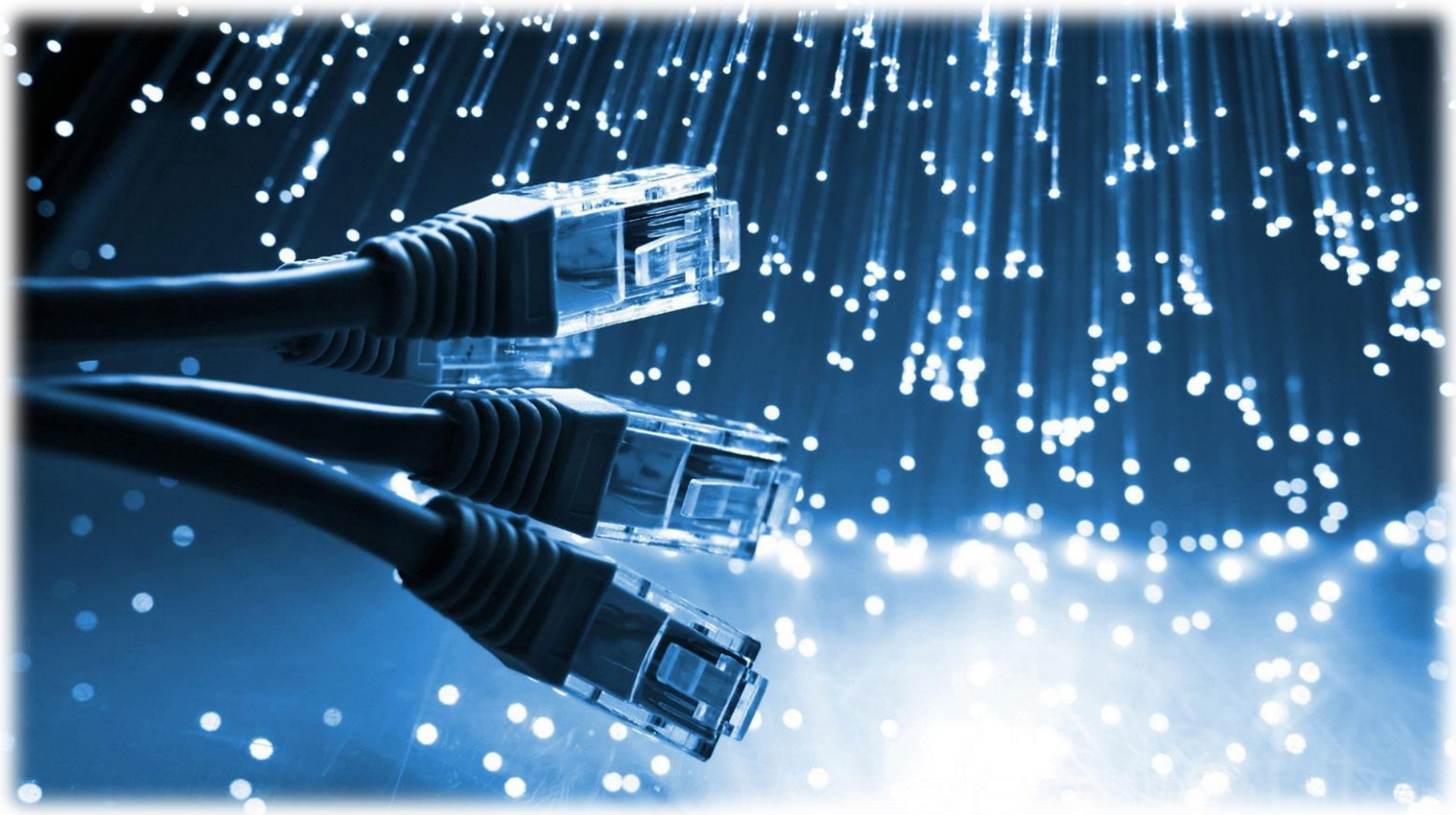
مرکز ماهر

مستند مرجع امن‌سازی

CISCO IOS 15



فهرست مطالب

مقدمه ۱

۱ واحد مدیریتی ۲

۱-۱ قوانین مدیریتی احراز هویت، مجوزهای دسترسی و حسابهای کاربری(AAA) ۲

۱-۱-۱ نحوه فعالسازی "AAA new-model" ۲

۱-۱-۲ نحوه فعالسازی "AAA authentication login" ۴

۱-۱-۳ فعالسازی "AAA authentication enable default" ۶

۱-۱-۴ تنظیم کردن "login authentication" برای "line con 0" ۷

۱-۱-۵ تنظیم کردن "login authentication" برای "line tty" ۸

۱-۱-۶ نحوه تنظیم کردن "login authentication" برای "line VTY" ۹

۱-۱-۷ نحوه فعالسازی "AAA accounting" برای ثبت تمام دسترسیهای انجام شده از طریق "commands 15" ۱۰

۱-۱-۸ نحوه فعالسازی و تنظیم "AAA accounting connection" ۱۱

۱-۱-۹ نحوه تنظیم "AAA accounting exec" ۱۳

۱-۱-۱۰ فعالسازی "AAA accounting network" ۱۵

۱-۱-۱۱ نحوه فعالسازی "AAA acounting" ۱۶

۱-۲ قوانین دسترسی ۱۷

۱-۲-۱ فعالسازی "privilege1" برای کاربران محلی ۱۷

۱-۲-۲ نحوه تنظیم "transport input SSH" برای کانکشنهای "line vty" ۱۸

۱-۲-۳ نحوه تنظیم "no exec" برای "line aux 0" ۱۹

۱-۲-۴ ایجاد "access-list" برای استفاده توسط "line vty" ۲۰

۱-۲-۵ نحوه تنظیم "access-class" برای "line vty" ۲۲

۱-۲-۶ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن آن به حدود ۱۰ دقیقه برای "line aux" ۲۳

۱-۲-۷ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن این بازه زمانی به حدود ۱۰ دقیقه برای "line console" ۲۴
۱-۲-۸ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن به حدود ۱۰ دقیقه برای "line tty" ۲۵
۱-۲-۹ تنظیم کردن "exec-timeout" به جهت کاهش و یا رساندن آن به حدود ۱۰ دقیقه برای "line vty" ۲۷
۱-۲-۱۰ نحوه تنظیم "transport input none" برای "line aux 0" ۲۹
۱-۳ قوانین اعلان ۳۱
۱-۳-۱ نحوه تنظیم کردن "banner-text" برای "banner exec"..... ۳۱
۱-۳-۲ نحوه تنظیم "banner-text" برای "banner login" ۳۳
۱-۳-۳ تنظیم "banner-text" برای "banner motd" ۳۵
۱-۴ قوانین مربوط به کلمات عبور ۳۷
۱-۴-۱ نحوه تنظیم "Password" برای "enable secret"..... ۳۷
۱-۴-۲ نحوه فعالسازی "service password-encryption"..... ۳۹
۱-۴-۳ نحوه تنظیم "username secret" برای تمام کاربران..... ۴۰
۱-۵ قوانین SNMP ۴۲
۱-۵-۱ نحوه تنظیم "NO SNMP-SERVER" برای غیرفعالسازی SNMP در مواقعی که نیازی به آن وجود ندارد. ۴۲
۱-۵-۲ نحوه تنظیم نکردن "private" برای "snmp-server community" ۴۳
۱-۵-۳ نحوه تنظیم نکردن "public" برای "snmp-server community" ۴۴
۱-۵-۴ نحوه تنظیم نکردن "RW" برای هر "snmp-server community" ..... - ۴۵ -
۱-۵-۵ نحوه تنظیم کردن ACL برای هر "snmp-server community" ۴۶
۱-۵-۶ نحوه ایجاد یک "access-list" برای SNMP..... ۴۷
۱-۵-۷ نحوه تنظیم "SNMP-Server Host" برای SNMP ۴۸
۱-۵-۸ نحوه تنظیم کردن "SNMP-Server enable traps SNMP" ۵۰
۱-۵-۹ نحوه فعالسازی "priv" برای هر "SNMP-Server Group" با استفاده از "SNMPv3"..... ۵۱
۱-۵-۱۰ در هنگام استفاده از SNMPv3، "AES 128" می‌تواند جزو کمترین نیاز برای "Server user SNMP" باشد..... ۵۲
۲ واحد کنترل ۵۳
۲-۱ قوانین سرویس سراسری ۵۳

۲-۱-۱ راهاندازی SSH ۵۳
۲-۱-۱-۱ تنظیمات مربوط به پیشنیازهای سرویس SSH ۵۴
۲-۱-۱-۱-۱ "Hostname" را تنظیم کنید ۵۴
۲-۱-۱-۱-۲ "ip domain name" را تنظیم کنید ۵۵
۲-۱-۱-۱-۳ مقدار "modulus" در "crypto key generate rsa" را بزرگتر یا مساوی 2048 تنظیم کنید ۵۶
۲-۱-۱-۱-۴ "seconds" را برای "ip ssh timeout" تنظیم کنید ۵۷
۲-۱-۱-۱-۵ مقدار بیشینه برای "ip ssh authentication-retries" را تنظیم کنید ۵۸
۲-۱-۱-۲ مقدار نسخه ۲ را برای "ip ssh version" تنظیم کنید ۵۹
۲-۱-۲ "no cdp run" را تنظیم کنید ۶۰
۲-۱-۳ "no ip bootp server" را تنظیم کنید ۶۱
۲-۱-۴ "no service dhcp" را تنظیم کنید ۶۲
۲-۱-۵ "no ip identd" را تنظیم کنید ۶۳
۲-۱-۶ "service tcp-keepalives-in" را تنظیم کنید ۶۴
۲-۱-۷ "service tcp-keepalives-out" را تنظیم کنید ۶۵
۲-۱-۸ "no service pad" را تنظیم کنید ۶۶
۲-۲ قوانین ثبت وقایع ۶۷
۲-۲-۱ "logging on" را تنظیم کنید ۶۸
۲-۲-۲ "buffer size" را برای "logging buffered" تنظیم کنید ۶۹
۲-۲-۳ "logging console critical" را تنظیم کنید ۷۰
۲-۲-۴ آدرس IP را برای "logging host" تنظیم کنید ۷۱
۲-۲-۵ "logging trap informational" را تنظیم کنید ۷۲
۲-۲-۶ "service timestamps debug datetime" را تنظیم کنید ۷۳
۲-۲-۷ "logging source interface" را تنظیم کنید ۷۴
۲-۳ قوانین NTP ۷۵
۲-۳-۱ کلیدهای رمزگذاری برای NTP را لازم بدانید ۷۵

۲-۳-۱-۱ "ntp authenticate" را تنظیم کنید ۷۶
۲-۳-۱-۲ "ntp authentication-key" را تنظیم کنید ۷۷
۲-۳-۱-۳ "ntp trusted-key" را تنظیم کنید ۷۸
۲-۳-۱-۴ "key" را برای هر "ntp server" تنظیم کنید ۷۹
۲-۳-۲ "ip address" را برای "ntp server" تنظیم کنید ۸۰
۲-۴ قوانین Loopback ۸۱
۲-۴-۱ یک "interface loopback" ایجاد نمایید ۸۲
۲-۴-۲ برای AAA "source-interface" را تنظیم نمایید ۸۳
۲-۴-۳ "ntp source" را به رابط loopback تنظیم نمایید ۸۴
۲-۴-۴ "ip tftp source-interface" را به رابط loopback تنظیم نمایید ۸۵
۳ واحد داده ۸۶
۳-۱ قوانین مسیردهی ۸۶
۳-۱-۱ نحوه تنظیم کردن "no ip source-route" ۸۷
۳-۱-۲ نحوه تنظیم "no ip proxy-arp" ۸۸
۳-۱-۳ نحوه فعالسازی "no interface tunnel" ۸۹
۳-۱-۴ نحوه تنظیم کردن "ip verify unicast source reachable-via" ۹۰
۳-۲ اعمال "border Router Filtering" ۹۱
۳-۲-۱ نحوه تنظیم "ip access-list extended" به جهت ممانعت از دسترسی آدرسهای خصوصی از شبکههای خارجی ۹۱
۳-۲-۲ نحوه تنظیم "ip access group" بر روی رابط خارجی ۹۳
۳-۳ Neighbor Authentication ۹۴
۳-۳-۱ نیاز به احراز هویت "EIGRP" در زمان استفاده از پروتکلهای مسیریابی ۹۴
۳-۳-۱-۱ نحوه تنظیم "key chain" ۹۵
۳-۳-۱-۲ نحوه فعالسازی "key" ۹۶
۳-۳-۱-۳ نحوه تنظیم کردن "key string" ۹۷

۳-۳-۱-۴ نحوه تنظیم کردن "address-family ipv4 autonomous-system" ۹۸
۳-۳-۱-۵ نحوه تنظیم نمودن "af-interface default" ۹۹
۳-۳-۱-۶ نحوه تنظیم نمودن "authentication key-chain" ۱۰۰
۳-۳-۱-۷ نحوه تنظیم کردن "authentication mode md5" ۱۰۱
۳-۳-۱-۸ نحوه تنظیم کردن "ip authentication key-chain eigrp" ۱۰۲
۳-۳-۱-۹ نحوه تنظیم کردن " ip authentication mode eigrp' " ۱۰۳
۳-۳-۲ نیاز به احراز هویت OSPF در پروتکلهای استفاده شده ۱۰۴
۳-۳-۲-۱ نحوه تنظیم نمودن "authentication message-digest" برای "OSPF area" ۱۰۴
۳-۳-۲-۲ نحوه تنظیم "ip ospf message-digest-key md5" ۱۰۵
۳-۳-۳ نیاز به احراز هویت RIPv2در پروتکلهای استفاده شده ۱۰۶
۳-۳-۳-۱ نحوه تنظیم نمودن "key chain" ۱۰۷
۳-۳-۳-۲ نحوه تنظیم نمودن "key" ۱۰۸
۳-۳-۳-۳ نحوه تنظیم نمودن "key-string" ۱۰۹
۳-۳-۴ نحوه تنظیم نمودن "ip rip authentication key chain" ۱۱۰
۳-۳-۵ نحوه تنظیم نمودن "ip rip authentication mode" به "md5" ۱۱۱
۳-۴ نیاز به احراز هویت BGP در پروتکلهای استفاده شده ۱۱۲
۳-۴-۱ تنظیمات مربوط به "neighbor password" ۱۱۳

قراردادهای تایپی

قراردادهای تایپی زیر در کل راهنما استفاده شده است:

قرارداد	معنی
فونت `Consolas`	برای بلوک کد، دستور و نمونه اسکریپت استفاده شده است. متن باید دقیقا به صورتی که نوشته شده است تفسیر شود. پس زمینه کرمی برای بررسی دستورات و پس زمینه سبز برای دستورات اصلاحی می‌باشد.
متن با حروف کج داخل براکت زاویه مانند *<LOCAL_USERNAME>*	متن کج داخل براکت زاویه نشان دهنده یک متغیر می‌باشد و نیازمند تعویض با یک مقدار واقعی است.

تشریح کاربست‌پذیری پروفایل

پیکربندی‌های مشخص شده در هر پروفایل می‌توانند در دو سطح زیر به کار روند:

- سطح ۱

برای پروفایل‌هایی که در این سطح قرار می‌گیرند، ویژگی‌های زیر را می‌توان معرفی نمود:

  - کاملا عملی و همراه با احتیاط هستند.
  - مزیت امنیتی واضح ارائه می‌دهند.
  - تامین کارایی و تکنولوژی فراتر از حد قابل قبول.

- سطح ۲

پروفایل‌های قرار گرفته در سطح ۲، نمونه‌های گسترش یافته پروفایل‌هایی هستند که در سطح ۱ دسته بندی می‌گردند. از جمله ویژگی‌های این دسته می‌توان به موارد زیر اشاره نمود:

  - برای محیط‌هایی که برقراری امن جزو مهم‌ترین مشخصه‌ها به شمار می‌رود، کاربرد این دسته بسیار مناسب تلقی می‌گردد.
  - به عنوان روش‌های دفاعی بسیار مناسب در مقابل آسیب‌پذیری‌ها تلقی می‌گردد.
  - در مواردی این دسته از پروفایل‌ها می‌توانند منجر به افت کارایی گردند.

جدول کلمات اختصاری

CDP	Cisco Discovery Protocol
HSRP	Hot Standby Router Protocol
STP	Spanning Tree Protocol
IKE	Internet Key Exchange
ICMP	Internet Control Message Protocol
NTP	Network Time Protocol
ARP	Address Resolution Protocol
IGMP	Internet Group Management Protocol
SSH	Secure Shell
Cisco IOS	Cisco Interconnect Operating System
RSA	Rivest Shamir Adleman
BOOTP	Bootstrap Protocol
DoS	Denial of Service
DHCP	Dynamic Host Configuration Protocol
PAD	Packet Assembler/Disassembler
AAA	Authentication Authorization Accounting
SNMP	Simple Network Management Protocol

RADIUS	Remote Authentication Dial-In User Service
TACACS+	Terminal Access Controller Access-Control System Plus
PPP	Point-to-Point Protocol
SLIP	Serial Line Internet Protocol
NCP	Network Control Program
AES	Advanced Encryption Standard

مقدمه

در یک شبکه تجهیزات گوناگونی از شرکت‌های مختلف با ویژگی‌های متفاوت وجود دارد که ایمن‌سازی آنها از اهمیت بسیار برخوردار است. همان‌طوری که می‌دانید شرکت سیسکو جزو شرکت‌های برتر در زمینه تولید محصولات مربوط به شبکه است که مکان مناسبی در بازار برای خود کسب کرده است. در این گفتار سعی داریم در مورد نحوه ایمن‌سازی سیستم عامل IOS سیسکو مطالب و دستورات پیکربندی را ارائه نماییم که پیاده-سازی آنها در IOS می‌تواند تا حد بالایی مفید واقع گردد. در اینجا قصد بررسی سیستم‌عامل IOS ورژن 15.0M که بر روی روترهای سیسکو عمل می‌کند را خواهیم داشت. پیکربندی‌هایی که در ادامه خواهید دید برای مدیران شبکه، متخصصان امنیتی و افرادی که قصد امن‌سازی شبکه خود را دارند کارا خواهد بود.

۱ واحد مدیریتی

واحد مدیریتی وظیفه دارد، سرویس‌ها، تنظیمات، مجوزهای عبور کاربران، جریان‌های داده‌ای مربوط به فایروال-های متصل به روتر سیسکو را به جهت ایمن‌سازی هر چه بیشتر بررسی نماید. برای انجام این کار واحد مدیریتی از پروتکل‌هایی نظیر SNMP و RADIUS و +TACACS استفاده می‌کند.در ادامه قصد داریم در مورد هر کدام از قوانینی که توسط واحد مدیریتی چک می‌شود، توضیحاتی را ارائه نماییم.

۱-۱ قوانین مدیریتی احراز هویت، مجوزهای دسترسی و حساب‌های کاربری(AAA)

قوانین مدیریتی در حوزه احراز هویت، مجوزهای دسترسی و کنترل حساب‌های کاربری به اختصار "AAA" نامیده می‌شود. معماری "AAA" به دنبال مکانیزمی برای یافتن تغییرات انجام شده و اجرای سیاست‌های امنیتی است.

۱-۱-۱ نحوه فعال‌سازی "AAA new-model"

کاربست‌پذیری[1] پروفایل:

- سطح ۱

توضیح: دستوری که در ادامه نشان خواهیم داد، سرویس"AAA new-model" را فعال خواهد نمود.

دلیل: معماری AAA یک منبع مدیریتی معتبری را برای کنترل دسترسی‌ها و نظارت بر نحوه دسترسی انجام گرفته، فراهم می‌آورد. به علاوه کنترل مرکزی AAA، نحوه دسترسی را بهبود می‌بخشد. از جمله سرویس‌های دیگری که واحد مدیریتی AAA در اختیار قرار می‌دهد، می‌توانیم به مواری هم‌چون کنترل حساب‌های کاربری و تصدیق آنها و نحوه دسترسی آنها به منابع، ساده کردن و کاهش هزینه‌های مربوط به ایجاد حساب‌های کاربری و مدیریت آنها، اشاره نماییم.

بررسی: با وارد کردن دستور زیر در محیط کامندی IOS می‌توانید از فعال بودن این سرویس مطلع شوید. در خروجی این دستور نمایش عبارت "No" به مفهوم غیرفعال بودن این سرویس است.

```
hostname# show running-config | incl aaa new-model
```

[1] Applicability

اصلاح: به جهت فعال‌سازی سرویس AAA در IOS از دستور زیر می‌توانید استفاده کنید.

```
hostname(config)# aaa new-model
```

تاثیر: پیاده‌سازی سرویس AAA به عنوان یک متد دسترسی، مخرب و زیان‌آور می‌تواند تلقی گردد، به همین خاطر در بیشتر IOSها این سرویس غیرفعال است. بنابراین قبل از فعال‌سازی AAA بایستی ضوابط و معیارهای مربوط به احراز هویت مانند رمزهای عبور، صفحات ورود، پاسخ‌های صادر شده، نیازمندی‌های مربوط به کاربران و متدهای دسترسی دوباره مورد بازبینی قرار گیرد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۲ نحوه فعال‌سازی "AAA authentication login"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: به جهت کنترل دسترسی و احراز هویت در صفحات ورود می‌توانیم از سرویس AAA استفاده نماییم.

دلیل: استفاده از سرویس AAA به جهت احراز هویت و برقراری ارتباط با دستگاه‌های مختلف و مدیریت مرکزی و جامع شبکه می‌تواند بسیار کارا تلقی گردد. اثری که این سرویس در این حوزه می‌تواند از خود نشان دهد، مواردی چون جلوگیری از ورود کاربران غیرمجاز با نام‌های کاربری و رمزهای ورود جعلی است. این قوانین تعبیه شده در سرویس AAA می‌تواند به صورت محلی و یا شبکه‌ای اجرا گردد. حالت جایگزین سناریو بالا می‌تواند مواقعی باشد که سرویس AAA در شبکه غیرقابل دسترس است و در این مواقع می‌توان به صورت محلی، اجازه دسترسی به روتر یا سوئیچ داده شود. برای مشخص کردن دسترسی محلی کافی است قبل از دستور مربوط به AAA، از کلمه کلیدی local استفاده نماییم.

بررسی: برای تشخیص فعال بودن سرویس AAA در صفحه ورود کافی است از دستور زیر استفاده کنید. اگر در پاسخ دستور، خروجی مشاهده نشد به معنی غیرفعال بودن این ویژگی است.

```
hostname# show run | incl aaa authentication login
```

اصلاح: برای فعال‌سازی این خصوصیت در IOS کافی است، دستور زیر وارد شود.

```
hostname(config)# aaa authentication login {default | aaa_list_name} [passwd-
expiry] method1 [method2]
```

تاثیر: همانند مواردی که در دستور مرحله قبل مطرح شد، در اینجا هم نقاط ضعفی هم‌چون آنها وجود دارند که برای غیرفعال‌سازی آن در IOS تصمیم‌گیری شده است. برای فعال کردن این سرویس بایستی ضوابط و معیارهای مربوط به احراز هویت مانند رمزهای عبور، صفحات login، پاسخ های صادر شده، نیازمندی‌های مربوط به کاربران و متدهای دسترسی دوباره مورد بازبینی قرار گیرند و سپس برحسب ضرورت و نیاز این سرویس فعال گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض مقدار این سرویس غیرفعال است.

۱-۱-۳ فعال‌سازی "AAA authentication enable default"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: احراز هویت کاربرانی که به مد EXEC دسترسی می‌یابند.

دلیل: استفاده از "AAA authentication enable default"برای برقراری تعامل و مدیریت دستگاه‌های موجود در شبکه توانایی برقراری مدیریت یکپارچه شبکه را فراهم می‌آورند و هم‌چنین از ورود و دسترسی‌های غیرمجاز تا حد بالایی چه به صورت محلی و چه به صورت دسترسی از طریق شبکه جلوگیری خواهد شد.

بررسی: به جهت فهمیدن فعال بودن سرویس "AAA authentication enable default" در سیستم عامل IOS ورژن ۱۵ از دستور زیر می‌توان استفاده کرد. در صورتی که در اجرای دستور خروجی دریافت نکردید به معنی غیرفعال بودن "AAA authentication enable default" است.

```
hostname#show running-config | incl aaa authentication enable
```

اصلاح: برای فعال‌سازی این سرویس کافی است از دستور زیر استفاده نمایید.

```
hostname(config)# aaa authentication enable default {method1} enable
```

تاثیر: با فعال‌سازی این سرویس امکان دارد موارد غیرقابل انتظاری در شبکه رخ دهد که برای جلوگیری از این موارد در اکثر حالات این سرویس به صورت پیش‌فرض غیرفعال است. بنابراین بایستی قبل از فعال کردن این سرویس مواردی نظیر مجوزهای دسترسی، کلمات عبور و... بررسی گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۴ تنظیم کردن "login authentication" برای "line con 0"

کاربست‌پذیری پروفایل

- سطح ۱

توضیح: کاربرانی که به سوئیچ‌ها و روترها از طریق پورت سریال کنسول دسترسی می‌یابند، بایستی اعتبارسنجی گردند.

دلیل: استفاده از سرویس احراز هویت کاربران که توسط سرویس "AAA" در اختیار قرار می‌گیرد، نکات مدیریتی مناسب و متمرکز را در شبکه پیاده‌سازی می‌نماید. استفاده از این سرویس نیاز به مجوزهایی با نام کاربری و کلمه عبور مناسب دارد. که چه در صورت دسترسی محلی و چه در صورت دسترسی از طریق شبکه بایستی رعایت گردد.

بررسی: با وارد کردن دستور زیر در محیط کامندی IOS خواهید فهمید که آیا این سرویس فعال است یا خیر. در صورتی که اجرای کد زیر خروجی نداشته باشد، به این معنی است که این سرویس در IOS غیرفعال است.

```
hostname#sh run | sec line | incl login authentication
```

اصلاح: در صورتی که بخواهید این سرویس را در IOS ورژن ۱۵ فعال نمایید، کافی است از دستورات زیر استفاده کنید. توجه نمایید که برای فعال‌سازی هر "line con" بایستی این دستورات را برای هر کدام وارد کنید. در دستورات زیر همان‌طور که مشاهده می‌نمایید، فقط "line console 0" فعال شده است.

```
hostname(config)#line console 0
hostname(config-line)#login authentication {default | aaa_list_name}
```

تاثیر: فعال‌سازی "line login" توسط "AAA" می‌تواند تبعات مدیریتی منفی را به بار آورد، به همین خاطر در اکثر سیستم‌عامل‌های IOS این سرویس غیرفعال است. مشخص است که برای فعال‌سازی این سرویس جنبه‌های منفی آن بایستی در نظر گرفته شود.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۵ تنظیم کردن "login authentication" برای "line tty"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اعتبارسنجی کاربرانی که به روترها و سوئیچ‌ها از طریق پورت TTY متصل می‌شوند.

دلیل: اعتبارسنجی انجام شده، توسط معماری AAA مدیریت و نظارت بر نحوه دسترسی متمرکز و جامعی را در اختیار مدیران شبکه قرار می‌دهد. به صورت پیش‌فرض سرویس AAA به کاربرانی که چه به صورت محلی و چه از طریق شبکه اقدام به دسترسی نموده‌اند با استفاده از نام کاربری و کلمات عبور معتبر اجازه دسترسی می-دهد.

بررسی: برای اینکه از فعال بودن یا نبودن این سرویس در سیستم‌عامل IOS مطلع شوید، کافی است از دستور زیر استفاده نمایید. در صورتی که اجرای دستور زیر نتیجه‌ای را به عنوان خروجی نداشته باشد، به مفهوم غیرفعال بودن سرویس مورد نظر خواهد بود.

```
hostname#sh run | sec line | incl login authentication
```

اصلاح: به جهت فعال‌سازی این سرویس بایستی از دستورات زیر استفاده نمایید. توجه کنید که برای فعال-سازی هر پورتی بایستی این دستور را برای تک تک آنها بنویسید.

```
hostname(config)#line tty {line-number} [ending-line-number]
hostname(config-line)#login authentication {default | aaa_list_name}
```

تاثیر: فعال‌سازی سرویس "AAA login authentication" برای پورت TTY می‌تواند در موارد کنترل نشده‌ای اثرات مخربی را بر جای بگذارد. به همین خاطر در بیشتر مواقع این سرویس در سیستم‌عامل IOS غیرفعال می‌باشد. بنابراین لازم است قبل از فعال‌سازی این سرویس جوانب انجام این کار بر روی نام‌های کاربران و کلمات عبور سنجیده شود.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۶ نحوه تنظیم کردن "login authentication" برای "line VTY"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اعتبارسنجی کاربرانی که به روترها و سوئیچ‌ها از طریق پورت VTY دسترسی پیدا می‌نمایند.

دلیل: استفاده از سرویس اعتبارسنجی AAA ویژگی‌هایی هم‌چون مدیریت متمرکز و جامعی را مهیا می‌نماید. این سرویس صحت نام‌های کاربری و کلمات عبور کاربرانی که به صورت محلی و یا از طریق شبکه به روترها و سوئیچ‌ها دسترسی پیدا می‌کنند، صحت‌سنجی می‌نمایند.

بررسی: برای تشخیص فعال بودن "AAA authentication" برای پورت VTY از دستور زیر می‌توانید استفاده نمایید. اگر اجرای این دستور خروجی را در پی نداشته باشد، به مفهوم غیرفعال بودن این سرویس است.

```
hostname#sh run | sec line | incl login authentication
```

اصلاح: در صورتی که بخواهید سرویس "AAA authentication" را برای پورت VTY فعال کنید، کافی است از طریق دسترسی مجاز AAA دستورات زیر را وارد نمایید.

```
hostname(config)#line vty {line-number} [ending-line-number]
hostname(config-line)#login authentication {default | aaa_list_name}
```

تاثیر: فعال‌سازی سرویس "AAA login authentication" برای پورت VTY می‌تواند در موارد کنترل نشده‌ای اثرات مخربی را بر جای بگذارد. به همین خاطر در بیشتر مواقع این سرویس در سیستم‌عامل IOS غیرفعال می‌باشد. بنابراین لازم است قبل از فعال‌سازی این سرویس جوانب انجام این کار بر روی نام‌های کاربران و کلمات عبور سنجیده شود.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۷ نحوه فعال‌سازی "AAA accounting" برای ثبت تمام دسترسی‌های انجام شده از طریق "commands 15"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: اعمال حسابرسی به تمامی دستوراتی که از سطح دسترسی مشخصی استفاده می‌نمایند.

دلیل: سیستم AAA که به جهت احراز هویت و اعتبارسنجی و حسابرسی استفاده می‌شود، منبع مدیریتی و نظارتی یکپارچه‌ای را برای دستگاه‌های مرتبط فراهم می‌نماید. استفاده از چنین منابع مدیریتی متمرکز، نحوه دسترسی کاربران را مدیریت و کنترل می‌کند. به علاوه چنین مدیریت و نظارت در شبکه‌های نسبتا بزرگ که از سمت این نوع معماری صادر می‌شود، می‌تواند منجر به ساده‌سازی کنترل و کاهش هزینه برای مدیران شبکه به جهت ایجاد حساب یا حذف یک حساب گردد. سیستم حسابرسی AAA از طریق "RADIUS" و "TACACS+" عملیات مدیریتی و اصلاح حساب‌ها را آسان نموده و مدیران شبکه را از قید پیچیدگی‌های ممکن رها می‌سازند.

بررسی: به جهت بررسی فعال و یا غیرفعال بودن این سرویس می توانید از دستور زیر استفاده نمایید.

```
hostname# sh run | incl aaa accounting commands
```

اصلاح: در صورت غیرفعال بودن این سرویس برای فعال‌سازی کافی است، از دستور زیر استفاده نمایید.

```
hostname (config)#aaa accounting commands 15 {default | list-name | guarantee-
first} {start-stop | stop-only | none} {radius | group group-name}
```

تاثیر: با فعال‌سازی سرویس "AAA accounting" برای تعیین سطوح دسترسی دستورات انجام گرفته و ثبت آنها در سرورهای مربوطه به جهت بررسی و آنالیز و نظارت بیشتر می‌توان استفاده نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۸ نحوه فعال‌سازی و تنظیم "AAA accounting connection"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: به جهت بدست آوردن اطلاعاتی در مورد کانکشن‌های خروجی از سمت سرور می‌توانید از این سرویس استفاده نمایید.

دلیل: سیستم AAA که به جهت احراز هویت و اعتبارسنجی و حسابرسی استفاده می‌شود، منبع مدیریتی و نظارتی یکپارچه‌ای را برای دستگاه‌های مرتبط فراهم می‌نماید. استفاده از چنین منابع مدیریتی متمرکز، نحوه دسترسی کاربران را مدیریت و کنترل می‌کند. به علاوه چنین مدیریت و نظارت در شبکه‌های نسبتا بزرگ که از سمت این نوع معماری صادر می‌شود، می‌تواند منجر به ساده‌سازی کنترل و کاهش هزینه برای مدیران شبکه به جهت ایجاد حساب یا حذف یک حساب گردد. سیستم حسابرسی AAA از طریق "RADIUS" و "TACACS+" عملیات مدیریتی و اصلاح حساب‌ها را آسان نموده و مدیران شبکه را از قید پیچیدگی‌های ممکن رها می‌سازند.

بررسی: به جهت آگاه شدن از فعال بودن یا نبودن این سرویس در سیستم‌عامل IOS ورژن ۱۵ می‌توانید از دستور زیر با یک نوع سطح دسترسی استفاده نمایید.

```
hostname#sh run | incl aaa accounting connection
```

اصلاح: در صورت غیرفعال بودن، می‌توانید به جهت فعال‌سازی از دستور زیر استفاده کنید.

```
hostname(config)#aaa accounting connection {default | list-name | guarantee-
first} {start-stop | stop-only | none} {radius | group group-name}
```

تاثیر: پیاده‌سازی و فعال کردن سیستم حسابرسی AAA تمامی اتصالات انجام گرفته به سرور را ثبت می‌نمایند. بنابراین سازمان بایستی این گزارشات منظم ثبت شده را برای یافتن استثناءها و مشکلات موجود بررسی نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۹ نحوه تنظیم "AAA accounting exec"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: از قابلیت این سیستم می‌توانیم به اعمال حسابرسی مربوط به EXEC اشاره کنیم.

دلیل: سیستم AAA که به جهت احراز هویت و اعتبارسنجی و حسابرسی استفاده می‌شود، منبع مدیریتی و نظارتی یکپارچه‌ای را برای دستگاه‌های مرتبط فراهم می‌نماید. استفاده از چنین منابع مدیریتی متمرکز، نحوه دسترسی کاربران را مدیریت و کنترل می‌کند. به علاوه چنین مدیریت و نظارت در شبکه‌های نسبتا بزرگ که از سمت این نوع معماری صادر می‌شود، می‌تواند منجر به ساده‌سازی کنترل و کاهش هزینه برای مدیران شبکه به جهت ایجاد حساب یا حذف یک حساب گردد. سیستم حسابرسی AAA از طریق "RADIUS" و "TACACS+" عملیات مدیریتی و اصلاح حساب‌ها را آسان نموده و مدیران شبکه را از قید پیچیدگی‌های ممکن رها می‌سازند.

بررسی: در صورتی که بخواهید از وضعیت این سیستم و فعال بودن حساب AAA برای EXEC مطلع شوید می‌توانید از دستور زیر استفاده نمایید.

```
hostname#sh run | incl aaa accounting exec
```

اصلاح: برای فعال کردن این سرویس می‌توانید از دستور زیر استفاده نمایید.

```
hostname(config)#aaa accounting exec {default | list-name | guarantee-first}
{start-stop | stop-only | none} {radius | group group-name}
```

تاثیر: فعال‌سازی و استفاده از این سرویس، امکان ثبت گزارش‌های مرتبط با EXEC را در طرف سرور فراهم می‌نمایند. اطلاعات ثبت شده شامل داده‌هایی چون زمان‌های شروع و خاتمه، نام‌های کاربری و برخی داده‌های مفید در ارتباط با دستگاه‌های مرتبط هستند. سازمان‌ها بایستی با آنالیز و بررسی این اطلاعات از وجود برخی مشکلات و استثناءها مطلع گردند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۱۰ فعال‌سازی "AAA accounting network"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: از این ویژگی می‌توان برای اعمال حسابرسی به تمام سرویس‌های درخواست مرتبط با شبکه استفاده نمود.

دلیل: سیستم AAA که به جهت احراز هویت و اعتبارسنجی و حسابرسی استفاده می‌شود، منبع مدیریتی و نظارتی یکپارچه‌ای را برای دستگاه‌های مرتبط فراهم می‌نماید. استفاده از چنین منابع مدیریتی متمرکز، نحوه دسترسی کاربران را مدیریت و کنترل می‌کند. به علاوه چنین مدیریت و نظارت در شبکه‌های نسبتا بزرگ که از سمت این نوع معماری صادر می‌شود، می‌تواند منجر به ساده‌سازی کنترل و کاهش هزینه برای مدیران شبکه به جهت ایجاد حساب یا حذف یک حساب گردد. سیستم حسابرسی AAA از طریق "RADIUS" و "TACACS+" عملیات مدیریتی و اصلاح حساب‌ها را آسان نموده و مدیران شبکه را از قید پیچیدگی‌های ممکن رها می‌سازند.

بررسی: به جهت بررسی فعال بودن این سرویس می‌توانیم از دستور زیر استفاده نماییم.

```
hostname#sh run | incl aaa accounting network
```

اصلاح: در صورت غیرفعال بودن این ویژگی می‌توانید با استفاده از دستور زیر آن را فعال نمایید.

```
hostname(config)#aaa accounting network {default | list-name | guarantee-first}
{start-stop | stop-only | none} {radius | group group-name}
```

تاثیر: پیاده‌سازی حسابرسی شبکه‌ای AAA، باعث ایجاد یکسری رکوردهای حسابرسی بر طبق ARA,PPP,SLIP,NCP می‌شود. برای بدست آوردن نتایج مطلوب، لازم است مدیران شبکه گزارش‌های جمع‌آوری شده را به دقت مطالعه کنند تا به وجود اشکالات و استثناءهای ممکن پی‌برند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۱-۱۱ نحوه فعال‌سازی "AAA acounting"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: پیاده‌سازی حسابرسی برای همه رویدادهای مربوط به سیستم که در ارتباط با رویدادهای مربوط به کاربران نیست. مانند رویدادهای مربوط به بارگذاری.

دلیل: سیستم AAA که به جهت احراز هویت و اعتبارسنجی و حسابرسی استفاده می‌شود، منبع مدیریتی و نظارتی یکپارچه‌ای را برای دستگاه‌های مرتبط فراهم می‌نماید. استفاده از چنین منابع مدیریتی متمرکز، نحوه دسترسی کاربران را مدیریت و کنترل می‌کند. به علاوه چنین مدیریت و نظارت در شبکه‌های نسبتا بزرگ که از سمت این نوع معماری صادر می‌شود، می‌تواند منجر به ساده‌سازی کنترل و کاهش هزینه برای مدیران شبکه به جهت ایجاد حساب یا حذف یک حساب گردد. سیستم حسابرسی AAA از طریق "RADIUS" و "TACACS+" عملیات مدیریتی و اصلاح حساب‌ها را آسان نموده و مدیران شبکه را از قید پیچیدگی‌های ممکن رها می‌سازند.

بررسی: به جهت تشخیص فعال بودن یا نبودن این سرویس می‌توان از دستور زیر استفاده نمود.

```
hostname#sh run | incl aaa accounting system
```

اصلاح: در صورت فعال نبودن این سرویس می‌توان از دستور زیر استفاده کرد.

```
hostname(config)#aaa accounting system {default | list-name | guarantee-first}
{start-stop | stop-only | none} {radius | group group-name}
```

تاثیر: با فعال‌سازی سیستم حسابرسی AAA، همانطور که اشاره نمودیم می‌تواند باعث ذخیره‌سازی داده‌های مرتبط با رویدادهای سمت سرور گردد. به جهت داشتن بهترین نوع کارایی بایستی، این داده‌ها توسط مدیران شبکه آنالیز و بررسی شود. تا در صورت رخ دادن هرگونه مشکل و استثناءهایی از آنها جلوگیری نماییم.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۲ قوانین دسترسی

قوانین در کلاس‌های دسترسی مختلف، منجر به اجرای ضابطه‌های کنترلی دررابطه با ارتباط دستگاه‌ها با هم-دیگر خواهد شد.

۱-۲-۱ فعال‌سازی "privilege1" برای کاربران محلی

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: این سرویس سطح دسترسی برای کاربران را تنظیم می‌نماید.

دلیل: پیکربندی اولیه دستگاه‌ها نیازی به احراز هویت قدرتمندی نخواهند داشت. در نتیجه این عمل می‌تواند منجر به حملات مختلفی از سمت نفوذگران گردد. ایجاد یک کاربر محلی با سطح دسترسی ۱ فقط به کاربر مربوطه امکان دسترسی به دستگاه با مجوز EXEC ارائه می‌نماید. با این سطح دسترسی کاربر موردنظر توانایی اعمال تغیرات را نخواهد داشت. برای اعمال تغیرات بایستی کلمه عبور معتبر رمزنگاری شده‌ای مورد استفاده قرار گیرد.

بررسی: برای بررسی فعال بودن این ویژگی کافی است از دستور زیر در IOS ورژن ۱۵ استفاده نمایید.

```
hostname#show run | incl privilege
```

اصلاح: برای فعال‌سازی این سرویس می‌توانید از دستور زیر استفاده نمایید.

```
hostname(config)#username <LOCAL_USERNAME> privilege 1
```

تاثیر: سازمان‌ها بایستی یکسری سیاست‌های لازم برای ایجاد کاربرانی با سطح دسترسی ۱ و کلمات عبور رمزنگاری شده، اقدام نمایند. تا به این طریق از خطرات مرتبط با دسترسی‌های غیرمجاز جلوگیری کنند. پیکربندی‌های اولیه فاقد چنین تنظیماتی هستند.

۱-۲-۲ نحوه تنظیم "transport input SSH" برای کانکشن‌های "line vty"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: انتخاب پروتکل SSH

دلیل: از پیکربندی VTY برای دسترسی غیرمستقیم و از راه دور به دستگاه‌ها استفاده می‌شود و به این ترتیب از دسترسی غیرمجاز تا حد بالایی جلوگیری می‌شود.

بررسی: با استفاده از دستور زیر می‌توانید از وجود پروتکل SSH در ارتباط با پورت VTY مطلع شوید.

```
hostname#sh run | sec vty
```

اصلاح: برای فعال‌سازی این سرویس می‌توانید از دستور زیر استفاده نمایید.

```
hostname(config)#line vty <line-number> <ending-line-number>
hostname(config-line)#transport input ssh
```

تاثیر: برای کاهش خطرات مرتبط با دسترسی‌های غیرمجاز یک سازمان بایستی از پروتکل‌های SSH برای دسترسی به پورت‌های VTY استفاده نماید.

۱-۲-۳ نحوه تنظیم "no exec" برای "line aux 0"

کاربست‌پذیری پروفایل:

- **سطح ۱**

توضیح: استفاده از دستور "no exec" برای محدود ساختن میزان دسترسی‌ها صورت می‌گیرد.

دلیل: پورت‌های غیرقابل استفاده به دلیل اینکه مسیری برای نفوذ فراهم می‌آورند، بایستی غیرفعال گردند. برخی از دستگاه‌های جانبی و پورت‌های کنسولی می توانند برای دسترسی محلی و پیکربندی دستگاه‌ها استفاده گردند. پورت‌های کنسولی به صورت نرمال جزو پورت‌هایی است که برای اعمال پیکربندی و تنظیمات از آن حتی به صورت غیرمستقیم می‌توان استفاده کرد. از پورت‌های کمکی برای دسترسی از طریق dial-up استفاده می‌شود.

بررسی: با استفاده از دستور زیر می‌توان فهمید که آیا EXEC برای پورت کمکی، غیرفعال است یا خیر. در صورت غیرفعال بودن عبارت "no exec" نشان داده می‌شود.

```
hostname#sh run | sec aux
hostname#sh line aux 0 | incl exec
```

اصلاح: در صورت فعال بودن این سرویس کافیست، با استفاده از دستور زیر آن را غیرفعال کنید.

```
hostname(config)#line aux 0
hostname(config-line)#no exec
```

تاثیر: سازمان‌ها با استفاده از دستور "no exec" می‌توانند، خطرات ناشی از دسترسی غیرمجاز از طریق پورت "aux" را به حداقل برسانند. در مقابل دسترسی کاربران مجاز از طریق این پورت همانند گذشته می‌تواند انجام شود.

۱-۲-۴ ایجاد "access-list" برای استفاده توسط "line vty"

کاربست‌پذیری پروفایل:

- **سطح ۱**

توضیح: لیست دسترسی انتقال پکت‌ها در یک اینترفیس مشخص و دسترسی به پورت "vty" کنترل می‌کند. بعلاوه میزان بروزرسانی پکت‌های مربوط به مسیردهی را محدود می‌نماید. نرم‌افزار cisco IOS بعد از یافتن یک هم‌خوانی، چک کردن لیست دسترسی توسعه‌یافته را متوقف می‌سازد.

دلیل: "VTY ACLs" آدرس‌هایی که تلاش می‌نمایند تا به روترها دسترسی پیدا کنند، ثبت و آنها را کنترل می‌کند. نحوه پیکربندی پورت VTY برای استفاده توسط ACL به گونه‌ای است که دسترسی کاربران به منابع حساس را مدیریت و آنها را محدود می‌سازد. شما بایستی کاربرانی که سعی دارند پیکربندی‌های یک دستگاه مشخص را تغییر دهند، محدود سازید. برای انجام این کار می‌توانید از یکسری پروتکل‌های مشخصی استفاده کنید. برای مثال، شما قادر به محدود ساختن آن دسته از دسترسی‌هایی خواهید بود که سعی دارند به host مشخصی دسترسی یافته و تنظیمات مورد نظر خود را روی آنها اعمال نمایند. به همین خاطر تمام پورت‌های VTY بایستی از یک ACL استفاده نمایند.

بررسی: از دستور زیر می‌توان استفاده کرد تا تشخیص دهیم که آیا ACL ایجاد شده است یا خیر. توجه داشته باشید که بایستی لیست دسترسی را برای انجام این کار بررسی نمایید.

```
hostname#sh ip access-list <vty_acl_number>
```

اصلاح: با دستورات زیر می‌توانید دسترسی به یک دستگاه مشخص را از طریق پورت "VTY ACL" محدود سازید.

```
hostname(config)#access-list <vty_acl_number> permit tcp <vty_acl_block_with_mask> any
hostname(config)#access-list <vty_acl_number> permit tcp host <vty_acl_host> any
hostname(config)#deny ip any any log
```

تاثیر: سازمان‌ها بایستی دسترسی غیرمجاز به یک منبع را محدود سازند. این کار همان‌طور که اشاره نمودیم با ایجاد یک لیست دسترسی VTY انجام می‌شود. در مقابل استفاده از پورت VTY بدون داشتن لیست دسترسی خطرات ناشی از دسترسی غیرمجاز را افزایش می‌دهد.

۱-۲-۵ نحوه تنظیم "access-class" برای "line vty"

کاربست‌پذیری پروفایل:

- **سطح ۱**

توضیح: تنظیمات "access-class" جریان‌های داده‌ای ورودی و خروجی از طریق پورت vty به تجهیزات cisco را از طریق لیست دسترسی محدود می‌سازد.

دلیل: در لیست دسترسی که برای یک دستگاه سیسکو در شبکه ایجاد می‌کنیم با توجه به آدرس دستگاه در شبکه و آدرس کاربران غیرمجاز دسترسی به منابع را محدود می‌سازیم.

بررسی: برای بررسی اینکه که ACL فعال است یا نه. می‌توانید از دستور زیر استفاده کنید. توجه کنید که بایستی لیست دسترسی تعریف شده با اجرای این دستور بررسی شود.

```
hostname#sh run | sec vty <line-number> <ending-line-number>
```

اصلاح: با استفاده از دستور زیر می‌توانید دسترسی به یک دستگاه از طریق پورت VTY را محدود نمایید.

```
hostname(config)#line vty <line-number> <ending-line-number>
hostname(config-line)# access-class <vty_acl_number> in
```

تاثیر: با اعمال "access class" به پورت vty باعث محدود ساختن بیشتر دسترسی‌ها به دستگاه می‌گردد و خطرات ناشی از دسترسی غیرمجاز را بسیار کاهش می‌دهد.

۱-۲-۶ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن آن به حدود ۱۰ دقیقه برای "line aux"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اگر در فاصله زمانی معینی جریان ورودی مشخصی صورت نگیرد، یکی از قابلیت‌های exec این است که اقدام به متوقف کردن ارتباطی که از طریق پورت صورت گرفته است می‌کند.

دلیل: این اقدام می‌تواند تا حد بسیار زیادی دسترسی‌های غیرمجاز صورت گرفته را لغو سازد. برای مثال، اگر مدیر شبکه سیستم کامپیوتری خود را که بدون رمز ورود است، به مدت یک روز روشن رها سازد در صورت تعیین بازه زمانی مناسب قفلی بر روی سیستم اعمال شده و از دسترسی‌های غیرمجاز می‌توان جلوگیری نمود. برای مطلع شدن از این حالت و بازه‌های زمانی تعریف شده به سیاست‌های محلی در چارچوب سازمانتان مراجعه فرمایید. در بسیاری از مواقع این فاصله زمانی ۱۰ دقیقه یا کمتر تعریف شده است.

بررسی: با اعمال دستور زیر می‌توانید تشخیص دهید که آیا بازه زمانی در سیستم‌عامل تعریف شده است یا خیر. فقط به نکته‌ای بایستی توجه نمود که در صورتی که بازه زمانی exec به مدت ۱۰ دقیقه تعریف شده باشد، این مقدار در پیکربندی نمایش داده نخواهد شد.

```
hostname#sh run | sec line aux 0
```

اصلاح: در صورت تمایل، می‌توانید در مواقعی که برای مدت زمان مشخصی از سیستم استفاده نمی‌کنید ارتباطتان قطع گردد. برای انجام این کار با استفاده از دستور زیر این بازه زمانی را بر حسب دقیقه وارد نمایید.

```
hostname(config)#line aux 0
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

تاثیر: سازمان‌ها بایستی از استفاده غیرمجاز با کنترل و متوقف کردن sessionsهای ایجاد شده، پیشگیری نمایند.

۱-۲-۷ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن این بازه زمانی به حدود ۱۰ دقیقه برای "line console"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اگر در فاصله مشخص جریان ورودی معینی صورت نگیرد، یکی از قابلیت‌های exec می‌تواند اقدام به متوقف نمودن ارتباطی که از طریق پورت صورت گرفته است، باشد.

دلیل: این اقدام می‌تواند تا حد بسیار زیادی دسترسی‌های غیرمجاز صورت گرفته را لغو سازد. برای مثال، اگر مدیر شبکه سیستم کامپیوتری خود را که بدون رمز ورود است، به مدت یک روز روشن رها سازد در صورت تعیین بازه زمانی مناسب قفلی بر روی سیستم اعمال شده و از دسترسی‌های غیرمجاز می‌توان جلوگیری نمود. برای مطلع شدن از این حالت و بازه‌های زمانی تعریف شده به سیاست‌های محلی در چارچوب سازمانتان مراجعه فرمایید. در بسیاری از مواقع این فاصله زمانی ۱۰ دقیقه یا کمتر تعریف شده است.

بررسی: با اعمال دستور زیر می‌توانید تشخیص دهید که آیا بازه زمانی در سیستم‌عامل تعریف شده است یا خیر. فقط به نکته‌ای که بایستی توجه کرد این است که در صورتی که بازه زمانی به مدت ۱۰ دقیقه تعریف شده باشد، این مقدار در پیکربندی نمایش داده نخواهد شد.

```
hostname#sh run | sec line con 0
```

اصلاح: در صورت تمایل، می‌توانید در مواقعی که برای مدت زمان مشخصی از سیستم استفاده نمی‌کنید ارتباطتان قطع گردد. برای انجام این کار با استفاده از دستور زیر این بازه زمانی را بر حسب دقیقه وارد نمایید.

```
hostname(config)#line con 0
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

تاثیر: سازمان‌ها بایستی از دسترسی‌های غیرمجاز با کنترل و متوقف کردن sessionsها پیشگیری نمایند. با فعال‌سازی "exec-timeout" می‌توان تا حد بالایی از دسترسی‌های غیرمجاز جلوگیری کنیم.

۱-۲-۸ نحوه تنظیم "exec-timeout" به جهت کاهش و یا رساندن به حدود ۱۰ دقیقه برای " line tty"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اگر در فاصله زمانی معینی جریان ورودی معینی صورت نگیرد، یکی از قابلیت‌های exec این است که اقدام به متوقف کردن ارتباطی که از طریق پورت صورت گرفته است می‌کند. اگر کانکشنی وجود نداشته باشد خصوصیت exec حالت ترمینال را به صورت بیکار نشان می‌دهد و session مربوط به کانکشن ورودی را قطع خواهد کرد.

دلیل: این اقدام می‌تواند تا حد بسیار زیادی دسترسی‌های غیرمجاز صورت گرفته را لغو سازد. برای مثال، اگر مدیر شبکه سیستم کامپیوتری خود را که بدون رمز ورود است، به مدت یک روز روشن رها سازد در صورت تعیین بازه زمانی مناسب قفلی بر روی سیستم اعمال شده و از دسترسی‌های غیرمجاز می‌توان جلوگیری نمود. برای مطلع شدن از این حالت و بازه‌های زمانی تعریف شده به سیاست‌های محلی در چارچوب سازمانتان مراجعه فرمایید. در بسیاری از مواقع این فاصله زمانی ۱۰ دقیقه یا کمتر تعریف شده است.

بررسی: با اعمال دستور زیر می‌توانید تشخیص دهید که آیا بازه زمانی در سیستم‌عامل تعریف شده است یا خیر. فقط به نکته‌ای که بایستی توجه کرد این است که در صورتی که بازه زمانی به مدت ۱۰ دقیقه تعریف شده باشد، این مقدار در پیکربندی نمایش داده نخواهد شد.

```
hostname#sh line tty <tty_line_number> | begin Timeout
```

اصلاح: در صورت تمایل، می‌توانید با اجرای دستور زیر، در مواقع پایان بازه زمانی (۱۰دقیقه یا کمتر) ارتباط را به صورت خودکار قطع نمایید.

```
hostname(config)#line tty {line_number} [ending_line_number]
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

تاثیر: سازمان‌ها بایستی از دسترسی غیرمجاز با کنترل و متوقف نمودن sessionsها پیشگیری نمایند. با فعال-سازی "exec-timeout" می‌توان تا حد بالایی از دسترسی‌های غیرمجاز جلوگیری نماییم.

۱-۲-۹ تنظیم کردن "exec-timeout" به جهت کاهش و یا رساندن آن به حدود ۱۰ دقیقه برای " line vty"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اگر در فاصله مشخص جریان ورودی مشخصی صورت نگیرد، یکی از قابلیت‌های exec این است که اقدام به متوقف کردن ارتباطی که از طریق پورت صورت گرفته است می‌کند. اگر کانکشنی وجود نداشته باشد، خصوصیت exec حالت ترمینال را به صورت بیکار نشان می‌دهد و session مربوط به کانکشن ورودی را قطع خواهد کرد.

دلیل: این اقدام می‌تواند تا حد بسیار زیادی دسترسی‌های غیرمجاز صورت گرفته را لغو سازد. برای مثال، اگر مدیر شبکه سیستم کامپیوتری خود را که بدون کلمه عبور است، به مدت یک روز روشن رها سازد در صورت تعیین بازه زمانی مناسب قفلی بر روی سیستم اعمال شده و از دسترسی‌های غیرمجاز می‌توان جلوگیری نمود. برای مطلع شدن از این حالت و بازه‌های زمانی تعریف شده به سیاست‌های محلی در چارچوب سازمانتان مراجعه فرمایید. در بسیاری از مواقع این فاصله زمانی ۱۰ دقیقه یا کمتر تعریف شده است.

بررسی: با اعمال دستور زیر می‌توانید تشخیص دهید که آیا بازه زمانی در سیستم‌عامل تعریف شده است یا خیر. فقط به نکته‌ای که بایستی توجه کرد این است که در صورتی که بازه زمانی به مدت ۱۰ دقیقه تعریف شده باشد، این مقدار در پیکربندی نمایش داده نخواهد شد.

```
hostname#sh line vty <tty_line_number> | begin Timeout
```

اصلاح: در صورت تمایل، می‌توانید با اجرای دستور زیر در مواقع پایان بازه زمانی و در مواقع بیکاری (۱۰دقیقه یا کمتر) ارتباط را به صورت خودکار قطع نمایید.

```
hostname(config)#line vty {line_number} [ending_line_number]
hostname(config-line)#exec-timeout <timeout_in_minutes> <timeout_in_seconds>
```

تاثیر: سازمان‌ها بایستی از دسترسی غیرمجاز با کنترل و متوقف نمودن sessionsها جلوگیری نمایند. با فعال-سازی "exec-timeout" می‌توان تا حد بالایی از دسترسی‌های غیرمجاز جلوگیری کنیم.

۱-۲-۱۰ نحوه تنظیم "transport input none" برای "line aux 0"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: در مواقعی که بخواهید فقط به داده‌های مربوط به جریان‌های ورودی اجازه عبور دهید، کافی است از دستور "no exec" استفاده نمایید.

دلیل: پورت‌های غیرقابل استفاده بایستی در صورت عدم نیاز غیرفعال باشند، چون این پورت‌های می‌توانند مسیری برای نفوذگران فراهم نمایند. برخی از دستگاه‌ها شامل یکسری پورت‌های اصلی و یا کمکی برای اتصال محلی و اعمال پیکربندی هستند. پورت‌های کنسولی جزو پورت‌های اولیه برای انجام پیکربندی دستگاه است. زمانی که بخواهیم از طریق دسترسی از راه دور برای انجام کارهایی نظیر پشتیبان‌گیری و.... اقدام نماییم، از پورت‌های کنسولی استفاده خواهیم کرد. از پورت‌های کمکی برای انجام کارهایی نظیر dial-up می‌کنیم.

بررسی: از دستور زیر می‌توان برای تشخیص غیرفعال بودن پورت‌های کمکی و جریان‌های ورودی مربوط به این پورت‌ها استفاده نمود. در صورت غیرفعال بودن این پورت‌ها عبارت "Allow transports are none" نمایش داده می‌شود.

```
hostname#sh line aux 0 | incl input transports
```

اصلاح: برای غیرفعال‌سازی داده‌های مربوط به جریان‌های ورودی از پورت‌های کمکی، می‌توانید از دستور زیر استفاده کنید.

```
hostname(config)#line aux 0
hostname(config-line)#transport input none
```

تاثیر: سازمان‌ها بایستی با غیرفعال کردن جریان‌های صادر شده از پورت‌های کمکی، از دسترسی‌های غیرمجاز جلوگیری نمایند. همان‌طور که مشاهده نمودید، این دستور در بالا با عبارت "transport input none" مشخص شده است.


مرکز ماهر

۱-۳ قوانین اعلان

در این قسمت قصد داریم در مورد قوانین مربوط به کاربران مجاز و اعلان‌هایی که قرار است به این کاربران در هنگام انجام کارهای معینی نمایش داده شود، سخن گوییم.

۱-۳-۱ نحوه تنظیم کردن "banner-text" برای "banner exec"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: دستوری که در ادامه معرفی خواهیم کرد، اعلانی را در هنگامی که پردازش exec ایجاد می‌شود، به کاربران نمایش خواهد داد. در این دستور، باگذاشتن فاصله‌های خالی و با استفاده از کاراکترهای جدا کننده مورد نظر می‌توانید چارچوبی را که قرار است نمایش داده شود، تنظیم کنید. در ادامه می‌توانید متن پیام مورد نظر خود را بیاورید و در آخر با استفاده از کاراکترهای جدا کننده دستور را خاتمه دهید. زمانی که یک کاربر به یک روتر متصل می‌شود، در ابتدا پیام "MOTD" نمایش داده می‌شود که نحوه "login" را مشخص خواهد نمود. بعد از اینکه کاربر با استفاده از نام کاربری و کلمات عبور وارد محیط پیکربندی روتر شد، بر اساس نوع ارتباط محتویات مربوط به EXEC به کاربر نشان داده می‌شود. برای ورود به محیط پیکربندی روتر با استفاده از دستور telnet دوباره بایستی، پیام تنظیم شده به کاربر نشان داده شود.

دلیل: network banner یک پیام الکترونیکی بوده و حاوی قوانینی در ارتباط با کاربرانی است که به صورت مجاز به صفحه پیکربندی وارد شده‌اند. از نقطه نظر قانونی، این پیام‌ها حاوی ۴ کاربرد اولیه و اساسی می‌باشند.

۱. از پیام‌ها برای تولید محتوای مانیتورینگ بلادرنگ استفاده می‌شود.
۲. از پیام‌ها برای اجازه بازیابی و تولید فایل‌های ذخیره شده بر طبق ECPA استفاده می‌شود.
۳. در یک شبکه دولتی پیام‌ها برای نمایش دادن چارچوب و قوانینی که بایستی از طرف کارکنان سازمان و افراد دیگر رعایت گردد، استفاده می‌شود.
۴. در یک شبکه غیردولتی از پیام‌ها برای منتشر کردن قوانین مدنظر مدیر شبکه که بایستی از طرف اعضا رعایت گردد، استفاده می‌شود.

بررسی: برای تشخیص اینکه آیا این پیام در IOS تنظیم شده است یا خیر، می‌توانید از دستور زیر استفاده نمایید. در صورتی که چنین تنظیماتی در نظر گرفته نشده باشد، اجرای دستور زیر خروجی را در پی نخواهد داشت.

```
hostname#sh running-config | beg banner exec
```

اصلاح: برای پیکربندی IOS به جهت نمایش اعلان EXEC به کاربران در هنگام دسترسی به دستگاه مشخص می‌توانید از دستور زیر را استفاده کنید.

```
hostname(config)#banner login c Enter TEXT message.
End with the character “c”.
 <banner-text>
 c
```

تاثیر: سازمان‌ها برای هشدار دادن و اطلاع‌رسانی به کاربران مجاز که به شبکه دسترسی می‌یابند، بایستی از طریق دستور "banner-text" برای تنظیم پیام‌ها اقدام نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۳-۲ نحوه تنظیم "banner-text" برای "banner login"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: دستوری که در ادامه معرفی خواهیم کرد، اعلانی را در هنگامی که پردازش exec ایجاد می‌شود، به کاربران نمایش خواهد داد. در این دستور، باگذاشتن فاصله‌های خالی و با استفاده از کاراکترهای جدا کننده مورد نظر می‌توانید چارچوبی را که قرار است نمایش داده شود، تنظیم کنید. در ادامه می‌توانید متن پیام مورد نظر خود را بیاورید و در آخر با استفاده از کاراکترهای جدا کننده دستور را خاتمه دهید. زمانی که یک کاربر به یک روتر متصل می‌شود، در ابتدا پیام "MOTD" نمایش داده می‌شود که نحوه "login" را مشخص خواهد نمود. بعد از اینکه کاربر با استفاده از نام کاربری و کلمات عبور وارد محیط پیکربندی روتر شد، بر اساس نوع ارتباط محتویات مربوط به EXEC به کاربر نشان داده می‌شود. برای ورود به محیط پیکربندی روتر با استفاده از دستور telnet دوباره بایستی، پیام تنظیم شده به کاربر نشان داده شود.

دلیل: network banner یک پیام الکترونیکی بوده و حاوی قوانینی در ارتباط با کاربرانی است که به صورت مجاز به صفحه پیکربندی وارد شده‌اند. از نقطه نظر قانونی، این پیام‌ها حاوی ۴ کاربرد اولیه و اساسی می‌باشند.

۱. از پیام‌ها برای تولید محتوای مانیتورینگ بلادرنگ استفاده می‌شود.
۲. از پیام‌ها برای اجازه بازیابی و تولید فایل‌های ذخیره شده بر طبق ECPA استفاده می‌شود.
۳. در یک شبکه دولتی پیام‌ها برای نمایش دادن چارچوب و قوانینی که بایستی از طرف کارکنان سازمان و افراد دیگر رعایت گردد، استفاده می‌شود.
۴. در یک شبکه غیردولتی از پیام‌ها برای منتشر کردن قوانین مدنظر مدیر شبکه که بایستی از طرف اعضا رعایت گردد، استفاده می‌شود.

بررسی: برای تشخیص اینکه آیا این پیام در IOS تنظیم شده است یا خیر، می‌توانید از دستور زیر استفاده نمایید. در صورتی که چنین تنظیماتی در نظر گرفته نشده باشد، اجرای دستور زیر خروجی را در پی نخواهد داشت.

```
hostname# show running-config | beg banner login
```

اصلاح: در صورت غیرفعال بودن این سرویس از طریق دستور زیر می‌توانید چارچوب اعلانی که قرار است به کاربرانی که سعی می‌کنند به منابع دسترسی داشته باشند، تنظیم کرد.

```
hostname(config)#banner login c
Enter TEXT message. End with the character 'c'.
<banner-text>
 c
```

تاثیر: سازمان‌ها برای هشدار دادن و اطلاع‌رسانی به کاربران مجازی که به شبکه دسترسی می‌یابند، بایستی از طریق دستور "banner-text" برای تنظیم پیام‌ها اقدام نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۳-۳ تنظیم "banner-text" برای "banner motd"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: دستوری که در ادامه معرفی خواهیم کرد، اعلانی را در هنگامی که پردازش exec ایجاد می‌شود، به کاربران نمایش خواهد داد. در این دستور، باگذاشتن فاصله‌های خالی و با استفاده از کاراکترهای جدا کننده مورد نظر می‌توانید چارچوبی را که قرار است نمایش داده شود، تنظیم کنید. در ادامه می‌توانید متن پیام مورد نظر خود را بیاورید و در آخر با استفاده از کاراکترهای جدا کننده دستور را خاتمه دهید. زمانی که یک کاربر به یک روتر متصل می‌شود، در ابتدا پیام "MOTD" نمایش داده می‌شود که نحوه "login" را مشخص خواهد نمود. بعد از اینکه کاربر با استفاده از نام کاربری و کلمات عبور وارد محیط پیکربندی روتر شد، بر اساس نوع ارتباط محتویات مربوط به EXEC به کاربر نشان داده می‌شود. برای ورود به محیط پیکربندی روتر با استفاده از دستور telnet دوباره بایستی، پیام تنظیم شده به کاربر نشان داده شود.

دلیل: network banner یک پیام الکترونیکی بوده و حاوی قوانینی در ارتباط با کاربرانی است که به صورت مجاز به صفحه پیکربندی وارد شده‌اند. از نقطه نظر قانونی، این پیام‌ها حاوی ۴ کاربرد اولیه و اساسی می‌باشند.

۱. از پیام‌ها برای تولید محتوای مانیتورینگ بلادرنگ استفاده می‌شود.
۲. از پیام‌ها برای اجازه بازیابی و تولید فایل‌های ذخیره شده بر طبق ECPA استفاده می‌شود.
۳. در یک شبکه دولتی پیام‌ها برای نمایش دادن چارچوب و قوانینی که بایستی از طرف کارکنان سازمان و افراد دیگر رعایت گردد، استفاده می‌شود.
۴. در یک شبکه غیردولتی از پیام‌ها برای منتشر کردن قوانین مدنظر مدیر شبکه که بایستی از طرف اعضا رعایت گردد، استفاده می‌شود.

بررسی: برای تشخیص اینکه آیا این پیام در IOS تنظیم شده است یا خیر، می‌توانید از دستور زیر استفاده نمایید. در صورتی که چنین تنظیماتی در نظر گرفته نشده باشد، اجرای دستور زیر خروجی را در پی نخواهد داشت.

```
hostname#sh running-config | beg banner motd
```

اصلاح: همان‌طوری که اشاره نمودیم اعلان "MOTD" بایستی در اولین بار متصل شدن کاربر نمایش داده شود. این اعلان را می‌توانیم، به صورت زیر تنظیم کنیم.

```
hostname(config)#banner motd c
Enter TEXT message. End with the character 'c'.
<banner-text>
 c
```

تاثیر: سازمان‌ها برای هشدار دادن و اطلاع‌رسانی به کاربران مجازی که به شبکه دسترسی می‌یابند، بایستی از طریق دستور "banner-text" برای تنظیم اعلان‌ها اقدام نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۴ قوانین مربوط به کلمات عبور

در قوانین مربوط به کلمات عبور تلاش برای ایمن ساختن و محفوظ نگه‌داشتن هرچه بیشتر آنها است.

۱-۴-۱ نحوه تنظیم "Password" برای "enable secret"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: استفاده از دستور "enable secret" باعث ایجاد یک لایه امنیتی اضافی برای فعال‌سازی کلمات عبور می‌شود. دستور "enable secret" بهترین نوع امنیت را با استفاده از توابع رمزنگاری مهیا می‌نماید.
این لایه امنیتی رمزنگاری شده، افرادی را که سعی می‌نمایند کلمات عبور را جعل نمایند، رفتار آنها را در سرور-های تعبیه شده ذخیره می‌نماید.

دلیل: یکی از نیازهای دستور "enable secret" دسترسی به مد exec می‌باشد. در مقدار پیش‌فرض کلمات عبور قدرتمندی تعیین نشده است و کاربران با فشار دادن کلید enter در قسمت مربوط به کلمه عبور می‌توانند وارد محیط پیکربندی شوند. با استفاده از دستوراتی که باعث فعال شدن کلمات عبور می‌گردند، می‌توانیم کاربران را به کار بردن کلمات عبور ملزم سازیم. نحوه رمزنگاری کلمات عبور با استفاده از الگوریتم‌هایی چون md5 صورت می‌گیرد که باعث ایجاد لایه‌های امنیتی مناسب می‌گردند و از به کار بردن کلمات عبور ضعیف جلوگیری می‌نمایند.

بررسی: از دستور زیر می‌توانید استفاده نمایید تا از فعال بودن یا نبودن سرویس "enable secret" مطلع شوید. در صورتی که اجرای دستور خروجی را در پی نداشته باشد به مفهوم غیر فعال بودن این سرویس است.

```
hostname#sh run | incl enable secret
```

اصلاح: برای فعال کردن این سرویس از دستور زیر می‌توانید استفاده کنید.

```
hostname(config)#enable secret <ENABLE_SECRET_PASSWORD>
```

تاثیر: سازمان‌ها بایستی از دسترسی exec با استفاده از سیاست‌های تعیین شده با تنظیم دستور "enable secret" محافظت نمایند. یکی از روش‌هایی که به انجام این کار کمک خواهد کرد، استفاده از دستوری است که در بالا به آن اشاره شد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۴-۲ نحوه فعال‌سازی "service password-encryption"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: زمانی که عملیات رمزنگاری کلمات عبور فعال باشد، فرم رمزنگاری شده‌ای از کلمات عبور برای سیستم‌هایی که در حال اجرا هستند نمایش داده خواهد شد.

دلیل: انجام چنین کاری نیاز به رمزنگاری کلمات عبور در یک فایل پیکربندی دارد. تا بدین‌ترتیب از ورود کاربران غیرمجاز برای فهمیدن الگو رمزنگاری جلوگیری نمایند. زمانی که چنین ویژگی فعال باشد، از دسترسی بیشتر افراد غیرمجاز جلوگیری خواهد شد.

بررسی: از دستور زیر می‌توان برای تشخیص فعال بودن این سرویس و امکان وجود رمزنگاری استفاده کرد.

```
hostname#sh run | incl service password-encryption
```

اصلاح: برای ایجاد رمزنگاری کلمات عبور ضعیف می‌توانیم، از دستور زیر استفاده نماییم.

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

تاثیر: سازمان‌هایی که از این ویژگی برای رمزنگاری استفاده می‌نمایند، تا حد بسیار زیادی از خطرات دسترسی کاربران غیرمجاز پیشگیری می‌نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۴-۳ نحوه تنظیم "username secret" برای تمام کاربران

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: استفاده از دستور "username secret" برای رمزنگاری نام‌های کاربری و کلمات عبور استفاده می-شود. برای رمزنگاری از الگوریتم‌هایی نظیر md5 می‌توان استفاده کرد. علت استفاده از الگوریتم md5 این است که بازیابی اطلاعات رمزنگاری شده، امکان پذیر نیست. به همین خاطر ما نمی‌توانیم از پروتکل‌هایی نظیر CHAP که نیاز به داده‌های رمز نشده دارند، استفاده کنیم.
به کار بردن این پیکربندی می‌تواند باعث ایجاد یک لایه امنیتی اضافی برای ایمن‌سازی هر چه بیشتر نام‌های کاربری و کلمات عبور گردد. از این روش می‌توانیم در شبکه‌های آسیب‌پذیر استفاده نماییم و از این جهت بسیار کارا تلقی می‌گردد.

دلیل: پیکربندی اولیه دستگاه‌ها نیازی به فعال‌سازی نام‌های کاربری وکلمات عبور قدرتمندی را ندارند. این‌کار می‌تواند در دسترسی افراد غیرمجاز کمک کننده باشد. ایجاد حساب‌های کاربری محلی با کلمات‌عبور رمزنگاری شده، خود می‌تواند لیستی از افراد مجازی باشد که توانایی دسترسی به منابع شبکه را خواهند داشت و از طرفی سرویس احراز هویت و اعتبارسنجی را به صورت خودکار دارا باشند.

بررسی: از دستور زیر می‌توانید برای تشخیص اینکه آیا رمزنگاری نام‌های کاربری و کلمات عبور فعال می‌باشند یا خیر، استفاده کنید. اگر در خروجی دستور زیر عبارت "secret" وجود نداشته باشد، به معنی غیرفعال بودن این ویژگی است.

```
hostname#show run | incl username
```

اصلاح: برای فعال کردن این سرویس کافیست، از دستور زیر استفاده کنید و عملیات رمزنگاری بر روی کلمات عبور را انجام دهید.

```
hostname(config)#username <LOCAL_USERNAME> secret <LOCAL_PASSWORD>
```

تاثیر: سازمان‌هایی که از سرویس "username secret" استفاده می‌نمایند، در واقع تا حد بسیار زیادی از دسترسی افراد غیرمجاز به دستگاه‌های Cisco IOS جلوگیری کرده و احتمال حاصل از دسترسی‌ها را بسیار کاهش می‌دهند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۵ قوانین SNMP

پروتکل SNMP، واسط استانداردی برای مدیریت و نظارت بر دستگاه‌های شبکه ایجاد می‌نماید. به دلیل اهمیت این پروتکل در این قسمت سعی در معرفی پیکربندی‌های مربوط به IOS در این رابطه خواهیم داشت. این تنظیمات باعث پیاده‌سازی مناسب این پروتکل در شبکه خواهند شد.

۱-۵-۱ نحوه تنظیم "NO SNMP-SERVER" برای غیرفعال‌سازی SNMP در مواقعی که نیازی به آن وجود ندارد.

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: در هنگامی که از پروتکل SNMP استفاده‌ای در شبکه نمی‌شود، بایستی سرویس مربوط به آن که می‌تواند "خواندن" و یا "نوشتن" در پکت‌های مربوطه باشد، غیرفعال گردد.

دلیل: خصوصیت "خواندن" در SNMP باعث مدیریت و نظارت از راه دور دستگاه می‌گردد.

بررسی: برای اینکه از فعال نبودن SNMP در Cisco IOS مطلع گردید، کافی است دستور زیر را اجرا نمایید. اگر خروجی دستور زیر عبارت "SNMP agent not enable" باشد به مفهوم غیرفعال بودن این ویژگی است.

```
hostname#show snmp community
```

اصلاح: در صورت فعال بودن SNMP، از دستور زیر می‌توانید برای غیرفعال‌سازی استفاده کنید.

```
hostname(config)#no snmp-server
```

تاثیر: سازمان‌هایی که از سرویس‌های پروتکل SNMP استفاده نمی‌کنند، بایستی تمامی آنها را با دستور " no snmp-server" غیرفعال نمایند.

۱-۵-۲ نحوه تنظیم نکردن "private" برای "snmp-server community"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: SNMP می‌تواند مجوز "read-only" را به تمامی کاربران ارائه دهد.

دلیل: تعیین مجوزی از نوع "private" می‌تواند در جلوگیری از دسترسی غیرمجاز جلوگیری کند.

بررسی: برای اینکه از نوع دسترسی "public" و یا "private" مطلع شوید، از دستور زیر می‌توانید استفاده کنید.

```
hostname# show snmp community
```

اصلاح: برای غیرفعال‌سازی "private" در سرویس SNMP می‌توانید از دستور زیر استفاده نمایید.

```
hostname(config)#no snmp-server community {private}
```

تاثیر: سازمان‌ها برای کاهش خطرات ناشی از دسترسی غیرمجاز پیکربندی‌هایی که به حالت "private" مربوط می‌شوند را بایستی غیرفعال نمایند.

۱-۵-۳ نحوه تنظیم نکردن "public" برای "snmp-server community"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: با تنظیم خصوصیت "read-only" می‌توان به تمامی اشیاء شبکه دسترسی پیدا نمود.

دلیل: تعیین مجوزی از نوع "public" می‌تواند در جلوگیری از دسترسی غیرمجاز جلوگیری کند.

بررسی: برای مطلع شدن از فعال بودن ویژگی "public" می‌توانید از دستور زیر استفاده نمایید.

```
hostname# show snmp community
```

اصلاح: برای غیرفعال‌سازی ویژگی "public" کافی است، از دستور زیر استفاده کنید.

```
hostname(config)#no snmp-server community {public}
```

تاثیر: سازمان‌ها برای کاهش خطرات ناشی از دسترسی غیرمجاز پیکربندی‌هایی که به حالت "public" مربوط می‌شوند را بایستی غیرفعال نمایند.

۱-۵-۴ نحوه تنظیم نکردن "RW" برای هر "snmp-server community"

کاربست‌پذیری پروفایل:

- **سطح ۱**

توضیح: اعطای سطح دسترسی read و write.
واحدهای مدیریتی می‌توانند برای بازیابی و ویرایش MIB اقدام نمایند.

دلیل: با فعال کردن خصوصیت read-write می‌توانید از طریق دسترسی از راه دور دستگاه مورد نظر را مدیریت کنید. فعال کردن این دو ویژگی به طور همزمان امکان‌پذیر است.

بررسی: برای اطمینان از اینکه خصوصیت RW در سیستم‌عامل فعال است یا خیر. می‌توانید از دستورات زیر استفاده نمایید.

```
hostname#show run | incl snmp-server community
```

اصلاح: در صورت غیرفعال بودن می‌توانید با استفاده از دستور زیر اقدام به فعال‌سازی این سرویس نمایید.

```
hostname(config)#no snmp-server community {write_community_string}
```

تاثیر: سازمان‌ها برای کاهش خطرات ناشی از دسترسی غیرمجاز بایستی سرویس wirte را غیرفعال نمایند.

۱-۵-۵ نحوه تنظیم کردن ACL برای هر "snmp-server community"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: این سرویس لیستی از آدرس‌های ip خاصی را مشخص می‌سازد که با استفاده از "community string" می‌توان به "snmp agent" دسترسی یافت.

دلیل: در صورت غیرفعال بودن ACL، هر کاربری با "community string" معتبر می‌تواند ترافیک ورودی و خروجی مربوط به روتر را نظارت و مانیتور نماید. برای جلوگیری از انجام این کار بایستی ACL به صورت صحیح و کاربردی تعریف گردد، تا به این صورت بتوان از دسترسی افراد محدودی به ایستگاه‌های مدیریتی جلوگیری نماییم. برای اطمینان بیشتر شما می‌توانید از snmpv3 استفاده نمایید، که به صورت خودکار عملیات احراز هویت و اعتبارسنجی و رمزنگاری داده‌ها را انجام می‌دهد.

بررسی: برای فهمیدن از فعال بودن ACL، می‌توانید از دستور زیر استفاده نمایید.

```
hostname#show run | incl snmp-server community
```

اصلاح: برای پیکربندی "SNMP community string" به جهت محدود کردن دسترسی‌های غیرمجاز به سیستم‌های مدیریتی می‌توانیم از دستور زیر استفاده کنیم.

```
hostname(config)#snmp-server community <community_string> ro {snmp_access-
list_number | snmp_access-list_name}
```

تاثیر: سازمان‌ها برای کاهش دسترسی‌های غیرمجاز، بایستی لیست کنترل دسترسی برای هر "SNMP-server communities" ایجاد نمایند. تا به این طریق با ایمن‌سازی هرچه بیشتر از نفوذ به مناطق حساس مدیریتی جلوگیری شود. برای اطمینان بیشتر شما می‌توانید از SNMPv3 استفاده کنید، که به صورت خودکار عملیات احراز هویت و اعتبارسنجی و رمزنگاری داده‌ها را انجام می‌دهد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۵-۶ نحوه ایجاد یک "access-list" برای SNMP

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: شما می‌توانید با استفاده از یک "access-list" پکت‌های ارسالی و دریافتی روی یک اینترفیس مشخص را کنترل کنید. یکی از قابلیت‌های SNMP در اختیار قرار می‌دهد عبارتنداز محدود ساختن دسترسی‌ها به محتوای پکت‌هایی است که مربوط به بروزرسانی یک روتر می‌باشند. سیستم‌عامل Cisco IOS به صورت خودکار افزایش محتوای "access-list" را متوقف می‌سازد.

دلیل: "SNMP ACL" تعیین می‌نماید که کدام آدرس ip با استفاده از پروتکل SNMP تحت مدیریت و نظارت قرار گیرد. در صورت فعال نبودن ACL، هر فردی با یک "SNMP community string" معتبر می‌تواند یک دستگاهی مانند روتر را مدیریت و نظارت کند. بنابراین با توصیفات ذکر شده بایستی با فعال نمودن ACL از طریق تعریف "SNMP community string" معتبر می‌توان عملیات اعتبارسنجی کاربران و محدود ساختن لیست دسترسی، امنیت را تا حد بالایی در یک سگمنت شبکه برقرار نمود.

بررسی: برای مطمئن شدن از فعال بودن ACL می توانید از دستور زیر استفاده کنید.

```
hostname#sh ip access-list <snmp_acl_number>
```

اصلاح: برای فعال‌سازی این سرویس می‌توانید از دستور زیر استفاده کنید تا به این طریق دسترسی‌های انجام شده به یک دستگاه مشخص محدود شود.

```
hostname(config)#access-list <snmp_acl_number> permit <snmp_access-list>
hostname(config)#access-list deny any log
```

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۵-۷ نحوه تنظیم "SNMP-Server Host" برای SNMP

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اعلان SNMP می‌تواند به عنوان یک تله برای احراز هویت دستگاه‌های مدیریتی فرستاده شود.

دلیل: در صورت فعال بودن SNMP برای مدیریت یک دستگاه مشخص، سیستم مدیریتی بایستی در هنگام دسترسی‌های غیرمجاز هشدارهای لازم را صادر نماید.

بررسی: با اجرای دستور زیر می‌توان فهمید که آیا این سرویس مربوط به SNMP فعال است یا خیر. در صورت وجود مقادیر مربوط به پیکربندی در خروجی دستور می‌توان فهمید که این سرویس فعال است.

```
hostname#show run snmp-server
```

اصلاح: در صورت غیرفعال بودن این سرویس می‌توانید برای فعال‌سازی و محدود ساختن ارسال پیام‌های مدیریتی به یک دستگاه مشخص، از دستور زیر استفاده نمایید.

```
hostname(config)# snmp-server host {ip_address} {trap_community_string} snmp
```

تاثیر: سازمان‌ها برای محدود کردن ارسال پیام‌های SNMP و کاهش دسترسی‌های غیرمجاز می توانند از این سرویس استفاده نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.


مرکز ماهر

۱-۵-۸ نحوه تنظیم کردن "SNMP-Server enable traps SNMP"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: اعلان SNMP می‌تواند به عنوان یک تله برای احراز هویت دستگاه‌های مدیریتی فرستاده شود.

دلیل: یکی از ویژگی‌های SNMP می‌تواند ثبت تله‌ها باشد.

بررسی: برای اطلاع از فعال بودن این سرویس می‌توانید از دستور زیر استفاده نمایید. در صورت وجود مقادیر مربوط به پیکربندی در خروجی دستور می‌توان فهمید که این سرویس فعال است.

```
hostname# show run snmp-server
```

اصلاح: برای فعال‌سازی این سرویس می‌توانید از دستور زیر استفاده نمایید.

```
hostname(config)# snmp-server enable traps snmp authentication linkup linkdown
coldstart
```

تاثیر: سازمان‌ها با استفاده از قابلیت‌هایی که SNMP در اختیار آنها قرار می‌دهد، می‌توانند از ورود ترافیک ناخواسته به یک دستگاه مشخص جلوگیری نمایند. شما همچنین می‌توانید برخی از انواع تله‌های مربوط به SNMP را فعال کنید.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۵-۹ نحوه فعال‌سازی "priv" برای هر "SNMP-Server Group" با استفاده از "SNMPv3"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: احراز هویت پکت‌ها با استفاده از رمزنگاری آنها توسط SNMPv3.

دلیل: نسخه SNMPv3 قابلیت‌های بیشتر و بهتری را برای تامین امنیت، نسبت به ورژن‌های قبلی در اختیار قرار می‌دهد. زمانی که از این ورژن استفاده می‌کنید، پکت‌های ارسالی می‌توانند به صورت رمزنگاری شده ارسال شوند تا در حین انتقال از نفوذپذیری توسط کاربران غیرمجاز جلوگیری شود.

بررسی: به جهت بررسی فعال بودن این سرویس و مشاهده گروه‌بندی‌های انجام شده می‌توانید از دستور زیر استفاده نمایید.

```
hostname# show snmp groups
```

اصلاح: برای هر گروه می‌توانید با استفاده از دستور زیر سیاسیت‌های لازم را تعیین کنید.

```
hostname(config)# snmp-server group {group_name} v3 priv
```

تاثیر: برای جلوگیری از اجرای دسترسی‌های غیرمجاز شما می‌توانید از این سرویس استفاده نمایید که با این ترتیب با رمزنگاری داده‌ها از دسترس‌ناپذیری آنها اطمینان حاصل کنید.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۱-۵-۱۰ در هنگام استفاده از SNMPv3 ،"AES 128" می‌تواند جزو کمترین نیاز برای "SNMP Server user" باشد.

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: به هنگام استفاده از SNMP، به کاربردن AES به عنوان یکی از کمترین نیازها برای رمزنگاری داده-های ارسالی محسوب می‌گردد.

دلیل: نسخه SNMPv3 قابلیت‌های بیشتر و بهتری را برای تامین امنیت، نسبت به ورژن‌های قبلی در اختیار قرار می‌دهد. در هنگام پیکربندی SNMPv3 می‌توانید رنج‌هایی که الگوریتم رمزنگاری انجام می‌شود، تعیین نمایید. الگوریتم رمزنگاری AES128 دارای حداقل طول و متدهایی است که در رمزنگاری می‌توان از آنها استفاده نمود.

بررسی: برای بررسی فعال بودن این سرویس می‌توانید از دستور زیر استفاده کنید.

```
hostname# show snmp user
```

اصلاح: برای فعال‌سازی این سرویس می‌توانید از دستور زیر استفاده نمایید و به این ترتیب خصوصیات SNMPv3 را به کار ببرید.

```
hostname(config)# snmp-server user {user_name} {group_name} v3 encrypted auth
sha {auth_password} priv aes 128 {priv_password} {acl_name_or_number}
```

تاثیر:سازمان‌ها با استفاده از SNMP می‌توانند خطرات ناشی از دسترسی افراد غیرمجاز را کاهش داده و با استفاده از تنظیمات "snmp-server user" و ویژگی‌های احراز هویت و سیاست‌های اخذ شده اقدام به رمزنگاری داده‌های ارسالی کنند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس در IOS فعال نمی‌باشد.

۲ واحد کنترل

واحد کنترل نظارت، بروزرسانی جدول مسیرها و به طورکلی فعالیت‌های پویای مسیریاب را بر عهده دارد. این .واحد شامل سرویس‌ها، تنظیمات و جریان‌های داده‌ای می‌باشد که عملیات، مدیریت ترافیک و موقعیت پویای مسیریاب را پشتیبانی و ثبت می‌کند. مثال‌های سرویس‌های واحد کنترل ثبت وقایع(مثلا Syslog)، پروتکل‌های مسیریابی و پروتکل‌های موقعیتی مانند CDP و HSRP، پروتکل‌های توپولوژی شبکه مانند STP و پروتکل‌های کنترل امنیت ترافیک مانند IKE را شامل می‌شود. پروتکل‌های کنترل شبکه مانند ICMP، NTP، ARP و IGMP که در مسیریاب دریافت و یا ارسال می‌شود نیز در این دسته‌بندی قرار می‌گیرند.

۲-۱ قوانین سرویس سراسری

قوانین مربوط به دسته سرویس‌های سراسری، سرور و کنترل سرویس‌ها را در برابر حملات و یا در معرض استفاده از آسیب‌پذیری قرار دادن آنها وادار به محافظت می‌کند.

۲-۱-۱ راه‌اندازی SSH

از استفاده از SSH برای برقراری جلسات کنترل از راه‌دور مسیریاب‌های سیسکو اطمینان حاصل نمایید.

۲-۱-۱-۱ تنظیمات مربوط به پیش‌نیازهای سرویس SSH

۲-۱-۱-۱-۱ "Hostname" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: از "hostname" در نام فایل‌های تنظیمات پیش‌فرض و محیط دستور استفاده می‌شود.

دلیل: نام دامنه پیش نیاز راه اندازی SSH می‌باشد.

بررسی: کار زیر را برای بررسی تنظیم دلیله زمانی محلی انجام دهید. نتیجه را با مشاهده پیکربندی درست رخداد فصل تابستان بررسی کنید.

```
hostname#sh run | incl hostname
```

اصلاح: یک نام میزبان مناسب برای مسیریاب تنظیم نمایید.

```
hostname(config)#hostname {router_name}
```

تاثیر: سازمان‌ها باید برای شبکه سازمانی خود برنامه‌ریزی کرده و نام میزبان‌های مناسبی را برای هر مسیریاب انتخاب نمایند.

مقدار پیش‌فرض: نام پیش‌فرض میزبان Router می‌باشد.

۲-۱-۱-۲ "ip domain name" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: نام دامنه پیش‌فرض را تعریف کنید تا سیستم عامل سیسکو نام میزبان‌های فاقد اعتبار را با استفاده از آن کامل کند.

دلیل: نام دامنه پیش نیاز راه اندازی SSH می‌باشد.

بررسی: کار زیر را برای بررسی تنظیم نام دامنه انجام دهید. تنظیم مناسب نام دامنه را بررسی کنید.

```
hostname#sh run | incl domain name
```

اصلاح: یک نام دامنه مناسب برای مسیریاب تنظیم نمایید.

```
hostname (config)#ip domain name {domain-name}
```

تاثیر: سازمان‌ها باید برای شبکه سازمانی خود برنامه‌ریزی کرده و نام دامنه مناسبی را برای مسیریاب انتخاب نمایند.

مقدار پیش‌فرض: هیچ دامنه‌ای ثبت نشده است.

۲-۱-۱-۱-۳ مقدار "modulus" در "crypto key generate rsa" را بزرگتر یا مساوی 2048 تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: از این دستور برای تولید زوج کلید RSA برای دستگاه سیسکو خود استفاده نمایید. کلیدهای RSA به صورت زوج کلید-یک کلید عمومی و یک کلید خصوصی- تولید می‌شوند.

دلیل: زوج کلید RSA پیش‌نیاز راه اندازی SSH می‌باشد و باید حداقل 2048 بیت باشد.
نکته: IOS مقدار بیت پیمانه را در فرآیند بازبینی نمایش نمی‌دهد.

بررسی: کار زیر را برای بررسی تنظیم زوج کلید RSA انجام دهید:

```
hostname#sh crypto key mypubkey rsa
```

اصلاح: یک زوج کلید RSA برای مسیریاب تولید نمایید.

```
hostname(config)#crypto key generate rsa general-keys modulus 2048
```

تاثیر: سازمان‌ها باید برای رمزنگاری شبکه سازمانی خود برنامه‌ریزی و پیاده‌سازی کنند و زوج کلید RSA مناسبی را برای مثال مقدار بزرگتر یا برابر 2048 برای پیمانه‌ها تولید نمایند.

مقدار پیش‌فرض: هیچ زوج کلید RSA وجود ندارد.

۲-۱-۱-۴ "seconds" را برای "ip ssh timeout" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: فاصله زمانی که مسیریاب منتظر کلاینت SSH برای پاسخ، قبل از قطع شدن تلاشی ناتمام برای ورود، می‌ماند.

دلیل: این کار باعث کاهش خطری می‌شود که در آن مدیر یک جلسه معتبر ورود را برای یک بازه زمانی طولانی ترک می‌کند.

بررسی: کار زیر را برای بررسی تنظیم زمان وقفه SSH انجام دهید. تنظیم مناسب زمان وقفه را بررسی کنید.

```
hostname#sh ip ssh
```

اصلاح: زمان وقفه SSH را تنظیم نمایید.

```
hostname(config)#ip ssh timeout [60]
```

تاثیر: سازمان‌ها باید یک سیاست امنیتی برای خود پیاده سازی نمایند که نیازمند تنظیمات زمان وقفه حداقل برای تمام مدیران شبکه را نیاز داشته باشد و سیاست مورد نظر را از طریق دستور "ip ssh timeout" اعمال نماید.

مقدار پیش‌فرض: SSH به صورت پیش‌فرض تنظیم نشده است.

۲-۱-۱-۱-۵ مقدار بیشینه برای "ip ssh authentication-retries" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: تعداد تلاش‌ها قبل از قطع اتصال جلسه ورود SSH می‌باشد.

دلیل: این عمل باعث محدود کردن تعداد دفعات تلاش ورود کاربران غیرمجاز بدون ایجاد جلسه ورود SSH جدید می‌باشد. این کار با محدود کردن تعداد تلاش‌ها برای ورود در یک اتصال SSH باعث کاهش میزان موفقیت حملات Brute Force می‌شود.

بررسی: کار زیر را برای بررسی تنظیم تعداد تلاش‌های ورود SSH انجام دهید. تنظیم مناسب تعداد تلاش برای ورود را بررسی کنید.

```
hostname#sh ip ssh
```

اصلاح: زمان وقفه SSH را تنظیم نمایید.

```
hostname(config)#ip ssh authentication-retries [3]
```

تاثیر: سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که تعداد تلاش‌های ورود را برای شبکه‌های مدیریتی محدود کند و سیاست مورد نظر را از طریق دستور "ip ssh authentication-retries" اعمال نماید.

مقدار پیش‌فرض: SSH به صورت پیش‌فرض فعال نمی‌باشد. زمانی که فعال شود، مقدار پیش‌فرض ۳ می‌باشد.

۲-۱-۱-۲ مقدار نسخه ۲ را برای "ip ssh version" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: نسخه SSH را برای اجرا شدن بر روی مسیریاب مشخص نمایید.

دلیل: SSH نسخه ۱ دارای چندین آسیب‌پذیری جدی بوده است که باعث شد دیگر به عنوان یک پروتکل امن شناخته نشود. در نتیجه SSH نسخه ۲ در سال ۲۰۰۶ به عنوان استاندارد اینترنت تصویب شد.
مسیریاب‌های سیسکو از هر دو نسخه پشتیبانی می‌کنند، ولی به دلیل ضعف SSH نسخه ۱ باید فقط از استاندارد بعدی آن استفاده شود.

بررسی: کار زیر را برای بررسی تنظیم SSH نسخه ۲ انجام دهید. تنظیم مناسب SSH نسخه ۲ را بررسی کنید.

```
hostname#sh ip ssh
```

اصلاح: مسیریاب را برای استفاده از SSH نسخه ۲ تنظیم نمایید.

```
hostname(config)#ip ssh version 2
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن پروتکل‌های فعلی را بررسی کرده و از استفاده از امن‌ترین نسخه‌های پروتکل‌ها اطمینان حاصل نماید.

مقدار پیش‌فرض: SSH به صورت پیش‌فرض فعال نمی‌باشد. زمانی که فعال شود، SSH در حالت سازگاری کار می‌کند (نسخه ۱ و ۲ پشتیبانی می شود).

۲-۱-۲ "no cdp run" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سرویس CDP را در دستگاه غیرفعال کنید.

دلیل: CDP یک پروتکل اختصاصی می‌باشد که دستگاه‌های سیسکو برای شناسایی یکدیگر بر روی یک بخش شبکه از آن استفاده می‌کنند. این پروتکل در نظارت بر شبکه و در مواقع برطرف کردن مشکلات مفید می‌باشد ولی به دلیل حجم اطلاعاتی که در پرس‌وجوها در اختیار قرار می‌دهند، به عنوان یک تهدید امنیتی شناخته می‌شود. علاوه بر این حملات DOS هم شناخته شده‌اند که از CDP استفاده می‌کنند. CDP باید کاملا غیرفعال شود مگر اینکه لازم باشد.

بررسی: کار زیر را برای بررسی فعال بودن CDP انجام دهید. بررسی کنید که نتیجه "CDP is not enabled" را نشان می‌دهد.

```
hostname#show cdp
```

اصلاح: سرویس CDP را به صورت سراسری غیرفعال نمایید.

```
hostname(config)#no cdp run
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن پروتکل‌های شبکه را محدود ساخته و غیرفعال کردن تمام پروتکل‌های غیر لازم و ناامن را صریحا لازم سازد.

مقدار پیش‌فرض: بر روی تمامی پلتفرم‌ها به جز Cisco 10000 Series Edge Services Router فعال می‌باشد.

۲-۱-۳ "no ip bootp server" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سرویس BOOTP را در دستگاه مسیریاب خود غیرفعال کنید.

دلیل: BOOTP به یک مسیریاب اجازه اختصاص IPها را می‌دهد. این پروتکل باید غیرفعال شود مگر اینکه نیاز خاصی به آن باشد.

بررسی: کار زیر را برای بررسی فعال بودن BOOTP انجام دهید. بررسی کنید که "no ip bootp server" نتیجه‌ای را برگرداند.

```
hostname#show run | incl bootp
```

اصلاح: سرور BOOTP را غیرفعال نمایید.

```
hostname(config)#no ip bootp server
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن پروتکل‌های شبکه را محدود ساخته و غیرفعال کردن تمام پروتکل‌های غیر لازم و ناامن مانند " ip bootp server" را صریحا لازم سازد.

مقدار پیش‌فرض: فعال می‌باشد.

۲-۱-۴ "no service dhcp" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سرور DHCP و ویژگی‌های عامل رله را در مسیریاب خود غیرفعال کنید.

دلیل: سرور DHCP دربردارنده پارامترهای تنظیمات اتوماتیک مانند آدرس IP پویا، برای سیستم‌های درخواست کننده می‌باشد. به جای آن باید از یک سرور اختصاصی که در یک ناحیه مدیریتی امن قرار گرفته شده است، به عنوان سرویس دهنده DHCP استفاده شود. مهاجمان می‌توانند از آن برای حملات DoS استفاده نمایند.

بررسی: کار زیر را برای بررسی فعال بودن سرویس DHCP انجام دهید. بررسی کنید که نتیجه‌ای را برنگرداند.

```
hostname#show run | incl dhcp
```

اصلاح: سرور DHCP را غیرفعال نمایید.

```
hostname(config)#no service dhcp
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن پروتکل‌های شبکه را محدود ساخته و غیرفعال کردن تمام پروتکل‌های غیر لازم و ناامن مانند DHCP را صریحا لازم سازد.

مقدار پیش‌فرض: به صورت پیش‌فرض فعال می‌باشد، با این حال نیازمند تنظیم مجموعه DHCP برای فعال کردن سرور DHCP می‌باشد.

۲-۱-۵ "no ip identd" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سرور تعیین هویت identd را غیرفعال کنید.

دلیل: پروتکل تعیین هویت، شناسایی پروتکل TCP یک کاربر را ممکن می‌سازد. این افشای اطلاعات به طور بالقوه می‌تواند اطلاعاتی درباره کاربران را در اختیار مهاجم قرار دهد.

بررسی: کار زیر را برای بررسی فعال بودن identd انجام دهید. بررسی کنید که نتیجه‌ای را برنگرداند.

```
hostname#show run | incl identd
```

اصلاح: سرور identd را غیرفعال نمایید.

```
hostname(config)#no ip identd
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن پروتکل‌های شبکه را محدود ساخته و غیرفعال کردن تمام پروتکل‌های غیر لازم و ناامن مانند پروتکل تعیین هویت (identd) را صریحا لازم سازد.

مقدار پیش‌فرض: به صورت پیش‌فرض فعال می‌باشد.

۲-۱-۶ "service tcp-keepalives-in" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: بسته‌های keepalive را در اتصالات شبکه‌ای ورودی بیکار، تولید کنید.

دلیل: اتصالات کهنه از منابع استفاده می‌کنند و می‌توانند به صورت بالقوه در جهت دسترسی غیرمجاز ربوده شوند. سرویس keepalive-in در TCP بسته‌های keepalive را در اتصالات شبکه‌ای ورودی بیکار (که توسط میزبان راه دور آغاز شده) تولید می‌کند. این سرویس به دستگاه اجازه شناسایی قطع شدن جلسات و یا زمانی که میزبان راه دور از کار میافتد را می‌دهد. در صورت فعال بودن، بسته‌های keepalive هر ۱ دقیقه یکبار در اتصالات بیکار فرستاده می‌شوند. در صورت عدم دریافت بسته‌های keepalive، اتصال در ۵ دقیقه و در صورت دریافت بسته reset، بلافاصله بسته می‌شود.

بررسی: کار زیر را برای بررسی فعال بودن این ویژگی انجام دهید. بررسی کنید که در نتیجه یک رشته باز می-گردد.

```
hostname#show run | incl service tcp
```

اصلاح: سرویس keepalives-in را فعال نمایید.

```
hostname(config)#service tcp-keepalives-in
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن مدت زمان اجازه ادامه جلسه‌های اتمام یافته را محدود ساخته و این سیاست را از طریق فرمان "tcp-keepalives-in" اعمال نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض غیرفعال می‌باشد.

۷-۱-۲ "service tcp-keepalives-out" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: بسته‌های keepalive را در اتصالات شبکه‌ای خروجی بیکار، تولید کنید.

دلیل: اتصالات کهنه از منابع استفاده می‌کنند و می‌توانند به صورت بالقوه در جهت دسترسی غیرمجاز ربوده شوند. سرویس keepalive-in در TCP بسته‌های keepalive را در اتصالات شبکه‌ای ورودی بیکار(که توسط میزبان راه دور آغاز شده) تولید می‌کند. این سرویس به دستگاه اجازه شناسایی قطع شدن جلسات و یا زمانی که میزبان راه دور از کار میافتد را می‌دهد. در صورت فعال بودن، بسته‌های keepalive هر ۱ دقیقه یکبار در اتصالات بیکار فرستاده می‌شوند. در صورت عدم دریافت بسته‌های keepalive، اتصال در ۵ دقیقه و در صورت دریافت بسته reset، بلافاصله بسته می‌شود.

بررسی: کار زیر را برای بررسی فعال بودن این ویژگی انجام دهید. بررسی کنید که در نتیجه یک رشته باز می-گردد.

```
hostname#show run | incl service tcp
```

اصلاح: سرویس keepalives-out را فعال نمایید.

```
hostname(config)#service tcp-keepalives-out
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن مدت زمان اجازه ادامه جلسه‌های اتمام یافته را محدود ساخته و این سیاست را از طریق فرمان "tcp-keepalives-out" اعمال نماید.

مقدار پیش‌فرض: به صورت پیش‌فرض غیرفعال می‌باشد.

۲-۱-۸ "no service pad" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سرویس X.25 PAD را غیرفعال نمایید.

دلیل: در صورتی که سرویس PAD لازم نباشد، این سرویس را برای جلوگیری از دسترسی مهاجمان به مجموعه فرمان X.25 PAD در روی یک مسیریاب، غیرفعال کنید.

بررسی: کار زیر را برای بررسی غیرفعال بودن این ویژگی انجام دهید. بررسی کنید که نتیجه‌ای را برنگرداند.

```
hostname#show run | incl service pad
```

اصلاح: سرویس PAD را غیرفعال نمایید.

```
hostname(config)#no service pad
```

تاثیر: برای کاهش خطر دسترسی‌های غیرمجاز، سازمان‌ها باید سیاست امنیتی را پیاده‌سازی کنند که در آن استفاده از سرویس‌های غیرضروری مانند سرویس PAD را محدود سازد.

مقدار پیش‌فرض: به صورت پیش‌فرض فعال می‌باشد.

۲-۲ قوانین ثبت وقایع

قوانین مربوط به دسته ثبت وقایع کنترل‌هایی را اعمال می‌کند که سابقه فعالیت‌های سیستم و حوادث را در اختیار ما قرار می‌دهد.

۱-۲-۲ "logging on" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: ثبت وقایع پیام‌های سیستمی را فعال نمایید.

دلیل: ثبت وقایع، سابقه‌ای از فعالیت‌های دستگاه سیسکو به ترتیب وقوع را ارائه می‌کند و اجازه نظارت بر روی رویدادهای عملیاتی و امنیتی را می‌دهد.

بررسی: کار زیر را برای بررسی فعال بودن این ویژگی انجام دهید. بررسی کنید که نتیجه‌ای را برنگرداند.

```
hostname#show run | incl logging on
```

اصلاح: ثبت وقایع را فعال نمایید.

```
hostname(config)#logging on
```

تاثیر: فعال کردن فرمان "logging on" در Cisco IOS، نظارت بر تهدیدات دستگاه‌های شبکه سازمان را اعمال می‌کند.

مقدار پیش‌فرض: به صورت پیش‌فرض ثبت وقایع فعال نمی‌باشد.

۲-۲-۲ "buffer size" را برای "logging buffered" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: ثبت وقایع پیام‌های سیستمی به یک بافر محلی را فعال نمایید.

دلیل: دستگاه می‌تواند پیام‌های گزارشی را در یک بافر حافظه داخلی ذخیره و یا کپی نماید. داده بافر شده در یک جلسه exec یا enabled exec در یک مسیریاب قابل دسترس است. این شکل از ثبت وقایع برای اشکال زدایی و نظارت زمانی که به مسیریاب وارد شده‌اید، مفید است.

بررسی: کار زیر را برای بررسی فعال بودن این ویژگی انجام دهید. بررسی کنید که در نتیجه یک رشته باز می-گردد.

```
hostname#show run | incl logging buffered
```

اصلاح: ثبت وقایع بافر شده (با کمترین اندازه) را پیکربندی کنید. اندازه پیشنهادی 64000 می‌باشد.

```
hostname(config)#logging buffered [log_buffer_size]
```

تاثیر: جرم یابی و بررسی داده در مدیریت خطرات تکنولوژی مفید می‌باشد و یک سازمان می‌تواند از چنین سیاستی با فعال نمودن فرمان "logging buffered" استفاده نماید.

مقدار پیش‌فرض: به صورت پیش‌فرض هیچ بافر ثبت وقایع تنظیم نشده است.

۲-۲-۳ "logging console critical" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: فعال بودن ثبت وقایع در کنسول دستگاه و محدود بودن به یک سطح شدت منطقی (به دلیل جلوگیری از تاثیر زیاد بر کارایی و مدیریت سیستم) را بررسی کنید.

دلیل: این تنظیمات میزان شدت پیام‌هایی که به عنوان پیام‌های کنسولی تولید خواهند شد را مشخص می‌کند. ثبت وقایع در کنسول باید به پیام‌هایی که نیازمند اشکال زدایی سریع، و در زمان ورود به دستگاه باید نشان داده شوند، محدود شود. این شکل از ثبت وقایع دائمی نمی‌باشد؛ به این معنی که پیام‌های چاپ شده در کنسول در مسیریاب ذخیره نمی‌شوند. ثبت وقایع کنسولی زمانی که اپراتورها از کنسول استفاده می‌کنند سودمند است.

بررسی: کار زیر را برای بررسی فعال بودن این ویژگی انجام دهید. بررسی کنید که در نتیجه یک رشته باز می-گردد.

```
hostname#show run | incl logging console
```

اصلاح: سطح ثبت وقایع کنسولی را پیکربندی کنید.

```
hostname(config)#logging console critical
```

تاثیر: ثبت پیام‌های وقایع بحرانی در کنسول برای یک سازمان در مدیریت خطرات مهم می‌باشد. فرمان"logging console" زمانی مفید واقع می‌شود که پیام‌های بحرانی را به طور مناسب ثبت نماید.

مقدار پیش‌فرض: به صورت پیش‌فرض تمام پیام‌ها را ثبت می‌کند.

۲-۲-۴ آدرس IP را برای "logging host" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: پیام‌های سیستمی و خروجی دیباگ را در یک میزبان راه دور ثبت کنید.

دلیل: مسیریاب‌های سیسکو می‌توانند پیام‌های خود را به سرویس Syslog، که به سبک Unix است، ارسال نمایند. یک سرویس Syslog به طور ساده پیام‌ها را دریافت کرده و براساس تنظیمات موجود در یک فایل پیکربندی ساده، در فایل ذخیره می‌کند و یا در خروجی چاپ می‌کند. این شکل از ثبت وقایع به دلیل ذخیره سازی بلند مدت و ایمن وقایع، بهترین گزینه می‌باشد (بافر ثبت وقایع داخلی دستگاه‌ها ظرفیت کمی برای ذخیره وقایع دارد). علاوه بر این، ثبت وقایع در یک سیستم خارجی بر اساس بیشتر استانداردهای امنیتی الزامی بوده و پیشنهاد می‌شود. در صورت علاقه و یا لزوم استفاده بر اساس قوانین و مقررات، می‌توان از سرور syslog ثانوی برای افزونگی استفاده کرد.

بررسی: کار زیر را برای بررسی فعال بودن سرور syslog انجام دهید. بررسی کنید که یک و یا بیشتر آدرس IP باز می‌گردد.

```
hostname#sh log | incl logging host
```

اصلاح: یک یا بیشتر سرور syslog با آدرس IP تعیین کنید.

```
hostname(config)#logging host syslog_server
```

تاثیر: ثبت پیام‌های وقایع یک فرآیند مهم برای مدیریت خطرات یک سازمان می‌باشد. فرمان "logging host" آدرس‌های IP میزبان‌های ثبت را تنظیم می‌کند و فرآیند ثبت وقایع را اعمال می‌کند.

مقدار پیش‌فرض: پیام‌های ثبت وقایع سیستمی به میزبان راه دور فرستاده نمی‌شود.

۵-۲-۲ "logging trap informational" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: پیام‌های ثبت شونده در سرورهای syslog را بر اساس سطح شدت محدود کنید.

دلیل: این شدت پیام‌هایی که تله SNMP و یا پیام‌های syslog را تولید می‌کند را تعیین می‌کند. این گزینه باید "debugging" (7) یا "information" (6) و نه کمتر، تنظیم شود.

بررسی: کار زیر را برای بررسی فعال بودن یک سرور syslog برای تله‌های SNMP انجام دهید. بررسی کنید که "level informational" باز می‌گردد.

```
hostname#sh log | incl trap logging
```

اصلاح: تله SNMP و سطح ثبت وقایع syslog را پیکربندی کنید.

```
hostname(config)#logging trap informational
```

تاثیر: ثبت پیام‌های وقایع یک فرآیند مهم برای مدیریت خطرات تکنولوژی یک سازمان می‌باشد. فرمان "logging trap" میزان شدت پیام‌ها را تنظیم می‌کند و فرآیند ثبت وقایع را اعمال می‌کند.

مقدار پیش‌فرض: غیرفعال است.

۶-۲-۲ "service timestamps debug datetime" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: سیستم را تنظیم کنید تا مهر زمانی را به پیام‌های اشکال زدایی و پیام‌های ثبت وقایع سیستمی اضافه کند.

دلیل: اضافه کردن مهر زمانی در پیام‌های ثبت وقایع، اجازه مرتبط کردن وقایع و دنبال کردن حملات شبکه بین چند دستگاه را می‌دهد. فعال کردن سرویس مهر زمانی برای علامت زدن زمان پیام‌های ثبت وقایع تولید شده، به دست آوردن یک نگاه جامع از رویدادها را ساده‌تر می‌کند و باعث اشکال زدایی سریعتر مشکلات و حملات می‌شود.

بررسی: کار زیر را برای بررسی فعال بودن اطلاعات اضافی انجام دهید. بررسی کنید که در نتیجه یک رشته دستور باز می‌گردد.

```
hostname#sh run | incl service timestamps
```

اصلاح: پیام‌های اشکال زدایی را برای اضافه کردن مهر زمانی تنظیم کنید.

```
hostname(config)#service timestamps debug datetime {msec} show-timezone
```

تاثیر: ثبت پیام‌های وقایع یک فرآیند مهم برای مدیریت خطرات تکنولوژی یک سازمان و ایجاد یک جدول زمانی از رویدادها حیاتی می‌باشد. فرمان "service timestamps " تاریخ و زمان را بر روی ورودی‌های ارسال شده به میزبان ثبت وقایع تنظیم می‌کند و فرآیند ثبت وقایع را اعمال می‌کند.

مقدار پیش‌فرض: مهر زمانی بر روی پیام‌های ثبت وقایع و اشکال‌زدایی اعمال می‌شوند.

۷-۲-۲ "logging source interface" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: آدرس Ipv4 یا IPv6 سیستم ثبت وقایع بسته‌ها را مشخص کنید.

دلیل: این کار بدین صورت ضروری می‌باشد که مسیریاب پیام‌های ثبت وقایع را به سرور ثبت وقایع که آدرس IP ثابتی دارد ارسال می‌کند.

بررسی: کار زیر را برای بررسی اینکه آیا سرویس ثبت وقایع متعلق به آدرس رابط منبع می‌باشد، انجام دهید. بررسی کنید که در نتیجه یک رشته دستور باز می‌گردد.

```
hostname#sh run | incl logging source
```

اصلاح: ثبت وقایع را به رابط loopback اتصال دهید.

```
hostname(config)#logging source-interface loopback {loopback_interface_number}
```

تاثیر: ثبت پیام‌های وقایع یک فرآیند مهم برای مدیریت خطرات تکنولوژی یک سازمان و ایجاد یک منبع ثابت برای پیام‌ها برای میزبان ثبت وقایع حیاتی می‌باشد. فرمان "logging source interface loopback" یک آدرس IP ثابت برای ارسال پیام‌ها به میزبان ثبت وقایع تنظیم می‌کند و فرآیند ثبت وقایع را اعمال می‌کند.

مقدار پیش‌فرض: آدرس رابط عمومی استفاده شده است.

۲-۳ قوانین NTP

پروتکل زمان شبکه به مدیران اجازه می‌دهد تا زمان سیستمی تمام سیستم‌های سازگار خود را تنها از یک منبع تنظیم کنند که باعث حصول اطمینان از مهر زمانی ثابت برای ثبت وقایع و پروتکل‌های احراز هویت می‌شود. NTP یک استاندارد اینترنت می‌باشد که در RFC1305 تعریف شده است.

۲-۳-۱ کلیدهای رمزگذاری برای NTP را لازم بدانید

کلیدهای رمزگذاری باید برای سرورهای NTP تنظیم شود.

۲-۳-۱-۱ "ntp authenticate" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: احراز هویت NTP را فعال کنید.

دلیل: استفاده از NTP احراز هویت شده، تضمین می‌کند که دستگاه سیسکو اجازه بروزرسانی‌های زمان را فقط به سرورهای NTP مجاز می‌دهد.

بررسی: از خط فرمان، دستورات زیر را اجرا نمایید:

```
hostname#show run | include ntp
```

اصلاح: احراز هویت NTP را پیکربندی کنید.

```
hostname(config)#ntp authenticate
```

تاثیر: سازمان‌ها باید ۳ میزبان NTP برای تنظیم زمان ثابت در کل سازمان ایجاد نمایند. فعال کردن فرمان "ntp authenticate"، احراز هویت بین میزبان‌های NTP را اجرا می‌کند.

مقدار پیش‌فرض: احراز هویت NTP فعال نمی‌باشد.

۲-۳-۱-۲ "ntp authentication-key" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: یک کلید احراز هویت برای NTP تعریف نمایید.

دلیل: استفاده از کلید احراز هویت درجه بالاتری از امنیت را فراهم می‌کند، به این صورت که فقط سرورهای NTP احراز هویت شده قادر به بروزرسانی زمان برای دستگاه‌های سیسکو خواهند بود.

بررسی: از خط فرمان، دستورات زیر را اجرا نمایید:

```
hostname#show run | include ntp authentication-key
```

اصلاح: زنجیره کلید NTP و کلید رمزگذاری را با استفاده از دستورات زیر پیکربندی نمایید.

```
hostname(config)#ntp authentication-key {ntp_key_id} md5 {ntp_key}
```

تاثیر: سازمان‌ها باید ۳ میزبان NTP برای تنظیم زمان ثابت در کل سازمان ایجاد نمایند. فعال کردن فرمان "ntp authentication-key"، احراز هویت بین میزبان‌های NTP را اجرا می‌کند.

مقدار پیش‌فرض: کلید احراز هویتی برای NTP تعریف نشده است.

۲-۳-۱-۳ "ntp trusted-key" را تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: از احراز هویت، هویت سیستمی که NTP با آن همگام‌سازی می‌شود، اطمینان حاصل نمایید.

دلیل: این عمل احراز هویت، محافظت در برابر همگام‌سازی تصادفی سیستم با سیستم غیر قابل اعتماد دیگر را فراهم می‌سازد، محافظت به این دلیل انجام می‌گیرد که سیستم دیگر باید کلید احراز هویت درست را بداند.

بررسی: از خط فرمان، دستورات زیر را اجرا نمایید:

```
hostname#show run | include ntp trusted-key
```

دستور بالا باید همه سرورهای NTP پیکربندی شده با کلیدهای رمزگذاری را برگرداند. این مقدار باید با کل تعداد سرورهای پیکربندی شده مورد آزمایش برابر باشد.

اصلاح: کلید قابل اطمینان NTP را با استفاده از دستورات زیر پیکربندی نمایید.

```
hostname(config)#ntp trusted-key {ntp_key_id}
```

تاثیر: سازمان‌ها باید ۳ میزبان NTP برای تنظیم زمان ثابت در کل سازمان ایجاد نمایند. فعال کردن فرمان "ntp trusted-key"، احراز هویت رمزگذاری شده بین میزبان‌های NTP را اجرا می‌کند.

مقدار پیش‌فرض: احراز هویتِ هویت سیستم، غیرفعال می‌باشد.

۲-۳-۱-۴ "key" را برای هر "ntp server" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: کلید احراز هویت را برای NTP مشخص کنید.

دلیل: این ویژگی احراز هویت، محافظت در برابر همگام‌سازی تصادفی سیستم با سیستم غیر قابل اعتماد دیگر را فراهم می‌سازد، محافظت به این دلیل انجام می‌گیرد که سیستم دیگر باید کلید احراز هویت درست را بداند.

بررسی: از خط فرمان، دستورات زیر را اجرا نمایید:

```
hostname#show run | include ntp server
```

اصلاح: هر سرور NTP را برای استفاده از زنجیره کلید با استفاده از دستور زیر پیکربندی نمایید.

```
hostname(config)#ntp server {ntp-server_ip_address}{key ntp_key_id}
```

تاثیر: سازمان‌ها باید ۳ میزبان NTP برای تنظیم زمان ثابت در کل سازمان ایجاد نمایند. فعال کردن فرمان "ntp server key"، احراز هویت رمزگذاری شده بین میزبان‌های NTP را اجرا می‌کند.

مقدار پیش‌فرض: کلید NTP به صورت پیش‌فرض تعریف نشده است.

۲-۳-۲ "ip address" را برای "ntp server" تنظیم کنید

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: از این دستور در صورتی که می‌خواهید به سیستم اجازه همگام‌سازی ساعت نرم‌افزاری سیستم با سرور NTP مشخص شده را بدهید، استفاده نمایید.

دلیل: برای حصول اطمینان از اینکه زمان در مسیریاب سیسکو با بقیه دستگاه‌های شبکه شما سازگار است، حداقل ۲ (و ترجیحا حداقل ۳) سرور NTP خارج از مسیریاب باید پیکربندی شود. همچنین از پیکربندی دلیله زمانی و تنظیمات تغییر ساعت تابستانی تمام دستگاه‌ها اطمینان حاصل نمایید. برای سادگی، مقدار پیش فرض UTC استفاده نمایید.

بررسی: از خط فرمان، دستورات زیر را اجرا نمایید:

```
hostname#sh ntp associations
```

اصلاح: حداقل یک سرور NTP خارجی را با استفاده از دستور زیر پیکربندی نمایید.

```
hostname(config)#ntp server {ip address}
```

تاثیر: سازمان‌ها باید ۳ میزبان NTP برای تنظیم زمان ثابت در کل سازمان ایجاد نمایند. فعال کردن فرمان "ntp server ip address"، احراز هویت رمزگذاری شده بین میزبان‌های NTP را اجرا می‌کند.

مقدار پیش‌فرض: سروری به صورت پیش‌فرض پیکربندی نشده است.

۴-۲ قوانین Loopback

زمانی که یک مسیریاب می‌خواهد اتصالی به سرور راه دور مانند SYSLOG یا NTP برقرار کند، از نزدیکترین رابط برای آدرس منبع استفاده خواهد کرد. این امر می‌تواند مشکلاتی را به دلیل تفاوت احتمالی در منبع به وجود آورد که به صورت بالقوه باعث عدم قبولی بسته‌ها در دیواره آتش و یا به کارگیری نادرست توسط میزبان دریافت کننده می‌شود.

برای جلوگیری از این مشکلات، مسیریاب باید با یک رابط loopback پیکربندی شود تمام سرویس‌ها باید به این آدرس محدود شوند.

۲-۴-۱ یک "interface loopback" ایجاد نمایید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: یک رابط loopback پیکربندی نمایید.

دلیل: رابط loopback نرم‌افزاری، یک رابط همیشه فعال را شبیه سازی می‌کند. این رابط یک رابط مجازی می-باشد که در تمام پلتفرم‌ها پشتیبانی می‌شود. دیگر آدرس‌های loopback باعث سوءاستفاده، پیکربندی اشتباه و تناقضات احتمالی می‌شود. رابط‌های loopback اضافی باید قبل از استفاده توسط پرسنل امنیتی محلی ثبت و تایید شوند.

بررسی: دستور زیر را برای بررسی تنظیم یک رابط loopback اجرا نمایید. بررسی کنید که یک آدرس IP برای رابط loopback تعریف شده، برگردد.

```
hostname#sh ip int brief | incl Loopback
```

اصلاح: یک رابط loopback تعریف و پیکربندی نمایید.

```
hostname(config)#interface loopback <number>
hostname(config-if)#ip address <loopback_ip_address> <loopback_subnet_mask>
```

تاثیر: سازمان‌ها باید برنامه ریزی کرده و رابط‌های loopback را برای شبکه سازمانی خود ایجاد نمایند. رابط-های loopback اطلاعات شبکه‌ای حیاتی مانند شناسه‌های OSPF مسیریاب و نقاط قطع برای جلسات پروتکل مسیریابی را فراهم می‌آورد.

مقدار پیش‌فرض: رابط loopback به صورت پیش‌فرض تعریف نشده است.

۲-۴-۲ برای AAA "source-interface" را تنظیم نمایید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: AAA را به استفاده از آدرس IP یک رابط مشخص، برای تمامی بسته‌های AAA خروجی وادار نمایید.

دلیل: این کار لازم است تا سرور AAA (RADIUS یا TACACS+) به راحتی مسیریاب‌ها را شناسایی کرده و درخواست‌ها را با آدرس IP آنها احراز هویت نماید.

بررسی: دستور زیر را برای بررسی محدود بودن سرویس‌های AAA به یک رابط منبع اجرا نمایید. بررسی کنید که در نتیجه یک رشته برگردد.

```
hostname#sh run | incl tacacs source | radius source
```

اصلاح: سرویس‌های AAA را به رابط loopback محدود نمایید.

```
Hostname(config)#ip {tacacs|radius} source-interface loopback
{loopback_interface_number)
```

تاثیر: سازمان‌ها باید AAA را برای نظارت موثر بر دستگاه‌های شبکه سازمانی خود طراحی و پیاده‌سازی نمایند. محدود کردن سرویس‌های AAA به loopback رابط منبع این سرویس‌ها را فعال می‌سازد.

۲-۴-۳ "ntp source" را به رابط loopback تنظیم نمایید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: یک آدرس منبع خاص را در بسته‌های NTP استفاده نمایید.

دلیل: آدرس منبع را برای استفاده در ارسال ترافیک NTP، تنظیم نمایید. این زمانی ممکن است ضروری باشد که سرور NTP که با آن ارتباط برقرار می‌کنید ترافیک را بر اساس آدرس IP فیلتر می‌کند.

بررسی: دستور زیر را برای بررسی محدود بودن سرویس‌های NTP به یک رابط منبع اجرا نمایید. بررسی کنید که در نتیجه یک رشته برگردد.

```
hostname#sh run | incl ntp source
```

اصلاح: سرویس‌های NTP را به رابط loopback محدود نمایید.

```
hostname(config)#ntp source loopback {loopback_interface_number}
```

تاثیر: سازمان‌ها باید سرویس‌های NTP برای ایجاد زمان رسمی برای تمامی دستگاه‌های شبکه سازمانی را برنامه ریزی و پیاده سازی کنند. تنظیم "ntp source loopback" باعث اعمال آدرس IP مناسب برای سرویس-های NTP می‌شود.

مقدار پیش‌فرض: آدرس منبع توسط رابط خروجی مشخص می‌شود.

۲-۴-۴ "ip tftp source-interface" را به رابط loopback تنظیم نمایید

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: آدرس IP یک رابط را به عنوان آدرس منبع اتصالات TFTP مشخص کنید.

دلیل: این کار از آن جهت ضروری می‌باشد که سرورهای TFTP به راحتی بتوانند بر اساس آدرس IP، مسیریابها را شناسایی و درخواست‌ها را احراز هویت نمایند.

بررسی: دستور زیر را برای بررسی محدود بودن سرویس‌های TFTP به یک رابط منبع اجرا نمایید. بررسی کنید که در نتیجه یک رشته برگردد.

```
hostname#sh run | incl tftp source-interface
```

اصلاح: سرویس‌های TFTP را به رابط loopback محدود نمایید.

```
hostname(config)#ip tftp source-interface loopback
```

تاثیر: سازمان‌ها باید سرویس‌های TFTP را برای سازمان برنامه ریزی و پیاده سازی کنند. تنظیم " tftp source-interface loopback" باعث فعال سازی شناسایی مسیریاب‌ها و احراز هویت درخواست‌ها بر اساس آدرس IP در سرورهای TFTP می‌شود.

مقدار پیش‌فرض: آدرس نزدیکترین رابط به مقصد به عنوان آدرس منبع انتخاب می‌شود.

۳ واحد داده

واحد داده به سرویس‌ها و تنظیمات مرتبط با انتقال داده‌ها از طریق روترها اطلاق می‌گردد.واحد داده همه موارد را شامل می‌شود و اختصاصی به واحدهای کنترلی و مدیریتی ندارد. تنظیمات یک روتر در ارتباط با واحد داده‌ها شامل پیکربندی‌های مربوط به لیست اینترفیس‌های دسترسی،IPSecتنظیمات مربوط بهNAT ها و همچنین اعمال پیکربندی‌های ممکن برای کنترل ترافیک عبوری از روترها را شامل می‌گردد.

۳-۱ قوانین مسیردهی

سرویس‌های غیرضروری بایستی غیرفعال گردند.

۳-۱-۱ نحوه تنظیم کردن "no ip source-route"

کاربست‌پذیری پروفایل:

- سطح ۱

توضیح: برای مدیریت هرچه بهتر پکت‌های ip بهتر است هدرهای غیرضروری را غیرفعال نمایید.

دلیل: مسیردهی از مبدا یکی از ویژگی‌هایی است که برای هدایت تک تک پکت‌ها استفاده می‌شود. از این ویژگی در ساختار بسیاری از حملات مربوط به روترهای cisco استفاده شده است. اغلب روترهای شرکت cisco پردازش و دریافت این گونه پکت‌ها را قبول می‌کنند، مگر اینکه این ویژگی در ساختار روتر غیرفعال شده باشد.

بررسی: به جهت آگاهی از فعال بودن این سرویس کافی است از دستور زیر استفاده نمایید.

```
hostname#sh run | incl ip source-route
```

اصلاح: برای غیرفعال‌سازی این سرویس کافی است از دستور زیر استفاده نمایید.

```
hostname(config)#no ip source-route
```

تاثیر: سازمان‌ها بایستی با در نظر گرفتن سیاست‌های خود سرویس‌هایی که مد نظرشان نمی‌باشد را غیرفعال نموده تا به این طریق از نفوذپذیری به چهارچوب شبکه تا حد زیادی جلوگیری نمایند. یکی از این سرویس‌ها، "ip source-route" است که بایستی غیرفعال باشد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس فعال می‌باشد.

۳-۱-۲ نحوه تنظیم "no ip proxy-arp"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: "proxy ARP" بایستی برای تمام واسط‌ها غیرفعال گردد.

توضیح: با استفاده از پروتکل ARP می‌توانیم در لایه ۲ یعنی لایه Network یک ترجمه مناسب بین آدرس ip و آدرسMAC ایجاد نماییم. از سرویس "proxy ARP" برای فهمیدن ادرس‌های دستگاه‌های موجود در شبکه می‌توانیم استفاده کنیم تا به این طریق ترافیک مورد نظر را به سمت یک دستگاه خاص صادر نماییم تا با این کار پیام‌های broadcast را در محدوده مشخصی ارسال نماییم. برای برقراری هرچه بیشتر امنیت در شبکه لازم است تا پیام‌های "proxy ARP" هرچه بیشتر محدود شوند.

بررسی: برای اطلاع از فعال بودن این سرویس کافی است از دستور زیر استفاده کنید.

```
hostname#sh ip int {interface} | incl proxy-arp
```

اصلاح: به جهت غیرفعال سازی این سرویس از دستور زیر استفاده کنید.

```
hostname(config)#interface {interface} hostname(config-if)#no ip proxy-arp
```

تاثیر: سازمان‌ها بایستی با در نظر گرفتن سیاست‌های خود سرویس‌هایی که مد نظرشان نمی‌باشد را غیرفعال نموده تا به این طریق از نفوذپذیری به چهارچوب شبکه تا حد زیادی جلوگیری نمایند. یکی از این سرویس‌ها، "ip-proxy-arp" است که بایستی غیرفعال باشد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس فعال می‌باشد.

۳-۱-۳ نحوه فعال‌سازی "no interface tunnel"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: فعال بودن سرویس "no interface tunnel" قابل تشخیص می‌باشد.

دلیل: از سرویس " tunnel interface " برای انجام کارهای مخرب استفاده می‌شود. بنابراین یک مدیر شبکه در استفاده از این سرویس در شبکه خود و جوانب آن بایستی کاملا آگاه باشد.

بررسی: برای اطلاع یافتن از فعال بودن این سرویس کافی است از دستور زیر استفاده نمایید.

```
hostname#sh ip int brief | incl tunnel
```

اصلاح: برای غیرفعال کردن سرویس ذکر شده می‌توانید از دستور زیر استفاده کنید.

```
hostname(config)#no interface tunnel {instance}
```

تاثیر: سازمان‌ها بایستی با در نظر گرفتن سیاست‌های خود سرویس‌هایی که مد نظرشان نمی‌باشد را غیرفعال نموده تا به این طریق از نفوذپذیری به چهارچوب شبکه تا حد زیادی جلوگیری نمایند. یکی از این سرویس‌ها، "tunnel interfaces" است که بایستی غیرفعال باشد تا از بروز حملات مختلف در شبکه جلوگیری گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس غیرفعال می‌باشد.

۳-۱-۴ نحوه تنظیم کردن "ip verify unicast source reachable-via "

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: بررسی پکت‌های ورودی به منظور تشخیص ادرس فرستنده پکت‌های دریافتی صورت می‌گیرد.

دلیل: برای جلوگیری از ip-spoofing می توانیم این سرویس را غیرفعال نماییم.

بررسی: به جهت اطلاع از فعال بودن این سرویس می‌توانید از این دستور استفاده نمایید.

```
hostname#sh ip int {interface} | incl verify source
```

اصلاح: به جهت غیرفعال کردن این سرویس می‌توانید از دستور زیر استفاده کنید.

```
hostname(config)#interface {interface_name} hostname(config-if)#ip verify unicast
source reachable-via rx
```

تاثیر: سازمان‌ها بایستی با در نظر گرفتن سیاست‌های خود سرویس‌هایی که مد نظرشان نمی‌باشد را غیرفعال نموده تا به این طریق از نفوذپذیری به چهارچوب شبکه تا حد زیادی جلوگیری نمایند.

مقدار پیش‌فرض: به صورت پیش‌فرض این سرویس غیرفعال می‌باشد

۳-۲ اعمال "border Router Filtering"

با استفاده از"border filtering " می‌توانیم شبکه داخلی خود را به یک شبکه خارجی الحاق نماییم و همچنین عملیات فیلترینگ را به طور مناسب بر روی شبکه انجام دهیم.

۳-۲-۱ نحوه تنظیم "ip access-list extended" به جهت ممانعت از دسترسی آدرس‌های خصوصی از شبکه‌های خارجی

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: دستوری که در ادامه معرفی خواهد شد، روتر را در مد پیکربندی "access-list" قرار می‌دهد. از این دستور می‌توانید برای اعمال قوانین ممنوعیتی و یا مجاز در دسترسی به قسمت‌های مختلف شبکه استفاده نمایید.

دلیل: پیکربندی‌های کنترلی مربوط به دسترسی می‌تواند در جلوگیری از حملاتی مانند " spoofing" بسیار موثر باشد. برای کاهش اثربخشی "ip spoofing" می‌توانیم از پیکربندی‌های تنظیم شده در ارتباط با کنترل دسترسی استفاده نماییم تا بدین طریق از دسترسی آدرس‌های غیرمجازشبکه‌های خارجی ممانعت گردد. با استفاده از سیاست‌های تعبیه شده در یک سازمان می‌توان قوانینی در زمینه کنترل دسترسی‌ها اعمال نمود.

بررسی: به جهت بررسی لیست آدرس‌های دسترسی می‌توانیم از دستور زیر استفاده کنیم.

```
hostname#sh ip access-list {name | number}
```

اصلاح: از پیکربندی مربوط به ACL برای محدود ساختن هرچه بیشتر آدرس‌های خارجی می‌توان استفاده نمود.

```
hostname(config)#ip access-list extended {name | number}

hostname(config-nacl)#deny ip {internal_networks} any log hostname(config-
nacl)#deny ip 127.0.0.0 0.255.255.255 any log

hostname(config-nacl)#deny ip 10.0.0.0 0.255.255.255 any log

hostname(config-nacl)#deny ip 0.0.0.0 0.255.255.255 any log

hostname(config-nacl)#deny ip 172.16.0.0 0.15.255.255 any log

hostname(config-nacl)#deny ip 192.168.0.0 0.0.255.255 any log

hostname(config-nacl)#deny ip 192.0.2.0 0.0.0.255 any log

hostname(config-nacl)#deny ip 169.254.0.0 0.0.255.255 any log

hostname(config-nacl)#deny ip 224.0.0.0 31.255.255.255 any log

hostname(config-nacl)#deny ip host 255.255.255.255 any log

hostname(config-nacl)#permit {protocol} {source_ip} {source_mask} {destination}
{destination_mask} log

hostname(config-nacl)#deny any any log

hostname(config)#interface <external_interface>

hostname(config-if)#access-group <access-list> in
```

تاثیر: سازمان‌ها بایستی چارچوب سیاستی خود را به گونه‌ای مشخص نمایند که حد و مرزهای بین شبکه داخلی و خارجی حفظ گردد. به همین جهت می‌توان از 'ip access-list' استفاده نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این لیست دسترسی تعریف نمی‌شود.

۳-۲-۲ نحوه تنظیم "ip access group"بر روی رابط خارجی

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: دستوری که در ادامه معرفی خواهد شد، روتر را در مد پیکربندی "access-list" قرار می‌دهد. از این دستور می‌توانید برای اعمال قوانین ممنوعیتی و یا مجاز در دسترسی به قسمت‌های مختلف شبکه استفاده نمایید.

دلیل: پیکربندی‌های کنترلی مربوط به دسترسی می‌تواند در جلوگیری از حملاتی مانند " spoofing" بسیار موثر باشد. برای کاهش اثربخشی "ip spoofing" می‌توانیم از پیکربندی‌های تنظیم شده در ارتباط با کنترل دسترسی استفاده نماییم تا بدین طریق از دسترسی آدرس‌های غیرمجازشبکه‌های خارجی ممانعت گردد. با استفاده از سیاست‌های تعبیه شده در یک سازمان می‌توان قوانینی در زمینه کنترل دسترسی‌ها اعمال نمود.

بررسی: به جهت بررسی "access group" بر روی یک واسط مناسب می‌توانید از دستور زیر استفاده کنید.

```
hostname#sh run | sec interface {external_interface}
```

اصلاح: برای تنظیم "access group" بر روی یک واسط خارجی می‌توانیم دستور زیر را به کار بریم.

```
hostname(config)#interface {external_interface} hostname(config-if)#ip access-group
{name | number} in
```

تاثیر: سازمان‌ها بایستی با توجه به سیاست‌های مد نظر خود و با استفاده از یک طرح مناسب و قابل پیاده‌سازی لیست دسترسی خود را ایجاد نمایند. برای ایجاد این لیست دسترسی می‌توانیم از دستور " ip access group" استفاده کنیم.

مقدار پیش‌فرض: به صورت پیش‌فرض این لیست دسترسی تعریف نمی‌شود.

۳-۳ Neighbor Authentication

فعال‌سازی احراز هویت در عملیات مسیریابی

۳-۳-۱ نیاز به احراز هویت "EIGRP" در زمان استفاده از پروتکل‌های مسیریابی

بررسی احراز هویت EIGRP به جهت فعال‌سازی آن در مواقعی که از پروتکل‌های مسیریابی استفاده می‌شود.

۳-۳-۱-۱ نحوه تنظیم "key chain"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: با استفاده از تعریف "key chain" می‌توان عملیات احراز هویت را در هنگام استفاده از پروتکل‌های مسیریابی انجام داد. "key chain" حداقل بایستی یک کلید داشته باشد و تعداد کلیدها می تواند تا 2,147,483,647 افزایش یابد.
توجه: از "key chains" فقط در EIGRP و DRP و RIPv2 می‌توان استفاده نمود.

دلیل: پروتکل‌های مسیریابی هم‌چون EIGRP و DRP و RIPv2 توانایی استفاده از "key chain" به جهت احرازهویت دارند.

بررسی: به جهت اطلاع یافتن از تعریف یک "key chain" مناسب می‌توانیم از دستور زیر استفاده کنیم.

```
hostname#sh run | sec key chain
```

اصلاح: برای ایجاد یک "key chain" از دستور زیر می‌توانیم استفاده کنیم.

```
hostname(config)#key chain {key-chain_name}
```

تاثیر: سازمان‌ها بایستی بر اساس متدهای به کار گرفته شده درپروتکل‌های مسیردهی به جهت احراز هویت بایستی سیاست‌های امنیتی مناسب را طرح‌ریزی و اجرا نمایند. استفاده از "key chain" برای اعمال چنین سیاست‌های برای یک شبکه مناسب می‌باشد.

مقدار پیش‌فرض: به صورت پیش‌فرض "key chain" تنظیم نشده است.

۳-۳-۱-۲ نحوه فعال‌سازی "key"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: پیکربندی مربوط به احراز هویت "key" با استفاده از "key chain"

دلیل: این پیکربندی جزوی از تنظیمات مربوط به احراز هویت در مسیریابی می‌باشد.

بررسی: به منظور مطلع شدن از تعریف یک "key chain" مناسب از دستور زیر می‌توان استفاده نمود.

```
hostname#sh run | sec key chain
```

اصلاح: برای اعمال این پیکربندی از دستور زیر می‌توانید استفاده نمایید.

```
hostname(config-keychain)#key {key-number}
```

تاثیر: سازمان‌ها بایستی بر اساس متدهای به کار گرفته شده درپروتکل‌های مسیردهی به جهت احراز هویت بایستی سیاست‌های امنیتی مناسب را طرح‌ریزی و اجرا نمایند. استفاده از "key number" در پیکربندی‌های مربوط به "key chain"برای اعمال چنین سیاست‌های برای یک شبکه مناسب تلقی می‌گردد.

۳-۳-۱-۳ نحوه تنظیم کردن "key string"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: نحوه انجام پیکربندی مربوط به احراز هویت رشته‌ای برای یک کلید.

دلیل: این پیکربندی بخشی از تنظیمات مربوط به احراز هویت در مسیریابی می‌باشد.

بررسی: به منظور مطلع شدن از تعریف یک "key chain" مناسب از دستور زیر می‌توان استفاده نمود.

```
hostname#sh run | sec key chain
```

اصلاح: اعمال پیکربندی مربوط به "key string" به صورت زیر می‌باشد.

```
hostname(config-keychain-key)#key-string <key-string>
```

تاثیر: : سازمان‌ها بایستی بر اساس متدهای به کار گرفته شده درپروتکل‌های مسیردهی به جهت احراز هویت بایستی سیاست‌های امنیتی مناسب را طرح‌ریزی و اجرا نمایند. استفاده از "key string" در پیکربندی‌های مربوط به "key chain"برای اعمال چنین سیاست‌های برای یک شبکه مناسب تلقی می‌گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی تنظیم نمی‌گردد.

۳-۳-۱-۴ نحوه تنظیم کردن "address-family ipv4 autonomous-system"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: اعمال پیکربندی "EIGRP address family"

دلیل: BGP یک پروتکل تشکیل شده از چند پروتکل برای انجام عمل مسیریابی است و ویژگی "address-family" می‌تواندمنجر به محدود سازی انجام عملیات مبادله با یکسری از نودهای همسایه گردد.

بررسی: به جهت اطمینان یافتن از فعال بودن ویژگی "address-family" از دستور زیر می‌توانید استفاده کنید.

```
hostname#sh run | sec router eigrp
```

اصلاح: برای اعمال پیکربندی‌های مربوط به EIGRP در ارتباط با "address-family" از دستورات زیر می‌توانید استفاده کنید.

```
hostname(config)#router eigrp <virtual-instance-name>
hostname(config-router)#address-family ipv4 autonomous-system {eigrp_as-number}
```

تاثیر: سازمان‌ها بایستی بر اساس متدهای به کار گرفته شده درپروتکل‌های مسیردهی به جهت احراز هویت بایستی سیاست‌های امنیتی مناسب را طرح‌ریزی و اجرا نمایند. استفاده از "address-family " در پیکربندی‌های مربوط به EIGRP برای اعمال چنین سیاست‌های برای یک شبکه مناسب تلقی می‌گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نشده است.

۳-۳-۱-۵ نحوه تنظیم نمودن "af-interface default"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: برای تعریف نمودن کاربرانی که قصد داریم واسط EIGRP به صورت پیش‌فرض بر روی آنها اعمال گردد، به "address-family" وابسته خواهد بود.

دلیل: تنظیم نمودن بخشی از "EIGRP address-family".

بررسی: با انجام دستور زیر می‌توانید از تنظیمات این بخش مطلع گردید.

```
hostname#sh run | sec router eigrp
```

اصلاح: برای پیکربندی از دستورات زیر می‌توانید استفاده نمایید.

```
hostname(config)#router eigrp <virtual-instance-name>
hostname(config-router)#address-family ipv4 autonomous-system {eigrp_as-number}
hostname(config-router-af)#af-interface default
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. استفاده از 'af-interface default' برای واسط‌های EIGRP می‌تواند در نائل شدن به اهداف بالا کارا تلقی گردد و با محدودسازی هرچه بیشتر تبادلات بین شبکه‌ها موثر واقع گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نشده است.

۳-۳-۱-۶ نحوه تنظیم نمودن "authentication key-chain"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: پیکربندی "EIGRP address family key chain"

دلیل: این تنظیمات در حوزه پیکربندی‌های مربوط به احراز هویت "EIGRP" می‌باشد.

بررسی: به جهت مطلع شدن از تنظیم "key chain" مناسب از دستور زیر می‌توانید استفاده کنید.

```
hostname#sh run | sec router eigrp
```

اصلاح: برای اعمال پیکربندی‌های مربوط به "EIGRP address family key chain" از دستور زیر می‌توانید استفاده کنید.

```
hostname(config)#router eigrp <virtual-instance-name>

hostname(config-router)#address-family ipv4 autonomous-system {eigrp_as-number}

hostname(config-router-af)#af-interface {interface-name}

hostname(config-router-af-interface)#authentication key-chain {eigrp_key
chain_name}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. استفاده از "address-family" برای واسطهای EIGRP می‌تواند در نائل شدن به اهداف بالا کارا تلقی گردد و با محدودسازی هرچه بیشتر تبادلات بین شبکه‌ها موثر واقع گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این مقدار "key chain" برای "EIGRP"فعال نمی‌باشد.

۳-۳-۱-۷ نحوه تنظیم کردن "authentication mode md5"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: با پیکربندی‌های مربوط به احراز هویت می‌توانیم از ورود منابع تائید نشده با نمایش پیام‌های مربوطه تا حد ممکن جلوگیری کنیم.

دلیل: این پیکربندی مربوط به بخشی از تنظیمات احراز هویتی EIGRP می‌باشد.

بررسی: با استفاده از دستور زیر می‌توانید از تنظیم شدن مد احراز هویتی "address family" اطمینان حاصل نمایید.

```
hostname#sh run | sec router eigrp
```

اصلاح: درصورت تنظیم نبودن این مد کافی است با استفاده از دستور زیر آن را فعال نمایید.

```
hostname(config)#router eigrp <virtual-instance-name>
hostname(config-router)#address-family ipv4 autonomous-system {eigrp_as-number}
hostname(config-router-af)#af-interface {interface-name}
hostname(config-router-af-interface)#authentication mode md5
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. به کار بردن " authentication mode" برای "EIGRP address-family" می‌تواند در محدودسازی هرچه بیشتر و اعمال سیاست‌های بین شبکه‌ها موثر واقع گردد.

مقدار پیش‌فرض: به صورت پیش‌فرض این مقدار تعریف نشده می‌باشد.

۳-۳-۱-۸ نحوه تنظیم کردن "ip authentication key-chain eigrp"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: مشخص کردن نوع احراز هویتی که درهر نوع واسط EIGRP استفاده می‌شود.

دلیل:با پیکربندی مربوط به احراز هویت در EIGRP و اعمال"key-chain number" مبادله پکت‌ها بین شبکه‌ها بسیار محدود خواهد شد.

بررسی: برای اطلاع یافتن از تنظیم شدن یک "key chain" بر روی یک اینترفیس مناسب کافی است از دستور زیر استفاده نماییم.

```
hostname#sh run int {interface_name} | incl key-chain
```

اصلاح: برای پیکربندی واسط با "EIGRP key chain" از دستور زیر می‌توانید استفاده کنید.

```
hostname(config)#interface {interface_name}
hostname(config-if)#ip authentication key-chain eigrp {eigrp_as-number} {eigrp_key-chain_name}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با پیکربندی " ip authentication key chain" بر روی واسط EIGRP می‌توانیم این سیاست‌های مورد نظر را اعمال نماییم.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نمی‌شود.

۳-۳-۱-۹ نحوه تنظیم کردن " ip authentication mode eigrp' "

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: با پیکربندی‌های مربوط به احراز هویت می‌توانیم از ورود منابع تائید نشده با نمایش پیام‌های مربوطه تا حد ممکن جلوگیری کنیم.

دلیل: این پیکربندی مربوط به بخشی از تنظیمات "EIGRP" می‌باشد.

بررسی: با استفاده از دستور زیر می‌توانید از تعریف یک مد مربوط به احراز هویت بر روی یک واسط مناسب مطمئن شوید.

```
hostname#sh run int {interface_name} | incl authentication mode
```

اصلاح:. در صورتی که بخواهید این پیکربندی را انجام دهید، می‌توانید با استفاده از دستور زیر واسط خود را بر روی "EIGRP authentication mode " تنظیم نمایید.

```
hostname(config)#interface {interface_name} hostname(config-if)#ip authentication
mode eigrp {eigrp_as-number} md5
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی مربوط به " ip authentication mode'" بر روی یک اینترفیس برای EIGRP توسط اعداد یا مدهای کاری می‌توانید سیاست-های محدود کننده مناسبی را برای تبادلات بین شبکه‌ها ایجاد نمایید.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نمی‌شود.

۳-۳-۲ نیاز به احراز هویت OSPF در پروتکل‌های استفاده شده

برای بررسی فعال بودن احراز هویت مربوط به OSPF در مواقعی که این کار عملی می‌باشد صورت می‌گیرد.

۳-۳-۲-۱ نحوه تنظیم نمودن "authentication message-digest" برای "OSPF area"

کاربست‌پذیری پروفایل:

- سطح 2

توضیح: فعال‌سازی احراز هویت MD5 برای OSPF

دلیل: این پیکربندی مربوط به بخش از تنظیمات احراز هویتی OSPF است.

بررسی: به جهت مطلع شدن از تعریف "message digest" برای OSPF از دستور زیر استفاده نمایید.

```
hostname#sh run | sec router ospf
```

اصلاح: برای پیکربندی "message digest" برای OSPE از دستور زیر می‌توانید استفاده کنید.

```
hostname(config)#router ospf <ospf_process-id>
hostname(config-router)#area <ospf_area-id> authentication message-digest
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی مربوط به "authentication message-digest" برای OSPF می‌توانید سیاست‌های محدود کننده مناسبی را برای تبادلات بین شبکه‌ها ایجاد نمایید.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی تنظیم نشده است.

۳-۳-۲-۲ نحوه تنظیم "ip ospf message-digest-key md5"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: فعال‌سازی احراز هویت "OSPF MD5 ".

دلیل: این پیکربندی بخشی از تنظیمات مربوط به احراز هویتOSPF می‌باشد.

بررسی: برای مطلع شدن از تعریف "MD5 key" روی یک اینترفیس مناسب از دستور زیر می‌توانید استفاده نمایید.

```
hostname#sh run int {interface}
```

اصلاح: برای تنظیم نمودن یک اینترفیس مناسب برای "Message Digest authentication" می‌توانید از دستور زیر استفاده کنید.

```
hostname(config)#interface {interface_name}
hostname(config-if)#ip ospf message-digest-key {ospf_md5_key-id} md5 {ospf_md5_key}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی مناسب برای " ip ospf message-digest-key md5"می‌توانید سیاست‌های محدود کننده مناسبی را برای تبادلات بین شبکه‌ها ایجاد نمایید.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی تنظیم نشده است.

۳-۳-۳ نیاز به احراز هویت RIPv2در پروتکل‌های استفاده شده

پروتکل RIP نمونه‌ای از پروتکل‌های اصلی است که برای مسیریابی داخلی در برخی از شبکه‌ها استفاده می‌گردد. پروتکل RIP جزء پروتکل‌های پیچیده‌ای محسوب می‌شود که گزینه‌های مختلفی در انجام پیکربندی دارا بوده که برخی از فواید این گزینه‌ها در شروع امکان دارد چندان واضح نباشد. با بررسی پروتکل RIP با دو گونه از تنظیمات مربوط به احراز هویت مواجه خواهیم بود که در مواقعی که به صورت عملی از این پروتکل استفاده می‌شود، قابل مشاهده خواهد بود.

۳-۳-۳-۱ نحوه تنظیم نمودن "key chain"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: با تعریف "authentication key chain" می‌توان ویژگی احراز هویت را برای پروتکل مسیریابی RIPv2فعال نمود.

دلیل: این ویژگی بخی از فرایند احراز هویت در مسیریابی می‌باشد.

بررسی: با استفاده از دستور زیر می‌توانید از تعریف یک "key chain" مناسب مطلع گردید.

```
hostname#sh run | sec key chain
```

اصلاح: برای منتشر نمودن یک "" مناسب از دستور زیر استفاده نمایید.

```
hostname(config)#key chain {rip_key-chain_name}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی مناسب در بخش احراز هویت مربوط به "key-chain" برای پروتکل RIPv2 می‌توانید سیاست‌های محدود کننده مناسبی را برای تبادلات بین شبکه‌ها ایجاد نمایید.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی تنظیم نشده است.

۳-۳-۳-۲ نحوه تنظیم نمودن "key"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: پیکربندی کلید احراز هویت روی یک "key chain"

دلیل: این پیکربندی بخشی از تنظیمات مربوط به احراز هویت در مسیردهی می‌باشد.

```
hostname#sh run | sec key chain
```

اصلاح: برای اعمال پیکربندی "key number".

```
hostname(config-keychain)#key {key-number}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی مناسب در بخش احراز هویت مربوط به "key " برای پروتکل RIPv2 می‌توانید سیاست‌های محدود کننده مناسبی را برای تبادلات بین شبکه‌ها ایجاد نمایید.

۳-۳-۳-۳ نحوه تنظیم نمودن "key-string"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: نحوه پیکربندی احراز هویت "string" برای یک "key"

دلیل: این پیکربندی بخشی از تنظیمات مربوط به احراز هویت در مسیریابی می‌باشد.

بررسی: ابتدا بایستی بررسی نمایید که یک "key chain" مناسب تعریف شده است.

```
hostname#sh run | sec key chain
```

اصلاح: پیکربندی "key string" به صورت زیر می‌باشد.

```
hostname(config-keychain-key)#key-string <key-string>
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با استفاده از "key-string" برای یک "key chains" می‌توان سیاست‌های مناسبی روی پروتکل‌های مسیریابی اعمال نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نمی‌شود.

۳-۳-۳-۴ نحوه تنظیم نمودن "ip rip authentication key chain"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: با فعال‌سازی احراز هویت در پروتکل RIPv2 می‌توان از تنظیمات مربوط به "key" در یک اینترفیس مطمئن شد.

دلیل: این پیکربندی جزوی از تنظیمات مربوط به احراز هویت RIPv2می‌باشد.

بررسی: با استفاده از دستور زیر می‌توانید از فعال بودن یک "key chain"بر روی یک اینترفیس مطلع شوید.

```
hostname#sh run int {interface_name}
```

اصلاح: برای پیکربندی اینترفیس با استفاده از پروتکل RIPv2 و تنظیم "key chain" از دستور زیر می‌توان استفاده کرد.

```
hostname(config)#interface {interface_name}
hostname(config-if)#ip rip authentication key-chain {rip_key-chain_name}
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با اعمال پیکربندی " ip rip authentication key chain" می‌توان سیاست‌های مناسبی روی تبادلات انجام گرفته در بین شبکه‌ها اعمال نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نشده است.

۳-۳-۳-۵ نحوه تنظیم نمودن "ip rip authentication mode" به "md5"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: نحوه پیکربندی اینترفیس با استفاده از "RIPv2 key chain"

دلیل: این پیکربندی بخشی از تنظیمات احراز هویت RIPv2 می‌باشد.

بررسی: با استفاده از دستور زیر می‌توانید پیکربندی مناسبی را روی اینترفیس مناسب اعمال نمایید.

```
hostname#sh run int <interface>
```

اصلاح: با دستور زیر می‌توانید احراز هویت مربوط به RIPv2 بر روی اینترفیس ضروری تنظیم نمایید.

```
hostname(config)#interface <interface_name> hostname(config-if)#ip rip
authentication mode md5
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با استفاده از " ip rip authentication mode md5" می‌توان سیاست‌های مناسبی روی تبادلات انجام گرفته در بین شبکه‌ها اعمال نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نشده است.

۳-۳-۴ نیاز به احراز هویت BGP در پروتکل‌های استفاده شده

پروتکل BGP یکی از پروتکل‌های اصلی کاربردی در زمینه هدایت و مسیریابی می‌باشد. پروتکل BGPجزء پروتکل‌های پیچیده‌ای محسوب می‌شود که گزینه‌های مختلفی در انجام پیکربندی دارا بوده که برخی از فواید این گزینه‌ها در شروع امکان دارد چندان واضح نباشد. با بررسی پروتکل RIP با دو گونه از تنظیمات مربوط به احراز هویت مواجه خواهیم بود که در مواقعی که به صورت عملی از این پروتکل استفاده می‌شود، قابل مشاهده خواهد بود.

۳-۳-۴-۱ تنظیمات مربوط به "neighbor password"

کاربست‌پذیری پروفایل:

- سطح ۲

توضیح: فعال‌سازی احراز هویت MD5 بر روی کانکشن tcp ایجاد شده در بین دو نود BGP

دلیل:با اعمال چنین قوانین مربوط به احراز هویت می‌توان از مسیریابیغیرمجاز تا حد بالایی جلوگیری نمود.

بررسی: با استفاده از دستور زیر می‌توان فهمید که آیا رمز عبور مناسب در همسایگی نودها تعریف شده است یا خیر.

```
hostname#sh run | sec router bgp
```

اصلاح: با استفاده از دستور زیر می‌توان پیکربندی‌های مربوط به احراز هویت BGP را در نودها برقرار نمود.

```
hostname(config)#router bgp <bgp_as-number>

hostname(config-router)#neighbor <bgp_neighbor-ip | peer-group-name> password
<password>
```

تاثیر: سازمان‌ها بایستی سیاست‌های امنیتی جامعی را طرح‌ریزی نمایند که به جهت انجام این‌کار به متدهای سخت‌گیرانه احراز هویت برای پروتکل‌های مسیردهی نیازمند می‌باشند. با استفاده از " neighbor password" در پروتکل BGP می‌توان سیاست‌های محدود کننده ای در زمین احراز هویت مطرح نمود.

مقدار پیش‌فرض: به صورت پیش‌فرض این پیکربندی اعمال نشده است.