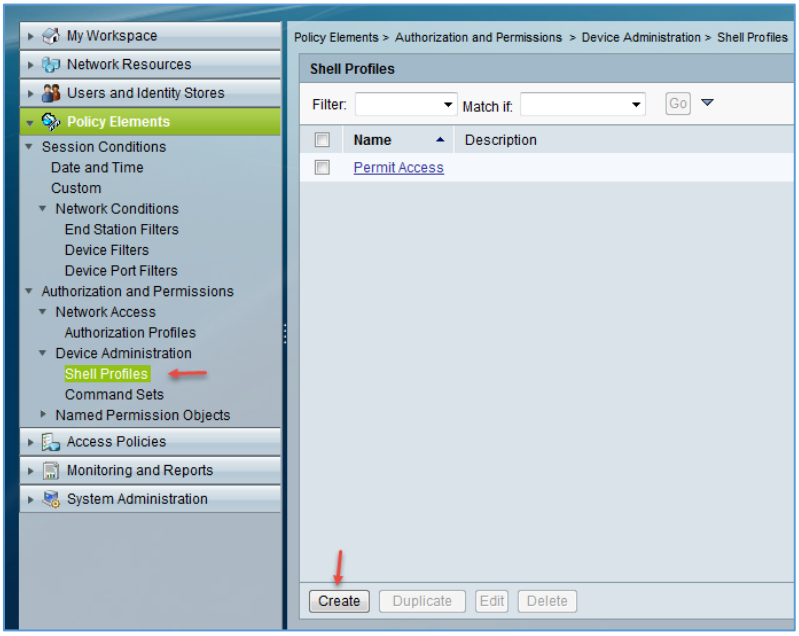
در مرحله بعد باید گروهی که کاربران در آن قرار دارند را به نرم‌افزار اضافه کنید که برای این کار وارد تب Directory Groups شوید و بر روی Select کلیک کنید.



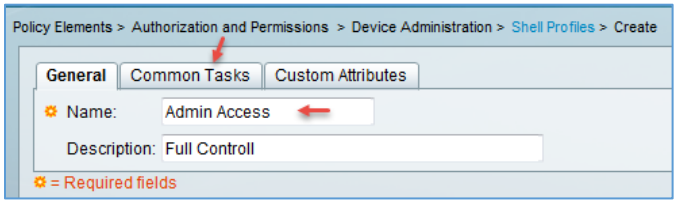
در این قسمت گروه Domain Admins را انتخاب می‌کنیم، که در این گروه کاربران مورد نظر ما قرار دارند.

بر روی ok کلیک کنید.

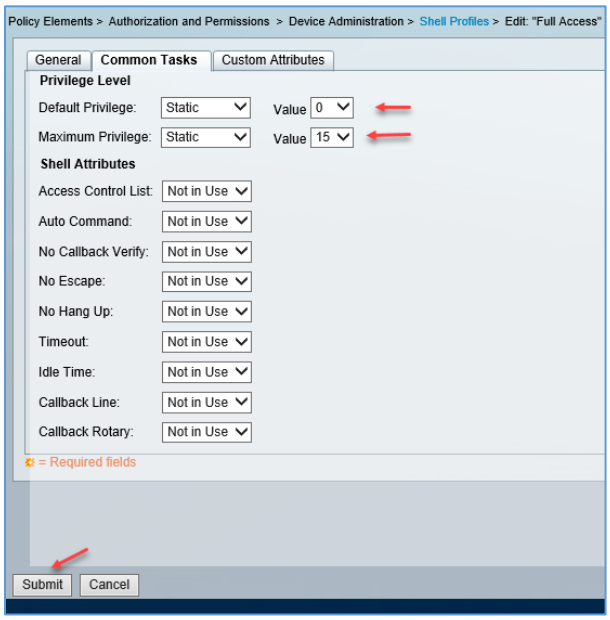
بعد از اینکه نرم‌افزار را به Active Directory متصل کردید و گروه مورد نظر را به لیست اضافه کردید باید یک پروفایل برای دسترسی افراد به دستگاه‌ها ایجاد کنیم، منظور از پروفایل یعنی اینکه هر کسی که عضو آن شود دارای توانایی‌هایی است که برای آن مشخص می‌کنیم.



به مانند شکل روبرو وارد Policy Elements شوید و گزینه‌ی Shell Profiles را انتخاب کنید و در صفحه باز شده بر روی Create کلیک کنید.

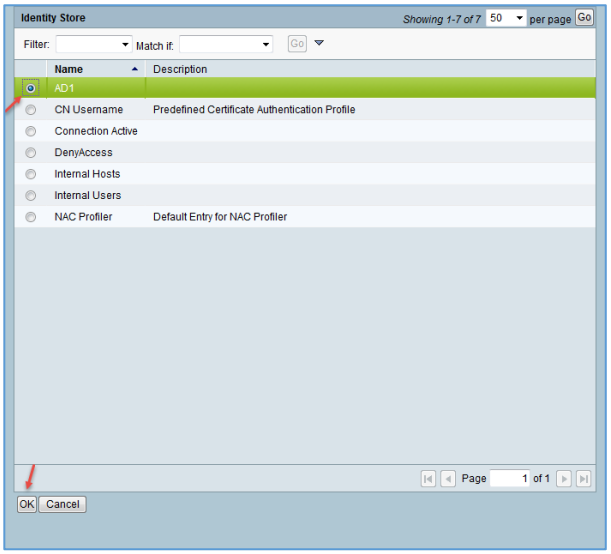


در این صفحه نام و توضیحات مورد نظر خود را وارد کنید و وارد تب Common Task شوید.



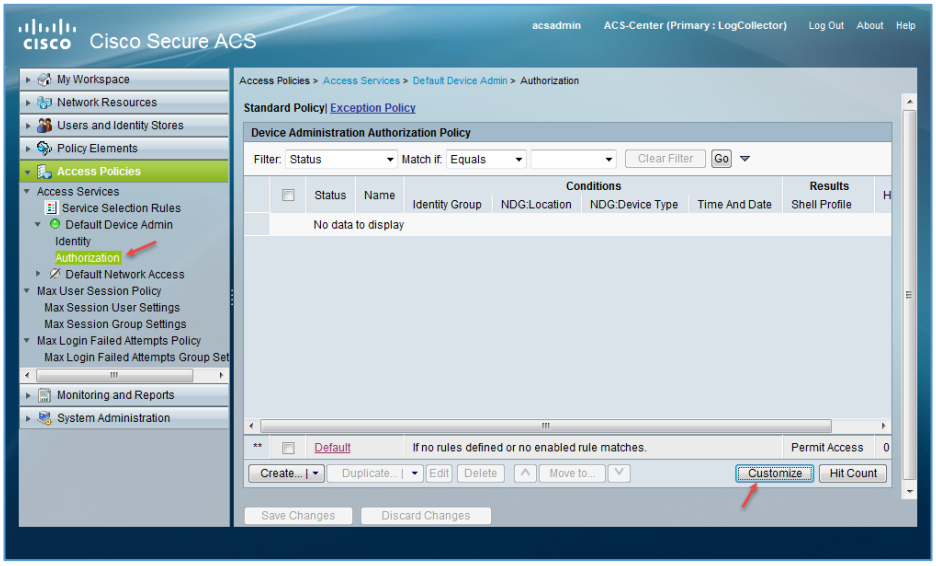
در این قسمت باید به Profile مورد نظر دسترسی لازم به منابع را بدهیم، برای این کار گزینه‌ی Static را انتخاب کنید و در قسمت Value باید عدد صفر و پانزده را انتخاب کنید و بر روی Submit کلیک کنید تا Profile مورد نظر ایجاد شود، به این نکته توجه کنید که سطح صفر کمترین دسترسی را دارد و سطح پانزده بیشترین، که بسته به نیاز خود باید دسترسی لازم را انتخاب کنید.

بعد از انجام کار صفحه قبل، باید ACS را طوری تنظیم کنیم که از این به بعد از کاربران Active Directory برای بحث احراز هویت استفاده کند، برای همین از سمت چپ از قسمت Access Policies گزینه‌ی Identity را انتخاب کنید و در صفحه باز شده بر روی Select کلیک کنید.

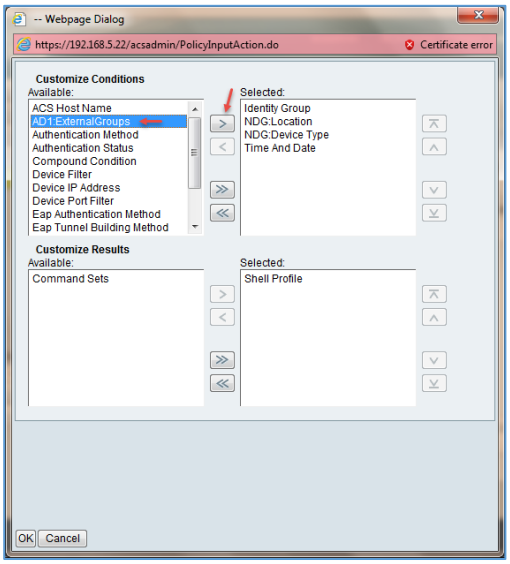


در این صفحه باید گزینه‌ی AD1 را انتخاب و بر روی OK کلیک کنید.

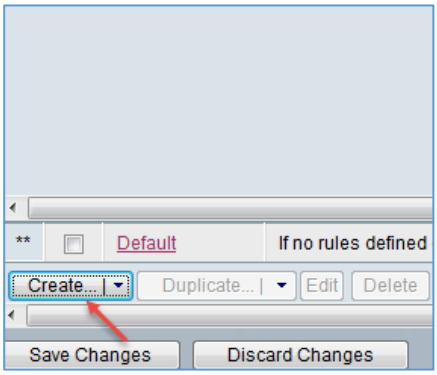
با این کار ACS از Active Directory اطلاعات را دریافت می‌کند.



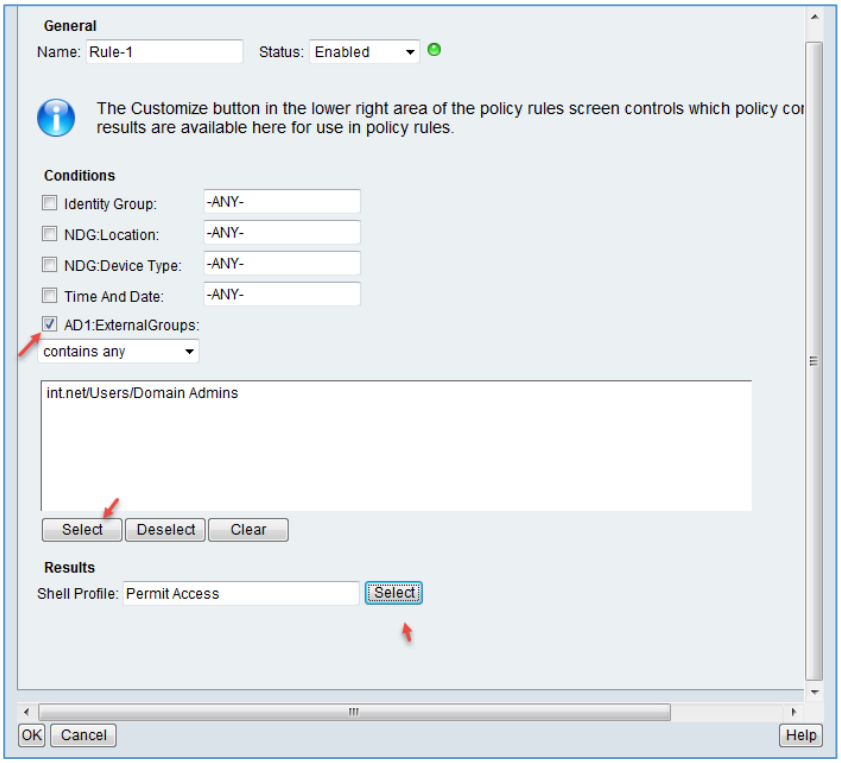
بعد از اینکه تنظیمات Active را انجام دادید وارد قسمت Authorization شوید و در صفحه باز شده بر روی Customize کلیک کنید.



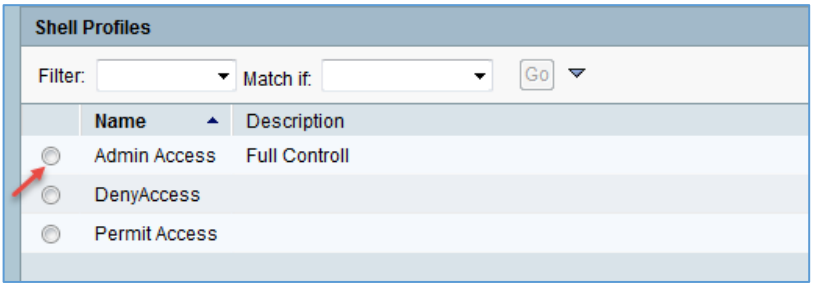
در این صفحه AD1 مربط به Active Directory را به لیست اضافه و بر روی OK کلیک کنید.



بر روی Create کلیک کنید تا یک کانکشن جدید برای Authorization ایجاد کنیم.



در این صفحه گزینه‌ی AD1:ExternalGroups را انتخاب کنید و بعد بر روی Select کلیک کنید و گروه مورد نظر را که از قبل اضافه کردیم، انتخاب کنید، بعد از این کار باید در قسمت Shell Profile پروفایلی را که ایجاد کردیم را انتخاب کنید.



در این صفحه باید پروفایل مورد نظر خود را که ایجاد کردید را انتخاب و بر روی Create کلیک کنید تا تنظیمات اعمال شود.

ارتباط سوئیچ و روتر با نرم‌افزار ACS

در این بخش می‌خواهیم از نرم‌افزار ACS به صورت عملی استفاده کنیم، برای این کار اگر دستگاه فیزیکی ندارید می‌توانید از نرم‌افزارهای مجازی مانند GNS3 برای ارتباط با سرور استفاده کنید که آموزش این نرم‌افزار و نحوه ارتباط روتر با بیرون از نرم‌افزار در کتاب CCNA آموزش داده شده است ولی برای درک بیشتر و ارائه روش‌های جدیدتر دوباره این نرم‌افزار را به همراه IOU راه‌اندازی می‌کنیم.

قبل از شروع کار باید با دو پروتکل TACACS + و RADIUS که در سرویس AAA از آنها برای ارتباط با دیگر نرم‌افزارها استفاده می‌شود، بیشتر آشنا شویم.

پروتکل TACACS+

TACACS+ یا Terminal Access Controller Access-Control System پروتکلی از شرکت سیسکو می‌باشد که از سال ۱۹۹۳ به عنوان یک استاندارد برای احراز هویت به کار گرفته شده است. این پروتکل از به صورت پیش فرض از پورت ٤٩ (TCP,UDP) برای تبادل ارتباط خود استفاده می‌کند.

پروتکل Radius

Radius یا Remote Authentication Dial-In User Service یک پروتکل شبکه است که در ورژن جدید آن بر روی پورت ۱۸۱۲ عمل می‌کند و مدیریت تایید هویت، مجوز و دسترسی را به کاربرانی که می‌خواهند از یک سرویس در شبکه استفاده کنند می‌دهد، این پروتکل مختص شرکت خاصی نیست و به صورت عمومی ارائه شده است و اکثر سیستم‌ها از این پروتکل پشتیبانی می‌کنند.

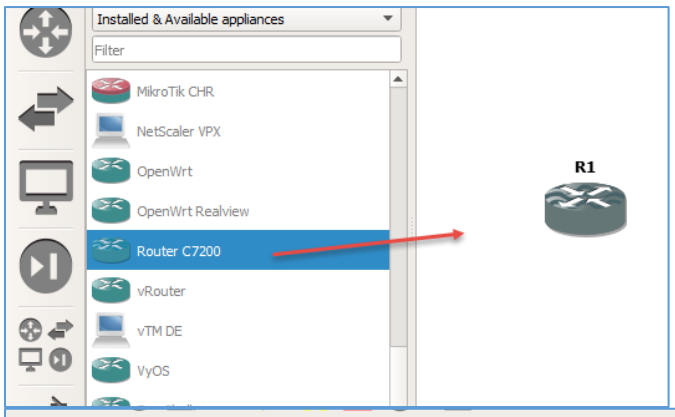
Radius یک پروتکل سرویس دهنده و گیرنده (Server/Client) است در لایه Application مدل OSI کار می‌کند و برای تبادل اطلاعات از دو پروتکل TCP و UDP استفاده می‌کند، این پروتکل بیشتر بر روی سیستم‌عامل‌های لینوکس و ویندوز پیاده‌سازی می‌شود.

تفاوت بین پروتکل Radius و TACACS+

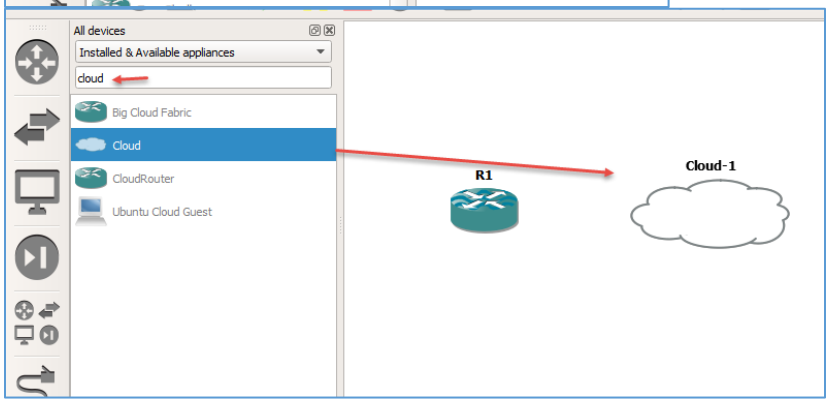
	+TACACS	Radius
عملکرد	این پروتکل سه فرآیند Authentication، Authorization و Accounting را به صورت جداگانه انجام می‌دهد و عملکرد جداگانه‌ای بر روی آنها دارد	این پروتکل دو گزینه‌ی Authentication و Authorization را با هم انجام می‌دهد.
استاندارد	مختص شرکت سیسکو است و بسیار خوب عمل می‌کند.	به صورت عمومی در دسترس است و می‌توان روی هر دستگاه پیاده‌سازی شود
لایه انتقال	بر روی پورت TCP عمل می‌کند	بر روی پورت UDP عمل می‌کند
محرمانگی	کل بسته‌های عبوری را رمزنگاری می‌کند و یکی از مهمترین ویژگی‌های آن می‌باشد.	فقط بسته‌هایی که دارای رمز عبور باشند را رمزنگاری می‌کند.
دسترسی	میزان دسترسی کاربران را می‌تواند مشخص کند.	نمی‌تواند
پشتیبانی	از پروتکل‌های NetBIOS Frame Control Protocols، X.25، AppleTalk، NOVEL NASI پشتیبانی می‌کند.	نمی‌کند

ارتباط سوئیچ یا روتر با نرم‌افزار ACS

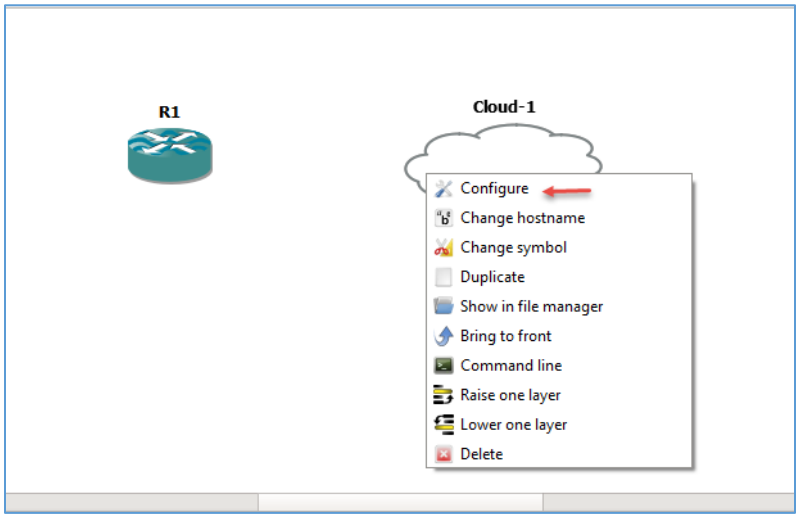
در این قسمت می‌خواهیم از طریق سوئیچ یا روتر به نرم‌افزار ACS متصل شویم و کار احراز هویت را برای آن دستگاه مورد نظر از طریق ACS انجام دهیم.



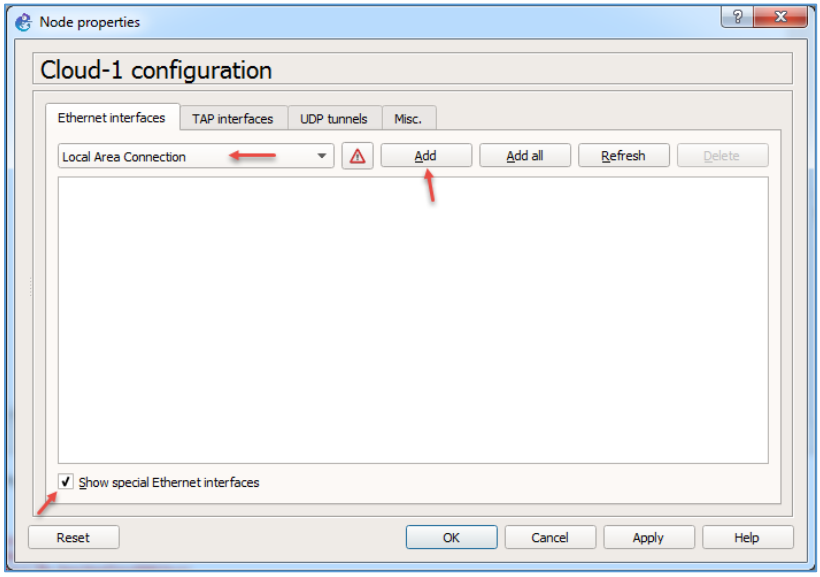
نرم‌افزار GNS3 را اجرا کرده و روتر C7200 که با هم ایجاد کردیم را به نرم‌افزار اضافه کنید.



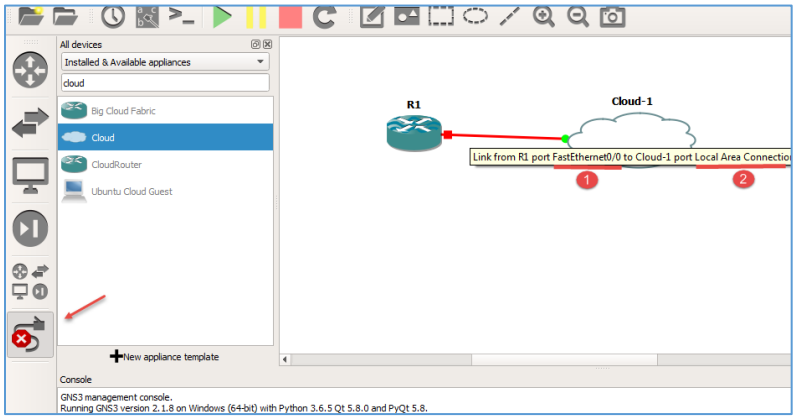
در ادامه یک Cloud به صفحه اضافه کنید تا بتوانید به سرور ACS از طریق آن متصل شویم.



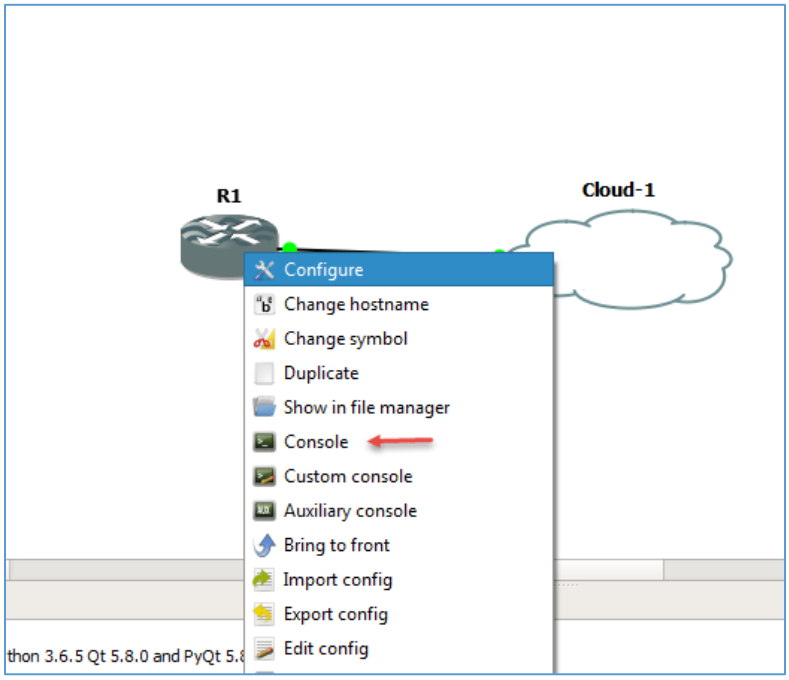
برا اینکه Cloud را به کارت شبکه اصلی شبکه متصل کنید بر روی آن کلیک راست و گزینه‌ی Configure را انتخاب کنید.



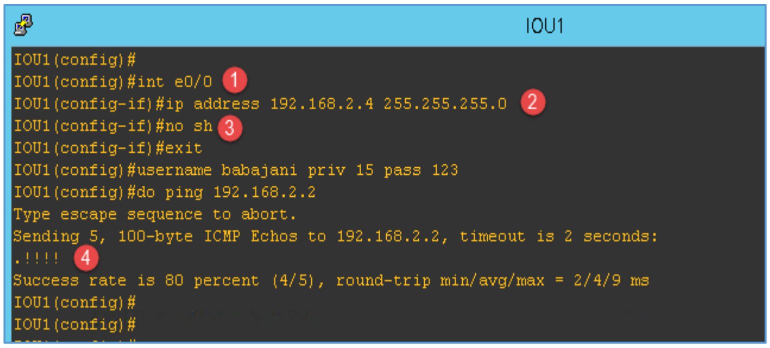
در تب Ethernet interfaces باید کارت شبکه اصلی سیستم را انتخاب کنید، برای این کار تیک گزینه‌ی Show special Ethernet interfaces را انتخاب کنید و از منوی کشویی، کارت شبکه اصلی را انتخاب و بر روی Add کلیک و در آخر بر روی OK کلیک کنید.



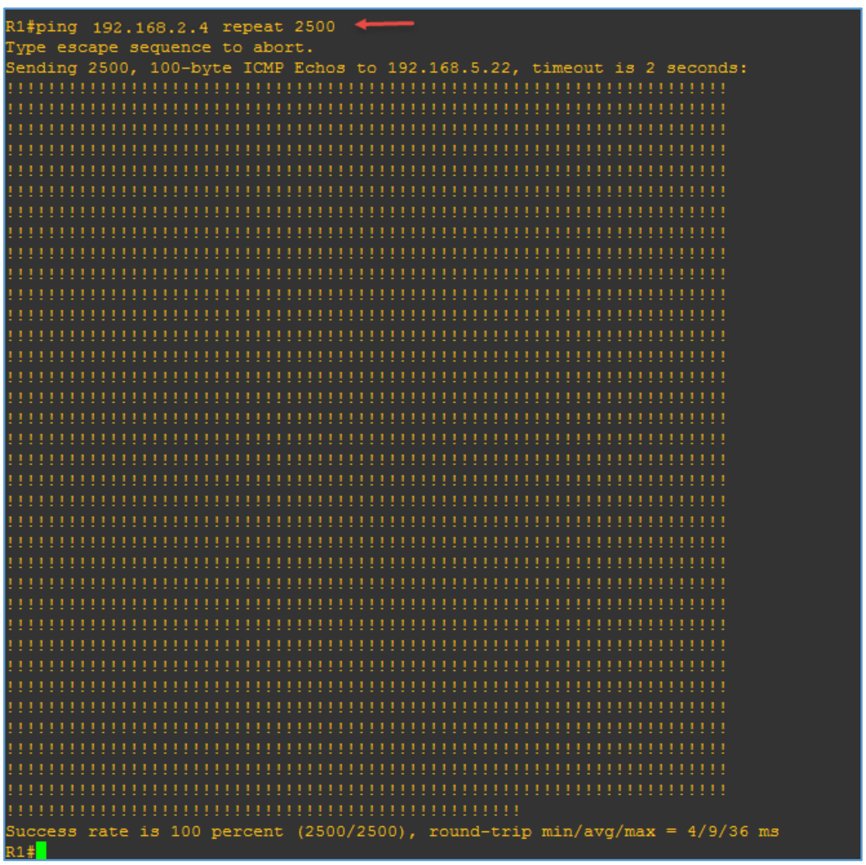
در ادامه کابل را انتخاب و از پورت FastEtherneet0/0 یک کابل به کارت شبکه اصلی که در اینجا Local Area Connection است بکشید.



بعد از انجام مراحل بالا، روتر R1 را روشن کنید و بعد بر روی آن کلیک راست کنید و گزینه‌ی Console را انتخاب کنید تا بتوانیم تنظیمات مربوط به شبکه را انجام دهیم.



همانطور که مشاهده می‌کنید، کنسول مربوط به R1 اجرا شده است، برای اینکه تست کنیم که روتر R1 سرور ACS را می‌بینند، باید در قسمت شماره‌ی یک وارد interface 0/0 که به Cloud متصل است شویم و آدرس مورد نظر به صورتی که در قسمت شماره‌ی دو مشخص شده وارد کنیم و در قسمت شماره‌ی سه با دستور No Sh پورت مورد نظر را روشن کنیم، توجه داشته باشید برای متصل شدن به روتر از طریق Telnet باید یک UserName و Password هم تعریف کنیم و بعد برای تست نهایی آدرس IP سرور ACS را Ping می‌گیریم، در قسمت شماره‌ی چهار مشخص شده است که با موفقیّت توانستید به سرور ACS از طریق R1 متصل شوید.

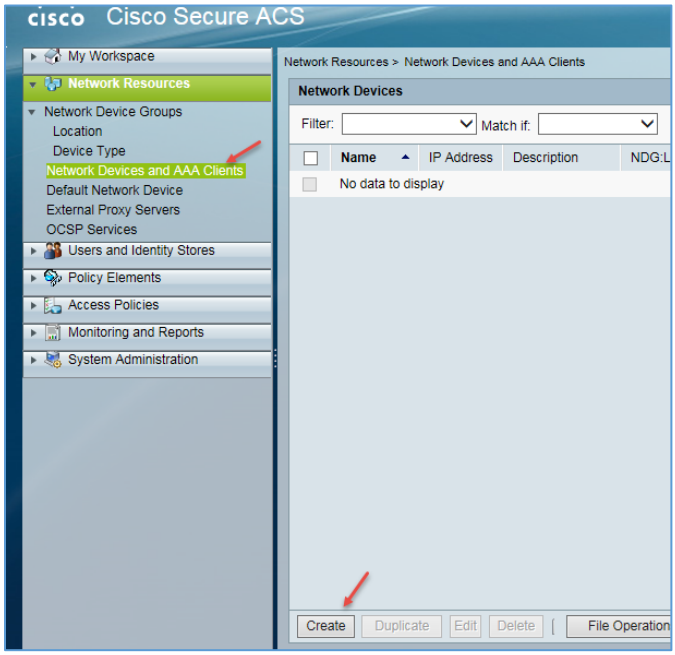


یک نکته ساده، برای اینکه زمانی که از Ping استفاده می‌کنید بخواهید این دستور مدام تکرار شود به مانند شکل روبرو در آخر دستور ping دستور repeat را وارد و بعد از آن از عددی بین ۱ تا ۲۱٤۷٤۸۳٦٤۷ استفاده کنید، هر چقدر عدد بیشتر زمان Ping هم طولانی تر خواهد بود.

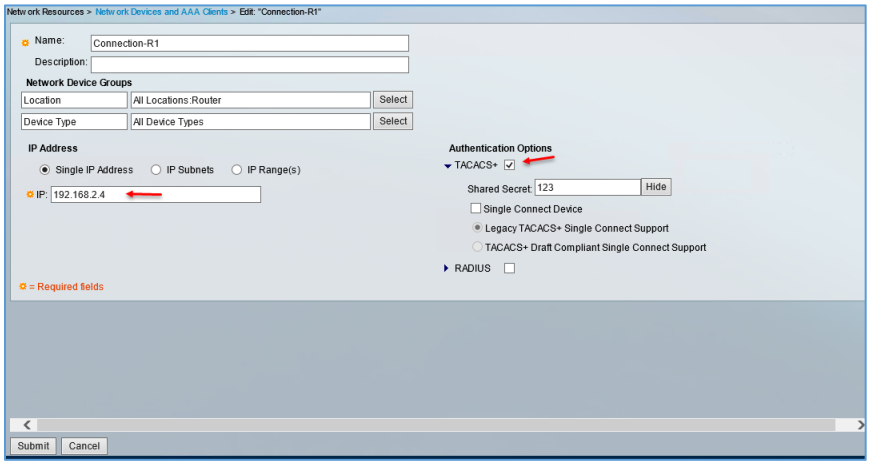
تذکر: برای ذخیره کردن تنظیمات در روتر از دستور running-config startup-config استفاده کنید، دستورات اولیه روترها و سوئیچ‌ها در کتاب CCNA بررسی شده و می‌توانید از سایت این کتاب را دانلود کنید.

راه اندازی AAA Server

در این بخش می‌خواهیم به سرویس AAA که در قسمت‌های قبلی در مورد آن صحبت کردیم بپردازیم، این سرویس سه کار احراز هویت (Authentication)، مجوز دسترسی (Authorization) و بررسی رویدادها (Accounting) انجام خواهد داد، اگر توجه کرده باشید در قسمت‌های قبلی نرم‌افزار ACS را راه اندازی کردیم و آن را به سرویس Active Directory ویندوز متصل کردیم، می‌خواهیم سرویس AAA اطلاعات کاربری خود را از طریق Active Directory دریافت کند.



برای شروع کار، باید یک کانکشن بین دستگاه‌هایی که قرار است از سرویس ACS استفاده کنند بزنیم، مثلاً در قسمت قبل یک روتر در GNS3 ایجاد کردیم و IP آن را ۱۹۲.۱۶۸.۵.۱۹ در نظر گرفتیم، در این قسمت گزینه‌ی Network Devices and AAA Clients را انتخاب کنید و در صفحه باز شده بر روی گزینه‌ی Create کلیک کنید.



در قسمت Name یک نام به دلخواه خود وارد کنید، در قسمت IP Address باید آدرس روتر یا دستگاه مورد نظر که قرار است بر روی آن سرویس AAA فعال شود را وارد کنید که البته می‌توانید یک Subnet یا رنج آدرس برای آن مشخص کنید در قسمت Authentication options تیک گزینه‌ی TACACS+ را انتخاب کنید و یک رمز عبور برای آن قرار دهید که در اینجا 123 در نظر گرفته شده است و در آخر بر روی Submit کلیک کنید تا Connection مورد نظر ایجاد شود.

بعد از ایجاد رمز عبور وارد روتر R1 که در نرم‌افزار GNS3 ایجاد کردیم می‌شویم و تنظیمات زیر را انجام می‌دهیم.

IOU1

```
IOU1(config-if)#
IOU1(config-if)#
IOU1(config-if)#aaa new-model
IOU1(config)#tacacs-server host 192.168.2.2 key 123
 Warning: The cli will be deprecated soon
 'tacacs-server host 192.168.2.2 key 123'
 Please move to 'tacacs server <name>' CLI
IOU1(config)#aaa authentication login default group tacacs+
IOU1(config)#line vty 0 4
IOU1(config-line)#login authentication default
```

با دستور زیر سرور AAA بر روی روتر فعال خواهد شد:

aaa new-model

tacacs-server host 192.168.5.36 key 123

توجه داشته باشید برای اینکه ارتباط بین سرور ACS و روتر را چک کنیم می‌توانیم از دستور زیر استفاده کنیم:

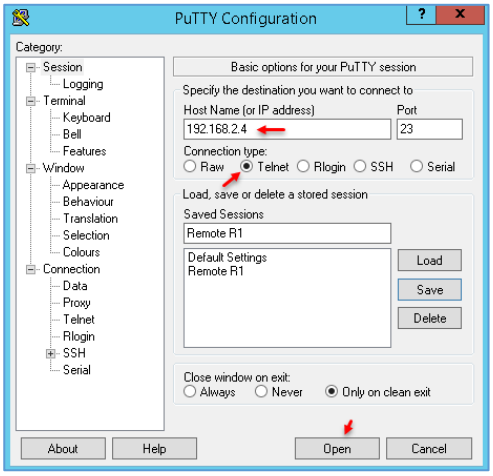
R1#test aaa group tacacs+ babajani Password legacy

Attempting authentication test to server-group tacacs+ using tacacs+

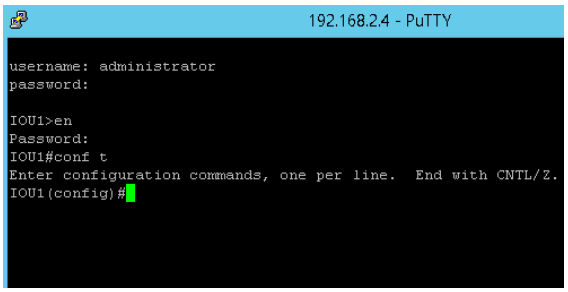
User was successfully authenticated.

در دستور بالا به جای نام کاربری و رمز عبور مشخص شده با رنگ قرمز باید نام کاربری که در اکتیو دایرکتوری وجود دارد و عضو گروه Domain Admin است را وارد کنید که بعد از اجرا، پیغام successfully authenticated مشخص کننده ارتباط درست بین Router و ACS است.

aaa authentication login default group tacacs+



با اجرای دستور بالا، احراز هویت روتر از طریق نرم‌افزار ACS انجام خواهد شد، برای تست این موضوع، ارتباط Telnet با روتر R1 برقرار می‌کنیم که برای انجام آن می‌توانید از نرم‌افزار Putty استفاده کنید در این نرم‌افزار گزینه‌ی Telnet را انتخاب کنید و آدرس روتر مورد نظر که بر روی آن با دستور (Line vty 0 4) سرویس Telnet را فعال کردید را وارد و بر روی Open کلیک کنید.



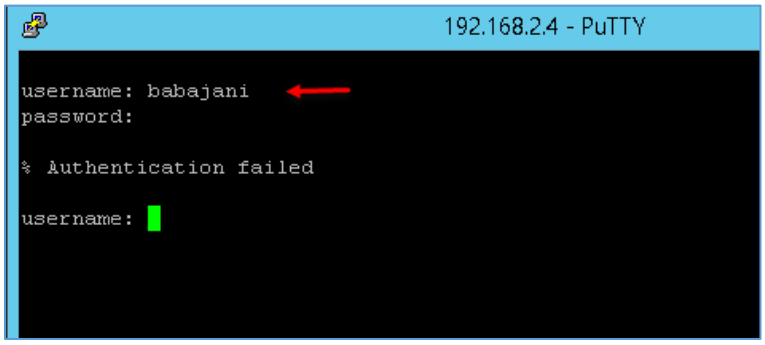
در شکل روبرو با استفاده از کاربر Administrator که در Active قرار دارد توانستیم به روتر متصل شویم.

نکته: زمانی‌که از دستور Enable در این قسمت استفاده می‌کنید اگر چنانچه Enable Password در روتر تعریف نشده باشد، اجازه ورود به روتر را پیدا نخواهید کرد، پس باید این دستور در روتر اجرا شود.

تذکر: وقتی در روتر از دستور زیر برای فعال سازی سرویس AAA استفاده می‌کنید:

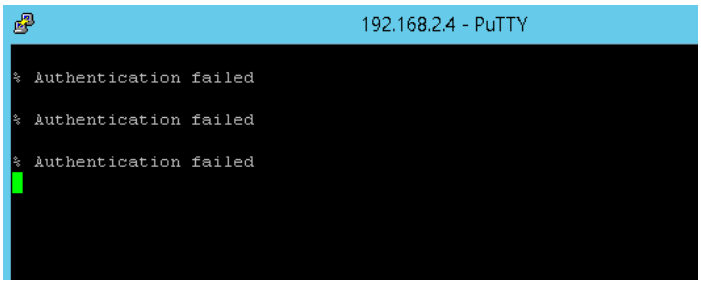
aaa authentication login default group tacacs+

به یاد داشته باشید که استفاده از کلمه +tacacs در آخر این دستور باعث می‌شود که رمز عبور، فقط و فقط از طریق نرم‌افزار ACS خوانده شود و دیگر نمی‌توانید از Username و Password که در روتر تعریف کردید استفاده کنید.



همانطور که در شکل روبرو مشاهده می‌کنید، به روتر از طریق Telnet متصل شدیم، اگر با نام کاربری که در قسمت قبل بر روی روتر تعریف کردیم وارد آن شویم با خطا روبرو مواجه خواهیم شد.

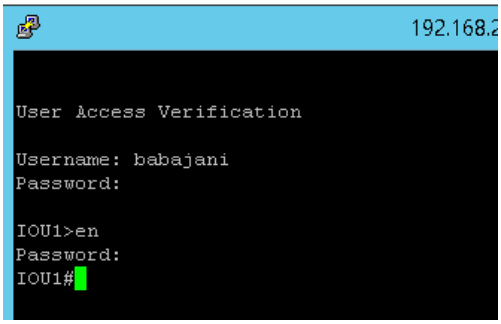
این موضوع یک مشکل اساسی ایجاد خواهد کرد، اگر چنانچه سرور ACS از کار بیفتد و از مسیر خارج شود دیگر به هیچ عنوان نمی‌توانید وارد تنظیمات روتر شوید، برای تست این موضوع سرور ACS را خاموش می‌کنیم و همانطور که در شکل روبرو مشاهده می‌کنید، برای ارتباط با روتر با سه خطای پشت هم مواجه می‌شوید.



برای حل این مشکل باید کاری کنید که همزمان از ACS و هم از دیتابیس خود روتر استفاده شود، برای این کار باید در روتر دستور زیر را وارد کنید:

aaa authentication login default group tacacs+ local

در دستور بالا کلمه local اضافه شده است، پس روتر طبق اولویتی که تعریف کردید اگر سرور ACS در دسترس بود از اطلاعات خود سرور ACS استفاده خواهد کرد و هر چقدر هم تلاش کنید تا از نام کاربری روتر استفاده کنید موفّق نخواهید بود، ولی اگرACS از مسیر خارج شود و در دسترس نباشد، نام کاربری به صورت محلی و از داخل خود روتر صدا زده خواهد شد.



همانطور که در شکل روبرو مشاهده می‌کنید توانستیم با کاربر babajani وارد روتر شویم.

در ادامه می‌خواهیم سرویس Authorization و Accounting را روی روتر فعال کنیم و با این سرویس‌ها می‌توانیم برای کاربران، سطح دسترسی و نوع دستورات را برای آنها مشخص کنیم.

در ادامه می‌خواهیم مشخص کنیم که هر کاربر، چه دستوراتی را بتواند در روتر یا سوئیچ و دیگر دستگاه‌ها اجرا کند که به این مرحله Authorization گفته می‌شود.

aaa authorization exec default group tacacs+ local

با دستور بالا سرویس Authorization فعال خواهد شد که سطح دسترسی کاربر را بررسی خواهد کرد، همانطور که گفتیم هم از tacacs+ استفاده می‌کنیم و هم از دیتابیس Local تا همدیگر را پوشش دهند.

نکته: اگر این دستور را در روتر وارد کنید و تنظیمی روی روتر در ادامه برای آن انجام ندهید کاربر دیگر نمی‌تواند وارد روتر شود.

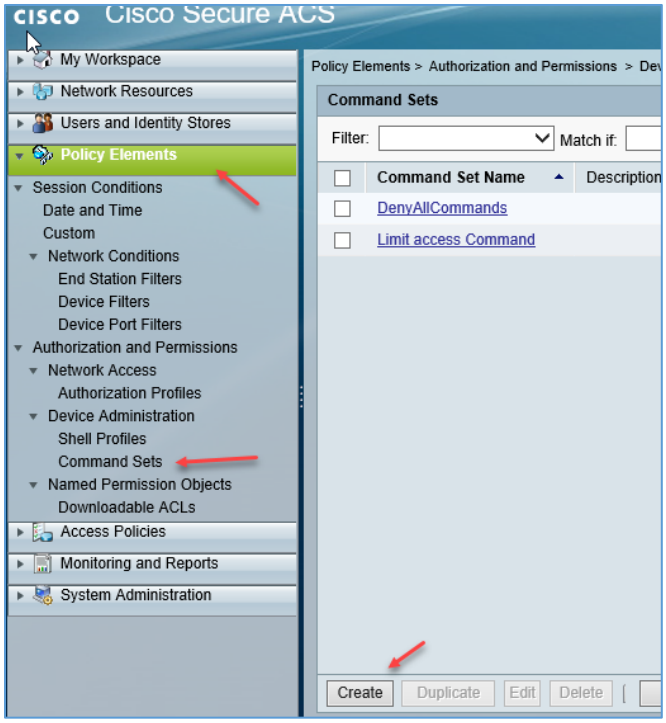
دستورات زیر را در روتر مورد نظر برای سطح‌ها مختلف دسترسی وارد کنید.

aaa authorization commands 0 default group tacacs+ local

aaa authorization commands 1 default group tacacs+ local

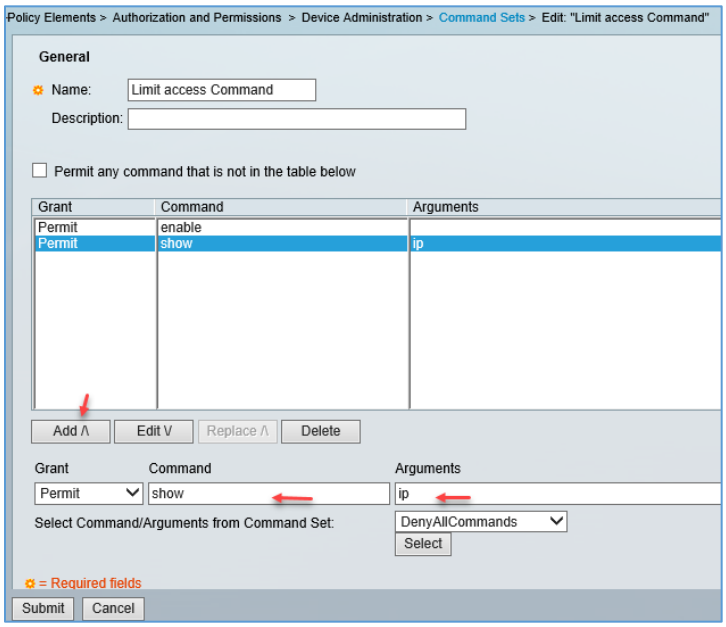
aaa authorization commands 15 default group tacacs+ local

بعد اجرا کردن دستورات بالا از طریق Telnet وارد روتر شوید و یک دستور را اجرا کنید، متوجه خواهید شد دستور مورد نظر اجرا نشده و با خطای روبرو مواجع می‌شوید، توجه داشته باشید اگر بعد از دستورات علامت سوال قرار دهید دستورات دیگر را نشان می‌دهد ولی اگر بخواهید آن را اجرا کنید با خطا روبرو می‌شوید.



برای تنظیم این دستور در ACS از قسمت Policy Elements وارد Shell Profiles شوید و بر روی Create کلیک کنید.

در این قسمت می‌توانید گروه‌های مختلفی ایجاد کنید که دارای دسترسی‌های مختلفی به دستورات اجرایی داشته باشند.

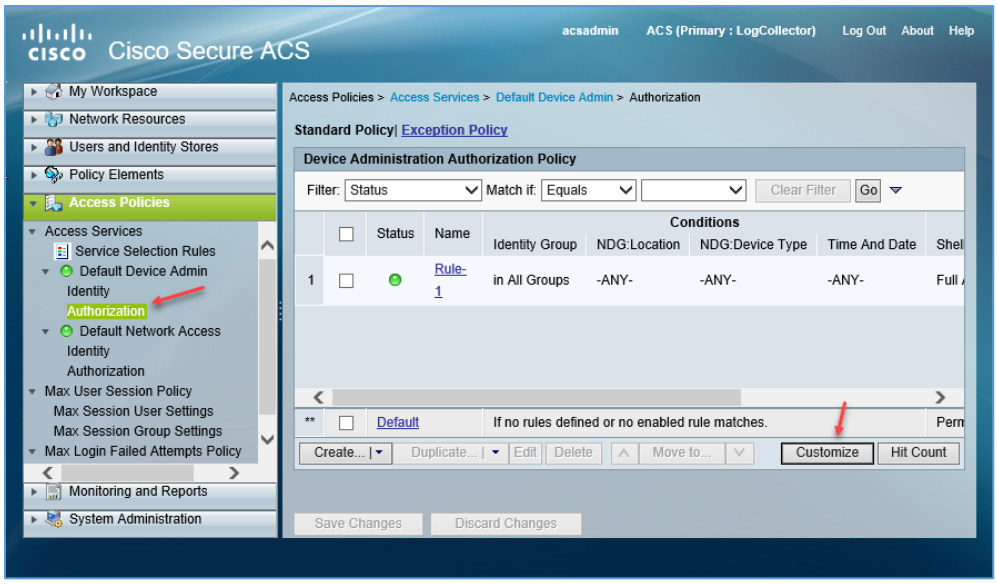


در این صفحه یک نام برای گروه خود در نظر بگیرید و برای اینکه دستورات مشخص شده‌ای را که کاربر بتواند با آنها کار کند را به لیست اضافه کنید باید در قسمت Grant گزینه‌ی Permit را انتخاب و دستور را در قسمت Command بنویسید، همانطور که مشاهده می‌کنید دستور show نوشته شده است و دستوری که در Arguments نوشته

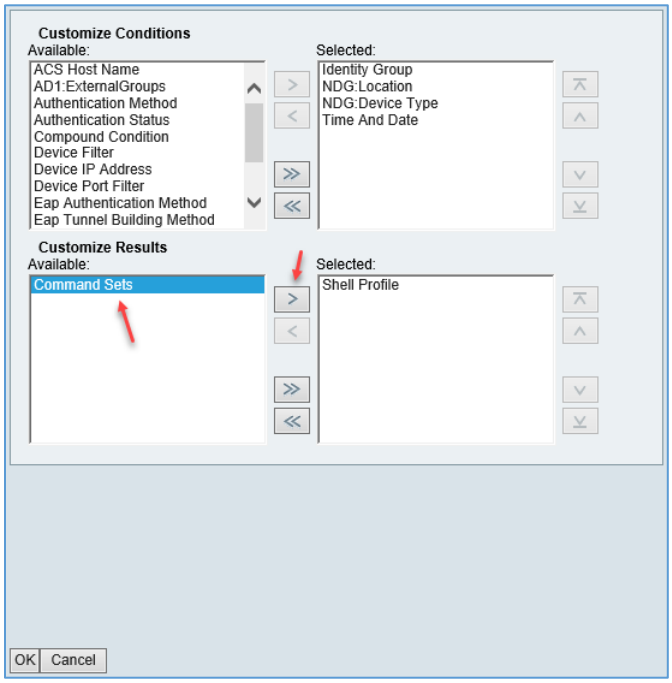
می‌شود ادامه دستور قبلی است یعنی در این دستور Show IP اجازه اجرا شدن دارد که با هم تست خواهیم کرد، بعد از وارد کردن دستور حتماً بر روی Add^ کلیک کنید تا به لیست اضافه شود، دستورات دیگری را هم می‌توانید به لیست اضافه کنید.

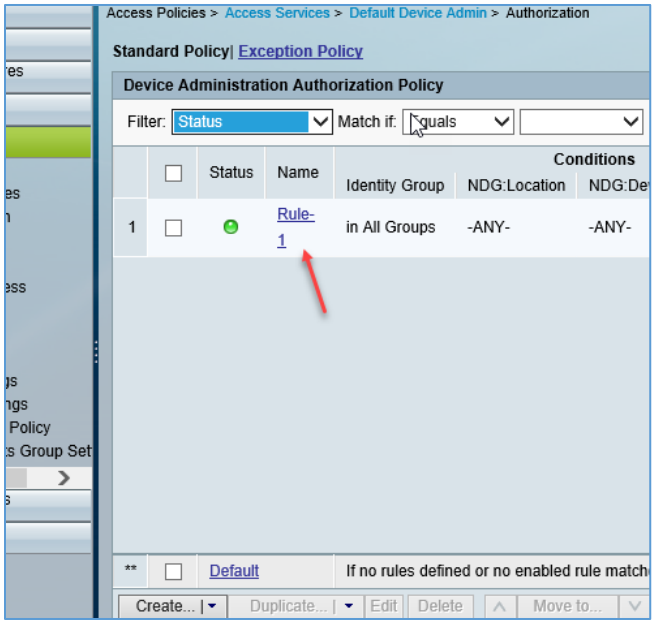
نکته: اگر در شکل قبل تیک گزینه‌ی Permit any command that is not in the table below را انتخاب کنید تمام دستورات برای کاربر مورد نظر اجرا خواهد شد و هر دستوری را که در لیست وارد کنید بی‌فایده است و دستورات به صورت کامل اجرا خواهند شد.

بعد از ایجاد گروه به مانند شکل از قسمت Authorization بر روی گزینه‌ی Customize کلیک کنید.

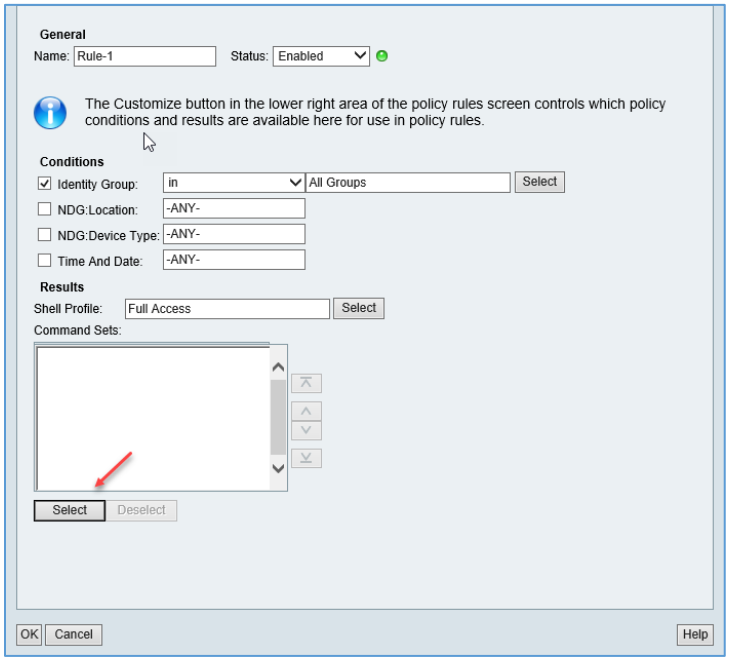


در این صفحه اگر به قسمت Coustomize Results توجه کنید گزینه‌ی Command Sets را مشاهده می‌کنید که باید آن را با کلید مشخص شده به لیست اصلی اضافه کنید.





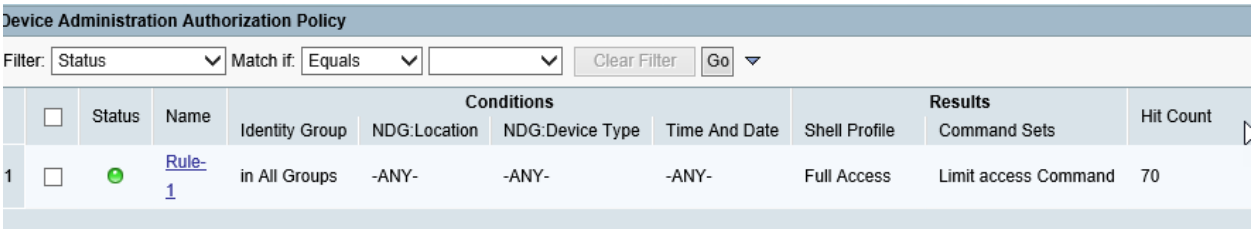
بعد ازانجام کار قبلی وارد Rule-1 که قبلاً ایجاد کردید شوید.



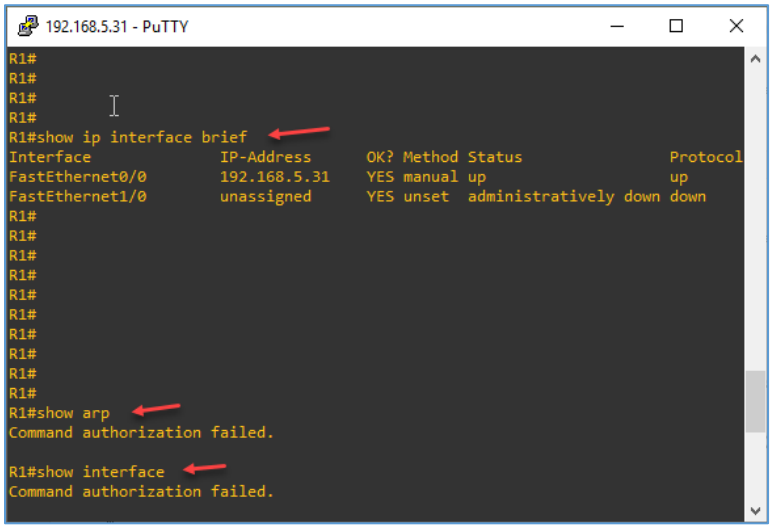
در این قسمت باید بر روی Select کلیک کنید و گروهی را که برای Command با نام Limit access command ایجاد کردید را انتخاب و بر روی OK کلیک کنید و در آخر بر روی Save Changes کلیک کنید تا تنظیمات ذخیره شود.

نکته: زمانی که ACS را به صورت مجازی اجرا می‌کنید سعی کنید در زمانبندی مشخص از ماشین آن SnapShot تهیه کنید تا به مشکلی بر نخورید.

همانطور که در شکل زیر مشاهده می‌کنید، ستون Command Sets اضافه شده است.



نکته: اگر در شکل یک به ستون Hit Count نگاه کنید یک عدد را مشاهده می‌کنید، این عدد یک شمارنده است و زمانی که کاربر از دستورات در خط فرمان استفاده کند این شماره تغییر خواهد کرد.



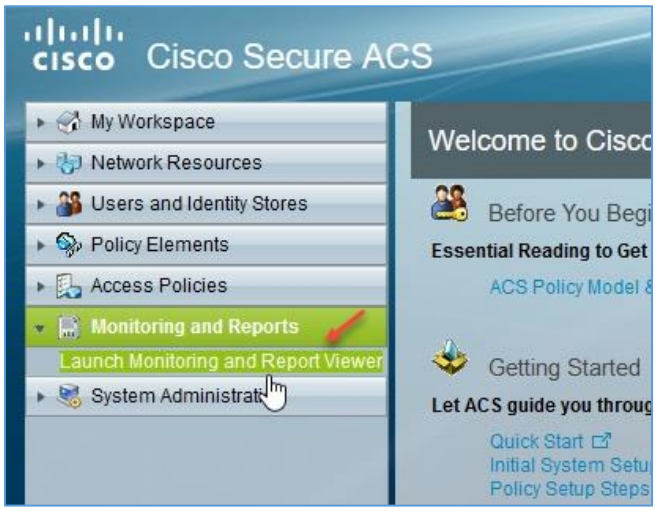
برای تست این موضوع اگر با Telnet به روتر مورد نظر متصل شوید و دستور Show Ip Interface Brief را اجرا کنید می‌بینید به خوبی این دستور اجرا می‌شود چون اجازه دسترسی را در گروه مورد نظر صادر کرده بودیم ولی اگر دستور Show arp را اجرا کنید چون در لیست نیست با خطای Command authorize failed مواجه خواهید شد که این کار می‌تواند در کنترل کاربران به شما بسیار کمک کند.

در ادامه دستور بعدی که باید فعال کنیم Accounting است، این دستور برای بررسی عملکرد کاربر ایجاد شده است، که باید بعد از Authentication و Authorization فعال شود.

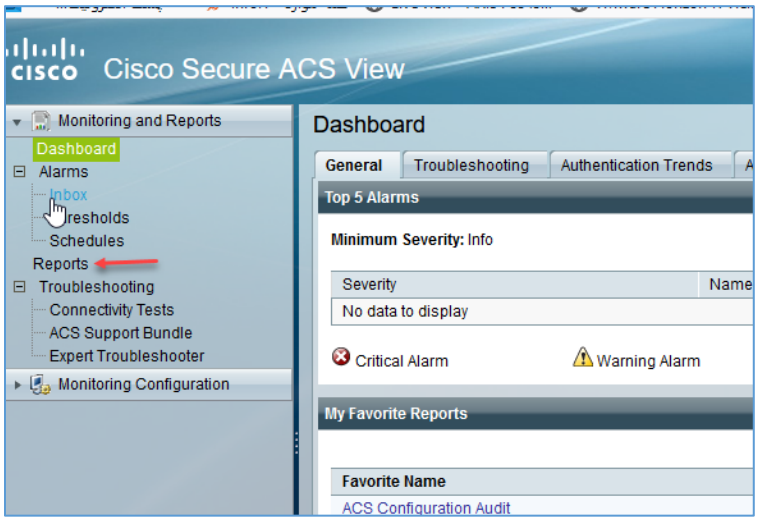
aaa accounting commands 0 default start-stop group tacacs+

aaa accounting commands ۱ default start-stop group tacacs+

aaa accounting commands ۱۵ default start-stop group tacacs+



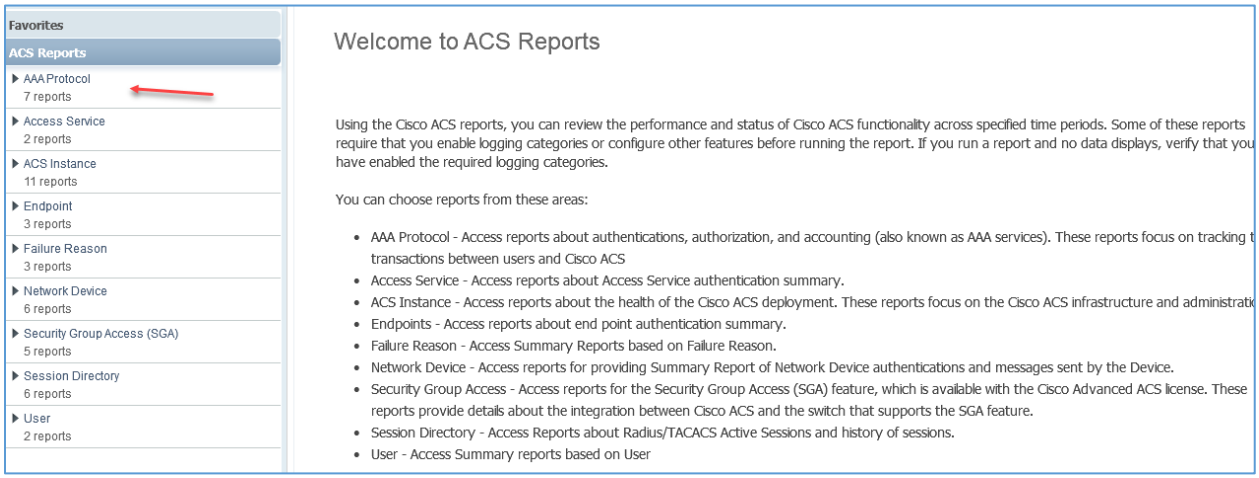
بعد از فعال کردن Accounting ، اگر کاربران هر دستوری را اجرا کنند در گزارش‌گیری ثبت خواهد شد، برای اینکه گزارشات کارکرد کاربران را در AAA مشاهده کنیم باید به مانند شکل روبرو بر روی Lunch Monitoring and Report Viewer کلیک کنید.

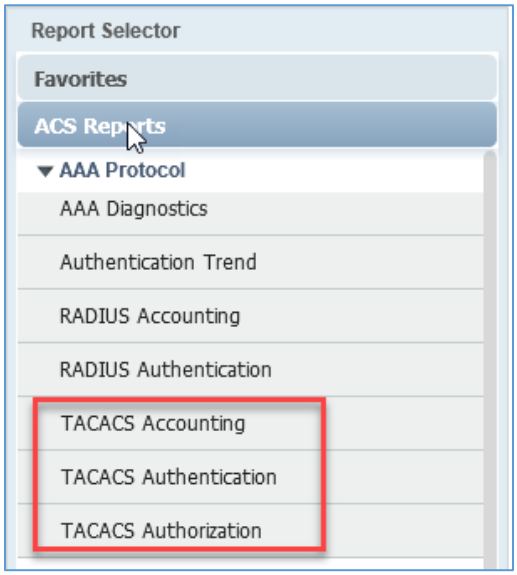


در این صفحه برای نمایش گزارشات نرم‌افزار ACS باید بر روی Reports کلیک کنید.

نکته: برا اینکه صفحه Reports برای شما به نمایش گذاشته شود نیاز به نرم‌افزار Flash Player دارید که باید از قبل بر روی سیستم نصب باشد.

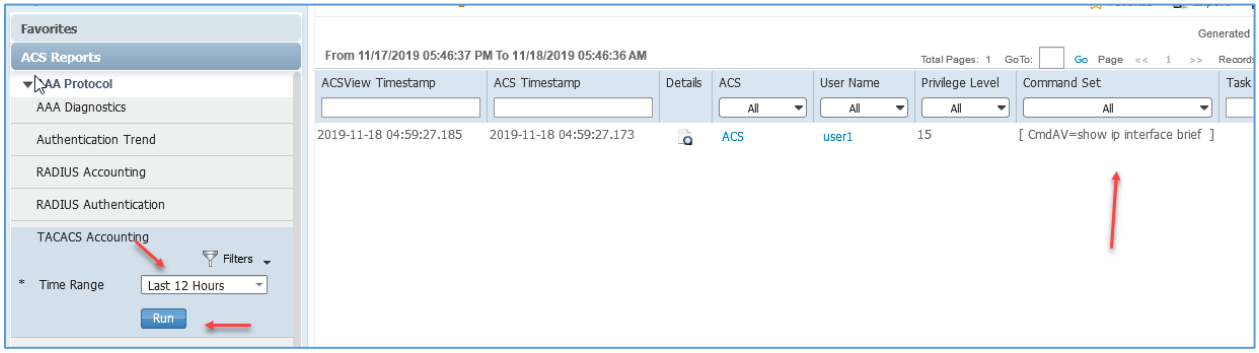
همانطور که در شکل زیر مشاهده می‌کنید صفحه گزارشات باز شده است و دارای گزینه‌های متعدد است، برای اینکه گزارشات مربوط به AAA را مشاهده کنیم بر روی AAA Protocol کلیک کنید.



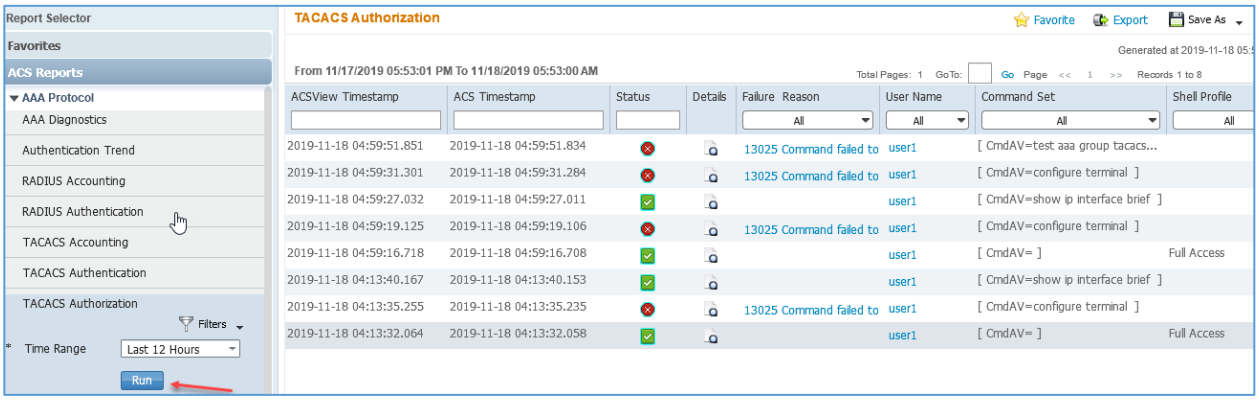


در قسمت AAA Protocol دو پروتکل TACACS+ و RADIUS را مشاهده می‌کنید، برای اینکه گزارشات مربوط به TACACS را مشاهده کنید، باید بر روی هر یک از گزینه‌ها کلیک کنید.

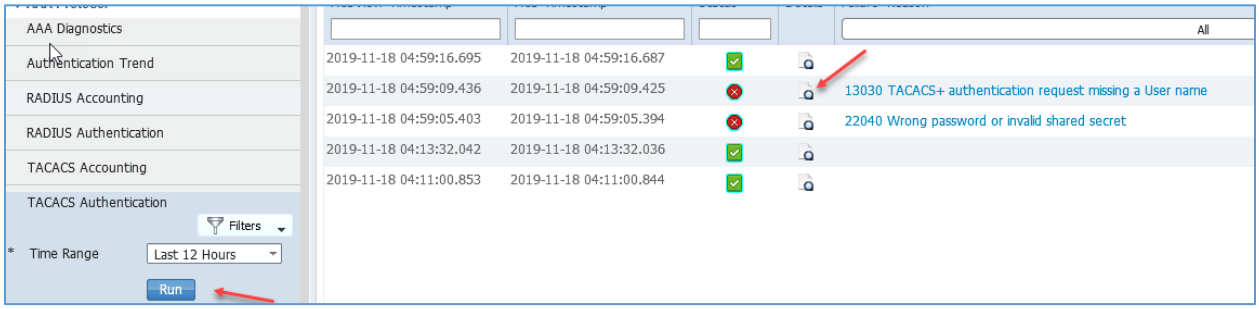
در شکل زیر بر روی TACACS Accounting کلیک کنید و مقدار زمان آن را مشخص و بر روی Run کلیک کنید، همانطور که مشاهده می‌کنید یک گزارش از دستوراتی که کاربر user1 ثبت کرده است را مشاهده می‌کنید که این موضوع واقعاً می‌تواند برای مدیریت کاربران بسیار کمک کننده باشد.

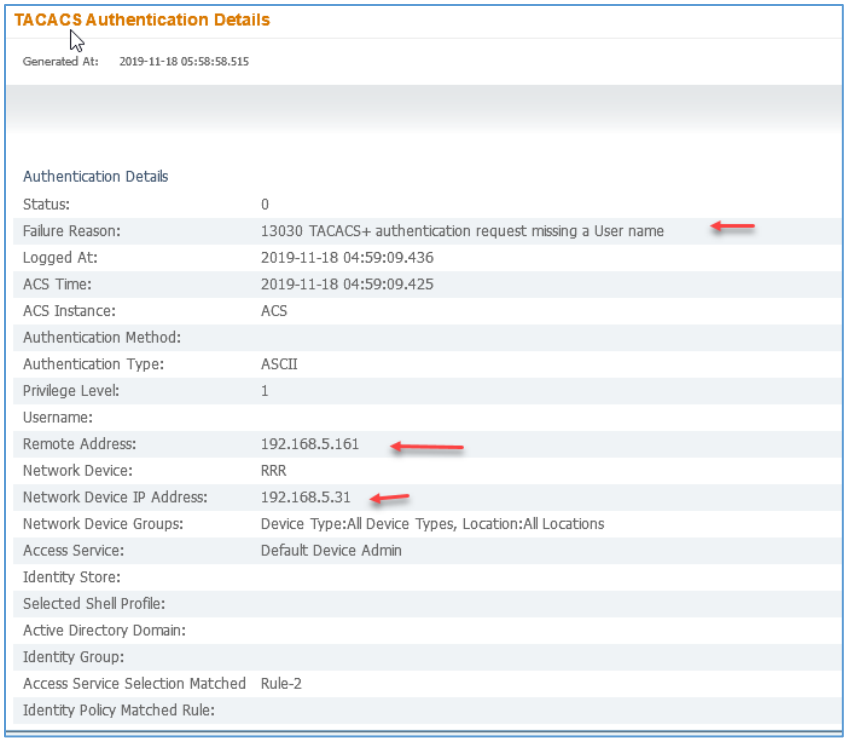


در شکل زیر قسمت Authorization را مشاهده می‌کنید که نشان می‌دهد کاربر تلاش داشته چه دستوراتی را اجرا کند و دستوراتی که در آن مجوز نداشته با ضربدر قرمز مشخص شده است، توجه داشته باشید آخرین تغییرات در اول سطر قرار می‌گیرد.



قسمت Authentication هم نشان می‌دهد که کاربر برای احراز هویت چه کاری انجام داده، اگر بر روی آیکون مشخص شده در شکل زیر کلیک کنید می‌توانید جزئیات کار را مشاهده کنید.





TACACS Authentication Details

Generated At: 2019-11-18 05:58:58.515

Authentication Details	
Status:	0
Failure Reason:	13030 TACACS+ authentication request missing a User name
Logged At:	2019-11-18 04:59:09.436
ACS Time:	2019-11-18 04:59:09.425
ACS Instance:	ACS
Authentication Method:	
Authentication Type:	ASCII
Privilege Level:	1
Username:	
Remote Address:	192.168.5.161
Network Device:	RRR
Network Device IP Address:	192.168.5.31
Network Device Groups:	Device Type:All Device Types, Location:All Locations
Access Service:	Default Device Admin
Identity Store:	
Selected Shell Profile:	
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched	Rule-2
Identity Policy Matched Rule:	

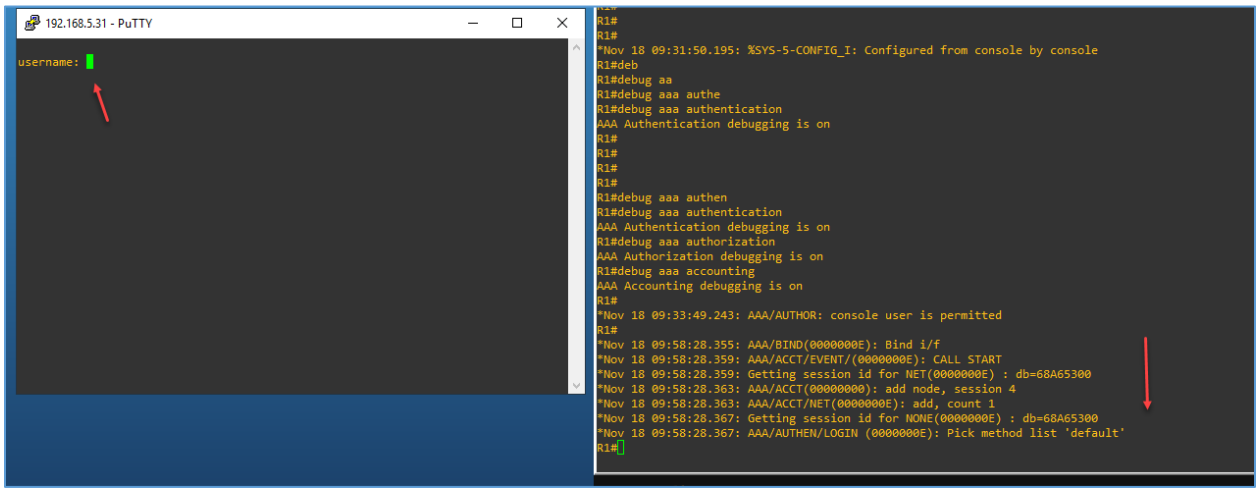
همانطور که در شکل روبرو مشاهده می‌کنید جزئیات کار مشخص شده است که در قسمت Remote Address مشخص شده است که چه آدرسی تلاش کرده به دستگاه 192.168.5.31 متصل شود که البته نام کاربری را به اشتباه وارد کرده است.

برای اینکه رویدادهای مربوط به AAA را در روتر مشاهده کنید می‌توانید دستور Debug را برای آن فعال کنید که برای این کار در روتر مورد نظر دستور زیر را وارد کنید:

```
R1#debug aaa authentication
AAA Authentication debugging is on
R1#debug aaa authorization
AAA Authorization debugging is on
R1#debug aaa accounting
AAA Accounting debugging is on
```

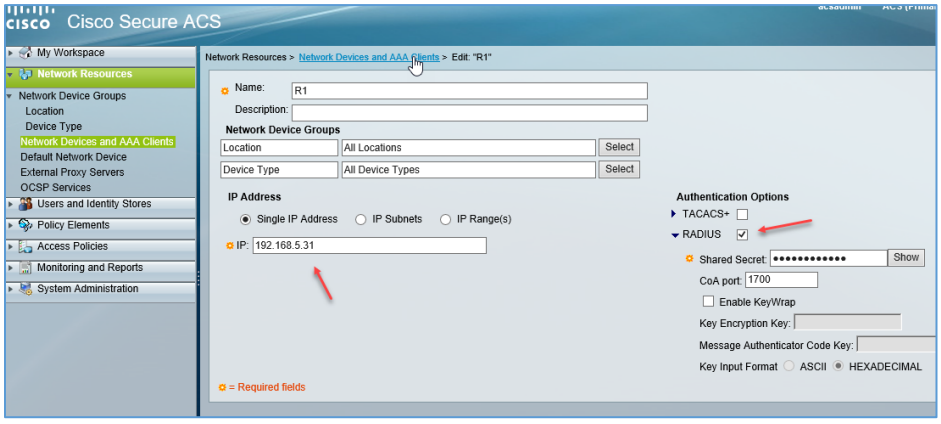
توجه داشته باشید که بعد از فعال کردن این دستورات، کارهایی که در زمینه‌ی AAA در روتر انجام شود به عنوان یک رویداد به شما نمایش داده خواهد شد.

همانطور که در شکل زیر مشاهده می‌کنید، زمانی که کاربر به روتر R1 از راه دور و از طریق Telnet متصل شد رویدادهای مربوط به AAA و authentication به نمایش گذاشته شد، که می‌تواند کمک کننده باشد و بیشتر در بحث Trublshoting مورد استفاده قرار میگیرد.



فعال‌سازی Radius در ACS

برای فعال‌سازی Radius در ACS باید دقیقاً همان کاری که برای TACACS انجام دادید را اجرا کنید فقط با یک تغییر جزئی.



وارد نرم‌افزار ACS شوید و از قسمت Network Resources بر روی گزینه‌ی Network Devices and AAA Clients کلیک کنید و یک Rule جدید ایجاد کنید و به مانند شکل، باید به جای انتخاب TACACS+ گزینه‌ی RADIUS را انتخاب کنید و رمز عبور آن را وارد کنید، توجه داشته باشید که پورت پیش‌فرض آن 1700 است، بعد از وارد کردن آدرس روتر و رمز عبور مشخص، اطلاعات را ذخیره کنید، با این کار تنظیمات قبلی که انجام داده بودید بر روی پروتکل RADIUS اجرا خواهد شد.

در ادامه باید دستورات روتر را به صورت زیر وارد کنید:

برای فعال‌سازی AAA باید دستور زیر را وارد کنید:

```
R1(config)#aaa new-model
```

برای ارتباط با سرور Radius باید دستور زیر را وارد کنید و آدرس و نام کاربر و رمز عبور را که مربوط به سرور Radius است را وارد کنید:

```
R1(config)#radius-server host 192.168.5.36 key test@12345
```

در دستورات زیر Authentication و Authorization را برای Radius فعال می‌کنیم:

```
R1(config)#aaa authentication enable default group radius
R1(config)#aaa authentication login default group radius local
R1(config)#aaa authorization exec default group tacacs+ local
```

در ادامه دستورات باید برای Telnet دستور زیر را وارد کنید.

```
R1(config)#line vty 0 4
R1(config-line)#login authentication default
```

بعد از انجام تنظیمات برای اینکه ارتباط را تست بگیریم باید از دستور زیر استفاده کنیم، که در قسمت آخر مشخص شده است که به درستی سرور Radius در دسترس است، فقط به این نکته توجه کنید که باید به جای user1 نام کاربری خود را به همراه رمز عبور آن وارد کنید.

```
R1#test aaa group radius user1 qq2123 legacy
*Nov 18 10:47:41.819: %SYS-5-CONFIG_I: Configured from console by console
R1#test aaa group radius user1 qq2123 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

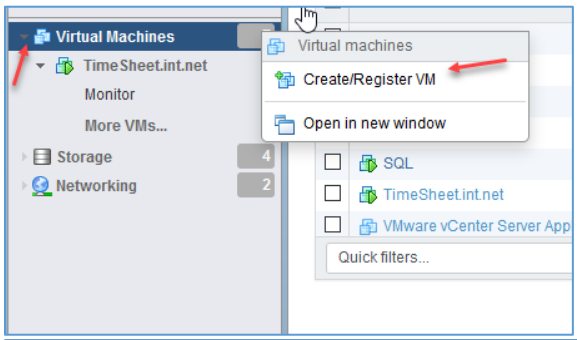
فصل پنجم – نصب و راه‌اندازی CISCO ISE

ISE (Cisco Identity Services Engine) یکی از جدیدترین نرم‌افزارها در مبحث AAA است که به نوعی جایگزین کامل ACS است و امروزه اکثر شرکت‌ها با این نرم‌افزار تمام تجهیزات خود را از نظر AAA کنترل می‌کنند.

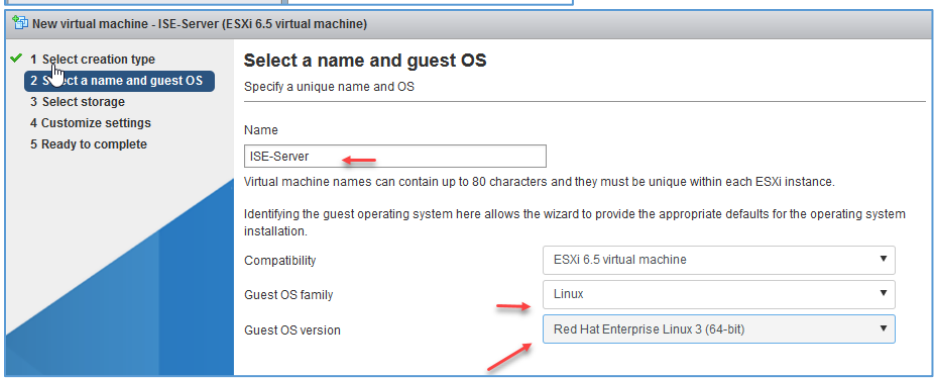
در این بخش می‌خواهیم نرم‌افزار CISCO ISE را دانلود و بر روی نرم‌افزار VMware Workstation آن را اجرا کنیم، البته می‌توانید در دیگر نرم‌افزارهای مجازی هم آن را اجرا کنید.

برای دانلود نرم‌افزار می‌توانید از لینک زیر استفاده کنید:

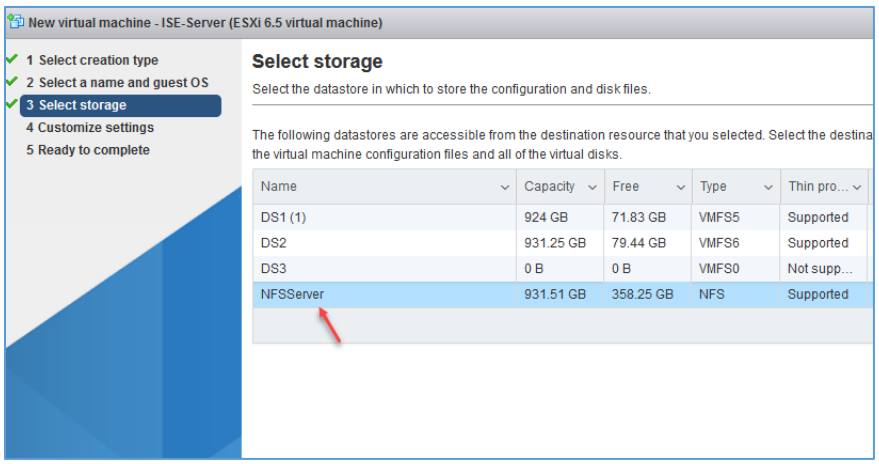
https://hellodigi.ir/network/cisco/701-cisco-identity-services-engine-ise-2-0-0-306.html



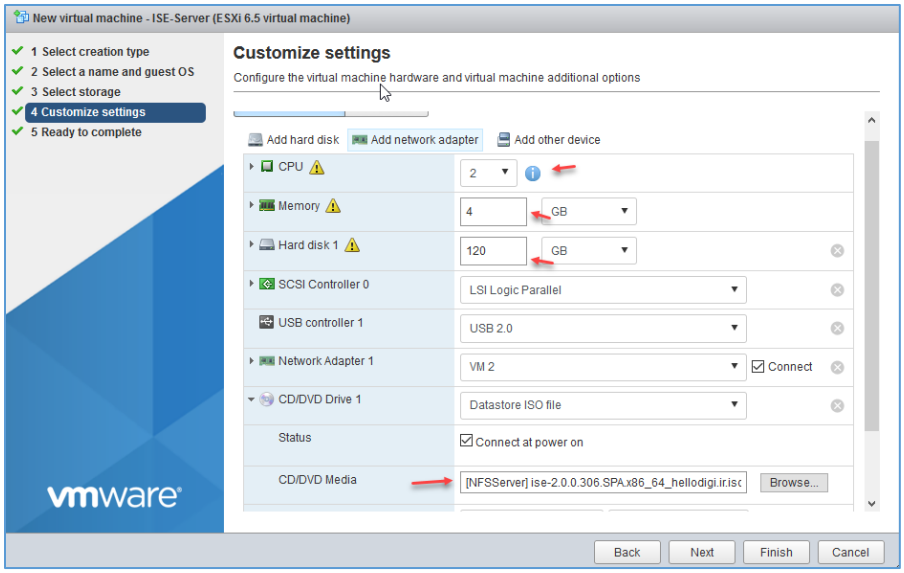
برای نصب این نرم‌افزار از ESXi 6.5 استفاده می‌کنیم و یک ماشین مجازی با دو هسته CPU و ٤ گیگ رم نیاز دارد که تنظیمات آن را انجام می‌دهیم.



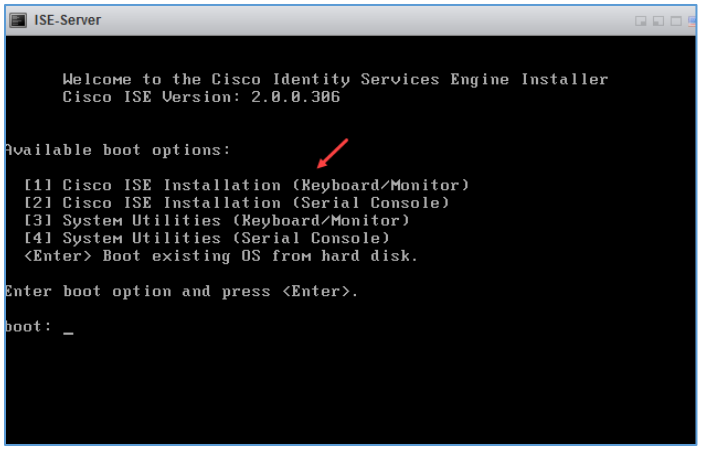
در این صفحه نام ماشین مجازی خود را وارد کنید و نوع سیستم‌عامل را Linux در نظر بگیرید و ورژن آن را هم Red Hat Enterprise Linux 3 در نظر بگیرید و بر روی next کلیک کنید.



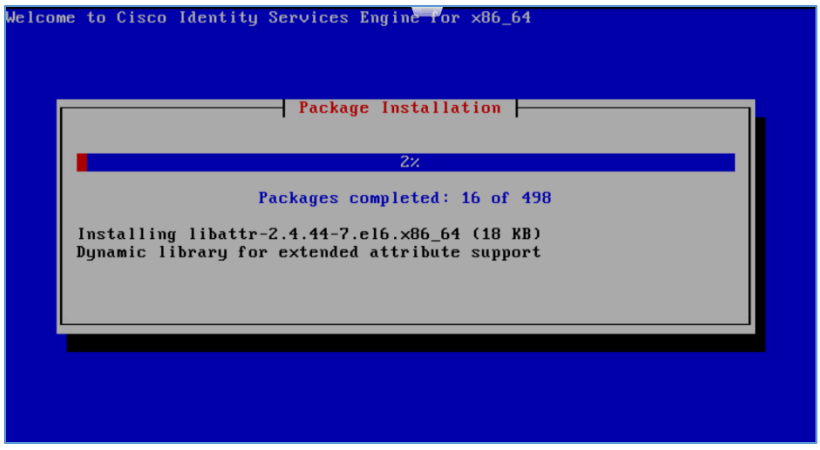
در صفحه روبرو باید محل ذخیره‌سازی را در هارد مورد نظر انتخاب کنید، توجه داشته باشید حداقل ۱۲۰ گیگابایت فضای خالی وجود داشته باشد.



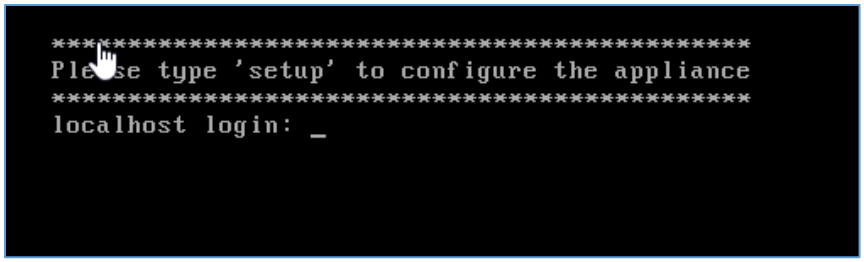
در این قسمت باید تعداد هسته CPU را حداقل ۲ در نظر بگیرید، مقدار رم ٤ گیگابایت و هارد دیسک آن را هم حداقل ۱۲۰ گیگابایت در نظر بگیرید که بهتر است حداقل ۲۰۰ باشد، توجه داشته باشید در قسمت CD/DVD باید فایل ISO مربوط به نرم‌افزار ISE که در قسمت قبل دانلود کردید را معرفی کنید تا ماشین از روی آن فایل بتواند ISE را راه‌اندازی کند، بر روی Finish کلیک کنید و ماشین مورد نظر را روشن کنید.



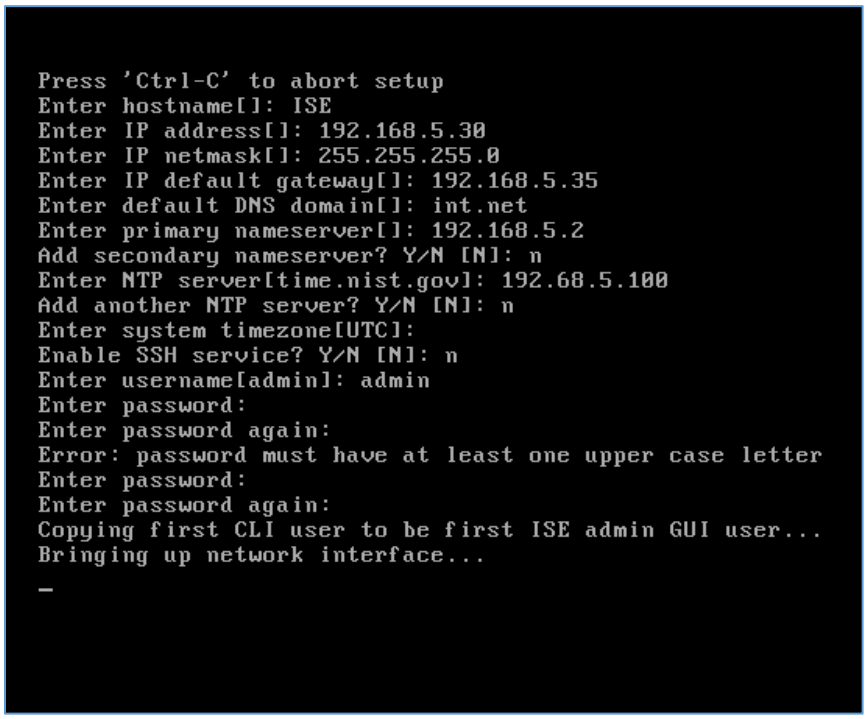
در این قسمت ٤ گزینه را مشاهده میکنید، برای نصب ISE باید عدد یک را وارد و بر روی Enter فشار دهید، بعد از این کار نرم‌افزار تنظیمات سخت‌افزاری را چک می‌کند در صورت مشکل به شما پیغام خواهد داد و اگر هم درست باشد ادامه خواهد داد.



بعد از انتخاب کلید یک ، نصب نرم‌افزار به صورت اتوماتیک انجام می‌شود.



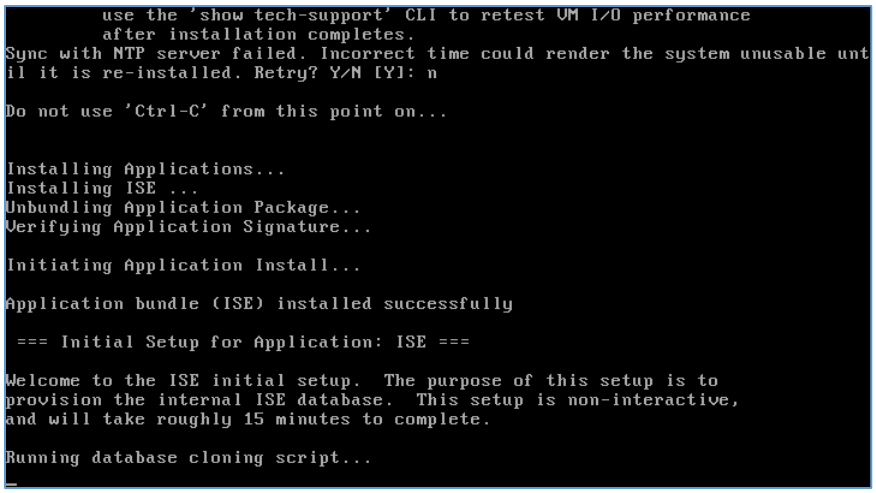
بعد از نصب ISE سیستم Restart شده و شکل روبرو ظاهر می‌شود که باید با وارد کردن دستور Setup تنظیمات اولیه آن را انجام دهید.



در این صفحه باید به ترتیب نام هاست، آدرس IP، Sunbnet، gateway، Domain و NTP Server را وارد کنید.

آدرس IP این سرور 192.168.5.30 در نظر گرفته شده است.

بعد از وارد کردن تنظیمات کار تکمیل می‌شود و سرویس‌های مورد نظر ISE اجرا خواهند شد.

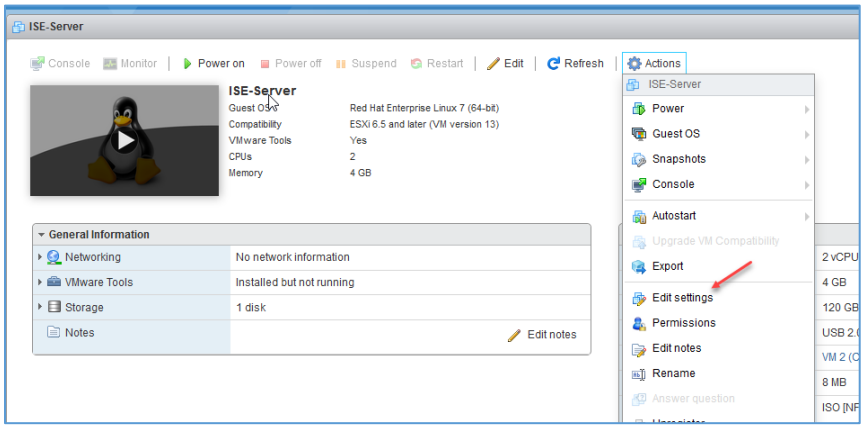


بسته به نوع سروری که برای ISE در نظر می‌گیرید، نصب سرویس و اجرای آن بین ۲۰ دقیقه تا چند ساعت زمان‌بر خواهد بود، همانطور که مشاهده می‌کنید سرویس‌ها اجرا شده و در مرحله‌ی نهایی آن قرار دارد.

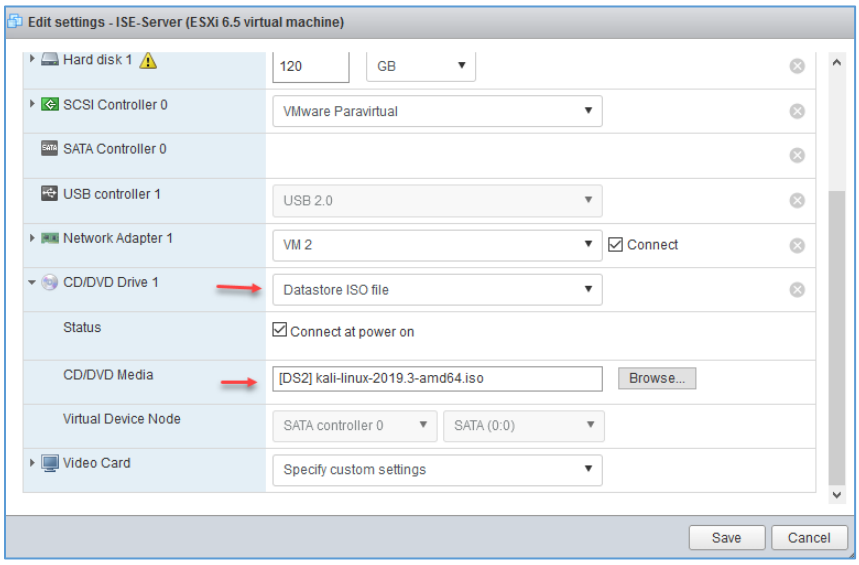
فعال‌سازی نرم‌افزار Cisco ISE

بعد از نصب کامل این نرم‌افزار باید لایسنس مورد نظر آن را فعال کنید، برای این کار یا باید لایسنس اورجینال را از سایت فروشنده تهیه کنید یا اینکه از لایسنس‌های کرک شده استفاده کنید، که متاسفانه اکثر نرم‌افزارها کرک می‌شوند.

برای اینکه لاینس نرم‌افزار را فعال کنیم باید به مانند نصب ACS یک سیستم لینوکس را در زمان بوت اجرا کنیم که در اینجا یک کالی لینوکس را در ESXi آپلود می‌کنیم و آن را در بوت ماشین مجازی ISE اجرا می‌کنیم.

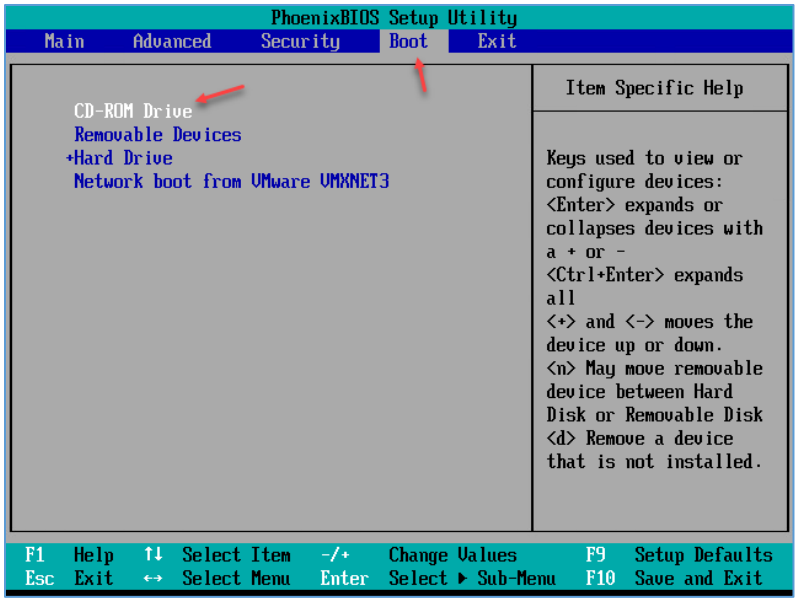


وارد تنظیمات مربوط به ماشین مجازی خود شوید.



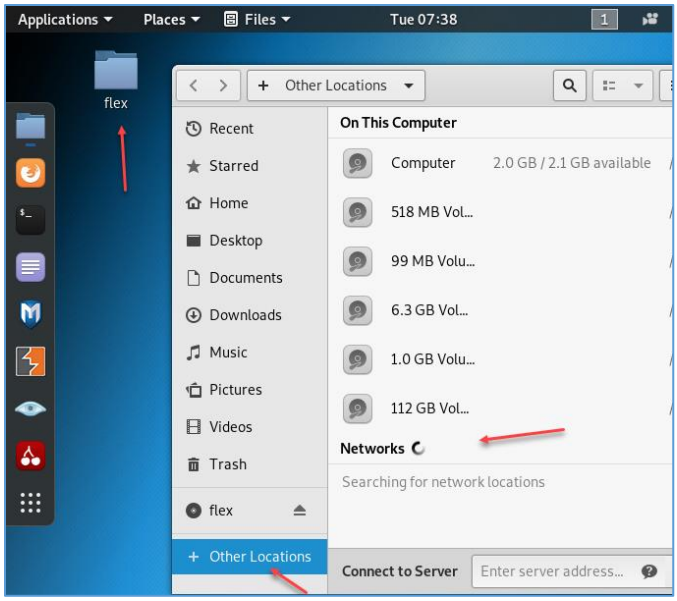
در این صفحه باید در قسمت CD/DVD فایل لینوکس کالی را انتخاب کنید که البته می‌توانید از ورژن‌های دیگر لینوکس هم استفاده کنید.

نکته: بهتر است پوشه Flex که در فایل دانلود شده ISE قرار دارد را به یک فایل iso تبدیل کنید (با نرم‌افزار PowerISO تبدیل کنید) و در همین قسمت یک CD/DVD جدید ایجاد کنید و فایل مورد نظر را به آن معرفی کنید تا بتوانیم در لینوکس آن را باز کنیم.



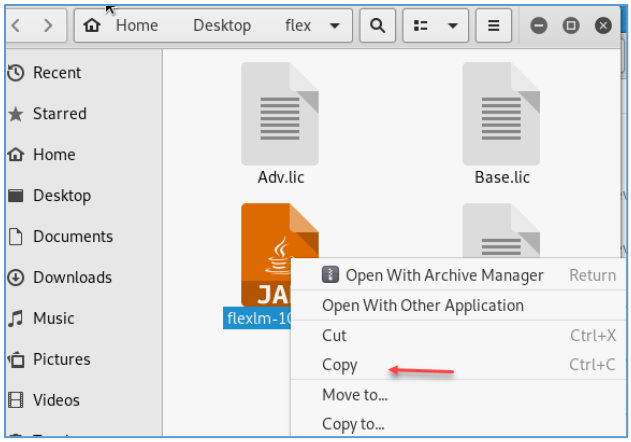
بعد از Restart کردن ماشین مجازی باید بر روی کلید F2 فشار دهید تا وارد صفحه Boot شوید و از قسمت Boot و با کلید + یا – گزینه‌ی CD-Rom Drive را به سطر اول بیاورید و بر روی کلید F10 فشار دهید تا اطلاعات ذخیره شود.

بعد از اجرا شدن لینوکس باید گزینه‌ی Live را انتخاب کنید.

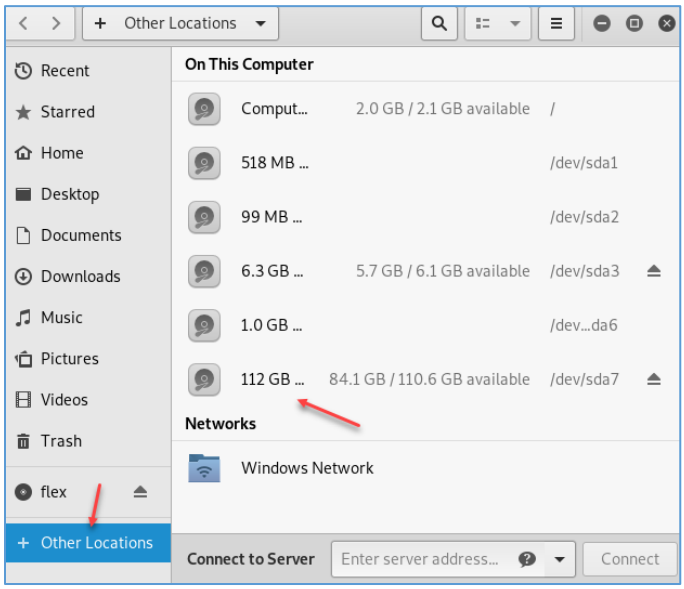


باید پوشه flex را بر روی Desktop کپی کنید که این کار یا از طریق شبکه می‌توانید انجام دهید و یا اینکه به صورت فایل ISO آن را به ماشین اضافه کنید که این موضوع را در شکل روبرو مشاهده می‌کنید.

در ادامه پوشه flex را باز کنید و فایل flexlm-10.9 را کپی بگیرید.



در ادامه Other Locations را انتخاب کنید، و پارتیشنی که بیشترین حجم را دارد را انتخاب کنید و وارد آن شوید که این موضوع در شکل روبرو مشخص شده است.

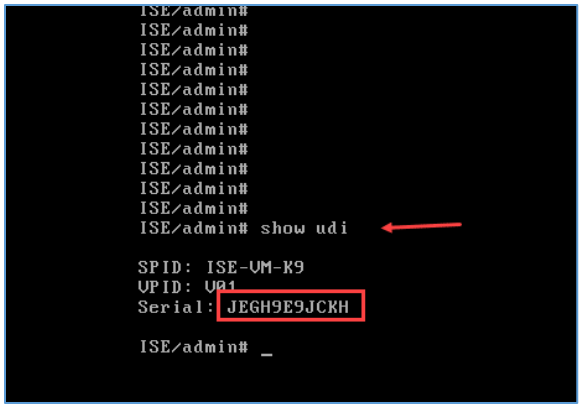


بعد از ورود به هارد مورد نظر باید به دو مسیر جداگانه بروید و فایل مورد نظر را در آن Replace کنید یا جایگزین.

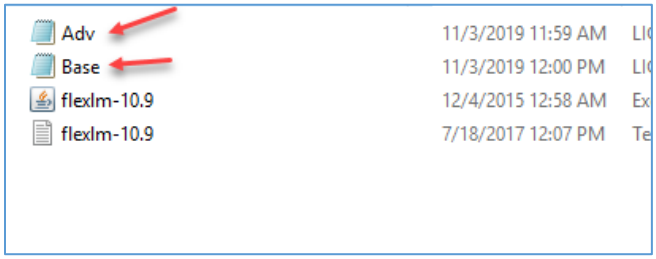
/opt/CSCOcpm/upgrade/javalib/flexlm-10.9.jar

/opt/CSCOcpm/appsrv/apache-tomcat-6.0.29/lib/flexlm-10.9.jar

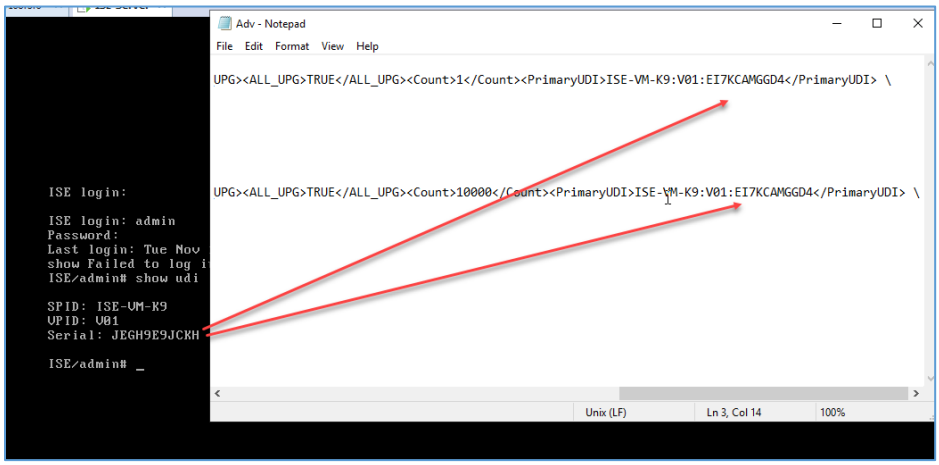
بعد از جایگزینی باید سرور را Restart کنید البته قبل از آن باید Boot آن را به حالت قبل برگردانید تا سیستم‌عامل ISE اجرا شود.



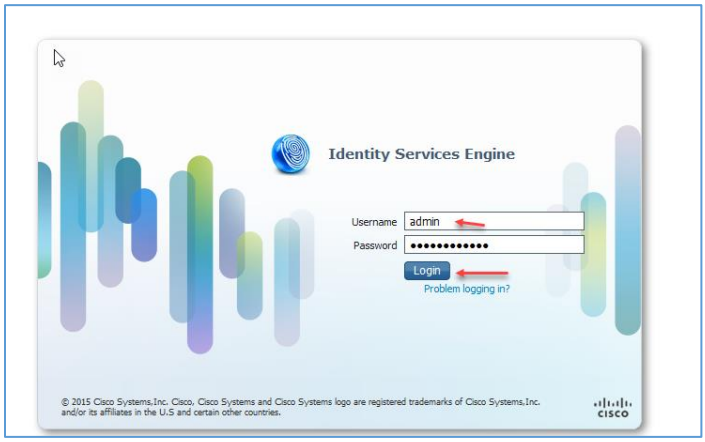
بعد از اجرا شدن ISE با نام کاربری و رمز عبور وارد آن شوید و دستور Show udi را وارد کنید، بعد از اجرا به شما یک شماره سریال می‌دهد که بر روی هر ماشین مجازی یا سیستم فیزیکی متغییر است، آن را یاداشت کنید تا در ادامه از آن استفاده کنیم.



وارد پوشه Flex شوید و دو فایل لایسنس را با Notpad باز کنید.



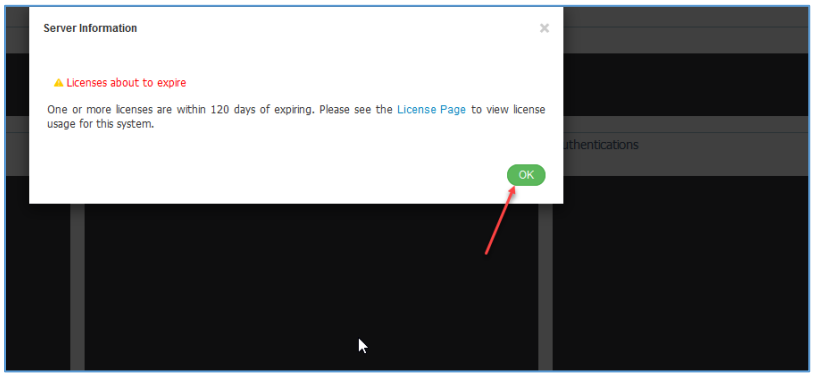
در این قسمت باید شماره‌ای (JEGH9E9JCKH) را که یاداشت کردید را به جای شماره‌های قدیمی (EI7KCAMGGD4) قرار دهید و فایل را ذخیره کنید برای هر دو فایل همین کار را انجام دهید.



بعد از اجرای تنظیمات بالا یک مرورگر در سیستم خود باز کنید و آدرس سرور ISE را وارد کنید تا شکل روبرو ظاهر شود، بعد از آن نام کاربری و رمز عبوری را که در مراحل قبل وارد کردید را وارد و تایید کنید.

```
ISE/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3199
Database Server                        running          42 PROCESSES
Application Server                     initializing
Profiler Database                      running          4220
AD Connector                           running          6248
M&T Session Database                   running          2695
M&T Log Collector                      running          6142
M&T Log Processor                      running          6062
Certificate Authority Service          running          6021
SXP Engine Service                     disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
% WARNING: ISE DISK SIZE NOT LARGE ENOUGH FOR PRODUCTION USE
% RECOMMENDED DISK SIZE: 200 GB, CURRENT DISK SIZE: 128 GB
```

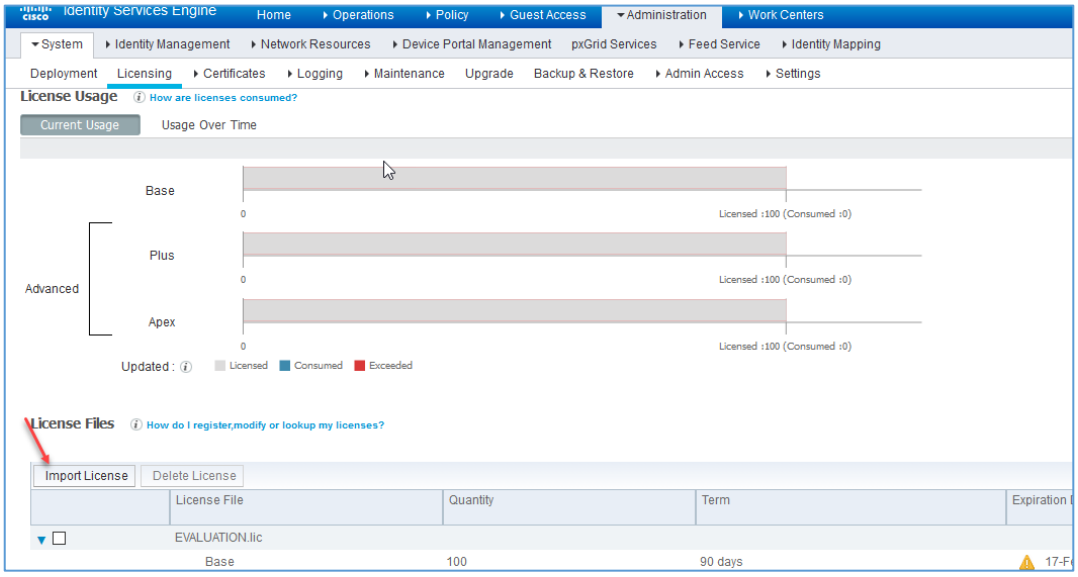
نکته: اگر چنانچه صفحه وب برای شما باز نشد، می‌توانید وضعیت سرویس Application Server را در ISE بررسی کنید که در شکل روبرو در حالت Initializing قرار دارد و در این حالت صفحه مورد نظر باز نخواهد شد و باید کمی صبر کنید تا به حالت running تغییر حالت دهد.

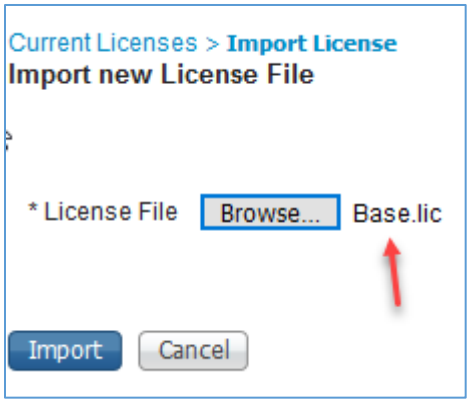


بعد از ورود با چند پیغام مواجه خواهید شد که یکی از آنها مربوط به لایسنس است و باید بر روی License Page کلیک کنید.

نکته: صفحه ISE نیاز به Flash Palyer دارد که باید آن را دانلود و نصب کنید.

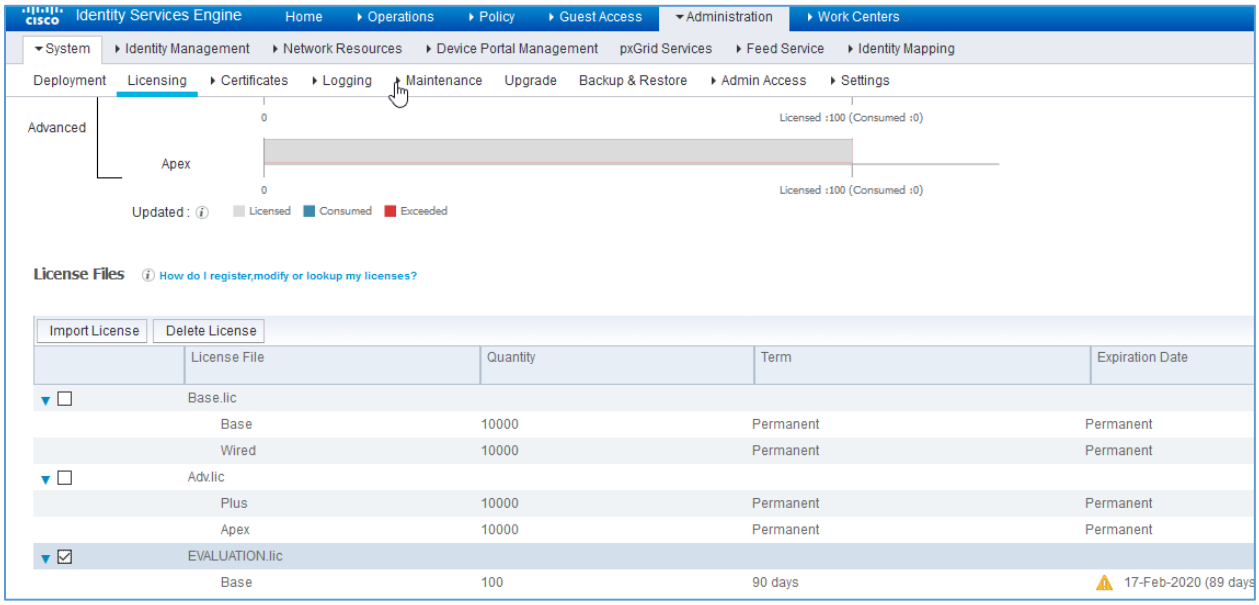
در شکل زیر باید فایل لایسنسی را که تغییر دادیم به برنامه معرفی کنیم برای همین کار باید بر روی IMPORT License کلیک کنید.



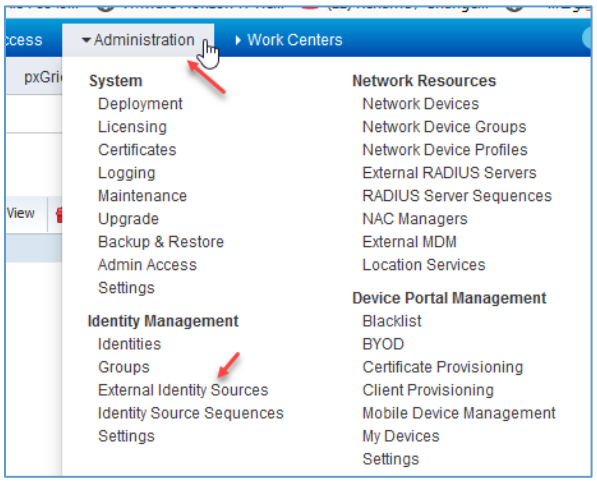


در این قسمت باید بر روی Browse کلیک کنید و اول فایل Base.lic را انتخاب و بر روی Import کلیک کنید و بعد از آن دوباره باید لایسنس Adv.lic را انتخاب و Import کنید.

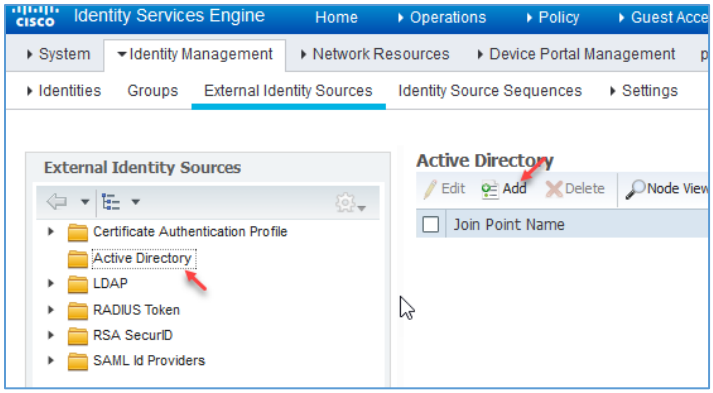
همانطور که در شکل زیر مشاهده می‌کنید لایسنس‌ها به درستی اضافه شده‌اند و حالا می‌توانیم بر روی نرم‌افزار کار کنیم.



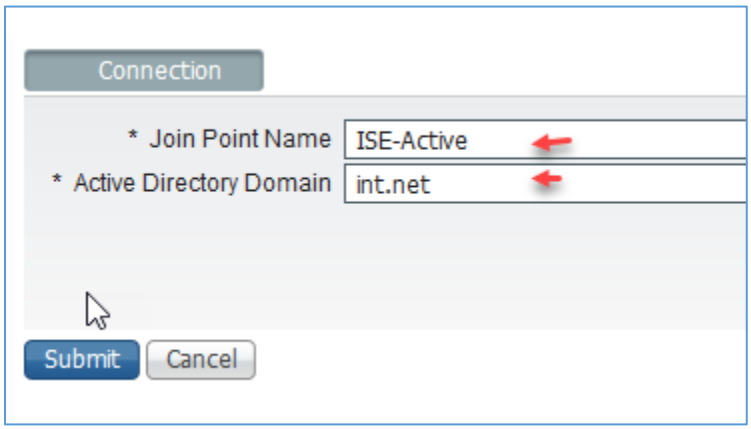
عضو کردن Cisco ISE در Active Directory



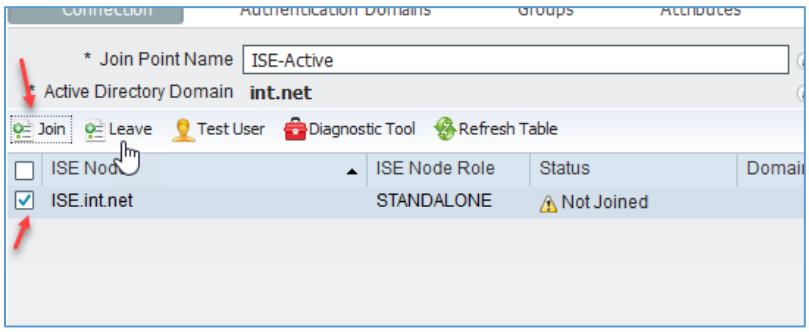
بعد از راه‌اندازی Cisco ISE می‌توانید آن را به سرویس Active Directory شبکه خود متصل کنید تا احراز هویت از طریق آن انجام شود، از منوی Administration بر روی External identity Sources کلیک کنید.



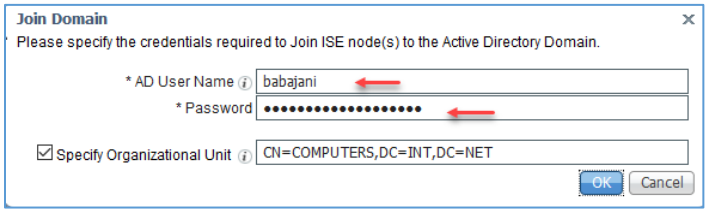
در این صفحه از سمت چپ بر روی Active Directory کلیک کنید و در صفحه‌ی باز شده بر روی Add کلیک کنید.



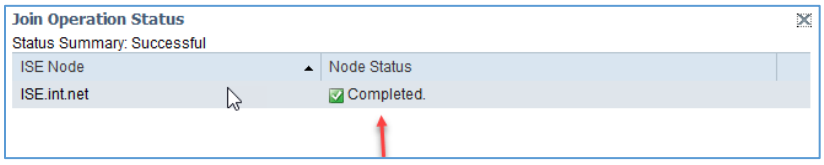
در این صفحه یک نام برای پروفایل خود وارد کنید و در قسمت Active Directory Domain نام دومین خود را وارد کنید و بر روی Submit کلیک کنید.



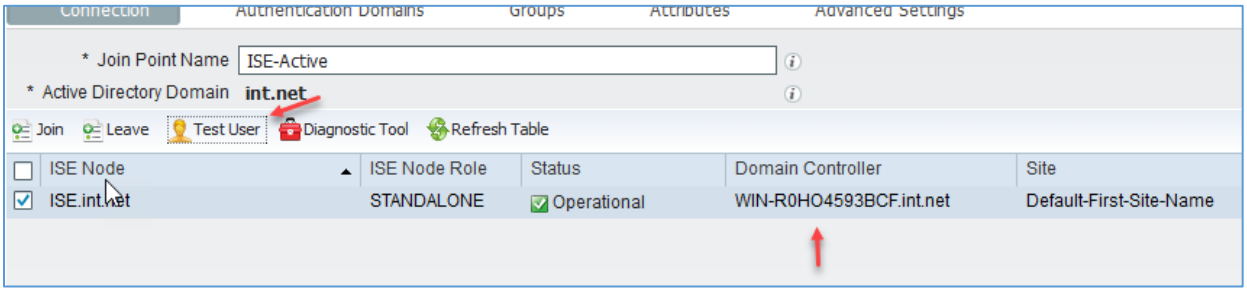
در این صفحه پروفایل خود را انتخاب کنید و بر روی Join کلیک کنید.

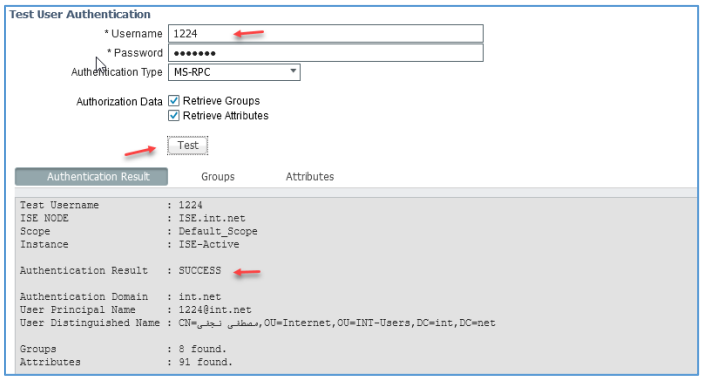


در این قسمت نام کاربری و رمز عبور مربوط به دومین خود را که دسترسی کاملی هم دارد را وارد کنید، در قسمت پائین آن به صورت پیش‌فرض اکانت مربوط به ISE در واحد Computers قرار می‌گیرد که شما در صورت نیار می‌توانید آن را تغییر دهید، بعد از کلیک بر روی OK شکل روبرو ظاهر می‌شود که نشان از موفقیت کار می‌دهد.

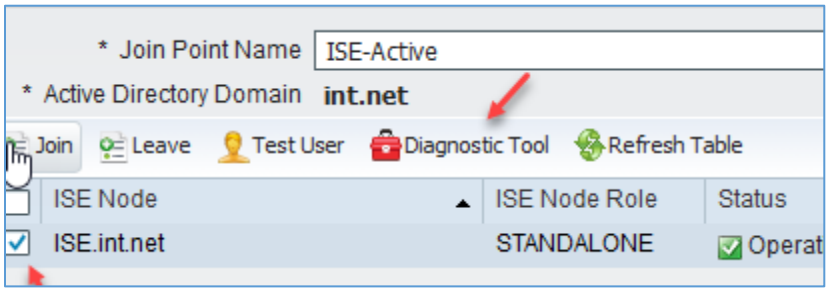


همانطور که در شکل زیر مشاهده می‌کنید ISE عضو دومین int.net شده است که Domain Controller آن هم مشخص شده است، برای اینکه تست بگیریم کاربران Active Directory بر روی ISE شناسایی می‌شوند یا نه، یابد بر روی Test User کلیک کنید.

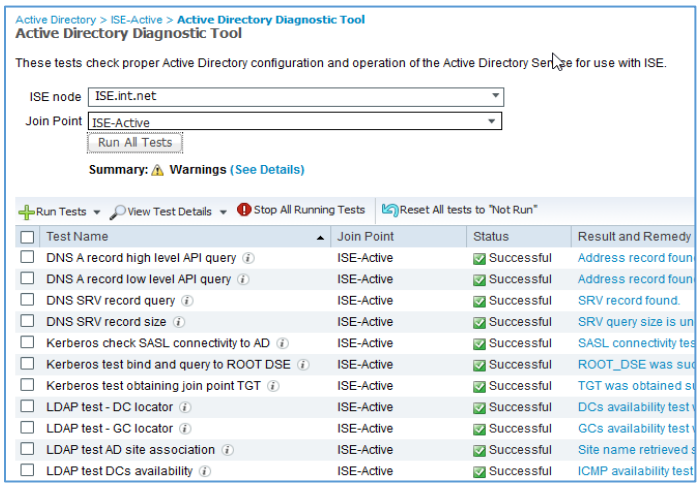




در این صفحه شماره‌ی کاربری 1224 که یک کاربر Active Directory است وارد شده است، با کلیک بر روی Test نتایج آن در زیر آن مشخص شده است که کلمه SUCCESS نشان دهنده‌ی موفقیت کار است، در تب‌های دیگر می‌توانید اطلاعات بیشتری از این کاربر بدست بیاورید.

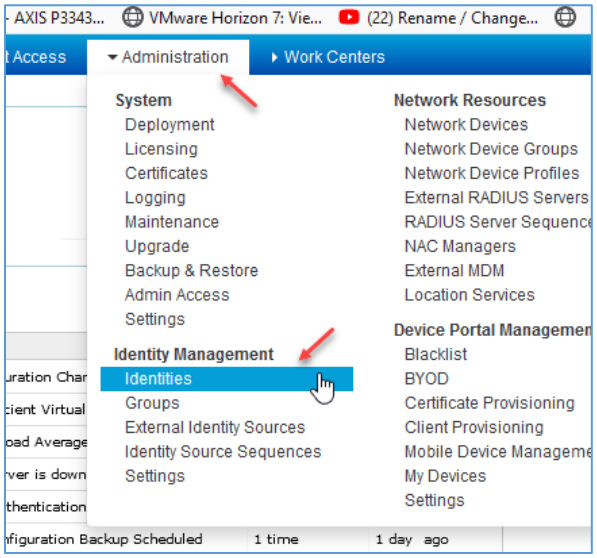


گزینه‌ای دیگر با نام Diagnostic Tool وجود دارد که در شکل هم مشخص شده است و برای تست کامل با جزئیات بیشتر می‌توانید از آن استفاده کنید.

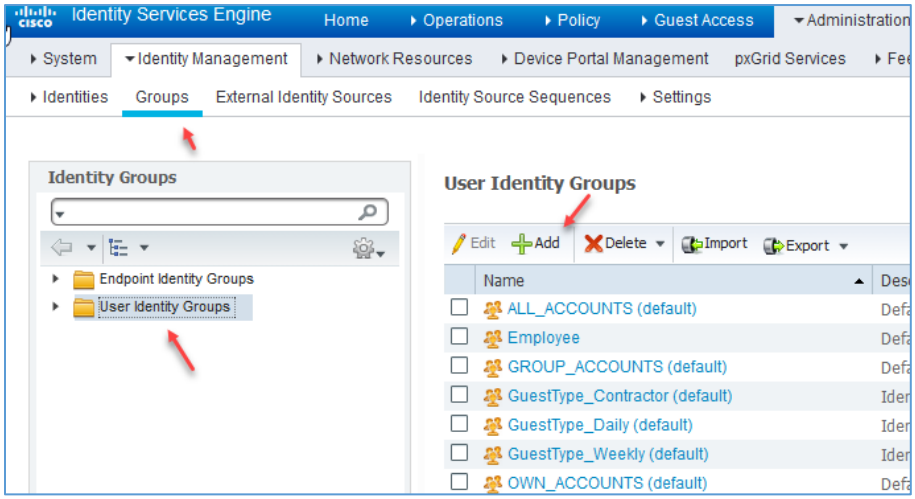


با کلیک بر روی Run All Tests تست‌های مورد نیاز انجام می‌شود و نتیجه آن در شکل روبرو مشخص شده است.

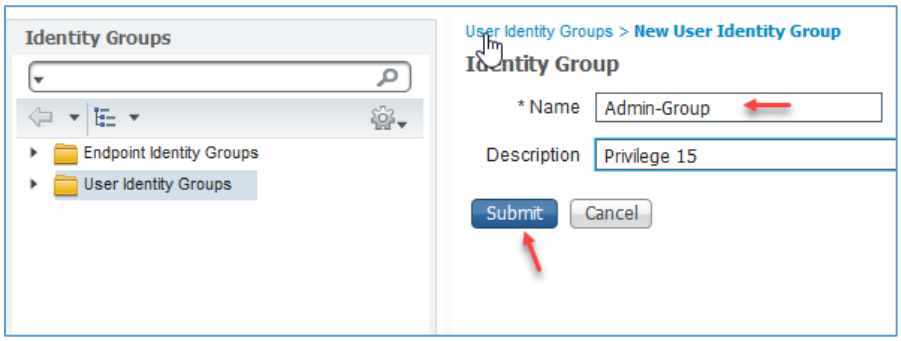
تعریف کاربر داخلی در CISCO ISE



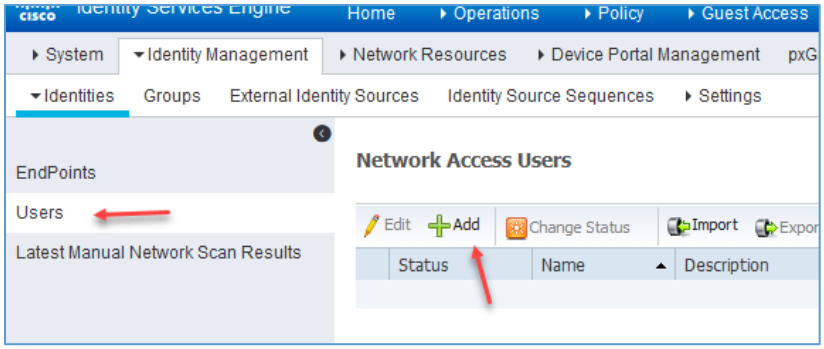
در این قسمت می‌خواهیم کاربران Local که در در ISE تعریف می‌شود را ایجاد کنیم و از طریق آن به روترها و دستگاه‌های دیگر شبکه متصل شویم، برای شروع کار از منوی Administration گزینه‌ی Identities را انتخاب کنید.



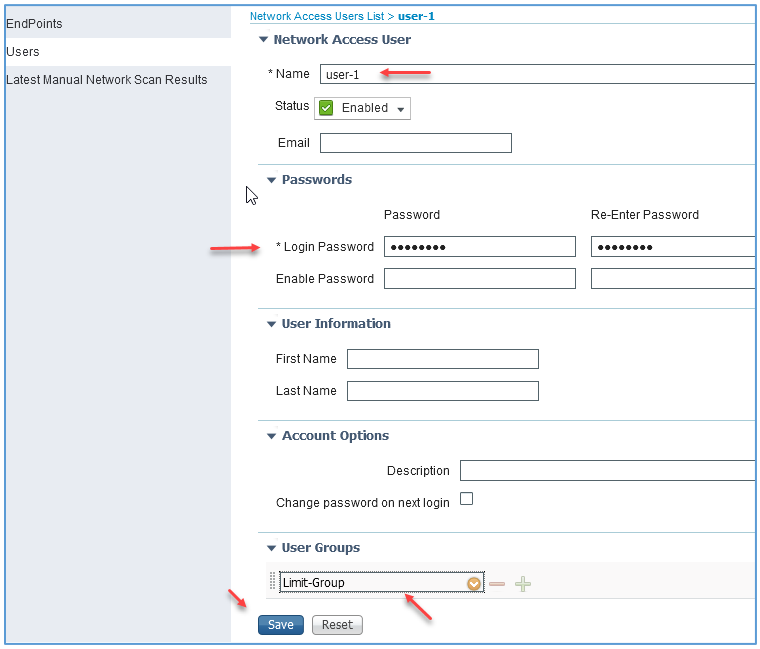
قبل از هر کاری باید دو گروه برای کاربران Admin و کاربران معمولی تعریف کنیم و دسترسی‌های لازم را به آنها بدهیم، برای این کار وارد تب Group شوید و بر روی User identity Groups و بعد بر روی Add کلیک کنید.



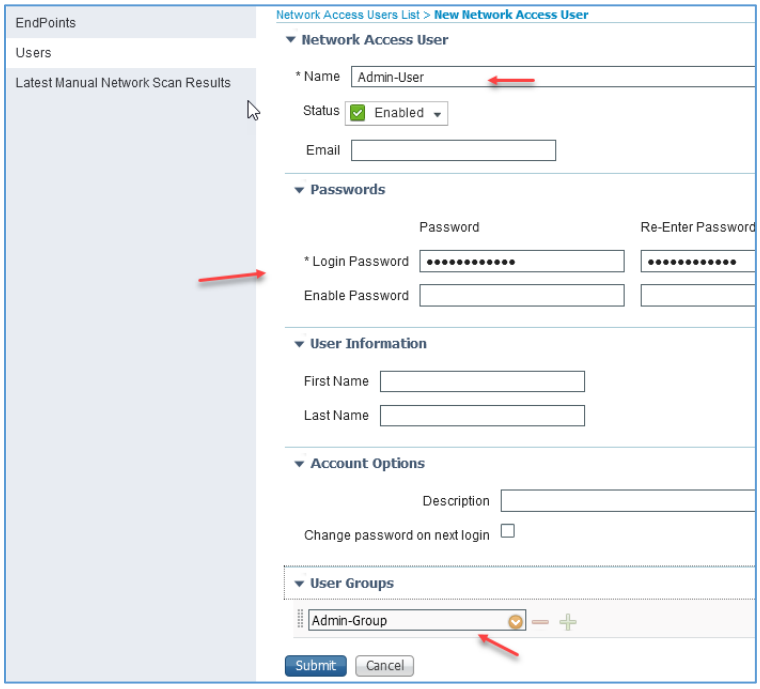
در این قسمت یک نام برای گروه خود وارد کنید، که در اینجا یک نام برای گروه Admin و دیگری برای گروه کاربران معمولی ایجاد می‌کنیم.



در ادامه وارد Users شوید و بر روی Add کلیک کنید.



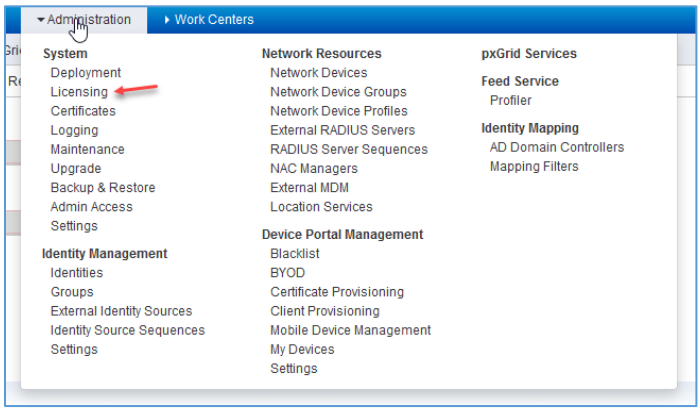
در این صفحه باید نام کاربری مورد نظر را وارد کنید و یک رمز عبور پیچیده برای آن در نظر بگیرید در آخر صفحه هم می‌توانید یک گروه برای این کاربر در نظر بگیرد که گروه Limit-Group را که در قسمت قبل ایجاد کردیم را انتخاب کنید و بر روی دکمه Submit کلیک کنید.



کاربر دیگری با نام Admin-user ایجاد کنید و آن را عضو گروه Admin-Group کنید و بر روی Submit کلیک کنید.

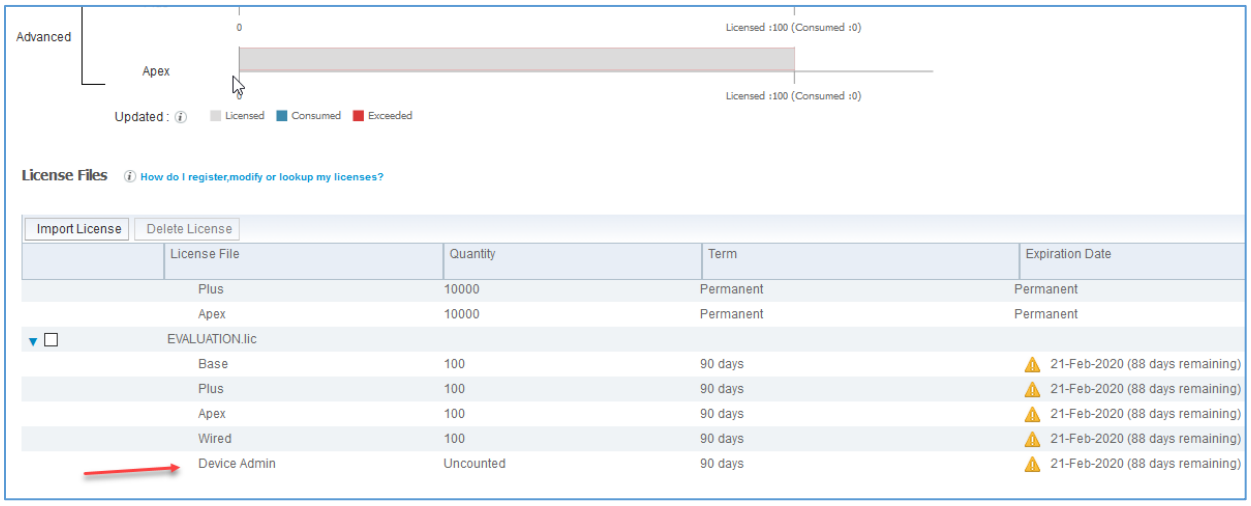
فعال‌سازی AAA در CISCO ISE

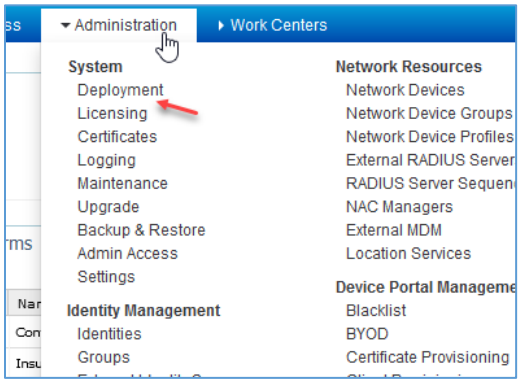
بعد از متصل کردن ISE به Active Directory و همچنین تعریف کاربر داخلی در ادامه کار می‌خواهیم سرویس AAA را برای دستگاه‌های شبکه در ISE فعال کنیم، برای این کار به ادامه مبحث توجه کنید.



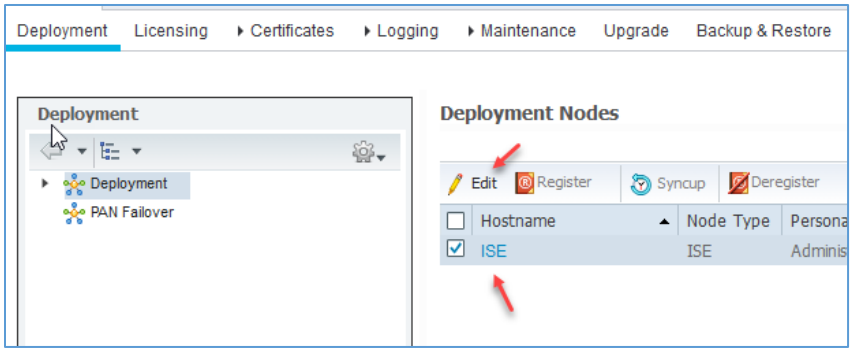
قبل از شروع هر کاری باید لایسنس مورد نظر که برای ISE فعال است را بررسی کنیم تا ببینیم اجزای مورد نظر ما فعال شده است یا نه، برای این کار از قسمت Administration بر روی Licensing کلیک کنید.

در تصویر زیر اگر به قسمت Device Admin توجه کنید، مقدار Quantity آن برابر Uncounted قرار گرفته که باید آن را تغییر دهیم.

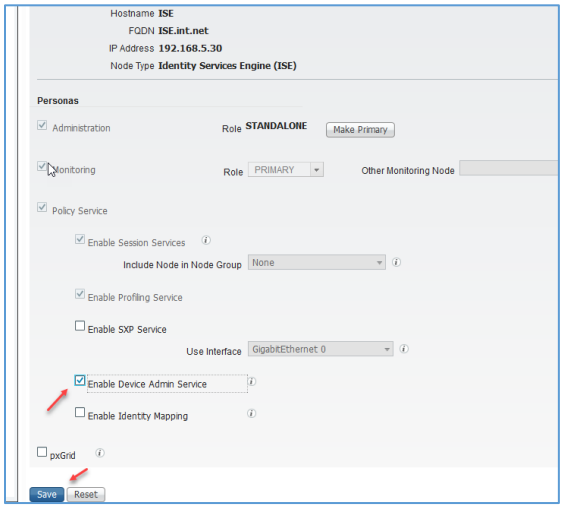




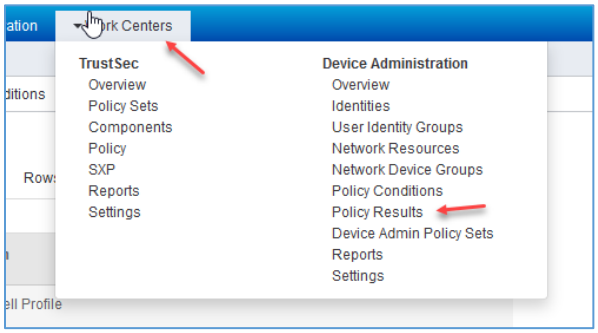
وارد منوی Administration شوید و گزینه‌ی Deployment را انتخاب کنید.



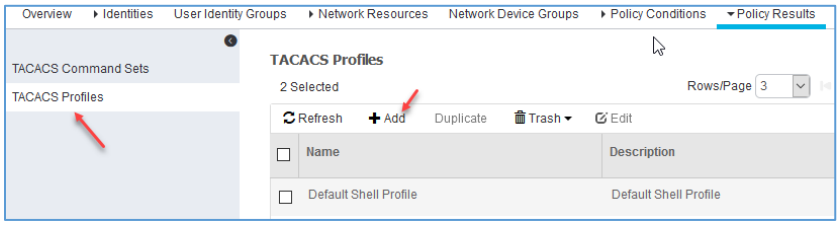
در این قسمت سرور ISE را انتخاب و بر روی دکمه Edit کلیک کنید.



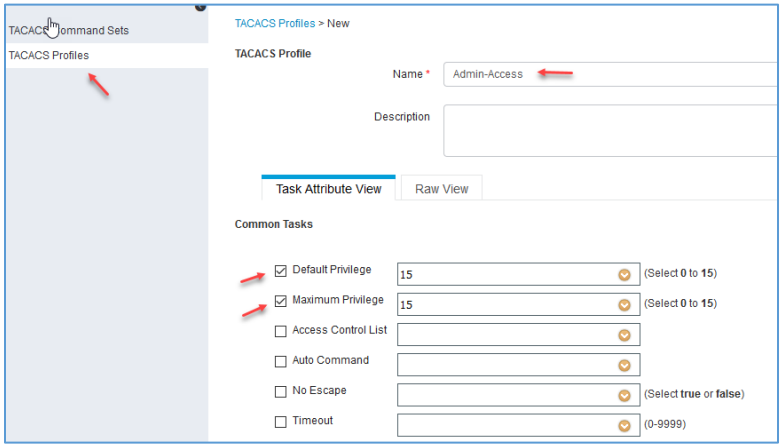
در این صفحه تیک گزینه‌ی Enable Device Admin Service را انتخاب کنید و بر روی Save کلیک کنید.



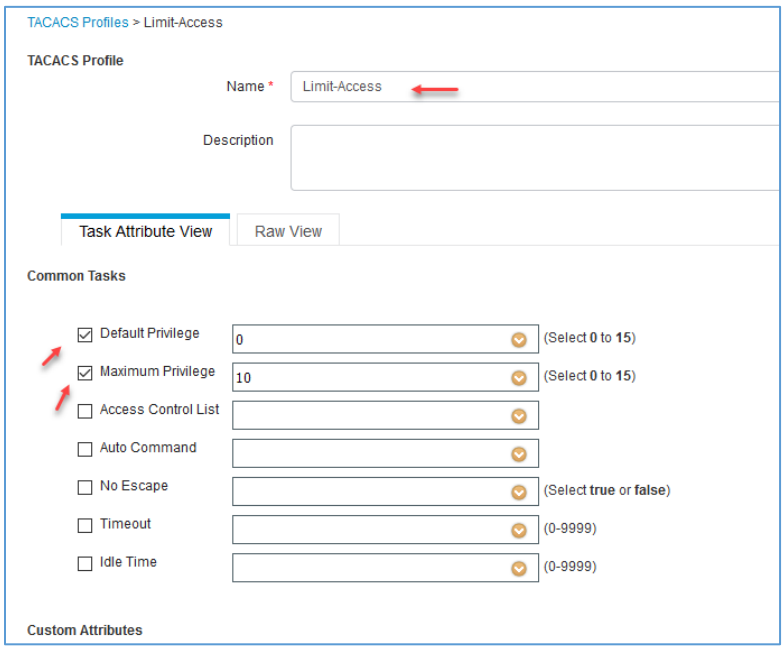
در ادامه باید پروفایل‌های مربوط به سطح دسترسی را ایجاد کنیم تا برای کاربران مشخص کنیم که به چه سطحی دسترسی داشته باشند و مجوز اجرای چه دستوری داشته باشند، برای این کار از منوی Work Centers گزینه‌ی Policy Results را انتخاب کنید.



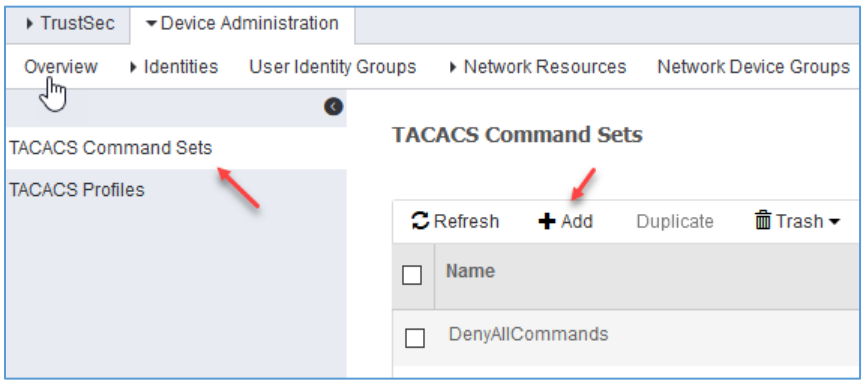
از سمت چپ وارد TACACS Profiles شوید و بر روی Add کلیک کنید.



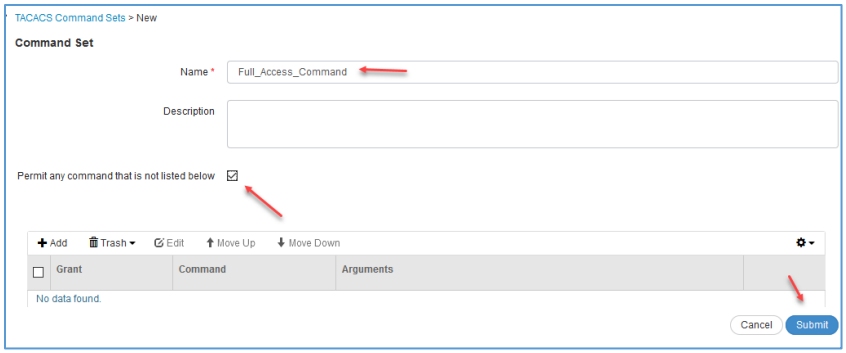
در این قسمت نامی برای پروفایل مورد نظر خود وارد کنید و در قسمت Common Tasks تیک دو گزینه‌ی اول را انتخاب کنید و سطح دسترسی آن را در بالاترین سطح یعنی ۱۵ قرار دهید، با این کار کاربرانی که به این پروفایل متصل شوند توانایی اجرای هر کاری را دارند.



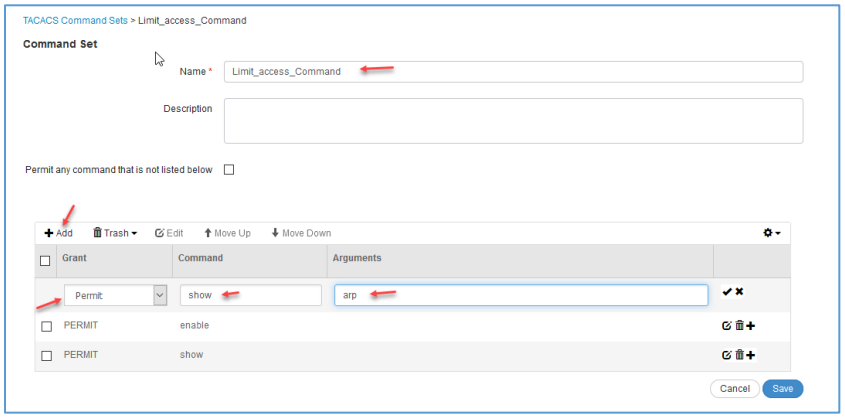
پروفایل دیگری با نام Limit-Access ایجاد می‌کنیم و سطح دسترسی آن را 0 و 10 در نظر می‌گیریم، هر چه عدد کوچکتر باشد سطح دسترسی کاربر کمتر خواهد بود.



در ادامه باید یک پروفایل برای Command ایجاد کنیم، برای این کار از سمت چپ وارد TACACS Command Sets شوید و بر روی Add کلیک کنید.

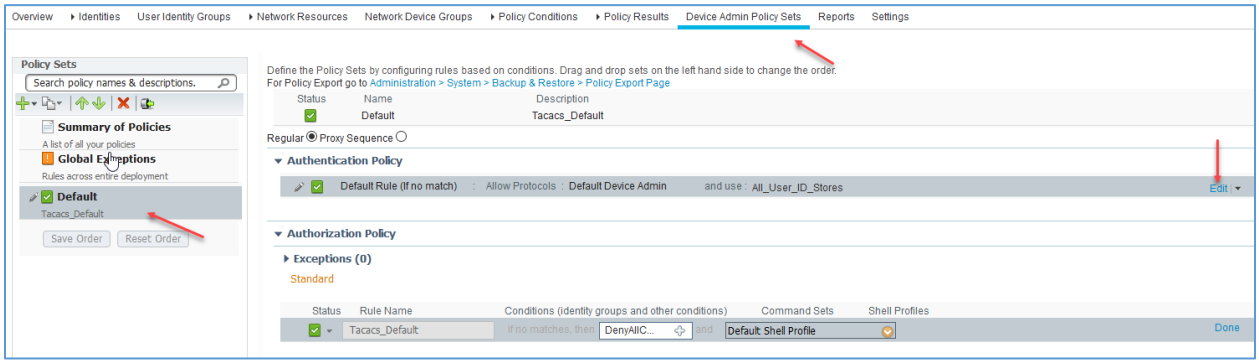


در این صفحه نام Full_Access_Command را وارد کنید و اگر تیک گزینه‌ی مشخص شده را انتخاب کنید تمام کاربرانی که دسترسی به این پروفایل دارند می‌توانند تمام دستورات را اجرا کنند البته اگر بخواهید می‌توانید دستورات خاصی را در لیست زیری آن مشخص کنید تا کاربر نتواند آن را اجرا کند، بر روی Submit کلیک کنید.

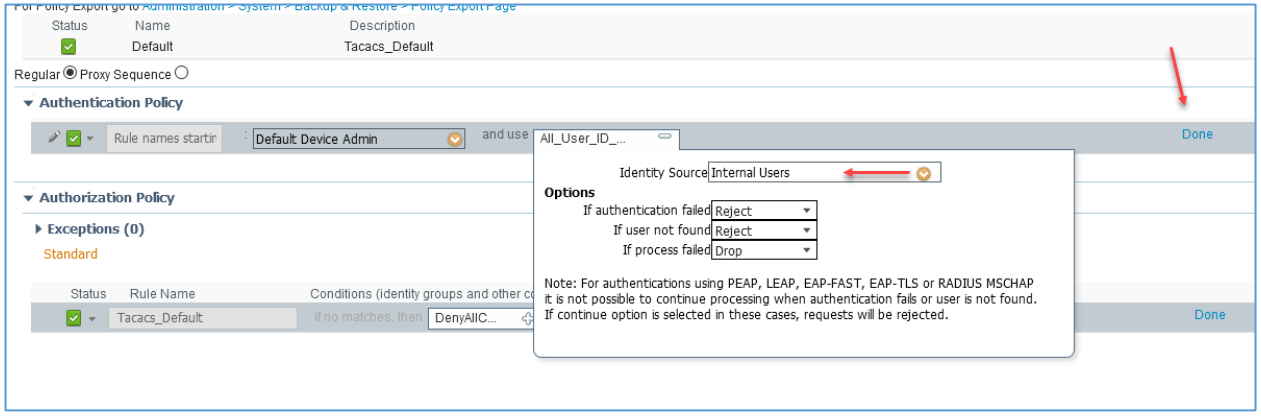


گروه دیگری هم با نام Limit_access_Command ایجاد می‌کنیم و این بار دستوراتی را که کاربر مجاز به استفاده از آن است را با کلیک بر روی Add به لیست اضافه می‌کنیم، به مانند شکل دستور Show با زیر دستور Arp دسترسی Permit داده شده است و این بدان معناست کاربر در روتر می‌تواند دستور Show Arp را اجرا کند.

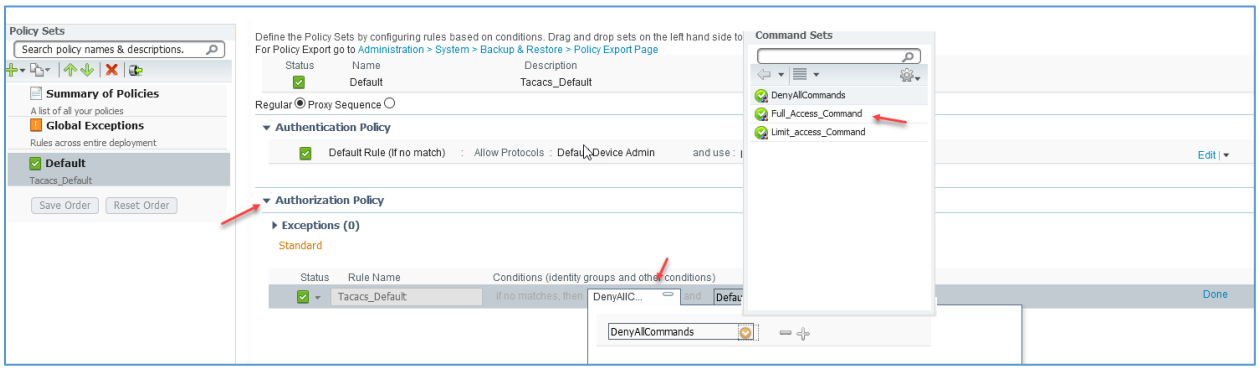
بعد از انجام مراحل بالا باید تنظیم نهایی را انجام دهیم تا دستگاه‌ها بتوانند از این سیاست پیروی کند، برای این کار وارد Device Admin Policy Sets شوید و بر روی Default کلیک کنید و در صفحه باز شده در قسمت Authentication Policy بر روی Edit کلیک کنید.



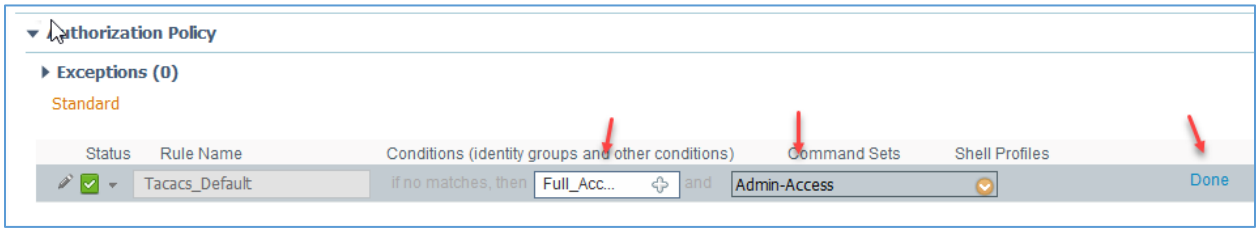
در شکل زیر از قسمت Identity Users گزینه‌ی Internal را انتخاب کنید و بر روی Done کلیک کنید، توجه داشته باشید به جای گزینه‌ی Internal می‌توانید از پروفایل Active Directory که از قبل ایجاد کردیم استفاده کنید.



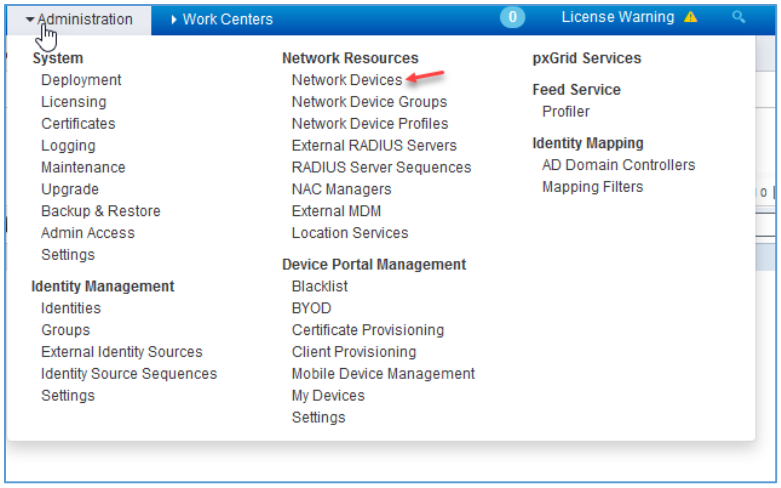
در شکل زیر و در سمت Authorization Policy که مربوط به بررسی دستورات است بر روی Edit کلیک کنید و از قسمت اول پروفایل Full_Access_Command را که ایجاد کرده بودید را انتخاب کنید.



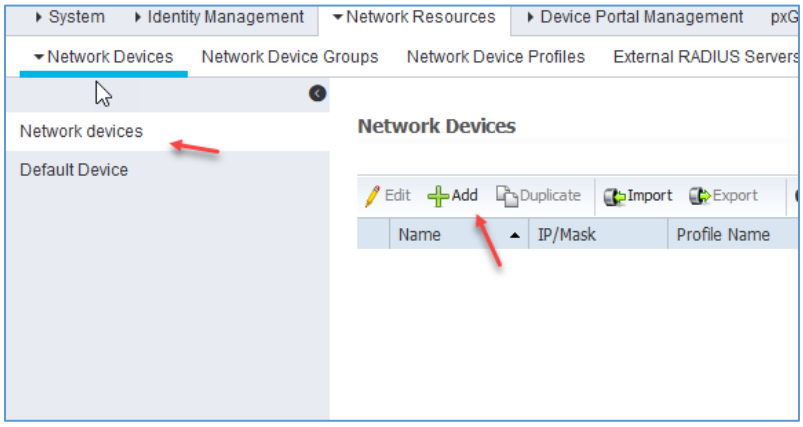
در ادامه و در قسمت Command Sets هم Admin-Access را انتخاب کنید و بر روی Done کلیک کنید.



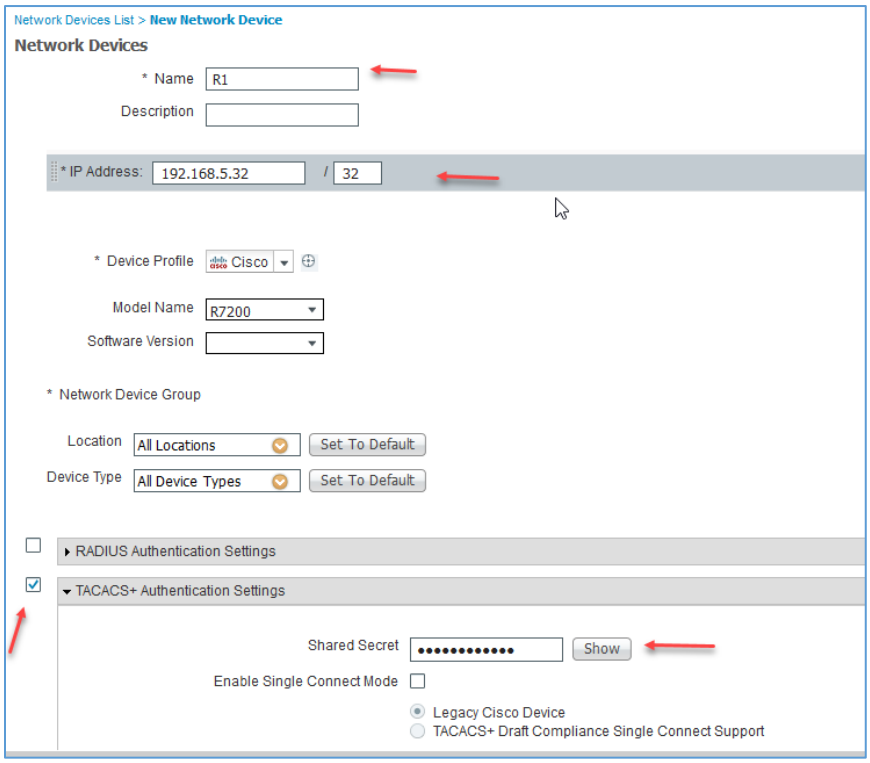
در آخر حتماً بر روی دکمه Save در پائین صفحه کلیک کنید تا تنظیمات به درستی اعمال شود، با انجام این مراحل Authentication، Authorization و Accounting فعال شده و در ادامه باید دستگاه‌ها را به ISE متصل کنیم



در ادامه کار باید در CISCO ISE یک Connection با دستگاه مورد نظر خود برقرار کنیم که برای این کار از منوی Administration بر روی Network Devices کلیک کنید.

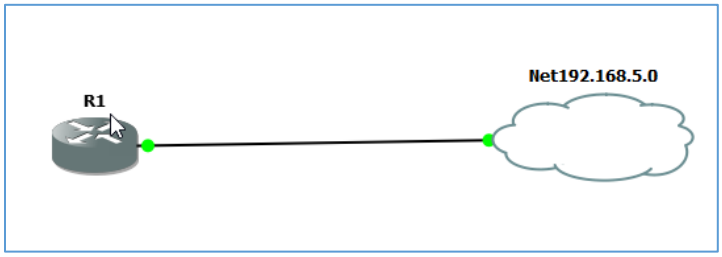


در این صفحه وارد Network devices شوید و بر روی Add کلیک کنید.



در این صفحه نام دستگاه خود را به همراه توضیحات مربوط به آن وارد کنید، در قسمت IP Address آدرس دستگاه و در قسمت پائین صفحه باید پروتکل احراز هویت را مشخص کنید که در اینجا می‌خواهیم از TACACS+ استفاده کنیم، تیک مورد نظر را انتخاب و یک رمز پیچیده برای آن وارد کنید و در آخر بر روی Submit کلیک کنید.

همه چیز از طرف CISCO ISE آماده شده و حالا باید وارد دستگاه خود شوید و دستورات مشخص شده را وارد کنید، توجه داشته باشید این دستورات تفاوت خاصی با دستوراتی که در قسمت ACS برای روتر وارد کردید ندارد، به مانند قبل یک روتر را در نرم‌افزار GNS3 با استفاده از Cloud به شبکه داخلی 192.168.5.0 متصل می‌کنیم که البته این کار را در قسمت ACS به طور کامل توضیح دادیم.



تنظیمات روتر R1

وارد Interface fast0/0 شوید، و آدرس IP مورد نظر را به مانند زیر، وارد و پورت را روشن کنید:

```
R1(config)#int fast 0/0
R1(config-if)#ip address 192.168.5.32 255.255.255.0
R1(config-if)#no sh
```

در ادامه باید با دستور زیر سرویس AAA را برای روتر فعال کنیم:

```
R1(config-if)#aaa new-model
```

با دستور زیر ارتباط با CISCO ISE برقرار می‌شود، توجه کنید که رمز عبور را در قسمت قبل وارد کرده بویم

```
R1(config)#tacacs-server host 192.168.5.30 key Test@123456
```

برای اینکه مشخص شود که ارتباط با سرور ISE برقرار است بهتر است از دستور زیر برای این کار استفاده کنید:

```
R1#test aaa group tacacs+ admin-user Test@123456 legacy
Attempting authentication test to server-group tacacs+ using tacacs+

User was successfully authenticated.
```

همانطور که در دستور بالا مشاهده می‌کنید پیغام "User was successfully authenticated" را که نشان دهنده ارتباط درست است را مشاهده می‌کنید.

در ادامه دستورات باید سه سرویس Authentication , Authorization , Accounting را فعال کنیم:

سه دستور زیر برای فعال‌سازی Authentication به کار می‌رود:

```
R1(config)#aaa authentication login default local group tacacs+

R1(config)#aaa authentication login console local
R1(config)#aaa authentication enable default group tacacs+ enable
```

این دستورات برای فعال سازی Authorization به کار می‌رود:

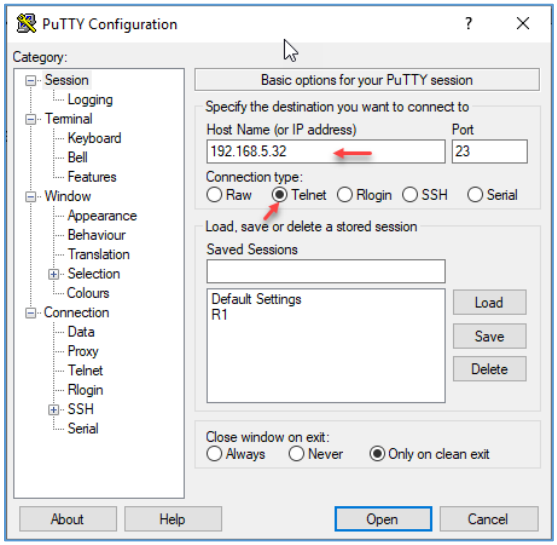
```
R1(config)#aaa authorization config-commands

R1(config)#aaa authorization exec default local group tacacs+

R1(config)#aaa authorization commands 15 default local group tacacs+
```

دستورات زیر هم برای فعال‌سازی Accounting است:

```
R1(config)#aaa accounting exec default start-stop group tacacs+

R1(config)#aaa accounting commands 1 default start-stop group tacacs+

R1(config)#aaa accounting commands 15 default start-stop group tacacs+
```

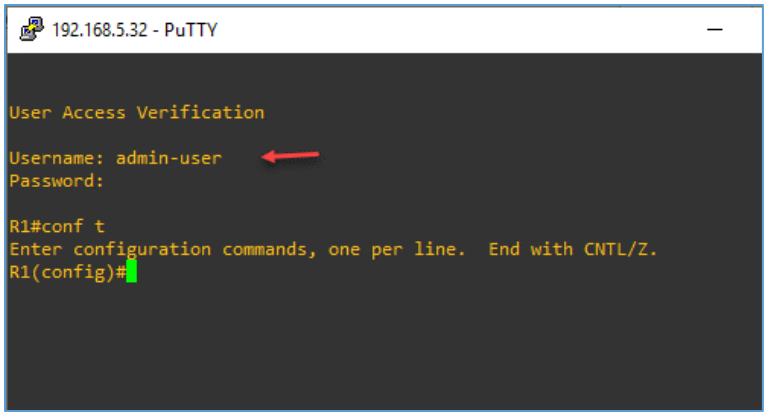
در آخر کار باید وارد Line شوید و سرویس Authentication را برای Telnet فعال کنید:

```
R1(config)#line vty 0 4
R1(config-line)#login authentication default
```

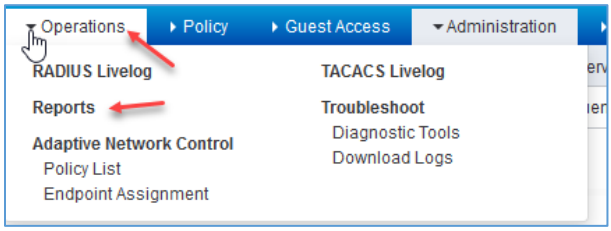


بعد از اجرای دستورات بالا با نرم‌افزار Putty یک ارتباط Telnet با روتر R1 که آدرس IP آن 192.168.5.32 است برقرار می‌کنیم.

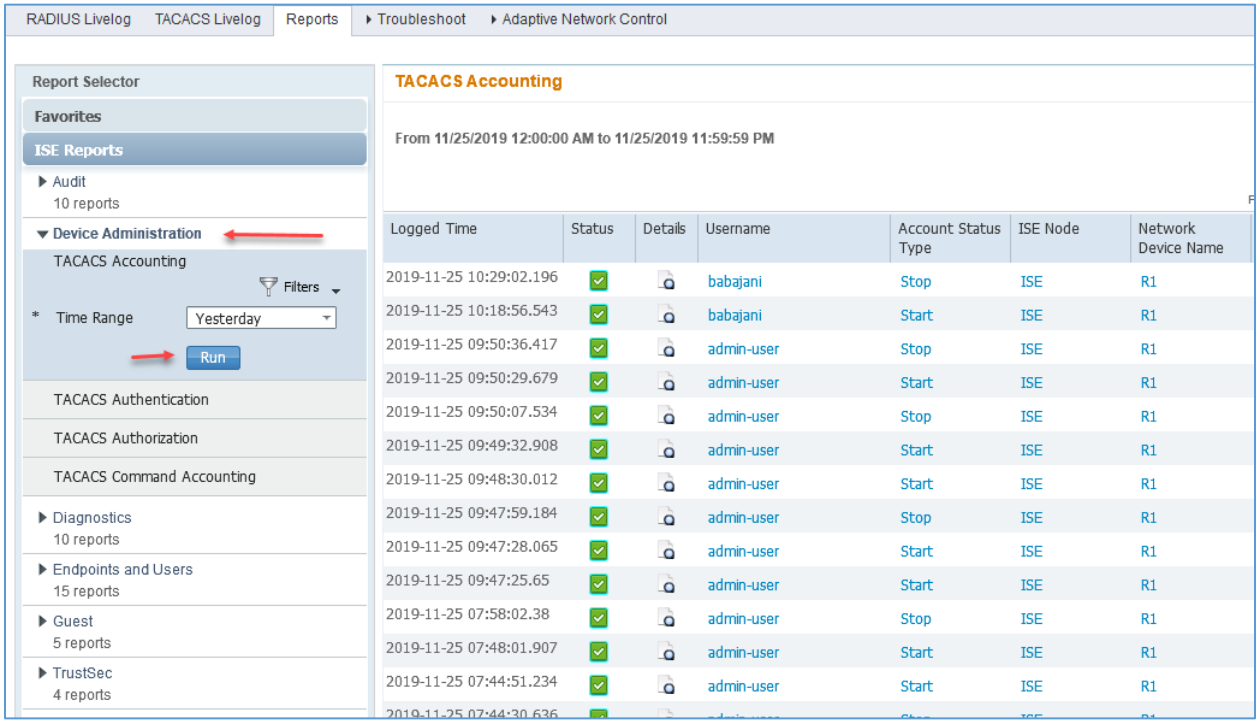
همانطور که مشاهده می‌کنید با استفاده از کاربر Admin-user توانستیم به روتر متصل شویم.



برای اینکه گزارشی از عملکرد سرویس AAA مشاهده کنید باید وارد منوی Operations در ISE شوید و گزینه‌ی Reports را انتخاب کنید.



در شکل زیر باید وارد Device Administration شوید و از زیر مجموعه آن یکی از گزینه‌های Authenticatin, Authorization و Accounting را انتخاب کنید و گزارش آن را مشاهده کنید.



فصل ششم – بررسی فایروال ASA شرکت سیسکو

خانواده‌ی دستگاه‌های ASA شرکت سیسکو از دستگاه های امنیتی محافظت از شبکه‌های سازمانی و مراکز داده‌ای هستند که امکان دسترسی کاربران به اطلاعات و منابع شبکه را در هر زمان و هر مکان و با استفاده از هر دستگاهی فراهم می‌کند . دستگاه های ASA شرکت سیسکو، در سرتاسر جهان گسترده شده‌اند که این موضوع نشان دهنده قدرت این نوع فایروال‌ها است.

ویژگی ها و قابلیت ها

ASA (Cisco Adaptive Security Appliance) نرم‌افزار اصلی سیستم عامل برای خانواده سیسکو ASA است. ASA همچنین با سایر فناوری‌های امنیتی ادغام شده است تا راه حل‌های جامع را ارائه دهند که به طور مداوم نیازهای امنیتی را در بر می‌گیرد.

از مزایای ASA می‌توان به موارد زیر استفاده کرد:

- یکپارچه کردن ارتباطات VPN و IPS
- پشتیبانی از AAA که در اوایل کتاب در مورد آن صحبت کردیم

- ایجاد Access Listهای استاندارد و پیشرفته که به اختصار ACL نام دارد.
- انجام سرویس‌های NAT، Routing، DHCP و....
- یکی از قابلیت‌های مهم ASA این است که تهدیدات مهم شبکه را شناسایی می‌کند و اجازه ورود آن به شبکه را نخواهد داد و همچنین می‌تواند تهدیدات پیشرفته را هم با الگوریتم خاص خودش شناسایی کند.

فایروال مفهومی است که توسط یک دستگاه واحد و یا گروهی از دستگاه‌ها اجرا می‌شود و عملکرد اصلی فایروال جلوگیری از ورود ترافیک ناخواسته است.

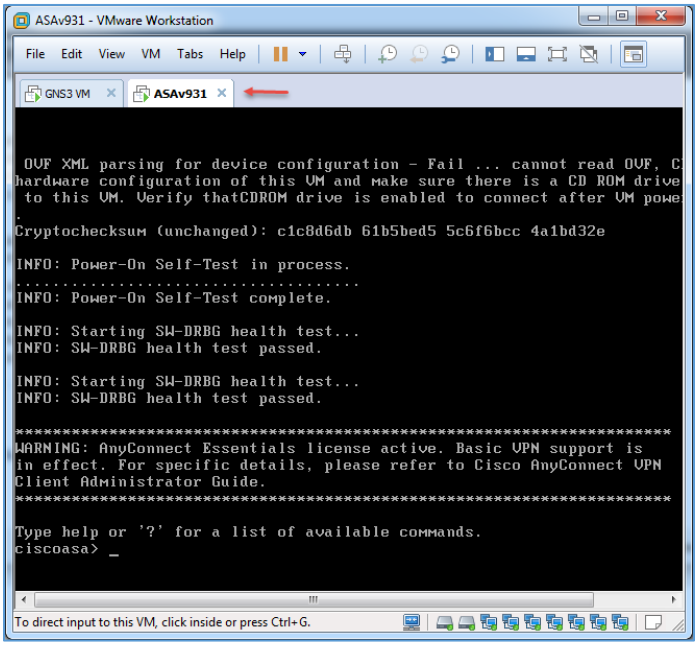
نصب و راه‌اندازی فایروال سیسکو ASA

برای راه‌اندازی فایروال سیسکو نیاز به دستگاه سخت‌افزاری آن داریم که در بازار امروز (٦ شهریور ١٣٩٧) یک فایروال ASA 5550 قیمتی بالای ٣٠ میلیون دارد که برای ما که می‌خواهیم کارهای تستی بر روی آن انجام دهیم واقعاً قیمت بالایی است، به خاطر همین باید به صورت مجازی بر روی GNS3 پیاده‌سازی کنید.

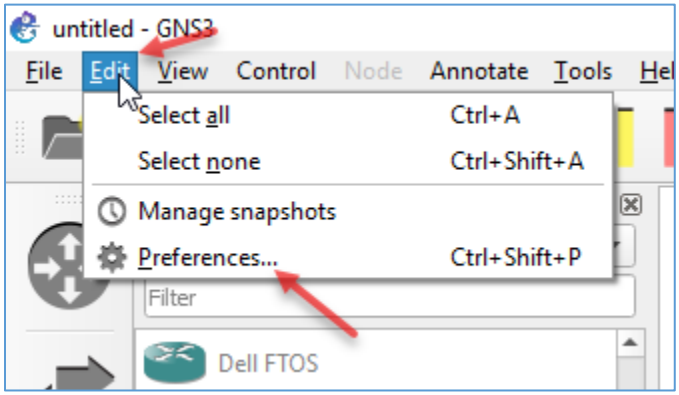
روش اول:

برای شروع کار فایل آماده VMware مربوط به فایروال ASA را از لینک زیر دانلود کنید:

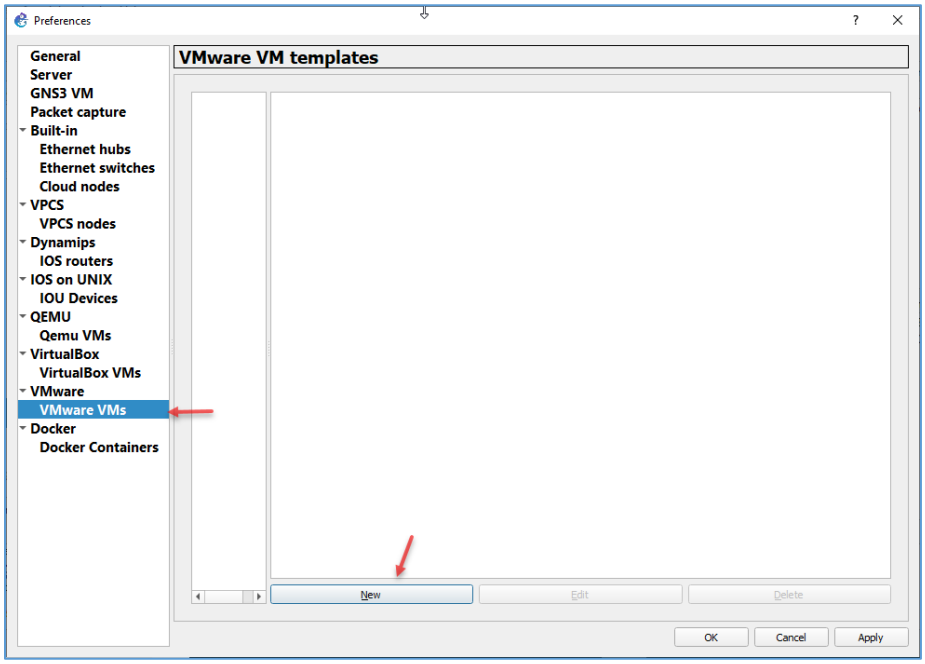
http://dl.hellodigi.ir/dl.hellodigi.ir/dl/cisco/asa/ASAv931.rar



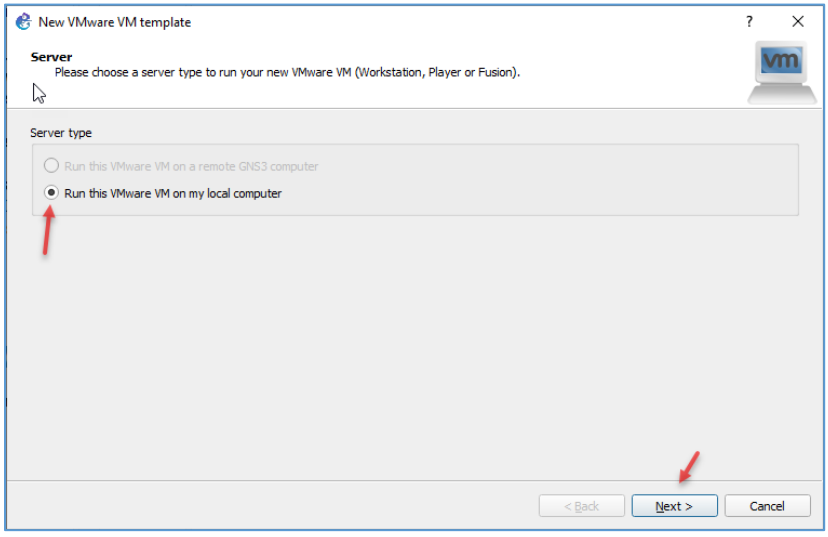
بعد از دانلود ماشین مجازی مربوط به فایروال ASA آن را اجرا کنید، در شکل روبرو این کار انجام شده است و ماشین به درستی اجرا شده است، برای ورود به مد جدید دستور Enable را وارد و بر روی Enter فشار دهید و در قسمت Password هم فقط بر روی Enter فشار دهید، در ادامه می‌خواهیم نحوه کانفیگ آن را با هم یاد بگیریم.



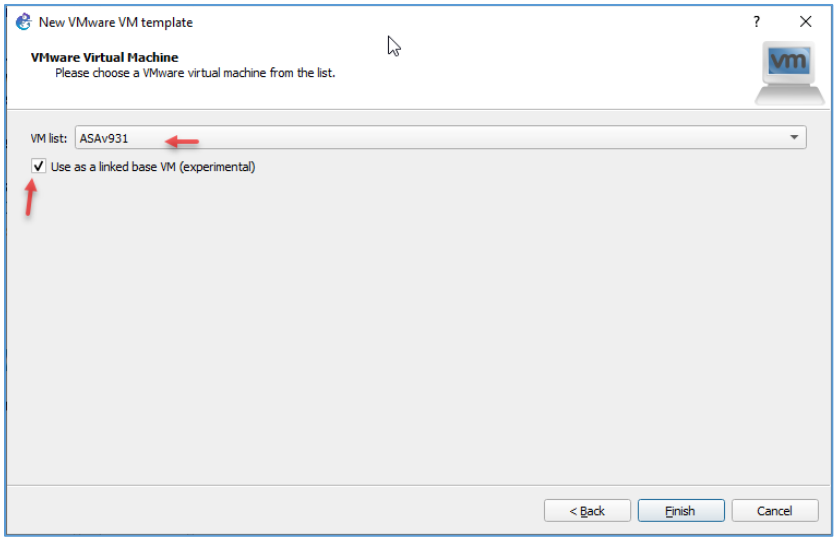
برای تنظیم فایروال در GNS3 به مانند شکل از منوی Edit گزینه‌ی Preferences را انتخاب کنید.



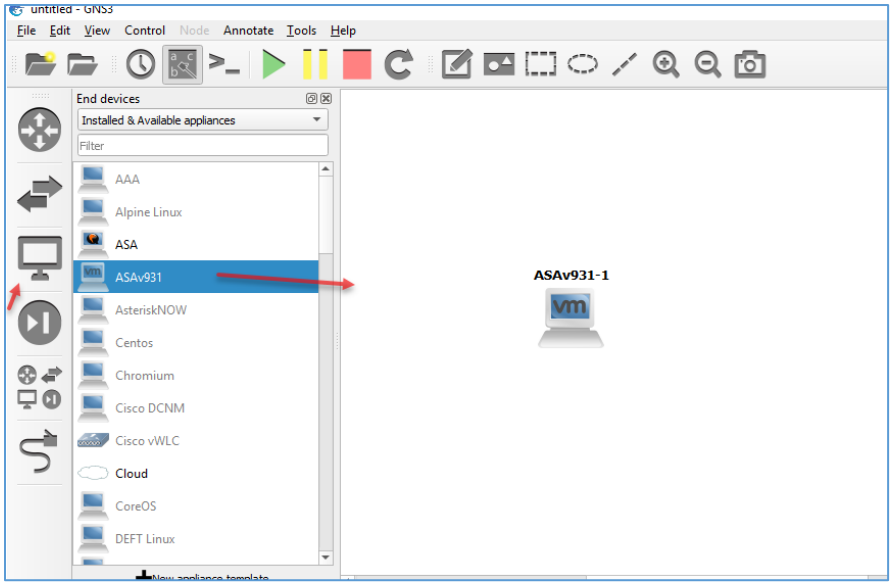
در این صفحه از سمت چپ گزینه‌ی VMware VMs را انتخاب کنید و بر روی New کلیک کنید.



در این صفحه گزینه‌ی Run this VMware on my local computer را انتخاب و بر روی Next کلیک کنید.



در این صفحه باید ماشین مورد نظر که مربوط به فایروال ASA است را از لیست انتخاب کنید، توجه داشته باشید برای اینکه مانند روتر یا سوئیچ چند دستگاه فایروال بر روی GNS3 فعال کنید می‌توانید تیک گزینه‌ی مورد نظر را بزنید تا یک کپی از این ماشین ایجاد شود.

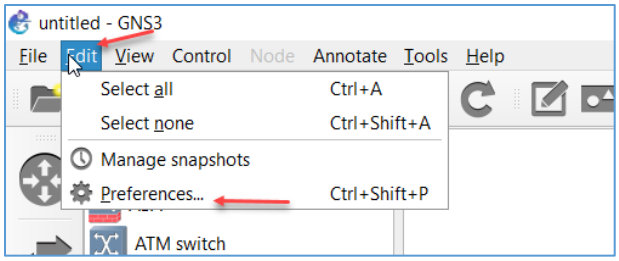


در نرم‌افزار GNS3 وارد قسمت Browse End Devices شوید و فایروال مورد نظر را به لیست اضافه کنید، توجه داشته باشید از همین فایروال می‌توانید چند تا دیگه هم در صفحه قرار دهید.

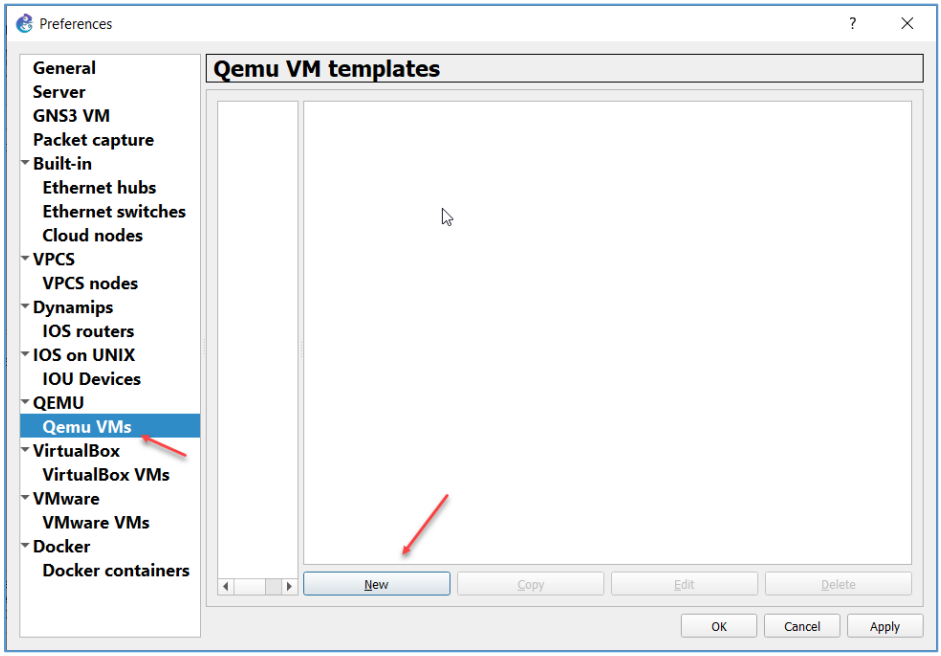
روش دوم:

در روش دوم که روش راحت‌تر و قابل اعتمادتری است استفاده از فایل qcow2 که می‌توانید از لینک زیر آن را دانلود کنید:

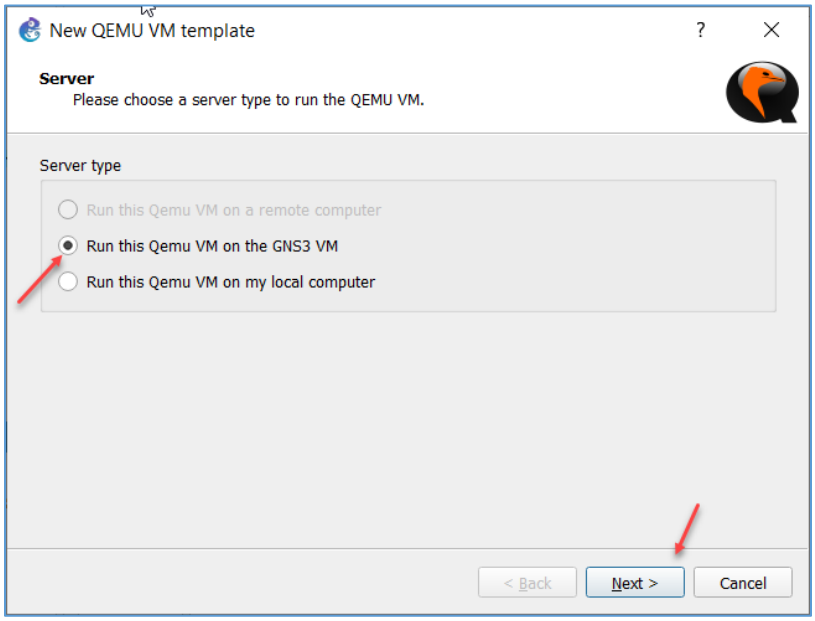
http://dl1.technet24.ir/Downloads/Cisco/ASA/asav9-12-2-4.qcow2



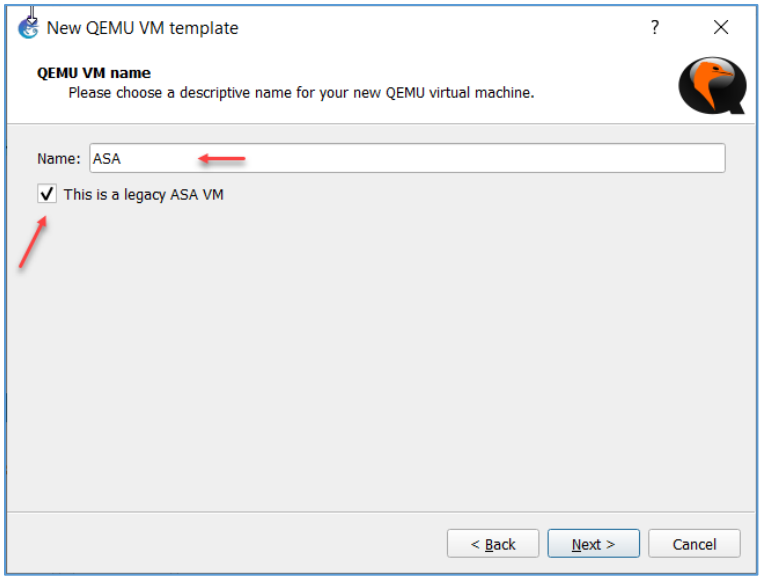
بعد از دانلود فایل مورد نظر وارد نرم‌افزار GNS3 شوید و از منوی Edit بر روی گزینه‌ی Prefrences کلیک کنید.



در این صفحه برای اضافه کردن فایل ASA به نرم‌افزار GNS3 باید بر روی New کلیک کنید.

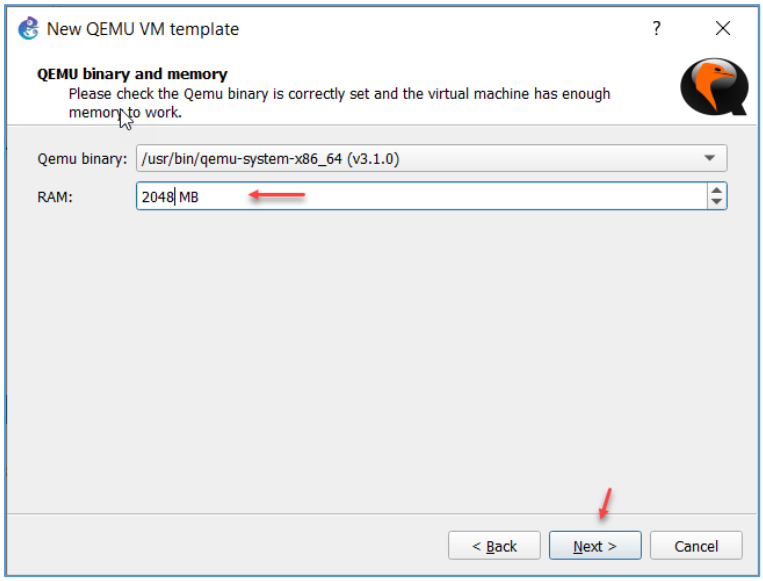


در این صفحه گزینه‌ی Run this Qemu vm on the GNS3 VM را انتخاب کنید تا فایل ASA بر روی ماشین GNS3 آپلود شود.

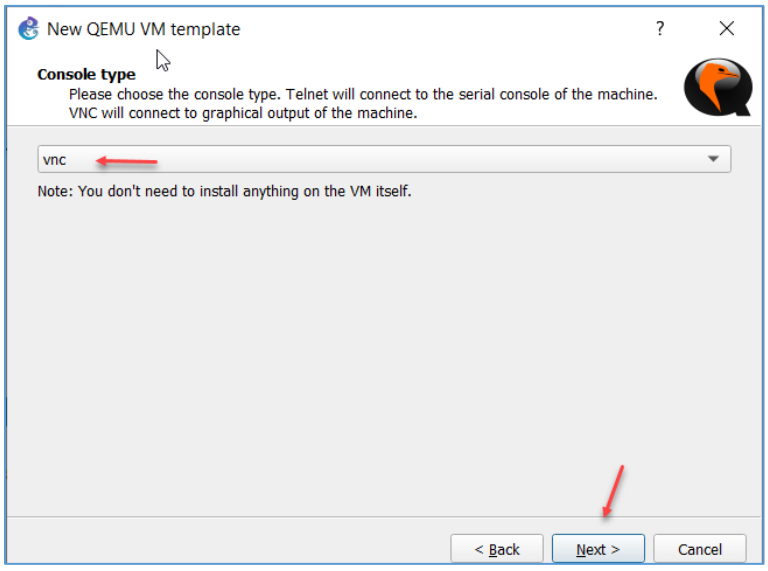


یک نام برای فایروال خود در نظر بگیرید و تیک گزینه‌ی مورد نظر را هم انتخاب کنید، با این کار تنظیمات اضافه‌تری را در ادامه کار مشاهده خواهید کرد.

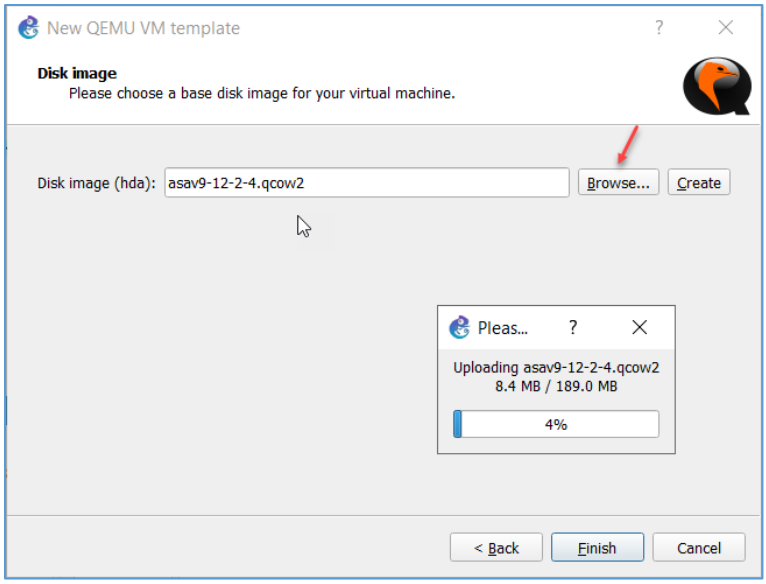
تذکر: اگر از ویندوز۱۰ یا ویندوز سرور ۲۰۱۹ استفاده می‌کنید نیاز به انتخاب این تیک نیست.



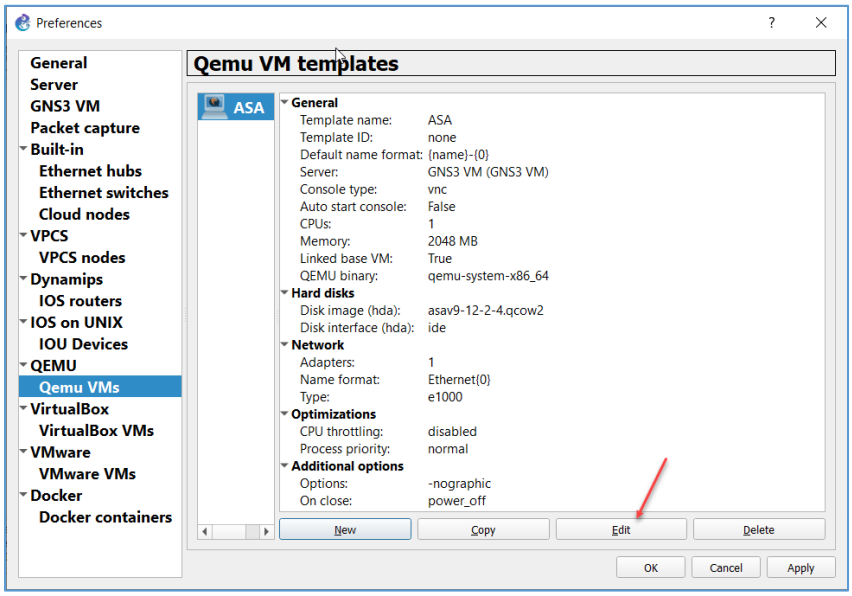
مقدار رم مربوط به این دستگاه را مشخص کنید که بهتر است که حداقل ۲ گیگابایت باشد.



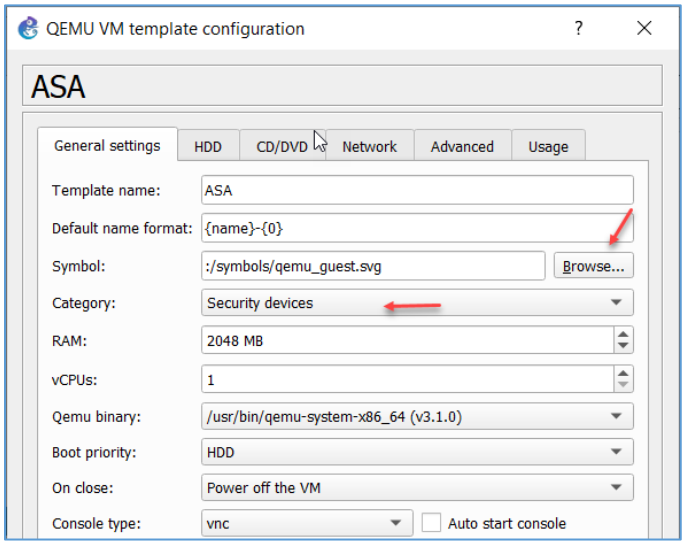
در این قسمت گزینه‌ی VNC را انتخاب کنید، توجه داشته باشید به صورت پیش‌فرض گزینه‌ی Telnet برای آن فعال نشده است و باید بعد از اجرا شدن فایروال آن را فعال کنید.



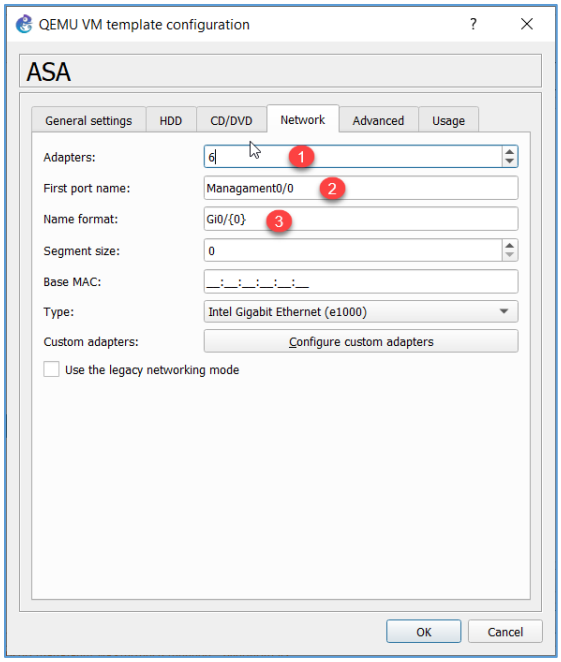
در این صفحه باید بر روی Browse کلیک کنید و فایل دانلود شده مربوط به ASA که با پسوند qcow2 است را انتخاب کنید تا مانند شکل روبرو آپلود انجام شود.



بعد از ایجاد فایروال ASA بر روی Edit کلیک کنید.

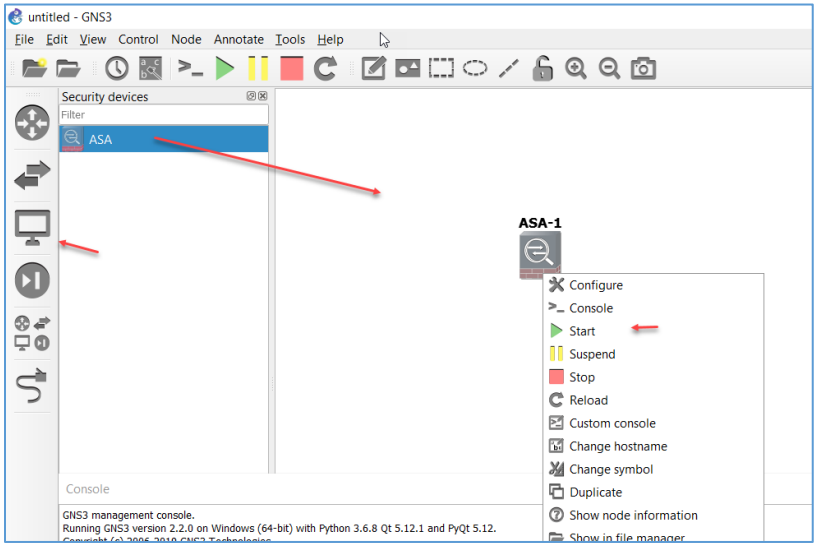


در تب General از قسمت Symbol بر روی Browse کلیک کنید و آیکون مربوط به ASA را از لیست اول انتخاب کنید و از قسمت Category هم گزینه‌ی Secuirty Devices را انتخاب کنید.

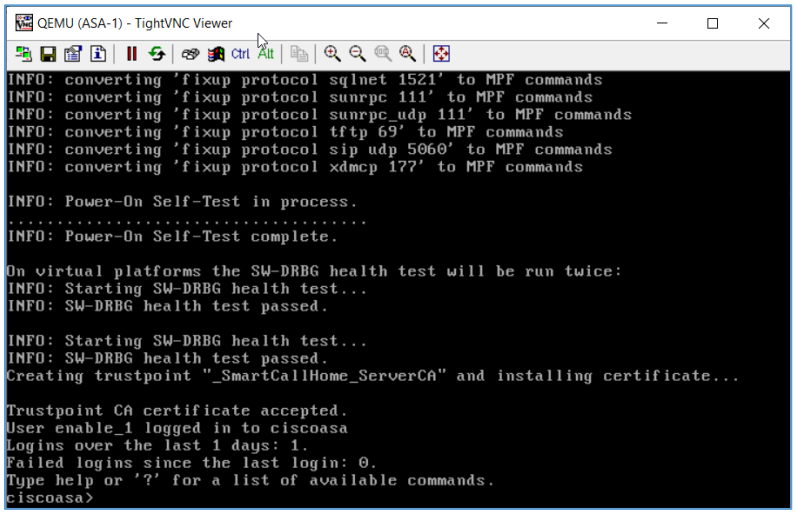


در تب Network و در قسمت Adapters عدد ۶ را وارد کنید تا ۶ کارت شبکه برای این دستگاه در نظر گرفته شود، در قسمت First Port Name نام Management0/0 را وارد کنید که اولین پورت در ASA است، در قسمت Name format نام G0/{0} را وارد کنید تا ۵ پورت بعدی هم با نام گیگابایت اسم گذاری شوند.

تذکر: اگر این قسمت را به درستی تنظیم نکنید ASA به خوبی اجرا نخواهد شد.



در این قسمت بعد از ایجاد ASA از قسمت Security Devices آیکون ASA را کشیده و در صفحه رها کنید بر روی آن کلیک راست کنید و گزینه‌ی Start را کلیک کنید تا فایروال ASA روشن شود، اگر بر روی آن دو بار کلیک کنید کنسول VNC باز خواهد شد.



همانطور که در شکل روبرو مشاهده می‌کنید فایروال ASA به صورت کامل اجرا شده.

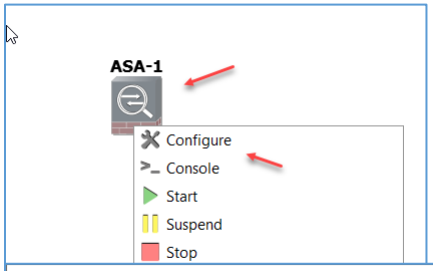
تذکر: توجه داشته باشید در بعضی مواقع فایروال یک بار اجرا و بعد Restart می‌شود و دوباره شروع به بوت می‌کند که مشکلی خاصی نیست.

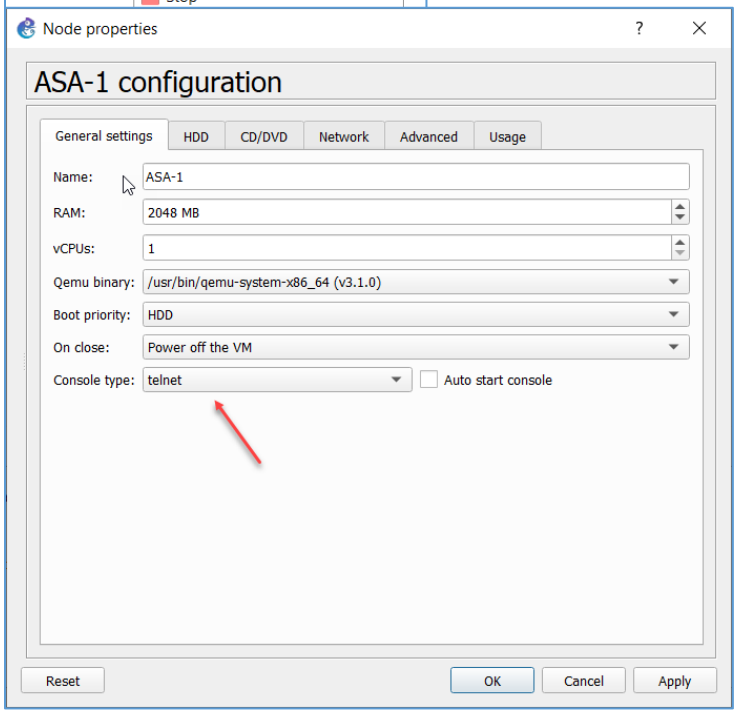
فعال کردن Telnet در ASA

برای اینکه دسترسی راحت‌تری به ASA داشته باشید بهتر است که قابلیت Telnet را برای آن فعال کنید تا بتوانید با نرم‌افزارهای دیگر مانند Putty یا SecurCRT آن را باز کنید، برای این کار ASA را از طریق کنسول VNC فعال کنید و دستورات زیر را اجرا کنید:

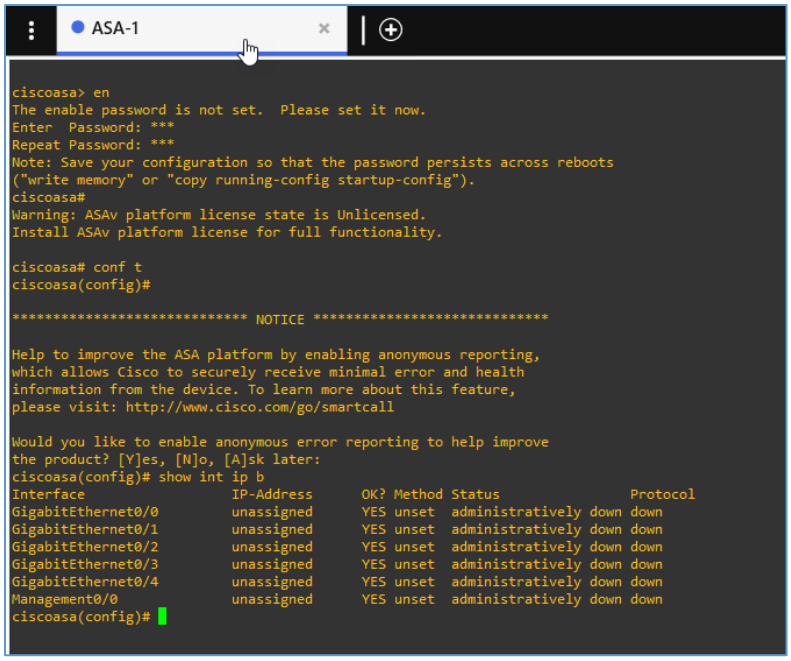
```
ciscoasa#conf t
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

بعد از دستور آخر دو بار بر روی Enter فشار دهید تا تنظیات اعمال شود، بعد از انجام تنظیمات بالا یک بار فایروال را خاموش و بر روی آن کلیک راست کنید و گزینه‌ی Configure را انتخاب کنید.





در این صفحه از قسمت Console type گزینه‌ی Telnet را انتخاب و بر روی OK کلیک کنید و بعد از آن فایروال را روشن کنید، اگر کنسول آن را اجرا کنید با نرم‌افزار Telnet که در GNS3 تنظیم کردید باز خواهد شد.



همانطور که در شکل روبرو مشاهده می‌کنید فایروال روشن شده است؛ برای اینکه وارد مد Privilage شوید از دستور Enable یا اختصار en استفاده می‌کنیم که بعد از آن از شما رمز عبور جدید درخواست می‌شود که آن را وارد و با فشار Enter می‌توانید وارد مد Privilage شوید، بعد از وارد شدن به مد مورد نظر با دستور Show Interface IP brief می‌توانید لیست Interfaceهایی که ایجاد کردید را مشاهده کنید.

نصب و راه اندازی ASDM بر روی فایروال

نرم‌افزار ASDM به همراه فایروال ارائه می‌شود و برای تنظیم و ایجاد سیاست‌های سازمانی به صورت گرافیکی کاربرد دارد یعنی با نصب آن دیگر نیازی به وارد کردن اطلاعات به صورت Command نیست، البته همه دستورات را پشتیبانی نمی‌کند و در بعضی مواقع باید به صورت Command تنظیمات را انجام دهید.

برای شروع، اول باید بر روی Firewall آدرس IP را به صورت دستی و یا اتوماتیک تنظیم کنیم، در دستور زیر وارد Interface Managemet 0/0 می‌شویم و آدرس آن را 192.168.5.28 در نظر می‌گیریم.

```
ciscoasa(config)# int management 0/0
ciscoasa(config-if)# ip address 192.168.5.28 255.255.255.0
ciscoasa(config-if)# nameif mgmt
INFO: Security level for "mgmt" set to 0 by default.
ciscoasa(config-if)# no sh
```

بعد از وارد کردن IP حتماً باید برای هر Interface یک نام در در نظر بگیریم که این کار را با دستور Nameif انجام می‌دهیم که mgmt همان نام اینترفیس است که در ادامه در مورد نام اینترفیس بیشتر توضیح خواهیم داد، در آخر هم باید اینترفیس مورد نظر را با دستور No shutdown روشن کنید.

در ادامه باید نرم‌افزار ASDM را اجرا کنیم برای این کار اول باید پروتکل HTTP را بر روی سرور فعال کنیم که برای این منظور از دستور زیر استفاده می‌کنیم:

با دستور زیر سرویس HTTP فعال خواهد شد

```
ciscoasa(config)# http server enable
```

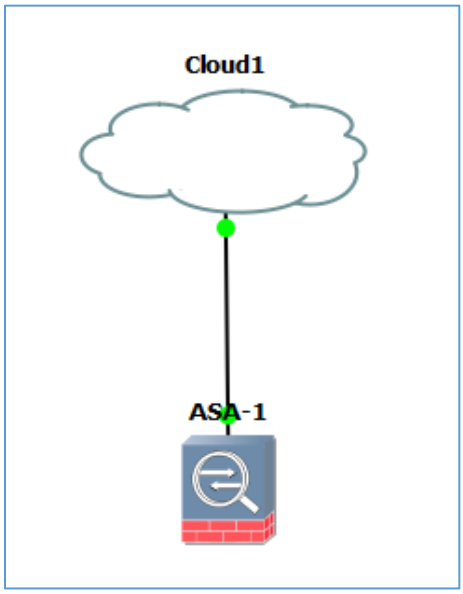
با این دستور به فایروال اعلام می‌کنیم که شبکه ۱۹۲.۱۶۸.۵.۰ می‌تواند به سرویس HTTP دسترسی داشته باشد.

```
ciscoasa(config)# http 192.168.5.0 255.255.255.0 mgmt
```

برای اینکه دسترسی کامل شود باید پروتکل SSL را بر روی فایروال با دستور زیر فعال کنیم، در این دستور برای امنیت بیتشر از رمزنگاری‌ها و هش‌های مختلفی می‌توانید استفاده کنید.

```
ciscoasa(config)# ssl encryption 3des-sha1 rc4-md5 aes256-sha1
```

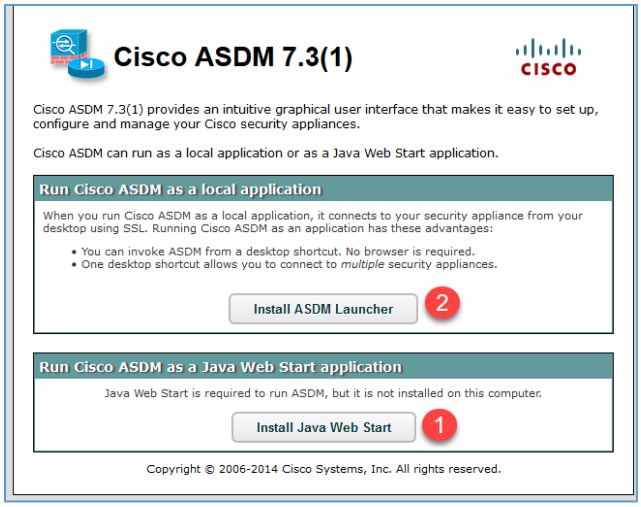
نکته مهم: دستور بالا در نسخه‌های قدیمی تر ASA کاربرد داشته و در نسخه جدید نیازی به استفاده از این دستور نیست.



توجه داشته باشید برای دسترسی به ASA از طریق شبکه باید یک Cloud به صفحه اضافه کنید و آن را به ASA متصل کنید، فقط توجه داشته باشید که کارت شبکه آن را به درستی انتخاب کنید.

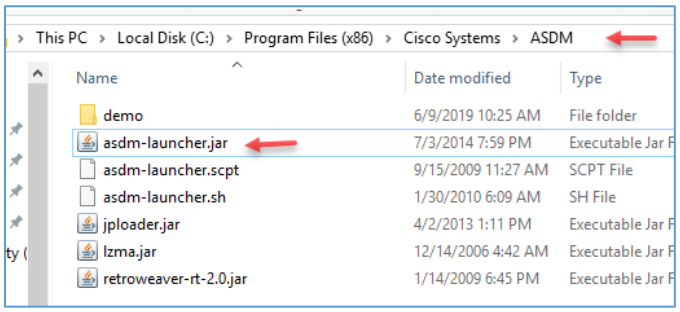
در ادامه وارد مرورگر خود شوید و آدرس زیر را اجرا کنید.

https://192.168.5.28/

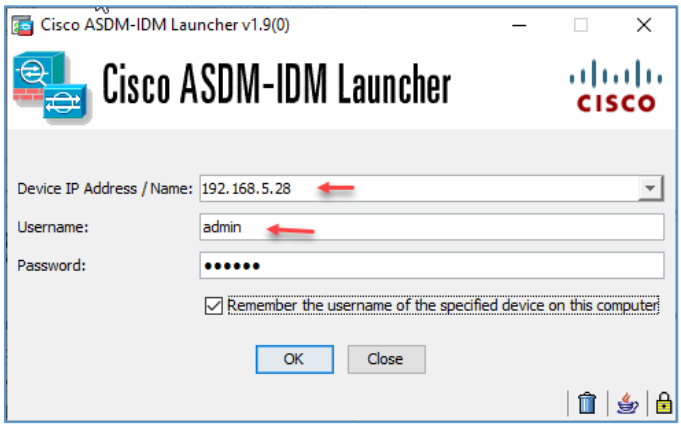


بعد از اجرا کردن آدرس بالا صفحه‌ی روبرو ظاهر می‌شود که برای شروع کار اول باید گزینه‌ی دوم یعنی جاوا را از سایتش دانلود و نصب کنید، ورژنی که در این کتاب استفاده شده و با این فایروال ASA همخوانی داشته ورژن Java Runtime Enviroment 8 Update 74 (64-bit) بوده که بدون مشکل اجرا شد، بعد از نصب جاوا بر روی شماره‌ی دو کلیک کنید که یک فایل نصبی برای شما دانلود خواهد شد آن را اجرا و نصب کنید و بعد از طریق Desktop یا Start آن را اجرا کنید، اگر در این مسیرها فایل اجرایی را پیدا نکردید می‌توانید وارد آدرس زیر شوید و فایل را اجرا کنید.

C:\Program Files (x86)\Cisco Systems\ASDM

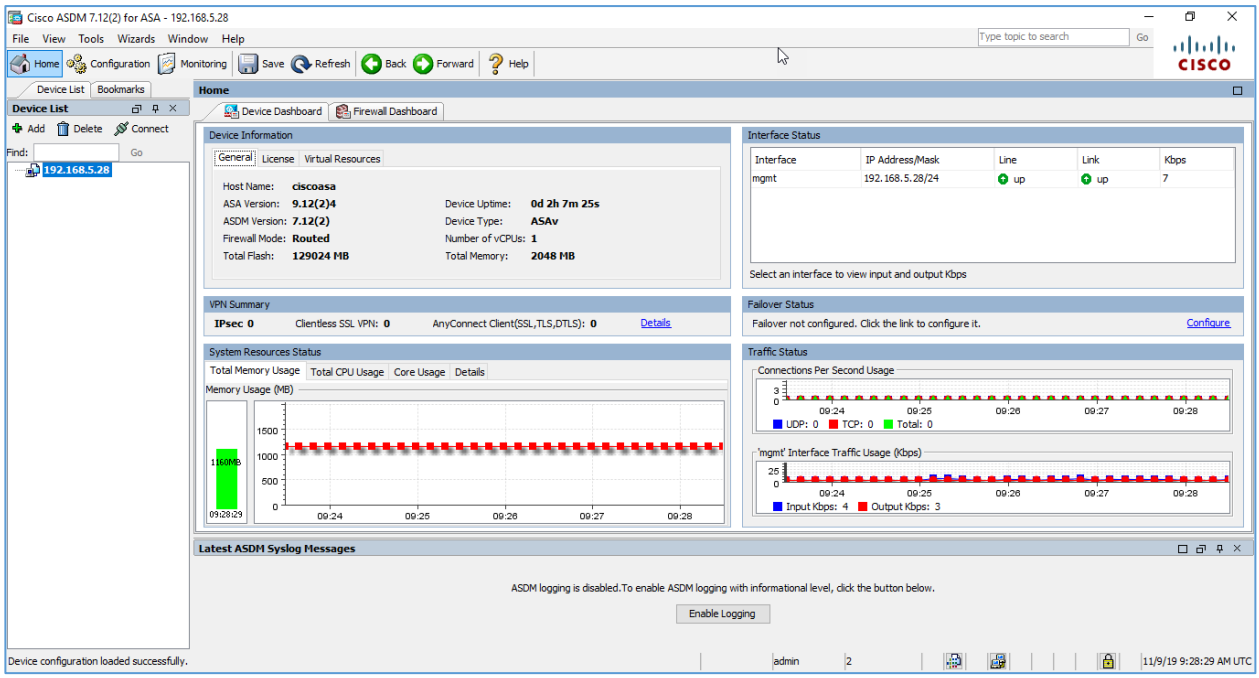


همانطور که در شکل روبرو مشاهده می‌کنید در آدرس مورد نظر فایل asdm-launcher.jar را اجرا کنید.

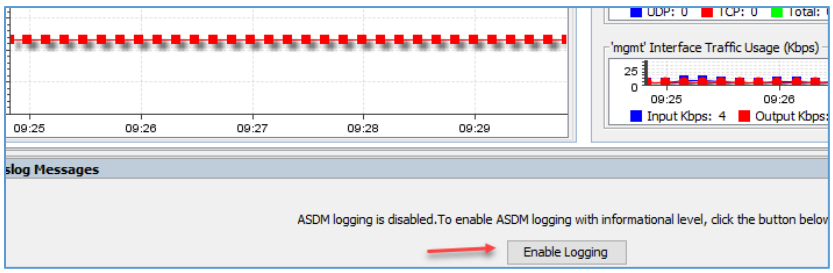


همانطور که مشاهده می‌کنید ASDM-IDM به درستی اجرا شده است که در قسمت اول باید آدرس IP دستگاه ASA را وارد کنید و در ادامه باید یک نام کاربری و رمز عبور در ASA وارد کنید تا بتوانید در این قسمت استفاده کنید.

همانطور که در شکل زیر مشاهده می‌کنید نرم‌افزار ASDM به درستی اجرا شده است، این نرم‌افزار داری بخش‌های مختلفی است، در تب Home داشبوردهای مختلفی را مشاهده می‌کنید، که در قسمت Device Information اطلاعات فایروال مانند نام، ورژن، نوع و ... را مشاهده می‌کنید، در قسمت Interface Status هم Interfaceهای فعال مشخص شده است، همانطور که می‌دانید در حال حاضر فقط یک Interface Management فعال شده است، مقدار مصرف رم و CPU را میتوانید از قسمت System Resources Status مشاهده کنید، گزینه‌هایی دیگری هم وجود دارند که در صورت نیاز بررسی خواهیم کرد.



در اولین قدم باید سرویس logging را فعال کنید که برای این کار به مانند شکل زیر بر روی Enable Logging کلیک کنید.

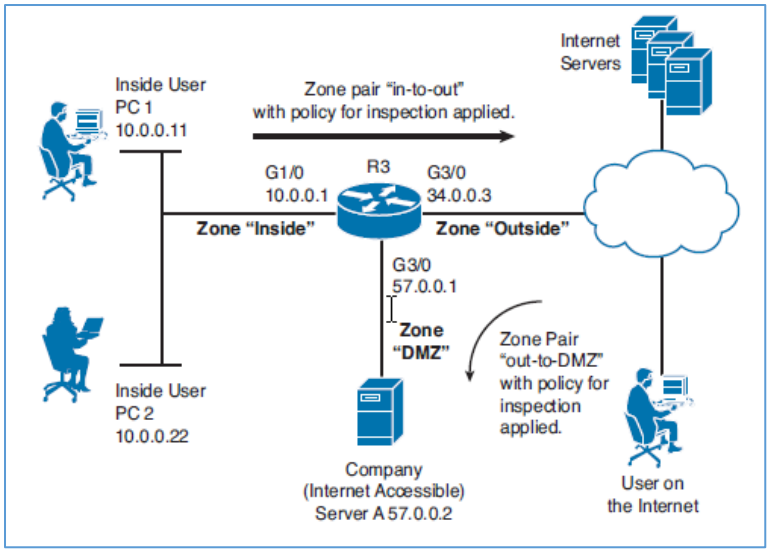


گزینه‌های بسیار دیگری هم وجود دارد که در خلال کار و در ادامه به آنها می‌پردازیم، در حال حاضر باید بخش‌های مهم مربوط به فایروال را با هم بررسی کنیم.

بررسی Zone-Based Firewall یا ZBE

تا به اینجا فایروال را به صورت مجازی نصب و راه‌اندازی کردیم و نرم‌افزار ASDM را هم برای آن به صورت اولیه اجرا کردیم و در ادامه کتاب به صورت کامل آن را بررسی می‌کنیم، برای اینکه با عملکرد فایروال سیسکو بیشتر آشنا شویم بهتر است موضوعاتی را در این قسمت بررسی کنیم.

اصولاً برای کار با فایروال باید منطقه‌های کاری آن را بشناسید، فایروال‌ها به طور معمول از سه منطقه تشکیل شده‌اند که البته می‌توانید نام این مناطق و تعداد آنها را تغییر دهید، در شکل زیر سه منطقه Inside، Outside و DMZ را مشاهده می‌کنید که هر کدام قوانین خاص خودشان را دارند که در زیر بررسی خواهیم کرد.



منطقه Inside :

در این منطقه‌دستگاهایی که قرار دارند می‌توانند بدون مشکل با شبکه خارجی ارتباط برقرار کنند و دسترسی آنها کامل در نظر گرفته می‌شود، هر منطقه در فایروال با عددی با عنوان Security Level مشخص می‌شوند که هر چه این عدد بالاتر باشد دستگاه‌هایی که در این منطقه قرار دارند دسترسی کاملتری به شبکه داخلی و خارجی دارند، اصولاً این عدد برای منطقه داخلی به صورت پیش‌فرض ۱۰۰ در نظر گرفته می‌شود.

نکته اول : به صورت پیش‌فرض ترافیک بین منطقه یا همان Zone مختلف اجازه عبور ندارد و باید برای آنها Policy تعریف شوید که در ادامه انجام خواهیم داد.

نکته دوم : ترافیک در یک منطقه یا Zone را هم می‌شود بررسی کرد .

منطقه DMZ :

در این Zone سرورهایی قرار می‌گیرند که بخواهیم از طریق اینترنت یا شبکه خارجی به آنها دسترسی داشته باشیم، اصولاً Security Level که برای این Zone در نظر گرفته می‌شود عددی بین منطقه Inside و Outside است، این منطقه به این خاطر طراحی شده تا سرورهایی که اهمیت کمتری به نسبت سرورهای دیگر دارند در دسترس کاربران خارجی قرار گیرند و باید تلاش شود در این منطقه هیچ سرور مهمی قرار نگیرد.

منطقه Outside :

در این Zone دسترسی کاملاً محدود شده و باید مدیر شبکه Policy مورد نظر خود را برای دسترسی به شبکه DMZ تعریف کند، توجه داشته باشید که Security Level آن صفر در نظر گرفته می‌شود و به هیچ عنوان نمی‌تواند به شبکه داخلی دسترسی داشته باشد.

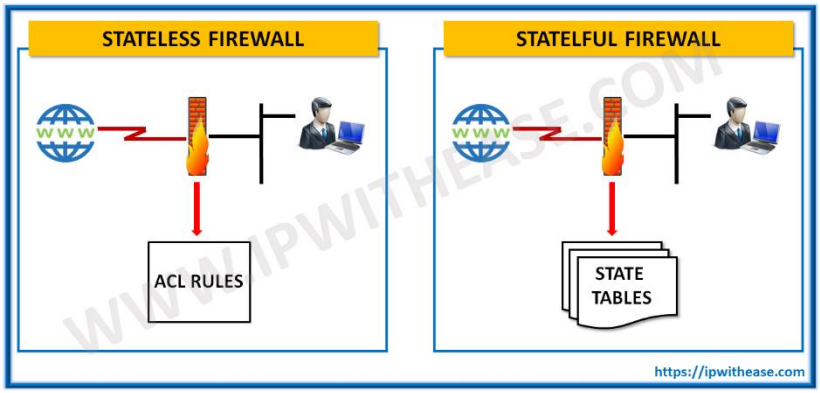
فایروال سیسکو دارای ویژگی‌های زیر است:

- Stateful inspection.
- Application inspection.
- Packet filtering.
- URL filtering.
- Transparent firewall (implementation method).
- Support for virtual routing and forwarding (VRF).
- Botnet traffic filtering
- Advanced malware protection (AMP)
- High availability
- AAA support

ویژگی Stateful inspection

این ویژگی به عنوان dynamic packet filtering هم شناخته می‌شود و برای بررسی پکت‌های عبوری از فایروال کاربرد دارد، این فن‌آوری جایگزین روش قدیمی static packet filtering شده است، در فن‌آوری قدیمی static packet filtering که در لایه ۳ و ٤ مدل OSI کار میکرد، فقط و فقط هدر بسته‌ها بررسی می‌شد که همین کار باعث می‌شد مهاجم با قرار دادن پاسخ در هدر می‌توانست به اطلاعات دست پیدا کند، اما در تکنولوژی Stateful inspection این مشکلات برطرف شده است.

همانطور که گفتیم کاربران خارج از شبکه به هیچ عنوان نمی‌توانند به داخل شبکه در فایروال دسترسی داشته باشند، این مشکل برای کاربرانی که از شبکه داخلی به شبکه خارجی یا همان اینترنت مراجعه می‌کنند وجود دارد که برای حل آن از تکنولوژی Stateful inspection استفاده شده است در این تکنولوژی اطلاعات کاربرانی که می‌خواهند به اینترنت دسترسی داشته باشند مانند پورت مبدا و مقصد به همراه آدرس IP مبدا و مقصد در دیتابیسی با عنوان Stateful ذخیره می‌شوند و فایروال در زمان ورود ترافیک به شبکه داخلی آن را با این دیتابیس مقایسه می‌کند که اگر ترافیک با آن هماهنگی داشت اجازه عبور را می‌دهد که این می‌تواند یک ویژگی عالی فایروال باشد، نکته‌ی مهمی که در رابطه با این تکنولوژی باید بدانیم این است که از حملات مرگبار Dos و Spoofing جلوگیری می‌کند و جلوی ترافیک ناخواسته به شبکه را خواهد گرفت.



فایروال‌های دیگری هم وجود دارد که از روش Stateless پشتیبانی می‌کنند که از سرعت خوبی برخوردار است ولی امنیت آن پائینتر از روش Stateful است.

در زیر تفاوت دو روش را مشاهده می‌کنید که Stateful بسیار قدرتمند است ولی از منابع سخت‌افزاری بیشتری استفاده می‌کند.

Parameters	Stateless	Stateful
Philosophy	Treats each packet in isolation and does not relates to connection state	Stateful firewalls maintain context about active sessions and use "state information" to speed packet processing
Filtering decision	Based on information in packet headers	Based on flows
Memory and CPU intensive	Low	High
Security	Low	High
Connection Status	Unknown	Known
Performance	Fast	Slower
Related terms	Header info, IP address, port no etc.	State information, pattern matching etc.

ویژگی Application inspection

اصولاً این ویژگی از فایروال بر روی لایه‌ی هفتم تمرکز دارد و برای نرم‌افزارهایی کاربرد دارد که از پورت‌های داینامیک برای ارتباط استفاده می‌کنند، در ویژگی قبلی Stateful inspection زیاد نمی‌توانست بر روی پورت‌های داینامیک کار کند و آنها را نمی‌توانست شناسایی کند و به خاطر همین فایروال‌ها از ویژگی Application inspection استفاده می‌کنند تا تمام جزئیات ترافیک شناسایی شود.

ویژگی Packet filtering

در این ویژگی می‌توانیم Access List مختلفی از نوع Standard و یا Extended ایجاد کنیم و در جهت ورودی Inbound و یا Outbound در Interface اعمال کنیم.

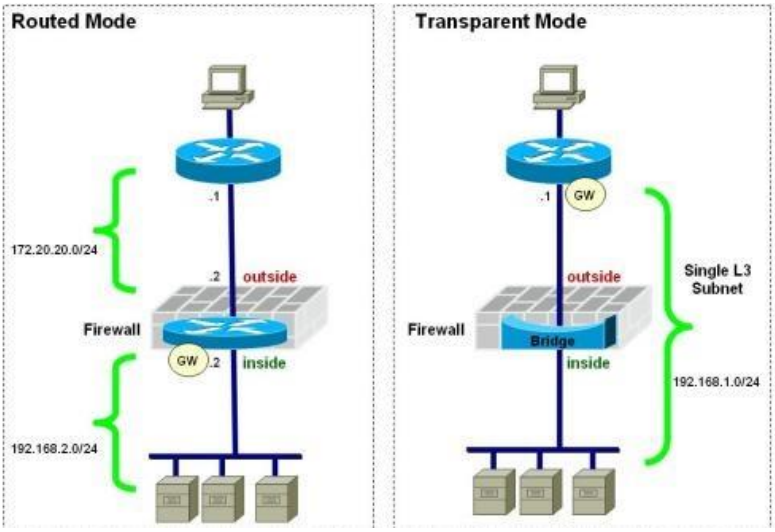
اصولا کلمه Inbound در فایروال به ترافیکی گفته می‌شود که می‌خواهد از Security Level پائینتر به Security Level بالاتر دسترسی داشته باشد مثلاً دسترسی منطقه Outside به DMZ و کلمه‌ی Outbound هم برای دسترسی از شبکه Inside به شبکه Outside یا اینترنت است که Security Level بالاتر به پائینتر می‌شود.

ویژگی URL filtering

در این قابلیت با استفاده از دیتابیس‌های سایت‌های مشخص شده ترافیک مربوط به URL را بررسی کنیم و به آنها اجازه عبور بدهیم و یا جلوی آنها را بگیرم، البته می‌توانیم فقط از آنها Log تهیه کنیم.

ویژگی Transparent firewall (implementation method)

فایروال‌های ASA شرکت سیسکو در دو حالت Transparent و Routed کار می‌کنند.

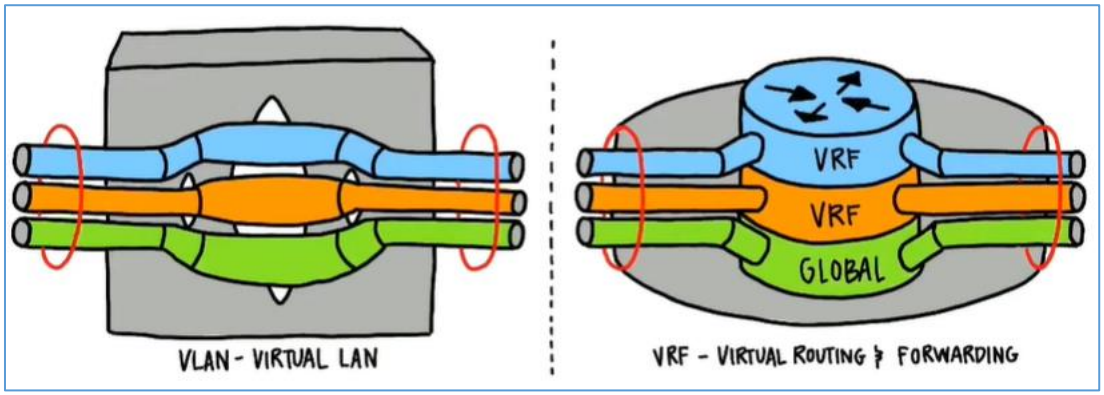


در شکل بالا دو حالت Routed Mode و Transparent Mode را مشاهده می‌کنید که در حالت Routed Mode فایروال به عنوان یک Gateway در بین دو شبکه Inside و Outside قرار می‌گیرد و به عنوان یک فایروال و روتر عمل می‌کند این نوع فایروال در لایه سوم مدل OSI کار می‌کنند، توجه داشته باشید در این حالت باید برای هر یک از Interfaceها یک Subnet جدا تعریف شود و خود فایروال عملیات Routing را بین آنها انجام می‌دهد.

در شکل سمت راست حالت Transparent را که به حالت مخفی هم مشهور است مشاهده می‌کنید در این شبکه به Interfaceهای فایروال IP اختصاص داده نمی‌شود و فقط کابل شبکه به هر دو طرف آن متصل است و یک Subnet در شبکه وجود دارد، این فایروال اصولاً پشت روتر Gateway قرار می‌گیرد و عملیات نظارت بر بسته‌ها را انجام می‌دهد، توجه داشته باشید در این حالت فایروال در لایه دوم و برای عبور ترافیک لایه سوم باید دسترسی لازم را با Access List به فایروال معرفی کنید، توجه داشته باشید برای مدیریت این فایروال باید برای پورت Management آن یک آدرس IP در همان Subnet تعریف کرد.

ویژگی Support for virtual routing and forwarding یا VRF:

این ویژگی برای ایجاد چندین جدول مسیریابی کاربرد دارد و بیشتر در فناوری MPLS به کار می‌رود، با این ویژگی می‌توانید برای هر کاربر یک جدول مسیریابی مختص ایجاد کنید و این جداول با هم ارتباطی نداشته باشند، در شکل زیر و سمت راست، ارتباط VLAN در سوئیچ انجام می‌شود و سمت چپ، ارتباط VRF را که در روتر کارایی دارد، مشاهده می‌کنید، می‌توان گفت VRF نوعی از Vlan است با این تفاوت که در روتر اجرا می‌شود، توجه داشته باشید اگر از VRF بدون استفاده از MPLS استفاده کنیم به آن VRF Lite گفته می‌شود.



ویژگی Access control lists (ACL) are not required as a filtering method to implement the policy

در این ویژگی از فایروال به این نکته اشاره می‌کند که لیست کنترل دسترسی یا همان ACL به عنوان یک روش فیلترینگ مورد نیاز نیست.

فعال‌سازی SSH در ASA

برای اینکه دسترسی آسانتری به فایروال ASA داشته باشیم و تنظیمات خود را بر روی آن انجام دهیم بهتر است سرویس SSH را بر روی آن فعال کنیم که برای این کار به صورت زیر عمل کنید:

با دستور زیر رمز عبور ورود به Privilege مد را فعال می‌کنیم که به صورت پیش‌فرض رمز عبوری بر روی آن قرار گرفته نبود.

```
ciscoasa(config)# enable password 3isco-pass
```

بعد از فعال کردن رمز عبور باید نام کاربری و رمز عبور آن را هم فعال کنید تا بتوانید از طریق سرویس SSH به فایروال ASA متصل شوید، برای این کار از دستور زیر استفاده کنید، توجه کنید که 3isco به عنوان نام کاربری و 3isco-pass به عنوان رمز عبور در نظر گرفته شده است.

```
ciscoasa(config)# username 3isco password 3isco-pass privilege 15
```

دستور بعدی که باید اجرا کنیم ایجاد دسته کلید برای ارتباط است که دستور آن را در زیر مشاهده می‌کنید.

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

بعد از اجرای دستور بالا با اخطار و سوال زیر مواجه می‌شوید که دسته کلید از قبل وجود دارد و آیا می‌خواهید با آن جایگزین کنید که کلمه Yes را وارد کنید.

```
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
```

برای اینکه احراز هویت انجام شود با دستور زیر به ASA اعلام می‌کنیم که احراز هویت را به صورت محلی یا همان Local انجام دهید یعنی با این کار نام کاربری و رمز عبور را که در قسمت قبل تعریف کردید مورد تایید قرار می‌گیرد.

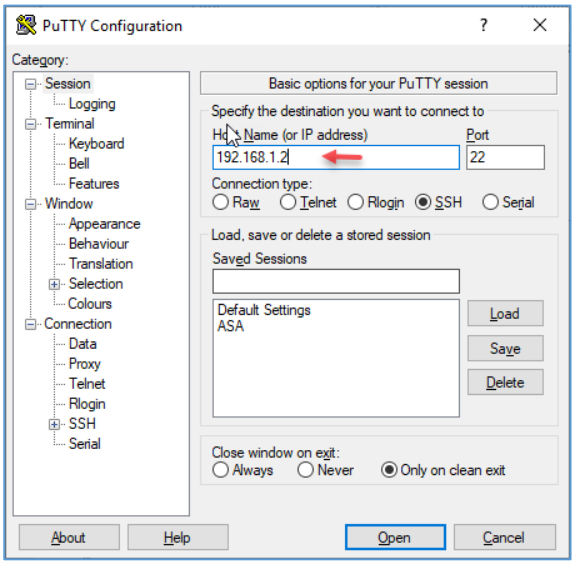
نکته مهم در اجرای دستور زیر این است که کلمه LOCAL را باید به صورت حروف بزرگ بنویسید.

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

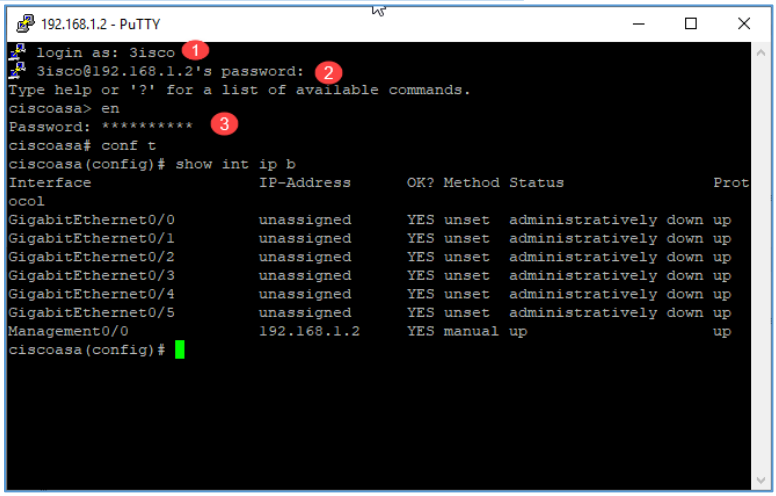
بعد از انجام تمام دستورات بالا باید به ASA بگوییم که SSH را بر روی چه رنج آدرس و اسم پورتی فعال کند، که برای این کار از دستور زیر استفاده می‌کنیم، توجه داشته باشید نام mgmt مربوط به اینترفیس Management است که در قسمت قبل بر روی آن آدرس تعریف کردیم.

```
ciscoasa(config)# ssh 192.168.1.0 255.255.255.0 mgmt
```

تا به اینجا سرویس SSH را بر روی فایروال فعال کردیم و حالا می‌توانیم با نرم‌افزارهای مختلف مانند Putty یا Secure CRT به فایروال متصل شویم.



نرم‌افزار Putty را از اینجا دانلود و اجرا کنید و به مانند شکل روبرو گزینه‌ی SSH را انتخاب و آدرس سرور ASA را وارد کنید و بر روی Open کلیک کنید، بعد از این کار از شما سوال خواهد شد که آیا دسته کلید مورد تایید است که باید بر روی Yes کلیک کنید.



همانطور که مشاهده می‌کنید، برای ورود نام کاربری درخواست شده که در قسمت اول وارد می‌کنیم و در قسمت دوم رمز عبور مربوط به آن را و بعد از آن برای ورود به مد privilege باید از دستور Enable استفاده کنید و بعد از آن هم باید رمز عبوری را که با دستور Enable Password فعال کردید را وارد کنید.

حالا می‌توانیم بدون ورود به ماشین مجازی و فقط با استفاده از سرویس SSH فایروال ASA را مدیریت کنیم.

نکته: به صورت پیش‌فرض مقدار زمان پایدار بودن ارتباط یک دقیقه می‌باشد و اگر در این یک دقیقه با فایروال کار نکنید ارتباط شما قطع خواهد شد که برای رفع این مشکل باید دستور زیر را در فایروال اجرا کنید:

اگر بعد از دستور ssh timeout علامت سوال قرار دهید مشاهده خواهید کرد که این عدد می‌تواند بین ۱ تا ۶۰ دقیقه متغیر باشد که در اینجا مقدار ۱۵ دقیقه ثبت شده است.

```
ciscoasa(config)# ssh timeout ?
configure mode commands/options:
  <1-60>  Idle time in minutes after which a ssh session will be closed
ciscoasa(config)# ssh timeout 15
```

اجرای C3PL در روتر سیسکو

در سیسکو مفهومی با نام ZBPFW داریم که برای اجرای سیاست‌ها در دستگاه‌های سیسکو کاربرد دارد، از طریق این ویژگی، پورت‌های مختلف فایروال به Security Zoneهای مختلی تقسیم می‌شود که در قسمت قبل آن را بررسی کردیم. سیسکو برای اجرا کردن سیاست‌های خود از زبانی به نام C3PL یا همان Cisco Common Classification Policy Language استفاده می‌کند در این زبان سه موضوع در هر اجرا مورد بررسی قرار می‌گیرد که عبارت‌اند از:

Class maps: برای شناسایی ترافیک عبوری در دستگاه‌های سیسکو مورد استفاده قرار می‌گیرد، برای اینکه ترافیک در جریان را کنترل کنید یک سری سیاست‌ها در قالب Class MAP تعریف می‌کنید و این ترافیک را که در ادامه با یک مثال بررسی خواهیم کرد کنترل می‌کنید، اصولاً Class MAP ترافیک‌های زیر را مورد بررسی قرار می‌دهد.:

- ترافیک‌هایی که بین لایه سه و چهار مدل OSI جریان دارند، مانند ترافیک IP مقصد و مبدا، ترافیک پورت‌های دستگاه مورد نظر و ترافیک پورت‌های مدیریتی.
- ترافیک‌هایی که در لایه‌ی هفتم از مدل OSI کاربرد دارند مانند: کوکی‌های پروتکل HTTP، آدرس‌های HTTP، عنوان و محتوای پروتکل HTTP یا دستورات پروتکل FTP.

Policy MAP: در این قسمت Class Map مورد نظر شناسایی شده و اکشن مورد نظر طبق آن اجرا می‌شود، در کل Policy MAP دارای چهار اکشن به صورت زیر است:

نام اکشن	توضیحات	کاربرد
Inspect	مجاز برای بررسی ترافیک	برای ترافیک کاربران که از داخل به بیروت از فایروال ارتباط برقرار می‌کنند کاربرد دارد.
Pass	اجازه عبور ترافیک را می‌دهد	این نوع ترافیک زمانی که از شبکه خارج می‌شوند دیگر به شبکه داخلی وارد نمی‌شوند و به خاطر همین ترافیک آن بررسی نخواهد شد.
Drop	اجازه عبور ترافیک را نمی‌دهد.	این گزینه اجازه عبور هیچ ترافیکی را بین Zone های مختلف را نمی‌دهد.
Log	Log گیری از بسته‌ها	اگر بخواهید از اطلاعات بسته‌ها، Pass، Drop اطلاعات بدست آورید باید این گزینه را فعال کنید.

Service Policy : در این قسمت مشخص می‌کنیم که Policy MAP در چه جایی یا اینترفیسی اجرا شود.

برای اینکه بیشتر با این مبحث آشنا شویم یک مثال را با هم بررسی می‌کنیم.

Zone Based Firewall در نسخه IOS ۱۲.٦ کارایی دارد و به عنوان جایگزینی برای Context-Based Access Control یا همان CBAC معرفی شد.

Zone Based Firewall از ویژگی Stateful inspection و Application inspection در لایه ۳ (Network Layer) تا لایه ۷ (Application Layer) پشتیبانی می‌کند.

همانطور که گفتیم فایروال مبتنی بر منطقه یا همان ZBFW یک فایروال Statful است و این بدان معنا است که هر چیزی که از فایروال خارج شود آن را به خاطر می‌سپارد و در برگشت اجازه ورود می‌دهد، در مورد این موضوع در قسمت‌های قبل به طور کامل صحبت کردیم.

یک نکته مهم در استفاده از ZBFW این است که اگر شرکتی‌توانایی خرید فایروال ASA را نداشته باشد با این فایروال که در داخل روتر فعال می‌شود می‌توانید جایگزین آن کنید با توجه به این نکته که روتر باید از سری ISR یا Integrated Services Routers باشد مانند سری 3900 و 2900 .

مراحل پیکربندی فایروال مبتنی بر Zone Based Firewall :

۱- ایجاد منطقه امنیتی

۲- عضو کردن Interface مورد نظر در منطقه مشخص شده.

۳- ایجاد Policy

۴- ایجاد Zone Pair

۵- اعمال کردن Policy بر روی Zone pair .

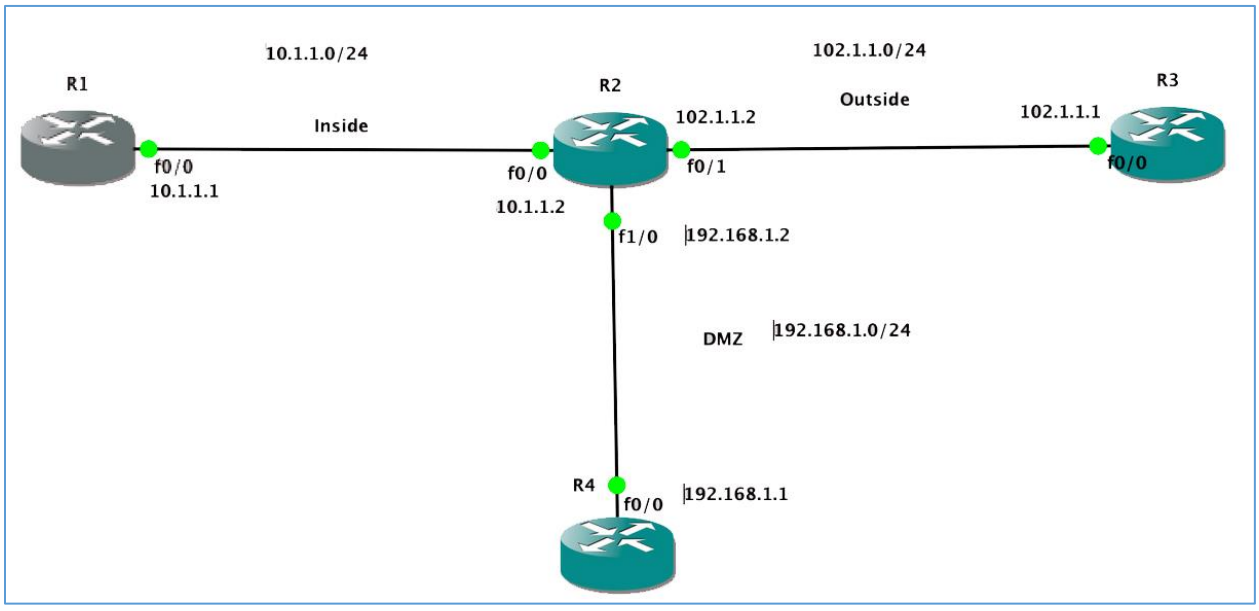
توپولوژی شبکه:

در زیر یک مثال را در GNS3 با هم بررسی می‌کنیم، در این مثال چهار روتر را مشاهده می‌کنید که R2 به عنوان ZBF عمل می‌کند و دارای سه منطقه Inside, Outside, DMZ است.

کاری که می‌خواهیم در این سناریو انجام دهیم این است که:

۱- از طریق R1 که در منطقه Inside قرار دارد بتوانیم، پروتکل TCP, UDP, ICMP برای دسترسی به منطقه Outside که روتر R3 قرار دارد فعال کنیم.

۲- از طریق روتر R1 که در منطقه Inside قرار دارد بتوانیم از طریق پروتکل HTTP , Telnet به منطقه DMZ دسترسی پیدا کنیم.



دستورات روتر R1 :

در دستور زیر وارد Interface f0/0 می‌شویم، و آدرس روتر R1 را وارد و پورت را روشن می‌کنیم، بعد از آن با دستور IP Route مشخص می‌کنیم که هر شبکه‌ای را که روتر R1 نمی‌داند به روتر R2 ارسال کند.

```
R1(config)#int f0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

دستورات روتر R2 :

وارد پورت F0/0 شوید و آدرس IP مورد نظر را که با روتر R1 در ارتباط است را وارد و بعد از آن پورت را روشن کنید.

```
R2(config)#int f0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
```

در ادامه وارد پورت F0/1 شوید و آدرس مورد نظر را وارد کنید، این پورت با روتر R3 در ارتباط است.

```
R2(config)#int f0/1
R2(config-if)#ip add 102.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
```

وارد پورت F1/0 شوید و IP مورد نظر را که به سمت روتر R4 است را وارد و پورت را روشن کنید.

```
R2(config)#int f1/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
```

دستورات روتر R3 :

در این روتر وارد پورت F0/0 شوید ور آدرس IP را وارد و پورت را روشن کنید.

R3(config)#**int f0/0**
R3(config-if)#**ip address 102.1.1.1 255.255.255.0**
R3(config-if)#**no shut**
R3(config-if)#**exit**

در ادامه یک IP Route به سمت روتر R2 بنویسید تا شبکه‌ای که روتر R3 نمی‌شناسد به سمت روتر R2 فرستاده شود.

R3(config)#**ip route 0.0.0.0 0.0.0.0 102.1.1.2**
R3(config)#**exit**

دستورات روتر R4 :

وارد پورت F0/0 شوید و آدرس IP را که در رنج پورت F1/0 روتر R2 است را وارد و پورت را روشن کنید.

R4(config)#**int f0/0**
R4(config-if)#**ip address 192.168.1.1 255.255.255.0**
R4(config-if)#**no shut**
R4(config-if)#**exit**

در ادامه یک IP Route به سمت روتر R2 بنویسید تا شبکه‌ای که روتر R4 نمی‌شناسد به سمت روتر R2 فرستاده شود.

R4(config)#**ip route 0.0.0.0 0.0.0.0 192.168.1.2**
R4(config)#**exit**

برای اینکه مطمئن شویم روترها با هم در ارتباط هستند بهتر است از دستور Ping برای تست ارتباط استفاده کنیم.

Ping روتر R1 با روتر R3

R1#**ping 102.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 102.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms

Ping روتر R2 با روتر R4

R2#**ping 192.168.1.1**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/22/32 ms

Ping روتر R3 با روتر R1

R3#**ping 10.1.1.1**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/44 ms
R3#

Ping روتر R4 با روتر R1 و R3

R4#**ping 10.1.1.1**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/38/44 ms

R4#**ping 102.1.1.1**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/28/40 ms
خوب تا به اینجا به روترها آدرس IP دادیم و ارتباط آنها را هم تست کردیم در ادامه باید Security Zone ایجاد کنیم و Interfaceها را داخل آن قرار دهیم.

ایجاد Security Zone

در زیر سه منطقه Inside, Outside, DMZ را در روتر R2 که روتر اصلی است ایجاد می‌کنیم.

R2(config)#**zone security inside**
R2(config-sec-zone)#**exit**

```
R2(config)#zone security outside
R2(config-sec-zone)#exit

R2(config)#zone security dmz
R2(config-sec-zone)#exit
```

عضو کردن Interface در Security Zone مورد نظر

در این قسمت وارد پورت F0/0 شوید و آن را در منطقه Inside قرار دهید.

```
R2(config)#interface f0/0
R2(config-if)#zone-member security inside
R2(config-if)#exit
```

وارد پورت F0/1 شوید و آن را عضو منطقه‌ی Outside کنید.

```
R2(config)#int f0/1
R2(config-if)#zone-member security outside
R2(config-if)#exit
```

وارد پورت F1/0 شوید و آن را عضو منطقه‌ی DMZ کنید.

```
R2(config)#int f1/0
R2(config-if)#zone-member security dmz
R2(config-if)#exit
```

بعد از انجام مراحل بالا حالا باید سیاست‌های خود را در این مناطق اعمال کنیم.

اجرای سناریو اول

ایجاد Class MAP

در مرحله اول با دستور class-map یگ گروه با نام cmap1 ایجاد می‌کنیم:

```
R2(config)#class-map type inspect match-any cmap1
```

بعد از آن با دستور Match سه پروتکل TCP, UDP, ICMP را به این گروه اضافه می‌کنیم:

```
R2(config-cmap)#match protocol tcp
R2(config-cmap)#match protocol udp
R2(config-cmap)#match protocol icmp
R2(config-cmap)#exit
```

ایجاد Policy MAP

با دستور policy-map یک گروه با نام pmap1 ایجاد می‌کنیم:

R2(config)#**policy-map type inspect pmap1**

بعد از این کار باید داخل Policy Map که در بالا ایجاد کردید Class Map را صدا بزنید:

توجه داشته باشید، دستور زیر داخل policy-map در حال اجرا است.

R2(config-pmap)#**class type inspect cmap1**
R2(config-pmap-c)#**inspect**
R2(config-pmap-c)#**exit**
R2(config-pmap)#**exit**

ایجاد Zone Pair

با این دستور یک گروه با نام Int_out ایجاد می‌کنیم و اجازه دسترسی شبکه Inside را به شبکه Outside می‌دهیم.

R2(config)#**zone-pair security in_out source inside destination outside**

بعد از این که Zone Pair را در مرحله قبل ایجاد کردید وارد آن می‌شویم و دستور زیر را برای ارتباط دادن Policy Map به Zone Pair استفاده می‌کنیم:

R2(config-sec-zone-pair)#**service-policy type inspect pmap1**
R2(config-sec-zone-pair)#**exit**
R2(config)#**exit**

با انجام سناریو اول حالا می‌توانید از روتر R1 روتر R3 را ping کنید چون به پروتکل ICMP اجازه عبور دادیم و همچنین می‌توانید از طریق روتر R1 به روتر R3 یک ارتباط Telnet برقرار کنید.

اجرای سناریو دوم

در سناریو دوم می‌خواهیم در منطقه Inside و Dmz به دو پروتکل Http و Telnet اجازه عبور دهیم به طوری که روتر R1 بتواند از طریق این دو پروتکل به روتر R4 که در منطقه DMZ است متصل شود.

در این قسمت دیگر توضیحات اضافه نمی‌دهیم و فقط دستورات را پشت سر هم اجرا می‌کنیم:

R2(config)#**class-map type inspect match-any cmap2**
R2(config-cmap)#**match protocol telnet**
R2(config-cmap)#**match protocol http**
R2(config-cmap)#**exit**

R2(config)#**policy-map type inspect pmap2**
R2(config-pmap)#**class type inspect cmap2**
R2(config-pmap-c)#**inspect**
R2(config-pmap-c)#**exit**

R2(config)#**zone-pair security in_dmz source inside destination dmz**
R2(config-sec-zone-pair)#**service-policy type inspect pmap2**
R2(config-sec-zone-pair)#**exit**

بعد از وارد کرد دستورات بالا و اجازه دادن به دو پروتکل Http و Telnet حالا باید وارد روتر R4 شوید و Telnet و Http را با دستورات زیر فعال کنید.

R4(config)#**line vty 0 4**
R4(config-line)#**password 3isco**
R4(config-line)#**exit**
R4(config)#**ip http server**

بعد از اینکه دستورات را وارد کردید می‌توانیم ارتباط را تست بگیریم:

R1#**telnet 192.168.1.1**

Trying 192.168.1.1 ... Open

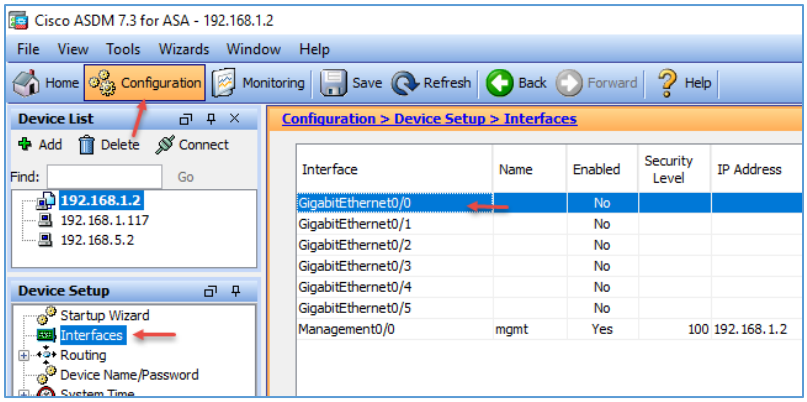
User Access Verification

Password:
R4>en
% No password set
R4>exit

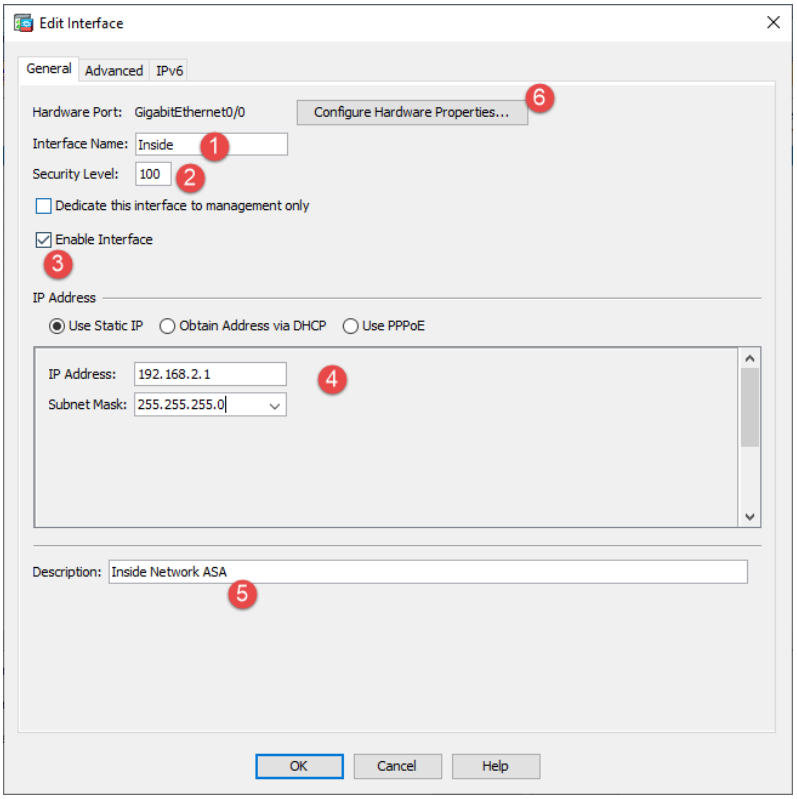
[Connection to 192.168.1.1 closed by foreign host]
R1#

فعال‌سازی سرویس DHCP در ASA

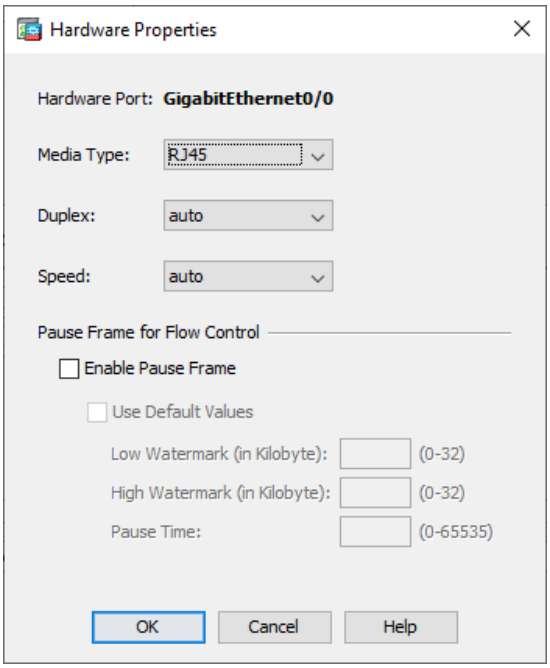
برای شروع کار با فایروال ASA می‌خواهیم سرویس DHCP را روی آن فعال کنیم برای این کار باید اول شبکه داخلی را مشخص کنیم که اصولاً نام پیش‌فرض آن را Inside در نظر می‌گیرند.



برای این که از طریق نرم افزار ASDM به اینترفیس مورد نظر خود آدرس دهیم وارد تب Configuration شوید و از قسمت Device Setup گزینه‌ی Interfaces را انتخاب کنید، در این صفحه همه‌ی Interfaceها برای شما مشخص شده است، اگر توجه کنید Management همان Interface است که از طریق آن به نرم‌افزار ASDM متصل شده‌ایم، برای اینکه سرویس DHCP را فعال کنیم باید آن را بر روی شبکه داخلی خود اجرا کنیم برای همین Interface GigaEthernet0/0 را به عنوان Interface داخلی در نظر میگیریم و به آن آدرس می‌دهیم، برای این کار بر روی آن دو بار کلیک کنید.

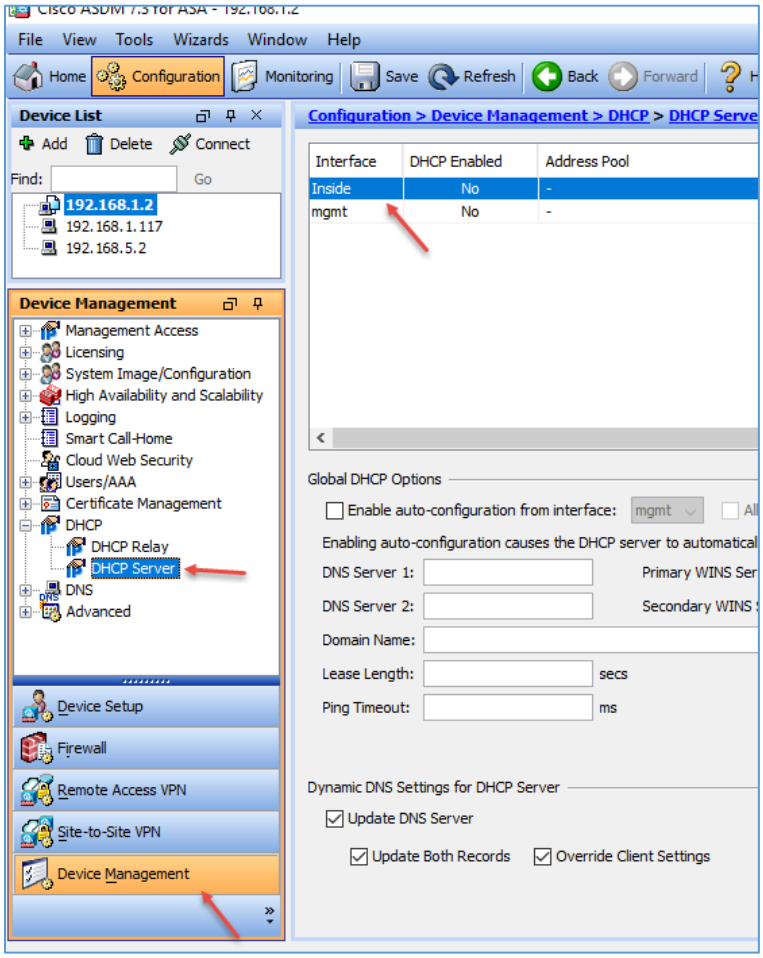


در این صفحه و در قسمت شماره‌ی یک نام Interface را Inside وارد می‌کنیم، در قسمت شماره‌ی دو عدد ۱۰۰ را برای این Interface در نظر می‌گیریم که چون به شبکه داخلی متصل است حداکثر دسترسی را برای آن در نظر می‌گیریم، با انتخاب تیک گزینه‌ی سه این Interface فعال خواهد شد، در قسمت شماره چهار آدرس و در قسمت شماره‌ی پنج توضیحات Interface را وارد کنید.

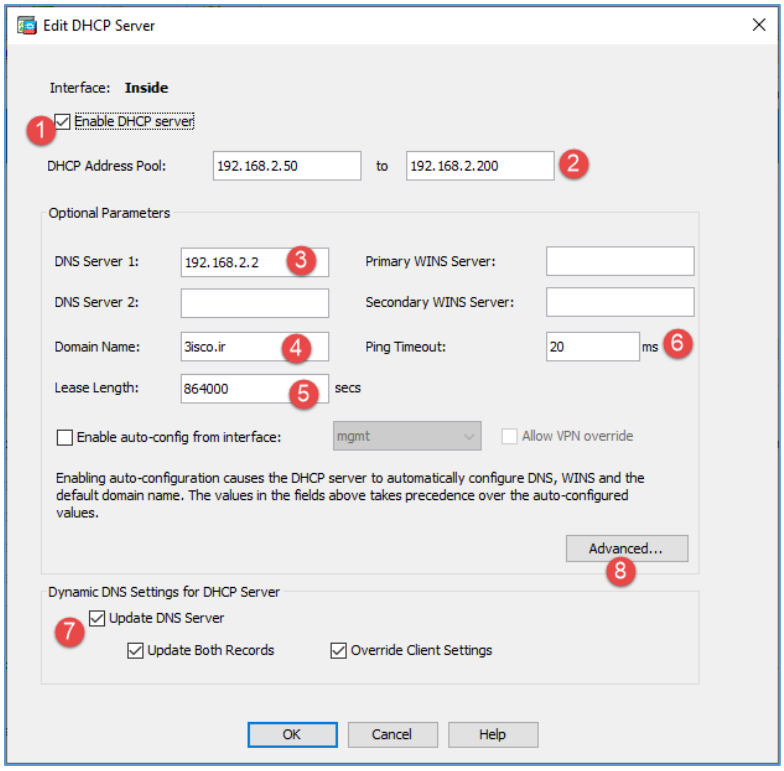


اگر در صفحه قبل بر روی شماره‌ی شش یعنی Configure کلیک کنید صفحه روبرو ظاهر خواهد شد که می‌توانید تنظیمات مربوط سرعت، نوع ارتباط و ... را انجام دهید.

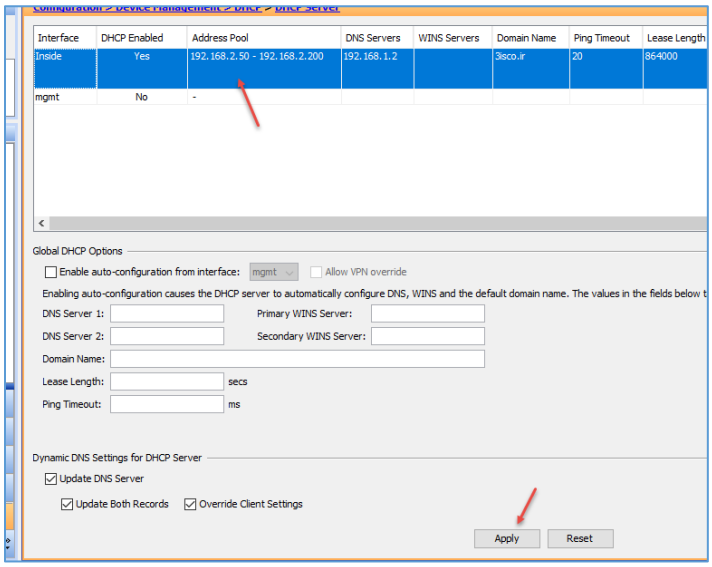
بعد از انجام این تنظیمات بر روی OK کلیک کنید، بعد از اینکه بر روی OK کلیک کنید اطلاعات به سرور ASA ارسال می‌شود و اطلاعات ذخیره خواهند شد.



برای فعال سازی سرویس DHCP از سمت چپ بر روی Device Management کلیک کنید و گزینه‌ی DHCP Server را انتخاب کنید همانطور که در لیست مشاهده می‌کنید دو Interface وجود دارد که قبلاً آنها را ایجاد کردیم، بر روی گزینه‌ی Inside دو بار کلیک کنید.

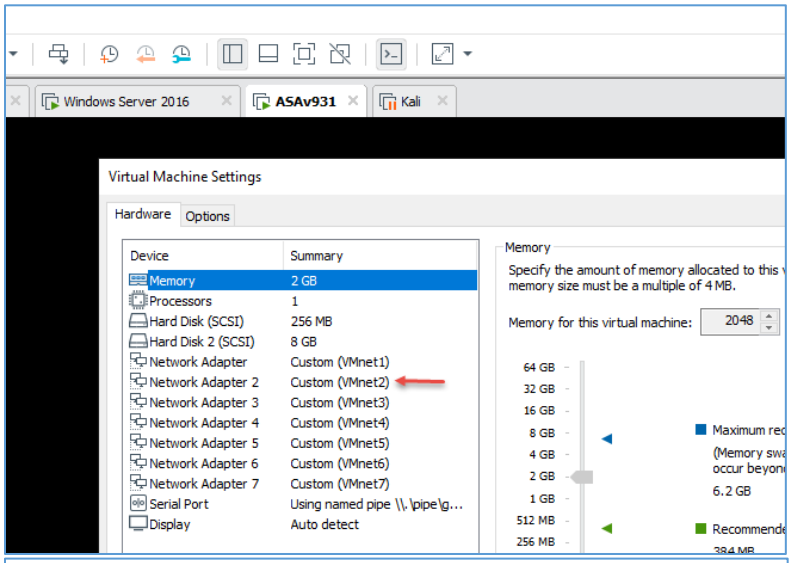


در قسمت شماره‌ی یک با انتخاب تیک گزینه‌ی Enable DHCP Server سرویس DHCP فعال خواهد شد، در قسمت شماره‌ی دو باید رنج IP را برای تخصیص دادن به کلاینت‌ها مشخص کنید، در قسمت شماره‌ی سه می‌توانید سرور DNS خود را وارد کنید، در قسمت شماره‌ی چهار نام دومین شبکه را وارد کنید، در قسمت شماره‌ی پنجم باید مشخص کنید که چند ثانیه کلاینت زمان دارد که آدرس مورد نظر خود را در اختبار داشته باشد در این قسمت ۸٦٤۰۰۰ ثانیه نوشته شده است که برابر ۱۰ روز است و اگر در این ۱۰ روز کلاینت مورد نظر در شبکه فعال نباشد آدرس که به آن تخصیص داده شده از آن پس گرفته خواهد شد، در قسمت شماره‌ی شش مقدار زمان برای ارتباط با کلاینت‌ها مشخص شده است که برابر ۲۰ ثانیه است، در قسمت شماره‌ی هفت با انتخاب تیک مورد نظر رکوردهای DNS در صورت نیاز آپدیت خواهد شد، در قسمت شماره‌ی هشت گزینه‌های مختلفی وجود دارد که مثلاً یکی از این گزینه‌ها انتخاب آدرس Gateway است. بعد از انجام تنظیمات بر روی OK کلیک کنید.

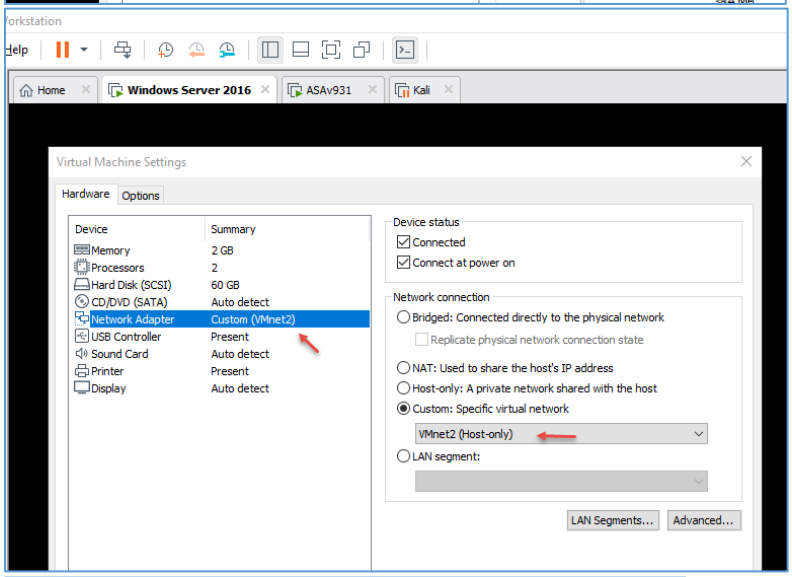


همانطور که مشاهده می‌کنید در قسمت Inside تنظیمات اعمال شده است و برای اینکه بر روی دستگاه ASA هم اعمال شود باید بر روی Apply کلیک کنید.

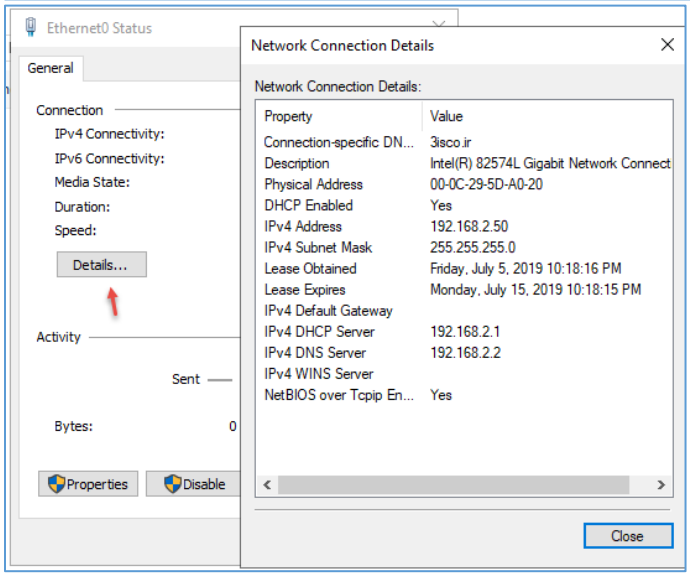
بعد از انجام این کار اگر کلاینتی به اینترفیس Inside متصل شود به صورت اتوماتیک دارای IP خواهد شد.



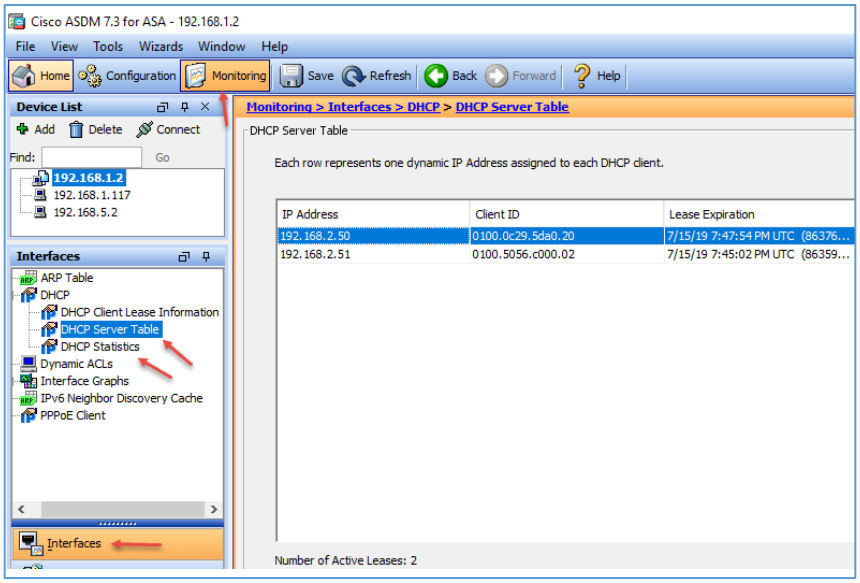
اگر به کارت شبکه متصل شده به ASA دقت کنید، کارت شبکه VMnet2 مربوط به Inside است که برای تست سرویس DHCP یک ویندوز سرور ۲۰۱۶ را به این کارت شبکه متصل می‌کنیم و نتیجه را مشاهده می‌کنیم.

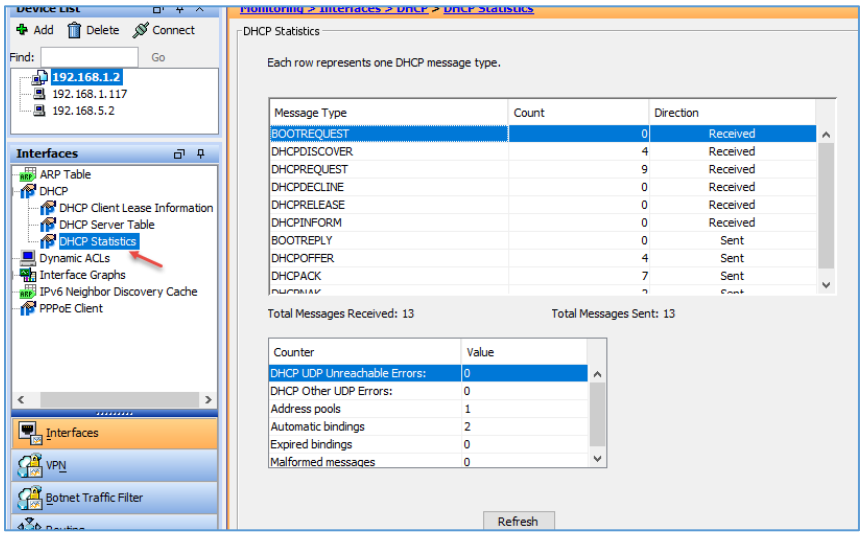


همانطور که مشاهده می‌کنید کارت شبکه VMnet2 برای ویندوز سرور ۲۰۱۶ انتخاب شده است.



همانطور که کارت شبکه ویندوز مورد نظر را مشاهده می‌کنید نام دومین، رنج آدرس و بقیه تنظیمات به درستی برای آن اعمال شده است.





برا اینکه متوجه شوید چه آدرس‌هایی به کلاینت‌ها تخصیص داده شده باید وارد ASDM شوید و از قسمت Monitoring وارد Interfaces شوید و از قسمت DHCP گزینه‌ی DHCP Server Table را انتخاب کنید، همانطور که مشاهده می‌کنید آدرس‌هایی که به کلاینت ها داده شده مشخص شده است، در قسمت DHCP Statistics می‌توانید جزئیات دقیق‌تر آن را مشاهده کنید که تعداد دفعات درخواست و تایید مشخص شده است.

کار با VPN و چرا از آن استفاده می‌کنیم

امروزه اکثر شرکت‌های بزرگ دارای چندین شعبه در سرتاسر کشور یا جهان هستند و ارتباط آنها با هم یک امر بسیار مهم و حیاتی است که این مهم با استفاده از تکنولوژی‌های موجود برقرار می‌شود.

برای اینکه امنیت کاربران و شبکه حفظ شود بهترین راه حل ایجاد یک سرویس VPN برای کارمندان آن شرکت برای دسترسی به اطلاعات آن است تا بدین صورت در مرحله اول امنیت اطلاعات و در مرحله دوم دوری راه تاثیری در روند کار نداشته باشد.

VPN یا همان Virtual private network در اصل یک شبکه‌ی اختصاصی است که از جاهای مختلف دنیا می‌توانند به شبکه اصلی آن سازمان متصل شوند، که این کار از طریق اینترنت امکان پذیر است و نیاز به راه‌اندازی یک خط اختصاصی با شعبه‌های مختلف آن سازمان نیست.

زمانی که VPN را برای شرکت خود راه‌اندازی می‌کنید به این معنا است که کاربران با فعال کردن آن یک تونل بین سیستم خودشان و روتر شرکت ایجاد می‌کنند که روی آن انواع پروتکل‌های رمزنگاری فعال شده است و به هیچ عنوان کسی نمی‌تواند به اطلاعات آن دست پیدا کند، چون هر کاربر دارای یک نام کاربری و رمز عبور است که مختص خودش است و کسی دیگری به این اطلاعات دست پیدا نخواهد کرد.

مزایای استفاده از VPN :

- ✓ گسترش محدوده جغرافیائی ارتباطی
- ✓ بهبود وضعیت امنیت
- ✓ کاهش هزینه‌های عملیاتی در مقایسه با روش‌های سنتی نظیرWAN
- ✓ کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور

- ✓ بهبود بهره‌وری
- ✓ توپولوژی آسان

در این قسمت می‌خواهیم یک شبکه اختصاصی با VPN ایجاد کنیم و کاربرد آن را فرا بگیریم.

انواع VPNها

۱- IPsec

مخفف کلمه‌ی IP Security است که برای انتقال اطلاعات به صورت امن طراحی شده است، در این پروتکل از چندین پروتکل استفاده شده تا بسته‌های ارسالی به صورت کاملاً امن به دست گیرنده برسند، البته در این حالت هر دو طرف سرویس‌دهنده و سرویس‌گیرنده باید از یک کلید استفاده کنند تا بین آنها احراز هویت شکل بگیرد، این پروتکل در لایه 3 مدل OSI کار می‌کند و یکی از ویژگی‌های مهم آن این است که زمانی که در لایه 3 کار می‌کند می‌تواند از پروتکل‌های انتقال UDP و TCP به صورت کامل محافظت کند.

۲- SSL

Secure Sockets Layer این پروتکل بین سرور و کلاینت قرار می‌گیرد و ارتباط را رمزنگاری می‌کند، در بیان دیگر زمانی که یک صفحه وب را با پروتکل HTTP باز می‌کنید اطلاعات به صورت Plain Text ردوبدل می‌شود و همین موضوع باعث می‌شود مهاجم به راحتی از طریق گوش دادن به خط مورد نظر به اطلاعات دست پیدا کنند، به همین خاطر پروتکل HTTPS اجرا شد و درون آن توسط SSL رمزنگاری شده است تا دیگر هیچ اطلاعاتی درز نکند، توجه داشته باشید که این پروتکل در لایه ٤ مدل OSI کار می‌کند.

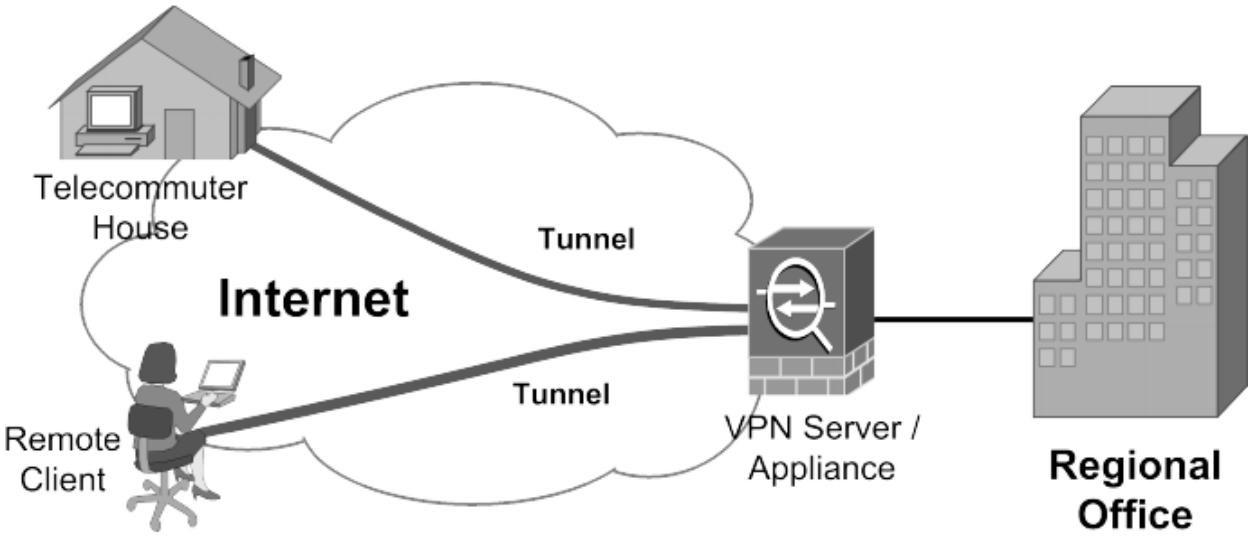
۳- MPLS

Multiprotocol Label Switching یک نوع VPN است که با نام MPLS L3VPN شناخته می‌شود و برای ارتباط چندین سایت در نقاط مختلف کاربرد دارد، در MPLS به صورت پیش‌فرض رمزنگاری وجود ندارد و برای امن کردن آن باید از IPSEC استفاده کنید.

دو نوع اصلی VPN

۱- Remote-access

بعضی از کاربران نیاز دارند تا از راه دور بتوانند به منابع شبکه دسترسی داشته باشند برای همین از VPNهای نوع Remote-Access استفاده می‌کنند، برای ایجاد امنیت در این نوع VPNها از IPSEC و SSL استفاده می‌شود، بسیاری از کسانی که از محصولات سیسکو استفاده می‌کنند از این نوع استفاده می‌کنند، درشکل زیر هم همین موضوع مشخص شده است.



۲- Site-to-siteیچ

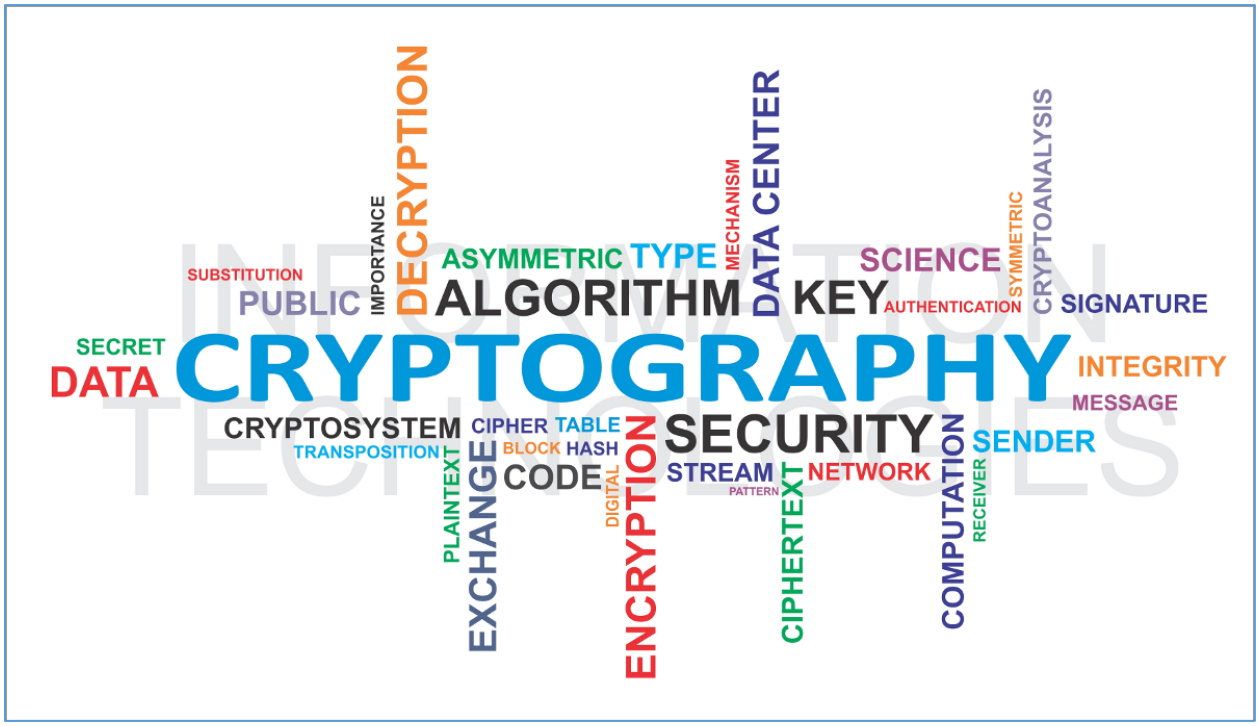
در این نوع ارتباط شرکتهایی که دارای چندین شعبه در جاهای مختلف دنیا هستند می‌توانند با این فناوری شبکه خود را یکپارچه کنند، در این نوع ارتباط دیگر مشتری نیاز نیست که برای خود یک VPN کانکشن ایجاد کند بلکه روترهای ارتباطی با هم دیگر ارتباط VPN دارند.

مزایای اصلی استفاده از VPN در هر دو نوع Site to Site و Remote Access عبارتند از:

- ✓ محرمانه بودن
- ✓ یکپارچگی داده ها
- ✓ تأیید اعتبار
- ✓ حفاظت

رمزنگاری

رمزنگاری یا همان Cryptography به دانشی گفته می‌شود که در آن اطلاعات به صورت یک کلید رمزنگاری می‌شود که این کار توسط الگورتم مربوط به آن انجام می‌شود و فقط کسی می‌تواند از این اطلاعات استفاده کند که اطلاعات لازم مانند کلید و الگوریتم مربوط به آن را بداند.



بررسی برخی از اصطلاحات

Decryption

برای آشکارسازی اطلاعات Encryption شده مورد استفاده قرار می‌گیرد و نام آن را رمزگشایی هم می‌نامند.

Plain text

متن اولیه که رمزنگاری نشده و یک رمز آشکار است و مهاجمان به راحتی می‌توانند به آن دست پیدا کنند.

Cipher

الگوریتمی برای رمزگذاری و رمزشکنی است و از سرعت‌عمل خوبی برخوردار است.

Cryptanalysis

به باز کردن قفل‌های Cipher گفته می‌شود یا خواندن متن قفل شده‌ی آن.

Intruder

در لغت به معنای مزاحم یا مخل است و در رمزنگاری به معنای کسی است که یک کپی از پیام رمزنگاری شده دارد و قصد رمزگشایی آن را دارد. منظور از شکستن رمز، Decrypt کردن آن متن که خود دو نوع است. Active intruder که می‌تواند اطلاعات را روی خط عوض کند و تغییر دهد و passive intruder که فقط می‌تواند اطلاعات روی خط را داشته باشد و قابلیت تغییر آن‌ها را ندارد.

Protocol

به روش یا قراردادی که بین دو یا چند نفر برای تبادل اطلاعات گذاشته می‌شود گفته می‌شود.

Intrusion Points

نقاطی که یک نفوذگر بتواند به اطلاعات با ارزش دست پیدا کند.

Internal Access Point

به سیستم‌هایی گویند که در اتاق یا در شبکه داخلی مستقرند و هیچ امنیتی (LocalSecurity) روی آن‌ها تنظیم نشده باشد و احتمال حمله به آن‌ها وجود دارد.

External Access Point

تجهیزاتی که ما را به شبکه خارجی مانند اینترنت متصل می‌کنند یا Applicationهایی که از طریق اینترنت کار می‌کنند و احتمال حمله به آن‌ها وجود دارد.

Key

به اطلاعاتی گفته می‌شود که با استفاده از آن بتوان cipher text (متنی که cipher شده) را به plain text تبدیل کرد. (یا برعکس) به عبارت ساده یک متن رمز شده توسط یک Key با الگوریتم مناسب، به متن ساده تبدیل می‌شود.

کلیدهای متقارن (Symmetric) و نامتقارن (Asymmetric)

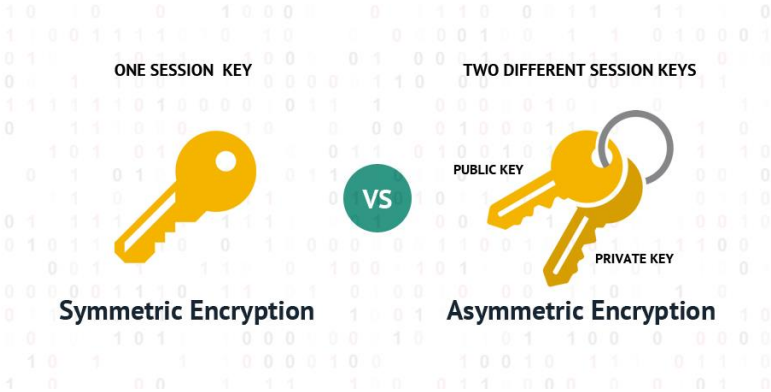
رمزنگاری کلید متقارن

رمزنگاری کلید متقارن یا تک کلیدی، به آن دسته از الگوریتم‌ها، پروتکل‌ها و سیستم‌های رمزنگاری گفته می‌شود که در آن هر دو طرف رد و بدل اطلاعات از **یک کلید رمز یکسان** برای عملیات رمزگذاری و رمزگشایی استفاده می‌کنند. در این قبیل سیستم‌ها، یا کلیدهای رمزگذاری و رمزگشایی یکسان هستند یا با رابطه‌ای بسیار ساده از یکدیگر قابل استخراج هستند.

واضح است که در این نوع از رمزنگاری، باید یک کلید رمز مشترک بین دو طرف تعریف گردد. چون کلید رمز باید کاملاً محرمانه باقی بماند، برای ایجاد و رد و بدل کلید رمز مشترک باید از کانال امن استفاده نمود یا از روش‌های رمزنگاری نامتقارن استفاده کرد. نیاز به وجود یک کلید رمز به ازای هر دو نفرِ درگیر در رمزنگاری متقارن، موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌گردد.

الگوریتم‌هایی که در Symmetric به کار می‌رود عبارت‌اند از:

- ✓ DES
- ✓ DES۳
- ✓ AES
- ✓ IDEA
- ✓ RC2, RC4, RC5, RC6
- ✓ Blowfish



رمزنگاری کلید نامتقارن

رمزنگاری کلید نامتقارن، در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن پیشنهاد شد. در این نوع از رمزنگاری، به جای یک کلید مشترک، از یک زوج کلید به نام‌های کلید عمومی و کلید خصوصی استفاده می‌شود. کلید خصوصی تنها در اختیار دارندهٔ آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد. کلید عمومی در اختیار کلیهٔ کسانی که با دارندهٔ آن در ارتباط هستند قرار داده می‌شود.

به مرور زمان، به غیر از حل مشکل انتقال کلید در روش متقارن، کاربردهای متعددی برای این نوع از رمزنگاری مطرح گردیده‌است. در سیستم‌های رمزنگاری نامتقارن، بسته به کاربرد و پروتکل مورد نظر، گاهی از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود و گاهی نیز، بر عکس، کلید خصوصی برای رمزگذاری و کلید عمومی برای رمزگشایی به کار می‌رود.

دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می‌گردند. رابطهٔ ریاضی بین این دو کلید به گونه‌ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی، عملاً ناممکن است.

الگوریتم‌هایی که در Asymmetric به کار می‌روند عبارت اند از:

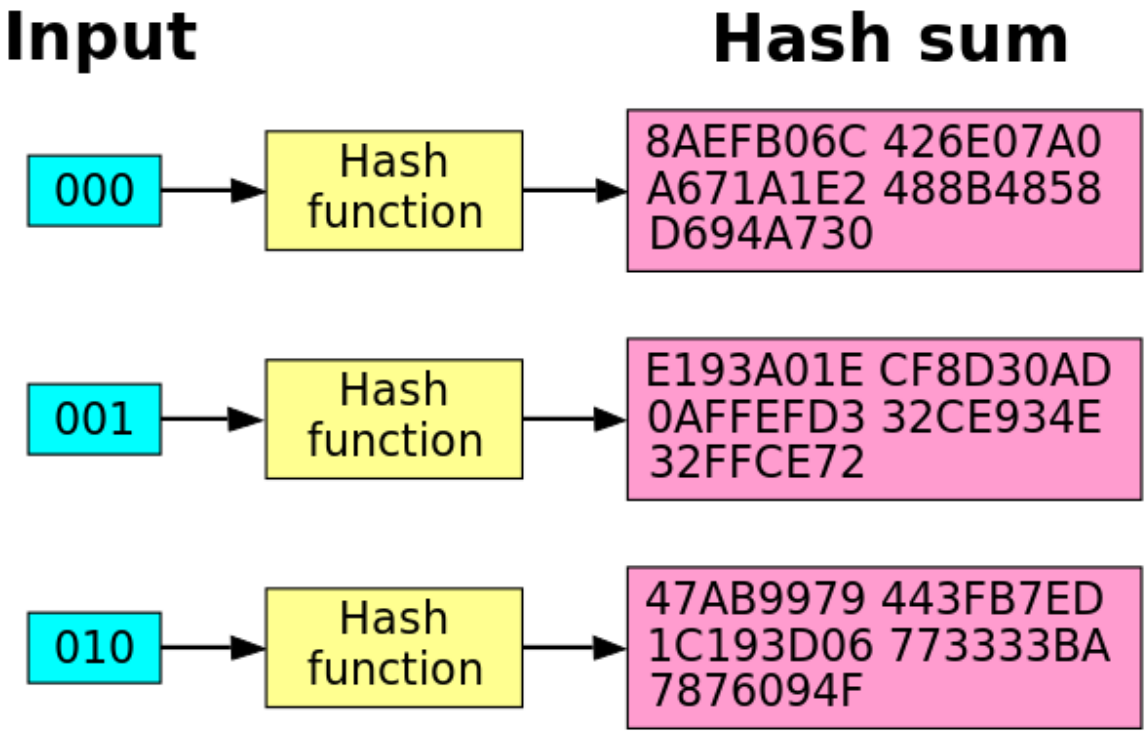
- RSA ✓
- DH ✓
- ElGamal ✓
- DSA ✓
- ECC ✓

مقایسه رمزنگاری کلید متقارن و کلید نامتقارن

اصولاً رمزنگاری کلید متقارن و کلید نامتقارن دارای دو ماهیت متفاوت هستند و کاربردهای متفاوتی نیز دارند. بنا بر این مقایسه این دو نوع رمزنگاری بدون توجه به کاربرد و سیستم مورد نظر کار دقیقی نخواهد بود. اما اگر معیار مقایسه، به‌طور خاص، حجم و زمان محاسبات مورد نیاز باشد، باید گفت که با در نظر گرفتن مقیاس امنیتی معادل، الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن می‌باشند.

هش کردن (Hashing)

در این روش یک ورودی از اطلاعات دریافت می‌شود و بعد از اجرای یک الگوریتم بر روی آن ورودی تبدیل به اعداد و حروف خواهد شد که در شکل زیر این موضوع را مشاهده می‌کنید که مثلاً با ورود عدد ۰۰۰ و اعمال الگوریتم هش روی آن کد نهایی آن به صورت کامل تغییر کرده و هک کردن آن کاملاً سخت شده است.



انواع الگوریتم‌های هش عبارت‌اند از:

نوع الگوریتم	اندازه
BLAKE-256	256 bits
BLAKE-512	512 bits
BLAKE2s	Up to 256 bits
BLAKE2b	Up to 512 bits
ECOH	224 to 512 bits
FSB	160 to 512 bits
GOST	256 bits
Grøstl	Up to 512 bits
HAS-160	160 bits
HAVAL	128 to 256 bits
JH	224 to 512 bits
MD2	128 bits
MD4	128 bits
MD5	128 bits
MD6	Up to 512 bits
RadioGatún	Up to 1216 bits
RIPEMD	128 bits
RIPEMD-128	128 bits
RIPEMD-160	160 bits
RIPEMD-320	320 bits
SHA-1	160 bits
SHA-224	224 bits
SHA-256	256 bits
SHA-384	384 bits
SHA-512	512 bits
SHA-3 (originally known as Keccak)	arbitrary
Skein	arbitrary
Snefru	128 or 256 bits
Spectral Hash	512 bits
Streebog	256 or 512 bits
SWIFFT	512 bits
Tiger	192 bits
Whirlpool	512 bits

از بین این الگوریتم‌ها بیشترین استفاده از الگوریتم‌های MD5، SHA1، SHA2 می‌شود.

بررسی IPsec وSSL

IPsec یا همان Internet Protocol security عبارت است از مجموعه‌ای از چندین پروتکل که برای ایمن‌سازی پروتکل اینترنت در ارتباطات بوسیله احراز هویت و رمزگذاری در هر بسته(packet) در یک سیر داده به کار می‌رود. این پروتکل محصول مشترک مایکروسافت و سیسکو است که در نوع خود جالب توجه است.

IPsec بر خلاف دیگر پروتکلهای امنیتی نظیر SSL, TSL, SSH که در لایه انتقال (لایه ٤) به بالا قرار دارند در لایه شبکه یا همان لایه ۳ مدل مرجع OSI کار می‌کند یعنی لایه که IP در آن قرار دارد که باعث انعطاف بیشتر این پروتکل می‌شود به‌طوری‌که می‌تواند از پروتکل‌های لایه ٤ نظیر TCP و UDP محافظت کند.

مزیت بعدی IPsec به نسبت بقیه پروتکلهای امنیتی نظیر SSL این است که: نیازی نیست که برنامه بر طبق این پروتکل طراحی شود.

الگوریتم‌های رمزنگاری تعریف شده برای استفاده با IPSEC شامل:

- ✓ SHA1 برای حفاظت از صداقت و صحت
- ✓ DES برای محرمانگی
- ✓ AES برای قابلیت اعتماد

IPSEC معمولاً در ارتباط با IP V6 توسعه داده شده و در اصل در تمام پیاده‌سازی‌های استاندارد از IPV6، IPSEC مورد نیاز است. IPSEC برIPاده‌سازی IPV4 اختیاری است و در IPV4 اغلب برای ایمن‌سازی ترافیک مورد استفاده قرار می‌گیرد.

خانواده پروتکل IPSec شامل دو پروتکل است. یعنی سرآیند احراز هویت یا AH یا همان authentication header وESP هر دوی این پروتکل‌ها از IPSec مستقل خواهد بود.

پروتکل AH

بطور خلاصه پروتکل AH در واقع تأمین‌کننده سرویس‌های امنیتی زیر خواهد بود:

- ✓ تمامیت داده ارسالی
- ✓ تصدیق هویت مبدأ داده ارسالی

- ✓ رد بسته‌های دوباره ارسال شده

پروتکل Encapsulation Security Payload(ESP)

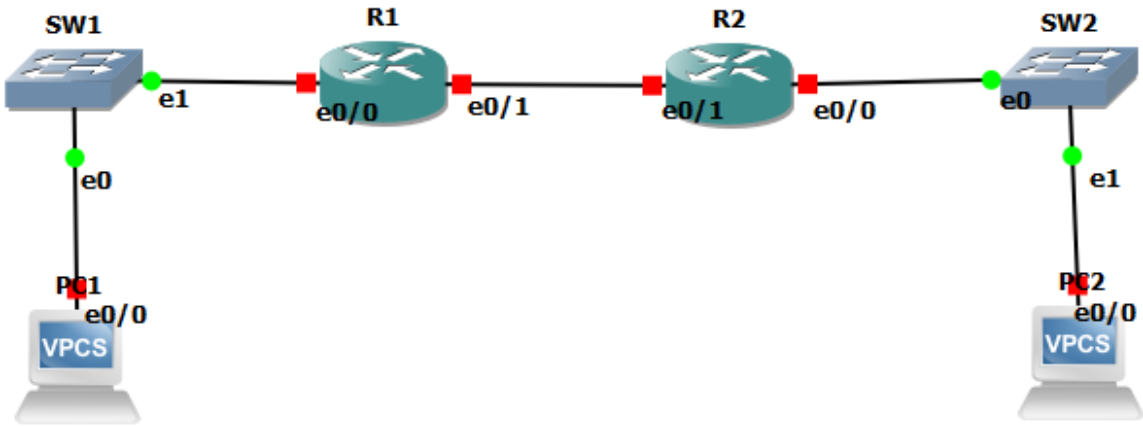
پروتکل ESP سرویس‌های امنیتی زیر را ارائه می‌کند:

- ✓ محرمانگی
- ✓ احراز هویت مبدأ داده ارسالی
- ✓ رد بسته‌های دوباره ارسال شده

ایجاد VPN در دستگاه‌های سیسکو

بررسی Site To Site VPN با استفاده از IPSEC

بعد از بررسی اولیه VPN در این قسمت می‌خواهیم برای ایجاد VPN از دستگاه‌های سیسکو استفاده کنیم، که این کار را در نرم‌افزار GNS3 انجام می‌دهیم به مانند شکل زیر ٤ روتر و دو سوئیچ به لیست اضافه کنید، توجه داشته باشید PC1 و PC2 همان روتر هستند که با کلیک راست بر روی آنها و انتخاب Change Symbol آیکون آنها را به PC تغییر حالت دادیم، در ادامه به ترتیب تنظیمات مربوط به هر دستگاه را انجام می‌دهیم.



تنظیمات مربوط به آدرس IP و انجام Route

تنظیمات روتر R1

```
R1#conf t
R1(config-if)#int e0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#int e0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no sh
```

در دستورات بالا وارد پورت‌های مورد نظر روتر R1 شدیم و آدرس IP را برای آنها مشخص و پورت را روشن کردیم.

تنظیمات روتر R2

```
R2#conf t
R2(config)#int e0/1
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int e0/0
R2(config-if)#ip address 172.16.2.1 255.255.255.0
R2(config-if)#no sh
```

تنظیمات PC1

```
PC1#conf t
PC1(config)#int e0/0
PC1(config-if)#ip address 172.16.1.2 255.255.255.0
PC1(config-if)#no sh
```

تنظیمات PC2

```
PC2#conf t
PC2(config)#int e0/0
PC2(config-if)#ip address 172.16.2.2 255.255.255.0
PC2(config-if)#no sh
```

بعد از اینکه با دستور PING ارتباط بین دستگاه‌ها را مطمئن شدید باید از دستور Route برای معرفی شبکه‌ها به هم استفاده کنیم.

برای اینکه از پروتکل‌های مسیریابی هم استفاده کنیم در این قسمت پروتکل EIGRP را فعال می‌کنیم تا شبکه های این دستگاه‌ها به هم معرفی شوند.

روتر R1

```
R1(config)#router eigrp 100
R1(config-router)#network 192.168.1.0
R1(config-router)#network 172.16.1.0
```

روتر R2

```
R2(config)#router eigrp 100
R2(config-router)#network 192.168.1.0
R2(config-router)#network 172.16.2.0
```

کلاینت PC1

```
PC1(config)#router eigrp 100
PC1(config-router)#net 172.16.1.0
```

کلاینت PC2

```
PC2(config)#router eigrp 100
PC2(config-router)#net 172.16.2.0
```

با انجام مراحل بالا اگر از طریق PC1 به PC2 دستور PING را اجرا کنید مطمئناً این دو دستگاه همدیگر را می‌بینند.

```
PC1#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5 ms
```

یکی از ویژگی‌های IPSEC این است که خط ارتباطی را بین دو روتر یا دستگاه امن می‌کند، اگر در همین حالت این فناوری بین دو خطوط استفاده نشود هر کسی می‌تواند با ابزارهای لازم به اطلاعات گوش دهد و به اطلاعاتی که نیاز دارد دست پیدا کند، مثلاً اگر در PC2 سرویس Telnet را فعال کنید و بخواهید از طریق PC1 به آن دسترسی داشته باشید، فرد مهاجم با استفاده از نرم‌افزارهای اسنیف مانند Nmap یا Wireshark به اطلاعات شما مانند نام کاربری و رمز عبور دست پیدا خواهد کرد که برای حل این مشکل یکی از راه‌های پیشنهادی که بسیار کارایی دارد استفاده از فناوری IPSEC است.

تنظیمات مربوط به IPSEC

تنظیم روتر R1

```
R1(config)#crypto isakmp policy 1
```

با دستور crypto و انتخاب isakmp رمزنگاری بر روی این خط فعال می‌شود.

```
R1(config-isakmp)#encryption 3des
```

نوع رمزگذاری را می‌توانید با دستور encryption انتخاب کنید که باید یکی از گزینه‌های AES, 3DES, DES را انتخاب کنید که 3DES انتخاب خوبی خواهد بود چون از قدرت رمزگذاری بیشتری برخوردار است.

```
R1(config-isakmp)#hash md5
```

در مورد هشینگ هم در قسمت‌های قبلی صحبت کردیم که گزینه‌ی MD5 را انتخاب می‌کنیم.

```
R1(config-isakmp)#authentication pre-share
```

در این قسمت باید نوع تایید ارتباط بین دو روتر را مشخص کنید که pre-share انتخاب شده است.

```
R1(config-isakmp)#group 2
```

در قسمت Group گزینه‌های مختلفی وجود دارد که در زیر لیست آنها را مشاهده می‌کنید:

- Diffie-Hellman group 1 (768 bit)
- 14 Diffie-Hellman group 14 (2048 bit)
- 15 Diffie-Hellman group 15 (3072 bit)
- 16 Diffie-Hellman group 16 (4096 bit)
- 19 Diffie-Hellman group 19 (256 bit ecp)
- Diffie-Hellman group 2 (1024 bit)
- 20 Diffie-Hellman group 20 (384 bit ecp)
- 24 Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
- 5 Diffie-Hellman group 5 (1536 bit)

گروه شماره‌ی ۲ می‌توانید انتخاب مناسبی باشد، Hellman group برای ایجاد امنیت بین دو نقطه نا امن کاربرد دارد.

نکته مهم : اگر اطلاعات بین روترها بسیار حیاتی و مهم باشد بهتر است که گروهی به غیر از گروه‌های 1,2,5 انتخاب شود چون این گروه‌ها معروف به AVOID هستند و سطح امنیتی مناسبی در برابر تعدیدات ارائه نخواهند داد.

```
R1(config-isakmp)#lifetime 86400
```

در این قسمت می‌توانید حداکثر زمان فعال بودن ارتباط بین دو دستگاه را مشخص کنید که عددی بین ۱ تا ۸٦٤۰۰ است که در این قسمت بالاترین گزینه انتخاب شده است، این عدد بر روی حسب ثانیه می‌باشد.

```
R1(config)#crypto isakmp key 123456 address 192.168.1.2
```

با این دستور یک رمز عبور ۱۲۳٤٥٦ ایجاد خواهد شد که مربوط به آدرس روتر روبرویی است.

```
R1(config)#ip access-list extended 100
R1(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

برای اینکه به آدرس شبکه داخلی پشت روترها اجازه عبور بین تونل IPSEC را دهیم باید یک Access-list در هر دو روتر ایجاد کنیم و دسترسی لازم را بدهیم، در دستور بالا یک اکسس لیست شماره‌ی ۱۰۰ که از نوع extended است را ایجاد می‌کنیم و در داخل آن به دو شبکه 172.16.1.0 و 172.16.2.0 اجازه عبور می‌دهیم، البته از این اکسس لیست در ادامه استفاده خواهیم کرد.

```
R1(config)#crypto ipsec transform-set IPTS esp-3des esp-md5-hmac
```

دستور بعدی ایجاد بسته انتقال IPSEC با استفاده از دستور transform-set است که دارای رمزنگاری esp-3des و esp-md5-hmac است، توجه داشته باشید که کلمه IPTS برای این بسته وارد کرده‌ایم که شما می‌توانستید هر نامی برای آن وارد کنید، فقط توجه داشته باشید که از این نام در ادامه استفاده خواهیم کرد.

```
R1(config)#crypto map MAP1 10 ipsec-isakmp
```

با دستور بالا ارتباط MAP با Ipsec برقرار خواهد شد.

```
R1(config-crypto-map)#set peer 192.168.1.2
```

با دستور Set peer آدرس روتر R2 را وارد می‌کنیم.

```
R1(config-crypto-map)#set transform-set IPTS
```

با دستور بالا یک بسته با نام IPTS برای Transform-set ایجاد خواهد شد.

```
R1(config-crypto-map)#match address 100
```

با این دستور اکسس لیستی که با شماره‌ی ۱۰۰ ایجاد کردیم در این MAP قرار خواهد گرفت.

```
R1(config-crypto-map)# int e0/1
R1(config-if)#crypto map MAP1
*May  7 08:33:35.543: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

در مرحله آخر برای فعال‌سازی MAP باید وارد Interface شوید که به روتر روبریی متصل است که در سناریوی ما پورت e0/1 است، بعد از ورود با دستور crypto map MAP1 فعال‌سازی این دستورات به طور کامل بر روی این پورت انجام می‌شود که در آخر جمله "ISAKMP is ON " نشان دهنده فعال‌سازی آن است.

همه دستورات روتر R1 در یک نگاه

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
```

```
R1(config)#crypto isakmp key 123456 address 192.168.1.2
R1(config)#ip access-list extended 100
R1(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
R1(config)#crypto ipsec transform-set IPTS esp-3des esp-md5-hmac
R1(config)#crypto map MAP1 10 ipsec-isakmp
R1(config-crypto-map)#set peer 192.168.1.2
R1(config-crypto-map)#set transform-set IPTS
R1(config-crypto-map)#match address 100
R1(config-crypto-map)# int e0/1
R1(config-if)#crypto map MAP1
```

تنظیم روتر R2

در این قسمت فقط دستورات مربوط به روتر R2 را قرار می‌دهم چون توضیحات آن دقیقاً مانند روتر R2 است با این تفاوت که آدرس IP در آن متفاوت وارد می‌شود.

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encryption 3des
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config)#crypto isakmp key 123456 address 192.168.1.1
```

رمز عبوری که در روتر R1 تعریف کردیم دقیقاً همان رمز را به همراه آدرس روتر روبرو وارد می‌کنیم.

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
```

در دستور بالا آدرس مبدا و مقصد چون از طرف روتر ۲ است تغییر کرده است.

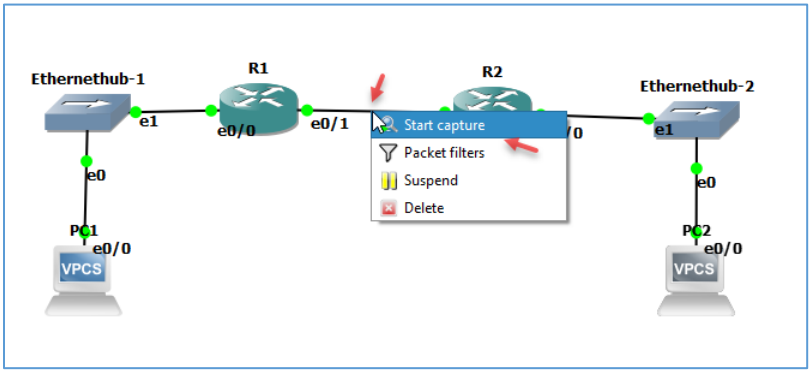
```
R2(config)#crypto ipsec transform-set IPTS esp-3des esp-md5-hmac
R2(config)#crypto map MAP1 10 ipsec-isakmp
```

```
R2(config-crypto-map)#set peer 192.168.1.1
```

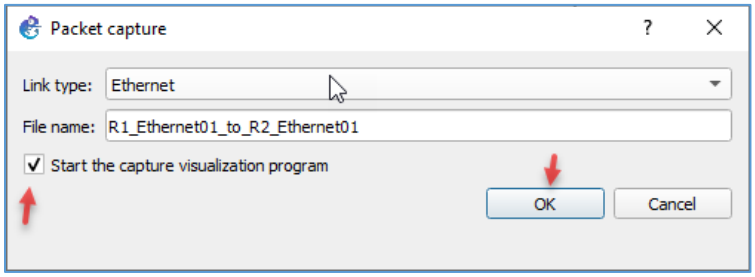
آدرس روتر R1 را برای ارتباط وارد می‌کنیم.

```
R2(config-crypto-map)#set transform-set IPTS
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#int e0/1
R2(config-if)#crypto map MAP1
```

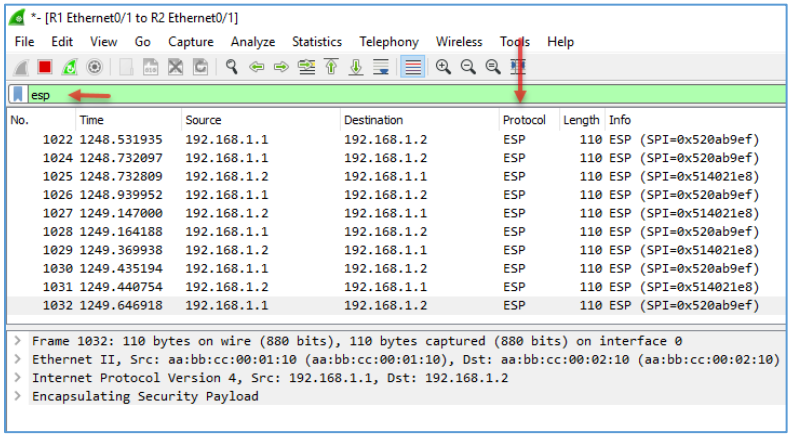
با انجام این مراحل توانستیم ارتباط بین دو روتر را به صورت کاملاً امن ایجاد کنیم، برای اینکه متوجه شوید که ارتباط بین دو روتر به چه صورت است، باید بر روی لینک بین دو روتر کلیک راست کنید و گزینه‌ی Start Capture را انتخاب کنید، با این کار نرم‌افزار Wireshark برای شما در صوت نصب بودن اجرا خواهد شد.



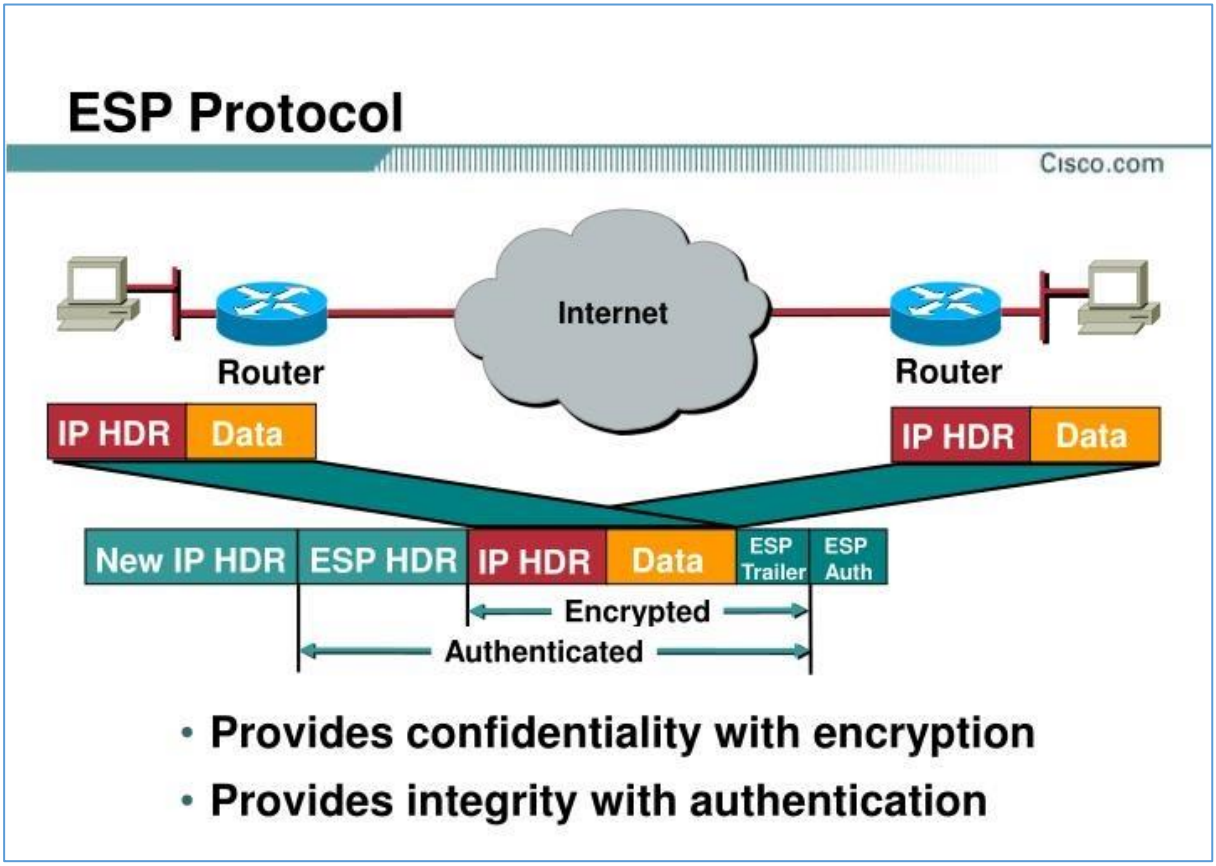
در این صفحه تیک گزینه‌ی مورد نظر را انتخاب و بر روی ok کلیک کنید.



اگر از PC1 به PC2 یک Ping اجرا کنید یا کاری دیگر انجام دهید تمام ارتباط با استفاده از پروتکل ESP (Encapsulating Security Payload) امن شده است و دسترسی به اطلاعات آن امکان پذیر نیست که این موضوع را در شکل روبرو مشاهده می‌کنید، برای مشخص کردن پروتکل ESP بهتر است این کلمه را در فیلترینگ وارد کنید.



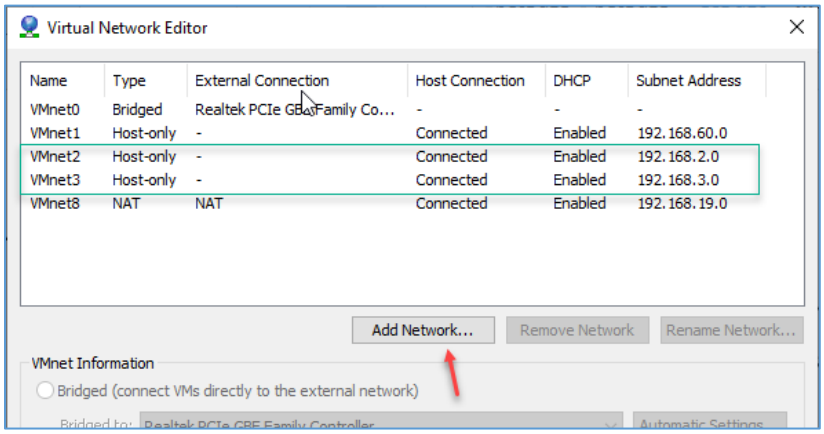
در مورد پروتکل ESP می‌توان گفت که این پروتکل سه عملیات رمزنگاری، احراز هویت، محافظت را برای داده‌های شما انجام می‌دهد، البته ESP از هدر بسته‌ها محافظت نمی‌کند و بسته‌هایی که در داخل بسته‌ی دیگر قرار می‌گیرند را رمزنگاری می‌کند، به طور کل در یک شبکه مبتنی بر IP اول هدر IP قرار می‌گیرد و پشت آن ESP، که در زیر شکل زیر هدر کلی ESP را مشاهده می‌کنید.



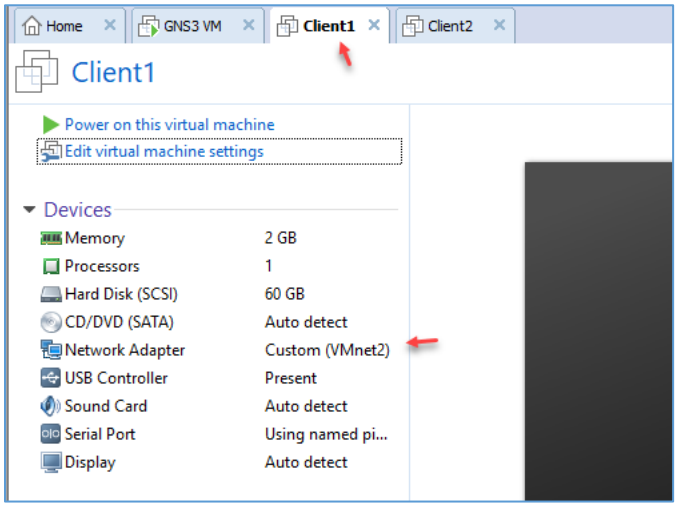
کار با Site To Site VPN در ASDM

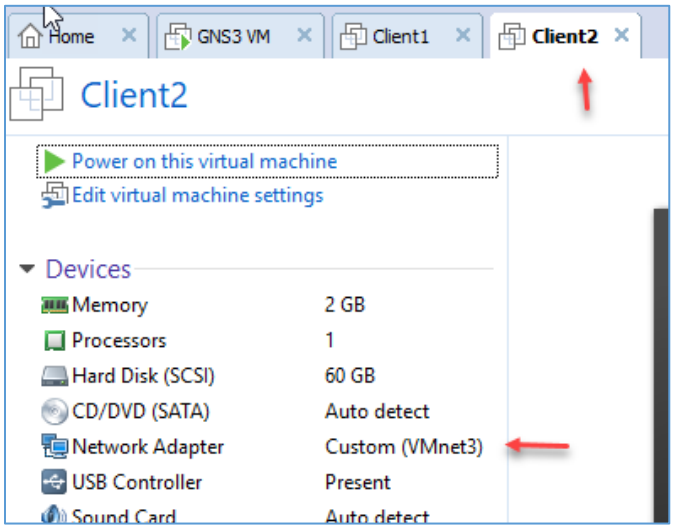
در این قسمت میخواهیم عملیات Site To Site VPN را بین دو فایروال ASA از طریق نرم افزار ASDM انجام دهیم.

برای شروع کار به نیاز به دو فایروال ASA و دو کلاینت داریم که کلاینت خود را در این قسمت دو تا ویندوز ۷ مجازی در نظر می‌گیریم و به صورت Cloud آنها را به ASA متصل می‌کنیم، برا اینکه بتوانیم از ماشین مجازی استفاده کنیم باید دو کارت شبکه برای آنها ایجاد کنیم که این کار را با ایجاد دو کارت شبکه VMnet2,3 انجام می‌دهیم، به آدرس IP آنها هم توجه کنید، همانطور که می‌دانید این کار در سرویس Virtual Network Editor انجام می‌شود.

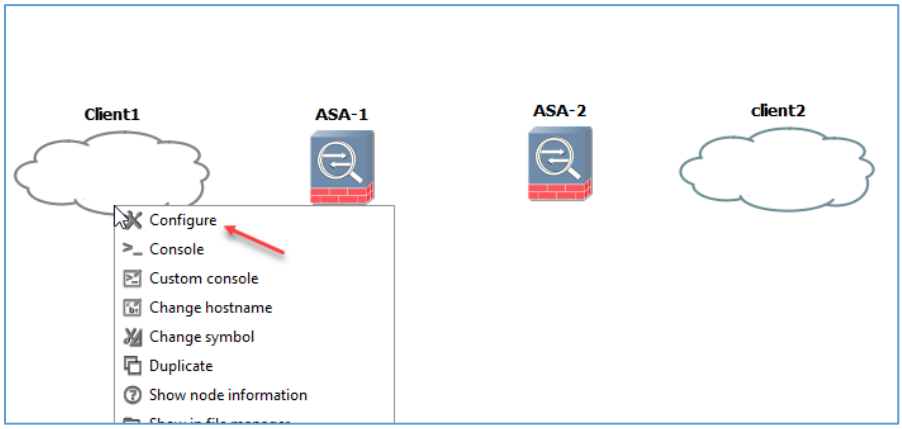


در نرم‌افزار VMware Workstation دو ماشین مجازی با نام‌های Client1 و Client2 ایجاد کردیم و به Client1 کارت شبکه VMnet2 را اختصاص دادیم.

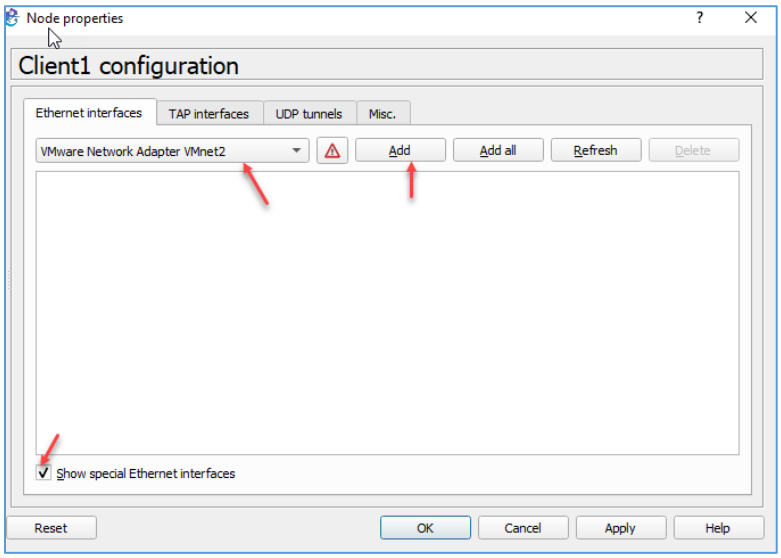




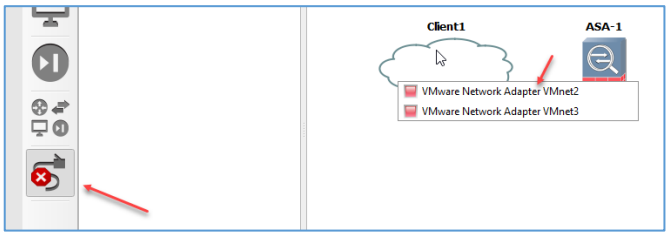
و برای Client2 هم کارت شبکه VMnet3 را اختصاص دادیم که در ادامه باید به آنها IP اختصاص دهیم.



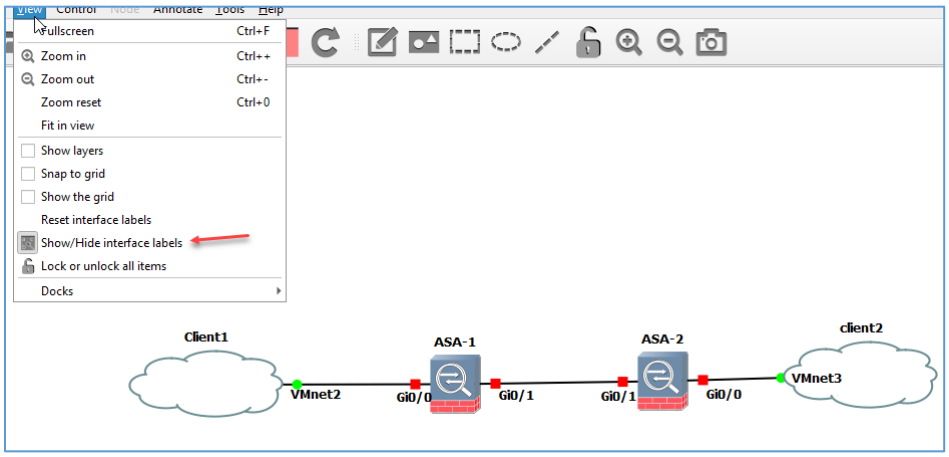
به مانند شکل دو فایروال ASA و دو Cloud را به صفحه‌ی GNS3 اضافه کنید و نام آنها را به مانند روبرو تغییر دهید، بر روی یکی از Cloudها کلیک راست کنید و گزینه‌ی Configure را انتخاب کنید.



در این صفحه باید همه کارت شبکه‌های فعلی را انتخاب و Delete کنید بعد از خالی شدن صفحه تیک گزینه‌ی Show special Ethernet interface را انتخاب کنید تا لیست کارت شبکه‌های مخفی نمایش داده شود بعد از آن کارت شبکه‌ی VMnet2 و VMnet3 را انتخاب و به لیست اضافه کنید، دقیقا همین کار را هم در Cloud دوم انجام دهید.



بعد از انجام مراحل بالا بر روی لینک کلیک کنید و بعد از کلیک بر روی Client1 کارت شبکه‌ی VMnet2 را انتخاب کنید برای Cloud دوم یعنی Client2 هم کارت شبکه‌ی VMnet3 را انتخاب کنید و به فایروال متصل کنید.



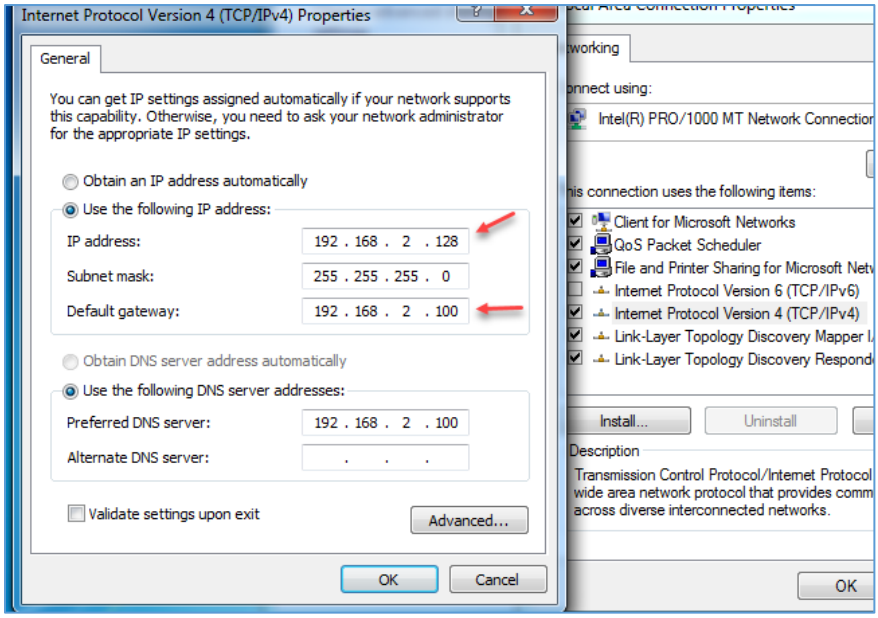
شکل کلی پروژه به صورت روبرو خواهد بود که در آن نام Interfaceها مشخص شده است، اگر بخواهید در GNS3 نام Interface را مشاهده کنید باید از طریق منوی View گزینه‌ی Show/Hide interface lables را انتخاب کنید تا نام آنها مشخص شود، اگر چنانچه نام Interface را بخواهید ویرایش کنید باید بر روی آن کلیک راست کنید و گزینه‌ی Text edit را انتخاب کنید.

```
ciscoasa(config-if)# hostname ASA1
ASA1(config)#
ASA1(config)#
ASA1(config)#
ASA1(config)#
ASA1(config)#
ASA1(config)#
ASA1(config)# int gigabitEthernet 0/0
ASA1(config-if)# ip address 192.168.2.100 255.255.255.0
ASA1(config-if)# nameif inside
ASA1(config-if)# no sh
ASA1(config-if)# http server enable
ASA1(config)# http 192.168.2.0 255.255.255.0 inside
ASA1(config)# int gigabitEthernet 0/1
ASA1(config-if)# ip address 10.10.10.1 255.255.255.0
ASA1(config-if)# nameif outside
ASA1(config-if)# no sh
ASA1(config-if)#
```

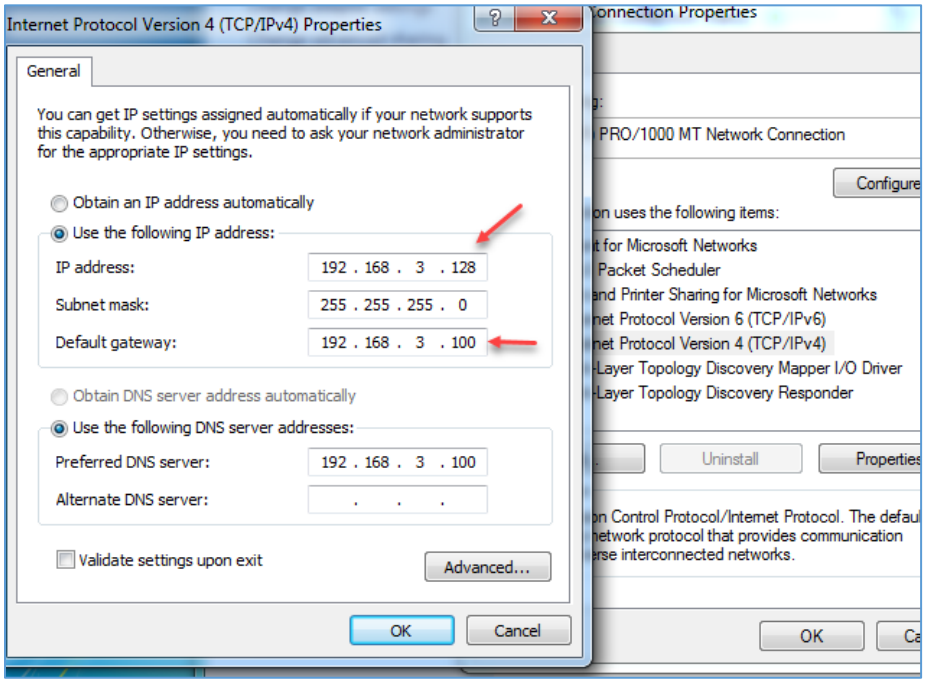
در ادامه کار فایروال‌ها را روشن کردن و تنظیمات مربوط به آدرس IP و دسترسی آن را توسط ASDM تنظیم می‌کنیم که این موضوع را در شکل روبرو مشاهده می‌کنید، این تنظیمات مربوط به فایروال ASA1 است.

```
ciscoasa(config)# hostname ASA2
ASA2(config)#
ASA2(config)#
ASA2(config)# int g0/0
ASA2(config-if)# ip address 192.168.3.100 255.255.255.0
ASA2(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA2(config-if)# no sh
ASA2(config-if)# http server enable
ASA2(config)# http 192.168.3.0 255.255.255.0 inside
ASA2(config)# int g0/1
ASA2(config-if)# ip address 10.10.10.2 255.255.255.0
ASA2(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA2(config-if)# no sh
ASA2(config-if)#
```

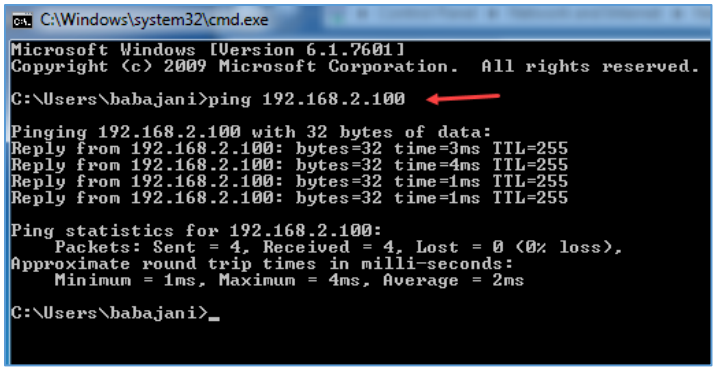
این هم تنظیمات مربوط به فایروال ASA2 اگر توجه کرده باشید دستور http را هم در interface داخلی یا همان inside فعال کردیم تا بتوانیم از طریق نرم‌افزار ASDM به فایروال دسترسی داشته باشیم.



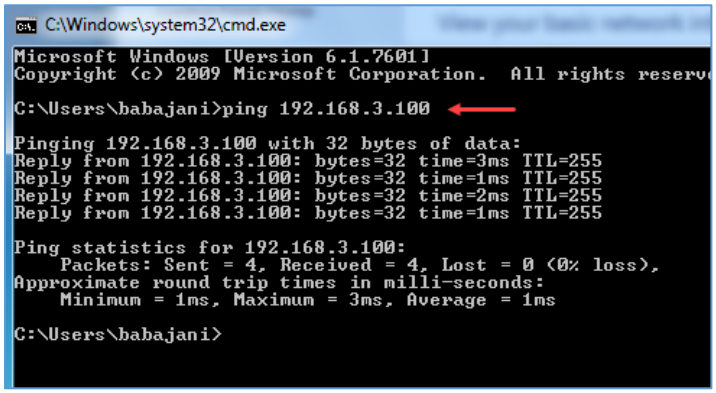
توجه داشته باشید در داخل کلاینت هم باید آدرس شبکه را مشخص کنید، برای این کار در Client1 آدرس مورد نظر را وارد کنید و توجه داشته باشید که Default Gateway را هم وارد کنید که همان فایروالی است که به آن متصل شده است.



در Client2 هم باید به صورت روبرو آدرس IP را وارد کنید و در قسمت Gateway هم آدرس فایروال را وارد کنید.



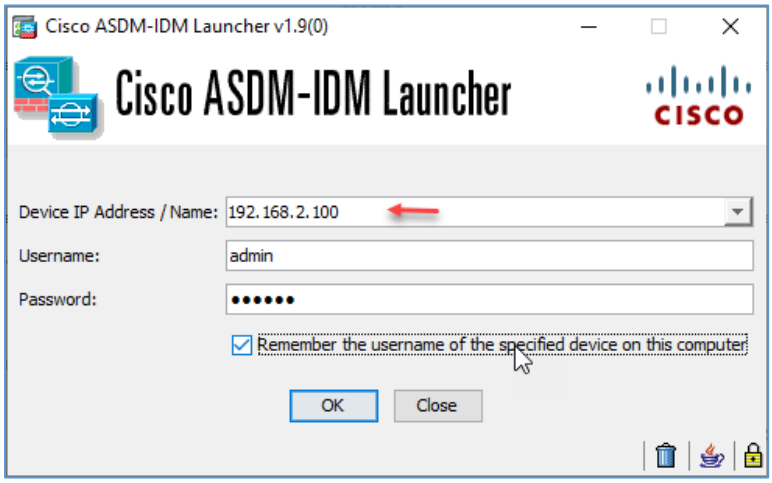
بعد از انجام کارهای بالا وارد کلاینت‌ها شوید و فایروال روبروی آنها را تست بگیرید که این موضوع را در شکل مقابل مشاهده می‌کنید.



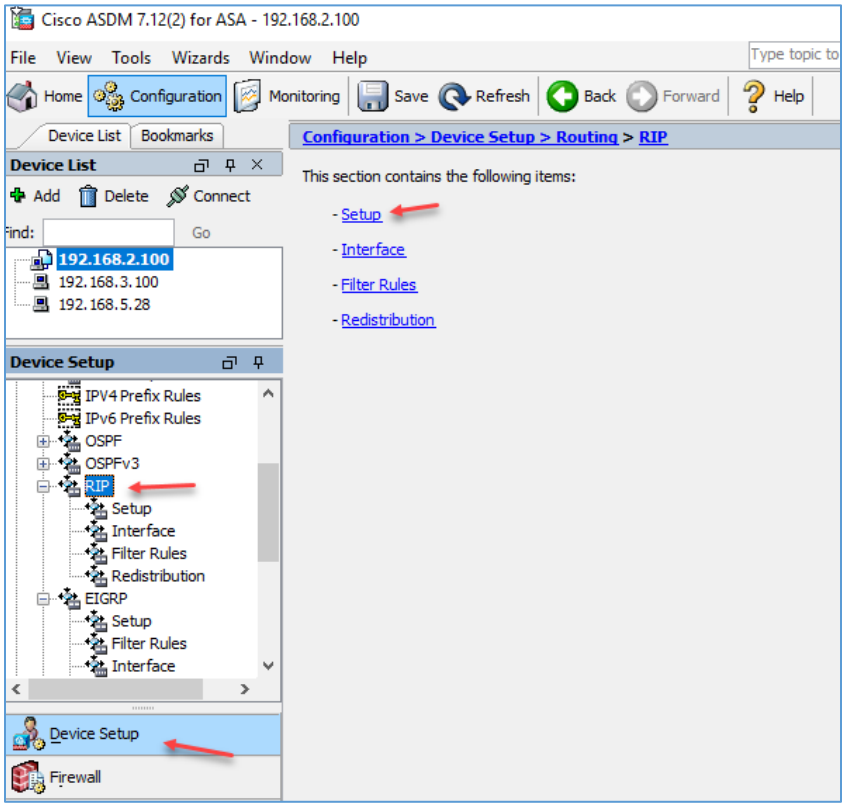
در Client2 هم تست Ping را انجام دهید تا خیالمان از بابت این موضوع راحت باشد.

بعد از انجام تست به مرحله نهایی کار میرسیم و آن هم این است که باید کاری کنیم که Client1 بتواند در یک خط ارتباطی امن Client2 را ببیند، که این کار را در ادامه با دقت انجام خواهیم داد.

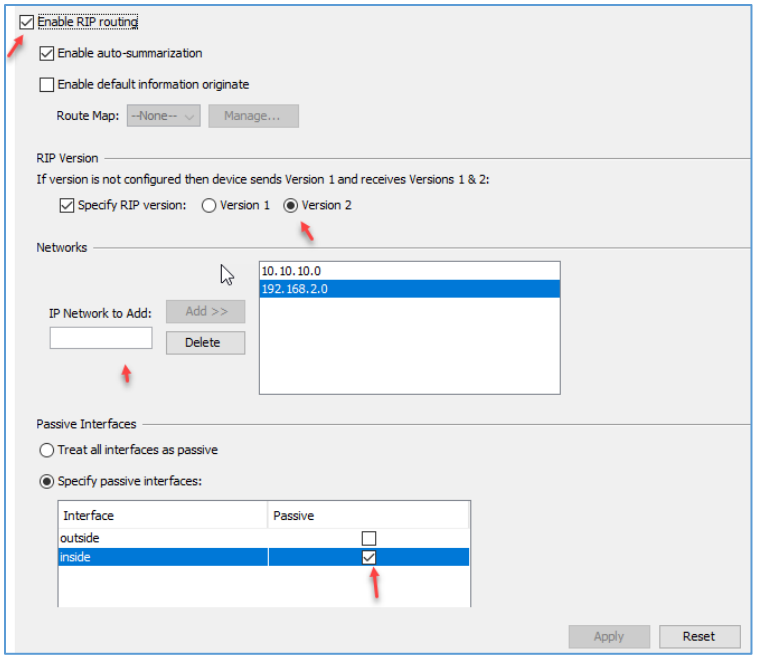
برای اینکه بتوانیم از طریق ASDM به فایروال متصل شویم نیاز به Username و Password داریم که باید در فایروال تعریف کنید.



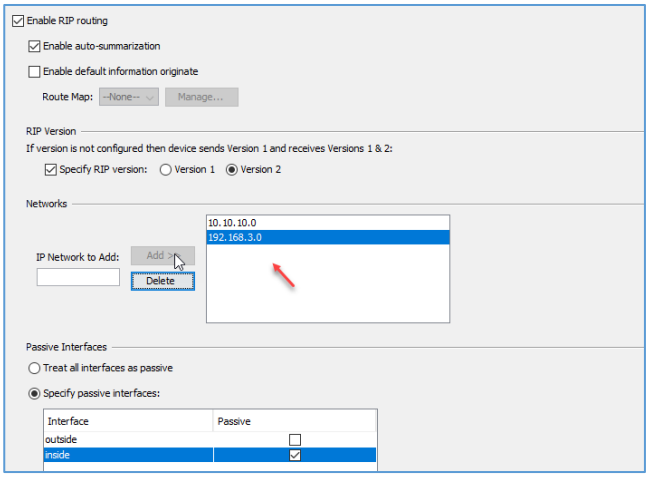
ASDM-IDM را اجرا کنید و آدرس فایروال ASA1 را به همراه نام کاربری و رمز عبور مربوط به آن وارد کنید، توجه داشته باشید تمام این کارها را باید در روتر دوم هم انجام داد.



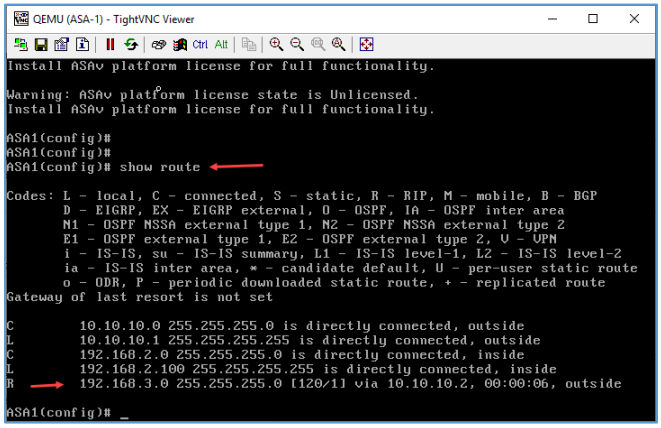
در صفحه ASDM اولین کاری که باید انجام دهیم این است که باید شبکه‌ی دو فایروال را از طریق پروتکل‌های مسیریابی به هم معرفی کنیم البته این کار را می‌شود از طریق Static Route هم انجام داد ولی در این قسمت سعی کردیم از پروتکل RIP برای این کار استفاده کنیم، به مانند شکل از قسمت Device Setup بر روی RIP کلیک کنید و در صفحه باز شده گزینه‌ی Setup را انتخاب کنید.



در این صفحه تیک گزینه‌ی Enable RIP routing را انتخاب کنید تا این پروتکل فعال شود، در قسمت RIP Version گزینه‌ی Version2 را انتخاب کنید، در قسمت Networks باید شبکه‌هایی که به فایروال ASA1 متصل است را وارد و بر روی Add کلیک کنید تا به لیست اضافه شود و در آخر برای اینکه این پروتکل اطلاعات خود را فقط به شبکه outside ارسال کند باید تیک گزینه‌ی inside را انتخاب کنید در آخر هم بر روی Apply کلیک کنید تا تنظیمات بر روی فایروال اعمال شود.

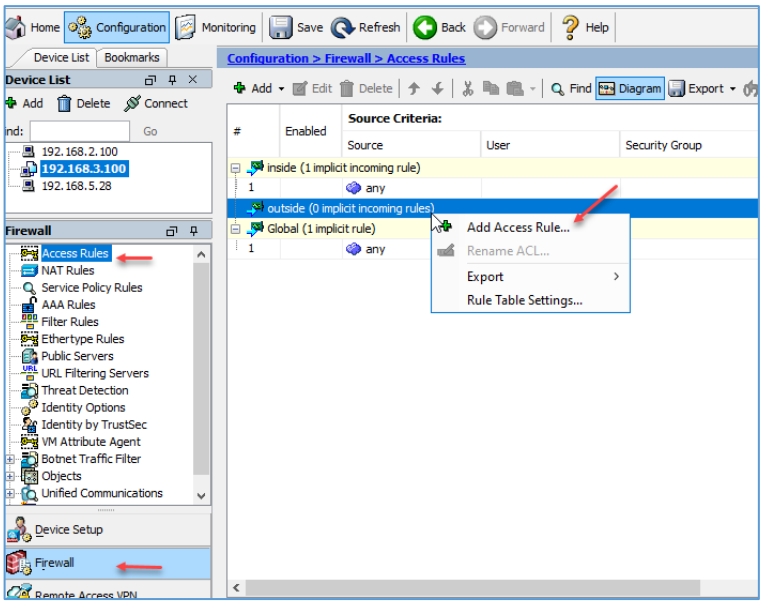


همین کار را باید در ASA2 هم انجام دهید که در شکل روبرو این موضوع را مشاهده می‌کنید.

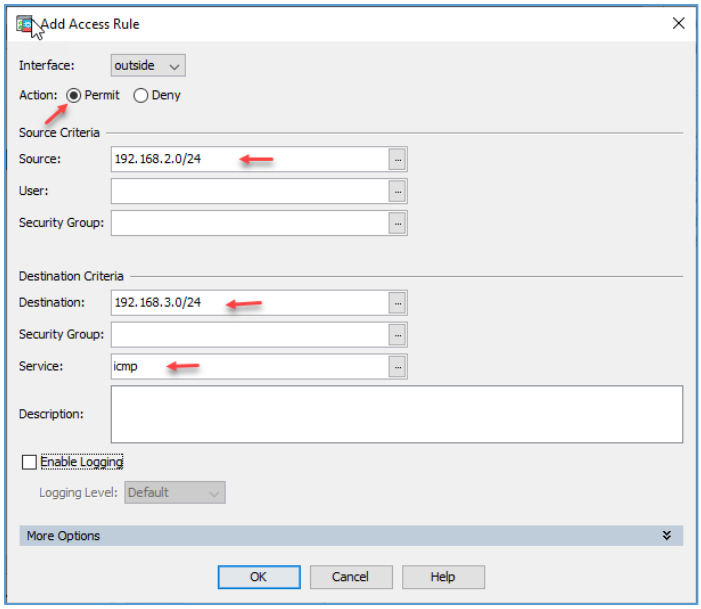


اگر بعد از فعال شدن پروتکل RIP وارد فایروال شوید و دستور Show route را وارد کنید مشاهده خواهید کرد که شبکه پشت فایروال‌ها به فایروال روبروی ارسال شده است.

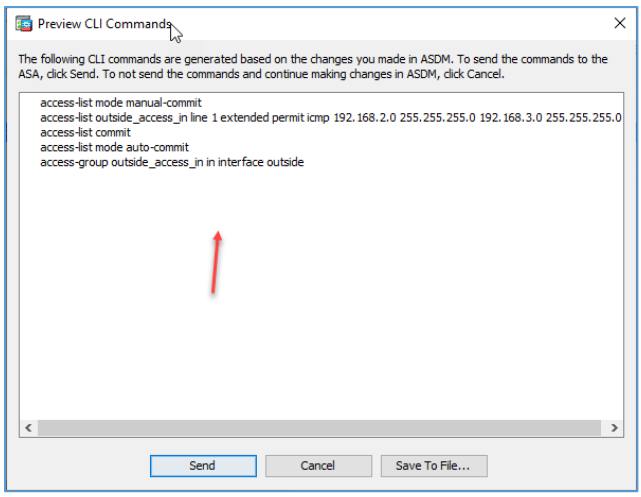
نکته: با اینکه پروتکل RIP فعال شده است ولی کلاینت‌ها به هیچ عنوان نمی‌توانند همدیگر را ببینند و دلیل آن هم این است که ترافیک به صورت پیش‌فرض بین دو فایروال عبور نمی‌کند و برای اینکه به آنها اجازه دهیم باید Access-List تعریف کنیم.



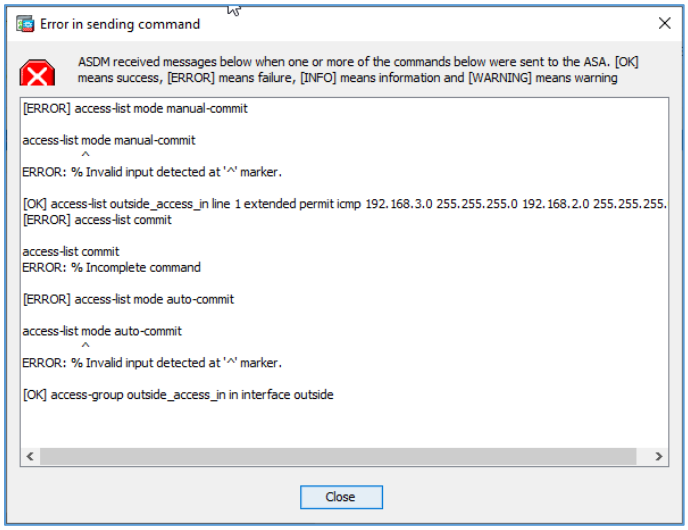
از طریق ASDM به فایروال ASA2 متصل شوید و از قسمت Firewall بر روی Access Rules کلیک کنید، در صفحه باز شده باید Access_list خود را بر روی خروجی اعمال کنیم، یعنی اینکه باید بگوییم به شبکه ۱۹۲.۱۶۸.۲.۰ برای ورود به شبکه ۱۹۲.۱۶۸.۳.۰ اجازه بده که برای این کار بر روی outside کلیک راست کنید و بر روی Add Access Rule کلیک کنید.



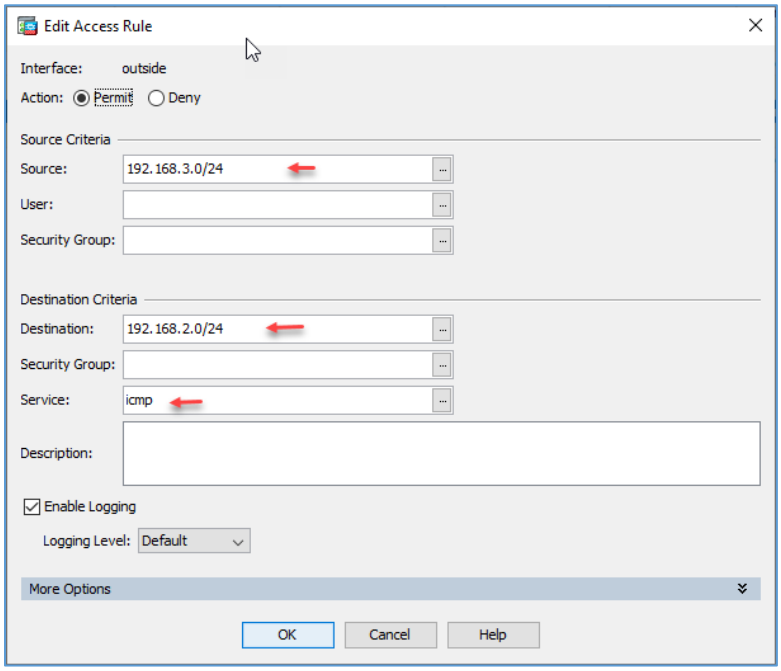
در قسمت Action باید Permit یا همان اجازه دادن را انتخاب کنید، در قسمت Source باید آدرس شبکه Inside همین فایروال را وارد کنید و در قسمت Dstionation باید آدرس شبکه خارجی که قرار است وارد شبکه Inside شود را وارد کنید منظور همان شبکه پشت فایروال ASA1 است و برای اینکه سرویس‌های دسترسی را محدود کنیم بهتر است موارد مورد نیاز را انتخاب کنیم که در قسمت Service گزینه‌ی ICMP را انتخاب و بر روی OK کلیک کنید.



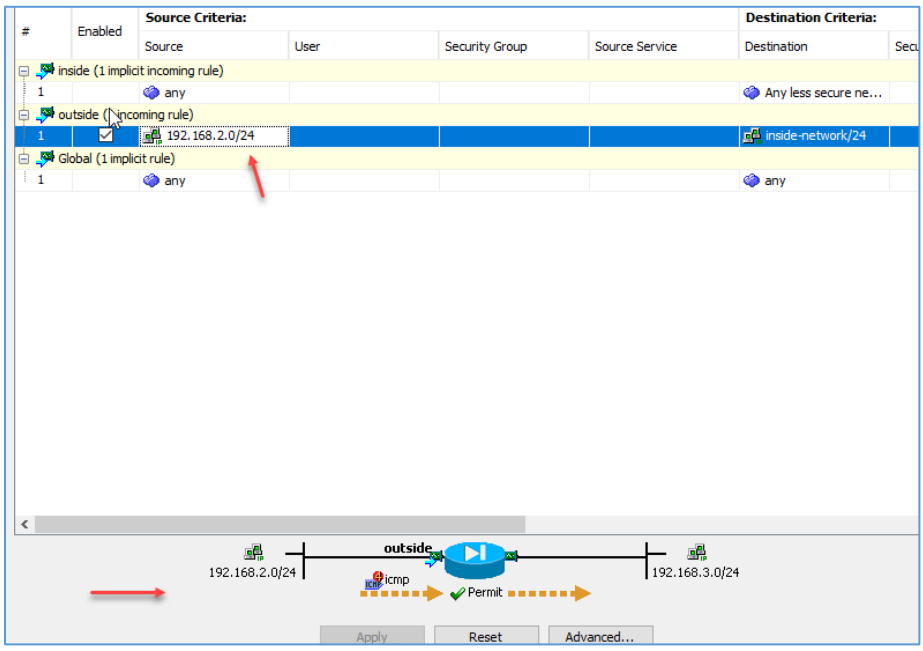
بعد از کلیک بر روی Apply دستورات مورد نظر را در شکل روبرو مشاهده خواهید کرد بعد از کلیک بر روی Send دستورات بر روی فایروال اعمال می‌شود.



توجه داشته باشید در بعضی موارد بعد از کلیک کردن بر روی Send با خطاهایی مواجه خواهید شد که این بخاطر پشتیبانی نکردن فایروال از بعضی دستورات است ولی مشکلی نیست و دستور اصلی بر روی فایروال اجرا خواهد شد، این موضوع را در شکل روبرو مشاهده می‌کنید، در کنار دستوراتی که تایید و اعمال شدند حرف OK نوشته شده است.

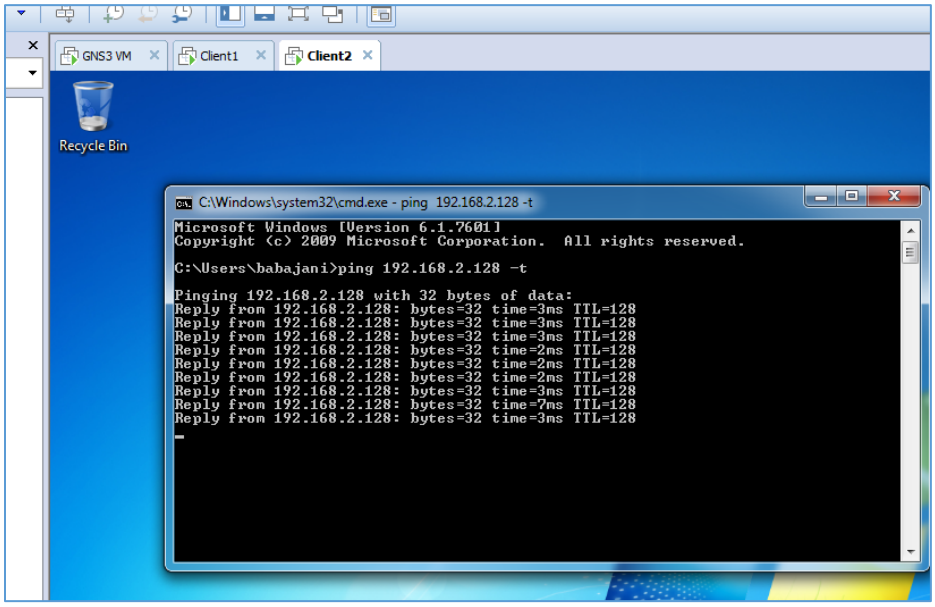


در فایروال ASA1 هم به مانند شکل روبرو تنظیمات را انجام دهید و آن را بر روی فایروال اعمال کنید، در این فایروال باید اجازه دسترسی شبکه 192.168.3.0 را به شبکه داخلی یعنی 192.168.2.0 بدهید.

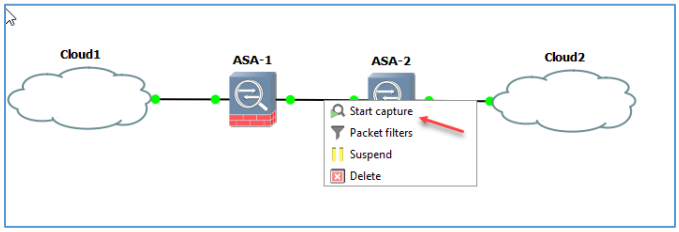


در این قسمت اگر بر روی Rule مورد نظر که ایجاد کردیم کلیک کنید در پایین صفحه آن به صورت گرافیکی نحوه ترافیک ورودی به فایروال مشخص شده است که در این شکل شبکه‌ی 192.168.2.0 اجازه ورود از طریق پورت Outside به داخل شبکه 192.168.3.0 را دارد که البته فقط و فقط سرویس ICMP دسترسی مورد نیاز را دارد و برای سرویس‌های دیگر باید دوباره Access-list تعریف کنید.

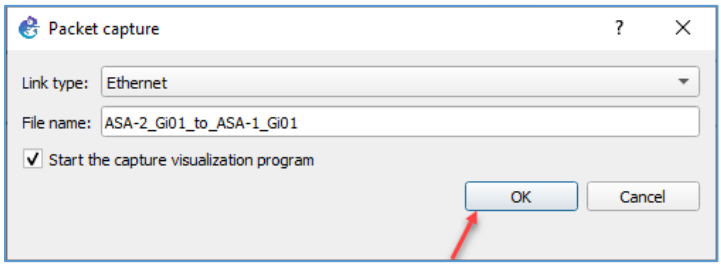
بعد از تنظیم RIP و Access-List باید بررسی کنید که ماشین Client همدیگر را Ping می‌دهند یا نه، که در شکل روبرو مشاهده می‌کنید که آدرس 192.168.2.128 توسط Client2 در دسترس است و برعکس آن هم امکان‌پذیر است، خوب همه چیز آماده است تا عملیات Site To Site VPN را از طریق ASDM بر روی فایروال‌ها اعمال کنیم.

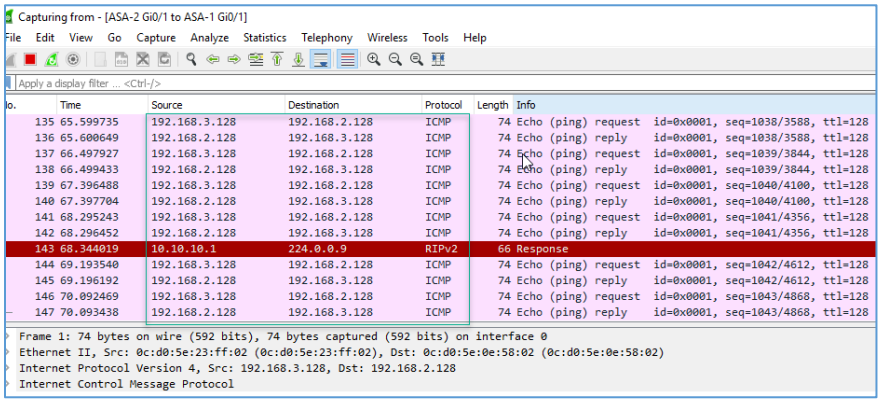


برای اینکه مزایای استفاده از VPN را بدانیم بهتر است قبل از فعال کردن آن لینک ارتباطی بین ASA1 و ASA2 را Capture کنیم تا ببینیم قبل و بعد از اعمال VPN چه تغییراتی انجام می‌شود، به خاطر همین موضوع بر روی خط میانی دو فایروال کلیک راست کنید و گزینه‌ی Start capture را انتخاب کنید.

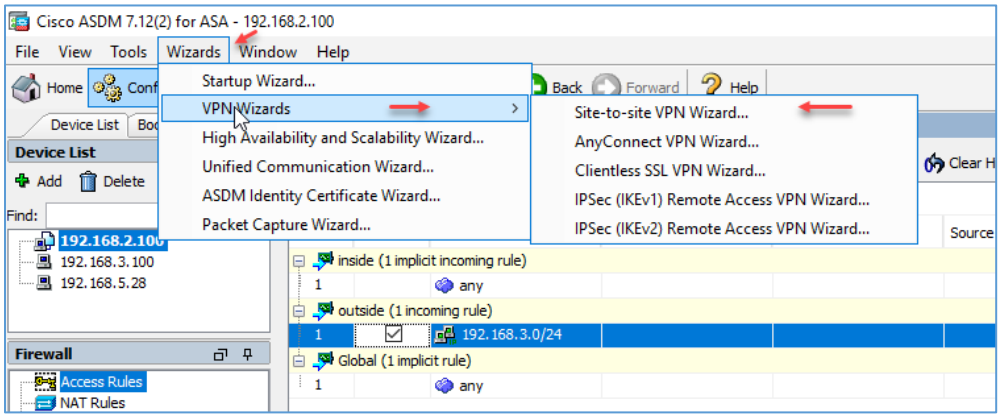


در این قسمت تیک گزینه‌ی مورد نظر را انتخاب کنید و بر روی OK کلیک کنید.

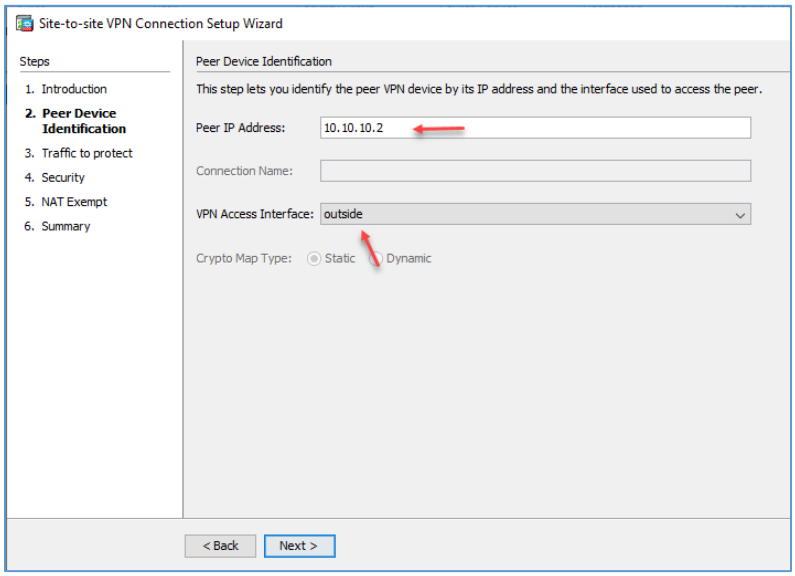




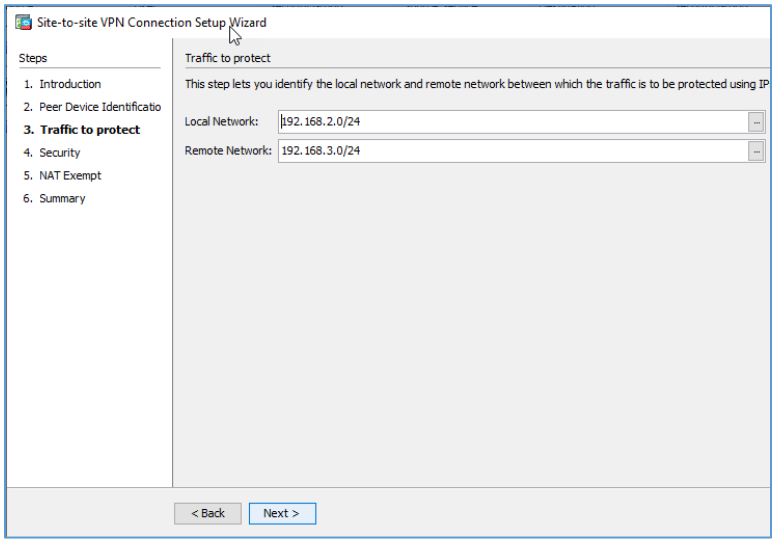
در شکل روبرو مشاهده می‌کنید که پروتکل‌هایی مانند ICMP به راحتی قابل Capture شدن است و اگر یک رمزی هم بین آنها قرار بگیرد به راحتی قابل شناسایی است، برای حل این مسائل امنیتی باید VPN بین دو فایروال راه بندازیم.



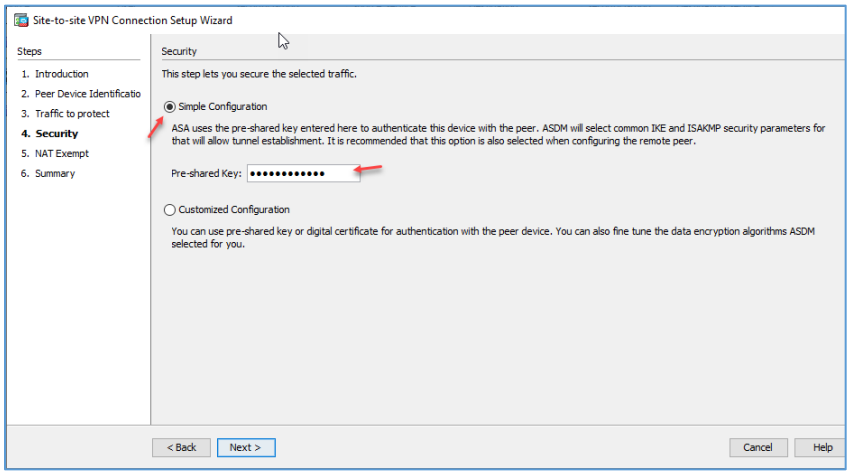
وارد ASDM مربوط به روتر ASA1 شوید و از منوی Wizards و از قسمت VPN Wizards گزینه‌ی Site-to-site VPN Wizard را انتخاب کنید.



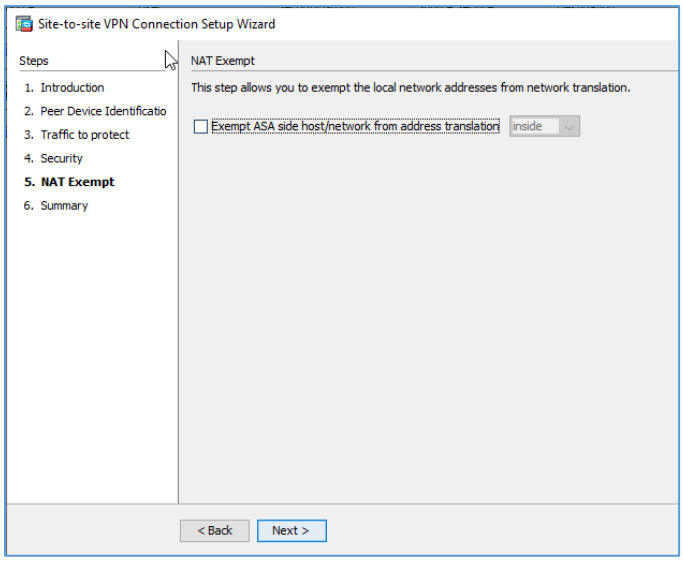
در این صفحه باید در قسمت Peer IP Address آدرس فایروال روبرویی را که در این سناریو 10.10.10.2 است را وارد کنید و در قسمت VPN Access Interface باید خروجی را Outside انتخاب کنید.



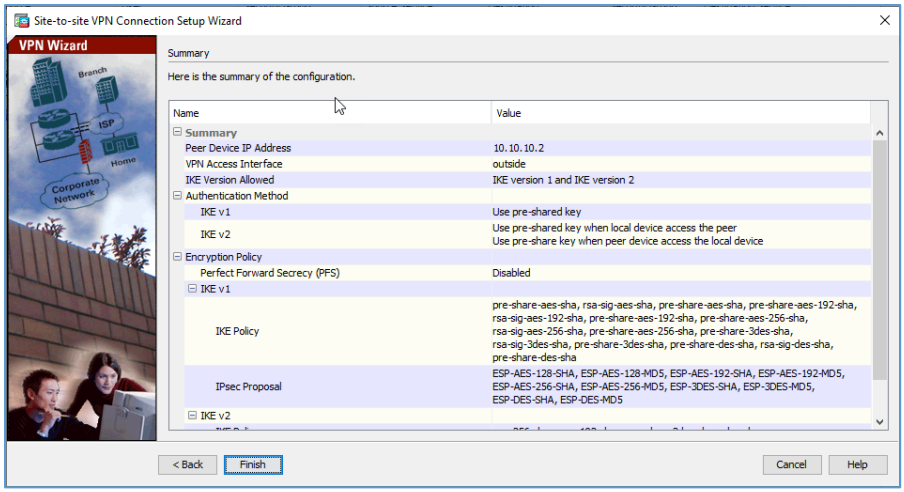
در این صفحه و در قسمت Local Network باید شبکه داخلی فایروال که به طرف Inside است را وارد کنید و در قسمت Remote Network باید شبکه داخلی فایروال روبرو یعنی ASA2 را وارد کنید.



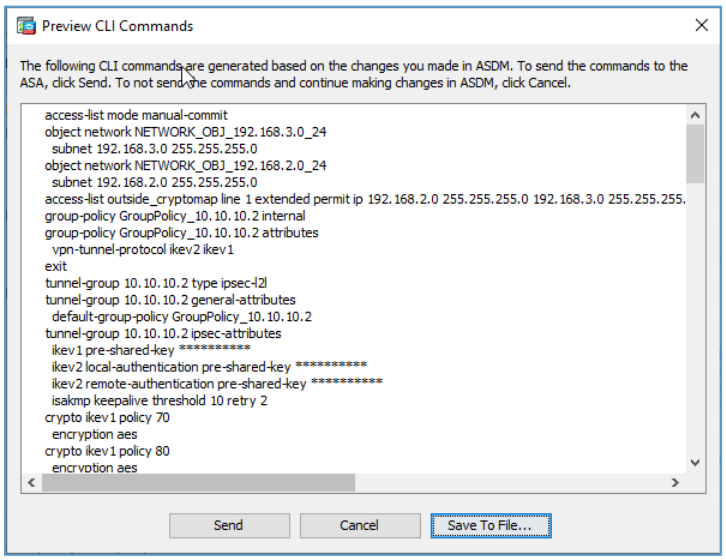
در این صفحه گزینه‌ی اول را انتخاب کنید و یک رمز عبور خوب و به دلخواه وارد کنید، توجه داشته باشید از این رمز باید در فایروال دومی هم استفاده کنید تا ارتباط به درستی برقرار شود، در گزینه‌ی Customized گزینه‌های پیشرفته‌تری هم وجود دارد مثلاً استفاده از گواهینامه‌های امنیتی بین دو فایروال و...



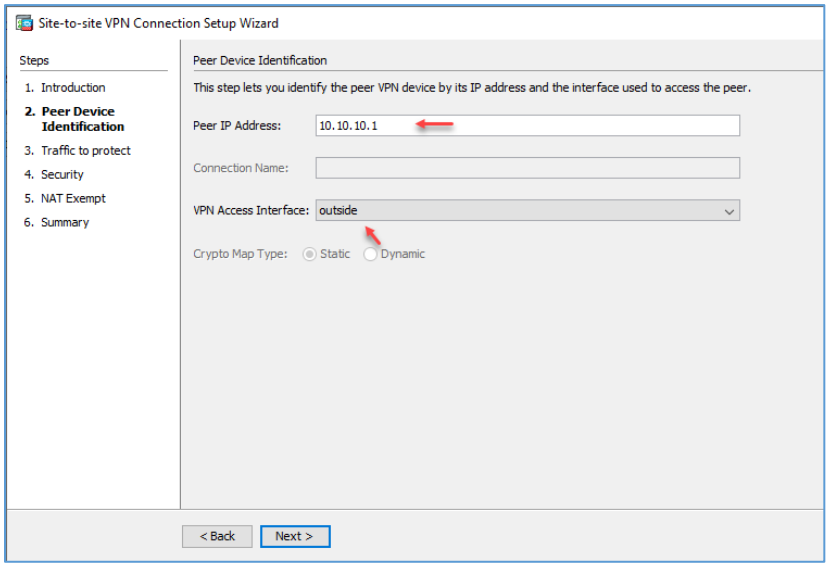
در این قسمت هم اگر در شبکه خود از پروتکل NAT استفاده می‌کنید برای عبور از فایروال حتماً باید تیک گزینه‌ی مورد نظر را انتخاب کنید که در این قسمت نیازی به این کار نیست.



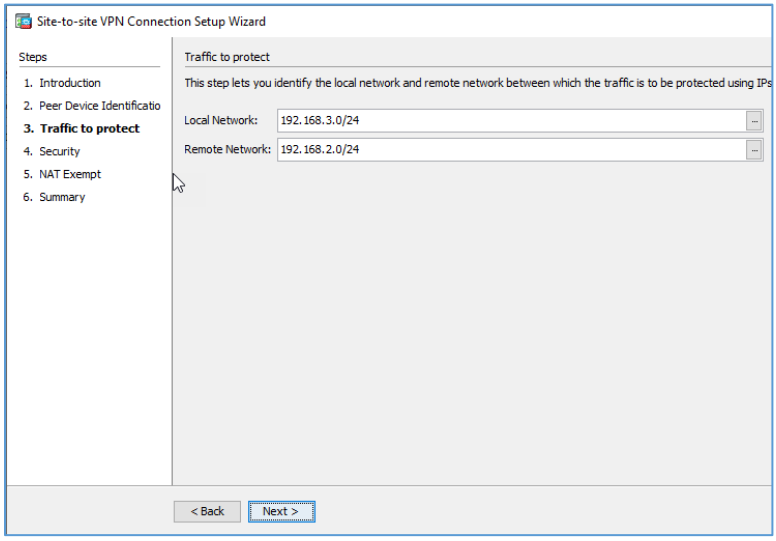
تنظیمات نهایی را مشاهده می‌کنید که با کلیک بر روی Finish تنظیمات اعمال خواهد شد.



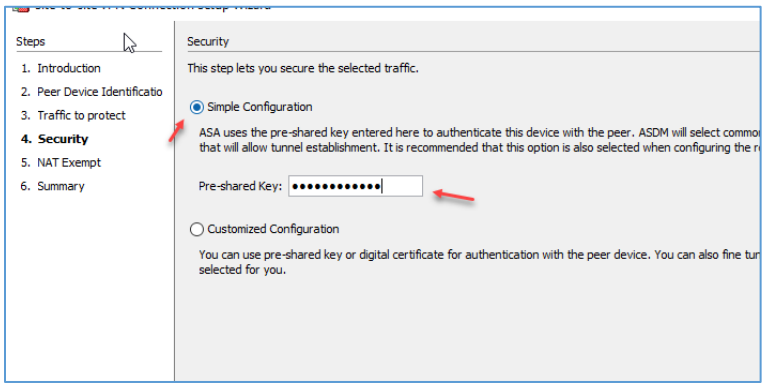
در این صفحه کل دستورات این عملیات مشخص شده است که با کلیک بر روی Send دستورات اعمال می‌شود، توجه داشته باشید برای اینکه این تنظیمات را در مکانی دیگر ذخیره کنید باید بر روی Save To File کلیک کنید، اگر بعد از کلیک بر روی Send با چند خطا مواجه شدید به آن توجه نکنید و پنجره‌ها را ببندید.



بعد از اعمال دستورات در ASA1 باید همین دستورات را در ASA2 پیاده‌سازی کنیم به مانند شکل روبرو در قسمت Peer IP Address باید آدرس فایروال روبرویی یعنی ASA1 را وارد و Interface آن را Outside در نظر می‌گیریم.

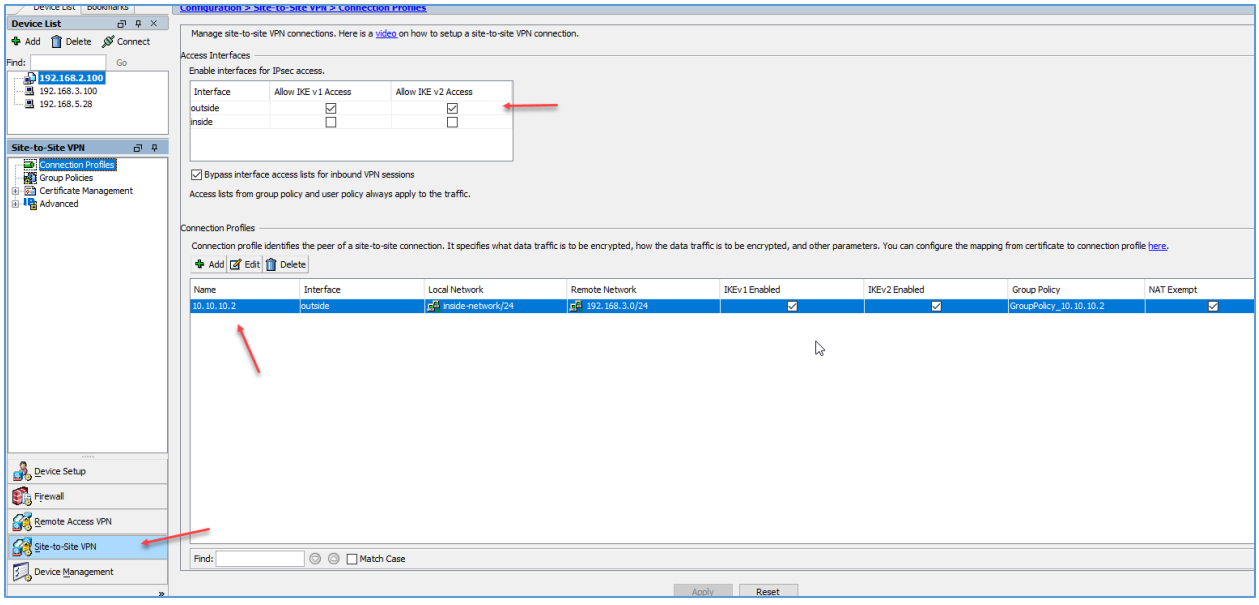


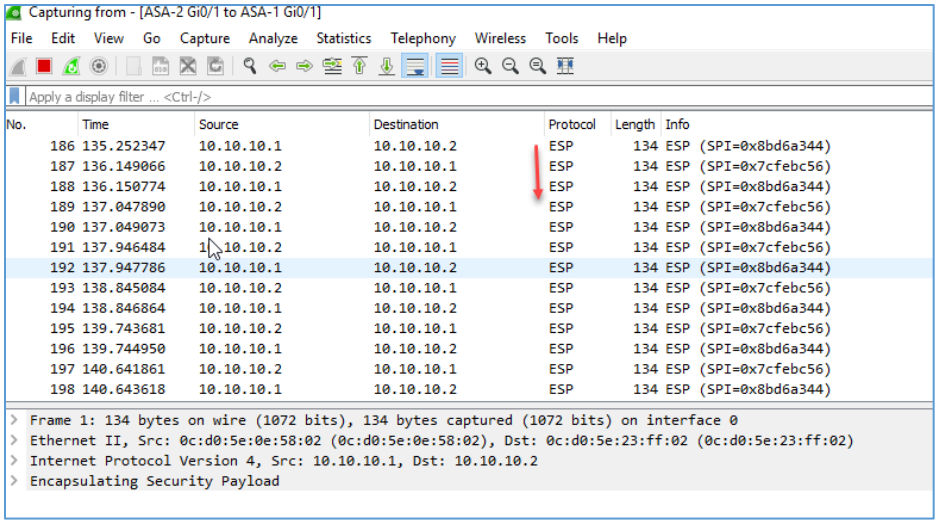
در این قسمت باید شبکه داخلی و شبکه فایروال دوم را وارد کنید که در شکل روبرو مشخص شده است.



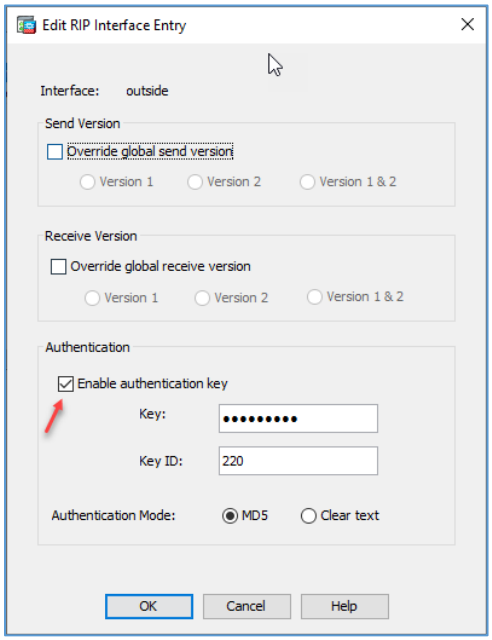
در این قسمت باید رمزی را که در ASA1 وارد کردید را در این قسمت هم دقیقاً همان را وارد کنید تا ارتباط بین دو فایروال انجام شود.

به مانند شکل زیر اگر وارد قسمت Site-to-site VPN شوید، پروفایل ایجاد شده برای ارتباط Site-to-Site را مشاهده خواهید کرد.

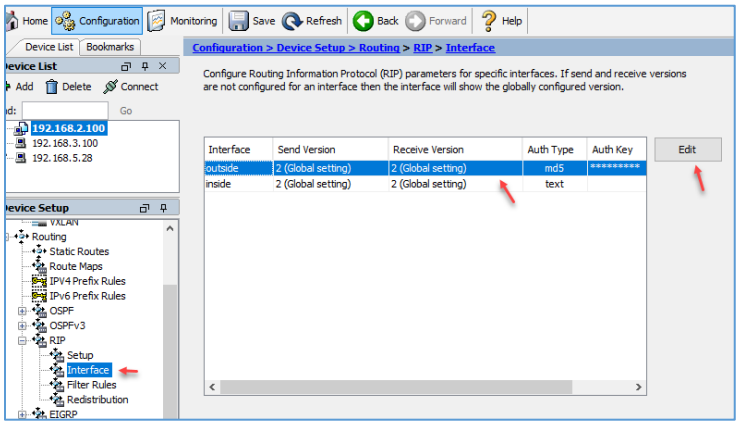




اگر دوباره وارد Wireshark شوید مشاهده می‌کنید که پروتکل و آدرس IP به نسبت قبل تغییر کرده است و پروتکل ESP جای آن را گرفته است و تمام ارتباطات به صورت رمز شده در آمده.



نکته‌ای که در پروتکل RIP آن را فراموش کردیم این است که بهتر است در زمان راه‌اندازی RIP رمز عبوری بین دو شبکه RIP ایجاد کنید که برای این کار باید در قسمت RIP وارد Interface شوید و خروجی Outside را انتخاب و بر روی Edit کلیک کنید، در شکل روبرو باید در قسمت Authentication تیک گزینه‌ی Enable authentication key را انتخاب کنید و رمز عبور که عدد یا حرف باشد را وارد و یک ID برای آن در نظر بگیرید و همین اطلاعات را در فایروال دوم هم وارد و تنظیمات را اعمال کنید.



البته در شبکه‌های واقعی که با سیسکو کار می‌کنید بهتر است از پروتکل مسیریابی EIGRP که از امنیت بالاتری برخوردار است استفاده کنید و یا اینکه از Static Route استفاده کنید.

یک دستور کاربردی در Command line می‌توانید استفاده کنید تا دستوراتی را که وارد کردید به راحتی و مختصر مشاهده کنید برای این کار باید از دستور زیر استفاده کنید.

Show Running-config | include access-list

با استفاده از دستور بالا می‌توانید لیست دستوراتی که در آنها access-list به کار رفته را مشاهده کنید که در زیر این موضوع مشخص شده است، در شکل زیر دو access-list مشاهده می‌کنید که یکی را خودمان برای سرویس ICMP فعال کردیم و دیگری هم در زمان ایجاد Site-to-Site VPN ایجاد شده است.

```
ASA1(config)# show running-config | include access-list
access-list outside_access_in extended permit icmp 192.168.3.0 255.255.255.0 192
.168.2.0 255.255.255.0
access-list outside_cryptomap extended permit ip 192.168.2.0 255.255.255.0 192.1
68.3.0 255.255.255.0
threat-detection statistics access-list
ASA1(config)# _
```

کار با AnyConnect VPN در ASDM

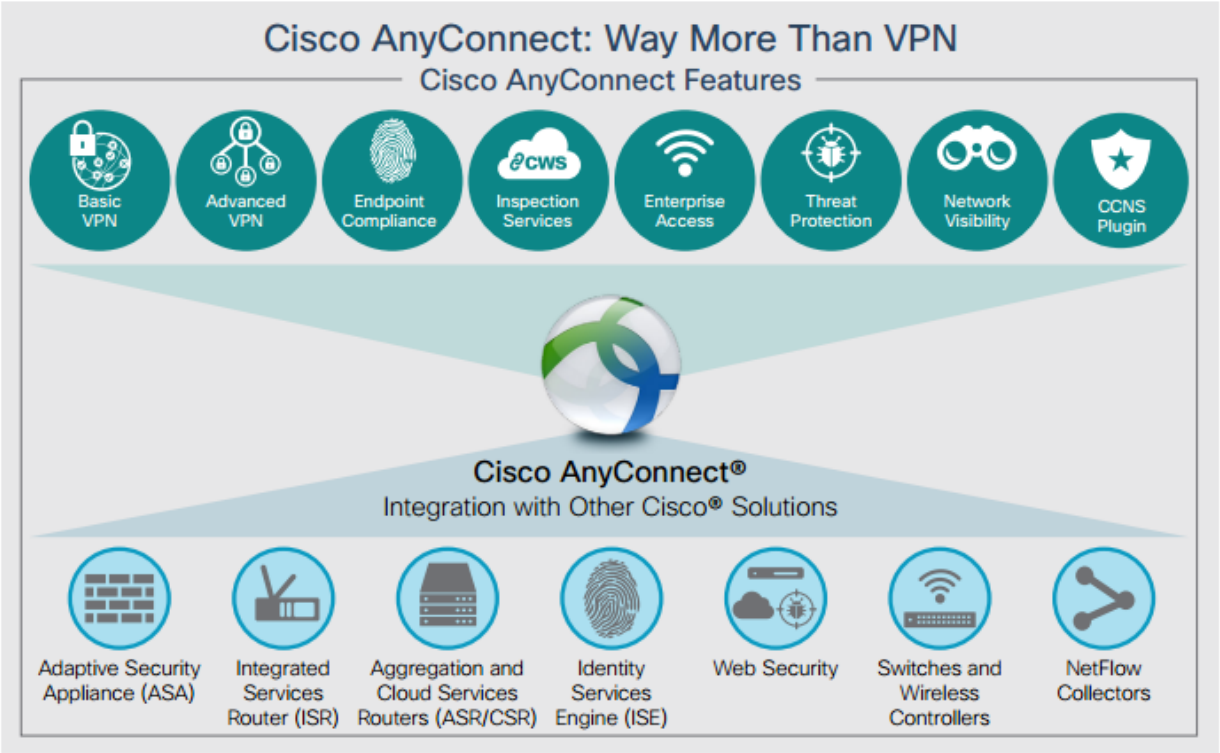
در نظر بگیرید کارمندان یک سازمان به صورت دوره‌کاری از سرتاسر دنیا قرار است به شبکه داخلی شما متصل شوند و از منابع آن استفاده کنند، این موضوع نیاز به این دارد که امنیت و سرعت آن را تضمین کنید، به خاطر همین موضوع شرکت سیسکو از VPN با نام AnyConnect استفاده کرده است که این امر را تحقق می‌بخشد.

در کنار اینکه شما با استفاده از AnyConnect به شبکه داخلی سازمان خود Remote می‌زنید می‌توانید از دیگر ویژگی‌های امنیتی آن هم استفاده کنید

شعار سیسکو برای این نرم‌افزار این است که به هر نوع دستگاهی در هر زمان و از هر مکان یک دسترسی ایمن و قابل اطمیان دهید.

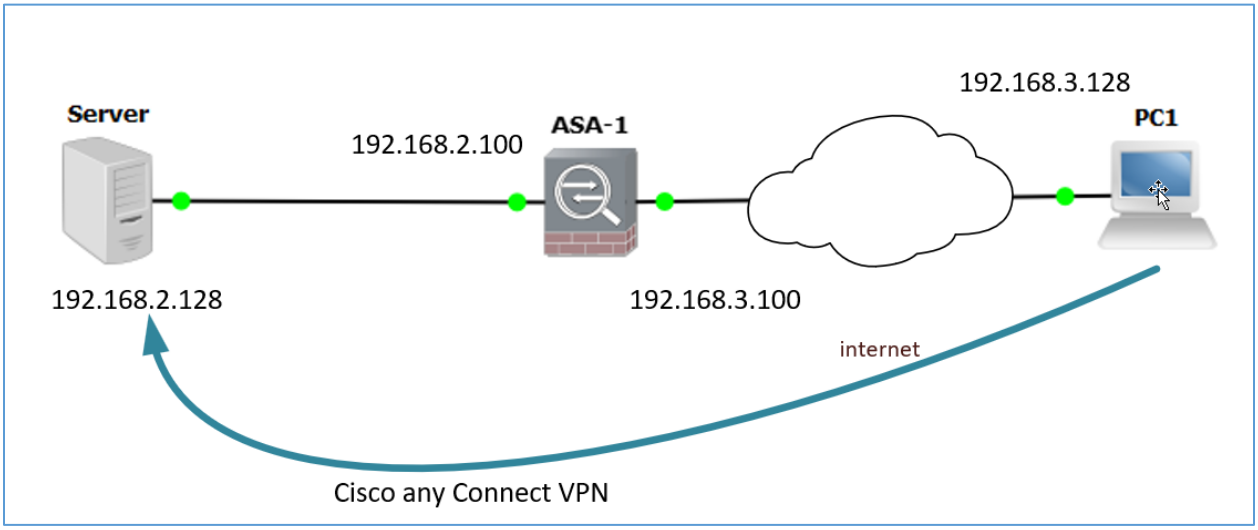
یکی از ویژگی‌های مهم Anyconnect متصل شدن به نرم‌افزار ACS و ISE است و با این کار در چندین مرحله کاربران احراز هویت و شناسایی می‌شوند.

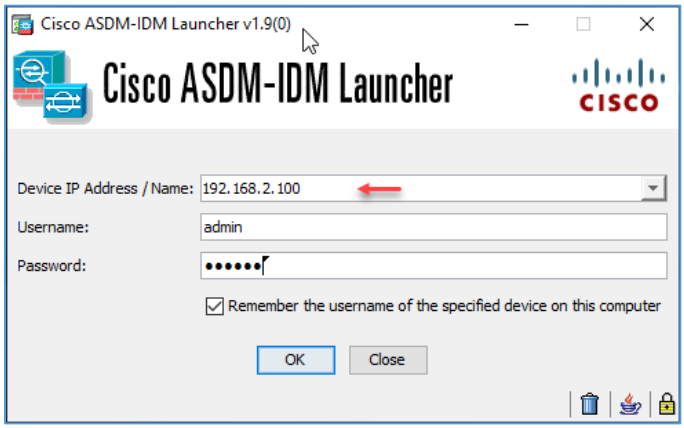
در زیر ویژگی‌های مهم AnyConnect را مشاهده می‌کنید که واقعاً قابل تامل است.



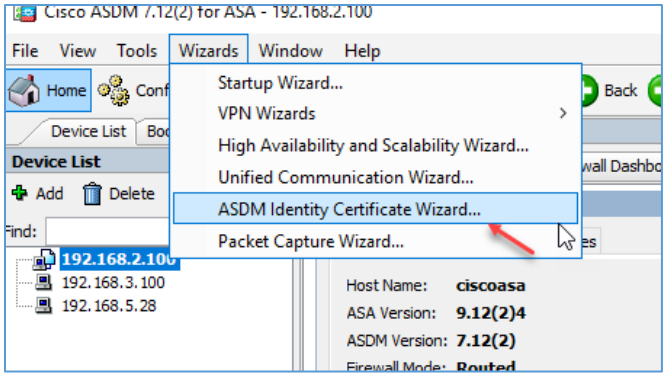
در شکل زیر یک ASA سیسکو به همراه یک سرور و یک کلاینت را مشاهده می‌کنید که Server در شبکه داخلی قرار دارد و PC1 در شبکه outside یا خارجی، می‌خواهیم سرویس Anyconnect را در ASA راه‌اندازی کنیم تا PC1 بتوانید با VPN به شبکه inside یا همان شبکه 192.168.2.0 دسترسی پیدا کند.

نکته: تنظیماتی که در این قسمت برای ارتباط دستگاه‌ها قرار دادیم دقیق همان تنظیماتی است که در قسمت قبل و در Site to Site VPN انجام دادیم با این تفاوت که در این قسمت یک دستگاه ASA قرار دارد و سروری که در شبکه Inside قرار دارد یک ویندوز سرور ۲۰۱۲ است که بر روی Vmware Workstation فعال شده است و از طریق کارت شبکه VMnet2 به این Cloud متصل شده است، منظور از Cloud همین سرور است که آیکون آن را از ابر به سرور تغییر دادیم، قرار است که Pc1 بتواند بعد از ارتباط anyconnect یک وب سایت را در سرور باز کند.

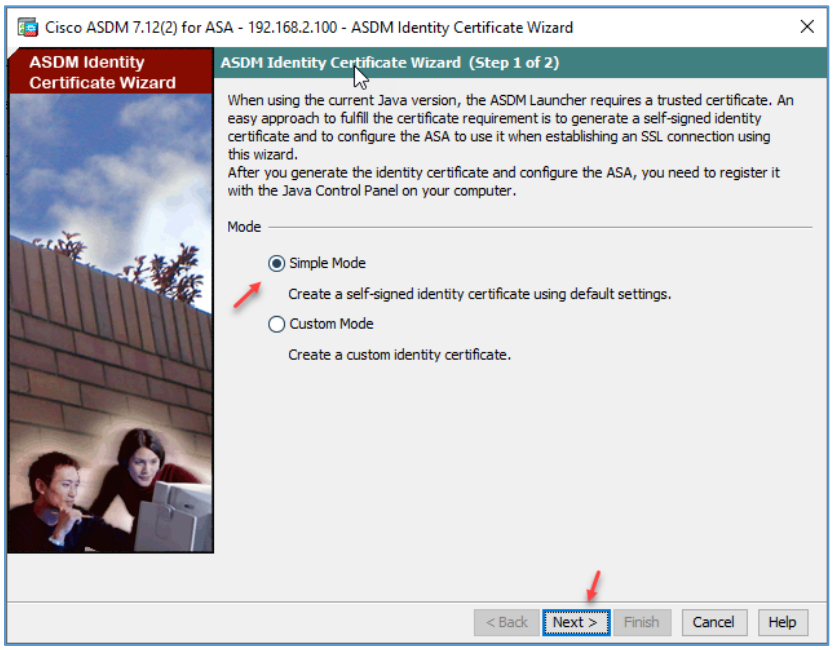




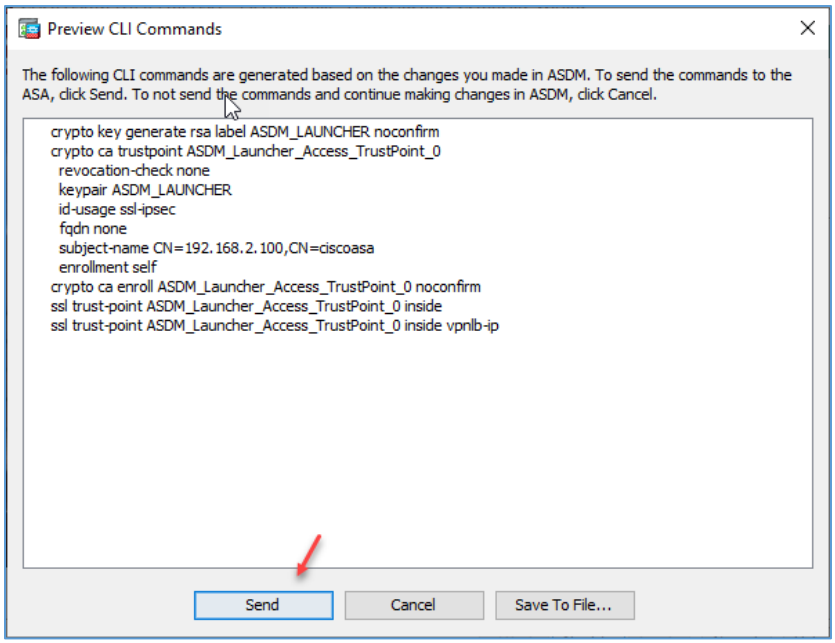
بعد از انجام تنظیمات در فایروال ASA-1 باید از طریق ASDM به آن متصل شویم که از طریق آدرس 192.168.2.100 که بر روی Inisde ست شده است این کار را انجام می‌دهیم.



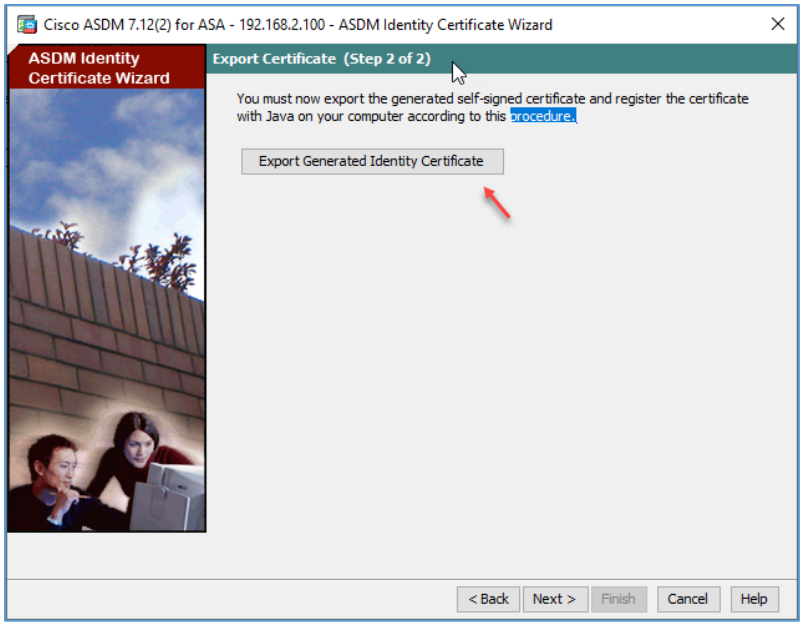
بعد از ورود به ASDM از طریق منوی Wizards گزینه‌ی ASDM identity Certificate Wizard را انتخاب کنید.



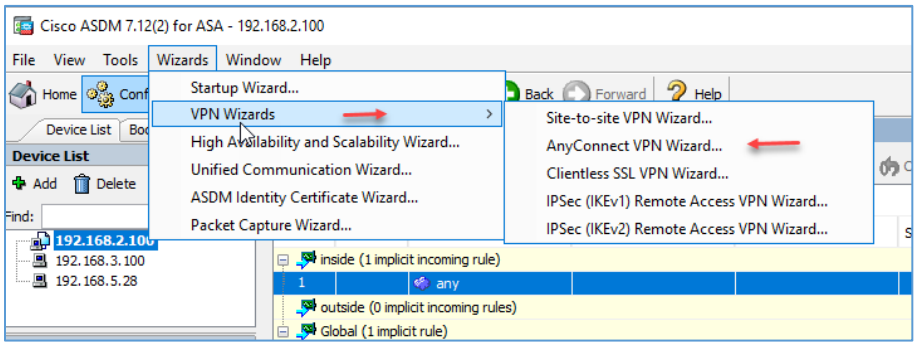
در این قسمت گزینه‌ی simple Mode را انتخاب کنید.



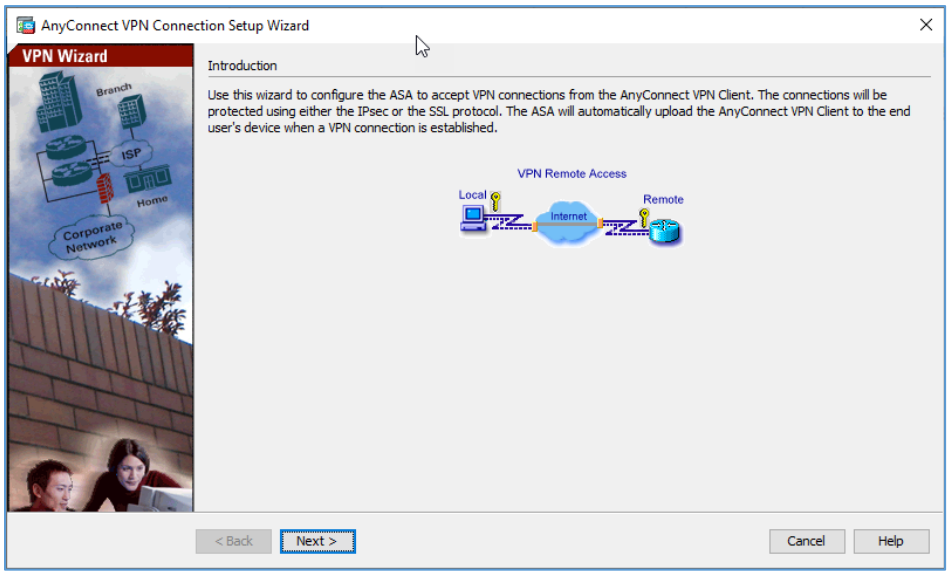
در این صفحه دستوراتی که برای این عملیات مورد نیاز است مشخص شده است، که با کلیک بر روی Send دستورات بر روی فایروال اعمال می‌شود.



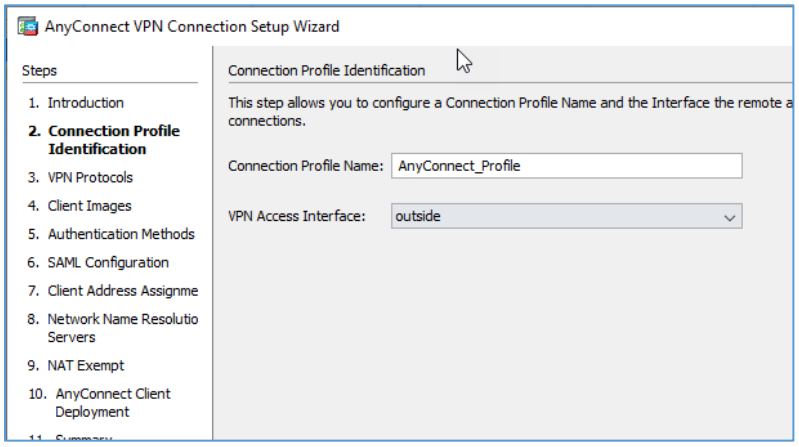
در این صفحه هم می‌توانید با کلیک بر روی گزینه‌ی مورد نظر از CA یا همان Certificate ایجاد شده یک Export تهیه کنید.



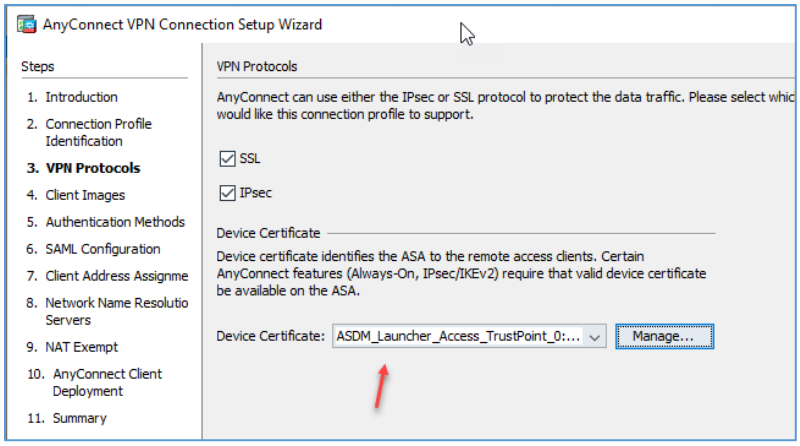
بعد از انجام مراحل بالا وارد منوی Wizards شوید و از قسمت VPN Wizards گزینه‌ی AnyConnect VPN Wizard را انتخاب کنید.



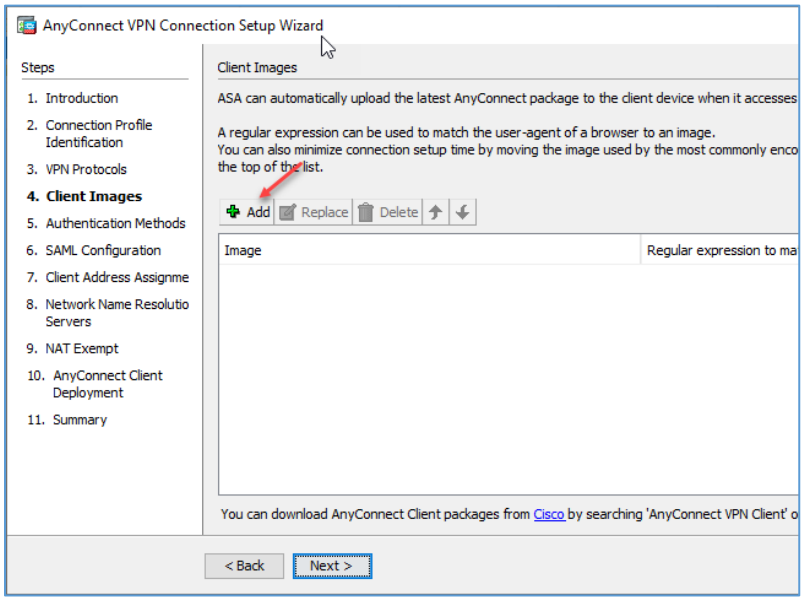
در صفحه اول نحوه ارتباط بین شبکه داخلی و خارجی مشخص با شکل مشخص شده است، بر روی Next کلیک کنید.



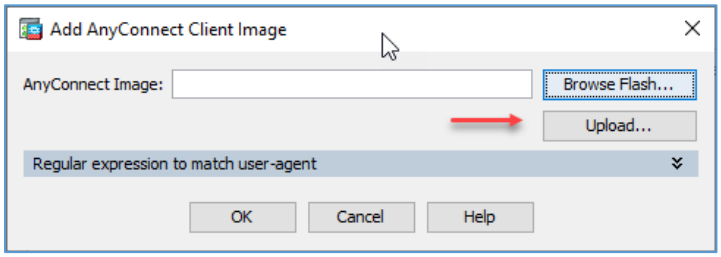
در این صفحه باید یک نام برای Profile خود وارد کنید و در قسمت VPN Access Interface باید مشخص کنید که سرویس VPN بر روی کدام پورت اجازه کار داشته باشد که در اینجا پورت outside که شبکه خارجی است انتخاب شده است.



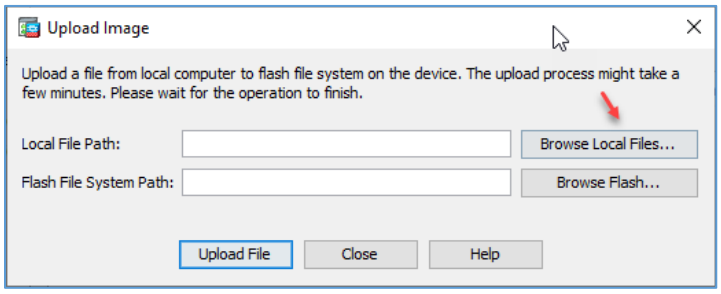
در این قسمت باید تیک هر دو گزینه را انتخاب کنید تا امنیت کار هم از طریق گواهی‌نامه‌ی SSL و هم از طریق IPsec چک شود، در قسمت Device Certificate باید همان گواهینامه‌ای که در قسمت اول این بحث ایجاد کردید را انتخاب و بر روی Next کلیک کنید.



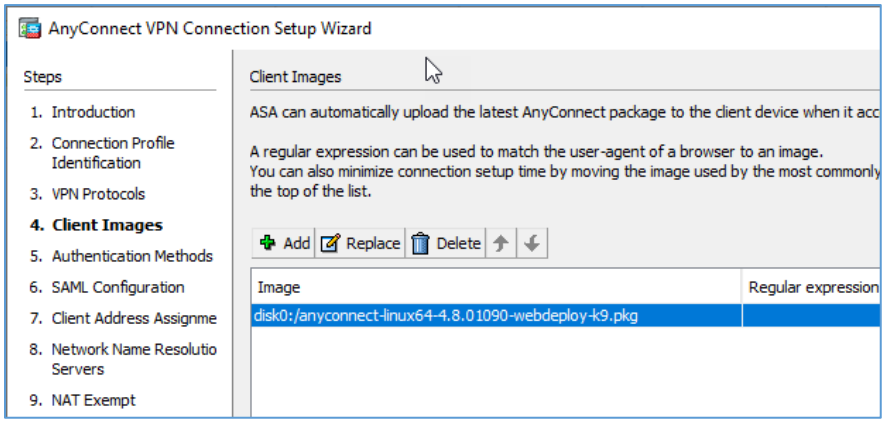
در این قسمت باید آخرین پکیج AnyConnect را از سایت سیسکو دانلود و به نرم‌افزار معرفی کنید، فایل Anyconnect باید با پسوند pkg باشد که اگر موفق نشدید آن را از سایت Cisco دانلود کنید؛ می‌توانید از این قسمت دانلود کنید، بعد از دانلود بر روی Add کلیک کنید.



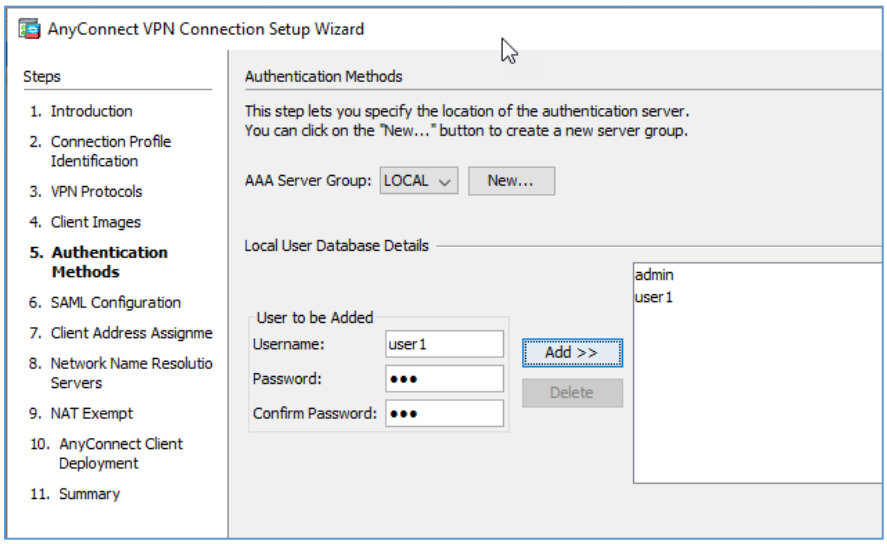
چنانچه فایل از قبل در حافظه Flash دستگاه فایروال موجود باشد باید بر روی Browse Flash کلیک کنید و اگر هم فایل را دانلود کردید بر روی Upload کلیک کنید.



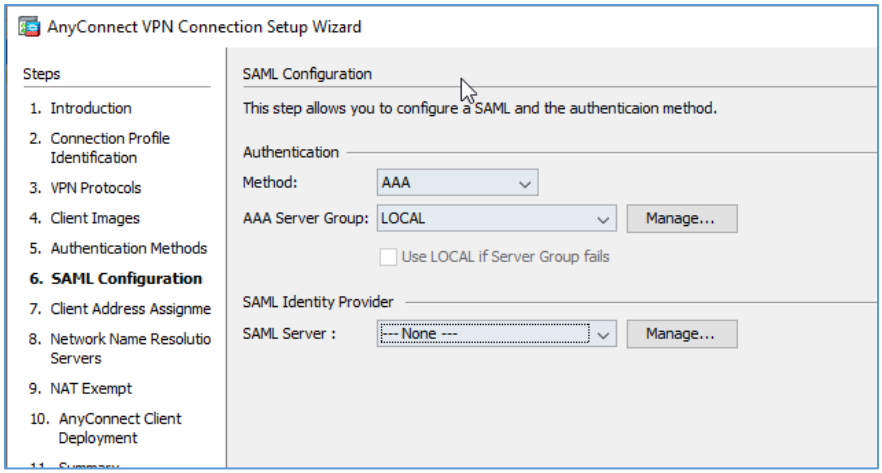
در این قسمت بر روی Browse Local Files کلیک کنید و فایل مورد نظر را انتخاب و Upload کنید.



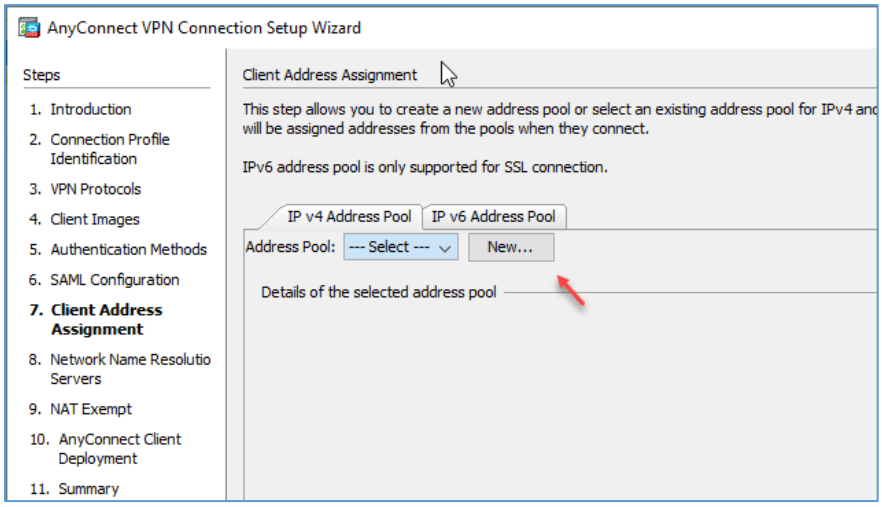
همانطور مشاهده می‌کنید فایل (anyconnect-win-4.8.01090-webdeploy-k9.pkg) آپلود و به لیست اضافه شده است، برای ادامه کار بر روی Next کلیک کنید.



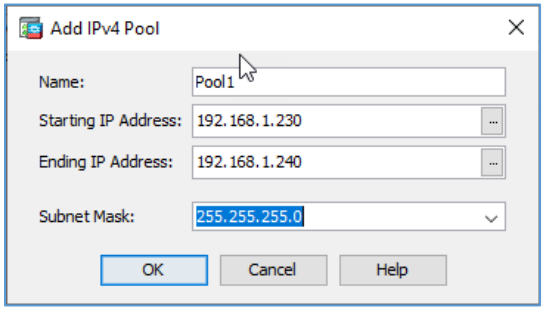
در این قسمت اگر از سرور ACS یا ISE برای بحث احراز هویت استفاده می‌کنید می‌توانید بر روی New کلیک کنید و آدرس سرور را با تنظیمات آن وارد کنید، در غیر این صورت باید نام کاربری و رمز عبور داخلی فایروال را انتخاب کنید، البته در پائین صفحه می‌توانید کاربر دلخواه خود را اضافه یا حذف کنید، توجه داشته باشید کاربر Admin که از قبل ایجاد کرده بودیم در لیست وجود دارد.



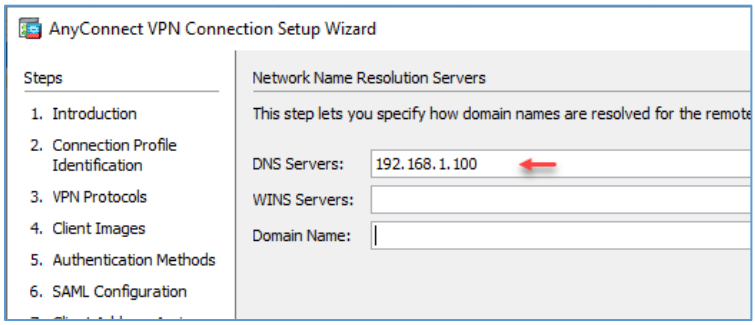
در این صفحه اگر سرور Authentication یا همان احراز هویت داخلی دارید گزینه‌ی Local را انتخاب کنید و یا اگر از سرور خارجی مانند ACS استفاده می‌کنید باید گزینه را تغییر دهید.



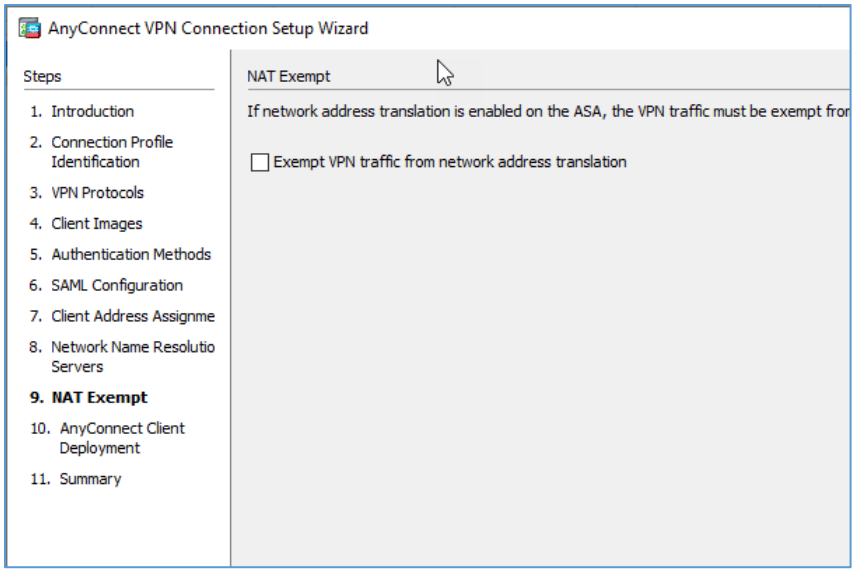
در این صفحه باید یک Pool یا یک رنج IP برای کلاینت‌هایی که می‌خواهند با VPN به شبکه داخلی متصل شوند ایجاد کنید، برای این کار در قسمت IPV4 بر روی New کلیک کنید.



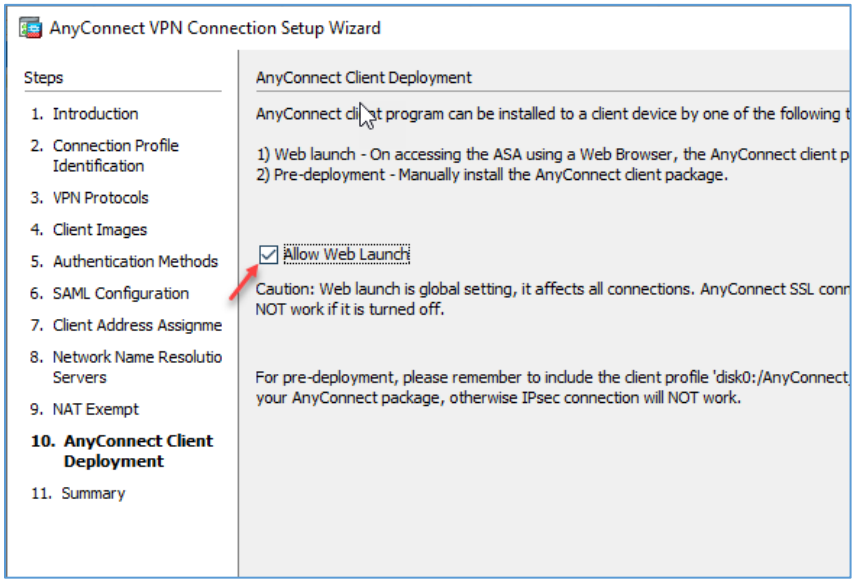
نام، رنج IP و Subnet را برای این Pool مشخص کنید، زمانی که کاربران از AnyConnect برای متصل شدن استفاده کنند یکی از این آدرس‌ها به صورت اتوماتیک به آنها اختصاص داده می‌شود.



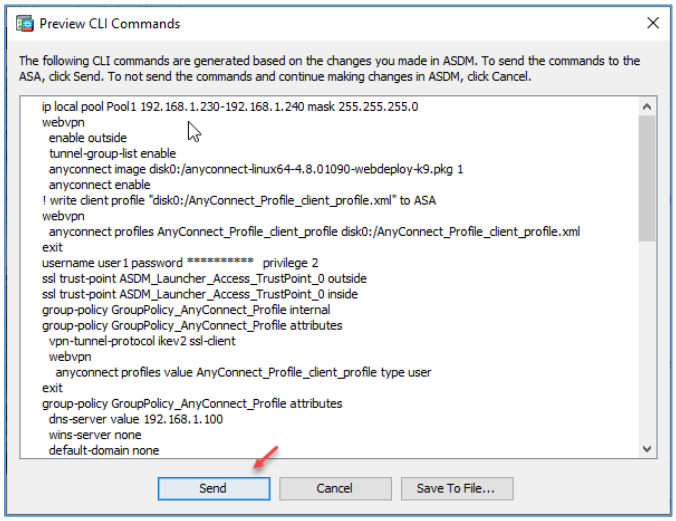
در این صفحه باید آدرس DNS, WINS و نام Domain را مشخص کنید.



در این صفحه اگر از پروتکل NAT در فایروال خود استفاده می‌کنید برای تبدیل آدرس باید تیک گزینه‌ی مورد نظر را انتخاب کنید تا کارایی آن حفظ شود.

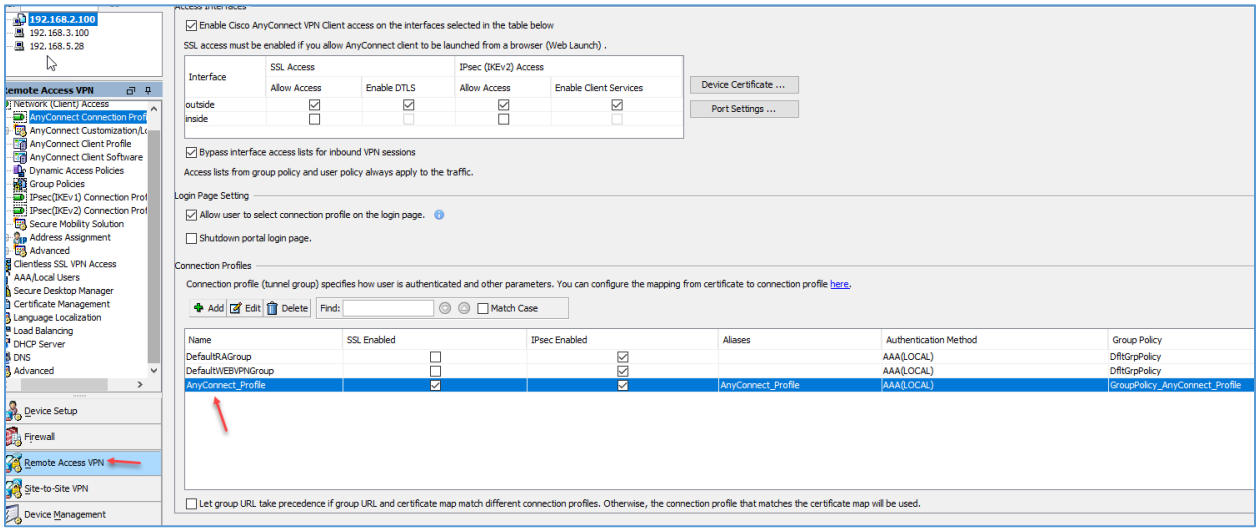


در این قسمت برای اینکه به نرم‌افزار Anyconnect برای کلاینت‌ها دسترسی داشته باشیم می‌توانیم تیک گزینه‌ی Allow Web Launch را انتخاب کنید، بر روی Next کلیک کنید.

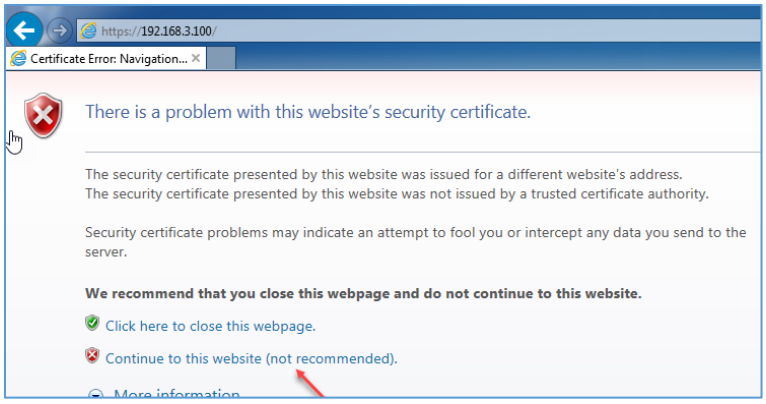


در صفحه آخر اگر بر روی Finish کلیک کنید، دستورات نهایی به مانند شکل روبرو ظاهر می‌شوند و با کلیک بر روی Send روی فایروال اعمال می‌شوند.

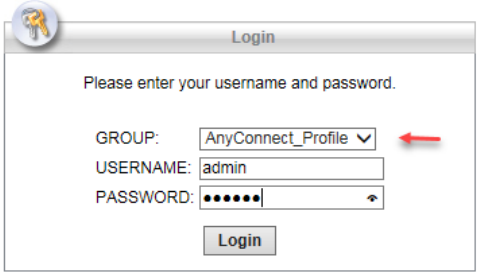
همانطور که در شکل زیر مشاهده می‌کنید پروفایل مورد نظر برای دسترسی کلاینت‌ها ایجاد شده است و همه چیز برای اتصال کلاینت به فایروال از طریق VPN امکان پذیر است.

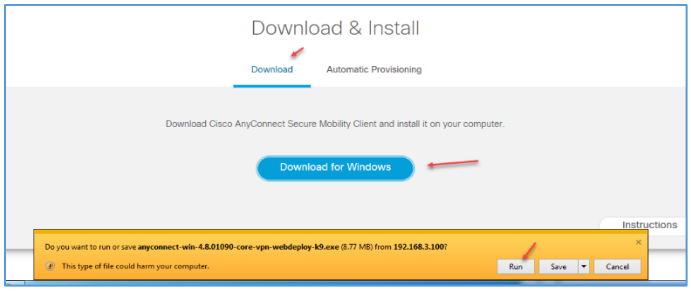


در ادامه باید وارد کلاینت (PC1) شویم و AnyConnect را تست بگیریم، همانطور که گفتیم برای اینکه به نرم‌افزار AnyConnect دسترسی داشته باشیم دو راه وجود دارد یکی اینکه از اینجا فایل (anyconnect-win-4.8.01090-predeploy-k9.zip) را دانلود و بر روی کلاینت نصب کنید و یا اینکه یک مرورگر باز کنید و آدرس پورت outside که 192.168.3.100 است را در مرورگر به صورت https://192.168.3.100 وارد کنید که در شکل روبرو این موضوع را مشاهده می‌کنید با وارد شدن به آدرس فایروال صفحه روبرو ظاهر می‌شود که باید بر روی Continue to this website کلیک کنید تا از گواهینامه امنیتی نامعتبر آن صرفنظر کند.



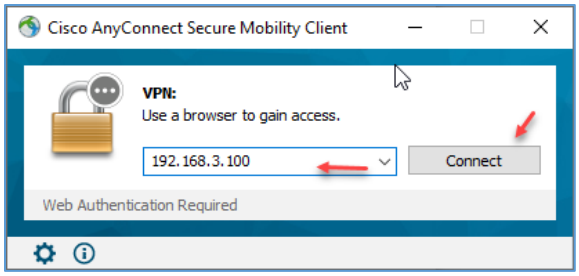
در صفحه بعد که در شکل روبرو مشاهده می‌کنید باید پروفایلی را که در قسمت قبل ایجاد کردیم را انتخاب و نام کاربری و رمز عبور تعریف شده در فایروال را وارد و بر روی Login کلیک کنید.





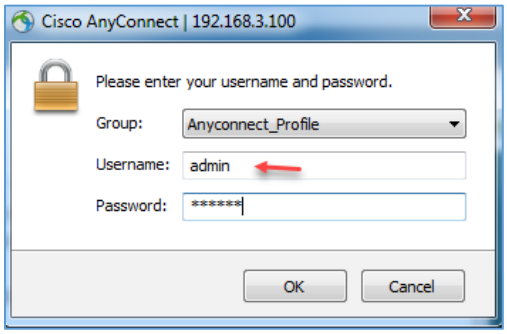
بعد از ورود با این صفحه روبرو خواهید شد که باید وارد تب Download شوید و بر روی Download for Windows کلیک کنید و در نوار باز شده بر روی Run کلیک کنید و آن را نصب کنید.

نکته: در زمان راه‌اندازی AnyConnect باید فایل‌های مربوط به Any Connect که برای ورژن‌های مختلف از سیستم‌عامل است را در فایروال آپلود کنید تا زمانی که در دستگاه‌های مختلف این آدرس سایت را باز می‌کنید ورژن مخصوص به آن برای شما باز شود.

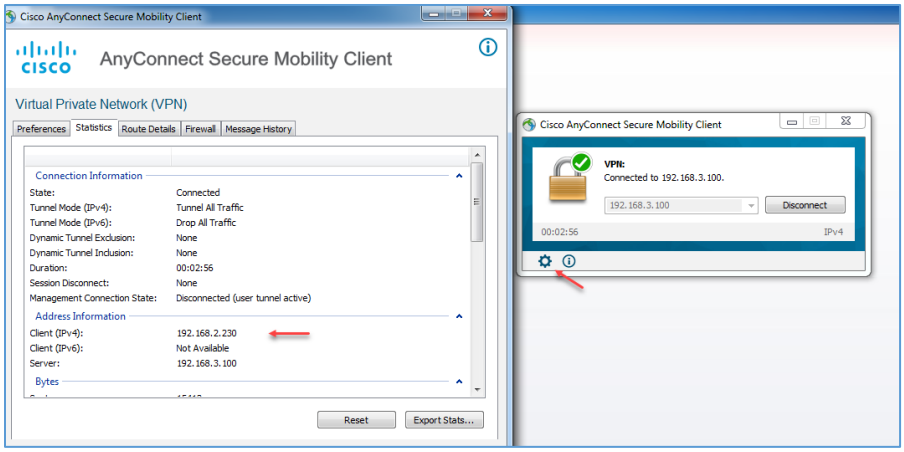


بعد از نصب، آن را اجرا کرده و به مانند شکل روبرو آدرس outside فایروال را که در اینجا 192.168.3.100 است را وارد کنید و بر روی Connect کلیک کنید.

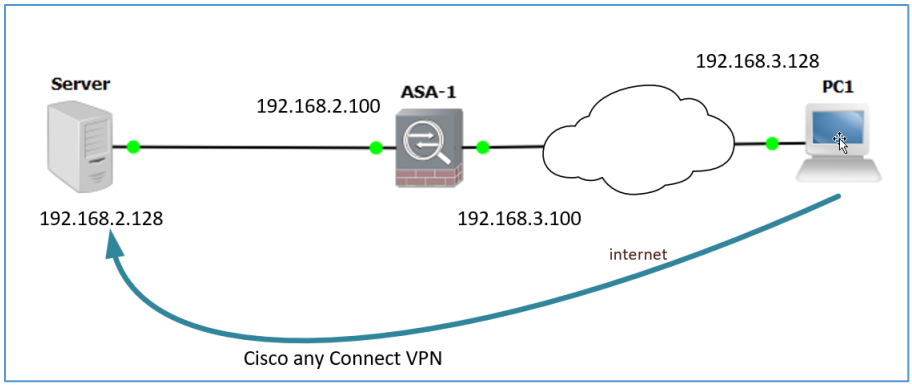
در هنگام Connect به علت معتبر نبودن Certificate با اخطار روبرو مواجه خواهید شد که باید بر روی Connect Anyway کلیک کنید.



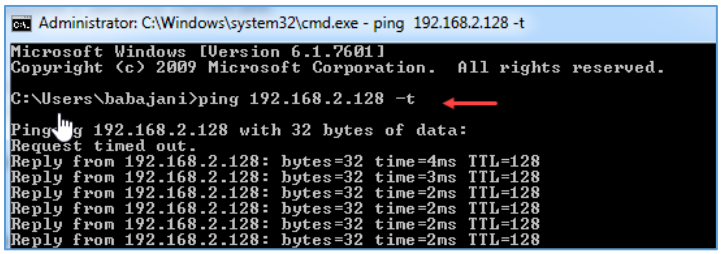
در این قسمت باید پروفایل مورد نظر خود را انتخاب و نام کاربری و رمز عبور تعریف شده را وارد و بر روی OK کلیک کنید.



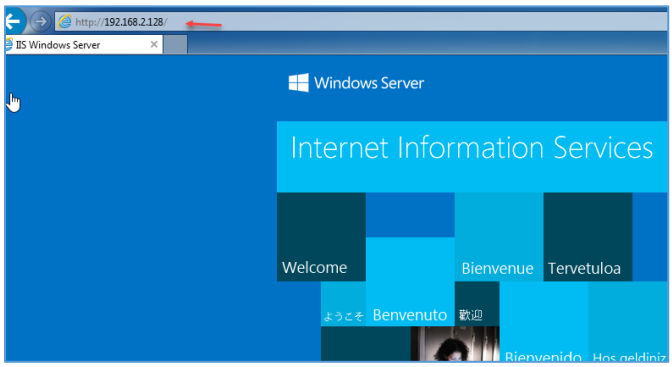
همانطور که مشاهده می‌کنید VPN متصل شده است و برای اینکه جزئیات آن را مشاهده کنید باید بر روی آیکون مورد نظر کلیک کنید، در تب Statistics آدرس IP، مقدار زمان متصل بود و بقیه جزئیات نوشته شده است.



به سناریو خود باز می‌گردیم در این سناریو توانستیم از طریق PC1 با استفاده از AnyConnect VPN به فایروال ASA-1 متصل شدیم و حالا باید شبکه 192.168.2.0 را مشاهده کنیم، برای اینکه بیشتر با کار آشنا شوید، بر روی سرور با آدرس 192.168.2.128 سرویس IIS راه‌اندازی کردیم و می‌خواهیم از طریق PC1 سایت سرور را باز کنیم.

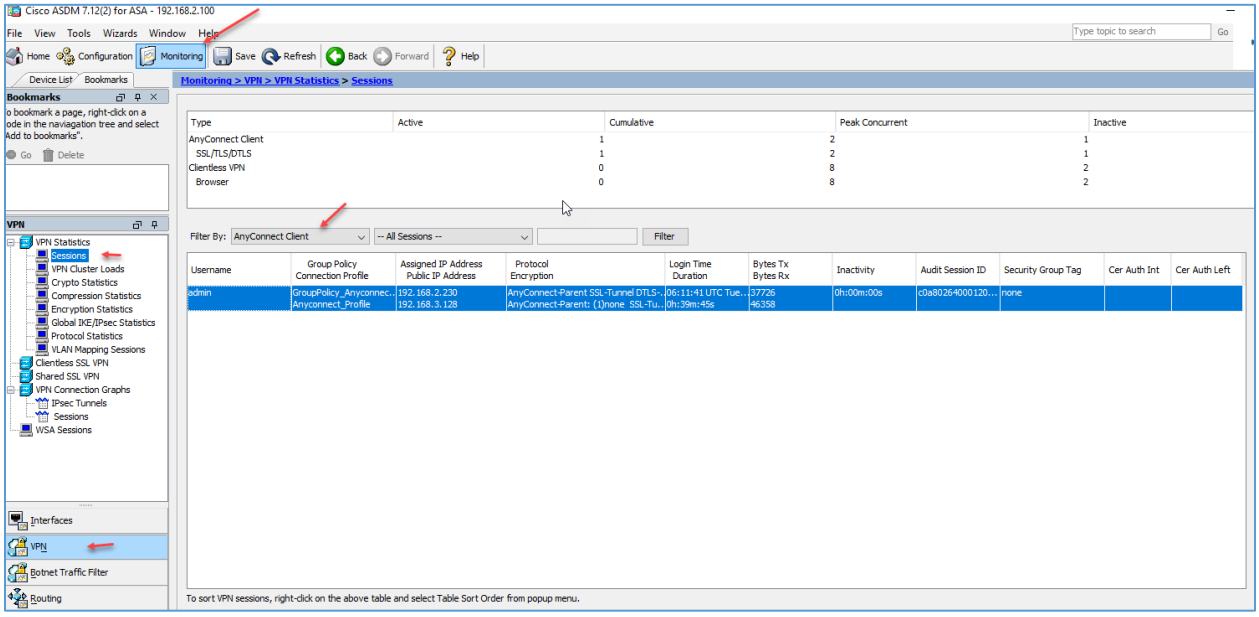


همانطور که مشاهده می‌کنید بعد از متصل شدن VPN توانستیم از طریق PC1 سرور 192.168.2.128 را Ping بگیریم.

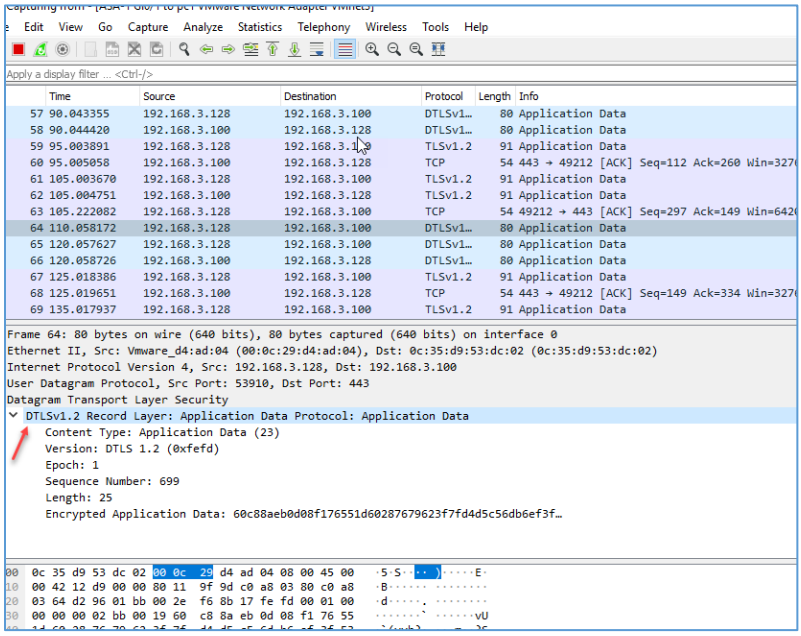


در شکل روبرو وب سایت سرور را مشاهده می‌کنید که از طریق PC1 باز شده است.

نرم‌افزار ASDM را باز کنید و وارد تب Monitoring شوید، در این صفحه از سمت چپ بر روی VPN کلیک کنید و از بین گزینه‌های موجود بر روی Sessions کلیک کنید، در این قسمت تمام کانکشن‌هایی که به فایروال زده شده مشخص می‌شود، برای اینکه کانکشن مربوط به AnyConnect را مشاهده کنیم باید از قسمت Filter By گزینه‌ی AnyConnect Client را انتخاب کنید که در شکل زیر این موضوع مشخص شده است و کانکشنی که از PC1 با آدرس 192.168.3.128 به فایروال زدیم مشخص شده است.



بعد از ارتباط vpn برای اینکه جزئیات ارتباط بین کلاینت و فایروال را مشاهده کنیم بر روی خط بین دو دستگاه کلیک راست کنید و گزینه‌ی Start capture را انتخاب کنید، همانطور که در شکل روبرو مشاهده می‌کنید دو پروتکل DTLS و TLS که برای ارتباط VPN است در حال کار است و اطلاعات بین دو دستگاه را رمزنگاری کرده است، DTLS با UDP و پروتکل TLS با TCP کار می‌کنند.

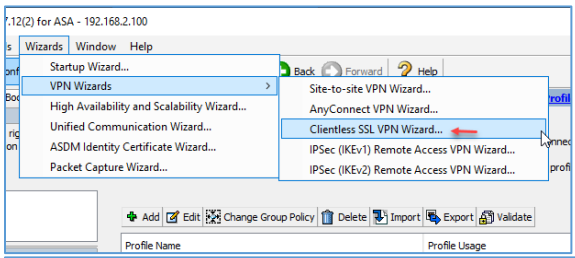


پروتکل DTLS یا همان Datagram Transport Layer Security پروتکل ارتباطی است که امنیت برنامه‌های مبتنی بر UDP را حفظ می‌کند تا از شنود پیام و جعل آن توسط دیگران جلوگیری کند، اگر کتاب CCNA R&S بنده را مطالعه کرده باشید در انجا به این نکته اشاره کردم که پروتکل UDP از نوع ارتباط connectionless است و ارتباطات در آن از نظر امنتی بررسی نمی‌شود ولی مزیتی که دارد سرعت آن به نسبت TCP بیشتر است، این پروتکل DTLS امنیت UDP را تضمین می‌کند.

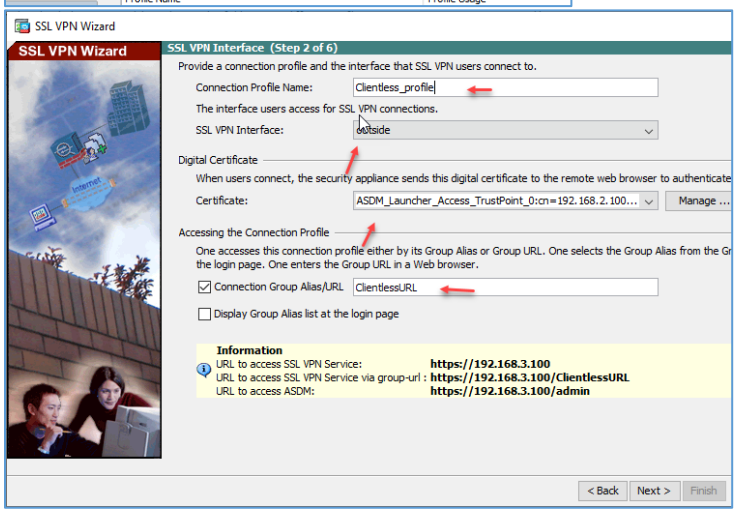
پروتکل TLS یا همان Transport Layer Security هم پروتکل ارتباطی امن برای ارتباطات TCP است و هنگامی که با TLS ارتباط برقرار کرده باشد تمام اطلاعت رمزنگاری خواهد شد، توجه داشته باشید که پروتکل TLS به همراه پروتکل SSL کار می‌کنند.

کار با Clientless SSL VPN در ASDM

در این قسمت بدون اینکه نیازی به ارتباط از طریق VPN داشته باشیم، دسترسی به منابع شبکه داخلی از طریق Web انجام می‌شود، یعنی اینکه می‌توانید سایت‌هایی را مشخص کنید که کاربران با کلیک بر روی آن صفحه آن سایت را مشاهده کنند و یا اینکه برای File sharing از آن استفاده کنید، البته امنیت این روش از AnyConnect کمتر است.

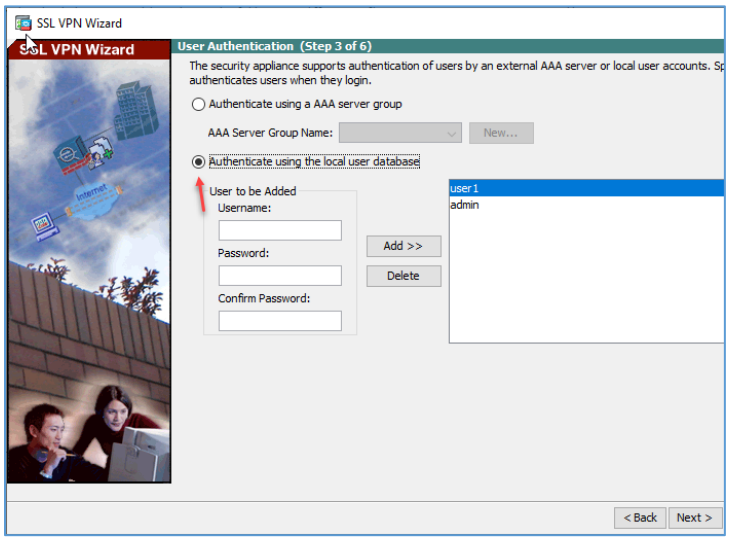


همان سناریوی قبلی را که بین سه دستگاه PC1، ASA1 و Server بود را در نظر بگیرید، وارد نرم‌افزار ASDM شوید و از منوی Wizards و از قسمت VPN Wizards گزینه‌ی Clientless SSl VPN را انتخاب کنید.

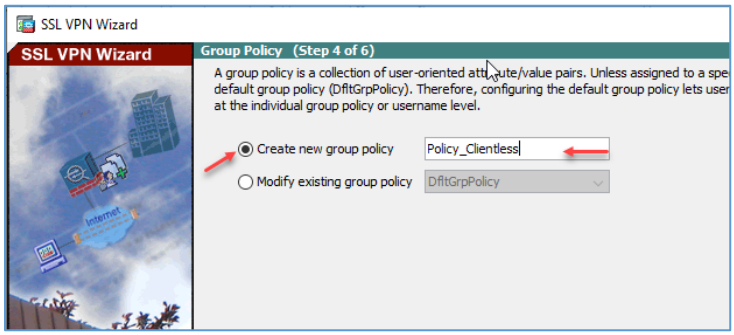


در این صفحه یک نام برای این Profile وارد کنید، و Interface که باید بر روی آن سرویس ارائه شود را outside در نظر بگیرید، certificate که در قسمت Anyconnect ایجاد کردیم را انتخاب و در آخر تیک گزینه‌ی مورد نظر را انتخاب کنید و یک نام برای گروه

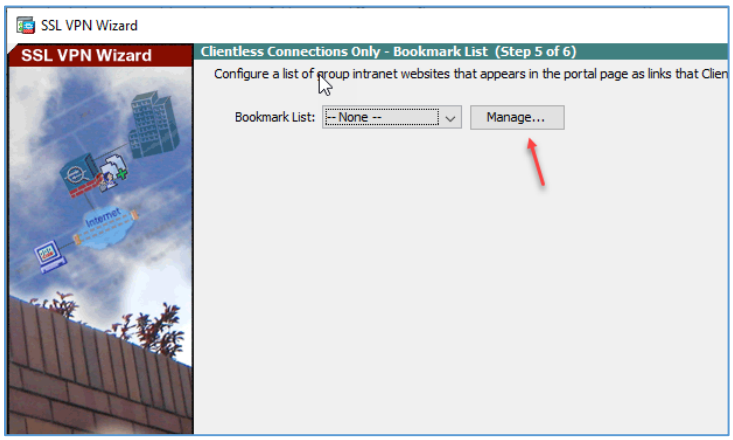
خود وارد کنید، اگر به شکل زیر توجه کنید، آدرس‌هایی که برای دسترسی به فایروال نیاز است مشخص شده است، بر روی Next کلیک کنید.



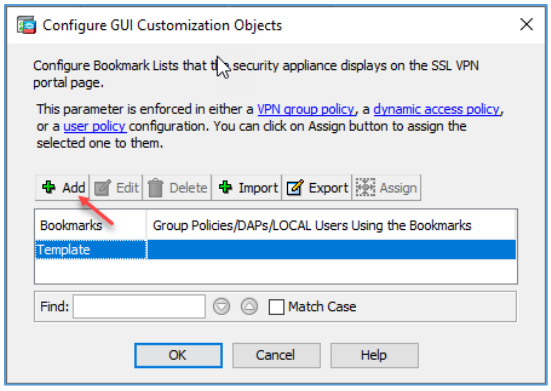
در این صفحه باید مشخص کنید که احراز هویت به چه شکلی مشخص شود، گزینه‌ی اول برای حالتی است که از سرور AAA در شبکه خود استفاده می‌کنید و گزینه‌ی دوم زمانی است که این سرورها را در دسترس ندارید و می‌خواهید از رمز محلی مربوط به خود فایروال استفاده کنید، البته می‌توانید خودتان کاربران مورد نظر خود را اضافه کنید، ولی سعی کنید در شبکه واقعی یک سرور ACS راه‌اندازی کنید و Active Directory خود را به آن متصل کنید تا کاربران بتوانند با نام کاربری و رمز خودشان وارد فایروال شوند.



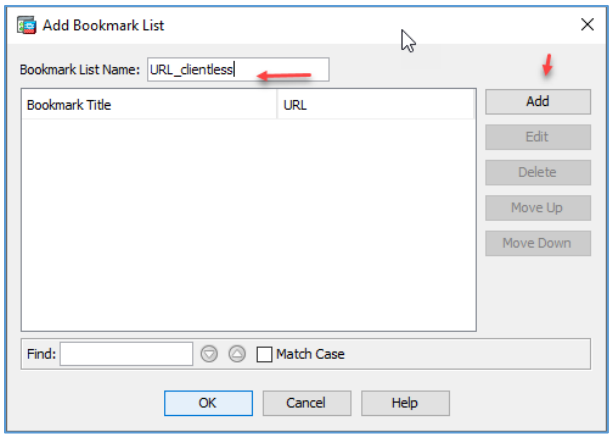
در این قسمت باید یک Policy جدید ایجاد کنید تا تنظیمات مشخص را بر روی آن اعمال کنیم، نام مورد نظر خود را وارد کنید.



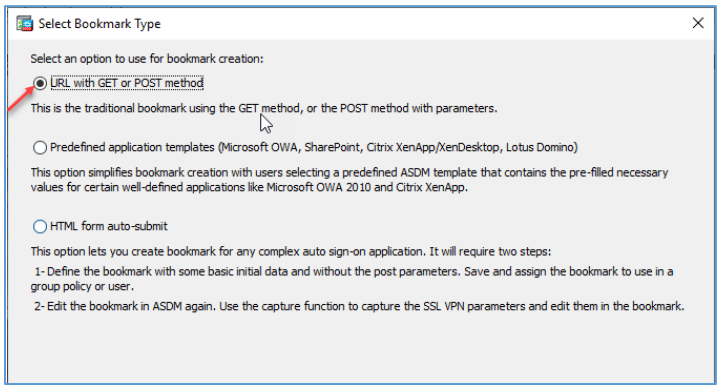
در این صفحه باید یک لیست Bokmark از آدرس‌های سرورهای داخلی تا زمانی که کاربران سایت را باز می‌کنند بتوانند به راحتی به این آدرس‌ها دسترسی داشته باشند.



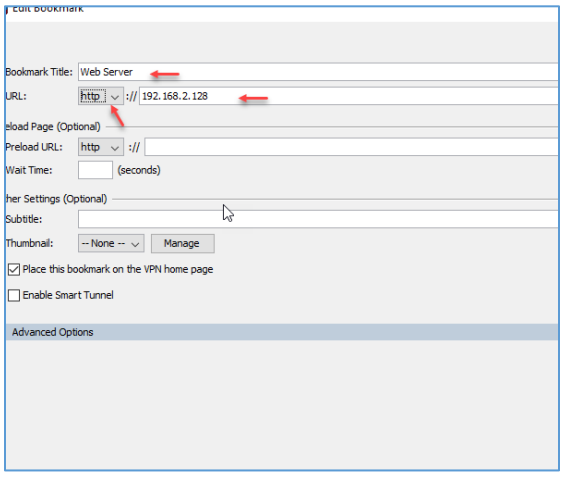
در این صفحه باید بر روی Add کلیک کنید و Bookmark خود را ایجاد کنید.



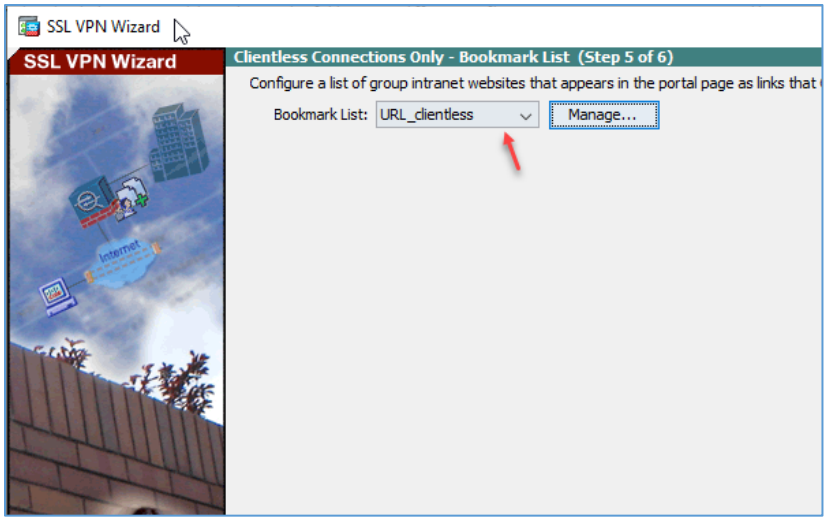
در این قسمت نام Bookmark خود را وارد و بر روی Add کلیک کنید.



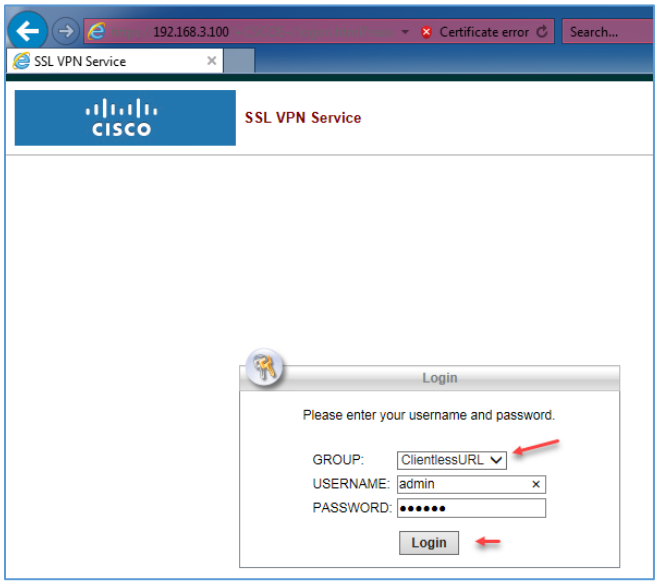
گزینه‌ی اول را انتخاب و بر روی OK کلیک کنید.



در این قسمت باید یک نام برای آدرس خود در نظر بگیرید و در قسمت URL باید پروتکل و آدرس آن را مشخص کنید که در اینجا پروتکل Http برای باز کردن وب سایت 192.168. 2.128 انتخاب شده است، بعد از این کار بر روی OK کلیک کنید تا آدرس به لیست اضافه شود.



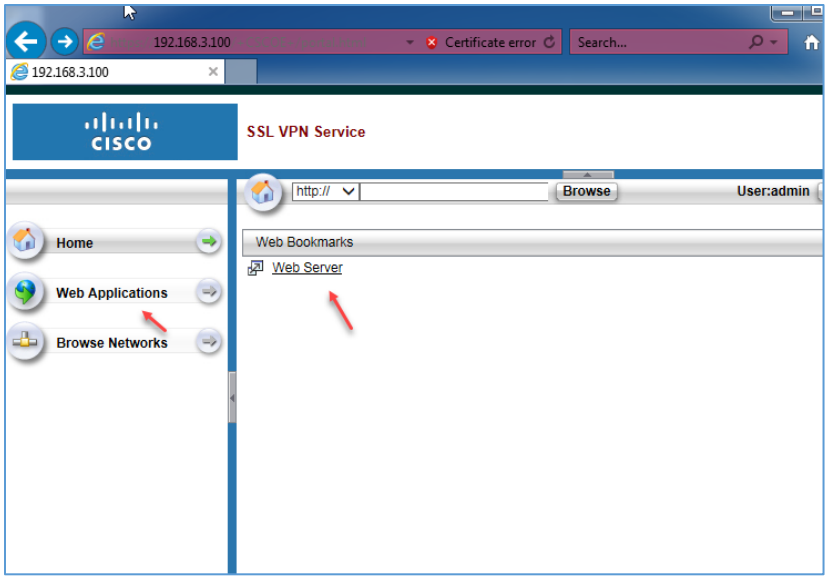
بعد از ایجاد، Bookmark را انتخاب کنید و بر روی Next کلیک کنید در صفحه بعد هم بر روی Finish کلیک کنید تا عملیات انجام شود.



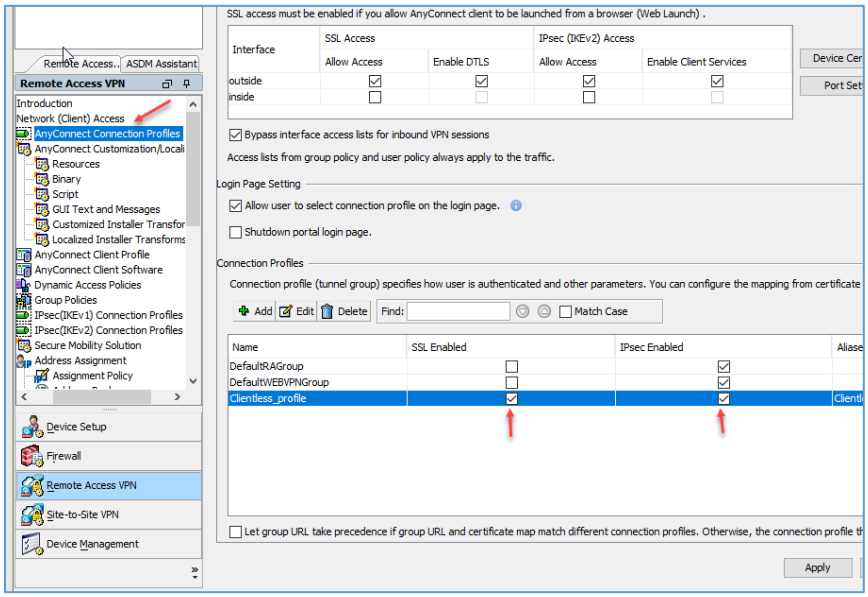
برای تست کار وارد PC1 شوید و از طریق مرورگر آدرس زیر را اجرا کنید.

https://192.168.2.128

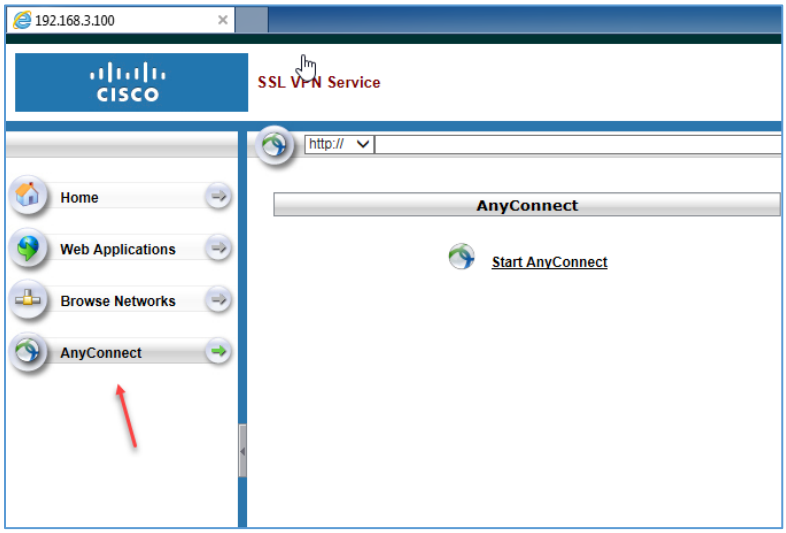
با این کار شکل روبرو ظاهر می‌شود و می‌توانید با نام کاربری و رمز عبور و انتخاب پروفایل مورد نظر وارد سایت شوید.



همانطور که مشاهده می‌کنید سایت باز شده است و Bookmark مورد نظر را مشاهده می‌کنید با کلیک بر روی آن می‌توانید سایت مورد نظر را باز کنید، توجه داشته باشید در قسمت بالای آن می‌توانید آدرس دلخواه خود را وارد کنید.



اگر هم بخواهید Anyconnect VPN را هم در لیست سایت فایروال مشاهده کنید باید وارد Remote Access VPN شوید و بر روی AnyConnect Connection Profiles کلیک کنید و از لیست همان Profile مورد نظر که ایجاد کرده بودید را به مانند شکل فعال کنید.



اگر دوباره وارد سایت شوید گزینه‌ی AnyConnect را هم مشاهده می‌کنید.

فصل هفتم – ایجاد امنیت در لایه دوم شبکه

در این بخش می‌خواهیم انواع روش‌های امنیتی را در لایه دوم شبکه پیاده‌سازی کنیم که یکی از جاهایی است که مهاجمان بیشتر حمله را دارند و اگر به درستی از آن جلوگیری نکنید می‌تواند ضربه سنگینی به پیکره‌ی شبکه شما وارد کنند.

در این بخش به موضوعات گوناگونی خواهیم پرداخت که لیست آن را در زیر مشاهده می‌کنید:

- بررسی حفاظت از پروتکل Spanning Tree Protocol
- بررسی تکنولوژی BPDU
- بررسی تکنولوژی Root Gurd
- تحلیل و بررسی سرویس Port Security
- ایجاد امنیت در سرویس DHCP
- تحلیل و بررسی Spoofing MAC Addresses
- تحلیل و بررسی DHCP Snooping
- تحلیل و بررسی IP source guard
- تحلیل و بررسی Dynamic Arp Inspection
- تحلیل و بررسی تکنولوژی تشخیص (IDS)
- تحلیل و بررسی Private VLAN

بررسی حفاظت از پروتکل Spanning Tree Protocol

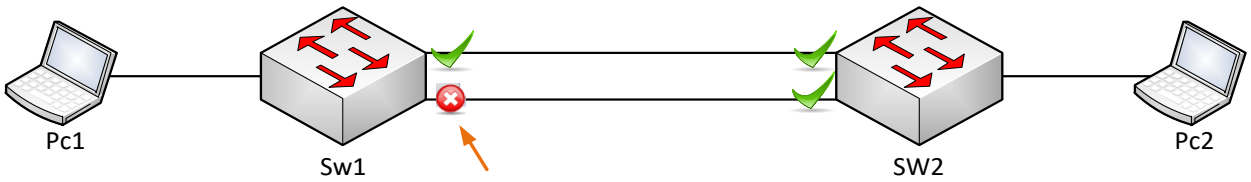
در این بخش نگاهی به پروتکل STP می‌اندازیم و روش‌های محافظت از این پروتکل حیاتی را با هم بررسی می‌کنیم.

STP (Spanning Tree Protocol)

پروتکل STP توسط سازمان IEEE با شماره‌ی 802.1D استاندارد شده است و شرکت سازنده‌ی آن DCE است.

کار این پروتکل این است که وقتی شبکه در Loop قرار می‌گیرد، بعضی از interface های اضافه را ShutDown می‌کند و فقط به یک طرف اجازه‌ی ارسال و دریافت اطلاعات می‌دهد.

این پروتکل از طریق الگوریتمی به نام STA (Spanning Tree Algorithm) برای این کار استفاده می‌کند که کار این الگوریتم به این صورت است که کل ساختار شبکه را به صورت یک درخت درآورده و جاهایی را که Loop در آن ایجاد شده، مهار می‌کند. در شکل زیر، ۲ سوئیچ با دو لینک به هم متصل شده‌اند و پروتکل STP برای جلوگیری از Loop، یکی از لینک‌ها را از رده خارج کرده است.



نحوه‌ی کارکرد الگوریتم STA

قبل از این کار به چند موضوع می‌پردازیم:

:Bridge ID

شناسه‌ای است برای تمایز دادن سوئیچ‌ها در پروتکل STP، پس می‌توان گفت با کمک این شناسه، سوئیچ‌ها در یک شبکه قابل تشخیص هستند و اجزای تشکیل‌دهنده‌ی Bridgr Id دو چیز است:

- **Priority**: عددی است روی سوئیچ‌های شرکت سیسکو که به صورت پیش‌فرض ۳۲۷۶۹ است.
- **Mac Address**: آدرس Mac پورت مورد نظر در سوئیچ.

پس Bridge ID، جمع این دو گزینه می‌شود. به شکل صفحه‌ی قبل توجه کنید؛ در سوئیچی که پروتکل STP روی آن اجرا شده است (که با جهت‌نما آن را مشخص کردیم) در مد Privileged دستور زیر را وارد کنید:

```
Switch# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address     0001.C9A6.90A3
Cost       19
(Port       1(FastEthernet0/1
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

(Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1
Address     0090.0C6C.EE69
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  20

Interface       Role Sts Cost      Prio.Nbr Type
--------------------------------- -------- --------- --- ---- -----------------

Fa0/1           Root FWD 19        128.1    P2p
Fa0/2           Altn BLK 19        128.2    P2p
Fa0/3           Desg FWD 19        128.3    P2p
```

این اعداد به رنگ قرمز در نتیجه مشخص شده‌اند.

Root Bridge:

برای انتخاب یک سوئیچ به عنوان root Bridge تمام Bridge IDهای مختلف سوئیچ‌ها باهم مقایسه می‌شوند و هرکدام که کوچک‌تر بود، همان سوئیچ به عنوان Root Bridge انتخاب می‌شود.

:BPDU

فریمی در سوئیچ است که برای انتقال اطلاعات بین سوئیچ‌ها کاربرد دارد و یکی دیگر از ویژگی‌های آن این است که تغییر ساختار شبکه را خیلی سریع به دیگر سوئیچ‌ها در شبکه اطلاع می‌دهد.

:Root Port

پورتی است که ارتباط مستقیم با Root Bridge دارد و از طریق آن انتخاب می‌شود.

:Designated port

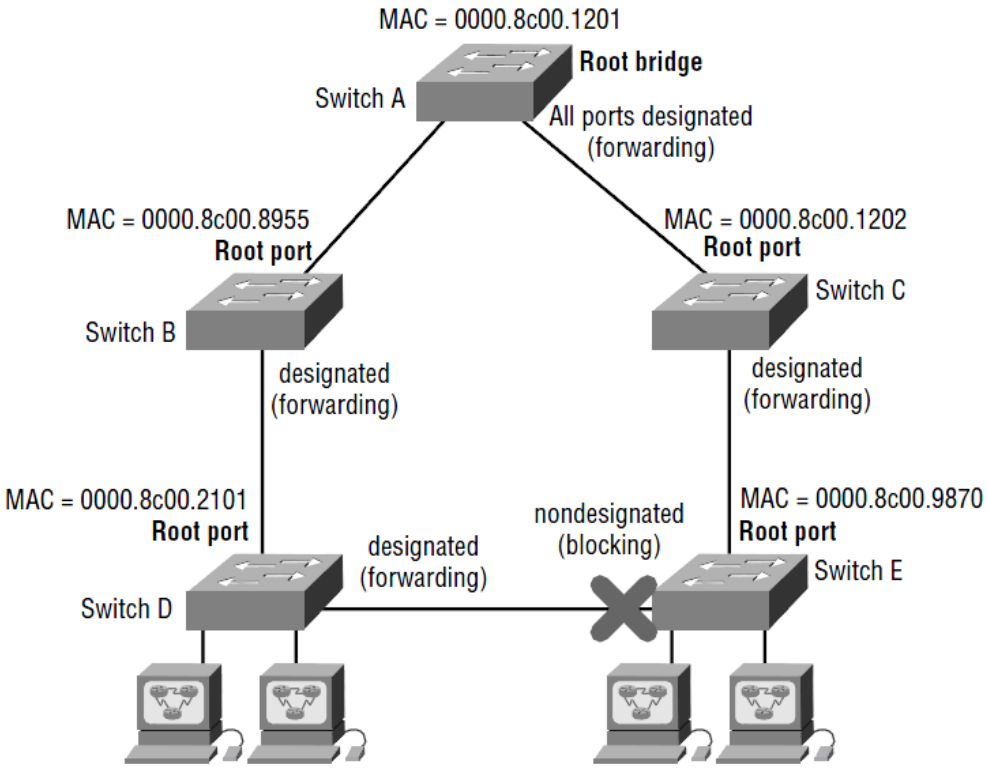
پورتی از سوئیچ است که به عنوان Forwarding انتخاب می‌شود و کار ارسال و دریافت اطلاعات را انجام می‌دهد.

:NonDesignated port

برای جلوگیری از loop این پورت shutdown می‌شود.

پس در کل در الگوریتم STA هر سوئیچ Bridge ID خود را محاسبه می‌کند و بعد، از طریق BPDU آن را در شبکه تبلیغ می‌کند، بعد Bridge ID خود را با دیگر سوئیچ‌ها مقایسه می‌کند، اگر Bridge ID خودش کمتر از دیگران باشد، Bridge ID خود را در شبکه تبلیغ می‌کند، اما اگر یکی کمتر از خود را پیدا کند آن را در قالب فریم BPDU به دیگر سوئیچ‌ها اعلام می‌کند تا در آخر کار بعد از مقایسه، Bridge ID کمترین Bridge ID به دست آید که آخرین سوئیچ با کمترین Bridge Id به عنوان Root Bridge انتخاب می‌شود. بعد از این کار، نوبت به انتخاب وضعیت پورت‌ها است که چه پورتی در چه وضعیتی قرار دارد.

در شکل صفحه‌ی بعد، تمام مراحل بالا وجود دارد. اگر به شکل توجه کنید، Switch A به علت کوچک‌تر بودن Mac Address نسبت به بقیه‌ی سوئیچ‌ها، به عنوان Root bridge انتخاب شده است و هر دو پورت آن به حالت Forwarding رفته است. پورت‌های سوئیچ‌های B و C که به سوئیچ A متصل هستند به عنوان Root Port انتخاب شده‌اند. پورت بعدی سوئیچ‌های B و C به عنوان پورت Forwarding انتخاب شده‌اند و به همین ترتیب بقیه‌ی پورت‌ها انتخاب می‌شوند. برای جلوگیری از loop یکی از پورت‌های سوئیچ E به حالت Nondesignated رفته و Block شده است که البته این پورت به نسبت پورت دیگر دارای cost بیشتر و پهنای باند کمتری بوده است.



پس اگر مراحل کار الگوریتم STA را طبق مراحل زیر در نظر بگیریم، متوجه‌ی کار این الگوریتم خواهیم شد.

۱- سوئیچ‌ها، Bridge ID خود را مشخص می‌کنند.

۲- در این مرحله، هر سوئیچ Bridge ID خود را تحت فریم BPDU به دیگر سوئیچ‌ها تبلیغ می‌کند تا پایین‌ترین Bridgr ID مشخص شود و بعدازآن، Root Bridge مشخص می‌شود.

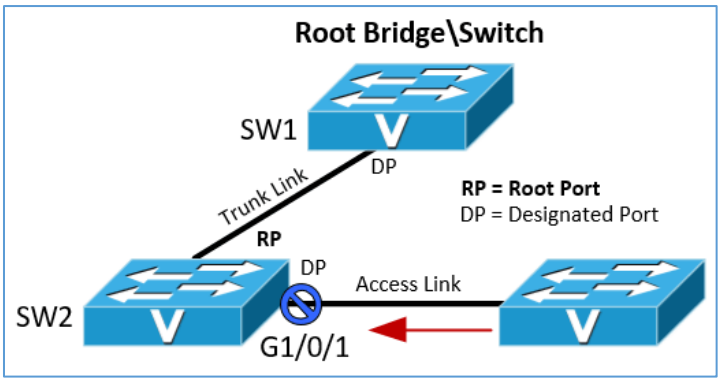
۳- باید Designated Port انتخاب شود که پورت‌های متصل به سوئیچ Root Bridge به عنوان Designated Port انتخاب می‌شوند و کار ارسال و دریافت اطلاعات را انجام می‌دهند. در بین دو سوئیچ هم پورتی که کمترین cost را داشته باشد، به عنوان Designated Port انتخاب می‌شود.

۴- در این مرحله که مرحله‌ی مهمی است در آن قسمت که loop ایجاد می‌شود، یکی از پورت‌ها که پهنای باند کمتر و Cost بیشتر داشته باشد، به عنوان پورت NonDesignated Port انتخاب و Block می‌شود. اگر چنانچه هر دو فاکتور پهنای باند و cost یکی باشد، معیار انتخاب Bridge ID بزرگ‌تر است.

تا به اینجا سرویس STP را بررسی کردیم و روش کار آن را آموختید، در ادامه روش‌های محافظتی برای جلوگیری از خرابکاری در این سرویس را می‌آموزیم.

بررسی BPDU Guard

یک شبکه را در نظر بگیرید که دارای چند سوئیچ می‌باشد و چندین سیستم به هر یک از سوئیچ‌ها متصل شده است، به صورت پیش‌فرض پورت‌هایی که از یک سوئیچ به سوئیچ دیگر متصل شده باشد در حالت Trunk قرار دارد و دستگاه‌های دیگر مانند کلاینت‌ها در حالت Access قرار می‌گیرند، در شکل زیر سه سوئیچ را مشاهده می‌کنید، سوئیچ SW1 که به عنوان سوئیچ Root مشخص شده است با سوئیچ SW2 ارتباط دارد و پورت آنها در حالت Trunk قرار گرفته است، ولی پورت دیگر سوئیچ SW2 در حالت Access قرار دارد و اصولاً باید کلاینت‌ها، سرورها، چاپگرها و... به آن متصل شوند، ولی اگر یک مهاجم یک سوئیچ را به این پورت متصل کند می‌تواند در شبکه اختلال ایجاد کند.

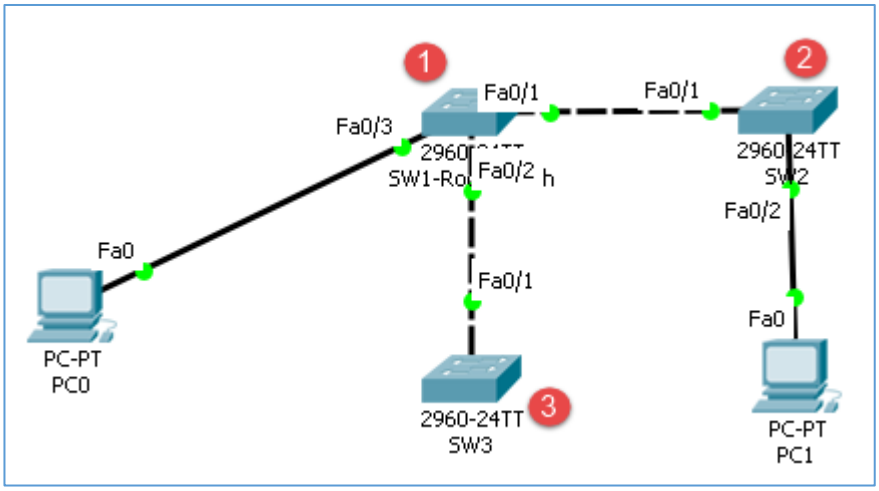


برای جلوگیری از این کار باید دستور زیر را در پورت G1/0/1 سوئیچ SW2 وارد کنید:

```
Switch(config)#int G1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
```

با اجرای این دستور در پورت مورد نظر اگر چنانچه سوئیچ به آن پورت متصل شود و بخواهد فریم BPDU ارسال کند، با فعال بود BPDU Guard، پورت مورد نظر خاموش خواهد شد.

برای اینکه این موضوع بهتر برای شما جا بیفتد به مثال بعدی در این مورد توجه کنید.



در شکل روبرو سه سوئیچ و دو PC را به نرم‌افزار PacketTracer اضافه کردیم، سوئیچ SW1 که در قسمت شماره‌ی یک مشخص شده است، به عنوان سوئیچ اصلی در نظر گرفته شده است، و سوئیچ‌ها به همراه کلاینت‌ها بدون هیچ مشکلی به آن متصل شده‌اند، ولی برای ایجاد امنیت می‌خواهیم BPDU Guard را روی پورت سوئیچ شماره‌ی یک اعمال کنیم، ولی قبل از آن به این نکته اشاره کنیم که بهتر است همه پورت‌های سوئیچ را در حالت BPDU Guard قرار دهید و فقط بر روی پورت‌هایی که به سوئیچ اصلی متصل می‌شوند این گزینه را فعال نکنید.

```
Switch(config)#interface range fastEthernet 0/2-24
```

با دستور بالا وارد تمام پورت‌های سوئیچ شماره‌ی یک می‌شویم به جزء پورت Fa0/1 که به سوئیچ شماره‌ی دو متصل است.

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 1
```

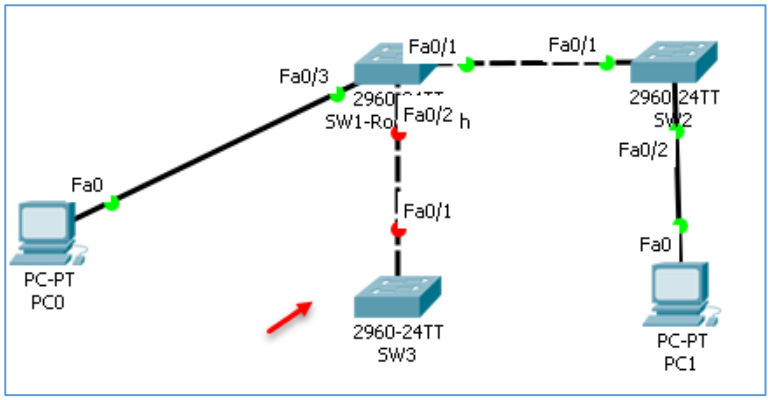
با این دستور پورت های سوئیچ در حالت Access قرار می‌گیرند

```
Switch(config-if-range)#spanning-tree bpduguard enable
```

با اجرای دستور بالا ارتباط بین سوئیچ شماره یک با سه به علت فعال سازی BPDU Guard قطع خواهد شد و با پیغام زیر مواجه می‌شوید

```
Switch(config-if-range)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port
FastEthernet0/2 with BPDU Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on 0/2, putting 0/2 in err-disable state
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

در پیغام بالا، به این موضوع اشاره شد که از پورت FastEthernet0/2 فریم BPDU دریافت شد که به خاطر فعال بودن سرویس BPDU Guard پورت مورد نظر خاموش شده است.



همانطور که در شکل روبرو مشاهده می‌کنید، پورت Fa0/2 در سوئیچ شماره‌ی یک خاموش شده است و ارتباط را قطع کرده است.

اگر چنانچه بعد از خاموش شدن پورت نیاز باشد که آن را روشن کنید، راحت‌ترین راه آن است که وارد آن پورت شوید و از دستورات Shutdown و No Shutdown استفاده کنید که این کار یک روش معمول برای تمام مدیران شبکه است؛ حال اگر در محل مورد نظر قرار نداشته باشد آن وقت چه باید کرد؟

برای حل این مشکل باید از مد Recovery استفاده کنید، برای این کار از دستور زیر استفاده کنید:

```
Switch(config)#errdisable recovery cause bpduguard
```

با دستور بالا مد Recovery برای سرویس BPDU فعال می‌شود.

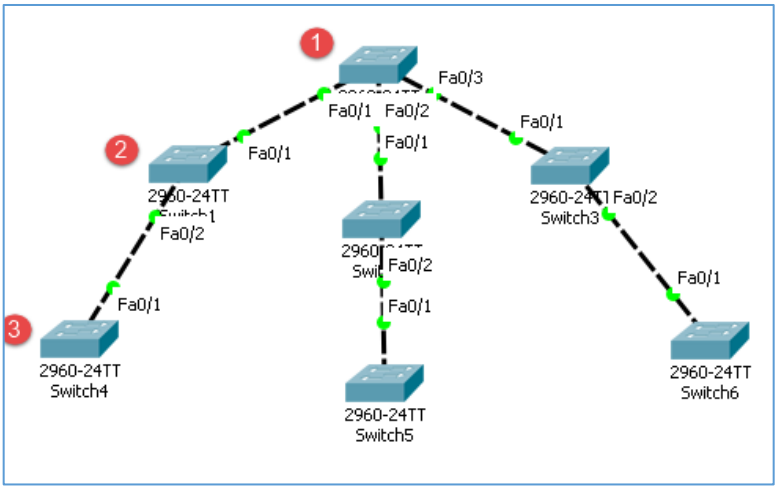
```
Switch(config)#errdisable recovery interval 180
```

در این دستور زمان روشن شدن پورت ۱۸۰ ثانیه در نظر گرفته شده است.

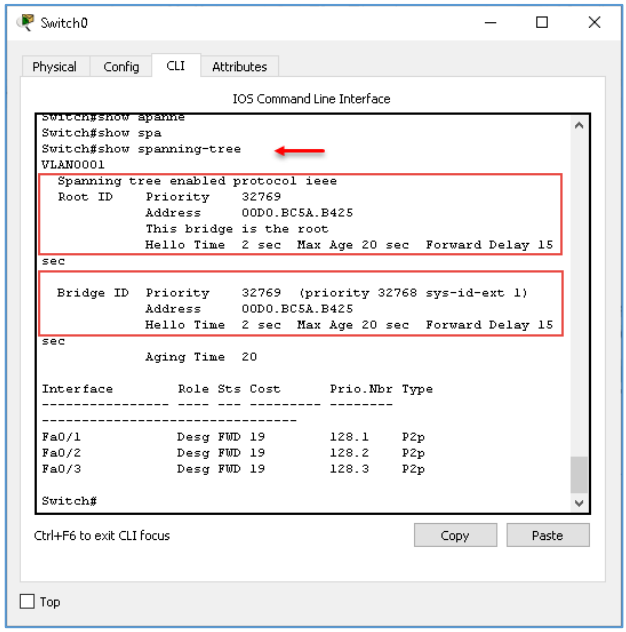
پس نتیجه این کار این شد که کسی بدون اجازه نمی‌تواند سوئیچ غیر مجاز به شبکه اضافه کند و پروتکل STP را دستکاری کند.

تحلیل و بررسی Root Guard

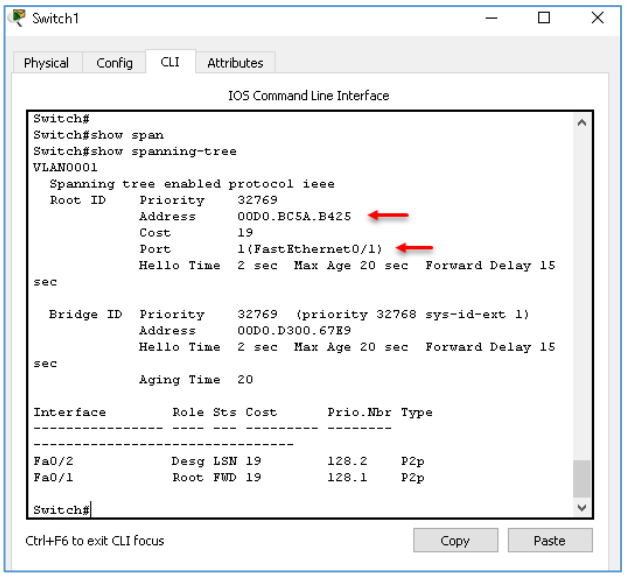
یکی از دیگر روش‌های منحصر به فرد سیسکو برای محافظت از پروتکل STP استفاده از Root Guard است، این سرویس قابلیت اطمینان، کنترل و امنیت را در شبکه افزایش می‌دهد، در این سرویس با انتخاب یک سوئیچ به عنوان Root به بقیه‌ی سوئیچ‌ها اجازه نمی‌دهد که به عنوان سوئیچ Root فعالیت کنند، در ادامه این موضوع را به طور کامل بررسی می‌کنیم.



در این شکل چندین سوئیچ در نرم‌افزار Packet Tracer اضافه شده است، با توجه به ساختار شبکه، سوئیچ شماره‌ی یک باید به عنوان Root Bridge انتخاب شود، و همانطور که در درس قبلی به آن اشاره کردیم سوئیچ Root Brige از طریق شماره‌ی Priority انتخاب می‌شود.



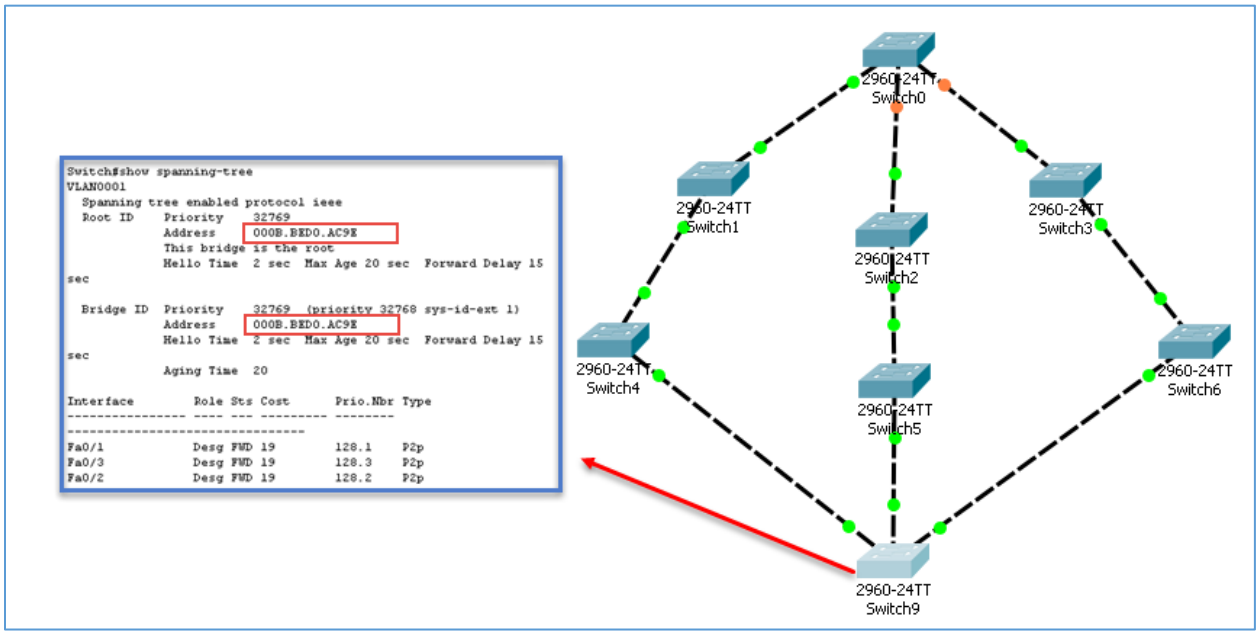
به مانند شکل، برای اینکه متوجه شویم که آیا سوئیچ شماره‌ی یک به عنوان Root انتخاب شده یا نه از دستور show spanning-tree استفاده می‌کنیم؛ در قسمت اول شماره‌ی Priority و آدرس MAC سوئیچ Root مشخص شده است و در قسمت شماره‌ی دو مشخصات همین سوئیچی که انتخاب کردیم مشخص شده است، اگر توجه کرده باشید همین سوئیچ شماره‌ی یک به عنوان Root انتخاب شده است.

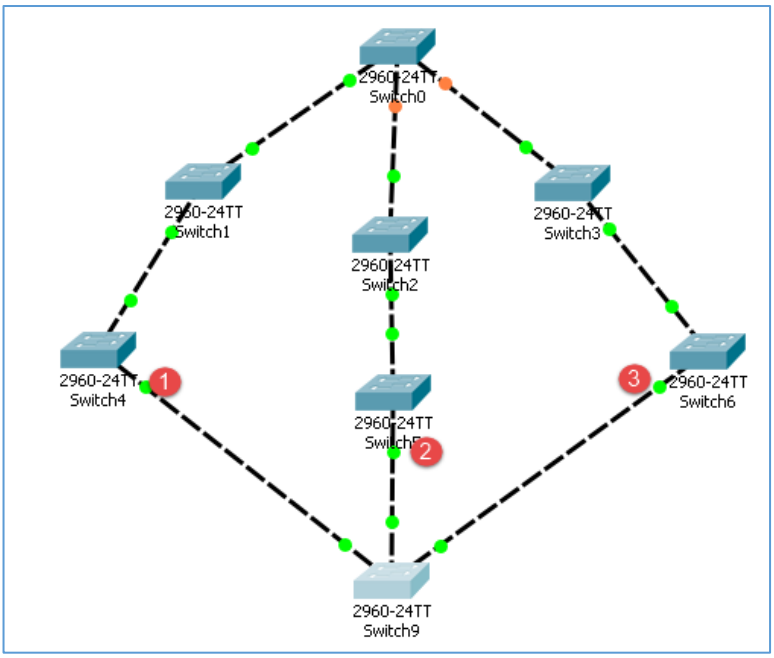


اگر دستور show spanning-tree را در سوئیچ شماره‌ی دو وارد کنید، نتیجه به صورت شکل روبرو مشخص شده است، در قسمت اول سوئیچ Root با MAC آدرس 00D0.BC5A.B425 مشخص شده است که این آدرس مربوط به سوئیچ شماره‌ی یک می‌باشد و در قسمت Port هم FastEthernet0/1 نوشته شده است که نشان می‌دهد اطلاعات را از این مسیر از سوئیچ Root دریافت می‌کند.

همانطور که مشاهده کردید سوئیچ شماره‌ی یک به عنوان Root در این ساختار انتخاب شده است، حال اگر یک مهاجم Priority خود را در سوئیچ تغییر دهد، همه سوئیچ‌ها سوئیچ مهاجم را به عنوان Root قبول خواهند کرد.

اگر به شکل زیر توجه کنید یک سوئیچ جدید به شبکه ما اضافه شده که همان سوئیچ مهاجم است، با اضافه شدن سوئیچ آدرس Root به سوئیچ جدید تغییر کرده است که این می‌تواند بسیار خطرناک باشد.

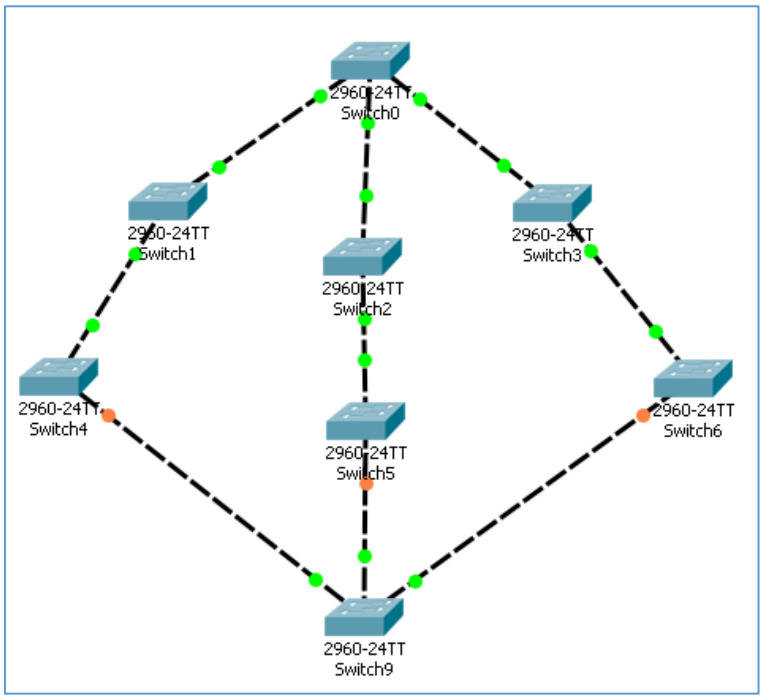




برای جلوگیری از این نوع حملات می‌توانیم در پورت‌هایی که احتمال بیشتری دارد تا مهاجم از آن طریق به شبکه حمله کند، دستور زیر را وارد کنید:

spanning-tree guard root

توجه داشته باشید این دستور باید در داخل Port مورد نظر که به بیرون متصل است اجرا شود.



همانطور که مشاهده می‌کنید، دستور spanning-tree guard root در سه سوئیچ اجرا شد و نتیجه آن این شد که مهاجمی که با Piority کمتر در تلاش بود که خود را به عنوان Root معرفی کند بلاک شد و دوباره سوئیچ Root همان سوئیچ شماره‌ی یک شد.

تفاوت‌های بین دو سرویس Root Guard و BPDU Guard

سرویس BPDU و Root تفاوت خاصی با هم ندارند و هر دو برای یک هدف ایجاد شده‌اند، ولی اگر دقیق‌تر به موضوع نگاه کنیم، سرویس BPDU زمانی فعال می‌شود که یک مهاجم بخواهد یک سوئیچ را به شبکه شما متصل کند، که بعد از این کار چون سوئیچ‌ها به همدیگر فریم BPDU ارسال می‌کنند آن پورت خاموش می‌شود و مدیر شبکه باید به صورت دستی آن پورت را روشن کند و یا اینکه سرویس errdisable را برای آن فعال کند تا بعد از مدت زمان مشخص آن پورت روشن شود.

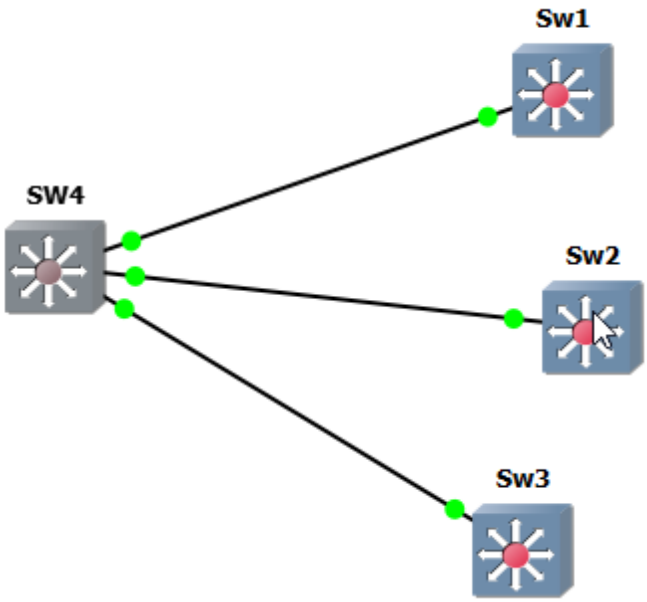
اما سرویس Root Guard تا زمانی که مهاجم سعی در تغییر Priority نکند واکنشی از خود نشان نمی‌دهد، ولی اگر Priority تغییر کند و سوئیچ Root تغییر کند، آن پورت بلاک خواهد شد.

در کل، برای امنیت بیشتر سوئیچ‌ها در شبکه از هر دو سرویس به طور همزمان استفاده کنید تا از خطرات آن جلوگیری کنید.

بررسی پروتکل CDP و LLDP

این دو پروتکل برای نمایش لیست دستگاه‌هایی است که به یک روتر یا سوئیچ متصل شده‌اند، CDP یا همان Cisco Discovery Protocol مختص شرکت سیسکو بوده و فقط در دستگاه‌های این شرکت کارای دارد و LLDP یا همان Link Layer Discovery Protocol یک پروتکل عمومی است که هم در سیسکو و هم در دستگاه‌های دیگر کاربرد دارد.

بیاید با یک مثال که از کتاب CCNA R&S بنده است پروتکل CDP را بررسی کنیم و امنیت آن را هم به چالش بکشیم.



در این مثال از ٤ سوئیچ استفاده می‌کنیم که سوئیچ‌های ۱، ۲ و ۳ به سوئیچ ٤ متصل هستند. می‌خواهید بدانید چه دستگاه‌هایی از چه مدلی به سوئیچ SW4 متصل است، برای این کار از دستور زیر استفاده می‌کنیم:

وارد سوئیچ ٤ شوید و در مد Privileged، دستور زیر را وارد کنید:

SW4#**show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

```
                D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
Sw1            Eth 0/0          128            R S I       Linux Uni Eth 0/0
Sw2            Eth 0/1          128            R S I       Linux Uni Eth 0/1
Sw3            Eth 0/2          129            R S I       Linux Uni Eth 0/0
```

همان‌طور که مشاهده می‌کنید با اجرای دستور show cdp neighbors، لیست سوئیچ‌های متصل به این سوئیچ را با ویژگی‌های سوئیچ‌های مربوطه نمایش داد.

در این دستور به ما شماره‌ی پورت، شماره‌ی دستگاه، نوع دستگاه، پورت ورودی به سوئیچ و مقدار زمانی که طول کشید سوئیچ دستگاه‌های متصل به خودش را شناسایی کند را نمایش می‌دهد.

برای اینکه به جزئیات بیشتر در مورد دستگاه‌های متصل شده دست پیدا کنیم از دستور زیر استفاده می‌کنیم:

```
SW4# show cdp neighbors detail
```

پروتکل CDP هر ٦٠ ثانیه یک‌بار، اطلاعات مربوط را به دستگاه‌های متصل به خود ارسال می‌کند و دستگاه‌هایی که این پیام را دریافت می‌کنند در جدولی که معرفی کردیم، ذخیره می‌کنند.

یکی از مشکلاتی که این دو پروتکل (CDP , LLDP) دارد این است که مهاجم با گوش دادن به خط ارتباطی آنها می‌تواند به اطلاعات خوبی دست پیدا کند.

وارد سوئیچ شوید و دستور Show lldp را وارد کنید که نتیجه آن را در زیر مشاهده می‌کنید که این پروتکل به صورت پیش‌فرض غیر فعال است و اگر هم فعال بود با دستور no lldp run می‌توانید آن را غیر فعال کنید.

```
SW4#show lldp

% LLDP is not enabled
```

برای غیر فعال کردن پروتکل CDP هم می‌توانید از دستورات زیر استفاده کنید:

```
SW4(config)#no cdp run
```

با دستور بالا CDP غیر فعال خواهد شد و برای اینکه متوجه شویم دستور به خوبی اجرا شده باید دستور Show cdp را اجرا کنید.

```
SW4(config)#do sh cdp
% CDP is not enabled
```

نکته اول: برای اینکه CDP را فقط در Interface مشخص غیر فعال کنید باید از دستورات زیر استفاده کنید:

```
SW4(config)#interface ethernet 0/0
SW4(config-if)#no cdp enable
```

نکته دوم : CDP در لایه ۲ عمل می‌کند و می‌تواند اطلاعاتی را برای مهاجمان، به عنوان مثال(نوع دستگاه ، نسخه‌های سخت افزاری و نرم‌افزاری ،جزئیات آدرس VLAN و IP و موارد دیگر) ارسال کند که این می‌تواند بسیار نگران کننده باشد.

ایجاد امنیت در سرویس DHCP

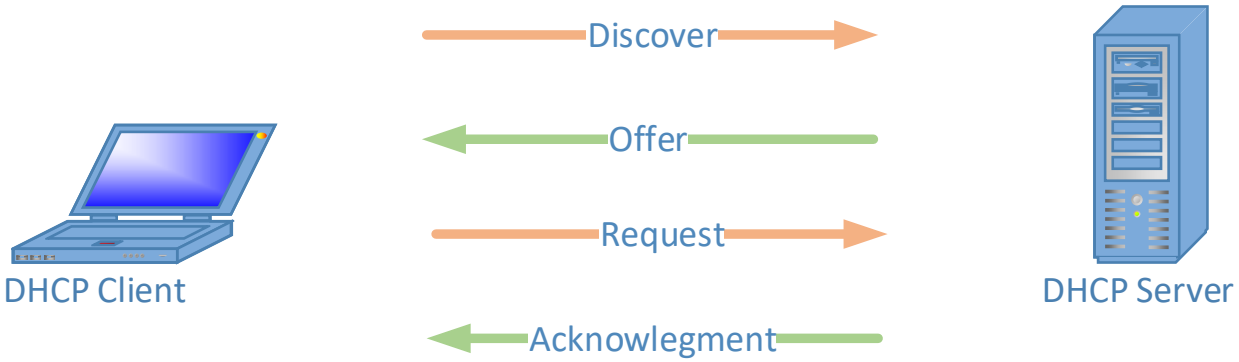
یکی از پرکاربردترین سرویس استفاده شده در شبکه‌های مختلف، سرویس DHCP می‌باشد. این سرویس به صورت پویا به همه کلاینت های موجود در شبکه آدرس IP می‌دهد؛ مثلاً اگر در مجموعه‌ی شبکه ی خود ۲۰۰ کامپیوتر داشته باشید، دیگر لازم نیست که پشت تک تک کامپیوترها بنشینید و IP وارد کنید؛ فقط کافی است سرویس DHCP را روی سرور اصلی فعال کنید و کامپیوترها را در حالت دریافت IP به صورت اتوماتیک قرار دهید. به همه‌ی کامپیوترها IP در رنج مشخص‌شده تخصیص داده خواهد شد.

در این قسمت می‌خواهیم روش‌هایی را ارائه دهیم تا مهاجمان با استفاده از ابزارهای موجود نتوانند از طریق این سرویس به منابع شبکه دسترسی داشته باشد، برای ایجاد امنیت نیاز به دستگاه‌های سیسکو مانند سوئیچ دارید تا بتوانید این قابلیت امنیتی را در آن فعال کنید.

عملکرد DHCP به چهار قسمت پایه تقسیم می‌گردد

- ✓ اکتشاف (DHCP Discovery)
- ✓ پیشنهاد (DHCP Offer)
- ✓ درخواست (DHCP Request)
- ✓ تصدیق (DHCP Acknowledgement)

این چهار مرحله به صورت خلاصه با عنوان DORA شناخته می‌شوند.



DHCP Discovery (اکتشاف DHCP)

هر سرویس گیرنده (کاربر) برای شناسایی سرورهای DHCP موجود اقدام به فرستادن پیامی در زیر شبکه خود می‌کند. مدیرهای شبکه می‌توانند مسیریاب محلی را به گونه پیکربندی کنند که بتواند بسته داده‌ای DHCP را به یک سرور DHCP دیگر که در زیر شبکه متفاوتی وجود دارد، بفرستد. این مهم باعث ایجاد بسته داده با پروتکل UDP می‌شود که آدرس مقصد ارسالی آن 255.255.255.255 یا آدرس مشخص ارسال زیر شبکه می‌باشد. کاربر (سرویس گیرنده) DHCP همچنین می‌تواند آخرین IP آدرس شناخته شده خود را درخواست بدهد. اگر سرویس گیرنده همچنان به شبکه متصل باشد در این صورت IP آدرس معتبر می‌باشد و سرور ممکن است که درخواست را بپذیرد. در غیر اینصورت، این امر بستگی به این دارد که سرور به عنوان یک مرجع معتبر باشد. یک سرور به عنوان یک مرجع معتبر درخواست فوق را نمی‌پذیرد و سرویس گیرنده را مجبور می‌کند تا برای درخواست IP جدید عمل کند.

DHCP Offer (پیشنهاد DHCP)

زمانی که یک سرور DHCP یک درخواست را از سرویس گیرنده (کاربر) دریافت می‌کند، یک IP آدرس را برای سرویس گیرنده رزرو می‌کند و آن را با نام DHCP Offer برای کاربر می‌فرستد. این پیام شامل: MAC آدرس (آدرس فیزیکی دستگاه) کاربر؛ IP آدرسی پیشنهادی توسط سرور؛ IP Subnet Mask؛ زمان تخصیص IP (lease Duration) و IP آدرس سروری می‌باشد که پیشنهاد را داده است.

DHCP Request (درخواست DHCP)

سرویس گیرنده با یک درخواست به مرحله پیشین پاسخ می‌گوید. یک کاربر می‌تواند پیشنهادهای مختلفی از سرورهای متفاوت دریافت کند. اما فقط می‌تواند یکی از پیشنهادها را بپذیرد. بر اساس تنظیمات شناسایی سرور در درخواست و فرستادن پیام‌ها (identification option)، سرورها مطلع می‌شوند که پیشنهاد کدام یک پذیرفته شده‌است. هنگامی که سرورهای DHCP دیگر این پیام را دریافت می‌کنند، آن‌ها پیشنهادهای دیگر را، که ممکن است به کاربر فرستاده باشند، باز پس می‌گیرند و آن‌ها را در مجموعه IPهای در دسترس قرار می‌دهند.

DHCP Acknowledgement (تصدیق DHCP)

هنگامی که سرور DHCP، پیام درخواست DHCP را دریافت می‌کند، مراحل پیکربندی به فاز پایانی می‌رسد. مرحله تصدیق شامل فرستادن یک بسته داده‌ای (DHCP Pack) به کاربر می‌باشد. این داده بسته‌ای شامل: زمان تخصیص IP یا هرگونه اطلاعات پیکربندی که ممکن بوده‌است که سرویس گیرنده درخواست کرده باشد، می‌باشد. در این مرحله فرایند پیکربندی IP کامل شده‌است.

پیغام‌های DHCP در دیتا گرام‌های UDP حمل می‌شوند و در سمت سرویس دهنده از شماره پورت ٦٧ و در سمت سرویس گیرنده از پورت ٦٨ استفاده می‌کند. پروتکل‌هایی که در ارتباط با DHCP کار می‌کنند شامل IP, BOOTP , UDP, TCP, RARP می‌باشند.

مشکلات امنیتی پروتکل DHCP

همانطور که گفته شد پیغام DHCP Discovery یک پیغام Broadcast است، از این رو در صورتی که بیش از یک سرور DHCP در شبکه موجود باشند، هرکدام از آن سرورها به صورت مجزا به سیستم درخواست کننده پاسخ می‌دهند، در این حالت، سیستمی که پیغام DHCP Discovery را فرستاده است با آن سروری عملیات را ادامه می‌دهد که پیغام DHCP Offer آن زودتر به دستش رسیده باشد. از این رو در صورتی که یک سرور DHCP تقلبی یا به اصطلاح Rogue DHCP در شبکه وجود داشته باشد درخواست DHCP Discovery به آن می‌رسد و شروع به ادامه دادن مراحل سرویس DHCP می‌کند.

در صورتی که DHCP Offer پیشنهاد شده از سمت سرور تقلبی، زودتر از پیغام DHCP Offer پیشنهاد شده از سمت سرور اصلی DHCP برسد، سیستمی که در ابتدا درخواست IP کرده بوده است از یک سرور DHCP مخرب IP را دریافت کرده است.

دریافت IP از سمت سرور تقلبی به خودی خود مشکلی را ایجاد نمی‌کند، اما حالتی را در نظر بگیریم که حمله کننده تغییراتی را در رنج IP که می‌خواهد به کاربران پیشنهاد بدهد ایجاد کند. تغییرات می تواند به یکی از حالت های زیر به وجود آید:

پیشنهاد کردن رنج شبکه اشتباه

در این نوع حمله، رنج شبکه تغییر کرده و کاربر یک رنج اشتباه را دریافت خواهد کرد. به طور مثال در صورتی که رنج شبکه ما ۱۰.۱۰.۱۰.۰ با زیر شبکه‌ی 24 است، حمله کننده یک IP از رنج ۱۹۲.۱۶۸.۱.۰ با زیر شبکه‌ی 26 به آن می‌دهد، با به وجود آوردن این تغییر این سیستم خاص امکان برقراری ارتباط با شبکه داخلی خود را ندارد و کار کردن با آن مختل می‌شود.

تغییر در تنظیمات default gateway

این حمله یکی از انواع حمله‌های ترکیبی به حساب می‌آید. نحوه کار شخص حمله کننده در این روش به این گونه است که در IP پیشنهاد شده به کاربر، IP خودش را به عنوان Default Gateway قرار می‌دهد. در مرحله بعدی حمله کننده با نصب کردن نرم افزارهای جاسوسی شبکه مانند Wireshark می‌تواند تمامی ارتباطات آن سیستم را مانیتور کند و از اطلاعات مورد نظر در راستای اهداف غیر قانونی خود استفاده کند.

تغییر در DNS سرور

این روش حمله کردن را می‌توان خطرناک‌ترین نوع حمله در بین این دسته از حملات به شمار آورد. ماهیت حمله به این صورت است که حمله کننده در مرحله اول حمله یک Website تقلبی مالی، اجتماعی، ایمیل و ... همانند وب سایت های دیگر را طراحی کرده است. مرحله بعد راه اندازی یک DNS سرور تقلبی است بدین صورت که به جای برگرداندن IP واقعی سایت مورد نظر کاربر(مثل Gmail.com، bank.com و ...) IP وبسایت خود را به کاربر انتقال می‌دهد. در این صورت تمامی اطلاعات اکانت کاربر به دست حمله کننده می‌رسد.

روش دیگر مورد استفاده حمله کننده برای تخریب سرویس DHCP

در روش‌های حمله‌ای که در مرحله قبل صحبت شد، فرض بر وجود داشتن همزمان هر دو سرور مخرب و اصلی در شبکه داخلی بود. در این حالت با توجه به زودتر رسیدن یا نرسیدن پیغام DHCP Offer سرور مخرب به کاربران، اطلاعات آن کاربران خاص توسط حمله کننده جاسوسی (Sniff) می‌شود، آیا از دید حمله کننده این روش یک روش بهینه است؟ آیا راه حلی برای sniff تمامی سیستم‌ها وجود دارد؟ پاسخ این‌جاست که در صورتی که سرور اصلی DHCP به گونه‌ای مورد حمله قرار گیرد که قادر به سرویس‌دهی نباشد، تمامی سیستم های درون شبکه را می‌توان تحت کنترل خود داشت.

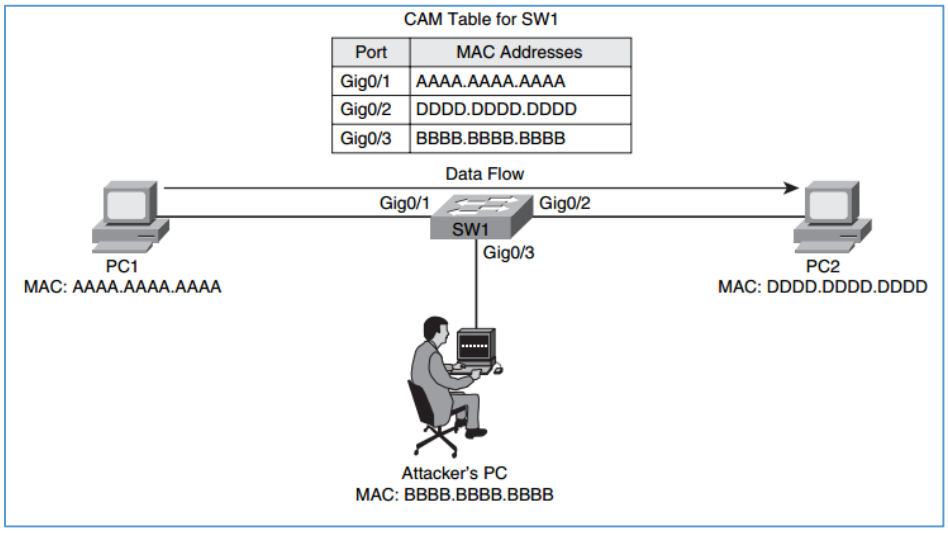
از این رو از روشی به نام Flooding برای از کار انداختن سرویس DHCP استفاده می‌شود. روش کار به این گونه است که حمله کننده با فرستادن درخواست‌های DHCP Discovery متوالی با MAC Address های تولید شده به صورت تصادفی پایگاه داده IPهای سرور DHCP را خالی می‌کند. حالا هنگامی که یک کاربر عادی DHCP Discovery را Broadcast می‌کند، دیگر سرور DHCP اصلی به دلیل موجود نداشتن IP پیغام DHCP Offer را نمی‌فرستد و تنها جواب از سمت سرویس DHCP راه‌اندازی شده توسط حمله کننده به دست کاربر می‌رسد.

نحوه دفاع در برابر حملات به سرور DHCP

حال که از دید حمله کننده با نحوه‌ی حمله به سرور DHCP آشنا شدیم، نوبت به بررسی راه‌حل‌های دفع حمله است. بدین منظور از دو روش Port-security و DHCP Snooping استفاده می‌شود.

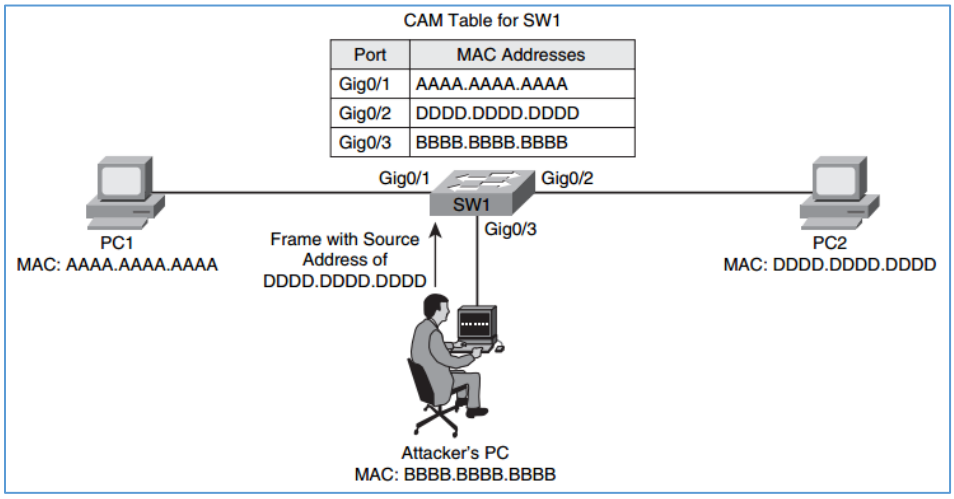
تحلیل و بررسی Spoofing MAC Addresses

همانطور که می‌دانید آدرس MAC یک آدرس منحصر به فرد می‌باشد و برای هر دستگاه یک آدرس در نظر گرفته خواهد شد، نوع دیگری از حمله جعل کردن آدرس Mac است که در زیر این روش را بررسی خواهیم کرد.

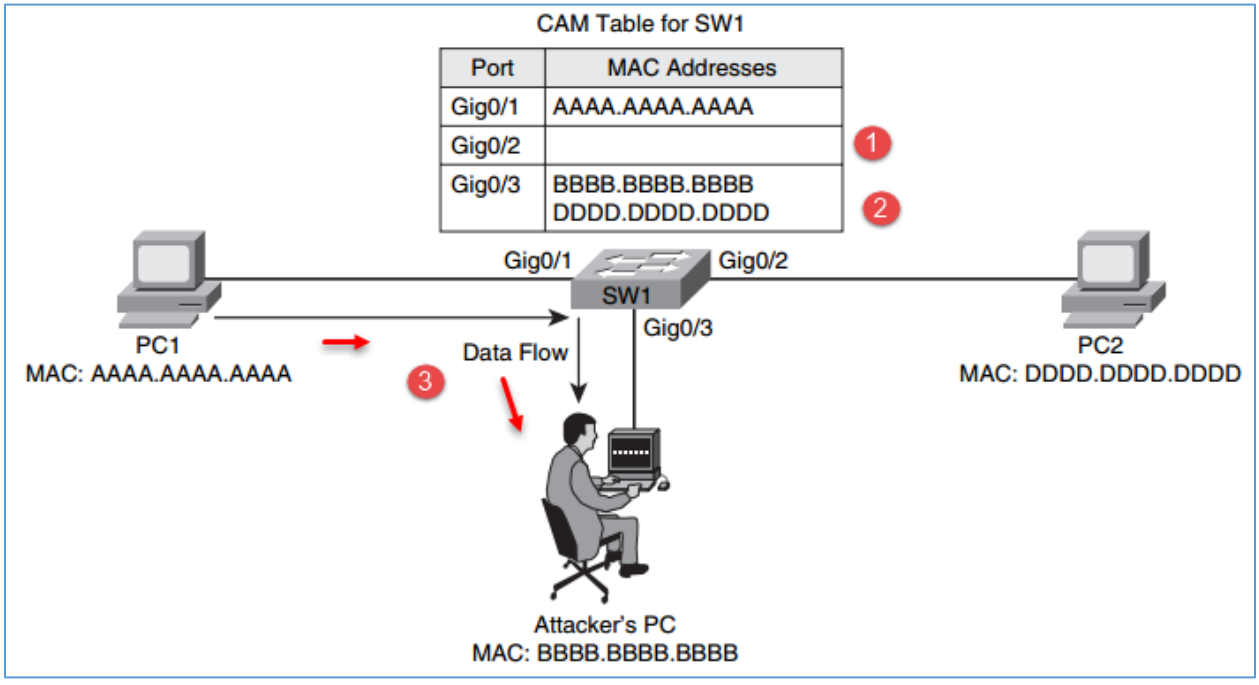


در شکل روبرو سه سیستم را مشاهده می‌کنید که به سوئیچ متصل شده‌اند و آدرس MAC آنها در جدول سوئیچ ثبت شده است.

در شکل زیر سیستم "Attacker's Pc " با ارسال یک Frame در شبکه آدرس مک جعلی خود یعنی DDDD.DDDD.DDDD که مربوط به PC2 است را به سوئیچ اعلام می‌کند، سوئیچ هم در زمان مشخص شده جدول خود را آپدیت می‌کند و با این کار ترافیکی که قبل از آن به سیستم PC2 ارسال می‌شد به سمت سیستم Attacker's ارسال می‌شود و با این روش اطلاعات به خطر خواهد افتاد.



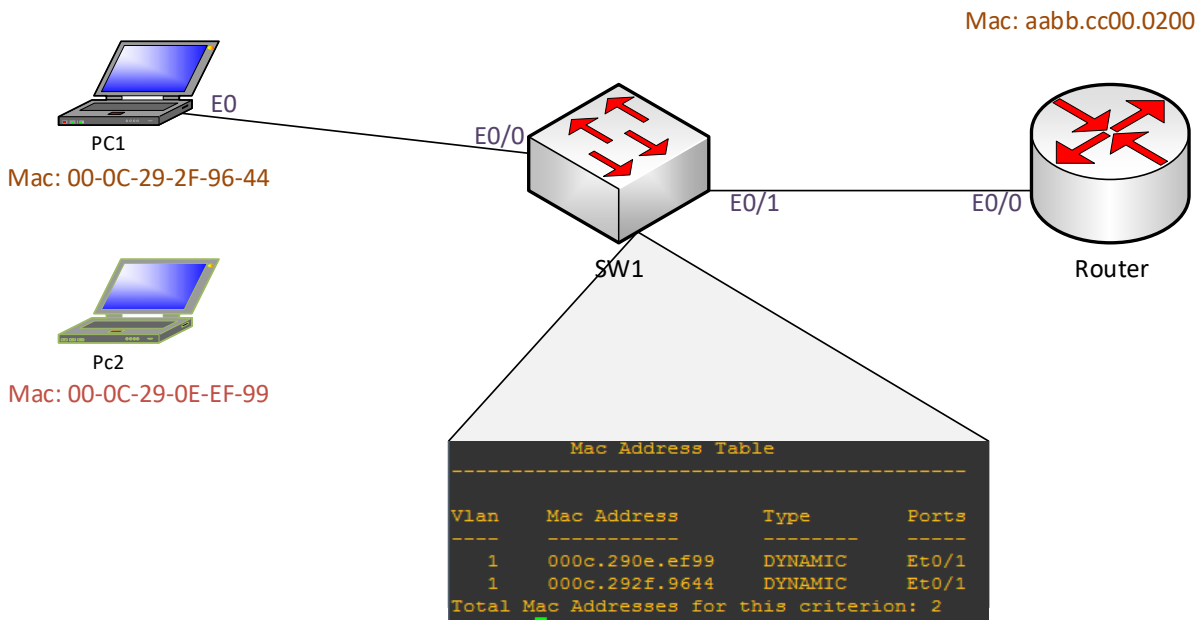
همانطور که در شکل زیر مشاهده می‌کنید، در قسمت اول در جدول سوئیچ آدرس MAC در پورت Gig0/2 که قبلاً به PC2 متصل شده بود خالی شده است و به جای آن در قسمت دوم پورت Gig0/3 دارای دو آدرس MAC است که یکی از آنها آدرس MAC جعلی مربوط به PC2 است و در قسمت شماره‌ی سه تمام ترافیک به روتر مهاجم ارسال خواهد شد، در قسمت بعد با استفاده از PortSecurity در سوئیچ امنیت ایجاد خواهیم کرد.



کار با Port Security

در این قسمت می‌خواهیم روش امنیتی Port Security را بر روی سوئیچ‌های سیسکو راه‌اندازی کنیم، مثالی که برای این روش می‌توان زد این است که اگر شبکه سازمان خود را در نظر بگیرید و کاربران شما بخواهند از منابع شبکه در سیستمی استفاده کنند که عضو آن شبکه نیست و واقعاً می‌تواند برای شبکه شما بسیار بد و یک ضعف امنیتی بزرگ باشد، اگر کاربر کابل شبکه متصل شده به سوئیچ را به لپ تاپ شخصی خود متصل کند، می‌تواند به منابع شبکه دسترسی پیدا کند.

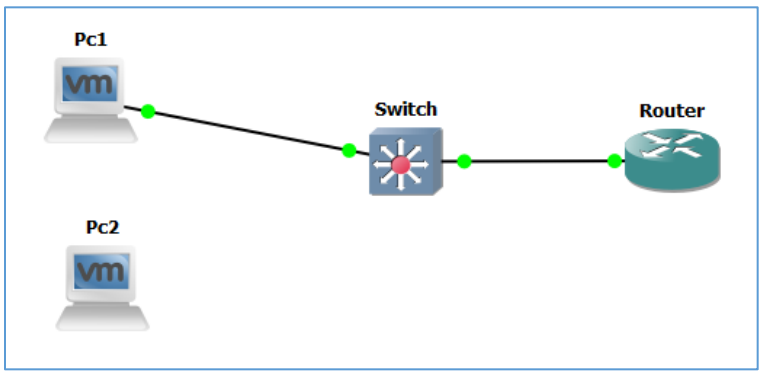
اما شرکت سیسکو برای جلوگیری از دزدیده شدن اطلاعات به این شکل روشی را تهت عنوان Port Security در سوئیچ‌های خود اضافه کرده که اگر چنانچه کاربری از یک سیستم غیرمجاز برای متصل شدن به شبکه استفاده کند، پورت مربوط به آن سیستم در سوئیچ خاموش خواهد شد و فقط توسط مدیر شبکه روشن می‌شود.



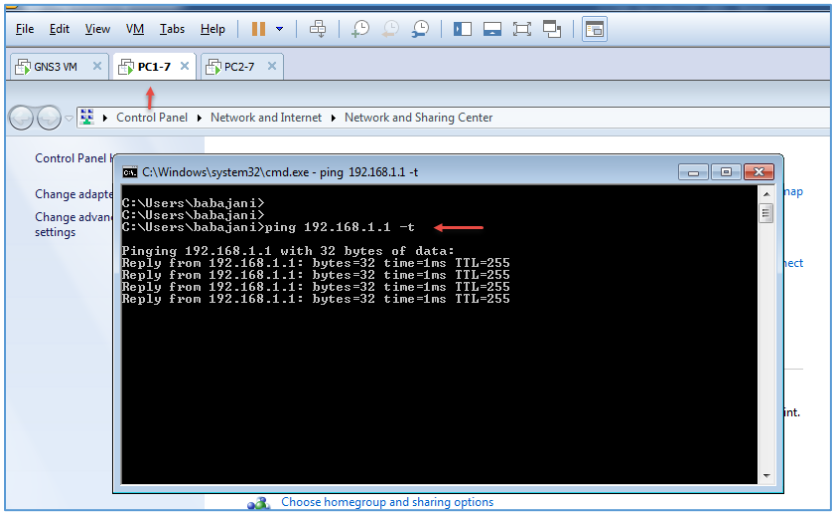
در شکل بالا که برای شما آماده کردیم دو Client به همراه یک سوئیچ و روتر را مشاهده می‌کنید که می‌خواهیم عملیات Port Security را روی آن انجام دهیم، در شکل بالا یک روتر و یک کلاینت به سوئیچ متصل شده‌اند و بعد از اتصال به پورت‌های آنها IP داده شده است.

Device	Port	Address
PC1	E0	192.168.1.2
Router	E0/0	192.168.1.1

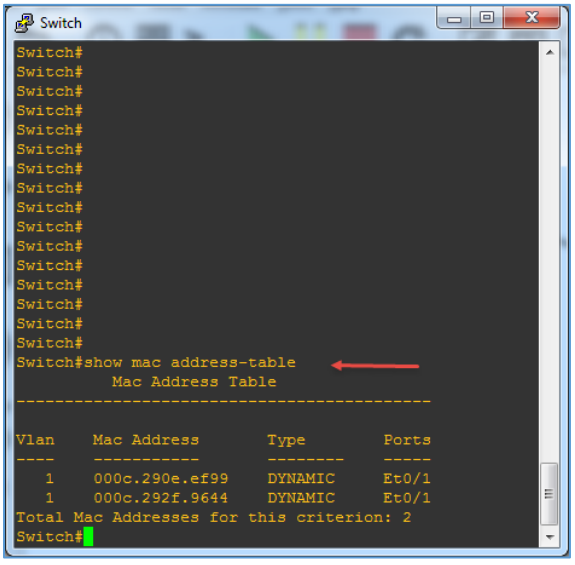
اگر به جدول MAC Table مربوط به سوئیچ(SW1) نگاه کنید، هر دو مک آدرس مربوط به روتر و کلاینت در آن ثبت شده است، حالا می‌خواهیم در ادامه با اجرای دستور Port Security اجازه ندهیم PC2 به سوئیچ متصل شود.



GNS3 را اجرا کنید و دو کلاینت که قبلاً با هم ایجاد کردیم و بر روی آنها ویندوز ۷ نصب کردیم را به لیست اضافه کنید، و یک سوئیچ لایه ۲ که در شکل با نام Switch مشخص است و یک سوئیچ لایه 3 که با نام Router مشخص شده است را به لیست اضافه کنید، تنظیمات مربوط به IP را بر روی روتر و کلاینت (PC1) که در جدول قبلی وارد کردیم را انجام دهید.



بعد از تنظیم IP وارد کلاینت PC1 شوید و روتر مورد نظر را Ping بگیرید، بعد از اینکه ارتباط اوکی بود به مرحله بعد می‌رویم.



وقتی یک دستگاه به سوئیچ متصل شود با اولین اتصال و درخواست کار از سوئیچ، آدرس Mac آنها در جدولی به نام Mac address Table ذخیره می‌شود و دستور Show Mac Address-Table به شما آدرس‌های Mac دستگاه‌های متصل شده به سوئیچ را نمایش می‌دهد.

در جدول زیر دستورات مربوط به Port Security را برای Interface بررسی می‌کنیم:

	دسورات	هدف
مرحله اول	Switch(config)# interface interface_id	با این دستور وارد Interface مورد نظر می‌شویم مانند: Interface Fastethernet 0/0
مرحله دوم	Switch(config-if)# switchport mode access	با این دستور پورت مورد نظر به نوع Access تغییر خواهد کرد، توجه داشته باشید به صورت پیش‌فرض تمام پورت‌های سوئیچ بر روی dynamic desirable قرار دارد که بر روی این نوع پورت نمی‌توان Port Security را فعال کرد.
مرحله سوم	Switch(config-if)# switchport port-security	برای فعال کردن Port Security بر روی interface مورد نظر باید از این دستور استفاده کرد.
مرحله چهارم	Switch(config-if)# switchport port-security maximum value	با این دستور می‌توانید مشخص کنید که تعداد مک آدرس‌هایی که بر روی این پورت قرار است فعالیت کنند را مشخص کنید که این عدد می‌تواند بین ۱ تا ٤٠٩٧ باشد که به صورت پیش‌فرض بر روی ۱ قرار دارد.
مرحله پنجم	Switch(config-if)# switchport port-security violation {restrict | Protect | shutdown}	از این دستورات هم برای ایجاد نقض در کار استفاده می‌شود یعنی اینکه اگر کاربری از یک MAC آدرس نا آشنا استفاده کند پورت مورد نظر خاموش خواهد شد، این دستور دارای سه گزینه است: Shutdown که به صورت پیش‌فرض فعال است و پورت مورد نظر را خاموش خواهد کرد. Protect

		در این حالت به بسته‌هایی اجازه‌ی عبور می‌دهد که آدرس Mac آنها در سوئیچ تعریف شده باشد. Restrict این دستور هم به مانند دستور قبلی عمل می‌کند اما در قسمتی از دستور Show Port-Security در ستون Violation شماره‌ی آن را تغییر می‌دهد.
مرحله ششم	Switch(config-if)# switchport port-security limit rate invalid-source-mac	تعیین نرخ بسته‌های اشتباه.
مرحله هفتم	Switch(config-if)# switchport port-security mac-address mac_address	با این دستور می‌توانید به صورت دستی Mac Address سیستمی که قرار است به پورت مورد نظر متصل شود را وارد کنید.
مرحله هشتم	Switch(config-if)# switchport port-security mac-address sticky	این دستور باعث می‌شود که مک آدرس مربوط به سیستم مورد نظر به صورت اتوماتیک در جدول سوئیچ قرار بگیرد و نیاز به ورود به صورت دستی نیست.
مرحله نهم	Switch# show port-security address interface interface_id Switch# show port-security address	نمایش جزئیات عملکرد دستور Port Security به صورت کلی و بر روی Interface .

بعد از آشنایی با دستورات، حالا نوبت آن رسیده که این دستورات را روی سوئیچ پیاده کنیم، برای این کار طبق نقشه‌ای که در صفحات قبل ایجاد کردیم، بر روی سوئیچ مورد نظر دو بار کلیک کنید و دستورات زیر را وارد کنید.

Switch#configur Terminal	با این دستور وارد مد Global شوید.

Switch(config)#interface ethernet 0/0	با این دستور وارد پورت ethernet 0/0 می‌شویم که به سیستم کلاینت PC1 متصل است.
Switch(config-if)#switchport mode access	دستور مورد نظر مد پورت را به Access تغییر می‌دهد تا دستور Port Security بتواند بر روی آن اجرا شود.
Switch(config-if)#switchport Port-Security	دستور switchport Port-Security ویژگی Port Security را بر روی Interface مورد نظر فعال می‌کند.
Switch(config-if)#switchport Port-Security mac-address sticky	با این دستور به سوئیچ اعلام می‌کنیم که مک آدرس سیستمی که به این پورت متصل است را دریافت و در جدول خودت قرار بده.
Switch(config-if)#switchport Port-Security maximum 1	در این قسمت باید مشخص کنید در این پورت چند Mac Address قابلیت اضافه شدن به لیست دارند که در این دستور عدد ۱ انتخاب شده و فقط اولین سیستمی که به این پورت متصل شده آدرس Mac آن در لیست قرار می‌گیرد.
Switch(config-if)#Switchport port-security violation Shutdown	اگر در دستور قبلی Mac آدرسی به غیر از Mac آدرس سیستم فعلی بخواهد به متصل شود عملیات خاموش شدن پورت روی آن فعال خواهد شد، و فقط مدیر شبکه می‌تواند آن را روشن کند.

بعد از اجرای دستورات بالا و فعال‌سازی قابلیت Port Security می‌توانید با اجرای دستور زیر از وضعیت این دستور با خبر شوید.

Switch(config-if)# Show Port-Security

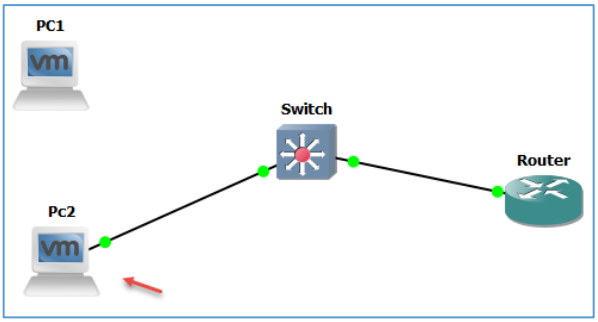
```
Switch(config-if)#do sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Et0/0          1             1                0          Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

همانطور که در شکل صفحه قبل مشاهده می‌کنید بر روی پورت E0/0 این سرویس فعال شده است، در ستون شماره‌ی یک مقدار آدرس مشخص شده است که فقط یک آدرس اجازه دارد در جدول قرار بگیرد، در ستون شماره‌ی دو این یک آدرس توسط Pc1 تکمیل شده است و اگر سیستم دیگری را به آن پورت متصل کنید در قسمت شماره‌ی سه به جای صفر عدد یک قرار خواهد گرفت و بعد در قسمت شماره‌ی چهار هم عملیات Shutdown اجرا خواهد شد. برای اینکه آدرس Mac ذخیره شده بر روی پورت مورد نظر را مشاهده کنید باید از دستور زیر استفاده کنید:

```
Switch#show port-security address
```

```
Switch#show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    000c.292f.9644    SecureSticky                  Et0/0       -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

در شکل روبرو دستور مورد نظر اجرا و آدرس MAC و شماره پورت آن مشخص شده است.



حالا برای اینکه سرویس Port Security را تست کنیم، در پروژه‌ی مورد نظر کابل PC2 را به پورتی متصل می‌کنیم که PC1 به آن متصل بوده است، با اولین پکتی که به سمت سوئیچ ارسال شود پورت مورد نظر خاموش خواهد شد.

```
Switch(config-if)#
*Sep 16 08:08:48.132: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disab
le state
Switch(config-if)#
*Sep 16 08:08:48.132: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0
00c.290e.ef99 on port Ethernet0/0.
*Sep 16 08:08:49.139: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Switch(config-if)#
*Sep 16 08:08:50.134: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
```

همانطور که در شکل بالا مشاهده می‌کنید سرویس Port Security بر روی پورت E0/0 که آدرس Mac آن تغییر کرده اجرا شده است و پورت مورد نظر خاموش شده است و سیستم Pc2 نمی‌تواند از منابع شبکه استفاده کند، البته خود سیستم PC1 هم اگر دوباره به پورت E0/0 متصل شود باز هم پورت مورد نظر خاموش خواهد بود و حتماً باید مدیر مربوطه دستوراتی را که در ادامه بررسی می‌کنیم را اجرا کند تا آن پورت روشن شود.

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
     Et0/0            1            1                1         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

بعد از اینکه پورت مورد نظر خاموش شد اگر دستور Show Port-Security را اجرا کنید در جلوی زیر ستون چهارم عدد یک قرار گرفته و نشان دهنده این است که تناقضی در MAC آدرس ایجاد شده است.

برای اینکه پورتی که خاموش شده را روشن کنیم دو راه وجود دارد:

۱- حذف کردن دستورات Port Security، که باید قبل از همه‌ی دستورات حرف No را قرار دهید و بعد از این کار پورت مورد نظر را روشن کنید.

۲- یا می‌توانید زمان Recovery را برای سوئیچ تغییر دهید، به این صورت که زمانی که پورت مورد نظر خاموش می‌شود با دستوری مشخص شود که بعد از چه زمانی دوباره به حالت اول برگردد.

```
Switch(config)#errdisable recovery cause psecure-violation
```

با این دستور تمام پورت‌هایی که بر روی آنها Port Security اجرا شده در حالت Errdisable قرار خواهند گرفت.

```
Switch(config)#errdisable recovery interval 60
```

در این دستور عدد ٦٠ یعنی ٦٠ ثانیه، بعد از این زمان حالت Errdisable اجرا خواهد شد و پورت مورد نظر روشن خواهد شد، اگر در این ٦٠ ثانیه سیستم Pc1 به سوئیچ متصل شده باشد پورت مورد نظر روشن باقی خواهد ماند و اگر نباشد دوباره آن پورت خاموش می‌شود.

بعد از اجرای دستور بالا، بعد از ٦٠ ثانیه قسمت سبز رنگ شکل زیر نمایش داده می‌شود و پورت مورد نظر روشن خواهد شد و بعد از این کار MAC آدرس دویاره بررسی خواهد شد اگر با آدرسی که در Port Security ذخیره شده هماهنگ باشد پورت مورد نظر روشن خواهد ماند و اگر درست نباشد دوباره به مانند شکل در قسمت آبی رنگ پورت خاموش خواهد شد.

```
Switch#
*Sep 16 11:09:06.469: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Et0/0
Switch#
*Sep 16 11:09:08.469: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Sep 16 11:09:09.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch#
*Sep 16 11:09:54.375: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/0, putting Et0/0 in err-disable state
Switch#
*Sep 16 11:09:54.375: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 000c.290e.ef99
 on port Ethernet0/0.
*Sep 16 11:09:55.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Switch#
*Sep 16 11:09:56.384: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
Switch#
```

اضافه کردن MAC آدرس به صورت دستی

شاید بخواهید بر روی یک پورت سوئیچ چند آدرس MAC تعریف کنید، تا همزمان چند دستگاه شبکه بتوانند از آن پورت استفاده کنند، برای تعریف این کار باید به صورت زیر عمل کنید.

اول از همه باید مقدار ورودی MAC آدرس را تغییر دهید، در قسمت قبلی مقدار MAC آدرس را بر روی یک قرار دادیم، که اگر بخواهید مقدار بیشتری را در لیست قرار دهید باید آن مقدار را تغییر دهید:

```
Switch(config-if)#switchport port-security maximum 5
```

با این دستور می‌توانید به مقدار پنج آدرس MAC به لیست سوئیچ اضافه کنید، توجه داشته باشید برای پاک کردن دستورات میتوانید از کلمه‌ی No در اول آنها استفاده کنید.

```
Switch(config-if)#switchport-security mac-address 54-04-A6-B1-6C-B0
```

در این دستور آدرس MAC مورد نظر به صورت دستی به لیست اضافه شده است.

```
Switch(config-if)#do sh port-security address
              Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    000c.290e.ef99    SecureDynamic                 Et0/0       -
   1    000c.292f.9644    SecureDynamic                 Et0/0       -
   1    0026.5a71.601a    SecureConfigured              Et0/0       -
   1    5404.a6b1.6cb0    SecureConfigured              Et0/0       -
   1    5404.a6b1.fc20    SecureConfigured              Et0/0       -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 4
Max Addresses limit in System (excluding one mac per port) : 4096
```

در این قسمت با دستور Show Port-security Address لیست ۵ آدرس MAC را مشاهده می‌کنید، اگر به ستون Type نگاهی بیندازید، دو گزینه وجود دارد که یکی Dynamic یعنی همان اتوماتیک و دیگری Configured که به صورت دستی مشخص می‌کند که MAC آدرس به لیست مورد نظر اضافه شده است.

```
Switch(config-if)#do sh port-security interface E0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 5
Configured MAC Addresses   : 3
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.290e.ef99:1
Security Violation Count   : 0
```

با دستور Show Port-Security interface E0/0 می‌توانید مشاهده کنید که روی پورت Ethernet0/0 سرویس Port Security فعال است یا نه، که در تصویر فعال بودن این سرویس با گزینه‌ی Enabled مشخص شده است.

حذف آدرس MAC بعد از غیر فعال شدن کلاینت

در این قسمت می‌خواهیم روشی را با هم بررسی کنیم که اگر کلاینتی بعد از مثلاً ۱۰ دقیقه ارتباط خود را با سوئیچ قطع کرد، آدرس MAC آن از لیست سوئیچ مورد نظر حذف شود، برای این کار از دستورات زیر استفاده کنید:

```
Switch(config-if)#switchport port-security aging time  10
```

در دستور بالا مقدار زمان Agin برابر ۱۰ دقیقه قرار گرفته است که این زمان می‌تواند بین ۱ تا ۱٤٤۰ دقیقه متغیر باشد، اگر در این ۱۰ دقیقه ارتباط کلاینت‌ها با سوئیچ قطع شود، آدرس Mac آنها از لیست حذف خواهد شد.

```
Switch(config-if)#switchport port-security aging type inactivity
```

این دستور نوع Aging را بر روی inactivity قرار می‌دهد، یعنی اینکه از زمان پشتیبانی می‌کند و با دستور قبلی هماهنگ می‌شود.

```
Switch(config-if)#switchport port-security aging time 10
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#do sh port-security address
            Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0026.5a71.601a    SecureConfigured              Et0/0       -
   1    5404.a6b1.6cb0    SecureConfigured              Et0/0       -
   1    5404.a6b1.fc20    SecureConfigured              Et0/0       -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 4096
```

در این شکل دو دستور مشخص شده اجرا شده است، بعد از این دستورات ارتباط کلاینت‌ها را با سوئیچ قطع کنید و بعد از ده دقیقه دستور Show Port-security address را اجرا کنید که مشاهده خواهید کرد که دو آدرس MAC که به صورت اتوماتیک به لیست اضافه شده بودند در این قسمت حذف شدند.

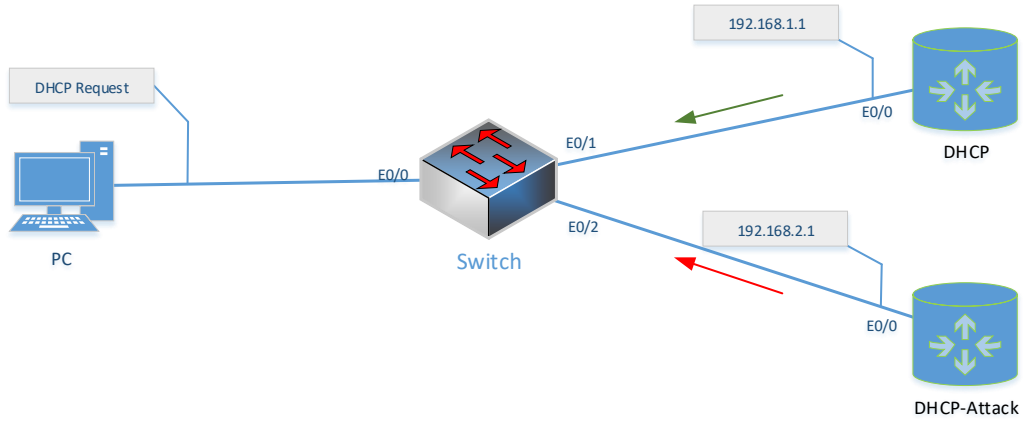
```
Switch(config-if)#do sh port-security interface e0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 3
Configured MAC Addresses   : 3
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.290e.ef99:1
Security Violation Count   : 0
```

با اجرای دستور Show Port-Security interface e0/0 در قسمت مشخص شده Aging Time و Aging Type مشخص شده است.

تحلیل و بررسی DHCP Snooping

حتماً در شبکه‌ی خود از سرویس پرکاربرد DHCP استفاده می‌کنید، یکی از بزرگترین مشکلاتی که این سرویس میتواند ایجاد کند، این است که یک سرویس دهنده‌ی DHCP دیگری به اشتباه یا به صورت عمدی وارد شبکه شود و کلاینت‌های شبکه به اشتباه با سرویس دهنده‌ی جدید ارتباط برقرار می‌کنند و آدرس IP و اطلاعات در این زمینه را از سرور غیر واقعی دریافت می‌کنند، این مورد می‌تواند یکی از انواع حملات به شبکه باشد که برای حل آن باید از ویژگی DHCP Snooping استفاده کرد که در ادامه آن را بررسی خواهیم کرد.

برای شروع شکل زیر را پیاده سازی کنید:



در شکل صفحه بالا دو روتر به عنوان سرویس دهنده‌ی DHCP ایفای نقش می‌کنند و PC برای دریافت اطلاعات از DHCP درخواست IP می‌کند، روتری که با نام DHCP در شکل قرار دارد همان DHCP اصلی است که کلاینت PC باید اطلاعات IP را از آن دریافت کند، ولی اگر یک مهاجم یک سرویس DHCP دیگر که در شکل با نام DHCP Attack معرفی شده را در شبکه فعال کند می‌تواند PC را وادار کند تا از اطلاعات آن استفاده کند، برای حل این مشکل باید سرویس DHCP Snooping را فعال کنیم.

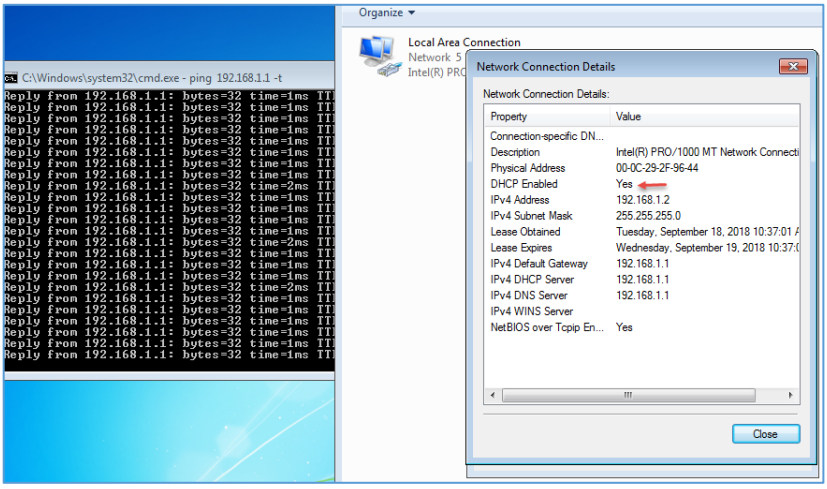
برای شروع، روی هر دو روتر سرویس DHCP را با دستورات زیر فعال می‌کنیم:

تنظیمات روتر DHCP

در مورد سرویس DHCP در کتاب CCNA++ آموزش کامل را دادم که می‌توانید آن را مطالعه کنید.

در این دستور یک Pool با نام P1 ایجاد می‌کنیم.	Switch(config-if)#ip dhcp pool p1

Switch(config-if)#network 192.168.1.0 255.255.255.0	آدرس زیر شبکه مربوط به شبکه DHCP را وارد می‌کنیم.
Switch(config-if)#default-router 192.168.1.1	این قسمت مربوط به تعریف Gateway است.
Switch(config-if)#dns-server 192.168.1.1	تعریف سرور DNS که خود سرور DHCP است.



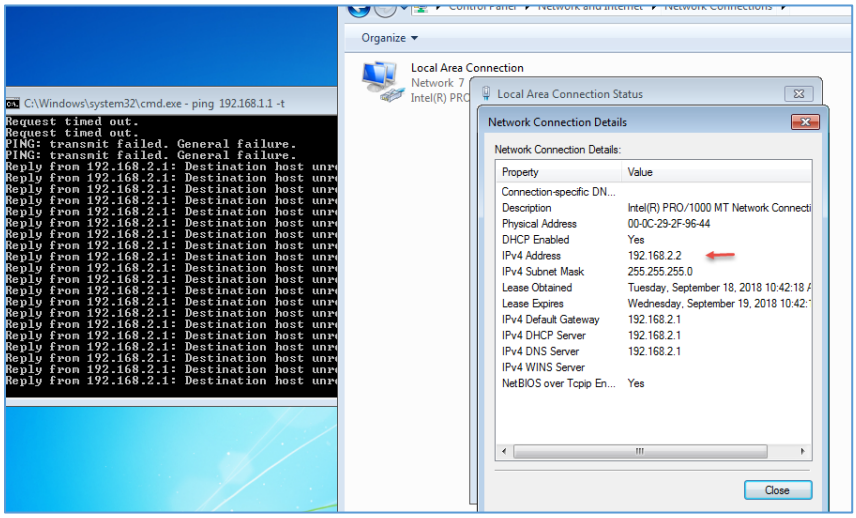
بعد از اینکه سرویس DHCP فعال شد اگر وارد کلاینت شوید و کارت شبکه را بر روی حالت اتوماتیک قرار دهید به مانند شکل روبروIP را از روتر DHCP دریافت خواهد کرد و روتر DHCP را می‌توان Ping کرد.

تنظیمات روتر DHCP - Attack

بعد از اینکه روتر DHCP را فعال کردید و کلاینت Pc هم از آن IP دریافت کرد، حالا می‌خواهیم روتر دوم را برای DHCP فعال کنیم، برای این کار از دستورات زیر استفاده کنید.

Switch(config-if)#ip dhcp pool p2	در این دستور یک Pool با نام P2 ایجاد می‌کنیم.
Switch(config-if)#network 192.168.2.0 255.255.255.0	آدرس زیر شبکه مربوط به شبکه DHCP را وارد می‌کنیم.
Switch(config-if)#default-router 192.168.2.1	این قسمت مربوط به تعریف Gateway است.

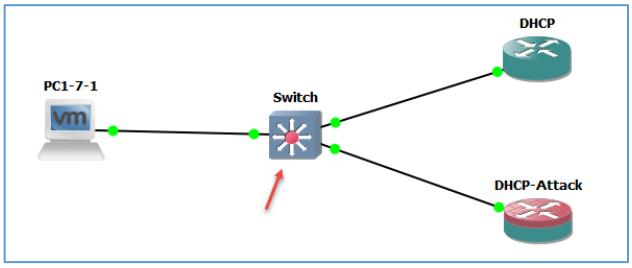
Switch(config-if)#dns-server 192.168.2.1	تعریف سرور DNS که خود سرور DHCP است.



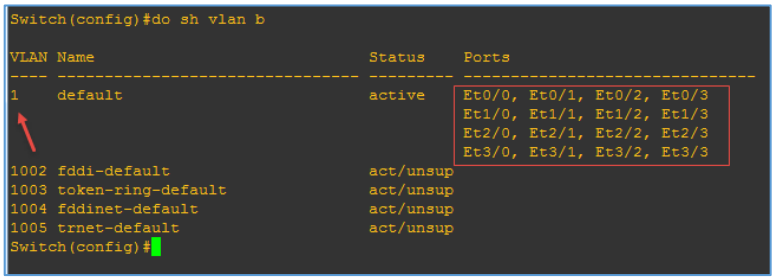
بعد از فعال کردن روتر دوم اگر کارت شبکه مربوط به Pc را غیرفعال و دوباره فعال کنید، آدرسی که از شبکه خواهد گرفت یک آدرس جدید در رنج روتر DHCP-Attack است که این همان مشکی است که در قسمت‌های قبلی بیان کردیم.

برای حل چنین مشکلی باید یک سری دستورات را در سوئیچ وارد کنیم تا مشخص کنیم که سرور اصلی DHCP کدام است.

همان‌طور که همه‌ی شما در جریان هستید تمام پورت‌های سوئیچ‌ها به صورت پیش‌فرض در Vlan 1 قرار دارند و البته می‌توانید Vlanهای مختلفی تعریف و پورت‌ها را به آن اضافه کنید، برای اینکه سرویس DHCP Snooping را فعال کنیم باید اول این سرویس را روی Vlan اجرا کنیم.



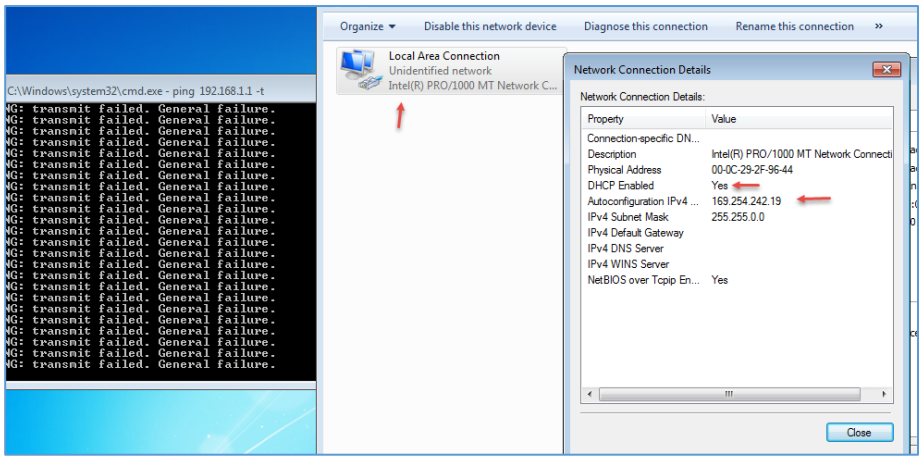
برای شروع کار بر روی Switch دو بار کلیک کنید تا وارد صفحه Command آن شوید.



با دستور Show Vlan brief می‌توانید شماره VLan را مشاهده کنید که در این قسمت شماره یک است و همه پورت‌ها در آن قرار دارند.

با این دستور سرویس DHCP Snooping فعال خواهد شد.	Switch(config)#ip dhcp snooping
با این دستور سرویس Snooping بر روی Vlan1 فعال خواهد شد.	Switch(config)#ip dhcp snooping vlan 1

بعد از فعال کردن دو دستور بالا دیگر هیچ سرویس دهنده‌ی DHCP نمی‌تواند به کلاینت‌ها IP ارائه دهد.



بعد از اینکه دو دستور را در سوئیچ اجرا کردید اگر Pc درخواست IP دهد دیگر سوئیچ به هیچ سرویس دهنده‌ی DHCP این اجازه را نخواهد داد و کلاینت IP اشتباه خواهد گرفت.

برای اینکه روتر DHCP اصلی را به سوئیچ معرفی کنیم و بگوییم که این روتر همان روتر DHCP اصلی ما است باید از دستور زیر در پورتی که به روتر DHCP متصل است استفاده کنیم:

Switch(config)#interface Ethernet 0/2

با این دستور وارد Interface Ethernet 0/2 که به روتر DHCP متصل شده است.

Switch(config-if)#ip dhcp snooping trust

با این دستور به سوئیچ اعلام می‌کنیم که این پورت که به روتر DHCP متصل است جزو پورت‌هایی باشد که اجازه دارد سرویس DHCP روی آن فعال باشد.

بعد از اینکه پورت مورد نظر را Trust کردید، باید بقیه پورت‌های سوئیچ را Untrust یا غیر قابل اعتماد کنید، برای این کار کافی است وارد پورت مورد نظر شوید و دستو زیر را اجرا کنید:

Switch(config)#int range e0/3-24

با این دستور وارد رنجی از پورت که از شماره‌ی ۳ تا ۲٤ است شدیم، البته می‌توانید فقط وارد یک پورت شوید.

```
Switch(config-if-range)#no ip dhcp snooping trust
```

با این دستور همه پورت‌ها Untrust می‌شوند.

با دستور show ip dhcp snooping می‌توانید مشاهده کنید که چه پورت‌هایی فعال و چه پورت‌هایی غیرفعال هستند، اگر به دستور زیر توجه کنید در ستون Trusted گزینه‌ی Yes و No قرار داده شده است.

```
Switch#show ip dhcp snooping
Interface            Trusted    Rate limit (pps)
-----------------    -------    ------------------------
Ethernet0/2          yes        unlimited
Ethernet0/1          no         unlimited
```

تحلیل و بررسی Private VLAN

در این بخش می‌خواهیم به دنیای VLAN سری بزنیم، همانطور که می‌دانید همه کلاینت‌ها و سرورها برای دسترسی به شبکه به سوئیچ متصل می‌شوند و همه‌ی پورت‌های سوئیچ هم در یک VLAN قرار دارد ولی بین آنها هیچ امنیتی وجود ندارد و همه‌ی کلاینت‌ها می‌توانند همدیگر را ببینند، ولی در کل نیازی نیست که کلاینت‌ها بتوانند به یک سری از سروروها دسترسی داشته باشند و باید دسترسی آنها را با استفاده از Private VLAN قطع کرد که این کار را در این قسمت با هم انجام می‌دهیم.

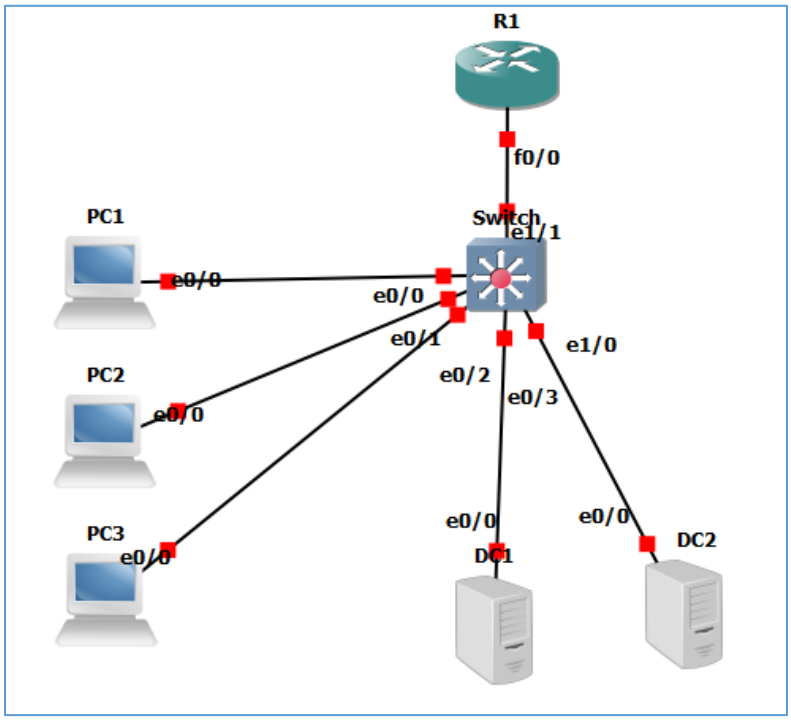
Private VLAN به دو نوع مختلف تقسیم می‌شود که در زیر مشاهده می‌کنید.

Primary VLAN یا همان VLAN اصلی که می‌تواند به همه سرورها و کلاینت‌ها متصل باشد.

Secondary VLAN یا همان VLAN ثانویه خود به دو بخش Isolated و Community تقسیم می‌شود که سیستم‌هایی که در VLAN از نوع Isolated در نظر گرفته می‌شوند با هیچ کلاینت یا سروری در ارتباط نخواهند بود و فقط با VLAN از نوع Primary در ارتباط خواهند بود.

کلاینت‌هایی که در VLAN از نوع Community در نظر گرفته می‌شوند فقط می‌توانند با کلاینت‌هایی که در همان VLAN Community قرار دارند ارتباط برقرار کنند، مثلاً ارتباط یک اتاق خاص با هم، البته این نوع VLAN می‌تواند با VLAN از نوع Primary ارتباط داشته باشد.

در این قسمت یک مثال در مورد Private Vlan را با هم بررسی می‌کنیم تا به صورت عملی عملکرد این VLAN را مورد تست قرار دهیم.



طبق شکل روبرو یک روتر، یک سوئیچ، دو سرور و سه کلاینت را به لیست GNS3 اضافه کنید.

در زیر لیست آدرس IP برای هر کدام از سیستم‌ها را مشاهده می‌کنید، طبق جدول به هر یک از سیستم‌ها IP مورد نظر آنها را تخصیص دهید و بعد از این کار دستور Ping را اجرا کنید تا از ارتباط بین آنها مطمئن شوید.

System Name	IP Address
R1	192.168.1.1
PC1	192.168.1.2
PC2	192.168.1.3
PC3	192.168.1.4
DC1	192.168.1.5
DC2	192.168.1.6

برای اینکه بتوانیم از دستورات Privat Vlan در سوئیچ استفاده کنید باید پروتکل VTP را در حالت Transparent قرار دهید تا این دستورات در سوئیچ قابل قبول باشد.

```
Switch#conf t
Switch(config)#vtp mode transparent
```

با دستور بالا VTP در حالت Transparent قرار خواهد گرفت.

در ادامه کار سه کلاینت PC1 , PC2 , PC3 را در یک VLAN شماره‌ی ۱۰۰ قرار می‌دهیم و نوع VLAN آن را community در نظر می‌گیریم.

```
Switch(config)#vlan 100
Switch(config-vlan)#private-vlan community
```

در دستور بالا Vlan با شماره ۱۰۰ تعریف شده و نوع آن را community در نظر گرفتیم که در ادامه کار این Vlan را به پورت‌های کلاینت‌ها تخصیص می‌دهیم.

```
Switch(config)#vlan 200
Switch(config-vlan)#private-vlan isolated
```

در دستور بالا VLAN با شماره‌ی ۲۰۰ ایجاد کردیم که نوع آن را isolated در نظر گرفیم که باید به سرورهای DC1 و DC2 بدهیم.

```
Switch(config)#vlan 300
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#private-vlan association 100,200
```

با دستور بالا VLAN به شماره‌ی ۳۰۰ از نوع Primary در نظر گرفته شده که باید به پورتی تخصیص دهیم که به سمت روتر ارسال می‌شود، در دستور آخر هم باید مشخص کنیم چه VLanهایی با VLAN Primary در ارتباط هستند.

تا به اینجا سه تا VLAN تعریف کردیم که نوع آنها را مشخص کردیم، حال در ادامه می‌خواهیم پورت‌های هر سیستم را به این VLANها تخصیص دهیم.

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 300 100,200
```

در دستور بالا وارد پورت ethernet 1/1 که به روتر R1 متصل است شدیم، بعد از آن از دستور promiscuous برای معرفی این پورت به عنوان پورت اصلی استفاده می‌کنیم ، در ادامه برای اینکه شماره‌ی VLAN اصلی و فرعی را به این پورت معرفی کنیم از دستور switchport private-vlan mapping 300 100,200 استفاده می‌کنیم که

شماره‌ی اول که ۳۰۰ است مربوط به VLAN Primary است که مربوط به همین پورت است و شماره‌های ۱۰۰ و ۲۰۰ که مربوط به VLANهای دیگر است باید به این پورت معرفی کنیم تا دسترسی لازم را به آن داشته باشند.

```
Switch(config-if)#interface range ethernet 0/0-2
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 300 100
```

در دستور بالا وارد سه پورتی شدیم که به PC1 ,PC2 ,PC3 متصل شده است، با دستور switchport mode private-vlan host به پورت مورد نظر اعلام کردیم که این سه پورت به کلاینت متصل خواهد شد و دستور switchport private-vlan host-association 300 100 هم برای معرفی VLAN اصلی و فرعی کاربرد دارد.

نکته: دستور Host عموماً به سیستم‌هایی داده می‌شود که در شبکه داخلی قرار داشته باشند و بخواهند با دنیای بیرون ارتباط برقرار کنند.

```
Switch(config)#int e0/3
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 300 200
Switch(config-if)#int e1/0
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 300 200
```

در دستورات بالا وارد دو پورتی شدیم که به سرور DC1 و DC2 متصل شده است و دستور مورد نظر را برای آنها اجرا کردیم.

تا به اینجا توانستیم VLAN مورد نظر را تعریف کنیم و پورت‌های مشخص شده را درون VLAN قرار دهیم، حال اگر بخواهیم کارکرد این عمل را مشاهده کنیم، می‌توانیم از دستور زیر استفاده کنیم:

```
Switch#show vlan private-vlan
Primary  Secondary  Type            Ports
-------  ---------  ----------------  -----------------------------------------
300      100        community       Et0/0, Et0/1, Et0/2, Et1/1
300      200        isolated        Et0/3, Et1/0, Et1/1
```

با استفاده از دستور show vlan private-vlan می‌توانید مشاهده کنید که چه VLANهایی به عنوان VLAN اصلی و ثانویه انتخاب شده‌اند و نوع آنها را می‌توانید مشاهده کنید، در قسمت Port هم مشخص شده است که Et0/0 که به عنوان پورت Primary در نظر گرفتیم در هر دو قسمت قرار دارد .

تحلیل و بررسی IP source guard

پروتکل اصلی برای ارسال داده‌ها در شبکه اینترنت و بسیاری از شبکه‌های کامپیوتری پروتکل اینترنت یا همان IP است. سرآیند هر بسته IP شامل فیلدهای مختلفی می‌باشد، از جمله آدرس مبدأ و مقصد بسته. در حالت کلی آدرس مبدا، آدرسی است که بسته را ارسال کرده‌است. با جعل کردن سرآیند بسته، این آدرس تغییر می‌کند و به آدرس دیگر اشاره می‌کند و مهاجم می‌تواند این‌طور نشان دهد که بسته توسط ماشین دیگری ارسال شده‌است. بنابراین ماشینی که بسته جعل شده را دریافت می‌کند، پاسخ را به آدرس مبدأ جعل شده ارسال می‌کند، همان‌طور که از این توضیحات نیز مشخص می‌شود، این روش اصولاً زمانی استفاده می‌شود که مهاجم به پاسخ اهمیتی نمی‌دهد یا می‌تواند از روش‌های مختلفی پاسخ را حدس بزند. البته در موارد خاص، مهاجم می‌تواند پاسخ را ببیند یا آن را به سمت ماشین خود هدایت نماید. این موارد بیشتر زمانی است که مهاجم آدرسی را در LAN یا WAN یکسانی جعل می‌کند.

جعل آدرس IP، در حقیقت حیله ایست که معمولاً بر روی سرورها اعمال می‌شود و معمولاً بدین منظور استفاده می‌شود که سیستم مقابل را طوری فریب دهد تا فرض کند مقصدی که از آن اطلاعات دریافت می‌کند شما نیستید! در نهایت کامپیوتر مقصد بسته‌های اطلاعاتی را از شما دریافت خواهد کرد اما پیش خود بر این فرض خواهد بود که این بسته‌ها از ماشین دیگری دریافت می‌شوند. مثالی در این زمینه این مطلب را روشن تر می‌سازد: در این مثال: IP Address خود را به صورت فرضی 203.45.98.1 (واقعی) در نظر می‌گیریم. IP Address سیستم قربانی را نیز 202.14.12.1 (قربانی) در نظر گرفته می‌شود. IP Address را هم که می‌خواهیم وانمود کنیم متعلق به ما است را برابر 202.14.12.1 (تقلبی) است. در حالت عادی، هنگامی که دیتا گرام‌ها از کامپیوتری با آدرس IP واقعی به سمت قربانی خارج می‌شود، مسلماً اطلاعات دریافتی توسط قربانی نیز مشخصه آدرس IP شما را در بر دارد و این به این معنا است که کاملاً طرف مقابل کامپیوتر قربانی (که شما هستید)، به راحتی قابل شناسایی خواهد بود. اکنون حالتی را در نظر بگیرید که شما می‌خواهید بسته‌هایی را برای قربانی ارسال کنید، اما او گمان

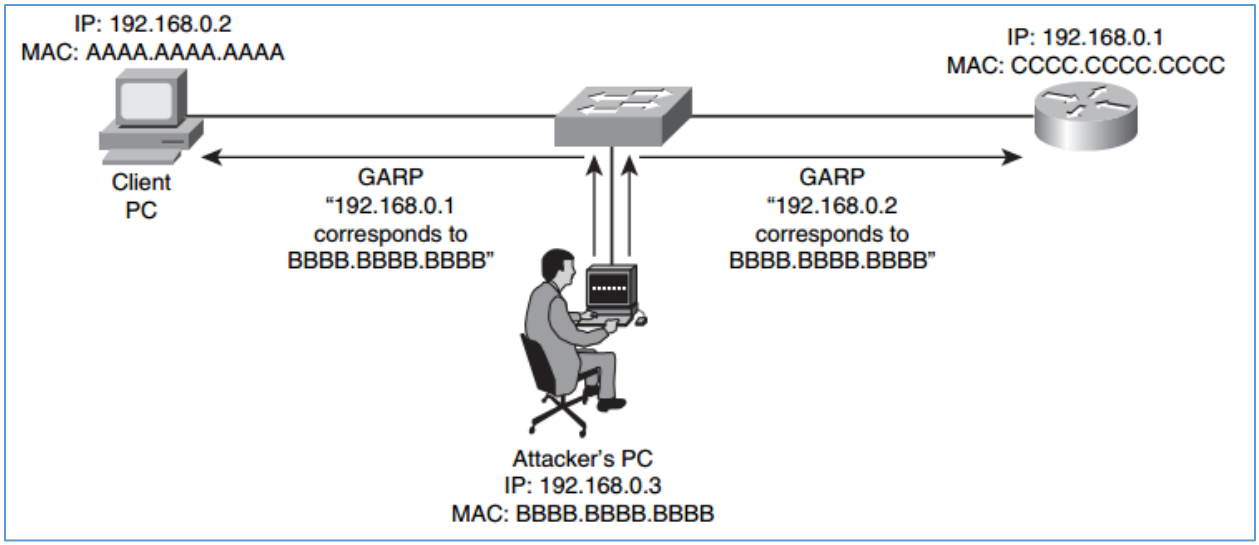
کند که این بسته‌ها از سیستم تقلبی دیگر(Fake) با آدرس IP برابر 173.23.45.89 می‌آیند. در این حالت بایستی از مکانیزم جعل آدرس IP استفاده کرد.

جهل آدرس IP همیشه بد نخواهد بود و برای تست هم به کار می‌رود تا از امنیت آن مطلع وب‌سایت و شبکه با خبر شوند.

تحلیل و بررسی Dynamic Arp Inspection

پروتکل ARP که مخفف کلمه‌ی Address Resolution Protocol است، برای تبدیل آدرس IP (لایه‌ی شبکه) به آدرس MAC (لایه‌ی پیوند داده) کاربرد دارد، که این پروتکل یک پروتکل ضروری برای لایه‌ی اینترنت است.

به علت اینکه پروتکل ARP بیشترین کاربرد را دارد، مهاجم‌ها با روش‌های غیرقانونی سعی در دور زدن آن دارند. در شکل زیر سیستم "Client PC " را مشاهده می‌کنید که با روتر پیش‌فرض آن 192.168.0.1 است و اطلاعات را با این روتر رد و بدل می‌کند، اگر در این بین یک سیستم مهاجم با نام "Attacker’s PC " وجود داشته باشد، برای اینکه خود را به جای سیستم " Client PC " به روتر معرفی کند، با ارسال پیام‌های ARP (GRAP) هم به کلاینت و هم به روتر خود را در وسط کار قرار می‌دهد، مثلاً در این شکل "Attacker’s PC " آدرس مک خود را به جای آدرس مک روتر "BBBB.BBBB.BBBB" جا می‌زند و این کار باعث می‌شود که سیستم مورد نظر اطلاعات خود را به مهاجم ارسال کند و به همین ترتیب مهاجم با دستکاری در آن، اطلاعات را به سمت روتر مورد نظر خود ارسال می‌کند؛ این نوع حملات با نام ARP spoofing شناخته می‌شوند و از نوع man-in-the-middle است.



توجه داشته باشید که GRAP که به اختصار به نام Gratuitous Address Resolution Protocol شناخته می‌شود کمکی برای شناسایی آدرس IP تکراری در شبکه است که این کار را با ارسال Broadcast در شبکه انجام می‌دهد، باارسال broadcast سیستم‌هایی که در شبکه قرار دارند اگر به این پیغام پاسخ دهند یعنی اینکه آدرس مورد نظر متعلق به آنها است و نمی‌توان از آن استفاده کرد.

در قسمت‌های قبلی از سرویس DHCP snooping استفاده کردیم، زمانی که این سرویس فعال می‌شود یک جدول که شامل آدرس MAC و آدرس IP است ایجاد می‌شود و می‌توانید با کمک این جدول از حملات ARP جلوگیری کنید.

یکی از ویژگی‌های امنیتی در پروتکل ARP استفاده از DAI یا همان Dynamic Arp Inspection است که با استفاده از جدول DHCP snooping بررسی می‌شود اگر بسته‌ی ARP از پورتی که Trust است دریافت شود، اجازه عبور به آن را می‌دهد و اگر از پورتی دیگر دریافت شود فقط در صورتی که آدرس مک با آدرس IP یکی باشد اجازه عبور را می‌دهد.

برای فعال‌سازی ویژگی Dynamic Arp Inspection به صورت زیر عمل کنید:

برای شروع اول باید DAI را بر روی Vlan مورد نظر خود در سوئیچ اجرا کنید، که دستور آن به صورت زیر می‌باشد.

```
Switch(config)# ip arp inspection vlan 1
```

بعد از آن باید در Interface که به سوئیچ متصل است دستور زیر را وارد کنید:

```
Switch(config)#interface Ethernet 0/2
Switch(config-if)# ip arp inspection trust
```

توجه داشته باشید به صورت پیش‌فرض ویژگی DAI در همه‌ی پورت‌های سوئیچ در حالت Untrust است و فقط باید در پورت قابل اعتماد که در سوئیچ قرار دارد بر روی Trust قرار بگیرد.

پس در این موضوع یاد گرفتیم که چگونه جلوی مهاجم را که خود را به عنوان یک سیستم میانی جا می‌زد بگیریم، که این کار را با تعریف دستورات مورد نظر در پورت مشخص شده انجام می‌دهیم.

تحلیل و بررسی تکنولوژی تشخیص (IDS/IPS)

سیستم تشخیص نفوذ سیسکو(IDS) و سیستم پیشگیری از نفوذ (IPS)، سیستم‌هایی هستند که رویکرد دفاع از عمق دارند و از شبکه‌ی شما در برابر ترافیک‌های مخرب محافظت می‌کند، در این بخش به طور کلی این سیستم‌ها را با هم بررسی می‌کنیم.

IDS مخفف عبارت **Intrusion Detection System** و IPS مخفف کلمه‌ی **Intrusion Prevention Systems** است.

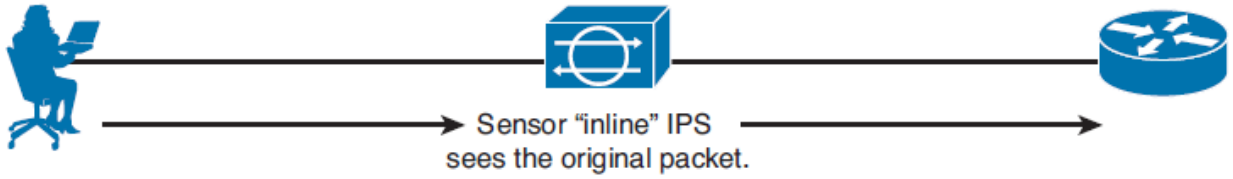
سنسور چیست

سنسور وسیله‌ای است که ترافیک شبکه را بررسی می‌کند و سپس بر اساس آن ترافیک تصمیم می‌گیرد چه کاری انجام دهد، آیا آن ترافیک مخرب است یا نه، توجه داشته باشید این نوع سیستم‌ها بر اساس قوانینی که برای آن نوشته شده عمل می‌کند و هیچ وقت نمی‌توانید سیستمی را پیدا کنید که به صورت ۱۰۰ درصد درست عمل کند.

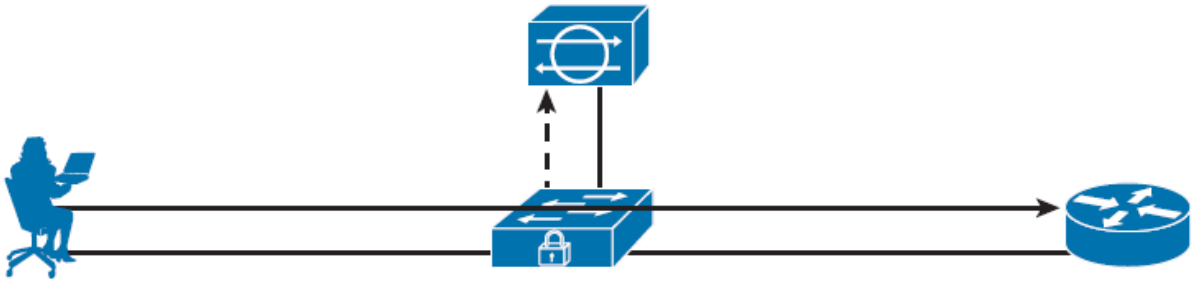
تفاوت بین IPS و IDS

همانطور که گفتیم IPS یک سیستم پیشگیری از نفوذ است که جلوی ترافیک‌های مخرب را می‌گیرد به این صورت که سیستم‌های IPS در مرز بین دو شبکه قرار می‌گیرند و ترافیک را به صورت کامل بررسی می‌کنند که شکل آن را در زیر مشاهده می‌کنید، اگر ترافیک عبوری با سنسورهای تعبیه شده در IPS یکی باشد آن ترافیک متوقف خواهد شد و بسته مورد نظر Drop می‌شود و به مقصد نهایی خود نمی‌رسد.

یکی از مشکلاتی که سیستم‌های IPS دارند این است که اگر بنا به دلایلی سیستم IPS از کار بیفتد و یک خط جایگزین برای آن طراحی نشده باشد، کل شبکه از مسیر خارج خواهد شد و این می‌تواند مشکل‌ساز باشد.



اما سیستم IDS یا همان سیستم تشخیص نفوذ یک کپی از ترافیک شبکه را بررسی خواهد کرد و اگر در این ترافیک به اطلاعات مخربی دست پیدا کند آن را در قالب گزارشی به مدیر شبکه ارسال خواهد کرد تا بر روی آن ترافیک مورد نظر اقدامات امنیتی انجام گیرد ولی سیستم IDS به خودی خود نمی‌تواند بر روی ترافیک مورد نظر که مخرب است عملیاتی را انجام دهد و آن ترافیک را Drop کند، در زیر شکل سیستم IDS را مشاهده می‌کنید که IDS در بیرون از ترافیک اصلی حضور دارد و توسط سوئیچ یک نسخه از ترافیک برای بررسی برای آن ارسال می‌شود.



موضوع	IDS	IPS
موقعیت در جریان شبکه	در جریان شبکه حضور ندارد ولی یک کپی از ترافیک شبکه برای بررسی برای آن ارسال می‌شود	در جریان شبکه حضور دارد و بر روی ترافیک‌های مخرب عمل تعریف شده را انجام می‌دهد
حالت	خارج از باند ترافیک است	حالت درون خطی

تاخیر	تاخیر در شبکه ایجاد نمی‌کند چون خارج از باند عمل می‌کند	مقدار کمی تاخیر ایجاد می‌کند چون به صورت آنلاین ترافیک را بررسی می‌کند
تاثیر خرابی سنسور	هیچ تاثیری ندارد	تاثیر دارد و سرعت را در عملیات کاهش می‌دهد
عملکرد بر روی ترافیک مخرب	به صورت پیش‌فرض نمی‌تواند جلوی ترافیک‌های مخرب را بگیرد ولی ویژگی‌هایی دارد که بتوان از یک سیستم درون خطی استفاده کند	این سیستم بسته‌های مخرب را حذف می‌کند و اجازه نمی‌دهد به شبکه راه پیدا کنند
توانایی نرمال‌سازی	چون به صورت برون‌خطی و بیرون از ترافیک اصلی کار می‌کند، نمی‌تواند بر روی بسته‌ها اصلاحی انجام دهد	به خاطر اینکه IPS به صورت درون خطی کار می‌کند می‌تواند بسته‌ها را بر اساس قوانینی که برای آن تعریف شده اصلاح و دستکاری کند

اصلاحات مثبت و منفی در IPS و IDS

- False positive به موقعیتی گفته می‌شود که سنسور به اشتباه ترافیک‌های سالم را به عنوان ترافیک مخرب در نظر بگیرد.
- False negative به ترافیکی مخربی که از شبکه عبور کند و توسط سنسور شناسایی نشود می‌گویند.
- True positive به ترافیکی مخربی می‌گویند که توسط سنسور به درستی شناسایی شود.
- True negative به ترافیک سالم شبکه اشاره دارد.

روش‌های مختلفی که یک سنسور می‌تواند ترافیک مخرب را شناسایی کند شامل موارد زیر است:

- Signature-based IPS/IDS

مبتنی بر امضاء است و توسط شرکت‌های ارائه دهنده‌ی IPS/IDS مانند سیسکو ارائه می‌شوند، در این روش مجموعه‌ای از قوانین برای پیدا کردن ترافیک مخرب ایجاد شده است که اکثر آنها به صورت پیش‌فرض غیرفعال هستند و در صورت نیاز باید آنها را فعال کرد.

- Policy-based IPS/IDS

مبتنی بر تعریف سیاست است که در آن شما می‌توانید مشخص کنید چه چیزی در شبکه فعال باشد یا نباشد، مثلاً می‌توانید مشخص کنید که پروتکل Telnet در شبکه غیر فعال باشد.

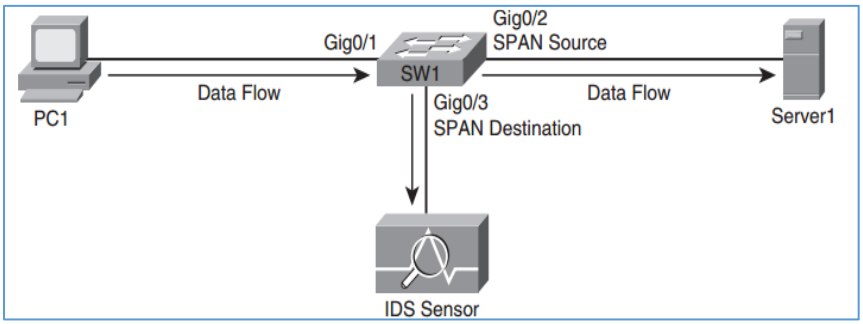
- Anomaly-based IPS/IDS

مبتنی بر ناهنجاری است به این صورت که اگر تعداد درخواست‌های یک ارتباط بیش از حد مجاز شود، IPS می‌تواند آن ارتباط را قطع و مخرب اعلام کند.

- Reputation-based IPS/IDS

مبتنی بر اعتباراست به این صورت که مجموعه‌ای از سیستم‌ها در سرتاسر جهان در یک گروه جمع می‌شوند و سنسورهایی که در IPS تعبیه شده می‌توانند بر اساس تجربه دیگر دستگاه‌ها در سرتاسر دنیا نسبت به شناسایی ترافیک مخرب عمل کنند.

در زیر نحوه‌ی تنظیم سوئیچ برای ارسال اطلاعات به سیستم IDS را مشاهده می‌کنید، البته تنظیم IDS/IPS در دوره‌های بعدی بررسی خواهد شد و مختص این دوره نیست.



زمانی که دستگاه IDS را به سوئیچ متصل می‌کنید، برای اینکه بتوانید پورت مورد نظر خود را در این دستگاه مانیتور کنید برای این کار باید به صورت زیر عمل کنید:

Switch(config-if)# **monitor session 1 source interface gigabitethernet0/2**

در دستو بالا به سوئیچ SW1 اعلام کردیم که پورت gigabitethernet0/2 منبعی برای مانیتور کردن است.

Switch(config-if)# **monitor session 1 destination interface gigabitethernet0/3**

در این دستور هم به سوئیچ اعلام می‌کنیم که پورت مقصد برای ارسال ترافیک gigabitethernet0/3 است که به دستگاه IDS متصل شده است. با این دو دستور به سوئیچ گفتیم که یک کپی از اطلاعات Server1 را به سمت دستگاه IDS ارسال کن تا مورد بررسی قرار گیرد.

پیشنهادهای سیسکو برای امن نگه داشتن شبکه

۱- محدود کردن دسترسی به سوئیچ‌های لایه دو و دسترسی دادن به یک کاربر ادمین.

۲- استفاده از ACS یا همان Access Control List برای مدیریت کاربران و دسترسی‌ها به دستگاه‌های شبکه.

۳- اگر از پروتکل‌های مدیریتی در شبکه استفاده می‌کنید باید از آخرین ورژن آن مانند SNMP V3 استفاده کنید، توجه داشته باشید استفاده از SNMP V1 و SNMP V2 باعث انتقال اطلاعات به صورت Clear Text خواهد شد و همین امر باعث ایجاد خطر در شبکه خواهد شد.

۴- سرویس‌های بلاء استفاده در سوئیچ را غیرفعال کنید.

۵- استفاده از سرویس Port Security برای کاهش تعداد Mac Address بر روی یک پورت در سوئیچ.

۶- اطلاعات کاربران را به سمت VLAN Native در مد Trunk و پروتکل 802.1Q ارسال نکنید.

۷- تمام پورت‌های بلاء استفاده در سوئیچ را به صورت دستی خاموش کنید.

۸- استفاده از مکانیزم‌های امنیتی BPDU و Root Gurd برای محافظت از پروتکل STP .

۹- فعال کردن DHCP snooping و DAI برای مبارزه با حملات man-in-the-middle.

فصل هشتم – بررسی پروتکل IPV6

شبکه‌هایی که با آن‌ها در حال حاضر کار می‌کنیم، بیشتر آن‌ها از IPV4 استفاده می‌کنند، به دلیل تولید بسیار زیاد ادوات الکترونیکی و استفاده‌ی آن‌ها از اینترنت این آدرس‌ها در حال اتمام می‌باشند که همین امر باعث شد که محققان سازمان Internet Engineering Task Force (IETF) مدل جدید آن را با عنوان IPv6 معرفی کردند که بسیار بیشتر از ipv4 آدرس در اختیار جامعه قرار داده است، البته IPV5 هم وجود داشت که به خاطر مشکلاتی که در سر راه قرار داشت، گسترش نیافت و به فراموشی سپرده شد.

ویژگی‌های ipv6:

فضای آدرس‌دهی بسیار بزرگ:

همان‌طور که می‌دانید، ipv4 از ۳۲ بیت تشکیل شده است، اما ipv6 از ۱۲۸بیت تشکیل شده است که به صورت زیر بیان می‌شود:

2^128 = 340,282,366,920,938,463,374,607,431,770,000,000

این تعداد ip addressهایی است که این پروتکل پشتیبانی می‌کند که واقعاً زیاد است، یعنی در هر مترمربع کره‌ی زمین، چندین هزار آدرس IP اختصاص داده می‌شود.

استفاده نشدن از NAT:

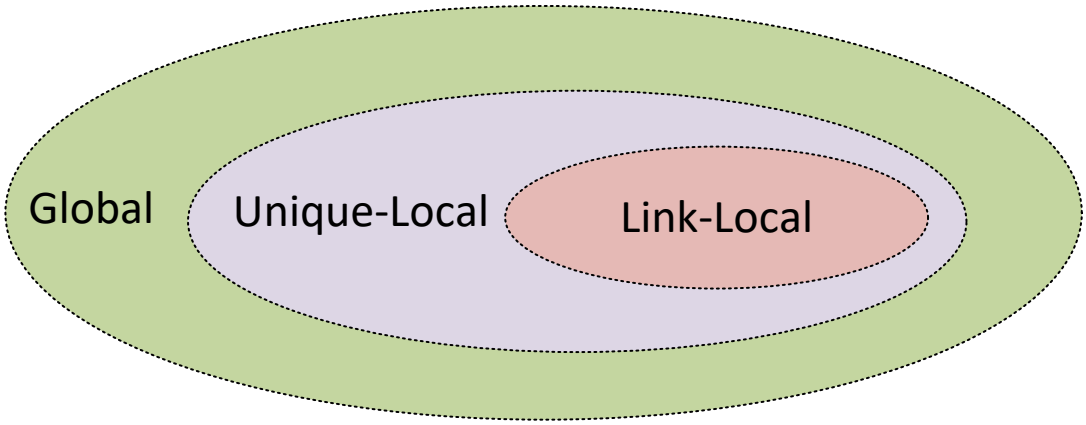
همان‌طور که می‌دانید، IPV4 برای خارج شدن از شبکه‌ی داخلی و ورود به اینترنت باید تبدیل به IPهای VALID می‌شد که این کار را با ترجمه‌ی آدرس‌های Invalid به Valid انجام می‌دادیم که به آن NAT می‌گفتند، اما در مورد IPV6 این چنین نیست و روش دیگری برای این موضوع مورد استفاده قرار می‌گیرد.

حذف شدن آدرس‌های Broadcast:

در این پروتکل، به علت افزایش تعداد آدرس‌های Multicast دیگر خبری از Broadcast نیست و آدرس‌ها به صورت Unicast و Multicast و Anycast می‌باشند.

Unicast:

به آدرس‌هایی گفته می‌شود که برای ارتباط بین یک مبدأ و مقصد استفاده می‌شوند.



Global unicast address: به مفهوم آدرس‌های unicast قابل انتقال در اینترنت است (قابلیت آدرس‌دهی در اینترنت را دارد) و شبیه به نوع متناظر آن در IPv4 می‌باشد، به این نوع آدرس‌ها Aggregatable Address نیز می‌گویند، که به مانند شکل Subnet آن از سه قسمت 3,45,16 بیت تشکیل شده است که جمعاً می‌شود ٦٤ بیت و قسمت Interface آن هم از ٦٤ بیت تشکیل شده است.

3 bits	45 bits	16 bits	64 bits
001	Global Routing Prefix	Subnet ID	Interface ID

این ساختار از قسمت‌های زیر تشکیل شده است:

Unique local address: این آدرس‌ها را با نام Site-Local unicast هم می‌شناسند که قابلیت انتقال در اینترنت را نداشته و عملکرد این نوع آدرس‌ها دقیقاً شبیه به آدرس‌های local یا Private در IPv4 است. این

آدرس‌ها با ۸ بیت ثابت (FD) شروع می‌شوند و به دنبال آن ٤٠ بیت صفر و سپس 16 بیت مربوط به Subnet ID است که معمولاً آن را هم صفر در نظر می‌گیرند.٦٤ بیت پایانی هم که Interface ID است که برای هر کامپیوتر منحصربه‌فرد است.

8 bits	40 bits	16 bits	64 bits
FD	Global ID	Subnet ID	Interface ID

Link local address: شبیه به آدرس‌های Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرس‌ها را می‌توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند را تخصیص داد. این آدرس‌ها که در غیاب DHCP Server ایجاد می‌شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس، در کادر محاوره‌ای Properties کارت شبکه گزینه‌ی obtain IPv6 address automatically را انتخاب کنیم، سیستم عامل به طور خودکار بر اساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می‌دهد، این آدرس‌ها اصولاً برای رسیدن به گره‌های متصل شده به همان دستگاه مورد استفاده قرار می‌گیرن.

یکی از نکات مهم در این نوع آدرس‌ها این است که روترها بسته‌هایی که دارای آدرس Link Local باشند به Interfaceهای دیگر انتقال نمی‌دهند، توجه داشته باشید که تمام Interfaceها دارای آدرس link-local هستند.

Special unicast address: مانند Loopback ::1

Multicast:

برای ارتباط یک مبدأ با چند مقصد مشخص‌شده استفاده می‌شود که این مقصد در یک گروه قرار دارند؛ این آدرس جایگزین Broadcast در ipv4 شده است. در ادامه، جدول کامل این آدرس‌ها قرار گرفته شده است.

Anycast:

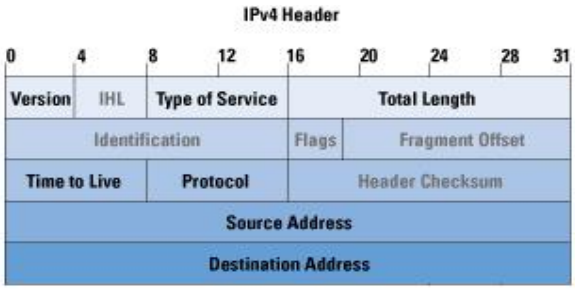
در این آدرس‌دهی برای مثال روتر شما برای رسیدن به یک سرور چند مسیر را در پیش رو دارد، روتر مسیری را انتخاب می‌کند که کمترین Cost را داشته باشد، پس آدرس Anycast آدرسی است برای انتخاب بهترین مسیر تا رسیدن به یک سرور و یا انتخاب یک سرور بین چند سرور یکسان که هزینه‌ی کمتری دارد.

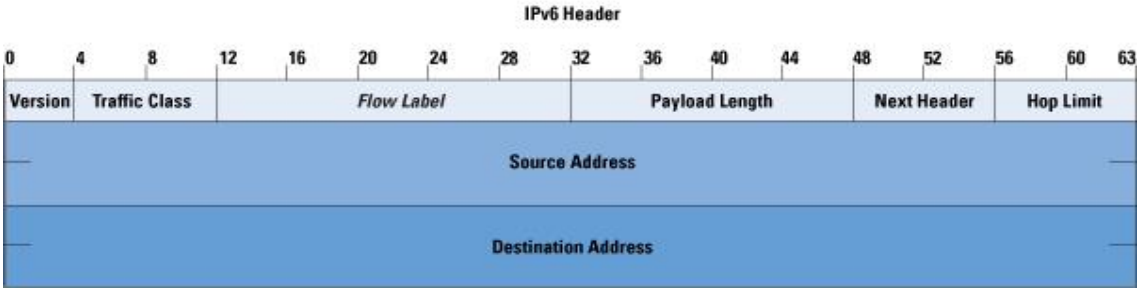
در جدول زیر تفاوت اصلی بین IPV4 و IPV6 را مشاهده می‌کنید:

IPV4	IPV6
پشتیبانی از ۲ به توان ۳۲ آدرس IP که برابر ٤,٢٩٤,٩٦٧,٢٩٦ آدرس است	پشتیبانی از ۲ به توان ۱۲۸ آدرس که بسیار بسیار زیاد است و می‌شود گفت پایانی ندارد
به خاطر محدودیت فضا باید از پروتکل NAT استفاده کرد.	به علت داشتن تعداد بالای آدرس از NAT به صورت پیش‌فرض استفاده نمی‌شود.
برای اختصاص دادن آدرس به میزبان‌ها باید از سرویس DHCP استفاده کنند و یا اینکه به صورت دستی وارد کنند.	در این ورژن میزبان‌ها دارای آدرس اختصاصی هستند که می‌توانند از آنها استفاده کنند، البته از سرویس DHCP هم می‌توانید در این پروتکل استفاده کنید.
در این پروتکل از IPSEC پشتیبانی می‌شود ولی یک گزینه‌ی اختیاری است که می‌توان از آن استفاده کرد تا محافظت از بسته‌های IP از طریق رمزگذاری، اعتبارسنجی و .. انجام شود.	در این پروتکل به صورت پیش‌فرض IPSEC پشتیبانی می‌شود و فعال است و نیازی به تنظیم آن در IPSEC نیست.
استفاده از broadcasts که در پروتکل ARP استفاده می‌شود.	از broadcasts و ARP به هیچ عنوان استفاده نمی‌کند ولی به جای آن از Multicast و Neighbor Discovery Protocol یا همان NDP استفاده می‌کند، ND جایگزین ARP می‌شود.
از پروتکل لایه ٤ پشتیبانی می‌کنند، TCP , UDP	از پروتکل لایه ٤ پشتیبانی می‌کنند، TCP , UDP
ار پروتکل‌های FTP, HTTP پشتیبانی می‌کنند.	ار پروتکل‌های FTP, HTTP پشتیبانی می‌کنند.

تفاوت Header های ipv4 و ipv6:

اگر به IPV4 دقیق نگاه کنید، متوجه‌ی پیچیده‌تر بودن آن نسبت به IPV6 می‌شوید، در واقع ipv6 خیلی ساده‌تر از IPV4 است.





هر یک از گزینه‌های موجود در این Header ها را باهم مورد بررسی قرار می‌دهیم:

Version: این فیلد ٤ بیتی بوده و نشان‌دهنده‌ی نسخه‌ی IP موجود است.

Traffic Class: برای مشخص کردن کلاس‌های مختلف و مشخص کردن اولویت پکت‌ها IPV6 استفاده می‌شود و طول آن 8 بیت است.

Flow Label: طول این فیلد 20 بیت است. یکی از ویژگی‌های آن پشتیبانی از QOS است که یکی از ویژگی‌های جدید در IPV6 است و توانایی مسیریابی ترافیک مشخص را در شبکه می‌دهد.

Payload Length: طول این بخش 20 بیت است که شامل طول بخش بسته‌ی IPV6 است.

NextHeader: طول این فیلد 8 بیت است که نشان‌دهنده‌ی نوع Header در IPV6 است.

Hop Limit: طول این فیلد ۸ بیت است که برای مشخص کردن تعداد روترهایی است که بسته‌ی اطلاعاتی از آن رد می‌شود، یعنی زمانی‌که این بسته از یک روتر در سر راه رد می‌شود یک شماره از این زمان کم می‌شود و تا زمانی که این شماره به پایان برسد و بسته مورد نظر حذف شود.

Source Address: نشان‌دهنده‌ی آدرس مبدأ است.

DestinationAddress: نشان‌دهنده‌ی آدرس مقصد است.

روش آدرس‌دهی در IPV6:

IPV6 از ۱۲۸ بیت تشکیل شده است یعنی از ۸ قسمت ۱۶ بایتی تشکیل شده است که هر قسمت آن به صورت hexadecimal است یعنی از ۰ تا F و توسط (:) هر قسمت از قسمت دیگر جدا می‌شود، در زیر جدول تبدیل اعداد به Hexadecimal را که مربوط به IPV6 است را مشاهده می‌کنید.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

در زیر یک نمونه از آدرس IPV6 را مشاهده می‌کنید که دارای ۸ بخش است، البته کمی کیج کننده!

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

روش‌هایی را برای کوتاه کردن آن به کار وجود دارد که در این قسمت بررسی می‌کنیم.

روش اول – حذف صفرهای ابتدایی:

در این روش هر چه صفر قبل از یک عدد وجود دارد را حذف می‌کنیم:

2001:0DA8:E800:0000:0260:3EFF:FE47:0001

2001: DA8:E800:0: 260:3EFF:FE47: 1

روش دوم – حذف صفرهای پشت سر هم:

در این روش اگر بین یک کلون " : " چندین صفر وجود داشت، می‌توانید صفرها را حذف کرده و فقط کلون را قرار دهیم. به روش زیر توجه کنید:

2001:0000:0000:2260:3EFF:FE47:0001

2001:: 2260:3EFF:FE47:1

همان‌طور که مشاهده می‌کنید به جای صفرهایی که در قسمت ۲ و ۳ قرار داشتند، فقط :: قرار دادیم که همین کار باعث کوتاه شدن این IP شده است.

تذکر مهم: دو بار استفاده از کلون یا :: در یک IP امکان‌پذیر نیست و مشکل ایجاد می‌شود.

در آدرس‌دهی IPV4 اگر یادتان باشد ما از IP address به همراه SubnetMask استفاده می‌کردیم که چنین موضوعی در IPv6 وجود ندارد و به جای آن از Subnet Prefix استفاده می‌کنیم.

در IPV6 چیزی به نام NETMASK وجود ندارد و جایگزین آن Prefix است، در واقع Prefix جداکننده‌ی NET ID از HOST ID است.

Net ID Host ID

2014:2015:0000:0000:BC02:0000:0001:0002/64

در مثال بالا ٦٤/ به این معناست که از سمت چپ ٦٤ بیت به جلو برویم و بعد از ٦٤ بیت قسمت HOST ID شروع می‌شود و قبل از آن مربوط به NET ID می‌شود. هر عدد در اینجا معادل ٤ بیت است.

انواع آدرس‌های ipv6:

روش‌های آدرس‌دهی به صورت Unicast:

فرم کلی Global Unicast:

از چپ به راست

FP	TLA-ID	RES	NLA-ID	SLA-ID	INTERFACEID
۳ بیت	۱۳ بیت	۸ بیت	۱۶ بیت	۲۴ بیت	۶۴ بیت

FP: نشان‌دهنده‌ی نوع IPV6 است (Format Prefix) ipهای PUBLIC ورژن ٦ در حالت باینری با ۰۰۱ شروع می‌شود.

TLA-ID: مخفف (TopLevel Aggregator Identifire) دسته‌بندی IPهایی هستند که به جاهای بزرگ، مانند قاره‌ها اختصاص پیدا می‌کنند.

RES: یعنی رزرو شده است.

NLA-ID: مخفف (Next Aggregator Identifire) IPهای منحصربه‌فردی هستند که به جاهای بزرگ، مانند کشورها اختصاص پیدا می‌کنند.

SLA-ID: مخفف (Site Level) ipهای منحصربه‌فردی هستند که به جاهای بزرگ، مانند شهرها و سازمان‌های بزرگ اختصاص پیدا می‌کنند.

ipهای خاصی در IPV6 وجود دارند که به شرح زیر می‌باشند:

::/128 یک آدرس نامشخص ابتدای یک بایت است که می‌خواهد آدرس Link-Local را مشخص کند.

::/0 این آدرس معادل 0.0.0.0 در IPV4 است و برای مسیریابی به صورت دستی از این آدرس استفاده می‌کنند.

1::/128 این آدرس معادل آدرس LoopBack است که در ipv4 به صورت 127.0.0.1 بوده است و برای تست کارت شبکه و پروتکل TCP/IP استفاده می‌شود.

FE80::/10 آدرس Link Local Unicast است که شبیه به آدرس 169.254.x.x است.

FF00::/8 آدرس‌های مربوط به Multicast است.

آدرس‌های Multicast:

این آدرس‌ها جایگزین Broadcast در IPV4 شده‌اند و برای کارهای زیر استفاده می‌شوند:

- برای استفاده در سرویس DHCP.
- اعلام مسیرها در روترها که قبلاً به صورت Broadcast در IPV4 آموختیم.
- برای تقاضاهای روتر.
- و...
- این آدرس‌ها از ۸ بیت پسوند Prefix استفاده می‌کنند که به صورت FF00::/8 است، default Gateway برای کلاینت‌ها وجود ندارد.

در جدول زیر، انواع ipهای multicast برای پروتکل‌ها و سرورها و ... را مشاهده می‌کنید:

Address	توضیحات
ff02::1	همه‌ی گره‌ها در بخش شبکه‌های محلی
ff02::2	تمام روترها در بخش شبکه‌های محلی
ff02::5	برای الگوریتم spf مربوط به OSPFV3
ff02::6	مربوط به همه‌ی روترهای DR در پروتکل OSPF
ff02::8	مربوط به پروتکل IS-IS

مربوط به پروتکل RIP	ff02::9
مربوط به پروتکلEIGRP	ff02::a
مربوط به روترهای Protocol Independent Multicast (PIM)	ff02::d
گزارش مربوط به MLDv2 تعریف‌شده در RFC 3810	ff02::16
همه‌ی سرورهای DHCP و Real Agentها در شبکه‌ی محلی	ff02::1:2
تمام میزبان‌های LLMNR (Link Local Multicast Name Resolution) در شبکه‌ی محلی	ff02::1:3
همه‌ی سرورهای DHCP در سایت شبکه‌ی محلی	ff05::1:3
مربوط به Service Discovery Protocol	ff0x::c
مربوط به Multicast Domain Name System (DNS)	ff0x::fb
مربوط به Network Time Protocol	ff0x::101

IPV6 می‌تواند به صورت خودکار توسط روش‌های زیر تنظیم شود:

stateful Auto configuration
stateless Auto configuration
EUI – 64

Stateful Auto configuration:

در این روش که سرویس DHCP از آن استفاده می‌کند یک آدرس با طول ۱۲۸ بیت واگذار می‌شود

Stateless Auto configuration:

در این روش یک IPV6 که ۱۲۸ بیت است را نصف می‌کند و ٦٤ بین از آن را استفاده و ٦٤ بیت دوم را بعداً استفاده می‌کند، یعنی اینکه ٦٤ بین از یک آدرس واگذار می‌شود و ٦٤ بیت در یک زمان دیگر استفاده می‌شود.

EUI – 64:

در این روش روتر برای اختصاص دادن IP به کلاینت مورد نظر از آدرس Mac کلاینت در IPv6 استفاده می‌کند به این صورت که ٦٤ بین اول به صورت دستی وارد می‌شود و ٦٤ بیت دوم از طریق Mac address دستگاه مورد

نظر استخراج می‌شود، اما آدرس Mac، ٤٨ بیتی است. برای حل این مشکل از مقدار FFFE در وسط آدرس Mac استفاده می‌کنند و به‌این‌ترتیب آدرس مورد نظر به دستگاه مورد نظر داده می‌شود.

مثلاً برای واردکردن آدرس به این روش، وارد اینترفیس می‌شویم و از آدرس زیر استفاده می‌کنیم:

Router(config-if)# ipv6 address 2011:1111:11::1/64 eui-64

بعد از اینکه آدرس را وارد کردیم با دستور **Show IPV6 Interface Berife** می‌توانیم آدرس اصلی را مشاهده کنیم که به صورت زیر است:

Static Address	Mac Address
2011:1111:11:0:	2D0:97FF:FE51:6A02

همان‌طور که مشاهده می‌کنید در قسمت دوم برای کامل کردن آن، از آدرس Mac دستگاه مورد نظر استفاده کرده است.

تهدیدات مشترک در IPV4 و IPV6

۱- **Application layer attacks**

در این تهدید مهاجم از طریق سرویس‌های شبکه اقدام به حمله مخرب می‌کند، برای جلوگیری از این نوع حملات باید از طریق دستگاه‌های امنیتی مانند ASA و یا استفاده از سیستم پیشگیری از نفوذ IPS از آنها جلوگیری کرد.

۲- **Unauthorized access**

در شبکه‌های مختلف افرادی وجود دارند که بدون اجازه دسترسی به شبکه بتوانند به منابع شبکه دسترسی داشته باشند، که راه حل آن استفاده از سیستم‌های احراز هویت مانند AAA که در این کتاب به طور کامل آن را بررسی کردیم، استفاده از این نوع سیستم‌ها باعث می‌شود هر کاربر برای دسترسی نیاز به رمز عبور داشته باشد و تمام عملکردهایی که در شبکه انجام می‌دهد هم در گزارشگیری آن ثبت خواهد شد.

۳- **Man-in-the-middle attacks**

حملات مرد میانی با نام Bucket Bridge Attack هم شناخته می‌شوند، در این نوع حمله مهاجم خود را بین دو سیستم قرار می‌دهد و از روش‌های خاصی برای بدست آوردن اطلاعات سیستم‌ها استفاده می‌کند که در فصل اول درباره‌ی آن توضیح دادیم، برای جلوگیری از این روش می‌توان از پروتکل مسیریابی STP محافظت کرد و احراز هویت را در لایه ۳ که مربوط به مسیریابی است پیاده‌سازی کرد.

۴- **Sniffing or eavesdropping**

این نوع حمله به عنوان استراق سمع شناخته می‌شود که مهاجم در این روش به ترافیک عبوری گوش می‌دهد و یا در اصطلاح Sniff می‌کند و از آن طریق می‌تواند سوئیچ‌ها را با استفاده از قابلیت content-addressable memory (CAM) مجبور کنند Frameهای خود را به همه‌ی پورت‌های خود ارسال کنند که این موضوع باعث می‌شود سوئیچ از کار بیفتد، برای محافظت در برابر این حملات باید در سوئیچ سرویس Port Security را فعال کنید تا در هر پورت یک MAC address مجاز فعال شود و اجازه ورود MAC Address دیگری را به آن ندهد، البته در این مورد قبلاً صحبت کردیم.

۵- **Denial-of-service (DoS) attacks**

حملات انکار سرویس یا DOS که می‌تواند یک وب سرویس را از کار بیندازد، در مورد این حمله هم در فصل‌های قبل صحبت کردیم، برای جلوگیری از آن هم باید ترافیک شبکه را به صورت کامل رصد کرد تا ترافیک مشکوک مشخص شوند که برای این کار می‌توانیم از فایروال ASA و سرویس شناسایی IDS استفاده کنیم.

۶- **Spoofed packets**

در این نوع حملات مهاجم بسته‌های جعلی را در شبکه تزریق می‌کند، که بهترین راه حل برای جلوگیری از آن فیلتر کردن ترافیک ورودی به شبکه است، با این کار ترافیکی که ادعا می‌کند از داخل شبکه منشا گرفته متوقف خواهد شد.

۷- **Attacks against routers and other network devices**

غیرفعال کردن خدمات و سرویس‌های غیر ضروری در شبکه و خاموش کردن دستگاه‌های که نیاز به استفاده از آن نیست.

استفاده از ipv6 در پروتکل RIP :

پروتکل RIP را با عنوان RIP NG برای IPV6 می‌شناسند، برای فعال کردن RIP برای استفاده از IPV6 باید قبل از هر کاری ipv6 unicast-routing را فعال کنید. اگر این قسمت را فعال نکنید به شما پیغام خطا می‌دهد و می‌گوید که ipv6 Routing فعال نشده، پس قبل از هر چیز این دستور را اجرا کنید، بعد با دستور زیر پروتکل RIP برای IPV6 فعال می‌شود:

ipv6 router rip RIPNG

این دستور با دستورات گذشته که برای RIP تعریف می‌کردیم، متفاوت است و یک اسم باید برای این RIP وارد کنیم که در این دستور از اسم RIPNG استفاده کردیم و شما می‌توانید هر اسم دیگری را وارد کنید، بعد از فعال شدن RIP دیگر لازم نیست که شبکه‌های متصل به روتر را در RIP تعریف کنیم، باید وارد اینترفیس مربوطه شویم و RIP را روی این اینترفیس فعال کنیم، به صورت زیر:

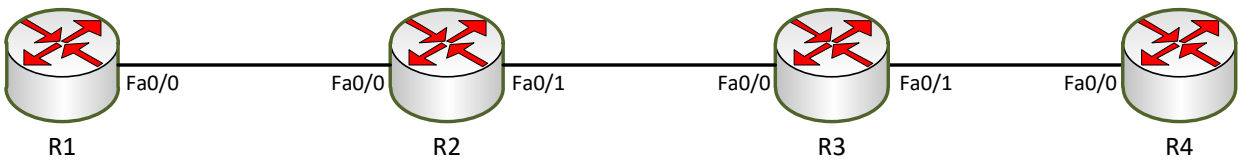
R1(config-rtr)#**int s0/1**

R1(config-if)#**ipv6 rip RIPNG enable**

همان‌طور که مشاهده می‌کنید وارد اینترفیس S0/1 شدیم و پروتکل RIP با نام RIPNG که قبلاً ایجاد کرده‌ایم را فعال کردیم.

شماره‌ی پورت برای پروتکل RIP Ng ، 520 با پروتکل UDP است.

مثال برای RIP NG:



در این مثال می‌خواهیم به اینترفیس‌ها، آدرسی از نوع IPV6 بدهیم و بعد ازآن RIP را فعال کنیم:

این شکل را در نرم‌افزار خود ایجاد کنید.

وارد روتر R1 می‌شویم و دستور زیر را وارد می‌کنیم:

```
R1#conf t
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router rip rip1
R1(config)# int f0/0
R1(config-if)# ipv6 address 2011:111:12::1/64
R1(config-if)#ipv6 rip rip1 enable
```

همان‌طور که مشاهده می‌کنید در مرحله‌ی اول با دستور ipv6 unicast-routing باعث فعال شدن IPV6 Routing شدیم. بعد از آن RIP را با نام RIP1 تعریف کردیم، وارد اینترفیس شدیم و آدرس IPV6 مربوطه را وارد کردیم. این آدرس به این صورت است که ۱۲ را به عنوان شماره‌ی روترها که بین روتر ۱ و ۲ است وارد کردیم و 1:: هم شماره‌ی مختص این اینترفیس است. در آخر هم پروتکل Rip را که با نام RIP1 ایجاد کردیم، بر روی این اینترفیس فعال می‌کنیم.

وارد روتر R2 می‌شویم و دستور زیر را وارد می‌کنیم:

```
R2#conf t
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router rip rip1
R2(config)# int f0/0
R2(config-if)# ipv6 address 2011:111:12::2/64
R2(config-if)#ipv6 rip rip1 enable
R2(config)# int f0/1
R2(config-if)# ipv6 address 2011:111:23::1/64
R2(config-if)#ipv6 rip rip1 enable
```

در R2 در هر دو اینترفیس پروتکل RIP را فعال کردیم و آدرس متفاوت وارد کردیم.

وارد روتر R3 می‌شویم و دستور زیر را وارد می‌کنیم:

```
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router rip rip1
R3(config-rtr)#int f0/0
R3(config-if)#ipv6 address 2011:1111:23::2/64
R3(config-if)#ipv6 rip rip1 en
R3(config-if)#ipv6 rip rip1 enable
R3(config-if)#no shutdown
R3(config-if)#int f0/1
R3(config-if)#ipv6 address 2011:1111:34::1/64
R3(config-if)#ipv6 rip rip1 enable
Router(config-if)#no shutdown
```

وارد روتر R4 می‌شویم و دستور زیر را وارد می‌کنیم:

```
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router rip rip1
Router(config-rtr)#int f0/0
Router(config-if)#ipv6 address 2011:1111:34::2/64
Router(config-if)#ipv6 rip rip1 enable
Router(config-if)#no shutdown
```

بعد از اتمام کار وارد روتر R1 شوید و روتر R4 را Ping کنید:

```
R1(config-if)#do ping 2011:1111:34::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2011:1111:34::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
```

برای نمایش جدول روتینگ در ipv6 از دستور زیر استفاده می‌کنیم:

R1#show ipv6 route

```
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2011:1111:12::/64 [0/0]
     via ::, FastEthernet0/0
L   2011:1111:12::1/128 [0/0]
     via ::, FastEthernet0/0
R   2011:1111:23::/64 [120/2]
     via FE80::290:CFF:FEA4:8B01, FastEthernet0/0
R   2011:1111:34::/64 [120/3]
     via FE80::290:CFF:FEA4:8B01, FastEthernet0/0
L   FF00::/8 [0/0]
      via ::, Null0
```

واژه نامه

3DES یا Triple DES یک فرایند رمزنگاری ۱۶۸ بیتی (3*56bit) است، این الگوریتم بر پایه تعدا تکرار تشکیل شده است که در سه مرحله انجام می‌شود، به این نوع الگوریتم‌ها الگوریتم کلید متقارن هم می‌گویند.

AAA از سه قسمت Authentication, Authorization, Accounting تشکیل شده است که کار احراز هویت، بررسی دسترسی و ثبت وقایع را انجام می‌دهد.

AAA server مسئول اجرای خدمات RADIUS و +TACACS در شبکه است.

ACS یا Access Control Server نرم‌افزاری مختص به شرکت سیسکو که مسئول اجرای خدمات RADIUS و +TACACS است.

Advanced malware protection (AMP) یک محافظ پیشرفته از بدافزار است که توسط سیسکو برای تجهیزات امنیتی FirePower طراحی شده است.

AES یا Advanced Encryption Standard یک الگوریتم زمزنگاری کلید متقارت است که کلیدهای آن در اندازه‌های ۱۲۸، ۱۹۲ و ۲۵۶ بیتی است.

Amplification DDoS attacks یک نوع حمله که در آن هکر با استفاده از درخواست‌های بزرگتر سعی می‌کند تعداد زیادی بسته را به یک مقصد ارسال کند.

antispam filters یک فیلتر چند لایه که میتنی بر اعتبار ایمیل سیسکو و هوشمندی در تهدیدات است.

AnyConnect یک سرویس برای ایجاد ارتباط امن با استفاده از پروتکل‌های IPSEC و SSL که به کاربرانی که در یک شبکه نامشخص قرار دارند یک ارتباط امن ارائه می‌دهد.

ASA یا Adaptive Security Appliance فایروال تخصصی شرکت سیسکو است.

Asset دارایی‌های یک شرکت که باید از آن در برابر حملات محافظت کرد.

Asymmetrical الگوریتم نامتقارن رمزگذاری دو طرفه که یک کلید برای رمزگذاری و یک کلید دیگر برای رمزگشایی استفاده می‌شود.

audit بررسی دقیق شبکه با استفاده از مجموعه‌ای از فرایندها که نام دیگر آن هم جمع‌آوری اطلاعات در شبکه است.

Authentication method list لیست روش‌هایی که برای احراز هویت استفاده می‌شود، مانند TACACS+، RADIUS، Enable Password، vty line و ...

Authorization method list لیست روش‌هایی که به کاربر مجوز استفاده از منابع شبکه را می‌دهد مانند TACACS+، RADIUS و Kerbros

back doors یا درب‌های پشتی، روشی است که در آن مهاجم با روش‌هایی سیستم قربانی را از راه دور کنترل می‌کند.

brute-force (password-guessing) attacks نوعی حمله است که در آن مهاجم به اصطلاح سعی در بمبارن رمز عبور کاربر می‌کند تا شاید بتوانند به آن رمز دست پیدا کنید.

BYOD (Bring Your Own Device) به روش‌هایی گفته می‌شود که کاربرن نهایی را قادر می‌سازد با هر دستگاهی بتوانند به شبکه آن سازمان متصل شوند.

BYOD device به دستگاه‌های شخصی کاربر برای متصل شدن به شبکه شرکت بدون در نظر گرفتن موقعیت جغرافیایی.

C3PL زبان سیاست طبقه‌بندی سیسکو است که با استفاده از class maps و policy maps ترافیک را کنترل می‌کند.

CA یا Certificate authority سیستمی برای صدور گواهینامه‌های امنیتی برای ایجاد اعتماد دو طرفه.

CCP ابزاری برای مدیریت و پیکربندی روترهای سیسکو که تحت وب است و نام کامل آن Cisco Configuration Professional است.

CCP communities مربوط به اجزای نرم‌افزار CCP که برای ساماندهی دستگاه‌های شبکه مورد استفاده قرار می‌گیرد.

CCP templates پیکربنی‌هایی که می‌توان برای چندین دستگاه مجداداً استفاده کرد که مربوط به اجزای نرم‌افزار CCP است.

CCP user profiles روشی برای محدود کردن تنظیمات CCP به کاربران.

CDP یا Cisco Discovery Protocol پروتکلی مختص شرکت سیسکو است که جهت کشف اطلاعات در شبکه طراحی شده است.

CERT بخشی از انستستوی مهندسی نرم‌افزار در دانشگاه ملون (پیتسبورگ، پنسیلوانیا) که یک مرجع کامل در مورد امنیت شبکه و سایبری است.

Cisco AnyConnect یک نرم‌افزار برای کاربران نهایی که می‌توانند از هر شبکه‌ای به صورت ایمن به شبکه اصلی سازمان متصل شوند.

Cisco AnyConnect Secure Mobility Client full-tunnel VPN با استفاده از نرم‌افزار AnyConnect می‌توانید یک ارتباط امن با شبکه ایجاد کنید با این قابلیت که پروتکل‌های TCP و UDP رمزنگاری می‌شوند.

Cisco SIO یک سری راه‌حل در جهت کمک به بهبود شبکه که تهدیدات، آسیب‌پذیری، تجزیه و تحلیل را برای کاهش حملات انجام می‌دهد.

ClamAV یک موتور آنتی ویروس منبع باز است که توسط شرکت‌های مختلف برای دستگاه‌های خودشان پیکربندی شده و پشتیبانی می‌شود.

Class map بخشی از چهارچوب سیاست‌های MFP یا همان Modular Policy Framework است که در دستگاه‌های مختلف برای مشخص کردن ترافیک به کار می‌رود.

class map type inspect این نوع Class Mapها نوع خاصی از کلاس هستند که ترافیک‌های منطقه‌ای در فایروال را مورد بررسی قرار می‌دهند.

Clientless SSL VPN دسترسی محدود به منابع VPN که در برخی از پروتکل‌ها امکانپذیر است پروتکل‌هایی که از TLS پشتیبانی می‌کنند مانند HTTPS، CIFS .

Computer viruses یک نرم‌افزار مخرب است که فایل‌های میزبان یا منطقه‌ای از سیستم‌ها را آلوده می‌کند و پیامدهای نامطلوبی به همراه خواهد داشت مانند حذف تمام داده‌ها، رمزنگاری انها و سرقت اطلاعات.

Control plane برای محافظت و بررسی بار کاری بر روی CPU در دستگاه‌های مختلف است که با روش‌های خاصی این بار کاری را کنترل می‌کند تا دستگاه مورد نظر از کار نیفتد.

Control plane policing (CoPP) سیاست‌هایی که بر روی کاربر اعمال می‌شود تا ترافیک کاری آنها در شبکه کنترل شود، این نوع سیاست‌ها بر روی، کل جریان شبکه انجام خواهد شد.

Control plane protection (CPPr) مانند CoPP عمل می‌کند با این تفاوت که به صورت محدودتر و جزئیات ریزتر را مورد بررسی و اعمال سیاست قرار می‌دهد.

CRL یک لیست ابطال برای گواهینامه‌ها در شبکه است که مشتریان را از وضعیت گواهینامه‌شان در CA مطلع می‌کند.

Custom privilege level سطح صفر برای کاربر معمولی و سطح پانزده برای مدیر به صورت پیش‌فرض تعریف شده است و هر چیزی بین یک تا چهارده باشد به آن سطح سفارشی گفته می‌شود.

Data plane به سیستم‌های منطقی در شبکه گفته می‌شود مانند ترافیک کاربران نهایی به سرور داخلی شبکه.

DH group به الگوریتم‌های امنیتی اشاره دارد.

DHCP Snooping یک ویژگی امنیتی است که به مهاجمان یا سیستم‌هایی که می‌خواهند از طریق سرویس DHCP خود را در شبکه معرفی کنند اجازه دسترسی نمی‌دهد.

Digital Signature یک Hash **رمزنگاری** شده است که به طور خاص فرستنده پیام را مشخص و اعتبار پیام دریافت شده را تایید می‌کند.

Direct DDoS attacks حملات مستقسم DDos هنگامی اتفاق می‌افتد که منبع حمله ایجاد می‌شود.

Downloaders یک نرم‌افزار مخرب است که از طریق اینترنت نرم‌افزارهای مخرب را در سیستم مورد نظر اجرا می‌کند.

Dynamic ARP inspection (DAI) یک ویژگی امنیتی در بسته‌های ARP است، این ویژگی بسته‌هایی که IP و MAC آن نامعتبر باشد، حذف خواهد کرد.

Eavesdropping به هر روشی که به اطلاعات و داده‌ها گوش دهیم گفته می‌شود.

EUI-64 یا Extended Unique Identifier-64 یک استاندارد سازمان IEEE برای تبدیل MAC آدرس ٤٨ بیتی به ٦٤ بیت در IPV6 است.

exploit یک برنامه‌ی مخرب برای بهره‌برداری از آسیب‌پذیری استفاده می‌شود.

File sandboxing در صورت شناسایی بدافزار، CISCO AMP این قابلیت را دارد که این نوع پرونده‌ها را در sanbox ذخیره کند و برای تجزیه و تحلیل و تعیین سطح تهدید این نوع فایل‌ها از الگوریتم‌های یادگیری استفاده می‌کند.

hash در این روش یک ورودی از اطلاعات دریافت می‌شود و بعد از اجرای یک الگوریتم بر روی آن ورودی تبدیل به اعداد و حروف خواهد شد.

HMAC کد تایید هویت پیام Hash است که برای تاید صحت و تایید صحت داده‌ها استفاده شده است.

Identity certificate یک گواهینامه‌ی دیجیتال است که به کاربران، میزبان‌ها، ایمیل اختصاص داده می‌شود.

Identity Services Engine (ISE) یک نرم‌افزار از سیسکو که برای راه‌اندازی AAA، BYOD و ایجاد سیاست در شبکه مورد استفاده قرار می‌گیرد.

IDS (intrusion detection system) یک سیستم تشخیص نفوذ است که درباره‌ی حمله به شبکه به مدیران آن هشدار می‌دهد ولی مهمترین کار آن فقط هشدار است و نمی‌تواند جلوی آن را بگیرد.

IKE Phase 1 فاز یک مربوط به تبادل کلید که در مورد پارامترهای طول عمر، رمزنگاری، گروه DH، هش کردن و ایجاد تونل صحبت می‌کند.

IKE phase 2 در فاز دوم تبادل کلید فناوری IPSEC به صورت واقعی اجرا می‌شود.

Immunet یک نرم‌افزار آنتی ویروس رایگان است که توسط Cisco Sourcefire نگهداری می‌شود.

IPS (intrusion prevention system) یک سیستم تشخیص نفوذ است که در مورد حمله به شبکه گزارش می‌دهد و مهمترین تفاوت آن با IDS این است که جلوی عملکر مهاجم را در شبکه می‌گیرد.

IPsec به مجموعه‌ای از پروتکل‌ها گفته می‌شود که برای محافظت از محتوای بسته IP که در لایه سه کار می‌کند به کار می‌رود.

key loggers نرم‌افزارهایی که تلاش می‌کنند اطلاعات ورودی کاربر از طریق صفحه کلید را بدست بیاورند که این اطلاعات می‌تواند شامل رمز عبور، پین‌کدها، شماره کارت‌های اعتباری و ... باشد.

LDAP مخفف Lightweight Directory Access Protocol است که دارای یک API است و به سرویس Active Directory متصل می‌شود و می‌توانید از آن طریق اطلاعات را تغییر دهید.

lifetime مقدار زمانی است که مثلاً یک کلید برای اعتبار خود از آن استفاده می‌کند.

LLDP (Link Layer Discovery Protocol) یک پروتکل عمومی برای کشف در شبکه است.

logic bombs یک برنامه مخرب است که توسط مهاجم برای خرابکاری در شبکه شما طراحی و اجرا می‌شود و بعد از مدت زمان مشخصی خود را از روی شبکه قربانی پاک خواهد کرد.

Mailers and mass-mailer worms نوعی از پیام‌های worms است که خود را در لای پیام‌های ارسالی در ایمیل پنهان می‌کند.

Malvertising نوعی عمل مخرب است که اصولاً بر روی مرورگرها اجرا می‌شود و کاربران را ناخواسته به سمت سایت‌های مشخص می‌فرستد.

Man-in-the-middle attack نوعی استراق سمع است که مهاجم خود را بین یک مکالمه قرار می‌دهد و به اطلاعات آنها دست پیدا می‌کند، مانند وایرلس، روتر و...

Management plane به ترافیک داخل شبکه می‌گویند که با استفاده از پروتکل‌های مختلف مانند SSH, HTTPS و... باید آن را امن کرد و توسط سرویس SNMPv3 به اطلاعات کاملی از آن رسید.

MD5 یک عملکرد رمزنگاری ۱۲۸ بیتی است که برای امن کردن رمز عبور و Hash کردن آن استفاده می‌شود.

MD5 route authentication برای تایید اعتبار در جدول‌های مسیریاب‌ها باید از این نوع Hash استفاده کرد تا ارتباط بین روترها به صورت امن انجام شود این نوع رمزنگاری در روتینگ پروتکل‌های OSPF, EIGRP, RIPv2, BGP کاربرد دارد.

Method list لیست روش‌های موجود برای استفاده از AAA مانند TACACS+ و RADIUS و...

MPF یا Modular Policy Framework پیکربندی‌هایی برای ایجاد قوانین برای فایروال مانند ترافیک، QOS که دارای سه مولفه اصلی Class Map, Policy Map, Service Policy است.

NA یا Neighbor Advertisement مربوط به تبلیغات همسایگی در IPV6 است.

Named Access Control list (ACL) ایجاد یک لیست دسترسی برای یک منبع خاص برای دسترسی به یک شبکه و ... که دارای دو نوع استاندارد و پیشرفته است که در نوع پیشرفته آن حتی می‌توانید مشخص کنید چه نوع سرویسی اجازه عبور داشته باشد.

NAT یا Network Address Translation برای ترجمه آدرس از شبکه داخلی به شبکه اینترنت کاربرد دارد، مثلاً اگر آدرس شبکه داخلی ۱۹۲.۱۶۸.۱.۱باشد برای دسترسی کلاینت به اینترنت این آدرس تبدیل می‌شود به یک آدرس Valid که این آدرس در دنیای اینترنت مورد قبول است.

Network antivirus قابلیت آنتی ویروس در دستگاه‌های زیرساختی شبکه.

Next-Generation IPS (NGIPS) مجموعه جدید از راه حل‌های IPS که با نام Cisco FirePOWER NGIPS هم شناخته می‌شود و دارای چندین لایه محافظتی با بازرسی بالا است که شبکه شما را در برابر مهاجمان امن نگه می‌دارد.

NFP یا Network foundation protection که دارای سه مولفه Management Plane, Control Plane, Data Plane است و دارای راه‌کارهایی برای حفظ امنیت و کاهش بار دستگاه‌های شبکه است.

NS یا neighbor solicitation برعکس NA است و برای درخواست همسایگی در IPv6 استفاده می‌شود.

NTP یا Network Time Protocol مربوط به پروتکل زمان است که می‌توانید با کمک آن تمام سیستم‌های داخل شبکه خود را بر روی یک زمان مشخص تنظیم کنید، مثلاً یک روتر را به عنوان سرور NTP قرار دهید و بقیه دستگاه‌ها را ملزم کنید که از این روتر پیروی کنند.

Packet filtering اطلاعاتی مانند آدرس منبع و مقصد و پورت منبع و مقصد را بررسی می‌کند.

Parser View یکی دیگر از روش‌های اختصاص دستورات به کاربران این است که یک View ایجاد کنیم و دستورات را به آن view اختصاص دهیم و کاربران هم با عضو شدن در آن View می‌توانند از دستورات آن view استفاده کنند و دسترسی لازم را داشته باشند.

PAT یا Port Address Translation که زیرمجموعه‌ی پروتکل NAT است که زمانی که یک آدرس محلی به یک آدرس در اینترنت ترجمه می‌شود یک پورت باید به آن آدرس اضافه شود که آن پورت همان PAT است.

Personally, identifiable information (PII) نوعی از اطلاعات است مانند نام، تاریخ تولد، آدرس‌ها و....

Phishing یک نوع حمله است که در آن مهاجم با استفاده از ایمیل به کارمندان یک موسسه یا یک سازمان یک نامه ارسال می‌کند و در آن با روش‌هایی از آنان درخواست می‌شود که اطلاعاتی را برای مهاجم ارسال کنند.

PKCS#10 یک کلید عمومی برای Cryptography که شماره‌ی آن ۱۰ است و برای فرمت پرونده است و برای ارسال گواهینامه استفاده می‌شود.

PKCS#12 کلید عمومی شماره‌ی ۱۲ که برای ذخیره کلیدهای خصوصی است به همراه گواهینامه‌های کلید عمومی.

PKCS#7 یک استاندارد کلید عمومی با شماره‌ی ۷ است که برای توزیع دیجیتال گواهینامه‌ها کاربرد دارد.

PKI یا Public key infrastructure یک معماری مقیاس پذیر که شامل نرم افزار ، سخت افزار ، افراد ، و رویه ها برای تسهیل مدیریت گواهی های دیجیتال است.

Policy map جزئی از MPF و C3PL است که مشخص می‌کند کدام Class MAP اجرا شود.

policy map type inspects نوعی از فایروال است که در Zoned-Based Firewalls کاربرد دارد، و همچنین در ASA برای بررسی عمیق‌تر بسته‌ها استفاده می‌شود.

Public key بخشی از یک جفت کلید است که در PKI با افراد دیگر به اشتراک گذاشته می‌شود.

Quantitative روشی برای ارزیابی ریسک که از یک مدل ریاضی مبتنی بر داده‌ها استفاده می کند.

RA جزئی از پروتکل IPV6 برای آگاهی از سایر دستگاه‌هایی که از این آدرس استفاده می‌کنند.

RADIUS یا Remote Authentication Dial-In User Service یک روش برای ارتباط دستگاه‌ها با سرور AAA مانند ACS است.

Ransomware نوعی از بدافزار است که سیستم را به خطر می‌اندازد، طریقه کار آن هم این است که با آلوده کردن سیستم، از قربانی باج‌گیری می‌کنند تا قربانی بتواند این بدافزار را از سیستم خود پاک کند.

Risk اندازه‌گیری احتمال حمله موفقیت آمیز با اندازه‌گیری سطح تهدید در برابر آسیب‌پذیری خاص.

Risk rating قبل از اینکه اقدامات امنیتی در شبکه شما اعمال سود شبکه شما از نظر احتمال حمله رتبه‌بندی می‌شود.

Root certificate بالاترین سطح گواهینامه است.

Rootkits مجموعه ابزارهایی که یک مهاجم برای بالا بردن سطح دسترسی به شبکه استفاده می‌کند تا به صورت کامل کنترل سیستم آسیب دیده را در دست بگیرد.

RSA یک الگورتم کلید عمومی است که در سال ۱۹۷۷ توسط Rivest, Shamir, Adleman توسعه داده شده که در حال حاضر اکثر مرورگرها برای تایید اعتبار از آن استفاده می‌کنند.

Secure bootset بخشی از ویژگی CISCO IOS است که برای جلوگیری از پاک شدن اطلاعات در Flash و NVRAM مورد استفاده قرار می‌گیرد.

Secure Copy (SCP) یک روش امن برای کپی کردن تنظیمات و اطلاعات دستگاه‌های شبکه است.

SecureX چارچوب امنیتی سیسکو برای ایجاد و اجرای سیساست‌های امنیتی در سرتاسر شبکه.

Security levels یک سطح در ASA که اگر عدد آن بیشتر باشد یعنی دسترسی بیشتر و اگر هم کمتر باشد یعنی دسترسی کمتر خواهد بود.

Service policy مشخص می‌کند که Policy Map در کدام Interface اجرا شود.

SFR نسان دهنده‌ی یک امضاء خاص در IPS برای مشخص کردن حمله است.

SHA1 یا همان Secure Hash که جانشین خوبه MD5 است و توسط آژانس امنیت ملی NSA توسعه یافته است.

Signature files بسته امضایی که IPS/IDS را در برابر روش‌های جدید حمله به روز می‌کند، بسته های امضای IOS IPS شبیه IPS/IDS است.

Signature micro-engines بخشی از IPS/IDS که به طور مشترک از گروهی از امضاها را دسته بندی و پشتیبانی می‌کند.

SNMP یا Simple Network Management Protocol پروتکلی برای مدیریت دستگاه‌های شبکه است که مورد استفاده قرار می‌گیرد.

Snort یک فناوری کشف و پیشگیری از نفوذ است که توسط شرکت Sourcefire که در حال حاضر بخشی از سیسکو است توسعه یافته ایست.

Spammers یک نوع بدافزار است که هدف آن ارسال پیام‌های ناخواسته برای کاربران است تا از طریق آن از کاربران بخواهند به ایمیل‌ها پاسخ دهند و یا اینکه بر روی لینک‌های مخرب آن کلیک کنند.

Spoofed Address تغییر آدرس منبع بسته IP یا همان سرقت هویت یک آدرس IP.

Spoofing روشی برای جعل کردن آدرس IP، MAC، Email که در آن مهاجم وانمود می‌کند که یکی از دستگاه‌ها یا کاربران شبکه است.

SSH یا Secure Shell که یک جایگزین امن برای Telnet است و از طریق آن می‌توانید به CLI دستگاه در شبکه دست پیدا کنید.

SSL یا Secure Sockets Layer که در پروتکل HTTPS کاربرد دارد و یک روش امن برای ارتباط با وب‌سایت‌ها است.

ACL standard/extended برای فیلتر کردن بسته‌ها کاربرد دارد و در دو حالت استاندارد و پیشرفته به کار می‌روند.

Stateful Filtering این ویژگی به عنوان dynamic packet filtering هم شناخته می‌شود و برای بررسی پکت‌های عبوری از فایروال کاربرد دارد.

SVI رابط مجازی یا همان VLAN در سوئیچ است.

Symmetrical به معنای هر دو طرف یکسان است و برای کلیدهای رمزنگاری و رمزگشایی استفاده می‌شود.

syslog روشی برای جمع آوری اطلاعات از دستگاه‌های شبکه که با کمک آن می‌توانید امنیت کار را افزایش دهید.

TACACS+ سیستمی برای احراز هویت است که می‌تواند برای برقراری ارتباط بین سرور AAA و مشتری استفاده شود.

Threat تهدیدات زمانی رخ می‌دهد که مهاجم در بخش قبلی آسیب‌پذیری‌های یک سیستم را شناسایی کند و بتواند از آن طریق به شبکه ما ضربه بزند.

TLS یا Transport Layer Security بر اساس SSL طراحی شده ولی بیشتر به عنوان استاندارد IETF مورد استفاده قرار می‌گیرد.

TLP یا Traffic Light Protocol مجموعه‌ای از قوانین که توسط CERT نامگذاری شده و برای اطمینان از اینکه اطلاعات حساس با کاربر مشخص و صحیح به اشتراک گذاشته شود.

Transform set مجموعه از پروتکل IPsec که در فاز IKE مورد استفاده قرار می‌گیرد.

Transparent firewall این نوع فایروال در لایه دوم مدل OSI پیاده‌سازی شده است ولی توانایی تجزیه و تحلیل ترافیک در لایه ۳ و بالاتر را دارا است.

Trojan horses یک نوع از بدافزار است که برای اجرای دستورالعمل‌هایی مشخص ایجاد شده است، این تروجان برای حذف پرونده‌های، سرقت داده‌ها و به خطر افتادن یکپارچگی سیستم مورد استفاده قرار می‌گیرد.

VPN یا Virtual private network یک شبکه خصوصی و مجازی است و برای رمزنگاری، احراز هویت و یکپارچگی داده‌ها مورد استفاده قرار می‌گیرد.

Vulnerability نقص یا ضعف در طراحی سیستم که باعث می‌شود مهاجم از آن بهره‌برداری کند.

Worms به ویروس‌هایی گفته می‌شود که خود را از طریق شبکه تکثیر می‌کنند و در اکثر موارد یک دستورالعمل خاص را در سیستم‌های شبکه اجرا می‌کنند.

Zone pairs به جریان ترافیک در شبکه گفته می‌شود که مثلاً جریان ترافیک از شبکه داخلی به شبکه خارجی گفته می‌شود و می‌توانید سیاست‌های ترافیکی خود را روی آن پیاده‌سازی کنید.

منابع

Sybex - CCNA Security Study Guide Exam 210-260 - Michael Watkins
Kevin Wallace, CCIE No. 7945

CCNA Security 210-260 Official Cert Guide - OMAR SANTOS (CISSP-463598), JOHN STUPPI (CCIE NO. 11154)

Cisco ASA - All-in-One Firewall, IPS, Anti-X, andVPN Adaptive Security Appliance, Second Edition Jazib Frahim (CCIE No. 5459), OMAR SANTOS (CISSP-463598)

CCNP SWITCH 642-813 - David Hucaby, CCIE No. 4594

CCNA ++ - Farshid babajani – 3isco.ir

http://www.firewall.cx

https://www.cyberpolice.ir

http://cisco.com

http://vcenter.ir

https://ipwithease.com

https://www.gullynetworkers.com

کتاب‌های آموزشی شبکه

در زیر چند کتاب دیگر نویسنده را مشاهده می‌کنید که می‌توانید در زمینه‌های دیگر شبکه از آنها استفاده کنید:

- مدیر شبکه ۱
- مدیر شبکه ۲
- کریو کنترل
- لینوکسUbuntu
- ایکسچنج و اسکایپ
- مهندسی مایکروسافت
- اکتیودایرکتوری ۲۰۰۸
- CCNA Route & Switch
- شیرپوینت را قورت دهید ویرایش دوم
- شیرپوینت را قورت دهید ویرایش اول
- مایکروسافتSQL
- همه کتاب‌ها
- کتاب آموزشیISA Server
- PowerForms
- VMware Systems 2020

تمام این کتاب‌ها طی چندین سال نوشته شده و بسیار می‌تواند شما را برای اجرای یک مدیریت خوب در شبکه کمک کند.

تماس با ما

آدرس ایمیل :

Farshid_Babajani@live.com

Info@3isco.ir

موبایل :

0919 9926 216

کانال تلگرام :

https://t.me/ciscopress

تلگرام نویسنده:

https://t.me/farshidbabajani