مرکز تخصصی
آپا
دانشگاه صنعتی اصفهان
(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

معرفی نرم‌افزار Snort

قسمت دوم : راه‌اندازی و ملاحظات امنیتی

شهریور ۱۳۹۲

www.nsec.ir

۲-۱ سیستم مورد نیاز برای نصب Snort

قبل از هر چیز ذکر این نکته ضروری است که Snort جهت ذخیره Log فایل ها به فضای دیسک زیادی نیاز دارد. پس همواره یک فضای دیسک مناسبی را جهت ذخیره Log فایل ها در نظر بگیرد.

Snort جهت نصب نیاز به سخت افزار خاصی ندارد اما موارد زیر پیشنهاد می شود:

- یک کارت شبکه مجزا برای اتصال به نرم افزار Snort از راه دور و ایجاد تغییرات.
- حدود ۹ گیگابایت فضای هاردیسک برای پارتیشن /var
- انتخاب کارت شبکه مناسب با توجه به سرعت خط شبکه. اگر سرعت شبکه ۱۰۰ مگا بیت می باشد کارت شبکه شما نیز باید حداقل این سرع را پشتیبانی کند در غیر این صورت برخی از پکت ها را از دست خواهد داد.
- سیستم عامل پیشنهادی در درجه اول BSD ها و نهایتاً Linux با کرنل بالاتر از 2.4 می باشد.

بعد از نصب سیستم عامل از وجود برنامه های زیر روی سیستم عامل اطمینان کسب کنید:

- autoconf and automake
- gcc
- lex and yacc
- آخرین نسخه libcap از tcpdump.org

موارد فوق برای زمانی مورد نیاز است که می‌خواهد Snort را از منبع آن کامپایل کنید در غیر این صورت نیاز به وجود آنها نیست.

۲-۲ نصب و راه اندازی Snort

در این بخش نحوه نصب و راه اندازی Snort بر روی سیستم عامل ویندوز برای معماری raditional Network-based را قدم به قدم نمایش خواهیم داد.

می‌توان از یک ابزار کمکی بسیار مفید به نام IDScenter استفاده نماییم که مدیریت و کنترل گرافیکی و بیشتری برای Snort مهیا می‌نماید.

آخرین نسخه از Snort برای ویندوز را می‌توانید از این آدرس زیر دریافت نمایید .

http://www.Snort.org/dl/binaries/win32

آخرین نسخه از IDScenter را نیز می‌توانید از این آدرس زیر دریافت نمایید.

http://www.engagesecurity.com/downloads/#idscenter

همچنین Snort برای کار کردن ، احتیاج به WinPcap دارد . آخرین نسخه این نرم افزار را می‌توانید از آدرس زیر دریافت نمایید

http://www.winpcap.org/install/default.htm

بعد از دانلود کردن برنامه مراحل زیر را می‌بایست برای نصب Snort انجام داد:

- برنامه اجرایی دانلود شده را اجرا نمایید.
- بر روی دکمه I Agree کلیک نمایید
- چنانچه قصد ندارید از MS Sql Server یا Oracle برای ذخیره log ها استفاده نمایید ، گزینه اول یا همان I do not plan ... را انتخاب نمایید.
- گزینه Next را کلیک نمایید.
- تمام Feature ها را انتخاب نموده و بر روی دکمه Next کلیک نمایید.
- مسیر نصب را انتخاب نموده و بر روی دکمه Next کلیک نمایید.
- نصب شروع شده و بعد از پایان مراحل نصب ، دکمه Close را کلیک نمایید.
- نرم افزار WinPcap را نصب نمایید.

۲-۲-۱ راه‌اندازی و تنظیم Snort

گزینه‌های زیادی برای اجرای Snort وجود دارد. همانطورکه در بخش‌های قبل اشاره شد Snort در سه حالت می‌تواند اجرا شود که در بین بخش طریق راه‌اندازی و اجرای هر کدام از گزینه‌ها بیان می‌گردد:

- حالت sniff کننده[1]: در این حالت Snort تنها بسته‌ها را از شبکه می‌خواند و آن‌ها را روی صفحه نمایش, نشان می‌دهد. ساده‌ترین گزینه اجرا در این حالت حالتی است که تنها سرآیند بسته های TCP/IP را روی صفحه نمایش نشان می‌دهد. تنها سرآیندهای TCP، ICMP,UDP و IP نمایش داده می‌شود:

```
./Snort –v
```

با استفاده از گزینه d– می‌توان محتوای بسته را هم مشاهده کرد:

```
./Snort –vd
```

اگر بخواهیم سرآیند لایه دو یا Datalink هم مشاهده شود از گزینه e– استفاده می‌کنیم:

```
./Snort -vde
```

- حالت ثبت‌کننده بسته‌ها: بسته‌ها را در فایل‌هایی روی دیسک ذخیره می‌کند. در این حالت باید یک شاخه را برای ثبت بسته‌ها درنظر گرفت.

```
./Snort –dev –l ./log
```

برای اجرای دستور فوق, ابتدا باید شاخه log را ایجاد کرد. بسته‌ها بر اساس آدرس IP در شاخه‌هایی در شاخه تعیین‌شده به صورت سلسله مراتبی ثبت می‌شوند. با دستور بالا بسته‌ها گاهی براساس آدرس ماشین دور۲ و گاهی با آدرس محلی۳ در شاخه‌ها ثبت می‌شود. اگر مانند زیر آدرس محلی را در دستور مشخص کنیم, بسته‌ها در شاخه اصلی log در زیرشاخه‌هایی که نامشان بر اساس آدرس remote (آدرسی غیر از 192.168.1) ثبت می‌شوند.

```
./Snort –dev –l ./log –h 192.168.1.0/24
```

در صورتیکه بخواهیم سرعت ثبت بالاتر باشد و بررسی بسته‌های ثبت‌شده را به آینده موکول کنیم ثبت را در حالت باینری انجام می‌دهیم:

```
./Snort –l ./log –b
```

در این حالت تمام بسته‌ها در یک فایل به فرمت tcpdump در شاخه ثبت ذخیره می‌شوند. این فایل را با هر نرم‌افزار sniffer که فرمت tcpdump را پشتیبانی کند قابل خواندن است, مانند tcpdump یا Ethereal . با Snort هم با استفاده از گزینه r– می‌توان این فایل را خواند:

---

[1] sniffer
[2] remote
[3] local

./Snort –dv –r packet.log

دستور زیر تنها بسته‌های ICMP را از فایل tcpdump می‌خواند:

./Snort –dvr packet.log icmp

– حالت سیستم تشخیص نفوذ شبکه: این حالت پیچیده‌ترین و کامل‌ترین حالت است که ترافیک شبکه را آنالیز می‌کند و با قوانین تعریف‌شده تطبیق می‌دهد و سپس بر اساس قانونی که با بسته‌ها مطابق می‌شود عملی را اجرا می‌کند. اگر نام فایل قوانین Snort.conf باشد دستور زیر Snort را در حالت NIDS اجرا می‌کند:

./Snort –dev –l ./log –h 192.168.1.0/24 –c Snort.conf

با اجرای این دستور بسته‌هایی که توسط قوانین trigger می‌شوند در فایل ثبت می‌شوند. البته در این حالت بهتر است برای بالابردن سرعت گزینه‌های –v و e– را حذف کنیم, زیرا اصلاً در حالت NIDS به این گزینه‌ها نیازی هم نیست.

در حالت NIDS می‌توان هشدارها را همان‌طور که در بخش قبل ذکر شد به طرق متفاوت ثبت کرد که معمولترین آن ثبت در پایگاه داده است. در بخش نصب کامل سیستم تشخیص نفوذ به طور مفصل استفاده از پایگاه داده برای ثبت هشدارها و اطلاعات مفید, بحث خواهد شد.

شکل استاندارد هشداری که توسط Snort تولید می‌شود مانند زیر است:

[**] [116:56:1] (Snort_decoder): T/TCP Detected [**]

عدد اول شناسه تولیدکننده هشدار است که به آن GID۴ گوییم. این عدد بیان‌گر جزئی۵ از Snort است که هشدار را تولید کرده. لیست تمام GIDها در شاخه etc/generators از سورس Snort قرار دارد. به‌طور مثال در هشدار بالا کد 116 مربوط به جزء واگشای۶ Snort است. عدد دوم شناسه خود Snort است که به آن SIDv گوییم. لیستی از SIDها در etc/gen-msg.map/ قرار دارد. SID به طور صریح به صورت گزینه‌ای در قانون ذکر می‌شود. در هشدار ذکرشده در بالا کد 56 مربوط به یک رویداد T/TCP است. عدد سوم مربوط به تعداد بازبینی‌ها و تغییر قانون مربوطه است. ۸ بدین معنا که در نوشتن قوانین هر بار در قانون تغییری اعمال می‌شود این عدد یکی افزوده می‌شود. در ادامه هم همان‌طور که ملاحظه می‌شود پیغام متناسب با هشدار آمده است. در حالتی که از ثبت هشدارها در پایگاه داده استفاده کنیم هر یک از این فیلدها به طور جداگانه در جداول ثبت خواهد شد.

– حالت inline : در این حالت Snort بسته ها را به جای libpcap از iptables دریافت می‌کند, سپس بر اساس قوانینی که برای آن تعریف شده از iptables می‌خواهد که بسته‌ها را عبور۹ دهد یا دور اندازد۱۰.

[4] Generator ID
[5] Component
[6] decoder
[7] referred to as Signature ID)[7] Snort ID (sometimes
[8] revision ID
[9] pass
[10] drop

۲-۳ تأمین امنیت Snort

مانند هر سیستم دیگری که روی شبکه نصب می‌کنید تأمین امنیت خود سیستم Snort نیز بسیار با اهمیت است. آیا Snort هم قابل هک‌شدن است؟چه حمله‌های شناخته‌شده‌ای در حال حاضر برای Snort وجود دارد؟اگر حمله‌کننده‌ای طرحی برای compromiseکردن سیستم Snort بریزد چه حمله‌هایی ما را تهدید خواهد کرد؟

این‌ها سؤالاتی است که برای هر سیستمی مطرح است ولی برای یک سیستم امنیتی اهمیتی دوچندان دارد. یک طرح قوی و مورد اطمینان, امنیت هر سیستم را جداگانه درنظر می‌گیرد که این شامل Snort هم می‌شود و تضمین می‌کند که هیچ single point of failer وجود ندارد.

Snort سیستم مستعدی برای پذیرش حمله ها است. حمله کننده ها دو روش را در برخورد با Snort می‌توانند دنبال کنند. می‌توانند خود سیستم Snort را مورد حمله قرار دهند و یا به سرویس‌ها و سیستم عامل ماشینی که به عنوان یک سنسور Snort استفاده می‌شود حمله کنند.

۲-۴ تشخیص سیستم Snort روی شبکه

بهتر است که سیستم Snort را با حداقل دو کارت شبکه تنظیم کرد. یکی برای آرام‌گوش‌دادن[11] به ترافیک شبکه, و دیگری برای مدیریت سنسور و ارسال هشدارها. معمولا دو کارت شبکه به دو شبکه کاملا مجزا متصل می‌شوند. این یک فرض کاملا عاقلانه و معمول است که کارت شبکه گوش‌دهنده یک رابط مخفی[12] باشد تا توسط حمله‌کننده‌های روی شبکه محلی تشخیص داده نشود.

رابط‌های مخفی بدون آدرس IP تنظیم می‌شوند, ولی این بدان معنی نیست که آن‌ها به ترافیک شبکه جواب نمی‌دهند. بسته‌های خاص ARP پیشرفته می‌توانند برای تشخیص یک کارت شبکه در حالت promiscuous به کار روند. برنامه‌هایی هستند که با روش‌های مشابهی یک واسط promiscuous را تشخیص می‌دهند مانند Antisniff یا Neped .

از مشکلات معمولی که وجود دارد هنگامی است که از active response یا IPS استفاده می‌شود, در این حالت IDS وجود خود را به حمله‌کننده اعلام می‌کند.

اگر حمله کننده ها ترافیک هشدارهای IDS را مشاهده کنند نیز سیستم Snort را می‌توانند کشف کنند. مشاهده ترافیک هشدارها توسط حمله کننده ها زیان های قابل توجهی خواهد داشت. اگر ترافیک هشدارها بدون رمزنگاری ارسال شود و یا حتی در غیر این صورت هم اگر حمله‌کننده خیلی ماهر باشد, هر دو این حالات برای ما زیان‌آور است. هر اطلاعات امنیتی حساس که می‌خواهیم ارسال کنیم باید حفاظت شود. باید از رمزنگاری استفاده کرد, یا شبکه فیزیکی جدا بدین منظور در نظر گرفت و یا چند نوع تاکتیک به کار برد تا از عدم رؤیت ترافیک توسط حمله کننده ها مطمئن شویم.

اگر حمله کننده ها ترافیک هشدارها را مشاهده کنند به راحتی می‌توانند بفهمند IDS چه نوع مجموعه قانونی استفاده می‌کند. سپس با طرح‌ریزی از triggerشدن بسته‌هایشان توسط IDS جلوگیری کنند. اطلاعاتی راجع به سیستم IDS برای حمله کننده بسیار با اهمیت است, می‌توانند اطلاعاتی راجع

[11] Silent Listening
[12] Stealth interface

به نوع مقابله سیستم با حمله‌ها به دست آورند و نیز نقطه آسیب پذیری سیستم را کشف کنند. به طور کلی متوجه می‌شوند که IDS مربوطه چه چیز را می‌بیند و چه را نمی‌بیند. اکنون راههای مقابله چیست؟

اول این که باید مطمئن شد که سنسور IDS به پویش[13]های حمله کننده ها برای کشف واسط های شبکه در حالت promiscuous پاسخ نمی دهند. یک راه در این زمینه, راه حل سخت‌افزاری است. برای sniff از یک کابل اترنت با سیم دریافت و بدون سیم ارسال استفاده می‌کنیم. در این صورت هیچ سیگنال الکتریکی از طریق سیم ارسال نمی‌شود و در نتیجه کارت شبکه قادر به لودادن خود با ارسال یک جواب ناخواسته نخواهد بود.

دوم این که برای جلوگیری از sniffشدن ترافیک هشدارها, از روش های مدیریتی مطمئن در سیستم خود استفاده کنیم. برای مدیریت راه دور سنسورهای Snort, SSH توصیه می‌شود. این پروتکلی است که نوع Deviceی که استفاده می شود را لو نمی‌دهد و رمزشده است, بنابر این ترافیک هشدارها به راحتی قابل مشاهده دیگرانی که شبکه را sniff می کنند نیست.

۲-۵ حمله‌های تهدیدکننده Snort

دو نوع حمله به Snort وجود دارد:

حمله‌هایی که برای غیرکاراکردن Snort به عنوان یک سیستم تشخیص نفوذ طراحی شده است, برنامه هایی مانند stick و snot برای غلبه بر Snort از تحریک کردن Snort به منظور تولید هشدارهای فراوان و ناکارآمد استفاده می کنند در این حالت سیستم از یک حمله واقعی که در انبوه ترافیک سرگرم‌کننده گنجانده شده است غافل می شود. حمله های DOS در برابر Snort مانند حمله های ICMP header size از این قبیل حمله ها هستند.

نوع دیگری از حمله ها از Snort به عنوان یک سرویس شبکه قابل اکسپلویت[14] استفاده می کنند. این حمله ها با هدف اجرای یک کد دلخواه حمله کننده یا به دست‌آوردن دسترسی روی ماشینی که Snort نصب است طراحی و اجرا می شوند

حمله‌ای که به نسخه های قبلی Snort رایج بود در آسیب‌پذیری سر ریزبافر موجود در پیش‌پردازنده RPC قرار داشت. حمله کننده از این طریق می توانست سنسور Snort را crash کند و یا کد اکسپلویت خود را روی سیستم اجرا کند. در این مورد حمله کننده نیاز به آدرس IP سنسور هم نداشت تنها کافی بود بسته‌های اکسپلویت خود را به شبکه‌ای که از طریق Snort محافظت می‌شود ارسال کند.

در این زمینه گروه های توسعه دهنده Snort و ابزارها در به روز کردن تولیدات همیشه سعی در رفع آسیب‌پذیری‌های سیستم ها و نرم افزارها دارند. بنابراین باید ازطریق گروه های امنیتی در جریان مشکلات و آسیب‌پذیری ها باشیم و سیستم خود را همواره با راه حل‌ها و patchهای جدیدی که ارائه می‌شود رفع نقص نماییم. ISS یکی از این گرو های امنیتی است که در آن مشکلات نرم‌افزارها بیان شده و راه‌های مقابله و حل آسیب‌پذیری‌ها ارائه می‌شود. گاهی یک آسیب‌پذیری خاص در یکی از پیش‌پردازنده ها کشف می‌شود در این صورت تا قبل از یافتن راه حل رفع آن باید آن پیش‌پردازنده را در سیستم غیرفعال کرد.

در این زمینه همچنین می توانیم توسط ابزارهایی مانند StackGuard (که هنگام کامپایل یک برنامه, اقداماتی جهت محفوظ ماندن برنامه مقابل سرریزبافر انجام می دهد) یا SubDomain امنیت سیستم را بالا بریم.

[13] probe
[14] exploit

حمله دیگر ممکن است مواجه سیستمی شود که Snort بر آن نصب است, از آسیب‌پذیری‌های موجود در سیستم‌عاملی که Snort بر آن نصب است و یا نرم افزارهای دیگری که همراه Snort نصب شده است استفاده کند. بنابر این باید امنیت تمامی اجزای سیستم را به خوبی تأمین کرد.

توصیه دیگری که می‌شود این که کامپایلرها را از روی ماشینی که Snort روی آن نصب است, بردارید تا حمله‌کننده‌ها نتوانند اکسپلویت‌ها را به راحتی کامپایل کنند.

۲-۶ معماری Snort در شبکه

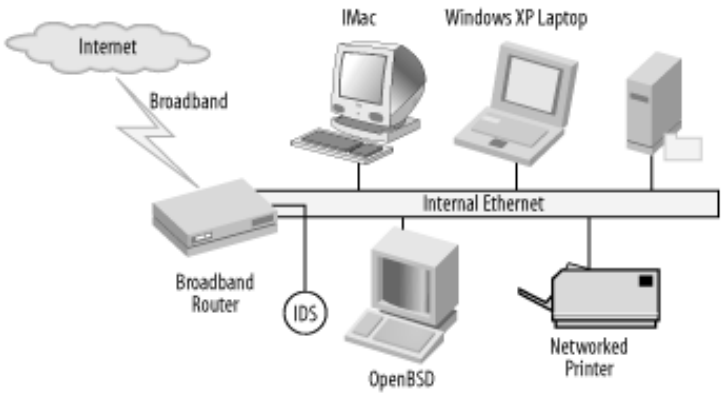
بهتر است تعدادی سنسور در محل‌های مختلف قرار دادتا هر یک محدوده‌ای از شبکه را تحت نظر داشته باشد. بعضی مناطقی که برای مانیتورکردن باید در نظر داشت, شامل موارد زیر است:

- هر نقطه ای که از خارج به شبکه دسترسی دارد. (برای مثال اینترنت, شبکه بی‌سیم یا VPN)
- دو طرف هر ابزار فیلترکننده.
- ناحیه DMZ[۱۵].
- محل اتصال شبکه‌های داخلی بین زیرشبکه‌ها.
- کل شبکه داخلی برای بررسی مشکلات داخلی.

یک مسئله این است که IDS را قبل یا بعد از فایروال قرار دهیم. اگر IDS بیرون از فایروال قرار گیرد تمام حمله‌هایی که از خارج متوجه شبکه است تشخیص داده می‌شود. بدون توجه به این که حمله‌ها توسط فایروال متوقف خواهند شد یا نه. درواقع یک IDS که خارج از فایروال است با رویدادهای بیشتری مواجه است. اگر بخواهیم تنها ترافیکی که از فایروال عبور می‌کند را مورد بررسی قرار دهیم IDS را بعد از فایروال قرار می‌دهیم. بهتر است یک IDS بیرون و دیگری را درون آن قرار دهیم.

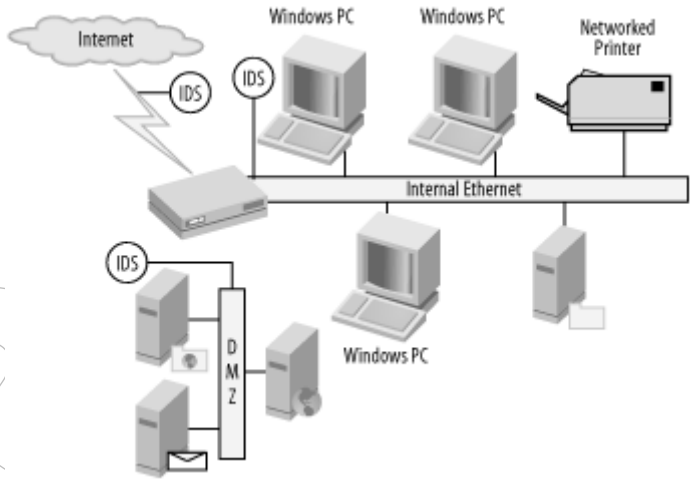
شکل ۲-۱ یک شبکه کوچک را نشان می دهد. در این شبکه همان‌طور که نشان داده شده است, یک IDS بعد از فایروال قرار گرفته است که ترافیک عبوری از فایروال را کنترل می‌کند. در این شبکه تهدیدهای درونی از طرف کاربران شبکه نادیده گرفته شده است.

[15] Dimilitarized Zone



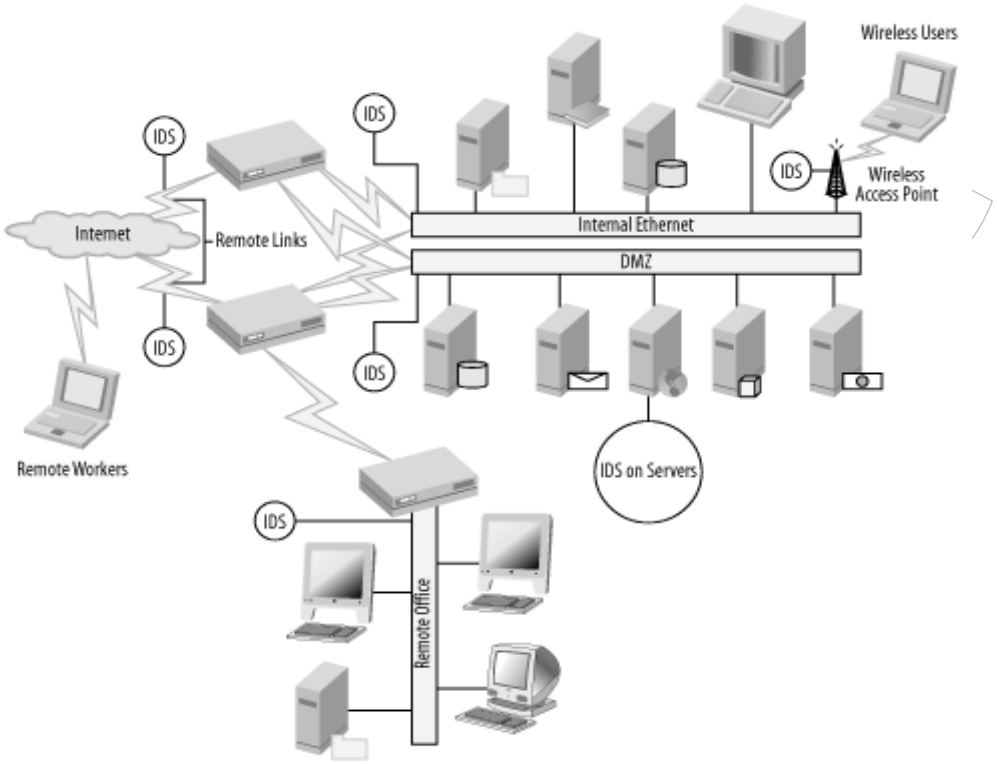
شکل ۲-۱ طرحی از یک home network

در یک شبکه در اندازه متوسط مناطق قابل توجهی برای مانیتورکردن وجود دارد. در این حالت نیز یک IDS بعد از فایروال قرار می‌گیرد. همچنین باید DMZ را مانیتور کرد. این ناحیه بیشترین تهدید را برای ما دارد. این ناحیه شامل سرورهای وب, mail, FTP و دیگر سرویس‌هایی که به طور گسترده با شبکه خارجی در ارتباط است می شود. همچنین هر چه شبکه بزرگتر می شود نیاز به سنسورهایی است تا تهدیدهای داخلی شبکه را تحت نظر داشته باشد. در شکل ۲-۲ که یک شبکه در اندازه متوسط را نشان می‌دهد قبل از فایروال هم IDS قرار گرفته است. با مقایسه ترافیک قبل از فایروال با ترافیک گذشته از فایروال می‌توان میزان عملکرد فایروال را نیز ارزیابی کرد.



شکل ۲-۲ شبکه‌ای در اندازه متوسط

شکل ۲-۳ یک شبکه در اندازه بزرگ را نشان می‌دهد, همان‌طور که ملاحظه می‌شود نقاط مهم زیادی در این شبکه وجود دارد.



شکل۲-۳ شبکه‌ای در اندازه بزرگ

سرورهای زیادی در DMZ قرار دارد, بیش از یک اتصال به اینترنت وجود دارد, نقاط دسترسی[16] wireless وجود دارد, تعدادی کاربران از طریق VPN به شبکه متصل هستند. سنسورها را باید به‌گونه ای قرار داد که بیشتر این نواحی را حتی المقدور بپوشاند.

[16] Access point