باسمه تعالی

پیکربندی امن سوئیچ‌های نسل جدید سیسکو NX-OS

(بخش دوم)

فهرست مطالب

۱ مقدمه

نرم‌افزار NX-OS سیسکو با استفاده از سوئیچ‌های NX-OS، شبکه را در برابر تخریب و انواع حملات در لایه‌ی شبکه محافظت می‌کند. در این گزارش به معرفی مجموعه مستندات مربوط به پیکربندی امن NX-OS، با استفاده از قابلیت‌ها و توانمندی‌های امنیتی آن، همراه با بررسی مثال‌های کاربردی پرداخته می‌شود.

۲ پیکربندی RADIUS

سرویس‌های احرازهویت[۱]، مجوزدهی[۲] و حساب کاربری[۳](AAA) امکان تأیید هویت، اعطای دسترسی، و پیگیری اقدامات کاربران در مدیریت تجهیزات NX-OS سیسکو را فراهم می‌کنند. دستگاه‌های NX-OS سیسکو از پروتکل‌های کنترل دسترسی از راه دور RADIUS[۴] یا پروتکل TACACS+[۵] پشتیبانی می‌کنند [1]. دستگاه‌های NX-OS سیسکو براساس شناسه کاربری و کلمات عبور ارائه شده، و با استفاده از پایگاه‌های داده محلی یا احرازهویت از راه دور یا مجوزدهی محلی با یک یا چند سرویس‌دهنده AAA، سرویس احرازهویت یا مجوزدهی را اجرا می‌کنند. یک کلید سری، امنیت ارتباطات بین دستگاه NX-OS سیسکو و سرویس‌دهنده‌های AAA را فراهم می‌کند. یک کلید سری مشترک می‌تواند تمام سرویس‌دهنده های AAA یا یک سرویس‌دهنده‌ی خاص AAA را پیکربندی کند. امنیت AAA سرویس‌های زیر را ارائه می‌دهد:

- احرازهویت

احرازهویت، شامل نام‌کاربری و کلمه‌ی عبور، چالش و پاسخ، پشتیبانی از انواع پیام‌ها، و رمزگذاری وابسته به پروتکل امنیتی انتخابی می‌باشد. احرازهویت، روند تأیید هویت فرد یا دستگاهی است که به تجهیزات سیسکو NX-OS دسترسی دارد. براساس شناسه کاربری و کلمه‌ی عبور ارائه شده از سوی سازمان برای دسترسی به دستگاه NX-OS سیسکو مورد بررسی قرار می‌گیرد. دستگاه‌های

---

[۱] Aut hentication
[2] Authorization
[3] Accounting
[4] Remote Access Dial-In User Service
[۵] Terminal Access Controller Access Control device Plus

NX-OS سیسکو، احرازهویت محلی (با استفاده از جستجو در پایگاه‌داده محلی) یا احرازهویت از راه دور (با استفاده از یک یا چند سرویس‌دهنده RADIUS یا +TACACS) را فعال می‌کنند [1].

- مجوزدهی

سرویس‌دهنده‌ی AAA، مجموعه‌ای از ویژگی‌هایی که کاربران مجاز به انجام آن می‌باشند را توصیف می‌کند. مجوزدهی در نرم‌افزار NX-OS سیسکو توسط ویژگی‌های گرفته شده از سرویس‌دهنده‌های AAA ارائه شده است. این سرویس‌ها می‌تواند توسط سرویس‌دهنده‌های امنیت از راه دور مانند RADIUS و +TACACS انجام گیرد.

- حساب کاربری

روشی برای جمع‌آوری اطلاعات، ثبت اطلاعات به صورت محلی، و ارسال اطلاعات به سرویس‌دهنده AAA برای صدور صورت حساب و یا فعالیت‌های کاربران می‌باشد.

خصوصیات حساب‌کاربری و فایل‌های ثبت وقایع در هر ارتباط ثبت و استفاده می‌شوند. فایل‌های ثبت وقایع برای تولید گزارش و اهداف عیب‌یابی و حسابرسی استفاده می‌شوند. فایل‌های ثبت وقایع به صورت محلی ذخیره و به سرویس‌دهنده‌های AAA از راه دور ارسال می‌شوند. خدمات AAA مزایای متعددی از قبیل انعطاف‌پذیری و کنترل دسترسی پیکربندی، و قابلیت مقیاس‌پذیری را ارائه می‌دهند.

استقرار موفق سرویس‌های AAA شامل چندین پیش‌شرط است:

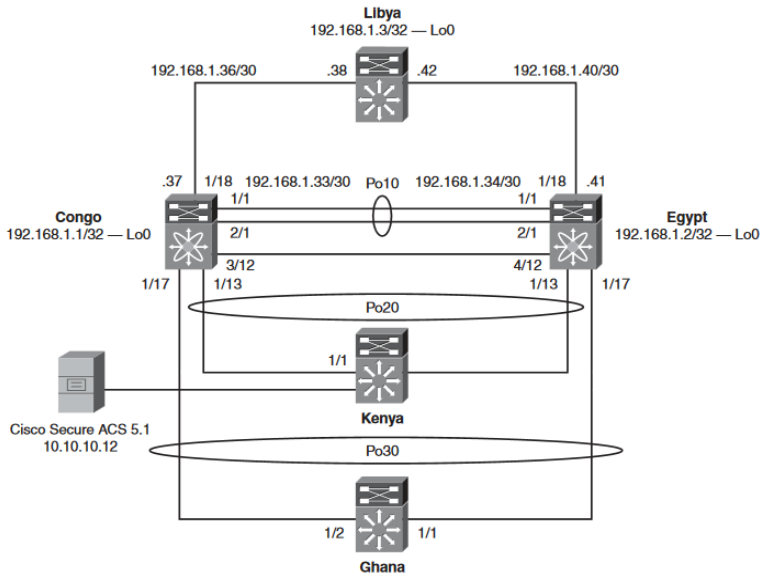
- تأیید سرویس‌دهنده‌های RADIUS یا +TACACS از طریق آدرس IP قابل دسترس است.
- تأیید دستگاه NX-OS سیسکو که به عنوان یک سرویس‌گیرنده به سرویس‌دهنده‌ی AAA متصل و پیکربندی شده است.
- پیکربندی یک کلید سری و اشتراکی در دستگاه NX-OS سیسکو و سرویس‌دهنده‌ی از راه دور AAA.
- تأییدیه‌ای که با مشخص کردن درگاه فیزیکی منبع، سرویس‌دهنده راه دور به درخواست‌های AAA دستگاه NX-OS سیسکو پاسخ می‌دهد.

پروتکل +TACACS، اعتباری را فراهم می‌کند که کاربران به یک دستگاه NX-OS سیسکو دسترسی پیدا کنند. سرویس +TACACS در پایگاه‌داده +TACACS نگهداری می‌شود. +TACACS، احرازهویت، مجوزدهی دسترسی، و قابلیت‌های حساب کاربری را فراهم می‌کند. پروتکل +TACACS از درگاه TCP 49 برای انتقال ارتباطات استفاده می‌کند.

RADIUS یک پروتکل سرویس‌گیرنده/سرویس‌دهنده است که از طریق آن سرویس‌دهنده‌های دسترسی از راه دور با یک سرویس‌دهنده مرکزی ارتباط برقرار می‌کنند تا هویت کاربران را تأیید کنند و اجازه دسترسی به سیستم یا سرویس درخواست شده را بدهند. RADIUS پروفایل‌های کاربران را در پایگاه‌داده مرکزی حفظ می‌کند و تمام سرویس‌دهنده‌های از راه دور می‌توانند آن را به اشتراک بگذارند.

سرویس‌دهنده‌ی Cisco Secure ACS درخواست‌های احرازهویت را بر روی درگاه‌های شماره ۱۶۴۵ و ۱۸۱۲ قبول می‌کند [2]. برای حساب کاربری RADIUS، Cisco Secure ACS بر روی درگاه‌های ۱۶۴۶ و ۱۸۱۳ بسته‌های حساب‌کاربری را می‌پذیرد.

مثال ۱: روش‌های احرازهویت برای ورود به کنسول توسط احرازهویت RADIUS، براساس توپولوژی شبکه‌ای، در شکل ۱ پیکربندی شده است.



شکل ۱ توپولوژی شبکه‌ای امن مورد استفاده در سراسر گزارش [2]

توجه: به غیر از موارد ذکر شده، برای تمام نمونه‌های پیکربندی باقی مانده در طول مستند به توپولوژی شبکه‌ای که در شکل ۱ نشان داده شده است، مراجعه نمایید.

مثال ۲: پیکربندی AAA RADIUS برای تأیید هویت کنسول

```
Switch-2#
Switch-2# conf t
Switch-2 (config)# interface loopback0
Switch-2 (config)# ip address 192.168.1.2/32
Switch-2 (config)# ip radius source-interface loopback0
```

```
Switch-2 (config)# radius-server host 10.10.10.12 key 7 "QTSX123" authentication
accounting
Switch-2 (config)# aaa authentication log in console group radius
Switch-2 (config)# interface loopback0
Switch-2 (config)# ip address 192.168.1.1/32
Switch-2 (config)# exit
Switch-2#
```

مثال ۳: پیکربندی روش‌های احرازهویت ورود به سیستم پیش‌فرض

```
Switch-2#
Switch-2 (config)# interface loopback0
Switch-2 (config)# ip address 192.168.1.2/32
Switch-2 (config)# ip radius source-interface loopback0
Switch-2 (config)# radius-server host 10.10.10.12 key 7 "QTSX123" authentication
accounting
Switch-2 (config)# aaa authentication login  console group radius
Switch-2 (config)# exit
Switch-2# copy running-config startup-config
```

توجه: پیکربندی و عملیات AAA محلی برای VDC[۶]، به غیر از روش‌های کنسول پیش‌فرض و فایل‌های ثبت وقایع حساب کاربری AAA است. پیکربندی و روش‌های احرازهویت AAA برای ورود کنسول فقط به VDC پیش‌فرض اعمال می‌شود.

۲-۱ توزیع پیکربندی RADIUS

CFS[۷]، دستگاه NX-OS را قادر می‌سازد تا پیکربندی RADIUS را برای سایر دستگاه‌های NX-OS سیسکو در شبکه توزیع کند. هنگامی‌که توزیع CFS را برای یک ویژگی در دستگاه خود فعال می‌کنید، دستگاه وابسته به یک ناحیه CFS شامل سایر دستگاه‌های موجود در شبکه است که برای توزیع CFS این ویژگی، فعال شده است.

[۶] Virtual Device Context

[۷] Cisco Fabric Services

توزیع RADIUS CFS به صورت پیش‌فرض غیرفعال است. برای فعال‌کردن توزیع پیکربندی RADIUS، از دستور زیر استفاده کنید [2]:

```
Switch-2 (config) # radius distribute
```

برای اعمال تغییرات پیکربندی RADIUS در پایگاه‌داده موقت به پیکربندی در حال اجرا و توزیع RADIUS، از دستور زیر استفاده کنید:

```
Switch-2 (config) # radius commit
```

توجه: سرویس‌دهنده RADIUS و کلیدهای عمومی منحصربه‌فرد هستند و از طریق جلسات CFS توزیع نمی‌شوند. CFS سرویس‌دهنده RADIUS یا دستورات AAA را توزیع نمی‌کند.

مثال ٤: این مثال تأیید می‌کند که هیچ پیکربندی RADIUS در Switch-1 وجود ندارد.

```
Switch-1#before cfs:
Switch-1# show running-config radius
!Command: show running-config radius
!Time: Thu Oct 8 18:01:04 2009
version 4.2(2a)
Switch-1#
```

مثال ٥: این مثال تأیید می‌کند که پیکربندی RADIUS در Switch-2 وجود ندارد.

```
Switch-2# show running-config radius
!Command: show running-config radius
!Time: Thu Oct 8 18:00:24 2009
version 4.2(2a)
```

مثال ٦: چگونگی پیکربندی RADIUS در Switch-2

```
Switch-2#
Switch-2# conf t
Switch-2(config)# ip radius source-interface loopback 0
Source-interface configuration is exempted from CFS distribution
Switch-2(config)# radius-server host 10.10.10.12 key NXOS123
Switch-2(config)# aaa authentication login console group radius
Switch-2(config)# radius commit
```

مثال ٧: این مثال پیکربندی RADIUS که از طریق توزیع CFS ارائه شده است را تأیید می‌کند.

```
Switch-2(config)# show running-config radius
!Command: show running-config radius
```

```
!Time: Thu Oct 8 18:09:31 2009
version 4.2(2a)
radius distribute
radius-server retransmit 0
radius-server host 10.10.10.12 authentication accounting
radius commit
Switch-2(config)#
```

مثال ۸: نحوه تأیید پیکربندی RADIUS CFS

```
Switch-2# show radius-cfs
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done
Switch-2#

Switch-2# show radius-server
retransmission count:1
timeout value:5
deadtime value:0
source interface:loopback0
total number of servers:1
following RADIUS servers are configured:
      10.10.10.12:
          available for authentication on port:1812
          available for accounting on port:1813
Switch-2#
Switch-2# show cfs peers
Physical Fabric
Switch WWN                 IP Address
-------------------------------------------------------------------------------------------------------------------
-----------------------------
20:00:00:1b:54:c2:78:c1 172.26.32.39                                  [Local]
20:00:00:1b:54:c2:76:41 172.26.32.37
Total number of entries = 2
Switch-2# show cf status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Enabled
Switch-2# show cfs merge status
Application        Scope        Vsan        Status
Radius        Physical-fc-ip     -          Success
Switch-2# copy running-config startup-config
```

توجه: اگر سرویس‌دهنده RADIUS غیرفعال شود، رفتار پیش‌فرض تعریف شده این است که مجدداً به احرازهویت محلی NX-OS بازگردانده شود.

مثال ۹: مدیر درگاه فیزیکی Gigabit Ethernet 1/1 متصل به سرویس‌دهنده Cisco ACS RADIUS را قطع می‌کند [2].

```
Kenya# config t
Kenya(config)#int gi1/1
Kenya(config-if)#shutdown
Kenya(config-if)# exit
Kenya(config)# exit

Kenya#show interfaces gigabitEthernet 1/1
GigabitEthernet1/1 is administratively down, line protocol is down (disabled)
  Hardware is Gigabit Ethernet Port, address is 0018.73b1.e280 (bia 0018.73b1.e280)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, link type is auto, media type is 10/100/1000-TX
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:01:09, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    114119 packets input, 73777471 bytes, 0 no buffer
    Received 59680 broadcasts (48762 multicasts)
    0 runs, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
  3453776 packets output, 281211243 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

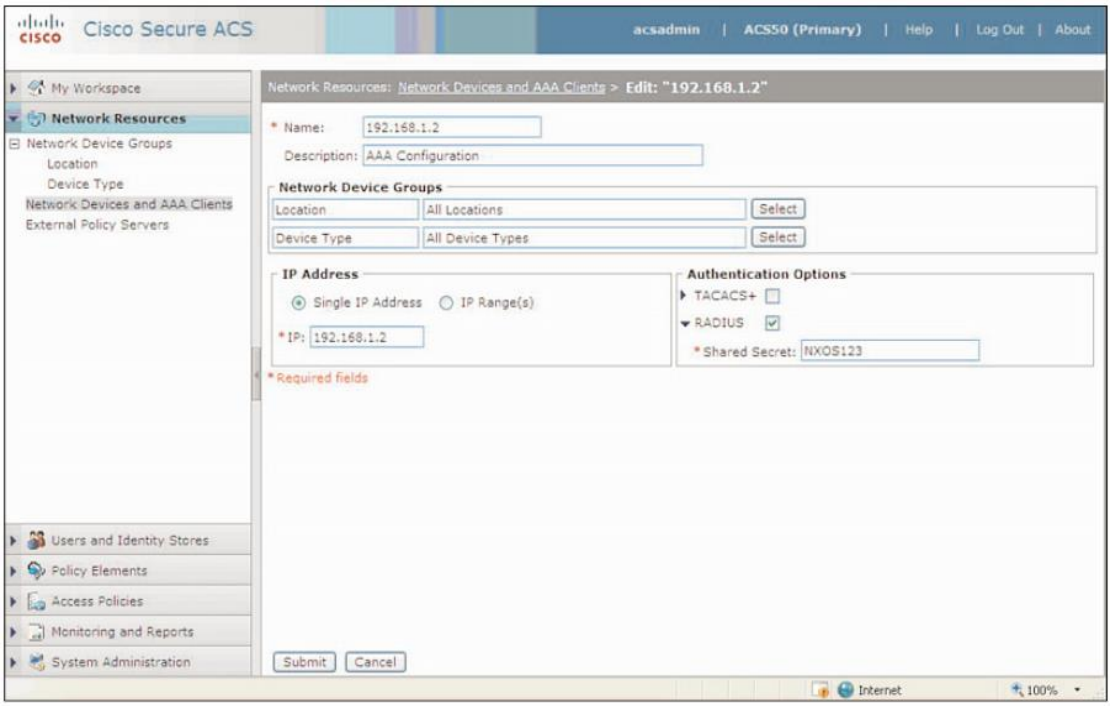
مثال ۱۰: با استفاده از Telnet (که توصیه نمی‌شود و در این مثال فقط با هدف آموزش بیان شده است) به عنوان مدیر به دستگاه Nexus 7000 NX-OS، وارد می‌شود.

```
[hk@hk ~]$ telnet Switch-1
Trying 172.26.32.37...
Connected to Switch-1.
Escape character is '^]'.
User Access Verification
login: admin
Password:

Remote AAA servers unreachable; local authentication done


Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Switch-1# ping 10.10.10.12
PING 10.10.10.12 (10.10.10.12): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 10.10.10.12 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
Switch-1#
```

شکل‌های ۲ تا ۵ مراحل پیکربندی Cisco Secure ACS GUI را نشان می‌دهند.



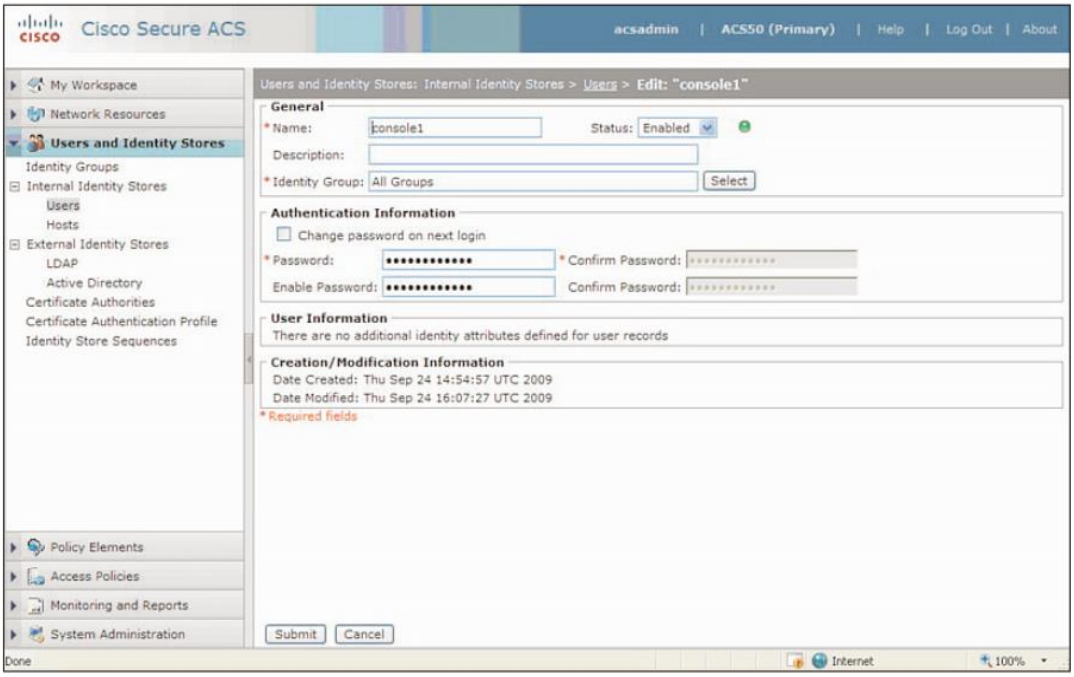
شکل ۲ نمایش پیکربندی Cisco Secure ACS RADIUS ویژه [3]

شکل ۲ پیکربندی امن Cisco Secure ACS RADIUS را نشان می‌دهد. Loopback دستگاه NX-OS و کلید سری مشترکی را تعریف می‌کند که به هماهنگی بین دستگاه NX-OS و سرویس‌دهنده Cisco Secure ACS نیاز دارد.

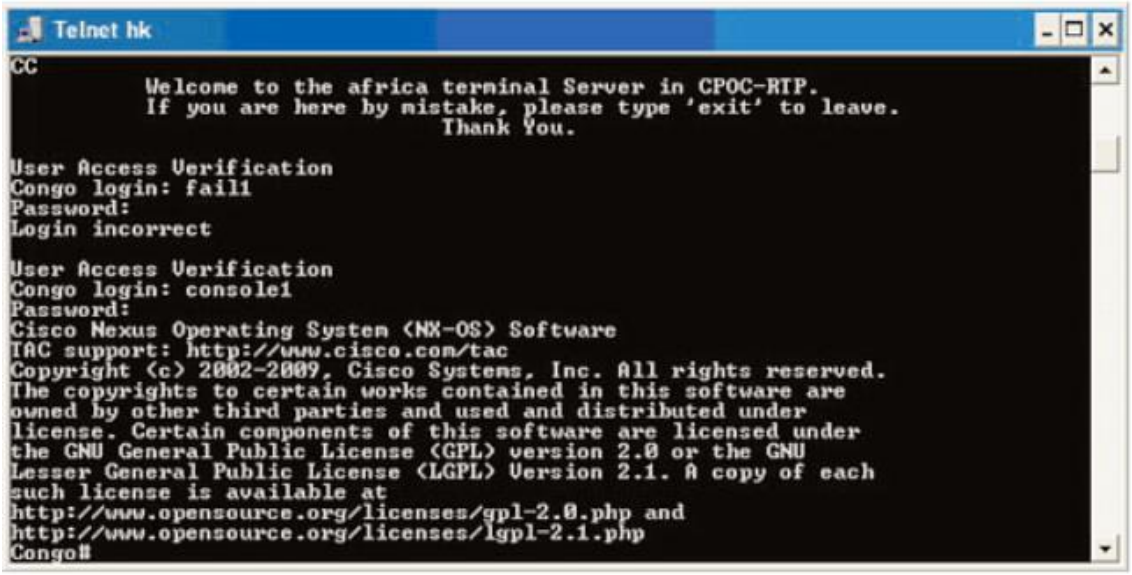
شکل ۳ روش اضافه کردن یک کاربر به پایگاه‌داده امن سیسکو را نشان می‌دهد. کاربر کنسول ۱ برای نشان دادن کنسول احرازهویت AAA RADIUS اضافه شده است.

شکل ٤ نشان‌دهنده یک احرازهویت موفق و واردشدن با کاربر کنسول ۱ از طریق درگاه فیزیکی کنسول Async دستگاه NX-OS است.

شکل ۵ گزارش موفق‌بودن احرازهویت RADIUS در سرویس‌دهنده Cisco Secure ACS را تأیید می‌کند.



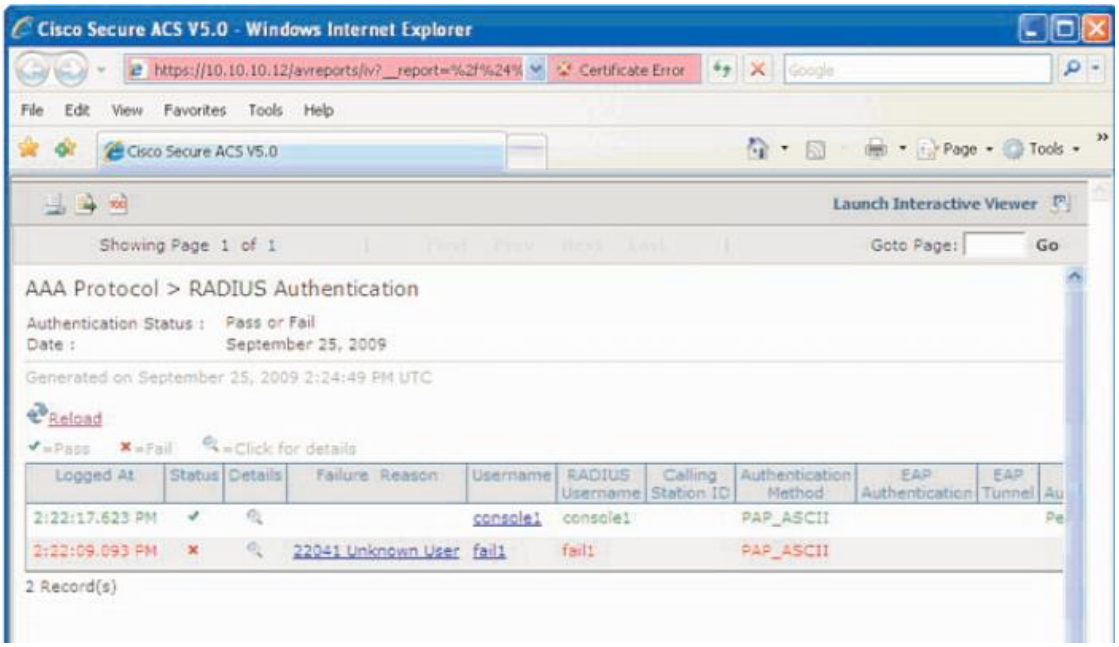
شکل ۳ اضافه‌کردن یک کاربر به پایگاه‌داده امن سیسکو RADIUS [2]



شکل ٤ یک احرازهویت موفق برای کاربر کنسول ۱ از طریق واسط کنسول [2]

۳ پیکربندی TACACS+

پروتکل TACACS+ اعتباری را فراهم می‌کند که کاربران به یک دستگاه NX-OS سیسکو دسترسی پیدا کنند. سرویس TACACS+ در پایگاه‌داده TACACS+ نگهداری می‌شود. TACACS+، احرازهویت، مجوزدهی دسترسی، و قابلیت‌های حساب کاربری را فراهم می‌کند. پروتکل TACACS+ از درگاه TCP 49 برای انتقال ارتباطات استفاده می‌کند.



شکل ۵ تأیید موفقیت کاربر کنسول ۱ از طریق پروتکل RADIUS

۳-۱ فعال‌کردن TACACS+

ویژگی TACACS+ به صورت پیش‌فرض غیرفعال است. TACACS+ باید به طور صریح ویژگی TACACS+ را برای دسترسی به دستورات پیکربندی و تأیید احرازهویت فعال کند. برای بررسی وضعیت ویژگی پیش‌فرض TACACS+، از دستور زیر استفاده کنید:

```
Switch-2# show feature |i tacacs
tacacs          1     disabled
```

برای فعال‌کردن ویژگی TACACS+، پیکربندی را همان‌طور که در مثال ۱۱ نشان داده شده است، انجام دهید.

مثال ۱۱: فعال‌کردن TACACS+ Feature/Process

```
Switch-2#
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# feature tacacs+
Switch-2(config)# show feature | i tacacs
tacacs          1         enabled
Switch-2(config)# exit
Switch-2# copy running-configuration startup=configuration
```

برای تأیید فعال‌بودن قابلیت TACACS+، دستور زیر را وارد کنید:

```
Switch-2# show feature |i tacacs+
tacacs          1         enabled
Switch-2#
```

۳-۲ توزیع پیکربندی TACACS+

CFS، دستگاه NX-OS را قادر می‌سازد تا پیکربندی RADIUS را برای سایر دستگاه‌های NX-OS سیسکو در شبکه توزیع کند. هنگامی‌که توزیع CFS را برای یک ویژگی در دستگاه خود فعال می‌کنید، دستگاه وابسته به یک ناحیه CFS شامل سایر دستگاه‌های موجود در شبکه است که برای توزیع CFS این ویژگی، فعال شده است. برای فعال‌کردن توزیع TACACS+ CFS، دستور زیر را وارد کنید.

```
Switch-2 (config)# tacacs+ distribute
```

مثال ۱۲: برای بررسی توزیع TACACS+ CFS، دستور show tacacs+ status را وارد کنید.

```
Switch-2(config)# show tacacs+ status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable
last operation: enable
last operation status: success
Switch-2(config)#
```

۳-۲-۱ پیکربندی عمومی کلیدهای TACACS+

کلیدهای سری +TACACS را می‌توان در سطح عمومی برای تمام سرویس‌دهنده‌های مورد استفاده توسط دستگاه NX-OS پیکربندی کرد. کلید سری یک رشته متن مخفی مشترک بین دستگاه NX-OS سیسکو و سرویس‌دهنده میزبان +TACACS است.

توجه: سرویس‌دهنده +TACAC و کلیدهای عمومی منحصربه‌فرد هستند و از طریق جلسات CFS توزیع نمی‌شوند. CFS سرویس‌دهنده RADIUS یا دستورات AAA را توزیع نمی‌کند.

مثال ۱۳: روش پیکربندی کلیدهای سرویس‌دهنده +TACACS

```
Switch-2(config)# tacacs-server key 0 NXOS123
Global key configuration is exempted from CFS distribution
Switch-2(config)# show tacacs-server
Global TACACS+ shared secret:*********
timeout value:5
deadtime value:0
source interface:any available
total number of servers:0
```

۳-۲-۲ پیکربندی سرویس‌دهنده میزبان +TACACS

برای دسترسی به سرویس‌دهنده +TACACS از راه دور، باید آدرس IP یا نام میزبان برای سرویس‌دهنده +TACACS را پیکربندی کنید. در مثال زیر آدرس IP سرویس‌دهنده +TACACS، 10.10.10.12 است.

توجه: سرویس‌دهنده‌های +TACACS 64 می‌توانند تعریف و یا پیکربندی شوند.

مثال ١٤: این مثال نحوه پیکربندی سرویس‌دهنده میزبان +TACACS را نشان می‌دهد. آدرس IP مربوط به سرویس‌دهنده +TACACS Cisco Secure ACS است.

```
Switch-2(config)# tacacs-server host 10.10.10.12
Switch-2(config)# show tacacs+ pend
Pending          pending-diff
Switch-2(config)# show tacacs+ pending
tacacs-server key 7 QTSX123
tacacs-server host 10.10.10.12
Switch-2(config)# tacacs+ commit
Switch-2(config)# show tacacs-server
Global TACACS+ shared secret:*********
Timeout value:5
Deadtime value:0
source interface:any available
total number of servers:1
```

```
following TACACS+ servers are configured:
    10.10.10.12:
        available on port:49
Switch-2(config)# show tacacs+ pending
No active CFS distribution session exist for TACACS+
Switch-2(config)# copy running-config startup-config
[########################################] 100%
Switch-2(config)#
```

توجه: دستور tacacs+ commit پیکربندی پایگاه‌داده موقت را به پیکربندی در حال اجرا تغییر می‌دهد.

۳-۲-۳ پیکربندی گروه سرویس‌دهنده‌های TACACS+

با NX-OS، می‌توانید اعتبار کاربران یک یا چند سرویس‌دهنده AAA از راه دور را با استفاده از گروه سرویس‌دهنده‌ها مشخص و تأیید کنید؛ اعضای گروه باید به پروتکل TACACS+ وابسته باشند.

مثال ۱۵: نحوه پیکربندی گروه‌های سرویس‌دهنده TACACS+

```
Switch-2(config)# aaa group server tacacs+ TACACS+Server
Switch-2(config-tacacs+)# server 10.10.10.12
Switch-2(config-tacacs+)# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TACACS+Server:
            server 10.10.10.12 on port 49
            deadtime is 0
Switch-2(config-tacacs+)#
```

مثال ۱۶: چگونگی پیکربندی روش‌های احرازهویت پیش‌فرض TACACS+ برای Telnet و SSH

```
Switch-2(config)# aaa authentication login default group TACACS+Server
Switch-2(config)# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
source interface:loopback0
total number of servers:1
following TACACS+ servers are configured:
        10.10.10.12:
            available on port:49
Switch-2(config)#
```

۳-۳ پیکربندی واسط منبع +TACACS

شما می‌توانید چندین واسط لایه‌ی ۳ داشته باشید، و همچنین می‌توانید واسط منبع عمومی گروه‌های +TACACS برای استفاده در هنگام دسترسی به +TACACS را مشخص کنید، به همین خاطر قابلیت دسترسی IP بین دستگاه NX-OS و سرویس‌دهنده ACS Secure Cisco مورد نیاز است.

توجه: واسط‌های مختلف منبع را می‌توان برای گروه‌های خاص +TACACS مشخص کرد. به صورت پیش‌فرض دستگاه NX-OS هر رابط کاربری موجود در لایه ۳ را انتخاب می‌کند.

توجه: توجه داشته باشید، با فعال شدن CFS +TACACS، پیکربندی source-interface از توزیع CFS معاف است.

مثال ۱۷: این مثال توزیع پیکربندی CFS +TACACS در سوئیچ ۲ را تأیید می‌کند.

```
Switch-1(config)# ip tacacs source-interface loopback 0
Source-interface configuration is exempted from CFS distribution
Switch-1(config)#
Switch-1#

CFS on the second Switch
Switch-1(config)# show feature| i tacacs+
Tacacs           1       disabled
Switch-1(config)# feature tacacs+
Switch-1(config)# show feature | i tacacs+
Tacacs           1       enabled
Switch-1(config)# tacacs+ distribute
Switch-1(config)# show tacacs+ status
distribution : disabled
session ongoing: no
session db: does not exist
merge protocol status:

last operation: none
last operation status: none
Switch-1(config)# show running-config tacacs+
!Command: show running-config tacacs+
!Time: Thu Oct 1 14:15:42 2009
version 4.2(2a)
feature tacacs+
Switch-1(config)# tacacs+ distribute
Switch-1(config)# show tacacs+ status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done
```

```
last operation: enable
last operation status: success
Switch-1(config)# show running-config tacacs+

!Command: show running-config tacacs+
!Time: Thu Oct 1 14:16:02 2009

version 4.2(2a)
feature tacacs+

tacacs+ distribute
tacacs-server host 10.10.10.12
tacacs+ commit
```

مثال ۱۸: احرازهویت Telnet موفق با استفاده از+TACACS را نشان می‌دهد.

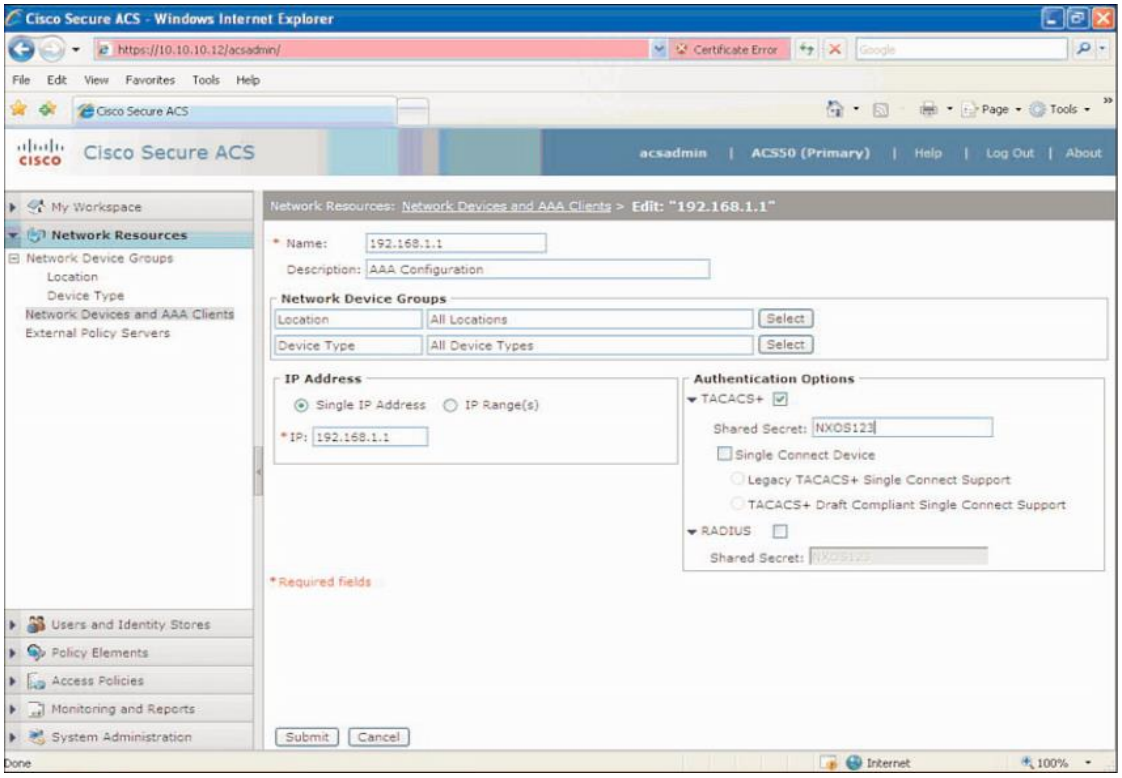
```
[hk@hk ~]$ telnet Switch-2
Trying 172.26.32.39...
Connected to Switch-2.
Escape character is '^]'.
User Access Verification
login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Switch-2#
```

مثال ۱۹: مدیر رفتار پیش‌فرض واسط Gigabit Ethernet1/1 متصل به سرویس‌دهنده امن سیسکو ACS +TACACS را قطع می‌کند.

```
Kenya(config)#int gi1/1
Kenya(config-if)#shut
Kenya(config-if)#
--------------------------------------------------------------------------------
```

```
Switch-2# ping 10.10.10.12
PING 10.10.10.12 (10.10.10.12): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 10.10.10.12 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
Switch-2#
[hk@hk ~]$ telnet Switch-2
Trying 172.26.32.39...
Connected to Switch-2.
Escape character is '^]'.
User Access Verification
login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Switch-2#
2009 Oct 1 15:59:05 Switch-2 %TACACS-3-TACACS_ERROR_MESSAGE: All servers failed
to
respond
2009 Oct 1 16:00:31 Switch-2 %TACACS-3-TACACS_ERROR_MESSAGE: All servers failed
to
Respond
```

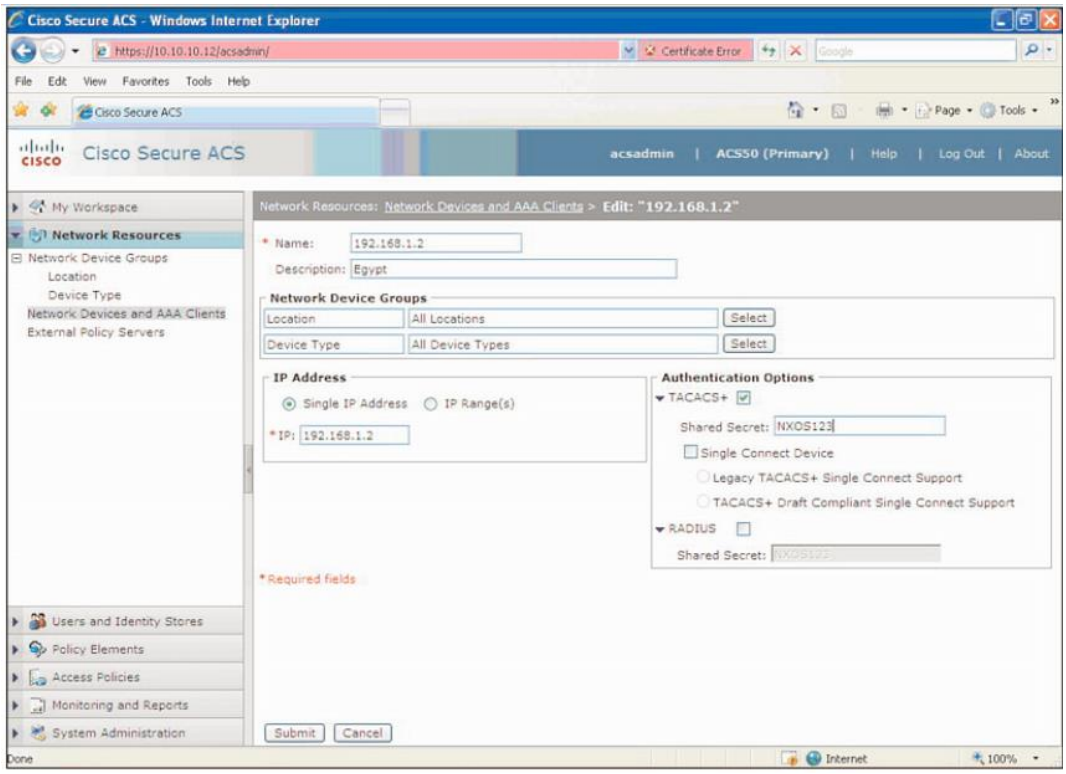
شکل ٦ پیکربندی امن سیسکو ACS TACACS+ را نشان می‌دهد، که loopback دستگاه NX-OS و کلید سری که به هماهنگی بین دستگاه NX-OS و سرویس‌دهنده ACS Secure Cisco نیاز دارد، را تعریف می کند.



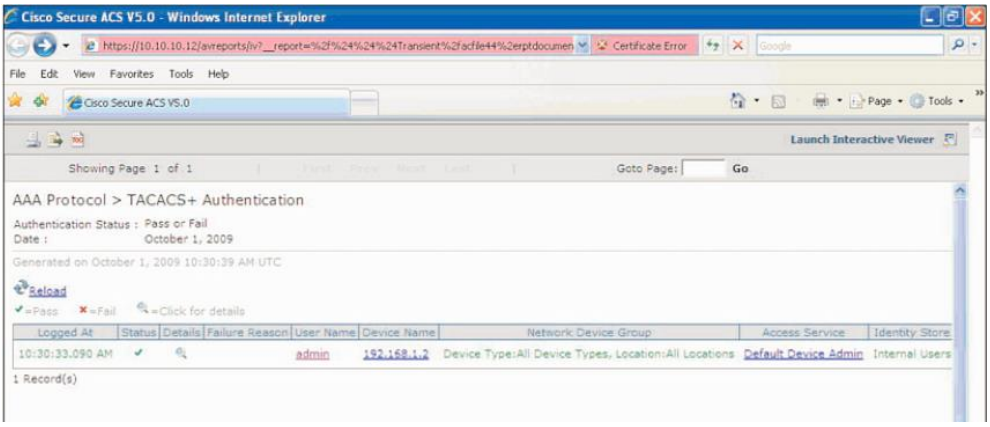
شکل ٦ پیکربندی +TACACS پیکربندی اختصاصی امن سیسکو ACS

شکل ۷ پیکربندی دستگاه‌های NX-OS که برای هر کدام از آنها تعریف شده است را نشان می‌دهد.

شکل ۸، +TACACS احرازهویت موفق کاربر برای دسترسی SSH به دستگاه NX-OS را نشان می‌دهد.



شکل ۷ اضافه کردن دستگاه‌های NX-OS به سیستم پشتیبان ACS امن سیسکو



شکل ۸ احرازهویت موفق از طریق +TACACS برای کاربر admin

٤ پیکربندی SSH

پیکربندی SSH از سرویس‌دهنده، سرویس‌گیرنده، و کلیدهای سرویس‌دهنده تشکیل شده است. سرویس‌دهنده SSH دستگاه‌های NX-OS را فعال می‌کند تا اتصال امن و رمزگذاری‌شده در سرویس‌گیرنده

SSH برقرار شود. SSH از رمزنگاری قوی برای احرازهویت استفاده می‌کند. برنامه سرویس‌گیرنده در پروتکل SSH برای تأیید هویت و رمزگذاری دستگاه اجرا می‌شود.

سرویس‌گیرنده SSH یک دستگاه NX-OS را برای ایجاد یک اتصال امن و رمزگذاری شده به هر دستگاه اجراکننده‌ی سرویس‌دهنده SSH، قادر می‌سازد.

پیاده‌سازی سرویس‌دهنده SSH و سرویس‌گیرنده SSH قابلیت همکاری با پیاده‌سازی‌های عمومی و تجاری را فراهم می‌سازد.

NX-OS از کلیدهای زیر برای سرویس‌دهنده SSH پشتیبانی می‌کند:

- SSH نیاز به کلید سرویس‌دهنده برای برقراری ارتباط امن با دستگاه NX-OS دارد. شما می‌توانید از کلیدهای سرویس‌دهنده SSH برای گزینه‌های SSH زیر استفاده کنید:
  - SSH نسخه ۲ از رمزنگاری کلید عمومی RSA[۸] استفاده می‌کند.
  - SSH نسخه ۲ از DSA[۹] استفاده می‌کند.
- قبل از فعال‌کردن سرویس SSH مطمئن شوید که یک جفت کلید سرویس‌دهنده SSH با نسخه مناسب داشته باشید. شما می‌توانید جفت کلید سرویس‌دهنده SSH را با توجه به نسخه سرویس‌دهنده SSH مورد استفاده قرار دهید. سرویس SSH دو نوع جفت کلید را برای استفاده از SSH نسخه ۲ می‌پذیرد:
  - گزینه DSA، برای پروتکل SSH نسخه ۲، جفت کلید DSA را تولید می‌کند.
  - گزینه RSA، جفت کلید RSA را برای پروتکل SSH نسخه ۲، تولید می‌کند.
- SSH از قالب‌های کلید عمومی زیر پشتیبانی می‌کند:
  - OpenSSH
  - IETF Secure Shell (SECSH)

توجه: اطمینان حاصل کنید که شما در VDC صحیح هستید (یا از دستور switchto vdc استفاده کنید).

[۸] Rivest, Shamir, and Adelman

[۹] Digital System Algorithm

برای فعال‌کردن فرآیند ماژولار SSH، دستورات زیر را وارد کنید:

```
Switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-1(config)# feature ssh
```

مثال ۲۰: این مثال چگونگی ایجاد کلید سرویس‌دهنده SSH را نشان می‌دهد. کلید پیش‌فرض سرویس‌دهنده SSH یک کلید RSA است که با استفاده از ۱۰۲٤ بیت تولید می‌شود.

```
Switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-1(config)# ssh key rsa 2048
rsa keys already present, use force option to overwrite them
Switch-1(config)# ssh key rsa 2048 force
deleting old rsa key.....
generating rsa key(2048 bits).....
generated rsa key
Switch-1(config)# feature ssh
Switch-1(config)# exit
```

مثال ۲۱: چگونگی تأیید کلیدهای سرویس‌دهنده SSH که در دستگاه NX-OS تولید شده‌اند

```
Switch-1# show ssh key
**************************************
rsa Keys generated:Wed Sep 30 14:38:37 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAsxCDzRe9HzqwzWXSp5kQab2NlX9my68RdmFFsM0
M+fAB
GNdwd5q01g5AKfuqvnrkAl7DR9n0d2v2Zde7JbZx2HCUjQFGEVAlK2a7I6pfCBschiRUf6j/7D
BcCdHf
1SQrTTvQLhwEhFkbginXqlhuNjSbJj5uxMZYEInenxLswNe7Kc/Ovdw3lBbxdgHCKOSTrVs47
PKshwST
PBcoqX/7Df5oCW8Um8ipJ0U3/7lnZlEE9Uz+ttT1zYf1ApqfsErAGT4wZo973Iza0Ub3lyWBnC
hQBN6n
ScxvYk/1wuqF4P0nS4ujnW9X+pxvBE1JedQDf6f0rj+Txt9L5AfqYnI+bQ==
bitcount:2048
fingerprint:
15:63:01:fc:9f:f7:66:35:3c:90:d3:f8:ed:f8:bb:16
**************************************
```

مثال ۲۲: نحوه بررسی ارتباطات سرویس‌دهنده SSH با دستگاه NX-OS را نشان می‌دهد.

```
Switch-1# show int mgmt 0
```

```
mgmt0 is up
Hardware: GigabitEthernet, address: 001b.54c1.b448 (bia 001b.54c1.b448)
Internet Address is 172.26.32.37/27
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
full-duplex, 1000 Mb/s
Auto-Negotiation is turned on
1 minute input rate 952 bits/sec, 1 packets/sec
1 minute output rate 648 bits/sec, 0 packets/sec
Rx
12649 input packets 11178 unicast packets 951 multicast packets
520 broadcast packets 1423807 bytes
Tx
7653 output packets 6642 unicast packets 953 multicast packets
58 broadcast packets 943612 bytes
[hk@hk .ssh]$ ssh admin@172.26.32.37
User Access Verification
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

مثال ۲۳: بررسی پیکربندی سرویس‌دهنده SSH در دستگاه NX-OS را نشان می‌دهد.

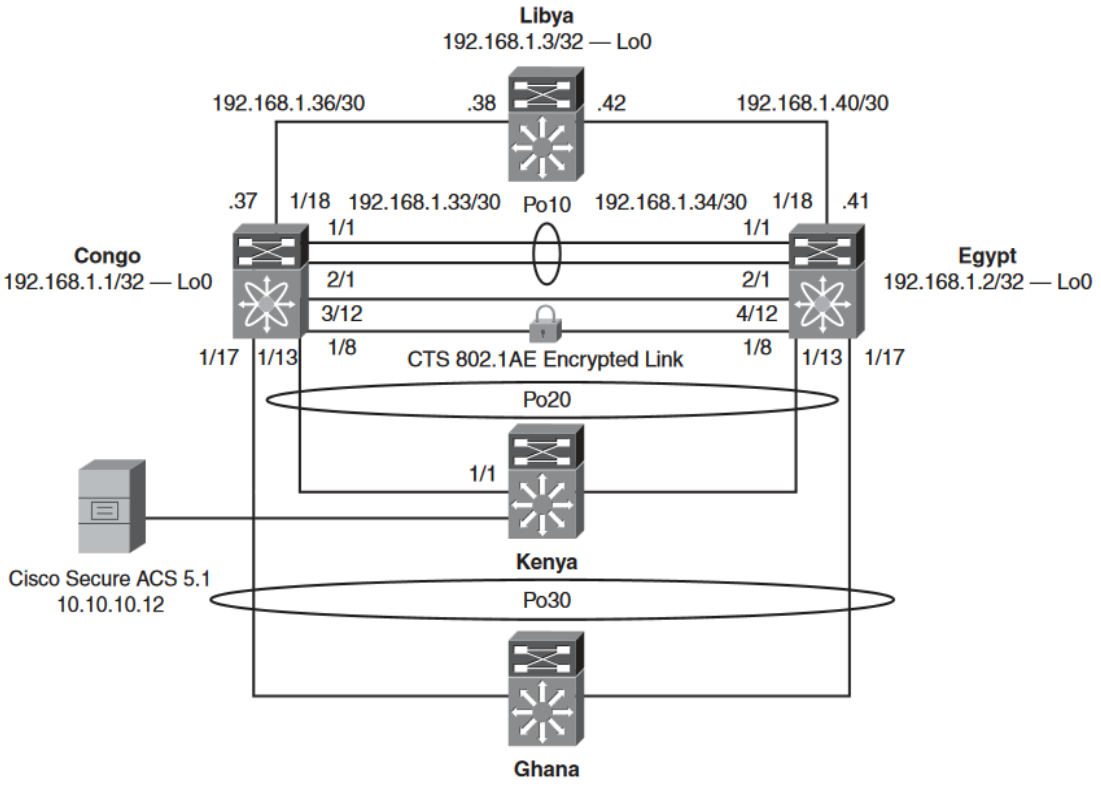
```
Switch-1# show ssh server
ssh version 2 is enabled
Switch-1# show ssh key
**************************************
rsa Keys generated:Wed Sep 30 14:38:37 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAsxCDzRe9HzqwzWXSp5kQab2NlX9my68RdmFFsM0
M+fABGNdwd5q01g5
AKfuqvnrkAl7DR9n0d2v2Zde7JbZx2HCUjQFGEVAlK2a7I6pfCBschiRUf6j/7DBcCdHf1SQrT
TvQLhwEhF
kbginXqlhuNjSbJj5uxMZYEInenxLswNe7Kc/Ovdw3lBbxdgHCKOSTrVs47PKshwSTPBcoqX/7
Df5oCW8Um
8ipJ0U3/7lnZlEE9Uz+ttT1zYf1ApqfsErAGT4wZo973Iza0Ub3lyWBnChQBN6nScxvYk/1wuqF
4P0nS4uj
nW9X+pxvBE1JedQDf6f0rj+Txt9L5AfqYnI+bQ==
bitcount:2048
```

```
fingerprint:
15:63:01:fc:9f:f7:66:35:3c:90:d3:f8:ed:f8:bb:16
```

۵ پیکربندی TrustSec سیسکو

NX-OS با استفاده از ویژگی امنیتی TrustSec، محرمانگی و یکپارچگی داده‌ها را فراهم می‌کند و رمزگذاری لایه پیوند استاندارد IEEE802.1AE با رمزنگاری AES، ۱۲۸ بیتی را پشتیبانی می‌کند. رمزگذاری لایه پیوند به اطمینان از صحت داده انتها به انتها کمک می‌کند و امکان قراردادن دستگاه‌های سرویس امنیتی در مسیر رمزگذاری شده را فراهم می‌آورد.

امروزه رمزگذاری لایه‌ی پیوند IEEE 802.1AE نقطه‌به‌نقطه است. معماری امنیت TrustSec با ایجاد دستگاه‌های شبکه قابل اعتماد، شبکه‌های امن را ایجاد می‌کند که در آن‌ها هر دستگاه توسط همسایگان خود تأیید شده است. برای پیکربندی‌ها در این بخش، به توپولوژی شبکه در شکل ۹ مراجعه کنید.



شکل ۹ توپولوژی سیسکو CTS 802.1AE

برای تأیید ویژگی‌های 802.1x و CTS در دستگاه NX-OS و فعال‌کردن CTS، دستورات زیر را وارد کنید:

```
Switch-2# conf t
```

```
Switch-2 (config)# feature dot1x
Switch-2 (config)# feature cts
```

برای تأیید اینکه ویژگی‌های 802.1x و CTS فعال هستند، دستور زیر را وارد کنید:

```
Switch-2# show run cts
feature dot1x
feature cts
```

توجه: شناسه و کلمه عبور در دستگاه منحصربه‌فرد CTS، حداکثر ۳۲ کاراکتر دارند و حساس به حروف هستند.

مثال ۲٤: این مثال نحوه پیکربندی شناسه دستگاه منحصربه‌فرد CTS را نشان می‌دهد.

```
Switch-2(config)#
cts device-id Switch-2-cts password CTS_TrustSec123
Switch-2(config) # interface Ethernet1/8
Switch-2(config-if)# description to Switch-1
Switch-2(config-if)# switchport
Switch-2(config-if)# switchport access vlan 500
Switch-2(config-if)# cts manual
Switch-2(config-if-cts-manual)# sap pmk deadbeef modelist gcm-encrypt
Switch-2(config-if)# mtu 9216
Switch-2(config-if)# no shutdown
Switch-2(config)# interface Vlan500
Switch-2(config-if)# no shutdown
Switch-2(config-if)# ip address 1.1.1.1/24
```

برای فعال‌کردن ویژگی‌های 802.1x و CTS در دستگاه NX-OS و برای پشتیبانی CTS در Switch-1، دستورات زیر را وارد کنید:

```
Switch-1# conf t
Switch-1(config)# feature dot1x
Switch-1(config)# feature cts
```

برای تأیید اینکه ویژگی‌های 802.1x و CTS فعال هستند، دستور زیر را وارد کنید:

```
Switch-2# show run cts
feature dot1x
```

```
feature cts
```

مثال ۲۵: این مثال نحوه پیکربندی شناسه دستگاه منحصربه‌فرد CTS در Switch-1 را نشان می‌دهد.

```
Switch-1(config)#
cts device-id Switch-1-cts password CTS_TrustSec123
Switch-1(config)# interface Ethernet1/8
Switch-1(config-if)# description to Switch-2
Switch-1(config-if)# switchport
Switch-1(config-if)# switchport access vlan 500
Switch-1(config-if)# cts manual
Switch-1(config-if)# sap pmk deadbeef modelist gcm-encrypt
Switch-1(config-if)# mtu 9216
Switch-1(config-if)# no shutdown
Switch-1(config# interface Vlan500
Switch-1(config-if)# no shutdown
Switch-1(config-if)# ip address 1.1.1.2/24
--------------------------------------------------------------------------------
Switch-2# show runn int e1/8
!Command: show running-config interface Ethernet1/8
!Time: Wed Sep 30 18:25:19 2009
version 4.2(2a)
interface Ethernet1/8
description to Switch-1
cts manual
sap pmk deadbeef00000000000000000000000000000000000000000000000000000000
switchport
switchport access vlan 500
mtu 9216
no shutdown
```

مثال ۲۶: تأیید پیکربندی CTS در Switch-2

```
Switch-2# show runn cts
!Command: show running-config cts
!Time: Wed Sep 30 18:25:27 2009
version 4.2(2a)
feature cts
cts device-id Switch-2-cts password 7 FPW_LrpxlVoh123
interface Ethernet1/8
cts manual
sap pmk deadbeef00000000000000000000000000000000000000000000000000000000
```

```
Switch-2# show cts interface e1/8
CTS Information for Interface Ethernet1/8:
CTS is enabled, mode: CTS_MODE_MANUAL
IFC state: CTS_IFC_ST_CTS_OPEN_STATE
Authentication Status: CTS_AUTHC_SKIPPED_CONFIG
Peer Identity:
Peer is: Unknown in manual mode
802.1X role: CTS_ROLE_UNKNOWN
Last Re-Authentication:
Authorization Status: CTS_AUTHZ_SKIPPED_CONFIG
PEER SGT: 0
Peer SGT assignment: Not Trusted
SAP Status: CTS_SAP_SUCCESS
Configured pairwise ciphers: GCM_ENCRYPT
Replay protection: Enabled
Replay protection mode: Strict
Selected cipher: GCM_ENCRYPT
Current receive SPI: sci:23ac65020c0000 an:2
Current transmit SPI: sci:23ac6409d80000 an:2
Switch-2#
```

مثال ۲۷: پیکربندی CTS در Switch-1 را تأیید می‌کند.

```
Switch-1# show runn int e1/8
!Command: show running-config interface Ethernet1/8
!Time: Wed Sep 30 18:24:39 2009
version 4.2(2a)
interface Ethernet1/8
description to Switch-2
cts manual
sap pmk deadbeef00000000000000000000000000000000000000000000000000000000
switchport
switchport access vlan 500
mtu 9216
no shutdown
Switch-1# show runn cts
!Command: show running-config cts
!Time: Wed Sep 30 18:24:48 2009
version 4.2(2a)
feature cts
cts device-id Switch-1-cts password 7 FPW_LrpxlVoh123
interface Ethernet1/8
cts manual
sap pmk deadbeef00000000000000000000000000000000000000000000000000000000
Switch-1# show cts interface e1/8
CTS Information for Interface Ethernet1/8:
CTS is enabled, mode: CTS_MODE_MANUAL
```

```
IFC state: CTS_IFC_ST_CTS_OPEN_STATE
Authentication Status: CTS_AUTHC_SKIPPED_CONFIG
Peer Identity:
Peer is: Unknown in manual mode
802.1X role: CTS_ROLE_UNKNOWN
Last Re-Authentication:
Authorization Status: CTS_AUTHZ_SKIPPED_CONFIG
PEER SGT: 0
Peer SGT assignment: Not Trusted
SAP Status: CTS_SAP_SUCCESS
Configured pairwise ciphers: GCM_ENCRYPT
Replay protection: Enabled
Replay protection mode: Strict
Selected cipher: GCM_ENCRYPT
Current receive SPI: sci:23ac6409d80000 an:1
Current transmit SPI: sci:23ac65020c0000 an:1
```

مثال ۲۸:این مثال تأیید VLAN مورد استفاده برای CTS را نشان می‌دهد.

```
Switch-1# show vlan
VLAN Name Status Ports
--------------------------------------------------------------------------------
1 default active Po10
5 Switch-1_Switch-2_Transit active Po10
10 Secure_Subnet active Po10, Po20, Po30
100 Server_Subnet1 active Po10, Po30
500 CTS_TrustSec active Po10, Eth1/8
VLAN Type
1       enet
5       enet
10      enet
100     enet
500     enet
---- -----
```

مثال ۲۹: بررسی ارتباطات با استفاده از دستور ping، بین Switch-1 و Switch-2 (دو سوئیچ Nexus 7000) را نشان می‌دهد. فریم ping رمزشده Nexus 7000 از طریق برنامه WireShark تعبیه شده و روی Switch-2 اجرا می‌شود. آزمون ping، ترافیک را از طریق جلسه رمزنگاری CTS 802.1AE بین Switch-1 و Switch-2 تأیید می‌کند.

```
Started ping from Switch-1:
Switch-1# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
```

```
64 bytes from 1.1.1.1: icmp_seq=0 ttl=254 time=1.189 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=254 time=0.702 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=254 time=0.718 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=254 time=0.601 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=254 time=0.604 ms
Switch-2# ethanalyzer local interface inband detail limit-captured-frames 200
Frame 4 (98 bytes on wire, 98 bytes captured)
Arrival Time: Sep 30, 2009 18:39:12.837070000
[Time delta from previous captured frame: 0.255613000 seconds]
[Time delta from previous displayed frame: 0.255613000 seconds]
[Time since reference or first frame: 0.256374000 seconds]
Frame Number: 4
Frame Length: 98 bytes
Capture Length: 98 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:data]
Ethernet II, Src: 00:1b:54:c2:76:41 (00:1b:54:c2:76:41), Dst: 00:1b:54:c2:78:c1
(00:1b:54:c2:78:c1)
Destination: 00:1b:54:c2:78:c1 (00:1b:54:c2:78:c1)
Address: 00:1b:54:c2:78:c1 (00:1b:54:c2:78:c1)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
Source: 00:1b:54:c2:76:41 (00:1b:54:c2:76:41)
Address: 00:1b:54:c2:76:41 (00:1b:54:c2:76:41)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory
default)
Type: IP (0x0800)
Internet Protocol, Src: 1.1.1.2 (1.1.1.2), Dst: 1.1.1.1 (1.1.1.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 84
Identification: 0x43b2 (17330)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0x73f2 [correct]
[Good: True]
[Bad : False]
Source: 1.1.1.2 (1.1.1.2)
Destination: 1.1.1.1 (1.1.1.1)
Internet Control Message Protocol
```

```
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x5573 [correct]
Identifier: 0x572d
Sequence number: 0 (0x0000)
Data (56 bytes)
0000 e1 a5 c3 4a cd e7 03 00 cd ab 00 00 cd ab 00 00 ...J.....
0010 cd ab 00 00 cd ab 00 00 cd ab 00 00 cd ab 00 00 ................
0020 cd ab 00 00 cd ab 00 00 cd ab 00 00 cd ab 00 00 ................
0030 30 31 32 33 34 35 36 37 01234567
Data: E1A5C34ACDE70300CDAB0000CDAB0000CDAB0000CDAB0000...
```

۵-۱ راه‌حل‌های بین مراکز داده در لایه ۲

اصلی‌ترین درخواست سرویس‌گیرنده در لایه ۲ اتصال بین مراکز داده به جای کاربردهای مجازی‌سازی خوشه‌ای و سرویس‌دهنده است. با توجه به شرایط لایه ۲ نیاز به رمزنگاری وجود دارد که با رعایت کردن قوانین و مقررات مربوطه و یا سایر عوامل قابل قبول است.

Nexus 7000 از رمزنگاری Linksec نقطه‌به‌نقطه 802.1ae، در تمامی درگاه‌های سخت‌افزاری پشتیبانی می کند. با توجه به شکل ۱۰ اگر یک محیط MPLS[۱۰] دارید، می‌توانید سوئیچ‌های Nexus 7000 را با یک ASR1000 یا Catalyst 6500 اجرایی در حالت درگاه EoMPLS، متوقف کنید. حالت پورت EoMPLS شبیه یک سیم برای Nexus 7000 است. اطمینان حاصل کردن از ارسال پیام‌های SAP[۱۱] واحد داده برای رمزنگاری CTS از طریق یک شبه سیم (EoMPLS (PW، مهم است. همچنین VPC[۱۲] در Nexus 7000 برای یک محیط Loop-Free Spanning-tree و STP ایزوله شده، فعال می‌شود. بنابراین شما می‌توانید یک ریشه STP در هر مرکز داده داشته باشد. همان‌طور که رمزگذاری MPLS چالش‌هایی را به وجود می‌آورد؛ اگر MPLS مورد نیاز نباشد، Nexus 7000 TrustSec می‌تواند داده‌ها را در یک مرکز داده از راه دور محافظت کند.

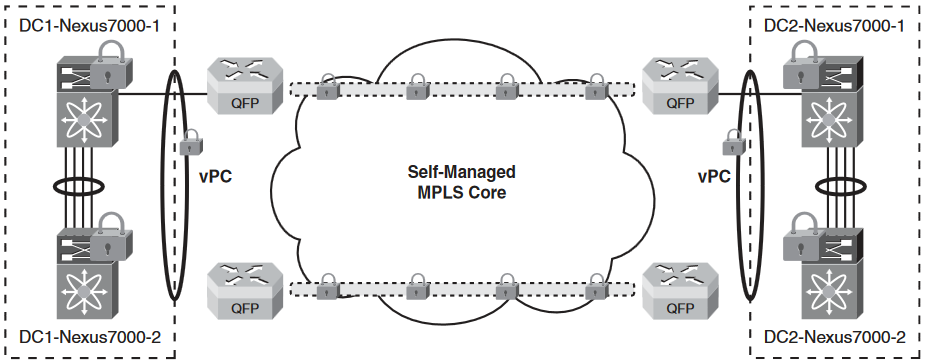
---

[۱۰] Multiporotocol Label Swiching

[۱۱] Security Association Protocol

[۱۲] Virtual Port-Channel

شکل ۱۰ رابط متصل‌کننده به مرکز داده را نشان می‌دهد، که اتصالات P2P را با رمزگذاری از طریق ابر MPLS فراهم می‌کند. Nexus 7000s و ASR1002s به ترتیب با Cisco TrustSec و پورت حالت EoMPLS PW پیکربندی می‌شوند.



شکل ۱۰ اتصال مرکز داده از بین MPLS Cloud Leveraging Cisco TrustSec در Nexus 7000 [3]

٦ پیکربندی IP ACLs

ACL[۱۳]ها مجموعه‌ای از قوانین هستند که می‌توانید برای فیلترکردن ترافیک استفاده کنید. هر قانون یک مجموعه‌ای از شرایط را مشخص می‌کند که برای یک بسته باید برآورده شود تا با قانون تطبیق داشته باشد. اولین قانون تطبیق، تعیین این است که آیا بسته مجاز یا رد شده است. ACLها از شبکه و میزبان‌های خاص در برابر ترافیک غیرضروری یا ناخواسته محافظت می‌کنند. NX-OS از IPv4 و IPv6 IP ACL برای ایجاد و اعمال به واسط‌های کاربری، واسط‌های VLAN و port-channels پشتیبانی می‌کند [2].

مثال ۳۰: ایجاد یک جلسه پیکربندی و ورود به حالت پیکربندی جلسه را نشان می‌دهد.

```
Switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-1(config)# configure session ACL-TCP-IN
Config Session started, Session ID is 3
```

مثال ۳۱: نحوه ایجاد ACL برای فعال‌کردن TCP را نشان می‌دهد.

[۱۳] Access Control Lists

```
Switch-1(config-s)# ip access-list TCP1
Switch-1(config-s-acl)# permit tcp any any
Switch-1(config-s-acl)# exit
Switch-1(config-s)# save bootflash:SessionMgrTCPIn
Switch-1(config-s)# interface ethernet 1/1
```

مثال ۳۲: نحوه استفاده از ACL به واسط کاربری را نشان می‌دهد و مسیر استفاده از گروه دسترسی را تعیین می‌کند.

```
Switch-1(config-s-if)# ip access-group TCP1 in
```

مثال ۳۳: نحوه تأیید پیکربندی را به طور کلی بر اساس پیکربندی سخت‌افزار و نرم‌افزارهای موجود و منابع نشان می‌دهد.

```
Switch-1(config-s-if)# verify
Verification Successful
```

مثال ۳٤: تأیید تغییرات پیکربندی در جلسه فعلی و اعمال تغییرات به دستگاه

```
Switch-1(config-s)# commit
Commit Successful
```

مثال ۳۵: تأیید مدیریت جلسه و ACL

```
Switch-1# conf t
Switch-1(config)# configure session ACL-TCP-IN
Config Session started, Session ID is 3
Switch-1(config-s)# ip access-list TCP1
Switch-1(config-s-acl)# permit tcp any any
Switch-1(config-s-acl)# interface e1/1
Switch-1(config-s-if)# ip access-group TCP1 in
Switch-1(config-s-if)# show configuration session
config session IP-ACL1
config session ACL-TCP-IN
0001 ip access-list TCP1
0002 permit tcp any any
0003 interface Ethernet1/1
0004 ip access-group TCP1 in
Number of active configuration sessions = 3
Switch-1(config-s-if)# save bootflash:SessionMgrTCPIn
```

```
Switch-1(config-s)# verify
Verification Successful
Switch-1(config-s)# commit
Commit Successful
Switch-1# show access-lists TCP1
IP access list TCP1
10 permit tcp any any
Switch-1# show running-config interface e1/1
!Command: show running-config interface Ethernet1/1
!Time: Sat Oct 10 12:10:55 2009
version 4.2(2a)
interface Ethernet1/1
description to Switch-2
ip access-group TCP1 in
switchport
switchport access vlan 500
mtu 9216
no shutdown
Switch-1#
```

۷ پیکربندی MAC ACLs

MAC ACLها اطلاعات ترافیکی را در سرآیند لایه ۲ بسته‌ها، برای فیلترکردن ترافیک، مطابقت می‌دهند. طبقه‌بندی بسته‌های MAC شما را قادر می‌سازد تا کنترل کنید که آیا MAC ACL در یک واسط لایه‌ی ۲ به تمام ترافیک، از جمله ترافیک IP، یا تنها ترافیک غیر IP اعمال می‌شود. MAC ACLها را می‌توان فقط برای دسترسی به ترافیک استفاده کرد.

مثال ۳۶: این مثال نشان می‌دهد که چگونه یک MAC ACL را ایجاد کرده و پیکربندی ACL را وارد کنید.

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# mac access-list mac-acl
Switch-2(config-mac-acl)# permit 0050.561f.73d3 0050.56bc.48dd any
```

مثال ۳۷: چگونگی حفظ آمار عمومی و شمارنده‌ای، برای بسته‌هایی که با قوانین ACL مطابقت دارند، را نشان می‌دهد. این سوئیچ آمار عمومی برای بسته‌هایی که با قوانین ACL مطابقت دارند را حفظ می‌کند.

```
Switch-2(config-mac-acl)# statistics per-entry
```

مثال ۳۸: نحوه تأیید پیکربندی MAC ACL را نشان می‌دهد.

```
Switch-2(config-mac-acl)# show mac access-lists mac-acl
MAC access list mac-acl
statistics per-entry
10 permit 0050.561f.73d3 0050.56bc.48dd any
Switch-2(config-mac-acl)# exit
Switch-2(config)# exit
Switch-2(config)# mac access-list mac-acl
Switch-2(config-mac-acl)# 100 permit 0050.561f.73d3 0000.00ff.ffff any
Switch-2# show mac access-lists mac-acl
MAC access list mac-acl
statistics per-entry
10 permit 0050.561f.73d3 0050.56bc.48dd any
100 permit 0050.561f.73d3 0000.00ff.ffff any
```

مثال ۳۹: تغییر دنباله اعداد ACL مختص به قانون در یک MAC ACL

```
Switch-2(config)# resequence mac access-list mac-acl 200 10
Switch-2(config)# exit
Switch-2# show mac access-lists mac-acl
MAC access list mac-acl
statistics per-entry
200 permit 0050.561f.73d3 0050.56bc.48dd any
210 permit 0050.561f.73d3 0000.00ff.ffff any
Switch-2#
```

۸ پیکربندی VLAN ACLها

VLAN ACL یک برنامه از MAC ACL یا IP ACL است. شما می‌توانید پیکربندی VACLها را به تمام بسته‌های داخل یا خارج از یک VLAN یا در پل ارتباطی داخل یک VLAN اعمال کنید. VACLها برای فیلترکردن بسته‌های امنیتی و هدایت ترافیک به واسط فیزیکی خاص گسترش یابند.

توجه: VACLها با جهت (ورود یا خروج) تعریف نمی‌شوند.

مثال ٤٠: نحوه پیکربندی یک VACL به نام acl-mac-map برای انتقال ترافیک مجاز توسط یک MAC ACL را نشان می‌دهد.

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# vlan access-map acl-mac-map
Switch-2(config-access-map)# match mac address mac-acl
```

```
Switch-2(config-access-map)# action forward
Switch-2(config-access-map)# statistics per-entry
Switch-2(config-access-map)# exit
Switch-2(config)# exit
Switch-2# show runn aclmgr
!Command: show running-config aclmgr
!Time: Thu Oct 1 17:19:24 2009
version 4.2(2a)
mac access-list mac-acl
statistics per-entry
200 permit 0050.561f.73d3 0050.56bc.48dd any
210 permit 0050.561f.73d3 0000.00ff.ffff any
vlan access-map acl-mac-map 10
match mac address mac-acl
action forward
statistics per-entry
Switch-2#
```

مثال ٤١: نحوه اعمال VACL به لیست VLAN را نشان می‌دهد.

```
Switch-2(config)# vlan filter acl-mac-map vlan-list 10
Switch-2(config)# show running-config aclmgr
!Command: show running-config aclmgr
!Time: Thu Oct 1 17:24:17 2009
version 4.2(2a)
mac access-list mac-acl
statistics per-entry
    200 permit 0050.561f.73d3 0050.56bc.48dd any
    210 permit 0050.561f.73d3 0000.00ff.ffff any
vlan access-map acl-mac-map 10
   match mac address mac-acl
   action forward
   statistics per-entry
vlan filter acl-mac-map vlan-list 10
Switch-2(config)#
```

۹ پیکربندی Port Security

Port Security شما را قادر می‌سازد تا درگاه فیزیکی و درگاه port-channel را در لایه ۲ پیکربندی امن کنید که ترافیک ورودی را از مجموعه‌ی محدودی از آدرس‌های MAC فعال می‌کند. آدرس‌های MAC در مجموعه محدود، secure MAC addresses نامیده می‌شوند. علاوه بر این، دستگاه، ترافیک را از این آدرس‌های MAC در یک واسط دیگر درون همان VLAN فعال نمی‌کند. تعداد آدرس‌های MAC که دستگاه می‌تواند امن کند برای هر درگاه فیزیکی خروجی قابل پیکربندی است.

مثال ٤٢: نحوه تأیید ویژگی Port Security را نشان می‌دهد و اگر در حال حاضر غیرفعال است، آن را فعال کنید.

```
Switch-2(config)# show feature |i port
eth_port_sec    1      disabled
Switch-2(config)# feature port-security
Switch-2(config)# show feature |i port
eth_port_sec    1      enabled
Switch-2(config)#
```

مثال ٤٣: نحوه فعال‌کردن Port Security در واسط لایه ۲ را نشان می‌دهد.

```
Switch-2#
conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# int e1/1
Switch-2(config-if)# switchport port-security
Switch-2(config-if)#
Switch-2# show running-config port-security
!Command: show running-config port-security
!Time: Thu Oct 1 17:41:20 2009
version 4.2(2a)
feature port-security
interface Ethernet1/1
switchport port-security
Switch-2#
```

توجه: هنگامی‌که Port Security در یک واسط غیرفعال است، تمام پیکربندی Port Security برای واسط، از جمله هر گونه آدرس Secure MAC در واسط آموزش داده شده، از بین می‌رود.

مثال ٤٤ نحوه فعال‌کردن Sticky MAC Address Learning را نشان می‌دهد. هنگامی‌که Sticky MAC را روی یک رابط فعال می‌کنید، سوئیچ، آموزش پویا را انجام نمی‌دهد و به جای آن Sticky Learning را انجام می‌دهد. این سوئیچ، Sticky Secure MAC Addresses نیست.

مثال ٤٤: فعال‌کردن Sticky MAC Address Learning

```
Switch-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# int e1/1
Switch-2(config-if)# switchport port-security mac-address sticky
Switch-2(config-if)# exit
Switch-2# show running-config port-security
```

```
!Command: show running-config port-security
!Time: Thu Oct 1 17:43:06 2009
version 4.2(2a)
feature port-security
interface Ethernet1/1
switchport port-security
switchport port-security mac-address sticky
Switch-2#
```

توجه: اگر sticky learning در یک واسط غیرفعال باشد؛ واسط به حالت پیش‌فرض MAC Address Learning بازگردانده می‌شود.

مثال ٤٥: این مثال نشان می‌دهد که چگونه یک Static Secure MAC Address را به Ethernet 1/1 اضافه کنید. StaticMAC با استفاده از آدرس‌های MAC برای برنامه‌های ناسازگار مفید است.

```
Switch-2#  conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-2(config)# int e1/1
Switch-2(config-if)# switchport port-security mac-address 0050.561f.73d3
Switch-2(config-if)# exit
Switch-2# show running-config port-security
!Command: show running-config port-security
!Time: Thu Oct 1 17:46:20 2009
version 4.2(2a)
feature port-security
interface Ethernet1/1
switchport port-security
switchport port-security mac-address 0050.561F.73D3
Switch-2# show port-security
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
------------------------------------------------------------------------------
-----
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
------------------------------------------------------------------------------
Ethernet1/1 1 1 0 Shutdown
==============================================================================
====================
Switch-2#
```

۹-۱ اقدامات و تخلفات امنیتی

هنگامی که یک نقص امنیتی اتفاق می‌افتد، پیکربندی عملیات در هر واسط با Port Security فعال شده و عکس‌العمل متناسب با پیکربندی به شرح زیر روی می‌دهد:

- shutdown: واسطی که بسته‌ی مخرب دریافت کرده را غیرفعال می‌کند؛ بازسازی مجدد واسط کاربری، پیکربندی Port Security که شامل Secure MAC Address است را حفظ می‌کند.
- errdisable: اگر رابط کاربری غیرفعال گردد یا خاموشی رخ دهد برای فعال‌شدن مجدد واسط کاربری به طور خودکار، دستور پیکربندی عمومی را بایستی مجدد پیکربندی کنید، یا می‌توانید به صورت دستی با وارد کردن دستورات پیکربندی shutdown و no shutdown مجدداً واسط را راه اندازی کنید.
- restrict: پس از اینکه ۱۰۰ نقض امنیتی رخ می‌داد، دستگاه تمام ترافیک ورودی را از MAC Address غیرمجاز حذف می کند. علاوه بر این، دستگاه یک اعلان SNMP را برای هر نقض امنیتی تولید می‌کند.
- protect: از رخداد نقض‌های بیشتر جلوگیری می‌کند.

مثال ٤٦ پیکربندی نقض Port Security 1/1 در واسط اترنت

```
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)# switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shtudown mode
Switch-2(config-if)# switchport port-security violation
```

مثال ٤٧: پیکربندی حداکثر تعداد آدرس‌های MAC در واسط اترنت ۱/۱

```
Switch-2(config)# int e1/1
Switch-2(config-if)# switchport port-security maximum 51
Switch-2(config-if)# show port-security
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
------------------------------------------------------------------------------
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
------------------------------------------------------------------------------
```

```
Ethernet1/1 51 0 0 Shutdown
================================================================
====================
Switch-2(config-if)#
Switch-2# show port-security int e1/1
Port Security : Enabled
Port Status : Secure UP
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
Maximum MAC Addresses : 51
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Security violation count : 0
Switch-2#
```

۱۰ 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.