به نام خدا

پیکربندی امن

Cisco Firewall Internet Edge

مرکز مدیریت راهبردی افتا

SCFI-Cisco Firewall Internet Edge – v1.0

فروردین ۹۶

نسخه ۱,۰

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 Internet Edge 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 Internet Edge 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:

SCFI-1: مسیریابی

شرح اجمالی:

پیکربندی مسیریاب روی یک دیواره‌آتش مرزی اینترنت باید به گونه‌ای صورت گیرد که از دست‌کاری کردن ترافیک شبکه و محرومیت از سرویس، جلوگیری کند.

SCFI-1-1: نیاز به مسیریابی‌های ایستا برای دروازه گام بعد اینترنت (سطح۱، قابل شمارش)

شرح اجمالی:

یک مسیریابی ایستا باید بین دیواره‌آتش و دروازه اینترنت گام بعد، به منظور تسهیل در پیکربندی و جلوگیری از دست‌کاری مسیر اینترنت، پیکربندی شود.

نحوه پیاده‌سازی:

برای مسیریابی کردن پیش‌فرض از سمت دیواره‌آتش به مسیریاب دروازه گام بعد اینترنت، کد زیر را پیکربندی کنید:

```
hostname(config)#route if_name dest_ip mask gateway_ip [distance]
```

SCFI-1-2: جلوگیری از اعلان‌های پروتکل روتینگ در اینترفیس‌های عمومی (سطح۱، قابل شمارش)

اعلان‌های پروتکل مسیریابی بر روی فایروال لبه اینترنت باید غیرفعال باشد تا از حمله روی خود فرآیند مسیریابی جلوگیری کند.

SCFI-1-2-1: پروتکل OSPF (سطح۱، قابل شمارش)

نحوه پیاده‌سازی:

ناحیه‌های OSPF را با استفاده از کد زیر پیکربندی کنید، این نواحی آدرس‌های شبکه برای اتصالات اینترنت را در بر نمی‌گیرد.

```
hostname(config)#router ospf process_id
hostname(config-router)#area area-id range ip-address mask [advertise | not-advertise ]
```

SCFI-1-2-2: پروتکل RIP (سطح۱، قابل شمارش)

نحوه پیاده‌سازی:

پیکربندی RIP موجب می‌شود اینترفیس‌های که برای اتصال به اینترفیس عمومی استفاده می‌شوند به حالت منفعل درآیند و اعلان مسیریابی‌ها را انجام ندهند.

```
hostname(config)#router rip as-num
hostname(config-router) #network network_address
hostname(config-router)#passive-interface [default | if_name]
```

SCFI-1-2-3: پروتکل EIGRP (سطح۱، قابل شمارش)

نحوه پیاده‌سازی:

پیکربندی EIGRP موجب می‌شود اینترفیس‌های که برای اتصال به اینترفیس عمومی استفاده می‌شوند به حالت منفعل درآیند و اعلان مسیریابی‌ها را انجام ندهند.

```
hostname(config)#router eigrp as-num
hostname(config-router) #network network_address
hostname(config-router)#passive-interface [default | if_name]
```

SCFI-1-3: توزیع مجدد مسیر پیش‌فرض ایستا به پروتکل‌های مسیریابی داخلی (سطح۱، قابل شمارش)

شرح اجمالی:

بررسی شود که پیکربندی احرازهویت، مجوزدهی و حساب کاربری (AAA) از سرورها و پروتکل‌های مورد نیاز استفاده نماید.

نحوه پیاده‌سازی:

پروتکل‌های امنیتی طراحی‌شده، سرور، کلید و زمان اتمام که برای کاربران احرازهویت شده استفاده می‌شود، را با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#aaa-server {server-tag} protocol {Kerberos | ldap | nt | radius | sdi |tacacs+}
hostname(config)#aaa-server {server-tag} host {aaa_server-ip} [key] [timeout seconds]
```

SCFI-1-4: نیاز به احرازهویت پروتکل مسیریابی برای مسیریابی داخلی

پروتکل‌های مسیریابی باید برای استفاده از احرازهویت به منظور جلوگیری از دست‌کاری بدون احرازهویت شده، پیکربندی شوند. اگر دیواره‌آتش برای تزریق مسیرها به جدول مسیریابی استفاده می‌شود، باید از احرازهویت استفاده نماید.

SCFI-1-4-1: نیاز به احرازهویت EIGRP برای مسیرهای داخلی (سطح۱، قابل شمارش)

شرح اجمالی:

بررسی شود که اگر از روتینگ پروتکل EIGRP استفاده می‌شود، در جایی که امکان دارد، احرازهویت EIGRP فعال گردد.

نحوه پیاده‌سازی:

قابلیت احرازهویت همسایه را برای EIGRP، در جایی که این امکان وجود دارد، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#interface <interface_name>
hostname(config-if) #authentication mode eigrp as-num md5
hostname(config-if)#authentication key eigrp as-num key key-id key-id
```

SCFI-1-4-2: نیاز به احرازهویت OSPF برای مسیرهای داخلی (سطح۱، قابل شمارش)

شرح اجمالی:

بررسی شود در جایی که امکان احرازهویت OSPF وجود دارد، احرازهویت OSPF فعال گردد.

نحوه پیاده‌سازی:

قابلیت احرازهویت همسایه را برای OSPF، در جایی که این امکان وجود دارد، با استفاده از کد زیر پیکربندی کنید:

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

یا

```
hostname(config)#interface <interface_name>
hostname(config-if) #ospf authentication [message-digest | null]
hostname(config-if)#ospf message-digest-key key_id md5 key
```

SCWF-1-4-3: نیاز به احرازهویت RIPv2 برای مسیرهای داخلی (سطح۱، قابل شمارش)

شرح اجمالی:

بررسی شود که اگر از روتینگ پروتکل RIPv2 استفاده می‌شود، در جایی که امکان دارد، احرازهویت RIPv2 فعال گردد.

نحوه پیاده‌سازی:

قابلیت احرازهویت همسایه را برای RIPv2، در جایی که این امکان وجود دارد، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#interface <interface_name>
hostname(config-if) #rip authentication mode {text | md5}
hostname(config-if)#rip authentication key key key-id key-id
```

SCFI-2: دسترس‌پذیری

شرح اجمالی:

اتصالات سخت‌افزاری و ISP اضافه معمولا برای محافظت در برابر خرابی‌های سخت‌افزاری و شبکه، مورد استفاده قرار می‌گیرد.

SCFI-2-1: نیاز به کلید عدم‌موفقیت (سطح۱، قابل شمارش)

شرح اجمالی:

کلیدهای عدم‌موفقیت باید برای احرازهویت و رمزنگاری اطلاعات ناموفقی که بین فایروالها مبادله می‌شود، استفاده شوند.

نحوه پیاده‌سازی:

با استفاده از کد زیر کلید عدم‌موفقیت را بر روی هر دو فایروال، پیکربندی کنید:

```
hostname(config)#failover key password
```

SCFI-3: مدیریت

شرح اجمالی:

پروتکل‌های مدیریتی نباید بر روی ارتباطات اینترنتی عمومی فعال باشند. تمامی ارتباطات شبکه‌ای در میان فایروال‌ها باید لاگ شوند.

SCFI-3-1: ممنوع کردن SNMP (سطح۱، قابل شمارش)

شرح اجمالی:

برای جلوگیری از حدس زدن Community String نباید SNMP بر روی اینترفیس عمومی که به اینترنت متصل است فعال گردد.

نحوه پیاده‌سازی:

دسترسی خواندن SNMP به دستگاه را با استفاده از کد زیر، غیرفعال کنید:

```
hostname(config)#clear configure snmp-server
```

SCFI-3-2: ممنوع کردن مدیریت فایروال از طریق اینترفیس های عمومی (سطح۱، قابل شمارش)

شرح اجمالی:

فایروال می‌تواند از طریق telnet، ssh و ssl بوسیله‌ی مدیر دستگاه یکپارچه، مدیریت شود. این ابزارهای مدیریتی نباید بر روی اینترفیس‌های عمومی متصل به اینترنت فعال گردند.

نحوه پیاده‌سازی:

دسترسی مدیریت برای یک شبکه داخلی یا یک اینترفیس مدیریتی اختصاص یافته را، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#management-access <interface_name>
```

SCFI-4: ترجمه آدرس شبکه (NAT)

شرح اجمالی:

برای جلوگیری از دسترسی مستقیم به کاربر داخل شبکه و دستگاه‌های زیرساختی که به صورت عمومی قابل دسترس نیستند، باید NAT پیکربندی گردد.

SCFI-4-1: نیاز به NAT برای دسترسی دستگاه‌های کاربر به اینترنت (سطح۱، قابل شمارش)

شرح اجمالی:

برای دسترسی شبکه داخلی به اینترنت، NAT را پیکربندی کنید.

نحوه پیاده‌سازی:

برای تمام نواحی شبکه داخلی که کاربران نیاز به دسترسی به اینترنت دارند، NAT را با استفاده از کد زیر پیکربندی کنید.

```
hostname(config)#object network <object_name>
hostname(config-network-object)#nat [(real_ifc, mapped_ifc)] dynamic mapped_obj [pat-pool mapped_obj [round-robin]] [interface] [dns]
```

SCFI-5 : قوانین فایروال

شرح اجمالی:

قوانین فایروال باید به شیوه‌ای ساخته شوند که قابلیت اجرای خط‌مشی‌های سازگار و منسجم را داشته باشد. به علاوه، تمامی اتصالاتی که بر اساس خط‌مشی رد می‌شوند، رخدادشان باید ثبت گردد تا برای تجزیه‌وتحلیل تلاش‌های نفوذ، مورد استفاده قرار گیرند.

SCFI-5-1: نیاز به اشیاء شبکه برای ساخت قانون (سطح۱، قابل شمارش)

شرح اجمالی:

اشیاء شبکه را برای اعمال خط‌مشی یکسان به یک هاست یا شبکه یا بازه‌ای از آدرس‌ها، پیکربندی کنید.

نحوه پیاده‌سازی:

اشیاء شبکه را برای ایجاد قانون فایروال، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object network <object_name>
hostname(config-network-object)# {host ip_addr | subnet net_addr net_mask | range ip_addr_1
ip_addr_2}
```

SCFI-5-2: نیاز به اشیاء سرویس برای ساخت قانون (سطح۱، قابل شمارش)

شرح اجمالی:

اشیاء سرویس را برای پروتکل‌ها و پورت‌هایی که در ساخت قوانین استفاده خواهند شد، پیکربندی کنید.

نحوه پیاده‌سازی:

اشیاء سرویس را برای ایجاد قانون فایروال، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object network <object_name>
hostname(config-network-object)#service {protocol | icmp icmp-type |  icmp6 icmp6-type |
{tcp | udp} [source operator port] [destination operator port]}
```

SCFI-5-3: نیاز به گروه‌های شیء شبکه برای ساخت قانون (سطح۱، قابل شمارش)

شرح اجمالی:

گروه‌های شیء شبکه ساختارهای خط‌مشی ادغام شده‌ای می‌سازند که بوسیله ادغام اشیاء شبکه به یک گروه منطقی از دستگاه‌ها و شبکه‌ها، کار ساخت قوانین را آسان می‌نماید.

نحوه پیاده‌سازی:

گروه‌های شیء شبکه را برای بازه‌ای از آدرس‌ها و هاست‌ها، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object-group network grp_id
hostname(config-network)#network-object {object_name | host ip_address | ip_address mask}
```

SCFI-5-4: نیاز به توضیحات گروه شیء شبکه (سطح۱، قابل شمارش)

شرح اجمالی:

توضیحات را برای گروه‌های اشیاء به منظور کمک در عیب‌یابی و بررسی هدف قوانین، پیکربندی کنید.

نحوه پیاده‌سازی:

توضیحات گروه‌های شیء را با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object-group network grp_id
hostname(config-network)#description text
```

SCFI-5-5: نیاز به گروه‌های شیء سرویس برای ساخت قانون (سطح۱، قابل شمارش)

شرح اجمالی:

گروه‌های شیء شبکه ساختارهای خط‌مشی ادغام شده‌ای می‌سازند که بوسیله ادغام اشیاء شبکه به یک گروه منطقی از پورت‌ها و پروتکل‌ها، کار ساخت قوانین را آسان می‌نماید.

نحوه پیاده‌سازی:

گروه‌های شیء سرویس را با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object-group service I {tcp | udp | tcp-udp}
hostname(config-service)#port-object {eq port | range begin_port end_port}
```

SCFI-5-6: نیاز به توضیحات گروه شیء سرویس (سطح۱، قابل شمارش)

شرح اجمالی:

توضیحات را برای گروه‌های اشیاء به منظور کمک در عیب‌یابی و بررسی هدف قوانین، پیکربندی کنید.

نحوه پیاده‌سازی:

توضیحات گروه‌های شیء را با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#object-group service grp_id {tcp | udp | tcp-udp}
hostname(config-service)#description text
```

SCFI-5-7: نیاز به ثبت وقایع برای قانون پیش‌فرض ردکردن (سطح۱، قابل شمارش)

شرح اجمالی:

ترافیک‌هایی که بر اساس قوانین فایروال رد شده‌اند باید به منظور بایگانی برای استفاده‌های نادرست بالقوه رخدادهایشان ثبت شود.

نحوه پیاده‌سازی:

تمامی ورودی‌های پیش‌فرض ردشده را همراه با کلمه کلیدی رخداد روی اجزای اینترنت، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#access-list access_list_name deny ip any any [log [[level] [interval secs] |
disable | default]]
```

SCFI-6: کشف تهدیدات

تکنولوژی‌های کشف تهدیدات باید به منظور بلاک کردن ترافیک و آدرس‌های شبکه بدخواه شناخته‌شده، پیکربندی گردد.

SCFI-6-1: نیاز به فیلتر کردن ترافیک بات‌نت (سطح۲، قابل شمارش)

شرح اجمالی:

فیلتر ترافیک بات‌نت، پایگاه‌داده‌ای است که به صورت پویا آپدیت می‌شود و سایت‌های بدخواه شناخته‌شده را لیست می‌کند و مانع از اتصال شبکه کلاینت‌ها به این بخش‌ها از اینترنت می‌شود.

SCFI-6-1-1: نیاز به آپدیت‌های فیلتر پویا (سطح۲، قابل شمارش)

شرح اجمالی:

آپدیت فیلتر پویا را پیکربندی و فایروال را برای استفاده از پایگاه‌داده حاوی لیست سایت‌های بدخواه شناخته‌شده جدید، تنظیم کنید.

نحوه پیاده‌سازی:

فایروال را برای آپدیت و استفاده از دیتابیس بات‌نت، با استفاده از کد زیر پیکربندی کنید:

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

SCFI-6-1-2: نیاز به DNS Snooping (سطح۲، قابل شمارش)

شرح اجمالی:

DNS Snooping برای شناسایی ارسال درخواست‌های دستگاه به سمت سرورها و سایت‌های بدخواه، استفاده می‌شود.

نحوه پیاده‌سازی:

DHCP Snooping و به کارگیری آن در اینترفیس‌های داخلی را با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#class-map name
hostname(config-cmap) #match port udp eq domain
hostname(config)#policy-map name
hostname(config-pmap) #class name
hostname(config-pmap-c) #inspect dns [map_name] dynamic-filter-snoop
hostname(config)#service-policy policymap_name interface interface_name
```

SCFI-6-1-3: نیاز به فیلتر ترافیک باتنت (سطح۲، قابل شمارش)

شرح اجمالی:

اشیاء سرویس برای پروتکل‌ها و پورت‌هایی که در ساخت قانون استفاده می‌شوند، را پیکربندی کنید.

نحوه پیاده‌سازی:

اشیاء سرویس را برای ساخت قانون فایروال، با استفاده از کد زیر پیکربندی کنید:

```
hostname(config)#access-list access_list_name extended {deny | permit} protocol
source_address mask [operator port] dest_address mask [operator port]
hostname(config)#dynamic-filter enable [interface name] [classify-list access_list]
hostname(config)#dynamic-filter drop blacklist [interface name] [action classify-list
subset_access_list] [threat-level {eq level | range min max}]
 hostname(config)#dynamic-filter ambiguous-is-black
```

پیوست

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCFI-1		مسیریابی			
SCFI-1-1		نیاز به مسیریابی‌های ایستا برای دروازه گام بعد اینترنت (سطح۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-1-2		جلوگیری از اعلان‌های پروتکل روتینگ در اینترفیس‌های عمومی (سطح۱، قابل شمارش)		-	-
SCFI-1-2-1		پروتکل OSPF (سطح۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-1-2-2		پروتکل RIP (سطح۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCFI-1-2-3		پروتکل EIGRP) سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-1-3		توزیع مجدد مسیر پیش‌فرض ایستا به پروتکل‌های مسیریابی داخلی (سطح ۱، قابل شمارش)		مقدار پیش‌فرض برای aaa-server غیرفعال است.	-
SCFI-1-4		نیاز به احرازهویت پروتکل مسیریابی برای مسیریابی داخلی		-	-
SCFI-1-4-1		نیاز به احرازهویت EIGRP برای مسیرهای داخلی (سطح ۱، قابل شمارش)		به صورت پیش‌فرض احرازهویت EIGRP غیرفعال است.	-
SCFI-1-4-2		نیاز به احرازهویت OSPF برای مسیرهای داخلی (سطح ۱، قابل شمارش)		به صورت پیش‌فرض احرازهویت OSPF غیرفعال است.	-
SCFI-1-4-3		نیاز به احرازهویت RIPv2 برای مسیرهای داخلی (سطح ۱، قابل شمارش)		به صورت پیش‌فرض احرازهویت RIPv2 غیرفعال است.	-
SCFI-2		**دسترس‌پذیری**			
SCFI-2-1		نیاز به کلید عدم‌موفقیت (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-3		**مدیریت**			
SCFI-3-1		ممنوع کردن SNMP) سطح ۱، قابل شمارش)		به‌صورت پیش‌فرض SNMP فعال نمی‌باشد.	-
SCFI-3-2		ممنوع کردن مدیریت فایروال از طریق اینترفیس های عمومی (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-4		**ترجمه آدرس شبکه (NAT)**			

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCFI-4-1		نیاز به NAT برای دسترسی دستگاه‌های کاربر به اینترنت (سطح ۱، قابل شمارش)		به صورت پیش‌فرض NAT غیرفعال است.	-
SCFI-5		قوانین فایروال			
SCFI-5-1		نیاز به اشیاء شبکه برای ساخت قانون (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-2		نیاز به اشیاء سرویس برای ساخت قانون (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-3		نیاز به گروه‌های شیء شبکه برای ساخت قانون (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-4		نیاز به توضیحات گروه شیء شبکه (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-5		نیاز به گروه‌های شیء سرویس برای ساخت قانون (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-6		نیاز به توضیحات گروه شیء سرویس (سطح ۱، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-5-7		نیاز به ثبت وقایع برای قانون پیش‌فرض ردکردن (سطح ۱، قابل شمارش)		به صورت پیش‌فرض ثبت ردکردن همه وقایع، غیرفعال می‌باشد.	-
SCFI-6		کشف تهدیدات			
SCFI-6-1		نیاز به فیلتر کردن ترافیک بات‌نت (سطح ۲، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-6-1-1		نیاز به آپدیت‌های فیلتر پویا (سطح ۲، قابل شمارش)		مقدار پیش‌فرض ندارد.	-

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCFI-6-1-2		نیاز به DNS Snooping (سطح۲، قابل شمارش)		مقدار پیش‌فرض ندارد.	-
SCFI-6-1-3		نیاز به فیلتر ترافیک باتنت (سطح۲، قابل شمارش)		مقدار پیش‌فرض ندارد.	-