بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش هشتم: اجرای الزامات پایه امنیتی

در این فصل در مورد اجرای موارد امنیتی بحث می‌شود و یک مجموعه از ابزارها نیز معرفی خواهند شد. خواننده ممکن است از این فصل به عنوان نقطه شروع استفاده کند و سپس از ابزارهای پیشرفته‌تری بهره ببرد. در این فصل راهنمایی دقیق از چگونگی پیاده‌سازی هر ابزار همراه با نمونه‌هایی از آن‌ها ارائه می‌شوند.

محافظت از پسوردهای محلی

تجهیزات زیرساخت همیشه حاوی پسوردهای محلی و اطلاعات محرمانه‌ای هستند که نیاز است به صورت امن از آن‌ها محافظت شود. علاوه بر این به منظور اجرای سیاست استفاده از پسورد قدرتمند، اطلاعات محرمانه و پسوردها باید با استفاده از رمزگذاری محافظت شوند.

۱. رمزگذاری پسورد محلی:

رمزگذاری پسورد به صورت اتوماتیک را با دستور service password-encryption می‌توان فعال کرد. در صورت پیکربندی، تمام پسوردها به صورت اتوماتیک رمزگذاری می‌شوند.

```
Router(config)# service password-encryption
```

۲. فعال کردن امنیت:

پسورد در این حالت با دستور enable secret تعریف می‌شود. فعال کردن دسترسی از طریق این پسورد باید با یک پروتکل AAA مانند TACACS+ یا RADIUS انجام شود.

```
Router(config)# enable secret <strong-password>
```

۳. پسورد خطوط VTY:

این پسوردها برای هر خط تعریف می‌شوند. همچنین ممکن است برخی دستگاه‌ها بیش از ۵ خط VTY داشته باشند.

```
linevty 0 4
password<strong-password>
```

سرویس‌های AAA

AAA روشی برای کنترل دسترسی می‌باشد. همه دسترسی‌های مدیریتی (SSH، telnet، HTTP و HTTPS) باید با AAA کنترل شوند.

۱. فعال کردن AAA:

AAA با دستور aaa new-model فعال می‌شود. برای اطمینان از اینکه ID نشست در همه بسته‌ها معتبر است، باید دستور aaa session-id common پیکربندی شود.

```
aaa new-model
!
aaa session-id common
```

۲. تعریف گروه سرورها:

گروه سرورهای AAA باید تنظیم شود. در صورت امکان، بهتر است یک کلید جداگانه برای هر سرور استفاده شود. آدرس IP مبدا برای TACACS یا ارتباط RADIUS نیز باید پیکربندی شود.

```
tacacs-server host <TAC+server1> single-connection key <strong-key>
tacacs-server host <TAC+server2> single-connection key <strong-key>
radius-server host <RADserver1>auth-port 1645 acct-port 1646 key <strong-key>
radius-server host <RADserver2>auth-port 1645 acct-port 1646 key <strong-key>
!
aaa group server tacacs+ <TACACS-group>
server<TAC+server1>
server<TAC+server2>
!
aaa group server radius <RADIUS-group>
server<RADserver1>
server<RADserver2>
!
! Define the source interface to be used to communicate with the TACACS+/RADIUS servers
iptacacs source-interface <Loopback or OOB interface>
ip radius source-interface <Loopback or OOB interface>
```

۳. اجرای احراز اصالت برای ورود به سیستم:

باید یک لیست از کاربران مجاز تعریف شود و به کنسول VTY و همه خط‌های دسترسی استفاده شده، اعمال گردد. RADIUS و +TACACS به عنوان متد اولیه استفاده می‌شود.

```
aaa authentication login <authen-exec-list> group <AAA-group> local-case
!
line con 0
login authentication <authen-exec-list>
!
linevty 0 4
login authentication <authen-exec-list>
!
```

۴. فعال کردن احراز اصالت:

با این کار اعتبارسنجی دسترسی به TACACS+ یا RADIUS فعال می‌شود. اگر از TACACS+ استفاده می‌شود، بایستی پسورد به ازای هرکاربر فعال شود. اگر RADIUS استفاده می‌شود، بایستی یک کاربر با اسم $15enab$ ایجاد کرده و پسورد enable را برای آن تنظیم نمود. RADIUS از این نام کاربری خاص برای فعال کردن اعتبارسنجی استفاده می‌کند:

```
aaa authentication enable default group <AAA-group>enable
```

۵. اجرای مجوز exec:

با پیکربندی این حالت، مطمئن می‌شویم که فقط کاربرانی که دارای سطح دسترسی مدیر شبکه هستند، می‌توانند به محیط exec دسترسی داشته باشند:

```
aaa authorization exec author-exec-list group <AAA-group> if-authenticated
line vty 0 4
authorization exec <author-exec-list>
```

۶. فعال کردن حسابداری:

برای پایش ارتباطات، exec accounting باید فعال گردد. همچنین برای حسابداری رویدادهای سطح سیستم، باید حسابداری سیستم فعال شود:

```
aaa accounting send stop-record authentication failure
aaa accounting exec default start-stop group tacacs-group
aaa accounting commands 15 default start-stop group tacacs-group
aaa accounting system default start-stop group tacacs-group
```

دسترسی به تجهیز با سطح مجوز مدیر شبکه

۱. دسترسی telnet:

در صورت امکان از SSH به جای telnet استفاده شود. دسترسی telnet می‌تواند توسط محدود کردن خط به telnet کنترل شود، در صورتیکه از یک ACL برای کنترل ورودی استفاده شده باشد.

۲. دسترسی SSH:

دسترسی SSH در صورت وجود با استفاده از دستورات زیر فعال می‌گردد. دسترسی SSH می‌تواند با محدود کردن خط به SSH کنترل شود، در صورتی‌که از یک ACL برای کنترل ورودی استفاده شده باشد.

```
! Configure a hostname and domain name
Router(config)# hostname <router-host-name>
Router (config)# ip domain-name <domain-name>
! Generate an RSA key pair, automatically enabling SSH.
Router (config)# cry key generate rsa
! Configure time-out and number of authentication retries.
Router (config)# ip ssh time-out 60
Router (config)# ip ssh authentication-retries 2
```

۳. دسترسی HTTP:

در صورت امکان از HTTPs به جای HTTP باید استفاده گردد.

```
aaa authentication login default group tacacs-group local-case
aaa authorization exec default group tacacs-group local
ip http server
ip http access-class 22
ip http authentication aaa
access-list 22 permit 172.26.0.0 0.0.255.255
access-list 22 deny any log
line vty 0 3
transport input telnet
```

۴. دسترسی HTTPS:

```
aaa authentication login default group tacacs-group local-case
aaa authorization exec default group tacacs-group local
no ip http server
!
ip http secure-server
!
```

```
ip http access-class 22
ip http authentication aaa
access-list 22 permit 172.26.0.0 0.0.255.255
access-list 22 deny any log
line vty 0 3
transport input telnet
```

محدود کردن پروتکل‌ها و خط‌های دسترسی

۱. غیرفعال کردن خطوط دسترسی غیرضروری:

پورت‌های که استفاده نمی‌شوند را با استفاده از دستور no exec می‌توان غیر فعال کرد.

```
line aux 0
no exec
```

۲. محدود کردن پروتکل‌های ورودی‌ها و خروجی‌ها:

محدود کردن خروجی‌ها از سوء استفاده از سیستم به عنوان حمله‌کننده به اهداف دیگر، جلوگیری می‌کند.

```
line vty 0 4
 transport input ssh
 transport output ssh
 transport preferred none
```

۳. محدود کردن منابع با ACL:

از ACL برای کنترل منابع استفاده می‌شود. منبع معمولاً زیر شبکه‌ای می‌باشد که در آن مدیران قرار دارند. آخرین VTY موجود برای دسترسی به تجهیز رزرو می‌شود. همچنین باید یک access-class پیکربندی گردد تا اطمینان حاصل شود که این VTY تنها توسط سیستم‌های قابل اعتماد و شناخته شده قابل دسترسی می‌باشند:

```
! Grants access from management subnet. Set port to 22 for SSH and 23 for telnet.
access-list 111 permit tcp <management-subnet> <inverse-mask> any eq <port>
access-list 111 deny ip any any log-input
! ACL for last resort access
access-list 112 permit tcp host <management-station> any eq <port>
access-list 112 deny ip any any log-input
line vty 0 3
access-class 111 in
!
line vty 4
access-class 112 in
```

۴. تنظیم وقفه‌ها:

در خطوطی که مورد استفاده قرار گرفته شده‌اند، باید وقفه‌ها تنظیم شوند. TCP-keepalives برای شناسایی و بستن جلسات معلق استفاده می‌شود.

```
service tcp-keepalives-in
!
line vty 0 4
session-timeout 3
exec-timeout 10 0
```

زیرساخت مسیریابی

۱. احراز اصالت همسایه‌ها:

احراز اصالت همسایه‌ها در همه روترها باید فعال شود. همچنین بهتر است برای برقراری ارتباط همسایگی با دیگر روترها، برای هر ارتباط از کلیدهای متفاوت استفاده شود.

```
! OSPF MD5 authentication
interface <interface-type/number>
ip ospf message-digest-key <key-number> md5 <strong-password>
!
router ospf <process>
network <network> <mask> area <area-number>
area <area-number> authentication message-digest
! EIGRP authentication
key chain <key-chain-name>
key 1
key-string <strong-password>
!
interface <interface-type/number>
ip authentication mode eigrp <process> md5
```

```
ip authentication key-chain eigrp <process> <key-chain-name>
!
router eigrp <process>
network <network>
!
```

۲. تعریف همتای استاتیک:

در صورت استفاده از EIGRP، همتایان استاتیک در بخش‌های همه‌پخشی باید پیکربندی شوند:

```
router eigrp <process>
network <network>
neighbor <peer-address> <interface-type/number>
```

۳. اینترفیس پسیو پیش فرض:

در برخی سناریوها، نیاز است EIGRP یا OSPF بر روی تعداد زیادی از اینترفیس‌ها فعال گردد. فعال کردن پروتکل مسیریابی بر روی آن اینترفیس‌ها می‌تواند به طور مستقیم در شبکه‌های متصل پخش گردد. در این سناریوها ممکن است فرد بخواهد پروتکل مسیریابی را در یک محدوده شبکه با چندین اینترفیس فعال کند:

```
router <protocol> <process>
! Disable routing updates on all interfaces by default
passive-interface default
! Explicitly enable routing updates on interfaces where you expect routing peers
no passive-interface <interface-type/number>
```

۴. بررسی امنیت BGP TTL:

در صورت استفاده از BGP، بررسی امنیت TTL بر روی روترهای متصل به همتایان BGP بیرونی، باید پیکربندی شود:

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

فیلترینگ مسیریابی

جهت پیاده‌سازی فیلترینگ مسیریابی، باید مراحل زیر را انجام داد:

۱. پیاده‌سازی فیلترینگ همتا در لبه‌ها:

فیلترهای ورودی در لبه‌ها باید پیاده‌سازی شوند تا اطمینان حاصل شود که تنها مسیرهای مورد انتظار در شبکه می‌توانند تعریف شوند. فیلترها در لبه‌ها باید اعمال شوند. کنترل آپدیت‌های مسیریابی ورودی در لبه WAN، از دسترسی دوگانه جهت سوء استفاده و تبدیل شدن شبکه به یک شبکه ترانزیت ترافیک جلوگیری می‌کند.

```
! Incoming route filter applied at the WAN edge and that only allows the branch subnet.
!
router eigrp <process>
network <network>
distribute-list 39 in <interface-type/number>
!
access-list 39 permit <remote-subnet> <inverse-mask>
```

۲. اجرای فیلتر کردن مسیرها در روترهای اصلی:

باید در شاخه‌ها و مکان‌های راه دور با شبکه اصلی، عملیات فیلتر کردن مسیرها انجام شود تا از انتشار اطلاعات مسیریابی نامعتبر جلوگیری شود.

در صورت استفاده از EIGRP، بایستی از دستور eigrp stub connected به منظور حصول اطمینان از انتشار تنها شبکه‌هایی که به طور مستقیم متصل شده‌اند، استفاده کرد.

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

در صورت استفاده از پروتکل‌های دیگر، باید فیلترهای بیرونی پیکربندی شوند:

```
! Outbound route filter applied at the branch router.
!
router ospf <process>
distribute-list 33 out <interface-type/number>
!
access-list 33 permit <branch-subnet> <inverse-mask>
```

۳. گزارش‌های مربوط به روترهای همسایه:

در همه روترها، باید تغییر وضعیت نشست‌های مربوط به روترهای همسایه گزارش‌گیری شود.

```
!Logging neighbor changes in EIGRP
router eigrp <process>
eigrp log-neighbor-changes
! Logging neighbor changes in OSPF
router ospf <process>
log-adjancey-changes
```

بقای دستگاه

جهت غیرفعال کردن سرویس‌هایی که مورد نیاز نیستند، مراحل زیر را باید انجام داد:

۱. مشخص کردن پورت‌های باز:

می‌توان از دستور show control-plane host open-ports برای مشاهده اینکه کدام پورت‌های UDP/TCP روتر در حال listening هستند و تعیین اینکه کدام سرویس‌ها باید غیرفعال شوند، استفاده کرد:

```
cr18-7200-3#show control-plane host open-ports
Active internet connections (servers and established)
Prot Local Address Foreign Address Service State
tcp *:22 *:0 SSH-Server LISTEN
tcp *:23 *:0 Telnet LISTEN
tcp *:63771 172.26.150.206:49 IOS host service ESTABLIS
udp *:49 172.26.150.206:0 TACACS service LISTEN
udp *:67 *:0 DHCPD Receive LISTEN
cr18-7200-3#
```

۲. اطمینان یافتن از آن‌که سرویس‌های کلی به طور پیش فرض غیرفعال، غیرفعال هستند:

در صورت نیاز باید از غیرفعال بودن finger ، identification (identd) و سرورهای TCP و UDP بر روی تمام روترها اطمینان حاصل کرد.

```
! Global Services disabled by default
Router(config)# no ip finger
Router(config)# no ip identd
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
```

۳. اطمینان یافتن از آن‌که سرویس‌های کلی به طور پیش فرض فعال، غیرفعال شده‌اند:

در صورت نیاز باید از غیرفعال بودن BOOTP، مسیریابی بر اساس آدرس IP مبدأ و سرویس‌های PAD بر روی تمام روترها اطمینان حاصل کرد.

```
! Disable BOOTP, IP Source Routing and PAD global services
Router(config)# no ip source-route
Router(config)# no ip bootp server
Router(config)# no service pad
```

۴. همه‌پخشی مستقیم IP:

باید همه‌پخشی مستقیم بر روی همه اینترفیس‌ها غیرفعال شود.

```
! Disable IP directed broadcasts on all interfaces
Router(config)# interface <interface-type/number>
Router(config-if)# no ip directed-broadcast
```

۵. غیرفعال کردن CDP:

زمانی که سرویس‌های جاری شبکه در معرض خطر هستند، باید CDP غیر فعال گردد، برای مثال بر روی تمام اینترفیس‌های خارجی که در مرز اینترنت هستند.

```
! Disable CDP on externally facing interfaces
Router(config)# interface <interface-type number>
Router(config-if)# no cdp enable
```

ACL های محافظ زیرساخت (iACLs)

همانطور که قبلاً گفته شد، iACL در صورت اعمال در لبه شبکه بسیار مفید است. لبه اینترنت و لبه WAN بهترین مکان برای پیاده‌سازی iACL می‌باشند. برای ایجاد iACL باید شناخت کافی از پروتکل‌ها و پورت‌های مجازی که در زیرساخت استفاده می‌شود، وجود داشته باشد. در نتیجه بهتر است با طراحی ACL شروع شود. در زیر مثال‌های ACL شرح داده شده است. توجه داشته باشید که هر ورودی باید طوری پیکربندی شده باشد که گزارش تولید کند:

```
access-list 133 permit eigrp any any log
access-list 133 permit icmp any any log
access-list 133 permit tcp any any eq tacacs log
access-list 133 permit udp any any eq ntp log
access-list 133 permit tcp any any eq 22 log
access-list 133 permit udp any any eq syslog log
access-list 133 permit ip any any log
```

زمانی‌که ACL طراحی شد، باید در همان اینترفیس iACL فعال گردد. بایستی مطمئن شد که ACL در طرف داخلی پیاده‌سازی شده باشد. در مثال زیر ACL در لبه WAN روتر تعریف شده است.

```
interface GigabitEthernet4/46
description To Branch 4
ip address 10.139.5.10 255.255.255.254
ip access-group 133 in
```

می‌توان فعالیت ACL را با استفاده از دستور show access-list و show logging مشاهده کرد.

```
cr18-7604-1#sh access-l 133
Extended IP access list 133
10 permit eigrp any any log (76 matches)
20 permit icmp any any log
30 permit tcp any any eq tacacs log (10 matches)
40 permit udp any any eq ntp log (8 matches)
50 permit tcp any any eq 22 log (35 matches)
60 permit udp any any eq syslog log (4 matches)
70 permit ip any any log (24 matches)
```

ورودی any any نشان می‌دهد که هنوز پروتکل‌ها و پورت‌هایی در زیرساخت وجود دارند که مشخص نشده‌اند. برای مشاهده اینکه کدام بسته‌ها با آخرین ورودی ACL منطبق هستند، می‌توان از دستور زیر استفاده کرد.

```
cr18-7604-1#sh logging
...
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(55786) -> 172.26.150.206(49), 1 packet
%SEC-6-IPACCESSLOGDP: list 133 permitted icmp 10.139.5.11 -> 172.26.159.166 (8/0), 1 packet
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(22) -> 172.26.159.166(11031), 1 packet
%SEC-6-IPACCESSLOGRP: list 133 permitted eigrp 10.139.5.11 -> 224.0.0.10, 34 packets
%SEC-6-IPACCESSLOGP: list 101 permitted udp 10.139.5.11(123) -> 172.26.158.236(123), 1 packet
%SEC-6-IPACCESSLOGDP: list 133 permitted icmp 10.139.5.11 -> 172.26.159.166 (8/0), 4 packets
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(22604) -> 172.26.150.206(49), 19 packets
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(55786) -> 172.26.150.206(49), 5 packets
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(22) -> 172.26.159.166(11031), 31 packets
%SEC-6-IPACCESSLOGRP: list 133 permitted eigrp 10.139.5.11 -> 224.0.0.10, 8 packets
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(13621) -> 172.26.150.206(49), 2 packets
%SEC-6-IPACCESSLOGRP: list 133 permitted eigrp 10.139.5.11 -> 224.0.0.10, 1 packet
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(22) -> 172.26.159.166(11032), 1 packet
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(40429) -> 172.26.159.167(22), 1 packet
%SEC-6-IPACCESSLOGP: list 133 permitted tcp 10.139.5.11(22604) -> 172.26.150.206(49), 7 packets
%SEC-6-IPACCESSLOGP: list 101 permitted udp 10.139.5.11(58557) -> 172.26.150.206(514), 4 packets
```

دستور show logging همچنین مبدأها، مقصدها و پورت‌های یک جریان ترافیک را به طور دقیق نشان می‌دهد.

```
access-list 133 permit eigrp host 10.139.5.11 host 224.0.0.10
access-list 133 permit icmp host 10.139.5.11 172.26.0.0 0.0.255.255
access-list 133 permit tcp host 10.139.5.11 eq 22 172.26.0.0 0.0.255.255
access-list 133 permit tcp host 10.139.5.11 172.26.0.0 0.0.255.255 eq 22
access-list 133 permit tcp host 10.139.5.11 host 172.26.150.206 eq 49
access-list 133 permit udp host 10.139.5.11 eq ntp host 172.26.158.236 eq ntp
access-list 133 permit udp host 10.139.5.11 host 172.26.150.206 eq syslog
access-list 133 permit ip any any log
```

۱. اکنون باید شناخت خوبی بر روی کنترل و مدیریت ترافیک شبکه حاصل شده باشد. ابتدا باید ورودی‌های ضد جعل برای محافظت از محدوده آدرس‌های شبکه تعریف شوند. در این مثال 172.26.0.0/16 در شبکه OOB رزرو شده است و درنتیجه هیچ بسته‌ای در این محدوده نباید از هیچ شاخه‌ای وارد شود.

```
!--- Module 1: Anti-spoofing, deny special use addresses
! Deny your OOB address space as a source in packets
access-list 101 deny ip 172.26.0.0 0.0.255.255 any
```

همچنین ورودی‌هایی برای مسدود کردن بسته‌های با آدرس IP مبدأ نامعتبر باید تعریف شوند.

```
!--- 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 101 deny ip 192.0.2.0 0.0.0.255 any
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
```

۲. در مرحله دوم، باید ورودی‌های لازم به منظور اجازه دادن به ترافیک‌هایی که از طریق ACL ها یادگرفته شده‌اند، تعریف گردد.

```
!--- Module 2: Explicit Permit
! Permit valid traffic destined to the infrastructure
access-list 101 permit eigrp host 10.139.5.11 host 224.0.0.10
access-list 101 permit icmp host 10.139.5.11 172.26.0.0 0.0.255.255
access-list 101 permit tcp host 10.139.5.11 eq 22 172.26.0.0 0.0.255.255
access-list 101 permit tcp host 10.139.5.11 172.26.0.0 0.0.255.255 eq 22
access-list 101 permit tcp host 10.139.5.11 host 172.26.150.206 eq 49
access-list 101 permit udp host 10.139.5.11 eq ntp host 172.26.158.236 eq ntp
```

```
access-list 101 permit udp host 10.139.5.11 host 172.26.150.206 eq syslog
```

۳. بایستی هر دسترسی دیگری به زیرساخت رد شود. در این مثال هر ترافیک دیگری به مقصدهای سه شبکه استفاده شده در زیرساخت، مسدود می‌شود. 10.139.5.0/24 برای لینک‌های WAN بین لبه و شاخه‌ها و 10.122.0.0/16 برای همه تجهیزات مرکزی استفاده می‌شود. 172.26.0.0/16 برای شبکه OBB رزرو شده است. ترافیک معتبر به این شبکه‌ها باید از طریق مرحله دوم اجازه انتشار پیدا کنند.

```
!--- Module 3: Explicit Deny to Protect Infrastructure
! Deny all other access to infrastructure
access-list 101 deny ip any 10.139.5.0 0.0.0.255
access-list 101 deny ip any 10.122.0.0 0.0.255.255
access-list 101 deny ip any 172.26.0.0 0.0.255.255
```

۴. در انتها بر حسب نیاز، آخرین خط ACL جهت رد کردن یا پذیرفتن هر ترافیک دیگری، پیکربندی می‌گردد. دراین مثال یک iACL برای لبه WAN ایجاد می‌شود که هدف آن، کنترل ترافیک به مقصد زیرساخت می‌باشد. در نتیجه از مجوز ورودی any any استفاده می‌گردد.

```
!--- Module 4: Explicit Permit/Deny for Transit Traffic
! Permit transit traffic enterprise inner iACL
access-list 101 permit ip any any
```

Port Security

Port Security یک ویژگی مفید برای کاهش ترافیک سیل‌آسای MAC و دیگر حمله‌های سرریز محتوای حافظه مربوط به لایه ۲ (CAM) می‌باشد. مرز دسترسی شبکه و مجموعه سرورها، نسبت به دیگر مکان‌های شبکه دارای اولویت بالاتری برای اعمال Port Security می‌باشند.

به منظور پیاده‌سازی Port Security ، باید مراحل زیر دنبال شوند:

۱. Port Security در لبه دسترسی:

Port Security در سوئیچ‌ها به منظور محدود کردن حداکثر تعداد آدرس‌های MAC مجاز بر روی هر پورت پیکربندی می‌شود. تعداد آدرس‌های MAC مجاز برحسب سیستم‌های متصل به سوئیچ می‌تواند تغییر کند. یک راه خوب برای شناسایی آدرس MAC به ازای هر پورت، بررسی جدول CAM با دستور show mac-address-table می‌باشد.

```
r17-3750-2#show mac-address-table vlan 20
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
All 0100.0ccc.cccc STATIC CPU
...
All ffff.ffff.ffff STATIC CPU
20 000f.352c.4bd1 DYNAMIC Gi2/0/48
20 0014.a92e.7737 DYNAMIC Gi2/0/47
20 0015.627f.abb0 DYNAMIC Gi2/0/47
20 0015.629c.2f33 DYNAMIC Gi2/0/47
Total Mac Addresses for this criterion: 25
cr17-3750-2#
```

در لبه دسترسی، تعیین اینکه به هر پورتی چه آدرس MAC متصل شده است دشوار می‌باشد، در نتیجه Port Security با مکانیزم یادگیری پویای آدرس MAC پیکربندی می‌گردد.

پورت‌هایی از سوئیچ که به کاربران انتهایی متصل هستند، باید به گونه‌ای پیکربندی شوند که تنها یک آدرس MAC بتواند به آن پورت متصل شود.

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

پورت‌هایی از سوئیچ که به IP phone متصل هستند، باید به دو آدرس MAC محدود گردند.

```
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
```

۲. Port Security در DMZs:

در محیط‌هایی که مکان سیستم‌ها به سختی تغییر می‌کند و موقعیت فیزیکی آن‌ها تقریباً ثابت است و همیشه به یک پورت مشخص سوئیچ متصل هستند، می‌توان Port Security را به گونه‌ای پیکربندی کرد که تنها یک آدرس MAC خاص اجازه برقراری ارتباط از طریق این پورت را داشته باشد.

دستور show mac-address-table، آدرس MAC متصل به پورت سوئیچ را نشان می‌دهد.

```
r17-3750-2#show mac-address-table vlan 20
    Mac Address Table
-------------------------------------------
Vlan    Mac Address     Type      Ports
----    -----------     --------  -----
All   0100.0ccc.cccc    STATIC    CPU
...
All   ffff.ffff.ffff    STATIC    CPU
20    000f.352c.4bd1    DYNAMIC Gi2/0/48
...
Total Mac Addresses for this criterion: 25
```

در مثال زیر نشان داده شده است که چگونه می‌توان یک پورت سوئیچ را به گونه‌ای محدود کرد که تنها یک سیستم خاص بتواند از طریق آن ارتباط برقرار کند.

```
Router(config)# interface gigabitethernet2/0/48
Router(config-if)# switchport port-security maximum 1
Router(config-if)# switchport port-security mac-address 000f.352c.4bd1
Router(config-if)# switchport port-security violation shutdown
Router(config-if)# switchport port-security
```

اگر از SNMP استفاده می‌شود، باید مکانیزم گزارش‌گیری SNMP به منظور ثبت گزارش‌های مربوط به آن دسته از ترافیک SNMP که سیاست‌های port-security را نقض کرده‌اند، فعال شود.

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

پایش شبکه از راه دور

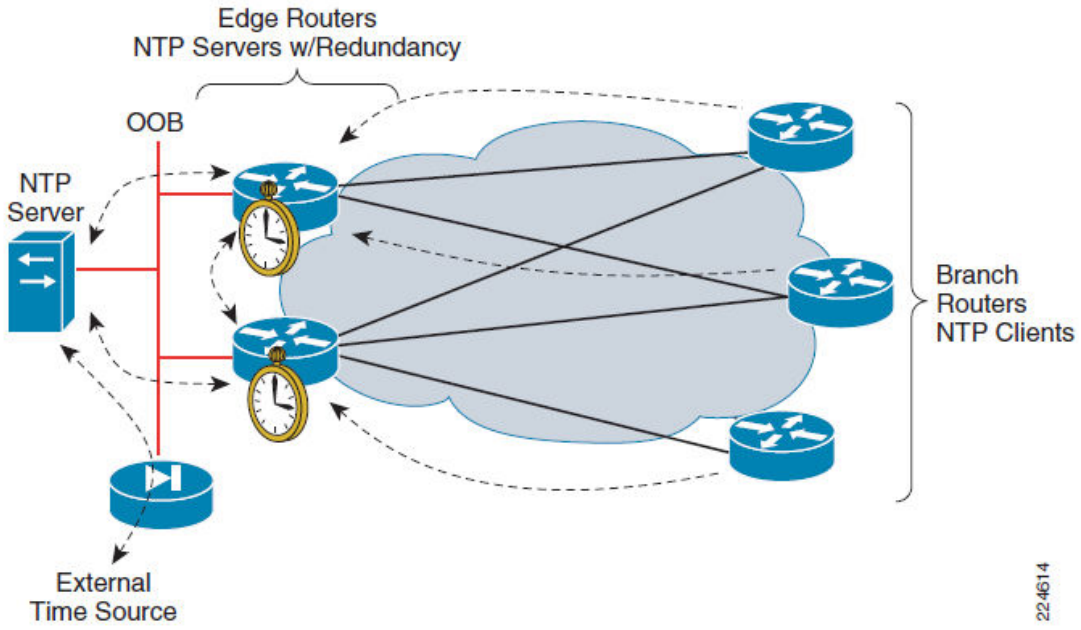
همگام‌سازی زمان به منظور تجزیه و تحلیل رویدادها و ارتباطات، یک مورد ضروری و مهم می‌باشد، بنابراین فعال کردن NTP بر روی تمام تجهیزات زیرساخت یک نیاز اساسی است.

هنگام اجرای NTP روش‌های زیر باید در نظر گرفته شود:

- طراحی NTP به صورت سلسله مراتبی در مقابل یک طراحی مسطح
- استفاده از یک منطقه زمانی در سراسر زیرساخت به منظور تسهیل تجزیه و تحلیل و همبستگی وقایع
- کنترل کاربرانی که می‌توانند با سرور NTP ارتباط داشته باشند و فعال سازی احراز اصالت NTP

طراحی NTP برای دفاتر راه دور

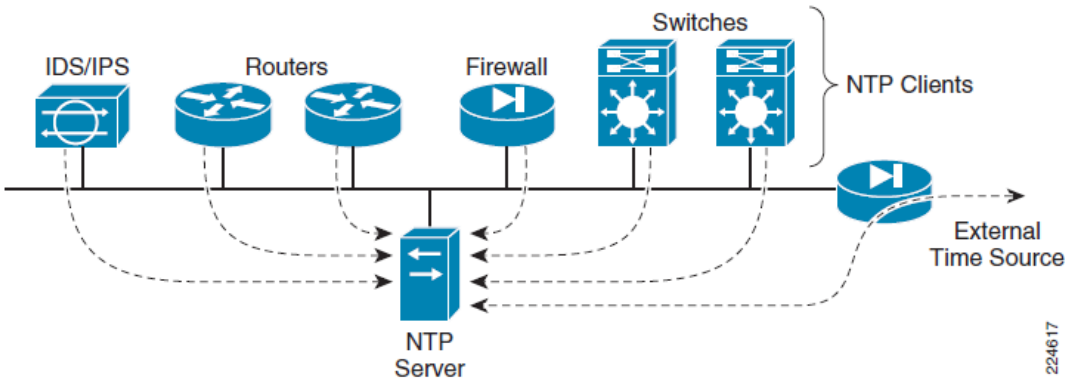
دفاتر راه دور به طور معمول توسط یک روتر که مرز یک شبکه WAN می‌باشد، به روتر و یا روترهای شبکه اصلی متصل می‌شوند که می‌توانند در طراحی NTP ملاک قرار بگیرند. نکته مهم این است که باید سرور زمانی که در داخل شبکه استفاده می‌شود، در یک بخش امن قرار بگیرد، مگر اینکه یک ساعت اتمی یا GPS در دسترس باشد. همچنین این سرویس دهنده‌های داخلی با منابع خارجی هم هماهنگ خواهند شد. پس از طراحی مسیریابی، امکان دارد روتر لبه WAN به عنوان سرور زمان از طریق ارتباط client/server با سرورهای زمان داخلی پیکربندی شود، و روترهای شاخه ممکن است به عنوان کلاینت از طریق ارتباط client/server با روتر لبه WAN همگام شوند. این طراحی در شکل ۱ نشان داده شده است.



شکل ۱- طرح NTP برای شبکه‌های WAN و دفاتر راه دور

طراحی NTP در دفتر اصلی

در دفتر اصلی می‌توان از یک شبکه مدیریت OOB استفاده کرد و از مزایای آن بهره برد. تبادلات NTP بر روی شبکه OOB، طراحی را مسطح و ساده می‌کند. در این سناریو تمام روترها و سوئیچ‌ها ممکن است به عنوان کلاینت از طریق ارتباط client/server با سرور زمان داخلی واقع در یک بخش امن ارتباط برقرار کرده و همگام شوند. این سرویس دهنده داخلی با منابع خارجی هم هماهنگ می‌شود. این طراحی در شکل ۲ نشان داده شده است.



شکل ۲- طرح NTP مبتنی بر OOB

در حالتی که شبکه مدیریت OOB وجود ندارد، می‌توان همان ساختار طراحی مسیریابی را اعمال کرد. روترهای مرکزی می‌توانند به عنوان سرور زمان از طریق ارتباط client/server با سرورهای زمان داخلی واقع در یک بخش امن و هماهنگ با منابع خارجی پیکربندی شوند. دیگر روترها که به عنوان روترهای distribution از آن‌ها نام برده می‌شود نیز می‌توانند به عنوان سرور زمان، از طریق ارتباط client/server با روترهای مرکزی پیکربندی شوند. همچنین تمام دیگر کلاینت‌های داخلی می‌توانند از طریق ارتباط client/server با روترهای distribution همگام شوند.

الف) سرورهای NTP

هنگامیکه روترها و سوئیچ‌ها به عنوان سرورهای زمان پیکربندی می‌شوند، مراحل زیر باید طی شود:

۱- فعال کردن اطلاعات برچسب زمان برای اشکال زدایی و گزارش‌گیری پیام‌ها

```
Router(config)# service timestamps debug datetime localtime show-timezone msec
Router(config)# service timestamps log datetime localtime show-timezone msec
```

۲- تنظیم کردن منطقه زمانی

```
Router(config)# clock timezone zone hours-offset [minutes-offset]
Router(config)# clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]
```

۳- تنظیم کردن آدرس IP مبدأ که برای بسته‌های NTP استفاده می‌شوند.

```
Router(config)# ntp source <interface-type/number>
```

۴- محدود کردن آدرس IP سرورها و تعیین همتایان آن‌ها که قرار است با هم ارتباط برقرار کنند.

```
Router(config)# access-list 10 remark ACL for NTP Servers and Peers
Router(config)# access-list 10 permit <NTPserver1>
Router(config)# access-list 10 permit <NTPserver2>
Router(config)# access-list 10 permit <NTPpeer1>
Router(config)# access-list 10 permit <NTPpeer2>
Router(config)# access-list 10 deny any log
!
Router(config)# ntp access-group peer 10
```

۵- باید آدرس IP های کلاینت‌هایی که می‌توانند با سرور ارتباط برقرار کنند، محدود شوند.

```
Router(config)# access-list 15 remark ACL for NTP Client
Router(config)# access-list 15 permit <Client1>
Router(config)# access-list 15 permit <Client2>
Router(config)# access-list 15 deny any log
!
Router(config)# ntp access-group serve-only 15
```

۶- فعال کردن مکانیزم احراز اصالت NTP

```
Router(config)# ntp authentication-key <key#> md5 <strong8charkey>
Router(config)# ntp trusted-key <key#>
Router(config)# ntp authenticate
```

۷- تعریف سرورهای NTP

```
Router(config)# ntp server <NTPserver1>
Router(config)# ntp server <NTPserver2>
```

۸- باید هر کدام از همتاهای NTP تعریف شوند.

```
Router(config)# ntp peer <NTPpeer1>
```

ب) کلاینت‌های NTP

هنگامی که روترها و سوئیچ‌ها به عنوان کلاینت پیکربندی می‌شوند، مراحل زیر را باید انجام داد:

۱-فعال کردن اطلاعات برچسب زمان برای اشکال زدایی و گزارش‌گیری پیام‌ها

```
Router(config)# service timestamps debug datetime localtime show-timezone msec
Router(config)# service timestamps log datetime localtime show-timezone msec
```

۲- تنظیم کردن منطقه زمانی

```
Router(config)# clock timezone zone hours-offset [minutes-offset]
Router(config)# clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]
```

۳- تنظیم کردن آدرس IP مبدأ که برای بسته‌های NTP استفاده می‌شوند.

```
Router(config)# ntp source <interface-type/number>
```

۴- فعال کردن مکانیزم احراز اصالت NTP

```
Router(config)# ntp authentication-key <key#> md5 <strong8charkey>
Router(config)# ntp trusted-key <key#>
Router(config)# ntp authenticate
```

۵-تعیین سرورهای NTP

```
Router(config)# ntp server <NTPserver1>
Router(config)# ntp server <NTPserver2>
```

آمارهای ترافیک تجهیزات

روترها و سوئیچ‌ها می‌توانند آمارهای ترافیک که برای پایش شبکه از راه دور ضروری است را به ازای هر اینترفیس و یا به صورت کلی نگه‌داری کنند. این اطلاعات حاوی آمارهای حداکثر ظرفیت و پهنای باند برای هر اینترفیس و همچنین آمارهای ویژگی‌های فعال شده و کلی ترافیک به ازای هر پروتکل می‌باشد.

به طور پیش فرض، IOS سیسکو آمارهای اینترفیس را بر اساس یک بازه زمانی ۵ دقیقه‌ای به طور متوسط محاسبه می‌کند. در حالی که تنظیمات پیش فرض برای اکثر روترها و سوئیچ‌ها به خوبی کار می‌کند، این بازه زمانی نمی‌تواند تأثیر ترافیک‌های ناگهانی، با حجم زیاد و پشت سر هم را منعکس کند. این امر برای تجهیزاتی که در مرز شبکه استفاده می‌شوند، مانند لبه اینترنت و لبه WAN بسیار مهم است. برای اینکه محاسبات

دقیق‌تر باشد و بتواند اثر ترافیک‌های ناگهانی را نیز منعکس کند، بایستی در اینترفیس‌های مرزی مدت زمان مربوط به جمع‌آوری داده‌ها را به یک دقیقه کاهش داد:

```
Router(config)# interface <interface-type number>
Router(config)# load-interval 60
```

اطلاعات وضعیت سیستم

روترها و سوئیچ‌ها مجموعه‌ای از اطلاعات مربوط به منابع سیستم که نشان دهنده حالت کلی و وضعیت سیستم است را نگه‌داری می‌کنند. در زیر بهترین شیوه برای تمام سوئیچ‌ها و روترها شرح داده شده است.

۱. آستانه حافظه:

باید هشدار مربوط به آستانه حافظه برای اطلاع‌رسانی زمانی که حافظه آزاد و در دسترس کمتر از یک مقدار مشخص باشد، فعال شود. یک روش، تنظیم آستانه حافظه آزاد به ۱۰ درصد کل حافظه می‌باشد. از دستور show memory برای دیدن کل حافظه و حافظه آزاد در دسترس می‌توان استفاده کرد.

در مثال زیر مقدار آستانه برای هر دو حافظه ورودی-خروجی و پردازنده برابر ٪۱۰ تنظیم شده است.

```
Router#show memory
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 6572AD00 915231348 27009876 888221472 374721396 361583220
I/O C000000 67108864 5856500 61252364 61233808 61232028
…
Router#
```

۲. فعال کردن حفاظت از مکانیزم گزارش‌گیری سیستم:

هنگامی که یک روتر توسط پروسه‌های زیادی اشباع می‌شود، مقدار حافظه موجود ممکن است به میزان کمی برسد که برای نشان دادن هشدارهای ضروری کافی نباشد. درنتیجه باید یک محدوده از حافظه به میزان حداقل ۱۰۰۰ کیلوبایت رزرو شود تا توسط روتر برای نمایش هشدارهای مهم استفاده شود:

```
Router(config)# memory reserve critical 1000
```

۳. هشدار SNMP مربوط به آستانه CPU باید فعال شود.

:SNMP

SNMP برای پایش و مدیریت تجهیزات در شبکه استفاده می‌شود. به منظور غیر فعال کردن آن از دستور no snmp-server در همه نسخه‌ها استفاده می‌شود.

از دستور show snmp برای دیدن agent آن می‌توان استفاده کرد.

```
Router# show snmp
%SNMP agent not enabled
Router#
```

زمانیکه SNMP مورد نیاز است، برای پیکربندی آن مراحل زیر باید طی شود:

۱. محدود کردن سیستم‌هایی که می‌توانند به SNMP agent که بر روی روتر یا سوئیچ در حال اجرا است، دسترسی داشته باشند:

```
Router(config)# access-list <ACL#> remark ACL for SNMP access to device
Router(config)# access-list <ACL#> permit <SNMPserver1>
Router(config)# access-list <ACL#> permit <SNMPserver2>
Router(config)# access-list <ACL#> deny any log
```

۲. در صورت استفاده از نسخه ۳ SNMP، باید دانلود همه آدرس IP های مسیریابی و جداول ARP محدود شوند.

```
! Define an SNMP view which denies queries to download the full IP routing and ARP tables
Router(config)# snmp-server view <restricted-view1> internet included
Router(config)# snmp-server view <restricted-view1> ipRouteTable excluded
Router(config)# snmp-server view <restricted-view1> ipNetToMediaTable excluded
Router(config)# snmp-server view <restricted-view1> at excluded
```

اجرای سیاست شبکه

uRPF

هنگامیکه uRPF در لبه اینترنت فعال می‌شود، باید مراحل زیر انجام شوند:

۱. در اینترفیس داخلی باید حالت محدود uRPF پیکربندی شود:

```
Router(config)# interface <Type Number>
Router(config-if)# ip verify unicast source reachable-via rx
```

۲. در اینترفیسی که مرتبط با اینترنت است، باید حالت آزاد uRPF پیکربندی شود:

```
Router(config)# interface <Type Number>
Router(config-if)# ip verify unicast source reachable-via any
```

لبه دسترسی:

حالت محدود uRPF باید در اولین تجهیز مسیریابی از لبه دسترسی دفتر اصلی یا دفاتر راه دور فعال شود:

```
Router(config)# interface <Type Number>
Router(config-if)# ip verify unicast source reachable-via rx
```

زیرساخت سوئیچینگ

در زیرساخت لایه ۲ باید مراحل زیر انجام شوند:

۱. ترانکینگ پویا در همه خطوط دسترسی سوئیچینگ باید غیرفعال شود:

```
Router(config)# interface type slot/port Router(config-if)# switchport mode access
```

برای غیر فعال کردن این ویژگی بر روی محدوده‌ای از پورت‌ها به روش زیر باید عمل کرد:

```
Router(config)# interface range type slot/first-port – last-port
Router(config-if)# switchport mode access
```

۲. گارد BPDU در پورت‌های متصل به کاربران انتهایی و پورت‌هایی که انتظار می‌رود در عملیات مربوط به پروتکل STP مشارکت نداشته باشند، با استفاده از دستور زیر باید فعال گردد.

```
Router(config)# interface type slot/port
Router(config-if)# spanning-tree portfast
Router(config-if)# spanning-tree bpduguard enable
```

برای فعال کردن گارد BDPU بر روی محدوده‌ای از پورت‌ها به روش زیر باید عمل کرد:

```
Router(config)# interface range type slot/first-port – last-port
Router(config-if)# spanning-tree portfast
Router(config-if)# spanning-tree bpduguard enable
```

۳. در برخی سوئیچ‌ها، اینترفیس‌ها به صورت پیش فرض فعال هستند. بهتر است که همه آن‌ها غیر فعال شوند و در یک VLAN بدون استفاده قرار گیرند:

```
Router(config)# interface type slot/port
Router(config-if)# shutdown
Router(config-if)# switchport access vlan <vlan_ID>
```

برای غیر فعال کردن محدوده‌ای از پورت‌ها و قرار دادن آن‌ها در یک VLAN بدون استفاده از دستور زیر استفاده می‌شود:

```
Router(config)# interface range type slot/first-port – last-port
Router(config-if)# shutdown
Router(config-if)# switchport access vlan <vlan_ID>
```