پیکربندی امن

Cisco IOS 12

مرکز مدیریت راهبردی افتا

CIS-Cisco-IOS-12

اسفند ۹۵

فهرست

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

---

[1] امنیت فضای تولید و تبادل اطلاعات

[2] فناوری اطلاعات و ارتباطات

[3] Risk management

مقدمه

این سند، راهنمایی برای پیکربندی امن Cisco IOS 12 است. در این سند مقادیر و تنظیمات مناسب برای امن سازی سیاست‌ها و پیکربندهای محصول یاد شده ارائه شده است. مدیر سامانه با استفاده از این سند می‌تواند تنظیمات ارائه شده را پیاده سازی نماید.

این سند توسط شرکت "امن پردازان کویر" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Cisco IOS 12 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

۱-SCIOS- سطح مدیریت[1]

سرویس‌ها، تنظیمات و تبادل داده در یک شبکه، به نحوه پیکربندی فایروال و روش‌های احراز صلاحیت و شناسایی که توسط مدیر شبکه تنظیم می‌شود بستگی دارد. مباحثی مانند روش‌های دسترسی به تنظیمات دستگاه (telnet , ssh , http , https) ، SNMP و پروتکل‌های امنیتی مانند RADIUS و +TACACS مواردی مدیریتی هستند که در هر شبکه مهم و حائز اهمیت هستند.

۱.۱-SCIOS- قوانین احراز هویت[2]، صلاحیت‌سنجی[3] و حسابرسی[4] (AAA)

قوانین AAA به منظور کنترل دسترسی به تجهیزات، رصد تغییرات و پیکربندی‌های تجهیزات و اعمال سیاست‌های امنیتی تنظیم می‌شوند.

۱.۱.۱-SCIOS- فعال کردن AAA

این دستور مرکز کنترل دسترسی AAA را فعال می‌کند. سرویس‌های AAA یک مرکز معتبر برای مدیریت و رصد دسترسی به تجهیزات را فراهم می‌کند. وجود مرکز کنترل موجب بهبود و ثبات نظارت بر کنترل دسترسی، سرویس‌هایی که پس از دسترسی قابل ارائه هستند و حسابرسی آنچه در زمان ورود رخ داده است؛ می‌گردد. همچنین این مرکز می‌تواند به سادگی سطح دسترسی افراد را کاهش داده یا برخی دسترسی‌ها را به ویژه در شبکه‌های بزرگ معتبر یا نامعتبر کند.

نحوه پیاده‌سازی:

فعالسازی کلی AAA با دستور زیر انجام می‌شود:

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

توجه:

در صورت عدم تنظیم روش‌های دسترسی، اجرای Cisco AAA می‌تواند عملکرد شبکه را دچار اشکالات جدی نماید، بنابراین پیشنهاد می‌شود قبل از اجرای آن سازمان، سیاست و روش‌های دسترسی مانند کلمات عبور، نحوه login، چالش‌های پیش رو در این زمینه را به دقت بررسی نموده و آنچه با عنوان روش‌های صلاحیت‌سنجی و کنترل دسترسی مطرح است را انتخاب کرده باشد.

[1] Management plane

[2] Authentication

[3] Authorization

[4] Accounting

۲.۱.۱-SCIOS– فعال کردن 'aaa authentication login'

دسترسی مدیریتی به هر دستگاه در شبکه می‌تواند با عبور از فیلتر AAA انجام پذیرد. استفاده از این روش برای صدور مجوز دسترسی امکانات امن با قابلیت‌های کنترل مرکزی و پایدار را مقدور می‌سازد. به صورت پیشفرض AAA در صورت ارائه نام کاربری و کلمه عبور معتبر اجازه ورود به تنظیمات دستگاه‌ها را صادر می‌کند. این کنترل بر کلیه کاربران محلی[5] یا غیرمحلی اعمال می‌گردد. همچنین امکان ورود اضطراری به دستگاه در صورت عدم دسترسی به سرور AAA از طریق نام کاربری و کلمات عبوری که در خود دستگاه تعریف شده‌اند، امکان‌پذیر است.

نحوه پیاده‌سازی:

تنظیمات ورود مدیریتی به دستگاه‌ها از طریق AAA به روش زیر انجام می‌شود:

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

توجه:

در صورت عدم تنظیم روش‌های دسترسی، اجرای Cisco AAA می‌تواند عملکرد شبکه را دچار اشکالات جدی نماید، بنابراین پیشنهاد می‌شود قبل از اجرای آن سازمان، سیاست و روش‌های دسترسی مانند کلمات عبور، نحوه login، چالش‌های پیش رو در این زمینه را به دقت بررسی نموده و آنچه با عنوان روش‌های صلاحیت‌سنجی و کنترل دسترسی مطرح است را انتخاب کرده باشد.

۳.۱.۱-SCIOS– فعال کردن 'aaa authentication enable default'

تنظیمات این بخش به منظور ارجاع تایید ورود به محیط EXEC (که با دستور enable رخ می‌دهد) به سرور AAA جهت صلاحیت‌سنجی و احراز هویت انجام می‌شود. استفاده از این روش برای صدور مجوز دسترسی امکانات امن با قابلیت‌های کنترل مرکزی و پایدار را مقدور می‌سازد. به صورت پیشفرض AAA در صورت ارائه نام کاربری و کلمه عبور معتبر اجازه ورود به تنظیمات دستگاه‌ها را صادر می‌کند. این کنترل بر کلیه کاربران محلی یا غیرمحلی اعمال می‌گردد.

نحوه پیاده‌سازی:

فعال‌سازی AAA به منظور کنترل دسترسی بر محیط EXEC با دستور زیر انجام می‌شود:

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

توجه:

در صورت عدم انجام تنظیمات لازم در خصوص دستور enable، اجرای Cisco AAA می‌تواند دسترسی به دستگاه را دچار اشکالات جدی نماید، بنابراین پیشنهاد می‌شود قبل از اجرای آن سازمان، سیاست و روش‌های دسترسی مانند کلمات عبور، نحوه login، چالش‌های پیش رو در این زمینه را به دقت بررسی نموده و آنچه با عنوان روش‌های صلاحیت‌سنجی و کنترل دسترسی مطرح است را انتخاب کرده باشد.

[5] Local users

SCIOS-٤.١.١- تنظیم 'login authentication for 'line con 0'

در این بخش تنظیمات لازم جهت ارجاع کنترل دسترسی به AAA برای اتصال به دستگاه از طریق پورت کنسول ارائه می-گردد. برای اجرای این امر بر روی خطوط دیگر ارتباطی مانند vty لازم است تنظیمات مشابه روی آن خطوط انجام شود.

نحوه پیاده‌سازی:

فعال‌سازی AAA به منظور کنترل دسترسی از طریق پورت کنسول با دستورات زیر انجام می‌شود:

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

توجه:

به منظور جلوگیری از ایجاد اختلال در دسترسی به دستگاه از طریق پورت کنسول، لازم است قبل از فعالسازی AAA با دستور فوق، تنظیمات کنترل دسترسی با دقت انجام شود.

SCIOS-٥.١.١- تنظیم 'login authentication for 'line tty'

در این بخش تنظیمات لازم جهت ارجاع کنترل دسترسی، به AAA برای اتصال به دستگاه از طریق خط tty ارائه می‌گردد. برای اجرای این امر بر روی خطوط دیگر ارتباطی مانند vty لازم است تنظیمات مشابه روی آن خطوط انجام شود.

نحوه پیاده‌سازی:

فعال‌سازی AAA به منظور کنترل دسترسی از طریق خطوط TTY با دستورات زیر انجام می‌شود:

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

توجه:

به منظور جلوگیری از ایجاد اختلال در دسترسی به دستگاه از طریق خطوط TTY، لازم است قبل از فعالسازی AAA با دستور فوق، تنظیمات کنترل دسترسی با دقت انجام شود.

SCIOS-٦.١.١- تنظیم 'login authentication for 'line vty'

در این بخش تنظیمات لازم جهت ارجاع کنترل دسترسی، به AAA برای اتصال به دستگاه از طریق خط vty ارائه می‌گردد. برای اجرای این امر بر روی دیگر خطوط ارتباطی لازم است تنظیمات مشابه روی آن خطوط انجام شود.

نحوه پیاده‌سازی:

فعال‌سازی AAA به منظور کنترل دسترسی از طریق خطوط VTY با دستورات زیر انجام می‌شود:

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

توجه:

به منظور جلوگیری از ایجاد اختلال در دسترسی به دستگاه از طریق خطوط VTY، لازم است قبل از فعالسازی AAA با دستور فوق، تنظیمات کنترل دسترسی با دقت انجام شود.

SCIOS-۷.۱.۱- تنظیم 'aaa accounting' به منظور logنگاری دستورات

به منظور ثبت فعالیت‌های کاربران با سطوح دسترسی مختلف(log نگاری کاربران) در صورت اجرای دستور روی دستگاه لازم است قابلیت aaa accounting برای آن سطح دسترسی فعال شود. با فعالسازی این امکان، مدیریت و رصد فعالیت کاربران توسط RADIUS یا TACACS ثبت و به سرور accounting ارسال می‌گردد لذا مشاهده اقدامات کاربران و آنالیز آنها برای سازمان فراهم می‌شود.

نحوه پیاده‌سازی:

فعال‌سازی AAA Accounting برای کاربران با بالاترین سطح دسترسی(۱۵) برای کلیه دستورات، به روش زیر انجام می‌شود.

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

SCIOS-۸.۱.۱- تنظیم 'aaa accounting connection'

در این بخش نحوه تنظیم دستگاه به منظور log نگاری کلیه اتصالات به خارج دستگاه انجام می‌شود. با فعالسازی این امکان، مدیریت و رصد اتصالات دستگاه توسط RADIUS یا TACACS ثبت و به سرور accounting ارسال می‌گردد.

نحوه پیاده‌سازی:

فعال‌سازی AAA Accounting برای ثبت وقایع برقراری ارتباط با محیط بیرون، به روش زیر انجام می‌شود.

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

توجه:

در تکمیل این بحث، لازم است که سازمان نسبت به بررسی وقایع ثبت شده و به روز رسانی سیاست‌های اعمالی بر مبنای تحلیل این وقایع اقدام نماید.

SCIOS-۹.۱.۱- تنظیم 'aaa accounting exec'

این بخش به منظور رصد و ثبت آنچه در محیط EXEC رخ می‌دهد، طراحی شده است.

نحوه پیاده‌سازی:

فعال‌سازی AAA Accounting برای ثبت وقایع EXEC Shell، به روش زیر انجام می‌شود.

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

توجه:

فعال‌سازی AAA accounting EXEC هرآنچه در بخش EXEC رخ می‌دهد مانند ساعت شروع و پایان، نام کاربر وارد شده و تاریخ اتصال را ثبت می‌کند، ثبت این وقایع بدون انجام تحلیل‌های لازم مفید فایده نخواهد بود لذا سازمان باید به طور منظم وقایع را مطالعه و سیاست‌های خود را به روزرسانی نماید.

SCIOS-۱۰.۱.۱- تنظیم 'aaa accounting network'

فعال‌سازی این بخش منجر به ثبت وقایع مربوط به درخواست سرویس‌های مختلف شبکه‌ای می گردد.

نحوه پیاده‌سازی:

فعال‌سازی AAA Accounting برای ثبت وقایع درخواست‌های شبکه‌ای، به روش زیر انجام می‌شود.

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

توجه:

فعال‌سازی AAA accounting network وقایع مربوط به پروتکل‌های مختلفی مانند SLIP , PPP, ARA و NCP را ثبت می‌نماید. در این بخش نیز تحلیل وقایع به منظور تجدید نظر و بهبود سیاست‌های سازمان الزامی است.

SCIOS-۱۱.۱.۱- تنظیم 'aaa accounting system'

این بخش به منظور ثبت آنچه در دستگاه رخ می‌دهد و به فعالیت کاربران مربوط نیست، طراحی شده است. فعال‌سازی این امکان کلیه وقایع مربوط به خود دستگاه مانند reload را در کلیه سطوح ثبت می‌نماید.

نحوه پیاده‌سازی:

فعال‌سازی AAA Accounting برای ثبت وقایع سیستمی دستگاه، به روش زیر انجام می‌شود.

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

SCIOS-۲.۱- قوانین دسترسی[6]

یکی از مهمترین مباحث برای تامین امنیت شبکه، کنترل دسترسی به مدیریت و تنظیمات دستگاه است. آنچه در ادامه ارائه می‌شود پیشنهادات کارآمد و اساسی به منظور افزایش امنیت در زمان اتصال به تنظیمات دستگاه است.

SCIOS-۱.۲.۱- تنظیم 'privilege 1' for local users

ایجاد دسترسی نامحدود به دستگاه برای تمام کاربران احتمال حملات مخرب را افزایش می‌دهد لذا لازم است برای کاربرانی که لازم است به دستگاه متصل شوند ولی اجازه ایجاد تغییرات اساسی را ندارند محدودیت‌هایی اعمال شود. سطح دسترسی ۱ به کاربر اجازه می‌دهد وارد بخش EXEC شده و تنظیمات را مشاهده کند اما امکان تعریف دستور جدید، حذف تنظیمات و یا تغییر آنها را ندارد. اگر کاربری در این سطح قصد دسترسی به سطوح بالاتر را داشته باشد باید کلمه عبور enable را وارد کند. لازم به ذکر است مکمل این امنیت، محدود کردن اتصال به دستگاه از طریق روش‌های امن مانند SSH است.

نحوه پیاده‌سازی:

اعمال سطح دسترسی ۱ برای کاربران با دستور زیر انجام می‌شود:

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

[6] Access Rule

توجه:

با توجه به اینکه تنظیمات پیش‌فرض دستگاه شرایط امنیتی قدرتمندی را برای ورود به بخش مدیریتی آن ارائه نمی‌دهد؛ اعمال سطح دسترسی محدود برای کاربران به همراه کلمه عبور رمزنگاری شده به منظور کاهش احتمال اتصالات غیرمجاز الزامی است.

۲.۲.۱–SCIOS تنظیم 'transport input ssh' for 'line vty' connections

اتصال امن به دستگاه از طریق line vty باید از طریق پروتکل SSH انجام شود.

نحوه پیاده‌سازی:

محدود کردن ورود از طریق line vty به روش SSH ، با دستورات زیر انجام می‌شود:

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

توجه:

به منظور کاهش احتمال ورودهای غیرمجاز، محدود کردن ورود از طریق خطوط vty به روش SSH الزامی است.

۳.۲.۱–SCIOS تنظیم 'no exec' for 'line aux 0'

پورت‌های بدون استفاده باید غیرفعال شوند چرا که مستعد اتصال غیر مجاز هستند. برخی از دستگاه‌ها دارای هر دو پورت aux و console به منظور اتصال مستقیم و پیکربندی دستگاه هستند، معمولا پورت console پورت اصلی پیکربندی است و aux برای اتصال dial-up از طریق مودم خارجی است. اجرای دستور no exec روی هر line باعث می‌شود آن line تنها اتصالات داخل به خارج را می‌پذیرد و امکان اتصال از بیرون به دستگاه غیرفعال می‌شود.

نحوه پیاده‌سازی:

محدود کردن جهت اتصال از طریق aux به داخل به خارج از طریق دستور زیر انجام می‌شود:

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

توجه:

سازمان می‌تواند خطر اتصالات غیر مجاز از طریق aux را با روش فوق کاهش دهد از طرفی عدم اجرای دستور فوق امکان اتصال از راه دور(remote) از طریق این خط را فراهم می‌کند که همانطورکه ذکر شد دسترسی مدیریتی به دستگاه از aux غیر مرسوم است.

٤.۲.۱–SCIOS ایجاد 'access-list' for use with 'line vty'

تعریف access list به منظور کنترل انتقال داده روی اینترفیس‌ها و خطوط مجازی (line vty) انجام می‌شود. زمانی که انطباق با قوانین access list رخ دهد نرم افزار cisco IOS ضمن صدور اجازه تبادل داده کنترل ترافیک را متوقف می‌کند.

اعمال access list بر VTY مشخص می‌کند چه آدرس‌هایی اجازه تلاش برای اتصال به روتر را دارند. در واقع این امر باعث محدود شدن مبدا اتصال مدیریتی به دستگاه می‌شود. در این صورت سازمان قادر خواهد بود اتصال و پیکربندی دستگاه را به یک یا

چند سیستم و یا شبکه از طریق پروتکل‌های مناسب محدود سازد. به عنوان مثال در صورتی که در access list تنها یک سیستم از طریق SSH تعریف شده باشد زمانیکه این access list به line vty اعمال شود هیچ سیستمی به جز سیستم مذکور نمی‌تواند به دستگاه دسترسی از راه دور داشته باشد، علاوه بر این، سیستم مجاز هم تنها اجازه برقراری اتصال SSH دارد.

نحوه پیاده‌سازی:

اعمال access list بر vty با دستورات زیر انجام می‌شود:

```
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
```

توجه:

سازمان می‌تواند خطر اتصالات غیر مجاز از طریق خطوط vty را با روش فوق کاهش دهد از طرفی عدم اجرای آن امکان اتصال مخرب از راه دور(remote) از طریق این خط را فراهم می‌کند. دقت شود access list روی تمام خطوط vty اعمال گردد.

SCIOS-۵.۲.۱- تنظیم 'access-class' for 'line vty'

به منظور کنترل کلیه اتصالات ورودی و خروجی مابین دستگاه و سیستم‌های مد نظر کارفرما، access-class بر خطوط vty اعمال می‌گردد. با این روش می‌توان نوع تجهیزاتی که آدرس آنها در access list تایید شده را مشخص نمود، همچنین امکان صدور اجازه دسترسی یا عدم دسترسی از دستگاه به آن تجهیزات در اینجا وجود دارد.

نحوه پیاده‌سازی:

اعمال access-class بر خطوط vty با دستورات زیر انجام می‌شود:

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

توجه:

اعمال access-class علاوه بر کنترل دسترسی از دستگاه به دیگر تجهیزات، باعث افزایش امنیت اتصال به دستگاه از مبدا تجهیزات مختلف می‌گردد.

SCIOS-٦.۲.۱- تنظیم 'exec-timeout' for 'line aux 0'

به منظور جلوگیری از سوء استفاده از اتصالاتی که توسط کاربر رها شده اند این امکان وجود دارد که پس از طی مدت زمان مشخصی که هیچ ورودی از طرف کاربر به دستگاه نرسید اتصال او قطع شود. به عنوان مثال اگر کاربری با سطح دسترسی مدیریتی سیستم خود را پس از اتصال به دستگاه رها کند، امکان سوء استفاده از این بستر وجود دارد. انتخاب مدت زمان برای این امر، باید تعادل مابین مسائل امنیتی(که پیشنهاد کاهش این زمان را می‌دهد) و امور کاری و پیکربندی(که زمان بیشتری را می‌طلبد) را برقرار کند؛ در بیشتر مواقع این زمان نباید بیشتر از ۱۰ دقیقه باشد.

نحوه پیاده‌سازی:

دستورات زیر نحوه اعمال زمان خروج از دستگاه بر پورت aux را نشان می‌دهد:

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

توجه:

سازمان باید برای جلوگیری از دسترسی غیرمجاز به اتصالاتی که در مدت زمان مشخصی بلا استفاده مانده‌اند خروج خودکار را فعال سازند، فعال کردن exec-timeout با تنظیم مدت زمان خروج مناسب این مهم را به نحو احسن انجام می‌دهد.

۷.۲.۱–SCIOS تنظیم 'exec-timeout' to 'line console 0'

به منظور جلوگیری از سوء استفاده از اتصالاتی که توسط کاربر رها شده اند این امکان وجود دارد که پس از طی مدت زمان مشخصی که هیچ ورودی از طرف کاربر به دستگاه نرسید اتصال او قطع شود. به عنوان مثال اگر کاربری با سطح دسترسی مدیریتی سیستم خود را پس از اتصال به دستگاه رها کند، امکان سوء استفاده از این بستر وجود دارد. انتخاب مدت زمان برای این امر، باید تعادل مابین مسائل امنیتی(که پیشنهاد کاهش این زمان را می‌دهد) و امور کاری و پیکربندی(که زمان بیشتری را می‌طلبد) را برقرار کند؛ در بیشتر مواقع این زمان نباید بیشتر از ۱۰ دقیقه باشد.

نحوه پیاده‌سازی:

دستورات زیر نحوه اعمال زمان خروج از دستگاه بر پورت کنسول را نشان می‌دهد:

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

توجه:

سازمان باید برای جلوگیری از دسترسی غیرمجاز به اتصالاتی که در مدت زمان مشخصی بلا استفاده مانده‌اند خروج خودکار را فعال سازند، فعال کردن exec-timeout با تنظیم مدت زمان خروج مناسب این مهم را به نحو احسن انجام می‌دهد.

۸.۲.۱–SCIOS تنظیم 'exec-timeout' To 'line tty'

به منظور جلوگیری از سوء استفاده از اتصالاتی که توسط کاربر رها شده اند این امکان وجود دارد که پس از طی مدت زمان مشخصی که هیچ ورودی از طرف کاربر به دستگاه نرسید اتصال او قطع شود. به عنوان مثال اگر کاربری با سطح دسترسی مدیریتی سیستم خود را پس از اتصال به دستگاه رها کند، امکان سوء استفاده از این بستر وجود دارد. انتخاب مدت زمان برای این امر، باید تعادل مابین مسائل امنیتی(که پیشنهاد کاهش این زمان را می‌دهد) و امور کاری و پیکربندی(که زمان بیشتری را می‌طلبد) را برقرار کند؛ در بیشتر مواقع این زمان نباید بیشتر از ۱۰ دقیقه باشد.

نحوه پیاده‌سازی:

دستورات زیر نحوه اعمال زمان خروج از دستگاه بر خطوط tty را نشان می‌دهد:

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

توجه:

سازمان باید برای جلوگیری از دسترسی غیرمجاز به اتصالاتی که در مدت زمان مشخصی بلا استفاده مانده‌اند خروج خودکار را فعال سازند، فعال کردن exec-timeout با تنظیم مدت زمان خروج مناسب این مهم را به نحو احسن انجام می‌دهد.

۹.۲.۱–SCIOS تنظیم 'exec-timeout' To 'line vty'

به منظور جلوگیری از سوء استفاده از اتصالاتی که توسط کاربر رها شده اند این امکان وجود دارد که پس از طی مدت زمان مشخصی که هیچ ورودی از طرف کاربر به دستگاه نرسید اتصال او قطع شود. به عنوان مثال اگر کاربری با سطح دسترسی مدیریتی سیستم خود را پس از اتصال به دستگاه رها کند، امکان سوء استفاده از این بستر وجود دارد. انتخاب مدت زمان برای این امر، باید تعادل مابین مسائل امنیتی(که پیشنهاد کاهش این زمان را می‌دهد) و امور کاری و پیکربندی(که زمان بیشتری را می‌طلبد) را برقرار کند؛ در بیشتر مواقع این زمان نباید بیشتر از ۱۰ دقیقه باشد.

نحوه پیاده‌سازی:

دستورات زیر نحوه اعمال زمان خروج از دستگاه بر خطوط vty را نشان می‌دهد:

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

توجه:

سازمان باید برای جلوگیری از دسترسی غیرمجاز به اتصالاتی که در مدت زمان مشخصی بلا استفاده مانده‌اند خروج خودکار را فعال سازند، فعال کردن exec-timeout با تنظیم مدت زمان خروج مناسب این مهم را به نحو احسن انجام می‌دهد.

۱۰.۲.۱–SCIOS تنظیم 'transport input none' for 'line aux 0'

پورت‌های بدون استفاده باید غیرفعال شوند چرا که مستعد ارتباط غیر مجاز هستند. برخی از دستگاه‌ها دارای هر دو پورت aux و console به منظور اتصال مستقیم و پیکربندی دستگاه هستند، معمولا پورت console پورت اصلی پیکربندی است و aux برای اتصال dial-up از طریق مودم خارجی است. امکان اتصال از راه دور به دستگاه با روش‌های مختلف از طریق aux به منظور امنیت بیشتر باید غیرفعال باشند. در این بخش نحوه انجام این تنظیمات ارائه می‌گردد.

نحوه پیاده‌سازی:

جلوگیری از اتصال از طریق aux با دستورات زیر میسر می‌گردد:

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

توجه:

سازمان می‌تواند خطر اتصالات غیر مجاز از طریق aux را با روش فوق کاهش دهد، از طرفی عدم اجرای دستور فوق امکان اتصال از راه دور(remote) از طریق این خط را فراهم می‌کند که همانطورکه ذکر شد دسترسی مدیریتی به دستگاه از aux غیر مرسوم است.

۳.۱-SCIOS- دستورات بنر[۷]

تنظیمات این بخش به منظور نمایش حقوق و قوانین و یا اطلاع‌رسانی به کاربران در زمان اتصال یا کار با دستگاه می‌باشد. انواع مختلفی از پیام در سیسکو وجود دارد که در ادامه نحوه تنظیم سه مورد اصلی آن ارائه می‌گردد.

۱.۳.۱-SCIOS- تنظیم 'the 'banner-text' for 'banner exec

فعال‌سازی این بخش باعث می‌شود زمانی که اقدامی در EXEC شروع می‌شود(خطی فعال شود یا اتصالی در جهت ورود به دستگاه از طریق خطوط vty رخ دهد) پیام مشخصی نمایش داده شود. روش کار بدین صورت است که پس از دستور banner exec یک یا چند فاصله ایجاد و پس از آن حرف یا کاراکتری به دلخواه تایپ می‌شود، سپس دستگاه درخواست نوشتن متن مورد نظر را می‌کند، به منظور اعلام خاتمه متن باید از همان حرفی که پس از دستور تایپ شد استفاده نمود.

زمانی که کاربر به دستگاه وصل می‌شود در ابتدا پیام روز (MOTD بخش ۱-۳-۳) نمایش داده می‌شود. پس از آن پیام تنظیم شده بر login (بخش ۱-۳-۲)ظاهر و در ادامه در صورت ورود کاربر به محیط exec، پیام مربوط به این قسمت نمایش داده خواهد شد.

نحوه پیاده‌سازی:

به منظور نمایش یک پیام خاص در زمان ورود به محیط exec از دستور زیر استفاده می‌شود، در مثال زیر از حرف c به منظور اعلام خاتمه متن استفاده شده است:

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

۲.۳.۱-SCIOS- تنظیم 'banner-text' for 'banner login'

فعال‌سازی این بخش باعث می‌شود زمانی که کاربر به دستگاه Login می‌کند پس از رویت پیام روز، آنچه در این بخش تنظیم می‌گردد نمایش داده شود. روش تنظیم مانند بخش قبل بدین صورت است که پس از دستور banner login یک یا چند فاصله ایجاد و پس از آن حرف یا کاراکتری به دلخواه تایپ می‌شود، سپس دستگاه درخواست نوشتن متن مورد نظر را می‌کند، به منظور اعلام خاتمه متن باید از همان حرفی که پس از دستور تایپ شد استفاده نمود.

زمانی که کاربر به دستگاه وصل می‌شود در ابتدا پیام روز (MOTD بخش ۱-۳-۳) نمایش داده می‌شود. پس از آن پیام تنظیم شده در این بخش ظاهر می‌گردد.

نحوه پیاده‌سازی:

به منظور نمایش یک پیام خاص در زمان login از دستور زیر استفاده می‌شود، در مثال زیر از حرف c به منظور اعلام خاتمه متن استفاده شده است:

[۷] Banner Rule

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

۳.۳.۱–SCIOS تنظیم 'banner-text' for 'banner motd'

فعال‌سازی پیام روز (Message Of The Day = MOTD) باعث می‌شود متن خاصی برای تمام کاربران با هر روشی که به دستگاه متصل گردند، نمایش داده شود. پیام روز می‌تواند در اطلاع‌رسانی به کاربران بسیار مفید باشد. غیرفعال کردن این پیام با دستور banner no motd انجام می‌گردد. روش تنظیم و فعال نمودن این نوع پیام مانند بخش قبل بدین صورت است که پس از دستور banner motd یک یا چند فاصله ایجاد و پس از آن حرف یا کاراکتری به دلخواه تایپ می‌شود، سپس دستگاه درخواست نوشتن متن مورد نظر را می‌کند، به منظور اعلام خاتمه متن باید از همان حرفی که پس از دستور تایپ شد استفاده نمود.

نحوه پیاده‌سازی:

به منظور نمایش یک پیام خاص برای تمام کاربران از دستور زیر استفاده می‌شود، در مثال زیر از حرف c به منظور اعلام خاتمه متن استفاده شده است:

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

۴.۱-SCIOS- دستورات گذرواژه[8]

۱.۴.۱-SCIOS- تنظیم 'password' for 'enable secret'

تنظیم enable secret به منظور برقراری امنیت در زمان اتصال به مد exec انجام می‌شود. به صورت پیش‌فرض کلمه عبوری برای این دسترسی وجود ندارد و کاربر با فشردن کلید enter وارد مد privilege می‌شود، اما در صورت اجرای دستور فوق دستگاه کاربر را وادار به وارد کردن رمز می‌نماید. اعمال دستور enable secret به جای enable password سطح امنیتی بالاتری را ارائه می‌نماید، زیرا کلمه عبور به صورت رمز نگاری شده ذخیره می‌شود (هش کلمه عبور ذخیره می‌شود). این روش نسبت به روش‌های لایه ۷ که بسیار ضعیف، پیشبینی‌پذیر و به راحتی معکوس‌پذیر هستند برتری اساسی دارد.

نحوه پیاده‌سازی:

فعال‌سازی enable secret با دستور زیر انجام می‌شود:

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

توجه:

فعال‌سازی enable secret به منظور رمز نگاری یک طرفه کلمه‌های عبور به روش MD5 برای سازمان الزامی است.

۲.۴.۱-SCIOS- فعال کردن 'service password-encryption'

فعال‌سازی سرویس password-encryption باعث می‌شود، فرم رمز نگاری شده‌ی کلمه عبور برای کاربران نمایش داده شود. در صورتی که فایل پیکربندی دستگاه توسط پروتکل‌های مخصوص این امر ذخیره شوند، در حالت پیش‌فرض کلیه کلمات عبور نمایش داده می‌شوند بنابراین دسترسی به کلمات عبور برای افراد غیرمجاز میسر می‌باشد، اما با فعالسازی سرویس password-encryption آنچه در فایل‌های پیکربندی نمایش داده می‌شود، رمزنگاری شده، قابل شناسایی نبوده و از دسترسی‌های مخرب جلوگیری می‌کند.

نحوه پیاده‌سازی:

فعال‌سازی سرویس password-encryption با دستور زیر انجام می‌شود:

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

توجه:

فعال‌سازی password-encryption خطر پی بردن افراد غیرمجاز به کلمات عبور را تا حد زیادی کاهش می‌دهد، اما الگوریتم رمزنگاری در اینجا خیلی قدرتمند نبوده و با روش‌های تحلیلی خاصی می‌توان به کلمات عبور دست یافت.

[8] Password Rule

۳.٤.۱–SCIOS– تنظیم 'username secret' for all local users

پیکربندی پیش‌فرض دستگاه قدرت چندانی در احراز هویت کاربران ندارد لذا امکان ورود مهاجمان وجود دارد بنابراین ایجاد کاربران محلی برای دستگاه با کلمات عبور رمزنگاری شده در زمان عدم وجود سرور AAA الزامی است. استفاده از username secret ، نام کاربری را مجهز به کلمه عبور رمزنگاری شده به روش MD5 می‌کند. MD5 یک روش رمزنگاری بسیار قدرتمند بوده که امکان رمزگشایی آن وجود ندارد، لذا استفاده از این روش در پروتکل‌هایی مانند CHAP که نیازمند رمزهای ساده و معمولی هستند، امکان‌پذیر نیست. Username secret یک لایه امنیتی بر نام کاربری می‌افزاید و استفاده از روش MD5 در زمان استفاده از سرور TFTP به منظور ذخیره‌سازی اطلاعات دستگاه بسیار سودمند و سطح امنیتی خوبی را ارائه می‌دهد.

نحوه پیاده‌سازی:

ساخت نام کاربری با کلمه عبور رمزنگاری شده با دستور زیر انجام می‌شود:

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

۵.۱–SCIOS– دستورات SNMP[9]

SNMP امکان رصد و مدیریت تجهیزات شبکه‌ای را فراهم می‌کند. در این بخش تنظیمت لازم برای استفاده من از این امکان ارائه می‌گردد.

آنچه در اینجا ارائه می‌گردد پیشنهادات امنیتی لازم برای سازمان‌هایی است که که از SNMP استفاده می‌نمایند.

۱.۵.۱–SCIOS– تنظیم 'no snmp-server' to disable SNMP when unused

در صورتی که سازمان از SNMP استفاده نمی‌کند باید این امکان را در هر دو حالت read و write غیرفعال سازد.

نحوه پیاده‌سازی:

غیرفعال کردن SNMP در هر دو حالت read , write با دستور زیر انجام می‌شود:

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

۲.۵.۱–SCIOS– عدم تنظیم 'private' for 'snmp-server community'

استفاده از کلمه پیش‌فرض "private" به عنوان community بسیار شناخته شده است و حدس زدن آن برای مهاجمان کار ساده ایست، از طرفی دستیابی به community، به کاربر حداقل دسترسی read only را می‌دهد؛ بنابراین پیشنهاد می‌شود به منظور جلوگیری از این نوع دسترسی غیرمجاز از کلمه دیگری به عنوان community استفاده شود.

[9] SNMP Rule

نحوه پیاده‌سازی:

حذف مقدار private به عنوان کلمه community به صورت زیر انجام می‌شود:

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

توجه:

به منظور کاهش خطر دسترسی‌های غیرمجاز، سازمان باید برخی مقادیر پیشفرض، قابل حدس و شناخته شده مانند "private" برای SNMP-Server community را غیرفعال نماید.

۳.۵.۱-SCIOS- عدم تنظیم 'public' for 'snmp-server community'

استفاده از کلمه پیش‌فرض "public" به عنوان community بسیار شناخته شده است و حدس زدن آن برای مهاجمان کار ساده ایست، از طرفی دستیابی به community، به کاربر حداقل دسترسی read only را می‌دهد؛ بنابراین پیشنهاد می‌شود به منظور جلوگیری از این نوع دسترسی غیرمجاز، از کلمه دیگری به عنوان community استفاده شود.

نحوه پیاده‌سازی:

حذف مقدار public به عنوان کلمه community به صورت زیر انجام می‌شود:

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

توجه:

به منظور کاهش خطر دسترسی‌های غیرمجاز، سازمان باید برخی مقادیر پیشفرض، قابل حدس و شناخته شده مانند "public" برای SNMP-Server community را غیرفعال نماید.

۴.۵.۱-SCIOS- عدم تنظیم 'RW' for any 'snmp-server community'

صدور مجوز read/write برای snmp-server community باعث می‌شود دسترسی کامل به کاربر snmp-server برای مشاهده و ایجاد تغییرات در تنظیمات دستگاه داده شود، این امر می‌تواند از لحاظ امنیتی مشکلاتی را به همراه داشته باشد؛ بنابراین پیشنهاد می‌شود در صورت عدم نیاز به ایجاد تغییرات در تنظیمات دستگاه از طریق snmp-server، امکان RW غیرفعال باشد و کلیه snmp-serverها دارای دسترسی read-only باشند.

نحوه پیاده‌سازی:

غیرفعالسازی community با دسترسی write به روش زیر انجام می‌شود:

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

توجه:

غیرفعالسازی دسترسی write برای snmp-serverها از لحاظ امنیتی و کاهش خطر دسترسی غیرمجاز به تنظیمات دستگاه، حائز اهمیت است.

۵.۵.۱-SCIOS- تنظیم 'the ACL for each 'snmp-server community

راه‌اندازی سرویس snmp موجب می‌شود، دسترسی به دستگاه با داشتن community string به راحتی رخ دهد، لذا به منظور محدود کردن این دسترسی لازم است IPهایی که مجاز هستند، تعیین و به صورت یک ACL بر این سرویس اعمال شود. با رعایت این موضوع تنها تعدادی محدودی از IPها که قابل اعتماد هستند، می‌توانند دستگاه را رصد و مدیریت نمایند. در این بخش نحوه اعمال یک ACL بر سرویس SNMP ارائه می‌شود. همچنین پیشنهاد می‌شود در صورت امکان، از SNMPv3 که قابلیت احراز هویت، صلاحیت سنجی و رمزنگاری داده را دارد استفاده شود.

نحوه پیاده‌سازی:

نحوه تنظیم SNMP community string و اعمال محدودیت دسترسی به دستگاه از طریق ACL با دستور زیر انجام شود:

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

توجه:

سازمان باید به منظور کاهش خطر دسترسی غیرمجاز به دستگاه و محدودسازی رصد و مدیریت دستگاه به نواحی قابل اعتماد، برای تمام snmp-server community ها لیست دسترسی و کنترلی را طراحی و اعمال نماید. افزایش سطح این امنیت می‌تواند با استفاده از SNMPv3 میسر شود.

۶.۵.۱–SCIOS– ساخت 'access-list' for use with SNMP

راه‌اندازی سرویس snmp موجب می‌شود، دسترسی به دستگاه با داشتن community string به راحتی رخ دهد، لذا به منظور محدود کردن این دسترسی لازم است IPهایی که مجاز هستند، تعیین و به صورت یک ACL بر این سرویس اعمال شود. با رعایت این موضوع تنها تعدادی محدودی از IPها که قابل اعتماد هستند، می‌توانند دستگاه را رصد و مدیریت نمایند. می‌توان ACL را به منظور کنترل ترافیک عبوری از یک اینترفیس، تنظیم نمود، به طوریکه کنترل دسترسی از طریق SNMP نیز به این طریق انجام شود.

نحوه پیاده‌سازی:

نحوه تعریف SNMP ACL برای محدود کردن دسترسی به دستگاه با دستورات زیر انجام می‌شود:

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

۷.۵.۱-SCIOS- تنظیم 'snmp-server host' when using SNMP

به همراه سرویس SNMP امکانات دیگری مانند سیستم اعلام هشدارها نیز قابل فعال‌سازی است، این سیستم که حالت‌های مختلفی دارد، می‌تواند غیر از امکانات مدیریت و رصد معمولی SNMP در پاسخ به SNMP-Server پیام‌هایی با محتوای هشدارها، restartها، برقراری ارتباطات، عدم موفقیت اتصال به روتر همسایه و دیگر اتفاقات مهم را نیز ارسال نماید. ارسال این پیام‌ها باید به یک مقصد امن و قابل اعتماد انجام شود، لذا لازم است مقصد پیام‌ها تعیین و برای اطمینان community string ویژه آن تعریف گردد. در این بخش روش انجام این تنظیمات ارائه خواهد شد.

نحوه پیاده‌سازی:

به روش زیر می‌توان community string را برای ارسال هشدارها به SNMP-Server به روش trap تعریف و مقصد پیام‌ها را محدود به IP خاصی نمود:

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

توجه:

محدودسازی مقصد پیام‌های SNMP به یک یا چند سیستم قابل اعتماد خاص، از الزامات فعال‌سازی سرویس SNMP در سازمان است.

۸.۵.۱–SCIOS– تنظیم 'snmp-server enable traps snmp'

فعال‌سازی سرویس snmp trap بدون اعمال محدودیت بر آن باعث می‌شود، کلیه انواع پیام‌ها از دستگاه به snmp-server ارسال شود، که در واقع بسیاری از این پیام‌ها محتوای کاربردی چندانی ندارند، لذا توصیه می‌شود به منظور کاهش ترافیک غیرمفید در شبکه،snmp trap محدود به موارد مفید و کاربردی برای شبکه شود.

نحوه پیاده‌سازی:

در دستور زیر پیام‌های snmp-trap به موارد احراز هویت، up و down شدن لینک‌ها و coldstart محدود شده است:

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

۹.۵.۱–SCIOS– تنظیم 'priv' for each 'snmp-server group' using SNMPv3

در صورت استفاده از SNMPv3 امکانات امنیتی بیشتری نسبت به نسخه‌های دیگر قابل تنظیم است. به طور کلی این امکانات شامل Message integrity به منظور حصول اطمینان از عدم تغییر داده در مسیر، Authentication برای تایید اعتبار مبدا داده و Encryption جهت رمزنگاری و درهم کردن داده‌ها به منظور جلوگیری از خوانش غیرمجاز آنها می‌باشند.

در زمان تعریف یک کاربر برای SNMPv3 به منظور حفاظت از تبادل داده، می‌توان امکانات امنیتی مختلفی را برروی آن اعمال نمود، AES128 حداقل سطح امنیتی است که باید به کار برده شود.

نحوه پیاده‌سازی:

برای هر گروه SNMPv3 که برروی روتر ساخته می‌شود، سطح امنیتی به روش زیر تنظیم شود:

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

توجه:

سازمان‌هایی که از SNMP استفاده می‌کنند، میتوانند با استفاده از تنظیمات snmp-server group v3 priv و به دنبال آن رمزگذاری داده‌ی در حال انتقال، به طور قابل ملاحظه‌ای خطر دسترسی‌های غیرمجاز را کاهش دهند.

۱۰.۵.۱-SCIOS-درخواست 'aes 128' as minimum for 'snmp-server user'

همانطوریکه در بخش قبل ذکر شد، استفاده از SNMPv3 سطح امنیتی بسیار خوبی در ارتباط بین مبدا و مقصد داده‌های SNMP ارائه می‌دهد، اما این سطح امنیتی با انجام تنظیمات مناسب فراهم خواهد شد. در زمان تعریف یک کاربر برای SNMPv3 به منظور حفاظت از تبادل داده، می‌توان امکانات امنیتی مختلفی را برروی آن اعمال نمود، AES128 حداقل سطح امنیتی است که باید به کار برده شود.

نحوه پیاده‌سازی:

برای هر کاربر SNMPv3 که برروی روتر ساخته می‌شود، سطح امنیتی به روش زیر تنظیم شود:

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

۲-SCIOS- سطح کنترلی[10]

Control Plane یکی از ویژگی های حفاظتی IOS است که از ورژن ۱۲,۳ به آن افزوده شده وهدف آن حفاظت از روتر و منابع آن و سرویس‌های حیاتی است. Control Plane مواردی مانند monitoring، بروزرسانی جدول مسیریابی، و بطورکلی پویایی عملکرد روتر را پوشش می‌دهد. این مورد حمایت از سرویس‌ها، تنظیمات، مسیر جریان اطلاعات، بررسی ترافیک عبوری و وضعیت پویایی روتر را کنترل می‌کند. به عنوان مثال، سلامت سرویس های حیاتی شامل (نه تنها) Routing و میزان استفاده از RAM و CPU و I/O های روتر می‌شوند.

۱.۲-SCIOS- دستورات محیط Global[11]

انجام دستورات در محیط Global و تنظیم سرویس‌ها برای محافظت در برابر حملات، جلوگیری از بهره‌برداری غیرمجاز از تجهیزات، و عدم انجام آن باعث افزایش ریسک آسیب‌پذیری به روتر در برابر حملات می‌شود.

۱.۱.۲-SCIOS- تنظیمات SSH

جهت اطمینان از امنیت ارتباط از راه دور به روتر استفاده از SSH الزامی است.

۱.۱.۱.۲-SCIOS- تنظیمیات پیش‌نیاز برای فعال کردن SSH

قبل از فعال‌سازی SSH انجام مراحل زیر الزامی می‌باشد.

۱,۱,۱,۱,۲-SCIOS- تنظیم نام دستگاه

نام دستگاه در اول خط فرمان و فایل پیکربندی دستگاه آورده می‌شود.

نحوه پیاده‌سازی:

با دستور زیر یک نام غیر از نام پیش فرض برای روتر انتخاب کنید.

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

توجه:

سازمان‌ها باید برنامه‌ای مشخص برای شبکه‌های سازمانی خود و انتخاب نام مناسب برای هر روتر داشته باشند.

۲,۱,۱,۱,۲-SCIOS- تنظیم نام دامنه

انتخاب domain name جهت استفاده IOS سیسکو برای تکمیل اسامی تجهیزات فاقد اعتبار و ناشناس

نحوه پیاده‌سازی:

[10] Control Plane

[11] Global Service Rules

یک نام دامنه برای روتر در نظر بگیریم

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

SCIOS-۳,۱,۱,۱,۲- تنظیم crypto key generate rsa

با استفاده از این دستور یک زوج کلید خصوصی و عمومی از نوع RSA برای تبادل اطلاعات تولید می‌شود.

نحوه پیاده‌سازی:

یک کلید با طول حداکثر 2048 با استفاده از دستور زیر برای سرویس SSH ایجاد کنیم

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

توجه:

سازمان‌ها باید برنامه ریزی مشخصی جهت تولید کلید تبادل و اجرای رمزنگاری شبکه با استفاده از کلید خصوصی و عمومی RSA با طول مناسب حداقل ۲۰۴۸ داشته باشند.

SCIOS-٤,١,١,١,٢- تنظیم زمان برای ارتباط SSH

مدت زمان انتظار که روتر برای قطع ارتباط کلاینت و یا ارتباط ناموفق صبر می‌کند را تعیین می‌کند و خطر دسترسی در صورت باز بودن ارتباط با سطح دسترسی مدیریتی به روتر را کاهش می‌دهد. برای تنظیم زمان پایان اتصال SSH از توسط زیر استفاده می‌شود. (زمان بین ۱ تا ۱۲۰ ثانیه تعیین می‌گردد.)

نحوه پیاده‌سازی:

برای تنظیم SSH Time out بر روی روتر از دستور زیر استفاده می‌شود:

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

SCIOS-٥,١,١,١,٢- محدودکردن ip ssh authentication-retries

تعداد دفعاتی که یک کاربر غیرمجاز، برای واردکردن نام کاربری و گذر واژه (قبل از برقراری ارتباط) می‌تواند از طریق ارتباط SSH وارد کند، را مشخص می‌کند. تنظیم این قابلیت باعث کاهش خطرات از طریق حملات brute force برای برقرای ارتباط از طریق SSH می‌شود و تعداد تلاش ناموفق را محدود می‌کند.

نحوه پیاده‌سازی:

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

SCIOS-۲.۱.۱.۲- استفاده از نسخه ۲ SSH

نسخه اول SSH دارای آسیب‌پذیرهای جدی می‌باشد و خطر حملات را افزایش می‌دهد، بنابراین دیگر به عنوان یک پروتکل امن استفاده نمی‌شود. در نتیجه از سال ۲۰۰۶ نسخه دوم SSH به عنوان یک استاندارد و پروتکل امن مورد استفاده قرار می‌گیرد.

نحوه پیاده‌سازی:

برای امنیت بیشتر SSH، نسخه ۲ را فعال کنید.

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

SCIOS-۲.۱.۲- غیرفعال کردن سرویس CDP

CDP که مخفف کلمات Cisco Discovery Protocol است به معنای پروتکل شناسایی سیسکو می باشد ، کاربرد اصلی CDP به اشتراک گذاری اطلاعات در خصوص Device های سیسکو که بصورت مستقیم به روترهای سیسکو متصل شده اند، می-باشد. این اطلاعات مواردی از قبیل نوع سیستم عامل یا IOS مورد استفاده و آدرس IP مربوط به دستگاه می باشد. بصورت پیشفرض پیام هایی که توسط Cisco Discovery Protocol یا CDP از همسایه های روتر یا Neighbor ها دریافت می‌شود برای سایر دستگاه های موجود در شبکه ارسال نمی‌شود و این بدین معناست که CDP فقط اطلاعات را به دستگاه‌هایی می‌دهد که بصورت مستقیم (Directly) به روتر متصل شده اند.

CDP تنها برای Monitoring و عیب‌یابی شبکه کاربرد دارد ولی باعث بالا بردن ریسک افشاء اطلاعات، و همچنین خطر احتمالی از کار افتادن روتر به وسیله حملات DoS بر روی پروتکل CDP را افزایش می‌دهد، بنابراین در غیر از موارد ضروری این پروتکل حتما باید غیرفعال باشد.

نحوه پیاده‌سازی:

برای غیرفعال کردن پروتکل CDP در محیط Global دستور زیر را وارد می‌نمائیم.

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

توجه: برای جلوگیری از دسترسی‌های غیرمجاز، پروتکل‌های غیرضروری از جمله CDP بر روی تجهیزات باید غیرفعال گردد.

SCIOS-۳.۱.۲- غیرفعال کردن سرویس BOOTP

BOOTP پروتکلی است که بوسیله آن دستگاههای موجود در شبکه در زمان Boot یا Startup می‌توانند از سرور مربوطه IP دریافت می‌کنند. BOOTP اجازه می‌دهد تا یک روتر به سیستم‌های متصل به آن IP بدهد. این قابلیت باید غیرفعال شود، مگر در مواردی که باتوجه به ساختار شبکه نیاز به فعال شدن آن باشد.

نحوه پیاده‌سازی:

جهت غیرفعال کردن BOOTP بر روی روتر از دستور زیر استفاده نمائید.

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

SCIOS-٤.١.٢- غیرفعال کردن سرویس DHCP

سوریس DHCP نیز مانند BOOTP عمل کرده و به تجهیزات امکان دریافت IP از روتر را بصورت اتوماتیک می‌دهد این سرویس نیز باید بجز موارد ضروری غیرفعال گردد و برای آدرس دهی به منابع شبکه باید از یک سرور اختصاصی استفاده شود تا از حملات DoS به روتر را کاهش دهد.

نحوه پیاده‌سازی:

برای غیرفعال کردن سرویس DHCP بر روی روتر از دستور زیر می‌توان استفاده نمود.

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

SCIOS-٥.١.٢- تنظیم no ip identd

پروتکل شناسایی امکان تعیین هویت کاربران را از طریق ارتباط TCP مشخص می‌کند و در صورتیکه روتر بعنوان یک Ident server در نظر گرفته شود احتمال افشای اطلاعات کاربران توسط یک Attacker را افزایش می‌دهد.

نحوه پیاده‌سازی:

برای غیرفعال کردن Ident Server بر روی روتر از دستور زیر استفاده نمائید.

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

SCIOS-٦.١.٢- تنظیم service tcp-keepalives-in

اتصالات کهنه باعث استفاده از منابع و خطر به دست آوردن دسترسی غیر مجاز را افزایش می‌دهد، پروتکل TCP Keeplives در جهت تولید بسته Keepalive در اتصالات از راه دور و آغاز شده از یک میزبان را برعهده دارد. این سرویس اجازه می‌دهد تا دستگاه زمانی که ارتباط میزبان از راه دور با شکست مواجه می‌شود عمل قطع ارتباط را انجام دهد. اگر این دستور فعال باشد هردقیقه یک بار بسته Keepalive در ارتباطات بیکار ارسال شود و اگر هیچ بسته‌ای دریافت نشود ارتباط را قطع کرده و در صورت دریافت بسته ارتباط را دوباره راه‌اندازی می‌کند.

نحوه پیاده‌سازی:

برای فعال کردن بسته ورودی سرویس Keepalive از دستور زیر استفاده کنید.

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

SCIOS-٧.١.٢- تنظیم service tcp-keepalives-out

نحوه پیاده‌سازی:

برای فعال کردن بسته خروجی سرویس Keepalive از دستور زیر استفاده کنید.

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

SCIOS-۸.۱.۲- غیرفعال کردن سرویس PAD

اگر روتر از خدمات PAD استفاده نمی‌کند، غیر فعال کردن این سرویس جهت جلوگیری از حملات بر روی PAD X.25 و دسترسی به خط فرمان روتر استفاد می‌شود.

نحوه پیاده‌سازی:

برای غیرفعال کردن سرویس PAD از دستور زیر استفاده می‌شود.

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

SCIOS-۲.۲- دستورات ثبت وقایع[12]

از دستورات Logging جهت مانیتور کردن اتصالات موفق و یا ناموفق، رخدادهای امنیتی و سیستمی، و debug وقایع رخ داده در روتر استفاده می‌شود.

SCIOS-۱.۲.۲- تنظیم logging on

این مورد امکان نظارت و ثبت رویدادهای زمان اتصال و حملات احتمالی به دستگاه‌های سیسکو را فراهم می‌سازد. فعال کردن logging بر روی IOS سیسکو جهت کنترل ریسک بر روی تجهیزات شبکه سازمان‌ها الزامی می‌باشد.

نحوه پیاده‌سازی:

برای فعال کردن Logging در محیط Global از دستور زیر استفاده شود.

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

SCIOS-۲.۲.۲- تنظیم 'logging buffered' for 'buffer size'

برای فعال کردن یک بافر محلی برای پیام‌های لاگ استفاده می‌شود. این دستور باعث می‌شود یک پیام به حافظه داخلی روتر کپی و برای نظارت مورد استفاده قرار گیرد. مقدار بافر پیشنهادی ۶۴۰۰۰ می‌باشد.

نحوه پیاده‌سازی:

مقدار بافر را برای پیام‌های Logging با دستور تعیین کنید.

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

SCIOS-۳.۲.۲- تنظیم 'logging console critical'

محدوده تولید پیام‌های اتصال به روتر از طریق کنسول را برای مدیریت منابع سیستم مشخص می‌کند، اتصال از طریق پورت کنسول فقط در موارد اضطراری و یا برای عیب‌یابی فوری باید انجام شود و چون این ارتباط پایدار می‌باشد ریسک خطرات ناشی از آن را برای سازمان افزایش می‌دهد، بنابراین مدیریت پیام‌های سیستمی از طریق این ارتباط برای سازمان حیاتی می‌باشد. بصورت پیش‌فرض برای تمامی پیام‌ها فعال می‌باشد و پیشنهاد می‌گردد برای پیام‌های Critical فعال شود.

[12] Logging Rule

نحوه پیاده‌سازی:

فعال‌سازی پیام‌های Critical برای پورت کنسول به صورت زیر انجام می‌شود.

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

SCIOS-٤.٢.٢- تنظیم 'logging host' IP address for

برای بررسی دقیق‌تر و ذخیره پیام‌های سیستمی راه‌اندازی یک سرور syslog برای روترهای سیسکو الزامی می‌باشد، با توجه به محدود بودن بافر روتر این روش ذخیره طولانی مدت پیام‌ها و بررسی آن در هر زمان، را ممکن می‌سازد.

نحوه پیاده‌سازی:

اختصاص یک سرور یا چند syslog برای ثبت وقایع‌نگاری با دستور زیر انجام می‌شود.

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

SCIOS-٥.٢.٢- تنظیم 'logging trap informational'

این مورد محدوده ارسال پیام‌های سیستمی به سرور syslog و مدیریت پروتکل SNMP و تولید آن توسط روتر را مشخص می‌کند. محدوده براساس تنظیم مقادیر ۷ (مربوط به پیام‌های Debugging) و یا ۶ (مربوط به پیام‌های Informational) می‌باشد

نحوه پیاده‌سازی:

مشخص کردن محدوده پیام‌های syslog و SNMP با دستور زیر انجام می‌شود.

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

SCIOS-٦.٢.٢- تنظیم 'service timestamps debug datetime'

برای فعال کردن برچسب زمانی timestamps بر روی پیام‌های Debug و محدود کردن آن براساس timezone استفاده می‌شود و باعث به دست آوردن یک دید جامع از زمان وقوع حوادث جهت رفع عیب و یا حملات را جهت مقابله امکان پذیر می‌کند.

نحوه پیاده‌سازی:

محدود کردن پیام‌های Debug به وسیله timestaamps با دستور زیر انجام می‌شود.

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

SCIOS-٧.٢.٢- تنظیم 'logging source interface'

آدرس IP منابع ورودی بسته‌های لاگ مشخص گردد و برای ثبت وقایع یک روتر از یک آدرس ثابت استفاده شود.

نحوه پیاده‌سازی:

منع ورود از طریق رابط Loopback با دستور زیر انجام می‌شود.

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

SCIOS-۳.۲ دستورات NTP[13]

پروتکل زمان شبکه[14] به مدیر شبکه این اجازه را می‌دهد، ساعت تمام تجهیزات شبکه را با یک منبع واحد تنظیم نماید. فعال-سازی این پروتکل به منظور تحلیل صحیح و موثر وقایع اهمیت بالایی دارد. NTP یک استاندارد اینترنت است که در RFC1305 تعریف شده است.

به منظور برقراری یک ارتباط امن با NTP Server باید کلمه عبوری برآن اعمال شود. در ادامه تنظیمات لازم در این خصوص ارائه خواهد شد.

SCIOS-۱.۳.۲ درخواست Encryption Keys for NTP

به منظور برقراری یک ارتباط امن با NTP Server باید کلمه عبوری برآن اعمال شود. در ادامه تنظیمات لازم در این خصوص ارائه خواهد شد.

نحوه پیاده‌سازی:

روش زیر انجام می‌گردد:

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

توجه:

سازمان باید برای ارائه تنظیمات زمانی پایدار، سه NTP host را تعیین نماید. فعال‌سازی NTP authentication می‌تواند ارتباط مابین این hostها را امن و انجام پروسه شناسایی را تحمیل نماید.

SCIOS-۱.۱.۳.۲ تنظیم 'NTP authenticate'

فعال کردن NTP authenticated به روتر این امکان را می‌دهد جهت آپدیت زمان خود تنها از طریق NTP server مجاز اقدام نماید.

نحوه پیاده‌سازی:

NTP authenticated یا دستور زیر فعال می‌گردد.

```
hostname(config)#
```

SCIOS-۲.۱.۳.۲ تنظیم 'ntp authentication-key'

[13] NTP Rule

[14] Network Time Protocol

پس از فعال‌سازی امکان شناسایی در پروتکل NTP ، لازم است به منظور حصول اطمینان از برقراری ارتباط با سرور قابل اعتماد، کلید رمزی تعریف گردد، در این صورت سطح امنیتی بالاتری به هنگام به روز رسانی زمان دستگاه‌ها وجود خواهد داشت.

نحوه پیاده‌سازی:

فعال‌سازی key id و کلید رمزی که به روش MD5 تولید شده است، با دستور زیر انجام می‌شود:

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

توجه:

سازمان باید برای ارائه تنظیمات زمانی پایدار، سه NTP host را تعیین نماید. فعال‌سازی ntp authentication-key می‌تواند ارتباط مابین این hostها را امن و انجام پروسه شناسایی را با رمزنگاری همراه سازد.

SCIOS-۳.۱.۳.۲- تنظیم 'ntp trusted-key'

به منظور جلوگیری از هماهنگی تصادفی دستگاه با سرورهای غیرمجاز، امکانی وجود دارد که از میان کلیدهای ساخته شده برای ntp، یک یا چند کلید با شماره مشخص را مورد اعتماد نمود. در این صورت اگر سروری بسته اطلاعاتی محتوی ntp را به دستگاه ارسال نماید، فقط در صورتی که این بسته حامل کلید رمز با شماره مورد اعتماد باشد، پذیرفته می‌شود. مزیت این امر در آن است که از میان کلیدهای موجود، کلیدهای خاصی امکان برقراری ارتباط را فراهم می‌کنند، لذا در صورت برقراری ارتباط به صورت تصادفی و یا دسترسی به برخی کلیدها، همچنان امکان پیشگیری از برقراری ارتباط ناسالم وجود دارد.

نحوه پیاده‌سازی:

فعال‌سازی trusted-key به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای ارائه تنظیمات زمانی پایدار، سه NTP host را تعیین نماید. فعال‌سازی trusted key می‌تواند ارتباط مابین این hostها را امن و انجام پروسه شناسایی را با رمزنگاری همراه سازد.

SCIOS-٤.١.٣.٢- تنظیم 'key' for each 'ntp sever'

به منظور جلوگیری از هماهنگی تصادفی دستگاه با سرورهای غیرمجاز، امکانی وجود دارد که هر سرور بتواند از کلید رمز خاصی استفاده نماید. این امر دسترسی را بسیار محدود می‌کند، به طوری که تنها کسانی می‌توانند به دستگاه اطلاعات ntp ارسال نمایند که اولا دارای کلید رمز باشند، ثانیا کلید رمز مربوطه در لیست کلیدهای مورد اعتماد باشد و ثالثا فرستنده دارای IP و کلید رمز خاصی که برایش تعریف شده باشد.

نحوه پیاده‌سازی:

اختصاص کلمه رمز برای هر NTP Server با دستور زیر انجام می‌شود:

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

توجه:

سازمان باید برای ارائه تنظیمات زمانی پایدار، سه NTP host را تعیین نماید. فعال‌سازی ntp server key می‌تواند ارتباط مابین این hostها را امن و انجام پروسه شناسایی را با رمزنگاری همراه سازد.

SCIOS-۲.۳.۲- تنظیم 'ip address' for 'ntp server

این دستور امکان همزمان‌سازی ساعت نرم‌افزار سیستم، با یک سرور NTP مشخص را تعیین می‌کند. برای اطمینان از اینکه زمان بر روی روتر سیسکو با دستگاه‌های دیگر در شبکه سازگار می‌باشد تنظیم حداقل دو یا سه سرور NTP خارجی الزامی می‌باشد.

نحوه پیاده‌سازی:

برای تنظیم حداقل یک NTP سرور خارجی از دستور زیر استفاده نمائید.

```
hostname(config)#ntp server {ip_address}
```

SCIOS-٤.٢- دستورات Loopback

زمانی که یک روتر، ارتباطی را با یک host راه دور، مانند SYSLOG یا NTP آغاز می‌کند، از نزدیک‌ترین رابط[15] (اینترفیس) خود به عنوان آدرس مبدا استفاده خواهد کرد. این مساله می‌تواند ارتباط را با چالش‌هایی مانند خاموش شدن رابط و یا مداخله فایروال در تبادل داده با رابط مربوطه روبه‌رو سازد. برای جلوگیری از این قبیل مشکلات لازم است که روتر ارتباطات را از طریق یک رابط loopback انجام دهد.

SCIOS-١.٤.٢- ساخت رابط Loopback

ساخت رابط (اینترفیس) مجازی به صورت loopback در ادامه توضیح داده خواهد شد. این رابط همواره روشن بوده و بر همه platformها قابل پیاده‌سازی است. استفاده متناوب از این نوع رابط می‌تواند باعث ایجاد پتانسیل سوء استفاده، ایجاد اشتباه در پیکربندی و تناقض شود. ایجاد تعداد بیشتر رابط loopback باید قبل از استفاده، مستند و تایید شده باشند.

نحوه پیاده‌سازی:

ساخت و پیکربندی یک اینترفیس loopback به روش زیر انجام می‌شود:

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

توجه:

[15] - Interface

لازم است که سازمان نسبت به تعیین و ایجاد اینترفیس‌های loopback برای شبکه‌های مهم و سازمانی اقدام نماید. این نوع اینترفیس می‌تواند اطلاعات بحرانی شبکه مانند ID روتر در پروتکل OSPF و مقصد داده‌های پروتکل‌های مسیریابی را فراهم سازد.

SCIOS-۲.٤.۲- تنظیم 'AAA 'source-interface

برای اینکه AAA Server (RADIUS , TACACS) به راحتی روتر را شناسایی نماید و درخواست‌های روتر را از طریق IP مشخصی دریافت نماید، لازم است که IP رابط مشخصی را برای ارسال داده‌ی AAA تعیین نمود، برای این منظور تنظیماتی که در ادامه ارائه می‌شود باید انجام گردد. لازم به ذکر است به دلایلی که در بخش ۲-۴ ارائه گردید، توصیه می‌شود این اینترفیس از نوع Loopback باشد.

نحوه پیاده‌سازی:

گره زدن سرویس‌های AAA به اینترفیس Loopback به روش زیر انجام می‌شود:

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

توجه:

سازمان به منظور استفاده موثر از رصد و مدیریت تجهیزات شبکه باید از AAA استفاده نماید. به منظور بهینه‌سازی این سرویس پیشنهاد می‌شود، ارتباطات از طریق رابط Loopback انجام شود.

SCIOS-۳.٤.۲- تنظیم 'ntp source' to Loopback Interface

پیشنهاد می‌شود به منظور استفاده بهینه از سرویس NTP ، مبدا مشخصی از نوع رابط Loopback برای ارسال این نوع داده تعریف گردد.

نحوه پیاده‌سازی:

گره زدن سرویس‌های NTP به رابط Loopback به روش زیر انجام می‌شود:

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

توجه:

سازمان به منظور تنظیم و هماهنگ‌سازی زمان دستگاه‌های موجود در شبکه، ملزم به استفاده از سرویس NTP و برقراری این نوع ارتباط با NTP Server است. جهت بهینه‌سازی این سرویس پیشنهاد می‌شود، ارتباطات از طریق رابط Loopback انجام شود.

-SCIOS-٤.٤.٢ تنظیم 'ip tftp source-interface' to the Loopback Interface

به منظور برقراری یک ارتباط بهینه با سرور TFTP و شناسایی ساده روتر لازم است یک IP مشخص و ثابت از روتر را در نظر گرفت. پیشنهاد می‌شود به دلایلی که در بخش ۲-۴ ذکر شد، این IP متعلق به یک رابط Loopback باشد. در ادامه نحوه اختصاص یک رابط Loopback به ارتباطات TFTP ذکر خواهد شد.

نحوه پیاده‌سازی:

گره زدن سرویس TFTP به رابط Loopback به روش زیر انجام می‌شود:

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

توجه:

سازمان به منظور ارسال و دریافت فایل‌های مختلف از دستگاه‌های سیسکو به دیگر سیستم‌ها و بالعکس، ملزم به استفاده از سرویس TFTP و برقراری این نوع ارتباط باTFTP Server است. جهت بهینه‌سازی این سرویس پیشنهاد می‌شود، ارتباطات از طریق رابط Loopback انجام شود.

-SCIOS-۳ سطح داده‌ها[16]

سطح داده شامل مواردی که در حوزه control plane و management plane است، نمی‌باشد. این بخش شامل لیست‌های دسترسی رابط، عملکرد فایروال، NAT و IPSec می‌باشد. در واقع این ناحیه به عبور داده از روتر مربوط بوده و تنظیمات سرویس-های ترافیک موثر[17] مانند تایید unicast RPF و CAR/QoS متعلق به این ناحیه می‌شوند.

-SCIOS-۱.۳ دستورات مسیریابی[18]

سرویس‌های غیر لازم باید غیرفعال شوند.

-SCIOS-۱.۱.۳ تنظیم 'no ip source-route'

Source routing امکانی است که به وسیله آن بسته می‌تواند از مسیر خاصی برای عبور استفاده نماید، این ویژگی که به صورت پیش‌فرض روی روترها فعال است، مستعد چندین نوع حمله می‌باشد لذا پیشنهاد می‌شود نسبت به غیرفعال‌سازی آن اقدام شود مگر در مواردی که استفاده ه از آن الزامی است.

نحوه پیاده‌سازی:

غیرفعال‌سازی source routing با دستور زیر انجام می‌شود:

[16] Data Plane

[17] Traffic-affecting

[18] Routing Rule

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

توجه:

سازمان باید نسبت به غیرفعال‌سازی سرویس‌های غیرضروری اقدام نماید. ویژگی ip source-route در بسیاری از حملات مورد استفاده قرار می‌گیرد، بنابراین غیرفعال‌سازی آن الزامی است.

۲.۱.۳-SCIOS- تنظیم 'no ip proxy-arp'

Proxy arp سرویسی است که زمانی که دستگاه به یک شبکه متصل می‌شود، پاسخ درخواست‌های ARPی که از اعضای شبکه‌های دیگر میرسد را با MAC خودش پاسخ داده و ترافیک را به آن اعضا ارسال می‌نماید.

این امکان در برخی موارد برای گسترش دامنه broadcast از طریق لینک‌های WAN استفاده می‌شود، اما در بیشتر مواقع از proxy arp به منظور برقراری امکان ارتباط سیستم‌هایی که subnet mask آنها به نحوی است که مقصد داده آنها در رنج IP خودشان قرار می‌گیرد اما مبدا و مقصد متصل به یک رابط مشابه از یک روتر نیستند و یا مبدا و مقصد به دو روتر متفاوت متصل هستند. در این صورت فرستنده با توجه به اینکه مقصد را در رنج خودش می‌بیند درخواست arp می‌فرستد، اما می‌دانیم این درخواست از روتر عبور نمی‌کند، اما در صورت فعال بودن proxy arp با توجه به اینکه روتر می‌داند مقصد داده در رنج مبدا است ولی متصل به یک رابط دیگر است، mac خود را به داده پیوست کرده و ترافیک را عبور می‌دهد. این امر در بسیاری موارد در شبکه داخلی راهگشاست اما فعال بودن این امکان روی رابط متصل یه شبکه‌های بیرونی و غیرقابل اعتماد مانند اینترنت می‌تواند از لحاظ امنیتی مشکلاتی را به همراه داشته باشد، لذا لازم است این ویژگی که به صورت پیشفرض روی تمام رابطهای روتر فعال است محدود شده و برروی پورت‌های غیر ضروری غیرفعال شود.

نحوه پیاده‌سازی

Proxy arp از طریق دستور زیر غیر فعال می‌شود:

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

توجه:

سازمان باید نسبت به غیرفعال‌سازی سرویس‌های غیرضروری اقدام نماید. ویژگی proxy arp به طور موثری می‌تواند امنیت شبکه داخلی را به خطر اندازد لذا غیرفعال‌سازی آن الزامی است.

۳.۱.۳-SCIOS- تنظیم 'no interface tunnel'

با وجود اینکه به صورت پیشفرض رابط تونلی روی روترها وجود ندارد با این حال وجود آن می‌تواند برای اهداف مخرب به کار برده شود، لذا لازم است، از عدم وجود این نوع رابط اطمینان حاصل نمود.

نحوه پیاده‌سازی:

با دستور زیر می‌توان تمام رابطهای تونل را غیرفعال کرد:

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

SCIOS-٤.١.٣- تنظیم 'ip verify unicast source reachable-via'

فعالسازی uRPF[19] باعث می‌شود روتر نسبت به مبدا داده و رابط حساس شود، به عبارت دیگر زمانی که این امکان بر روی اینترفیسی از روتر فعال شود، دریافت داده از این رابط به شرطی انجام می‌شود، که مبدا داده با جدول مسیریابی هماهنگ باشد. در این حالت اگر داده‌ای از یک IP معتبر به روتر برسد اما ورود داده از رابط که انتظار می‌رود نباشد، درخواست رد خواهد شد. فعال-سازی این ویژگی بر رابط‌های دارای ریسک حمله الزامی است.

نحوه پیاده‌سازی:

فعالسازی uRPF به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت و حفاظت از محرمانگی، اطمینان از عدم خوانش داده و جلوگیری از دسترسی غیرمجاز به دستگاه‌ها تدابیر و امکانات امنیتی را ارتقاء دهد. uRPF به صورت پویا از جدول روتر به منظور پذیرفتن یا نپذیرفتن داده‌ای که از یک اینترفیس میآید استفاده می‌کند.

SCIOS-٢.٣- مرز فیلترینگ مسیریاب[20]

یک دستگاه border-filtering می‌تواند به شبکه‌های داخلی مانند desktop networks یا DMZ و شبکه‌های خارجی مانند اینترنت وصل شود. در صورت انتخاب این گروه، فیلتر ترافیک ورودی و خروجی نیازمند تنظیمات قواعد امنیتی است.

SCIOS-١.٢.٣- تنظیم 'ip access-list extended'

اجرای این دستور روتر را در مد access-list قرار می‌دهد، که باعث می‌شود اجازه ورود یا عدم ورود با دستورات deny و permit در ACL تنظیم و اعمال شود. این امکان می‌تواند از حملات spoofing به طور موثری جلوگیری به عمل آورد. برای پیکربندی این امر لازم است کلیه ترافیکی که از شبکه بیرونی با مبدا ای که IP مشابه شبکه داخلی دارد، و وارد روتر می‌شود مسدود گردد. این تشابه می‌تواند شامل IP ، نام سیستم یا هر آدرس دیگری که برای تجهیزات داخل شبکه قرار داده شده است باشد. در صورتی که سازمان برخی از این نوع دسترسی را آزاد کند، قبل از دستور deny که تمام ترافیک با شرایط فوق را مسدود می‌کند باید یک دستور permit برای این امر تنظیم شود.

نحوه پیاده‌سازی:

تنظیم ACL برای محدودسازی مبدا داده به شبکه داخلی و جلوگیری از ورود به روتر از طریق شبکه خارجی با ویژگی‌های هویتی داخل شبکه با دستورات زیر انجام می‌شود:

[19] Unicast reverse-path forwarding

[20] Border Router Filtering

```
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
```

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، به طور موثری داخل و خارج شبکه را تفکیک نماید. تنظیم ACL می‌تواند با permit و deny کردن درخواست‌های ورود این مهم را فراهم نماید.

۲.۲.۳-SCIOS- تنظیم inbound 'ip access-group' on the External Interface

اجرای این دستور روتر را در مد access-list قرار می‌دهد، که باعث می‌شود اجازه ورود یا عدم ورود با دستورات deny و permit در ACL تنظیم و اعمال شود. این امکان می‌تواند از حملات spoofing به طور موثری جلوگیری به عمل آورد. برای پیکربندی این امر لازم است کلیه ترافیکی که از شبکه بیرونی با مبدا ای که IP مشابه شبکه داخلی دارد، و وارد روتر می‌شود مسدود گردد. این تشابه می‌تواند شامل IP ، نام سیستم یا هر آدرس دیگری که برای تجهیزات داخل شبکه قرار داده شده است باشد. در صورتی که سازمان برخی از این نوع دسترسی را آزاد کند، قبل از دستور deny که تمام ترافیک با شرایط فوق را مسدود می‌کند باید یک دستور permit برای این امر تنظیم شود.

نحوه پیاده‌سازی:

اعمال access-group بر رابط‌های متصل به شبکه خارجی(Untrust) با دستورات زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، اجازه ورود یا عدم ورود را بر مبنای ACL صادر نماید. استفاده از ip access-group می‌تواند این تدابیر را بر اساس شناسایی گروه‌ها تنظیم نماید.

SCIOS-۳.۳- احراز هویت همسایگی[21]

Routing authentication را فعال سازید.

SCIOS-۱.۳.۳- درخواست EIGRP Authentication if Protocol is Used

در صورت استفاده از پروتکل مسیریابی EIGRP لازم است ویژگی EIGRP authentication فعال شود. در این بخش نحوه فعال‌سازی تدابیر امنیتی لازم در خصوص این موضوع ارائه خواهد شد.

SCIOS-۱.۱.۳.۳- تنظیم 'key chain'

در صورتی می‌توان از authentication برای پروتکل‌های مسیریابی استفاده نمود که زنجیره کلید[22] تعریف شده باشد، یک زنجیره کلید متشکل از حداقل یک کلید و حداکثر ۲۱۴۷۴۸۳۶۴۷ تعداد کلید است. لازم به ذکر است از میان پروتکل‌های مسیریابی فقط DRP، EIGRP و RIPv2 از زنجیره کلید استفاده می‌نمایند.

نحوه پیاده‌سازی:

ساخت زنجیره کلید به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از زنجیره کلید می‌تواند پروتکل‌ها را مجبور استفاده از این سیاست‌ها نماید.

SCIOS-۲.۱.۳.۳- تنظیم کلید

برای هر زنجیره کلید باید یک کلید احراز هویت تنظیم کرد. تنظیمات این بخش از مقدمات ایجاد routing authentication است.

نحوه پیاده‌سازی:

ساخت کلید به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از کلید برای زنجیره کلیدها از الزامات اجرای این سیاست‌ها است.

[21] Neighbor Authentication

[22] Key chain

SCIOS-۳.۱.۳.۳- تنظیم رشته کلید

برای هر زنجیره کلید باید یک کلید احراز هویت تنظیم کرد. از طرفی هر کلید خود نیازمند یک رشته[۲۳] است. تنظیمات این بخش از مقدمات ایجاد routing authentication است.

نحوه پیاده‌سازی:

نوشتن key string برای هر کلید به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از کلید برای زنجیره کلیدها از الزامات اجرای این سیاست‌ها است.

SCIOS-٤.١.٣.٣- تنظیم 'address-family ipv4 autonomous-system'

BGP یک پروتکل مسیریابی چندگانه است و ویژگی address-family محدودیت تبادل داده با همسایه‌ها را فعال می‌سازد. توصیه می‌شود این امکان برای پروتکل مسیریابی EIGRP فعال شود.

نحوه پیاده‌سازی:

فعال‌سازی address family برای EIGRP به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از address-family این سیاست‌ها را با محدودسازی تبادل اطلاعات با تعداد محدود و از قبل شناخته شده‌ای از همسایه‌ها پیاده می‌نماید.

SCIOS-٥.١.٣.٣- تنظیم 'af-interface defaul'

کاربر می‌تواند با دستور فوق تنظیمات پیش‌فرض خود را همزمان بر تمام رابطهایی متعلق به address family است اعمال نماید. تنظیمات این بخش جزئی از EIGRP address family است.

نحوه پیاده‌سازی:

فعال‌سازی af-interface default برای EIGRP address family به روش زیر انجام می‌شود:

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

[23] string

```
hostname(config-router-af)#af-interface default
```

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از address-family این سیاست‌ها را با محدودسازی تبادل اطلاعات با تعداد محدود و از قبل شناخته شده‌ای از همسایه‌ها، پیاده می‌نماید.

SCIOS-٦.١.٣.٣- تنظیم 'authentication key-chain'

لازم است برای EIGRP address family یک زنجیره کلید به روشی که در ادامه ذکر خواهد شد، تنظیم نمود. در واقع تنظیمات این بخش جزئی از EIGRP Authenticatin است.

نحوه پیاده‌سازی:

فعال‌سازی زنجیره کلید بر EIGRP address family به روش زیر انجام می‌شود:

```
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}
```

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از address-family key chain این سیاست‌ها را با محدودسازی تبادل اطلاعات با تعداد محدود و از قبل شناخته شده‌ای از همسایه‌ها، پیاده می‌نماید.

SCIOS-٧.١.٣.٣- تنظیم 'authentication mode md5'

این بخش در ادامه و تکمیل کننده EIGRP authentication است و به منظور ایجاد شناسایی برای جلوگیری از دریافت داده از منابع تاییدنشده و پیشگیری از دریافت اطلاعات جعلی و محرز نشده، طراحی و اجرا می‌گردد.

نحوه پیاده‌سازی

فعال‌سازی مد MD5 باری شناسایی در EIGRP address family به روش زیر انجام می‌شود:

```
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
```

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از authentication mode برای EIGRP address family یا service-family این سیاست‌ها را با محدودسازی نوع احراز هویت مابین دستگاه‌های شبکه‌ای، اجرا می‌نماید.

SCIOS-۸.۱.۳.۳- تنظیم 'ip authentication key-chain eigrp'

اعمال زنجیره کلید EIGRP بر رابط، می‌تواند تبادل داده مابین دستگاه و همسایه را با احراز هویت همراه سازد، تا از خطر دریافت داده غیرمجاز از طریق همسایه شناسایی و تایید نشده مصون بماند.

نحوه پیاده‌سازی:

اعمال زنجیره کلید EIGRP برروی رابط به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از زنجیره کلید شناسایی برای EIGRP این سیاست‌ها را با محدودسازی احراز هویت مابین دستگاه‌های شبکه‌ای، اجرا می‌نماید.

SCIOS-۹.۱.۳.۳- تنظیم 'ip authentication mode eigrp'

با فعال‌سازی زنجیره کلید شناسایی EIGRP بر رابط، تعیین مد شناسایی می‌تواند این شناسایی را بهینه سازد.

نحوه پیاده‌سازی:

تعیین مد برای EIGRP authentication بر روی رابط می‌تواند به روش زیر انجام شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از مد MD5 در زنجیره کلید شناسایی برای پروتکل مسیریابی EIGRP این سیاست‌ها را با محدودسازی احراز هویت مابین دستگاه‌های شبکه‌ای، اجرا می‌نماید.

SCIOS-۲.۳.۳- درخواست OSPF Authentication if Protocol is Used

در صورت استفاده از پروتکل مسیریابی OSPF ، به کاربردن روش‌های شناسایی به منظور افزایش سطح امنیت تبادل اطلاعات مسیریابی، توصیه می‌شود.

SCIOS-۱.۲.۳.۳- تنظیم 'authentication message-digest'

در این بخش نحوه تنظیم مد MD5 به منظور انجام پروسه شناسایی در پروتکل OSPF ارائه می‌گردد. لازم به ذکر این بخش جزئی از تنظیمات OSPF Authentication است.

نحوه پیاده‌سازی:

فعال‌سازی مد MD5 در OSPF به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از مد MD5 در پروتکل مسیریابی OSPF این سیاست‌ها را با محدودسازی احراز هویت مابین دستگاه‌های شبکه‌ای، اجرا می‌نماید.

SCIOS-۲.۲.۳.۳- تنظیم 'ip ospf message-digest-key md5'

لازم است برای امنیت شناسایی در OSPF کلمه عبور و ID ، به روشی که در ادامه ارائه می‌شود، در این پروتکل تعریف شود.

نحوه پیاده‌سازی:

فعال‌سازی نام کاربری و کلمه عبور در مد MD5 برای OSPF با دستورات زیر امکان‌پذیر است:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. فعال‌سازی امکان ip ospf message-digest-key MD5 بر رابطهای مربوطه می‌تواند، سیاست‌های محدودسازی تبادل داده مسیریابی مابین دستگاه‌ها را اعمال نماید.

SCIOS-۳.۳.۳ درخواست RIPv2 Authentication if Protocol is Used

پروتکل مسیریابی RIP پروتکلی بر مبنای بردار فاصله[۲۴] است، که در برخی شبکه‌های داخلی مورد استفاده قرار می‌گیرد. این پروتکل حالت پیچیده‌ای داشته و برخی امکانات آن تاثیراتی در مسیریابی ایجاد می‌کنند که شاید در ابتدای امر مشهود نباشند. در صورت استفاده از RIPv2 باید نسبت به فعال‌سازی شناسایی و امکان احراز هویت در آن اقدام شود. در ادامه تنظیمات امنیتی که در زمان استفاده از این پروتکل الزامی به نظر می‌رسند ارائه خواهند شد.

SCIOS-۱.۳.۳.۳ تنظیم 'key chain'

قبل از هرچیز لازم است به منظور فعال‌سازی امکان احراز هویت در RIPv2 ، زنجیره کلید مختص آن تعریف شود.

نحوه پیاده‌سازی:

تعریف زنجیره کلید با دستور زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. تعیین کلمه عبور به منظور ایجاد محدودیت در پذیرفتن داده مسیریابی مابین روترها، می‌تواند در دستیابی به این مهم موثر باشد.

SCIOS-۲.۳.۳.۳ تنظیم کلید

هر زنجیره کلید نیازمند کلید مختص خود است، لذا در این بخش نحوه تعریف کلید برای زنجیره کلیدی که در بخش قبل تعریف شد، ارائه می‌گردد.

نحوه پیاده‌سازی:

تعریف کلید برای زنجیره کلید با دستور زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. تعیین کلمه عبور به منظور ایجاد محدودیت در پذیرفتن داده مسیریابی مابین روترها، می‌تواند در دستیابی به این مهم موثر باشد.

[24] Distance vector

SCIOS-۳.۳.۳.۳- تنظیم رشته کلید

در بخش قبل وارد مد ساخت کلید برای زنجیره کلید شدیم، برای هر کلیدی که در زنجیره کلید تعریف می‌شود لازم است یک رشته یا کلمه رمز اختصاص یابد، در ادامه نحوه تنظیم کلمه رمز بیان می‌شود

نحوه پیاده‌سازی:

تعریف کلمه رمز برای کلیدی که در زنجیره کلید ساخته شده با دستور زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. تعیین کلمه عبور به منظور ایجاد محدودیت در پذیرفتن داده مسیریابی مابین روترها، می‌تواند در دستیابی به این مهم موثر باشد.

SCIOS-٤.٣.٣.٣- تنظیم 'ip rip authentication key-chain'

برای فعال‌سازی پروسه شناسایی در پروتکل مسیریابی RIPv2 لازم است تنظیماتی که در ادامه ارائه می‌گردد، بر رابطی که داده مسیریابی از طریق آن رد و بدل می‌شود، انجام شود. لازم به ذکر است زنجیره کلیدی که در بخش‌های قبل ساخته شد و محتوی کلید و کلمه عبور بود، در اینجا اعمال می‌گردد.

نحوه پیاده‌سازی:

اعمال زنجیره کلید RIPv2 بر رابط به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. تعیین کلمه عبور به منظور ایجاد محدودیت در پذیرفتن داده مسیریابی مابین روترها، می‌تواند در دستیابی به این مهم موثر باشد.

SCIOS-٥.٣.٣.٣- تنظیم 'ip rip authentication mode' to 'md5'

تعیین مد شناسایی برای پروتکل مسیریابی RIPv2 در این بخش انجام می‌شود.

نحوه پیاده‌سازی:

تعیین مد شناسایی برای RIP به صورت زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. تعیین مد زنجیره کلید به منظور ایجاد محدودیت در پذیرفتن داده مسیریابی مابین روترها، می‌تواند در دستیابی به این مهم موثر باشد.

SCIOS-٤.٣.٣ درخواست BGP Authentication if Protocol is Used

BGP پروتکل مسیریابی است که در برخی شبکه‌های داخلی و خارجی(ISPها و اینترنت) مورد استفاده قرار می‌گیرد، مسیریابی در این پروتکل بر مبنای بردار مسیر[25] است. BGP یک پروتکل پیچیده و چندگانه بوده که فعال‌سازی امکانات آن می‌تواند تاثیراتی داشته باشد که در ابتدای امر ملموس نیستند. در صورت استفاده از این پروتکل، انجام تدابیر امنیتی مانند فعال‌سازی شناسایی و احراز هویت در زمان تبادل داده‌ی مسیریابی با دیگر روترها الزامی است.

SCIOS-١.٤.٣.٣ تنظیم 'neighbor password'

در زمان استفاده از BGP مانند دیگر پروتکل‌ها لازم است، پروسه شناسایی به منظور عدم پذیرش اطلاعات مسیریابی ناصحیح انجام شود. برای تحمیل انجام این پروسه به روتر، در زمان برقراری ارتباط با، همسایه تنظیمات این بخش الزامی است. فعال‌سازی مد MD5 در زمان برقراری ارتباطات TCP مابین دو روتر BGP ، از تنظیمات این پروسه است.

نحوه پیاده‌سازی:

پیکربندی شناسایی همسایه در پروتکل BGP به روش زیر انجام می‌شود:

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

توجه:

سازمان باید برای افزایش سطح امنیت شبکه داخلی با استفاده از تدابیر و تنظیمات امنیتی، سیاست‌های سختگیرانه‌ای را برای احراز هویت در پروتکل‌های مسیریابی وضع نماید. استفاده از کلمه عبور در ارتباط با همسایه در پروتکل BGP می‌تواند محدودیت قابل توجهی در ارتباط دو همسایه ایجاد نماید.

[25] Path vector

-SCIOS-۴ جدول ممیزی

جدول ممیزی خلاصه‌ای از تمامی الزامات بیان شده در متن سند می‌باشد. قابل ذکر است که ستون‌های "وضعیت" و "قابلیت پیاده‌سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارت‌های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده‌سازی، ممیز باید قابلیت پیاده‌سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده‌سازی نداشته باشد، علت عدم قابلیت پیاده‌سازی آن باید در ذیل جدول توضیح داده شود.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
CSIOS-۱		سطح مدیریت			
CSIOS-۱,۱		قوانین احراز هویت ، صلاحیت‌سنجی و حسابرسی (AAA)			
CSIOS-۱,۱,۱		فعال کردن AAA	دارد	ندارد	فعال کردن AAA new-model
CSIOS-۱,۱,۲		فعال کردن aaa authentication login	دارد	ندارد	فعال کردن برای Login user and password
CSIOS-۱,۱,۳		فعال کردن aaa authentication enable default	دارد	ندارد	تنظیمات پیش‌فرض AAA فعال گردد.
SCIOS-۱,۱,۴		تنظیم "login authentication for 'line con 0	دارد	ندارد	تنظیمات AAA برای پورت کنسول فعال گردد.
CSIOS-۱,۱,۵		تنظیم "login authentication for 'line tty	دارد	ندارد	تنظیمات AAA برای Line TTY فعال گردد.
SCIOS-۱,۱,۶		تنظیم "login authentication for 'line vty	دارد	ندارد	تنظیمات AAA برای Line VTY فعال گردد.
SCIOS-۱,۱,۷		تنظیم aaa accounting به منظور logانگاری دستورات	دارد	ندارد	تنظیمات Log برای AAA فعال گردد.
SCIOS-۱,۱,۸		تنظیم "aaa accounting connection	دارد	ندارد	تنظیم TACACS
SCIOS-۱,۱,۹		تنظیم "aaa accounting exec	دارد	ندارد	تنظیم AAA برای محیط EXEC
SCIOS-۱,۱,۱۰		تنظیم "aaa accounting network	دارد	ندارد	فعال‌سازی AAA Accounting برای ثبت وقایع درخواست‌های شبکه‌ای
SCIOS-۱,۱,۱۱		تنظیم "aaa accounting system	دارد	ندارد	فعال‌سازی AAA

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
					Accounting برای ثبت وقایع سیستمی دستگاه
CSIOS-۱,۲		قوانین دسترسی			
CSIOS-۱,۲,۱		تنظیم 'privilege 1' for local users	دارد	ندارد	تنظیم سطح دسترسی یک برای کاربران Local
CSIOS-۱,۲,۲		تنظیم 'transport input ssh' for 'line vty' connections	دارد	ندارد	تمام ارتباطات از راه دور بوسیله SSH انجام شود
CSIOS-۱,۲,۳		تنظیم 'no exec' for 'line aux 0'	دارد	ندارد	ارتباط از طریق پورت aux غیرفعال گردد
CSIOS-۱,۲,۴		ایجاد 'access-list' for use with 'line vty'	دارد	ندارد	تعریف کردن ACL مناسب برای ارتباطات VTY
CSIOS-۱,۲,۵		تنظیم 'access-class' for 'line vty'	دارد	ندارد	تعریف کردن Access Group مناسب برای ارتباطات VTY
SCIOS-۱,۲,۶		تنظیم 'exec-timeout' for 'line aux 0'	دارد	ندارد	تعریف حداقل ده دقیقه برای پورت AUX
SCIOS-۱,۲,۷		تنظیم 'exec-timeout' to 'line console 0'	دارد	ندارد	تعریف حداقل ده دقیقه برای پورت Consol
SCIOS-۱,۲,۸		تنظیم 'exec-timeout' To 'line tty'	دارد	ندارد	تعریف حداقل ده دقیقه برای ارتباط با TTY
SCIOS-۱,۲,۹		تنظیم 'exec-timeout' To 'line vty'	دارد	پنج دقیقه	تعریف حداقل ده دقیقه برای ارتباط با VTY
SCIOS-۱,۲,۱۰		تنظیم 'transport input none' for 'line aux 0'	دارد	ندارد	ارتباط از طریق پورت AUX باید غیرفعال گردد.
CSIOS-۱,۳		دستورات بنر			
SCIOS-۱,۳,۱		تنظیم 'the 'banner-text' for 'banner exec'	دارد	ندارد	تنظیم banner-text برای banner exec
SCIOS-۱,۳,۲		تنظیم 'banner-text' for 'banner login'	دارد	ندارد	تنظیم banner-text برای banner login
SCIOS-۱,۳,۳		تنظیم 'banner-text' for 'banner motd'	دارد	ندارد	تنظیم banner-text برای banner motd
CSIOS-۱,۴		دستورات گذرواژه			

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCIOS-۱,۴,۱		تنظیم "password' for 'enable secret	دارد	ندارد	فعال کردن enable secret بجای enable password
SCIOS-۱,۴,۲		فعال کردن "service password-encryption	دارد	ندارد	فعال کردن password encryption
SCIOS-۱,۴,۳		تنظیم 'username secret' for all local users'	دارد	ندارد	ساخت تمامی کاربران با استفاده از username secret
CSIOS-۱,۵		دستورات SNMP			
SCIOS-۱,۵,۱		تنظیم 'no snmp-server' to disable SNMP when unused	دارد	ندارد	غیرفعال کردن سرور SNMP در زمان عدم استفاده از آن
SCIOS-۱,۵,۲		عدم تنظیم 'private' for 'snmp-server community'	دارد	ندارد	عدم استفاده از کلمه private برای SNMP Community
SCIOS-۱,۵,۳		عدم تنظیم 'public' for 'snmp-server community'	دارد	ندارد	عدم استفاده از کلمه public برای SNMP Community
SCIOS-۱,۵,۴		عدم تنظیم 'RW' for any 'snmp-server community'	دارد	ندارد	عدم تنظیم قابلیت read-write برای SNMP Community
SCIOS-۱,۵,۵		تنظیم ACL for each 'snmp-server community'	دارد	ندارد	تنظیم ACL مناسب برای SNMP Community
SCIOS-۱,۵,۶		ساخت access-list' for use with SNMP'	دارد	ندارد	ایجاد ACL مناسب برای SNMP
SCIOS-۱,۵,۷		تنظیم 'snmp-server host' when using SNMP	دارد	ندارد	اختصاص سرور مانیتورینگ برای SNMP
SCIOS-۱,۵,۸		تنظیم "snmp-server enable traps snmp	دارد	ندارد	فعال سازی SNMP Trap یا توجه به نیازهای سرور SNMP
SCIOS-۱,۵,۹		۰تنظیم 'priv' for each 'snmp-server group' using SNMPv3	دارد	ندارد	فعال‌سازی ورژن ۳ SNMP
SCIOS-۱,۵,۱۰		درخواست 'aes 128' as minimum for 'snmp-server user'	دارد	ندارد	ایجاد حداقل سطح امنیتی AES128 برای SNMPv3
CSIOS-۲		سطح کنترلی			
SCIOS-۲,۱		دستورات محیط Global			
SCIOS-۲,۱,۱		تنظیمات SSH	دارد	ندارد	ایجاد ارتباط امن SSH
SCIOS-۲,۱,۱,۱		تنظیمات پیش‌نیاز برای فعال کردن SSH	دارد	ندارد	-

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCIOS-۲,۱,۱,۱,۱		تنظیم نام دستگاه	دارد	router switch	نام پیش‌فرض دستگاه را تغییر دهید.
SCIOS-۲,۱,۱,۱,۲		تنظیم نام دامنه	دارد	ندارد	تنظیم ip domain-name برای دستگاه
SCIOS-۲,۱,۱,۱,۳		تنظیم crypto key generate rsa	دارد	ندارد	تنظیم کلید ارتباطی RSA با طول حداقل ۲۰۴۸
SCIOS-۲,۱,۱,۱,۴		تنظیم زمان برای ارتباط SSH	دارد	ندارد	تنظیم ۶۰ ثانیه
SCIOS-۲,۱,۱,۱,۵		محدودکردن ip ssh authentication-retries	دارد	ندارد	در صورت فعال شدن بصورت پیش‌فرض ۳ ثانیه می‌باشد.
SCIOS-۲,۱,۱,۲		استفاده از نسخه SSH ۲	دارد	ندارد	فعال کردن نسخه SSH ۲
SCIOS-۲,۱,۲		غیرفعال کردن سرویس CDP	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۲,۱,۳		غیرفعال کردن سرویس BOOTP	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۲,۱,۴		غیرفعال کردن سرویس DHCP	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۲,۱,۵		تنظیم no ip identd	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۲,۱,۶		تنظیم service tcp-keepalives-in	دارد	دارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید برای بسته keepalive ورودی فعال گردد.
SCIOS-۲,۱,۷		تنظیم service tcp-keepalives-out	دارد	دارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید برای بسته keepalive خروجی فعال گردد.
SCIOS-۲,۱,۸		غیرفعال کردن سرویس PAD	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۲,۲		دستورات ثبت وقایع			
SCIOS-۲,۲,۱		تنظیم logging on	دارد	ندارد	فعال کردن logging
SCIOS-۲,۲,۲		تنظیم 'buffer size' for 'logging buffered'	دارد	ندارد	بافر بصورت پیش‌فرض فعال نمی‌باشد، مقدار پیشنهادی

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
					۶۴۰۰۰ می‌باشد.
SCIOS-۲,۲,۳		تنظیم 'logging console critical'	دارد	All Log	برای critical فعال گردد
SCIOS-۲,۲,۴		تنظیم IP address for 'logging host	دارد	ندارد	یک سرور اختصاصی برای ثبت وقایع در نظر گرفته شود.
SCIOS-۲,۲,۵		تنظیم 'logging trap informational	دارد	ندارد	Logging Informational
SCIOS-۲,۲,۶		تنظیم 'service timestamps debug datetime	دارد	Debug and logging message	برای debug فعال گردد
SCIOS-۲,۲,۷		تنظیم 'logging source interface	دارد	Wildcard Interface	Wildcard اینترفیس استفاده می‌شود
SCIOS-۲,۳		دستورات NTP			
SCIOS-۲,۳,۱		درخواست Encryption Keys for NTP	دارد	ندارد	فعال‌سازی Encryption Key برای NTP
SCIOS-۲,۳,۱,۱		تنظیم 'NTP authenticate	دارد	ندارد	فعال‌سازی NTP Authenticate
SCIOS-۲,۳,۱,۲		تنظیم 'ntp authentication-key	دارد	ندارد	تنظیم کلید احراز هویت برای NTP به روش MD5
SCIOS-۲,۳,۱,۳		تنظیم 'ntp trusted-key	دارد	ندارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید فعال گردد.
SCIOS-۲,۳,۱,۴		تنظیم 'key' for each 'ntp sever	دارد	ندارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید فعال گردد.
SCIOS-۲,۳,۲		تنظیم 'ip address' for 'ntp server	دارد	ندارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید فعال گردد.
SCIOS-۲,۴		دستورات Loopback			
SCIOS-۲,۴,۱		ساخت اینترفیس Loopback	دارد	ندارد	ساخت حداقل یک اینترفیس loopback
SCIOS-۲,۴,۲		تنظیم 'AAA 'source-interface	دارد	ندارد	ارسال درخواست برای سرور AAA بوسیله اینترفیس loopback
SCIOS-۲,۴,۳		تنظیم 'ntp source' to Loopback Interface	دارد	ندارد	ارسال درخواست برای سرور NTP بوسیله اینترفیس loopback

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCIOS-۲,۴,۴		تنظیم ' ip tftp source-interface' to the Loopback Interface	دارد	ندارد	ارسال درخواست برای سرور TFTP بوسیله اینترفیس loopback
SCIOS-۳		سطح داده‌ها			
SCIOS-۳,۱		دستورات مسیریابی	دارد	دارد	سرویس‌های غیرضروری باید غیرفعال گردد.
SCIOS-۳,۱,۱		تنظیم 'no ip source-route	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۳,۱,۲		تنظیم 'no ip proxy-arp	دارد	دارد	بصورت پیش‌فرض فعال می‌باشد و باید غیرفعال گردد.
SCIOS-۳,۱,۳		تنظیم 'no interface tunnel	دارد	ندارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید برای اطمینان غیرفعال گردد.
SCIOS-۳,۱,۴		تنظیم 'ip verify unicast source reachable-via'	دارد	ندارد	بصورت پیش‌فرض غیرفعال می‌باشد و باید برای افزایش امنیت فعال گردد.
SCIOS-۳,۲		مرز فیلترینگ مسیریاب			
SCIOS-۳,۲,۱		تنظیم "ip access-list extended	دارد	ندارد	تنظیم ACL Extended
SCIOS-۳,۲,۲		تنظیم inbound 'ip access-group' on the External Interface	دارد	ندارد	تنظیم Access group متناسب برای ACL Extended
SCIOS-۳,۳		احراز هویت همسایگی			
SCIOS-۳,۳,۱		درخواست EIGRP Authentication if Protocol is Used	دارد	ندارد	فعال‌سازی احراز هویت در صورت استفاده از پروتکل مسیریابیEIGRP
SCIOS-۳,۳,۱,۱		تنظیم "key chain	دارد	ندارد	تنظیم زنجیره کلید مناسب
SCIOS-۳,۳,۱,۲		تنظیم کلید	دارد	ندارد	تنظیم کلید مناسب برای زنجیره ایجاد شده
SCIOS-۳,۳,۱,۳		تنظیم زنجیره کلید	دارد	ندارد	تنظیم زنجیره کلید مناسب
SCIOS-۳,۳,۱,۴		تنظیم 'address-family ipv4 autonomous-system'	دارد	ندارد	فعال‌سازی address family برای تبادل داده با همسایه

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCIOS-۳,۳,۱,۵		تنظیم 'af-interface defaul	دارد	ندارد	فعال‌سازی بر روب اینترفیس-های address family
SCIOS-۳,۳,۱,۶		تنظیم 'authentication key-chain	دارد	ندارد	تنظیم زنجیره کلید مناسب برای احراز هویت EIGRP
SCIOS-۳,۳,۱,۷		تنظیم 'authentication mode md5	دارد	ندارد	فعال‌سازی مد MD5
SCIOS-۳,۳,۱,۸		تنظیم 'ip authentication key-chain eigrp	دارد	ندارد	اعمال زنجیره کلید EIGRP بر اینترفیس
SCIOS-۳,۳,۱,۹		تنظیم 'ip authentication mode eigrp	دارد	ندارد	تعیین مد برای EIGRP authentication بر روی اینترفیس
SCIOS-۳,۳,۲		درخواست OSPF Authentication if Protocol is Used	دارد	ندارد	فعال‌سازی احراز هویت در صورت استفاده از پروتکل مسیریابیOSPF
SCIOS-۳,۳,۲,۱		تنظیم "authentication message-digest	دارد	ندارد	فعال‌سازی مد MD5 در OSPF
SCIOS-۳,۳,۲,۲		تنظیم "ip ospf message-digest-key md5	دارد	ندارد	فعال‌سازی نام کاربری و کلمه عبور در مد MD5 برای OSPF
SCIOS-۳,۳,۳		درخواست RIP Authentication if Protocol is Used	دارد	ندارد	فعال‌سازی احراز هویت در صورت استفاده از پروتکل مسیریابیRIP
SCIOS-۳,۳,۳,۱		تنظیم "key chain	دارد	ندارد	تنظیم زنجیره کلید مناسب
SCIOS-۳,۳,۳,۲		تنظیم کلید	دارد	ندارد	تنظیم کلید مناسب برای زنجیره ایجاد شده
SCIOS-۳,۳,۳,۳		تنظیم زنجیره کلید	دارد	ندارد	تنظیم زنجیره کلید مناسب
SCIOS-۳,۳,۳,۴		تنظیم "ip rip authentication key-chain	دارد	ندارد	اعمال زنجیره کلید RIPv2 بر اینترفیس
SCIOS-۳,۳,۳,۵		تنظیم "ip rip authentication mode' to 'md5	دارد	ندارد	تعیین مد شناسایی برای RIP
SCIOS-۳,۳,۳		درخواست BGP Authentication if Protocol is Used	دارد	ندارد	فعال‌سازی احراز هویت در صورت استفاده از پروتکل مسیریابی BGP
SCIOS-۳,۳,۴,۱		تنظیم "neighbor password	دارد	ندارد	پیکربندی شناسایی همسایه در

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
					پروتکل BGP