تثبيت وحدة SFR النمطية على وحدة ASA 5585-X Hardware Module

المحتويات

المقدمة

توفر الوحدة النمطية ASA FirePOWER، المعروفة أيضا باسم ASA SFR، خدمات جدار الحماية وإمكانية الرؤية والتطبيقات (NGIPS) IPS من الجيل التالي، بما في ذلك الجيل التالي من البرامج الضارة (AMP). يمكنك تصفية عنوان URL والحماية المتقدمة من البرامج الضارة (AMP) والتحكم (AVC) في وضع سياق واحد أو متعدد، وفي الوضع الموجه أو الشفاف. إستخدام الوحدة النمطية
يصف هذا المستند المتطلبات الأساسية وعمليات التثبيت لوحدة FirePOWER (SFR) على وحدة الأجهزة ASA 5585-X. كما يوفر الخطوات اللازمة لتسجيل وحدة SFR باستخدام مركز إدارة FireSIGHT.

ملاحظة: توجد خدمات FirePOWER (SFR) على وحدة أجهزة في ASA 5585-X، بينما يتم تثبيت خدمات FirePOWER على سلسلة ASA 5512-X حتى 5555-X على وحدة برمجية، مما ينتج عنه إختلافات في عمليات التثبيت.

المتطلبات الأساسية

المتطلبات

تتطلب التعليمات الموجودة على هذا المستند الوصول إلى وضع EXEC ذي الامتيازات. أدخل

اطغض ،رورم ةملك نييعت متي مل اذإ .تازايتمالا يذ EXEC عضو ىلإ لوصولل enable رمألا
.طقف Enter لاخدإلا حاتفم ىلع

<#root>

```
ciscoasa>

enable

Password:
ciscoasa#
```

:ةيلاتلا تانوكملا رفوت مزلي ،ASA ىلع FirePOWER تامدخ تيبثت لجأ نم

- ثدحأ رادصإ وأ 9.2.2 رادصإلا ASA جمانرب
- يساسألا ماظنلا ASA 5585-X
- FirePOWER ةيطمنلا ةدحولا ةرادإ ةهجاو ةطساوب TFTP مداخ ىلإ لوصولا نكمي
- ثدحأ رادصإ وأ 5.3.1 رادصإلا عم FireSIGHT Management Center

ةئيب يف ةدوجوملا ةزهجألا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ متي :ةظحالم
حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب .ةصاخ ةيلمعم
.رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش تناك اذإ .(يضارتفا)

نيوكتلا

ءدبلا لبق

كيدل ناك اذإف ،ASA 5585-X لكيه يف نيتحتفلا ىدحإ امئاد لغشت ةركاذ نأل ارظن ASA SSM
AIP-SSM وأ SSP-CX (Context Aware) لثم SSP (SFR) FirePOWER تامدخ ريغ ىرخأ ةزهجأ ةدحو
(Advanced Inspection and Prevention Security)، بجيف ةلازإ تيبثت ةدحولا ىرخألا ريفوتل
فاقيإلل يلاتلا رمألا ليغشتب مق ،زاهجلل ةيطمن ةدحو ةلازإ لبق .SSP-SFR ل ةحاسم
:ةيطمن ةدحو ليغشت

<#root>

```
ciscoasa#

hw-module module 1 shutdown
```

ةرادإلاو تالباكلا

- ASA مكحت ةدحو ربع ةيطمنلا SFR ةدحول يلسلستلا ذفنملا ىلإ لوصولا كنكمي ال
.ASA 5585-X ىلع
- رمألا مادختساب يلصنلا مداخلا يف لمعلا ةسلج كنكمي ،SFR ةدحو ريفوت درجمب

session 1.

- يجب أن تعدت بشكل كامل ال SFR وحدة نمطية على ASA 5585-X، in order to استعملت الإدارة إثرنيت قارن و وحدة طرفية للتحكم جلسة على التسلسل إدارة وحدة طرفية وحدة نمطية و فصل من ال ASA إدارة قارن وحدة طرفية وحدة نمطية على ال SFR، أي يكون ميناء للتحكم.

ملحوظة: للعثور على حالة وحدة نمطية على ASA، قم بتشغيل الأمر show module 1 details" الذي يسترجع عنوان IP الخاص بإدارة وحدة SFR ومركز الدفاع المقترن.

تثبيت الوحدة النمطية FirePOWER (SFR) على ASA

1. قم بتنزيل صورة تمهيد تشغيل وحدة ASA FirePOWER SFR الأولية من Cisco.com إلى خادم TFTP يمكن الوصول إليه من واجهة إدارة ASA FirePOWER. يجب أن يكون اسم الصورة مثل asasfr-boot-5.3.1-152.img"

2. قم بتنزيل برنامج ASA FirePOWER System من Cisco.com إلى خادم HTTP أو HTTPS أو FTP يمكن الوصول إليه من واجهة إدارة ASA FirePOWER.

3. إعادة تشغيل وحدة SFR

الخيار 1: إن ال يتلقى أنت الكلمة إلى ال SFR وحدة نمطية، أنت يستطيع أصدرت التالي أمر من ال ASA لإعادة تمهيد الوحدة النمطية.

```
<#root>

ciscoasa#

hw-module module 1 reload


Reload module 1? [confirm]
Reload issued for module 1
```

الخيار 2: إذا كانت لديك كلمة المرور إلى وحدة SFR، فيمكنك إعادة تمهيد المستشعر مباشرة من سطر الأوامر الخاص به.

```
<#root>

Sourcefire3D login:

admin


Password:

Sourcefire Linux OS v5.3.1 (build 43)
```

```
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

>

system reboot
```

4. مقاطعة عملية تمهيد وحدة SFR باستخدام ESCAPE أو تسلسل الانكسار لبرنامج جلسة عمل المحطة الطرفية لوضع الوحدة النمطية في ROMMON.

```
The system is restarting...
CISCO SYSTEMS
Embedded BIOS Version 2.0(14)1 15:16:31 01/25/14

Cisco Systems ROMMON Version (2.0(14)1) #0: Sat Jan 25 16:44:38 CST 2014

Platform ASA 5585-X FirePOWER SSP-10, 8GE

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 8 seconds.

Boot interrupted.

Management0/0
Link is UP
MAC Address: xxxx.xxxx.xxxx

Use ? for help.

rommon #0>
```

5. قم بتكوين واجهة إدارة وحدة SFR باستخدام عنوان IP وحدد موقع خادم TFTP ومسار TFTP إلى صورة برنامج تمهيد تشغيل الكمبيوتر (BOOTSTRAP). أدخل الأوامر التالية لتعيين عنوان IP على الواجهة واسترداد صورة TFTP:

- مجموعة
- العنوان = ك_ip_address
- البوابة = your_gateway
- الخادم = your_tftp_server
- image = your_tftp_filepath
- تزامن
- tftp

! مثال على معلومات عنوان IP المستخدمة. تحديث لبيئتك.

<#root>

```
rommon #1>
ADDRESS=198.51.100.3

rommon #2>
GATEWAY=198.51.100.1

rommon #3>
SERVER=198.51.100.100

rommon #4>
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img

rommon #5>
sync

Updating NVRAM Parameters...

rommon #6>
tftp

ROMMON Variable Settings:
ADDRESS=198.51.100.3
SERVER=198.51.100.100
GATEWAY=198.51.100.1
PORT=Management0/0
VLAN=untagged
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp /tftpboot/asasfr-boot-5.3.1-152.img@198.51.100.100 via 198.51.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<truncated output>

Received 41235627 bytes

Launching TFTP Image...

Execute image at 0x14000
```

6. تسجيل الدخول إلى صورة التمهيد الأولية. تسجيل الدخول كمسؤول ومع كلمة المرور admin123

```
<#root>

Cisco ASA SFR Boot Image 5.3.1

asasfr login:

admin

Password:

Cisco ASA SFR Boot 5.3.1 (152)
   Type ? for list of commands
```

7. أستخدم صورة التمهيد الأولية لتكوين عنوان IP على واجهة إدارة الوحدة النمطية. أدخل أمر الإعداد لإدخال المعالج. يطلب منك تقديم المعلومات التالية:

- اسم المضيف: ما يصل إلى 65 حرفا وقيمة، لا توجد مسافات. الوصلات مسموح بها.
- عنوان الشبكة: يمكنك ضبط عناوين IPv4 وأ IPv6 الثابتة، وأ إستخدام DHCP (ل IPv4) وأ التكوين التلقائي عديم الحالة ل IPv6.
- معلومات DNS: يجب تحديد خادم DNS واحد على الأقل، كما يمكنك تعيين اسم المجال ومجال البحث.
- معلومات NTP: يمكنك تمكين NTP وتكوين خوادم NTP، لإعداد وقت النظام.

مثال المعلومات المستخدمة. تحديث لبيئتك !

```
<#root>

asasfr-boot>

setup


        Welcome to SFR Setup
    [hit Ctrl-C to abort]
Default values are inside []

  Enter a hostname [asasfr]:

sfr-module-5585

Do you want to configure IPv4 address on management interface?(y/n) [Y]:

Y
```

Do you want to enable DHCP for IPv4 address on management interface?(y/n) [N]:

N

Enter an IPv4 address [192.168.8.8]:

198.51.100.3

Enter the netmask [255.255.255.0]:

255.255.255.0

Enter the gateway [192.168.8.1]:

198.51.100.1

Do you want to configure static IPv6 address on management interface?(y/n) [N]:

N

Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address:

198.51.100.15

Do you want to configure Secondary DNS Server? (y/n) [n]:

N

Do you want to configure Local Domain Name? (y/n) [n]:

N

Do you want to configure Search domains? (y/n) [n]:

N

Do you want to enable the NTP service? [Y]:

N

Please review the final configuration:
Hostname: sfr-module-5585
Management Interface Configuration

IPv4 Configuration: static
IP Address:

198.51.100.3

Netmask:

255.255.255.0

```
Gateway:
198.51.100.1

IPv6 Configuration:     Stateless autoconfiguration

DNS Configuration:
DNS Server:
198.51.100.15

Apply the changes?(y,n) [Y]:
Y

Configuration saved successfully!
Applying...
Restarting network services...
Restarting NTP service...
Done.
```

8. أستخدم صورة التمهيد لسحب صورة برنامج النظام وتثبيتها باستخدام الأمر install system. قم بتضمين خيار عدم التأكيد إذا كنت لا تريد الاستجابة إلى رسائل التأكيد. استبدل ال url الكلمة المفتاح مع مكان .pkg مربد.

<#root>

```
asasfr-boot>
system install [noconfirm]
url
```

على سبيل المثال,

<#root>

```
>
system install http://Server_IP_Address/asasfr-sys-5.3.1-152.pkg

Verifying
Downloading
Extracting

Package Detail
Description:                    Cisco ASA-SFR 5.3.1-152 System Install
Requires reboot:                Yes
```

```
Do you want to continue with upgrade? [y]:
```

Y

```
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image ...
```

ملاحظة: عند اكتمال التثبيت في مدة تتراوح من 20 إلى 30 دقيقة، ستتم مطالبتك بالضغط على مفتاح Enter لإعادة التشغيل. اسمح لمدة 10 دقائق أو أكثر لتثبيت مكون التطبيق وبدء تشغيل خدمات FirePOWER الخاصة ب ASA. يجب أن يعرض إخراج تفاصيل العرض الوحدة النمطية 1 جميع العمليات ك up.

حالة الوحدة النمطية أثناء التثبيت

<#root>

```
ciscoasa#
```

show module 1 details

```
Getting details from the Service Module, please wait...
Unable to read details from module 1

Card Type:          ASA 5585-X FirePOWER SSP-10, 8GE
Model:              ASA5585-SSP-SFR10
Hardware version:   1.0
Serial Number:      JAD18400028
Firmware version:   2.0(14)1
Software version:   5.3.1-152
MAC Address Range:  58f3.9ca0.1190 to 58f3.9ca0.119b
App. name:          ASA FirePOWER
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       5.3.1-152
Data Plane Status:
```

Not Applicable

```
Console session:
```

Not ready

```
Status:
```

Unresponsiv

```
e
```

حالة الوحدة النمطية بعد التثبيت النهائي

```
<#root>

ciscoasa#

show module 1 details


Getting details from the Service Module, please wait...

   Card Type:          ASA 5585-X FirePOWER SSP-10, 8GE
                 Model:              ASA5585-SSP-SFR10
                               Hardware version:   1.0
                          Serial Number:      JAD18400028
                             Firmware version:   2.0(14)1
                            Software version:   5.3.1-152
   MAC Address Range:  58f3.9ca0.1190 to 58f3.9ca0.119b
                       App. name:          ASA FirePOWER
                                App. Status:        Up
                     App. Status Desc:   Normal Operation
                           App. version:       5.3.1-152
                                        Data Plane Status:

                                        Up


                                        Console session:

                                        Ready


                                        Status:

                                        Up


DC addr:            No DC Configured
Mgmt IP addr:       192.168.45.45
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       0.0.0.0
Mgmt web ports:     443
                                    Mgmt TLS enabled:   true
```

التكوين

تكوين برنامج FirePOWER

1. يمكنك الاتصال بوحدة ASA 5585-X FirePOWER من خلال أحد المنافذ الخارجية التالية:
   - منفذ وحدة تحكم ASA FirePOWER
   - SSH باستخدام واجهة ASA FirePOWER Management 1/0

ملاحظة: لا يمكنك الوصول إلى واجهة سطر الأوامر لوحدة جهاز ASA FirePOWER النمطية عبر اللوحة الخلفية ASA باستخدام الأمر session sfr.

2. بعد الوصول إلى الوحدة النمطية FirePOWER عبر وحدة التحكم، سجل الدخول باستخدام اسم المستخدم وكلمة المرور Sourcefire.

```
<#root>

Sourcefire3D login:

admin


Password:

Last login: Fri Jan 30 14:00:51 UTC 2015 on ttyS0

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a registered
  trademark of Sourcefire, Inc. All other trademarks are property of their respective
                                                                          owners.

                                        Sourcefire Linux OS v5.3.1 (build 43)
                                    Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

                                     Last login: Wed Feb 18 14:22:19 on ttyS0

                          System initialization in progress.  Please stand by.
                                You must configure the network to continue.
                              You must configure at least one of IPv4 or IPv6.
                                 Do you want to configure IPv4? (y/n) [y]:

y


                                 Do you want to configure IPv6? (y/n) [n]:

n


                       Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

dhcp


                  If your networking information has changed, you will need to reconnect.
                                [1640209.830367] ADDRCONF(NETDEV_UP): eth0: link is not ready
[1640212.873978] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
                             [1640212.966250] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
                               For HTTP Proxy configuration, run 'configure network http-proxy'

  This sensor must be managed by a Defense Center.  A unique alphanumeric registration
     key is always required.  In most cases, to register a sensor to a Defense Center,
      you must provide the hostname or the IP address along with the registration key.
                  'configure manager add [hostname | ip address ] [registration key ]'

       However, if the sensor and the Defense Center are separated by a NAT device, you
         must enter a unique NAT ID, along with the unique registration key. 'configure
                                 manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.

>
```

تكوين مركز إدارة FireSIGHT

بعد تثبيت برنامج وحدة FirePOWER على ASA وتسجيلها مع مركز إدارة FireSIGHT، يجب عليك استخدام FireSIGHT Management Center لتكوين ما يلي:

- لا يمكنك تكوين واجهات ASA FirePOWER.
- لا يمكنك إيقاف تشغيل أو إعادة تشغيل أو إيقاف تشغيل عمليات ASA FirePOWER بطريقة أخرى.
- لا يمكنك إنشاء نسخة احتياطية من أجهزة ASA FirePOWER أو استعادتها.
- لا يمكنك كتابة قواعد التحكم في الوصول لمطابقة حركة المرور باستخدام شروط علامة VLAN.

إعادة توجيه حركة المرور إلى وحدة SFR

يمكنك إعادة توجيه حركة المرور إلى وحدة FirePOWER الخاصة ب ASA عن طريق إنشاء سياسة خدمة تحدد حركة مرور معينة. من أجل إعادة توجيه حركة المرور إلى وحدة FirePOWER، اتبع الخطوات التالية:

الخطوة 1: حدد حركة مرور البيانات

أولا، حدد حركة المرور باستخدام الأمر access-list. في المثال التالي، يقوم بإعادة توجيه حركة مرور البيانات من جميع الواجهات. يمكنك أيضا القيام بذلك بالنسبة لحركة مرور معينة.

```
<#root>

ciscoasa(config)#

access-list sfr_redirect extended permit ip any any
```

الخطوة 2: مطابقة حركة المرور

يوضح المثال التالي كيفية إنشاء خريطة فئة ومطابقة حركة مرور البيانات على قائمة الوصول:

```
<#root>

ciscoasa(config)#

class-map sfr
```

```
ciscoasa(config-cmap)#
match access-list sfr_redirect
```

الخطوة 3: تحديد الإجراء

يمكنك تكوين الجهاز إما في عملية نشر خاملة ("monitor-only") أو داخل السطر. أنت تستطيع. يسمح الـ ASA على وقت في نفس الأسلوب داخلي وأسلوب مدرب سواء في حد على يشكل ال بنوع واحد فقط من نهج الأمان.

الوضع الداخلي

يتم أخرى إجراءات أي اتخاذ فيها بوغرمل ريغ رورملا ةكرح طاقسإ دعب ،نمضملا رشنلا يف لقنلاو ةجلاعملا نم ديزمل ASA ىلإ رورملا ةكرح عاجرإ متي ،ةسايسلا ةطساوب اهقيبطت ةيطمنلا ةدحولا نيوكتو ةسايس ةطيرخ ءاشنإ ةيفيك يلاتلا لاثملا حضوي .يئاهنلا FirePOWER يف عضولا نمضملا:

<#root>

```
ciscoasa(config)#
policy-map global_policy
```

```
ciscoasa(config-pmap)#
class sfr
```

```
ciscoasa(config-pmap-c)#
sfr fail-open
```

الوضع الخامل

في عملية نشر سلبية،

- يتم إرسال نسخة من حركة المرور إلى الجهاز، ولكن لا يتم إرجاعها إلى ASA.
- يتيح لك الوضع السلبي عرض ما كان الجهاز سيقوم به لحركة المرور، ويتيح لك تقييم محتوى حركة المرور، دون التأثير على الشبكة.

إذا كنت ترغب في تكوين الوحدة النمطية FirePOWER في الوضع الخامل، فاستخدم الكلمة الأساسية monitor-only كما يلي. إن لا يتضمن أنت الكلمة المفتاح، الحركة مرور أرسلت في أسلوب داخل.

<#root>

```
ciscoasa(config-pmap-c)#
sfr fail-open
```

```
monitor-only
```

الخطوة 4: تحديد الموقع

الخطوة الأخيرة هي تطبيق السياسة. يمكنك تطبيق سياسة بشكل عام أو على واجهة. يمكنك تجاوز السياسة العامة على واجهة بتطبيق سياسة خدمة على تلك الواجهة.

تطبق الكلمة الأساسية global خريطة السياسة على جميع الواجهات، وتطبق الواجهة السياسة على واجهة واحدة فقط. في المثال التالي، يتم السماح بسياسة عمومية واحدة. يتم تطبيق السياسة بشكل عام:

```
<#root>

ciscoasa(config)#

service-policy global_policy global
```

تحذير: خريطة السياسة global_policy هي سياسة افتراضية. إذا كنت تستخدم هذه النهج وتريد إزالة هذا النهج على جهازك لغرض أستكشاف الأخطاء وإصلاحها، فتأكد من فهمك لمضمونه.

مستند ذو صلة

- تسجيل جهاز باستخدام FireSIGHT Management Center
- نشر FireSIGHT Management Center على VMware ESXi
- سيناريوهات تكوين إدارة IPS على الوحدة النمطية 5500-X IPS

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).