# يف مكحتلا دعاوق مادختساب ASA نيوكت ةيفصتل FirePOWER تامدخ ىلإ لوصولا ىلإ AnyConnect VPN ليمع رورم ةكرح تنرتنإلا

## المحتويات

<u>المقدمة</u> المتطلبات الأساسية المكونات المستخدمة المشكلة محمين ASA الحدة النمطية ASA FirePOWER المدارة بواسطة تكوين ASDM وحدة ASDM النمطية المدارة بواسطة تكوين FMC <u>نتيجة</u>

## المقدمة

يصف هذا المستند كيفية تكوين قواعد سياسة التحكم في الوصول (ACP) لفحص حركة المرور التي تأتي من أنفاق الشبكة الخاصة الظاهرية (VPN) أو مستخدمي الوصول عن بعد (RA) واستخدام جهاز الأمان القابل للتكيف (ASA) من Cisco مع خدمات FirePOWER كبوابة إنترنت.

## المتطلبات الأساسية

#### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد و/أو الشبكة الخاصة الظاهرية (VPN) لشبكة IPSec التي تعمل بنظام النظير إلى النظير.
  - تكوين قائمة التحكم في الوصول (ACP) Firepower.
    - إطار عمل السياسة النمطية ASA (MPF).

#### المكونات المستخدمة

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

- ASA5506W الإصدار 2.7)9.6 الإصدار ASDM •
- الإصدار 6.1.0 330 من وحدة FirePOWER النمطية لمثال ASDM.
  - ASA5506W الإصدار 1)9.7 المثال FMC.
  - إصدار FirePOWER 6. 2. 0 من أجل مثال FMC.

• مركز إدارة Firepower (FMC)، الإصدار 6.2.0

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## المشكلة

يتعذر على ASA5500-X مع خدمات FirePOWER تصفية حركة مرور مستخدمي AnyConnect و/أو فحصها مثل حركة المرور التي يتم الحصول عليها من مواقع أخرى متصلة بأنفاق IPSec التي تستخدم نقطة واحدة من أمان المحتوى الأساسي.

من الأعراض الأخرى التي يغطيها هذا الحل عدم القدرة على تحديد قواعد معينة ل ACP للمصادر المذكورة دون ظهور مصادر أخرى.

هذا السيناريو شائع جدا لمعرفة متى يتم إستخدام تصميم TunneIAII لحلول VPN التي يتم إنهاؤها على ASA.

## الحل

ويمكن تحقيق ذلك بطرق متعددة. بيد أن هذا السيناريو يشمل التفتيش حسب المناطق.

### تکوین ASA

الخطوة 1. حدد الواجهات التي يتصل فيها مستخدمو AnyConnect أو أنفاق VPN ب ASA.

أنفاق نظير إلى نظير

هذه خردة لمخرج **خريطة تشفير تشغيل العرض**.

crypto map outside\_map interface **outside** 

مستخدمو AnyConnect

يظهر الأمر **show run webVPN** مكان تمكين الوصول إلى AnyConnect.

webvpn enable **outside** hostscan image disk0:/hostscan\_4.3.05019-k9.pkg hostscan enable anyconnect image disk0:/anyconnect-win-4.4.01054-webdeploy-k9.pkg 1 anyconnect image disk0:/anyconnect-macos-4.4.01054-webdeploy-k9.pkg 2 anyconnect enable **في هذا السيناريو، تستقبل الواجهة الخارجية**، كلا، مستخدمي RA وأنفاق نظير إلى نظير.

الخطوة 2. قم بإعادة توجيه حركة المرور من ASA إلى وحدة FirePOWER باستخدام سياسة عامة.

يمكن القيام بذلك باستخدام **تطابق أي** شرط أو قائمة تحكم في الوصول (ACL) معرفة لإعادة توجيه حركة المرور.

مثال مع **مطابقة أي** تطابق.

class-map SFR match any policy-map global\_policy class SFR sfr fail-open service-policy global\_policy global otil على مطابقة قائمة التحكم في الوصول (ACL). access-list sfr-acl extended permit ip any any class-map SFR match access-list sfr-acl policy-map global\_policy class SFR sfr fail-open

service-policy global\_policy global في سيناريو أقل شيوعا، يمكن إستخدام سياسة خدمة للواجهة الخارجية. لا يتم تغطية هذا المثال في هذا المستند.

#### الوحدة النمطية ASA FirePOWER المدارة بواسطة تكوين ASDM

الخطوة 1. عينت القارن الخارجي منطقة واحدة في **التشكيل > ASA FirePOWER تشكيل > إدارة الجهاز**. في هذه الحالة، تلك المنطقة تسمى **خارج**.

○ ○ ○ Configuration > ASA FirePOWER Configuration > Device Management > Interfaces										
firepower ASA5506W	You have una	pplied changes								
Device Interfaces	1									
Name 🔺	Security Zones									
firepower		Ø								
🛃 guest		Ø								
inside	inside	Ø								
🛃 nlp_int_tap		Ø								
😿 outside	Edit Interface ? ×	Ø								
🛃 wifi	ASA	Ø								
	Security Zone: outside   Store ASA FirePOWER Changes Cancel									

الخطوة 2. حدد **إضافة قاعدة** في **التكوين > تكوين ASA FirePOWER > السياسات > سياسة التحكم في الوصول**.

الخطوة 3. من علامة التبويب مناطق، حدد خارج المنطقة كمصدر ووجهة للقاعدة الخاصة بك.

Add Ru	ıle												? ×
Name	me Remote VPN Policy			C Enabled			Insert	t above rule 🔽 1					
Zone	es Netv	vorks	🔺 Users	Application	s Ports	URLs	SGT/ISE Attributes			[	Inspection	Logging	Comments
Availab	le Zones	Ç				S	Source Zones (1)			Destinati	ion Zones (1	L)	
🔍 Sea	rch by nam	e					🥞 outside		i i	🥞 outsie	de		Ξ.
الله المراجع ال المراجع المراجع المراجع المراجع المراجع	n de out side				Add to Source Add to Destinat	2 2 Dion							
												Add	Cancel

الخطوة 4. حدد الإجراء والعنوان وأي شروط أخرى مرغوبة لتعريف هذه القاعدة.

يمكن إنشاء قواعد متعددة لتدفق حركة المرور هذا. من المهم فقط أن نضع في الاعتبار أن مناطق المصدر والوجهة يجب أن تكون المنطقة المخصصة لمصادر الشبكة الخاصة الظاهرية (VPN) والإنترنت.

تأكد من عدم وجود سياسات عامة أخرى يمكن أن تتطابق قبل هذه القواعد. من المفضل أن تكون هذه القواعد أعلى من تلك المحددة إلى **أي** منطقة.

الخطوة 5. انقر فوق **تغييرات ASA FirePOWER للتخزين** ثم **نشر تغييرات FirePOWER** لتدخل هذه التغييرات حيز التنفيذ.

#### وحدة ASA FirePOWER النمطية المدارة بواسطة تكوين FMC

الخطوة 1. تخصيص منطقة واحدة للواجهة الخارجية في **الأجهزة > الإدارة > الواجهات**. في هذه الحالة، تلك المنطقة تسمى **المنطقة الخارجية**.

ASA5506W		
Device Interfaces		
Name 🔺	Security Zones	
inside	Edit Interface ? >	¢
😥 outside	ASA	
	Security Zone: outside-zone	
	Save Cancel	

الخطوة 2. حدد **إضافة قاعدة** في **السياسات > التحكم في الوصول > تحرير**.

الخطوة 3. من علامة التبويب **مناطق**، حدد **المنطقة الخارجية** كمصدر ووجهة للقاعدة الخاصة بك.

Prefilt	er Policy: Defau	ult Prefilter Po	Add Ru	le											?	×	
Rule	s Security I	Intelligence	Name VPN Traffic			Z Enabled Inse			Insert	ert into Mandatory				~			
68 F	ilter by Device		Action	Allow			▼ ○ □ 2 t	6 <i>D</i>									
#	Name	Source Zones	Zone	s Networks	VLAN Tags	🔺 Users	Applications	Ports	URLs	SGT/ISE Attributes			Inspection	Logging	Comments		
			Availabl	e Zones  🖒				Source	Source Zones (1)				Destination Zones (1)				
Mandatory - FirePOWER Poli     Search by name						🧠 outside-zone			i	🥞 outside-zone			6	9			
There are no rules in this section. /			🧠 🔔 ir	1													
👻 Default - FirePOWER Policy (		🔒 insid	inside														
There are no rules in this section. J				Add to													
Default Action		Inside_cbarrien															
			🚔 Outside			Add to Destination	Add to Destination										
		🌏 outside-zone															
			👬 Outs	ide_cbarrien													
												Add	Cancel	)			

الخطوة 4. حدد الإجراء والعنوان وأي شروط أخرى مرغوبة لتعريف هذه القاعدة.

يمكن إنشاء قواعد متعددة لتدفق حركة المرور هذا. من المهم فقط أن نضع في الاعتبار أن مناطق المصدر والوجهة يجب أن تكون المنطقة المخصصة لمصادر الشبكة الخاصة الظاهرية (VPN) والإنترنت.

تأكد من عدم وجود سياسات عامة أخرى يمكن أن تتطابق قبل هذه القواعد. من المفضل أن تكون هذه القواعد أعلى من تلك المحددة إلى **أي** منطقة.

الخطوة 5. انقر فوق **حفظ** ثم **نشر** لتفعيل هذه التغييرات.

## نتيجة

بعد انتهاء النشر، تتم الآن تصفية/فحص حركة مرور AnyConnect بواسطة قواعد ACP المطبقة. في هذا المثال، تم حظر عنوان URL بنجاح.

# **Access Denied**

You are attempting to access a forbidden site.

Consult your system administrator for details.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما