مثال على تكوين FWSM الأساسي

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
مشكلة: يعجز أن يمر ال VLAN حركة مرور من FWSM إلى ال ips مستشعر 4270
الحل
إصدار الحزم الخارجة عن الترتيب في FWSM
الحل
المشكلة: تعذر تمرير الحزم الموجهة غير المتماثلة عبر جدار الحماية
الحل
دعم NetFlow في FWSM
الحل
معلومات ذات صلة

المقدمة

يصف هذا وثيقة كيف أن يشكل التشكيل أساسي من جدار الحماية خدمات وحدة نمطية (FWSM) يركب إما في ال cisco 6500 sery مفتاح أو cisco 7600 sery مسحاج تخديد. هذا يتضمن التشكيل من العنوان، تقصير تحشد، ساكن إستاتيكي وحركي NATing، التحكم بالوصول قوائم (ACL) in order to سمحت الحركة مرور مرغوب أو منعت الحركة مرور غير مرغوب، تطبيق نادل مثل WebSense لتفتيش حركة مرور الإنترنت من الشبكة الداخلية، و WebServer لمستخدمي الإنترنت.

ملاحظة: في سيناريو التوفر العالي (HA) لبروتوكول FWSM، يمكن تجاوز الفشل المزامنة بنجاح فقط عندما تكون مفاتيح الترخيص هي نفسها تماما بين الوحدات النمطية. لذلك، لا يمكن أن يعمل تجاوز الفشل بين FWSMs مع تراخيص مختلفة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- الوحدة النمطية لخدمات جدار الحماية التي تشغل الإصدار 3.1 من البرنامج والإصدارات الأحدث
- المحولات من السلسلة Catalyst 6500، بالمكونات المطلوبة كما هو موضح:محرك المشرف مع برنامج Cisco IOS®، والمعروف باسم المشرف Cisco IOS، أو نظام التشغيل Catalyst (OS). راجع الجدول الخاص بإصدارات البرامج ومحرك المشرف المدعوم.بطاقة ميزة التحويل متعدد الطبقات (2 (MSFC مع برنامج Cisco IOS. راجع الجدول للحصول على إصدارات برنامج Cisco IOS software المدعومة.

[1] لا يدعم FWSM المشرف 1 أو 1A.

[2] عندما يستعمل أنت مادة حفازة os على المشرف، أنت يستطيع استعملت any of this دعم cisco ios برمجية إطلاق على ال MSFC. عندما يستعمل أنت cisco ios برمجية على المشرف، أنت تستعمل ال نفسه إطلاق على ال MSFC.

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

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين لموجهات سلسلة 7600 من Cisco، مع المكونات المطلوبة كما هو موضح:

- محرك المشرف مع برنامج Cisco IOS software. راجع الجدول الخاص بإصدارات برنامج Cisco IOS Software محرك المشرف المدعوم.
- MSFC 2 مع برنامج Cisco IOS. راجع الجدول للحصول على إصدارات برنامج Cisco IOS software المدعومة.

الاصطلاحات

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

معلومات أساسية

ال FWSM عالي الأداء، موفر للمساحة، جدار حماية ذو حالة تثبت في المادة حفازة 6500 sery مفتاح وال cisco 7600 sery مسحاج تخديد.

تحمي جدران الحماية الشبكات الداخلية من الوصول غير المصرح به من قبل المستخدمين على شبكة خارجية. يمكن لجدار الحماية أيضا حماية الشبكات الداخلية من بعضها البعض، على سبيل المثال، عندما تبقي شبكة الموارد البشرية منفصلة عن شبكة مستخدم. إذا كان لديك موارد شبكة يلزم أن تكون متوفرة لمستخدم خارجي، مثل خادم ويب أو FTP، فيمكنك وضع هذه الموارد على شبكة منفصلة خلف جدار الحماية، يطلق عليه منطقة مجردة من السلاح (DMZ). يسمح جدار الحماية بالوصول المحدود إلى المنطقة المنزوعة السلاح، ولكن لأن المنطقة المنزوعة السلاح تتضمن الملقمات العامة فقط، فإن الهجوم هناك يؤثر على الملقمات فقط ولا يؤثر على الشبكات الداخلية الأخرى. يمكنك أيضا التحكم عند وصول مستخدمين داخليين إلى شبكات خارجية، على سبيل المثال، الوصول إلى الإنترنت، إذا كنت تسمح فقط لعناوين معينة، أو كنت تتطلب المصادقة أو التفويض، أو كنت تنسق مع خادم تصفية URL خارجي.

يتضمن FWSM العديد من الميزات المتقدمة، مثل سياقات الأمان المتعددة المشابهة لجدران الحماية الافتراضية،

وجدار الحماية الشفاف (الطبقة 2) أو عملية جدار الحماية الموجهة (الطبقة 3)، ومئات الواجهات، وميزات كثيرة أخرى.

أثناء مناقشة الشبكات المتصلة بجدار الحماية، تكون الشبكة الخارجية أمام جدار الحماية، وتكون الشبكة الداخلية محمية وخلف جدار الحماية، بينما يسمح DMZ أثناء وجوده خلف جدار الحماية بالوصول المحدود إلى المستخدمين الخارجيين. لأن ال FWSM يسمح أنت شكلت كثير قارن مع مختلف أمن سياسة، أي يتضمن كثير داخلي قارن، كثير DMZs، وحتى كثير قارن خارجي إن يريد، هذا شرط استعملت بمفهوم عام فقط.

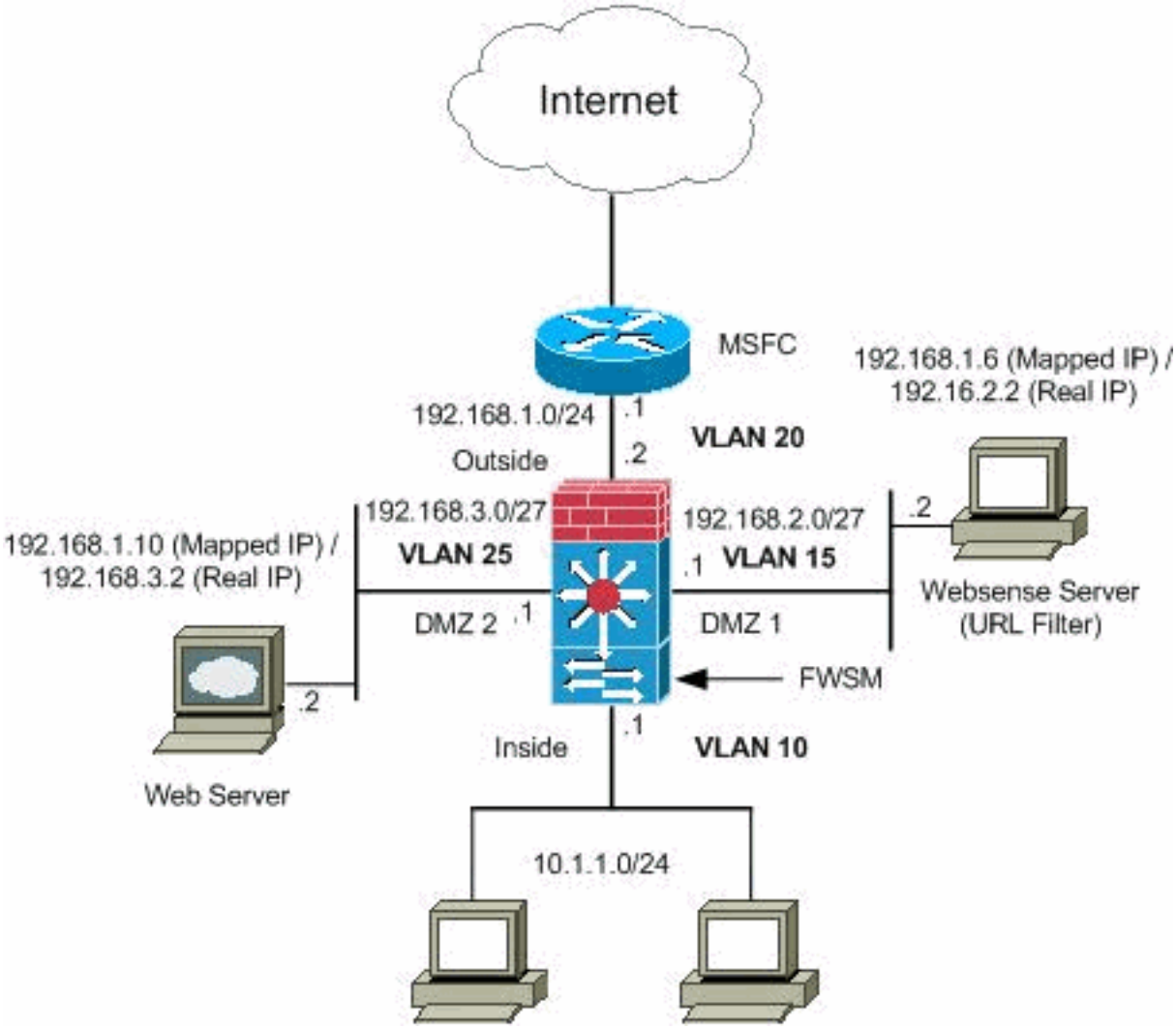
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين المحول Catalyst 6500 Series Switch
- تكوين FWSM

تكوين المحول Catalyst 6500 Series Switch

1. أنت يستطيع ركبت ال FWSM في المادة حفازة sery 6500 مفتاح أو ال cisco 7600 sery مسحاج تخديد. يكون تكوين كل من السلسلة متطابقا وتتم الإشارة إلى السلسلة بشكل عام في هذا المستند باسم **المحول.ملاحظة:** يلزمك تكوين المحول بشكل مناسب قبل تكوين FWSM.
2. **عينت VLANs إلى جدار الحماية خدمة وحدة نمطية**— يصف هذا قسم كيف أن يعين VLANs إلى ال FWSM. لا يتضمن FWSM أي واجهات مادية خارجية. وبدلا من ذلك، يستخدم واجهات شبكات VLAN. يعين VLANs إلى ال FWSM مماثل إلى كيف أنت تعين VLAN إلى مفتاح ميناء؛ ال FWSM يتضمن قارن داخلي إلى المفتاح بناء وحدة نمطية، إن يتواجد، أو ال يشارك حافلة.**ملاحظة:** راجع قسم تكوين شبكات VLAN من دليل تكوين البرنامج Catalyst 6500 Switches Software للحصول على مزيد من المعلومات حول كيفية إنشاء شبكات VLAN وتعيينها على منافذ المحول.**إرشادات شبكة VLAN:**أنت يستطيع استعملت VLANs خاص مع ال FWSM. عينت ال VLAN أساسي إلى ال FWSM؛ ال FWSM تلقائيا يعالج ثانوي VLAN حركة مرور.لا يمكنك إستخدام شبكات VLAN المحجوزة.أنت يستطيع لا يستعمل VLAN 1.إذا كنت تستخدم تجاوز فشل FWSM داخل هيكل المحول نفسه، فلا تقم بتعيين شبكة (شبكات) VLAN التي قمت بحجزها لتجاوز الفشل والاتصالات ذات الحالة لمنفذ المحول. ولكن، إذا كنت تستخدم تجاوز الفشل بين الهيكل، فيجب عليك تضمين شبكات VLAN في منفذ خط الاتصال بين الهيكل.إن لا يضيف أنت ال VLANs إلى المفتاح قبل أن أنت تعين هم إلى ال FWSM، ال VLANs خزنت في المشرف محرك قاعدة معطيات وأرسلت إلى ال FWSM حالما هم أضفت إلى المفتاح.عينت VLANs إلى ال FWSM قبل أن أنت تعين هم إلى ال MSFC.يتم تجاهل شبكات VLAN التي لا تفي بهذا الشرط من نطاق شبكات VLAN التي تحاول تعيينها على FWSM.**عينت VLANs إلى ال FWSM في cisco ios برمجية:**في برنامج Cisco IOS software، قم بإنشاء ما يصل إلى 16 مجموعة VLAN لجدار الحماية، ثم قم بتعيين المجموعات إلى FWSM. على سبيل المثال، يمكنك تعيين جميع شبكات VLAN إلى مجموعة واحدة، أو يمكنك إنشاء مجموعة داخلية ومجموعة خارجية، أو يمكنك إنشاء مجموعة لكل عميل. يمكن أن تحتوي كل مجموعة على شبكات VLAN غير محدودة.أنت يستطيع لا يعين ال VLAN إلى نفسه إلى يتعدد جدار مانع للحريق، مهما، أنت يستطيع عينت يتعدد جدار مانع للحريق مجموعة إلى FWSMs يتعدد. VLANs أن أنت تريد أن يعين إلى يتعدد FWSMs، مثلا، يستطيع أقمت في مجموعة منفصل من VLANs أن يكون فريد إلى كل FWSM.أتمت ال steps in order to عينت VLANs إلى ال FWSM:

```
Router(config)#firewall vlan-group firewall_group vlan_range
```

`vlan_range` يستطيع كنت one or much VLANs، مثلا، 2 إلى 1000 ومن 1025 إلى 4094، يعين إما رقم وحيد (n) مثل 5، 10، 15 أو مدى (n-x) مثل 5-10، 10-20.**ملاحظة:** تستهلك المنافذ الموجهة ومنافذ شبكات WAN شبكات VLAN الداخلية، لذلك من الممكن أن تكون شبكات VLAN في النطاق 1020-1100 قيد الاستخدام بالفعل.**مثال:**

```
firewall vlan-group 1 10,15,20,25
```

أتمت ال steps in order to عينت الجدار الناري مجموعة إلى ال FWSM.

```
Router(config)#firewall module module_number vlan-group firewall_group
```

`Firewall_group` هو رقم مجموعة واحد أو أكثر كرقم واحد (n) مثل 5 أو نطاق مثل 5-10.**مثال:**

```
firewall module 1 vlan-group 1
```

عينت VLANs إلى ال FWSM في مادة حفازة نظام برمجية— في مادة حفازة os برمجية، أنت تعين قائمة ميلان إلى جانب من VLANs إلى ال FWSM. أنت يستطيع عينت ال نفسه VLAN إلى يتعدد FWSMs إن يريد.

يمكن أن تحتوي القائمة على شبكات VLAN غير محدودة.أتمت ال steps in order to عينت VLANs إلى ال FWSM.

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

`vlan_list` يستطيع كنت one or much VLANs، مثلا، 2 إلى 1000 ومن 1025 إلى 4094، يعين إما رقم وحيد (n) مثل 5، 10، 15 أو مدى (n-x) مثل 5-10، 10-20.

إضافة الواجهات الظاهرية المحولة إلى MSFC— تسمى شبكة VLAN المعرفة على MSFC واجهة ظاهرية3. محولة. إن يعين أنت ال VLAN يستعمل ل ال SVI إلى ال FWSM، بعد ذلك ال MSFC ممر بين ال FWSM آخر طبقة 3 VLANs.لأسباب أمنية، افتراضيا، يمكن أن يوجد فقط SVI واحد بين ال MSFC و FWSM. على سبيل المثال، إذا قمت بتكوين النظام بشكل خاطئ باستخدام العديد من شبكات SVI، فيمكنك السماح لحركة مرور البيانات بالمرور حول FWSM إذا قمت بتخصيص كل من شبكات VLAN الداخلية والخارجية إلى MSFC.أتمت ال steps in order to شكلت ال SVI

```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

مثال:

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

تكوين المحول Catalyst 6500 Series Switch
Output Suppressed firewall vlan-group 1 10,15,20,25 *---!* firewall module 1 vlan-group 1 interface vlan 20 ip address 192.168.1.1 255.255.255.0 *!--- Output Suppressed*

ملاحظة: جلسة في ال FWSM من المفتاح مع الأمر مناسب للمفتاح نظام تشغيل:

- برنامج IOS من Cisco:

```
Router#session slot
```

- برامج Catalyst OS:

```
Console> (enable) session module_number
```

(إختياري) مشاركة شبكات VLAN مع وحدات الخدمة الأخرى— إذا كان المحول يحتوي على وحدات خدمة أخرى، على سبيل المثال، محرك التحكم في التطبيق (ACE)، فمن الممكن أن تكون مضطرا لمشاركة بعض شبكات VLAN مع وحدات الخدمة هذه. راجع تصميم الوحدة النمطية للخدمة مع ACE و FWSM للحصول على مزيد من المعلومات حول كيفية تحسين تكوين FWSM عند العمل مع الوحدات النمطية الأخرى.

تكوين FWSM

1. **شكلت قارن ل FWSM—** قبل أن أنت يستطيع سمحت حركة مرور عبر ال FWSM، أنت تحتاج أن يشكل قارن إسم وعنوان. يجب أيضا تغيير مستوى الأمان من الإعداد الافتراضي، وهو 0. إذا قمت بتسمية واجهة ، ولم تقم بتعيين مستوى الأمان بشكل صريح، فعندئذ يقوم FWSM بتعيين مستوى الأمان على 100.**ملاحظة:** يجب أن يكون لكل واجهة مستوى أمان من 0 (الأقل) إلى 100 (الأعلى). على سبيل المثال، يجب تعيين الشبكة الأكثر

أمانا، مثل شبكة المضيف الداخلية، إلى المستوى 100، بينما يمكن أن تكون الشبكة الخارجية المتصلة بالإنترنت من المستوى 0. يمكن أن تكون الشبكات الأخرى، مثل DMZ، في ما بين.أنت يستطيع أضفت أي VLAN id إلى التشكيل، غير أن فقط VLANs، مثلا، 10، 15، 20 و 25، أن يكون عينت إلى ال FWSM بالمفتاح يستطيع مررت حركة مرور. أستخدم الأمر **show vlan** لعرض جميع شبكات VLAN التي تم تعيينها إلى FWSM.

```
interface vlan 20
nameif outside
security-level 0
ip address 192.168.1.2 255.255.255.0
interface vlan 10
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
interface vlan 15
nameif dmz1
security-level 60
ip address 192.168.2.1 255.255.255.224
interface vlan 25
nameif dmz2
security-level 50
ip address 192.168.3.1 255.255.255.224
```

تلميح: في الأمر **name< *name*> ، يكون** *name***سلسلة نصية تصل إلى 48 حرفا وليست حساسة لحالة الأحرف.** يمكنك تغيير الاسم إذا قمت بإعادة إدخال هذا الأمر بقيمة جديدة. لا تدخل النموذج no، لأن هذا الأمر يؤدي إلى حذف جميع الأوامر التي تشير إلى هذا الاسم.

2. **تكوين المسار الافتراضي:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

يحدد المسار الافتراضي عنوان IP للعبارة (192.168.1.1) الذي يرسل إليه FWSM جميع حزم IP التي لا يحتوي على مسار متعلم أو ثابت. المسار الافتراضي هو ببساطة مسار ثابت مع 0/0.0.0.0 كعنوان IP للوجهة. تكون للمسارات التي تحدد وجهة معينة الأولوية على المسار الافتراضي.

3. يترجم **Dynamic NAT** مجموعة من العناوين الحقيقية (24/10.1.1.0) إلى تجمع من يخطط عنوان (192.168.1.20-192.168.1.50) أن يكون routable على الشبكة الوجهة. يمكن أن يتضمن التجمع المعين عناوين أقل من المجموعة الحقيقية. عندما مضيف أنت تريد أن يترجم ينفذ الشبكة غاية، ال FWSM يعين هو عنوان من ال يخطط بركة. تتم إضافة الترجمة فقط عندما يقوم المضيف الحقيقي بتهيئة الاتصال. تكون الترجمة موجودة فقط لمدة الاتصال، ولا يحتفظ المستخدم المعين بنفس عنوان IP بعد انتهاء مهلة الترجمة.

```
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0
access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
access-group Internet in interface inside
```

تحتاج إلى إنشاء قائمة تحكم في الوصول (ACL) لرفض حركة المرور من الشبكة الداخلية 24/10.1.1.0 للانتقال إلى شبكة 192.168.2.0) DMZ1) والسماح بالأنواع الأخرى لحركة المرور إلى الإنترنت من خلال تطبيق *إنترنت* قائمة التحكم في الوصول (ACL) إلى الواجهة الداخلية كإتجاه داخلي لحركة المرور الواردة.

4. **nat ساكن إستاتيكي** يخلق ترجمة ثابتة من عنوان (عناوين) حقيقي إلى يخطط عنوان (عناوين).مع NAT حركي و PAT، كل مضيف يستعمل عنوان مختلف أو ميناء لكل ترجمة تالية. لأن ال يخطط عنوان ال نفس ل كل اتصال متتابع مع ساكن إستاتيكي nat، وقاعدة ترجمة مستمرة يتواجد، ساكن إستاتيكي nat يسمح مضيف على الغاية شبكة أن يبدأ حركة مرور إلى يترجم مضيف، إن هناك يكون منفذ قائمة أن يسمح هو.الفرق الرئيسي بين NAT الديناميكي ونطاق من العناوين ل NAT ساكن إستاتيكي أن NAT يسمح مضيف بعيد ببدء اتصال بمضيف مترجم، إن هناك قائمة وصول أن يسمح هو، بينما لا يسمح حركي nat. أنت تحتاج أيضا عدد متساو من العناوين المعينة كعناوين حقيقية مع ساكن إستاتيكي nat.

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
access-list outside extended permit tcp any host 192.168.1.10 eq http
access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
status
access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000
access-group outside in interface outside
```

هذا إثنان ساكن إستاتيكي nat بيان. الأولى تعني ترجمة IP الحقيقي 192.168.2.2 على الواجهة الداخلية إلى 192.168.1.6 IP المعين على الشبكة الفرعية الخارجية شريطة أن تسمح قائمة التحكم في الوصول بحركة المرور من المصدر 192.168.1.30 إلى 192.168.1.6 IP المعين للوصول إلى خادم WebSense في شبكة DMZ1. وبالمثل، فإن جملة NAT الثابتة الثانية تعني ترجمة IP الحقيقي 192.168.3.2 على الواجهة الداخلية إلى 192.168.1.10 IP المعين على الشبكة الفرعية الخارجية تنص على أن قائمة التحكم في الوصول تسمح بحركة المرور من الإنترنت إلى 192.168.1.10 IP المخطط له للوصول إلى خادم الويب في شبكة DMZ2 والحصول على رقم منفذ UDP في النطاق 8766 إلى 3000.
يعين الأمر **url-server** الخادم الذي يشغل تطبيق تصفية WebSense URL. الحد هو 16 خادم عنوان 5URL. في وضع سياق واحد وأربعة خوادم عنوان URL في الوضع المتعدد، ولكن يمكنك إستخدام تطبيق واحد فقط، إما N2H2 أو WebSense، في وقت واحد. بالإضافة إلى ذلك، إذا قمت بتغيير التكوين الخاص بك على جهاز الأمان، فهذا لا يعمل على تحديث التكوين على خادم التطبيق. يجب أن يتم ذلك بشكل منفصل، وفقا لتعليمات المورد.يجب تكوين الأمر **url-server** قبل إصدار الأمر **filter** ل HTTPS و FTP. إذا تمت إزالة كافة خوادم URL من قائمة الخادم، فسيتم أيضا إزالة كافة أوامر التصفية المتعلقة بتصفية URL.بمجرد أن تقوم بتعيين الخادم، قم بتمكين خدمة تصفية URL باستخدام الأمر **filter url**.

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1
connections 5
```

يسمح الأمر **filter url** بمنع وصول المستخدمين الخارجيين من عناوين URL الخاصة ب World Wide Web التي تقوم بتعيينها باستخدام تطبيق تصفية WebSense.

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

تكوين FWSM

```
Output Suppressed interface vlan 20 nameif outside ---!
  security-level 0 ip address 192.168.1.2 255.255.255.0
  interface vlan 10 nameif inside security-level 100 ip
address 10.1.1.1 255.255.255.0 interface vlan 15 nameif
         dmz1 security-level 60 ip address 192.168.2.1
255.255.255.224 interface vlan 25 nameif dmz2 security-
 level 50 ip address 192.168.3.1 255.255.255.224 passwd
     fl0wer enable password treeh0u$e route outside 0 0
   192.168.1.1 1 url-server (dmz1) vendor websense host
         192.168.2.2 timeout 30 protocol TCP version 1
connections 5 url-cache dst 128 filter url http 10.1.1.0
255.255.255.0 0 0 !--- When inside users access an HTTP
   server, FWSM consults with a !--- Websense server in
      order to determine if the traffic is allowed. nat
   (inside) 1 10.1.1.0 255.255.255.0 global (outside) 1
   192.168.1.20-192.168.1.50 netmask 255.255.255.0 !---
   Dynamic NAT for inside users that access the Internet
```

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask
255.255.255.255 !--- A host on the subnet 192.168.1.0/24
requires access to the Websense !--- server for
management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask
255.255.255.255 !--- A host on the Internet requires
access to the Webserver, so the Webserver !--- uses a
static translation for its private address. access-list
Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any access-
group Internet in interface inside !--- Allows all
inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1 access-list
outside extended permit tcp any host 192.168.1.10 eq
http !--- Allows the traffic from the internet with the
destination IP address !--- 192.168.1.10 and destination
port 80 access-list outside extended permit tcp host
192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-
list outside extended permit udp host 192.168.1.30 host
192.168.1.6 eq pcanywhere-status !--- Allows the
management host 192.168.1.30 to use !--- pcAnywhere on
the Websense server access-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. access-
group outside in interface outside access-list WEBSENSE
extended permit tcp host 192.168.2.2 any eq http access-
group WEBSENSE in interface dmz1 !--- The Websense
server needs to access the Websense !--- updater server
on the outside. !--- Output Suppressed
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

1. عرض معلومات الوحدة النمطية وفقا لنظام التشغيل الخاص بك للتحقق من أن المحول يعترف بنظام التشغيل FWSM وأنه أتى به عبر الإنترنت:برنامج IOS من Cisco:

```
Router#show module
 .Mod Ports Card Type                              Model              Serial No
----------- ------------------ ---------------------------------------- ----- ---
Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y  2     1
port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619 48  48    2
Intrusion Detection System             WS-X6381-IDS       SAD04250KV5  2     3
Firewall Module                        WS-SVC-FWM-1       SAD062302U4  6     4
```

برامج Catalyst OS:

```
[Console>show module [mod-num
:The following is sample output from the show module command

                                                    Console> show module
Mod Slot Ports Module-Type              Model                Sub Status
------ --- ------------------ ------------------------ ----- ---- ---
    1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok     2    1   1
    Multilayer Switch Feature WS-F6K-MSFC         no  ok     1    1  15
    Intrusion Detection Syste WS-X6381-IDS        no  ok     2    4   4
    Firewall Module           WS-SVC-FWM-1        no  ok     6    5   5
```

```
1000BaseX Ethernet       WS-X6408-GBIC       no  ok     8    6   6
```

ملاحظة: يعرض الأمر **show module** ستة منافذ ل FWSM. هذا ميناء داخلي أن يكون جمعت معا كEtherChannel.

2.
```
Router#show firewall vlan-group
                    Group vlans
                    ------ -----
                 10,15,20 1
                   70-85 51
                     100 52
```

3.
```
Router#show firewall module
          Module Vlan-groups
                 1,51    5
                 1,52    8
```

4. أدخل الأمر لنظام التشغيل الخاص بك لعرض قسم التمهيد الحالي:برنامج IOS من Cisco:
```
[Router#show boot device [mod_num
```

مثال:
```
Router#show boot device
                    :[ mod:1]
                    :[ mod:2]
                    :[ mod:3]
                mod:4 ]: cf:4]
                mod:5 ]: cf:4]
                    :[ mod:6]
                mod:7 ]: cf:4]
                    :[ mod:8]
                    :[ mod:9]
```

برامج Catalyst OS:
```
Console> (enable) show boot device mod_num
```

مثال:
```
Console> (enable) show boot device 6
Device BOOT variable = cf:5
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. **إعداد قسم التمهيد الافتراضي**— بشكل افتراضي، يتم تمهيد FWSM من قسم التطبيق **cf:4**. ولكن، يمكنك إختيار التمهيد من قسم التطبيق **cf:5** أو إلى قسم الصيانة **cf:1**. لتغيير قسم التمهيد الافتراضي، أدخل الأمر لنظام التشغيل الخاص بك:برنامج IOS من Cisco:
```
Router(config)#boot device module mod_num cf:n
```

حيث n هو 1 (الصيانة) أو 4 (التطبيق) أو 5 (التطبيق).برامج Catalyst OS:
```
Console> (enable) set boot device cf:n mod_num
```

حيث n هو 1 (الصيانة) أو 4 (التطبيق) أو 5 (التطبيق).

2. **إعادة ضبط FWSM في برنامج Cisco IOS Software**—لإعادة ضبط FWSM، أدخل الأمر كما هو موضح:
```
[Router#hw-module module mod_num reset [cf:n] [mem-test-full
```

والوسيطة **cf:n** هي القسم، إما 1 (صيانة) أو 4 (تطبيق) أو 5 (تطبيق). إذا لم تحدد القسم، سيتم إستخدام القسم الافتراضي، وهو عادة **cf:4**.يعمل خيار **إختبار** الذاكرة **الكاملة**" على إختبار الذاكرة الكامل، والذي يستغرق

ست دقائق تقريبا.**مثال:**

```
Router#hw-mod module 9 reset
Proceed with reload of module? [confirm] y
reset issued for module 9 %
#Router
SNMP-5-MODULETRAP:Module 9 [Down] Trap%:00:26:55
... SP:The PC in slot 8 is shutting down. Please wait:00:26:55
```

لبرامج **Catalyst OS**:

```
[Console> (enable) reset mod_num [cf:n
```

حيث **cf:n** هو القسم، إما 1 (صيانة) أو 4 (تطبيق) أو 5 (تطبيق). إذا لم تحدد القسم، سيتم إستخدام القسم الافتراضي، وهو عادة **cf:4**.

ملاحظة: لا يمكن تكوين NTP على FWSM، لأنه يأخذ إعداداته من المحول.

مشكلة: يعجز أن يمر ال VLAN حركة مرور من FWSM إلى ال ips مستشعر 4270

أنت يعجز أن يمر الحركة مرور من FWSM إلى ال ips جهاز إستشعار.

الحل

من أجل فرض حركة المرور عبر بروتوكول الإنترنت (IPS)، تتمثل الخدعة في إنشاء شبكة محلية ظاهرية (VLAN) إضافية من أجل تقسيم إحدى شبكات VLAN الحالية لديك بشكل فعال إلى شبكتين ثم ربطها معا. فحصت هذا مثال مع VLAN 401 و in order to 501 أوضحت:

- إن يريد أنت أن يمسح حركة مرور على **VLAN** رئيسي 401، خلقت آخر **501** VLAN (كثير VLAN). بعد ذلك أعجزت ال VLAN قارن 401، أي المضيف في 401 يستعمل حاليا كمدخل تقصير.
- بعد ذلك يمكن 501 VLAN قارن مع *ال نفسه* عنوان أن أنت سابقا أعجزت على ال 401 VLAN قارن.
- وضعت واحد من ال ips قارن في 401 VLAN والآخر في 501 VLAN.

كل أنت ينبغي أن يعمل أن ينقل التقصير مدخل ل 401 VLAN إلى 501 VLAN. أنت تحتاج أن يتم ال نفسه تغير ل VLANs إن يتواجد. لاحظ أن شبكات VLAN هي أساسا مثل مقاطع شبكة LAN. يمكنك الحصول على بوابة افتراضية على قطعة سلك مختلفة عن البيئات المضيفة التي تستخدمها.

إصدار الحزم الخارجة عن الترتيب في FWSM

كيف يستطيع أنا أحل ال خارج الترتيب ربط إصدار في FWSM؟

الحل

قم بإصدار الأمر sysopt np completion-unit في وضع التكوين العام لحل مشكلة الحزمة التي خارج الترتيب في FWSM. تم إدخال هذا الأمر في الإصدار 3.2(5) من FWSM ويضمن إعادة توجيه الحزم بنفس الترتيب الذي تم استقبالها به.

المشكلة: تعذر تمرير الحزم الموجهة غير المتماثلة عبر جدار الحماية

لا يمكنك تمرير الحزم الموجهة بشكل غير متناسق من خلال جدار الحماية.

الحل

قم بإصدار الأمر set connection advanced-options tcp-state-bypass في وضع تكوين الفئة لاجتياز الحزم الموجهة بشكل غير متناسق عبر جدار الحماية. تم إدخال هذا الأمر في الإصدار 3.2(1) من FWSM.

دعم NetFlow في FWSM

هل يدعم FWSM Netflow؟

الحل

NetFlow غير مدعوم في FWSM.

معلومات ذات صلة

- صفحة دعم الوحدة النمطية لخدمات جدار الحماية Cisco Catalyst 6500 Series Firewall Services Module Support Page
- صفحة دعم المحولات Cisco Catalyst 6500 Series Switches
- صفحة دعم موجه السلسلة 7600 من Cisco
- شرح اعتراض FWSM TCP وملفات تعريف إرتباط SYN
- الدعم التقني والمستندات - Cisco Systems

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).