بسمه تعالی

پیکربندی امن سوئیچ‌های نسل جدید سیسکو NX-OS

(بخش سوم)

فهرست مطالب

۱ مقدمه

در این گزارش به بررسی مجموعه‌ای از پیکربندی‌های امنیتی مورد نیاز منطبق بر چک‌لیست‌های امنیتی در نسل جدید سوئیچ‌های NX-OS پرداخته می‌شود.

۲ پیکربندی DHCP Snooping

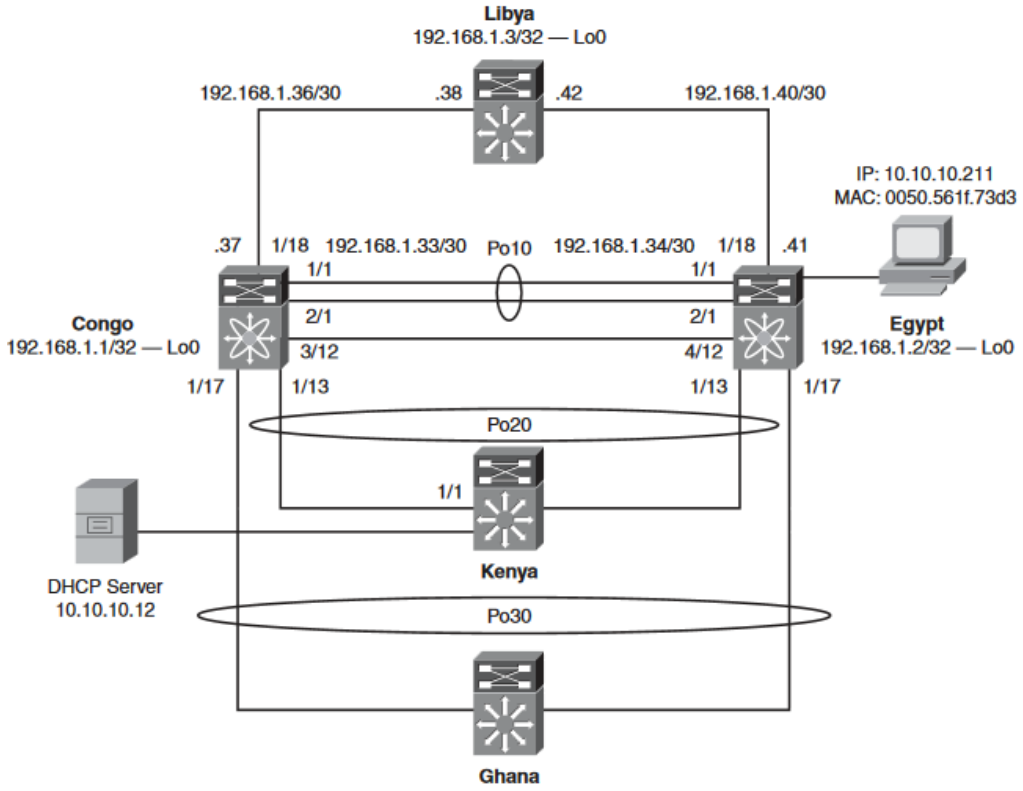
DHCP Snooping ناظر ترافیک بین میزبان‌های نامعتبر و سرویس‌دهنده‌های قابل اعتماد DHCP است. DHCP Snooping مسئولیت‌های زیر را انجام می‌دهد:

- پیام‌های DHCP دریافت شده از منابع غیرقابل اعتماد را تأیید می‌کند و پیام‌های نامعتبر را فیلتر می‌کند.
- تهیه و نگهداری پایگاه داده DHCP Snooping binding، که حاوی اطلاعاتی درباره میزبان‌های نامعتبر با آدرس‌های IP اجاره شده هستند.
- از پایگاه‌های داده DHCP Snooping binding برای تأیید درخواست‌های بعدی از میزبان‌های نامعلوم استفاده می‌شود.

توجه: به صورت پیش‌فرض این ویژگی در تمام VLANها غیرفعال است. DHCP Snooping بر روی هر VLAN فعال می‌باشد. به شکل ۱ برای پیکربندی در این بخش مراجعه کنید.

مثال ۱: نحوه فعال‌کردن و تأیید DHCP Snooping process/feature

```
Switch-2# show feature |i dhcp-snooping
dhcp-snooping 1 disabled
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# feature dhcp
Switch-2(config)# show feature |i dhcp-snooping
dhcp-snooping 1 enabled
Switch-2(config)#
Switch-2(config)# show running-config dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:08:40 2009
version 4.2(2a)
feature dhcp
service dhcp
ip dhcp relay
Switch-2(config)#
```



شکل ۱ توپولوژی DHCP Snooping

مثال ۲: نحوه فعال‌کردن DHCP Snooping در سطح عمومی

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# ip dhcp snooping
Switch-2(config)# show running-config dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:11:05 2009
version 4.2(2a)
feature dhcp
ip dhcp snooping
service dhcp
ip dhcp relay
Switch-2(config)#
```

مثال ۳: فعال‌کردن DHCP Snooping براساس VLAN

```
Switch-2(config)# ip dhcp snooping vlan 5,10,100,500
Switch-2(config)# show runn dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:12:28 2009
```

```
version 4.2(2a)
feature dhcp
ip dhcp snooping
ip dhcp snooping vlan 5,10,100,500
service dhcp
ip dhcp relay
Switch-2(config)
```

اگر دستگاه بسته‌ای را در یک واسط نامعلوم دریافت کند و Source MAC Address و آدرس سخت افزاری سرویس‌گیرنده DHCP مطابق نباشند، تأیید آدرس باعث می‌شود که دستگاه بسته را دراپ کند.

مثال ٤: نحوه فعال‌کردن تأیید DHCP Snooping MAC Address

```
Switch-2(config)# ip dhcp snooping verify mac-address
```

مثال ٥: نحوه پیکربندی واسط اترنت ۱/۱ منبع قابل اعتماد از پیام‌های DHCP

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# int e1/1
Switch-2(config-if)# ip dhcp snooping trust
Switch-2(config-if)# exit
Switch-2# show running-config dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:16:13 2009
version 4.2(2a)
feature dhcp
interface Ethernet1/1
ip dhcp snooping trust
ip dhcp snooping
ip dhcp snooping vlan 5,10,100,500
service dhcp
ip dhcp relay
Switch-2#
```

مثال ٦: نحوه تأیید پیکربندی DHCP Snooping

```
Switch-2# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
5,10,100,500
```

```
DHCP snooping is operational on the following VLANs:
5,10,100,500
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface Trusted
------------ -------
Ethernet1/1 Yes
Switch-2#
Switch-2# show ip dhcp snooping binding
MacAddress IpAddress LeaseSec Type VLAN Interface
0050.561f.73d3 10.10.10.211 1600 dynamic 100 ethernet4/1
---------------- --------------- -------- ---------- ---- -------------
Switch-2#
```

جدول DHCP binding MAC Address سرویس‌گیرنده را نشان می‌دهد؛ آدرس IP سرویس گیرنده به وسیله سرویس‌دهنده DHCP تعیین شده است.

۳ پیکربندی DAI[۱]

پروتکل ARP با نگاشت یک IP address به MAC address در دامنه همه‌پخشی لایه ۲، ارتباطات IP را فراهم می‌کند. مسائل امنیتی شناخته‌شده مرتبط با ARP، مانند حملات Snooping و Snooping ARP، با ارسال اطلاعات غلط به حافظه‌های ARP دستگاه‌های متصل به زیرشبکه بر روی میزبان‌ها، سوئیچ‌ها و مسیریاب‌های متصل به لایه‌ی ۲ شبکه تأثیر می‌گذارند.

DAI تضمین می‌کند که فقط درخواست‌هایARP معتبر هستند و پاسخ داده می‌شوند. هنگامی‌که DAI به درستی پیکربندی و فعال می‌شود، دستگاه NX-OS اقدامات زیر را انجام می‌دهد:

- تمام درخواست‌ها و پاسخ‌های ARP روی درگاه‌های غیرقابل اعتماد را متوقف می‌کند.
- اطمینان حاصل می‌کند که هر یک از این بسته‌های متوقف شده قبل از به‌روزرسانی حافظه ARP محلی یا قبل از ارسال بسته به مقصد معین، یک IP-to-MAC address binding معتبر دارد.
- دور انداختن بسته‌های ARP نامعتبر

[۱] Dynamic ARP Inspection

مثال ۷: نحوه فعال‌کردن DAI برای VLAN 10

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# ip arp inspection vlan 10
Switch-2(config)# show ip arp inspection vlan 10
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
Vlan : 10
-----------
Configuration : Enabled
Operation State : Active
Switch-2(config)#
```

۳-۱ حالت اطمینان DAI

یک دستگاه بسته‌های ARP را ارسال می‌کند و در واسط کاربری قابل اعتماد لایه‌ی ۲ دریافت می‌کند اما آنها را بررسی نمی‌کند. در واسط کاربری غیرقابل اعتماد، دستگاه تمام درخواست‌ها و پاسخ‌های ARP را متوقف می‌کند و اطمینان می‌دهد که بسته‌های متوقف شده قبل از به‌روزرسانی حافظه محلی و ارسال بسته به مقصد معین دارای IP-to-MAC address binding معتبر هستند.

توجه: به صورت پیش‌فرض، تمام واسط‌ها غیرقابل‌اعتماد هستند.

مثال ۸: پیکربندی DAI Trust State یک واسط لایه ی ۲

```
Switch-2(config)# int e1/1
Switch-2(config-if)# ip arp inspection trust
Switch-2(config-if)# show ip arp inspection int e1/1
Interface Trust State
-------------- -----------
Ethernet1/1 Trusted
Switch-2(config-if)#
```

مثال ۹: اعمال ACLها به VLAN برای محدودسازی DAI

```
Switch-2(config)# arp access-list arp-list
Switch-2(config-arp-acl)# 10 permit request ip 10.10.10.12 0.0.0.0 mac 0050.561f.73d3
EEEE.EEEE.EEEE
Switch-2(config-arp-acl)# exit
Switch-2(config)# ip arp inspection filter arp-list vlan 10
Switch-2(config)# show ip arp inspection vlan 10
```

```
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
Vlan : 10
-----------
Configuration : Enabled
Operation State : Active
ACL Match : arp-list
Switch-2(config)#
```

مثال ۱۰: فعال‌کردن اعتبارسنجی DAI اضافی

```
Switch-2(config)# ip arp inspection validate src-mac dst-mac ip
Switch-2(config)# show running-config dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:42:12 2009
version 4.2(2a)
feature dhcp
interface Ethernet1/1
ip dhcp snooping trust
ip arp inspection trust
ip dhcp snooping
ip dhcp snooping vlan 5,10,100,500
service dhcp
ip dhcp relay
ip arp inspection validate src-mac dst-mac ip
ip arp inspection vlan 10
ip arp inspection filter arp-list vlan 10
Switch-2(config)#
```

مثال ۱۱: نحوه تأیید پیکربندی DAI

```
Switch-2# show ip arp inspection
Source Mac Validation : Enabled
Destination Mac Validation : Enabled
IP Address Validation : Enabled
Vlan : 1
-----------
Configuration : Disabled
Operation State : Inactive
Vlan : 5
-----------
Configuration : Disabled
Operation State : Inactive
Vlan : 10
-----------
```

```
Configuration : Enabled
Operation State : Active
ACL Match : arp-list
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped = 2
ARP Res Dropped = 6
DHCP Drops = 8
DHCP Permits = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req = 0
IP Fails-ARP Res = 0
Vlan : 100
-----------
Configuration : Disabled
Operation State : Inactive
Vlan : 500
-----------
Configuration : Disabled
Operation State : Inactive
Switch-2# show ip arp inspection interface ethernet 1/1
Interface Trust State
------------- -----------
Ethernet1/1 Trusted
Switch-2# show ip arp inspection vlan 10
Source Mac Validation : Enabled
Destination Mac Validation : Enabled
IP Address Validation : Enabled
Vlan : 10
-----------
Configuration : Enabled
Operation State : Active
ACL Match : arp-list
Switch-2# show arp access-lists
ARP access list arp-list
10 permit request ip 10.10.10.12 255.255.255.0 mac 0050.561f.73d3 eeee.eeee
Switch-2#
```

٤ پیکربندی IP Source Guard

IP Source Guard بر روی هر یک از واسط‌های محدودیت‌ساز ترافیک پیکربندی شده است و تنها در صورتی اجازه ترافیک IP را می‌دهد که آدرس IP و آدرس MAC هر بسته با یکی از دو منبع IP & MAC address binding منطبق شود:

- ✓ ورودی‌ها در جدول DHCP snooping binding
- ✓ ورودی‌های استاتیک منبع IP

محدودسازی IP & MAC address bindingهای مورد اعتماد به جلوگیری از حملات spoofing، که در آنها مهاجم از آدرس IP یک میزبان معتبر برای دسترسی غیرمجاز به شبکه استفاده می‌کند، کمک می‌کند. برای دور زدن IP Source Guard، مهاجم باید هر دو آدرس IP و آدرس MAC یک میزبان معتبر را spoof کند. شما می‌توانید IP Source Guard را در واسط‌های لایه ۲ فعال کنید که توسط snooping DHCP مورد اعتماد نیستند. IP Source Guard از رابط‌هایی که برای کار در حالت دسترسی و حالت trunk پیکربندی شده‌اند، پشتیبانی می‌کند. به جز در موارد زیر، زمانی‌که اول IP Source Guard را فعال می‌کنید تمام ترافیک IP ورودی روی واسط مسدود می‌شود:

- بسته‌های DHCP، که DHCP snooping آن را بررسی و سپس فورووارد و یا دراپ می‌کند، به نتایج بررسی بسته‌ها وابسته‌اند.
- ترافیک IP ورودی‌های منبع IP استاتیک که در دستگاه NX-OS سیسکو پیکربندی شده است.

مثال ۱۲: چگونگی فعال‌کردن IP Source Guard در واسط لایه ۲ مربوط به Ethernet 1/1

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# interface ethernet 1/1
Switch-2(config-if)# ip verify source dhcp-snooping-vlan
Switch-2(config-if)# show running-config dhcp
!Command: show running-config dhcp
!Time: Thu Oct 1 18:47:28 2009
version 4.2(2a)
feature dhcp
interface Ethernet1/1
ip dhcp snooping trust
ip arp inspection trust
ip verify source dhcp-snooping-vlan
ip dhcp snooping
ip dhcp snooping vlan 5,10,100,500
service dhcp
```

```
ip dhcp relay
ip arp inspection validate src-mac dst-mac ip
ip arp inspection vlan 10
ip arp inspection filter arp-list vlan 10
Switch-2(config-if)#
```

مثال ۱۳: این مثال نشان می‌دهد که چگونه می‌توانید یک ورودی منبع IP استاتیکی را در واسط اترنت ۱/۱ اضافه کنید.

```
Switch-2(config)# ip source binding 10.10.10.12 0050.561f.73d3 vlan 10 interface e1
Switch-2(config)# show ip dhcp snooping binding
MacAddress IpAddress LeaseSec Type VLAN Interface
------------------------------------------------------------------------------
00:50:56:1f:73:d3 10.10.10.12 infinite static 10 Ethernet1/1
Switch-2(config)#
```

۵ پیکربندی مدیریت Keychain

مدیریت Keychain شامل ایجاد و نگهداری keychainها، که دنباله‌ای از کلیدها یا رمزهای به اشتراک گذاشته شده است، می‌باشد. از Keychainها می‌توان توسط ویژگی‌هایی از قبیل برقراری امنیت و ارتباطات مجاز پروتکل‌های مسیریابی با سایر دستگاه‌ها استفاده کرد.

مثال ۱٤: این مثال چگونگی پیکربندی مدیریت keychain و ایجاد یک keychain را نشان می‌دهد.

```
Switch-2(config)# key chain nexus
Switch-2(config-keychain)#
```

مثال ۱۵: این مثال چگونگی پیکربندی کلید برای keychain را نشان می‌دهد. پیش‌فرض را قبول می‌کند و همیشه برای یک کلید جدید ارسال می‌کند.

```
Switch-2(config-keychain)# key 7010
Switch-2(config-keychain)#
```

مثال ۱٦: چگونگی ارتباط keychain را نشان می‌دهد. این مثال نشان می‌دهد که keychain با احرازهویت OSPF ارتباط دارد.

```
ip ospf authentication key-chain nexus
```

مثال ۱۷: اتصال و مدیریت Keychain را تأیید می‌کند.

```
Switch-2# show key chain nexus
Key-Chain nexus
Key 1 -- text 7 070124545b1a12000e
accept lifetime (always valid) [active]
send lifetime (always valid) [active]
Switch-2# show ip ospf
Area BACKBONE(0.0.0.0)
Area has existed for 1d00h
Interfaces in this area: 3 Active interfaces: 3
Passive interfaces: 0 Loopback interfaces: 1
Message-digest authentication
SPF calculation has run 15 times
Last SPF ran for 0.000527s
Area ranges are
Number of LSAs: 8, checksum sum 0x3c6ce
```

٦ پیکربندی Traffic Storm Control

Traffic Storm زمانی رخ می‌دهد که بسته‌ها شبکه را سد کنند و باعث ایجاد ترافیک بیش از حد عملکرد شبکه شوند. خصوصیات Traffic Storm Control در NX-OS مانع از وقفه در درگاه‌های لایه ۲ توسط یک broadcast، multicast، و یا unicast traffic storm ناشناخته، بر روی واسط‌های فیزیکی می‌شوند. در NX-OS، مدیر اجازه نظارت بر سطوح ترافیک broadcast، multicast، و ترافیک Unicast دریافتی در یک فاصله زمانی ۱ ثانیه‌ای را دارد. در طول فاصله ۱ ثانیه، سطح ترافیک با سطح Traffic Storm Control پیکربندی شده مقایسه می‌شود. سطوح Storm Control به عنوان درصدی از پهنای‌باند موجود درگاه پیکربندی شده است. اگر ترافیک ورودی به سطح Traffic Storm Control پیکربندی شده به درصدی از پهنای باند درگاه برسد، تا زمانی که فاصله زمانی تمام شود، Traffic Storm Control را از بین می‌برد.

مثال ۱۸: نحوه پیکربندی Traffic Storm Control همه‌پخشی در واسط اترنت ۱/۱ را نشان می‌دهد.

```
Switch-2(config)# interface ethernet 1/1
Switch-2(config-if)# storm-control broadcast level 20
```

مثال ۱۹: درصد پهنای باند Storm Control همه‌پخشی روی واسط اترنت ۱/۱ را تأیید می‌کند.

```
Switch-2# show interface ethernet 1/1 counters storm-control
Port UcastSupp % McastSupp % BcastSupp % TotalSuppDiscards
--------------------------------------------------------------------------------
```

```
Eth1/1 100.00 100.00 20.00 0
Switch-2#
Switch-2# show interface ethernet 1/1 counters storm-control
--------------------------------------------------------------------------------
Port UcastSupp % McastSupp % BcastSupp % TotalSuppDiscards
--------------------------------------------------------------------------------
Eth1/1 100.00 100.00 20.00 0
Switch-2#
```

مثال ۲۰: نحوه پیکربندی Traffic Storm Control چندپخشی روی واسط اترنت ۱/۱ را نشان می‌دهد.

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# interface ethernet 1/1
Switch-2(config-if)# storm-control multicast level 20
```

مثال ۲۱: درصد پهنای باند Storm Control چندپخشی در واسط اترنت ۱/۱ را تأیید می‌کند.

```
Switch-2# show interface ethernet 1/1 counters storm-control
--------------------------------------------------------------------------------
-----
Port UcastSupp % McastSupp % BcastSupp % TotalSuppDiscar
--------------------------------------------------------------------------------
Eth1/1 100.00 20.00 20.00
Switch-2#
```

مثال ۲۲: نشان می‌دهد که چگونه Unicast Traffic Storm Control را روی واسط اترنت ۱/۱ پیکربندی کنید.

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# interface ethernet 1/1
Switch-2(config-if)# storm-control unicast level 20
Switch-2(config-if)#
```

مثال ۲۳: درصد پهنای باند کنترل طوفان Unicast در واسط اترنت ۱/۱ را تأیید می‌کند.

```
Switch-2# show interface ethernet 1/1 counters storm-control
--------------------------------------------------------------------------------
Port UcastSupp % McastSupp % BcastSupp % TotalSuppDiscar
--------------------------------------------------------------------------------
Eth1/1 20.00 20.00 20.00
```

```
Switch-2#
```

۷ پیکربندی Unicast RPF[۲]

Unicast RPF شانس‌های ناقص یا جعلی[۳] آدرس‌های IPv4 یا IPv6 منبع به یک شبکه را، با از بین بردن بسته‌های IPv4 یا IPv6 که آدرس IP منبع معتبری ندارند، کاهش می‌دهد. چندین تهدید امنیتی و یا انواع حملات مانند حملات منع سرویس (DoS)، حملات Smurf، و حملات TFN، از جعل یا تغییرات سریع آدرس‌های IPv4 یا IPv6 منبع استفاده می‌کنند. Unicast RPF با فرستادن تنها بسته‌هایی که دارای آدرس منبع های معتبر و سازگار با جدول مسیریابی IP هستند، حملات را منحرف می‌کنند. هنگامی‌که Unicast RPF روی یک واسط فعال می‌شود، دستگاه NX-OS تمامی‌بسته‌های ورودی دریافت شده در آن واسط را بررسی می‌کند تا اطمینان حاصل شود که آدرس منبع و واسط منبع که در جدول مسیریابی ظاهر می‌شود با واسطی که بسته را دریافت کرده است، مطابقت دارد.

RFP Unicast را می‌توان در دو حالت مختلف در واسط کاربری ورودی پیکربندی کرد:

- حالت Strict Unicast RPF

بررسی حالت Strict هنگامی موفقیت‌آمیز است که Unicast RFP در FIB برای آدرس منبع بسته تطبیقی پیدا کند، و واسط کاربری ورودی از طریق آن بسته دریافت شده با یکی از واسط‌های Unicast RPF در FIB مطابقت پیدا کند. اگر این بررسی ناکام باشد، بسته حذف می‌شود. شما می‌توانید هنگامی‌که جریان‌های بسته به صورت متقارن هستند، از این نوع برای تأیید Unicast RPF استفاده کنید.

- حالت Loose Unicast RPF

چک کردن حالت Loose زمانی موفق می‌شود که جستجوی یک آدرس منبع بسته در FIB، تطبیقی را برمی گرداند و نتیجه FIB نشان دهد که منبع از طریق حداقل یک واسط واقعی قابل دستیابی است. رابط ورودی که از طریق آن بسته دریافت می‌شود نیازمند مطابقت با هر واسط در نتیجه‌ی FIB نیست.

---

[۲] Reverse Path Forwarding

[۳] Spoofed

مثال ۲٤: نحوه پیکربندی Unicast RPF در واسط اترنت ۱/۱ برای IPv4 را نشان می‌دهد.

```
Switch-2(config)# interface ethernet 1/1
Switch-2(config-if)# ip address 20.20.20.20 255.0.0.0
Switch-2(config-if)#ip verify unicast source reachable-via any
Switch-2(config-if)# exit
```

مثال ۲۵: Unicast RPF را برای IPv4 بر روی واسط اترنت ۱/۱ تأیید می‌کند.

```
Switch-2(config)# show ip interface ethernet 1/1
IP Interface Status for VRF "default"(1)
Ethernet1/1, Interface status: protocol-up/link-up/admin-up, iod: 99,
IP address: 20.20.20.20, IP subnet: 20.0.0.0/8
IP broadcast address: 255.255.255.255
IP multicast groups locally joined: none
IP MTU: 9216 bytes (using link MTU)
IP primary address route-preference: 0, tag: 0
IP proxy ARP : disabled
IP Local Proxy ARP : disabled
IP multicast routing: disabled
IP icmp redirects: enabled
IP directed-broadcast: disabled
IP icmp unreachables (except port): disabled
IP icmp port-unreachable: enabled
IP unicast reverse path forwarding: loose
IP interface statistics last reset: never
IP interface software stats: (sent/received/forwarded/originated/consume
Unicast packets : 0/0/0/0/0
Unicast bytes : 0/0/0/0/0
Multicast packets : 0/0/0/0/0
Multicast bytes : 0/0/0/0/0
Broadcast packets : 0/0/0/0/0
Broadcast bytes : 0/0/0/0/0
Labeled packets : 0/0/0/0/0
Labeled bytes : 0/0/0/0/0
Switch-2(config)# exit
Switch-2 # show running-config interface ethernet 1/1
!Command: show running-config interface Ethernet1/1
!Time: Thu Oct 1 20:06:53 2009
version 4.2(2a)
interface Ethernet1/1
description to Switch-1
mtu 9216
ip address 20.20.20.20/8
ip verify unicast source reachable-via any
no shutdown
```

۸ پیکربندی Control Plane Policing

دستگاه NX-OS سیسکو سیاست‌هایی برای واحد کنترل ارائه می‌دهد تا از حملات DoS جلوگیری کند.

واحد سرپرستی ترافیک را به سه واحد کاربردی تقسیم می‌کند:

- واحد داده‌ها: بسته‌ها را از یک واسط به دیگری می‌فرستد؛ بسته‌ها برای سوئیچ از قبل تعیین شده نیستند.
- واحد کنترل: بسته‌ها را بین دستگاه‌ها کنترل می‌کند، بسته‌ها به مقصد مسیریاب آدرس می‌دهند.
- واحد مدیریت: واحد سرپرستی هر دو واحد مدیریت و کنترل را دارد و برای عملکرد شبکه حیاتی است.

به طور پیش‌فرض، هنگام بارگذاری برای اولین بار دستگاه NX-OS سیسکو، نرم‌افزار NX-OS سیسکو سیستم پیش‌فرض copp-system-policy را برای حفاظت واحد سرپرستی از حملات DoS نصب می‌کند. شما می توانید سطح حفاظت را با انتخاب یکی از گزینه‌های CoPP پیکربندی کنید:

- Strict
- Moderate
- Lenient
- None

برای تغییر سیاست پیش‌فرض CoPP از طریق اسکریپت راه‌اندازی اولیه، موارد زیر را وارد کنید:

```
Configure best practices CoPP profile
(strict/moderate/lenient/none) [strict]:
```

مثال ۲۶: سیاست پیش‌فرض Strict، سیستم کاری copp را نشان می‌دهد که می‌تواند بر اساس الزامات خاصی تغییر کند.

```
Switch-1(config-acl)# ip access-list copp-system-acl-igmp
Switch-1(config-acl)# 10 permit igmp any 224.0.0.0/3
Switch-1(config-acl)# ip access-list copp-system-acl-msdp
Switch-1(config-acl)# 10 permit tcp any gt 1024 any eq 639
Switch-1(config-acl)# 20 permit tcp any eq 639 any gt 1024
Switch-1(config-acl)# ip access-list copp-system-acl-ntp
Switch-1(config-acl)# 10 permit udp any any eq ntp
Switch-1(config-acl)# 20 permit udp any eq ntp any
Switch-1(config-acl)# ipv6 access-list copp-system-acl-ntp6
Switch-1(config-acl)# 10 permit udp any any eq ntp
Switch-1(config-acl)# 20 permit udp any eq ntp any
```

```
Switch-1(config-acl)# 20 permit tcp any eq bgp any gt 1024
Switch-1(config-acl)# ip access-list copp-system-acl-cts
Switch-1(config-acl)# 10 permit tcp any any eq 64999
Switch-1(config-acl)# 20 permit tcp any eq 64999 any
Switch-1(config-acl)# ip access-list copp-system-acl-dhcp
Switch-1(config-acl)# 10 permit udp any eq bootpc any
Switch-1(config-acl)# 20 permit udp any eq bootps any
Switch-1(config-acl)# 30 permit udp any any eq bootpc
Switch-1(config-acl)# 40 permit udp any any eq bootps
Switch-1(config-acl)# ip access-list copp-system-acl-eigrp
Switch-1(config-acl)# 10 permit eigrp any any
Switch-1(config-acl)# ip access-list copp-system-acl-ftp
Switch-1(config-acl)# 10 permit tcp any any eq ftp-data
Switch-1(config-acl)# 20 permit tcp any any eq ftp
Switch-1(config-acl)# 30 permit tcp any eq ftp-data any
Switch-1(config-acl)# 40 permit tcp any eq ftp any
Switch-1(config-acl)# ip access-list copp-system-acl-glbp
Switch-1(config-acl)# 10 permit udp any eq 3222 224.0.0.0/24 eq 3222
Switch-1(config-acl)# ip access-list copp-system-acl-hsrp
Switch-1(config-acl)# 10 permit udp any 224.0.0.0/24 eq 1985
Switch-1(config-acl)# ip access-list copp-system-acl-icmp
Switch-1(config-acl)# 10 permit icmp any any echo
Switch-1(config-acl)# 20 permit icmp any any echo-reply
Switch-1(config-acl)# ipv6 access-list copp-system-acl-icmp6
Switch-1(config-acl)# 10 permit icmp any any echo-request
Switch-1(config-acl)# 20 permit icmp any any echo-reply
Switch-1(config-acl)# ipv6 access-list copp-system-acl-icmp6-msgs
Switch-1(config-acl)# 10 permit icmp any any router-advertisement
Switch-1(config-acl)# 20 permit icmp any any router-solicitation
Switch-1(config-acl)# 30 permit icmp any any nd-na
Switch-1(config-acl)# 40 permit icmp any any nd-ns
Switch-1(config-acl)# 50 permit icmp any any mld-query
Switch-1(config-acl)# 60 permit icmp any any mld-report
Switch-1(config-acl)# 70 permit icmp any any mld-reduction
Switch-1(config-acl)# ip access-list copp-system-acl-igmp
Switch-1(config-acl)# 10 permit igmp any 224.0.0.0/3
Switch-1(config-acl)# ip access-list copp-system-acl-msdp
Switch-1(config-acl)# 10 permit tcp any gt 1024 any eq 639
Switch-1(config-acl)# 20 permit tcp any eq 639 any gt 1024
Switch-1(config-acl)# ip access-list copp-system-acl-ntp
Switch-1(config-acl)# 10 permit udp any any eq ntp
Switch-1(config-acl)# 20 permit udp any eq ntp any
Switch-1(config-acl)# ipv6 access-list copp-system-acl-ntp6
Switch-1(config-acl)# 10 permit udp any any eq ntp
Switch-1(config-acl)#20 permit udp any eq ntp any
Switch-1(config-acl)#10 permit tcp any any eq tacacs
Switch-1(config-acl)# 20 permit tcp any eq tacacs any
Switch-1(config-acl)# ipv6 access-list copp-system-acl-tacacs6
Switch-1(config-acl)# 10 permit tcp any any eq tacacs
Switch-1(config-acl)# 20 permit tcp any eq tacacs any
Switch-1(config-acl)# ip access-list copp-system-acl-telnet
```

```
Switch-1(config-acl)# 10 permit tcp any any eq telnet
Switch-1(config-acl)# 20 permit tcp any any eq 107
Switch-1(config-acl)# 30 permit tcp any eq telnet any
Switch-1(config-acl)# 40 permit tcp any eq 107 any
Switch-1(config-acl)# ipv6 access-list copp-system-acl-telnet6
Switch-1(config-acl)# 10 permit tcp any any eq telnet
Switch-1(config-acl)# 20 permit tcp any any eq 107
Switch-1(config-acl)# 30 permit tcp any eq telnet any
```

```
Switch-1(config-acl)# 40 permit tcp any eq 107 any
Switch-1(config-acl)# ip access-list copp-system-acl-tftp
Switch-1(config-acl)# 10 permit udp any any eq tftp
Switch-1(config-acl)# 20 permit udp any any eq 1758
Switch-1(config-acl)# 30 permit udp any eq tftp any
Switch-1(config-acl)# 40 permit udp any eq 1758 any
Switch-1(config-acl)# ipv6 access-list copp-system-acl-tftp6
Switch-1(config-acl)# 10 permit udp any any eq tftp
Switch-1(config-acl)# 20 permit udp any any eq 1758
Switch-1(config-acl)# 30 permit udp any eq tftp any
Switch-1(config-acl)# 40 permit udp any eq 1758 any
Switch-1(config-acl)# ip access-list copp-system-acl-traceroute
Switch-1(config-acl)# 10 permit icmp any any ttl-exceeded
Switch-1(config-acl)# 20 permit icmp any any port-unreachable
Switch-1(config-acl)# ip access-list copp-system-acl-undesirable
Switch-1(config-acl)# 10 permit udp any any eq 1434
Switch-1(config-acl)# ip access-list copp-system-acl-vpc
Switch-1(config-acl)# 10 permit udp any any eq 3200
Switch-1(config-acl)# ip access-list copp-system-acl-vrrp
Switch-1(config-acl)#10 permit 112 any 224.0.0.0/24
Switch-1(config-acl)#ip access-list copp-system-acl-wccp
Switch-1(config-acl)# 10 permit udp any eq 2048 any eq 2048
Switch-1(config-acl)# mac access-list mac-acl
Switch-1(config-acl)# statistics per-entry
```

```
Switch-1(config-acl)# 200 permit 0050.561f.73d3 0050.56bc.48dd any
Switch-1(config-acl)# 210 permit 0050.561f.73d3 0000.00ff.ffff any
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
critical
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-bgp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-bgp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-eigrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-igmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-msdp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-rip
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-vpc
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
exception
Switch-1(config-cmap-qos)# match exception ip option
```

```
Switch-1(config-cmap-qos)# match exception ip icmp unreachable
Switch-1(config-cmap-qos)# match exception ipv6 option
Switch-1(config-cmap-qos)# match exception ipv6 icmp unreachable
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
important
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-cts
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-glbp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-hsrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-vrrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-wccp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6-msgs
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim-reg
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
management
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ftp
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-ntp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ntp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-radius
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-sftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-snmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-telnet
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tftp
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-tftp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-radius6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-telnet6
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
monitoring
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-traceroute
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
normal
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-dhcp
Switch-1(config-cmap-qos)# match redirect dhcp-snoop
Switch-1(config-cmap-qos)# match protocol arp
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
redirect
Switch-1(config-cmap-qos)# match redirect arp-inspect
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
undesirable
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-undesirable
Switch-1(config-cmap-qos)# policy-map type control-plane copp-system-policy
Switch-1(config-cmap-qos)# class copp-system-class-critical
Switch-1(config-cmap-qos)# police cir 39600 kbps bc 250 ms conform transmit violate
drop
Switch-1(config-cmap-qos)# class copp-system-class-important
Switch-1(config-cmap-qos)# police cir 1060 kbps bc 1000 ms conform transmit violate
```

```
drop
Switch-1(config-cmap-qos)# class copp-system-class-management
Switch-1(config-cmap-qos)# police cir 10000 kbps bc 250 ms conform transmit violate
drop
Switch-1(config-cmap-qos)# class copp-system-class-normal
Switch-1(config-cmap-qos)#police cir 680 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-redirect
Switch-1(config-cmap-qos)#police cir 280 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-monitoring
Switch-1(config-cmap-qos)#police cir 130 kbps bc 1000 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-exception
Switch-1(config-cmap-qos)#police cir 360 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-undesirable
Switch-1(config-cmap-qos)# police cir 32 kbps bc 250 ms conform drop violate drop
Switch-1(config-cmap-qos)#class class-default
Switch-1(config-cmap-qos)#police cir 100 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)#control-plane
Switch-1(config-cmap-qos)# service-policy input copp-system-policy
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
critical
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-bgp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-bgp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-eigrp
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-igmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-msdp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-rip
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-vpc
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
exception
Switch-1(config-cmap-qos)# match exception ip option
Switch-1(config-cmap-qos)# match exception ip icmp unreachable
Switch-1(config-cmap-qos)# match exception ipv6 option
Switch-1(config-cmap-qos)#match exception ipv6 icmp unreachable
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
important
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-cts
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-glbp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-hsrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-vrrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-wccp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6-msgs
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim-reg
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
management
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ntp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ntp6
```

```
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-radius
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-sftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-snmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-telnet
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tftp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-radius6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs6
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-telnet6
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
monitoring
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-traceroute
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
normal
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-dhcp
Switch-1(config-cmap-qos)# match redirect dhcp-snoop
Switch-1(config-cmap-qos)# match protocol arp
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
redirect
Switch-1(config-cmap-qos)# match redirect arp-inspect
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-
undesirable
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-undesirable
Switch-1(config-cmap-qos)# policy-map type control-plane copp-system-policy
Switch-1(config-cmap-qos)# class copp-system-class-critical
Switch-1(config-cmap-qos)#police cir 39600 kbps bc 250 ms conform transmit violate
drop
Switch-1(config-cmap-qos)# class copp-system-class-important
Switch-1(config-cmap-qos)# police cir 1060 kbps bc 1000 ms conform transmit violate
drop
Switch-1(config-cmap-qos)# class copp-system-class-management
Switch-1(config-cmap-qos)#police cir 10000 kbps bc 250 ms conform transmit violate
drop
Switch-1(config-cmap-qos)#class copp-system-class-normal
Switch-1(config-cmap-qos)#police cir 680 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-redirect
Switch-1(config-cmap-qos)#police cir 280 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)#
class copp-system-class-monitoring
Switch-1(config-cmap-qos)#police cir 130 kbps bc 1000 ms conform transmit violate drop
Switch-1(config-cmap-qos)#class copp-system-class-exception
Switch-1(config-cmap-qos)#police cir 360 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-undesirable
Switch-1(config-cmap-qos)# police cir 32 kbps bc 250 ms conform drop violate drop
Switch-1(config-cmap-qos)# class class-default
Switch-1(config-cmap-qos)#police cir 100 kbps bc 250 ms conform transmit violate drop
```

```
Switch-1(config-cmap-qos)# control-plane
Switch-1(config-cmap-qos)# service-policy input copp-system-policy
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-critical
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-bgp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-bgp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-eigrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-igmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-msdp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ospf6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-rip
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-vpc
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-exception
Switch-1(config-cmap-qos)# match exception ip option
Switch-1(config-cmap-qos)# match exception ip icmp unreachable
Switch-1(config-cmap-qos)# match exception ipv6 option
Switch-1(config-cmap-qos)#match exception ipv6 icmp unreachable
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-important
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-cts
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-glbp
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-hsrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-vrrp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-wccp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6-msgs
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-pim-reg
Switch-1(config-cmap-qos)#class-map type control-plane match-any copp-system-class-management
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ntp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ntp6
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-radius
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-sftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-snmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-ssh6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-telnet
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tftp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tftp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-radius6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-tacacs6
Switch-1(config-cmap-qos)#match access-group name copp-system-acl-telnet6
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-monitoringSwitch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-icmp6
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-traceroute
```

```
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-normal
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-dhcp
Switch-1(config-cmap-qos)# match redirect dhcp-snoop
Switch-1(config-cmap-qos)# match protocol arp
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-Redirect
Switch-1(config-cmap-qos)# match redirect arp-inspect
Switch-1(config-cmap-qos)# class-map type control-plane match-any copp-system-class-undesirable
Switch-1(config-cmap-qos)# match access-group name copp-system-acl-undesirable
Switch-1(config-cmap-qos)# policy-map type control-plane copp-system-policy
Switch-1(config-cmap-qos)# class copp-system-class-critical
Switch-1(config-cmap-qos)# police cir 39600 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-important
Switch-1(config-cmap-qos)#police cir 1060 kbps bc 1000 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-management
Switch-1(config-cmap-qos)# police cir 10000 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-normal
Switch-1(config-cmap-qos)#police cir 680 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-redirect
Switch-1(config-cmap-qos)#police cir 280 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-monitoring
Switch-1(config-cmap-qos)#police cir 130 kbps bc 1000 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-exception
Switch-1(config-cmap-qos)#police cir 360 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# class copp-system-class-undesirable
Switch-1(config-cmap-qos)# police cir 32 kbps bc 250 ms conform drop violate drop
Switch-1(config-cmap-qos)# class class-default
Switch-1(config-cmap-qos)#police cir 100 kbps bc 250 ms conform transmit violate drop
Switch-1(config-cmap-qos)# control-plane
Switch-1(config-cmap-qos)# service-policy input copp-system-policy
```

۹ پیکربندی محدودیت‌های نرخ

محدودیت نرخ برای خارج‌شدن استثناها از واحد سرپرستی در دستگاه NX-OS سیسکو می‌تواند از هدایت بسته‌ها جلوگیری کند. محدودیت‌های نرخ در بسته‌ها در هر ثانیه برای انواع بسته‌های هدایت شده زیر پیکربندی می‌شوند:

- لیست دسترسی بسته‌های ورودی
- بسته‌های داده و کنترل در واحد سرپرستی کپی شده است

- بسته‌های storm control لایه ۲
- بسته‌های port security لایه ۲
- بسته‌های Glean در لایه ۳
- MTU[٤] لایه ۳ بسته‌های خراب شده را بررسی می‌کند
- بسته‌های مستقیما متصل شده چندپخشی لایه ۳
- بسته‌های گروه محلی چندپخشی لایه ۳
- بسته‌های نشتی RPF چندپخشی لایه ۳
- TTL[٥] لایه ۳ بسته‌های خراب شده را بررسی می‌کند
- بسته‌های کنترل لایه ۳
- بسته‌های دریافتی

فرمان کلی برای پیکربندی محدودیت نرخ به شرح زیر است:

```
Switch(config)# hardware rate-limit {access-list-فایل‌های ثبت وقایع |copy |layer-2 {port-secu-
rity |storm-control} |layer-3 {control |glean |mtu |multicast {directly-connect |local-groups
|rpf-leak} |ttl} |receive} packets
```

محدودیت‌های نرخ فقط به خروجی ترافیک اعمال می‌شود. اگر نیاز دارید که به ورودی خود محدودیت اعمال کنید، از CoPP استفاده کنید.

مثال ۲۷: پیکربندی‌های پیش‌فرض محدودیت نرخ را تأیید می‌کند.

```
Switch-2#
show hardware rate-limiter
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
Rate Limiter Class Parameters
------------------------------------------------------------------------
layer-3 mtu Config : 500
Allowed : 0
Dropped : 0
```

[٤] Maximum Transmission Unit

[٥] Time-To-Live

```
layer-3 multicast directly-connected Config : 3000
Allowed : 0
Dropped : 0
Total : 0
layer-3 multicast local-groups Config : 3000
Allowed : 0
Dropped : 0
Total : 0
layer-3 multicast rpf-leak Config : 500
Allowed : 0
Dropped : 0
Total : 0
layer-2 storm-control Config : Disabled
access-list-Log Config : 100
Allowed : 0
Dropped : 0
Total : 0
copy Config : 30000
Allowed : 197080
Dropped : 0
Total : 197080
receive
Config : 30000
Allowed : 905484
Dropped : 0
Total : 905484
layer-2 port-security Config : Disabled
layer-2 mcast-snooping Config : 10000
Allowed : 21
Dropped : 0
Total : 21
Switch-2#
```

مثال ۲۸: نشان می‌دهد که چگونه محدودیت‌های نرخ در بسته‌های کنترل لایه ۳ را پیکربندی کنید.

```
Switch-1(config)# hardware rate-limiter layer-3 control 50000
```

مثال ۲۹: نشان می‌دهد که چگونه پیکربندی نرخ برای بسته‌های Glean لایه ۳ را پیکربندی کنید.

```
Switch-1(config)# hardware rate-limiter layer-3 glean 500
```

مثال ۳۰: نشان می‌دهد که چگونه محدودیت‌های نرخ را برای محدودیت‌های storm control لایه ۲ پیکربندی کنید.

```
Switch-1(config)# hardware rate-limiter layer-2 storm-control 60000
```

مثال ۳۱: نشان می‌دهد چگونه تغییرات و پیکربندی محدودیت نرخ را تأیید کنید.

```
Dropped : 0
Total : 3
Switch-1# show hardware rate-limiter layer-2 storm-control
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
Rate Limiter Class Parameters
-----------------------------------------------------------------------
layer-2 storm-control Config : 60000
Allowed : 113
Dropped : 1
Total : 114
Switch-1# show hardware rate-limiter
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
Rate Limiter Class Parameters
-----------------------------------------------------------------------
layer-3 mtu Config : 500
Allowed : 0
Dropped : 0
Total : 0
layer-3 ttl Config : 500
Allowed : 7771
Dropped : 0
Total : 7771
layer-3 control Config : 50000
Allowed : 1042557
Dropped : 0
Total : 1042557
layer-3 glean Config : 500
Allowed : 3
Dropped : 0
Total : 3
layer-3 multicast directly-connected Config : 3000
Allowed : 0
Dropped : 0
Total : 0
layer-3 multicast local-groups Config : 3000
Allowed : 0
Dropped : 0
Total : 0
layer-3 multicast rpf-leak Config : 500
Allowed : 0
Dropped : 0
Total : 0
```

```
layer-2 storm-control Config : 60000
Allowed : 126
Dropped : 1
Total : 127
access-list-Log Config : 100
Allowed : 0
Dropped : 0
Total : 0
copy Config : 30000
Allowed : 2634651
Dropped : 0
Total : 2634651
receive Config : 30000
Allowed : 8275085
Dropped : 0
Total
: 8275085
layer-2 port-security Config : Disabled
layer-2 mcast-snooping Config : 10000
Allowed : 0
Dropped : 0
Total : 0
Switch-1#
```

۱۰ پیکربندی SNMPv3

این بخش فقط SNMPv3 را پوشش می‌دهد. SNMPv3 دسترسی امن دستگاه‌ها را با ترکیبی از چارچوب‌های احرازهویت و رمزگذاری بر روی شبکه فراهم می‌کند. ویژگی‌های امنیتی ارائه شده در SNMPv3 عبارتند از:

- یکپارچگی پیام: اطمینان حاصل می‌کند که یک بسته دستکاری نشده است
- احرازهویت: پیام از یک منبع معتبر است
- رمزگذاری: جلوگیری از منابع غیر مجاز

SNMPv3 برای هر دو مدل‌های امنیتی و سطوح امنیتی ارائه شده است. یک مدل امنیتی استراتژی احرازهویت برای کاربر و نقشی است که کاربر در آن قرار دارد. سطح امنیتی سطح مجاز امنیت در یک مدل امنیتی است. ترکیبی از یک مدل امنیتی و یک سطح امنیتی تعیین‌کننده‌ی این است که کدام مکانیزم امنیتی هنگام مدیریت یک بسته SNMP استفاده می‌شود.

مثال ۳۲: نحوه پیکربندی احرازهویت و حفظ حریم خصوصی کاربران با پیکربندی SNMP را نشان می‌دهد.

```
Switch-2(config)# snmp-server user manager auth sha MGTUser123 priv MGTUser
Switch-2(config)# show snmp user
```

```
SNMP USERS
User Auth Priv(enforce) Groups
____ ____ _____________ _______
admin md5 des(no) network-admin
manager sha des(no) network-operator
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
Switch-2(config)#
```

مثال ۳۳: نحوه اجرای رمزگذاری پیام SNMP برای هر کاربر پایه را نشان می‌دهد.

```
Switch-2(config)# snmp-server user manager enforcePriv
Switch-2(config)# show snmp user
SNMP USERS
---------------------------------------------------------------------
User Auth Priv(enforce) Groups
____ ____ _____________ _______
admin md5 des(no) network-admin
manager sha des(no) network-operator
enforcePriv
---------------------------------------------------------------------
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
User Auth Priv
____ ____ ____
```

مثال ۳٤: نحوه اجرای رمزگذاری پیام برای همه کاربران را نشان می‌دهد.

```
Switch-2(config)# snmp-server globalEnforcePriv
Switch-2(config)# show snmp user
SNMP USERS [global privacy flag enabled]
---------------------------------------------------------------------
User Auth Priv(enforce) Groups
____ ____ _____________ _______
admin md5 des(no) network-admin
manager sha des(no) network-operator
enforcePriv
---------------------------------------------------------------------
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
User Auth Priv
____ ____ ____
Switch-2(config)#
```

مثال ۳۵: نحوه اعمال کاربران SNMPv3 برای چندین نقش را نشان می‌دهد.

```
Switch-2(config)# snmp-server user manager network-admin
Switch-2(config)# show snmp user
SNMP USERS [global privacy flag enabled]
------------------------------------------------------------------------
User Auth Priv(enforce) Groups
____ ____ _____________ _______
admin md5 des(no) network-admin
manager sha des(no) network-operator
enforcePriv
network-admin
------------------------------------------------------------------------
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
User Auth Priv
____ ____ ____
Switch-2(config)# show role
Role: network-admin
Description: Predefined network admin role has access to all commands
on the switch
Rule Perm Type Scope Entity
------------------------------------------------------------------------
1 permit read-write
Role: network-operator
Description: Predefined network operator role has access to all read
commands on the switch
Rule Perm Type Scope Entity
1 permit read
Role: vdc-admin
Description: Predefined vdc admin role has access to all commands with
a VDC instance
Rule Perm Type Scope Entity
------------------------------------------------------------------------
1 permit read-write
Role: vdc-operator
Description: Predefined vdc operator role has access to all read comm
within a VDC instance
Rule Perm Type Scope Entity
------------------------------------------------------------------------
1 permit read
Role: enforcePriv
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
Switch-2(config)#
```

مثال ۳۶: نحوه ایجاد SNMP communities را نشان می‌دهد. SNMP communities مجموعه ای از میزبان هایی است که برای اهداف اداری گروه‌بندی می‌شوند.

```
Switch-2(config)# snmp-server community public ro
Switch-2(config)# snmp-server community private rw
Switch-2(config)# show snmp community
Community Group / Access context acl_filter
--------- -------------- ------- ----------
public network-operator
private network-admin
Switch-2(config)#
```

مثال ۳۷: نحوه پیکربندی گیرنده‌های اعلان را نشان می‌دهد. برای مثال، گیرنده اعلان می‌تواند تعیین کند که آیا یک اعلان پیام syslog شامل عناصر داده ساخت‌یافته از یک پیام SYSLOG است.

```
Switch-2(config)# snmp-server host 10.10.10.12 informs version 3 priv private
Switch-2(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
10.10.10.12 162 v3 priv inform private
Switch-2(config)#Configuring a Source Interface for SNMP Notifications
Switch-2(config)#show snmp source-interface
Notification source-interface
-------------------------------------------------------------------
trap -
inform -
```

مثال ۳۸: نحوه پیکربندی واسط منبع SNMP را نشان می‌دهد. واسط منبع، آدرس IP منبع پیام‌های SMTP را مشخص می‌کند، برای مثال پیام‌های trap.

```
Switch-2(config)# snmp-server source-interface traps loopback 0
Switch-2(config)# show snmp source-interface
Notification source-interface
-------------------------------------------------------------------------------
trap loopback0
inform -
-------------------------------------------------------------------------------
---------------
Switch-2(config)# snmp-server source-interface informs loopback 0
Switch-2(config)# show snmp source-interface
Notification source-interface
-------------------------------------------------------------------------------
trap loopback0
```

```
inform loopback0
------------------------------------------------------------------------------
Switch-2(config)#
```

مثال ۳۹: نحوه غیرفعال‌کردن اعلان‌های عمومی SNMP LinkUp/LinkDown را نشان می‌دهد.

```
Switch-2# show snmp trap
Trap type
Enabled
------------------------------------------------------------------------------
entity : entity_mib_change Yes
entity : entity_module_status_change Yes
entity : entity_power_status_change Yes
entity : entity_module_inserted Yes
entity : entity_module_removed Yes
entity : entity_unrecognised_module Yes
entity : entity_fan_status_change Yes
entity : entity_power_out_change Yes
link : linkDown Yes
link : linkUp Yes
link : extended-linkDown Yes
link : extended-linkUp Yes
link : cieLinkDown Yes
link : cieLinkUp Yes
callhome : event-notify No
callhome : smtp-send-fail No
cfs : state-change-notif No
cfs : merge-failure No
rf : redundancy_framework Yes
port-security : access-secure-mac-violation No
port-security : trunk-secure-mac-violation No
aaa : server-state-change No
license : notify-license-expiry Yes
license : notify-no-license-for-feature Yes
license : notify-licensefile-missing Yes
license : notify-license-expiry-warning Yes
hsrp : state-change No
upgrade : UpgradeOpNotifyOnCompletion No
upgrade : UpgradeJobStatusNotify No
feature-control : FeatureOpStatusChange No
snmp : authentication No
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# no snmp-server enable traps link linkup
Switch-2(config)#
no snmp-server enable traps link linkdown
Switch-2(config)#
show snmp trap
Trap type
```

```
Enabled
--------------------------------------------------------------------------------
entity : entity_mib_change Yes
entity : entity_module_status_change Yes
entity : entity_power_status_change Yes
entity : entity_module_inserted Yes
entity : entity_module_removed Yes
entity : entity_unrecognised_module Yes
entity : entity_fan_status_change Yes
entity : entity_power_out_change Yes
link : linkDown No
link : linkUp No
link : extended-linkDown Yes
link : extended-linkUp Yes
link : cieLinkDown Yes
link : cieLinkUp Yes
callhome : event-notify No
callhome : smtp-send-fail No
cfs : state-change-notif No
cfs : merge-failure No
rf : redundancy_framework Yes
port-security : access-secure-mac-violation No
port-security : trunk-secure-mac-violation No
aaa : server-state-change No
license : notify-license-expiry Yes
license : notify-no-license-for-feature Yes
license : notify-licensefile-missing
Yes
license : notify-license-expiry-warning Yes
hsrp : state-change No
upgrade : UpgradeOpNotifyOnCompletion No
upgrade : UpgradeJobStatusNotify No
feature-control : FeatureOpStatusChange No
snmp : authentication No
Switch-2(config)#
```

مثال ٤٠: نحوه غیرفعال‌کردن اعلان‌های SNMP LinkUp/LinkDown در یک واسط خاص را نشان می‌دهد.

```
Switch-2(config)# int e1/1
Switch-2(config-if)# no snmp trap link-status
```

مثال ٤١: نحوه فعال‌کردن اعلان‌های SNMP را نشان می‌دهد.

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# snmp-server enable traps
Switch-2(config)# show snmp trap
```

```
Trap type
Enabled
--------------------------------------------------------------------------------
entity : entity_mib_change Yes
entity : entity_module_status_change Yes
entity : entity_power_status_change Yes
entity : entity_module_inserted Yes
entity : entity_module_removed Yes
entity : entity_unrecognised_module Yes
entity : entity_fan_status_change Yes
entity : entity_power_out_change Yes
link : linkDown Yes
link : linkUp Yes
link : extended-linkDown Yes
link : extended-linkUp Yes
link : cieLinkDown Yes
link : cieLinkUp Yes
callhome : event-notify Yes
callhome : smtp-send-fail Yes
cfs : state-change-notif Yes
cfs : merge-failure Yes
rf : redundancy_framework Yes
port-security : access-secure-mac-violation Yes
port-security : trunk-secure-mac-violation Yes
aaa : server-state-change Yes
license : notify-license-expiry Yes
license : notify-no-license-for-feature Yes
license : notify-licensefile-missing Yes
license : notify-license-expiry-warning Yes
hsrp : state-change Yes
upgrade
: UpgradeOpNotifyOnCompletion Yes
upgrade : UpgradeJobStatusNotify Yes
feature-control : FeatureOpStatusChange Yes
snmp : authentication Yes
Switch-2(config)#
```

۱۱ معرفی ابزارهای امنیتی و مدیریتی

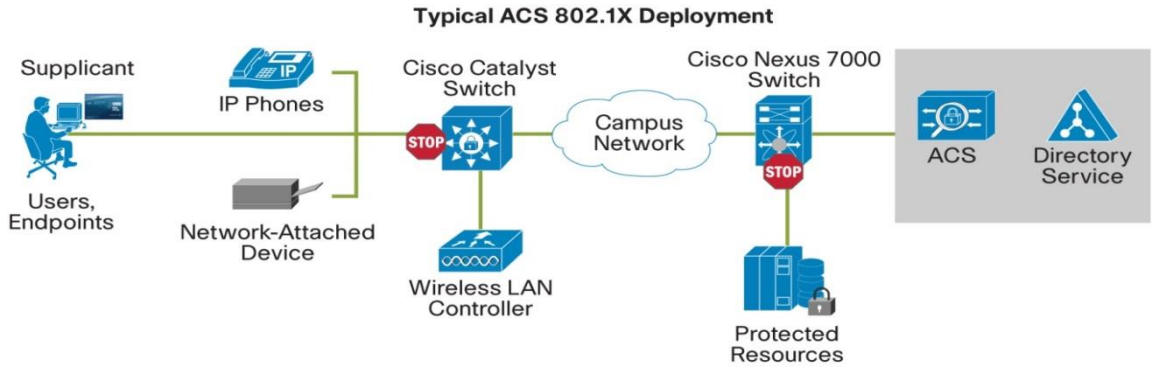
در این بخش به معرفی نمونه‌ی ابزارهای امنیتی و مدیریتی نسل جدید سیسکو می‌پردازیم [3] [2]:

- Cisco Secure Access Control System

زمانی‌که تعداد مسیریاب‌ها و سوئیچ‌ها زیاد باشد امکان این‌که کلمه عبور آنها را با هم اشتباه بگیریم یا فراموش کنیم زیاد است. برای رفع این مشکل نرم‌افزار ACS از پروتکل tacacs استفاده می‌کند. باید مسیریاب‌ها و

سوئیچ‌ها را طوری پیکربندی کنیم که برای ورود به مسیریاب یا سوئیچ، درخواست را به ACS بفرستد که آن را تأیید کند.

Cisco Secure ACS به عنوان یک نقطه مرکزی جهت کنترل دسترسی به شبکه و مدیریت تجهیزات مورد استفاده قرار می‌گیرد. Cisco Secure ACS سناریوهای بسیار زیادی را پیشتیبانی می‌کند که از آن جمله می توان به سناریوهایی مانند Remote Access، شبکه‌های بی‌سیم و 802.1X اشاره کرد. Cisco Secure ACS به عنوان یک نرم‌افزار پیش‌نیاز در زمینه AAA می‌باشد و بسیاری از سازمان‌های بزرگ از این نرم‌افزار استفاده می‌کنند. ACS تحت پلت‌فرم‌های مختلف ارائه شده است که می‌توان نسخه لینوکسی و نسخه ویندوزی آن را نام برد.



شکل ۲ ابزار امنیتی ACS 802.1x ارتقاء یافته

Cisco Secure ACS نرم‌افزار مبتنی بر سیستم‌عامل لینوکس با واسط کاربری تحت وب است که وظیفه احراز هویت، مجوزدهی و حساب‌کاربری را برای تجهیزات شبکه به طور متمرکز انجام می‌دهد. اگر بیش از یک نفر به مسیریاب‌ها، سوئیچ‌ها و دیواره‌های آتش سازمان شما دسترسی دارد، به این نرم‌افزار نیاز خواهید داشت. به کمک این نرم‌افزار برای هر فرد که به تجهیزات شبکه دسترسی دارد، یک حساب‌کاربری با سطح دسترسی مشخص تعیین می‌کنید. دسترسی را می‌توانید در بازه زمانی خاصی مشخص کنید. ممکن است بخواهید برخی از افراد سطح دسترسی کمی داشته و فقط بتوانند دستورات محدودی را بر روی تجهیزات شبکه اجرا کنند. علاوه بر این، ACS می‌تواند دستوراتی که کاربران بر روی تجهیزات شبکه اجرا می‌کنند را ثبت کند. این کار در عیب‌یابی شبکه کمک بسیار زیادی به شما می‌کند، چرا که مشخص است چه کاربری، بر روی چه دستگاهی و در چه زمانی، چه دستوری را اجرا کرده است.

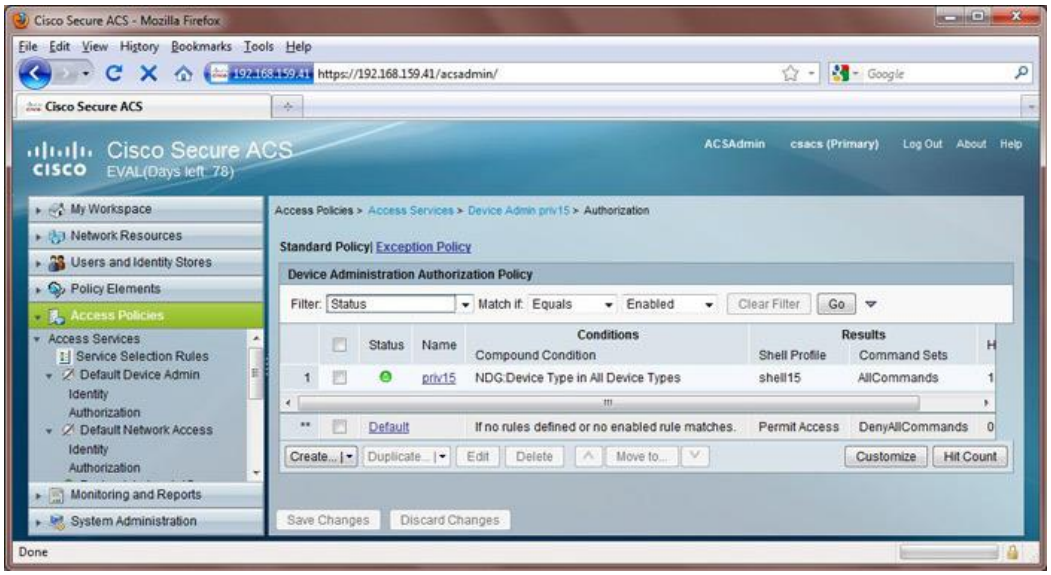
همچنین ACS قابلیت استفاده از پایگاه‌داده Active Directory برای احرازهویت را نیز دارد. با ادغام‌کردن ACS و Active Directory، دیگر نیاز به ساخت مجدد کاربران در پایگاه داده ACS نیست و می‌توانید سطح دسترسی بر روی تجهیزات شبکه را بر روی کاربران Active Directory مشخص کنید.

علاوه بر این، ACS می‌تواند احرازهویت را برای اتصال‌های PPPOE، PPTP، و یا هر نوع VPN انجام دهد. راه‌اندازی پروتکل امنیتی Dot1x نیز با استفاده از Cisco Secure ACS امکان‌پذیر است.

Secure ACS به صورت یک وسیله نرم‌افزاری بر روی DVD قرار دارد که می‌توان آن را بر روی بستر مجازی VMWare و یا یک سرویس‌دهنده مجزا نصب کرد. همچنین دستگاه سخت‌افزاری آن نیز وجود دارد که آخرین مدل آن CSACS-1121 بوده و بر روی آن ACS 5.4 نصب شده است. این دستگاه در تاریخ ۲۶ Feb سال ۲۰۱۳، قطع تولید شده است و جایگزین آن، مدل CSACS-3415-K9 می‌باشد. شکل ۳ دستگاه سخت افزاری مدل CSACS-1121 را نشان می‌دهد:

شکل ۳ دستگاه سخت افزاری مدل CSACS-1121

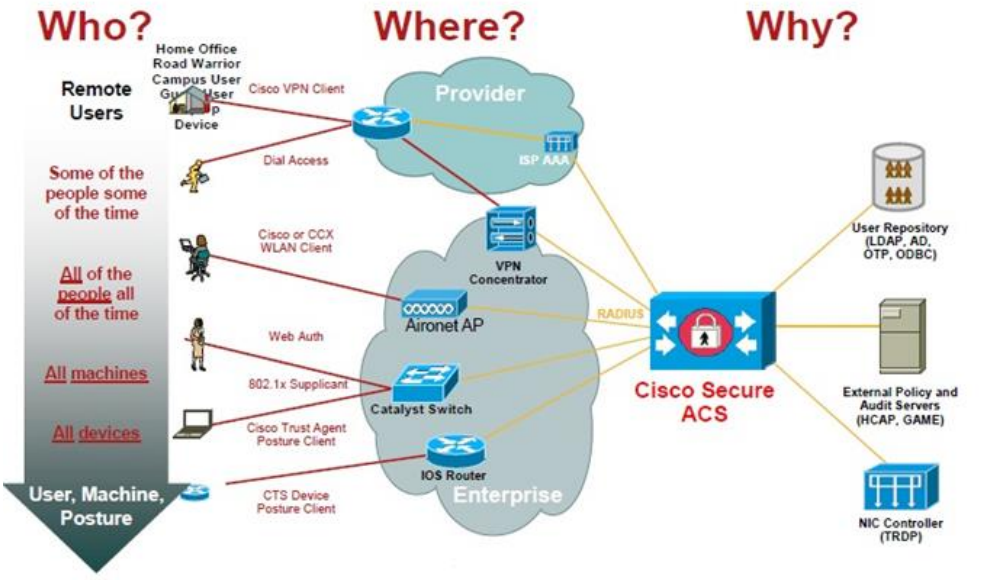
شکل ٤ بخشی از واسط کاربری Cisco Secure ACS 5.3 را نشان می‌دهد.



شکل ٤ واسط کاربری Cisco Secure ACS 5.3

Cisco Secure ACS به‌عنوان یک نقطه مرکزی برای مدیریت سیاست‌های دسترسی برای کاربران و همچنین دسترسی به تجهیزات عمل می‌کند، و به طور همزمان می‌تواند قابلیت‌های زیر را برای ما فراهم کند:

- ✓ Device administration: به این وسیله می‌توانیم مشخص کنیم که چه کسی و در چه سطحی به پیکربندی‌های دستگاه‌های شبکه دسترسی داشته باشد و عملکرد وی را ثبت کند.
- ✓ Remote Access: دسترسی‌های راه دور مانند VPN را با آن کنترل کنیم و سیاست‌های مورد نظر خود را روی آن اعمال کنیم.
- ✓ Wireless: به این وسیله می‌توانیم کاربران و دستگاه‌های بی‌سیم را کنترل و سیاست مورد نظر خود را روی آنها اعمال کنیم.
- ✓ LAN 802.1X: با استفاده از پروتکل 802.1x می‌توانیم دسترسی در لایه دوم را کنترل کنیم.
- ✓ Network admission control: کنترل ورودی شبکه



شکل ۵ ساختار کلی Cisco Secure ACS

- Cisco Identity Services Engine

شبکه‌های امروزی به سرعت در حال تغییر هستند به‌خصوص زمانی که کاربران یک دستگاه از هر جایی به روش‌هایی مختلف مانند اینترنت می‌خواهند به شبکه متصل شوند و برای این اتصال از دستگاه‌های مختلف

مانند لپ‌تاپ، تبلت، گوشی هوشمند و ... استفاده می‌کنند. این اتصال به شبکه از نقاط مختلف و دسترسی به منابع شبکه باعث افزایش بهره‌وری می‌شود، اما از سوی دیگر باعث کاهش امنیت و افزایش تهدیدات می‌شود چون وضعیت امنیتی دستگاه‌هایی که به شبکه متصل می‌شوند کنترل نمی‌شود. نگهداری و ردیابی تمام دستگاه‌هایی که به شبکه دسترسی پیدا می‌کنند یک کار بزرگ است و هر چه این میزان دسترسی بیشتر شود مدیریت و کنترل آن سخت‌تر می‌شود.

ISE نسل جدید سیستم شناسایی و کنترل دسترسی (جایگزین ACS) است که شبکه را قادر می‌سازد سرویس‌دهی را ساده‌تر انجام دهد و وضعیت امنیت زیرساخت را بهبود بخشد. معماری منحصربه‌فرد Cisco ISE این امکان را می‌دهد که به صورت Real time اطلاعات شبکه، کاربران و دستگاه‌ها را جمع‌آوری کند. سپس مدیر می‌تواند با استفاده از این اطلاعات برای شناسایی دسترسی به عناصر مختلف شبکه مانند سوئیچ‌ها، WLAN، VPN و غیره اقدام کند.

Cisco ISE محصول جدیدی است که راه‌حل‌ها و سرویس‌های مختلف امنیتی را در یک محصول به صورت یک‌جا برای ما فراهم می‌کند. این محصول کنترل دسترسی و راه‌حل‌های امنیتی برای ارتباطات کابلی، بی‌سیم و VPN را به صورت ساده و خودکار فراهم می‌کند.

شکل ٦ ساختار ISE

قابلیت‌های ISE:

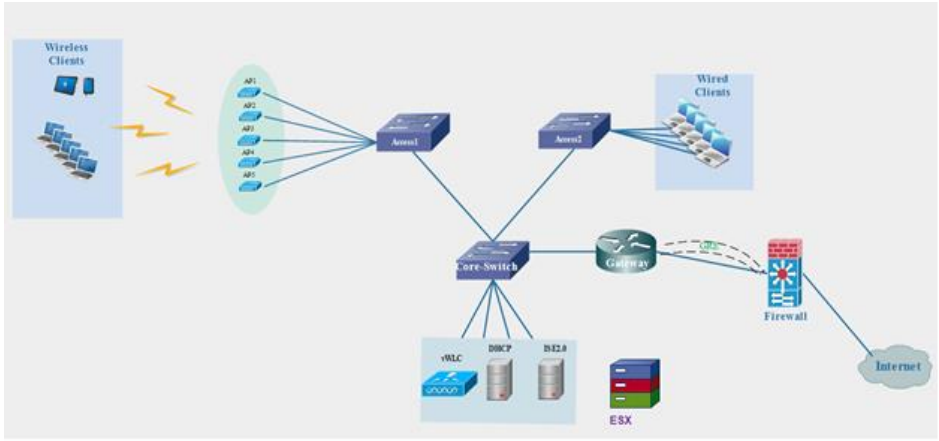
- قابلیت ایجاد پایگاه‌داده یکپارچه برای کاربران مهمان
- عدم وجود قابلیت Customize کردن صفحه Hotspot.

- عدم وجود سازگاری سامانه Hotspot با محصولات Apple، نیاز به bypass کردن این دستگاه‌ها.
- عدم وجود قابلیت تعریف‌کردن کلمه عبور کاربران توسط خودشان.
- وجود تمام بار مدیریتی سامانه Hotspot بر روی دوش مدیر شبکه در سایر محصولات موجود:
  - با استفاده از قابلیت Sponsor می‌توان ایجاد کاربران را بر عهده نفرات مشخص شده گذاشت.
  - یا این‌که ایجاد حساب کاربری توسط خود کاربر صورت گرفته و مدیر تنها وظیفه تأییدکردن آن را بر عهده داشته باشد.
- عدم وجود قابلیت پاک‌سازی[۶] پایگاه‌داده به صورت اتوماتیک بعد از گذشت مدت زمان مشخص از آخرین Login کاربر به شبکه مهمان.
- عدم وجود قابلیت تخصیص[۷]دادن کاربران به دستگاه‌هایی که از طریق آن قصد ورود به شبکه مهمان را دارند.
- عدم وجود قابلیت تعریف policy برای اتصال همزمان چندین دستگاه با یک حساب کاربری:
  - قطع آخرین session و صدور اجازه ورود به شبکه
  - منع ورود sessionهای جدید به شبکه بعد از تجاوز از حداکثر تعداد sessionهایی که قابلیت اتصال همزمان به شبکه را دارند.
- ارسال خودکار ایمیل شامل اطلاعات حساب کاربری
  - بعد از تأییدشدن توسط sponsor
  - بعد از ساخته‌شدن توسط admin
- به‌کارگیری سرویس‌دهنده Active Directory به منظور ایجاد پایگاه‌داده یکپارچه از کاربران
- بهره‌گیری از قابلیت‌های دیگر سامانه ISE مانند Dot1x، قابلیت BYoD، SSL VPN و ...
- راه اندازی Posture جهت محدودکردن دسترسی سرویس‌گیرنده‌ها به شبکه

[۶] Purging

[۷] Assign

در شکل ۷ یک نمونه سناریو پیاده‌سازی‌شده با استفاده از ISE برای دسترسی کاربران به اینترنت را مشاهده می‌کنید.



شکل ۷ سناریو پیاده‌سازی‌شده با استفاده از ISE

ویژگی‌های کلیدی Cisco ISE:

- پروتکل‌هایAAA: سیسکو ISE برای احرازهویت، مجوزدهی، و حساب‌کاربری از پروتکل RADIUS استفاده می‌کند.
- پروتکل‌های احرازهویت: از پروتکل‌های تأیید هویت مختلفی پشتیبانی می‌کند که شامل PAP، MS-CHAP، EAP-MD5، PEAP، EAP-FAST، و EAP-TLS می‌باشند.
- کنترل دسترسی: سیسکو ISE دامنه وسیعی از مکانیزم‌های کنترل دسترسی را برای ما فراهم می‌کند، مانند URL Redirect، Vlan Assignment، dACL[۸] و SGA tagging.

[۸] Downloadable Access Control Lists

- وضعیت: سیسکو ISE با استفاده از NAC-client-Agent یا web agent وضعیت دستگاه‌هایی که به شبکه متصل می‌شوند را بررسی می‌کند. یک مدیر شبکه می‌تواند شرایط مختلفی را برای بررسی تعیین کند مانند آنتی ویروس، وضعیت سیستم عامل و غیره.

- Profiling: Profiling برای شناسایی و آنالیز دستگاه‌های شبکه مورد استفاده قرار می‌گیرد. این دستگاه ها می‌تواند هر نوع دستگاهی که می‌خواهد به شبکه دسترسی پیدا کند باشد، مانند iPhone، iPad، laptop، printers و غیره. ISE به صورت پیش‌فرض دارای چندین Profiling برای این دستگاه‌ها می باشد. همچنین ما می‌توانیم Profiling مورد نظر خود را ایجاد کنیم و برای آن سیاست‌های خاصی در نظر بگیریم.

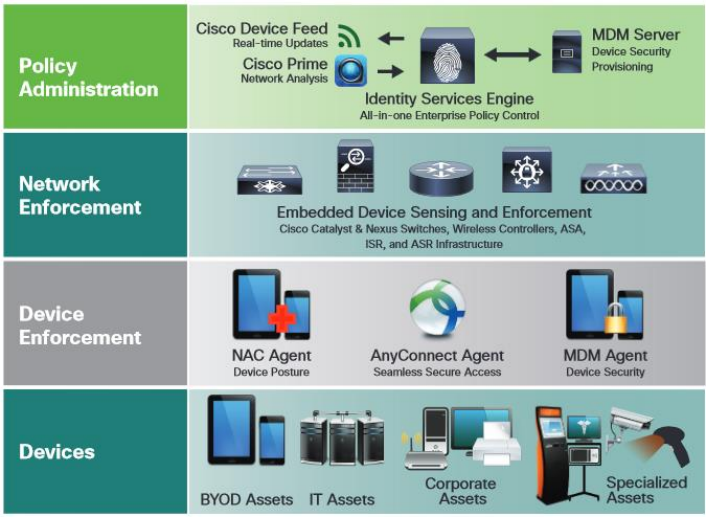
- مدل Policy: این مدل این امکان را فراهم می‌کند که با استفاده از ویژگی‌ها و نقش‌ها، کنترل دسترسی انعطاف‌پذیرتری داشته باشیم.

- مدیریت چرخه حیات مهمان: با این قابلیت می‌توان در ISE، کاربر با دسترسی خاص داشته باشیم و از آن برای کنترل کاربران مهمان استفاده کنیم.

- بسترهای استفاده: ISE را در دو پلت‌فرم می‌توان استفاده کرد. پلت‌فرم اول به عنوان یک دستگاه متصل می‌باشد، و پلت‌فرم دوم به عنوان یک دستگاه مجازی قابل استفاده است. ISE را می‌توان روی VMware نصب کرد.

- نظارت، عیب‌یابی و گزارش: در ISE نظارت، خطایابی، و گزارش‌گیری به سادگی و با محیط کاربرپسند انجام می‌شود.

نکته: ISE در حال حاضر از پروتکل TACACS+ پشتیبانی نمی‌کند و احتمالاً در نسخه۲ این پروتکل اضافه خواهد شد.



شکل ۸ اجزای ISE ارتقاءیافته

۱۲ مراجع

[۱] R. F. J. Kevin Corbinr, "NX-OS and Cisco Nexus Switching", USA: Cisco Press 800 East 96th Street, 2010.

[۲] Cisco, "Cisco Identity Services Engine (ISE)", 2013, www.cisco.com/go/trademarks.

[۳] C. ISE, "Cisco Identity Services Engine".

[٤] Cisco Security Research & Operations, "Cisco Guide to Securing NX-OS Software Devices", https://www.cisco.com/c/en/us/about/security-center/securing-nx-os.htm.

[٥] Cisco, "Cisco Nexus 7000 Series NX-OS Security Configuration Guide", Release 5.x, USA: http://www.cisco.com, 2017.

[٦] wikipedia, "Cisco Nexus switches", https://en.wikipedia.org/wiki/Cisco_Nexus_switches.

[٧] Cisco, "White Paper: Cisco IOS and NX-OS Software Reference Guide", https://www.cisco.com/c/en/us/about/security-center/ios-nx-os-reference-guide.html.