Comprendre l'extension des règles sur les périphériques FirePOWER

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Présentation du développement des règles
Extension d'une règle basée sur IP
Extension d'une règle basée sur IP à l'aide d'une URL personnalisée
Extension d'une règle basée sur IP à l'aide de ports
Extension d'une règle basée sur IP à l'aide de VLAN
Extension d'une règle basée sur IP avec des catégories d'URL
Extension d'une règle basée sur IP avec zones
Formule générale d'extension des règles
Dépannage d'un échec de déploiement dû à l'extension des règles
Informations connexes

Introduction

Ce document décrit la traduction des règles de contrôle d'accès vers le capteur lorsqu'elles sont déployées à partir de Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissances sur la configuration des politiques de contrôle d'accès sur FMC

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Firepower Management Center version 6.0.0 et ultérieure

- Image de défense pare-feu ASA (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) exécutant le logiciel version 6.0.1 et ultérieure
- Image SFR ASA Firepower (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5585-X) exécutant la version 6.0.0 et ultérieure du logiciel
- Capteur de la gamme Firepower 7000/8000 version 6.0.0 et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Une règle de contrôle d'accès est créée à l'aide d'une ou de plusieurs combinaisons de ces paramètres :

- Adresse IP (source et destination)
- Ports (source et destination)
- URL (catégories fournies par le système et URL personnalisées)
- Détecteurs d'applications
- Réseaux locaux virtuels (VLAN)
- Zones

En fonction de la combinaison des paramètres utilisés dans la règle d'accès, l'extension de la règle change sur le capteur. Ce document met en évidence diverses combinaisons de règles sur le FMC et leurs extensions respectives associées sur les capteurs.

Présentation du développement des règles

Extension d'une règle basée sur IP

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Acce	ss Control > Access Co	ontrol Network	Discovery App	lication Detectors	Correlation	Actions •								
Def Enter	Default Base Policy													
Ident Rule	ity Policy: <u>None</u> Security Intelligen	SSL Policy	r: <u>None</u> nses Advanced								Te In	heritance Settings	s 🗒 Policy Assign	ments (1)
db F	ilter by Device									O Add Cat	egory 🔘 Add Rul	e Search Rules		×
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action		
- P	landatory - Default Ba	se Policy (1-1)												
1	Rule-1	any	any	2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any	any	any	Allow	0000	J 🛙
v 0	efault - Default Base I	Policy (-)												
Ther	e are no rules in this sec	tion. Add Rule or Add	d Category											_
Defa	ult Action					_				Intrusion	Prevention: Balanced	d Security and Cor	nnectivity	\$ 📑

Il s'agit d'une règle unique sur le Management Center. Cependant, après son déploiement sur le capteur, il se développe en quatre règles, comme illustré dans l'image :

Lorsque vous déployez une règle avec deux sous-réseaux configurés comme source et deux hôtes configurés comme adresses de destination, cette règle est étendue à quatre règles sur le capteur.

Remarque : si l'accès doit être bloqué en fonction des réseaux de destination, il est préférable d'utiliser la fonctionnalité Listes de blocage sous Security Intelligence.

Extension d'une règle basée sur IP à l'aide d'une URL personnalisée

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Acces	is Control > Access C	ontrol Network	Discovery App	lication Detectors	Correlation	Actions •									
Def.	fault Base Policy														
Identi Rule	atity Policy: None SSL Policy: None Values Security Intelligence HTTP Responses Advanced														
itte F	Iter by Device Add Category & Add Rule Search Rules X														
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	🧿 🐚 🔳 🔹		
- M	andatory - Default Ba	se Policy (1-1)													
1	Rule-1	any	any	2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any	any	<pre>Ø facebook.com Ø twitter.com</pre>	Allow	0000	0	
👻 D	efault - Default Base	Policy (-)													
There	There are no rules in this section. Add Rule or Add Category														
Defa	ult Action									Intrusion	Prevention: Balanced	Security and Cor	inectivity 💙	\$ 1	

Il s'agit d'une règle unique sur le Management Center. Cependant, après son déploiement sur le capteur, il est développé en huit règles, comme illustré dans l'image :

268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (url "facebook 268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (url "twitter. 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (url "facebook 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (url "twitter. (log dcforward flowstart) (url "facebook 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (url "twitter. 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (url "facebook 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (url "twitter. 268435456 allow any any any any any any any any (ipspolicy 2)

Lorsque vous déployez une règle avec deux sous-réseaux configurés en tant que source, deux hôtes configurés en tant qu'adresses de destination et deux objets URL personnalisés dans une seule règle sur Management Center, cette règle est étendue à huit règles sur le capteur. Cela signifie que pour chaque catégorie d'URL personnalisée, il existe une combinaison de plages

IP/port source et de destination, qui sont configurées et créées.

Extension d'une règle basée sur IP à l'aide de ports

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Acces	is Control ► Access C	ontrol Network	Discovery App	lication Detectors	Correlation	Actions •								
Defa Enter a	Nefault Base Policy													
Identi	Intity Policy: None SSL Policy: None Interface SSL Policy: None Interface Settings 🗒 Policy Assignments (1)													
iiii Ei	ter by Device	ice HTTP Kespor	ises Advanced							Add Cat	egory 🙆 Add Rul	Search Rules		×
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	🙂 🔈 🔳 🦷	
т н	andatory - Default Ba	se Policy (1-1)												
1	Rule-1	any	any	2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any		Ø facebook.com Ø twitter.com	Allow	0000	e 6
🔻 D	efault - Default Base	Policy (-)												
There	are no rules in this sec	tion. Add Rule or Add	d Category											
Defa	efault Action Intrusion Prevention: Balanced Security and Connectivity 💌 🖇 📓													

Il s'agit d'une règle unique sur le Management Center. Cependant, après son déploiement sur le capteur, il est étendu en seize règles, comme le montre l'image :

268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "facebook.com 268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "twitter.com" 268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "facebook.co 268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "twitter.com 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "facebook.com 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "twitter.com" 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "facebook.co 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "twitter.com 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "facebook.com 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url "twitter.com" 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "facebook.co 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url "twitter.com 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "facebook.com 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url "twitter.com" 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "facebook.co 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url "twitter.com 268435456 allow any any any any any any any any (ipspolicy 2)

Lorsque vous déployez une règle avec deux sous-réseaux configurés en tant que source, deux hôtes configurés en tant qu'adresses de destination et deux objets URL personnalisés destinés à deux ports, cette règle s'étend à seize règles sur le capteur.

Remarque : si vous devez utiliser les ports dans la règle d'accès, utilisez les détecteurs d'applications qui sont présents pour les applications standard. Cela permet d'étendre les règles de manière efficace.

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Acce	ss Control > Access C	ontrol Network	Discovery App	lication Detectors	Correlation	Actions •								
Def	ter a description													
Ident Rule	Initial Policy: None SSL Policy: None International Security Intelligence HTTP Responses Advanced													
ill F	ilter by Device									Add Cat	egory 📀 Add Rul	e Search Rules		×
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action		
- P	landatory - Default Ba	se Policy (1-1)												
1	Rule-1	any	any	2.2.2.2	23.3.3.3 4.4.4.4	any	any	HTTP HTTPS	any	any	<pre> facebook.com</pre>	Allow	0000	0
v 0	efault - Default Base	Policy (-)												
Ther	e are no rules in this sec	tion. Add Rule or Add	l Category											
Defa	ult Action									Intrusion	Prevention: Balanced	Security and Cor	nnectivity	\$ 1

Lorsque vous utilisez des détecteurs d'applications au lieu de ports, le nombre de règles étendues passe de seize à huit, comme le montre l'image :

268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1 268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid 676:1, 1

Extension d'une règle basée sur IP à l'aide de VLAN

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Identi	ty Policy: None		SSL Policy: None															
		1.111									Ta In	heritance Setting	s 🖪	Polic	cy Ass	ignme	ants (1)
Ruit	Security In	telligence	HTTP Responses	Advanced						Add Catagory	Add Dule	Soarch Bulos						
	liter by Device									Add Category	S Add Rule	Search Kules	_			_	_	
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action		•		-		
-	landatory - Dono	tTouch (1-2)																
1	À AllowFile	any	any	any	any	⊚ Two ⊚ One	any	 1&1 Internet 1-800-Flowers 100ye.com 	any	any	any	🖋 Allow	Ũ	ľ		0	~	8
2	AllowtheRest	any	any	any	any	any	any	any	any	any	any	🛹 Allow	Û	•		0	P	8
- C	efault - DonotTo	uch (-)																
Ther	e are no rules in th	nis section. Add	I Rule or Add Categor	Y														
Defa	ult Action									Intrusion Prevent	tion: Balanced Sec	urity and Connec	tivity		_	~	\$	

La règle AllowFile a une seule ligne correspondant à deux ID de VLAN avec certains détecteurs d'application, des stratégies d'intrusion et des stratégies de fichier. La règle AllowFile se développe en deux règles.

268436480 allow any any any any any 1 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena 268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5) (filepolicy 1 ena

Les stratégies IPS et les stratégies de fichiers sont uniques pour chaque règle de contrôle

d'accès, mais plusieurs détecteurs d'applications sont référencés dans la même règle et ne participent donc pas à l'extension. Si vous considérez une règle avec deux ID de VLAN et trois détecteurs d'application, il n'y a que deux règles, une pour chaque VLAN.

Extension d'une règle basée sur IP avec des catégories d'URL

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Ident	ity Policy: None		SSL Policy: None												
											Tel Ini	neritance Setting	s 📑 Polic	y Assignm	nents (2)
Rul ma	Filter by Device	elligence H	ITTP Responses	Advanced						Add Category	Add Rule	Search Rules			×
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	U		
•	landatory - Dono	Touch (1-2)													
1	Block	any	any	any	any	any	any	any	any	any	Adult and Poi Alcohol and T	Block		0	a 🖉
2	AllowFile	🔩 Internal 🔩 DMZ	為 Internal	any	any	any	any	any	any	any	any	🛹 Allow		0	e 6
•	Default - DonotTo	uch (-)													
The	here are no rules in this section. Add Rule or Add Category														
Def	ult Action									Intrusion Prevent	tion: Balanced Secu	urity and Connec	ivity	*	\$ 📕

La règle de blocage bloque les catégories d'URL pour adulte et pornographie Toute réputation et Réputations en matière d'alcool et de tabac 1-3. Il s'agit d'une règle unique sur Management Center, mais lorsque vous la déployez sur le capteur, elle est étendue en deux règles, comme illustré ci-dessous :

268438530 deny any any any any any any any any (log dcforward flowstart) (urlcat 11) 268438530 deny any any any any any any any any (log dcforward flowstart) (urlcat 76) (urlrep le 60)

Lorsque vous déployez une seule règle avec deux sous-réseaux configurés comme source et deux hôtes configurés comme adresses de destination, ainsi que deux objets URL personnalisés destinés à deux ports avec deux catégories d'URL, cette règle s'étend à trente-deux règles sur le capteur.

Extension d'une règle basée sur IP avec zones

Les zones se voient attribuer des numéros qui sont référencés dans les stratégies.

Si une zone est référencée dans une stratégie, mais qu'elle n'est attribuée à aucune interface du périphérique vers lequel la stratégie est envoyée, la zone est considérée comme any et un any ne mène à aucune extension des règles.

Si la zone source et la zone de destination sont identiques dans la règle, le facteur de zone est considéré comme tout et une seule règle est ajoutée puisque TOUT n'entraîne aucune extension des règles.

Examinez la configuration d'une règle d'accès à partir du FMC, comme illustré dans l'image :

Ident	fentity Policy: None SSL Policy: No															
_											In In	heritance Setting	s 🖳 F	Policy	Assignn	nents (2)
Rul	es Security In	telligence HT	TP Responses	Advanced												
88 I	Filter by Device									Add Category	Add Rule	Search Rules				×
#	Source Name Dest Zones Source Networks Dest Networks Dest VLAN Tags Users Applications Src Ports								Src Ports	Dest Ports	URLs	Action	U (b 1		
• 1	fandatory - Dono	tTouch (1-2)														
1	Interfaces	為 Internal	為 Internal	any	any	any	any	any	any	any	any	🛹 Allow		b [0	6
2	Allow	any	any	any	any	any	any	any	any	any	any	🛹 Allow		6	0	a 🖯
• 1	Default - DonotTo	uch (-)														
Ther	sre are no rules in this section. Add Rule or Add Category															
Defa	ult Action	It Action									tion: Balanced Sec	urity and Connec	tivity		*	\$ 📑

Il y a deux règles. Une règle a des zones configurées, mais la zone source et la zone de destination sont identiques. L'autre règle n'a pas de configuration spécifique. Dans cet exemple, la règle d'accès Interfaces ne se traduit pas en règle.

268438531 allow any any any any any any any any (log dcforward flowstart)<----Allow Access Rule 268434432 allow any any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-----Defa

Sur le capteur, les deux règles apparaissent comme identiques, car le contrôle basé sur les zones impliquant les mêmes interfaces n'entraîne pas d'extension.

L'extension des règles d'accès aux règles de contrôle d'accès basées sur les zones se produit lorsque la zone référencée dans la règle est attribuée à une interface sur le périphérique.

Examinez la configuration d'une règle d'accès à partir du FMC comme indiqué ci-dessous :

Ident	ity Policy: None		SSL Policy: None												
											Te In	heritance Setting	s 🖳 Pol	icy Assigr	iments (2)
Rul	es Security In	telligence	HTTP Responses	Advanced											
đđ	Filter by Device									Add Category	Add Rule	Search Rules			20
#	Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applications									Dest Ports	URLs	Action	v b		
-	Mandatory - Dono	tTouch (1-2)													
1	À Interfaces	🍰 Internal	Internal External DMZ	any	any	any	any	any	any	any	any	🖋 Allow		0	<i>🖉</i> 🗎
2	Allow	any	any	any	any	any	any	any	any	any	any	🛹 Allow		0	0
-	Default - DonotTo	uch (-)													
The	re are no rules in this section. Add Rule or Add Category														
Def	ault Action					Intrusion Prevent	tion: Balanced Sec	urity and Connec	tivity	7	- \$ 📑				

La règle Interfaces implique des règles basées sur les zones avec la zone source comme zone interne et la zone de destination comme zone interne, externe et DMZ. Dans cette règle, les zones d'interface interne et DMZ sont configurées sur les interfaces et les zones externes n'existent pas sur le périphérique. Il s'agit de l'extension de la même :

268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <-----Rule for Internal to DMZ) 268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access rule 268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-----Default Une règle est créée pour une paire d'interfaces spécifique qui est Interne > DMZ avec une spécification de zone claire et une règle Interne > Interne n'est pas créée.

Le nombre de règles étendues est proportionnel au nombre de paires de zones source et de destination pouvant être créées pour les zones associées valides et il s'agit des mêmes règles de zone source et de destination.

Remarque : les règles désactivées du FMC ne sont pas propagées et ne sont pas étendues au capteur pendant le déploiement de la stratégie.

Formule générale d'extension des règles

Nombre de règles sur le capteur = (Nombre de sous-réseaux sources ou d'hôtes) * (Nombre de destinations) * (Nombre de ports sources) * (Nombre de ports de destination) * (Nombre d'URL personnalisées) * (Nombre de balises VLAN) * (Nombre de catégories d'URL) * (Nombre de paires de zones source et de destination valides)

Remarque : pour les calculs, toute valeur du champ est remplacée par 1. La valeur any dans la combinaison de règles est considérée comme 1 et n'augmente ni ne développe la règle.

Dépannage d'un échec de déploiement dû à l'extension des règles

En cas d'échec du déploiement après l'ajout de la règle d'accès, suivez les étapes mentionnées ci-dessous pour les cas où la limite d'extension de la règle a été atteinte

Consultez le fichier /var/log/action.queue.log pour les messages contenant les mots clés suivants :

Erreur - trop de règles - écriture de la règle 28, règles max 9094

Le message ci-dessus indique qu'il existe un problème avec le nombre de règles en cours d'extension. Vérifiez la configuration sur le FMC pour optimiser les règles en fonction des scénarios présentés ci-dessus.

Informations connexes

- <u>Guide de configuration de Firepower Management Center, version 6.0</u>
- <u>Assistance et documentation techniques Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.