بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش چهارم: دسترسی‌پذیری

امروزه بسیاری از روترها و سوئیچ‌ها مورد حملات سایبری قرار می‌گیرند که به نوعی برای آسیب‌رسانی به این دستگاه‌ها و یا ایجاد وقفه در سرویس‌دهی شبکه طراحی شده‌اند. از میان این حملات می‌توان به حمله منع‌سرویس به پروتکل‌های در دسترس و یا خارج از محدوده دسترسی عموم کاربران، حملات منع‌سرویس توزیع‌شده، حمله سیل‌آسا[1]، شناسایی و ارزیابی شبکه، دسترسی غیرمجاز به منابع و غیره اشاره نمود. در این گزارش قصد بر آن است که مجموعه‌ای از بهترین راه‌کارها برای مقابله با حملاتی از این دسته ارائه گردد تا از این طریق سوئیچ‌ها و روترها قابلیت مقابله و مقاومت در مقابل این تهدیدها را داشته باشند. چرا که یکی از پارامترهای مهم امنیت، مسئله در دسترس بودن منابع است و اگر سوئیچ‌ها و روترها به درستی پیکربندی نشده باشند، حملاتِ به قصد منع سرویس می‌توانند زیان‌های جبران‌ناپذیری را به شبکه وارد آورند.

غیرفعال‌سازی سرویس‌های غیرضروری

در روترها و سوئیچ‌های سیسکو، به طور پیش‌فرض تعدادی از سرویس‌ها فعال هستند که معمولاً برای عموم شبکه‌ها مورد نیاز است. ولی به دلیل اینکه انواع شبکه‌ها با یکدیگر متفاوت می‌باشند و ممکن است برخی از این سرویس‌ها درون شبکه‌ای مورد استفاده قرار نگیرند، باید غیرفعال شوند. این غیرفعال‌سازی کمک می‌کند تا منابع موجود هدر نروند. از طرف دیگر راه را برای افراد خراب‌کار که از آسیب‌پذیری‌های سرویس‌های مختلف برای حمله به این دستگاه‌ها استفاده می‌کنند، سخت‌تر خواهد ساخت. چرا که با غیرفعال شدن این سرویس‌ها، دیگر امکان اکسپلویت نمدن این سرویس‌ها (در صورتی که دارای آسیب‌پذیری باشند) وجود ندارد.

در این گزارش نحوه غیرفعال‌سازی برخی از این سرویس‌ها که معمولاً مورد استفاده قرار نمی‌گیرند، توضیح داده شده است. IOS سیسکو، دستور AutoSecure را در محیط CLI در نظر گرفته است که تمامی این سرویس‌های غیرضروری را غیرفعال می‌کند.

[1] flood attacks

در ادامه نحوه غیرفعال‌سازی سرویس‌های زیر که معمولاً در زیرساخت شبکه مورد استفاده قرار نمی‌گیرند، توضیح داده شده است:

- Cisco Discovery Protocol (CDP)
- Directed Broadcast
- Finger
- Maintenance Operations Protocol (MOP)
- IP BOOTP Server
- IP Redirects
- IP Source Routing
- PAD
- Proxy ARP
- Ident
- TCP and UDP Small Servers

Cisco Discovery Protocol (CDP)

پروتکل CDP یک پروتکل لایه ۲ است که برای مدیریت و مشکل‌یابی دستگاه‌های شبکه از طریق ارسال اطلاعات به دستگاه‌های همسایه مورد استفاده قرار می‌گیرد. با فعال‌سازی این پروتکل، مسئولین و ادمین‌های شبکه می‌توانند دستورات مربوط به این پروتکل را اجرا نموده و از پلتفرم، مدل، نسخه نرم‌افزار و یا حتی آدرس IP دستگاه‌های همسایه باخبر شوند.

CDP پروتکل بسیار مفیدی است، ولی می‌تواند اطلاعات بسیار حساسی را در اختیار فرد حمله‌گر قرار دهد. بهتر است که این پروتکل بر روی تمامی دستگاه‌ها غیرفعال باشد و تنها زمانی که به این پروتکل نیاز است (و یا بر روی اینترفیس‌های خاص در زمان‌های مورد نیاز) فعال گردد.

برای حالت‌هایی که از این پروتکل به منظور عیب‌یابی و بررسی امنیتی استفاده می‌شود، باید پروتکل برای همه دستگاه‌ها فعال گردد و تنها بر روی اینترفیس‌هایی که می‌توانند باعث ایجاد تهدید در شبکه شوند، غیرفعال گردد (به طور مثال بر روی اینترفیس ورودی اینترنت به شبکه).

برای غیرفعال‌سازی این پروتکل، از دستور no cdp run استفاده می‌شود:

```
Router(config)# no cdp run
```

برای غیرفعال‌سازی این سرویس بر روی یک یا چند اینترفیس، باید وارد محیط اینترفیس مورد نظر شده و دستور زیر را وارد نمود:

```
Router(config-if)# no cdp enable
```

Directed Broadcast

یک بسته IP همه‌پخشی مستقیم، بسته‌ای است که آدرس مقصد آن یک آدرس همه‌پخشی معتبر برای یک زیرشبکه است. هنگامی که یک بسته directed broadcast به دست یک روتر برسد که مستقیماً به زیرشبکه خود متصل شده و برای ارسال این دسته از بسته‌ها پیکربندی شده باشد، بسته بین تمامی آدرس‌های موجود در زیرشبکه پخش خواهد شد. به صورت پیش‌فرض تمامی نسخه‌های قدیمی سیسکو به این صورت برنامه‌ریزی شده‌اند که این بسته‌ها را به مقصد هدایت نمایند. ولی از آنجا که این قابلیت برای راه‌اندازی حملاتی مثل smurf مورد استفاده قرار می‌گیرد، در دستگاه‌های جدید برنامه‌ریزی شده است تا این بسته‌ها drop شوند.

برای غیرفعال‌سازی این پروتکل بر روی اینترفیس مورد نظر بایستی دستور زیر اجرا شود:

```
Router(configif) # no ip directed-broadcast
```

Finger

Finger پروتکلی است که برای مشاهده اطلاعات مربوط به کاربران وارد شده به یک سیستم از راه دور و یا دستگاه شبکه مورد استفاده قرار می‌گیرد. اگرچه که این سرویس داده‌های آن‌چنان حساسی را آشکار نمی‌کند، ولی یک حمله‌گر ممکن است بتواند از آن برای جمع‌آوری اطلاعات استفاده کند. به همین منظور توصیه می‌گردد که این سرویس نیز غیرفعال گردد.

در نسخه‌های قدیمی‌تر سیسکو که این سرویس به صورت پیش‌فرض فعال است، می‌توان با استفاده از دستور زیر این سرویس را غیرفعال نمود:

```
Router(config) # no service finger
```

در نسخه‌های 12.1(5) و 12.1(5)T از نرم‌افزار IOS سیسکو، این سرویس در حالت پیش‌فرض غیرفعال است. اگر finger روشن باشد ولی سرویس آن مورد نیاز نباشد، با استفاده از دستور زیر می‌توان آن را غیرفعال نمود:

```
Router(config) # no ip finger
```

Maintenance Operations Protocol (MOP)

این پروتکل توسط Digital Equipment Corporation توسعه داده شده است تا از آن برای برقراری ارتباط راه دور بین میزبان‌ها و سرورها استفاده شود. نرم‌افزار IOS سیسکو MOP را به منظور جمع‌آوری اطلاعات مربوط به پیکربندی هنگامی که با شبکه DECNet ارتباط برقرار می‌نمایند، پیاده‌سازی نموده است. به صورت پیش‌فرض این پروتکل بر روی تمامی اینترفیس‌های اترنت فعال است، درحالی که بر روی مابقی اینترفیس‌ها غیرفعال است. برای غیرفعال سازی این پروتکل بر روی هر اینترفیس از دستور زیر استفاده می‌شود:

```
Router(config-if) # no mop enabled
```

ضمناً پروتکل MOP به برخی از حملات آسیب‌پذیر است. به همین دلیل این پروتکل باید بر روی تمامی اینترفیس‌های در دسترس که به شبکه‌های خارجی متصل می‌باشند، غیرفعال گردد مگر اینکه متصل به شبکه‌ی DECNet باشند.

IP BOOTP Server

پروتکل BOOTP به ایستگاه‌های کاری بدون دیسک، در زمان بوت شدن کمک می‌کند تا به صورت پویا یک آدرس IP برای شناسایی در شبکه، آدرس IP سرور BOOTP و یک فایل پیکربندی را دریافت کنند. نرم‌افزار IOS سیسکو یک سرویس bootstrap پیاده‌سازی نموده است که به روتر این قابلیت را می‌دهد که همانند یک سرور BOOTP عمل نموده و سرویس‌های پیکربندی پویا را در اختیار سایر روترهای درون شبکه قرار دهد و در حالت پیش‌فرض فعال می‌باشد. برای غیرفعال‌سازی این سرویس باید دستور زیر بر روی روتر اجرا گردد:

```
Router(config) # no ip bootp server
```

IP Redirects

به صورت پیش‌فرض، نرم‌افزار IOS سیسکو پیام‌های ICMP redirect را هنگامی که مجبور به ارسال مجدد یک بسته از طریق همان اینترفیس دریافتی می‌شود، ارسال می‌کند. هم‌چنین بسته‌های ارسال مجدد ICMP، اطلاعات حساسی را فاش می‌کنند که فرد حمله‌گر می‌تواند از این اطلاعات برای یافتن توپولوژی شبکه استفاده کند. به همین جهت نیاز است که این سرویس بر روی تمامی اینترفیس‌های بیرونی شبکه غیرفعال

گردد. این سرویس به راحتی بر روی هرکدام از اینترفیس‌ها با استفاده از دستور زیر قابل غیرفعال‌سازی است:

```
Router(config-if) # no ip redirects
```

IP Source Routing

پروتکل IP از قابلیت مسیریابی مبتنی بر اساس آدرس فرستنده پشتیبانی می‌کند تا از این طریق مسیر ارسال بسته‌ها به طرف مقصد مورد نظر و یا مسیر بازگشت را کنترل نماید. امروزه این ویژگی‌ها به ندرت برای امور روزمره مورد استفاده قرار می‌گیرند. البته برخی از پیاده‌سازی‌های پروتکل IP بسته‌های source-routed را پردازش نمی‌نمایند و ممکن است از طریق ارسال یک بسته که قابلیت source routing دارد، دچار crash شوند. به همین دلیل نیاز است که این پروتکل غیرفعال گردد مگر اینکه مورد نیاز باشد.

برای اینکه نرم‌افزار بتواند هر بسته‌ای که قابلیت source-route در آن تنظیم شده است را دور بیاندازد، باید دستور زیر اجرا گردد:

```
Router(config) # no ip source-route
```

PAD

نرم‌افزار IOS سیسکو، یک سرویس تحت عنوان PAD (packet assembler/disassembler) فراهم نموده است که این اجازه را در اختیار بخش‌های مختلف مثل ترمینال قرار می‌دهد تا به شبکه‌های X.25 متصل گردد. با استفاده از این سرویس این دستگاه‌ها قابلیت ایجاد PAD session را به‌دست خواهند آورد. به صورت پیش‌فرض این سرویس بر روی نرم‌افزار IOS سیسکو فعال می‌باشد و از آن می‌توان برای به‌دست‌آوردن دسترسی‌های غیرمجاز استفاده نمود. به همین دلیل نیاز است که این سرویس غیرفعال گردد و برای این منظور کافی است که دستور زیر در ترمینال دستورات روتر اجرا گردد:

```
Router(config) # no service pad
```

Proxy ARP

پروتکل Proxy Address Resolution تکنیکی است که به کمک آن ماشین‌های درون یک زیرشبکه بدون پیکربندی مسیریابی و یا gateway، به یک زیرشبکه دیگر دسترسی پیدا خواهند نمود. Proxy ARP معمولاً به صورت پیش‌فرض بر روی روترها پیاده‌سازی می‌گردد و هنگامی که تنظیم می‌شود، روتر به نمایندگی از سیستم‌هایی که چند hop با آن فاصله دارند، به تمامی درخواست‌های ARP درون یک زیرشبکه محلی پاسخ خواهند داد.

سناریو به این صورت است که میزبان‌های محلی درخواست‌های ARP را برای هرکدام از مقصدها که هیچ اطلاعاتی از مسیریابی به سمت آنها در اختیار ندارند، ارسال می‌کنند. حال روتر در پاسخ با آدرس MAC خود به عنوان hop بعدی پاسخ خواهد داد. سیسکو به صورت پیش‌فرض از این قابلیت بر روی تمامی اینترفیس‌های خود استفاده می‌کند. که برای هر اینترفیس به راحتی با اجرای دستور زیر می‌توان این سرویس را غیرفعال نمود:

```
Router(config-if) # no ip proxy-arp
```

Ident

پروتکل TCP Client Identity Protocol (Ident) پروتکلی است که به سیستم اجازه می‌دهد تا هویت کاربری که می‌خواهد یک ارتباط TCP را برقرار نماید و یا میزبانی که به یک ارتباط TCP پاسخ می‌دهد را بررسی نماید. هنگامی که این سرویس پیاده‌سازی می‌شود، به کاربران این اختیار را می‌دهد تا اطلاعات هویتی را به راحتی از طریق متصل شدن به یک پورت در سیستم و درخواست اطلاعات به صورت متن، به‌دست آورند. تمامی این اطلاعات می‌توانند برای حمله به شبکه مورد نظر توسط فرد حمله‌گر مورد استفاده قرار گیرند. نرم‌افزار IOS سیسکو، سرویس Ident را در روترها در نظر گرفته است که در حالت پیش‌فرض غیرفعال است. به شدت توصیه می‌گردد که این سرویس در شبکه فعال نشود، ولی به هرحال در صورتی که این سرویس در روتر فعال شده بود، با اجرای دستور زیر به راحتی می‌توان آن را غیرفعال نمود:

```
Router(config) # no ip ident
```

TCP and UDP small Servers

این سرورهای کوچک عموماً بر روی سیستم‌های یونیکس اجرا می‌شوند و برای اهداف عیب‌یابی در شبکه طراحی شده‌اند. نرم‌افزار IOS سیسکو نیز یک پیاده‌سازی از این سرورهای کوچک UDP و TCP را در نظر گرفته است که سرویس‌های echo، chargen ، daytime و discard را فعال می‌کند. مگر در حالت‌های ضروری، این سرویس‌ها باید غیرفعال شوند. چراکه این سرویس‌ها می‌توانند توسط حمله‌گر برای جمع‌آوری اطلاعات و یا حمله به نرم‌افزارهای دستگاه‌ها مورد استفاده قرار گیرند.

این سرویس‌های کوچک به صورت پیش‌فرض بر روی نسخه‌های 11.2 و قبل‌تر از IOS سیسکو فعال هستند. ولی در نسخه‌های 11.3 به بعد دیگر فعال نیستند. به منظور غیرفعال‌سازی هرکدام از این سرویس‌ها از دستورات زیر باید استفاده نمود:

```
Router(config) # no service tcp-sm all-servers
Router(config) # no service udp-sm all-servers
```

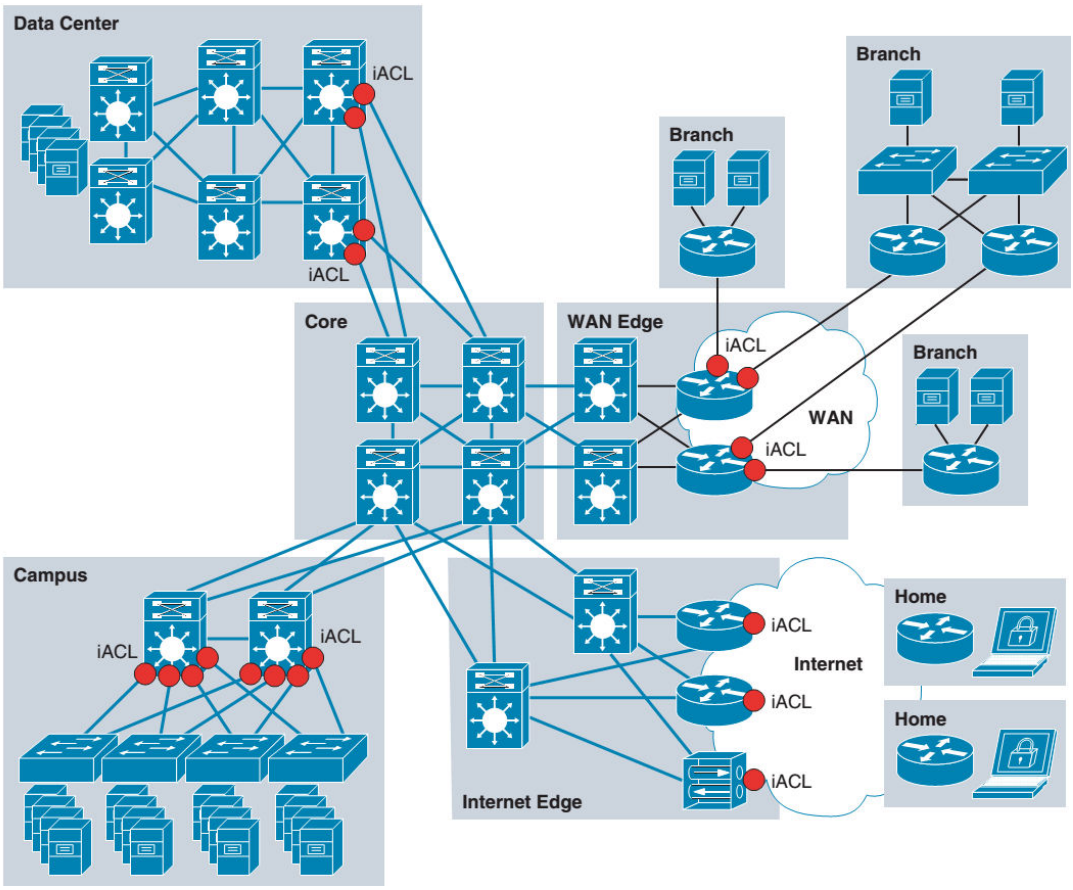
Infrastructure Protection Access Control Lists (iACLs)

iACL یک تکنیک کنترل دسترسی است که زیرساخت شبکه را از حملات داخلی و خارجی محافظت می‌کند. iACLها تکنیکی هستند که توسط مراکز عرضه‌کننده اینترنت برای محافظت از زیرساخت کلی شبکه طراحی شده است، ولی قابلیت به کارگیری در شبکه‌های کوچک‌تر و شرکت‌ها را نیز دارد.

برای معرفی دقیق‌تر تکنیک کنترل دسترسی، iACLها مدل توسعه‌داده شده از لیست‌های کنترل دسترسی هستند تا تنها به ترافیک‌های مجاز اجازه عبور داده و با مدیریت باندهای ترافیک درون دستگاه‌های شبکه مثل سوئیچ‌ها و روترها و منع نمودن عبور سایر بسته‌ها به درون شبکه، امکان کنترل و مقابله با حملات درون شبکه را فراهم نمایند. به طور مثال یک iACL توسعه‌داده شده توسط یک ISP، به صورتی تعریف می‌گردد تا تنها به ترافیک‌های BGP از طرف مبدأهای مجاز اجازه عبور بدهد.

پس می‌توان گفت که iACLها از طریق مدیریت ترافیک و کنترل دسترسی‌ها، روترها را از حملات دسترسی غیرمجاز و منع‌سرویس از طرف پروتکل‌ها و سورسهای غیرمجاز ایمن نگه می‌دارند. iACLها همچنین از حملات تزریق، دستکاری و یا حذف اطلاعات مسیریابی محافظت می‌کنند. البته لازم به ذکر است که iACLها نمی‌توانند در مقابل حملاتی که از طرف مبدأهای مجاز و بر روی پروتکل‌های مجاز اعمال می‌شوند، مقابله کنند.

iACLها باید بیشتر در شبکه‌های مرزی که زیرساخت شبکه توسط کاربران درونی و خارجی در دسترس قرار می‌گیرد و یا لبه‌های مدیریتی که تجهیزات و لینک‌ها تحت مدیریت‌های مختلف به هم متصل می‌گردند، مورد استفاده قرار بگیرند. همان‌طور که اشاره شد، یک مکان مناسب برای استفاده از این مکانیزم‌های کنترل دسترسی مرز بین ISPها است، یعنی جاهایی که بتوان به کمک iACL از حملات به شبکه جلوگیری نمود. نمونه‌های دیگر کاربرد iACL می‌توان به لبه‌های مرزی شبکه‌های تجاری، شبکه‌های WAN و غیره اشاره نمود.



ساختار iACL

به طور کلی جدای از اینکه iACLها باید مطابق با سناریوی پیاده‌سازی‌شده شبکه ایجاد شوند، ولی در حالت کلی دارای بخش‌های ثابت زیر هستند:

- ماژول اول: ورودی‌های مقابله با حملات جعل (spoofing)، ورودی‌های بلاک نمودن بسته‌های با آدرس IP محرمانه و یا سایر آدرس‌ها که برای محیط در نظر گرفته نباید قابل دسترس باشند.
- ماژول دوم: ورودی‌ها برای کنترل دسترسی دقیق ترافیک ارسال شده از طرف سورس‌های خارجی مجاز به درون زیرساخت اصلی شبکه که می‌تواند متعلق به پروتکل‌هایی همانند SSH، Telnet، SNMP و... باشد.
- ماژول سوم: deny نمودن تمامی ترافیک‌ها از مبدأهای خارجی که به طرف آدرس زیرساخت ارسال شده است.

- ماژول چهارم: اجازه دسترسی برای سایر ترافیک‌های عادی

ماژول اول برای جلوگیری از هرگونه ترافیک غیرمجاز و خطرناک به درون شبکه است، به طور مثال بسته‌هایی که آدرس مبدا آنها آدرس داخلی زیرساخت شبکه تعریف شده است، نباید به شبکه وارد شوند چرا که ممکن است توسط فردی در بیرون شبکه به قصد حمله به شبکه، دست‌کاری شده باشد. همچنین باید بسته‌هایی با آدرس مبدا رزرو شده نیز بلاک شوند.

در ادامه یک نمونه از ورودی‌های یک iACL برای یک شبکه ISP نشان داده شده است:

```
! Deny your infrastructure space as a source of external packets
access-list 101 deny ip your_infrastructure_block any
!--- Deny special-use address sources.
!--- See RFC 3330 for additional special-use addresses.
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
! Deny RFC1918 space from entering AS
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
```

ماژول دوم باید به ترافیک‌های کنترلی و مدیریتی مجاز (مثل BGP، OSPF، SNMP و یا SSH) به طرف تجهیزات داخلی زیرساخت شبکه اجازه عبور دهد. به همین منظور نیاز است تا دانشی از ترافیک‌های مجاز به درون شبکه داشته باشد. بنابراین کاملاً واضح است که اگر یک iACL بدون این دانش طراحی شده باشد، ممکن است در برخی از نقاط شبکه از عبور ترافیک‌های بسیار حساس و مهم شبکه جلوگیری شود. یک نکته بسیار مهم هم این است که اگر به درستی و دقت این قوانین تنظیم نشده باشند، ممکن است که نه تنها باعث محافظت از شبکه نشوند، بلکه خود این iACL ها باعث ایجاد یک حمله منع سرویس در داخل خود شبکه شوند.

تنظیمات زیر بخش دوم از یک iACL برای یک ISP در لبه دسترسی به اینترنت را نشان می‌دهد با این فرض که ترافیک خارجی مجاز از نوع پروتکل‌های eBGP و OSPF باشد:

```
! Permit eBGP session
access-list 101 permit tcp host bgp_peer host local_ip eq 179
```

```
access-list 101 permit tcp host bgp_peer eq 179 host local_ip
! Permit OSPF
access-list 101 permit ospf host ospf_neighbor host 224.0.0.5
! Permit DR multicast address, if needed
access-list 101 permit ospf host ospf_neighbor host 224.0.0.6
access-list 101 permit ospf host ospf_neighbor host local_ip
```

ماژول سوم از iACL سایر ترافیک‌هایی که به زیرساخت شبکه ارسال می‌شوند را بلاک می‌کند:

```
! Deny all other access to infrastructure
access-list 101 deny ip any your_infrastructure_block
```

ماژول چهارم و نهایی در نظر می‌گیرد که یا تمامی ترافیک مابقی اجازه عبور داشته باشند و یا بلاک شوند که این بسته به نوع سناریو شبکه باید بررسی شود. در مثال زیر این قوانین نشان داده شده است که اجازه دسترسی برای سایر بسته‌ها داده شده است:

```
! Permit transit traffic (ISP), enterprise inner iACL
access-list 101 permit ip any any
```

شبکه‌های ترافیک عمومی معمولاً در معرض ترافیک قرار دارند و ترانزیتی انجام نمی‌دهند، به همین دلیل ماژول چهارم از iACL در لبه دسترسی به اینترنت در این شبکه‌ها باید بیشتر مورد توجه قرار بگیرد. با توجه به وجود یا عدم وجود فایروال در شبکه و همچنین مطابق سیاست‌گذاری‌های امنیتی شبکه، این ماژول می‌تواند به نحوی پیکربندی شود که یا تمامی ترافیک را از خود عبور دهد و یا تمامی این ترافیک را بلاک کند. پس اگر فایروالی که در مقابل ترافیک شبکه در نظر گرفته شده است دسترسی به شبکه عمومی سازمان را کنترل می‌کند، می‌توان قوانین iACL را به نحوی تنظیم نمود که تمامی مابقی ترافیک را در ماژول چهارم عبور دهند.

روش پیشنهادی پیاده‌سازی iACL

همان‌طور که در قسمت‌های قبلی توضیح داده شد، در صورتی که یک iACL بدون دانش کافی از پروتکل‌های شبکه و تجهیزاتی که استفاده شده طراحی شود، می‌تواند شبکه را در شرایط نامطلوبی قرار دهد

که در نهایت به حمله DoS منتهی می‌شود. به‌همین دلیل بسیار مهم است که قبل از پیاده‌سازی iACL، یک دانش کافی از ترافیک‌های رد و بدل شده درون شبکه داشت.

به همین منظور برای پیاده‌سازی یک iACL بایستی مراحل زیر را دنبال نمود:

- گام۱: شناسای پروتکل‌های استفاده‌شده درون شبکه با استفاده از یک discovery ACL: در این مرحله بایستی یک ACL برای شناسایی و دسته‌بندی طراحی نمود که به تمامی پروتکل‌هایی که به دستگاه‌های زیرساخت‌های شبکه دسترسی دارند، اجازه عبور می‌دهد. در این ACL باید آدرس فرستنده any بوده و آدرس مقصد نیز باید آدرس شبکهِ کل زیرساخت شبکه مورد نظر باشد.
- گام۲: بررسی بسته‌های شناسایی‌شده و فیلتر نمودن دسترسی‌ها به زیرساخت شبکه: پس از اینکه بسته‌های فیلترشده توسط discovery ACL شناسایی شدند، بایستی یک ACL تعریف کرد که به تمامی بسته‌های با آدرس مبدا any به سمت زیرساخت شبکه که برای پروتکل‌های مورد نظر ارسال می‌شوند، اجازه عبور دهد.
- گام۳: محدود نمودن محدوده آدرس‌های IP: پس از پیدا نمودن درک کلی از پروتکل‌هایی که باید به درون شبکه راه یابند، باید دسترسی به پروتکل‌های شناخته‌شده و آدرس‌هایی که نیاز به احراز اصالت دارند، مورد بررسی قرار بگیرد. به طور مثال برای یک ISP باید به طور خاص اجازه به همسایه‌های خارجی BGP داد.
- گام۴ (اختیاری): محدود نمودن آدرس مقصدها برای iACL: در این فاز نهایی، آدرس‌های مقصد برای پروتکل‌های خاص محدود می‌گردند.

Receive Access Control Lists (rACLs)

rACL برای محافظت روترهای مرکزی (هسته) از ترافیک‌های غیرضروری مورد استفاده قرار می‌گیرد که می‌توانند عملکرد سیستم را مورد تاثیر قرار دهند. rACLها ابتدا برای روترهای سری ۱۲۰۰۰ از سیسکو طراحی شده بودند ولی هم‌اکنون برای سایر پلتفرم‌های سیسکو مثل ۷۵۰۰ و یا ۱۰۰۰۰ نیز در دسترس می‌باشد.

به عبارت ساده‌تر، rACL یک لیست کنترل دسترسی است که ترافیک‌های ارسالی به طرف RP در معماری‌های مختلف سیسکو مثل سیسکو سری ۱۲۰۰ را کنترل می‌کند.

روش پیشنهادی پیاده‌سازی rACL

برای پیاده‌سازی rACL بایستی مراحل زیر را دنبال کرد:

- گام۱: با استفاده از discovery ACL پروتکل‌های استفاده شده در شبکه را شناسایی کرد.
- گام۲: بسته‌های شناسایی‌شده را بررسی نموده و دسترسی به RP را فیلتر نمود.
- گام۳: رنج آدرس‌های مبدا را محدود کرد.
- گام۴: محدود نمودن دسترسی‌های rACL تا تنها آدرس‌های مبدا شناخته شده اجازه دسترسی داشته باشند. به عبارت دیگر بایستی دسترسی را به نحوی محدود کرد که تنها آدرس‌هایی که با RP ارتباط برقرار می‌کنند، اجازه داشته باشند.
- گام۵ (اختیاری): محدود نمودن آدرس‌های مقصد در rACL

Control Plane Policing (CoPP)

CoPP یک زیرساخت امنیتی است که از control plane در روترها و سوئیچ‌ها از طریق اعمال سیاست‌های QoS (که ترافیک پردازش‌شده در CPU را تنظیم می‌کند) محافظت می‌کند. در واقع با استفاده از CoPP، سیاست‌های QoS توسط CPU مدیریت می‌شود. این امر کمک می‌کند که control plane در روترها و سوییچ‌ها از برخی حمله‌ها در امان باشند (مانند حملات شناسایی و همینطور DoS مستقیم).

از لحاظ عملکرد، CoPP دقیقاً پس از تصمیم‌گیری در مورد مسیریابی یا سوییچینگ و قبل از ارسال ترافیک به control plane وارد عمل می‌شود. در صورت فعال بودن CoPP، سلسله‌ی وقایع به صورت زیر انجام می‌گردد:

- گام۱: یک بسته بر روی پورت ورودی روتر/سوییچ که CoPP در آن فعال است وارد می‌شود.
- گام۲: پورت ورودی، عملیات مربوطه و سرویس‌های QoS را انجام می‌دهد.
- گام۳: بسته به پردازنده‌ی سوییچ/روتر ارسال می‌شود.
- گام۴: پردازنده‌ی سوییچ/روتر عملیات تصمیم‌گیری مربوط به سوییچینگ/روتینگ را انجام می‌دهد و مشخص می‌کند که آیا بسته باید به control plane ارسال شود یا خیر.

- گام۵: بسته‌های ارسالی برای control plane توسط CoPP پردازش می‌شود و با توجه به سیاست‌های آن کلاس از ترافیک، به control plane تحویل داده می‌شود و یا drop می‌شود. بسته‌هایی که مقاصد دیگر دارند، به صورت عادی ارسال می‌شوند.

در مقایسه با rACLها، قابلیت ایجاد محدودیتِ نرخ که در CoPP وجود دارد، آن را برای مقابله با حملات DoS علیه control plane مقاوم‌تر می‌سازد. در حالت کلی، CoPP برای تمامی روترها و سوییچ‌ها پیشنهاد می‌شود، خصوصاً آنها که در معرض اینترنت یا سایر شبکه‌های خارجی قرار دارند. با این حال، برخی کاربران ممکن است همچنان rACL را به دلیل سادگی ترجیح دهند.

کلاس‌بندی ترافیک CoPP

از آنجاییکه CoPP ترافیک را فیلتر می‌کند، لازم است قبل از پیاده‌سازی درک کاملی از ترافیک مجاز به مقصد RP و SP وجود داشته باشد. در غیر این صورت ممکن است CoPP برخی ترافیک‌های ضروری را بلاک کند.

قبل از پیاده‌سازی CoPP باید ترافیک‌های لازم شناخته شده و کلاس‌بندی شود. در ادامه برخی از دسته‌های کلی معرفی می‌شود:

- BGP: این دسته مربوط به ترافیکی است که تنظیمات مربوط به همسایگی‌ها در پروتکل BGP را انجام می‌دهد.
- IGP: این دسته مربوط به ترافیک‌های پروتکل‌های مسیریابی داخلی مانند OSPF، EIGRP و RIP می‌شود.
- Interactive Management: این دسته برخی ترافیک‌های معمول که برای تنظیمات و عملیات‌های مختلف در شبکه به کار می‌رود را شامل می‌شود. برای مثال می‌توان پروتکل‌های SSH، NTP، SNMP و TACACS را نام برد.
- File Management: ترافیک‌های مربوط به انتقال فایل همانند پروتکل‌های FTP و TFTP در این دسته جای می‌گیرند.
- Reporting: ترافیک مربوط به گزارش عملکرد شبکه در این دسته جای می‌گیرند که سرویس‌هایی مانند SAA را شامل می‌شود.

- Monitoring: این ترافیک مربوط به مانیتورینگ روتر می‌شود. برای مثال می‌توان درخواست‌های ping و traceroute در پروتکل ICMP را مثال زد.
- Critical Applications: این کلاس مربوط به ترافیک‌هایی است که برای یک شبکه‌ی خاص حیاتی هستند. از جمله‌ی آنها می‌توان پروتکل‌های GRE، HSRP، VRRP، SIP، DLSw، DHCP، IPSec و ترافیک‌های multicast را مثال زد.
- Layer 2 Protocols: این دسته برای بسته‌های پروتکل‌های ARP به کار می‌رود. با استفاده از CoPP می‌توان نرخ بسته‌های ARP را محدود کرد تا منابع RP کمتر استفاده شود.
- Undesirable: برای منع دسترسی ترافیک‌های ناخواسته و بدخواه به RP به کار می‌رود. این دسته مواقعی به کار می‌آید که بایستی یک ترافیک خاص همیشه نادیده گرفته شود (تا اینکه در یک دسته خاص قرار گیرد).
- Default: تمامی ترافیک‌هایی که در هیچ‌یک از کلاس‌های تعریف‌شده قرار نگیرند، جزو این دسته محسوب می‌شوند. بهتر است دسترسی به RP برای این ترافیک (با نرخ محدود) داده شود. همچنین می‌توان با بررسی و شناسایی این دسته، برخی دسته‌های جدید را کشف کرد و سپس برای آنها کلاس جداگانه تعریف کرد.

روش پیشنهادی پیاده‌سازی CoPP

پیشنهاد می‌گردد که مراحل زیر انجام گردند:

- گام۱: شِمای کلاس‌بندی برای شبکه‌ی مورد نظر مشخص شود. بایستی این کار با توجه به پرکاربردترین ترافیک‌های شبکه انجام گیرد.
- گام۲: باید ACLهای مربوط به کلاس‌بندی را تنظیم نمود.
- گام۳: باید ترافیک واقعی را بررسی کرده و کلاس‌بندی‌ها را به طور مناسب بازتنظیم کرد.
- گام۴: باید آدرس‌های مبدأ را به رنج آدرس‌های شبکه‌ی خود محدود نمود.
- گام۵: باید ACLها را محدود به آدرس‌های مبدأِ مجاز کرد.
- گام۶: باید با اعمال محدودیت بر روی نرخ، سیاست‌های CoPP را پالایش نمود.

Control Plane Protection (CPP)

Control Plane Protection یک ویژگی امنیتی است که برخی قابلیت‌های CoPP را گسترش می‌دهد. CPP با تقسیم کردن Control Plane به سه sub-interface اجازه می‌دهد سیاست‌های محدودیت نرخ به شکل جداگانه در آنها اجرا شود. به‌علاوه، CPP از port-filtering و همینطور صفِ آستانه‌ای نیز استفاده می‌کند. port-filtering مکانیزمی برای دور انداختن زودهنگامِ بسته‌هایی است که متعلق به پورت‌های بسته‌ی TCP/UDP هستند. در مکانیزم صف آستانه‌ای نیز تعداد بسته‌های هر پروتکل که در صف ورودیِ control plane نگهداری می‌شوند، محدود می‌شود. این موجب می‌شود که از غوطه‌ور شدن صف ورودی به بسته‌های مربوط به یک پروتکل خاص جلوگیری شود.

اولین لایه‌ی محافظتی توسط CoPP فراهم می‌شود که تمام بسته‌های به مقصد control plane را در سطحی انبوه کنترل می‌کند. پس از آنکه ترافیک توسط CoPP پردازش شده و به CPP تحویل داده می‌شود، لایه‌ی دوم از محافظت اعمال می‌شود که عبارتست از تقسیم کردن به سه دسته‌ی جداگانه. هر دسته توسط یک sub-interface در control plane پردازش می‌شود که سیاست‌های متفاوتی برای محدودیت نرخ دارند. سه sub-interface که توسط CPP در control plane پیاده می‌شود عبارتند از:

- host subinteface: کنترل بسته‌هایی که مقصد آنها interface خود روتر هستند را بر عهده دارد.
- transit subinterface: بسته‌هایی که روتر مسئولیت فوروارد کردن آنها را دارد کنترل می‌کند.
- CEF-exception subinterface: بسته‌هایی که به دلیل ویژگی‌های ورودیِ تنظیم‌شده در مسیر فورواردِ CEF هدایت شده‌اند و یا مستقیماً توسط درایور اینترفیس به صف ورودی control plane ارسال شده‌اند (مثل ARP، L2 Keepalive و ترافیک غیرِ IP) را کنترل می‌کند.

ترتیب رویدادها در CPP بدین شرح است:

- گام۱: بسته وارد روتری می‌شود که CoPP در اینترفیس ورودی آن تنظیم شده است.
- گام۲: اینترفیس، سرویس‌های پایه را بر روی پورت ورودی و QoS انجام می‌دهد.
- گام۳: بسته به پردازشگر روتر ارسال می‌شود.

- گام۴: پردازشگر تصمیم‌گیری مربوط به روتینگ را انجام داده و مشخص می‌کند آیا بسته باید به سمت control plane ارسال شود یا خیر.
- گام۵: بسته‌هایی که به مقصد control plane ارسال می‌شوند، توسط CoPP پردازش شده و بر اساس سیاست‌های مربوط به هر کلاس از ترافیک، تصمیم‌گیری در مورد drop شدن یا تحویل بسته به CPP اتخاذ می‌شود. بسته‌های مقاصد دیگر به صورت عادی فوروارد می‌شوند.
- گام۶: CPP بسته‌ها را با توجه به subinterface مربوط به آنها دسته‌بندی می‌کند.
- گام۷: بسته‌هایی که توسط هر subinterface دریافت می‌شود، بر اساس سیاست‌های تنظیم‌شده، drop شده و یا به صف ورودی control plane ارسال می‌شود.
- گام۸: به‌علاوه، بسته‌هایی که به host subinterface ارسال می‌شوند، می‌توانند بر اساس سیاست‌های Port-filter و یا آستانه‌ی صف نیز در مورد آنها تصمیم‌گیری شود.

CPP نیز مشابه با CoPP با فیلتر کردن ترافیک ناخواسته، از RP در روترهای Cisco IOS محافظت می‌کند. این موضوع از control plane در برابر ترافیکی که ممکن است بخشی از حمله‌ی DoS باشد محافظت می‌کند و موجب می‌شود پایداری شبکه حتی در شرایط حمله نیز بهتر حفظ شود.

روش پیشنهادی پیاده‌سازی CPP

از آنجا که CPP با حفاظت از RP پایداری شبکه را در شرایط حمله افزایش می‌دهد، باید حتماً به عنوان یک مکانیزم محافظتی در تمامی روترهای مبتنی بر نرم‌افزار پیاده شود. به دلیل اینکه CPP ترافیک را فیلتر می‌کند، باید قبل از پیاده‌سازی آن درک کاملی از شرایط ترافیک مجاز به مقصد روتر وجود داشته باشد. در غیر این صورت، ممکن است برخی ترافیک مجاز نیز مسدود شود که این خود می‌تواند شرایط انجام حمله‌ی DoS را مهیا سازد.

Port Security

برای مقابله با MAC flooding و سایر حملات CAM overflow در لایه دو، آدرس‌های MAC که اجازه‌ی ارسال ترافیک بر روی یک پورت خاص دارند، مشخص و محدود می‌شوند. Port Security به دو طریق می‌تواند لیست آدرس‌های مجازِ MAC را به دست آورد:

- تشخیص پویای آدرس‌های MAC
  - ماکزیمم تعداد آدرس‌های MAC که مجاز به استفاده از یک پورت هستند مشخص می‌شود.
  - برای محیط‌های پویا همچون لبه‌ی دسترسی
- تنظیم استاتیک آدرس‌های MAC
  - آدرس‌های استاتیک MAC مجاز بر روی هر پورت را مشخص می‌کند.
  - برای محیط‌های استاتیک مانند server farm یا DMZ مناسب می‌باشد.

به دو صورت ممکن است تخلف امنیتی به وقوع بپیوندد:

- تعداد MACهای مربوط به یک پورت به میزان ماکزیمم رسیده باشد و از یک آدرس ناشناسِ MAC بر روی آن پورت بسته دریافت شود.
- بسته‌ای متعلق به یک آدرس MAC مجاز بر روی یک پورت نامربوط ظاهر شود.

Port Security بر روی پورت‌های trunk نیز قابل اجراست اما نیاز به تنظیماتی ویژه دارد. در حالت trunk می‌توان تنظیمات Port Security را برای هر VLAN به طور جداگانه انجام داد.

حالت تخلف در Port Security	عکس‌العمل به تخلف	ایجاد اخطاریه	فعال‌سازی دوباره‌ی پورت پس از تخلف
Protect	بسته‌های با آدرس مبدا MAC ناشناخته drop می‌شوند	_	تشخیص دینامیک آدرس‌های MAC در هنگام کمتر بودن تعداد آدرس‌ها از مقدار ماکزیمم، ادامه پیدا می‌کند
Restrict	بسته‌های با آدرس مبدا MAC ناشناخته drop می‌شوند	• پیام Syslog تولید می‌شود. • شمارنده‌ی تخلف امنیتی افزوده می‌شود. • SNMP trap ایجاد می‌شود (در صورت فعال	تشخیص دینامیک آدرس‌های MAC در هنگام کمتر بودن تعداد آدرس‌ها از مقدار ماکزیمم، ادامه پیدا می‌کند

		بودن).	
Shutdown (default)	پورت غیرفعال می‌شود	• پیام Syslog تولید می‌شود • شمارنده‌ی تخلف امنیتی افزوده می‌شود • SNMP trap ایجاد می‌شود (اگر فعال باشد)	پورت تنها پس از تنظیم دستی می‌تواند دوباره فعال شود

تنظیمات Port Security

برای تنظیم Port Security به صورت پویا و حالت تخلف امنیتیِ restrict از دستورات زیر استفاده می‌شود:

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# switchport port-security maximum 2
Router(config-if)# switchport port-security violation restrict
Router(config-if)# switchport port-security
```

برای حالت استاتیک نیز باید از دستوراتی مشابه با دستورات زیر استفاده کرد:

```
tRouter(config)# interface gigabitethernet0/2
Router(config-if)# switchport port-security maximum 1
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# switchport port-security violation restrict
Router(config-if)# switchport port-security
```

برای تنظیم مدت زمان تایمرها (به دقیقه) برای تشخیص time-out نیز از دستورات زیر استفاده می‌شود:

```
Router(config)# interface gigabitethernet0/1
Router(config-if)# switchport port-security aging time 2
Router(config-if)# switchport port-security aging type inactivity
```

Port Security Logging

برای ثبت تخلف به شکل SNMP logging از دستور زیر استفاده می‌شود:

```
snmp-server enable traps port-security
```

همچنین برای کاهش بار دستگاه تحت حمله می‌توان محدودیت نرخ برای SNMP تعریف کرد:

```
tsnmp-server enable traps port-security trap-rate <max number of traps per second>
```

Redundancy

شبکه‌ها از بخش‌های مختلف نرم‌افزاری و سخت‌افزاری تشکیل شده‌اند که ممکن است از کار بیافتند یا تحت حمله واقع شوند. پیاده کردن طراحی‌های مازاد موجب می‌شود که پایداری شبکه افزایش یابد و در برابر حمله مقاوم‌تر باشد. روش‌های متفاوتی برای طراحی مازاد وجود دارد که می‌توان آن‌ها را این‌گونه نام برد:

- اینترفیس‌های پشتیبان
- اِلمان‌های مازاد
- دستگاه‌های Standby
- توپولوژیِ مازاد

اینترفیس‌های پشتیبان

اینترفیس پشتیبان، اینترفیسی است که در حالت standby فعالیت می‌کند (مادامی که اینترفیس اصلی از کار بیافتد). اینترفیس پشتیبان می‌تواند یک اینترفیس فیزیکی (مانند Basic Rate Interface یا BRI) یا یک اینترفیسِ دیالرِ پشتیبان باشد که در dialer pool استفاده می‌شود. در حالت standby، اطلاعات مربوط به این اینترفیس در جداول مسیریابی وارد نمی‌شود. اینترفیس‌های پشتیبان به صورت جفتی پیاده‌سازی می‌شوند و معمولاً برای پشتیبانی از ارتباطات ISDN BRI، خطوط نامتقارن و خطوط استیجاری استفاده می‌شوند. این اینترفیس‌ها با دستور زیر تنظیم می‌شوند:

```
interface serial 0
backup interface serial 1
```

المان‌های مازاد

برخی پلتفورم‌های ماژولار این اجازه را می‌دهند که بتوان پردازنده‌ی مسیریابی یا سایر بخش‌های مهم را به شکل مازاد نیز برای روتر تنظیم کرد. از جمله آن‌ها می‌توان موارد زیر را نام برد:

- High System Availability: در روترهای مدل Cisco 7500 می‌توان دو پردازنده‌ی مسیریابی (RP) در یک روتر نصب کرد تا در صورت از کار افتادن یکی، دیگری روتر را reboot کند. لذا روتر مدت زیادی را در حالت fail نخواهد بود.

- High Availability NPE Redundancy: این ویژگی که در روترهای مدل Cisco 7300 پیاده شده، باعث می‌شود که در صورت از کار افتادن NPE-G100، مازادِ آن (که مشابه با آن است) عملیات booting را انجام داده و کنترل line card ها را بر عهده گیرد.
- Route Processor Redundancy (RPR): در این حالت Cisco IOS می‌تواند قبل از switchover بر روی پردازنده‌ی standby عمل boot را انجام دهد اما تغییرات در حین اجرا در آن ذخیره نخواهند شد.
- Route Processor Redundancy Plus: در این روش تنظیمات شروع و همینطور تنظیمات در حین اجرا در دو پردازنده به صورت همزمان اعمال خواهد شد.
- Stateful Switchover (SSO): این حالت علاوه بر امکانات +RPR، از همزمانی line card ها و پروتکل‌ها و اطلاعات اپلیکیشن‌ها نیز ما بین دو RP پشتیبانی می‌کند.

دستگاه‌های standby

سیسکو مکانیزم‌ها و پروتکل‌های مختلفی را برای پیاده‌سازی دستگاه‌های standby پیاده کرده است که موجب افزایش دسترس‌پذیری در شبکه و سیستم می‌شوند. معمولاً دستگاه‌های standby به صورت جفت دستگاه اصلی پیاده می‌شوند اما برخی اوقات نیز دستگاه‌ها به صورت گروهی کار می‌کنند. مکانیسم‌های failover دستگاه‌های standby می‌تواند Active/Standby یا Active/Active و همینطور Stateless یا Stateful باشند:

- Active/Standby Failover: یکی از دستگاه‌ها فعال و دیگری standby است و در صورتی که دستگاه اول از کار بیافتد، دستگاه دوم شروع به کار می‌کند.
- Active/Active Failover: هر دو دستگاه فعالند. می‌توان در این حالت عملیاتی نظیر load balancing نیز انجام داد.
- Stateless Failover: در هنگام failover، تمامی اتصالاتی که قبلاً برقرار شده‌اند قطع می‌شود و کلاینت‌ها باید دوباره آنها را برقرار کنند.
- Stateful Failover: حالت مربوط به اتصالات به دستگاه دوم به طور مرتب منتقل می‌شود. لذا پس از Failover نیازی نیست که کلاینت‌ها دوباره اتصالات را برقرار کنند.

همچنین روترهای سیسکو از پروتکل‌های First Hop Redundancy مانند HSRP، VRRP و GLBP پشتیبانی می‌کنند. این پروتکل‌ها بدین منظور طراحی شده‌اند تا failover را به شکل transparent در روترِ first-hop انجام دهند. با این پروتکل‌ها، دو یا چند روتر در یک گروه قرار داده‌شده‌اند و هردو از یک آدرس IP استفاده می‌کنند (آدرس IP مجازی). آدرس IP مجازی در workstation هر کاربر پایانی به عنوان default gateway تنظیم شده و در ARP cache در هاست قرار دارد. یکی از روترهای گروه به عنوان روتر فعال انتخاب می‌شود و مسئول رسیدگی به تمامی ترافیکی است که به آدرس IP مجازی ارسال می‌شود. اگر روتر فعال fail شود، یکی از روترهای standby مسئولیت وی را بر عهده می‌گیرد.

توپولوژی مازاد

توپولوژی مازاد می‌تواند هم در سطح network و هم در سطح data link پیاده‌سازی شود. در هر دو حالت، استراتژی‌های redundancy بستگی به قابلیت‌های دینامیک شبکه برای بازیابی پس از خرابی دارد. در سطح network نیل به این هدف توسط پروتکل‌های روتینگ دینامیک مانند EIRP و OSP میسر می‌گردد و در سطح data link نیز این عمل توسط پروتکل‌های spanning tree صورت می‌پذیرد.

در هنگام پیاده‌سازی توپولوژی مازاد، باید اطمینان حاصل کرد که توپولوژی نهایی با سیاست‌های امنیتی و مکانیسم‌های کنترلیِ آن مکان سازگار است. به طور مشخص، هیچ مسیر مازادی نباید بتواند کنترل‌های آن شبکه را دور بزند.

خلاصه فصل

قابلیت/تکنیک امنیتی	حمله‌های مهارشده	مناسب برای
غیرفعال کردن سرویس‌های غیرضروری	دسترسی غیرمجاز، شناسایی، DoS مبتنی بر پروتکل‌های غیرمجاز، حملات amplification، دور زدن کنترل دسترسی	همه‌ی روترها و سوییچ‌ها
iACL	دسترسی غیرمجاز، شناسایی، DoS مبتنی بر پروتکل‌های غیرمجاز	لبه‌ی شبکه و اینترنت، لبه‌ی مدیریتی
rACL	دسترسی غیرمجاز، شناسایی، DoS مبتنی بر پروتکل‌های غیرمجاز	همه‌ی روترها خصوصاً در لبه‌ی اینترنت. rACL ساده‌تر از CoPP است
CoPP	دسترسی غیرمجاز، شناسایی، DoS مبتنی بر پروتکل‌های غیرمجاز،DoS مبتنی بر پروتکل‌های مجاز، DDoS	تمام دستگاه‌هایی که CoPP مبتنی بر سخت‌افزار ارائه می‌کنند
CPP	دسترسی غیرمجاز، شناسایی، DoS مبتنی بر پروتکل‌های غیرمجاز،DoS مبتنی بر پروتکل‌های مجاز، DDoS	دستگاه‌های IOS مبتنی بر نرم‌افزار
Redundancy	DDoS ،DoS	روترها و سوییچ‌های حیاتی