باسمه تعالی

مستند مرجع طراحی امن شبکه

(فصل دوم: امنیت پایه شبکه – Network foundation protection)

مقدمه

در این بخش مروری بر روی best practice ها موجود در حوزه امنیت پایه تجهیزات شبکه خواهد شد. مباحث پایه امنیت شبکه شامل موارد مهم و اساسی امنیتی می‌باشند که در ایجاد و توسعه یک ساختار امنیتی قوی مورد استفاده قرار می‌گیرند. در این فصل، تمرکز اصلی بر روی امن‌سازی زیرساخت خود شبکه می‌باشد، همچنانکه امن‌سازی سرویس‌های شبکه و موارد زیر نیز به عنوان محدوده‌های مهم در بحث امنیت شبکه باید مورد توجه قرار گیرند:

- دسترسی به تجهیزات زیرساخت
- زیرساخت مسیریابی
- انعطاف‌پذیری و استحکام نرم‌افزاری تجهیزات
- دسترسی از راه دور به شبکه
- اجرای سیاست‌های شبکه
- زیرساخت سوئیچینگ

تهدیدهای کلیدی در زیرساخت

تعدادی از تهدیدات مورد انتظار در زیرساخت شبکه عبارتند از:

- Denial-of-service (DoS)
- Distributed DoS (DDoS)
- Unauthorized access
- Session hijacking
- Man-in-the-middle (MITM) attack
- Privilege escalation
- Intrusions
- Botnets
- Routing protocol attacks
- Spanning tree attacks
- Layer ۲ attacks

Best Practice های دسترسی به تجهیزات زیرساخت

امن‌سازی تجهیزات زیرساخت شبکه (شامل مسیریاب‌ها، سوئیچ‌ها، سرورها و دیگر تجهیزات زیرساخت) یکی از مؤلفه‌های کلیدی برای امنیت کل شبکه محسوب می شود. یکی از مهمترین موارد، امنیت مدیریت دسترسی به این تجهیزات می‌باشد. اگر دسترسی به تجهیزات زیرساخت از کنترل خارج شود و به خطر بیافتد، دراین صورت مدیریت کل شبکه می تواند در خطر باشد. در نتیجه برقراری کنترل های مناسب برای جلوگیری از دسترسی‌های غیر مجاز به تجهیزات زیرساخت شبکه بسیار حساس می‌باشد.

برای دسترسی به تجهیزات زیرساخت شبکه می‌توان از روش‌های مختلفی استفاده کرد، از جمله استفاده از کنسول و ارتباطات غیر سنکرون و همچنین دسترسی از راه دور از طریق telnet، rlogin، http و ssh. برخی مکانیزم‌هایی که به طور پیش‌فرض فعال هستند، حداقل امنیت در آن‌ها در نظر گرفته شده است. برای مثال در پلتفرم‌های مبتنی بر نرم‌افزار IOS سیسکو دسترسی از طریق کنسول و مودم به طور پیش‌فرض فعال است. به همین دلیل هر تجهیز موجود در زیرساخت باید به طور دقیق راه‌اندازی و پیکربندی شود و فقط مکانیزم‌های دسترسی پشتیبانی‌شده روی آن‌ها فعال و به طور کامل امن‌سازی شده باشد.

گام‌های کلیدی به منظور تامین امنیت دسترسی‌های تعاملی و مدیریتی به یک تجهیز زیرساخت به صورت زیر قابل بیان است:

- محدود کردن دسترسی به تجهیز: محدود کردن دسترسی به پورت‌ها، منحصر کردن افراد مجاز و محدود ساختن روش‌های دسترسی مجاز
- ارائه اخطارهای مجاز
- اعتبارسنجی دسترسی: اطمینان از اینکه دسترسی به افراد، گروه‌ها و سرویس‌های احراز اصالت شده اعطا شود.
- فعالیت‌های مجاز: محدود کردن فعالیت‌های مجاز قابل انجام توسط کاربران، گروه‌ها و سرویس‌های مشخص

- اطمینان از حفظ محرمانگی داده‌ها: حفاظت از داده‌های حساس که به صورت محلی ذخیره شده‌اند (عدم توانایی مشاهده و کپی آن‌ها). این داده‌های حساس در حین تبادل از طریق کانال ارتباطی ممکن است در معرض حملاتی همچون sniffing، session hijacking و MITM[1] قرار گیرند.
- ثبت وقایع و حساب‌ها برای همه دسترسی‌ها: ثبت این که چه کسی، چه موقع به تجهیز دسترسی داشته و چه فعالیتی انجام داده است.

توجه: به منظور بررسی دسترسی‌ها و تعیین هرگونه دسترسی غیرمجاز، باید وقایع ثبت شده به طور مرتب بازبینی شوند.

محافظت از رمزهای عبور محلی

رمزهای عبور باید به وسیله‌ی یک سرور AAA مرکزی کنترل و نگهداری شوند. با این‌حال cisco IOS و تجهیزات زیرساختی دیگر بعضی از اطلاعات حساس را به صورت محلی ذخیره می‌کنند. دلیل این امر آن است که گاهی ممکن است سرورهای AAA در دسترس نباشند یا ذخیره نام‌های کاربری خاص منظوره، کلیدهای امنیتی و اطلاعات دیگر در مورد رمزعبور.

رمزنگاری[2] پسوردهای کلی، رمزنگاری user- password های محلی و قابلیت مخفی بودن ویژگی هایی هستند که در cisco ios برای کمک به امن کردن اطلاعات حساسی که به صورت محلی ذخیره شده اند دردسترس هستند:

- رمزنگاری اتوماتیک پسوردها با دستور عمومی service password-encryption فعال می‌شود. با یک‌بار فعال‌سازی این دستور، همه رمزهای عبور شامل پسورد کاربرانی که به صورت محلی تعریف شده‌اند به طور خودکار رمزنگاری می‌شوند.
- Local enable password با استفاده از دستور عمومی enable secret فعال می‌شود. فعال کردن دسترسی باید با استفاده از یک پروتکل AAA مانند TACACS+ انجام شود. Locally configured

[1] man in the middle

[2] encryption

enable password به عنوان یک مکانیزم جایگزین بعد از اینکه AAA پیکربندی شد، استفاده می‌شود.

- با دستور password line می‌توان برای هر lineای که برای مدیریت سیستم برنامه‌ریزی در نظر گرفته شده است، یک Line password تعریف نمود. لازم به ذکر است که line password برای پیکربندی اولیه استفاده می‌شود و وقتی AAA پیکربندی می‌شود، تحت تاثیر قرار نخواهد گرفت. همچنین لازم به ذکر است که بعضی از تجهیزات ممکن است بیشتر از ۵ عدد VTY داشته باشند. (https://learningnetwork.cisco.com/thread/۲۳۶۷)

لازم به ذکر است که الگوریتم رمزنگاری که به وسیله‌ی سرویس password-encryption استفاده می‌شود، یک رمز vigenere (نوع ۷) است که به آسانی می‌تواند بازگردانده شود. این دستور تنها به منظور اینکه افراد غیرمجاز رمزهای عبور را در فایل پیکربندی [۱] به سادگی از بالای شانه‌ی فرد مجاز نبینند، مفید است.

Cisco Ios برای بعضی از پسوردهایی که به صورت محلی ذخیره می‌شوند، یک الگوریتم رمزنگاری قوی‌تر (نوع ۵) را پیشنهاد می‌کند. به عنوان نمونه برای تعریف کاربران محلی به جای password keyword از secret keyword و به جای enable password از enable secret استفاده می‌گردد.

قطعه پیکربندی زیر استفاده از command های پیشنهاد شده را نشان می‌دهد:

```
Service password-encryption
Enable secret < strong-password>
Line vty ۰ ۴
Password < strong-password>
```

بنرهای مجاز اطلاع‌رسانی[۲]

توصیه می‌شود که بر روی تمام sessionهای ارتباطی، یک بنر به منظور اطلاع‌رسانی سیاست‌های امنیتی که کاربر ملزم به رعایت آن‌ها می‌باشد، ایجاد شود.

---

[۱] Configuration file

[۲] Implement notification banners

این اطلاعات شامل مواردی همچون تعیین کاربران مجاز و دسترسی آن‌ها و یا اخطار به کاربران غیر مجاز و عواقب دسترسی غیرمجاز آن‌ها می‌تواند باشد.

اگر از دیدگاه امنیتی به قضیه نگاه شود، دراین صورت در بنرها نباید هیچگونه اطلاعات خاصی درباره تجهیز از جمله نام، مدل، نرم‌افزار، محل قرارگیری، اپراتور و یا صاحب آن ذکر شود، به این دلیل که این نوع اطلاعات ممکن است برای حمله کننده مفید واقع شود.

مثالی از بنر اطلاع‌رسانی که بعد از ورود کاربر نشان داده می‌شود، می‌تواند به فرم زیر باشد:

```
banner login #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.
All activities performed on this device are logged and monitored.
#
```

توجه: در IOS سیسکو تنظیمات معینی برای نمایش این هشدارها در دسترس است. این موارد شامل banner motd، banner login، banner incoming و banner exec می‌باشند.

اجرای AAA (accounting و authorization ، authentication)

AAA یک چارچوب معماری برای پیکربندی سه اصل امنیتی مجزا از هم در کنار یکدیگر به روش ماژولار می‌باشد. این اصول در زیر آورده شده‌اند:

- Authentication: احراز اصالت کاربر قبل از اینکه بتواند به شبکه و یا سرویس‌های آن دسترسی داشته باشد.
- Authorization: تعیین سطح دسترسی برای کاربری که احراز اصالت شده است.
- Accounting: توانایی پیگیری دسترسی‌های کاربر که می‌تواند شامل مشخصات، زمان شروع و پایان اتصال، دستورات اجرا شده، تعداد بسته‌ها و یا بایت‌های ارسالی و دریافتی توسط وی باشد.

AAA یک راه‌کار مقدماتی و توصیه‌شده برای کنترل دسترسی است. همه دسترسی‌های مدیریتی (SSH، telnet، HTTP و HTTPS) بایستی با استفاده از AAA کنترل شوند.

از آنجایی که RADIUS از command authorization پشتیبانی نمی‌کند، این پروتکل زمانی که برای مدیریت دستگاه به کار می‌رود در مقایسه با+TACACS از اولویت پایین‌تری برخوردار است.

+TACACS از command authorization پشتیبانی کرده و اجازه کنترل اینکه چه command هایی بتواند در تجهیز اجرا شود و چه command هایی نتواند را می‌دهد.

در ادامه best practice هایی برای فعال کردن +TACACS در cisco IOS آمده است:

- AAA را با دستور عمومی aaa new-model فعال کنید. دستور aaa session-id common را برای حصول اطمینان از اینکه session id در همه‌ی packet های AAA در یک session نگهداری می‌شود، فعال نمائید.
- برای همه سرورهای AAA ، server groups را تعریف کنید. اگر امکان پذیر است برای هر سرور از یک کلید مجزا استفاده کنید. آدرس IP مبدا را برای ارتباطات +TACACS تنظیم کنید، ترجیحاً از آدرس IP مربوط به management interface out-of-band (OOB) یا loopback استفاده کنید.
- یک لیست از روش‌های login authentication تعریف کنید و آن را به console ، VTY و همه access line های استفاده شده اعمال کنید. از +TACACS به عنوان روش اصلی و از local authentication به عنوان روش جایگزین استفاده نمائید. فراموش نکنید که یک کاربر محلی برای روش جایگزین محلی تعریف کنید.
- فعال شدن دسترسی را با +TACACS ، احراز هویت[1] و از local enable به عنوان روش جایگزین استفاده نمائید. یک TACACS+ enable password برای هرکاربر پیکربندی کنید.
- exec authorization را برای اطمینان از اینکه دسترسی فقط برای کاربرانی امکان پذیر است که پروفایلشان با دسترسی مدیریتی تنظیم شده است، پیکربندی کنید. پروفایل‌های +TACACS با ویژگی shell (exec) پیکربندی می‌شوند.
- متد جایگزین تعریف کنید: اگر local username ها با سطوح دسترسی تعریف شده‌اند از local استفاده کنید و اگر authenticate شده است از دیگری استفاده کنید. برای اعمال فعال شدن

[1] Authenticate

دسترسی به صورت خودکار در +TACACS، پروفایل گروه یـا کـاربر را بـا تنظـیم کـردن privilege level آن روی ۱۵ پیکربندی کنید.

- Console authorization را اعمال کنید: به طـور پـیش فـرض authorization روی پـورت console اعمال نشده است. یک پیشـنهاد خـوب ایـن اسـت کـه console authorization را بـا aaa console authorization command فعال کنید تا این اطمینان حاصل شود که دسترسی فقط بـه کـاربران بـا سطح دسترسی مدیریتی داده شده است.
- دستور authorization را برای سطح دسترسی ۱۵ فعال کنید: به طور پیش فرض، دسترسـی مـدیریتی به IOS سطح دسترسی ۱۵ دارد. Command authorization را برای سطح دسترسی ۱۵ یا هرچیـز دیگری، اگر تعریف شده است ، فعال کنید.
- Exec accounting را برای مانیتور کردن اتصالات shell فعال کنید.
- دستور accounting را برای سطوح دسترسی که باید استفاده شود فعال کنید. System accounting را برای system-level events فعال کنید.

توجه: فعال کردن دسترسی می‌تواند به طور اتوماتیک به عنوان نتیجه‌ای از exec authorization انجام شـود. به این منظور، پروفایل‌های گروه یا کاربر +TACACS نیاز بـه پیکربنـدی دارنـد تـا سـطح دسترسـی روی ۱۵ تنظیم شود. Console Access ممکن است هنوز نیازمند اسـتفاده از یـک رمـز عبـور فعـال باشـد. در صـورت استفاده از cisco secure Access Control Server (ACS) ، هر کاربر با یک پسـورد فعـال خـاص مـی‌توانـد پیکربندی شود.

قطعه پیکربندی زیر استفاده از +TACACS را نشان می‌دهد:

```
! Enable AAA
aaa new-model
!
! Ensure common session ID
aaa session-id common
!
! Define server attributes
tacacs-server host <TAC+server۱> single-connection key <strong-key>
```

```
tacacs-server host <TAC+server۲> single-connection key <strong-key>
!
! Define server group
aaa group server tacacs+ <AAA-group>
server <TAC+server۱>
server <TAC+server۲>
!
! Define the source interface to be used to communicate with the TACACS+ servers
ip tacacs source-interface <Loopback or OOB interface>
!
! Set method list to enable login authentication
aaa authentication login <authen-exec-list> group <AAA-group> local-case
!
! Authenticate enable access
aaa authentication enable default group <AAA-group> enable
!
! Define method list to enforce exec authorization
aaa authorization exec <author-exec-list> group <AAA-group> if-authenticated
!
! Enforce console authorization
aaa authorization console
!
! Define method list to authorize the execution of administrative level commands
aaa authorization commands ۱۵ <author-۱۵-list> group <AAA-group> none
!
! Enable accounting
aaa accounting send stop-record authentication failure
aaa accounting exec default start-stop group <AAA-group>
aaa accounting commands ۱۵ default start-stop group <AAA-group>
aaa accounting system default start-stop group <AAA-group>
!
! Enforce method lists to console and vty access lines
line con ۰
 login authentication <authen-exec-list>
!
line vty ۰ ۴
```

```
authorization exec <author-exec-list>
login authentication <authen-exec-list>
authorization commands ۱۵ <author-۱۵-list>
!
```

امن‌سازی دسترسی مدیریتی

Best practice های زیر را برای امن‌سازی دسترسی مدیریتی دنبال کنید:

- دسترسی به SSH را زمانی که در دسترس است، به جای telnet که غیرامن است فعال کنید. از طول کلید حداقل ۲۰۴۸-bit استفاده کنید.
- دسترسی به HTTP را غیرفعال سازید. اگر ممکن است به جای HTTP که clear text را منتقل می‌کند از HTTPS استفاده کنید.
- Access line های غیرضروری را غیرفعال کنید. پورت‌های بدون استفاده را با no exec command غیرفعال کنید.
- در هر line استفاده شده، به صورت صریح پروتکل‌هایی را تعریف کنید که برای sessionهای ورودی و خروجی مجاز شده‌اند. محدود کردن session های خروجی از استفاده شدن host به وسیله مهاجم‌های دیگر جلوگیری می‌کند.
- از ACLs به منظور کنترل مبدا برای اینکه مشخص شود کدام session ها مجوز دارند، استفاده کنید. از extended ACL ها هم زمانی که دردسترس هستند استفاده کنید.
- برای اطمینان از اینکه VTY فقط به وسیله سیستم‌های شناخته شده و قابل اعتماد می‌تواند مورد دسترسی قرار بگیرد، یک access-class پیکربندی کنید.
- Idle and session timeout ها را در همه line های استفاده شده تنظیم کنید. TCP keepalive را برای شناسایی و بستن session های رها فعال کنید.

توجه: دسترسی HTTP از Default login authentication و default exec authorization استفاده می‌کند. به علاوه، سطح دسترسی برای کاربر باید روی ۱۵ تنظیم شود.

توجه: CS-MARS SSH device discovery از کلیدهای ۵۱۲ بیتی پشتیبانی نمی‌کند، برای سازگاری از طول کلید برابر یا بزرگتر از ۷۶۸ بیت استفاده کنید.

قطعه‌های پیکربندی زیر best practice ها برای فعال سازی SSH access را نشان می‌دهند:

```
! Prevent hung sessions in case of a loss of connection
service tcp-keepalives-in
!
! Define access class ACL to be used to restrict the sources of SSH sessions.
access-list <ACL#١> remark ACL for SSH
access-list <ACL#١> permit tcp <NOC-subnet١> <inverse-mask> any eq ٢٢
access-list <ACL#١> permit tcp <NOC-subnet٢> <inverse-mask> any eq ٢٢
access-list <ACL#١> deny ip any any log-input
!
! ACL for last resort access
access-list <ACL#٢> permit tcp host <management-station> any eq ٢٢
access-list <ACL#٢> deny ip any any log-input
! Configure a hostname and domain name
 hostname <hostname>
ip domain-name <domain-name>
!
! Generate an RSA key pair, automatically enabling SSH.
crypto key generate rsa
!
! SSH negotiation timeout of ٣٠ seconds
ip ssh timeout ٣٠
!
! SSH authentication attempts of ٢ before an interface reset
ip ssh authentication-retries ٢
!
! Enforce line access class ACL, access methods and timeouts for VTYs ٠ to ٣.
line vty ٠ ٣
access-class <ACL#١> in
!
! Incoming access via SSH only
```

```
transport input ssh
!
! No outgoing connections permitted
transport output none
!
! Incoming access not permitted if the request does not specify the transport protocol
transport preferred none
!
! Idle timeout of ۳ minutes
session-timeout ۳
!
! EXEC timeout of ۳ minutes
exec-timeout ۳ ۰
!
! Enforce access of last resource on VTY ۴.
line vty ۴
access-class <ACL□۲> in
transport input ssh
transport output none
transport preferred none
session-timeout ۳
exec-timeout ۳ ۰
 !
```

قطعه‌های پیکربندی زیر best practice ها برای فعال سازی HTTPS access را نشان می‌دهد:

```
! Enforce default login authentication and exec authorization
aaa authentication login default group <AAA-group> local-case
aaa authorization exec default group <AAA-group> local
!
! Define ACL to control the sources for HTTPS sessions
access-list <ACL#> permit <NOC-subnet> <inverse-mask>
access-list <ACL#> deny any log
!
! Disable HTTP and enable HTTPS
```

```
no ip http server
ip http secure-server
!
! Enforce HTTPS ACL and enable AAA
ip http access-class <ACL#>
ip http authentication aaa
!
! Restrict access to telnet. HTTPS access mode uses they telnet keyword.
line vty ۰ ۴
transport input telnet
```

Best practice های زیرساخت مسیریابی

مسیریابی یکی از مباحث مهم شبکه می‌باشد و حفظ امنیت آن از اهمیت بالایی برخوردار است. مسیریابی در معرض خطرها و حملات گوناگونی است، از تزریق به‌روزرسانی‌های غیر مجاز در جدول مسیریابی گرفته تا حملات DOS که مخصوصاً برای مختل کردن عملیات مسیریابی طراحی شده‌اند. اهداف این حملات می‌توانند مسیریابها، نشست‌های فعال و یا اطلاعات مسیریابی باشند. الگوهای طراحی cisco safe از اقدامات زیر برای امن‌سازی موثر routing plane استفاده می‌کند:

- محدود کردن عضویت در پروتکل مسیریابی: محدود کردن routing session ها به همسایه‌های نظیر قابل اعتماد، منابع معتبر و درستی routing update ها.
- کنترل انتشار مسیر: اعمال فیلترهای مسیر برای اطمینان از اینکه فقط اطلاعات مسیریابی معتبر انتشار می‌یابند. اطلاعات مسیریابی مبادله شده بین همسایه‌های نظیر و بین فرایندهای توزیع مجدد را کنترل کنید.
- ثبت کردن تغییرات وضعیت: تغییرات وضعیت session های همسایه یا مجاور را ثبت کنید.

محدود کردن عضویت در routing protocol

بسیاری از پروتکل‌های مسیریابی پویا دارای یک مکانیزم خودکار برای شناسایی مسیریاب‌های همسایه خود می‌باشند. به طور پیش فرض این مکانیزم تمام مسیریاب‌های مجاور را قابل اعتماد فرض می‌کند، در صورتی که می‌تواند این‌گونه نباشد. IOS سیسکو با در اختیار قرار دادن امکاناتی که در زیر آورده شده است، می‌تواند به برقراری ارتباطات فقط با همسایه‌های مجاور و مورد اعتماد منجر شود:

- احراز هویت همسایه[1] به منظور اطمینان از اعتبار همسایه مسیریابی و صحت آپدیت‌های مسیریابی آن‌ها مورد استفاده قرار می‌گیرد. برای BGP، IS-IS، OSPF، RIPv۲ و EIGRP از Message Digest authentication Algorithm Version ۵ (MD۵) به جای plain text authentication که ناامن است استفاده کنید. برای عمل کردن به طور مناسب، احراز هویت همسایه باید در هر دو سمت routing session انجام شود.
- از دستور passive-interface default در محدوده‌هایی از شبکه که تعداد زیادی از اینترفیس‌ها در محدوده مسیریابی قرار گرفته باشند، استفاده کنید. در حقیقت، زمانی که نخواهیم برخی از اینترفیس‌ها در شبکه تبادل ارتباط با دیگر همسایگان داشته باشند از این دستور استفاده می‌گردد. دستور passive interface default ، منطق پیکربندی را به default passive تغییر می‌دهد مگر اینکه اینترفیس صریحاً با no-passive interface command پیکربندی شده باشد. در این صورت آن اینترفیس اجازه انتشار آپدیت‌های مسیریاب در یک اینترفیس که انتظار می‌رود بخشی از فرایند مسیریابی باشد را نمی‌دهد.
- زمانی که از BGP استفاده می‌کنید، TTL security check که به عنوان Generalized ttl security mechanism (GTSM, RFC ۳۶۸۲) شناخته می‌شود را فعال کنید. TTL security check از routing-based Dos attack و همچنین حملات session reset و unauthorized peering که از سوی سیستم‌هایی هدایت می‌شود که به طور مستقیم در یک subnet به مسیریاب قربانی وصل نشده‌اند، جلوگیری می‌کند. به منظور عملکرد صحیح، TTL security check بایستی در هر دو انتهای BGP session پیکربندی شود.

توجه: تاثیرات دستور passive-interface باتوجه به نوع پروتکل‌های مسیریابی، متفاوت است. در RIP و IGRP ، passive- interface مسیریاب را از ارسال آپدیت‌ها به اینترفیس‌های انتخاب شده باز می‌دارد ولی

[1] Neighbor authentication

مسیریاب به گوش‌دادن و پردازش آپدیت‌های دریافت شده از همسایه‌های آن اینترفیس ادامه می‌دهد. در EIGRP و OSPF، دستور passive-interface از استقرار session های همسایه در اینترفیس‌های انتخاب شده جلوگیری می‌کند. بنابراین از انتشار آپدیت‌های مسیریابی جلوگیری و مانع از دریافت routing update های ورودی می‌شود.

توجه: TTL security check باید در هر دو انتهای peering session فعال شود وگرنه BGP session برقرار نمی‌شود.

قطعه پیکربندی زیر نحوه پیکربندی OSPF MD۵ neighbor authentication را نشان می‌دهد:

```
! OSPF MD۵ authentication
interface <interface-type/number>
ip ospf message-digest-key <key-number> md۵ <strong-password>
!
router ospf <process>
network <network> <mask> area <area-number>
      area < area-number> authentication message-digest
```

نحوه پیکربندی EIGRP MD۵ neighbor authentication در ادامه آمده است:

```
key chain <key-chain-name>
 key ۱
 key-string <strong-password>
 !
 interface <interface-type/number>
 ip authentication mode eigrp <process> md۵
 ip authentication key-chain eigrp <process> <key-chain-name>
!
 router eigrp <process>
 network <network>
 !
```

نحوه پیکربندی BGP MD۵ neighbor authentication را می‌توانید در ادامه مشاهده نمایید:

```
router bgp <AS>
no synchronization
bgp log-neighbor-changes
network <network>
neighbor <peer-IP-address> remote-as <AS>
neighbor <peer-IP-address> password <strong-password>
!
```

در cisco IOS، TTL security check برای هر peer با دستور neighbor ttl-security می‌تواند فعال شود:

```
router bgp as-number
neighbor ip-address ttl-security hops hop-count
```

کنترل انتشار مسیر

Route filtering ابزار مهم دیگری برای امن‌سازی تجهیزات مسیریابی است. اغلب پروتکل‌های مسیریابی از route filter به منظور جلوگیری از انتشار مسیر خاص پشتیبانی می‌نمایند. از آن‌جایی که این فیلترها مانع از انتشار شبکه‌های مورد نظر شده (برای مثال شبکه های با فضای آدرس خصوصی نباید در خارج از اینترنت منتشر شوند (RFC ۱۹۱۸)) و تنها امکان انتشار شبکه‌های موجه و درست را فراهم می‌سازند، از لحاظ امنیتی می‌توانند بسیار مؤثر باشند. Route filtering می‌تواند به دو نوع تقسیم شود: "فیلترکردن اطلاعات مسیرهای مبادله شده بین مسیریاب‌های همسایه" و نیز "فیلترکردن اطلاعات مسیریابی مبادله شده بین فرآیندهای مسیریابی در حالت redistribution درون یک مسیریاب".

- پیاده‌سازی peer prefix filtering در edge ها: فیلترهای ورودی[۱] را به منظور اطمینان از اینکه فقط مسیرهای مورد انتظار به شبکه معرفی شده‌اند در edge ها قرار دهید. بایستی یک تعادلی بین حداکثر میزان کنترل و بار عملیاتی تجهیز ایجاد گردد. فیلترها را در edge هایی قرار دهید که به احتمال زیاد اطلاعات مسیریابی نامعتبر به آن معرفی می‌شود (مثلاً WANedge). کنترل آپدیت‌های مسیریابی ورودی در WAN edge نه‌تنها فقط مانع از معرفی مسیرهای جعلی در branchها شده، بلکه مانع از آن می‌شود که زیرساخت به یک شبکه ترانزیت بدل شود.

[۱] Inbound filter

- اگر توزیع مجدد مسیر (redistribution) نیاز باشد، فیلترهای توزیع مجدد بایستی به منظور کنترل انتشار مسیرها فعال گردد. تنظیم فیلترهای توزیع مجدد مسیر، به محدود نگه داشتن تاثیرات تزریق بالقوه[۱] مسیرهای نامعتبر و جلوگیری از loop کمک و به پایداری شبکه یاری می‌رساند.
- Route filter را در stub router ها اعمال کنید.
- ثبت رخدادهای همسایه[۲]: ثبت تغییرات وضعیت session های همسایه را در همه مسیریاب‌ها فعال کنید.

مثال زیر استفاده از فیلترهای داخلی[۳] در WAN edge را نشان می‌دهد:

```
! Incoming route filter applied at the WAN edge and that only allows the branch subnet.
!
router eigrp <process>
network <network>
distribute-list ۳۹ in <interface-type/number>
!
 access-list ۳۹ permit <remote-subnet> <inverse-mask>
```

درصورت استفاده از EIGRP، از دستور eigrp stub connected به منظور اطمینان از انتشار شبکه‌هایی که به‌طور مستقیم متصل شده‌اند، استفاده نمایید:

```
router eigrp <process>
network <network>
 eigrp stub connected
```

اگر از پروتکل‌های دیگر استفاده می‌کنید، توصیه می‌شود از فیلترهای خروجی استفاده نمایید:

```
! Outbound route filter applied at the branch router.
 !
 router ospf <process>
distribute-list ۳۳ out <interface-type/number>
!
```

---

[۱] Potential injection

[۲] Neighbor logging

[۳] Inbound filter

access-list ۳۳ permit <branch-subnet> <inverse-mask>

مثال زیر استفاده از route-map با استفاده از دستور redistribute را نشان می‌دهد. در این مثال، مسیرها بین EIGRP و RIP توزیع مجدد می‌شوند. route-map rip-to-eigrp از وارد شدن شبکه ۱۰.۰.۰.۰/۸ به EIGRP جلوگیری می‌کند. به طور مشابه route-map rip-to-eigrp از وارد شدن شبکه ۲۰.۰.۰.۰/۸ به RIP جلوگیری می‌کند.

route-map rip-to-eigrp deny ۱۰

match ip address ۱

route-map rip-to-eigrp permit ۲۰

!

route-map eigrp-to-rip deny ۱۰

match ip address ۲

route-map eigrp-to-rip permit ۲۰

!

router eigrp ۱۰۰

network ۱۰.۰.۰.۰

redistribute rip route-map rip-to-eigrp

!

router rip

network ۲۰.۰.۰.۰

redistribute eigrp ۱ route-map eigrp-to-rip

!

access-list ۱ permit ۱۰.۰.۰.۰ ۰.۲۵۵.۲۵۵.۲۵۵

access-list ۲ permit ۲۰.۰.۰.۰ ۰.۲۵۵.۲۵۵.۲۵۵

ثبت تغییرات وضعیت

تغییرات وضعیت همسایه به طور مکرر (up یا down یا ریست شدن) از مشکلات رایج در ارتباطات شبکه و از عوامل ناپایداری شبکه‌ها بوده که بایستی همواره مورد توجه قرار گیرد. همچنین این امر ممکن است عامل

حملات مداوم در برابر تجهیزات شبکه باشد. ثبت تغییرات وضعیت session همسایه، یک راه‌کار مناسب به منظور شناسایی این مشکلات بوده و امکان عیب‌یابی را فراهم می‌سازد.

در اغلب پروتکل‌های مسیریابی، ثبت و ردگیری پیام تغییر وضعیت[1] به صورت پیش فرض فعال است. در این صورت هر زمانی که یک router session ، up یا down یا ریست شود مسیریاب یک log message را تولید می‌کند. اگر syslog فعال باشد، پیام به syslog server هدایت می‌شود در غیر این صورت در بافر داخلی مسیریاب نگه داشته می‌شود.

ثبت پیام تغییر وضعیت به طور پیش فرض در BGP غیرفعال است. برای فعال کردن آن از bgp log-neighbor-changes router استفاده می‌شود. به طور پیش فرض، EIGRP و OSPF تغییرات وضعیت را ذخیره می‌کنند. در غیر این صورت با استفاده از دستور eigrp log-neighbor-changes router برای EIGRP و دستور log-adjacency-changes router برای OSPF فعال می‌شود.

مثال زیر تغییرات همسایه برای BGP را در مد پیکربندی مسیریاب ذخیره می‌کند:

```
router bgp ۱۰
 bgp log-neighbor-changes
```

Best practice ها برای انعطاف‌پذیری و پایداری تجهیزات

مسیریاب‌ها و سوئیچ‌ها ممکن است به صورت مستقیم یا غیرمستقیم در معرض حملاتی که برای آن ها طراحی شده اند قرار گیرند. این حملات شامل DOS برپایه ی پروتکل‌های مجاز یا غیرمجاز، DDos، flood attacks، دسترسی غیرمجاز و... می‌باشد. در این بخش به مجموعه ای از best practice ها که در واقع به حفظ انعطاف‌پذیری و بقای مسیریاب‌ها و سوئیچ‌ها و همچنین در دسترس بودن شبکه حتی در حین حمله، کمک می‌کنند، اشاره شده است:

- غیرفعال کردن سرویس‌های غیرضروری
- محافظت از زیرساخت با استفاده از ACLs

[1] Status change message logging

- Control plane policing(COPP)
- امنیت پورت
- افزونگی

غیرفعال کردن سرویس‌های غیرضروری

به منظورکمک به راه‌اندازی و فعالیت در اغلب محیط‌های شبکه، مجموعه‌ای از سرویس‌ها بر روی مسیریاب‌ها و سوئیچ‌ها فعال است. البته به دلیل آن‌که همه شبکه‌ها نیازهای یکسانی ندارند بعضی از این سرویس‌ها ممکن است مورد نیاز نباشد. بنابراین می‌توان آن‌ها را غیرفعال کرد. غیرفعال کردن این سرویس‌های غیرضروری از دو جهت مفید خواهد بود: به حفظ منابع سیستم کمک می‌کند، پتانسیل سواستفاده‌های امنیتی را کم می‌نماید.

توجه: به عنوان یک راه‌کار، دستور auto secure CLI این امکان را فراهم می‌سازد که سرویس‌های غیرضروری غیرفعال شده در حالی‌که سایرسرویس‌های امنیتی فعال هستند.

توجه: قبل از اینکه یک سرویس را غیرفعال کنید، اطمینان حاصل کنید که آن سرویس مورد نیاز نیست.

بعضی از best practice های عمومی در این زمینه در ادامه آمده است:

- پورت های باز را شناسایی کنید: می‌توانید از دستور show control-plane host open-ports استفاده کنید تا متوجه شوید که مسیریاب به چه پورت‌های UDP/TCP گوش می‌دهد و متوجه شوید که کدام سرویس‌ها باید غیرفعال شوند.
- بعضی از سرویس‌های عمومی به طور پیش فرض غیر فعال هستند: مطمئن شوید که finger، identification(identd) و tcp and udp small servers به طور پیش فرض غیرفعال شده‌اند.
- بعضی از سرویس‌های عمومی به طور پیش فرض فعال هستند: به جز در مواقع مورد نیاز، BOOTP، IP source routing و سرویس‌های PAD را در همه‌ی مسیریاب‌ها به طور کلی غیرفعال کنید.
- IP directed broadcast: اطمینان حاصل کنید که directed broadcast در همه اینترفیس‌ها غیرفعال است.

- غیرفعال کردن CDP: CDP را برای اینترفیس‌هایی که در معرض خطر هستند غیرفعال کنید. برای مثال در اینترفیس‌های خارجی[1] مانند آن‌هایی که در edge اینترنت هستند و همچنین پورت‌های مختص به دیتا در لایه دسترسی (Access)
- پورت های دسترسی و externally facing: به جز در موارد مورد نیاز، MOP، IP redirect و proxy ARP را در تمامی دسترسی‌ها و اینترفیس‌های externally-facing غیرفعال کنید. این پورت‌ها شامل پورت‌های دسترسی[2] در campus ها و branch ها و همچنین پورت‌های externally-facing مانند آن‌هایی که در edge اینترنت هستند، می‌باشد.

در ادامه یک مثال برای اشاره به نحوه استفاده از دستور control-plane host open-ports آورده شده است:

```
cr۱۸-۷۲۰۰-۳show control-plane host open-ports
Active internet connections (servers and established)
Prot      Local Address   Foreign Address          Service                State
tcp       *:۲۲            *:۰                      SSH-Server             LISTEN
tcp       *:۲۳            *:۰                      Telnet                 LISTEN
tcp       *:۶۳۷۷۱         ۱۷۲.۲۶.۱۵۰.۲۰۶:۴۹        IOS host services      ESTABLIS
udp       *:۴۹            ۱۷۲.۲۶.۱۵۰.۲۰۶:۰                 TACACS service
LISTEN
udp       *:۶۷            *:۰                      DHCPD Receive          LISTEN

cr۱۸-۷۲۰۰-۳
```

توجه: دستور control-plane host open-ports در cisco IOS release ۱۲.۳(۴)T معرفی شده است. در نسخه‌های قبلی از دستور show ip sockets برای شناسایی پورت‌های باز UDP استفاده کنید و همچنین از دستورهای show tcp brief all و show tcp tcb برای شناسایی پورت های باز tcp استفاده کنید.

[1] External interface

[2] Access line

```
! Global Services disabled by default
no ip finger
no ip identd
no service tcp-small-servers
no service udp-small-servers
!
! Disable BOOTP, IP Source Routing and PAD global services
no ip source-route
no ip bootp server
no service pad
! Disable IP directed broadcasts on all interfaces
interface <interface-type/number>
no ip directed-broadcast
```

برای اینکه مطمئن شوید CDP در یک اینترفیس غیرفعال است از دستور show cdp interface استفاده کنیـد.
همچنین برای غیرفعال کردن آن از no cdp enable استفاده کنید.

در مثال زیر، CDP در اینترفیس FastEthernet ۲/۱ فعال است و در FastEthernet ۲/۰ غیرفعال شده است:

```
Router#show cdp interface FastEthernet ۲/۱
FastEthernet۲/۱ is up, line protocol is up
Encapsulation ARPA
Sending CDP packets every ۶۰ seconds
Holdtime is ۱۸۰ seconds
Routershow cdp interface FastEthernet ۲/۰
Router#
Router #sh run int fastEthernet ۲/۰
Building configuration...
Current configuration: ۱۶۳ bytes
!
interface FastEthernet۲/۰
ip address ۱۹۸.۱۳۳.۲۱۹.۵ ۲۵۵.۲۵۵.۲۵۵.۰
no cdp enable
end
! Disable MOP, IP Redirects,
interface <interface-type/number>
```

```
no mop enabled
no ip redirects
no ip proxy-arp
```

ACL های حفاظت از زیرساخت (iACLs)

(iACLs) یک تکنیک کنترل دسترسی است که از زیرساخت شبکه در برابر حملات داخلی و خارجی محافظت می‌کند. در حقیقت iACLs از نوع Extended ACL هستند که به منظور کنترل ترافیک مدیریتی و کنترلی وابسته به تجهیزات زیرساخت مثل سوئیچ‌ها و مسیریاب‌ها مورد استفاده قرار گرفته و مانع از عبور هر ترافیک دیگری به سمت فضای آدرس زیرساخت می‌شود. برای مثال یک iACL که در یک ISP peering edge تنظیم شده تا به BGP session هایی که از peer های شناخته شده مجوز دهد در حالیکه جلوی هر ترافیک دیگری که به سمت peering router های ISP و باقی‌مانده فضای آدرس زیرساخت می‌رود را می‌گیرد.

بیشترین استفاده iACLها در edge شبکه است که زیرساخت در دسترس کاربران داخلی و خارجی قرار می‌گیرد و نیز در مرزهای مدیریتی که تجهیزات یا لینک‌ها تحت مدیریت‌های مختلف قرار می‌گیرند. در یک شبکه سازمانی، iACLs ممکن است در بسیاری از edgeهای شبکه فعال گردد:

- WAN edge: زیرساخت core را از تهدیدات ممکن که از سوی remote branch office یا partner location ها می‌آید حفظ می‌کند.
- دسترسی به campus/branch: زیرساخت را از تهدیدات ممکن که از LAN ها ناشی می‌شود، محافظت می‌کند.
- Internet edge: فیلترهای edge ممکن است به گونه‌ایی طراحی شده باشند که مانند یک iACL عمل کنند تا از زیرساخت در برابر تهدیدات خارجی محافظت کنند.

اگرچه یک ساختار رایج برای ایجاد iACL ها وجود دارد ولی ACLهای واقعی به طور چشمگیری با توجه به محیط تفاوت دارند. یک iACL که بدون درک صحیحی از پروتکل‌ها و تجهیزات تنظیم شده باشد، به شدت ناکارآمد بوده و حتی ممکن است شرایط self-inflecting Dos را فراهم کند. iACL فقط زمانی باید اعمال شود که فهم درستی نسبت به پروتکل‌ها و پورت‌هایی که به طور قانونی به وسیله‌ی زیرساخت استفاده می‌شوند، به وجود آمده باشد. همچنین پیشنهاد می‌شود که در ابتدا با یک relaxed iACL شروع کنید و سپس همان‌طور که تاثیرات iACL مانیتور می‌شود، entryهای آن را تنظیم نمایید.

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. بنابراین control plane در روترها و سوئیچ‌ها از برخی حمله‌ها در امان می‌باشند (مانند حملات شناسایی و همینطور DoS مستقیم).

COPP برای تنظیم سیاست‌های مورد نظر از Mpdular QOS command-line interface (MQC) استفاده می‌کند. MQC امکان تفکیک ترافیک به کلاس‌های مجزا را فراهم نموده و به کاربر اجازه تعریف و اعمال سیاست‌های QOS مجزا به هر کلاس را می‌دهد. سیاست های QOS می‌تواند برای مجوز دادن یا drop کردن همه بسته‌ها یا drop کردن بسته‌هایی که سرعتشان بیشتر از یک مقدار مشخصی است، تنظیم می‌گردد. Copp برای محدوده وسیعی از platform های سیسکو در دسترس است که همه آن‌ها یک عملکرد پایه یکسان دارند. البته copp در بعضی از platform ها برای استفاده از مزایای معماری سخت‌افزاری خاصی ارتقاء پیدا کرده است. در نتیجه بعضی از platform ها فرم‌های پیشرفته copp را فراهم کرده اند. Platform های non-distributed یک مدل copp متمرکز[1] مبتنی بر نرم‌افزار را توسعه می‌دهند در حالیکه بعضی از platform های distributed نسخه های ارتقاء یافته‌ی COPP را فراهم می‌کنند. به علاوه به دلیل تفاوت‌های سخت‌افزاری، پشتیبانی پروتکل COPP ممکن است بسته به platform متفاوت باشد. مشابه iACLs، اگرچه یک ساختار رایج برای پیکربندی کلاس‌های COPP وجود دارد ولی سیاست‌ها و کلاس‌های واقعی بسته به محیط ممکن است به طور چشمگیری متفاوت باشند. پیاده‌سازی COPP بدون فهم درستی از پروتکل ها و تجهیزات ممکن است باعث ناکارآمدی شود و حتی شرایط self-inflecting DOS را فراهم نماید. سیاست های COPP فقط زمانی باید اعمال شود که فهم درستی نسبت به پروتکل‌ها و پورت‌هایی که به طور قانونی به وسیله‌ی زیرساخت استفاده می‌شوند، به وجود آمده باشد. همچنین پیشنهاد می‌شود که در ابتدا هیچ محدودیت سرعتی روی کلاس‌های ترافیک اعمال نگردد و همزمان با مانیتور کردن تاثیرات COPP به تدریج آن‌ها را پیکربندی نمود.

[1] Centralized software-based copp model

Port Security

به منظور مقابله با حملات منع دسترسی در لایه دو مانند MAC flooding برای ایجاد MAC address table exhaustion و یا حملات content addressable memory(CAM) overflow لایه ی دو از قابلیت port security در سوئیچ‌های سیسکو استفاده می‌شود. port security با محدود کردن آدرس های MAC که مجوز ارسال ترافیک به یک پورت مشخص را دارند، این حملات را مرتفع می‌سازد. وقتی port security روی یک پورت فعال می‌شود، فقط بسته‌های با آدرس MAC منبع مجاز اجازه دارند که از پورت عبور نمایند. منظور از آدرس MAC مجاز ، آدرس MAC امن شده است.

Port security یک لیست از آدرس های MAC امن شده را به یکی از دو طریق زیر می سازد:

- Dynamic learning of MAC address تعداد بیشینه‌ای از آدرس های MAC را که روی یک پورت learn شده و مجوز عبور دارند را تعریف می‌نماید. این روش برای محیط‌های پویا مانندaccess edge مفید است.
- Static configuration of MAC address آدرس MAC استاتیک مجاز روی یک پورت را تعریف می‌کند. این روش برای محیط‌های استاتیک مانند serverfarm ، lobby و Demilitarized network(DMZ) مفید است.

سناریوهای Deployment رایج شامل موارد زیر است:

- یک محیط پویا مانند یک access edge که بر روی یکی از پورت‌ها، Port security فعال شده و بیشینه تعداد آدرس‌های MAC آن برابر با ۱ تنظیم شده است. بنابراین فقط قادر است یک آدرس MAC را به طور پویا learn کرده و در غیر این‌صورت، عملیات پاسخ محافظتی را انجام دهد.
- یک محیط استاتیک و کنترل شده مانند serverfarm یا lobby که یک پورت ممکن است port security اش با آدرس MAC سرور یا کلاینت Lobby که به صورت استاتیک تعریف شده، فعال باشد.

- استقرار یک voice over ip(voip) که یک پورت ممکن است قابلیت port security با حداکثر تعداد آدرس MAC، سه تنظیم گردد. یک آدرس MAC برای ایستگاه کاری[1] مورد نیاز است و با توجه به سخت‌افزار یا نرم‌افزار سوئیچ ممکن است یک یا دو آدرس MAC برای تلفن مورد نیاز باشد.

در cisco IOS، Port security با استفاده از دستور switchport port-security روی یک اینترفیس می‌تواند فعال شود. مثال زیر dynamic port security را نشان می‌دهد که به دو MAC address محدود شده و به یک اینترفیس در حالت violation restrict اعمال شده است. این مثال می‌تواند در یک VOIP-enabled port اعمال شده باشد.

```
interface gigabitethernet۰/۱
switchport port-security maximum ۳
switchport port-security violation restrict
switchport port-security
switchport port-security aging time ۲
switchport port-security aging type inactivity
```

مثال زیر نشان می‌دهد که چگونه یک پورت فقط به وسیله آدرس MAC یک ماشین خاص می‌تواند محدود شود (مثلاً در یک محیط lobby).

```
interface gigabitethernet۰/۲
switchport port-security maximum ۱
switchport port-security mac-address ۱۰۰۰.۲۰۰۰.۳۰۰۰
switchport port-security violation restrict
switchport port-security
```

Redundancy

شبکه‌ها از چندین بخش نرم‌افزاری و سخت‌افزاری تشکیل شده اند که ممکن است دچار اختلال شده و یا در معرض حمله قرار گیرند. پیاده‌سازی طراحی‌های افزونه به برطرف کردن single point of failure کمک می‌کند.

[1] Work station

همچنین در دسترس بودن شبکه را بهبود بخشیده و آن را در برابر حملات مقاوم می‌نماید. به منظور پیاده‌سازی redundancy راه‌های مختلفی از یک اینترفیس پشتیبان گرفتن ساده تا ساخت توپولوژی‌های افزونه کامل وجود دارد. واضح است افزونه‌کردن همه المان‌های شبکه هزینه بر خواهد بود. بنابراین فقط برای آن‌هایی افزونگی طراحی می‌گردد که بر طبق نیازمندی‌های منحصر به فرد شبکه مورد نظر بیشترین استفاده را دارند.

الگوهای طراحی cisco safe [1] با محدوده‌ی وسیعی از افزونگی‌ها ساخته شده است:

- اینترفیس‌های پشتیبان
- افزونگی عناصر: استفاده از پردازنده‌ها و ماژول‌های افزونه
- تجهیزات آماده به کار: اولین پروتکل‌های افزونگی مانند HSRP ، VRRP و GLBP.
- افزونگی توپولوژیکی: طراحی‌های ساخته شده با مسیرهای افزونه در هر دو لایه data-link و network.

network telemetry

به منظور راه اندازی و اطمینان از در دسترس بودن شبکه ضروری است که نسبت به اتفاقاتی که در هر زمانی در شبکه می‌افتد، آگاهی و دید داشته باشیم. Network Telemetry قابلیت‌های شناسایی مفید و گسترده‌ای را پیشنهاد می کند که با سیستم تجزیه و تحلیل اختصاصی برای جمع آوری، هدایت و برقراری ارتباط بین فعالیت‌های مشاهده شده می‌تواند هماهنگ شود.

Network telemetry ارزان بوده و پیاده‌سازی آن نیز نسبتاً آسان است. شکل‌های گوناگون telemetry در زیرساخت شبکه شامل موارد زیر است:

- همگام‌سازی زمان[2]
- آمارگان ترافیک تجهیزات محلی
- اطلاعات وضعیت سیستم
- Best practice های رایج CDP
- Syslog
- SNMP

[1] Cisco safe design blueprint

[2] Time synchronization

- ACL logging
- Accounting
- Archive configuration change logger
- Packet capture

همگام سازی زمان (NTP)

همگام سازی زمان برای تحلیل و ارتباط برقرار کردن بین اتفاقات ضروری است بنابراین فعال‌سازی NTP روی همه اجزای زیرساخت یک نیاز اساسی محسوب می‌گردد. به منظور راه‌اندازی NTP بایستی به موارد زیر توجه نمود:

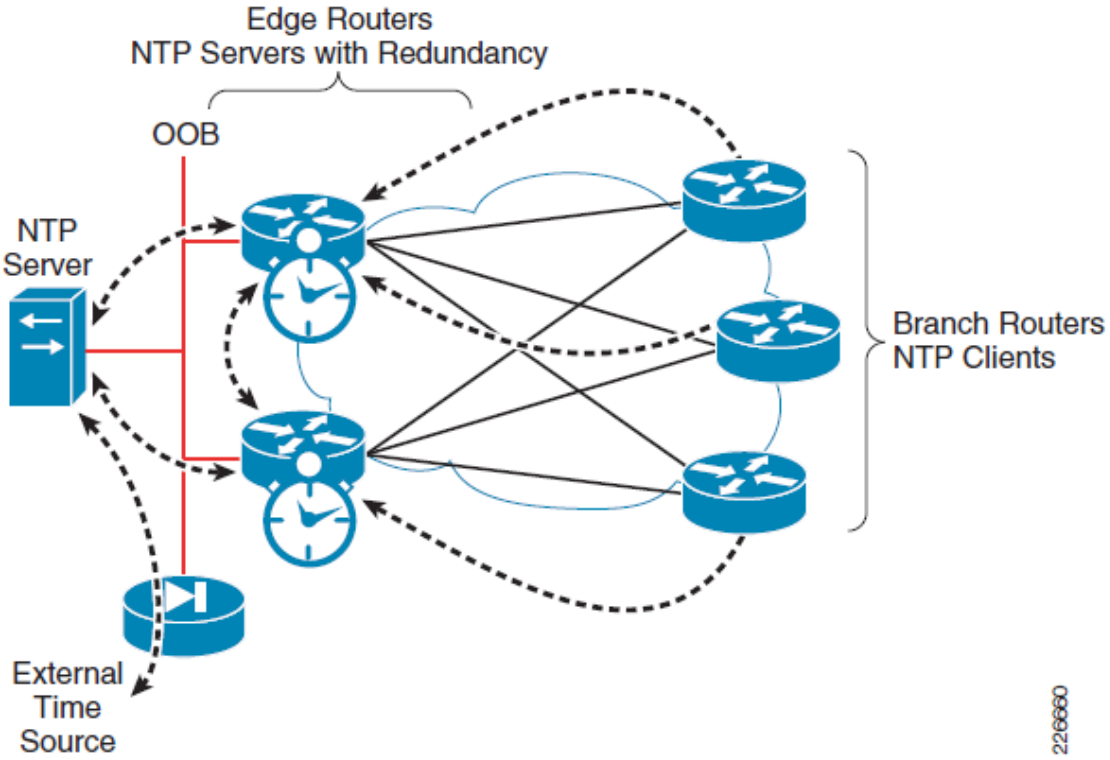
- یک طراحی NTP سلسله مراتبی به یک طراحی مسطح ترجیح داده می‌شود. طراحی سلسله‌مراتبی پایداری، مقیاس‌پذیری و نیز سازگاری بیشتری را فراهم می‌کند.
- در تمامی زیرساخت یک time zone رایج و مشخص را استفاده کنید تا آنالیز و ارتباط دادن اتفاقات آسان‌تر شود.
- کنترل کنید که کدام کلاینت ها و peer ها می‌توانند با یک NTP server صحبت کنند و NTP authentication را فعال کنید.

طراحی NTP برای remote offices

شعبه‌های یک office معمولاً در یک یا چند WAN edge router ادغام می‌شوند که این مسئله باید در طراحی NTP در نظر گرفته شود. در ادارات مرکزی معمولاً یک time server داخلی در یک ناحیه امن وجود دارد. علاوه براینکه یک ساعت GPS-based یا اتمیک داخلی وجود دارد، این time server های داخلی با time source های خارجی همگام خواهند شد. بعد از طراحی مسیریابی، مسیریاب‌های WAN edge با ارتباط کلاینت/سرور با time server های داخلی ممکن است به عنوان time server پیکربندی شوند. همچنین branch router ها با ارتباط کلاینت/سرور با مسیریاب‌های WAN edge می‌توانند به عنوان کلاینت پیکربندی شوند (سرورهای بدون زمان).

این طراحی در شکل ۱ به تصویر کشیده شده است.

Figure 2-1 NTP Design for the WAN Edge and Remote Offices



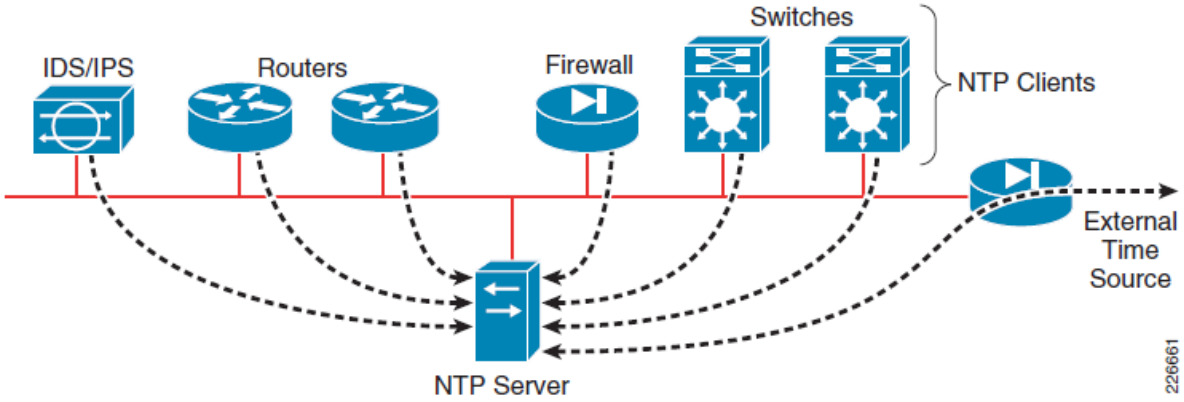
شکل ۱. طراحی NTP در اداره مرکزی[۱]

در ادارات مرکزی یا office اصلی، یک شبکه مدیریت OOB(Out-Of-Band) موجود می‌تواند مورد استفاده قرارگیرد. در این سناریو، همه مسیریاب‌ها و سوئیچ‌ها با ارتباط کلاینت/سرور با time server های داخلی که در یک ناحیه امن قرار گرفته‌اند، ممکن است به عنوان کلاینت‌ها (سرورهای بدون زمان) پیکربندی شوند. این time server های داخلی با time source های خارجی همگام[۲] شده‌اند. این طراحی در شکل ۲ نشان داده شده است.

[۱] Headquarter

[۲] synchronized

Figure 2-2 NTP Design Leveraging an OOB Management Network



شکل ۲. طراحی NTP در اداره مرکزی

قطعه پیکربندی زیر، پیکربندی NTP client را نشان می‌دهد:

```
! Enables timestamp information for debug messages
service timestamps debug datetime localtime show-timezone msec
!
! Enables timestamp information for log messages
service timestamps log datetime localtime show-timezone msec
!
! Sets the network-wide zone to GMT
clock timezone GMT ۰
!
! To periodically update the hardware clock, if present
ntp update-calendar
!
! Sets source IP address
ntp source <loopback or OOB interface>
!
! Defines servers
ntp server <NTP-Server۱>
ntp server <NTP-Server۲>
!
! Enables authentication
ntp authentication-key ۱۰ md۵ <strong-key>
```

ntp trusted-key ۱۰

ntp authenticate

قطعه پیکربندی زیر، پیکربندی NTP server را نشان می‌دهد:

```
! Enables timestamp information for debug messages
service timestamps debug datetime localtime show-timezone msec
!
! Enables timestamp information for log messages
service timestamps log datetime localtime show-timezone msec
!
! Sets the network-wide zone to GMT
clock timezone GMT ۰
!
! To periodically update the hardware clock, if present
ntp update-calendar
!
! Sets source IP address
ntp source <loopback or OOB interface>
!
!Restrict the IP addresses of the servers and peers this server will communicate with.
access-list <ACL۱> remark ACL for NTP Servers and Peers
access-list <ACL۱> permit <NTPpeer۱>
!
ntp access-group peer <ACL۱>
!
! Restrict the IP addresses of the clients that can communicate with this server.
access-list <ACL۲> remark ACL for NTP Client
access-list <ACL۲> permit <Client>
access-list <ACL۲> deny any log
!
ntp access-group serve-only <ACL۲>
!
! Enables authentication
ntp authentication-key ۱۰ md۵ <strong-key>
```

```
ntp trusted-key ۱۰
ntp authenticate
!
! Defines server and peer
ntp server <NTPserver۱>
ntp peer <NTPpeer۱>
```

آمار ترافیک تجهیزات محلی

آمار تجهیزات محلی پایه‌ای‌ترین و دردسترس‌ترین شکل از telemetry محسوب می‌شود که شامل اطلاعات پایه مانند آمار پهنای باند و نرخ‌گذردهی[۱] هر اینترفیس، آمار ترافیک هر پروتکل و ویژگی های فعال است.

در Cisco IOS، این اطلاعات از طریق CLI قابل دسترسی است. فرمت دستور و شکل خروجی و سایر ویژگی‌های آن، بسته به نوع platform متفاوت است.

آمار هر اینترفیس

در cisco IOS، آمار هر اینترفیس که شامل اطلاعات پهنای باند (bps) و نرخ‌گذردهی (pps) است، در دسترس می‌باشد. آمار هر اینترفیس با دستور show interface به سادگی قابل رؤیت خواهد بود.

مسیریاب‌های Cisco IOS به صورت پیش فرض از ۵-minute decaying average برای آمار اینترفیس استفاده می‌کنند. به منظور آن‌که آمار دقیق‌تری به دست آید می‌توان Decaying average را بر روی یک دقیقه تنظیم نمود. طول زمانی که برای محاسبه آمار اطلاعات استفاده می‌شود می‌تواند با استفاده از load-interval interface configuration command تغییر کند:

```
interface <interface-type number>
load-interval ۶۰
```

برای مشاهده‌ی سرعت one-minute input و one-minute output در یک اینترفیس:

```
Router#show interface <interface-type numer> | include ۱ minute
۱ minute input rate ۵۴۳۰۷۰۰۰ bits/sec, ۱۷۶۳۷ packets/sec
```

[۱] throughput

۱ minute output rate ۱۱۹۲۲۳۰۰۰ bits/sec, ۲۳۹۳۶ packets/sec

توجه: سرعت‌های بالای ورودی یا خروجی در یک زمان مشخص (مثلاً یک دقیقه) می‌تواند در شناسایی رفتارهای غیرعادی کمک‌رسان باشد.

لازم است counterهای اینترفیس به منظور بررسی‌های جدید پاکسازی گردد. البته قبل از آن بایستی در نظر داشته‌باشیم که اطلاعات مفید دور انداخته نشوند. برای پاک کردن counter های اینترفیس داریم:

Router#clear counters <interface-type number>

اطلاعات مبتنی بر IP برای هر اینترفیس

در Cisco IOS، Per-interface IP feature information اطلاعاتی را درباره ی خصوصیات IP پیکربندی شده برای هر اینترفیس فراهم می‌کند. این دستور به طور خاص برای شناسایی تعداد یا نام ACL های اعمال شده به منظور چک کردن ACL counter hit مفید است.

Per-interface IP feature information با استفاده از دستور show ip interface قابل رؤیت خواهد بود.

Router#show ip interface <interface-type number>

همچنین دستورshow ip interface آمار بسته‌های drop شده uRPF در هر اینترفیس را نشان می‌دهد:

Router#show ip interface <interface-type number> | include ۱ verification

!

Router#show ip interface FastEthernet ۲/۰| include verification

IP verify source reachable-via ANY

۷۹۴۴۰۷ verification drops

۱۸۷۴۴۲۸۱۲۹ suppressed verification drops

Global traffic IP statistic

در Cisco IOS، Global IP statistics اطلاعات مفید زیادی شامل Per-protocol count برای ICMP ، TCP ، UDP و ترافیک چندپخشی[1] را فراهم می‌کند. Global traffic IP statistics می‌تواند با استفاده از دستور show ip traffic مشاهده گردد.

این دستور برای عیب‌یابی کلی و همچنین شناسایی ناهنجاری‌ها خیلی مفید است.

Router#show ip traffic

همچنین دستور Show ip traffic آمار بسته‌های drop شده‌ی uRPF را نیز فراهم می‌کند و گزینه های آن می‌تواند برای دسترسی سریع به این اطلاعات استفاده شود:

Router#show ip traffic | include RPF
۰ no route, ۱۲۴۷۸۰۷۲۲ unicast RPF, ۰ forced drop

اطلاعات وضعیت سیستم (Memory ، cpu و process)

یک مسئله مهم و بالقوه در تجهیزات زیرساخت شبکه، پردازش‌های بالا می‌باشد. در Cisco IOS اطلاعات درباره بهره‌وری پردازنده با استفاده از دستور show processes cpu در یک پنجره ی ۵ ثانیه‌ای، یک دقیقه‌ای و ۵ دقیقه‌ای در دسترس است (شکل ۳).

```
Router#show processes cpu | exclude 0.00%__0.00%__0.00%
CPU utilization for five seconds: 38%/26%; one minute: 40%; five minutes: 43%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   5   192962596  13452649      14343  0.00%  0.52%  0.44%   0 Check heaps
  15   4227662201540855414        274  0.65%  0.50%  0.49%   0 ARP Input
  26   2629012683680473726         71  0.24%  0.29%  0.36%   0 Net Background
  50     9564564  11374799        840  0.08%  0.07%  0.08%   0 Compute load avg
  51    15291660    947844      16133  0.00%  0.03%  0.00%   0 Per-minute Jobs
  58    15336356  92241638        166  0.08%  0.02%  0.00%   0 esw_vlan_stat_pr
  67    10760516 506893631         21  0.00%  0.01%  0.00%   0 Spanning Tree
  68  31804659682556402094       1244  7.02%  7.04%  7.75%   0 IP Input
  69    25488912  65260648        390  0.00%  0.03%  0.00%   0 CDP Protocol
  73    16425564  11367610       1444  0.08%  0.02%  0.00%   0 QOS Stats Export
  81    12460616   1020497      12210  0.00%  0.02%  0.00%   0 Adj Manager
  82   442430400  87286325       5068  0.65%  0.73%  0.74%   0 CEF process
  83    68812944  11509863       5978  0.00%  0.09%  0.11%   0 IPC LC Message H
  95    54354632  98373054        552  0.16%  0.12%  0.13%   0 DHCPD Receive
  96    61891604  58317134       1061  1.47%  0.00%  4.43%   0 Feature Manager
```

[1] Multicast

شکل ۳. اطلاعات بهره‌وری پردازنده در بازه‌های زمانی مختلف

میزان مصرف بالای cpu برای فرآیند IP Input می‌تواند یک شاخص مناسب جهت تاثیر ترافیک ورودی و و خروجی در بار cpu در تجهیز مورد نظر باشد. همچنین بایستی توجه گردد، مبنای شناخت ناهنجاری در شبکه بر اساس شناخت دقیق از شبکه و وضعیت نرمال آن است.

اخطار آستانه[1] cpu و memory

Cisco IOS توانایی فرستادن اخطار زمانی که CPU و memory از یک حد آستانه تجاوز می‌کند را فراهم می‌کند:

- آستانه حافظه: به منظور اعلام هشدار در زمانی که میزان حافظه خالی در دسترس از یک آستانه مشخصی کمتر شود بایستی memory threshold syslog notification را فعال نمود. پیشنهاد می‌شود حد آستانه خالی‌بودن حافظه، بر روی ده درصد کل حافظه تنظیم گردد. از دستور show memory می‌توان به منظور مشاهده حافظه کل و میزان حافظه خالی موجود استفاده نمود.
- Critical system logging protection: وقتی یک مسیریاب به وسیله فرآیندها overload می‌شود، میزان حافظه دردسترس ممکن است به اندازه‌ای کم شود که حتی نتواند اخطارهای اساسی را نمایش دهد. بایستی یک ناحیه‌ی ۱۰۰۰ کیلوبایتی از حافظه برای فرستادن اخطارهای اساسی رزرو شود.
- Cpu threshold SNMP trap notification: ازدیاد بار cpu در سوئیچ ها و مسیریاب‌ها، می‌تواند بیانگر بروز یک اتفاق باشد. بنابراین پیشنهاد می‌شود فعال‌سازی اخطار در شرایط بالابودن cpu انجام گیرد. البته به یاد داشته باشید که بالابودن cpu همیشه نشان‌دهنده یک فعالیت مخرب نیست و منابع دیگر اطلاعات هم باید مورد توجه قرار بگیرند.

قطعه پیکربندی زیر مفاهیم بالا را نشان می‌دهد:

```
Router#show memory
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor ۶۵۷۲AD۰۰ ۹۱۵۲۳۱۳۴۸ ۲۷۰۰۹۸۷۶ ۸۸۸۲۲۱۴۷۲ ۳۷۴۷۲۱۳۹۶ ۳۶۱۵۸۳۲۲۰
```

[1] threshold

I/O C۰۰۰۰۰۰ ۶۷۱۰۸۸۶۴ ۵۸۵۶۵۰۰ ۶۱۲۵۲۳۶۴ ۶۱۲۳۳۸۰۸ ۶۱۲۳۲۰۲۸

…

Router#

کل حافظه‌ی پردازنده‌ی سیستم ۹۱۵۲۳۱۳۴۸ بایت است. بنابراین آستانه پردازنده روی ۹۱۵۲۳کیلوبایت تنظیم می‌شود. کل حافظه ی I/O سیستم ۶۷۱۰۸۸۶۴ بایت است بنابراین آستانه روی ۶۷۱۰ کیلوبیت تنظیم می‌شود:

memory free low-watermark processor ۹۱۵۲۳

memory free low-watermark io ۶۷۱۰

memory reserve critical ۱۰۰۰

snmp-server enable traps cpu threshold
snmp-server host <SNMP-station> traps <SNMP-community> cpu

system logging (syslog)

syslog اطلاعات عملیاتی ارزشمندی را شامل وضعیت سیستم، آمار ترافیک و اطلاعات دسترسی تجهیزات را فراهم می‌سازد. به همین دلیل، فعال‌سازی syslog در همه‌ی تجهیزات شبکه پیشنهاد می‌شود:

- گام اول: برای پیام‌های گزارش‌گیری و اشکال‌زدایی[۱]، timestamp را فعال کنید. اضافه کردن timestamp به پیام‌ها، آنالیز و ارتباط را تسهیل می بخشد.
- گام دوم: ثبت‌کردن پیام‌های سیستم در بافر محلی را فعال کنید. این کار، دسترسی به اطلاعات ذخیره شده را در زمان هایی که ارتباط با syslog server قطع شده است، به طور مستقیم از طریق مسیریاب یا سوئیچ فراهم می‌کند. لازم است بدانید که بافرهای محلی، به طور طبیعیcircular هستند. بنابراین بعد از اینکه بافر پر شد، پیام‌های جدیدتر، پیام‌های قدیمی‌تر را رونویسی می‌کنند.
- گام سوم: سطح اهمیت[۱] پیام‌ها بایستی مشخص شود. بنابراین تنها پیام‌هایی از یک سطح مشخصی کمتر هستند، گزارش می‌شوند. بهتر است برای سیستم‌های مهم یا سیستم‌هایی که بیشتر برای

[۱] debugging

کاربران remote یا خارجی در دسترس هستند مانند internet و WAN edge، گزارش‌های جزئی‌تری فراهم شود و برای بقیه زیرساخت فقط اخطارهای مهم و اساسی گزارش شود.

- گام چهارم: source ip address پیام‌های syslog را آدرس اینترفیس loopback یا اینترفیس OOB قرار دهید.
- گام پنجم: گزارش پیام‌ها به کنسول را غیرفعال کنید. بنابراین کنسول خالی از پیام باقی می‌ماند.

```
! Enable timestamps for debugging and logging messages.
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
! Enable system message logging to a local buffer.
logging buffered
!
! Logging for critical equipment.
logging trap informational
logging rate-limit ۱ except ۳
!
! Logging for non-critical equipment.
logging trap critical
!
! Define the syslog servers to be used.
logging facility <syslogserver>
!
! Set the source IP address of syslog messages.
 ! logging source-interface <loopback or OOB interface>
```

SNMP

SNMP یک فریم‌ورک استاندارد و یک زبان رایج برای مانیتورینگ و مدیریت تجهیزات شبکه را فراهم می‌کند. همچنین اطلاعات سیستمی و رویدادی باارزشی توسط این سرویس قابل دسترس خواهد بود. بنابراین فعال‌سازی آن در زیرساخت شبکه بسیار مهم است. نکته قابل توجه آنست که زمانی که نیازی به دسترسی به

[۱] Severity level

SNMP نیست، بایستی از غیرفعال بودن آن اطمینان حاصل کرد. دستور No SNMP- server همه نسخه‌های SNMP (SNMPv۱ , SNMPv۲c , SNMPv۳) در حال اجرا روی تجهیز را غیرفعال می‌کنند.

به منظور فعال‌سازی SNMP موراد زیر بایستی مدنظر قرار گیرد:

- گام اول: سیستم‌هایی که به SNMP در حال اجرا روی مسیریاب‌ها و سوئیچ‌ها دسترسی دارند را محدود کنید. بایستی تا حد ممکن دقت را رعایت کرد. برای مثال فقط به SNMP management station ها اجازه دسترسی دهید.
- گام دوم: اگر از SNMPv۳ (توصیه می‌شود) استفاده می‌کنید، یک SNMP view را اعمال کنید که دانلود از full ip routing و ARP table را محدود کند.
- گام سوم: اگر SNMPv۳ پشتیبانی شده است، فقط SNMPv۳ با بالاترین سطح امنیت که توسط مدیران SNMP پشتیبانی شده است را فعال کنید و همچنین هرجا که امکان پذیر است از ارتباطات رمز شده (priv) استفاده کنید.
- گام چهارم: آدرس IP منبع SNMP trap ها را آدرس اینترفیس loopback یا اینترفیس OOB قرار دهید.

مثال پیکربندی زیر برای محدودکردن دسترسی SNMPv۱ به read-only و همچنین از یک هاست SNMP واحد است.

```
access-list <ACL#> remark ACL for SNMP access to device
access-list <ACL#> permit <SNMP-host>
access-list <ACL#> deny any log
snmp-server community <SNMP-Community> RO <ACL#>
```

اعمال سیاست‌های شبکه

پیروی ترافیک ورودی شبکه از سیاست‌های شبکه (محدوده آدرس IP و نوع ترافیک)، نخستین گام در اجرای سیاست‌های شبکه محسوب می‌گردد. بسته‌های غیرعادی باید تا جایی که امکان‌پذیر است، در نزدیک‌ترین لبه شبکه دور انداخته شوند. این مسئله ریسک مخاطرات شبکه را به حداقل می‌رساند. گام‌های کلیدی برای اجرای سیاست‌های پایه‌ای شبکه به صورت زیر است:

- Access edge filtering

- IP spoofing protection

Access edge filtering

به منظور اعمال سیاست‌هایی مبنی بر اینکه کدام ترافیک اجازه ورود به سمت تجهیزات زیرساخت شبکه را دارد، مورد استفاده قرار می‌گیرد. در cisco IOS، access edge filtering برای control and data planes با استفاده از ACLs اجرایی می‌گردد.

IP spoofing protection

شامل دورانداختن ترافیکی است که آدرس مبدا غیرمعتبر دارد. امنیت پایه شبکه شامل source IP spoofing protection مبتنی بر BCP۳۸/RFC ۲۷۲۸ به منظور فیلتر کردن ترافیک ورودی است. بسته‌هایی با آدرس ip مبدا جعلی، می‌توانند بیانگر یک تهدید امنیتی باشند. مهاجمین به منظور جلوگیری از ردگیری، از این آدرس‌های جعلی به منظور حملات سایبری استفاده می‌نمایند. همچنین این آدرس‌های جعلی ممکن است برای هدایت کردن یک حمله از یک مبدا جعلی مورد استفاده قرار گیرند (reflection attack).

ترافیک جعلی با source ip address نامعتبر ممکن است شامل ترافیک از یکی از موارد زیر باشد:

- DSUA , RFC ۱۹۱۸ یا محدوده‌ی آدرس IP تخصیص نیافته
- محدوده آدرس IP معتبر ولی از سوی یک شبکه نامرتبط غیرقانونی

فیلتر نمودن ترافیک ورودی بر اساس BCP۳۸/RFC۲۸۲۷ این الزام را می‌گذارد که اگر حمله‌ای صورت بگیرد، تنها با آدرس‌های IP معتبر و قابل دسترس انجام شود. این موضوع، ردیابی مهاجم را تسهیل می‌بخشد.

Cisco تکنیک‌های زیر را به منظور فیلترکردن ترافیک ورودی، پیشنهاد می‌کند:

- Access control list (ACLs): ACLs یک تکنیک مرسوم برای فیلترنمودن آدرس‌های ip مبدا جعلی است. ACL ها به طور طبیعی پویا نیستند و بایستی به صورت دستی و بر اساس نیاز تنظیم گردند. از آنجایی که تنظیمات بی اساس acl به شدت بر روی عملکرد تجهیزات تاثیرگذار است، پیشنهاد می‌شود ACL ها فقط به شیوه‌ای محدود استفاده شوند، ACLها می‌توانند به عنوان یک مکمل برای uRPF به منظور سیاست‌های استاتیک مانند filtering RFC ۱۹۱۸، DSUA و آدرس های IP تخصیص

نیافته، مورد استفاده قرار گیرند. همچنین می‌تواند به عنوان یک مکمل برای uRPF loose mode به منظور حفاظت از جعل‌کردن آدرس ip مبدا زمانی که uRPF strict mode امکان پذیر نیست، استفاده شوند.

- uRPF: uRPF یک تکنیک پویا برای فعال‌سازی فیلتر ترافیک ورودی بر مبنای BCP۳۸/RFC۲۸۲۷ و نیز دور انداختن بسته‌هایی با source ip address نامعتبر برپایه reverse-path look-up فراهم می‌کند. طبیعت پویای آن مزایای کلیدی‌ای را فراهم می‌کند (پیشنهاد کردن overhead های عملکردی کمینه و تکنیک اجرای به هنگام و مقیاس پذیر). uRPF به طور کلی حداقل تاثیر عملکرد به یک دستگاه که برروی آن فعال است را معرفی می‌کند. uRPF به طور خاص به عنوان یک تکنولوژی مؤثر edge توسعه یافته است. بنابراین امکان کمینه کردن محدوده فضای آدرس ip معتبر و دورانداختن بسته‌های غیرعادی را تا جایی که ممکن است در نزدیکی مبدا، فراهم می‌سازد.
- IP source guard: این ویژگی در Switching به منظور جلوگیری از استفاده از آدرس های ip و MAC مبدا جعلی مورد استفاده قرار می‌گیرد. این ویژگی در تجهیزات سوئیچ لایه دو گسترش یافته و در درجه‌ی اول برای سرویس DHCP طراحی شده است. ماشین‌هایی با آدرس‌های استاتیک هم ممکن است پشتیبانی شوند اگرچه موجب افزایش پیچیدگی عملیاتی می‌گردد.
- DHCP secured IP address assignment / DHCP authorized ARP: این امکانات cisco IOS در مسیریاب‌هایی که توسط T-train پشتیبانی شده‌اند در دسترس است و عملکرد مشابهی در محیط مسیریابی مانند IP source Guard در یک محیط سوئیچینگ فراهم می‌نماید. بنابراین در routed environment که مسیریاب محلی همان DHCP server محلی است استفاده شده تا از استفاده از آدرس های IP و MAC مبدا جعلی جلوگیری کند.

توسعه ی uRPF در internet edge در مثال زیر نشان داده شده است:

```
! Configure uRPF strict mode on the internal interfaces
interface <Type Number>
ip verify unicast source reachable-via rx
!
! Configure uRPF loose mode on Internet facing interfaces
interface <Type Number>
ip verify unicast source reachable-via any
```

best practice های زیرساخت سوئیچینگ

امنیت پایه سوئیچینگ به گونه‌ای خواهد بود که اطمینان از در دسترس بودن شبکه سوئیچینگ لایه دو را فراهم نماید. گام‌های کلیدی برای امن سازی و مراقبت از زیرساخت سوئیچینگ عبارت است از:

- محدود کردن broadcast domains
- Spanning tree protocol (STP) security
- Port Security
- Best practice های رایج VLAN

محدود کردن broadcast domains

طبق تعریف، سوئیچ های LAN مسئول ارسال فریم‌های ناشناخته، فریم‌های multicast و فریم‌های broadcast در سراسر LAN و شکل دادن یک broadcast domain هستند. اگرچه broadcast domains اتصالات لایه دو بین سیستم‌ها در یک LAN را تسهیل می‌بخشد طراحی شبکه هایی با broadcast domain که به طور غیرضروری بزرگ است، زیان‌های بالقوه‌ای را ایجاد می‌نماید.

نخست آن‌که در شبکه‌های بزرگ، جریان فریم‌های multicast ، broadcast و ناشناخته ممکن است کارایی شبکه را کاهش دهد، حتی ممکن است عامل قطع اتصال باشد. به علاوه، broadcast domain یک failure domain را معرفی می‌کند که به موجب آن، معمولاً همه سیستم‌ها و سوئیچ‌ها در یک LAN متحمل failure می‌شوند. بنابراین بزرگترین broadcast domain، بیشترین تاثیر را در یک خرابی، متحمل می‌شود. در نهایت اینکه broadcast domain بزرگتر احتمال تهدیدات امنیتی را بالا می‌برد.

برای جلوگیری از چالش‌هایی که در بالا توصیف شد، broadcast domain را به چندین زیرشبکه ip یا VLAN تقسیم و از یک طراحی سلسله مراتبی استفاده می‌گردد. استفاده از اصول طراحی سلسله مراتبی شالوده‌ای برای توسعه‌ی LAN های مقیاس‌پذیر و قابل اطمینان فراهم می‌کند.

یک طراحی سلسله مراتبی مانند چیزی که در campus design پیشنهاد می‌شود، به محدود کردن اندازه broadcast domain کمک می‌نماید، توسعه را آسان و محدوده failure domain را کاهش می‌دهد.

امنیت spanning tree protocol

STP یک پروتکل مدیریت لینک است که براساس IEEE ۸۰۲.۱D تعریف شده است. STP در حالیکه از حلقه‌های ناخواسته در شبکه‌ها (که شامل چندین مسیر فعال است) جلوگیری می‌کند، افزونگی مسیر را فراهم می‌آورد. STP یک پروتکل به شدت پرکاربرد و مؤثر است ولی متاسفانه، برای نسخه‌های موجود پروتکل هیچ امنیتی درنظر گرفته نشده، در نتیجه در برابر انواع مختلفی از حملات آسیب‌پذیر است. STP هیچ authentication و encryption ی را برای بهبود تبادلات BPDU ها پیاده‌سازی نمی‌کند. به دلیل نداشتن authentication هر کسی می‌تواند با تجهیزات STP-enabled صحبت کند. مهاجم خیلی آسان می‌تواند BPDU های جعلی تزریق کند و یک محاسبه ی مجدد توپولوژی[1] را trigger کند. تغییر اعمال شده به STP topology می‌تواند شرایط Denial of service را فراهم کند یا اینکه مهاجم را به عنوان man-in-the-middle قرار دهد. به علاوه چون BPDUها رمز شده نیستند، امکان آن وجود دارد که جلوی انتقال BPDU ها گرفته و اطلاعات مهم توپولوژی فاش گردد.

STP شامل یک سری خطرات امنیتی است ولی در توپولوژی‌هایی که طراحی بدون loop امکان پذیر نیست، STP باید همراه با قابلیت‌های سیسکو که برای برطرف کردن این مشکلات توسعه داده شده‌اند، مورد استفاده قرار گیرد.

Cisco IOS تعدادی از قابلیت‌ها را به منظور محافظت از bridged network در برابر حملات رایج پیشنهاد می‌کند. در زیر best practiceهای پیشنهادی ارائه شده است:

- VLAN dynamic trunk negotiation trunking را در پورت‌هایی که به سمت کاربران نهایی است، غیرفعال کنید.
- از per-VLAN spanning tree (PVST) استفاده کنید.
- BPDU guard را پیکربندی کنید.
- STP root guard را پیکربندی کنید.
- پورت‌های بدون استفاده را غیرفعال و آن‌ها را در یک VLAN استفاده نشده قرار دهید.
- Port Security را فعال نمایید.
- Traffic storm control را فعال کنید.

[1] Topology calculation

```
! Disable dynamic trunking on all switching access lines
interface type slot/port
switchport mode access
!
! Enable BPDU guard on end user ports and other ports not expected to participate in Spanning Tree
interface type slot/port
spanning-tree portfast
spanning-tree bpduguard enable
!
! In some switching platforms interfaces are enabled by default. It is a good practice to disable all unused ports and place them into an unused VLAN
interface type slot/port
shutdown
switchport access vlan <vlan_ID>
```

Port Security

Port Security با محدودکردن آدرس‌های MAC ی که اجازه دارند ترافیک را به یک پورت مشخص ارسال نمایند، امکان جلوگیری از MAC flooding و حملات دیگر مانند سرریز بافر CAM لایه ی دو را فراهم می‌نماید.

Best practice های رایج VLAN

VLAN Hopping نمونه‌ایی از حملاتی است که دسترسی غیرمجاز یک کلاینت به VLANهای دیگر در یک سوئیچ را فراهم می‌کند. این نوع از حمله به راحتی با اعمال کردن best practice های رایج زیر می‌تواند برطرف شود:

- همیشه از یک VLAN ID اختصاصی برای همه‌ی پورت‌های TRUNK استفاده کنید.
- همه پورت‌های استفاده نشده را غیرفعال کنید و آن‌ها را در یک VLAN بدون استفاده قرار دهید.
- از VALN ۱ برای هرچیزی استفاده نکنید.
- همه پورت‌های user-facing را به عنوان non-trunking پیکربندی کنید (DTP off).
- Trunking را روی پورت‌های زیرساخت پیکربندی کنید.

- از همه modeهای tag شده برای native VLAN در trunk ها استفاده کنید.
- وضعیت پیش فرض پورت را روی غیرفعال تنظیم کنید.

پیوست ۱

جمع‌بندی تهدیدات و راه‌کارهای مقابله در زیرساخت شبکه

	BotNet	DOS	DDOS	دسترسی غیرمجاز	نفوذ	حملات پروتکل‌های مسیریابی	حملات لایه ۲	visibility	control
AAA				✓	✓			✓	✓
احراز هویت SNMP				✓	✓			✓	✓
SSH				✓	✓			✓	✓
سیاست پسورد قوی				✓	✓				✓
Session ACL		✓	✓	✓	✓			✓	✓
احراز هویت مسیریاب همسایه		✓		✓		✓			✓
فیلتر کردن مسیر		✓		✓		✓			✓
iACL	✓	✓	✓	✓	✓	✓	✓		✓
CoPP	✓	✓	✓	✓	✓	✓	✓		✓
افزونگی سیستم و توپولوژی	✓	✓	✓			✓	✓		✓