إستخدام دليل جدار حماية ASA الآمن

المحتويات

المقدمة

يصف هذا المستند المعلومات التي تساعدك على تأمين أجهزة Cisco ASA، والتي تزيد من الأمان الإجمالي لشبكتك.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Active Security Appliance (ASA) 9.16(1) والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

معلومات أساسية

هذا وثيقة مهيكل في 4 قسم.

1. تقوية مستوى الإدارة - ينطبق هذا على جميع الإدارة ذات الصلة بـ ASA/حركة مرور المرتبط مثل SNMP و SSH وما إلى ذلك.
2. تأمين التكوين - الأوامر التي يمكنك من خلالها إيقاف علم كلمات المرور وما إلى ذلك لعملية التكوين الجارية وما إلى ذلك.

3. التسجيل والمراقبة - ينطبق هذا على أي إعدادات تتعلق بتسجيل الدخول إلى ASA.
4. خلال حركة المرور - ينطبق هذا على حركة المرور التي تمر عبر ASA.

وتوفر تغطية ميزات الأمان في هذا المستند غالبًا تفاصيل كافية لكل لتكوين الميزة. ومع ذلك، في الحالات التي لا توفر فيها التفاصيل الكافية، يتم شرح الميزة بطريقة يمكنك من خلالها تقييم ما إذا كان مطلوبًا توجيه إضافي بالميزة أم لا. حيثما يكون ذلك ممكنًا ومناسبًا، يحتوي هذا المستند على توصيات، في حال تنفيذها، ستساعد على تأمين الشبكة.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع برنامج Cisco ASA الإصدار 9.1x.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

العمليات الآمنة

تعد عمليات الشبكة الآمنة موضوعًا جوهريًا. وعلى الرغم من أنه قد تم تخصيص معظم محتوى هذا المستند للتكوين الآمن لجهاز Cisco ASA، إلا أن عمليات التكوين وحدها لا تؤمن الشبكة بشكل كامل. تساهم الإجراءات التشغيلية المُستخدمة في الشبكة في الأمان بنفس قدر مساهمتها في تكوين الأجهزة الأساسية.

تحتوي هذه الموضوعات على توصيات تشغيلية نوصي بتنفيذها. تلقي هذه الموضوعات الضوء على المناطق الهامة المخصصة لعمليات الشبكة وهي ليست شاملة.

مراقبة استجابات واستشارات أمان Cisco

يعمل فريق الاستجابة لحوادث أمان منتجات Cisco (PSIRT) على إنشاء والحفاظ باسم "توجيهاتPSIRT"، الخاصة بالمشكلات المتعلقة بالمنتجات، التي يُشار إليها عادةً بالمنشورات، بالأمان في منتجات Cisco. الطريقة المُستخدمة للتواصل مع المشاكل الأقل خطورة هي "استجابة أمان Cisco". توفر استجابات وتوجيهات الأمان على PSIRT.

كما توفر معلومات إضافية حول وسائل التواصل هذه في نهج الثغرات الأمنية من Cisco.

للحفاظ على أمان الشبكة، يلزمك أن تكون على دراية باستجابات وتوجيهات الأمان من Cisco التي تم إصدارها. تحتاج إلى معرفة الثغرة الأمنية قبل إمكانية تقييم التهديد الذي يمكن أن يواجه الشبكة. ارجع إلى إعلانات تصنيف المخاطر على الثغرات الأمنية للمساعدة في عملية التقييم هذه.

الاستفادة من المصادقة والتفويض والمحاسبة

يعد إطار عمل المصادقة والتفويض والمحاسبة (AAA) أمرًا حيويًا لتأمين أجهزة الشبكة. كما يوفر إطار عمل المصادقة والتفويض والمحاسبة (AAA) مصادقة جلسات عمل الإدارة ويمكنه أيضًا تقييد المستخدمين بأوامر محددة ومُعرفة من قِبل المسؤول وتسجيل جميع الأوامر

التي تم إدخالها بواسطة جميع المستخدمين. راجع قسم المصادقة والتفويض والمحاسبة (AAA). في هذا المستند للحصول على مزيد من المعلومات حول كيفية الاستفادة من المصادقة والتفويض والمحاسبة (AAA).

تمركز جمع السجلات ومراقبتها

اكتساب المعرفة بشأن الأحداث القائمة والنشطة والمحظورة المتعلقة بالحوادث الأمنية، يجب أن تكون لمؤسستك استراتيجية موحدة لتسجيل الأحداث وربطها. يجب أن تعمل هذه الاستراتيجية على الاستفادة من التسجيل من جميع أجزاء الشبكة واستخدام الإمكانيات الرابطة القابلة للتخصيص والتي تم تجميعها في حزم مسبقاً.

بعد تنفيذ التسجيل المركزي، يجب عليك تطوير أسلوب منهجي لتحليل السجلات وتتبع الحوادث. وبناءً على احتياجات مؤسستك، يمكن أن يتراوح هذا الأسلوب من مراجعة بسيطة لبيانات السجل إلى التحليل المتقدم القائم على القواعد.

استخدام بروتوكولات آمنة عند الإمكان

يتم استخدام العديد من البروتوكولات لحمل بيانات إدارة الشبكة الحساسة. يجب أن تستخدم بروتوكولات آمنة كلما أمكنك ذلك. ويتضمن خيار البروتوكول الآمن استخدام الطبقة الآمنة (SSH) بدلاً من برنامج Telnet حتى يتم تشفير كل من بيانات المصادقة ومعلومات الإدارة. وبالإضافة إلى ذلك، يجب أن تستخدم بروتوكولات نقل الملفات الآمنة عند نسخ بيانات التكوين. والمثال على ذلك هو استخدام بروتوكول النسخ الآمن (SCP) بدلاً من FTP أو TFTP.

اكتساب إمكانية الرؤية لحركة مرور البيانات باستخدام NetFlow

يتيح لك NetFlow إمكانية مراقبة تدفقات حركة مرور البيانات في الشبكة. وبتصميمه في الأصل لتصدير معلومات حركة مرور البيانات إلى تطبيقات إدارة الشبكة، فإنه من الممكن أيضاً استخدام NetFlow لعرض معلومات تدفق البيانات على الموجّه. تتيح لك هذه الإمكانية الاطّلاع على حركة مرور البيانات التي تجتاز الشبكة في الوقت الفعلي. وبغض النظر عما إذا كانت معلومات التدفق يتم تصديرها إلى مجمّع بعيد أم لا، فإننا ننصحك بتكوين أجهزة الشبكة لـ NetFlow حتى يمكن استخدامه بشكل تفاعلي عند الحاجة.

إدارة التكوين

إدارة التكوين هي عملية يتم من خلالها اقتراح تغييرات التكوين ومراجعتها والموافقة عليها ونشرها. وضمن سياق تكوين جهاز Cisco ASA، هناك جانبان إضافيان في إدارة التكوين على قدر كبير من الأهمية: أرشفة التكوين وأمانه.

يمكنك استخدام أرشيفات التكوين لاستعادة التغييرات التي تم إجراؤها على أجهزة الشبكة. في إطار سياق أمني، يمكن استخدام أرشيفات التكوين أيضاً لتحديد التغييرات الأمنية التي تم إجراؤها ووقت حدوث هذه التغييرات. وبالتعاون مع بيانات سجل المصادقة والتفويض والمحاسبة (AAA)، يمكن أن تساعد هذه المعلومات في تدقيق الأمان لأجهزة الشبكة.

يحتوي تكوين جهاز Cisco ASA على العديد من التفاصيل الحساسة. أسماء المستخدمين وكلمات المرور ومحتويات قوائم التحكم في الوصول هي أمثلة على هذا النوع من المعلومات.

يلزم تأمين المستودع الذي تستخدمه لأرشفة تكوينات جهاز Cisco ASA. فقد يؤدي الوصول غير الآمن إلى هذه المعلومات إلى تقويض أمان الشبكة بالكامل.

مستوى الإدارة

يتكون مستوى الإدارة من وظائف تحقق أهداف إدارة الشبكة. وهذا المستوى يتضمن جلسات عمل الإدارة التفاعلية التي تستخدم الطبقة الآمنة (SSH)، وكذلك تجميع الإحصائيات باستخدام بروتوكول SNMP أو NetFlow. عندما تضع أمان جهاز الشبكة في الاعتبار، فمن المهم أن يكون مستوى الإدارة محمياً. إذا كانت الحادثة الأمني قادرة على تقويض وظائف مستوى الإدارة، فقد يكون من المستحيل عليك استرداد الشبكة أو جعلها مستقرة.

مستوى إدارة التعزيز

يُستخدم مستوى الإدارة للوصول إلى الجهاز وتكوينه وإدارته، وكذلك مراقبة عملياته والشبكة التي يتم نشره عليها. مستوى الإدارة هو المستوى الذي يسبق حركة مرور البيانات ويرسلها. تستخدم هذه الوظائف مستوى الإدارة قائمة البروتوكولات التالية:

- بروتوكول إدارة الشبكة البسيط
- بروتوكول طبقة الأمان
- بروتوكول نقل الملفات
- بروتوكول نقل الملفات المبسط
- بروتوكول النسخ الآمن
- TACACS+
- RADIUS
- Netflow
- بروتوكول وقت الشبكة
- Syslog
- ICMP
- الشركات الصغيرة والمتوسطة

ملاحظة: لا يوصى بتمكين برنامج Telnet لأنه نص عادي.

إدارة كلمة المرور

تتحكم كلمات المرور في الوصول إلى الموارد أو الأجهزة. ويتم تحقيق ذلك من خلال تعريف الطلبات. عند تلقي طلب للوصول إلى مورد أو جهاز، يتم اعتراض الطلب للتحقق من كلمة المرور والهوية، ويمكن منح الوصول أو رفضه أو تقييده بناءً على النتيجة. كأفضل ممارسة أمان، يجب إدارة كلمات المرور باستخدام خادم مصادقة RADIUS أو TACACS+. ومع ذلك، لاحظ أنه ما زالت هناك حاجة إلى كلمة مرور يتم تكوينها محلياً للوصول المميز في حالة فشل خدمات RADIUS أو TACACS+. وقد يحتوي الجهاز أيضاً على معلومات كلمة المرور الأخرى الموجودة ضمن التكوين الخاص به، مثل مفاتيح NTP أو سلسلة مجتمع SNMP أو مفاتيح بروتوكول التوجيه.

قام ASA 9.7(1) بتقديم تجزئة PBKDF2 لكلمات المرور المحلية. يتم تخزين اسم المستخدم

المحلي وتمكين كلمات المرور من كل الأطوال في التكوين باستخدام تجزئة وظيفة اشتقاق المفتاح المستندة إلى كلمة المرور 2 (PBKDF2). في السابق، كانت كلمات المرور من 32 حرفا والأقصر تستخدم طريقة التجزئة المستندة إلى MD5. تستمر كلمات المرور الموجودة بالفعل في إستخدام التجزئة المستندة إلى MD5 ما لم تقم بإدخال كلمة مرور جديدة. راجع الفصل "البرامج والتكوينات" في دليل تكوين العمليات العامة للحصول على إرشادات الخفض.

تمكين خدمة HTTP

لاستخدام ASDM، يلزمك تمكين خادم HTTPS، والسماح باتصالات HTTPS إلى ASA. يسمح جهاز الأمان بحد أقصى من 5 مثيلات ASDM متزامنة لكل سياق، إذا كان متوفرا، بحد أقصى 32 حالة ASDM بين جميع السياقات. لتكوين وصول ASDM:

```
http server enable <port>
```

السماح فقط ببروتوكولات IP المطلوبة في قائمة التحكم في الوصول (ACL). والسماح بوصول واسع النطاق ليس ممارسة جيدة.

```
http 0.0.0.0 0.0.0.0 <interface>
```

تكوين التحكم في الوصول إلى ASDM :

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

```
// Set server version
ASA(config)# ssl server-version tlsv1 tlsv1.1 tlsv.1.2

// Set client version
ASA(config) # ssl client-version tlsv1 tlsv1.1 tlsv.1.2
```

يتلقى ال ASA هذا شفرة يمكن in order to عرض افتراضيا.

```
ciscoasa(config)# ssl cipher ?

configure mode commands/options:
  default   Specify the set of ciphers for outbound connections
  dtlsv1    Specify the ciphers for DTLSv1 inbound connections
  dtlsv1.2  Specify the ciphers for DTLSv1.2 inbound connections
  tlsv1     Specify the ciphers for TLSv1 inbound connections
  tlsv1.1   Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2   Specify the ciphers for TLSv1.2 inbound connections
ciscoasa(config)# ssl cipher dtlsv1 ?

configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration string.
```

الإعداد الافتراضي عالي.

- تحدد الكلمة الأساسية all إستخدام كل التشفير: hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- تحدد الكلمة الأساسية المخصصة سلسلة تكوين تشفير تشفير تشفير تشفير مخصصة، مفصولة بعلامات.
- تحدد الكلمة الأساسية FIPS فقط الشفرات المتوافقة مع FIPS: hmac-sha1 hmac-sha2-256
- تحدد الكلمة المفتاحية عالية المشفرات عالية القوة (الافتراضية): hmac-sha2-256
- تحدد الكلمة الأساسية المنخفضة شفرات منخفضة، متوسطة، وعالية القوة: hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- تحدد الكلمة الأساسية متوسطة الشفرات متوسطة وعالية القوة: hmac-sha1 hmac-sha1-96 hmac-sha2-256

يستخدم ASA بشكل افتراضي شهادة موقعة ذاتيا مؤقتة تتغير على كل إعادة تشغيل. إذا كنت تبحث عن شهادة مفردة، يمكنك إستخدام هذه الشهادة الموقعة ذاتيا المدمجة.

يدعم ASA الإصدار 1.2 من TLS للاتصال الآمن لـ ASDM و SSVPN وعملاء بدون AnyConnect VPN. تم إدخال هذه الأوامر أو تم تعديلها: ssl client-version، ssl server-version، ssl cipher، ssl trust-point، ssl dh-group، show ssl، show ssl cipher، show vpn-sessiondb.

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
```

```
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
```

```
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

تمكين SSH

يسمح ASA باتصالات SSH إلى ASA ألغراض الإدارة. يسمح ASA بحد أقصى من 5 إتصالات متزامنة لكل سياق، إذا كان ذلك متاحا، مع حد أقصى يبلغ 100 اتصال مقسمة بين جميع السياقات.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

نوع زوج المفاتيح الافتراضي هو مفتاح عام. حجم المعامل الافتراضي هو 1024. يختلف مقدار مساحة NVRAM لتخزين أزواج المفاتيح باختلاف نظام ASA الأساسي. يمكن الوصول إلى حد إذا قمت بإنشاء أكثر من 30 زوج مفاتيح.

لإزالة أزواج المفاتيح من النوع المشار إليه (rsa أو dsa)،

```
crypto key zeroize { rsa | eddsa | ecdsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

تكوين SSH للوصول إلى الجهاز البعيد:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

لتبادل المفاتيح باستخدام إما طريقة تبادل المفاتيح Diffie-Hellman (DH) Group 1 أو DH

Group 14 أو Curve25519، أستخدم الأمر ssh key-exchange في وضع التكوين العام، بدءا من 9.1(2) ASA معدي DH-Group14-SHA1 ل SSH.

```
ASA(config)#ssh key-exchange group dh-group14-sha256
```

تكوين مهلة جلسات تسجيل الدخول

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

إدارة كلمة المرور

تتحكم كلمات المرور في الوصول إلى الموارد أو الأجهزة. ويتم تحقيق ذلك من خلال تعريف كلمة مرور أو سر يتم استخدامه من أجل مصادقة الطلبات. عند تلقي طلب للوصول إلى مورد أو جهاز، يتم اعتراض الطلب للتحقّق من كلمة المرور والهوية، ويمكن منح حق الوصول أو رفضه أو تقييده بناءً على النتيجة. كأفضل ممارسة أمان، يجب إدارة كلمات المرور باستخدام خادم مصادقة TACACS+ أو RADIUS. ومع ذلك، لاحظ أنه ما تزال هناك حاجة إلى كلمة مرور يتم تكوينها محليًا للوصول المميز في حالة فشل خدمات TACACS+ أو RADIUS. وقد يحتوي الجهاز أيضًا على معلومات كلمة المرور الأخرى الموجودة ضمن التكوين الخاص به، مثل مفتاح NTP أو سلسلة مجتمع SNMP أو مفتاح بروتوكول التوجيه.

تكوين مستخدم محلي وكلمة مرور مشفرة

```
username <local_username> password <local_password> encrypted
```

كلمة تمكين شكل

```
enable password <enable_password> encrypted
```

تكوين مصادقة AAA لوضع التمكين

```
ASA(config)#aaa authentication enable console LOCAL
```

المصادقة والتخويل والمحاسبة

يُعد إطار عمل المصادقة والتفويض والمحاسبة (AAA) أمرًا بالغ الأهمية لتأمين الوصول التفاعلي إلى أجهزة الشبكة. يوفر إطار عمل المصادقة والتفويض والمحاسبة (AAA) بيئة قابلة للتكوين بدرجة عالية يمكن تخصيصها استنادًا إلى احتياجات الشبكة.

مصادقة TACACS+

TACACS+ هو بروتوكول مصادقة يمكن لـ ASA إستخدامه لمصادقة مستخدمي الإدارة مقابل خادم AAA بعيد. ويمكن لهؤلاء المستخدمين الإداريين الوصول إلى جهاز ASA عبر بروتوكول HTTP أو telnet أو HTTPS أو SSH.

توفر مصادقة TACACS+، أو بشكل أعم مصادقة AAA، القدرة على استخدام حسابات المستخدمين الفردية لكل مسؤول شبكة. عندما تعتمد على كلمة مرور مشتركة واحدة،يتحسّن أمان الشبكة وتقوى القدرة على تحديد المسؤوليات لديك.

أما بروتوكول RADIUS هو بروتوكول مشابه في الغرض لـ TACACS+؛ ومع ذلك، الإ موقي TACACS+ بتشفير كلمة المرور المُرسلة عبر الشبكة فقط. في المقابل، يقوي TACACS+ بتشفير حمولة TCP بالكامل، والتي تتضمن كلاً من اسم المستخدم وكلمة المرور. ولهذا السبب، يقضل إستخدام بروتوكول TACACS+ على RADIUS عندما يكون TACACS+ مدعومًا من قبل خادم AAA. ارجع إلى مقارنة TACACS+ وRADIUS للحصول على مقارنة أكثر تفصيلاً بين هذين البروتوكولين.

يمكن تمكين مصادقة TACACS+ على جهاز Cisco ASA بتكوين مشابه للمثال التالي:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

توقيع صورة ASA والتحقق منها

بدءا من الإصدار 9.3.1 من البرنامج، يتم الآن توقيع صور ASA باستخدام توقيع رقمي. يتم التحقق من التوقيع الرقمي بعد تمهيد ASA.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Embedded Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
Computed Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
CCO Hash      SHA-512: 1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
Signature Verified


ASA(config)# verify /signature running
Requesting verify signature of the running image...
```

```
Starting image verification
Hash Computation:    100% Done!
Computed Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c


Get key records from key storage: PrimaryASA, key_store_type: 6
Embedded Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c

Returned. rc: 0, status: 1
The digital signature of the running image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
 Signer Information
 Common Name : abraxas
 Organization Unit : ASAv
 Organization Name : CiscoSystems
 Certificate Serial Number : 550DBBD5
 Hash Algorithm : SHA2 512
 Signature Algorithm : 2048-bit RSA
 Key Version : A
```

تكوين المنطقة الزمنية للساعة

```
clock timezone GMT <hours offset>
```

تكوين NTP

ال دعُي بروتوكول وقت الشبكة (NTP) خدمة خطيرة بوجه خاص، ولكن أي خدمة غير ضرورية قد تمثل تهديدا. إذا تم استخدام بروتوكول وقت الشبكة (NTP)، فمن المهم تكوين مصدر وقت دقيق. يلزم توفر وقت مناسب لمصادقات استخدام IPsec مثل قوثوم هب قوثومو وقت ضارغألا هب syslog (الدخول إلى النظام)، كما هو الحال أثناء التحقيقات الجنائية للهجمات المحتملة، وكذلك لاتصال VPN الناجح عند الاعتماد على شهادات مصادقة المرحلة الأولى.

- منطقة NTP الزمنية - عند تكوين بروتوكول وقت الشبكة (NTP)، يلزم تكوين المنطقة الزمنية بحيث يمكن ربط الطوابع الزمنية بدقة. عادةً ما يكون هناك نهجان لتكوين المنطقة الزمنية للأجهزة في الشبكة ذات الحضور العالمي. يتمثل أولهما في تكوين جميع أجهزة الشبكة باستخدام التوقيت العالمي المنسق (UTC) (توقيت جرينتش المركزي (GMT) سابقًا). بينما تتمثل الطريقة الأخرى في تكوين أجهزة الشبكة باستخدام المنطقة الزمنية المحلية. ويفضل خادم NTP ip_address [key_id] [مصدر interface_name]

- مصادقة NTP - إذا تمق تبتكوين مصادقة NTP، فإنه اهرفوت رضامنًا بتبادل رسائل NTP بين أقران NTP الموثوق بهم. قم بتمكين المصادقة باستخدام الأمر NTP Authentication، وتعيين مفتاح الموثوق به لهذا الخادم. إذا تمق تبتمكين المصادقة، فإن ASA ال يتصل بخادم NTP إلا إذا أستخدم المفتاح الموثوق به الصحيح في الحزم. لتمكين المصادقة مع خادم NTP، أستخدم الأمر ntp authentication في وضع التكوين العام.

```
ASA(config)#ntp authenticate
```

خدمة خادم DHCP (في حال عدم إستخدامها)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

ملاحظة: ال يدعم ASA CDP.

قائمة الوصول إلى مستوى التحكم

قواعد التحكم في الوصول لحركة مرور الإدارة إلى المربع (المعرفة بواسطة مثل هذه الأوامر مثل http أو ssh أو telnet) لها أسبقية أعلى من قائمة الوصول المطبقة مع خيار مستوى التحكم. لذلك، يمكن السماح لحركة مرور الإدارة المسموح بها هذه بالدخول حتى إذا تم رفضها بشكل صريح بواسطة قائمة الوصول إلى المربع.

```
access-list <name> in interface <Interface_name> control-plane
```

آمن نسا

فيما يلي البروتوكولات التي يمكن إستخدامها لنسخ/نقل الملفات إلى ASA.

نص واضح:

- FTP
- HTTP
- TFTP
- الشركات الصغيرة والمتوسطة

آمن:

- HTTPS
- يدعم ASA لعميل النسخ الآمن (SCP) عميل SCP لنقل الملفات من خادم SCP وإليه.

خلال حركة المرور

عشوائية رقم تسلسل TCP

يحتوي كل اتصال TCP على نظامي IS: أحدهما تم إنشاؤه بواسطة العميل والآخر تم إنشاؤه بواسطة الخادم. يقوم ASA بترتيب IS الخاص ب TCP SYN عشوائيا أثناء المرور في كل الاتجاهين الوارد والصادر.

كما أن عشوائية تنظيم "الدولة الإسلامية" من قبل المضيف المحمي تمنع المهاجم من إطلاق النار على "الدولة الإسلامية" التالية من أجل الحصول على اتصال جديد وربما إختطاف الجلسة الجديدة.

يمكن تعطيل تعيين الرقم التسلسلي الأولي ل TCP عشوائيا إذا لزم الأمر. على سبيل المثال:

- إذا كان هناك جدار حماية داخلي آخر يقوم أيضا بعشوائية أرقام التسلسل الأولية، فلا حاجة لجدران الحماية كلاهما للقيام بهذا الإجراء، حتى وإن كان هذا الإجراء لا يؤثر على حركة المرور.
- إذا كنت تستخدم الخطوات المتعددة ل eBGP من خلال ASA، وكانت نظائر eBGP تستخدم MD5. يكسر العشوائية المجموع الاختباري MD5.
- إذا إستخدمنا جهاز WAAS يتطلب من ASA عدم أخذ الأرقام التسلسلية للاتصالات بشكل عشوائي.

تناقص TTL

بشكل افتراضي، الى يتم تقليل TTL في رأس IP نظرا لأن ASA يظهر كخطوة موجه عند إجراء Traceroute.

dnsguard

فرض إستجابة DNS واحدة لكل استعلام. يمكن تمكينها باستخدام الأمر في وضع التكوين العام.

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

تكوين عمليات التحقق من تجزئة سلسلة الأجزاء

لتوفير إدارة إضافية لتجزئة الحزمة وتحسين التوافق مع NFS، أستخدم الأمر fragment في وضع التكوين العام.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

تكوين فحص البروتوكول

يلزم توفر محركات الفحص للخدمات التي تقوم بدمج معلومات عنونة IP في حزمة بيانات المستخدم، أو التي تفتح القنوات الثانوية على المنافذ المعينة بشكل ديناميكي. تتطلب هذه البروتوكولات أن يتم ASA فحص حزمة عميق بدل من تمرير الحزمة عبر المسار السريع. ونتيجة لهذا فإن محركات الفحص من الممكن أن تؤثر على الإنتاجية الإجمالية. ارجع إلى دليل تكوين ASA 9.4 للحصول على معلومات تفصيلية حول فحص بروتوكول طبقة التطبيق.

يمكن تمكين الفحص على ASA باستخدام هذا الأمر.

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

وبشكل افتراضي، يكون ل ASA global_policy enabled بشكل عام.

تكوين إعادة توجيه المسار العكسي للبث الأحادي

```
ip verify reverse-path interface <interface_name>
```

عند إسقاط حركة المرور بسبب فحص RPF، يعرض هذا عداد إسقاط ASP على زيادات ASA.

<#root>

```
ASA(config)# show asp drop

Frame drop:
  Invalid TCP Length (invalid-tcp-hdr-length)                 21
  Reverse-path verify failed (rpf-violated)                   90
```

```
// Check Reverse path statistics

ASA(config)# sh ip verify statistics

interface inside: 11 unicast rpf drops


interface outside: 79 unicast rpf drops
```

اكتشاف التهديد

يوفر اكتشاف التهديدات لمسؤولي جدار الحماية الأدوات الضرورية لتحديد الهجمات وفهمها وتوقفها قبل وصولها إلى البنية الأساسية للشبكة الداخلية. وللقيام بذلك، تعتمد هذه الميزة على عدد من العوامل المشغلة والإحصاءات المختلفة، التي يرد وصفها بمزيد من التفصيل في هذه الأقسام.

ارجع إلى وظيفة اكتشاف تهديدات ASA وتكوينها للحصول على شرح تفصيلي حول اكتشاف التهديدات على ASA.

مرشح علم النبات

يقوم عامل تصفية حركة مرور BotNet بمراقبة طلبات خادم اسم المجال (DNS) والاستجابات بين عملاء DNS الداخليين وخوادم DNS الخارجية. عند معالجة إستجابة DNS، يتم التحقق من المجال المقترن بالاستجابة مقابل قاعدة بيانات المجالات الضارة المعروفة. إذا كان هناك تطابق، يتم حظر أي حركة مرور إضافية إلى عنوان IP الموجود في إستجابة DNS.

البرامج الضارة هي برامج ضارة تم تثبيتها على مضيف غير معروف. يمكن اكتشاف البرامج الضارة التي تحاول نشاط الشبكة مثل إرسال بيانات خاصة (كلمات المرور أو أرقام بطاقات الائتمان أو ضربات المفاتيح أو بيانات خاصة) بواسطة عامل تصفية حركة مرور Botnet عندما يدأ البرنامج الضار الاتصال بعنوان IP سيئ معروف. يتحقق عامل تصفية حركة مرور Botnet من الاتصالات الواردة والصادرة مقابل قاعدة بيانات ديناميكية من أسماء المجالات وعناوين IP السيئة المعروفة (القائمة المحظورة)، ثم يقوم بتسجيل أي نشاط مريب أو حظره.

أنت يستطيع أيضا ألحق ال cisco قاعدة معطيات حركي مع قيد قائمة عنوان من إختيارك بأضفته إلى قائمة ساكن إستاتيكي محظورة. إذا كانت قاعدة البيانات الديناميكية تتضمن عناوين قائمة محظورة تعتقد أنه لا يمكن حظرها مسردة، يمكنك إدخالها يدويا في قائمة ثابتة مسموح بها. لا تزال عناوين القائمة المسموح بها توقوم بإنشاء رسائل syslog، ولكن لأنك تستهدف رسائل syslog للقائمة المحظورة فقط، فإنها إعلامية. راجع تكوين عامل تصفية حركة مرور Botnet للحصول على معلومات تفصيلية.

إضافات ذاكرة التخزين المؤقت ل ARP للشبكات الفرعية غير المتصلة

ال يستجيب ASA بشكل افتراضي إلى ARP لعناوين IP للشبكة الفرعية غير المتصلة مباشرة. إذا كان لديك عنوان NAT IP على ASA ال ينتمي إلى نفس الشبكة الفرعية IP لواجهة ASA، فيمكنك تمكين السماح ل ARP غير المتصل على ASA إلى ARP للوكيل ل

NATted IP.

```
arp permit-nonconnected
```

يوصى دائما بأن يكون التوجيه الصحيح على أجهزة تدفق البيانات من الخادم والتدفق ل NAT للعمل دون تمكين الأمر السابق.

التسجيل والمراقبة

تكوين SNMP

يسلط هذا القسم الضوء على العديد من الطرق التي يمكن إستخدامها من أجل تأمين نشر بروتوكول SNMP داخل أجهزة ASA. من المهم للغاية أن تتم تأمين بروتوكول SNMP بشكل صحيح من أجل حماية سرية كل من بيانات الشبكة وأجهزة الشبكة التي تمر من خلال هذه البيانات ومن أجل تكامل تلك البيانات وتوفّرها. يوفر كل بروتوكول SNMP ثورة من المعلومات حول حالة أجهزة الشبكة. يمكن حماية هذه المعلومات من المستخدمين الضارين الذين يريغبون في الاستفادة من هذه البيانات لتنفيذ هجمات ضد الشبكة.

سلاسل مجتمع SNMP

سلاسل المجتمع هي كلمات مرور يتم تطبيقها على جهاز ASA لتقييد الوصول، الوصول للقراءة فقط والوصول للقراءة والكتابة على السواء، إلى بيانات SNMP على الجهاز. يمكن إختيار سلاسل المجتمع هذه بعناية، كما هو الحال مع جميع كلمات المرور، لضمان أنها ليست تافهة. يمكن تغيير سلاسل المجتمع على فواصل زمنية منتظمة ووفقا لسياسات أمان الشبكة. على سبيل المثال، يمكن تغيير السلاسل عندما يقوم موظف بتغيير وظيفته أو بترك الشركة.

تمكين وصول قراءة SNMP

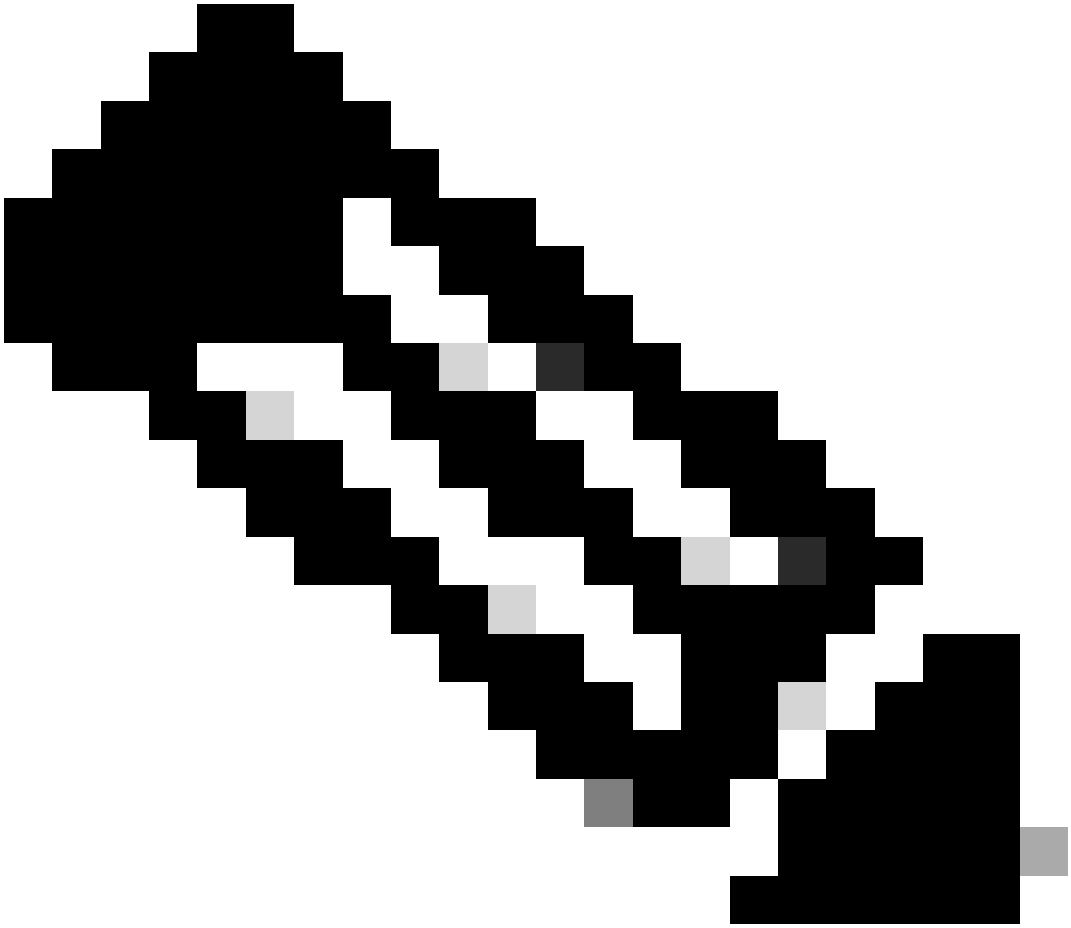
```
snmp-server host <interface_name> <remote_ip_address>
```

تمكين مضائد SNMP

```
snmp-server enable traps all
```

تكوين Syslog

يوصى بإرسال معلومات التسجيل إلى خادم syslog عن بعد. وهذا يجعل من الممكن ربط أحداث الشبكة والأمان ومراجعتها عبر أجهزة الشبكة بشكل أكثر فاعلية.



ملاحظة: يتم إرسال رسائل syslog بشكل غير موثوق به بواسطة UDP وفي نص واضح.

ولهذا السبب، يمكن أن تكون أي أوجه حماية تتحملها الشبكة لحركة مرور الإدارة (على سبيل المثال، التشفير أو الوصول خارج النطاق الترددي) موسعة لتضمين حركة مرور syslog. يمكن تكوين السجلات ليتم إرسالها إلى هذه الوجهة من ASA:

- ASDM
- مصدا
- وميض
- البريد الإلكتروني
- خادم FTP
- خادم SNMP كمالئمات
- خادم Syslogs

تكوين مستوى خطورة تسجيل وحدة التحكم

```
logging console critical
```

يتوفر أيضا syslog المستندة إلى TCP. يمكن إرسال جميع syslog إلى خادم syslog في وضع النص العادي أو في وضع التشفير في حالة بروتوكول TCP.

نص عادي

logging host interface_name syslog_ip [tcp/ port

مشفّر

logging host interface_name syslog_ip [tcp/ port | [آمنة]

إذا تعذر إنشاء اتصال TCP باستخدام خادم syslogs، يمكن رفض جميع الاتصالات الجديدة. يمكنك تغيير هذا السلوك الافتراضي من خلال إدخال الأمر logging allowed-hostdown.

تكوين الطوابع الزمنية في رسائل السجل

يساعدك تكوين الطوابع الزمنية للتسجيل على ربط الأحداث عبر أجهزة الشبكة. من المهم تنفيذ تكوين طابع زمني صحيح ومتسق للتسجيل لضمان إمكانية ربط بيانات التسجيل.

```
logging timestamp
```

للحصول على معلومات إضافية متعلقة ب syslog، ارجع إلى مثال تكوين ASA syslog.

تكوين NetFlow

وفي بعض الأحيان، ربما تحتاج إلى التعرف بسرعة على حركة مرور الشبكة وtraceback، وخاصة ًأثناء استجابة الحدث أو أداء الشبكة الضعيف. يمكن أن يوفر NetFlow إمكانية رؤية لجميع حركات المرور على الشبكة. وبالإضافة إلى ذلك، يمكن تنفيذ NetFlow باستخدام أدوات التجميع التي يمكنها توفير التحليل التلقائي وبتوجيه طويلة المدى.

يدعم Cisco ASA خدمات NetFlow الإصدار 9. توفر عمليات تنفيذ ASA و ASASM ل NSEL طريقة تعقب تدفق IP معبرة عن الحالة تقوم بتصدير السجلات التي تشير إلى أحداث مهمة في التدفق فقط. في تعقب التدفق الذي يحدد الحالة، تمر التدفقات المتتبعة بسلسلة من تغييرات الحالة. يتم إستخدام أحداث NSEL لتصدير البيانات حول حالة التدفق ويتم تشغيلها بواسطة الحدث الذي تسبب في تغيير الحالة.

ارجع إلى دليل تنفيذ Cisco ASA NetFlow للحصول على مزيد من المعلومات حول NetFlow على ASA:

تأمين التكوين

كلمات المرور في التكوين

تكون جميع كلمات المرور والمفاتيح إما مشفرة أو مبهمة . ال يكشف العرض running-config كلمات المرور الفعلية.

ال يمكن إستخدام النسخة الاحتياطية هذه للنسخ الاحتياطي/الاستعادة على ASA. سيتم إجراء النسخ الاحتياطي الذي يتم إستخدامه ألغراض الاستعادة باستخدام الأمر more system:running-config. يمكن تشفير كلمات مرور تكوين ASA باستخدام عبارة مرور أساسية. راجع تشفير كلمة المرور للحصول على معلومات تفصيلية.

إسترداد كلمة مرور الخدمة

يمكن أن يؤدي تعطيل هذه إلى تعطيل آلية إسترداد كلمة المرور وتعطيل الوصول إلى ROMMON. قد تكون الوسيلة الوحيدة للاسترداد من كلمات المرور المفقودة أو المنسية هي مسح جميع أنظمة الملفات بما في ذلك ملفات التكوين والصور من خالل ROMMON. يمكنك إجراء عملية نسخ إحتياطي للتكوين الخاص بك والحصول على آلية استعادة الصور من سطر أوامر ROMMON.

استكشاف الأخطاء وإصالحها

ال تتوفر معلومات حول أستكشاف الأخطاء وإصالحها.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).