روشهای مختلف تشخیص Firewall وتنظیم آنها در کارکردبا دیگر المانها

پروژه درس امنیت شبکه های کامپیوتری

زیرنظرجناب آقای دکتریزدیان

ارائه : پیام موسی زاده

دیواره های آتش

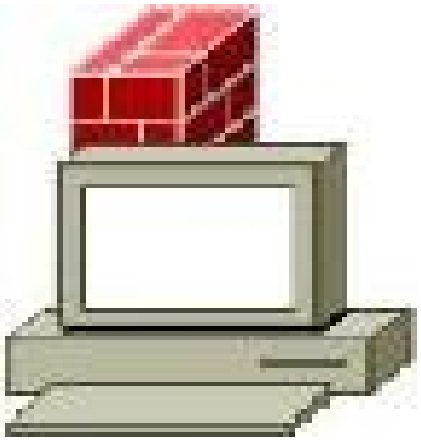
Firewalls

مقدمه

دیواره آتش جهت حفاظت از کامپیوترها (چه بصورت شبکه وچه بصورت انفرادی)در مقابل هرگونه تهدیدات خصمانه که میتواند منجر به سرقت اطلاعات ، از بین رفتن اطلاعات ویا دستکاری در اطلاعات ،که خود میتواند ناشی از افراد درون سازمانی ویا بیرونی باشد ،بکار گرفته میشود.

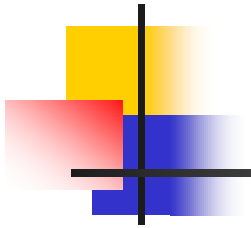
Types of firewalls (1)

1- Desktop Firewall



هرگونه نرم افزاری که جهت حفاظت از یک کامپیوتر منفرد میتواند روی سیستم عامل آن نصب شود ،میباشد.

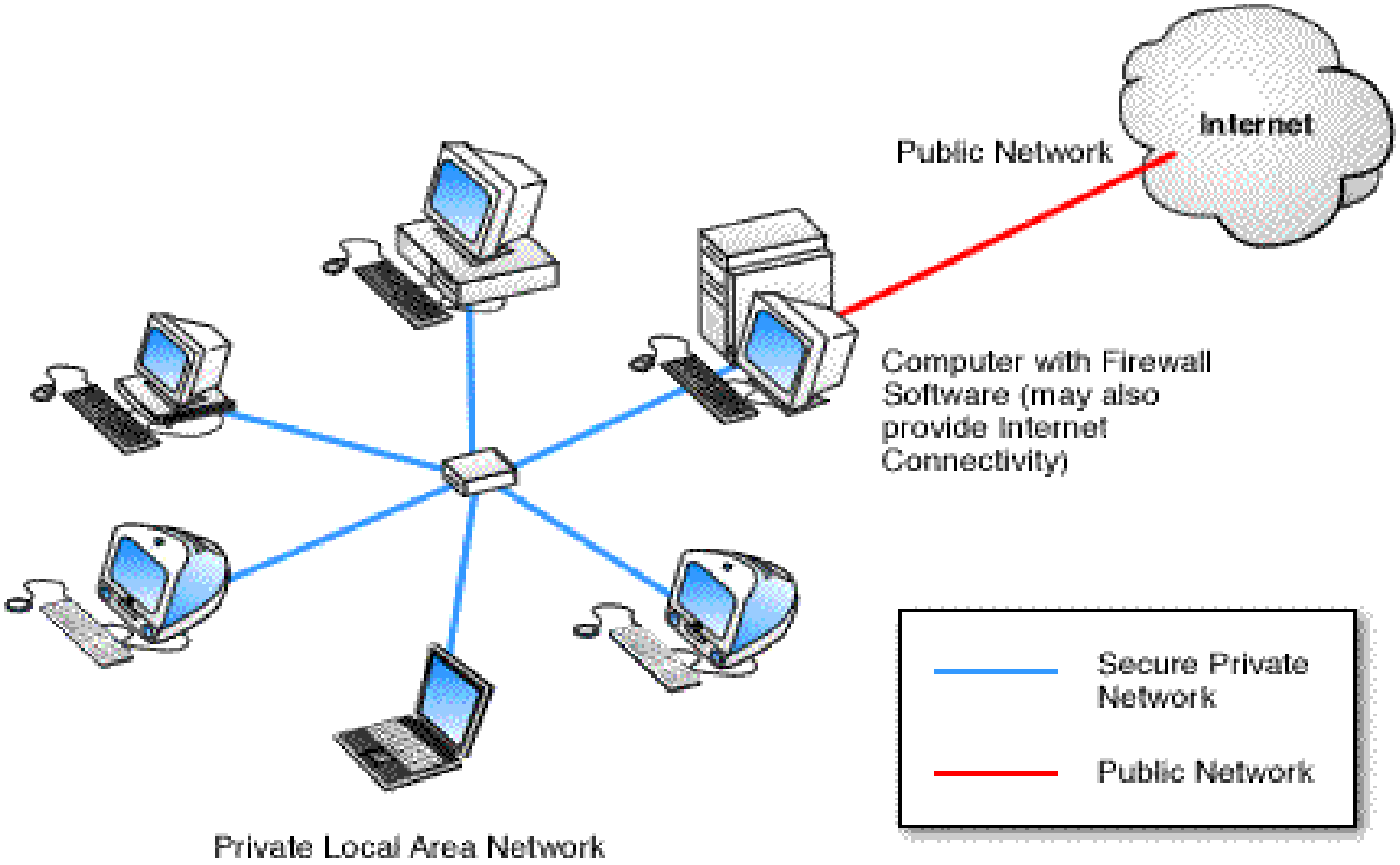
Types of firewalls (2)



2-Software Firewall

در این نوع از دیوارآتش ، یک بسته نرم افزاری دیواره آتش بر روی یک سیستم عامل یک Server در داخل شبکه نصب شده وآنرابه یک دیوارآتش تبدیل میکند.از این نوع دیوارآتش بیشتر به عنوان دیواره آتش نوع Application firewall استفاده میشود. دیواره آتش نرم افزاری (Software Firewall) دارای فیلترهای پیچیده ایی جهت بررسی محتویات ترافیک شبکه به لحاظ مناسب بودن فرمت ترافیک میباشند.اینگوه دیواره آتش معمولاً (نه همیشه) پشت دیواره آتش سخت افزاری قرار می گیرند.

Types of firewalls (3)



Types of firewalls (4)

3- Hardware Firewall

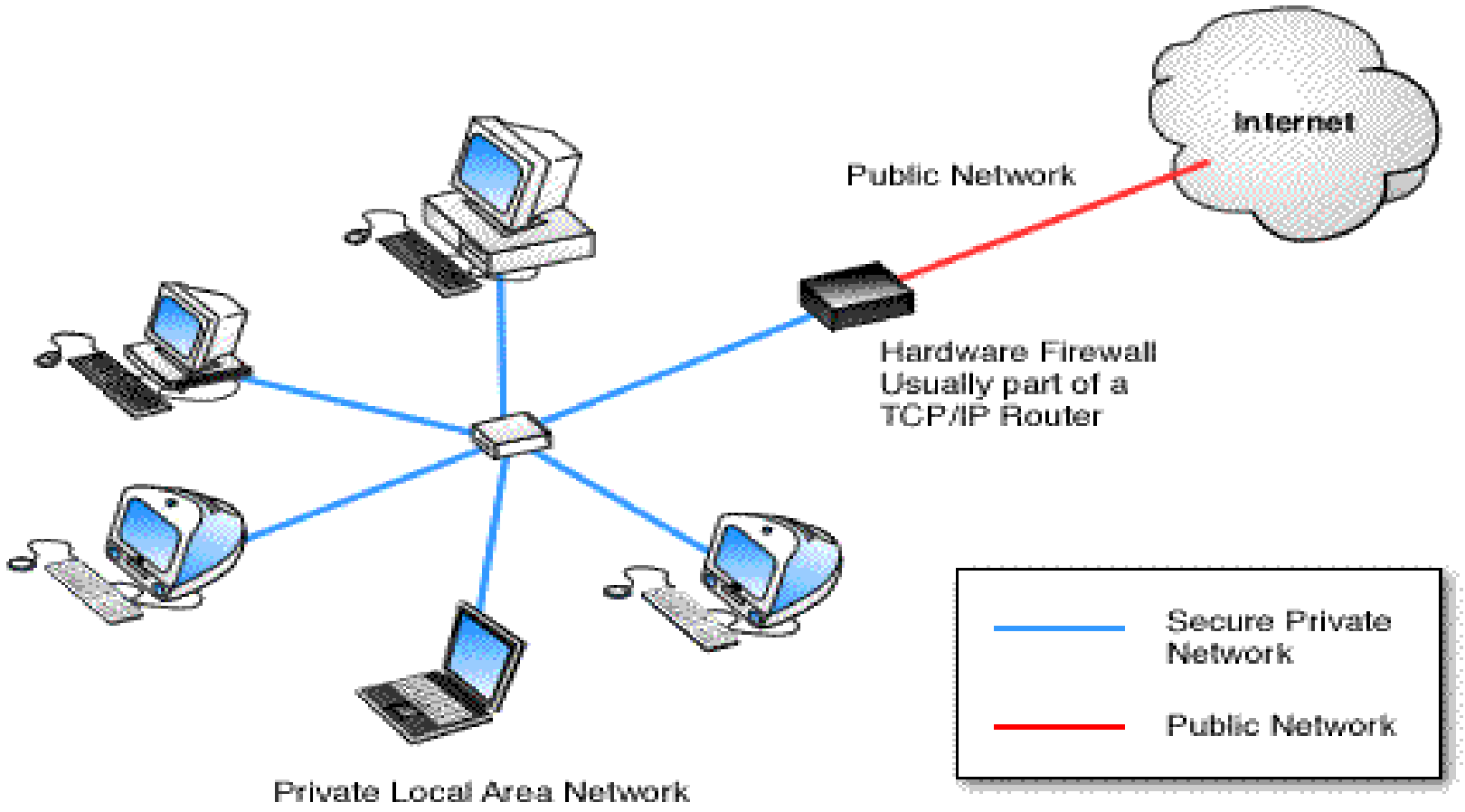
دیوارآتش سخت افزاری عبارت است از یک سخت افزار خاص با یک سیستم عامل ویژه (یا دارای هسته مرکزی سیستم عامل درونی).این نوع از دیواره آتش عبارت است از یک Router که دارای توانایی های خاص دیوارآتش نیز میباشد.طراحی این نوع از دیوارآتش بر این اساس بوده که بتوانند حجم عظیمی از اطلاعات را از خود عبور دهند.

Types of firewalls (5)

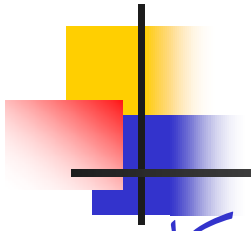
Hardware Firewall (continue)

اغلب دیوارآتش سخت افزاری در محل ارتباط شبکه داخلی باابیرون از سازمان قرار می گیرد.برخی اوقات دیوارآتش نرم افزاری و سخت افزاری تواماً با یکدیگر در یک شبکه مورداستفاده قرار می گیرند که در اینحالت دیوارآتش سخت فزاری ترافیک بیرون از شبکه را کنترل میکند ودیوار آتش نرم افزاری ترافیک داخل شبکه را.وقتی دیوارآتش سخت افزاری بتوسط حجم عظیمی از ترافیک ناخواسته بمباران میشود، دیوارآتش سخت افزاری ترافیک ناخواسته را حذف میکند.با این عمل نه تنها از دیوارآتش نرم افزاری حفاظت میکند بلکه اجازه میدهدکه دیوارآتش نرم افزاری بطور مناسب به بررسی ترافیک شبکه بپردازد واین خود باعث افزایش بازدهی شبکه نیزمیشود.

Types of firewalls (6)



Types of Firewalls from Technology point of view (1)



دیوارهای آتش همچنین میتوانند بر اساس تکنولوژیکی و کاربرد درنظرگرفته شده نیز تقسیم بندی شوند.

1. Packet Filtering
2. Circuit Gateways
3. Application Proxies
4. Hybrid

نکته: با توجه به لایه لایه بودن معماری شبکه ، دیواره آتش نیز لایه به لایه طراحی میشود.

Types of Firewalls from Technology point of view (2)

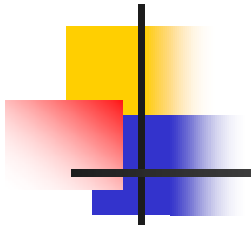
Packet Filtering

در لایه شبکه ، دیوار آتش فیلد های بسته IP را پردازش و تحلیل میکند .

موارد قابل بررسی:

آدرس مبدا
آدرس مقصد
شماره شناسایی یک دیتاگرام
شماره پروتکل
زمان حیات بسته

Types of Firewalls from Technology point of view (3)



Packet Filtering

دیوارآتش نوع فیلترکننده بر اساس نوع عمل فیلترینگ میتوانند به گروه های زیر تقسیم شوند:

1-Static Filtering

دراغلب مسیریاب ها مورد استفاده قرار می گیرند وقوانین فیلترینگ بصورت دستی مشخص می گردد.

2-Dynamic Filtering

اجازه میدهد که قوانین فیلترینگ بر اساس پاسخها به محیط بیرون معین شود.

3-Statefull Inspection

مشابه حالت Dynamic Filtering میباشد با این تفاوت که packetها با دقت بیشتری بازرسی میشوند.

Types of Firewalls from Technology point of view (4)

Circuit Gateways

در این لایه برای تحلیل بسته ها از فیلدهای سرآیند لایه انتقال استفاده میشود.
فیلدهای بسته لایه انتقال جهت بازرسی در دیواره آتش عبارتنداز:

- **شماره پورت پروسه مبدا ومقصد.**
- **بیتهای کنترلی ،فیلد** Sequence Number **،فیلد** Acknowledgement .

Types of Firewalls from Technology point of view (5)

Application Proxies

در لایه Application دیواره آتش فیلدهای سرآیند ومحتوای داده هابررسی میشوند.

در این لایه حفاظت بر اساس نوع سرویس و ماهیت برنامه کاربردی انجام میشود.

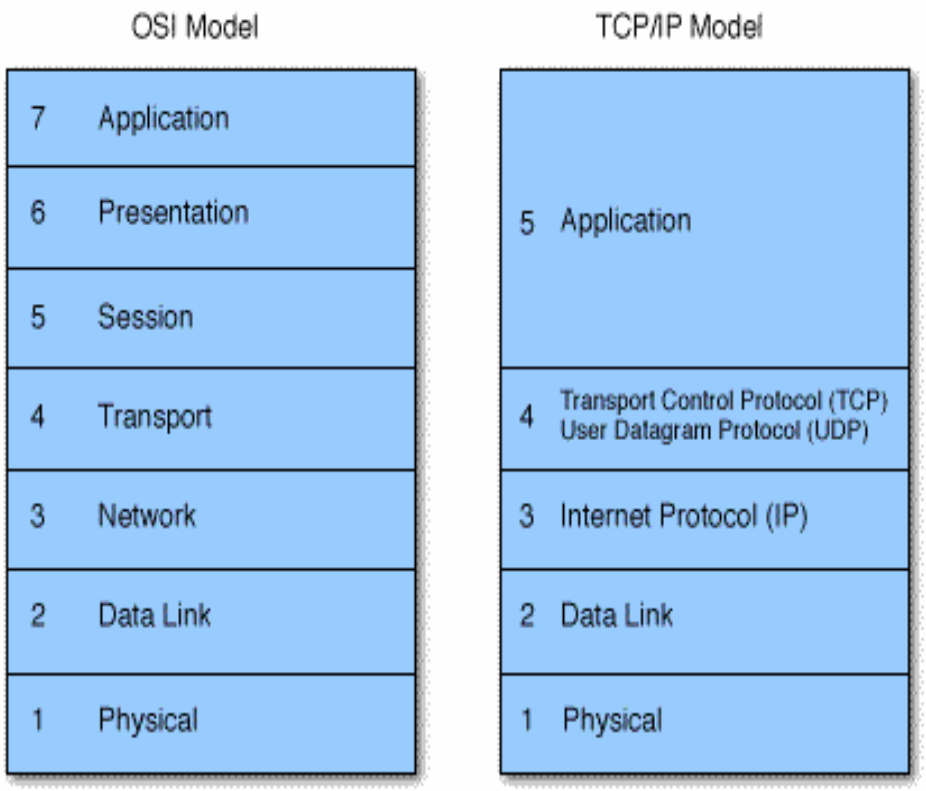
برای هر سرویس مجزا باید یکسری قوانین امنیتی مجزا تعریف کرد که این به نوبه خود باعث پیچیدگی در این لایه خواهد شد.

Types of Firewalls from Technology point of view (6)

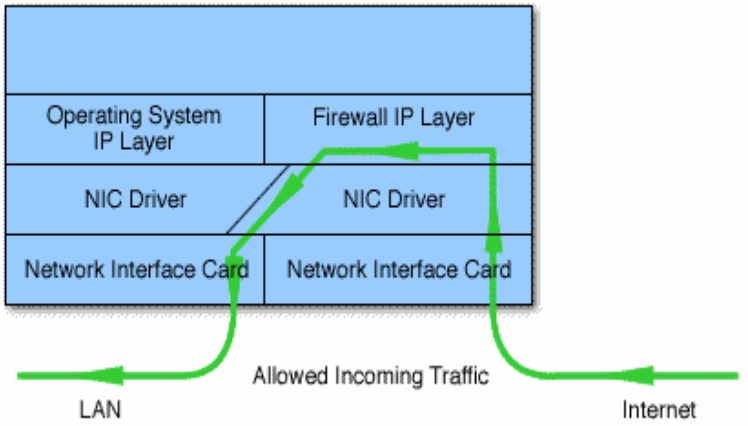
Hybrid Firewalls

دیوارآتش چندگانه یا Hybrid Firewalls همانطور که از اسم آنها مشخص میباشد از ترکیبی ازتکنولوژیهای مختلف سود می برند.بعنوان مثال یک Hybrid Firewalls میتواند شامل ترکیبی از packet filtering به همراه Application Proxy باشد.

مقایسه مدل TCP / IP و OSI

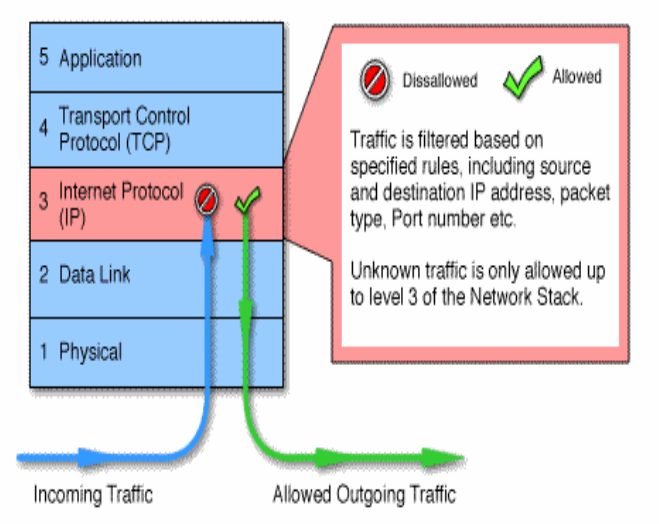


Professional Firewalls Have Their Own IP Layer.

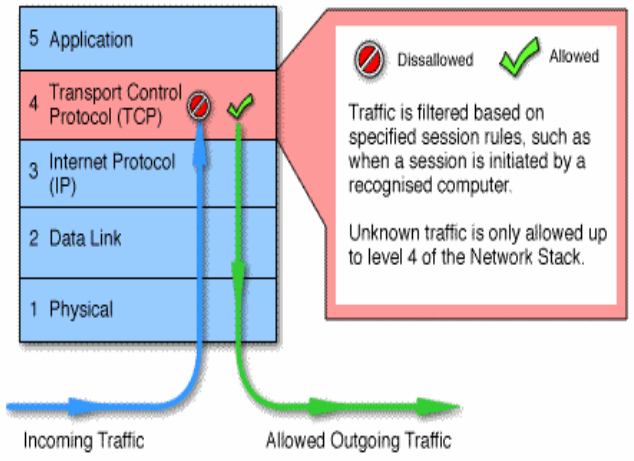


Firewalls at one glance

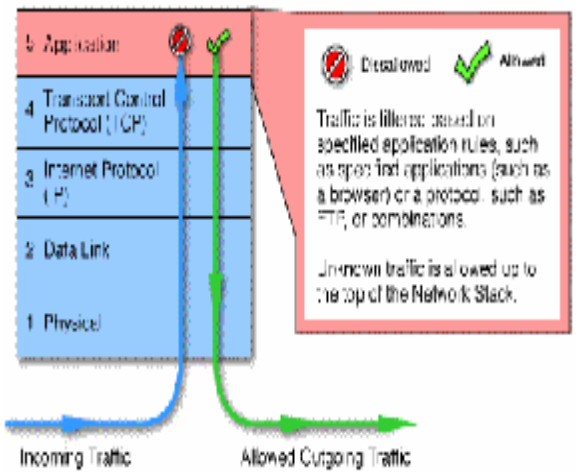
Packet Filtering



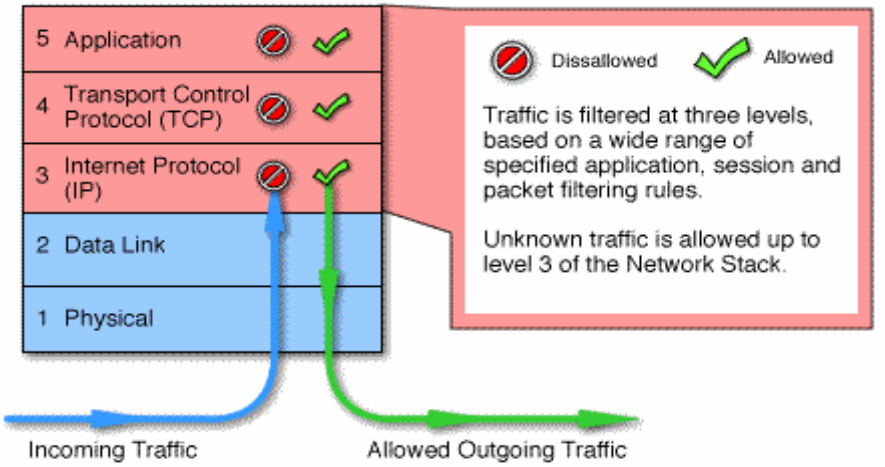
Circuit level Gateway



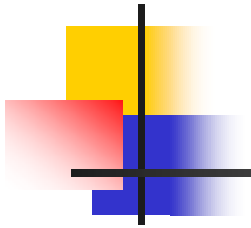
Application level Gateway



Hybrid Firewall (Stateful Multilayer Inspection)



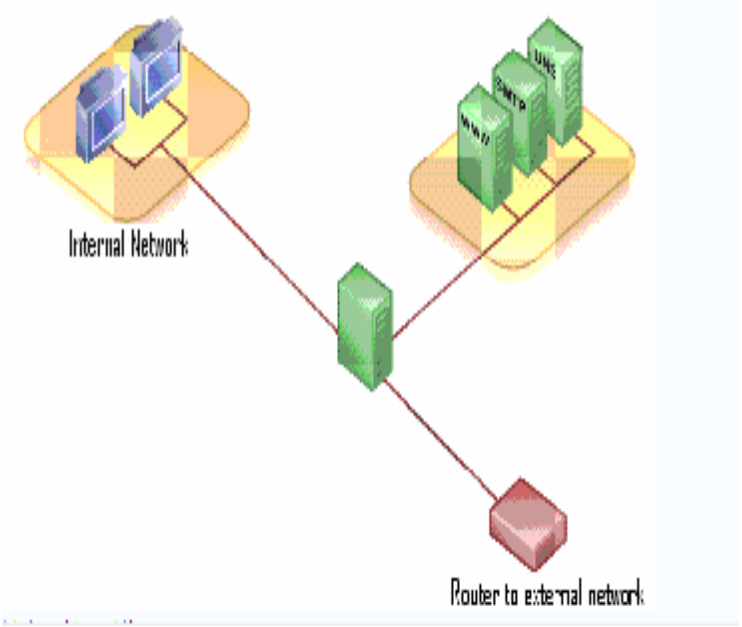
DMZ[Demilitarized zone] (1)

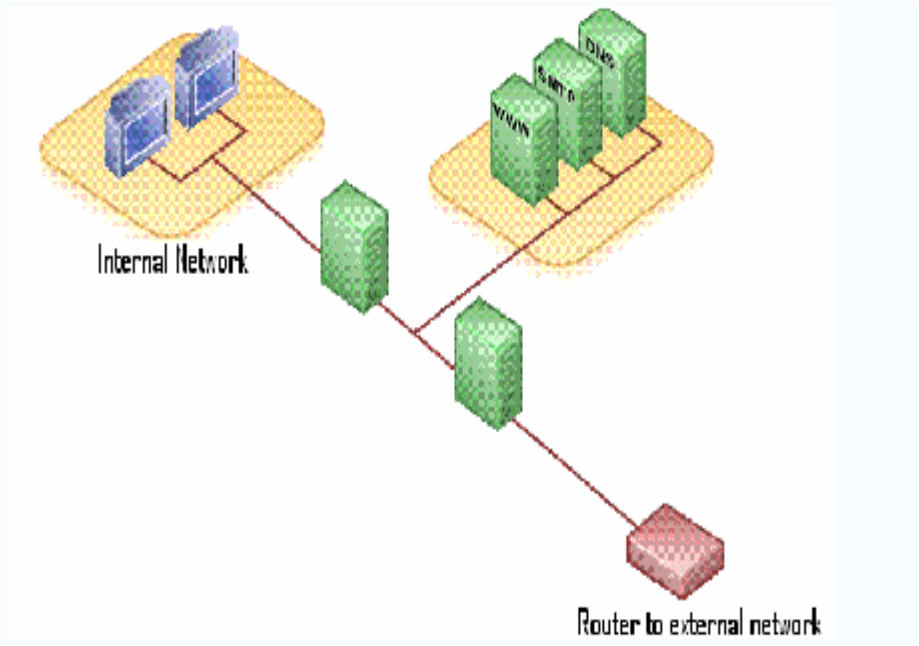


در امنیت کامپیوتری ، Demilitarize zone(DMZ) که تحت نامهای demarcation zone ویا perimeter network شناخته میشود، یک زیرشبکه ایی فیزیکی یا منطقی ازیک سازمان میباشد که سرویسهای قابل ارائه به بیرون سازمان از آنجا مدیریت و انجام میشود.هدف اصلی از DMZ اضافه کردن یک لایه امنیتی به شبکه LAN سازمان مطبوع میباشد.

به عبارت واضح ترهرسرویسی که قراراست به کاربران خارج از سازمان واگذارشود ،در این منطقه قرار می گیرد.از مهمترین این سرویسها میتوان به Web serverها،Mail serverها و DNS serverهااشاره نمود.

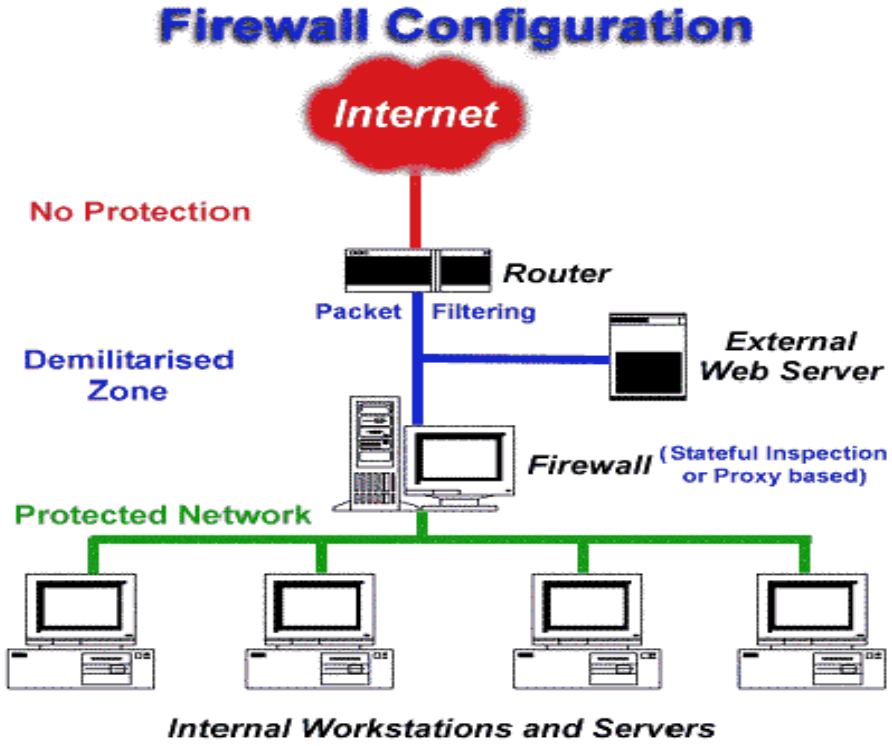
DMZ [Demilitarized zone] (2)





مزایای استفاده از شبکه های DMZ

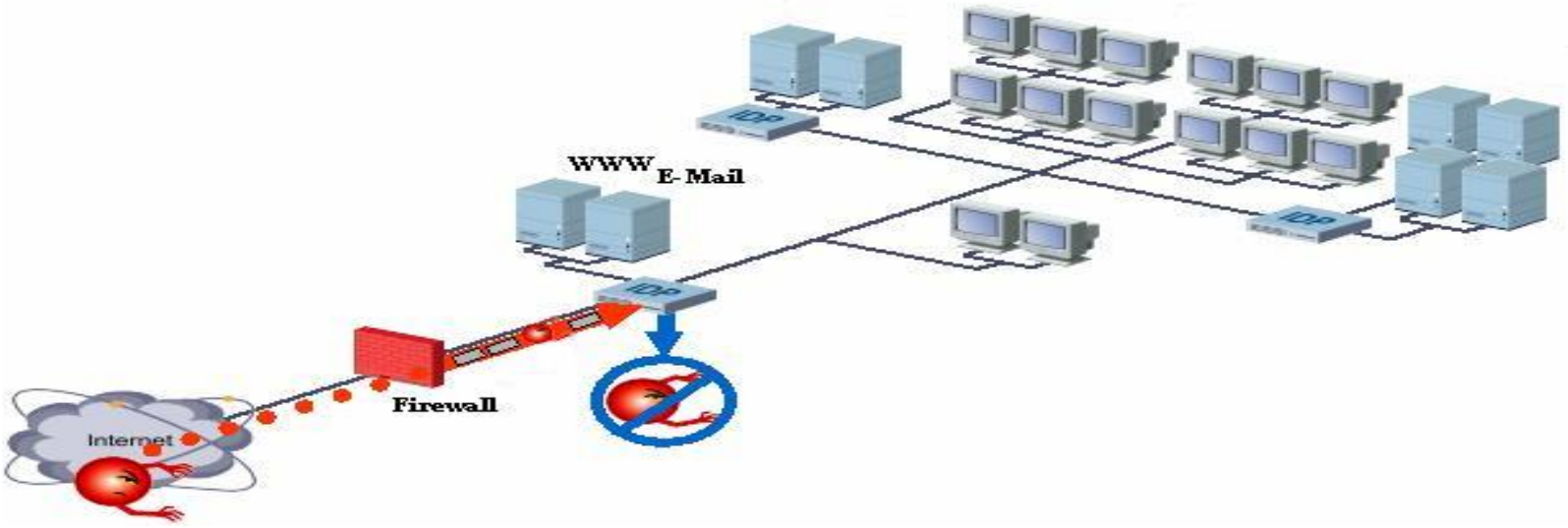
دلیل عمده استفاده از چنین شبکه هایی، بالابردن سطح امنیتی کل شبکه میباشد.Server هایی که باید با clientهای اینترنت در تماس باشند در DMZ قرارمی گیرندو سرورهای اصلی سازمان در شبکه داخلی قرار می گیرند.خود شبکه داخلی نیز بتوسط Firewall ، IDS & IPS و Honeypot محافظت میشوند.



** نکته مهم: اطلاعات اصلی و مهم سازمان را نباید در منطقه DMZ قرارداد.

DMZ

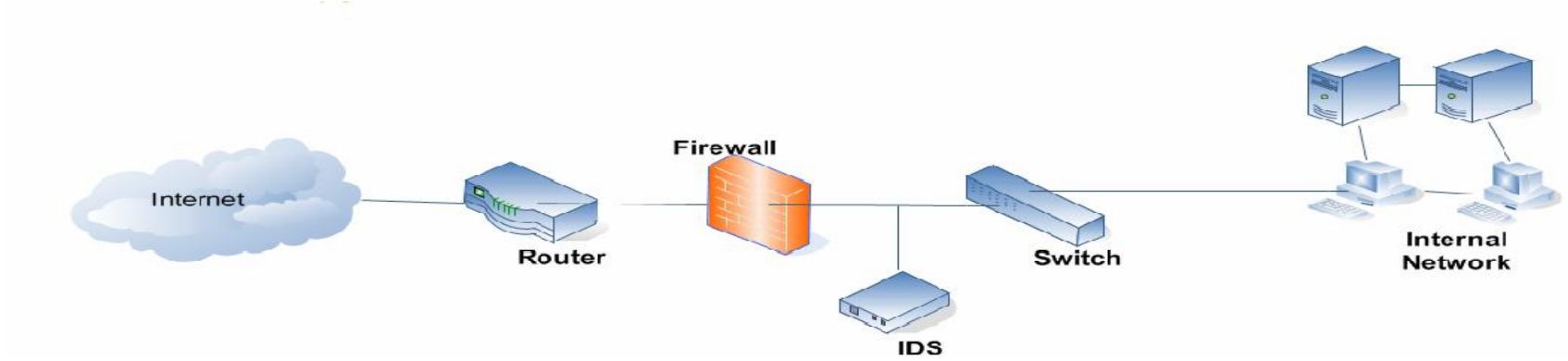
** ازشبکه DMZ میتوان برای تامین امنیت انواع ارتباطاتی که میتواند با شبکه داخلی برقرار شود استفاده نمود.برای مثال برخی از سازمانها دارای افرادی هستندکه با ادوات بی سیم(موبایل و...) می خواهند از منابع داخلی شبکه بمانند ایمیل و اطلاعات شخصی خود استفاده کنند.بکارگیری این نوع ارتباطات ریسک امنیتی شبکه را افزایش میدهد.در چنین وضعیتی میتوان سرورهای access point را در شبکه های DMZ قرار داد و بدین ترتیب از دسترسی مستقیم افراد به شبکه داخلی جلوگیری کرد. از سرورهای VPN نیز در چنین وضعیتی میتوان استفاده نمود.



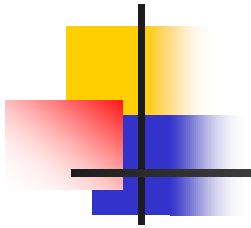
IDS & IPS-IDPs (۱)

سیستم کشف نفوذ یا IDS

نرم افزار یا سخت افزاری است که با تحلیل ترافیک جاری شبکه وتحلیل تقاضاها ، سعی در شناسایی فعالیتهای نفوذگران میکند ودر صورتی که تشخیص دهد ترافیک ورودی به یک شبکه یا سیستم مجاز و عادی نیست وناشی از یک نفوذگرمیباشد، به نحو مناسب مسئول شبکه را در جریان می گذارد.



اهداف IDS



اهداف بالقوه شامل موارد زیرمیتواندباشد:

1- شناسایی حمله ها

2- پیشگیری از حمله ها

3- شناسایی موارد نقض سیاست

4- جمع آوری مدارک

IDS & IPS-IDPs (۲)

تفاوت IDS و Firewall

با اینکه هر دو را میتوان از یک خانواده حساب کردولی تفاوتهایی نیز دارند:

1- دیوارآتش بوسیله یکسری قواعد وقوانین امنیتی که توسط مسئول شبکه تعییین میشوند کار کرده ومورد ورود وخروج بسته ها تصمیم گیری می کنند در صورتی که IDS ها بصورت غیر فعال و نظارتی بر ترافیک جاری شبکه عمل می کنند تا نقش گلوگاهی نداشته باشند.

2- IDS بعداز دیواره آتش ابداع شدند و دارای سیستم هوشمند کشف نفوذ میباشند واین در مواردی که حمله کننده به شبکه از روشی استفاده می کند که مسئول شبکه آنرا در دیوارآتش در نظر نگرفته است ،بسیار مفید میباشد.

انواع IDS

از نقطه نظر محل نظارت ، IDS ها به دوگروه تقسیم میشوند:

1- NIDS(Network IDS)

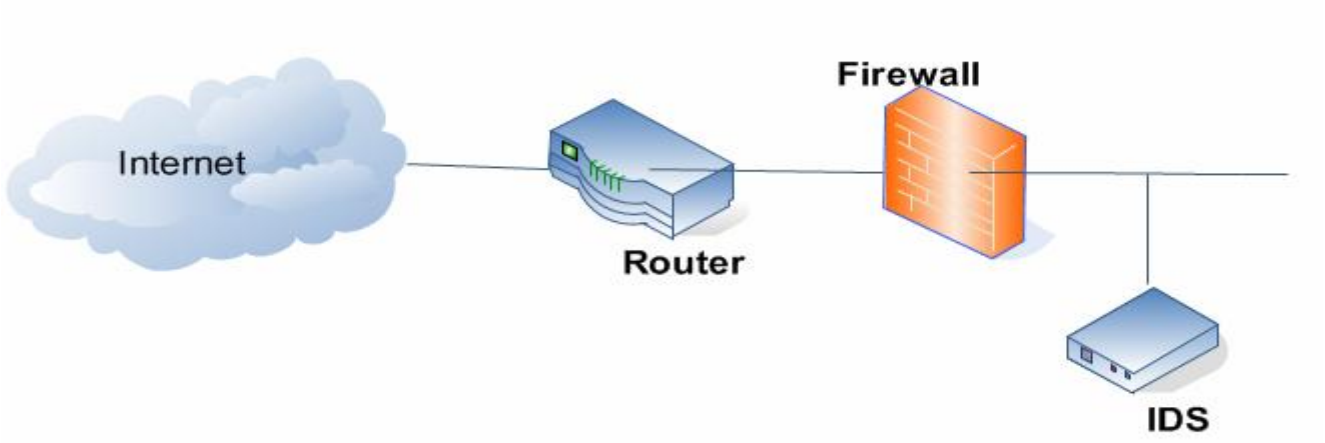
این گروه امنیت کل شبکه را به عهده گرفته ومحل قرارگرفتن آنها نیز درمجاورت مسیریاب مرزی شبکه است(محل ارتباط بین شبکه داخل ودنیای خارج)

2- HIDS(Host IDS)

این گروه بر روی تک تک سیستمهای یک شبکه نصب شده و هرکدام مسئولیت برقراری امنیت همان سیستم را به عهده می گیرند.

محل قرارگیری IDS ها نسبت به Firewall ها(1)

روش اول: در این حالت IDS پشت دیوارآتش قرار می گیرد.

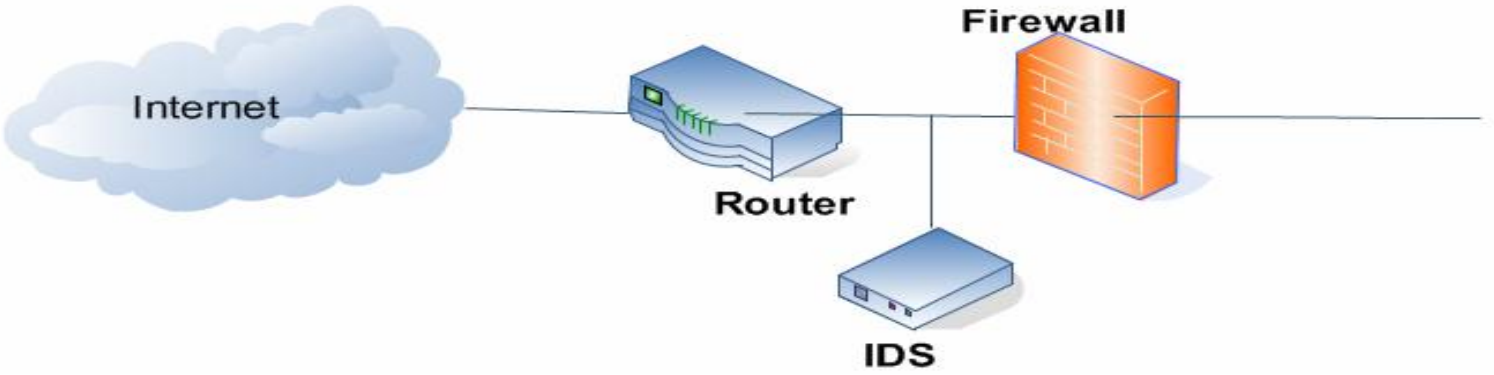


مزیت روش فوق در این است که دیوارآتش از IDS که خود جزیی از شبکه است مراقبت میکند.

ایراد روش فق در اینست که بسیاری از بسته ها ممکن است توسط دیوارآتش حذف شوند که در نتیجه IDS نمیتواند کل ترافیک شبکه را بطورکامل ببیند تا درموردآن تصمیمات هوشمندانه بگیرد

محل قرارگیری IDS ها نسبت به Firewall ها(2)

روش دوم :در این حالت IDS قبل از دیوارآتش قرار می گیرد .



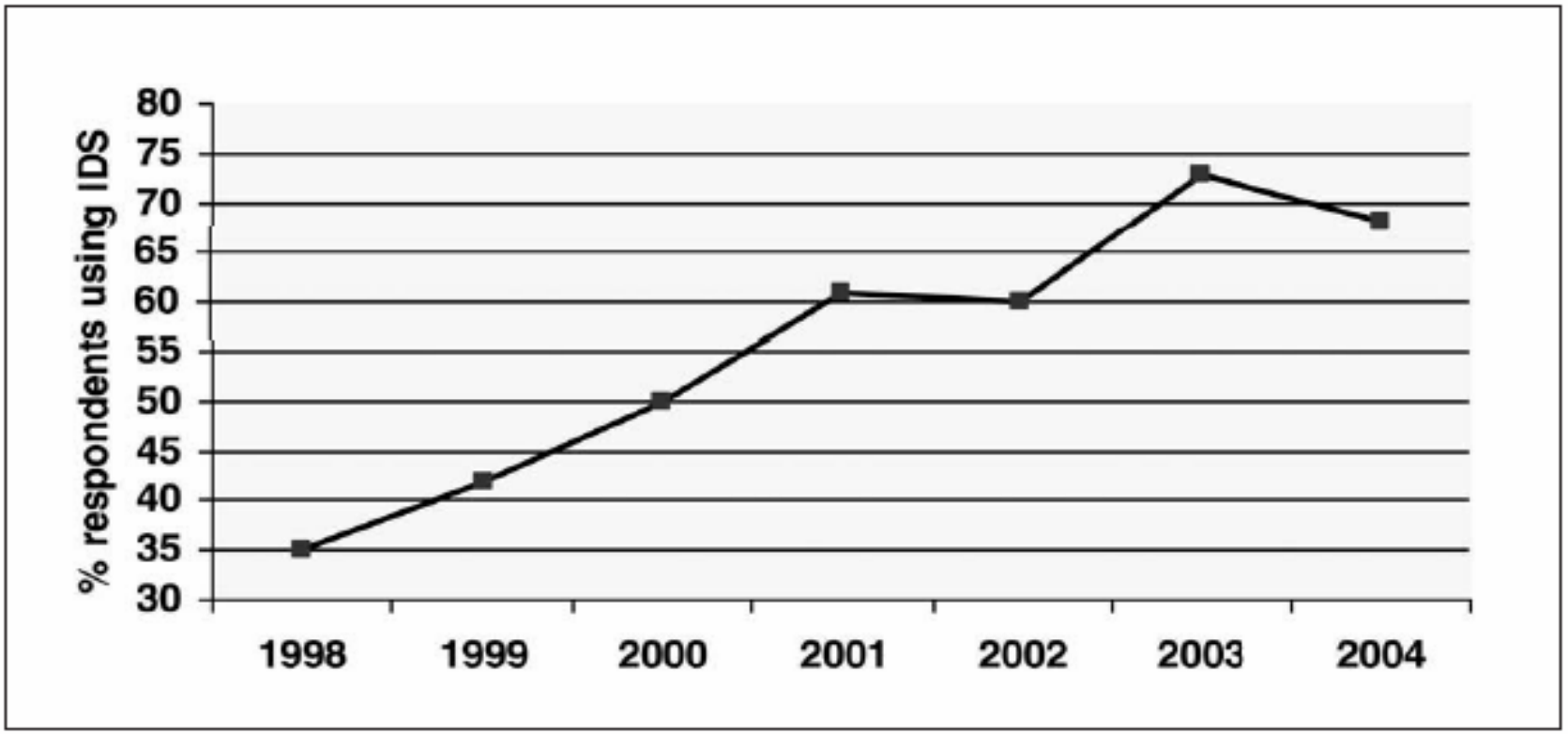
مزیت روش فوق در اینست که با مشکل قبلی ،یعنی حذف بسته ها روبرو نخواهیم بود.

ایراد اساسی در روش فوق اینست که Hacker به راحتی به نگهبان هوشمند دسترسی داشته ومیتوانند پیکربندی آنرا به راحتی تغییر دهند ودر اینصورت در نفوذ به شبکه با مشکلی اساسی مواجه نخواهند بود.

عملکرد IDSها در مواجه با یک ارتباط مشکوک

هنگامی که یک IDS تشخیص دهد ارتباط برقرار شده از طرف کاربر مجاز نیست ویا اینکه بسته ایی مشکوک بنظرمیرسد ،دست به کار میشود.
مثلاً با علائم هشداردهنده مسئول شبکه را مطلع میسازد ویا اینکه مبادرت به قطع کردن یک ارتباط TCP میکند.
نتایج تحلیل یک حمله برای کشف حملات مشابه در آینده و هوشمند نمودن سیستم امنیتی شبکه در IDS ذخیره میشود.
IDS ها نیز گاهاً در تجزیه وتحلیل ترافیک دچار اشتباه شده وپیام های هشدار دهنده صادر میکنند کهً به آن False Alarm می گویند.IDSهایی بهترهستند که میزان False Alarm آنها نزدیک به صفر باشد.

میزان گسترش استفاده از IDSها در سازمانها در ایالات متحده امریکا



Organisations using IDS technology
(source: CSI/FBI surveys)

IPS
(Intrusion Prevention System)

IPS چیست؟

همانطور که از اسم آن مشخص میباشد ،IPSها نه تنها وظیفه شناسایی حملات را بمانند IDSها به عهده دارند بلکه در کنار آن وظیفه جلوگیری از اجرای حملات و یا مسدود کردن ارتباط را به شناسایی انجام میدهند.

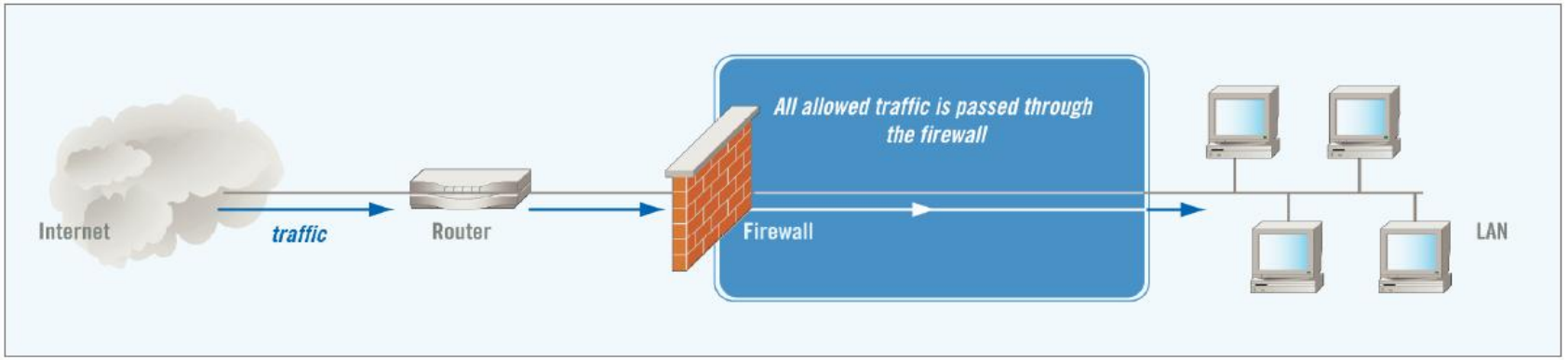
محل استقرار IPS

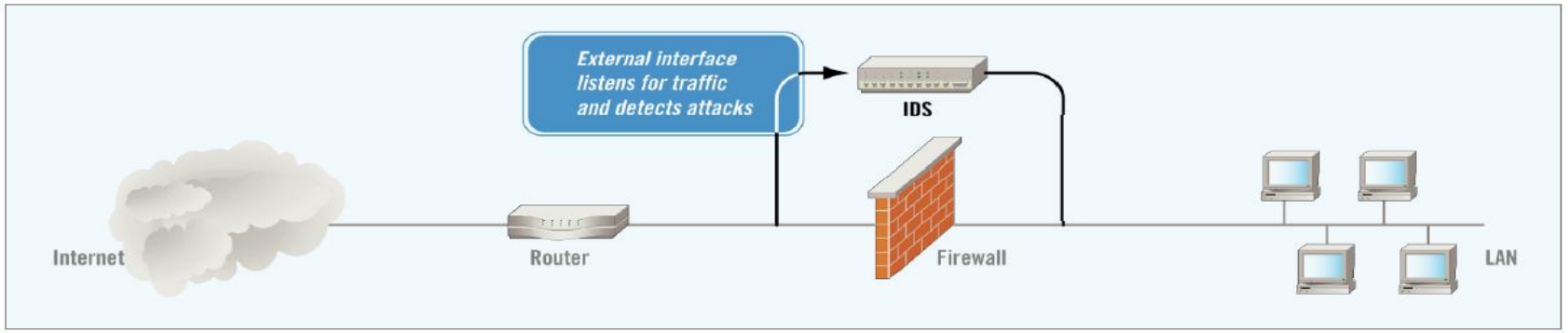
اغلب طراحی های تکنولوژیکی مربوط به IPS ها طوری است که آنها بتوانند در اولین محا ارتباط شبکه داخلی با دنیای بیرون قرار گرفته وجهت محافظت از شبکه درونی به ایفای نقش بپردازند.

(1)

انواع محلهای استقرار IPS

مروری سریع بر محلهای قرار گیری Firewall و IDS



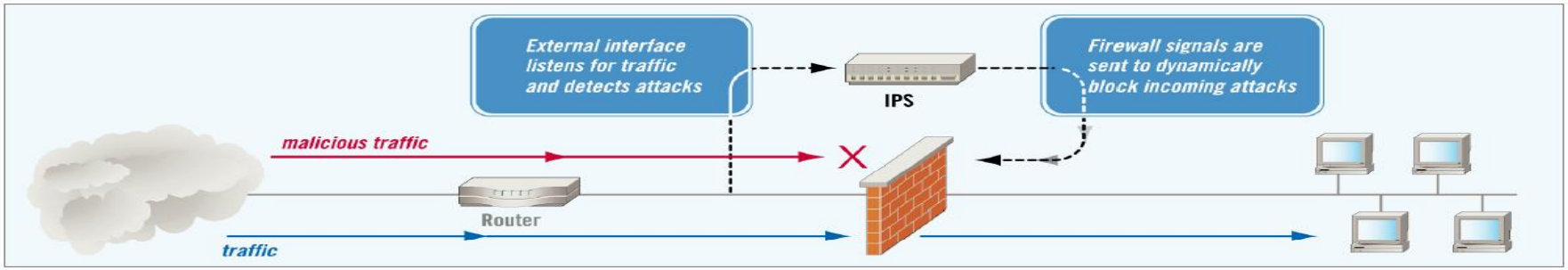


(2)

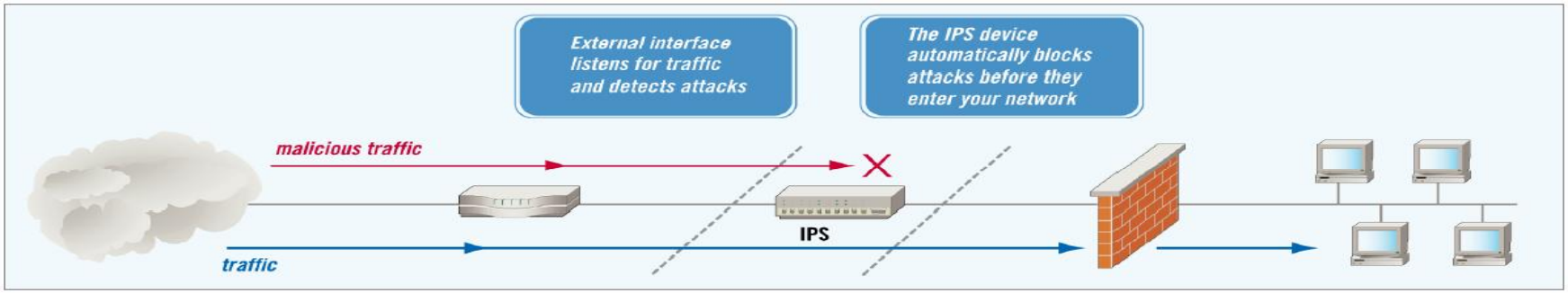
انواع محلهای استقرار IPS

دو حالت کلی به لحاظ محل قرار گیری را میتوان مد نظر داشت:

1) Out – Of –Band (OOB IPS)



2) In-Line IPS



(3)

انواع محلهای استقرار IPS

1) Out – Of –Band (OOB IPS)

همانطور که از شکل نیز مشخص میباشد نحوه قرارگیری این گروه در مدار به مانند IDSهامیباشد.پیشتر توضیح دادیم که IPSها به لحاظ تکنولوژی ساخت دارای سیستم شناسایی وآنالیز حمله و ترافیک ورودی هستند.
براساس استفاده از سیستم IDS درون ساخت یافته ،اینگونه سیستمهای IPS ضمن آنالیز ترافیک ورودی به مدیریت firewall نیز کمک کرده وآنرا در حذف اطلاعات مشکوک و خرابکارانه آموزش ویاری میدهد.

(4)

انواع محلهای استقرار IPS

2) In-Line IPS

این گروه نیز دارای عملکرد مشابه OOB IPS میباشندو تفاوت عمده آنها در اینست که این گروه دارای قدرت عملیاتی خیلی بیشتر وسریع تر نسبت به گروه اول در بلوکه ساختن ارتباطات مشکوک وخرابکارانه است. از این گروه ازIPSها جهت محافظت از شبکه داخلی در مقابل حملاتی که میتواندمنشاء داخلی نیزداشته باشد،استفاده نمود.(عمدتاًدرجاهائیکه با شرکای تجاری ،تأمین کنندگان وافراد داخل سازمان روبرو هستیم وبطور معمول از Firewallها استفاده نمیشود.

مزایا ومعایب IPS

همانطور که قبلاً نیز مطرح گردید از مزایای عمده IPSها میتوان به علکرد سریع و گازانبری آنها در مقابله با انواع حملات اشاره نمود.

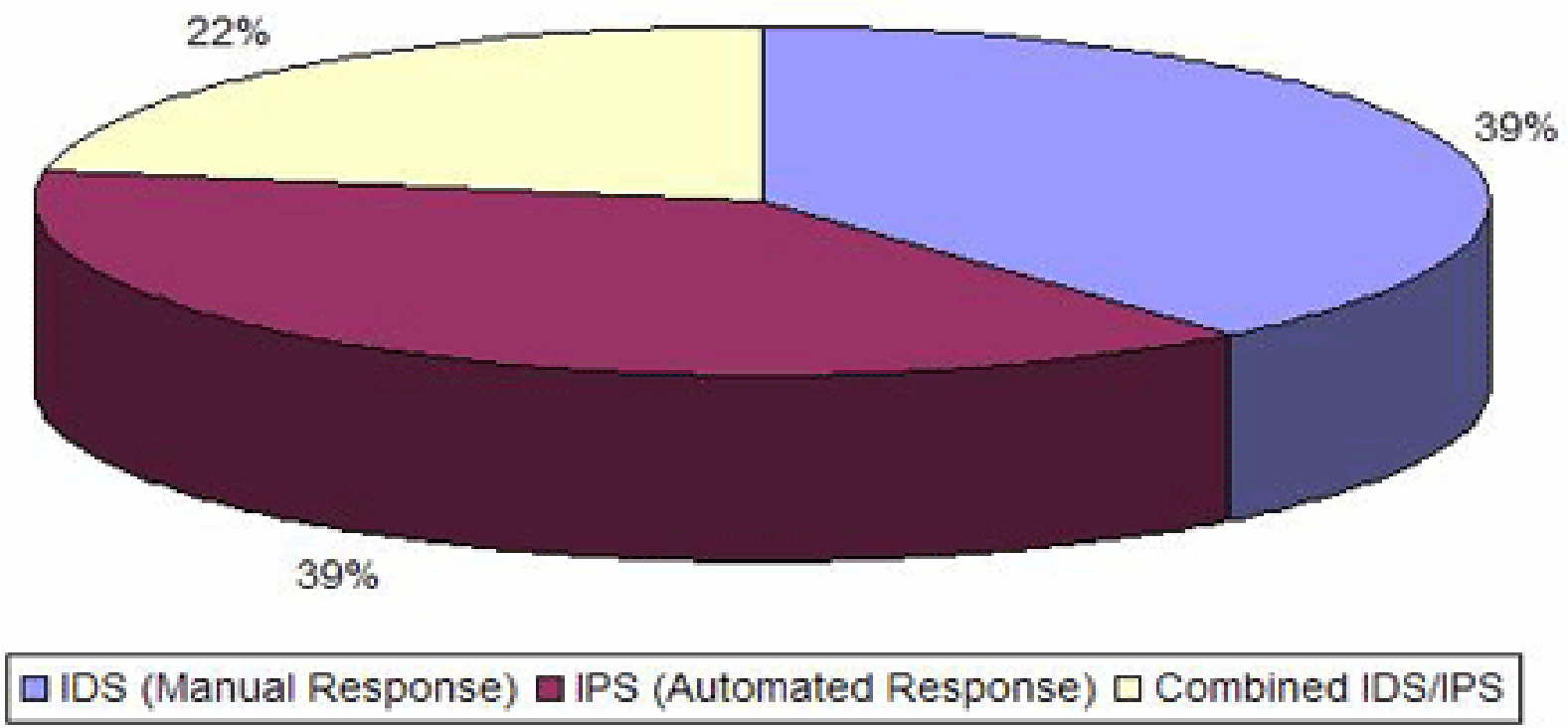
ازمعایب عمده آن میتوان به عواملی چون عدم امکان پاسخگویی به ترافیک شبکه بخصوص در مواقعی که با حجم بالایی از اطلاعات در شبکه مواجه هستیم ،اشاره نمود. یا ازجمله موارد دیگر میتوان به حمله مستقیم به خود IPS اشاره نمود که درچنین وضعیتی منجر به crash شدن IPS شده و شبکه از کار خواهد افتاد.

از جمله راه حلهای مفید برای بر طرف نمودن این مشکل میتوان به مواردی چون استفاده از back-up IPS ویا تغییراتوماتیک مسیرجریان داده توسط Router ویا پیکربندی خود IPS با حداقل تمهیدات به قسمی که بتواند از پس ترافیک شبکه بیاید،اشاره نمود.

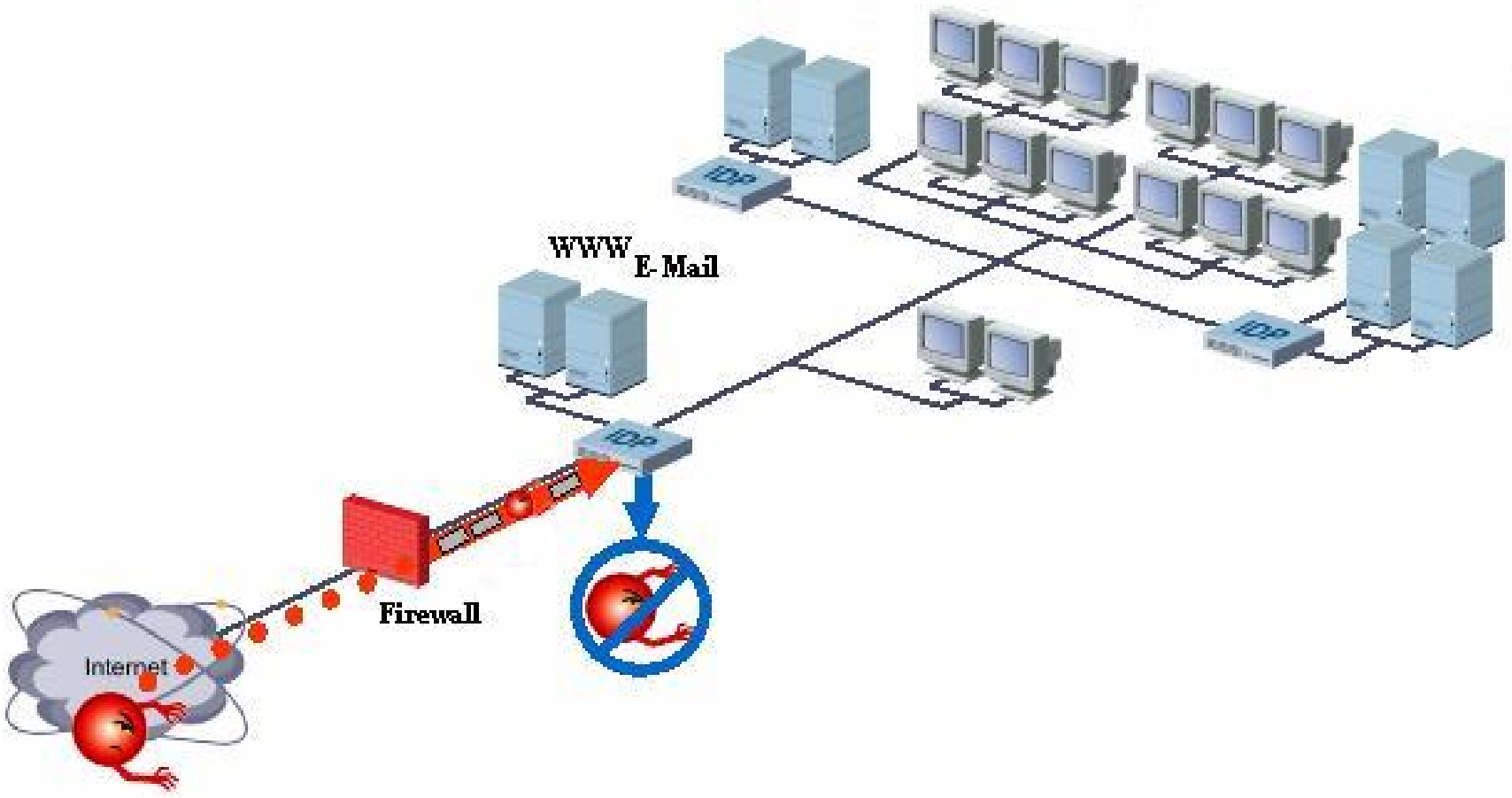
IDS vs IPS (1)

اینکه با قاطعیت اعلام کرد که کدام نوع از سیستمهای هشداردهنده فوق بر دیگری برتری مطلق دارد ، بدرستی امکان پذیرنیست ،ولی با پیشرفت تکنولوژی ،امروزه شاهد نسل جدیدی از سیستمهای هشدار سریع که ترکیبی از سیستمهای IPS وIDS هستند، می باشیم که به IDPs معروفند وخصوصیات اصلی اجداد خود را با قابلیتهای اضافه به همراه دارند.

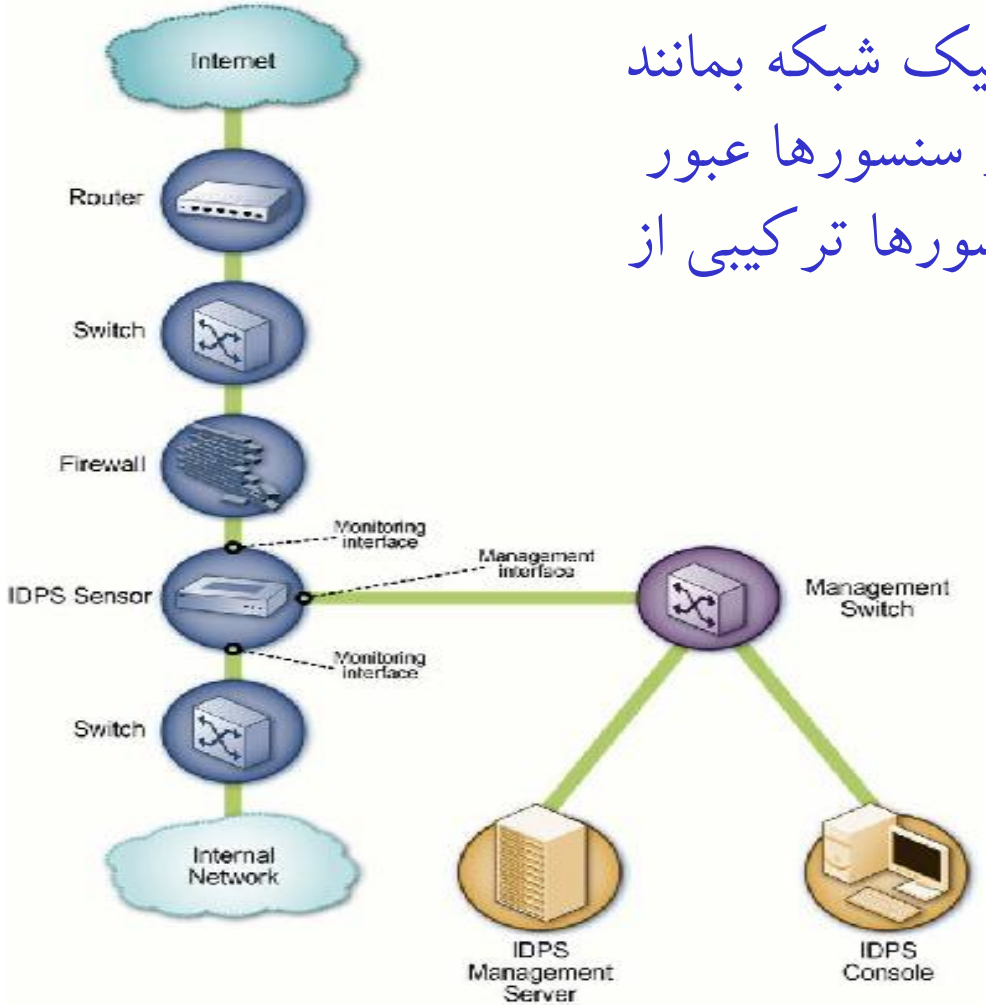
IDS vs IPS (2)


22%
39%
39%
IDS (Manual Response)
IPS (Automated Response)
Combined IDS/IPS

IDPS (IDS & IPS)

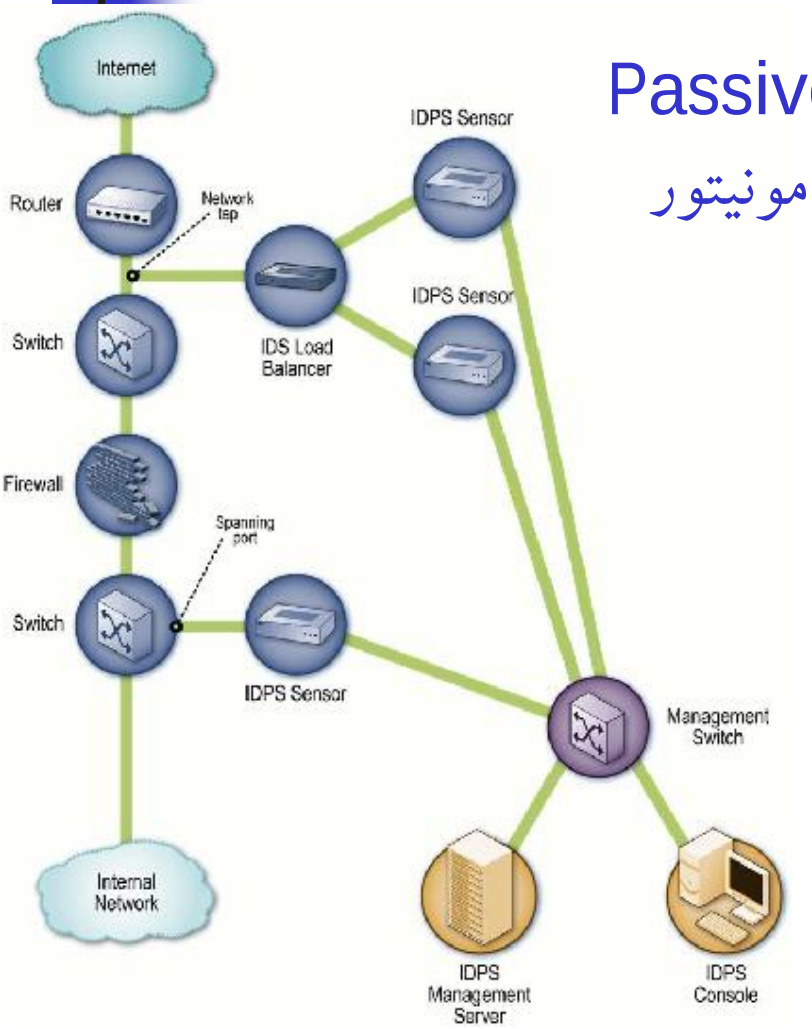


Inline Network-Based IDPS Sensor Architecture Example



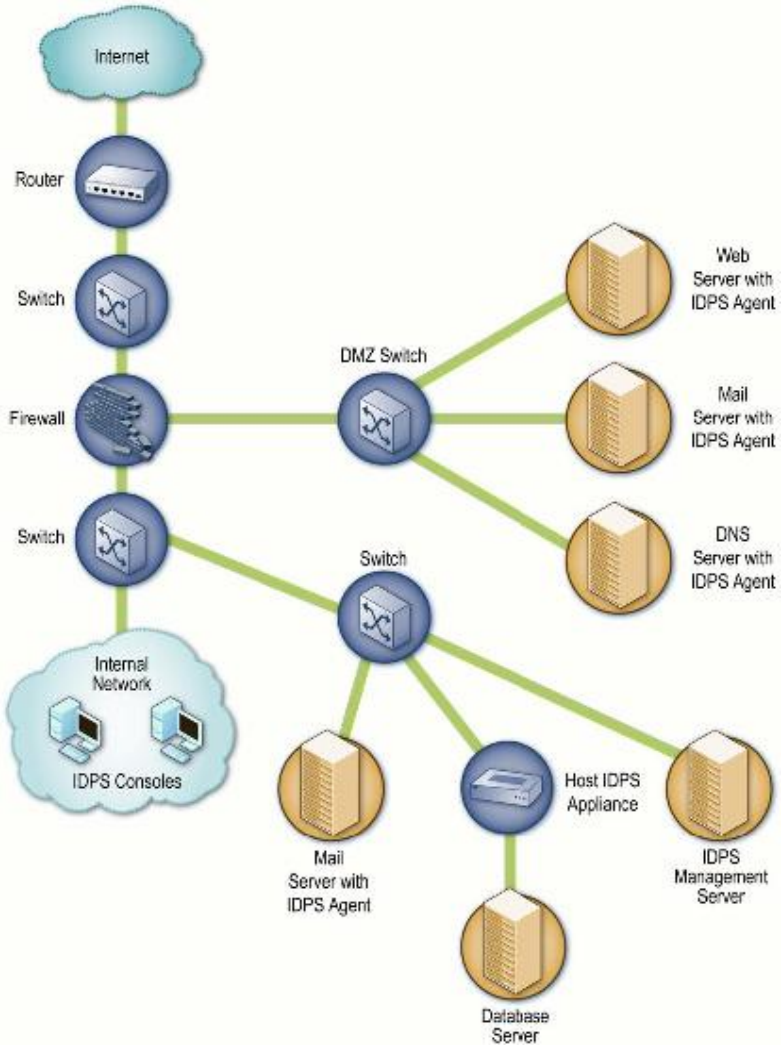
در این نحوه قرارگیری کل ترافیک شبکه بمانند آنچه که در دیوارآتش دیدیم از سنسورها عبور خواهندکرد. در حقیقت این سنسورها ترکیبی از FW/IDPS میباشند.

Passive Network-Based IDPS Sensor Architecture Example



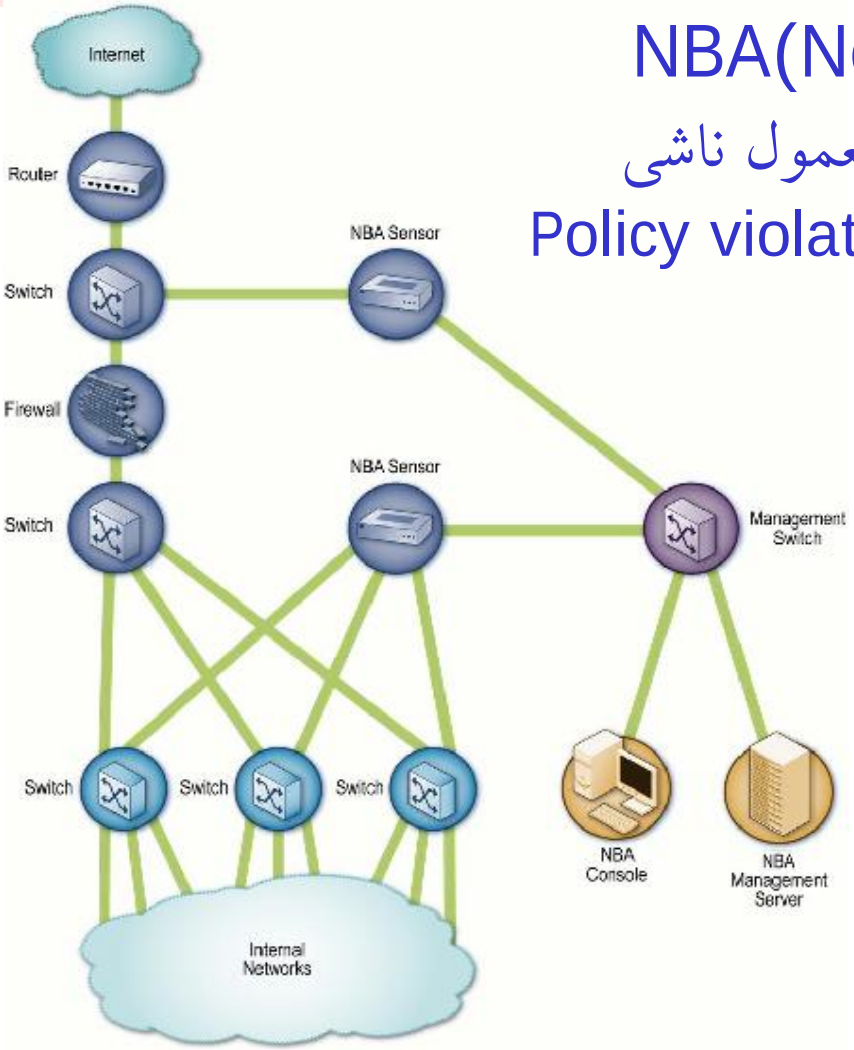
در طرز قرارگیری سنسورها در حالت Passive یک کپی از ترافیک عبوری از شبکه را مونیتور می کنند .

Host-Based IDPS Agent Deployment Architecture Example



در این نوع از معماری که بسیار ساده نیز میباشد ،عوامل کنترل روی Hostهای شبکه یک سازمان قرار می گیرند.در اینحالت عاملها از طریق شبکه به تبادل اطلاعات پرداخته و دارای سیستم مدیریت مجزا از شبکه نمی باشند

NBA Sensor Architecture Example



یک NBA(Network Behavior Analysis)
به بررسی ترافیک یک شبکه یا آمار غیر معمول ناشی
از حملاتی چون DDoS، Worms و Policy violation
می پردازد.

Gateway AV & IPS (1)

Gateway AV مناسب ترین وسیله برای مقابله virus، Trojan ، E-mail worms، IM worms ، phishing attack و Spyware میباشند و IPS مناسب تر برای مقابله با مشکلات مرتبط با شبکه از جمله ویروسهای شبکه ایی، نقاط ضعف شبکه ایی ومحدودسازی ویا قطع ارتباط ترافیک میباشند.

هر دو اطلاعات حاصله از ویروسها را در موتورهای جستجوی خود جهت استفاده در مقابله با حملات مشابه ذخیره می کنند.

Gateway AV & IPS (2)

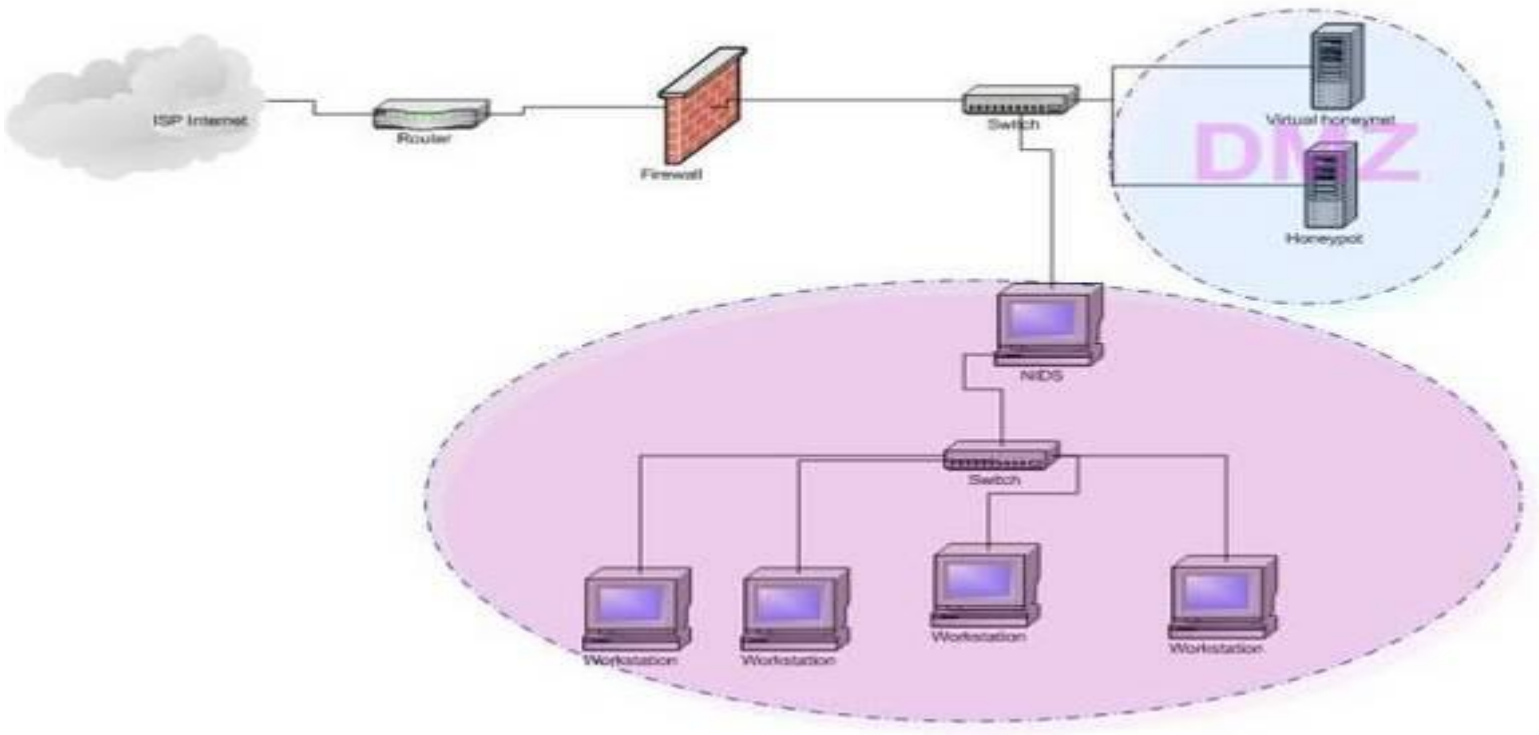
مهمترین تفاوت بین Gateway AV و IPS در نحوه تصدیق اطلاعات پس از بازرسی توسط موتورهای آنها میباشد.
Gateway AV پس از بازسازی کامل فایل به آن اضافه می کنند درصورتیکه تصدیق حاصل از بازرسی بتوسط IPS ها به جریانی از اطلاعات عبوری الصاق میشود. (IPSها به سایز فایلها حساس نیستندبنابراین خیلی سریعتر عمل می کنند.Gateway AV بعداز بازسازی کامل فایل عمل تصدیق اعتبار را انجام میدهند بنابر این از توان عملیاتی کمتری برخوردارند ولی در جاهائیکه سالم بودن کامل اطلاعات حائز اهمیت است، از الویت برخوردارند.

(1)
Honeypot & Honeynet

یک Honeypot یک سیستم کامپیوتری در یک شبکه است که به شبیه سازی یک یا چند سرویس قابل ارائه توسط سازمانها ،پرداخته و هدف اصلی آن به دام انداختن ، یادگیری الگوی حمله ومسیریابی حملات که بتوسط هکرهای فعال و خبره اجرا میشوند، میباشد.
Honeypot ها بطور فیزیکی در شبکه ای مستقل از شبکه اصلی قرار می گیرند.از جمله مهمترین محلهای قرارگیری آنها منطقهDMZ است.

(2)
Honeypot & Honeynet

Honeynet مجموعه ای از تعدادی Honeypotها میباشد که یک شبکه را تشکیل میدهند



Virtual Honeynet (1)

یک Virtual Honeynet عبارت است از یک سیستم که خصوصیات یک سیستم عامل را که میتوانند تمام سرویسهای متفاوتی را که قابل ارائه بتوسط کامپیوترهای مختلفی میباشد، عرضه کنند شبیه سازی میکند بطوریکه این کامپیوتر یک شبکه کامل به نظر می رسد.

مزایا :

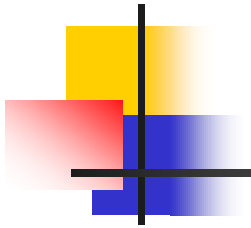
- مدیریت آسان
- درصورت آگاهی،کمتر مهاجمی به سیستم فوق حمله می کند.
- هزینه کمتر به دلیل استفاده از فقط یک کامپیوتر
- ایجاد سردرگمی در مهاجم

Virtual Honeynet (2)

معایب:

- محدویت سیستمهای عامل که بتوانند هماهنگی لازم را با نرم افزارایجاد وایفای نقش مجازی بطور کامل بازی کنند.
- محدودیت نرم افزاری موردنیاز (اغلب سیستمهای مجازی فقط سازگاری با محصولات سری X86 را دارند.)
- مشکل تمرکزگرایی، به قسمی که اگر Hacker بفهمد که با یک سیستم مجازی تله شده روبروبوده ،براحتی قادر به مختل کردن کل Virtual Honeynet خواهد بود.

Sniffer(1)



محصولاتی هستند که در ابتدا جهت کنترل تبادلات داده ای در یک شبکه بکار گرفته شدند.این محصولات میتوانند بصورت سخت افزاری ویا نرم افزاری باشند.از snifferها هم برای مدیریت قانونمندانه شبکه ها وهم برای سرقت اطلاعات میتوان استفاده نمود.

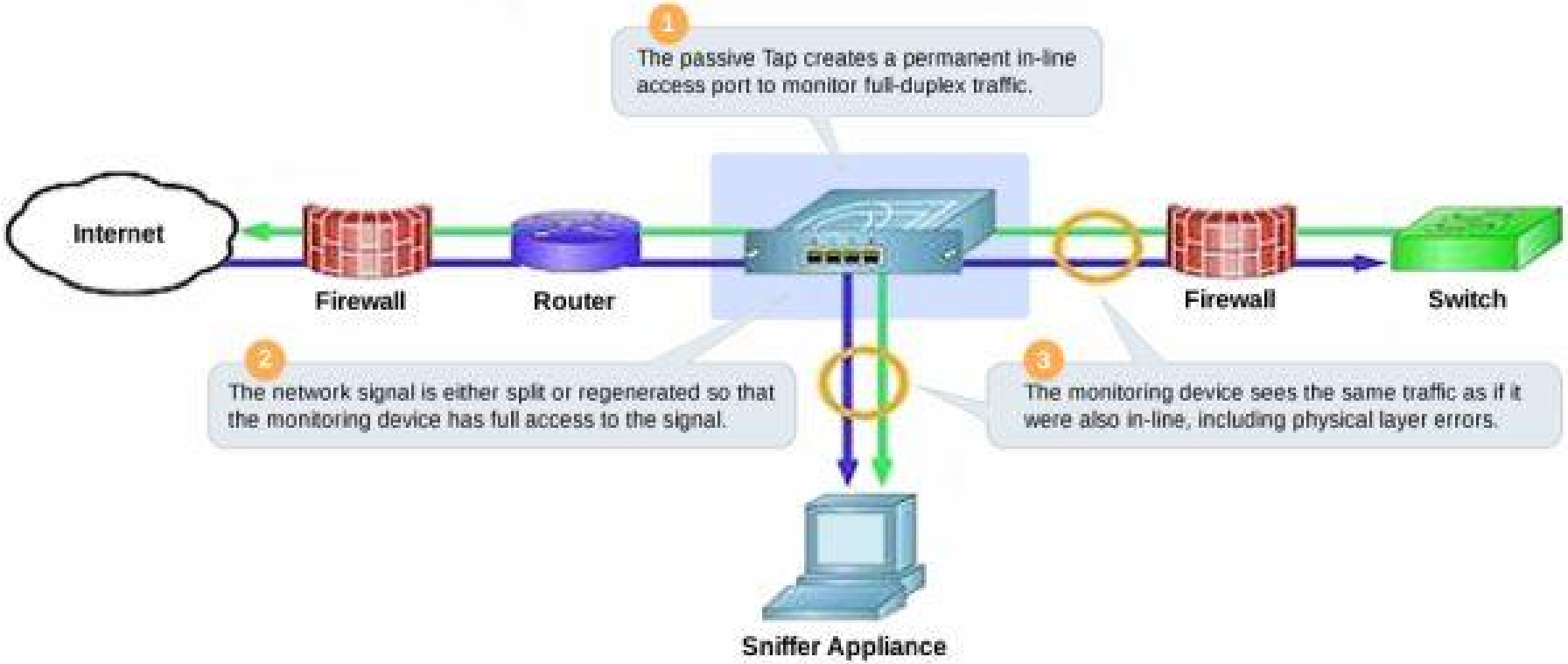
از جمله کاربردهای قانونمندانه آن میتوان به کنترل ترافیک شبکه ،آنالیزpacketها وعیب یابی شبکه ها اشاره نمود.

Sniffer(2)

HOW IT WORKS

Network Tap Technology

Network Taps use passive splitting or regeneration technology to transmit in-line traffic to an attached management or security device without datastream interference.



References

1- J.Stuart Broderick ,firewalls-Are they enough protection for Current networks,Information Security Technical Report, (2005) 10,204-212.

2- Karen Scarfone ,Peter Mell,Guide to Intrusion Detection and Prevention Systems (IDPS),National Institute of Standards and technology, February 2007,Special Publication 800-94.

3-Ian Poyenter,Beyond The Firewall:The Next Level of Network Security,Latis Networks,Inc.,January 2003.

4-Maria Papdaki and Steven Furnell , IDS or IPS: what is best?, Network Security(2004) 7,15-19.

5-Pete Lindstorm ,Intrusion Prevention Systems(IPS):Next Generation Firewalls,A Spire Research Report(2004)


با تشکرازهمراهی شما