پیکربندی امن

Cisco Firewall Benchmark

مرکز مدیریت راهبردی افتا

SCFI-CIS-Cisco-Firewall-Benchmark-V4.0

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 Firewall Benchmark است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

این سند توسط شرکت "بهین راهکار" 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 Firewall Benchmark 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.

تنظیمات:

سطح مدیریت

سطح مدیریت با سرویس‌ها و تنظیمات و جریان‌های داده مربوط به پیکربندی دستگاه امنیتی مبادله می‌کند.

SCFI-1: مدیریت پسورد

قوانینی برای اجرای رمزعبور تنظیم شود.

SCFI-1-1: حصول اطمینان از تنظیم "رمزعبور ورود"

شرح اجمالی:

رمزعبور ورود پیش‌فرض تغییر داده شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم رمزعبور ورود اجرا کنید:

```
hostname(config)#passwd <login_password>
```

جهت ورود به سیستم پارامتر `<login_password>` باید بصورت متن ساده استفاده شود.

SCFI-1-2: حصول اطمینان از تنظیم "رمزعبور فعال"

شرح اجمالی:

برای کاربرانی که دسترسی به حالت خاص و ویژه EXEC دارند، هنگامی که دستور فعال را اجرا می‌کنند، رمزعبور تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر برای تنظیم رمزعبور فعال اجرا کنید:

```
hostname(config)#enable password <enable_password> level <privilege_level>
```

جهت ورود به حالت فعال پارامتر <enable_password> باید بصورت متن ساده استفاده شود. اگر پارامتر <privilege_level> تنظیم نشده باشد، مقدار پیش‌فرض آن ۱۵ خواهد بود.

SCFI-1-3: حصول اطمینان از تنظیم "عبارت‌عبور کلید اصلی"

شرح اجمالی:

عبارت‌عبور کلید اصلی که برای رمزنگاری کلید مخفی موجود در فایل تنظیمات نسخه‌های نرم‌افزاری 8.3(1) به بالا استفاده می‌شود، تعریف گردد.

نحوه پیاده‌سازی:

- مرحله ۱: عبارت‌عبور کلید اصلی را با دستور زیر تنظیم کنید:

```
hostname (config)# key config-key password-encryption <passphrase>
```

طول <passphrase> بین ۸ تا ۱۲۸ کاراکتر می‌باشد.

- مرحله۲: رمزنگاری AES کلیدهای موجود در running-configuration را با دستور زیر فعال‌سازی کنید:

```
hostname(config)# password encryption aes
```

- مرحله۳: دستور زیر را جهت رمزنگاری کلیدهای موجود در startup-configuration اجرا کنید:

```
hostname(config)# write memory
```

SCFI-1-4: حصول اطمینان از غیرفعال بودن "بازیابی رمزعبور"

شرح اجمالی:

بازیابی رمزعبور (امکان بازیابی رمزعبور) غیرفعال شود.

نحوه پیاده‌سازی:

دستور زیر را جهت غیرفعال کردن "بازیابی رمزعبور" اجرا کنید:

```
hostname (config)# no service password-recovery
```

SCFI-1-5: حصول اطمینان از فعال بودن "خط‌مشی رمزعبور"

شرح اجمالی:

با تنظیم الزامات رمزعبور محلی برای تجهیزهای امنیتی، خط‌مشی رمزعبور شرکت را اجبار کنید.

نحوه پیاده‌سازی:

- مرحله۱: دستور زیر را جهت تنظیم مدت اعتبار رمزعبور برحسب روز، که برابر یا کمتر از ۱۸۰ می‌باشد، اجرا کنید:

```
hostname(config)#password-policy lifetime 30
```

- مرحله۲: دستور زیر برای مشخص شدن حداقل تعداد کاراکترهایی که باید بین پسورد قدیم و جدید تغییر کند، که باید بزرگتر یا مساوی ۱۴ باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-changes 14
```

- مرحله۳: دستور زیر برای تعیین حداقل تعداد حروف بزرگ در رمزعبور، که باید بزرگتر یا مساوی ۱ باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-uppercase 1
```

- مرحله۴: دستور زیر برای تعیین حداقل تعداد حروف کوچک در پسورد، که باید بزرگتر یا مساوی ۱ باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-lowercase 1
```

- مرحله۵: دستور زیر برای تعیین حداقل تعداد حروف عددی در پسورد، که باید بزرگتر یا مساوی ۱ باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-numeric 1
```

- مرحله۶: دستور زیر جهت تعیین حداقل تعداد حروف خاص در پسورد، که باید بزرگتر یا مساوی یک باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-special 1
```

- مرحله۷: دستور زیر برای تعیین حداقل طول پسورد که باید بزرگتر یا مساوی ۱۴ باشد، اجرا کنید:

```
hostname(config)#password-policy minimum-length 14
```

SCFI-2: مدیریت دستگاه

نام دستگاه تجهیز امنیتی را تنظیم کنید.

SCFI-2-1: حصول اطمینان از تنظیم "نام دامنه"

شرح اجمالی:

برای تجهیزهای امنیتی نام دامنه تنظیم گردد.

نحوه پیاده‌سازی:

- مرحله۱: نام دامنه شرکت یا سازمان <*enterprise_domain*> را بدست آورید.
- مرحله۲: جهت تنظیم نام دامنه دستور زیر را اجرا کنید:

```
hostname(config)#domain-name <enterprise_domain>
```

SCFI-2-2: حصول اطمینان از تنظیم "نام دامنه"

شرح اجمالی:

نام میزبان پیش‌فرض دستگاه تغییر داده شود.

نحوه پیاده‌سازی:

- مرحله۱: اصول نامگذاری شرکت یا سازمان را جهت تعیین <*name_of_device*> بدست آورید.
- مرحله۲: دستور زیر جهت تنظیم نام میزبان دستگاه اجرا کنید:

```
hostname(config)#hostname <name_of_device>
```

SCFI-2-3: حصول اطمینان از فعال بودن "عدم‌موفقیت"

شرح اجمالی:

عدم‌موفقیت بین یک دستگاه امنیتی و دیگر دستگاه امنیتی جهت دستیابی به دسترسی بالا فعال گردد.

نحوه پیاده‌سازی:

مراحل زیر را جهت فعال کردن active/standby failover دنبال کنید. دستورات باید در محیط execution اجرا شوند.

- مرحله۱: برای هر دستگاه، واسط فیزیکی لینک عدم‌موفقیت[۴] (<failover_interface_physical>) را مشخص کرده و یک نام (<failover_interface_name>)، یک آدرس IP (<failover_interface_ip>) و ماسک زیرشبکه (<failover_interface_mask>) به آن اختصاص دهید. آدرس IP هر دستگاه دیگر که به عنوان (<peer_failover_ip>) می‌باشد را مشخص کنید.
- مرحله۲: برای هر دستگاه، واسط فیزیکی لینک حالت (<state_interface_physical>) را مشخص کرده و نام (<state_interface_name>)، ادرس IP (<state_interface_IP>) و ماسک زیرشبکه (<state_interface_mask>) به آن اختصاص دهید. آدرس IP هر دستگاه دیگر که به عنوان (<peer_state_ip>) می‌باشد را مشخص کنید.
- مرحله۳: بر روی دستگاهی که بعنوان Active درنظر گرفته شده است دستور زیر را اجرا کنید تا آن را بعنوان node اولیه تنظیم کنید:

```
hostname(config)#failover lan unit primary
```

- مرحله۴: بر روی دستگاه Standby جهت تعیین آن بعنوان node ثانویه دستور زیر را اجرا کنید:

```
hostname(config)#failover lan unit secondary
```

- مرحله۵: بر روی هر دو دستگاه‌های امنیتی دستورات زیر را اجرا کنید:

```
hostname(config)# failover lan interface <failover_interface_name>
<failover_interface_physical>
```

[۴] Failover Link Physical Interface

```
hostname(config)#failover interface ip <failover_interface_name>
<failover_interface_ip> <failover_interface_mask> standby <peer_failover_ip>
hostname(config)#interface <failover_interface_physical>
hostname(config-if) #no shutdown
hostname(config)#failover link <state_interface_name> <state_interface_physical>
hostname(config)#failover interface ip <state_interface_name> <state_interface_ip>
<state_interface_mask> standby <peer_state_ip>
hostname(config)#interface <state_interface_physical>
hostname(config-if) #no shutdown
hostname(config)# failover
hostname(config)# write memory
```

SCFI-2-4: حصول اطمینان از غیرفعال بودن واسط‌های بلا استفاده

شرح اجمالی:

واسط‌های بلا استفاده غیرفعال گردند.

نحوه پیاده‌سازی:

- مرحله۱: نام فیزیکی (<interface_physical_name>) واسط‌های بلا استفاده‌ای که غیرفعال نشده‌اند را مشخص کنید.
- مرحله۲: برای هر یک از واسط‌های مشخص شده دستور زیر را اجرا کنید:

```
Hostname(config)#interface <interface_physical_name>
Hostname(config-if)#shutdown
```

SCFI-3: امنیت تصویر

جامعیت و صحت تصویر بررسی شود.

SCFI-3-1: حصول اطمینان از صحیح بودن "جامعیت تصویر"

شرح اجمالی:

پیش از ارتقاء دادن سیستم، درستی نرم‌افزار بارگذاری شده بررسی شود.

نحوه پیاده‌سازی:

- مرحله۱: محل تصوری جدید (<new_image_location>) در دستگاه امنیتی و مقدار کنترلی[۵] MD5 را از وب سایت Cisco.com بدست آورید.
- مرحله۲: دستور زیر را جهت بررسی یکی بودن مقدار کنترلی تصویر جدید با مقداری که در وب سایت Cisco.com درج شده، اجرا کنید:

```
hostname# verify <new_image_location> <md5_checksum>
```

- مرحله۳: اگر عبارت "Verified" در پایان خروجی دستور بالا نمایش داده شد، تصویر جدید معتبر می‌باشد. در صورتی که پیام "%Error Verifying" نمایش داده شود تصویر معتبر نمی‌باشد.

SCFI-3-2: حصول اطمینان از صحیح بودن "صحت تصویر"

شرح اجمالی:

بررسی تصاویر دیجیتالی امضا شده، تا مشخص شود تصویر اجرایی از منبع مورد اطمینان می‌باشد.

نحوه پیاده‌سازی:

- مرحله۱: خطاها بر روی سخت‌افزار و نرم‌افزار تصحیح گردد.
- مرحله۲: دستور زیر جهت بررسی صحت تصویر اجرا شده بر روی دستگاه امنیتی اجرا کنید:

[۵] Checksum

```
hostname# show software authenticity running | in CiscoSystems$
```

- مرحله۳: پیاده‌سازی تحویل امن سخت‌افزار و سخت‌گیری در موررد سرورهای توزیع‌کننده نرم‌افزار.

SCFI-4: احراز هویت، مجوزدهی و حسابرسی[۶]

طرح AAA (احراز هویت، مجوزدهی و حسابرسی)، الزامات امنیتی مربوط به کنترل دسترسی، عمدتاً در راستایی فراهم کردن مکانیزم‌های احرازهویت کاربر، کنترل مجوزهای آن‌ها و دنبال کردن رفتار آن‌ها بر روی سیستم، را پیاده‌سازی می‌کند. AAA یک روش اولیه برای احرازهویت کاربر فراهم می‌نماید و سپس یک روش پشتیبان‌گیری مشخص می‌سازد.

SCFI-4-1: قوانین AAA محلی

الزامات AAA را برای پایگاه‌داده محلی کاربران تنظیم کنید.

SCFI-4-1-1: حصول اطمینان از تنظیم حداکثر تعداد احراز هویت محلی AAA به کمتر یا مساوی ۳

شرح اجمالی:

حداکثر تعداد دفعاتی که کاربر محلی می‌تواند قبل از قفل شدن، پسورد اشتباه وارد کند محدود گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم حداکثر تعداد دفعات ورود ناموفق متوالی محلی به ۳مرتبه و کمتر اجرا کنید:

```
hostname(config)#aaa local authentication attempts max-fail 3
```

SCFI-4-1-2: حصول اطمینان از تنظیم نام کاربری و پسورد محلی

شرح اجمالی:

یک نام کاربری و پسورد محلی تنظیم شود.

نحوه پیاده‌سازی:

[۶] Authentication, Authorization, Accounting(AAA)

دستور زیر را برای تنظیم یک نام کاربری و پسورد محلی اجرا کنید:

```
hostname(config)#username <local_username> password <local_password> privilege <level>
```

مقدار privilege بین ۰ تا ۱۵ انتخاب می شود. در صورتی که تنظیم نشود مقدار پیش فرض ۲ خواهد بود.

SCFI-4-1-3: حصول اطمینان از وجود نداشتن اکانت‌های پیش‌فرض شناخته شده

شرح اجمالی:

اکانت‌های پیش‌فرض شناخته شده که پیکربندی شده‌اند، حذف گردند.

نحوه پیاده‌سازی:

- مرحله۱: اکانت مدیریتی خصوصی شده‌ی سازمان <customized_admin_account> و پسورد <admin_password> بدست آورده شود.
- مرحله۲: دستور زیر را جهت ایجاد اکانت مدیریتی ویژه همراه با سطح دسترسی متناسب <privilege_level> اجرا کنید:

```
hostname(config)#username <customized_admin_account> password <admin_password>
privilege <privilege_level>
```

- مرحله۳: دستور زیر را جهت حذف اکانت‌های پیش‌فرض شناخته شده حین بازرسی، اجرا کنید:

```
hostname(config)# no username <known_default_account>
```

SCFI-4-2: سرورهای AAA راه‌دور

سرورهای AAA را برای احرازهویت راه‌دور تنظیم کنید.

SCFI-4-2-1: حصول اطمینان از تنظیم صحیح "TACACS+/RADIUS"

شرح اجمالی:

گروه سرور AAA و هر سرور که از پروتکل TACACS+ یا RADIUS استفاده می‌کند، مشخص گردد.

نحوه پیاده‌سازی:

- مرحله۱: پروتکل استاندارد سازمان (protocol_name) برای احرازهویت (TACACS+/RADIUS) بدست آورده شود.
- مرحله۲: دستور زیر را برای تنظیم پروتکل مورد نیاز گروه سرور AAA اجرا کنید:

```
hostname(config)#aaa-server <server-group_name> protocol <protocol_name>
```

- مرحله۳: دستور زیر را برای تنظیم سرور AAA اجرا کنید:

```
hostname(config)#aaa-server <server-group_name> (<interface_name>) host
<aaaserver_ip> <shared_key>
```

Server-group_name: گروه سرور تنظیم شده در مرحله۲ را مشخص می‌نماید.

Interface_name: واسط شبکه‌ای که به سرور AAA دسترسی دارد.

aaa-server_ip: ادرس IP سرور AAA را مشخص می‌نماید.

shared_key: کلید عمومی +TACACS یا RADIUS را مشخص می‌نماید.

SCFI-4-3: احراز هویت AAA

قوانین احرازهویت AAA تعریف شوند.

SCFI-4-3-1: حصول اطمینان از تنظیم صحیح "aaa authentication enable console"

شرح اجمالی:

کاربرانی که قصد دسترسی به حالت Enable (privileged EXEC mode) بوسیله دستور "enable" را دارند، احرازهویت شوند.

نحوه پیاده‌سازی:

با استفاده از دستور زیر احرازهویت aaa را برای "دسترسی فعال" که از TACACS+ server-group بعنوان روش اولیه احرازهویت و پایگاه‌داده محلی بعنوان روش پشتیبان استفاده می‌کند، پیکربندی کنید:

```
hostname(config)# aaa authentication enable console <server-group_name> local
```

SCFI-4-3-2: حصول اطمینان از تنظیم صحیح "aaa authentication http console"

شرح اجمالی:

کاربران ASDM که تحت پروتکل HTTP به دستگاه امنیتی دسترسی دارند را احرازهویت کنید.

نحوه پیاده‌سازی:

با استفاده از دستور زیر احرازهویت aaa را برای "HTTP" که از TACACS+ server-group بعنوان روش اولیه احرازهویت و پایگاه‌داده محلی بعنوان روش پشتیبان استفاده می‌کند، پیکربندی کنید:

```
hostname(config)#aaa authentication http console <server-group_name> local
```

SCFI-4-3-3: حصول اطمینان از تنظیم صحیح "aaa authentication secure-http-client"

شرح اجمالی:

یک روش امن، SSL، برای محافظت از نام کاربری و پسورد ارسال شده بصورت متن ساده فراهم گردد.

نحوه پیاده‌سازی:

دستور زیر را برای تنظیم احرازهویت aaa ایمن برای پروتکل HTTP، اجرا کنید:

```
hostname(config)#aaa authentication secure-http-client
```

SCFI-4-3-4: حصول اطمینان از تنظیم صحیح "aaa authentication serial console"

شرح اجمالی:

کاربرانی که به دستگاه امنیتی بوسیله پورت serial console دسترسی دارند، احرازهویت گردند.

نحوه پیاده‌سازی:

با استفاده از دستور زیر احرازهویت aaa را برای "serial" که از TACACS+ server-group بعنوان روش اولیه احرازهویت و پایگاه‌داده محلی بعنوان روش پشتیبان استفاده می‌کند، پیکربندی کنید:

```
hostname(config)#aaa authentication serial console <server-group_name> local
```

SCFI-4-3-5: حصول اطمینان از تنظیم صحیح "aaa authentication ssh console"

شرح اجمالی:

کاربرانی که به دستگاه امنیتی با استفاده از ssh دسترسی دارند، احرازهویت گردند.

نحوه پیاده‌سازی:

با استفاده از دستور زیر احرازهویت aaa را برای "ssh" که از TACACS+ server-group بعنوان روش اولیه احرازهویت و پایگاه‌داده محلی بعنوان روش پشتیبان استفاده می‌کند، پیکربندی کنید:

```
hostname(config)#aaa authentication ssh console <server-group_name> local
```

SCFI-4-3-6: حصول اطمینان از تنظیم صحیح "aaa authentication telnet console"

شرح اجمالی:

کاربرانی که به دستگاه امنیتی با استفاده از telnet دسترسی دارند، احرازهویت گردند.

نحوه پیاده‌سازی:

با استفاده از دستور زیر احرازهویت aaa را برای "telnet" که از TACACS+ server-group بعنوان روش اولیه احرازهویت و پایگاه‌داده محلی بعنوان روش پشتیبان استفاده می‌کند، پیکربندی کنید:

```
hostname(config)#aaa authentication telnet console <server-group_name> local
```

SCFI-4-4: مجوزدهی AAA

قوانین مجوزدهی AAA تعریف شوند.

SCFI-4-4-1: حصول اطمینان از تنظیم صحیح "aaa command authorization"

شرح اجمالی:

منبع مجوزدهی برای دستوراتی که توسط مدیر یا کاربر وارد می‌شوند، تعریف شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تعیین سرورهای TACACS+/RADIUS (server_group_name) راه دور بعنوان منبع مجوزدهی و پایگاه‌داده محلی (LOCAL) را بعنوان روش ذخیره در صورتی که سرور راه‌دور در دسترس نباشد، اجرا کنید:

```
hostname(config)# aaa authorization command <server-group_name> local
```

این بدین معنی است که، هر سطح دسترسی دستورات تنظیم شده‌ای را دارد و هر نام کاربری با توجه به دسترسی و دستوراتی که در سرور راه‌دور تعریف شده، می‌تواند از دستورات استفاده کند.

SCFI-4-4-2: حصول اطمینان از تنظیم صحیح "aaa authorization exec"

شرح اجمالی:

دسترسی به حالت privileged EXEC، محدود شود.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن AAA authorization exec اجرا کنید:

```
hostname(config)# aaa authorization exec authentication-server
```

SCFI-4-5: حسابرسی AAA

قوانین حسابرسی AAA تعریف شوند.

SCFI-4-5-1: حصول اطمینان از تنظیم صحیح "aaa command accounting"

شرح اجمالی:

فعال کردن حسابرسی دسترسی مدیر را بوسیله مشخص کردن هر دستور یا دستورات یک سطح دسترسی مشخص شده یا بالاتر که بوسیله مدیر/ کاربر ضبط شده وارد شده و به سرور یا سرورهای حسابرسی ارسال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت ضبط تمامی دستورات وارد شده در تمام سطوح دسترسی و ارسال انها به سرور AAA اجرا کنید:

```
hostname(config)# aaa accounting command <server-group_name>
```

SCFI-4-5-2: حصول اطمینان از تنظیم صحیح "aaa accounting for SSH"

شرح اجمالی:

حسابرسی دسترسی مدیر بوسیله مشخص کردن شروع و پایان یک جلسه SSH فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت ضبط شروع و پایان یک جلسه SSH و ارسال آن به سرور AAA اجرا کنید:

```
hostname(config)# aaa accounting ssh console <server-group_name>
```

SCFI-4-5-3: حصول اطمینان از تنظیم صحیح "aaa accounting for Serial console"

شرح اجمالی:

حسابرسی دسترسی مدیر بوسیله مشخص کردن شروع و پایان یک جلسه Serial console فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت ضبط شروع و پایان یک جلسه serial console و ارسال ان به سرور AAA اجرا کنید

```
hostname(config)# aaa accounting serial console <server-group_name>
```

SCFI-4-5-4: حصول اطمینان از تنظیم صحیح "aaa accounting for EXEC mode"

شرح اجمالی:

حسابرسی دسترسی مدیر بوسیله مشخص کردن شروع و پایان یک جلسه EXEC فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت ضبط شروع و پایان یک جلسه exec mode و ارسال ان به سرور AAA اجرا کنید:

```
hostname(config)# aaa accounting enable console <server-group_name>
```

SCFI-5: قوانین بنر

قوانین کلاس بنر[۷]، حقوق قانونی را به کاربران مکاتبه می‌کنند.

SCFI-5-1: حصول اطمینان از تنظیم "ASDM banner"

شرح اجمالی:

پیام بنر برای دسترسی ASDM تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم بنر ASDM در جایی که <line_of_message> یک خط متن بنر باشد، اجرا کنید:

```
hostname(config)#banner asdm <line_of_message>
```

در صورتیکه متن بنر شامل چندین خط باشد دستور بالا را برای هر خط اجرا کنید.

SCFI-5-2: حصول اطمینان از تنظیم "EXEC banner"

شرح اجمالی:

[۷] Banner

پیام بنر برای دسترسی به حالت privileged EXEC تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم بنر EXEC در جایی که <line_of_message> یک خط متن بنر باشد، اجرا کنید:

```
hostname(config)#banner exec <line_of_message>
```

در صورتیکه متن بنر شامل چندین خط باشد دستور بالا را برای هر خط اجرا کنید.

SCFI-5-3: حصول اطمینان از تنظیم "LOGIN banner"

شرح اجمالی:

بنر LOGIN برای دسترسی به محیط Command Line Interface (CLI) تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم بنر LOGIN در جایی که <line_of_message> یک خط متن بنر باشد، اجرا کنید:

```
hostname(config)#banner login <line_of_message>
```

در صورتیکه متن بنر شامل چندین خط باشد دستور بالا را برای هر خط اجرا کنید.

SCFI-5-4: حصول اطمینان از تنظیم "MOTD banner"

شرح اجمالی:

بنر پیام روز (MOTD) برای اولین دسترسی به محیط CLI تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم بنر MOTD در جایی که <line_of_message> یک خط متن بنر باشد، اجرا کنید:

```
hostname(config)#banner motd <line_of_message>
```

در صورتیکه متن بنر شامل چندین خط باشد دستور بالا را برای هر خط اجرا کنید.

SCFI-6: قوانین SSH

الزامات SSH را تعریف کنید.

SCFI-6-1: حصول اطمینان از تنظیم "SSH source restriction" به آدرس IP مجاز

شرح اجمالی:

آدرس‌های IP کاربران مجاز جهت اتصال به دستگاه امنیتی بوسیله SSH، مشخص گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن محدودیت منبع دسترسی به SSH اجرا کنید:

```
hostname(config)#ssh <source_ip> <source_netmask> <interface_name>
```

SCFI-6-2: حصول اطمینان از فعال بودن "SSH version 2"

شرح اجمالی:

نسخه SSH به ۲ تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن نسخه ۲ SSH اجرا کنید:

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

SCFI-6-3: حصول اطمینان از بزرگتر یا مساوی بودن "RSA key pair" از ۲۰۴۸ بیت

شرح اجمالی:

یک RSA key pair استفاده شده بوسیله پروتکل SSH با طول حداقل ۲۰۴۸ بیت، ایجاد شود.

نحوه پیاده‌سازی:

- مرحله۱: اندازه استاندارد RSA key سازمان بزرگتر یا مساوی ۲۰۴۸ بیت، بدست آورده شود.
- مرحله۲: در صورتیکه روال حسابرسی یک key pairs را نشان داد، دستور زیر را جهت پاک کردن آن اجرا کنید:

```
hostname(config)#crypto key zeroize rsa
```

- مرحله۳: دستور زیر را جهت ایجاد RSA key pair صحیح، اجرا کنید:

```
hostname(config)# crypto key generate rsa modulus<enterprise_RSA_key_size>
```

- مرحله۴: دستور زیر را جهت ذخیره RSA keys در حافظه ماندگار، اجرا کنید:

```
hostname(config)# write memory
```

SCFI-6-4: حصول اطمینان از تنظیم فعال بودن "SCP protocol" برای ارسال فایل

شرح اجمالی:

پروتکل کپی ایمن[۸] فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن کپی ایمن، اجرا کنید:

```
hostname(config)# ssh scopy enable
```

SCFI-6-5: حصول اطمینان از غیرفعال بودن "Telnet"

شرح اجمالی:

دسترسی telnet جهت دسترسی به دستگاه امنیتی، در حالتی که ازقبل تنظیم شده باشد، غیرفعال گردد.

نحوه پیاده‌سازی:

- مرحله۱: دستور زیر را جهت غیرفعال کردن دسترسی telnet، اجرا کنید:

```
hostname(config)#no telnet 0.0.0.0 0.0.0.0 <interface_name>
```

- مرحله۲: دستور زیر را جهت پاک کردن تنظیمات telnet timeout، اجرا کنید:

[۸] Secure Copy protocol

```
hostname(config)#no telnet timeout <configured_timeout>
```

SCFI-7: قوانین HTTP

الزامات HTTP را تعریف کنید.

SCFI-7-1: حصول اطمینان از تنظیم "HTTP source restriction" به آدرس IP مجاز

شرح اجمالی:

آدرس‌های IP کاربران مجاز جهت اتصال به دستگاه امنیتی بوسیله HTTP، مشخص گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن محدودیت منبع دسترسی به HTTP اجرا کنید:

```
hostname(config)#http <source_ip> <source_netmask> <interface_name>
```

SCFI-7-2: حصول اطمینان از تنظیم "TLS 1.0" برای دسترسی HTTPS

شرح اجمالی:

نسخه SSL سرور به TLS 1.0 فعال گردد.

نحوه پیاده‌سازی:

برای ورژن 8.x دستور زیر را جهت فعال کردن الگوریتم AES256 اجرا کنید:

```
hostname(config)# ssl encryption aes256-sha1
```

برای ورژن 9.x دستور زیر را جهت فعال کردن الگوریتم AES256 اجرا کنید:

```
hostname(config)# ssl cipher tlsv1 custom AES256-SHA
```

SCFI-7-3: حصول اطمینان از تنظیم "SSL AES 256 encryption" برای دسترسی HTTPS

شرح اجمالی:

الگوریتم رمزنگاری SSL به AES256 تنظیم شود.

نحوه پیاده‌سازی:

برای ورژن 8.x دستور زیر را جهت فعال کردن الگوریتم AES256 اجرا کنید:

```
hostname(config)# ssl encryption aes256-sha1
```

برای ورژن 9.x دستور زیر را جهت فعال کردن الگوریتم AES256 اجرا کنید:

```
hostname(config)# ssl cipher tlsv1 custom AES256-SHA
```

SCFI-8: Session timeout

مقادیر زمان اتمام idle را تنظیم کنید.

SCFI-8-1: حصول اطمینان از تنظیم "console session timeout" به کمتر یا مساوی ۵ دقیقه

شرح اجمالی:

زمان اتمام idle را برای console session قبل از اینکه دستگاه امنیتی آن را پایان دهد، تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم console timeout به مقدار مساوی یا کمتر از ۵ دقیقه، اجرا کنید:

```
hostname(config)# console timeout 5
```

SCFI-8-2: حصول اطمینان از تنظیم "SSH session timeout" به کمتر یا مساوی ۵ دقیقه

شرح اجمالی:

زمان اتمام idle را برای SSH session قبل از اینکه دستگاه امنیتی آن را پایان دهد، تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم SSH timeout به مقدار مساوی یا کمتر از ۵ دقیقه، اجرا کنید:

```
hostname(config)# ssh timeout 5
```

SCFI-8-3: حصول اطمینان از تنظیم "HTTP session timeout" به کمتر یا مساوی ۵ دقیقه

شرح اجمالی:

زمان اتمام idle را برای HTTP session قبل از اینکه دستگاه امنیتی آن را پایان دهد، تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را جهت تنظیم HTTP timeout به مقدار مساوی یا کمتر از ۵ دقیقه، اجرا کنید:

```
hostname(config)# http server session-timeout 5
```

SCFI-9: قوانین ساعت

زمان دستگاه تنظیم شود.

SCFI-9-1: قوانین NTP

الزامات NTP (Network Time Protocol) تعریف شوند.

SCFI-9-1-1: حصول اطمینان از فعال بودن "NTP authentication"

شرح اجمالی:

احرازهویت NTP جهت دریافت اطلاعات زمانی فقط از منابع تصدیق شده، فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را جهت فعال کردن NTP authentication، اجرا کنید:

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

SCFI-9-1-2: حصول اطمینان از تنظیم صحیح "NTP authentication key"

شرح اجمالی:

کلیدی که برای احرازهویت سرورهای NTP استفاده می‌شود، تنظیم شود.

نحوه پیاده‌سازی:

- مرحله۱: دستور زیر را جهت تنظیم authentication key ID<key_id>، اجرا کنید:

```
hostname(config)# ntp trusted-key <key_id>
```

- مرحله۲: دستور زیر را جهت تنظیم authentication key <authentication_key>، اجرا کنید:

```
hostname(config)# ntp authentication-key <key_id> md5 <authentication_key>
```

SCFI-9-1-3: حصول اطمینان از وجود "trusted NTP server"

شرح اجمالی:

برای زمانیکه احرازهویت فعال شده باشد، جهت دریافت اطلاعات زمانی، یک NTP سرور تنظیم شود.

نحوه پیاده‌سازی:

- مرحله۱: بدست اوردن authentication key ID <key_id> و ادرس IP سرور NTP <ip_address> و رابط<interface_name> استفاده شده توسط دستگاه جهت ارتباط با سرور NTP
- مرحله۲: دستور زیر را جهت تنظیم NTP سرور تصدیق شده[۹]، اجرا کنید:

```
hostname(config)# ntp server <ip_address> key <key_id> source <interface_name>
```

[۹] Trusted

SCFI-9-2: حصول اطمینان از تنظیم صحیح "local timezone"

شرح اجمالی:

اطلاعات منطقه زمانی محلی جهت نمایش زمان متناسب توسط ASA برای کسانی که آن را مشاهده می‌کنند، تنظیم گردد.

نحوه پیاده‌سازی:

- مرحله۱: استاندارد نام منطقه زمانی(enterprise_zone_name) استفاده شده توسط سازمان(GMT, UTC, EDT, PST)، بدست آورده شود.
- مرحله۲: دستور زیر را جهت تنظیم مقادیر مورد نیاز، اجرا کنید:

```
hostname(config)# clock timezone <enterprise_zone_name> <local_offset>
```

SCFI-10: قوانین ثبت وقایع

قوانین کلاس ثبت وقایع، کنترل‌هایی را انجام می‌دهد که ضبط فعالیت‌ها و رویدادهای سیستمی را فراهم می‌سازد.

SCFI-10-1: حصول اطمینان از فعال بودن ثبت وقایع

شرح اجمالی:

ثبت وقایع دستگاه فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را برای فعال‌سازی ثبت وقایع اجرا کنید:

```
hostname(config)#logging enable
```

SCFI-10-2: حصول اطمینان از غیرفعال بودن نمایش لاگ بر روی کنسول

شرح اجمالی:

فعال بودن، فرستادن لاگ‌ها به serial console، موجب ایجاد اختلال در ارسال لاگ‌ها به سمت syslog server و buffer می‌شود زیرا سرعت تولید لاگ پیرو سرعت کنسول سریال می‌باشد.

نحوه پیاده‌سازی:

دستور زیر را برای غیرفعال‌سازی ثبت رخدادها در کنسول، اجرا کنید:

```
hostname(config)#no logging console
```

SCFI-10-3: حصول اطمینان از غیرفعال بودن نمایش لاگ‌ها بر روی مانیتور

شرح اجمالی:

logging to monitor غیرفعال گردد.

نحوه پیاده‌سازی:

دستور زیر را برای غیرفعال‌سازی مانیتور کردن رخدادها، اجرا کنید:

```
hostname(config)#no logging monitor
```

SCFI-10-4: حصول اطمینان از پیکربندی صحیح syslog host

شرح اجمالی:

تنظیم گیرنده اطلاع SNMP یا مدیریت SNMP یا NMS که بتواند به ASA وصل شود.

نحوه پیاده‌سازی:

دستور زیر را برای پیکربندی سرور Syslog، اجرا کنید:

```
hostname(config)# logging host <interface_name> <host_ip_address>
```

SCFI-10-5: حصول اطمینان از ثبت وقایع بر اساس IDدستگاه

شرح اجمالی:

در لاگ‌های تولید شده ID دستگاه قرار گرفته شده باشد.

نحوه پیاده‌سازی:

دستور زیر را برای فعال کردن ثبت وقایع بر اساس نام دستگاه، اجرا کنید:

```
hostname(config)#logging device-id hostname
```

در دستگاه‌های امنیتی multi-context از دستور زیر استفاده نمایید.

```
hostname(config)#logging device-id context-name
```

SCFI-10-6: حصول اطمینان از تنظیم سطح حساسیت تاریخچه ثبت وقایع به مساوی یا بالاتر از ۵

شرح اجمالی:

مشخص شود که چه پیام‌های Syslog ای به سمت SNMP Server فرستاده شود.

نحوه پیاده‌سازی:

دستور زیر را برای ثبت رخدادهای سطح ۵، اجرا کنید:

```
hostname(config)# logging history 5
```

SCFI-10-7: حصول اطمینان از فعال بودن ثبت وقایع همراه با Timestamp

شرح اجمالی:

به timestamp برای تولید و ثبت لاگ، اجازه داده شود.

نحوه پیاده‌سازی:

دستور زیر را برای فعال کردن TimeStamp برای ثبت رخدادها، اجرا کنید:

```
hostname(config)#logging timestamp
```

SCFI-10-8: حصول اطمینان از تنظیم امکان Syslog Logging به ۲۳

شرح اجمالی:

تنظیم امکان (location) بر روی Syslog Server برای رخدادهایی که از سمت تجهیزات امنیتی ارسال می‌گردد.

نحوه پیاده‌سازی:

دستور زیر را برای ثبت رخدادها با مقدار Facility برابر ۲۳، اجرا کنید:

```
hostname(config)# logging facility 23
```

SCFI-10-9: حصول اطمینان از تنظیم اندازه بافر ثبت وقایع به مساوی یا بزرگتر از 512 Kb

شرح اجمالی:

مشخص کردن سایز محلی بافر که بر روی آن رخدادها ذخیره می‌شود به طوریکه توسط مدیر شبکه چک شود.

نحوه پیاده‌سازی:

دستور زیر را برای تنظیم اندازه بافر ثبت رخدادها بر روی ۵۲۴۲۸۸، اجرا کنید:

```
hostname(config)# logging buffer-size 524288
```

SCFI-10-10: حصول اطمینان از تنظیم سطح حساسیت رخدادهای ذخیره شده در بافر به مساوی یا بزرگتر از ۳

شرح اجمالی:

مشخص میکند که چه پیام های Syslog به صورت موقت بر روی بافر محلی دخیره شود تا توسط مدیر شبکه چک شود.

نحوه پیاده‌سازی:

دستور زیر را برای تنظیم سطح حساسیت رخدادهایی که در بافر ذخیره می‌شود بر روی ۳، اجرا کنید:

```
hostname(config)# logging buffered 3
```

SCFI-10-11: حصول اطمینان از تنظیم سطح حساسیت Logging Trap به مساوی یا بزرگتر از ۵

شرح اجمالی:

مشخص می‌کند که چه پیام‌های Syslog به سمت سرور syslog ارسال شود.

نحوه پیاده‌سازی:

دستور زیر را برای بررسی اینکه logging trap برابر با ۵ باشد، اجرا کنید:

```
hostname(config)# logging trap 5
```

SCFI-10-12: حصول اطمینان از تنظیم بودن ارسال ایمیل ثبت وقایع برای Criticalتا Emergency

شرح اجمالی:

اگر رخدادی با سطح حساسیت Critical تا Emergency ثبت شد برای گیرنده مشخصی ایمیل ارسال شود.

نحوه پیاده‌سازی:

۱- برای فعال کردن ایمیل ثبت رخدادها از سطح حساسیت Critical به بالا از دستور زیر استفاده کنید:

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

۲- تعریف حساب کاربری ایمیل برای فایروال که توسط مدیر سرور ایمیل ساخته شده است.

```
hostname(config)#logging from-address <firewall_email_account>
```

۳- توسط دستور زیر ایمیل مدیر فایروال را وارد کنید تا در صورت ثبت رخداد توسط فایروال به حساب کاربری مدیر فایروال ایمیل ارسال شود.

```
hostname(config)#logging recipient-address <firewall_admin_email>
```

۴- با دستور زیر IPمیل سرور را پیکربندی کنید:

```
hostname(config)#smtp-server <mail_server_ip>
```

SCFI-11: قوانین SNMP

قوانین کلاس SNMP، مدیریت و ایمن شبکه و مانیتورینگ دستگاه را اجرا می‌کنند.

SCFI-11-1: حصول اطمینان از تنظیم "SNMP-Server Group" به "v3 priv"

شرح اجمالی:

گروه SNMP V3 با احرازهویت و حریم خصوصی، تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را برای پیکربندی گروه SNMP v3، اجرا کنید:

```
hostname(config)# snmp-server group <group_name>  v3 priv
```

SCFI-11-2: حصول اطمینان از تنظیم "snmp-server user" به "v3 auth SHA"

شرح اجمالی:

کاربر SNMP v3 همراه با احراز هویت SHA و رمزنگاری AES-256 تنظیم شود.

نحوه پیاده‌سازی:

دستور زیر را اجرا کنید:

```
hostname(config)#snmp-server user <snmp_username>  <group-name> v3 auth SHA
<authentication_password> priv AES 256 <encryption_password>
```

SCFI-11-3: حصول اطمیان ازتنظیم "snmp-server host" به "version 3"

شرح اجمالی:

تنظیم گیرنده اخطار SNMP یا مدیریت SNMP یا NMS که بتواند به ASA وصل شود.

نحوه پیاده‌سازی:

دستور زیر برای پیکربندی هاست SNMP v3، اجرا کنید:

```
hostname(config)# snmp-server host <interface_name> <host_ip_address> version 3
<snmp_user>
```

SCFI-11-4: حصول اطمینان از فعال بودن SNMP Traps

شرح اجمالی:

SNMP Trapsبرای ارسال به NMS، فعال شوند.

نحوه پیاده‌سازی:

دستورات زیر را برای فعال سازی SNMP Trap، اجرا کنید:

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

SCFI-11-5: حصول اطمینان از تنظیم نبودن رشته پیش فرض برای "SNMP community string"

شرح اجمالی:

حتما String پیش‌فرض با Community String متفاوت باشد.

نحوه پیاده‌سازی:

دستور زیر را برای پیکربندی SNMP Community String، اجرا کنید:

```
hostname(config)#snmp-server community <snmp_community_string>
```

سطح دسترسی (کنترلی)

سطح کنترلی، به‌روزرسانی‌های جدول مسیریابی، ترافیک هدایت شده سمت دستگاه امنیتی و به‌طور کلی عملیات پویای فایروال را پوشش می‌دهد. پروتکل‌های کنترل شبکه مانند، IGMP، ARP، ICMP نیز در این حوزه قرار می‌گیرند.

SCFI-1: احرازهویت پروتکل‌های مسیریابی

الزام امنیتی پروتکل‌های مسیریابی تعریف گردد.

SCFI-1-1: حصول اطمینان از فعال بودن احرازهویت پروتکل RIP

شرح اجمالی:

فعال کردن احرازهویت RIP v2 قبل از این که اطلاعات مسیریابی از همسایگان دریافت شود.

نحوه پیاده‌سازی:

۱- مشخص کردن واسطی که فایروال آپدیت‌های مسیریابی RIP را از طریق آن دریافت می‌کند.
۲- موافقت با روتر همسایه از طریق کلید احرازهویت و مشخص کردن کلید احراز هویت.
۳- دستورات زیر را برای فعال کردن احرازهویت RIP اجرا کنید:

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

SCFI-1-2: حصول اطمینان از فعال بودن احرازهویت پروتکل OSPF

شرح اجمالی:

فعال کردن احراز هویت OSPF قبل از این که اطلاعات مسیریابی از همسایگان دریافت شود.

نحوه پیاده‌سازی:

۱- مشخص کردن واسطی که فایروال آپدیت‌های مسیریابی OSPF و area ID را از طریق آن دریافت می‌کند.
۲- موافقت با روتر همسایه از طریق کلید احرازهویت و مشخص کردن کلید احراز هویت.
۳- دستورات زیر را برای فعال کردن احراز هویت OSPF اجرا کنید:

```
hostname(config)#interface <interface_name>
hostname(config-if) # ospf authentication message-digest
hostname(config-if) # ospf message-digest-key <key_id> md5 <key_value>
hostname(config-if) #exit
hostname(config)#area <area_id> authentication message-digest
```

SCFI-1-3: حصول اطمینان از فعال بودن احرازهویت پروتکل EIGRP

شرح اجمالی:

فعال کردن احراز هویت EIGRP قبل از این که اطلاعات مسیریابی از همسایگان دریافت شود.

نحوه پیاده‌سازی:

۱- مشخص کردن واسطی که فایروال آپدیت‌های روتینگ EIGRP و شماره AS برای EIGRP را از طریق آن دریافت می‌کند .
۲- موافقت با روتر همسایه از طریق کلید احرازهویت و مشخص کردن کلید احرازهویت.
۳- دستورات زیر را برای فعال کردن احرازهویت EIGRP اجرا کنید:

```
hostname(config)#interface <interface_name>
hostname(config-if) # authentication mode eigrp <as_number> md5
hostname(config-if)# authentication key eigrp <as_number> <key_value> key-id <key_id>
```

SCFI-2: حصول اطمینان از فعال بودن "noproxyarp" روی واسطهای غیرقابل اعتماد

شرح اجمالی:

کارکرد Proxy-ARP بر روی واسطهای غیرقابل اعتماد غیرفعال شود.

نحوه پیاده‌سازی:

۱- بدست آوردن نام واسطهای غیرقابل اعتماد.
۲- دستور زیر را برای غیرفعال کردن Proxy App بر روی واسط غیرقابل اعتماد اجرا کنید:

```
hostname(config)# sysopt noproxyarp <untrusted_interface_name>
```

SCFI-3: حصول اطمینان از فعال بودن "DNS Guard"

شرح اجمالی:

محافظت در مقابل حملاتی که به منظور آلوده کردن DNS cache انجام می‌شوند، فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را برای فعال کردن تابع **"DNS Guard"**، اجرا کنید:

```
hostname(config)# dns-guard
```

SCFI-4: حصول اطمینان از غیرفعال بودن سرویس‌های DHCP برای واسط‌های غیرقابل

شرح اجمالی:

سرویس DHCP غیرفعال شود.

نحوه پیاده‌سازی:

۱- بدست آوردن اسم واسط غیرقابل اعتماد.

۲- دستورات زیر برای غیرفعال‌سازی سرویس DHCP بر روی واسط‌های غیرقابل اعتماد، اجرا کنید:

```
hostname(config)#dynamic-filter updater-client enable
hostname(config)#dynamic-filter use-database
```

۳- دستور زیر را برای غیرفعال‌سازی سرویس DHCP Relay بر روی واسط‌های غیرقابل اعتماد، اجرا کنید:

```
hostname(config)# no dhcprelay enable <untrusted_interface_name>
```

SCFI-5: حصول اطمینان از محدود بودن ICMPبرای واسط‌های غیرقابل اعتماد

شرح اجمالی:

اجازه عبور ترافیک ICMP برای یک هاست‌ها یا زیرشبکه‌های مشخص داده شود و برای بقیه منابع ممنوع گردد.

نحوه پیاده‌سازی:

۱- بدست آوردن نام واسط‌های غیرقابل اعتماد, subnet قابل اعتماد و mask مربوطه.

۲- برای عبور ترافیک ICMP از سمت subnet قابل اعتماد بر روی واسط غیرقابل اعتماد دستور زیر را اجرا کنید:

```
hostname(config)# icmp permit <subnet> <mask> <untrusted_interface_name>
```

۳- دستور زیر را برای ممنوع کردن عبور ترافیک ICMP از هر منبعی روی واسط غیرقابل اعتماد، اجرا کنید:

```
hostname(config)# icmp deny any <untrusted_interface_name>
```

سطح داده

سطح داده برای سرویس‌ها و تنظیمات مربوط به داده‌ای که از دستگاه امنیتی عبور می‌کند، می‌باشد که شامل لیست‌های دسترسی واسط، فایروال عملیاتی، بررسی ترافیک، NAT و IPSEC است.

SCFI-1: حصول اطمینان از پیکربندی صحیح سرویس DNS

شرح اجمالی:

تنظیم DNS Server برای اجرای ارسال درخواست DNS

نحوه پیاده‌سازی:

۱- دستور زیر را برای فعال کردن DNS lookup، اجرا کنید:

```
hostname(config)# dns domain-lookup <interface_name>
```

interface_nameنام واسطی است که به سرور DNS متصل می‌گردد.

۲- گروه DNS Servers را پیکربندی کنید:

```
hostname(config)# dns server-group DefaultDNS
```

۳- آدرس‌های IP سرورهای DNS مجاز را بدست آورده شود، سپس از طریق دستور زیر در گروه DNS ها قرار داده می‌شوند.

```
hostname(config-dns-server-group)#name-server <dns_ip_address>
```

SCFI-2: حصول اطمینان از فعال بودن جلوگیری از نفوذ برای واسط‌های غیرقابل اعتماد

شرح اجمالی:

سیستم جلوگیری از نفوذ با قابلیت بررسی IP بر روی واسط‌های غیرقابل اعتماد، فعال گردد.

نحوه پیاده‌سازی:

۱- مشخص شود که هرگاه حمله‌ای تشخیص داده شد چه رفتاری صورت بگیرد. Drop (Packet از بین برود) Reset (Packet از بین برود و ارتباط ریست شود).
۲- دستور زیر رفتار مقتضی هنگام مواجهه با حمله را مشخص می‌کند.

```
hostname(config)# ip audit name <audit_name> attack action alarm <prevention_action>
```

۳- مشخص کردن واسط‌های غیر قابل اعتماد
۴- دستور زیر را برای فعال کردن جلوگیری از نفوذ روی واسط‌های غیرقابل اعتماد، اجرا کنید:

```
hostname(config)# ip audit interface <interface_name> <audit_name>
```

SCFI-3: حصول اطمینان از محدود بودن "packet fragments" روی واسط‌های غیرقابل اعتماد

شرح اجمالی:

دستگاه برای جلوگیری از ورود بسته‌های خرد بر روی واسط‌های غیرقابل اعتماد، تنظیم شود.

نحوه پیاده‌سازی:

۱- تهیه اسم واسط‌های غیرقابل اعتماد
۲- دستور زیر را برای جلوگیری از ورود بسته‌های خرد، اجرا کنید:

```
hostname(config)#fragment chain 1 <interface_name>
```

SCFI-4: حصول اطمینان از پیکربندی صحیح بازرسی برنامه‌های غیر-پیش‌فرض

شرح اجمالی:

قابلیت بررسی یک برنامه که در سیاست عمومی پیش‌فرض بررسی برنامه قرار ندارد، فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را برای فعال کردن بررسی پروتکل، اجرا کنید:

```
hostname(config)# policy-map global_policy
hostname(config-pmap) # class inspection_default
hostname(config-pmap-c) # inspect <protocol_name>
hostname(config-pmap-c) # exit
hostname(config-pmap) # exit
hostname(config)#service-policy global_policy global
```

SCFI-5: حصول اطمینان از فعال بودن محافظت در برابر DOS برا واسطهای غیرقابل اعتماد

شرح اجمالی:

قابلیت تشخیص بیشترین کانکشن‌ها ، بیشترین کانکشن‌های اولیه، بیشترین کانکشن‌ها از طرف یک کلاینت، بیشترین کانکشن‌های اولیه از یک کلاینت بر روی اینترفیس بیرونی، مشخص گردد.

نحوه پیاده‌سازی:

۱- تهیه یک مقدار استاندارد برای بیشترین کانکشن‌ها، بیشترین کانکشن‌های اولیه، بیشترین کانکشن‌های از طرف یک کلاینت و بیشترین کانکشن های اولیه از سمت یک کلاینت.

۲- دستور زیر را برای پیکربندی کلاسی که ترافیک حملات DOS را تشخیص دهد، اجرا کنید:

```
hostname(config)# class-map <class_name>
hostname(config-cmap)# match any
```

۳- پیکربندی سیاستی که تعداد بیشترین کانکشن‌ها را مشخص نماید و بر روی ترافیک پیکربندی شده در بالا اعمال گردد.

```
hostname(config)# policy-map <policy_name>
hostname(config-pmap) # class <class_name>
hostname(config-pmap-c) # set connection conn-max <enterprise_max_number>
hostname(config-pmap-c) # set connection embryonic-conn-max <enterprise_max_number>
hostname(config-pmap-c) # set connection per-client-embryonic-max
<enterprise_max_number>
hostname(config-pmap-c)# set connection per-client-max <enterprise_max_number>
```

پارامتر enterprise_max_number باید مقداری بین ۰ و ۶۵۵۳۵ داشته باشد.

۴- دستور زیر را برای این که سیاست پیکربندی شده در بالا بر روی اینترفیس‌های غیرقابل اعتماد اعمال گردد، اجرا کنید:

```
hostname(config-pmap-c)# service-policy <policy_name> interface
<untrusted_interface_name>
```

SCFI-6: حصول اطمینان از تنظیم "threat-detection statistics" به "tcp-intercept"

شرح اجمالی:

آمارهای تشخیص تهدید برای بلاک کردن حملات بوسیله tcp-intercept، فعال گردد.

نحوه پیاده‌سازی:

دستور زیر را برای فعال کردن آمارهای تشخیص تهدید برای tcp-intercept، اجرا کنید:

```
hostname(config)# threat-detection statistics tcp-intercept
```

SCFI-7: حصول اطمینان از تنظیم "ip verify" به "reverse-path" برای واسط‌های غیرقابل اعتماد

شرح اجمالی:

ارسال unicast Reverse-Path (uRPF) روی اینترفیس‌های غیر قابل اعتماد، فعال گردد.

نحوه پیاده‌سازی:

۱- تهیه اسم اینترفیس‌های غیر قابل اعتماد

۲- دستور زیر را به منظور فعال‌سازی محافظت در برابر جعل IP، اجرا کنید:

```
hostname(config)# ip verify reverse-path interface <interface_name>
```

SCFI-8: حصول اطمینان از تنظیم "security-level" به "0" برای واسط‌های متصل به اینترنت

شرح اجمالی:

بر روی اینترفیس‌های متصل به اینترنت Security Level بر روی صفر تنظیم شود.

نحوه پیاده‌سازی:

۱- تهیه اسم اینترفیس‌هایی که به اینترنت متصل شده می‌باشد.

۲- دستور زیر را برای تنظیم Security Level به مقدار صفر روی اینترفیس‌های مربوطه، اجرا کنید:

```
hostname(config)#interface <interface_physical_name>
hostname(config-if)#security-level 0
```

SCFI-9: حصول اطمینان از فعال بودن محافظت در برابر بات‌نت روی واسط‌های غیرقابل اعتماد

شرح اجمالی:

فیلتر کردن ترافیک بات‌نت روی اینترفیس‌های غیرقابل اعتماد.

نحوه پیاده‌سازی:

۱- دستور زیر را برای اطمینان از دسترس بودن DNS Server، اجرا کنید:

```
hostname#sh run | i name-server
```

۲- دستور زیر را برای دانلود لیستی از وب سایت‌های بدافزار و استفاده دستگاه از آن برای بررسی، اجرا کنید:

```
hostname(config)#dynamic-filter updater-client enable
hostname(config)#dynamic-filter use-database
```

۳- دستور زیر را جهت ایجاد Class Map برای دستگاه امنیتی، برای همخوانی ترافیک DNS، اجرا کنید:

```
hostname(config)#class-map <dns_class_map_name>
hostname(config-cmap)# match port udp eq domain
```

۴- اجرای دستور زیر Policy-Map ای میسازد که بوسیله آن ASA ترافیک همخوانی داشته با DNS را بررسی میکند تا اسامی دامین موجود در ترافیک DNS را با لیست وبسایت‌های بدرفتار مقایسه نماید.

```
hostname(config)#policy-map <dns_policy_map_name>
hostname(config-pmap) # class <dns_class_map_name>
hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
```

۵- برای اعمال بررسی بر روی اینترفیس مورد نظر دستور زیر را اجرا کنید:

```
hostname(config)# service-policy <dns_policy_map_name> interface
<untrusted_interface_name>
```

۶- دستور زیر را برای مانیتور کردن ترافیک باتنتها بر روی اینترفیس‌های غیرقابل اعتماد، اجرا کنید:

```
hostname(config)# dynamic-filter enable interface <untrusted_interface_name>
```

۷- دستور زیر را برای بلاک کردن کلیه ترافیک‌هایی که باتنت تشخیص داده شود، اجرا کنید:

```
hostname(config)# dynamic-filter drop blacklist interface <untrusted_interface_name>
```

SCFI-10: حصول اطمینان از فعال بودن فیلترینگ ActiveX

شرح اجمالی:

کنترل‌های ActiveX از ترافیکی که مربوط به پاسخ‌های HTTP است، از دستگاه امنیتی حذف گردد.

نحوه پیاده‌سازی:

۱- تهیه پورت‌های TCP مربوط به ترافیک HTTP که شامل ActiveX objects، IP و Mask کاربرهای داخلی که ترافیک HTTP را تولید کرده‌اند، IP و Mask سرورهای خارجی، تا کاربرهای داخلی که به آنها وصل شده‌اند و منبع ActiveX objects، مشخص گردند.

۲- دستور زیر را برای فیلتر کردن اپلت‌های ActiveX objects، اجرا کنید:

```
hostname(config)# filter activex <port> <internal_users_ip> <internal_users_mask>
<external_servers_ip> <external_servers_mask>
```

SCFI-11: حصول اطمینان از فعال بودن فیلترینگ اپلت‌های جاوا

شرح اجمالی:

برداشتن اپلت‌های جاوا از ترافیک پاسخ های HTTP که از ASA عبور می‌کند.

نحوه پیاده‌سازی:

۱- تهیه پورت های مربوط به ترافیک HTTP که شامل جاوا، IP و Mask کاربرهای داخلی که ترافیک HTTP را تولید کرده‌اند، IP و Mask سرورهای خارجی، تا کاربرهای داخلی که به آنها وصل شده‌اند و منبع جاوا، مشخص گردند.

۲- دستور زیر را برای فیلتر کردن اپلت‌های جاوا، اجرا کنید:

```
hostname(config)# filter java <port> <internal_users_ip> <internal_users_mask>
<external_servers_ip> <external_servers_mask>
```

SCFI-12: حصولاطمینان از پیکربندی صحیح رد صریح در لیست‌های دسترسی

شرح اجمالی:

از این که هر لیست دسترسی شامل جمله رد واضح باشد، تضمین شود.

نحوه پیاده‌سازی:

۱- تهیه اسم لیست دسترسی

۲- دستور زیر را برای پیکربندی رد صریح، اجرا کنید:

```
hostname(config)#<access-list_name> extended deny ip any any log
```

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 تنظیمات	مقدار پیش‌فرض	مقدار مطلوب
SCFI-1		مدیریت پسورد			
SCFI-1-1		حصول اطمینان از تنظیم "رمزعبور ورود"		رمزعبور پیش‌فرض "رمزعبور ورود" cisco می‌باشد.	
SCFI-1-2		حصول اطمینان از تنظیم "رمزعبور فعال"		به صورت پیش‌فرض "رمزعبور فعال" خالی می‌باشد.	
SCFI-1-3		حصول اطمینان از تنظیم "عبارت‌عبور کلید اصلی"		-	-
SCFI-1-4		حصول اطمینان از غیرفعال بودن "بازیابی رمزعبور"		به صورت پیش‌فرض "بازیابی رمزعبور" فعال می‌باشد.	
SCFI-1-5		حصول اطمینان از فعال بودن "خط‌مشی رمزعبور"		بصورت پیش‌فرض خط‌مشی رمزعبور غیرفعال می‌باشد. مقادیر زیر به صورت پیش فرض می‌باشد. مدت اعتبار: ۰ حداقل تغییرات: ۰ حداقل طول: ۳ حداقل حروف بزرگ: ۰ حداقل حروف کوچک: ۰ حداقل تعداد اعداد: ۰ حداقل حروف خاص: ۰	

SCFI-2		مدیریت دستگاه			
SCFI-2-1		حصول اطمینان از تنظیم "نام دامنه"		-	-
SCFI-2-2		حصول اطمینان از تنظیم "نام دامنه"		مقدار پیش‌فرض وابسته به پلت‌فرم است ولی به صورت معمول ciscoasa می‌باشد.	
SCFI-2-3		حصول اطمینان از فعال بودن "عدم‌موفقیت"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-2-4		حصول اطمینان از غیرفعال کردن درگاه[۱۰] های بدون استفاده		-	-
SCFI-3		امنیت تصویر			
SCFI-3-1		حصول اطمینان از صحیح بودن "جامعیت تصویر"		-	-
SCFI-3-2		حصول اطمینان از صحیح بودن "صحت تصویر"		ندارد	
SCFI-4		احراز هویت، میزان دسترسی و حسابرسی			
SCFI-4-1		قوانین AAA محلی		-	-
SCFI-4-1-1		حصول اطمینان از تنظیم حداکثر تعداد احراز هویت محلی AAA به کمتر یا مساوی ۳		aaa local authentication max login attempts به‌صورت پیش‌فرض غیرفعال است.	
SCFI-4-1-2		حصول اطمینان از تنظیم نام کاربری و پسورد محلی		مقدار نام کاربری پیش‌فرض استفاده شده برای اولین ارتباط SSH یا aaa authentication telnet console مقدار asa می‌باشد ولی برای ورژن‌های بالاتر از 8.4(2) مقدار پیش‌فرض برای نام کاربری وجود ندارد.	
SCFI-4-1-3		حصول اطمینان از وجود نداشتن اکانت‌های پیش‌فرض شناخته شده		مقدار نام کاربری پیش‌فرض استفاده شده برای اولین ارتباط SSH یا aaa authentication telnet console مقدار asa می‌باشد	

[۱۰] interface

				ولی برای ورژن‌های بالاتر از 8.4(2) مقدار پیش‌فرض برای نام کاربری وجود ندارد.	
SCFI-4-2		سرورهای AAA راه‌دور			
SCFI-4-2-1		حصول اطمینان از تنظیم صحیح "TACACS+/RADIUS"		پیکربندی سرور AAA به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-3		احرازهویت AAA			
SCFI-4-3-1		حصول اطمینان از تنظیم صحیح " aaa authentication enable console"		احرازهویت AAA به‌صورت پیش‌فرض برای " enable mode" غیرفعال است.	
SCFI-4-3-2		حصول اطمینان از تنظیم صحیح " aaa authentication http console"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-3-3		حصول اطمینان از تنظیم صحیح "aaa authentication secure-http-client"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-3-4		حصول اطمینان از تنظیم صحیح " aaa authentication serial console"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-3-5		حصول اطمینان از تنظیم صحیح " aaa authentication ssh console"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-3-6		حصول اطمینان از تنظیم صحیح " aaa authentication telnet console"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-4		کنترل دسترسی AAA			
SCFI-4-4-1		حصول اطمینان از تنظیم صحیح "aaa command authorization"		-	-
SCFI-4-4-2		حصول اطمینان از تنظیم صحیح "aaa authorization exec"		فعال نمی‌باشد.	
SCFI-4-5		حسابرسی AAA			

SCFI-4-5-1		حصول اطمینان از تنظیم صحیح "aaa command accounting"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-5-2		حصول اطمینان از تنظیم صحیح "aaa accounting for SSH"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-5-3		حصول اطمینان از تنظیم صحیح "aaa accounting for Serial console"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-4-5-4		حصول اطمینان از تنظیم صحیح "aaa accounting for EXEC mode"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-5		قوانین بنر			
SCFI-5-1		حصول اطمینان از تنظیم "ASDM banner"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-5-2		حصول اطمینان از تنظیم "EXEC banner"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-5-3		حصول اطمینان از تنظیم "LOGIN banner"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-5-4		حصول اطمینان از تنظیم "MOTD banner"		به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-6		قوانین SSH			
SCFI-6-1		حصول اطمینان از تنظیم "SSH source restriction" برای آدرس IP مجاز		-	-
SCFI-6-2		حصول اطمینان از فعال بودن "SSH version 2"		به صورت پیش فرض دستگاه امنیت اجازه SSH ورژن ۱ و ۲ را می‌دهد.	
SCFI-6-3		حصول اطمینان از بزرگتر یا مساوی بودن "RSA key pair" از ۲۰۴۸ بیت		-	-
SCFI-6-4		حصول اطمینانت از تنظیم فعال بودن "SCP protocol" برای ارسال فایل		-	-
SCFI-6-5		حصول اطمینان از غیرفعال بودن Telnet		-	-
SCFI-7		قوانین HTTP			

SCFI-7-1		حصول اطمینان از تنظیم "HTTP source restriction" برای آدرس IP مجاز		-	-
SCFI-7-2		حصول اطمینان از تنظیم "TLS 1.0" برای دسترسی HTTPS		-	-
SCFI-7-3		حصول اطمینان از تنظیم "SSL AES 256 encryption" برای دسترسی HTTPS		-	-
SCFI-8		Session timeout			
SCFI-8-1		حصول اطمینان از تنظیم "console session timeout" به کمتر یا مساوی ۵ دقیقه		به‌صورت پیش‌فرض Time out دارای مقدار ۰ می‌باشد. به این معنی که نشست کنسول پایان نمی‌یابد.	
SCFI-8-2		حصول اطمینان از تنظیم "SSH session timeout" به کمتر یا مساوی ۵ دقیقه		مقدار پیش‌فرض پایان نشست مقدار ۵ دقیقه می‌باشد.	
SCFI-8-3		حصول اطمینان از تنظیم "HTTP session timeout" به کمتر یا مساوی ۵ دقیقه		مقدار پیش‌فرض پایان نشست مقدار ۲۰ دقیقه می‌باشد.	
SCFI-9		قوانین ساعت			
SCFI-9-1		قوانین NTP		-	-
SCFI-9-1-1		حصول اطمینان از فعال بودن "NTP authentication"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-9-1-2		حصول اطمینان از تنظیم صحیح "NTP authentication key"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-9-1-3		حصول اطمینان از وجود "trusted NTP server"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-9-2		حصول اطمینان از تنظیم صحیح "local timezone"		به‌صورت پیش‌فرض time zone برابر با UTC می‌باشد.	
SCFI-10		قوانین ثبت وقایع			
SCFI-10-1		حصول اطمینان از فعال بودن ثبت وقایع		-	-
SCFI-10-2		حصول اطمینان از غیرفعال بودن نمایش لاگ بر روی کنسول		به‌صورت پیش‌فرض غیرفعال می‌باشد.	

SCFI-10-3		حصول اطمینان از غیرفعال بودن نمایش لاگ بر روی مانیتور		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-10-4		حصول اطمینان از پیکربندی صحیح syslog host		قابلیت Syslog Server به‌صورت پیش‌فرض پیکربندی نشده است.	
SCFI-10-5		حصول اطمینان از ثبت وقایع بر اساس ID دستگاه		-	-
SCFI-10-6		حصول اطمینان از تنظیم سطح حساسیت تاریخچه ثبت وقایع به مساوی یا بالاتر از ۵		دستگاه به‌صورت پیش‌فرض رخدادی به سمت سرور SNMP نمی‌فرستد.	
SCFI-10-7		حصول اطمینان از فعال بودن ثبت وقایع همراه با Timestamp		به‌صورت پیش‌فرض پیام‌های Syslog شامل Timestamp نمی‌باشد.	
SCFI-10-8		حصول اطمینان از تنظیم امکان Syslog Logging به ۲۳		مقدار پیش فرض Facility در ثبت رخدادها برابر با ۲۰ می‌باشد.	
SCWF-10-9		حصول اطمینان از تنظیم اندازه بافر ثبت وقایع به مساوی یا بزرگتر از 512 Kb		مقدار پیش فرض 4kb می‌باشد.	
SCFI-10-10		حصول اطمینان از تنظیم سطح حساسیت رخدادهای ذخیره شده در بافر به مساوی یا بزرگتر از ۳		-	-
SCFI-10-11		حصول اطمینان از تنظیم سطح حساسیت Logging Trap به مساوی یا بزرگتر از ۵		-	-
SCFI-10-12		حصول اطمینان از تنظیم بودن ارسال ایمیل ثبت وقایع برای Critical تا Emergency		-	-
SCFI-11		قوانین SNMP			
SCFI-11-1		حصول اطمینان از تنظیم "SNMP-Server Group" به "v3 priv"		-	-
SCFI-11-2		حصول اطمینان از تنظیم "snmp-server user" به "v3 auth SHA"		-	-

SCFI-11-3		حصول اطمینان ازتنظیم "snmp-server host" به "version 3"		-	-
SCFI-11-4		حصول اطمینان از فعال بودن SNMP Traps		به‌صورت پیش‌فرض فقط Syslog Traps فعال می‌باشد.	
SCFI-11-5		حصول اطمینان از تنظیم نبودن رشته پیش فرض برای "SNMP community string"		مقدار پیش‌فرض community String برابر با public می‌باشد.	
SCFI-1		احرازهویت پروتکل‌های مسیریابی			
SCFI-1-1		حصول اطمینان از فعال بودن احرازهویت پروتکل RIP		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-1-2		حصول اطمینان از فعال بودن احرازهویت پروتکل OSPF		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-1-3		حصول اطمینان از فعال بودن احرازهویت پروتکل EIGRP		به‌صورت پیش فرض غیرفعال می‌باشد.	
SCFI-2		حصول اطمینان از فعال بودن "noproxyarp" روی واسط‌های غیرقابل اعتماد		Proxy-ARP به صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-3		حصول اطمینان از فعال بودن "DNS Guard"		این قابلیت برای نرم‌افزار مربوطه غیرفعال می‌باشد.	
SCFI-4		حصول اطمینان از غیرفعال بودن سرویس‌های DHCP برای واسط‌های غیرقابل		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-5		حصول اطمینان از محدود بودن ICMPبرای واسط‌های غیرقابل اعتماد		ICMP به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-1		حصول اطمینان از پیکربندی صحیح سرویس DNS			
SCFI-2		حصول اطمینان فعال بودن جلوگیری از نفوذ در واسط‌های غیرقابل اعتماد		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-3		حصول اطمینان از محدود بودن "packet fragments" روی واسط‌های غیرقابل اعتماد		برای Fragment Chain مقدار پیش فرض ۲۴ میباشد.	

SCFI-4		حصول اطمینان از پیکربندی صحیح بازرسی برنامه‌های غیر-پیش‌فرض		به‌صورت پیش‌فرض خط‌مشی پیکربندی شامل دستورات زیر برای بررسی برنامه‌ها می‌باشد. class-map inspection_default match default-inspection-traffic policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect ip-options inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp service-policy global_policy global	
SCFI-5		حصول اطمینان از فعال بودن محافظت در برابر DOS برا واسط‌های غیرقابل اعتماد		بیشترین مقدار پیش فرض ۰ می‌باشد به این معنی که محدودیتی وجود ندارد.	
SCFI-6		حصول اطمینان از تنظیم "threat-detection statistics" به "tcp-intercept"		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-7		حصول اطمینان از تنظیم " ip verify" به "reverse-path" برای واسط‌های غیرقابل اعتماد		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-8		حصول اطمینان از تنظیم "security-level" به "0" برای واسط‌های متصل به اینترنت		به‌صورت پیش‌فرض Security Level تنظیم نشده است.	

SCFI-9		حصول اطمینان از فعال بودن محافظت در برابر بات‌نت روی واسط‌های غیرقابل اعتماد		به‌صورت پیش‌فرض غیرفعال می‌باشد.	
SCFI-10		حصول اطمینان از فعال بودن فیلترینگ ActiveX		به صورت پیش‌فرض ActiveX control filtering غیرفعال می‌باشد.	
SCFI-11		حصول اطمینان از فعال بودن فیلترینگ اپلت‌های جاوا		به صورت پیش‌فرض Java applet filtering غیرفعال می‌باشد.	
SCFI-12		حصولاطمینان از پیکربندی صحیح رد صریح در لیست‌های دسترسی		به صورت پیش‌فرض غیرفعال می‌باشد.	