پیکربندی امن

Cisco Firewall VPN Services V1.0

مرکز مدیریت راهبردی افتا

SCFI-CISCO- Firewall- VPN Services -V 1.0

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 VPN Service 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 "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 VPN Service 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: دسترسی از راه‌دور IPSEC VPN

شرح اجمالی:

IPSEC تکنولوژی متداولی است که برای فراهم آوردن ارتباطی امن در بستر اینترنت برای انجام کارها از راه‌دور، مورد استفاده قرار می‌گیرد.

SCFI-1-1: ایجاد یک خط‌مشی IKEv1

شرح اجمالی:

ایجاد یک خط‌مشی، که پارامترهایی را برای مذاکره IKE تعریف کند.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی خط‌مشی ISAKMP اجرا کنید:

```
hostname(config)# crypto ikev1 policy priority
```

SCFI-1-1-1: تنظیم نوع احرازهویت IKEv1

شرح اجمالی:

نوع احرازهویت برای تبادل ISAKMP تنظیم شود.

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev1-policy))# authentication {crack | pre-share | rsa-sig}
```

SCFI-1-1-2: تنظیم سطح رمزنگاری IKEv1

شرح اجمالی:

سطح رمزنگاری برای مذاکره IKE را بر الگوریتم AES یا بیشتر (الگوریتم AES با طول کلید بزرگتر یا الگوریتم قوی‌تری) تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev1-policy)# encryption {aes | aes-192 | aes-256}
```

SCFI-1-1-3: تنظیم درهم‌ساز IKEv1 (سطح ۱ ، قابل شمارش)

شرح اجمالی:

الگوریتم درهم‌ساز برای ISAKMP را بر SHA-1 یا بیشتر (الگوریتم SHA با طول درهم‌ساز بزرگتر) تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای تعیین سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev1-policy)# hash sha
```

SCFI-1-1-4: تنظیم گروه دیفی-هلمن برای IKEv1 (سطح ۱ ، قابل شمارش)

شرح اجمالی:

گروه دیفی-هلمن برای تبادل IKEv1 را بر گروه ۲ و یا بیشتر تنظیم کنید.

۱ – بیانگر گروه DH-۷۶۸ bit

۲ - بیانگر گروه DH-۱۰۲۴ bit

۳ - بیانگر گروه DH-۱۵۳۶ bit

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev1-policy)# group {2 | 5}
```

SCFI-1-1-5: تنظیم مدت اعتبار IKEv1 SA (سطح ۱ ، قابل شمارش)

شرح اجمالی:

مدت اعتبار پیوستگی امنیت (SA) برای ISAKMP را روی ۳۶۰۰ ثانیه یا کمتر تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای تعیین مدت اعتبار IKEv1 SA اجرا کنید:

```
hostname(config-ikev1-policy)# lifetime {3600}
```

SCFI-1-1-6: پیکربندی مجموعه تبدیل IKEv1 (سطح۱، قابل شمارش)

شرح اجمالی:

مجموعه تبدیل IKEv1 که از کپسوله‌سازی محموله امنیتی (ESP) با AES یا بیشتر استفاده می‌کند، را تعریف کنید.

نحوه پیاده‌سازی:

کد زیر را برای تنظیم تغییرات اجرا کنید:

```
hostname(config)# crypto ipsec ikev1 transform-set transform-set-name encryption-method
[esp-aes | esp-aes-192 | esp-aes-256]
```

SCFI-1-1-7: پیکربندی واسط IKEv1 (سطح۱، قابل شمارش)

شرح اجمالی:

برای اجرای تبادل ISAKMP واسط دیوارآتش تنظیم شود.

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config)# crypto ikev1 enable interface-name
```

SCFI-1-2: ایجاد یک خط‌مشی IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

ایجاد یک خط‌مشی، که پارامترهایی را برای مذاکره IKE تعریف کند.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی خط‌مشی ISAKMP اجرا کنید:

```
hostname(config)# crypto ikev2 policy priority
```

SCFI-1-2-1: تنظیم نوع احرازهویت IKEv2 (سطح۱،غیر قابل شمارش)

شرح اجمالی:

نوع احرازهویت برای تبادل IKEv2 تنظیم شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev2-policy)# authentication {crack | pre-share | rsa-sig}
```

SCFI-1-2-2: تنظیم سطح رمزنگاری IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

سطح رمزنگاری برای مذاکره IKEv2 را بر AES یا بیشتر تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev2-policy)# encryption {aes | aes-192 | aes-256}
```

SCFI-1-2-3: تنظیم درهم‌ساز IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

الگوریتم درهم‌ساز برای ISAKMP را بر SHA-1 یا بیشتر تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev2-policy)# hash {sha}
```

SCFI-1-2-4: تنظیم گروه دفی-هلمن برای IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

گروه دیفی-هلمن برای تبادل IKEv2 را بر روی گروه ۲ و یا بیشتر تنظیم کنید.

۱ – بیانگر گروه DH-۷۶۸ bit

۲ - بیانگر گروه DH-۱۰۲۴ bit

۳ - بیانگر گروه DH-۱۵۳۶ bit

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config-ikev2-policy)# group {2 | 5}
```

SCFI-1-2-5: تنظیم مدت اعتبار IKEv2 SA (سطح۱، قابل شمارش)

شرح اجمالی:

مدت اعتبار پیوستگی امنیت (SA) برای ISAKMP را روی ۳۶۰۰ ثانیه یا کمتر تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای تعیین مدت اعتبار IKEv2 SA اجرا کنید:

```
hostname(config-ikev2-policy)# lifetime {3600}
```

SCFI-1-2-6: پیکربندی طرح پیشنهادی IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

طرح پیشنهادی IKEv2 را تعریف کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی مجموعه تبدیل اجرا کنید:

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal proposal_name
```

SCFI-1-2-7: پیکربندی رمزنگاری و جامعیت طرح پیشنهادی IKEv2 (سطح۱، قابل شمارش)

شرح اجمالی:

الگوریتم‌های رمزنگاری و جامعیت طرح پیشنهادی IKEv2 که از کپسوله‌سازی محموله امنیتی (ESP) با AES و SHA-1 و یا بزرگتر استفاده می‌کند، را تعریف کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی مجموعه تبدیل اجرا کنید:

```
hostname(config-ipsec=proposal)# protocol {esp} {encryption {aes | aes192 | aes-256 | null} | integrity {sha-1}
```

SCFI-1-2-8: پیکربندی واسط IKEv2 (سطح۱، غیر قابل شمارش)

شرح اجمالی:

برای اجرای تبادل IKEv2 واسط دیوارآتش تنظیم شود.

نحوه پیاده‌سازی:

کد زیر را برای تنظیم سطح رمزنگاری اجرا کنید:

```
hostname(config)# crypto ikev2 enable interface-name
```

SCFI-1-3: تعریف کلید ISAKMP (سطح۱، قابل شمارش)

شرح اجمالی:

کلید از پیش اشتراک گذاشته‌ای که طرفین ارتباط برای احرازهویت یک‌دیگر از آن استفاده کنند، تعریف کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی کلید ISAKMP اجرا کنید:

```
hostname(config)# crypto isakmp key <key_string> <peer_ip_address>
```

SCFI-1-4: تعریف مجموعه تبدیل IPSEC (سطح۱، قابل شمارش)

شرح اجمالی:

مجموعه تبدیل IPSEC را تعریف کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی مجموعه تبدیل اجرا کنید:

```
hostname(config)# crypto ipsec transform-set <transform_set_name> {transform_option}
```

SCFI-1-5: تعریف ACL مطابق (سطح۱، قابل شمارش)

شرح اجمالی:

لیست کنترل دسترس (ACL) که طرح رمز برای تعیین ترافیک تحت محافظت از آن استفاده خواهد کرد، تعریف شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی IP سراسری نظیر رمز اجرا کنید:

```
hostname(config)# ip access-list extended <match_acl_name>
```

```
hostname(config-nacl)# permit ip <source_network> <source_network_mask>
<destination_network>  <destination network_mask>
```

SCFI-1-6: تعریف طرح رمز سراسری (سطح۱، قابل شمارش)

شرح اجمالی:

طرح رمز سراسری تعریف شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی طرح رمز سراسری اجرا کنید:

```
hostname(config)# crypto map <crypto_map_name> <sequence_number> ipsecisakmp
```

SCFI-1-6-1: تعریف IP نظیر برای IPSEC (سطح۱، قابل شمارش)

شرح اجمالی:

طرح رمز سراسری تعریف شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی IP سراسری نظیر رمز اجرا کنید:

```
hostname(config-crypto-map)# set peer <peer_ip_address>
```

SCFI-1-6-2: تعریف مجموعه تبدیل IPSEC (سطح۱، قابل شمارش)

شرح اجمالی:

مجموعه تبدیل تعریف شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی IP سراسری نظیر رمز اجرا کنید:

```
hostname(config-crypto-map)# set transform-set <transform_set_name>
```

SCFI-1-6-3: بکار بردن ACL مطابق برای IPSEC (سطح۱، قابل شمارش)

شرح اجمالی:

لیست کنترل دسترس (ACL) که طرح رمز برای تعیین ترافیک تحت محافظت از آن استفاده خواهد کرد، اعمال شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی IP سراسری نظیر رمز اجرا کنید:

```
hostname(config-crypto-map)# match address <match_acl_name>
```

SCFI-1-7: بکاربردن طرح رمز بر روی واسط (سطح۱، قابل شمارش)

شرح اجمالی:

واسط مناسب برای فعال کردن محافظت IPSEC روی آن، پیکربندی شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی IP سراسری نظیر رمز اجرا کنید:

```
hostname(config-if)# crypto map <crypto_map_name>
```

SCFI-2: دسترسی از راه‌دور SSL VPN (سطح ۱ و ۲، قابل شمارش)

شرح اجمالی:

SSL یک تکنولوژی VPN است که عموماً برای تامین امنیت ارتباطات مربوط به انجام راه‌دور کارها بر روی بستر اینترنت عمومی، استفاده می شود.

SCFI-2-1: نیاز به گواهی معتبر (سطح ۱، غیر قابل شمارش)

شرح اجمالی:

یک گواهی معتبر و مورد اعتماد، برای تشخیص هویت نقطه انتهایی SSL به کار می‌رود.

نحوه پیاده‌سازی:

پیکربندی یک گواهی فرآیندی چند مرحله‌ای است که بستگی به شخص‌ثالث ارائه‌دهنده گواهی دارد. برای اطلاعات بیشتر باید به مستندات پیکربندی دستگاه مراجعه شود.

SCFI-2-2: نیاز به آخرین Anyconnect نرم‌افزار مشتری (سطح ۱ ،غیر قابل شمارش)

شرح اجمالی:

آخرین نسخه Anyconnect نرم‌افزار مشتری باید بر روی ASA نصب شود و بر روی کامپیوترهای مشتری توسعه داده شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی تصویر Anyconnect پس از نصب بر روی حافظه فلش اجرا کنید:

```
hostname(config-webvpn)#anyconnect image <latest_image_pkg> 1
```

SCFI-2-3: نیاز به تعیین مدت زمان بیکاربودن SSL VPN(سطح ۱ ، قابل شمارش)

شرح اجمالی:

برای نشست‌های SSL VPN مدت زمان بیکاربودن را پیکربندی کنید. مقدار مدت زمان بیکاربودن SSL VPN را به ۱۵ دقیقه یا کمتر تنظیم کنید.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی مدت زمان بیکاربودن SSL VPN اجرا کنید:

```
hostname(config)#vpn-idle-timeout {minutes | none}
```

SCFI-2-4: جلوگیری از ذخیره محلی رمزعبور SSL VPN روی ماشین مشتری (سطح ۱ ، قابل شمارش)

شرح اجمالی:

ذخیره‌سازی محلی رمزعبور Anyconnect VPN بر روی ماشین کاربر را غیرفعال کنید.

نحوه پیاده‌سازی:

کد زیر را برای غیرفعال کردن ذخیره‌سازی محلی رمزعبور اجرا کنید:

```
hostname(config-group-policy)#password-storage disabled
```

SCFI-2-5: نیاز به تازه‌سازی کلید SSL Tunnel (سطح ۱ ، قابل شمارش)

شرح اجمالی:

برای بهبود امنیت تونل، کلید باید به‌روزرسانی شود و همزمان با آن تونلی جدید ایجاد شود. این فرایند به‌روزرسانی باید هر ۸ ساعت یک بار و یا کمتر انجام شود.

نحوه پیاده‌سازی:

کد زیر را برای پیکربندی روش تجدید کلید و مدت‌زمان اعتبار SSL VPN اجرا کنید (مدت‌زمان اعتبار بر حسب دقیقه نشان داده شده است):

```
hostname(config-group-webvpn) #anyconnect SSL rekey method SSL
hostname(config-group-webvpn)#anyconnect SSL rekey time 240
```

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		دسترسی از راه‌دور IPSEC VPN		ندارد	
SCFI-1-1		ایجاد یک خط‌مشی IKEv1		به صورت پیش‌فرض خط‌مشی ISAKMP وجود ندارد.	خط‌مشی ISAKMP پیکربندی شده باشد.
SCFI-1-1-1		تنظیم نوع احرازهویت IKEv1		به صورت پیش‌فرض هیچ خط‌مشی برای ISAKMPوجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، احرازهویت از قبل اشتراک گذاشته مقدار	نوع احرازهویت برای تبادل ISAKMP تنظیم شده باشد.

				پیش فرض قرار می‌گیرد.	
SCFI-1-1-2		تنظیم سطح رمزنگاری IKEv1		هیچ خط‌مشی برای ISAKMP وجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، رمزنگاری 3DES مقدار پیش فرض قرار می‌گیرد.	سطح رمزنگاری IKEv1 پیکربندی گردد.
SCFI-1-1-3		تنظیم درهم‌ساز IKEv1 (سطح ۱ ، قابل شمارش)		هیچ خط‌مشی برای ISAKMP وجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، الگوریتم SAH-1 مقدار پیش فرض قرار می‌گیرد.	درهم‌ساز IKEv1 پیکربندی گردد.
SCFI-1-1-4		تنظیم گروه دیفی-هلمن برای IKEv1 (سطح ۱ ، قابل شمارش)		هیچ خط‌مشی برای ISAKMP وجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، group 2 مقدار پیش فرض قرار می‌گیرد.	گروه دیفی-هلمن برای IKEv1 پیکربندی گردد.

SCFI-1-1-5		تنظیم مدت اعتبار IKEv1 SA (سطح ۱ ، قابل شمارش)		اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، ۸۶,۴۰۰ مقدار پیش‌فرض قرار می‌گیرد.	مدت اعتبار IKEv1 SA پیکربندی گردد.
SCFI-1-1-6		پیکربندی مجموعه تبدیل IKEv1 (سطح۱، قابل شمارش)		به صورت پیش‌فرض مجموعه تبدیل IKEv1 تنظیم نشده است.	مجموعه تبدیل IKEv1 پیکربندی گردد.
SCFI-1-1-7		پیکربندی واسط IKEv1 (سطح۱، قابل شمارش)		ندارد	
SCFI-1-2		ایجاد یک خط‌مشی برای IKEv2 (سطح۱، قابل شمارش)		به صورت پیش‌فرض خط‌مشی ISAKMP وجود ندارد.	خط‌مشی ISAKMP پیکربندی شود.
SCFI-1-2-1		تنظیم نوع احرازهویت IKEv2 (سطح۱،غیر قابل شمارش)		به صورت پیش‌فرض هیچ خط‌مشی برای ISAKMPوجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، احرازهویت از قبل اشتراک گذاشته مقدار	احرازهویت از قبل اشتراک گذاشته پیکربندی شود.

				پیش فرض قرار می‌گیرد.	
SCFI-1-2-2		تنظیم سطح رمزنگاری IKEv2 (سطح ۱، قابل شمارش)		هیچ خط‌مشی برای ISAKMP وجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، رمزنگاری 3DES مقدار پیش فرض قرار می‌گیرد.	سطح رمزنگاری IKEv2 پیکربندی گردد.
SCFI-1-2-3		تنظیم درهم‌ساز IKEv2 (سطح ۱، قابل شمارش)		هیچ خط‌مشی برای ISAKMP وجود ندارد. اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، الگوریتم SAH-1 مقدار پیش فرض قرار می‌گیرد.	درهم‌ساز IKEv2 پیکربندی گردد.
SCFI-1-2-4		تنظیم گروه دیفی-هلمن برای IKEv2 (سطح ۱، قابل شمارش)		اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، group 2 مقدار پیش فرض قرار می‌گیرد.	گروه دیفی-هلمن برای IKEv2 پیکربندی گردد.

SCFI-1-2-5		تنظیم مدت اعتبار IKEv2 SA (سطح ۱، قابل شمارش)		اگر به صورت صریح در خط‌مشی ISAKMP مقداری پیکربندی نشده باشد، ۸۶,۴۰۰ مقدار پیش‌فرض قرار می‌گیرد.	مدت اعتبار SA IKEv2 پیکربندی گردد.
SCFI-1-2-6		پیکربندی طرح پیشنهادی IKEv2 (سطح ۱، قابل شمارش)		هیچ پیشنهادی برای IKEv2 به صورت پیش‌فرض تعریف نشده است.	طرح پیشنهادی IKEv1 پیکربندی شود.
SCFI-1-2-7		پیکربندی رمزنگاری و جامعیت طرح پیشنهادی IKEv2 (سطح ۱، قابل شمارش)		هیچ پیشنهادی برای IKEv2 به صورت پیش‌فرض تعریف نشده است. 3DES رمزنگاری پیش‌فرض و SHA-1 الگوریتم پیش‌فرض مربوطه می‌باشد، هرگاه پیشنهادی برای IKEv2 تعریف نشود.	طرح پیشنهادی رمزنگاری و جامعیت IKEv2 پیکربندی گردد.
SCFI-1-2-8		پیکربندی واسط IKEv2 (سطح ۱، غیر قابل شمارش)		ندارد	
SCFI-1-3		تعریف کلید ISAKMP (سطح ۱، قابل شمارش)		به صورت پیش‌فرض کلید ISAKMP	کلید ISAKMP پیکربندی گردد.

				تنظیم نشده است.	
SCFI-1-4		تعریف مجموعه تبدیل IPSEC (سطح ۱، قابل شمارش)		به صورت پیش‌فرض هیچ گروه تبدیلی پیکربندی نشده است.	گروه تبدیل IPSEC پیکربندی گردد.
SCFI-1-5		تعریف ACL مطابق (سطح ۱، قابل شمارش)		به صورت پیش‌فرض هیچ تطابقی تنظیم نشده است.	ACL تطابق یافته‌ای پیکربندی گردد.
SCFI-1-6		تعریف طرح رمز سراسری (سطح ۱، قابل شمارش)		به صورت پیش‌فرض مقداری تنظیم نشده است.	طرح رمز سراسری پیکربندی گردد.
SCFI-1-6-1		تعریف IP نظیر برای IPSEC (سطح ۱، قابل شمارش)		به صورت پیش‌فرض هیچ نظیری تنظیم نشده است.	IP نظیر برای IPSEC پیکربندی گردد.
SCFI-1-6-2		تعریف مجموعه تبدیل IPSEC (سطح ۱، قابل شمارش)		به صورت پیش‌فرض مقداری تنظیم نشده است.	مجموعه تبدیل IPSEC پیکربندی گردد
SCFI-1-6-3		بکاربردن ACL مطابق برای IPSEC (سطح ۱، قابل شمارش)		به صورت پیش‌فرض هیچ آدرس همتایی تنظیم نشده است.	ACL تطابق یافته‌ای برای IPSEC پیکربندی گردد.
SCFI-1-7		بکاربردن طرح رمز بر روی واسط (سطح ۱، قابل شمارش)		به صورت پیش‌فرض هیچ	طرح رمز بر روی واسط

				طرح رمزی برای واسط تنظیم نشده است.	پیکربندی گردد.
SCFI-2		دسترسی از راه دور SSL VPN (سطح ۱ و ۲، قابل شمارش)		ندارد	
SCFI-2-1		نیاز به گواهی معتبر (سطح ۱، غیر قابل شمارش)		به صورت پیش‌فرض گواهینامه خود امضا شده مورد استفاده قرار می‌گیرد.	گواهینامه معتبر پیکربندی گردد.
SCFI-2-2		نیاز به آخرین Anyconnect نرم‌افزار مشتری (سطح ۱ ،غیر قابل شمارش)		به صورت پیش‌فرض هیچ تصویر Anyconnect نصب نشده است.	آخرین نسخه Anyconnect نرم افزار مشتری نصب گردد.
SCFI-2-3		نیاز به تعیین مدت زمان بیکاربودن SSL VPN (سطح ۱ ، قابل شمارش)		ندارد	مدت زمان بیکاربودن SSL VPN پیکربندی گردد.
SCFI-2-4		جلوگیری از ذخیره محلی رمزعبور SSL VPN روی ماشین مشتری (سطح ۱ ، قابل شمارش)		غیرفعال	غیر فعال
SCFI-2-5		نیاز به تازه‌سازی کلید SSL Tunnel (سطح ۱ ، قابل شمارش)		غیرفعال	غیر فعال