باسمه تعالی

پیکربندی امن سوئیچ‌های نسل جدید سیسکو NX-OS

(بخش اول)

فهرست مطالب

۱ مقدمه

NX-OS جدیدترین سیستم‌عامل شرکت سیسکو برای تجهیزات جدید این شرکت است. شرکت سیسکو برای برخی از تجهیزات مخابراتی خود همچون سوئیچ‌ها و مسیریاب‌ها سیستم‌عامل اختصاصی طراحی کرده است تا مدیر شبکه به راحتی بتواند آن‌ها را پیکربندی و آماده استفاده کند. در تجهیزات فیزیکی، سیستم‌عامل در نقش یک رابط نرم، کار پیکربندی سخت‌افزاری را راحت‌تر می‌کند. افرادی که با چنین تجهیزاتی سروکار دارند قطعاً بایستی با این سیستم‌عامل آشنایی داشته باشند تا بتوانند مسیریاب یا سوئیچ و سایر سخت‌افزارها را به درستی پیکربندی و راه‌اندازی کنند.

NX-OS بر مبنای لینوکس توسعه داده شده است و به صورت لایه میانی می‌تواند با سایر سیستم‌عامل‌های این شرکت نیز ارتباط برقرار کند. خط فرمان این سیستم‌عامل همانند سیستم‌عامل قبلی این شرکت یعنی IOS است. از ویژگی‌های کلیدی این سیستم‌عامل قدرتمند می‌توان به sysmgr یا مدیریت سیستم، PSS یا سرویس ذخیره مداوم داده‌ها و MTS یا سرویس تبادل پیام و تراکنش‌ها اشاره کرد.

اما یکی از سؤالاتی که مطرح می شود این است که تفاوت این سیستم‌عامل با سیستم‌عامل قدیمی سیسکو یعنی IOS چیست؟ NX-OS از دستور Login برای سوئیچ بین کاربران پشتیبانی نمی‌کند، بین لیست دسترسی استاندارد و توسعه‌یافته تفاوتی قائل نمی‌شود، از سرویس‌دهنده scp پایین‌تر از نسخه ۵٫۱ پشتیبانی نمی‌کند، به جای دستور write از copy استفاده می‌کند، وقتی کاربری به NX-OS دسترسی پیدا می‌کند به صورت مستقیم به سطح دسترسی تنظیم می شود، و در نهایت سرویس‌دهنده SSH به صورت پیش‌فرض فعال ولی Telnet غیرفعال است.

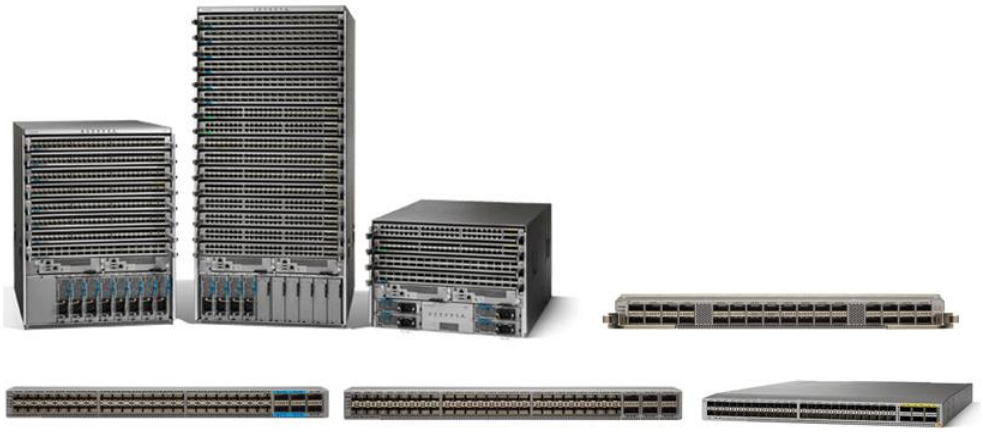
این سند به شما کمک می‌کند تا دستگاه‌های سیستم‌های نرم افزاری NX-OS سیسکو خود را امن کنید. این کار باعث افزایش امنیت کلی شبکه شما می شود. این سند در سه واحد طبقه‌بندی شده است که می‌توان با دسته‌بندی آن‌ها یک مرور کلی روی تمام خصوصیات امنیتی موجود در NX-OS سیسکو داشت. سه واحد عملیاتی یک شبکه عبارتند از: واحد مدیریت، واحد کنترل و واحد داده.

واحد مدیریتی: واحد مدیریتی، مسیر جریان ترافیک مورد استفاده در زمانی است که برای یک دستگاه NX-OS ارسال می‌شود. این واحد شامل برنامه‌ها و پروتکل هایی مانند SSH[۱] و SNMP[۲] است.

واحد کنترل: واحد کنترل، شبکه ترافیکی که برای حفظ عملکرد زیرساخت‌های شبکه مهم است را پردازش می‌کند. واحد کنترل شامل برنامه‌های کاربردی و پروتکل‌های بین دستگاه‌های شبکه، از جمله پروتکل‌های BGP[۳] و IGPs[۴] مانند EIGRP[۵] و OSPF[۶] است.

واحد داده: واحد داده، از طریق یک دستگاه شبکه داده را برمی‌گرداند و ترافیکی که به دستگاه محلی NX-OS ارسال می‌شود را شامل نمی‌شود.

خصوصیات امنیتی مورد بررسی در این سند، جزئیات مهم مورد نظر مهندسان و مدیران برای پیکربندی را ارائه می‌دهد. با این حال، حتی در مواردی که این کار انجام نشود، خصوصیات به گونه‌ای توضیح داده شده اند که شما می‌توانید تا میزان قابل توجهی خصوصیات مورد نیاز را ارزیابی کنید. این سند حاوی توصیه‌هایی است که در صورت پیاده‌سازی به امن‌سازی شبکه کمک می‌کنند.



[۱] Secure shell

[۲] Simple Network Management Protocol

[۳] Border Gateway Protocol

[۴] Interior gateway protocol

[۵] Enhanced Interior Gateway Routing Protocol

[۶] Open Shortest Path First

۱-۱ پیش‌نیازها

مهندسان و مدیران باید درک مفهومی از سیستم‌عامل NX-OS سیسکو و مفاهیم اولیه پیکربندی امن آن داشته باشند.

۱-۲ اجزای مورد استفاده

راهنمای این سند بر اساس نسخه NX-OS 5.1 سیسکو منتشر شده است. نسخه‌های پیشین نرم‌افزار NX-OS سیسکو ممکن است شامل تمام ویژگی‌ها یا قابلیت‌های مورد بحث در اینجا نباشد. اگر از نسخه‌ای غیر از نسخه NX-OS 5.1 (0) سیسکو استفاده می‌کنید، لطفاً از نکات منتشر شده و مستندات مربوط به آن نسخه برای جزئیات و ویژگی‌های پشتیبانی شده استفاده کنید.

این سند رهنمودهای مربوط به قابلیت‌های عمومی NX-OS سیسکو را ارائه می‌دهد. قابلیت‌های خاص سیسکو NX-OS ممکن است از یک پلت‌فرم به پلت‌فرم دیگر در محصولات خانواده‌ی Cisco Nexus متفاوت باشد. ممکن است برای یک پلت‌فرم خاص همه ویژگی‌ها در دسترس نباشد. لطفاً جزئیات یادداشت‌ها و مستندات مربوط به دستگاه‌های سخت‌افزاری خاص را برای جزئیات مربوط به ویژگی‌ها و قابلیت‌های پشتیبانی شده مورد بررسی قرار دهید.

۱-۳ اصول عملیات امن

اگرچه بیشتر این سند به پیکربندی امنیتی یک دستگاه NX-OS سیسکو اختصاص داده شده است ولی این پیکربندی به تنهایی امنیت شبکه را کامل نمی‌کند. روش‌های عملیاتی در استفاده از شبکه، مثل پیکربندی‌های دستگاه‌های پایه، به امنیت آن بسیار کمک می‌کند.

۱-٤ نظارت بر امنیت سیسکو، پرسش‌ها و پاسخ‌ها

تیم پاسخ به وقایع امنیتی سیسکو PSIRT[۷]، تولید و حمایت از نشریات را انجام داده‌اند. معمولاً توصیه‌های امنیتی PSIRT سیسکو، به نگرانی‌های امنیتی در محصولات سیسکو مربوط می‌شود و پاسخ امنیتی سیسکو برای نگرانی‌های شدیدتر مورد استفاده قرار می‌گیرد. توصیه‌های امنیتی و پاسخ‌های آن‌ها در

[۷] Cisco Product Security Incident Response Team

http://www.cisco.com/go/psirt موجود است. علاوه بر این، توصیه‌های امنیتی و پاسخ‌ها اغلب با بولتن‌های کاربردی کاهش آسیب‌پذیری سیسکو AMB[^] آمده است که جزئیات و پیکربندی‌های خاصی را برای راه حل‌های کاهش آسیب‌پذیری‌ها بیان کرده‌اند. لیست گسترده‌ای از پرسش و پاسخ‌های امنیتی Cisco AMB و Cisco PSIRT در پورتال امنیت سیسکو موجود است.

https://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

برای اطلاعات بیشتر در مورد خط مشی‌های امنیتی و آسیب‌پذیری سیسکو و همچنین اطلاع از تهدیدات جهت ارزیابی ریسک می‌توان به آدرس زیر مراجعه کرد.

https://www.cisco.com/web/about/security/intelligence/vulnerability-risk-triage.html

[^] Applied Mitigation Bulletins

۲ بررسی NX-OS

سوئیچ‌های Nexsus سیسکو به صورت اختصاصی جهت استفاده در مراکز داده در مقیاس و حجم ترافیک بالا و انتقال ترافیک در مرکز داده تا حجم ۱۷ ترابایت معرفی گردیده است. این کلاس از تجهیزات برای حداکثر قابلیت مقیاس‌پذیری و دسترسی‌پذیری بالا طراحی شده‌است. برخی از مزایای متعدد Cisco NX-OS عبارتند از:

- سیستم‌عامل یکپارچه مرکز داده
- انعطاف‌پذیری و مقیاس‌پذیری
- مبتنی بر مؤلفه یا پیمانه‌ای‌بودن
- قابلیت استفاده از مجازی‌سازی
- امنیت جامع، قابلیت دسترسی، قابلیت اطمینان و ویژگی‌های مدیریتی
- مسیریابی مبتنی بر IPv4 و IPv6

۲-۱ ویژگی‌های کلیدی و مزایای NX-OS

۲-۱-۱ VDC[۹]

این امکان در Nexus7000 اجازه می‌دهد که یک سوئیچ فیزیکی به چندین سوئیچ کاملاً مستقل منطقی تقسیم شود و واحد کنترل نیز به چند قسمت تقسیم شود، و بنابراین هر سوئیچ منطقی را مستقل ساخته تا مطمئن شود که هیچگونه وابستگی به یکدیگر ندارند. این قابلیت به منظور استقلال نگهداری سیستم‌ها استفاده می شود، به عنوان مثال بخش امنیت فقط به DMZ VDC دسترسی داشته باشد. VPCها هیچگونه ارتباطی با هم ندارند مگر این که ارتباط فیزیکی پورت‌های آن‌ها برقرار شود.

[۹] Virtual device contexts

سوئیچ‌های سیسکو سری Nexus 7000 را می‌توان بر اساس نیاز مشتری به دستگاه‌های مجاز تقسیم کرد. VDCها مزایای متعددی از قبیل جداسازی خطا، سطح مدیریت، جداسازی ترافیک داده‌ها و افزایش امنیت را ارائه می‌دهند.

۲-۱-۲ VPC[۱۰]

کاربرد اصلی این مورد در Nexus 7000 نیز استفاده از امکان تجمیع لینک در چند سوئیچ فیزیکی مختلف است ولی آن را به صورت متفاوتی انجام می‌دهد. تفاوت اصلی در این است که در واحد کنترل، VSSها به صورت واحد منطقی در نظر گرفته می‌شوند ولی در VPC این‌گونه نیست. بنابراین هر دو سوئیچ می‌توانند به صورت کاملاً مستقل عمل نمایند و به همین علت نیز EtherChannelهای ساخته شده بین چند سوئیچ قابلیت لایه سه ندارند و نیاز به استفاده از پروتکل‌هایی نظیر HSRP وجود دارد. سرویس‌دهنده را فعال یا سوئیچ می‌کند تا از یک EtherChannel در دو سوئیچ جریان بالا بدون یک پورت مسدود شده STP استفاده کند، تا امکان استفاده از تمام پهنای باند بالا را داشته باشد.

۲-۱-۲-۱ عملکرد مداوم سیستم

تعمیر و نگهداری، ارتقا و صدور نرم‌افزار می‌توانند بدون وقفه‌های سرویس به علت ماهیت پیمانه‌ای NX-OS و ویژگی‌هایی مانند ارتقای نرم‌افزار درون سرویس (ISSU) و قابلیت فرآیند برای راه‌اندازی مجدد، به صورت پویا انجام شوند.

۲-۱-۲-۲ امنیت

سیسکو NX-OS دارای ویژگی محرمانه بودن و یکپارچگی داده‌ها است، پشتیبانی از رمزگذاری استاندارد IEEE 802.1 AES با رمزنگاری پیشرفته ۱۲۸ بیتی (AES) امکان‌پذیر است. به علاوه CTS، به عنوان مثال، بسیاری از ویژگی‌های امنیتی اضافی مانند ACL[۱۱] و امنیت پورت‌ها را دارد.

---

[۱۰] Virtual Port-Channel

[۱۱] Access control list

۲-۱-۲-۳ خدمات پایه

مجوز پیش‌فرض که با NX-OS حمل می‌شـــود، پروتکل‌های لایه‌ی ۲ از قبیل Spanning Tree، شـــبکه‌های مجازی VLAN، VLANهای خصوصی و UDLD[۱۲] را شامل می‌شود.

۲-۱-۲-٤ بسته خدمات سازمانی

پروتکل‌های لایه۳ مانند OSPF ، BGP، ISIS[۱۳]، EIGRP، PBR[۱٤]، PIM[۱٥]، و GRE[۱٦].

۲-۱-۲-٥ بسته خدمات پیشرفته

VDC، CTS[۱۷] و OTV[۱۸] را ارائه می‌دهد.

۲-۱-۲-٦ مجوز انتقال خدمات

OTV و پروتکل MPLS (در صورت وجود) را ارائه می‌دهد. مثال زیر به سادگی نصب فایل لایسنس NX-OS را نشان می‌دهد.

```
! Once a license file is obtained from Cisco.com and copied to flash, it can be in-
stalled for the chassis.
! Displaying the host-id for License File Creation on Cisco.com:
congo# show license host-id
License hostid: VDH=TBM14404807
! Installing a License File:
congo# install license bootflash:license_file.lic
Installing license ..done
congo#
```

[۱۲] Unidirectional Link Detection

[۱۳] Intermediate System-to-Intermediate System

[۱٤] Policy-Based Routing

[۱٥] Protocol Independent Multicast

[۱٦] Generic Routing Encapsulation

[۱۷] Cisco TrustSec

[۱۸] Overlay Transport Virtualization

توجه داشته باشید که NX-OS برای تست خصوصیات یک دوره‌ی ۱۲۰ روزه را ارائه می‌دهد. در اینجا چگونگی فعال کردن یک دوره گارانتی ۱۲۰ روزه را داریم:

```
congo(config)# license grace-period
```

این ویژگی پس از ۱۲۰ روز گارانتی منقضی می‌شود. مجوز گارانتی فقط برای مدیر VDC، VDC1 فعال است.

۲-۲ سیستم‌عامل‌های پشتیبانی شده NX-OS

سیستم‌عامل NX-OS، که برای قابلیت مقیاس‌پذیری بالا و دسترسی به برنامه‌های کاربردی طراحی شده است، از انواع مختلف پلت‌فرم‌ها، از جمله موارد زیر پشتیبانی می‌کند:

Nexus 7000

Nexus 500

Nexus 2000

Nexus 1000V

Cisco MDS 9000

Cisco Unified Computing System (UCS)

Nexus 4000

۲-۳ NX-OS و مقایسه آن با IOS

اگر شما با واسط خط فرمان (CLI) سیسکو IOS آشنا هستید، CLI برای NX-OS مشابه سیسکو IOS است. اما تفاوت‌های کلیدی وجود دارد که قبل از کار با NX-OS باید بررسی شوند:

- هنگامی که شما برای اولین بار وارد NX-OS می‌شوید، به طور مستقیم به حالت EXEC می روید.

- NX-OS دارای یک ابزار راه‌اندازی است که کاربر را قادر می‌سازد تا پیش‌فرض‌های سیستم را مشخص کند، پیکربندی اولیه را انجام دهد و از یک خط مشی امنیتی کنترل از راه دور از پیش تعیین شده (CoPP)[۱۹] استفاده کند.
- NX-OS از یک ویژگی مبتنی بر مدل لایسنس استفاده می‌کند.
- مهلت دوره‌ای ۱۲۰ روزه لایسنس برای تست، پشتیبانی می‌شود اما بعد از تاریخ انقضا، خصوصیات به طور خودکار از تنظیمات حذف می‌شوند.
- NX-OS دارای توانایی فعال و غیرفعال کردن ویژگی‌هایی مانند OSPF، BGP و غیره از طریق فرمان پیکربندی است. دستورات پیکربندی و تأیید تا زمانی که ویژگی خاصی را فعال کنید، در دسترس نیستند.
- NX-OS از VDC پشتیبانی می‌کند که یک دستگاه فیزیکی را به دستگاه‌های منطقی تقسیم می کند. هنگامی که برای اولین بار وارد سیستم شوید، به صورت پیش‌فرض در VDC قرار دارید.
- SSHv2[۲۰] به صورت پیش‌فرض فعال است. (Telnet [۲۱] به صورت پیش‌فرض غیرفعال است).
- کاربری که به سیستم وارد می شود به عنوان مدیر از پیش تعریف شده است؛ یک کلمه عبور باید زمانی مشخص شود که سیستم برای اولین بار روشن می شود. با NX-OS، شما باید یک نام کاربری و کلمه عبور را وارد کنید؛ شما نمی‌توانید نام کاربری و کلمه ورود را غیرفعال کنید.
- NX-OS از یک تصویر کیک‌استارتر[۲۲] و یک تصویر سیستم استفاده می‌کند. هر دو تصویر در فایل پیکربندی به عنوان متغیرهای بوت کیک استارتر و سیستم شناسایی می‌شوند.

[۱۹] Control Plane Policing

[۲۰] Secure Shell version 2

[۲۱] یک پروتکل تحت شبکه است که در اینترنت و شبکه‌های محلی استفاده می‌شود.

[۲۲] Kickstarter: شرکتی آمریکایی و عام‌المنفعه برای کمک به پروژه‌های نوآورانه در زندگی بشر است که از استارت‌آپ‌هایی با ایده‌های نوین و خلاقانه استقبال می‌کند. ایده‌های جدید در همه زمینه‌ها از فناوری گرفته تا آشپزی در وب سایت این شرکت برای جذب سرمایه عمومی تحت پوشش قرار می‌گیرد. این وب‌سایت در اصل برای طرح و ایده‌های جدید، سرمایه لازم را برای تولید و انبوه‌سازی فراهم می‌کند.

- NX-OS دستور نوشتن را حذف کرد؛ استفاده از پیکربندی راه‌اندازی کپی در حال اجرا، و همچنین دستور syntax وجود دارد.

۲-٤ استفاده از احراز هویت، مجوز دسترسی و حساب کاربری

چارچوب احراز هویت، مجوز دسترسی و حساب کاربری[۲۳] (AAA) برای تأمین تجهیزات شبکه بسیار مهم است. چارچوب AAA تأییدیه جلسات مدیریت را ارائه می‌دهد، توانایی محدود کردن کاربران برای دستورات توسط مدیر و گزینه ورود به سیستم مشخص شده است.

۲-۵ جمع‌آوری و پایش فایل ثبت وقایع مرکزی

برای درک رخدادهای موجود، رخدادهای در حال ظهور و رخدادهای گذشته مربوط به حوادث امنیتی، سازمان باید یک استراتژی واحد داشته باشد. این استراتژی باید از اطلاعات ورودی سیستم از همه دستگاه‌های شبکه و از قابلیت همبستگی پیشگیرانه و قابل تنظیم استفاده کند.

پس از انجام مدیریت متمرکز، یک سازمان باید رویکرد ساختاری را برای وارد کردن تجزیه و تحلیل و ردیابی حوادث ایجاد کند. با توجه به نیازهای سازمان، این رویکرد می‌تواند از یک بررسی ساده و دقیق داده‌های ورودی به یک قانون پیشرفته و تجزیه و تحلیل مبتنی بر نقش چند عامل با استفاده از داده‌های مرتبط استفاده کند.

۲-٦ استفاده از پروتکل‌های امن در زمان ممکن

بسیاری از پروتکل‌ها برای حمل اطلاعات حساس مدیریت شبکه استفاده می‌شوند. شما باید هر زمان که ممکن است از پروتکل‌های امن استفاده کنید. به عنوان مثال، به جای Telnet از SSH استفاده کنید، بنابراین هر دو اطلاعات احراز هویت و اطلاعات مدیریت رمزگذاری می‌شوند. علاوه بر این، هنگام استفاده از داده‌های پیکربندی شده در میان دستگاه‌ها در یک محیط شبکه، باید از پروتکل‌های انتقال فایل استفاده کنید. به عنوان

[۲۳] Authentication, Authorization, and Accounting

مثال، از پروتکل SCP [۲۴] TFTP [۲۵] یا FTP[۲۶] استفاده کنید. از بین این پروتکل‌ها استفاده از پروتکل‌های امن تر توصیه می‌گردد.

۷-۲ افزایش ترافیک با NetFlow

NetFlow مهندسین و مدیران را قادر می‌سازد تا بر جریان‌های ترافیکی در سراسر شبکه نظارت داشته باشند و در اصل برای صدور اطلاعات ترافیکی به برنامه‌های مدیریت شبکه در نظر گرفته شده است. NetFlow همچنین می‌تواند برای نشان دادن جریان اطلاعات (یعنی رابط‌های منبع و مقصد، آدرس‌های IP، و پورت‌ها) در یک مسیریاب مورد استفاده قرار گیرد. این قابلیت به شما اجازه می‌دهد تا ترافیک در حال عبور از شبکه را در زمان واقعی یا با گرفتن اطلاعات برای مرجع ببینید. صرف نظر از اینکه آیا اطلاعات جریان به یک جمع کننده از راه دور فرستاده می‌شوند یا به صورت زنده مشاهده می‌شوند، باید دستگاه‌های شبکه را برای NetFlow پیکربندی کنید تا در صورت نیاز بتوانند در ظرفیت‌های مختلف (از جمله سناریوهای فعال و غیرفعال) استفاده شوند.

[۲۴] Secure Copy Protocol

[۲۵] Trivial File Transfer Protocol

[۲۶] File Transfer Protocol

۳ انجام پیکربندی مدیریتی

مدیریت پیکربندی فرآیندی است که با آن تغییرات پیکربندی بررسی، تأیید، و پیاده‌سازی می‌شوند. در بستر پیکربندی دستگاه Cisco NX-OS، دو جنبه اضافی مدیریت پیکربندی حیاتی هستند که از جمله آن‌ها می توان به آرشیو و امنیت پیکربندی اشاره نمود.

مهندسان و مدیران می‌توانند از آرشیو پیکربندی استفاده کنند تا تغییراتی که با دستگاه‌های شبکه ایجاد شده‌اند را بازگردانند. در زمینه امنیت، آرشیو پیکربندی همچنین می‌تواند برای تعیین اینکه چه تغییرات امنیتی انجام شده است مورد استفاده قرار گیرد، و هنگامی‌که این تغییرات در ارتباط با داده ورودی AAA رخ داد، این اطلاعات می‌تواند در ممیزی امنیت دستگاه‌های شبکه کمک کند.

پیکربندی دستگاه سیسکو NX-OS حاوی اطلاعات حساس بسیاری از جمله نام کاربری، گذرواژه و محتویات ACLها است. مخزن مورد استفاده برای بایگانی دستگاه NX-OS سیسکو باید امن باشد. دسترسی ناامن به این اطلاعات می‌تواند امنیت کل شبکه را تضعیف کند.

۳-۱ توصیه‌هایی برای ایجاد کلمات عبور قوی

هرگز کلمه‌های عبور را روی کاغذ یا سرویس‌های عمومی برخط نگذارید. کلمه‌های عبوری ایجاد کنید که به راحتی به یاد داشته باشید و هیچ‌کس نتواند به راحتی آن را حدس بزند. یک راه برای انجام این کار این است که یک کلمه عبور ایجاد کنید که بر اساس یک عبارت باشد. به عنوان مثال، عبارت می‌تواند "راهی برای یادآوری باشد" و کلمه عبور می‌تواند "TmB1w2R!" یا "Tmb1W> r ~" و یا برخی از عبارات دیگر باشد.

توجه: از مثال‌های ذکر شده در مستندات، به عنوان کلمه عبور استفاده نکنید.

۳-۱-۱ خصوصیات یک کلمه عبور قوی

کلمه عبور قوی دارای ویژگی‌های زیر است:

- حاوی هر دو نوع حروف بزرگ و کوچک (به عنوان مثال، a-z، A-Z) است.
- حاوی اعداد و نشانه و همچنین حروف (به عنوان مثال، ۰-۹،! @ # $٪ و :[] {} ` \ = ~ | + _ () *؛ '<>، /) است.
- حداقل هشت تا دوازده کاراکتر الفبایی عددی داشته باشید.
- یک کلمه به هیچ زبانی نیست، و عامیانه، گفتاری یا اصطلاح نیست.

- براساس اطلاعات شخصی مانند نام اعضای خانواده، و یا بر اساس اطلاعات موجود نیست.

۳-۱-۲ خصوصیات کلمه‌ی عبور ضعیف

کلمه‌ی عبور ضعیف دارای ویژگی‌های زیر است:

- دارای کمتر از هشت کاراکتر است.
- یک کلمه در یک فرهنگ لغت (انگلیسی یا خارجی) پیدا شده است.
- اصطلاح دیگری که به راحتی حدس زده یا یافت می‌شود، مانند: نام خانوادگی، حیوان خانگی، دوست، همکار، و یا شخصیت فانتزی.
- یک اصطلاح محاسباتی یا نام، مانند یک فرمان، سایت، شرکت، مدل یا برنامه.
- تاریخ تولد یا انواع دیگر اطلاعات شخصی، مانند یک آدرس یا شماره تلفن.
- یک الگوی ساده یا الگوی شماره، مانند aaabbb، qwerty، zyxwvuts یا ۱۲۳۳۲۱.
- هرکدام از موارد فوق، وارونه شوند.
- هر یک از موارد فوق، قبل یا بعد از آن یک رقم قرار گیرد، مانند secret1 یا 1secret.

۳-۱-۳ مبانی امنیت کلمه‌ی عبور

هرگز کلمه‌ی عبور خود را نشان ندهید.

علاوه بر این شما باید:

- هرگز در مورد کلمه عبور در مقابل دیگران صحبت نکنید.
- هرگز به قالب یک کلمه عبور اشاره نکنید (مانند نام خانوادگی من).
- هرگز کلمه عبور را با اعضای خانواده به اشتراک نگذارید.
- هرگز از نمادهای خارج از مجموعه کاراکتر استاندارد اسکی استفاده نکنید. بعضی از نمادها، مانند نماد پوند استرلینگ (£)، باعث به وجود آمدن مشکلات ورود به سیستم در برخی از سیستم‌ها می‌شوند.

۳-۲ امنیت واحد مدیریتی

واحد مدیریت شامل عملکردهایی برای دسترسی به اهداف مدیریتی شبکه است. این اهداف عبارتند از جلسات مدیریت تعاملی با استفاده از SSH و همچنین جمع‌آوری آمارها با ابزارها و پروتکل‌هایی مانند SNMP یا NetFlow، هنگام بررسی امنیت یک دستگاه شبکه، باید اطمینان حاصل کنید که واحد کنترل محافظت شده است. اگر یک حادثه امنیتی باعث تخریب وظایف سیستم مدیریتی شود، بازیابی یا تثبیت شبکه به یک چالش تبدیل خواهد شد.

بخش‌های زیر جزئیات خصـــوصـــیات امنیتی و پیکربندی‌های موجود در NX-OS را برای کمک به تقویت سیستم مدیریتی مشخص می‌کند.

۳-۲-۱ مقاوم‌سازی کلی واحد مدیریت

واحد مدیریت برای دسترسی، پیکربندی و مدیریت دستگاه، علاوه بر نظارت از عملکرد دستگاه و شبکه‌ای که در آن مستقر است، استفاده می‌کند. واحد مدیریت برای پشتیبانی از عملیات لیست شده در اینجا، ترافیک را دریافت و ارسال می‌کند. هر دو واحد مدیریت و کنترل دستگاه باید امن باشند زیرا عملکرد این واحدها به طور مستقیم بر عملکرد کلی دستگاه تأثیر می‌گذارد. پروتکل‌های زیر توسط سطح مدیریت استفاده می‌شود:

- SNMP
- Telnet (اختیاری)
- SSH
- FTP
- TFTP
- SCP
- TACACS+[۲۷]
- RADIUS[۲۸]
- NetFlow

[۲۷] Terminal Access Controller Access Control System

[۲۸] Remote Authentication Dial-In User Service

- NTP[۲۹]
- Syslog[۳۰]

باید برای کمک به اطمینان پیدا کردن از بقای واحدهای مدیریت و کنترل در حوادث امنیتی، اقداماتی صورت گیرد. اگر یکی از این واحدها با موفقیت مورد سوء استفاده قرار گیرد، همه واحدها می‌توانند به خطر بیفتند.

۳-۲-۲ مدیریت گذرواژه‌ها

کلمه‌های عبور یک سازوکار اولیه برای کنترل دسترسی به منابع و دستگاه‌ها هستند. حفاظت از کلمه عبور با تعریف یک کلمه عبور یا محرمانگی که برای تأیید درخواست‌ها مورد استفاده قرار می‌گیرد، کامل می‌شود. هنگامی‌که یک درخواست برای دسترسی به یک منبع یا دستگاه دریافت می‌شود، برای تأیید، درخواست به چالش کشیده می‌شود (معمولاً به صورت درخواست یک کلمه عبور و نام کاربری). پس از دسترسی بر اساس نتیجه تأیید اعتبار، می‌تواند قبول، رد یا محدود شود. به عنوان یک روش بهتر امنیتی، کلمه عبور باید با یک سرویس‌دهنده تایید TACACS+ یا RADIUS مدیریت شود. با این حال، توجه داشته باشید که یک نام کاربری و کلمه عبور به صورت محلی پیکربندی شده هنوز در صورت شکست برای دسترسی مجاز یک سرویس TACACS+ یا RADIUS ضروری است. علاوه بر این، یک دستگاه ممکن است اطلاعات کلمه عبور دیگری مانند کلید NTP، رشته ارتباطی SNMP یا کلید پروتکل مسیریابی موجود در پیکربندی آن داشته باشد.

د ستور enable secret در نرم‌افزار IOS سیسکو برای تنظیم کلمه عبور ا ست که د ستر سی خاص مدیریتی برای سیستم نرم‌افزار IOS سیسکو را در سیسکو NX-OS فراهم می‌کند. هیچ مفهومی از تنظیم فعال بودن یا فعال کردن کلمه عبور وجود ندارد. امتیازات توسط RBAC[۳۱] مدیریت می شود. عملکرد معادل با فعال کردن حالت دسترسی در نرم‌افزار IOS دستگاه سیسکو به یک حساب کاربری با مدیر شبکه اختصاص دارد.

علاوه بر این، بر خلاف نرم‌افزار سیسکو IOS، سیسکو NX-OS به صورت محلی یک اعتبار مشترک متقابل کاربر را به عنوان یک آیتم کلمه عبور شخص در پیکربندی فعال نمی‌کند. هر حساب کاربر گذرواژه خود را

[۲۹] Network Time Protocol

[۳۰] standard for message logging

[۳۱] Role-based access control

حفظ می‌کند (ذخیره شده به صورت محلی یا از طریق AAA)، و سطوح مجوز توسط نقش اختصاص داده شده به یک حساب کاربری داده، دیکته شده است. بنابراین شما باید از نقش‌های مدیر شبکه یا vdc-admin نسبت به تمام کلمه‌های عبور مورد استفاده‌ی تمام حساب‌های دارای امتیاز دسترسی محافظت کنید. اگر مدیریت کلمه عبور با استفاده از خدمات AAA متمرکز شود، این کار بسیار ساده شده است.

به صورت پیش‌فرض، NX-OS سیسکو از تمام گذرواژه‌های مورد استفاده در پیکربندی سیستم با استفاده از درهم‌سازی غیرقابل برگشت MD5 محافظت می‌کند و گزینه‌ای برای تغییر این عمل وجود ندارد.

۳-۲-۳ تأکید بر انتخاب کلمه عبور قوی

سیسکو NX-OS دارای قابلیتی است که به صورت اختیاری امکان بررسی اعتبار کلمه عبور را در هنگام ورود یا تنظیم کلمه عبور فراهم می‌کند. این ویژگی به طور پیش‌فرض فعال شده و از انتخاب یک کلمه‌عبور ضعیف جلوگیری می‌کند که نیاز به کلمه عبوری مطابق با معیارهای زیر است:

- حداقل اندازه آن هشت حرف است.
- شامل چندین کاراکتر متوالی (abcde، lmnopq و غیره) نیست.
- شامل کلمات فرهنگ لغت (دیکشنری انگلیسی) نیست.
- شامل کاراکترهای تکراری زیاد (aaabbb، ttttyyyy، و غیره) نیست.
- نام‌های معمول (جان، ماری، جو، سیسکو و غیره) نیست.
- شامل حروف بزرگ و کوچک است.
- شامل اعداد است.

اگر قدرت گذرواژه بررسی شود، پس از آنکه گذرواژه قوی فعال شد، سیستم هرگز کلمه عبور موجود را تأیید نمی‌کند. اگر چه توصیه نمی‌شود، اما بررسی کلمه عبور را می‌توان با استفاده از دستور nopassword strength-checking و یا اسکریپت راه انداز سیستم غیرفعال کرد.

۳-۲-٤ غیرفعال کردن سرویس‌های بدون استفاده

به عنوان یک روش بهتر است برای امنیت بیشتر، هر گونه خدمات و سرویس‌های غیرضروری را غیرفعال کنید. سیسکو NX-OS هیچ یک از پروتکل‌های TCP[۳۲] یا UDP[۳۳] را که به صورت پیش‌فرض در نرم‌افزار سیسکو IOS یا سایر سیستم‌عامل‌های شبکه یافت نمی‌شود را اجرا نمی‌کند. در نتیجه، این سرویس‌ها نیازمند غیرفعال کردن صریح نیستند. به صورت پیش‌فرض سیسکو NX-OS طوری طراحی شده است که بدون تنظیم واضح و شفاف، سرویس یا پروتکل‌های دسترسی از راه دور را اجرا نکند. SSH، SNMP و NTP سرویس‌های ضروری برای اجرا و مدیریت یک شبکه هستند. این خدمات به صورت پیش‌فرض فعال هستند، و در صورت نیاز می‌توانند به صورت جداگانه غیرفعال شوند. در طول راه‌اندازی اولیه، سیسکو NX-OS گزینه‌ای برای فعال سازی سرویس Telnet را ارائه می‌دهد. توجه داشته باشید که این سرویس در زمان راه‌اندازی مجدد بارگیری نمی‌شود. اگر این سرویس در هنگام اجرای اسکریپت تنظیم نشده باشد، می‌توان آنها را بعداً در صورت نیاز اضافه کرد. به دلایل امنیتی، توصیه سیسکو استفاده از SSH به جای Telnet است.

CDP[۳٤] یک پروتکل شبکه است که برای شناسایی سایر دستگاه‌های همسایه‌ای که CDP آن‌ها فعال است و برای نقشه توپولوژی یک شبکه استفاده می‌شود. CDP می‌تواند توسط سیستم‌های مدیریت شبکه یا در عیب یابی استفاده شوند. CDP به صورت پیش‌فرض در NX-OS سیسکو فعال است. CDP باید در تمام واسط هایی که به شبکه‌های نامشخص متصل هستند غیرفعال شود. این غیرفعال سازی با دستور واسط no cdp enable به طور کامل انجام می‌شود. توجه داشته باشید که CDP می‌تواند توسط کاربران مخرب یا شناسایی و نقشه‌برداری شبکه مورد سوءاستفاده قرار گیرد.

پروتکل LLDP[۳۵] یک پروتکل IEEE است که در استاندارد IEEE 802.1AB تعریف شده است. LLDP شبیه پروتکل CDP است، این پروتکل سازگاری بین دستگاه‌هایی که توسط پروتکل CDP پشتیبانی نمی‌شود را امکان پذیر می‌سازد. به صورت پیش‌فرض، LLDP در NX-OS سیسکو فعال نیست. برای فعال کردن آن، مجموعه ویژگی باید با استفاده از دستور پیکربندی سراسری feature lldp فعال شود. هنگامی‌که LLDP فعال

---

[۳۲] Transmission Control Protocol

[۳۳] User Datagram Protocol

[۳٤] Cisco Discovery Protocol

[۳۵] Link Layer Discovery Protocol

می‌شود، باید به همان شیوه‌ی پروتکل CDP رفتار کرده و روی همه‌ی رابط‌های غیرقابل‌اعتماد متصل شده به شبکه غیرفعال شود. برای کامل کردن آن، دستورهای پیکربندی واسط no lldp transmit و no lldp اجرا می شوند. دستور پیکربندی no feature lldp برای غیرفعال کردن LLDP سراسری اجرا می‌شود. مانند پروتکل CDP، پروتکل LLDP نیز می‌تواند توسط کاربران مخرب برای شناسایی و نقشه‌برداری شبکه مورد سوءاستفاده قرار گیرد.

۳-۲-۵ تنظیم مقدار EXEC Timeout

برای تنظیم بازه‌ی زمانی که فرمان EXEC منتظر ورودی‌های کاربر قبل از پایان دادن به یک جلسه است، دستور پیکربندی *exec-time* را اجرا کنید. دستور *exec-timeout* برای خروج از جلسات باید بر روی یک vty[۳۶] یا خط ترمینال فیزیکی tty[۳۷] که بیکار (غیرفعال) بماند استفاده شود. به صورت پیش‌فرض در NX-OS سیسکو جلسات طوری تنظیم شده‌اند که پس از ۳۰ دقیقه عدم فعالیت قطع شوند.

```
!
line console
 exec-timeout <minutes>
line vty
 exec-timeout <minutes>
!
```

۳-۲-۶ استفاده از واسط‌های مدیریتی

واحد مدیریت یک دستگاه می‌تواند در یک باند یا خارج از محدوده‌ی باند به یک رابط مدیریت فیزیکی یا منطقی دسترسی پیدا کند. در حالت ایده‌آل، دسترسی مدیریت به داخل و خارج باند وجود دارد، بنابراین واحد مدیریت در صورت قطع شبکه می‌تواند به آن دسترسی پیدا کند.

یکی از رایج‌ترین واسطه‌هایی که برای دسترسی در باند به دستگاه استفاده می‌شود واسط کاربری Loopback است. واسط‌های Loopback منطقی هستند؛ بنابراین همیشه وجود دارند، در حالی که واسط‌های فیزیکی می

[۳۶] Virtual Teletype

[۳۷] teletype

توانند حالت را تغییر دهند، و این واسط را به طور بالقوه غیرقابل دسترس کنند. شما باید یک واسط Loopback به عنوان یک واسط مدیریت برای هر دستگاه اضافه کنید. این واسط باید به طور انحصاری برای واحد مدیریت استفاده شود. این روش به مدیر اجازه می‌دهد تا در سراسر شبکه برای واحد مدیریت سیاست‌هایی را اعمال کند. پس از اینکه واسط Loopback روی یک دستگاه پیکربندی شد، می‌توان از پروتکل‌های واحد مدیریت مانند SSH، SNMP و syslog برای ارسال و دریافت ترافیک و رخدادهای امنیتی استفاده کرد.

بستگی به پلت‌فرم سیسکو NX-OS، یک واسط مدیریت اختصاصی ممکن است در دسترس باشد، همان‌طور که در مورد سوئیچ‌های سری ۷۰۰۰ سیسکو وجود دارد. در این موارد، واسط مدیریت فیزیکی می‌تواند برای دسترسی به واسط‌های مدیریت منطقی دستگاه استفاده شود. به طور معمول، این واسط مدیریت فیزیکی برای دسترسی از طریق جداول VRF[۳۸] جدا شده‌است، با مدیریت پیش‌فرض VRF مرتبط با واسط مدیریت فیزیکی. با محدود کردن ترافیک مدیریت به VRF مدیریت با استفاده از ACLها، می‌توان یک توپولوژی بسیار مؤثر مدیریت جانبی یا بیرون از باند ایجاد کرد.

۳-۲-۷ محدود کردن دسترسی به شبکه با ACLهای زیربنایی

ACL های زیربنایی(iACLها) یکی از مهم‌ترین کنترل‌های امنیتی هستند که برای جلوگیری از ارتباط مستقیم غیرمجاز به دستگاه‌های شبکه تعبیه شده‌اند. iACLها از این ایده استفاده می‌کنند که تقریباً تمام ترافیک شبکه به سادگی از شبکه عبور می‌کنند و برای خود شبکه مقصد/هدف نیستند.

کلید برای یک iACL ساختمان آن است. iACLها بر اساس شرایط ارتباطات مجاز بین سیستم‌های معتبر یا شبکه‌هایی که نیاز به برقراری ارتباط با دستگاه‌های زیرساخت شبکه را دارند، مطابق با سیاست‌ها و پیکربندی‌های امنیتی مقرر ساخته شده‌اند.

این ارتباطات مورد نیاز معمولاً شامل ترافیک واحد مدیریت و کنترل می‌شود. نمونه‌های رایج این نوع اتصالات خارج BGP (eBGP)، SSH و SNMP هستند. پس از اینکه اتصالات مورد نیاز اجازه داده شدند، تمام ترافیک‌های دیگر به زیرساخت به طور صریح رد می‌شوند.

[۳۸] Virtual Route Forwarding

تمام ترافیک‌هایی که مقصد دستگاه‌های زیرساختی نیستند و از شبکه عبور می‌کند، صریحاً مجاز می‌باشند. حفاظت ارائه شده توسط iACLها مربوط به هر دو واحد مدیریت و کنترل است. پیاده‌سازی iACLها نیز با استفاده از آدرس مشخص برای دستگاه‌های زیرساخت شبکه ساده‌تر می‌شود. این مثال پیکربندی iACL یک ساختار را نشان می‌دهد که می‌تواند به عنوان یک نقطه شروع در هنگام شروع روند اجرای iACL استفاده شود.

```
!
ip access-list extended ACL-INFRASTRUCTURE-IN
! !--- Permit required connections for routing protocols and
! !--- network management
  permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
  permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
  permit tcp host <trusted-management-stations> any eq 22
  permit udp host <trusted-netmgmt-servers> any eq 161
! !--- Deny all other IP traffic to any network device !
  deny ip any <infrastructure-address-space> <mask>
! !--- Permit transit traffic !
  permit ip any any
!
```

برای یک حفاظت قوی از دستگاه‌های زیرساخت، باید iACLهای مستقر شده در جهت ورود به تمام واسط هایی که برای آن‌ها یک آدرس IP پیکربندی شده دارد به کار برده شود، از جمله رابط‌هایی که به سازمان‌های دیگر، بخش‌های د ستر سی از راه دور، بخش‌های کاربر و بخش هایی در مراکز داده، مت صل می شوند. توجه داشـــته باشـــید، زمانی که حمله از یک آدرس مبدأ مورد اعتماد آغاز می‌شـــود، یک iACL دیگر نمی‌تواند حفاظت کامل در برابر آسیب پذیری‌ها را انجام دهد.

استفاده از پروفایل‌های پورت سیسکو NX-OS می‌تواند به شدت نگهداری و تعمیرات ACLها را ساده کند.

۳-۲-۸ محدودسازی بسته‌های ICMP

پروتکل ICMP[۳۹] به عنوان یک پروتکل کنترل IP طراحی شده است. به این ترتیب، پیام‌هایی که به آن انتقال می‌یابند به طور کلی می‌توانند انشعابات گسترده‌ای برای TCP و IP داشته باشند. اتصال ICMP خارجی به ندرت برای عملکرد مناسب شبکه مورد نیاز است، اگرچه ابزارهای عیب‌یابی شبکه ping و traceroute از ICMP استفاده می‌کنند.

سیسکو NX-OS توابعی را به طور خاص برای محدودسازی پیام‌های ICMP با نام یا نوع و کد ارائه می‌دهد. این مثال ACL، با استفاده از ورودی‌های کنترل دسترسی مثال‌های قبلی، اجازه می‌دهد تا از ایستگاه‌های مدیریت قابل اعتماد و سرویس‌دهنده‌های سیستم مدیریت شبکه در حالی که تمام بسته‌های دیگر ICMP مسدود شده‌اند، ping بگیرد:

```
!
ip access-list extended ACL-INFRASTRUCTURE-IN
! !--- Permit ICMP Echo (ping) from trusted management stations and servers !
 permit icmp host <trusted-management-stations> any echo
 permit icmp host <trusted-netmgmt-servers> any echo
! !--- Deny all other IP traffic to any network device !
 deny ip any <infrastructure-address-space> <mask>
! !--- Permit transit traffic !
 permit ip any any
!
```

۳-۲-۹ محدودسازی IP Fragmentation

محدودسازی بسته‌های IP Fragmentation می‌تواند یک چالش برای زیرساخت‌ها و دستگاه‌های امنیتی مشابه باشد. این چالش به دلیل این که اطلاعات لایه‌ی ٤ که برای محدودسازی بسته‌های TCP و UDP مورد استفاده قرار می‌گیرد، تنها در بخش‌ها و تکه‌های اولیه، وجود دارد. سیسکو NX-OS از یک روش خاص برای بررسی بخش‌بندی غیراولیه در برابر ACLهای پیکربندی استفاده می‌کند. سیسکو NX-OS این بخش‌بندی‌های

[۳۹] Internet Control Message Protocol

غیراولیه را در برابر ACL ارزیابی می‌کند و تمام اطلاعات محدودسازی لایه ٤ را نادیده می‌گیرد. این روش باعث می‌شود که بخش‌بندی‌های غیراولیه منحصراً روی بخش لایه ۳ از پیکربندی هر ورودی کنترل دسترسی ارزیابی شود.

```
!
ip access-list extended ACL-FRAGMENT-EXAMPLE
permit tcp any host 192.168.1.1 eq 80
deny tcp any host 192.168.1.1 eq 22
!
```

با توجه به این ماهیت غیرواقعی دستکاری تکه‌ها، IP Fragmentها اغلب سهواً توسط ACLها مجوز می‌گیرند. علاوه بر این، تکه تکه نمودن اغلب برای فرار از تشخیص توسط سیستم‌های تشخیص نفوذ استفاده می‌شود. به همین علت IP Fragmentation ها اغلب در حملات استفاده می‌شود و بنابراین باید در بالای هر iACL پیکربندی شده به طور واضح فیلتر شوند. این مثال ACL شامل محدودسازی جامعی از IP Fragmentationها است. توابع در این مثال باید در ارتباط با توابع نمونه‌های قبلی استفاده شوند.

```
!
ip access-list extended ACL-INFRASTRUCTURE-IN
! !--- Deny IP fragments using protocol-specific ACEs to aid in
! !--- the classification of attack traffic !
  deny tcp any any fragments
  deny udp any any fragments
  deny icmp any any fragments
  deny ip any any fragments
! !--- Deny all other IP traffic to any network device !
  deny ip any <infrastructure-address-space> <mask>
! !--- Permit transit traffic !
  permit ip any any
!
```

۳-۲-۱۰ امنیت جلسات مدیریت تعاملی

جلسات مدیریت برای دستگاه‌ها به شما این امکان را می‌دهد که اطلاعات مربوط به دستگاه و عملیات آن را مشاهده و جمع‌آوری کنید. اگر این اطلاعات برای یک کاربر مخرب افشا شود، دستگاه می‌تواند هدف حمله

قرار گیرد، به خطر انداخته شود و فرماندهی حملات دیگر را انجام دهد. هر کسی که دارای دسترسی خاص به دستگاه باشد، قابلیت کنترل کامل اجرایی این دستگاه را دارد. جلسات مدیریتی برای جلوگیری از افشای اطلاعات و دسترسی غیرمجاز ضروری هستند.

۳-۲-۱۰-۱ رمزگذاری جلسات مدیریت

از آنجا که اطلاعات در یک جلسه مدیریت تعاملی می‌توانند افشا شوند، این ترافیک باید رمزگذاری شود تا کاربر مخرب نتواند به داده‌های منتقل‌شده دسترسی یابد. رمزگذاری ترافیک به ما این اجازه را می‌دهد تا یک اتصال امن از راه دور به دستگاه داشته باشیم. اگر ترافیک یک جلسه مدیریت در متن واضحی بر روی شبکه ارسال شود، مهاجم می‌تواند اطلاعات حساس در مورد دستگاه و شبکه را دریافت کند.

یک مدیر می‌تواند رمزنگاری را ایجاد کند و با استفاده از SSH دسترسی از راه دور مدیریت را برای یک دستگاه امن کند. سیسکو NX-OS تنها از نسخه SSH 2.0[۴۰] پشتیبانی می‌کند. توجه داشته باشید که نسخه‌های SSHv1 و v2 با آن سازگار نیستند. همان‌طور که نسخه NX-OS 5.1، SSH در حالت FIPS[۴۱] اجرا می‌شود.

سیسکو NX-OS از SCP و SFTP[۴۲] نیز پشتیبانی می‌کند، که به ما اجازه می‌دهد تا یک اتصال رمزگذاری شده و امن برای کپی پیکربندی دستگاه یا تصاویر نرم‌افزاری داشته باشیم. SCP به SSH متکی است. مثال زیر پیکربندی SSH را بر روی دستگاه NX-OS سیسکو فعال می‌کند:

```
!
ip domain-name example.com
!
feature ssh
ssh key rsa 2048
!
ssh login-attempts <1-10> (default is 3)
```

[۴۰] SSHv2

[۴۱] The Federal Information Processing Standard

[۴۲] Secure FTP

```
!
This configuration example enables SCP and SFTP services:
!
feature scp-server
feature sftp-server
!
```

۳-۲-۱۰-۲ امنیت پورت کنسول، پورت کمکی و پردازنده مدیریت ارتباطی

در دستگاه‌های NX-OS سیسکو، پورت‌های کنسول و کمکی AUX خطوط آسنکرون هستند که برای دسترسی محلی و راه دور به یک دستگاه می‌توانند استفاده شوند. لازم است بدانید که پورت‌های کنسول در دستگاه‌های NX-OS سیسکو دارای امتیاز خاصی هستند. به طور خاص، این امتیازات به مدیر اجازه می‌دهد تا روند بازیابی کلمات عبور را انجام دهد. یک مهاجم غیرمجاز برای انجام بازیابی کلمه‌ی عبور، نیازمند دسترسی به پورت کنسول و توانایی قطع برق دستگاه یا دلیلی برای خرابی دستگاه است.

لازم است هر روشی که برای دسترسی به پورت کنسول یک دستگاه استفاده می‌شود با سطح امنیتی معادل امنیت دسترسی خاصی که برای یک دستگاه اجرا می‌شود، محافظت شود. پیکربندی روش‌های احرازهویت AAA و سیاست‌های اعمال شده برای مکانیزم ورود به سیستم به طور خودکار به کنسول، پورت AUX و روش‌های دسترسی Vty اعمال می‌شود.

پورت AUX (به عنوان com1 نامیده می‌شود) هنگامی‌که در دسترس است نمی‌تواند صریحاً غیرفعال شود. بنابراین AAA باید برای امنیت پورت AUX نیز به درستی پیکربندی شود. علاوه بر این، به شدت توصیه می‌شود که برای محدود کردن دسترسی فیزیکی به درگاه AUX اقدامات امنیتی فیزیکی اعمال شود.

بعضی از سیستم‌عامل‌های NX-OS سیسکو یک پردازنده مدیریت اتصال CMP[۴۳] اختیاری برای دسترسی خارج از باند به کنسول را فراهم می‌کنند. توابع CMP به طور داخلی به عنوان یک دستگاه مستقل، بسیار شبیه به یک پورت ILO[۴۴] در یک سرویس‌دهنده یا یک ترمینال سرویس‌دهنده ساخته شده‌اند. CMP یک

[۴۳] connectivity management processor

[۴۴] integrated lights-out

سیستم مستقل (یک نسخه تقلیل یافته از سیسکو NX-OS) را بر روی یک پردازنده سیستم مستقل اجرا می کند.

احرازهویت CMP با روش AAA با احرازهویت پیکربندی شده بر ناظر سیستم اصلی گره خورده است. اگر سرویس‌دهنده‌های پیکربندی AAA را بتوان از طریق ناظر اصلی دریافت کرد، CMP با استفاده از سیاست‌ها و روش‌های پیکربندی شده AAA تصدیق می شود. اگر سرویس‌دهنده AAA در دسترس نباشد، CMP از احرازهویت محلی استفاده می‌کند، و در مقابل یک پایگاه داده کاربر که به طور محلی در CMP ذخیره شده است، بررسی می‌شود.

برای امنیت کافی CMP (اگر از آن استفاده می‌شود) AAA باید بر روی ناظر سیستم اصلی پیکربندی شود. و احرازهویت پایگاه داده محلی CMP باید با یک رمز عبور تک کاربره تنظیم شود.

CMP با استفاده از پروتکل SSH بر روی یک شبکه IP قابل دسترسی است. اگر قصد استفاده از CMP را نداشته باشیم، می‌توان به سادگی با اختصاص ندادن یک آدرس IP به آن و یا از بین بردن آدرس IP از واسط CMP، آن را غیرفعال کرد.

۳-۲-۱۰-۳ کنترل خطوط vty

جلسات مدیریت تعاملی در NX-OS سیسکو از یک tty مجازی (vty) استفاده می‌کنند. خط vty برای تمام اتصالات پشتیبانی شده از راه دور شبکه توسط دستگاه استفاده می‌شود، صرف نظر از پروتکل SSH، (SCP یا Telnet) برای اطمینان از دسترسی به یک دستگاه از طریق یک جلسه مدیریت محلی یا از راه دور، باید کنترل‌های مناسبی بر روی خطوط vty اجرا شوند.

دستگاه‌های NX-OS سیسکو دارای تعداد محدودی از خطوط vty هستند؛ تعداد خطوط پیکربندی در دسترس را می‌توان با استفاده از دستور show run vshd تعیین کرد. به صورت پیش‌فرض تا ۱۶ جلسه vty به طور همزمان مجاز هستند. هنگامی‌که تمام خطوط vty در حال استفاده هستند، جلسات مدیریت جدید ایجاد نمی‌شود، و شرایط DoS[۴۵] برای دسترسی به دستگاه ایجاد می‌شود.

[۴۵] denial-of-service

ساده‌ترین شکل کنترل دسترسی برای vty از یک دستگاه استفاده از احرازهویت در تمام خطوط بدون در نظر گرفتن محل دستگاه در شبکه است. کنترل دسترسی vty را می‌توان با استفاده از دستورات پیکربندی access-class، از قابلیت CoPP[٤٦] و یا اعمال لیست‌های دسترسی به واسط در دستگاه انجام داد. احراز هویت می‌تواند با استفاده از پایگاه داده کاربر محلی و یا از طریق استفاده از AAA، که روش توصیه شده برای دسترسی مجاز به یک دستگاه است، اجرا شود. فرمان exec-timeout باید برای خروج از جلسات بر روی هر vty که بیکار بماند استفاده شود.

خطوط vty در NX-OS سیسکو به طور خودکار قبول می‌کند که اتصالات از هر پروتکل انتقال پیکربندی شده استفاده کنند. برای اینکه یک پروتکل خاص (به عنوان مثال، عدم امنیت) را از دسترسی به جلسات vty غیرفعال کنید، باید به طور سراسری آن پروتکل خاص را غیرفعال کنید. برای مثال، برای جلوگیری از جلسه Telnet به خط vty، باید Telnet را به طور سراسری با استفاده از دستور no feature telnet غیرفعال کنید.

۳-۲-۱۱ نمایش بنرهای هشدار دهنده

در بعضی از حوزه‌های حقوقی، شما نمی‌توانید بر کاربران مخرب را تحت پیگرد قانونی قرار داده یا نظارت قانونی کنید مگر اینکه آنها مطلع شوند که مجاز به استفاده از این سیستم نیستند. یکی از راه‌های ارائه این اطلاع‌رسانی این است که این اطلاعات را در یک پیام بنر قرار دهید که با دستور bannerlogin، NX-OS سیسکو پیکربندی شده است.

الزامات اطلاع رسانی حقوقی پیچیده و متفاوت وابسته به وضعیت است و باید با مشاور حقوقی مطرح شود. حتی در حوزه‌های قضایی، نظرات قانونی می‌توانند متفاوت باشند. برای همکاری با وکیل، یک بنر می‌تواند برخی یا همه اطلاعات زیر را ارائه دهد:

- توجه داشته باشید که این سیستم فقط باید توسط پرسنل مجاز که مجوز ورود دارند استفاده شود.
- توجه داشته باشید که هرگونه استفاده غیرمجاز از سیستم غیرقانونی است و می‌تواند به مجازات‌های مدنی و کیفری منجر شود.

[٤٦] control-plane policing

- توجه داشته باشید که هر گونه استفاده از سیستم را می‌توان بدون اطلاع قبلی تحت نظر گرفت و در نتیجه سیاهه‌های مربوطه می‌تواند به عنوان مدرک در دادگاه استفاده شود.
- اخطارهای خاصی که به موجب قوانین محلی مورد نیاز است.

از دیدگاه امنیتی، بنر ورودی نباید هیچ اطلاعات خاصی در مورد نام مسیریاب، مدل، نرم‌افزار یا مالکیت داشته باشد. این اطلاعات می‌تواند توسط کاربران مخرب مورد سوءاستفاده قرار گیرد.

۳-۲-۱۲ استفاده از AAA

چارچوب AAA برای امنیت دسترسی متقابل به دستگاه‌های شبکه بسیار مهم است. چارچوب AAA یک محیط بسیار قابل تنظیم است که می‌تواند بسته به نیازهای شبکه طراحی شده باشد.

۳-۲-۱۲-۱ احراز هویت +TACACS

+TACACS یک پروتکل احرازهویت است که دستگاه‌های NX-OS سیسکو برای احرازهویت کاربران مدیریت در مقابل یک سرویس‌دهنده از راه دور AAA می‌توانند از آن استفاده کنند. این کاربران مدیریت می توانند از طریق SSH یا Telnet به دستگاه NX-OS سیسکو دسترسی پیدا کنند.

احرازهویت +TACACS و یا به طور کلی احرازهویت AAA، توانایی متمرکز کردن اطلاعات احرازهویت و سیاست‌های مجاز را برای ما فراهم می‌کند. همچنین برای بهبود قابلیت اطمینان حساب‌های کاربری متمرکز مؤثر از معاملات مرتبط با AAA استفاده می‌شود.

RADIUS[۴۷] پروتکلی است که در هدف با +TACACS مشابه است. هر چند RADIUS تنها کلمه عبوری که در سراسر شبکه ارسال شده است را رمزگذاری می‌کند. در مقابل، + TACACS تمامی اجزا ارتباطی و ترافیکی TCP از جمله نام کاربری و کلمه عبور را رمزگذاری می‌کند. به همین دلیل زمانی که +TACACS توسط سرویس‌دهنده AAA و دستگاه شبکه پشتیبانی می‌شود، +TACACS بیش از RADIUS ترجیح داده می‌شود. احرازهویت +TACACS را می‌توان با استفاده از یک پیکربندی مشابه این مثال در دستگاه NX-OS سیسکو فعال کرد.

[۴۷] Remote Authentication Dial-In User Service

```
!
! TACACS+ must be enabled in NX-OS
feature tacacs+
aaa authentication login default group tacacs+
!
tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

پیکربندی قبلی می‌تواند به عنوان نقطه شروع برای یک الگوی احرازهویت AAA سازمان خاص استفاده شود.

۳-۲-۱۲-۲ احرازهویت Fallback

دستگاه NX-OS سیسکو اگر تمام سرویس‌دهنده‌های AAA پیکربندی شده در دسترس نباشند، می‌تواند به روش‌های احرازهویت ثانوی تکیه کند. گزینه‌های پیکربندی عبارتند از استفاده از احرازهویت محلی یا بدون احرازهویت اگر تمام سرویس‌دهنده‌های +TACACS پیکربندی شده در دسترس نباشند. شما نباید از گزینه None استفاده کنید چون در صورتی که سرویس‌دهنده‌های AAA قابل دسترسی نباشند، هیچ احرازهویتی صورت نمی‌گیرد. Fallback به طور بالقوه اجازه می‌دهد برای از بین بردن احرازهویت در دستگاه‌های شبکه یک حمله DoS به سرویس‌دهنده‌های AAA صورت پذیرد. در عوض، احرازهویت Fallback باید هنگامی‌که سرویس‌دهنده‌های AAA قابل دسترس نیستند بر روی استفاده از پایگاه داده محلی تنظیم شوند. این روش به یک کاربر محلی تعریف شده اجازه می‌دهد تا یک یا چند مدیر شبکه ایجاد کند. اگر +TACACS به طور کامل در دسترس نبود، هر مدیر می‌تواند از نام کاربری و کلمه‌ی عبور محلی خود استفاده کند. اگرچه این اقدام در زمان قطع +TACACS مسئولیت‌پذیری مدیران شبکه را افزایش می‌دهد، اما می‌تواند هزینه‌های اداری را نیز افزایش دهد زیرا حساب‌های کاربری محلی باید در تمام دستگاه‌های شبکه حفظ شوند. برخی از این هزینه‌ها می‌توانند با استفاده از سازوکار توزیع پیکربندی+TACACS NX-OS سیسکو، که از پروتکل Cisco Fabric Services استفاده می‌کند، کاهش یابد.

مثال زیر پیکربندی بر روی مثال قبلی احرازهویت+TACACS ساخته شده است، از جمله احرازهویت Fallback برای کلمه‌ی عبور که بصورت محلی با دستور enable secret پیکربندی شده است:

```
!
username admin password <password> role network-admin
!
```

```
aaa authentication login default group tacacs+
aaa authentication login default fallback error local
!
```

۳-۲-۱۲-۳ دستور مجوز +TACACS

دستور مجوز با +TACACS و AAA سازوکاری را فراهم می‌کند که هر دستوری که توسط یک کاربر وارد شده باشد را رد یا قبول می‌کند. هنگامی که کاربر وارد EXEC یا دستورات پیکربندی شود، NX-OS سیسکو هر دستور را به سرویس‌دهنده AAA پیکربندی شده ارسال می‌کند. سپس سرویس‌دهنده AAA از سیاست‌های پیکربندی شده خود برای اعطا یا رد دستور به کاربر خاص استفاده می‌کند. این پیکربندی را می توان به مثال قبلی احرازهویت AAA اضافه کرد تا مجوز دستور را اجرا کند:

```
!
aaa authorization commands default group <server group> [local]
aaa authorization config-commands default group <server group> [local]
!
```

۳-۲-۱۲-٤ دستور حساب کاربری +TACACS

هنگام پیکربندی، دستور حساب کاربری AAA اطلاعاتی در مورد هر EXEC یا دستور پیکربندی شده، ارسال می‌کند که به سرویس‌دهنده‌های +TACACS پیکربندی شده وارد شده‌اند. اطلاعات ارسال شده به سرویس‌دهنده‌های +TACACS عبارتند از دستور اجرا شده، تاریخ اجرا و نام کاربری که کاربر دستور آن را وارد می‌کند. حساب کاربری دستور را با استفاده از RADIUS پشتیبانی نمی‌کند.

این مثال پیکربندی دستور حساب کاربری AAA را برای تمام دستورات وارد شده فعال می‌کند. این پیکربندی بر روی نمونه‌های قبلی که حاوی پیکربندی سرویس‌دهنده‌های TACACS است ایجاد می‌شود.

```
!
aaa accounting default group <server group>
!
```

۳-۲-۱۲-۵ سرویس‌دهنده‌های AAA اضافی

اگر سرویس‌دهنده‌های AAA که در محیط مورد استفاده قرار می‌گیرند از کار بیفتند و یا با خطا روبرو شوند، این روش کمک می‌کند تا اطمینان حاصل شود که اگر یک سرویس‌دهنده AAA در دسترس نباشد دسترسی مدیریت مانند دسترسی به SSH امکان پذیر است.

هنگام طراحی یا پیاده‌سازی راه حل یک سرویس‌دهنده AAA اضافی، این نکات را در ذهن داشته باشید:

- در دسترس بودن سرویس‌دهنده‌های AAA در حین خرابی‌های احتمالی شبکه
- قراردادن مکان سرویس‌دهنده‌های AAA به صورت جغرافیایی
- بار در سرویس‌دهنده‌های AAA شخصی در حالت ثابت و شرایط خرابی
- زمان تأخیر شبکه بین سرویس‌دهنده‌های دسترسی شبکه و سرویس‌دهنده‌های AAA
- هماهنگ‌سازی پایگاه‌داده‌های سرویس‌دهنده AAA

NX-OS سیسکو پیکربندی گروه‌های سرویس‌دهنده‌ها برای سرویس‌های AAA اضافی، هم RADIUS و هم +TACACS را پشتیبانی می‌کند. به شدت توصیه می‌شود که این امکان برای ارائه قابلیت اطمینان سرویس‌های AAA استفاده شود. در ادامه یک مثال از پیکربندی گروه سرویس‌دهنده +TACACS برای سرویس‌دهنده‌های AAA اضافی آمده است:

```
!
tacacs-server host <tacacs+ server1 IP>
tacacs-server host <tacacs+ server2 IP>
tacacs-server host <tacacs+ server3 IP>
! Global key for all TACACS+ servers (you can optionally define individual keys per server)
tacacs-server key <key>
!
aaa authentication group <group name>
  server <tacacs+ server1 IP>
  server <tacacs+ server2 IP>
  server <tacacs+ server3 IP>
!
```

۳-۲-۱۳ امنیت SNMP

این بخش چندین روش که برای امن‌سازی استفاده از SNMP در دستگاه‌های NX-OS سیسکو استفاده می‌شود را مورد بحث قرار می‌دهد. SNMP باید به درستی امن گردد تا از محرمانه بودن، یکپارچگی و دسترسی هم داده‌های شبکه و هم دستگاه‌های شبکه از طریق انتقال داده‌ها، محافظت شود. SNMP اطلاعات فراوانی را درباره سلامتی دستگاه‌های شبکه ارائه می‌دهد. این اطلاعات باید از کاربران مخربی که می‌خواهند از این اطلاعات برای حملات علیه شبکه استفاده کنند، محافظت شود.

۳-۲-۱۳-۱ SNMP Community String

Community Stringها کلمه‌های عبور هستند که برای یک دستگاه NX-OS سیسکو با محدود کردن دسترسی، تنها دسترسی به خواندن و نوشتن داده‌های SNMP در دستگاه اجرا می‌شود. این Community String ها ، همانند تمام کلمه‌های عبور، باید با دقت انتخاب شوند تا اطمینان حاصل شود که قوی هستند. String Communityها باید با فواصل منظم و مطابق با سیاست‌های امنیتی شبکه تغییر کنند. به عنوان مثال، رشته‌ها باید زمانی که یک مدیر شبکه تغییر نقش دهد یا شرکت را ترک کند، تغییر کنند. این خطوط پیکربندی یک Community String فقط خواندنی از READONLY و یک Community String خواندن و نوشتن از READWRITE را تنظیم می‌کند:

```
!
snmp-server community READONLY ro
snmp-server community READWRITE rw
!
```

توجه داشته باشید که مثال‌های ماقبل Community String انتخاب شده‌اند تا به طور واضح استفاده از این Stringها را توضیح دهند. با هر کلمه عبور دیگری که برای محیط‌ها تولید استفاده می‌شود، String Community باید با احتیاط انتخاب شوند و باید شامل مجموعه‌ای از علامت‌های حروف الفبا، عددی و غیر عددی باشند که به راحتی با استفاده از حملات فرهنگ لغت حدس زده یا به خطر انداخته نشوند.

۳-۲-۱۳-۲ SNMP Community Stringها با ACLها

علاوه بر Community Stringها، یک ACL باید اعمال شود که بیشتر دسترسی SNMP را به گروهی از منبع آدرس‌های IP محدود کند. این پیکربندی دسترسی فقط خواندنی SNMP را تا انتهای دستگاه‌های

میزبانی که در فضـای آدرس 192.168.100.0/24 قرار دارند، محدود می‌کند و دسـترسـی خواندن و نو شتن SNMP را تنها در دستگاه میزبان 192.168.100.1 محدود می‌کند.

توجه داشته باشید که دستگاه‌های مجاز توسط این ACLها برای دسترسی به اطلاعات SNMP نیاز به String مناسب Community درخواست شده دارند.

```
!
ip access-list allow_snmp_ro
permit ip 192.168.100.0/24 any
!
ip access-list allow_snmp_rw
permit ip host 192.168.100.1 any
!
snmp-server community READONLY use-acl allow_snmp_ro
snmp-server community readwrite use-acl allow_snmp_rw
!
```

۳-۲-۱۳-۳ iACLها

iACLها برای کمک به اطمینان از اینکه تنها میزبان نهایی با آدرس IPهای معتبر می‌تواند ترافیک SNMP را به دستگاه NX-OS سیسکو ارسال کند، مستقر می‌شوند. یک iACL باید شامل خط مشی باشد که بسته‌های SNMP غیرمجاز در پورت UDP ۱٦۱ را انکار کند.

۳-۲-۱۳-٤ SNMP نسخه ۳

SNMP نسـخه ۳ (SNMPv3) توسـط RFC3410، RFC3411، RFC3412، RFC3413، RFC3414 و RFC3415 و یک پروتکل مبتنی بر استانداردهای متقابل برای مدیریت شبکه تعریف شده است. SNMPv3 دسـترسـی امن به دسـتگاه‌ها را با احرازهویت و بسـته‌های رمزنگاری انتخابی بر روی شـبکه فراهم می‌کند. هنگام استفاده ازSNMP، SNMPv3 می‌تواند برای اضافه کردن یک لایه امنیتی دیگر استفاده شود. SNMPv3 شامل سه گزینه پیکربندی اولیه است:

- no auth: این حالت به هیچ احرازهویت و رمزگذاری بسته‌های SNMP نیاز ندارد.
- auth: این حالت به احرازهویت بسته SNMP بدون رمزگذاری نیاز دارد.
- priv: این حالت به احرازهویت و رمزگذاری (حریم خصوصی) هر بسته SNMP نیاز دارد.

یک engineID معتبر باید وجود داشته باشد تا از امنیت سازوکار احرازهویت SNMPv3 یا احرازهویت و رمزگذاری برای بسته‌های SNMP استفاده کند؛ به صورت پیش‌فرض، engineID به صورت محلی تولید می‌شود. engine ID را می‌توان با دستور show snmp engineID نمایش داد که در این مثال نشان داده شده است:

```
Nexus7000-Lab# show snmp engineID
Local SNMP engineID: [Hex] 8000000903001B54C24100
        [Dec] 128:000:000:009:003:000:027:084:194:065:000
```

توجه داشته باشید که اگر engineID تغییر کند، همه حساب‌های کاربری SNMP باید دوباره تنظیم شوند. به صورت پیش‌فرض SNMPv3 در NX-OS سیسکو فعال است و به صراحت نمی‌تواند غیرفعال شود.

برای دسترسی به یک دستگاه NX-OS سیسکو با استفاده از SNMPv3، یک کاربر یا مدیر باید یک حساب کاربری معتبر SNMP را داشته باشد. حساب‌های کاربری SNMP را می‌توان صریحاً ایجاد کرد و یا به طور خودکار توسط سیستم تولید می‌شود تا با حساب‌های معتبر تأییدشده از طریق احرازهویت محلی یا بر پایه‌ی AAA هماهنگ شوند.

شما می‌توانید به وضوح SNMP را پیکربندی کنید که مستلزم احرازهویت پیام و رمزنگاری برای درخواست‌های ورودی است. به صورت پیش‌فرض، طرف SNMP درNX-OS سیسکو پیام‌های SNMPv3 را بدون احرازهویت و رمزنگاری می‌پذیرد. توصیه می‌شود که احرازهویت و رمزگذاری برای پیام‌های SNMPv3 بایستی اجرا شود.

دستور پیکربندی عمومی زیر، رمزگذاری پیام SNMP را برای تمام کاربران اعمال می‌کند:

```
!
snmp-server globalEnforcePriv
!
```

این دستورصریحاً SNMPv3 را پیکربندی می‌کند. کاربر snmpv3 با یک رمز عبور احرازهویت MD5 authpassword و یک رمزعبور privessword از رمزگذاری AES-128:

```
!
snmp-server user snmpv3user auth sha authpassword priv aes-128 privpassword
!
```

۳-۲-۱٤ ثبت بهترین عملکردها

ثبت وقایع و رخداد به سیستم به شما این امکان را می‌دهد تا عملکرد دستگاه NX-OS سیسکو و شبکه‌ای که در آن مستقر شده است را مشاهده کنید. سیسکو NX-OS چند گزینه‌ی قابل تغییر برای ورود به سیستم را ارائه می‌دهد که می‌تواند به مدیریت شبکه و اهداف یک سازمان کمک کند.

بخش‌های زیر بعضی از بهترین شیوه‌های ورود به سیستم اصلی را ارائه می‌دهند که به مدیر کمک می‌کنند که با موفقیت از ورود به سیستم استفاده کند، در حالی که تأثیر ورود به یک دستگاه NX-OS سیسکو را کاهش می‌دهد.

۳-۲-۱٤-۱ ارسال فایل‌های ثبت وقایع به یک Central Location

شما باید اطلاعات ثبت وقایع و رخدادها به سیستم را به سرویس‌دهنده از راه دور syslog ارسال کنید. با انجام این کار، می‌توانید رخدادهای شبکه و امنیت را در دستگاه‌های شبکه به طور مؤثرتر یکپارچه و بررسی کنید. توجه داشته باشید که پیام‌های Syslog به طور غیرمستقیم توسط UDP و در متن آشکار انتقال می‌یابند. به همین علت، هر حفاظتی که یک شبکه به ترافیک مدیریت (به عنوان مثال، رمزگذاری و دسترسی خارج از باند) ارائه می‌دهد باید تعمیم داده شود تا شامل ترافیک syslog گردد.

این مثال یک دستگاه NX-OS سیسکو برای ارسال اطلاعات ورودی به سرویس‌دهنده از راه دور Syslog با استفاده از مثال مدیریت VRF را پیکربندی می‌کند.

```
!
logging server <ip-address|hostname> use-vrf management
!
```

۳-۲-۱٤-۲ تعیین سطح ورود به سیستم

هر جزء نرم‌افزار داخلی سیستم NX-OS سیسکو که قابلیت ثبت رخدادها به سیستم با استفاده از امکانات syslog را دارد، می‌تواند یکی از هشت شدت سطح که محدوده‌ی آن از سطح صفر یعنی اضطراری، تا سطح ۷ یعنی اشکال‌زدایی، است را تعیین کند. شدت سطح انتخاب شده، جزئیات و فراوانی پیام‌های تولید شده برای اجزاء آن را تعیین می‌کند. مگر اینکه به طور خاص مورد نیاز باشد، توصیه می‌شود که از ورود سیستم به سطح ۷ جلوگیری کنید. ورود به سیستم در سطح ۷ باعث افزایش بار CPU در دستگاه می‌شود که می‌تواند به بی‌ثباتی دستگاه و شبکه منجر شود.

مثال زیر پیکربندی پیام‌های ورودی که به سرویس‌دهنده‌های از راه دور Syslog (به سطوح شدت ٦ یعنی اطلاعاتی تا صفر یعنی اضطراری) ارسال می‌شوند را محدود می‌کند:

```
!
logging server <ip-address|hostname> 6 use-vrf management
!
```

۳-۲-۱٤-۳ جلسات کنسول یا نظارت فایل ثبت وقایع

با NX-OS سیسکو می‌توانید فایل ثبت وقایع را برای جلسات نظارت یا برای کنسول ارسال کنید. با این حال، انجام این کار می‌تواند بار CPU یک دستگاه NX-OS سیسکو را افزایش دهد، بنابراین توصیه نمی شود. علاوه بر این، بهتر است اطلاعات ورودی به سیستم را به log buffer محلی یا log file محلی ارسال کنید، که می‌تواند با استفاده از دستور show logging نمایش داده شود.

از دستورات پیکربندی سراسری nologging console و nologging monitor برای غیرفعال کردن ورود به جلسات کنسول و نظارت استفاده کنید. مثال زیر پیکربندی استفاده از این دستورات را نشان می‌دهد:

```
!
no logging console
no logging monitor
!
```

اگر خروجی یک رخداد برای اهداف عیب‌یابی مورد نیاز باشد، برای جلسات نظارت vty و جلوگیری از استفاده از آن در کنسول باید آن را فقط به طور موقت فعال کنید. مطمئن شوید که ثبت رخداد در سیستم برای جلسات نظارت پس از عیب‌یابی کاملاً غیرفعال شده است.

۳-۲-۱٤-٤ ورود به Log File

نرم‌افزار NX-OS سیسکو استفاده از یک بافر ثبت[٤٨] محلی در قالب یک فایل ثبت را پشتیبانی می‌کند تا مدیر بتواند پیام ثبت محلی تولید شده را مشاهده کند. استفاده از بافر ثبت به فایل ثبت به شدت توصیه می‌شود. به صورت پیش‌فرض، فایل ثبت در حافظه مدیا اسلات logflash ذخیره می‌شود که توسط logflash: device در

[٤٨] log

NX-OS سیسکو در خط فرمان CLI نشان داده می‌شود. نام فایل برای فایل ثبت به صورت پیش‌فرض messages است، که استاندارد UNIX آن loging file است. با استفاده از دستورloging file، می‌توان نام فایل ثبت را تغییر داد، اما محل فایل ثبت (logflash) را نمی‌توان تغییر داد.

دو گزینه پیکربندی وجود دارد که در هنگام پیکربندی buffered logging قابل توجه هستند: اندازه buffered logging و سطوح شدت پیام ذخیره شده در بافر. اندازه فایل ثبت و سطوح شدت پیام‌های ارسال شده به آن را می‌توان با استفاده از دستور سراسری logging logfile پیکربندی کرد. یک مدیر می‌تواند محتویات logging buffer را از طریق دستور EXEC show logging ببیند.

مثال زیر پیکربندی را با اندازه فایل ثبت ١٦٣٨٤ بایت و سطح شدت ٦ یعنی اطلاعاتی، تنظیم می‌کند و تعیین می‌کند که پیام‌ها در سطوح صفر (اضطراری) تا ٦ (اطلاعاتی) ذخیره شوند. نام پیش‌فرض فایل ثبت را نگه می‌دارد:

```
!
logging source-interface Loopback 0
!
```

٣-٢-١٤-٥ پیکربندی Logging Source Interface

برای ارائه‌ی یک سطح بالاتر از هماهنگی در هنگام جمع‌آوری و بازبینی پیام‌های ثبت وقایع، بایستی پیکربندی ایستا واسط ورودی منبع را از طریق دستور واسط logging source-interface انجام دهید. پیکربندی ایستا یک واسط ورودی منبع کمک می‌کند تا اطمینان حاصل کنیم که همان آدرس IP در تمام پیام‌های ثبتی که از یک دستگاه شخصی NX-OS ارسال می‌شود، نمایش داده می‌شود. برای این هدف، باید از یک واسط loopback به عنوان logging source استفاده کنید.

این مثال استفاده از دستور پیکربندی سراسری logging source-interface را نشان می‌دهد تا مشخص شود که آدرس IP واسط loopback 0 باید برای تمام message logها استفاده شود:

```
!
logging source-interface Loopback 0
!
```

۳-۲-۱۴-۶ پیکربندی Logging Time Stamps

پیکربندی Logging Time-Stamps به شما کمک می‌کند تا رخدادهای مربوط به دستگاه‌های شبکه را یکپارچه کنید. این مهم است که یک پیکربندی logging time-stamp را درست و منطبق انجام دهید تا اطمینان حاصل شود که می‌توانید logging data را به هم مرتبط کنید. باید پیکربندی Logging Time-Stamps تا دقت میلی ثانیه محاسبه شوند.

این مثال شامل پیکربندی logging time-stamps با دقت میلی ثانیه است:

```
!
logging timestamp milliseconds
!
```

۳-۲-۱۵ مدیریت پیکربندی NX-OS سیسکو

سیسکو NX-OS شامل چندین خصوصیت است که یک فرم مدیریت پیکربندی را می‌تواند در یک دستگاه NX-OS سیسکو فعال کند. چنین خصوصیاتی شامل عملیاتی برای آرشیو پیکربندی‌ها و بازگرداندن یک پیکربندی به یک نسخه قبلی و ایجاد پیکربندی دقیق تغییرات فایل ثبت وقایع است.

۳-۲-۱۵-۱ پیکربندی Checkpoint و Rollback

NX-OS سیسکو امکان یکپارچه‌ای برای تولید پیکربندی Checkpointها ارائه می‌دهد. این خصوصیت به سیستم اجازه می‌دهد تا یک آرشیو از پیکربندی snapshot را نگهداری کند. پیکربندی دستگاه می‌تواند توسط مدیر در هر زمان به هر کدام از پیکربندی Checkpointهای آرشیو شده Rollback شود.

یک پیکربندی Checkpoint دستی می‌تواند با دستور Checkpoint آغاز شود. پیکربندی خودکار Checkpointها را می‌توان به طور دوره‌ای با ترکیب خصوصیات Checkpoint و زمانبندی از NX-OS سیسکو تولید کرد. پیکربندی زیر یک زمانبندی کاری ایجاد می‌کند تا به طور خودکار هر یک ساعت از هشت ساعت یک پیکربندی Checkpoint تولید کند:

```
!
feature scheduler
!
scheduler job name auto_checkpoint
checkpoint
end-job
```

```
!
scheduler schedule name 8hr_checkpoint
job name auto_checkpoint
time start now repeat 00:08:00
!
```

Checkpointها در سیستم داخلی، Checkpoint در پایگاه داده با دستور show checkpointsummary نمایش داده می‌شوند و محتویات حقیقی فایل‌های Checkpoint را می‌توان با showcheckpoint نمایش داد.

یک پیکربندی در حال اجرا می‌تواند با استفاده از دستور rollback به checkpoint بازگردانده شود.

۳-۲-۱۵-۲ پیکربندی تغییر Notification و Logging

NX-OS سیسکو می‌تواند رخدادهای تغییر پیکربندی فایل ثبت وقایع را همراه با تغییرات شخصی وقتی که دستور AAA حساب کاربری فعال باشد، ثبت کند. با فعال شدن دستور حساب کاربری، تمام دستورات CLI وارد شده، از جمله دستورات پیکربندی، به سرویس‌دهنده AAA پیکربندی شده وارد می‌شوند. با استفاده از این اطلاعات، یک پیگیری قانونی برای رخدادهای تغییر پیکربندی همراه با دستورات شخصی که برای این تغییرات وارد شده است، می‌تواند ضبط و بررسی شود. با وجود این قابلیت، به شدت توصیه می شود که دستور AAA برای حساب کاربری فعال و پیکربندی شود.

۳-۲-۱۶ امنیت واحد کنترل

توابع واحد کنترل شامل پروتکل‌ها و عملیات‌های ارتباطی بین دستگاه‌های شبکه برای انتقال داده از منبع به مقصد است. این شامل پروتکل‌های مسیریابی مانند BGP و همچنین پروتکل‌هایی نظیر ICMP می‌باشد.

مهم است که رخدادها در واحدهای مدیریت و داده تأثیر ناسازگاری بر روی واحد کنترل نداشته باشند. اگر یک رخداد واحد داده مانند یک حمله DoS بر واحد کنترل تأثیر بگذارد، می‌تواند تمام شبکه را ناپایدار کند. اطلاعات این بخش در مورد خصوصیات NX-OS سیسکو است و پیکربندی‌هایی که می‌تواند به انعطاف پذیری واحد کنترل کمک کند.

۳-۲-۱۶-۱ مقاوم‌سازی کلی واحد کنترل

حفاظت واحد کنترل از یک دستگاه شبکه ضروری است، زیرا واحد کنترل کمک می‌کند تا اطمینان حاصل شود که واحدهای مدیریت و داده محفوظ و قابل استفاده هستند. اگر واحد کنترل در طول یک حادثه امنیتی

ناپایدار شود، پایداری شبکه قابل بازیابی نیست. در بسیاری از موارد، غیرفعال کردن دریافت و انتقال حروف خاصی از پیام‌ها در یک واسط می‌تواند بار CPU که برای پردازش بسته‌های غیر ضروری مورد نیاز است را کاهش دهد.

۳-۲-۱۶-۲ پیام‌های هدایتگر IP ICMP

یک پیام مسیریابی ICMP زمانی که یک بسته دریافت شده و به همان واسط انتقال یافته، می‌تواند توسط یک مسیریاب ایجاد شود. در این وضعیت، مسیریاب یک بسته را به جلو می‌فرستد و یک پیام هدایتگر ICMP را به فرستنده بسته اصلی ارسال می‌کند. این رفتار به فرستنده اجازه می‌دهد که مسیریاب را دور بزند و بسته‌های بعدی را به طور مستقیم به مقصد (یا به مسیریاب نزدیک به مقصد) ارسال کند. وقتی یک شبکه IP درست کار می‌کند که یک مسیریاب فقط به میزبان‌ها در زیرشبکه‌های محلی خود پیام‌های ارسال بفرستد. به عبارت دیگر، پیام‌های ارسال ICMP هرگز نباید فراتر از مرز لایه‌ی 3 باشد.

دو نوع پیام ارسال ICMP وجود دارد: پیام‌های نوع یک برای یک آدرس میزبان و پیام‌های نوع دوم برای کل زیرشبکه. یک کاربر مخرب می‌تواند از قابلیت مسیریاب برای فرستادن پیام‌های هدایتگرICMP با ارسال پیوسته ی بسته‌ها به مسیریاب استفاده کند، و مسیریاب را برای پاسخ با پیام‌های هدایتگر ICMP مجبور گرداند، که در نتیجه موجب تأثیر منفی بر CPU و عملکرد مسیریاب می‌شود. برای جلوگیری از ارسال پیام‌های هدایت گر ICMP مسیریاب، از دستور پیکربندی واسط no ip redirects استفاده کنید.

۳-۲-۱۶-۳ پیام‌های غیر قابل دسترسی ICMP

محدودسازی با یک واسط لیست دسترسی موجب انتقال پیام‌های غیر قابل دسترس ICMP به منبع ترافیک محدود شده می‌شود. تولید این پیام‌ها می‌تواند بهره وری از CPU را در دستگاه افزایش دهد.

شما می‌توانید تولید پیام‌های غیرقابل دسترسی ICMP را با استفاده از دستور پیکربندی واسط noip unreachables غیرفعال کنید.

۳-۲-۱۶-٤ سرویس NTP

سرویس NTP اگر به صورت صحیح پیکربندی شود، سرویس زیاد خطرناکی نیست، اما هر سرویس غیرضروری می‌تواند یک مسیر حمله را نشان دهد. اگر NTP استفاده شود، باید مطمئن شوید که برای استفاده

از احرازهویت درست یک منبع زمانی معتبر صریحاً پیکربندی شود. زمان دقیق و قابل اطمینان می‌تواند برای اهداف ورود، مانند تحقیقات قانونی حملات بالقوه، بسیار مفید باشد.

پیکربندی احرازهویت NTP این اطمینان را فراهم می‌کند که پیام‌های NTP بین جفت NTPهای مورد اعتماد رد و بدل می شوند. شما باید احرازهویت NTP را در صورت امکان فعال کنید. علاوه بر این، برای مقا صد دقت و انفصال، شما باید چندین منبع زمان سرویس‌دهنده NTP را در دستگاه NX-OS پیکربندی کنید که به عنوان یک سرویس‌گیرنده‌ی NTP عمل می‌کنند.

۳-۲-۱۶-۵ محدودکردن اثر ترافیک واحد کنترل بر CPU

حفاظت از واحد کنترل مهم است. از آنجا که عملکرد نرم‌افزار و تجربه کاربر نهایی بدون حضور ترافیک داده‌ها و مدیریت دچار مشکل می‌شود، بقای واحد کنترل کمک می‌کند تا این اطمینان حاصل شود که دو واحد دیگر محفوظ و قابل استفاده هستند.

۳-۲-۱۶-۶ درک ترافیک واحد کنترل

برای اینکه از واحد کنترل دستگاه NX-OS سیسکو به درستی محافظت کنید باید انواع ترافیک‌هایی که پردازش آن توسط CPU تغییر می‌کند را درک کنید. ترافیک پردازش تغییر یافته به طور معمول متشکل از دو نوع ترافیک است. نوع اول ترافیکی که به دستگاه NX-OS سیسکو هدایت می‌شود و باید مستقیماً توسط CPU دستگاه NX-OS سیسکو مورد استفاده قرار گیرد. این ترافیک شامل این دسته‌ها است:

- دریافت ترافیک مجاور: این ترافیک شامل یک ورودی در جدول CEF[۴۹] است که در آن هاپ مسیریاب بعدی دستگاه خودش است، که توسط بخش receive در خروجی show ip cef، CLI نشان داده می‌شود. این نشانه برای هر آدرس IP که نیاز به مدیریت مستقیم توسط CPU دستگاه NX-OS سیسکو داشته باشد، از جمله آدرس IPهای واسط، فضای آدرس چندپخشی و فضای آدرس همه‌پخشی است.

[۴۹] Cisco Express Forwarding

نوع دوم ترافیکی که توسط CPU پردازش می‌شود، ترافیک واحد داده با مقصد دیگری است که خارج از دستگاه NX-OS سیسکو قرار می‌گیرد و نیاز به پردازش ویژه توسط CPU دارد. این نوع رفتار معمولاً پلت فرم خاصی دارد و به پیاده‌سازی سخت‌افزاری خاص پلت‌فرم NX-OS سیسکو وابسته است. بعضی از پلت فرم‌ها انواع ترافیک واحد داده در سخت‌افزار را اداره می‌کنند و در نتیجه به مداخله کمتر CPU نیاز دارند. صرف نظر از قابلیت‌های کنترل کردن سخت‌افزاری، باید منابع بالقوه ترافیک واحد کنترل را که می‌تواند روی سیستم CPU تاثیر بگذارد، درک کند. اگر چه لیست کاملی از ترافیک واحد داده که بتواند CPU را تحت تأثیر قرار بدهد در دست نیست، اما این نوع ترافیک به طور بالقوه تغییر می‌کند و بنابراین می‌تواند بر عملکرد واحد کنترل تأثیر بگذارد:

- ACL logging : ترافیک ورودی ACL شامل هر بسته‌ای است که به دلیل یک تطبیق (مجاز یا غیرمجاز) از یک ورودی کنترل دسترسی (که از کلمه کلیدی log برای آن استفاده می‌شود) تولید می‌شود.
- uRPF[۵۰]: uRPF مورد استفاده در ارتباط با ACL ممکن است منجر به فرآیند سوئیچینگ بسته‌های خاص شود.
- IP options: تمام بسته‌های IP باید با گزینه‌های موجود توسط CPU پردازش شود.
- Fragmentation: هر بسته به IP Fragmentation نیاز دارد، باید به CPU منتقل شود.
- TTL expiry: بسته‌هایی که مقدار TTL کمتر یا برابر ۱ دارند، به ICMP Time Exceeded (ICMP Type 11, Code 0) نیاز دارند. پیام‌ها باید فرستاده شوند، که نتیجه در CPU پردازش شود.
- پیام‌های غیر قابل دسترسی ICMP: بسته‌های که اثرشان در پیام‌های غیر قابل دسترسی ICMP به علت مسیریابی، MTU، یا فیلترینگ توسط CPU، پردازش می‌شود.

[۵۰] Unicast Reverse Path Forwarding

- ترافیک مورد نیاز یک درخواست ARP: مقصدهایی که برای ورود ARP وجود ندارند نیازمند پردازش توسط CPU هستند.
- ترافیک Non-IP: تمام تراکنش‌های غیر آی پی توسط CPU پردازش می‌شود.

لیست زیر جزئیات چند روش برای تعیین نوع ترافیک توسط پردازنده دستگاه NX-OS را شرح می‌دهد:

- دستور show ip cef اطلاعات گره‌های بعدی برای هر پیشوند IP که در جدول CEF قرار دارد، را فراهم می‌کند.
- فرمان show interface switching اطلاعاتی در مورد تعداد بسته‌هایی که در حال پردازش توسط یک دستگاه هستند را ارائه می‌دهد.
- دستور show ip traffic اطلاعاتی در مورد تعداد بسته‌های IP ارائه می‌دهد:
  - با یک مقصد محلی (یعنی دریافت ترافیک adjacency)
  - نیاز به تکه تکه شدن دارند.
  - به فضای آدرس همه پخشی ارسال می‌شوند.
  - به فضای آدرس چندپخشی ارسال می‌شوند.

دریافت ترافیک adjacency می‌تواند از طریق استفاده از دستور show ip cache flow شناسایی شود. هر جریانی که برای دستگاه NX-OS تعیین شده یک واسط مقصد (DstIf) محلی دارد.

۳-۲-۱۶-۷ iACL

iACLها ارتباطات خارجی از شبکه به دستگاه را محدود می‌کنند.

شما باید iACLها را برای محافظت از واحد کنترل روی تمام دستگاه‌های شبکه پیاده‌سازی کنید.

۳-۲-۱۶-۸ CoPP

خصوصیت CoPP می‌تواند برای محدودکردن بسته‌های IP که برای زیرساخت دستگاه خودشان تعیین شده اند استفاده شود و به پردازش CPU واحد کنترل نیاز دارد. پیکربندی CoPP شبیه به پیکربندی QoS واحد داده است و از همان ساختارهای پیکربندیMQC[۵۱] استفاده می‌کند.

در این مثال، یک پیکربندی CoPP ایجاد می‌شود که در آن ترافیک SSH تنها از میزبان‌های قابل اعتماد مجاز است تا به CPU دستگاه NX-OS سیسکو دسترسی پیدا کند. تمام ترافیک دیگر واحد کنترل مجاز است.

توجه: رد کردن ترافیک از طریق آدرسIPهای نامشخص یا غیر قابل اعتماد می‌تواند از اتصال میزبان‌ها با آدرس‌های IP پویا به دستگاه NX-OS سیسکو جلوگیری کند.

```
!
access-list ALLOW_TRUSTED_SSH
  deny tcp <trusted-addresses> <mask> any eq 22
  permit tcp any any eq 22
  deny ip any any
!
class-map type control-plane match-all COPP-KNOWN-UNDESIRABLE
  match access-group name ALLOW_TRUSTED_SSH
!
policy-map type control-plane COPP-INPUT-POLICY
  class COPP-KNOWN-UNDESIRABLE
     police 1 conform drop violate drop
!
control-plane
  service-policy input COPP-INPUT-POLICY
!
```

[۵۱] Modular QoS CLI

۳-۲-۱۷ امنیت واحد داده

اگر چه واحد داده مسئول انتقال داده‌ها از منبع به مقصد است، در حقیقت امنیت واحد داده در این سه واحد اهمیت کمتری دارد. به همین دلیل، هنگام تأمین امنیت یک دستگاه شبکه، باید واحدهای کنترل و مدیریت را نسبت به واحد داده در اولویت قرار دهیم. با این حال، در داخل خود واحد داده، خصوصیات بسیاری برای پیکربندی وجود دارد که می‌تواند امنیت ترافیک را تضمین کند. بخش‌های زیر جزئیات این ویژگی‌ها و گزینه‌ها را بیان می‌کند به طوری که شما می‌توانید به راحتی شبکه خود را امن کنید.

۳-۲-۱۷-۱ مقاوم‌سازی کلی واحد داده

بیشتر جریان‌های ترافیک واحد داده در سراسر شبکه توسط پیکربندی مسیریابی شبکه تعیین شده است. با این حال، توابع شبکه IP برای تغییر مسیر بسته‌ها در سراسر شبکه در دسترس هستند.

۳-۲-۱۷-۲ غیرفعال کردن IP Source Routing

مسیریابی منبع IP با استفاده از گزینه‌های Loose Source Route و Record Route پشت سر هم، و یا همراه Strict Source Route با گزینه‌ی Record Route برای فعال کردن منبع از دیتاگرام IP و مشخص کردن مسیر شبکه‌ای که بسته را می‌گیرد، استفاده می‌شود. این تابع می‌تواند در جستجو برای مسیریابی ترافیک در اطراف کنترل‌های امنیتی شبکه مورد استفاده قرار گیرد. اگر گزینه‌های IP به طور کامل از طریق IP Options Selective Drop غیرفعال نشده باشند، این مهم است که شما مسیر منبع IP را غیرفعال کنید. مسیریابی منبع IP، که به صورت پیش‌فرض در تمامی نسخه‌های NX-OS فعال شده است، از طریق دستور پیکربندی سراسری noip source-route غیرفعال می‌شود. این مثال پیکربندی استفاده از این دستور را نشان می‌دهد:

```
!
no ip source-route
!
```

۳-۲-۱۷-۳ غیرفعال کردن پیام‌های ICMP Redirect

پیام‌های ICMP Redirect برای آگاه کردن شبکه از مسیری بهتر به مقصد IP استفاده می‌کند. به صورت پیش‌فرض،NX-OS سیسکو یک پیام Redirect را ارسال می‌کند و در صورتی که بسته‌ای دریافت کند باید از طریق واسطی که از آن دریافت شده است، مسیریابی شود.

در برخی موارد، مهاجم ممکن است قادر به ایجاد دستگاه NX-OS برای فرستادن بسیاری از پیام‌های ICMP Redirect باشد، که موجب افزایش بار پردازنده می‌شود. به همین دلیل، انتقال پیام‌های ICMP Redirect باید غیرفعال شود. پیام‌های ICMP Redirect همانطور که در پیکربندی مثال نشان داده شده است با استفاده از دستور پیکربندی واسط no ip redirects غیرفعال می‌شوند:

```
!
interface ethernet 1/1
    no ip redirects
!
```

۳-۲-۱۷-٤ غیرفعال کردن یا محدود کردن IP Directed Broadcasts

IP Directed Broadcasts امکان ارسال یک بسته پخش IP به یک زیر شبکه از راه دور IP را فراهم می‌کند. پس از اینکه بسته به شبکه راه دور می‌رسد، دستگاه ارسال IP این بسته را به عنوان پیام همه‌پخشی لایه ۲ به تمام ایستگاه‌های زیر شبکه ارسال می‌کند. این تابع به عنوان تقویت‌کننده و منعکس‌کننده‌ی کمکی در چندین حمله، از جمله حمله smurf استفاده می‌شود.

نسخه‌های فعلی NX-OS سیسکو این قابلیت را به صورت پیش‌فرض غیرفعال کرده‌اند. با این حال، می‌توان آن را با دستور پیکربندی واسط ip directed-broadcast فعال کرد.

۳-۲-۱۷-۵ محدودسازی ترافیک عبوری با ACLها

شما می‌توانید کنترل کنید که چه ترافیکی با استفاده از ACLها از شبکه عبور می‌کند. در مقابل، iACLها به دنبال محدودسازی ترافیکی هستند که برای شبکه مشخص شده است. محدودسازی ارائه شده توسط ACLها زمانی مفید است که برای محدودسازی ترافیک یک گروه خاصی از دستگاه‌ها یا ترافیک در حال عبور از شبکه مطلوب باشد.

این نوع محدودیت به طور سنتی تو سط دیواره‌های آتش انجام می شود. با این حال، در برخی موارد ممکن است مفید باشد که این محدودیت را بر روی یک دستگاه سیسکو NX-OS در شبکه انجام دهید: برای مثال، هنگامی‌که محدودسازی باید انجام شود، اما هیچ دیواره آتشی وجود ندارد.

۳-۲-۱۷-٦ محدودسازی بسته‌های ICMP

ICMP به عنوان یک پروتکل کنترلی برای IP طراحی شده است. به این ترتیب، پیام‌هایی که انتقال می‌دهند، به طور کلی می‌توانند انشعابات گسترده‌ای در پروتکل‌های TCP و IP داشته باشند. ICMP توسط ابزارهای عیب‌یابی شبکه ping و traceroute و نیز شناسایی مسیر MTU استفاده می‌شود؛ با این حال، اتصال ICMP خارجی برای عملکرد مناسب شبکه به ندرت مورد نیاز است.

NX-OS سیسکو به طور خاص توابع را برای محدودسازی پیام‌های ICMP با نام یا نوع و کد ارائه می‌دهد. این مثال ACL، ICMP را از شبکه‌های مورد اعتماد می‌پذیرد، درحالی که تمام بسته‌هایICMP از منابع دیگر مسدود شده‌اند:

```
!
ip access-list ACL-TRANSIT-IN
! !--- Permit ICMP packets from trusted networks only !
 permit icmp <trusted-networks>/<mask> any
! !--- Deny all other IP traffic to any network device !
 deny icmp any any
!
```

۳-۲-۱۷-۷ محدودسازی Fragmentهای IP

همانطور که قبلا در بخش دسترسی محدود به شبکه با زیرساخت ACLها در این سند بحث شده است، محدودسازی بسته‌های IP Fragment شده می‌تواند حالت چالش را برای تجهیزات امنیتی داشته باشد.

به دلیل ماهیت غیرواقعی دستکاری Fragment، Fragmentهای IP اغلب به طور غیرمجاز توسط ACLها مجاز می‌شوند. Fragment اغلب برای فرار و جلوگیری از تشخیص استفاده می‌شود که به کمک سیستم‌های تشخیص نفوذ انجام می‌شود. به همین علت، Fragmentهای IP اغلب در حملات استفاده می‌شوند و باید به صورت واضح در بالای هر ACLهای پیکربندی شده فیلتر شوند. ACL نشان داده شده در اینجا شامل محدودیت جامعی از Fragmentهای IP است. تابع نمایش داده شده در این مثال باید در رابطه با توابع نمایش داده شده در مثال‌های قبلی مورد استفاده قرار گیرد:

```
!
ip access-list ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
```

```
!--- classification of attack traffic !
  deny tcp any any fragments
  deny udp any any fragments
  deny icmp any any fragments
  deny ip any any fragments
!
```

۳-۲-۱۷-۸ پیاده‌سازی حفاظت Antispoofing

در بسیاری از حملات جعل[۵۲] در IP آدرس منبع مؤثر است مگر اینکه منبع واقعی را از یک حمله پنهان کنند و از ردیابی دقیق آن جلوگیری کنند. سیسکو NX-OS برای حفاظت از حملاتی که بر spoofing آدرس IP منبع تکیه دارد، منبع uRPF را ارائه می‌دهد. علاوه بر این، ACLها وnullrouting اغلب به عنوان یک ابزار برای جلوگیری از spoofing استفاده می‌شوند.

محافظت از منبع IP در کاهش spoofing برای شبکه‌هایی که تحت کنترل مستقیم مدیریت هستند با اجرای درگاه سوئیچ، آدرس فیزیکی و تأیید آدرس‌های منبع موثر هستند. uRPF تأیید شبکه منبع را فراهم می‌کند و می‌تواند حملات spoofing از شبکه‌هایی که تحت کنترل مستقیم مدیریت نیستند را کاهش دهد. امنیت درگاه ها می‌تواند برای اعتبارسنجی آدرس فیزیکی در لایه دسترسی مورد استفاده قرار گیرد. DAI[۵۳] باعث کاهش مسیرهای حمله‌ای می‌شود که از ARP poisoning[۵۴] در بخش‌های محلی استفاده می‌کند.

۳-۲-۱۷-۹ پیکربندی uRPF[۵۵]

uRPF یک دستگاه را قادر می‌سازد تا تأیید کند که آدرس منبع بسته‌ی ارسال شده را می‌توان از طریق واسط بسته‌ی رسیده، دریافت کرد. شما نباید بر روی uRPF به تنهایی برای حفاظت در برابر spoofing تکیه کنید. اگر یک مسیر بازگشت مناسب برای آدرس IP منبع وجود داشته باشد، بسته‌های جعلی می‌توانند از طریق یک

---

[۵۲] spoofing

[۵۳] Dynamic ARP Inspection

[۵۴] Address Resolution Protocol

[۵۵] Unicast Reverse Path Forwarding

واسط باuRPF فعال وارد شبکه شوند. uRPF برای فعال کردن CEF[۵۶] در هر دستگاه بر پایه یک واسط پیکربندی می‌گردد. uRPF را می‌توان در دو حالت پیکربندی کرد: loose یا strict.

حالت loose در مواردی که مسیریابی نامتقارن وجود دارد ترجیح داده می‌شود، زیرا حالت strict برای رد بسته‌ها در این شرایط شناخته شده است. در هنگام پیکربندی دستور پیکربندی واسط ip verify، کلمه کلیدی any حالت loose و حالت strict را پیکربندی می‌کند. مثال زیر پیکربندی این ویژگی را نشان می‌دهد:

```
!
interface Ethernet <slot>/<port>
ip verify unicast source reachable-via [any | rx]
!
```

۳-۲-۱۷-۱۰ استفاده از IP Source Guard

IP Source Guard یک ابزار مؤثر پیشگیری از spoofing است. اگر شما روی واسط‌های لایه ۲ کنترل داشته باشید می‌توانید آن را مورد استفاده قرار دهید. IP Source Guard از پروتکل DHCP snooping[۵۷] استفاده می کند تا به صورت پویا درگاه ACL (PACL) را در واسط لایه‌ی ۲ پیکربندی کند، هر گونه ترافیک آدرس‌های IP که به جدول اتصال منبع IP وابسته نیست را رد می‌کند. IP Source Guard می‌تواند به واسط‌های لایه‌ی ۲ متعلق به VLANهای فعال برای DHCP snooping اعمال شود. این دستورات DHCP snooping را فعال می‌کند:

```
!
feature dhcp
ip dhcp snooping
!
```

پس از فعال کردن DHCP snooping ، این دستورات محافظ IP را فعال می‌کند:

```
!
interface ethernet <slot>/<port>
  ip verify source dhcp-snooping vlan
```

[۵۶] Cisco Express Forwarding

[۵۷] Dynamic Host Configuration Protocol

```
!
```

۳-۲-۱۷-۱۱ استفاده از Port Security

پیکربندی Port Security یا امنیت پورت برای کاهش جعل آدرس‌های فیزیکی در واسط دسترسی استفاده می‌شود. امنیت درگاه می‌تواند از آدرس‌های فیزیکی یادگیری پویا (sticky) استفاده کند تا پیکربندی اولیه را تسهیل کند. پس از اینکه امنیت پورت یک نقض آدرس فیزیکی را تشخیص داد، می‌تواند از یکی از چهار حالت violation استفاده کند: محافظت، محدودکردن، خاموش‌کردن و خاموش‌کردن VLAN، در مواردی که یک پورت فقط برای یک ایستگاه کاری با استفاده از پروتکل‌های استاندارد دسترسی پیدا می‌کند، ممکن است حداکثر مقدار ۱ کافی باشد. (نکته: پروتکل‌هایی مانند پروتکل HSRP[۵۸] که از آدرس فیزیکی مجازی استفاده می‌کنند هنگامی‌که حداکثر مقدار ۱ تنظیم می‌شود، عمل نمی‌کنند.)

```
!
feature port-security
interface <slot>/<port>
  switchport
  switchport port-security [mac address sticky]
!-- Optionally enable sticky MAC address learning
!
```

۳-۲-۱۷-۱۲ استفاده از DAI

DAI می‌تواند برای کاهش حملات ARP poisoning در بخش‌های محلی مورد استفاده قرار گیرد. حمله ARP poisoning روشی است که یک مهاجم اطلاعات ARP جعلی را به یک بخش محلی ارسال می‌کند. این اطلاعات برای خراب کردن حافظه ARP و سایر دستگاه‌ها طراحی شده است. غالبا یک مهاجم از ARP poisoning برای انجام حمله «شخصی در میانه» استفاده می‌کند.

DAI رابطه‌ی آدرس IP-to-MAC تمام بسته‌های ARP را بر روی پورت‌های نامطمئن تأیید و حفاظت می کند. در محیط‌های DHCP، DAI از داده‌هایی استفاده می‌کند که با خصوصیت DHCP snooping تولید می شوند. بسته‌های ARP که در واسط‌های غیرقابل‌اعتماد دریافت می‌شوند معتبر نیستند و بسته‌های نامعتبر در

[۵۸] Hot Standby Router Protocol

واسط‌های غیر قابل اعتماد از بین می‌روند. در محیط‌های غیر DHCP، استفاده از ACLهای ARP ضروری است.

این دستورات DHCP snooping را فعال می‌کنند:

```
!
feature dhcp
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

پس از فعال شدن DHCP snooping ، این دستورات DAI را فعال می‌کنند:

```
!
ip arp inspection vlan <vlan-range>
!
```

در محیط‌های غیر DHCP، ACLهای ARP برای فعال کردن DAI ضروری هستند. این مثال پیکربندی اولیه DAI با ACLهای ARP را نشان می‌دهد:

```
!
arp access-list <acl-name> permit ip host <sender-ip> mac host <sender-mac>
!
ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

۳-۲-۱۷-۱۳ پیکربندی Antispoofing ACLها

ACLها به صورت دستی پیکربندی شده و می‌توانند حفاظت Antispoofing ایستا را در برابر حملات شناخته شده که از فضای آدرس IP بی‌استفاده و غیرقابل‌اعتماد استفاده می‌کنند، انجام دهند. معمولاً این antispoofing ACLها به ترافیک ورودی در مرزهای شبکه به عنوان یک جزء از یک ACL بزرگتر اعمال می‌شوند. ACLهای Antispoofing نیاز به نظارت منظم دارند زیرا می‌توانند به طور مرتب تغییر کنند. Spoofing در ترافیک ناشی از شبکه محلی با استفاده از ACLهای خروجی که ترافیک را به آدرس‌های محلی معتبر محدود می‌کنند، کاهش می‌یابد.

این مثال نشـان می‌دهد که چگونه ACLها می‌توانند با محدود کردن IP جعلی اسـتفاده شـوند. این ACL بر روی واسـط مورد نظر وارد می‌شـود. ورودی‌های کنترل دسـترسـی که این ACL را تشـکیل می‌دهند کامل نیستند. (اگر این نوع ACLها را پیکربندی کنید، به دنبال یک مرجع به روز باشید که کامل باشد.)

```
!
ip access-list ACL-ANTISPOOF-IN
  deny ip 10.0.0.0 0.255.255.255 any
  deny ip 192.168.0.0 0.0.255.255 any
!
interface ethernet <slot>/<port>
  ip access-group ACL-ANTISPOOF-IN in
!
```

۳-۲-۱۷-۱٤ محدودکردن تأثیر ترافیک واحد داده روی CPU

هدف اولیه مسیریاب‌ها و سوئیچ‌ها انتقال بسته‌ها و فریم‌ها از طریق دستگاه به سمت مقصد نهایی است. این بسته‌ها، که توسط دستگاه‌های مستقر در سراسر شبکه حمل می‌شوند، می‌توانند بر عملکرد پردازنده یک دستگاه تأثیر بگذارند. واحد داده، که شامل ترافیک عبوری از دستگاه‌های شبکه است، باید به کمک اطمینان از عملکردهای واحدهای مدیریت و کنترل امن شد. اگر ترافیک عبوری دلیل دستگاه برای روند ترافیک سوئیچ باشد، واحد کنترل یک دستگاه را می‌تواند تحت تأثیر قرار داد که ممکن است منجر به اختلال در عملیات شود.

خصوصیات و انواع ترافیک‌هایی که CPU را تحت تأثیر قرار می‌دهند.

این لیست (اگرچه کامل نیست) شامل انواع ترافیک‌های واحد داده‌ای است که ممکن است نیاز به پردازش CPU خاص داشته باشد:

- ورودی ACL: ترافیک ورودی ACL شامل هر بسته‌ای است که به دلیل یک تطبیق (مجاز یا غیرمجاز) از یک ورودی کنترل دسترسی (که از کلمه کلیدی log برای آن استفاده می‌شود) تولید می‌شود.
- uRPF :uRPF مورد استفاده در ارتباط با ACL ممکن است منجر به فرآیند سوئیچینگ بسته‌های خاص شود.
- گزینه‌های IP: تمام بسته‌های IP باید با گزینه‌های موجود توسط CPU پردازش شود.

- تکه تکه نمودن بسته‌ها: هر بسته IP که نیاز به تکه تکه شدن دارد، باید به CPU منتقل شود.
- انقضای TTL : بسته‌هایی که مقدار TTL کمتر یا برابر ۱ دارند، به ICMP Time Exceed (ICMP Type11, Code0) نیاز دارند. پیام‌ها باید فرستاده شوند، که نتیجه در CPU پردازش شود.
- پیام‌های غیر قابل دسترسی ICMP: بسته‌هایی که اثرشان در پیام‌های غیر قابل دسترسی ICMP به علت مسیریابی، MTU، یا پالایش توسط CPU، پردازش می‌شود.
- ترافیک مورد نیاز یک درخواست ARP: مقصدهایی که برای ARP ورودی ندارند نیازمند پردازش توسط CPU هستند.
- ترافیک غیر IP : تمام تراکنش‌های غیر IP توسط CPU پردازش می‌شود.

۳-۲-۱۷-۱۵ شناسایی و ردیابی ترافیک

در مواردی ممکن است مجبور باشید به سرعت ترافیک شبکه را شناسایی و ردیابی کنید، مخصوصاً هنگام پاسخ به حادثه یا هنگامی‌که عملکرد شبکه ضعیف باشد. طبقه‌بندی ACLها و NetFlow دو سازوکار اصلی برای انجام این کار با استفاده از NX-OS سیسکو هستند. NetFlow روی تمام ترافیک شبکه به ما دید می دهد. علاوه بر این، NetFlow با جمع‌کننده‌هایی که long-term trending و تحلیل خودکار دارند پیاده‌سازی می‌شود. ACLهای طبقه‌بندی جزء ACLها هستند و به برنامه‌ریزی برای شناسایی ترافیک خاص و مداخله دستی در طی تحلیل نیاز دارند. این بخش‌ها یک مرور کلی از خصوصیات ارائه می‌دهد.

۳-۲-۱۷-۱۶ NetFlow

NetFlow با ردیابی جریان‌های شبکه فعالیت غیرمرتبط با امنیت و امنیت شبکه را شناسایی می‌کند. داده‌های NetFlow را می‌توان با استفاده از CLI[۵۹] مشاهده و تجزیه و تحلیل کرد، و یا می‌توان آن‌ها را با جمع‌کننده رایگان یا تجاری نرم‌افزارNetFlow برای جمع‌آوری و تجزیه و تحلیل فرستاد. جمع‌کنندگان NetFlow، از طرق long-term trending، می‌توانند تحلیل رفتار و کاربرد شبکه را ارائه دهند. عملکرد NetFlow با انجام بررسی و تحلیل روی صفات خاص در بسته‌های IP و ایجاد جریان بهبود می‌یابد. NetFlow 5 یک نسخه رایج از NetFlow است؛ با این حال، نسخه ۹ بیشتر قابل گسترش است. جریان NetFlow را می‌توان با استفاده

[۵۹] Command-line interface

از نمونه گرفتن از داده‌های ترافیکی در محیط‌های با حجم بالا ایجاد کرد. مثال زیر پیکربندی اولیه این ویژگی را نشان می‌دهد:

```
!
! - Enable the NetFlow feature
feature netflow
!
! - Define a flow record. There are also predefined standard records that can be used.
flow record FLOW_RECORD_EXAMPLE
  description Example flow record
  match ip protocol
  collect counter bytes
  collect flow direction
  collect interface input
  collect interface output
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
!
! - Create a flow exporter
flow exporter EXAMPLE_FLOW_EXPORTER
  destination <IP address> use-vrf <vrf name>
  source <interface>
  version {5 | 9}
!
! - Create a flow monitor
flow monitor EXAMPLE_FLOW_MONITOR
  description <string>
  exporter EXAMPLE_FLOW_EXPORTER
  record { EXAMPLE_FLOW_RECORD | netflow-original | netflow protocol-port }
!
! - Apply the flow monitor to an interface
interface ethernet <slot>/<port>
  ip flow monitor EXAMPLE_FLOW_MONITOR {input | output}
!
```

۳-۲-۱۷-۱۷ طبقه‌بندی ACLها

طبقه‌بندی ACLها نسبت به ترافیک مسیر یک واسط به ما دید می‌دهد. سیاست‌های امنیتی ACLهای طبقه‌بندی شده یک شبکه تغییر نمی‌کنند و معمولاً برای پروتکل‌های شخصی طبقه‌بندی شده، آدرس‌های منبع یا مقصدها ساخته می‌شوند. برای مثال، یک ورودی کنترل دسترسی که تمام ترافیک را می‌تواند به پروتکل‌ها یا پورت‌های خاص تقسیم کند. این طبقه‌بندی دقیق‌تری برای ترافیک در ورودی‌های کنترل دسترسی خاص است که می تواند به ارائه درک از ترافیک شبکه‌ای کمک کند. یک مدیر برای کمک به شناسایی انواع ترافیک ممنوعه می تواند پاسخ انکار ضمنی را در پایان یک ACL به ورودی‌های کنترل دسترسی جدا کند.

یک مدیر می‌تواند توسط ACLها طبقه‌بندی با نمایش لیست دسترسی و دستورات EXEC، clear ip access-list counters و show access-list پاسخ رخداد را تسریع کند.

مثال زیر پیکربندی یک ACL طبقه‌بندی برای شناسایی ترافیک SMB[۶۰] مخرب را نشان می‌دهد.

```
!
ip access-list ACL-SMB-CLASSIFY
remark Existing contents of ACL
remark Classification of SMB specific TCP traffic
deny tcp any any eq 139
deny tcp any any eq 445
deny ip any any
!
```

برای شناسایی ترافیکی که از طبقه‌بندی ACL استفاده می‌کند، از دستور EXEC، show access-list acl-name استفاده کنید. شمارنده ACL را می‌توان با استفاده از دستور EXEC، clear ip access-list counters acl-name پاک کرد.

[۶۰] small and medium-sized business

۳-۲-۱۷-۱۸ کنترل دسترسی با VLAN Mapها و PACLها

VLAN ACLها (VACLها)، یا VLAN Mapها و PACLها، قابلیت اجرای کنترل دسترسی بر روی ترافیک غیررسمی را فراهم می‌کنند که به دستگاه‌های انتهایی نسبت به ACLها نزدیک‌تر است و به واسطه‌های مسیریابی شده اعمال می‌شوند.

بخش‌های زیر مروری کلی از ویژگی‌ها، مزایا و موارد احتمالی استفاده از NX-OS سیسکو برای VACLها و PACLها را ارائه می‌دهند.

۳-۲-۱۷-۱۹ کنترل دسترسی با VLAN Mapها

VACLها یا VLAN Mapها برای تمام بسته‌هایی که به VLAN وارد می‌شوند، اعمال می‌شوند. قابلیت اجرای کنترل دسترسی برای ترافیک داخل VLAN را فراهم می‌کنند. این کنترل با استفاده از ACLها در واسطه‌های مسیریابی شده امکان پذیر نیست. برای مثال، یک VLAN Map می‌تواند برای جلوگیری از میزبان‌هایی که در یک VLAN مشابه با یکدیگر ارتباط برقرار می‌کنند، استفاده شود، درنتیجه فرصت برای مهاجمان محلی یا کرم‌ها برای سوءاستفاده از میزبان در همان بخش شبکه کاهش می‌یابد.

برای جلوگیری از استفاده‌ی بسته‌های VLAN Map، می‌توانید یک ACL ایجاد کنید که با ترافیک منطبق باشد و در VLAN Map این اقدام را با drop تنظیم کنید. پس از پیکربندی نقشه VLAN، تمام بسته‌هایی که به LAN وارد می‌شوند، به طور پیوسته در برابر پیکربندی VLAN Map ارزیابی می‌شوند. نقشه‌های دسترسی VLAN از لیست آدرس‌های دسترسی IPv4 و MAC پشتیبانی می‌کنند، اما از ورود به IPv6 ACL پشتیبانی نمی‌کنند. مثال زیر با استفاده از لیست دسترسی ویژگی‌های این پیکربندی را نشان می‌دهد:

```
!
ip access-list <acl-name>
permit <protocol> <src-address> <src-port> <dst-address> <dst-port>
!
vlan access-map <name> <number>
  match ip address <acl-name>
  action <drop|forward>
!
```

مثال زیر استفاده از یک VLAN Map برای رد دسترسی به پورت‌های TCP، ۱۳۹ و ٤٤٥ را نشان می‌دهد.

```
!
ip access-list VACL-MATCH-ANY
  permit ip any any
!
ip access-list VACL-MATCH-PORTS
  permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
  permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!
!
vlan access-map VACL 20
  match ip address VACL-MATCH-PORTS
  action drop
!
vlan access-map VACL 30
  match ip address VACL-MATCH-ANY
  action forward
!
```

۳-۲-۱۷-۲۰ کنترل دسترسی با PACLها

PACLها را می‌توان فقط در جهت ورودی به واسط‌های فیزیکی لایه ۲ یک سوئیچ اعمال کرد. همانند VLAN Mapها، PACLها کنترل دسترسی را بر روی ترافیک لایه ۲ یا مسیریابی نشده ارائه می‌دهند. پیکربندی برای ایجاد PACLها، که بر روی VLAN Mapها و ACLهای مسیریاب مورد توجه قرار می‌گیرد، همانند ACLهای مسیریاب است. اگر یک ACL به یک واسط لایه ۲ اعمال شود، آنگاه آن را به عنوان PACL می شناسند. پیکربندی شامل ایجاد IPv4، IPv6 یا ACL آدرس فیزیکی و اعمال آن به واسط لایه ۲ است.

مثال زیر با استفاده از لیست دسترسی ویژگی‌های این پیکربندی را نشان می‌دهد:

```
!
ip access-list extended <acl-name> permit <protocol> <source-address>
<source-port> <destination-address> <destination-port>
!
interface <type> <slot/port> switchport mode access switchport access vlan
<vlan_number> ip access-group <acl-name> in
```

```
!
```

۳-۲-۱۷-۲۱ کنترل دسترسی با ACLهای آدرس فیزیکی

طبقه‌بندی بسته‌های MAC به شما این امکان را می‌دهد تا کنترل کنید که آیا یک ACL MAC که در یک واسط لایه‌ی ۲ است، به تمام ترافیک وارد شده در واسط، از جمله ترافیک IP یا تنها ترافیک غیر IP، اعمال می شود. شما می‌توانید بسته‌بندی MAC را تنها در واسط‌های لایه ۲ فعال یا غیرفعال کنید. برای پیکربندی یک واسط به عنوان لایه ۲، از دستور switchport استفاده کنید.

مثال زیر نحوه فعال کردن طبقه‌بندی بسته‌های MAC و اینکه چگونه یک واسط اترنت را به عنوان لایه ۲ پیکربندی کنید، را نشان می‌دهد.

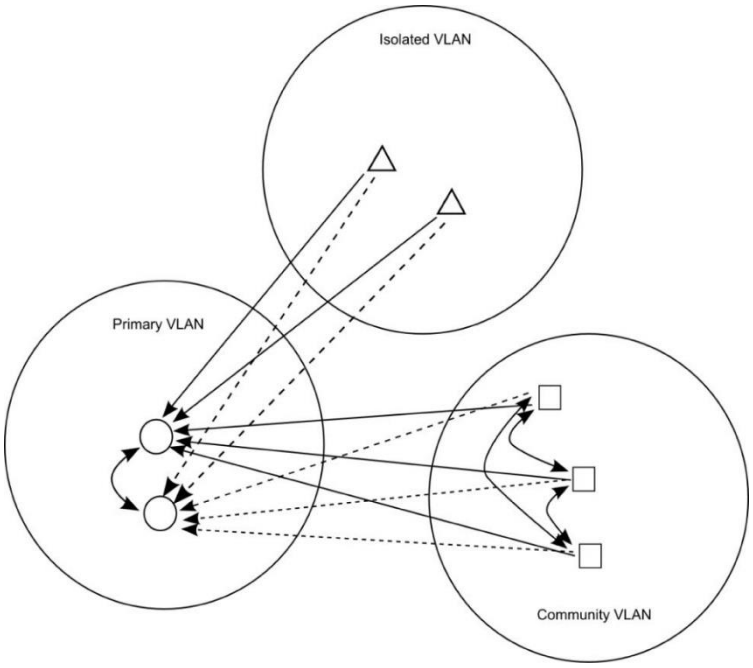
```
switch# conf t
switch(config)# interface ethernet 2/3
switch(config-if)# switchport
switch(config-if)# mac packet-classify
switch(config-if)#
```

نکته: این دستور در نسخه ی 4.2(1) یا نسخه‌های بعد از آن پشتیبانی می‌شود.

۳-۲-۱۷-۲۲ VLANهای خصوصی

VLANهای خصوصی(PVLANها) یک خصوصیت لایه ۲ هستند که اتصال بین ایستگاه‌های کاری یا سرویس‌دهنده‌ها در یک VLAN را محدود می‌کنند. بدون PVLANها، تمام دستگاه‌های VLAN لایه‌ی ۲ می توانند آزادانه ارتباط برقرار کنند. در برخی از حالات شبکه، با محدود کردن ارتباط بین دستگاه‌ها در یک VLAN تنها می‌توان به امنیت کمک کرد. محدود کردن الگوهای ارتباطی ممکن در یک VLAN با استفاده از PVLANها می‌تواند یک ابزار مؤثر امنیتی را ارائه دهد. به عنوان مثال، PVLANها اغلب برای ممنوع کردن ارتباط بین سرویس‌دهنده‌ها در یک زیرشبکه قابل دسترس عموم استفاده می‌شوند. اگر یک سرویس‌دهنده به خطر افتاده باشد، عدم اتصال به سرویس‌دهنده‌های دیگر به دلیل استفاده از PVLANها می‌تواند مؤثر باشد.

سه نوع ساختار VLAN در زمینه PVLAN وجود دارد: VLANهای ایزوله، community VLANها و VLANهای اولیه. پیکربندی PVLANها از VLAN اولیه و ثانویه استفاده می‌کند. VLAN اصلی شامل تمام پورت‌های پرکاربرد است که برای روابط یک به چند به گره‌ها در سایر انواع VLANها نگاشت می‌شود، که شامل یک یا چند VLAN ثانویه است که می‌توانند جدا یا community VLAN باشند (شکل ۱).



شکل ۱: رابطه بین انواع VLANها و پورت‌ها در PVLANها

۳-۲-۱۷-۲۳ VLANهای ایزوله

پیکربندی یک VLAN ثانویه به عنوان یک VLAN ایزوله به طور کامل از ارتباط بین دستگاه‌های VLAN ثانویه جلوگیری می‌کند. تنها یک VLAN ایزوله در هر VLAN اولیه وجود دارد، و فقط پورت‌های پرکاربرد می‌توانند با پورت‌های یک VLAN ایزوله ارتباط برقرار کنند. VLANهای ایزوله می‌بایست در شبکه‌های نامعلوم و در شرایطی که در ارتباط بین گره‌ها اعتمادی وجود ندارد استفاده شوند، مانند شبکه‌هایی که از کاربر مهمان پشتیبانی می‌کنند.

مثال زیر VLAN 11 را به عنوان یک VLAN ایزوله پیکربندی می‌کند و آن را با VLAN اولیه، VLAN 20 هماهنگ می‌کند. همچنین واسط اترنت ۱/۱ را به عنوان یک پورت ایزوله در VLAN 11 پیکربندی می‌کند:

```
! - In order to use Private VLANs the feature must first be enabled
feature private-vlan
!
vlan 11 private-vlan isolated
!
```

```
vlan 20
  private-vlan primary
  private-vlan association 11
!
interface ethernet 1/1
  description *** Port in Isolated VLAN ***
  switchport mode private-vlan host
  switchport private-vlan host-association 20 11
!
```

۳-۲-۱۷-۲٤ Community VLANها

یک VLAN ثانویه که به عنوان یک VLAN Community پیکربندی شده، بین بخش‌های VLAN و همچنین با هر پورت پرکاربرد VLAN اولیه ارتباط برقرار می‌کند. با این وجود، هیچ ارتباطی بین دو VLAN Community یا از یک VLAN Community به یک VLAN ایزوله امکان‌پذیر نیست. این VLANها باید برای گروه‌بندی سرویس‌دهنده‌هایی که نیاز به اتصال به یکدیگر دارند استفاده شوند، اما برای اتصال به سایر دستگاه‌های VLAN نیازی نیست. این سناریو در یک شبکه قابل دسترس عموم و یا هر جا که سرویس‌دهنده وب را به مشتریان غیر قابل اعتماد ارائه می‌دهد مشترک است، اما باید برای عملکرد نرمال یک اعتماد داخلی و یک رابطه بین خودی را حفظ گردد. مثال زیر یک VLAN Community تنها را پیکربندی می‌کند و سوئیچ پورت اترنت ۲/۱ را به عنوان عضو آن VLAN پیکربندی می‌کند.

```
!
vlan 12
  private-vlan community
!
vlan 20
  private-vlan primary
  private-vlan association 12
!
interface ethernet 1/2
  description *** Port in Community VLAN ***
  switchport mode private-vlan host
  switchport private-vlan host-association 20 12
```

```
!
```

۳-۲-۱۷-۲۵ پورت‌های بی‌قاعده

پورت‌هایی که در VLAN اولیه قرار می‌گیرند، به عنوان پورت‌های بی‌قاعده شناخته می‌شوند. پورت‌های بی قاعده می‌توانند با تمام پورت‌های دیگر در VLAN اولیه و ثانویه ارتباط برقرار کنند. واسط‌های مسیریاب یا دیواره‌ی آتش رایج‌ترین دستگاه‌های موجود در این VLANها هستند. مثال زیر پیکربندی، ترکیب مثال‌های قبلی VLAN ایزوله و Community VLANها است و پیکربندی واسط اترنت 1/12 را به عنوان یک پورت بی‌قاعده به آن اضافه می‌کند:

```
!
feature private-vlan
!
vlan 11
  private-vlan isolated
!
vlan 12
  private-vlan community
!
vlan 20
  private-vlan primary
  private-vlan association 11-12
!
interface ethernet 1/1
  description *** Port in Isolated VLAN ***
  switchport mode private-vlan host
  switchport private-vlan host-association 20 11
!
interface ethernet 1/2
  description *** Port in Community VLAN ***
  switchport mode private-vlan host
  switchport private-vlan host-association 20 12
!
interface ethernet 1/12
  description *** Promiscuous Port ***
```

```
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 20 add 11-12
!
```

هنگام پیاده‌سازی PVLANها، باید اطمینان حاصل کنید که پیکربندی لایه‌ی ۳ در اینجا محدودیت‌هایی که توسط PVLAN اعمال می‌شود را پشتیبانی می‌کند و اجازه نمی‌دهد پیکربندی PVLAN با مسیریابی منحرف شود. محدودسازی لایه ۳ با استفاده از یک مسیریاب ACL یا دیواره‌ی آتش می‌تواند از عدم کارکرد صحیح پیکربندی PVLAN جلوگیری کند.

٤ مراجع

[1] R. F. J. Kevin Corbinr, “NX-OS and Cisco Nexus Switching”, USA: Cisco Press 800 East 2010.
[2] “Cisco Guide to Securing NX-OS Software Devices”, Available: https://www.cisco.com/c/en/us/about/security-center/securing-NX-OS.htm.
[3] “Cisco Nexus 7000 Series NX-OS Security Configuration Guide”, Release 5.x, USA: http://www.cisco.com, 2017.
[4] “Cisco Nexus switches”, https://en.wikipedia.org/wiki/Cisco_Nexus_switches.
[5] “White Paper: Cisco IOS and NX-OS Software Reference Guide”, Available: https://www.cisco.com/c/en/us/about/security-center/ios-NX-OS-reference-guide.html.