به نام خدا

پیکربندی امن

Cisco IOS Internet Edge

Version 1.1.0

مرکز مدیریت راهبردی افتا

SCSW-CISCO-IOS-EDGE -1.1.0

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، تجهیزات سیسکو با سیستم‌عامل Cisco IOS version 15.0M می‌باشد. 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 "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 version 15.0M 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

SCWS-۱: ناحیه‌بندی شبکه به منظور محافظت در برابر حملات

IOS های سیسکو از ورژن ۱۲,۴ به بعد امکان تعریف سیاست‌های امنیتی بر مبنای تعریف نواحی شبکه (ZFW[1]) را دارا می‌باشند.یک Zone، مرز شبکه را براساس سطح امنیتی مورد نیاز آن، مشخص می‌کند. استفاده از مدل ZFW در مقایسه با مدل مبتنی بر رابط (Interface)، دارای این مزیت است که می‌توان سیاست‌های را بین Zone ها تعریف نمود و این نسبت به تعریف سیاست برای هر رابط (Interface) کاراتر است. همچنین علاوه بر استفاده از ACLs، میتوان در ZFW از امکاناتی نظیر Stateful Packet Filtering، URL Filtering، کاهش حملات DoS و در نهایت کنترل و بازرسی کاربردها استفاده کرد.

SCWS-۱-۱: تعریف نواحی

شرح اجمالی

تعریف ناحیه در روترها امکان‌پذیر است. تعداد نواحی هر شبکه وابسته به معماری شبکه می‌باشد و در هر شبکه حداقل دو ناحیه با سطح امنیتی غیر قابل اعتماد[2] (که همان فضای اینترنت باشد) و ناحیه قابل اعتماد[3] (شبکه داخلی) وجود دارد.

نحوه پیاده‌سازی

به منظور تعریف یک ناحیه جدید دستور زیر اجرا می‌گردد:

```
hostname(config)# zone security <zone_name>
```

[1] Zone-Base Policy Firewall

[2] Untrust

[3] Trust

SCWS-۱-۲ : **تعریف** Access List

شرح اجمالی

ACL ها به منظور کنترل دسترسی نواحی تعریف می‌شوند. دسترسی یا عدم دسترسی هر ناحیه(که بر اساس تجهیزات، شبکه‌ها و پروتکل‌ها قابل تعریف است) طبق نیاز هر شبکه تنظیم می‌گردد.

نحوه پیاده سازی

برای تعریف ACL جدید دستور زیر اجرا می‌گردد:

```
hostname(config)# access-list <access_list_number_or_name> <permit|deny> <protocol> <source>
<destination> [log]
```

SCWS-۱-۳: تعریف Class-Map

شرح اجمالی

Class-Mapها به منظور طبقه‌بندی ترافیک‌های ورودی و خروجی ایجاد می‌شوند. این شناسایی می‌تواند از طریق ACL یا پروتکل انجام شود. هر class-map نیازمند حداقل یک ACL یا پروتکل است. انتخاب ACLها یا پروتکل‌ها، بستگی به سیاست‌های امنیتی سازمان دارد.

نحوه پیاده سازی

برای تعریف Class-map جدید دستور زیر اجرا می‌گردد:

```
hostname(config)# class-map type inspect {match-any | match-all } <class_map_name>
```

۱-۳-۱-SCSW: تعریف پروتکل در Class-Map

شرح اجمالی

همانطورکه در بخش قبل ذکر شد class-map به منظور شناسایی و کنترل ترافیک نیازمند تعریف ACL یا پروتکل است، در این بخش نحوه تعریف پروتکل برای یک class-map ارائه می‌گردد.

نحوه پیاده سازی

برای تعریف پروتکل در Class-map جدید دستور زیر اجرا می‌گردد:

```
hostname(config-cmap)# match protocol <protocol_name>
```

۱-۳-۲- SCSW: تعریف Access-Group

شرح اجمالی

در این بخش نحوه اعمال یک ACL به یک class-map ارائه می‌شود. در واقع ACLی که در بخش‌های قبل تعریف شد به شکل access-group برروی class-map تنظیم می‌شود.

نحوه پیاده سازی

برای اعمال access-group جدید دستور زیر اجرا می‌گردد:

```
hostname(config-cmap)# match access-group <access_list_number_or_name>
```

SCSW-۱-۴: تعریف Policy-map

شرح اجمالی

این بخش یکی از الزامات تعریف و گسترش ZFW Policy است. پس از تعریف class-map که وظیفه شناسایی ترافیک را برعهده دارد، لازم است اقدام مورد نظر برروی ترافیک انجام شود، این اقدام می‌تواند از نوع inspect, drop , pass و یا log باشد. تنظیمات نوع و نحوه اعمال سیاست‌های فوق از طریق policy-map انجام می‌شود.

نحوه پیاده سازی

برای تعریف دستور زیر اجرا می‌گردد:

```
hostname(config)# policy-map type inspect <policy_map_name>
```

SCSW -۱-۴-۱: اعمال class-map در policy-map

شرح اجمالی

هر policy-map ترافیک شبکه را بر اساس یک یا تعداد بیشتری class-map ارزیابی می‌کند. class-map براساس سیاست-های یک سازمان تعیین می‌شود.

نحوه پیاده سازی

برای تعریف class-map در policy-map دستور زیر اجرا می‌گردد:

```
hostname(config-pmap)# class type inspect <class_map_name>
```

SCSW-۱-۴-۱-۱: تنظیم policy-map class

شرح اجمالی

در این بخش فعالسازی policy-map به منظور بازرسی ترافیک انجام می‌شود. هر policy-map براساس یک یا چند class-map، ترافیک را بررسی می‌کند.

نحوه پیاده سازی

به منظور تنظیم بازرسی بر policy-map لازم است دستور زیر اجرا شود:

```
hostname(config-pmap-c)# inspect
```

SCSW-۱-۵: تعریف نگاشت ناحیه[۴] (Zone-pair)

شرح اجمالی

به صورت پیشفرض هیچ ترافیکی مابین zone ها اجازه عبور ندارد، به منظور صدور این اجازه لازم است، zone های مبدا و مقصد در یک zone-pair قرار بگیرند، که در ادامه تنظیمات آن ارائه می‌گردد. در اینجا دو نکته حائز اهمیت است؛ اول اینکه کنترل ترافیک مابین zone مبدا و مقصد توسط policy-map هایی که در این بخش اعمال می‌شوند انجام می‌گیرد، دوم اینکه در هر zone-pair دسترسی و یا محدودیت‌های اعمالی تنها در جهت مبدا به مقصد صادق است و در صورت نیاز به ایجاد دسترسی از مقصد به مبدا لازم است zone-pair جدیدی با محدودیت‌های مختص آن تعریف شود.

نحوه پیاده سازی

برای تعریف zone-pair دستور زیر اجرا گردد:

```
hostname(config)# zone-pair security <zone_pair_name> source <source_zone> destination
<destination_zone> service-policy type inspect <policy_map_name>
```

SCSW-۱-۵-۱: نوشتن توضیحات برای zone-pair

شرح اجمالی

به منظور فهم بهتر zone-pair ها و مشخص شدن هدف از ایجاد آن‌ها در این بخش قابلیت نوشتن توضیحاتی بر zone-pair تعریف شده است، چرا که نام‌گذاری به تنهایی نمی‌تواند هدف از ساخت آن را به وضوح نشان دهد.

نحوه پیاده سازی

به منظور نوشتن توضیحات بر zone-pair دستور زیر اجرا می‌شود:

```
hostname(config-sec zone-pair)# description <zone_pair_description>
```

[۴] - Zone Mapping

SCSW-۱-۵-۲: اعمال policy به zone-pair

شرح اجمالی

همانطورکه قبلا ذکر شد کنترل ترافیکی که مابین zone ها جریان دارد توسط zone-pair انجام می‌شود. لذا در صورت تعریف zone-pair اجازه عبور از zone مبدا به مقصد داده می‌شود، اما کنترل نوع ترافیک عبوری، محدودسازی براساس ACL و دیگر موارد امنیتی در زمان عبور داده از مبدا به مقصد، نیازمند یک یا چند policy است. اعمال policy ها بر zone-pair به روشی که در ادامه ارائه می‌شود، صورت می‌پذیرد.

نحوه پیاده سازی

برای اعمال policy بر zone-pair دستور زیر اجرا گردد:

```
hostname(config-sec zone-pair)# service-policy type inspect <policy_map_name>
```

SCSW-۱-۶: تعریف zone بر روی اینترفیس

شرح اجمالی

هر اینترفیسی که لازم است برروی آن سرویس‌های ZFW راه اندازی شود ، باید در zone مشخصی که مناسب آن است، قرار بگیرد. ناحیه‌ای که اینترفیس در آن قرار میگیرد باید دارای سطح امنیتی متناسب با آنچه به این اینترفیس متصل می‌گردد(تجهیزات، سیستم‌ها و برنامه‌ها) باشد.

نحوه پیاده سازی

برای قرار دادن یک اینترفیس در یک zone دستورات زیر اجرا می‌گردند:

```
hostname(config)# int <interface>
hostname(config-if)# zone-member security <zone_name>
```

SCSW-۲: افزایش محدودیت‌های دسترسی به تنظیمات دستگاه (دسترسی مدیریت)

روتری که در لبه شبکه قرار می‌گیرد قابل دسترس از فضای داخل و بیرون شبکه است، بنابراین لازم است به منظور افزایش سطح امنیت، دسترسی به تنظیمات آن دارای محدودیت باشد. در بخش‌های زیر تنظیمات مربوط به این محدودیت‌ها ارائه می‌گردد.

SCSW-۲-۱: حداقل طول کلمه عبور

شرح اجمالی

افزایش سطح امنیت دسترسی به تنظیمات روتر موجب جبوگیری از دسترسی‌های غیر مجاز و مخرب می‌گردد، لذا پیشنهاد می‌شود که کلمه عبور حداقل ۱۵ کاراکتر باشد. مکمل این بحث روش‌های دسترسی امن از راه دور مانند SSH می‌باشند.

نحوه پیاده سازی

تنظیم حداقل طول کلمه عبور با دستور زیر انجام می‌شود:

```
hostname(config)# security passwords min-length <length>
```

SCSW-۲-۲: ایجاد تاخیر مابین تلاش‌های کاربران برای اتصال به دستگاه

شرح اجمالی

ایجاد تاخیر مابین تلاش‌های کاربران به منظور اتصال به دستگاه، سرعت حملات رمزعبور را کاهش می‌دهد. دسترسی-های امن مانند SSH در اینجا نیز مد نظر هستند .

نحوه پیاده سازی

ایجاد تاخیر مابین تلاش‌های اتصال با دستور زیر انجام می‌شود:

```
hostname(config)# login delay <length_in_seconds>
```

SCSW-۲-۳: حفاظت از روتر در برابر نواحی غیر قابل اعتماد

شرح اجمالی

روتری که در لبه شبکه قرار دارد، اولین نقطه دفاع در برابر حملات می‌باشد و لذا می‌بایست ترافیک ورودی شبکه را کنترل نماید. به منظور افزایش سطح امنیت لیست کنترلی دسترسی (ACL) می‌بایست تعریف گردد. هدف از ایجاد این ACL، محافظت از روتر در برابر اینترفیس که در ناحیه غیر قابل اعتماد قرار دارد[5]، ارتباطات با روتر بعدی و Anti-spoofing، می‌باشد.

نحوه پیاده سازی

دستورات زیر نحوه ایجاد ACL برای کنترل ترافیک در ورودی شبکه را ارائه می‌دهد:

```
hostname(config)# ip access-list extended <internet_edge_acl_name> hostname(config-nacl)# deny tcp any <internet_edge_network> <internet_edge_network_wildcard_mask > fragments
hostname(config-nacl)# deny udp any <internet_edge_network> <internet_edge_network_wildcard_mask > fragments
hostname(config-nacl)# deny icmp any <internet_edge_network> <internet_edge_network_wildcard_mask > fragments
hostname(config-nacl)# <anti-spoofing_acl_lines_from_baseline_document> hostname(config-nacl)# permit tcp host <internet_edge_router_ip> host <bgp_peer_router_ip> eq bgp
hostname(config-nacl)# permit tcp host <internet_edge_router_ip> eq bgp host <bgp_peer_router_ip>
hostname(config-nacl)# deny ip any <internet_edge_network> <internet_edge_network_wildcard_mask>
hostname(config-nacl)# permit ip any any
```

SCSW-۲-۳-۱: اعمال لیست کنترل دسترسی لبه اینترنت

شرح اجمالی

پس از ایجاد لیست کنترل دسترسی، باید برروی اینترفیس (خارجی) مد نظر اعمال شود تا از آن محافظت گردد.

[5] - Router's Untrusted Intefrace

نحوه پیاده سازی

دستورات زیر ACL ایجاد شده را برروی یک اینترفیس اعمال می‌کند:

```
hostname(config)# interface <external_interface>
hostname(config-if)# ip access-group <internet_edge_acl_name> in
```

SCSW-۲-۴: تعریف اینترفیس مدیریت[6]

شرح اجمالی

به منظور کاهش ریسک حمله به امکانات مدیریتی دستگاه از بیرون شبکه، پیشنهاد می‌شود دسترسی به دستگاه از طریق روش‌های مختلف مانند SSH و SNMP محدود به اینترفیس‌های Trust باشد. در ادامه نحوه انجام تنظیمات لازم برای این موضوع ارائه می‌گردد.

نحوه پیاده سازی

دستورات زیر امکان دسترسی به دستگاه از طریق یک اینترفیس مناسب(trust) را فراهم می‌کند.

```
hostname(config)# control-plane host
hostname(config-cp-host)# management-interface <trusted_interface_type>
<trusted_interface_number> allow <mgmt_protocol_1> [mgmt_protocol_2] [...]
```

[6] Management interface

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
SCSW-۱		تنظیمات پیشنهادی			
SCSW-۱,۱		توسعه ناحیه‌بندی شبکه به منظور محافظت در برابر حملات		ندارد	حداقل دو ناحیه
SCSW-۱,۱,۱		تعریف نواحی		ندارد	حداقل دو ناحیه Untrust ,Trust
SCSW-۱,۱,۲		تعریف لیست کنترل دسترسی (ACL)		ندارد	تعریف ACL متناسب با سیاست‌های سازمان و طبق نیاز هر شبکه
SCSW-۱,۱,۳		تعریف Class-Map		ندارد	تعریف Class Map متناسب با سیاست-های سازمان و طبق نیاز هر شبکه
SCSW-۱,۱,۳,۱		تعریف پروتکل در Class-Map		ندارد	محدودسازی پروتکل-ها مطابق با سیاست-های سازمان و طبق نیاز هر شبکه
SCSW-۱,۱,۳,۲		تعریف Access-Group		ندارد	متناسب با ACL و تعریف Class Map شده و طبق نیاز هر شبکه

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCSW-۱,۱,۴		تعریف Policy-map		ندارد	مطابق با سیاست‌های سازمان و طبق نیاز هر شبکه
SCSW-۱,۱,۴,۱		اعمال class-map در policy-map		ندارد	متناسب با Policy Map تعریف شده و طبق نیاز هر شبکه
-۱,۱,۴,۱,۱ SCSW		تنظیم policy-map class		ندارد	متناسب با Policy Map و Class تعریف شده و طبق نیاز هر شبکه
SCSW-۱,۱,۵		تعریف Zone-pair		ندارد	متناسب با Zone-های تعریف شده (حداقل یک عدد)
SCSW-۱,۱,۵,۱		نوشتن توضیحات برای zone-pair		ندارد	-
SCSW-۱,۱,۵,۲		اعمال policy به zone-pair		ندارد	متناسب با Zone-Pair تعریف شده و طبق نیاز هر شبکه
SCSW-۱,۱,۶		تعریف zone بر روی اینترفیس		ندارد	-
SCSW-۱,۲		افزایش محدودیت‌های دسترسی به تنظیمات دستگاه			
SCSW-۱,۲,۱		حداقل طول کلمه عبور		ندارد	حداقل ۱۵ کاراکتر
SCSW-۱,۲,۲		ایجاد تاخیر مابین تلاش‌های کاربران برای اتصال به دستگاه		ندارد	۵ ثانیه
SCSW-۱,۲,۳		حفاظت از روتر در برابر نواحی Untrust		ندارد	تعریف ACL مناسب با سیاست‌های سازمان

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCSW-۱,۲,۳,۱		اعمال ACL لبه اینترنت		ندارد	تعریف ACL مناسب با سیاست‌های سازمان
SCSW-۱,۲,۴		تعریف اینترفیس مدیریت		ندارد	-