Configurer et utiliser les stratégies de préfiltre FTD

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Exemple d'utilisation de stratégie de préfiltre 1
Point principal
Exemple d'utilisation de stratégie de préfiltre 2
Tâche 1. Vérifier la stratégie de préfiltre par défaut
Exigence de la tâche
Solution
Vérification CLI (LINA)

Introduction

Ce document décrit la configuration et le fonctionnement des politiques de préfiltrage de Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- ASA5506X qui exécute le code FTD 6.1.0-195
- FireSIGHT Management Center (FMC) qui exécute 6.1.0-195
- Deux routeurs Cisco IOS® 3925 exécutant des images 15.2

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Une politique de préfiltrage est une fonctionnalité introduite dans la version 6.1 et sert trois objectifs principaux :

- 1. Faire correspondre le trafic en fonction des en-têtes internes et externes
- 2. Fournir un contrôle d'accès anticipé qui permet à un flux de contourner complètement le moteur Snort
- 3. Servez-vous d'espace réservé pour les entrées de contrôle d'accès (ACE) migrées à partir de l'outil de migration Adaptive Security Appliance (ASA).

Configurer

Exemple d'utilisation de stratégie de préfiltre 1

Une politique de préfiltrage peut utiliser un type de règle de tunnel qui permet à FTD de filtrer en fonction du trafic tunnelisé d'en-tête IP interne et/ou externe. Au moment de la rédaction de cet article, le trafic tunnelisé se réfère à :

- Encapsulation de routage générique (GRE)
- IP-en-IP
- IPv6-en-IP
- Port Teredo 3544

Considérez un tunnel GRE comme illustré dans l'image.



Lorsque vous envoyez une requête ping de R1 à R2 à l'aide d'un tunnel GRE, le trafic passe par le pare-feu, comme illustré dans l'image.

1 2016-05-31 02:15:15.	10.0.0.1	10.0.0.2	ICMP	138 Echo	(ping)	request	id=0x0013,	seq=0/0,
2 2016-05-31 02:15:15.	10.0.0.2	10.0.0.1	ICMP	138 Echo	(ping)	reply	id=0x0013,	seq=0/0,
<								
⊕ Frame 1: 138 bytes on wir	e (1104 bits), 1	38 bytes capt	ured (1104	bits)				
Ethernet II, Src: CiscoIn	c_8d:49:81 (c8:4	c:75:8d:49:81), Dst: Ci	scoInc_a1	:2b:f9	(6c:41:6a	:a1:2b:f9)	
Internet Protocol Version	4, Src: 192.168	.75.39 (192.1)	58.75.39),	Dst: 192	.168.70	5.39 (192.	168.76.39)	duter
Generic Routing Encapsula	tion (IP)							
Internet Protocol Version	4, Src: 10.0.0.	1 (10.0.0.1),	Dst: 10.0	.0.2 (10.	0.0.2)		inner	
■ Internet Control Message	Protocol							

Si le pare-feu est un périphérique ASA, il vérifie l'en-tête IP externe comme indiqué dans l'image.

L2 Header	Outer IP Header src=192.168.75.39 dst=192.168.76.39	GRE Header	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7
--------------	--	---------------	--	----

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

, idle 0:00:17, bytes 520, flags

Si le pare-feu est un périphérique FirePOWER, il vérifie l'en-tête IP interne comme indiqué dans l'image.

L2 Header Src=192.168.7 dst=192.168.7	5.39 6.39	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7
--	--------------	--	----

Avec la politique de préfiltrage, un périphérique FTD peut faire correspondre le trafic en fonction des en-têtes internes et externes.

Point principal

Périphérique	Chèques
ASA	IP externe
Renifleur	IP interne
FTD	IP externe (préfiltre) + IP interne (politique de contrôle d'accès (ACP))

Exemple d'utilisation de stratégie de préfiltre 2

Une stratégie de préfiltrage peut utiliser un type de règle de préfiltrage qui peut fournir un contrôle d'accès anticipé et permettre à un flux de contourner complètement le moteur Snort, comme illustré dans l'image.



Tâche 1. Vérifier la stratégie de préfiltre par défaut

Exigence de la tâche

Vérification de la stratégie de préfiltrage par défaut

Solution

Étape 1. Accédez à Politiques > Contrôle d'accès > Préfiltre. Une stratégie de préfiltrage par défaut existe déjà, comme illustré dans l'image.

Over	view Analysis	Policies	Devices	Objects	AMP			Deploy) 📀	System	Help 🔻	mikis 🔻
Acces	s Control > Prefilte	r Netwo	ork Discovery	Applica	tion Detectors	Correlation	Actions •					
									Obje	ct Manager	nent Acce	ss Control
											🔘 New i	Policy
Pro	efilter Policy				Domain		Last	Modified				
D	Default Prefilter Policy Default Prefilter Policy w	/ vith default a	ction to allow a	ll tunnels	Global		2016 Modi	-04-22 21:43 fied by "admin	:25		D 🥖 E	j.

Étape 2. Choisissez Edit pour afficher les paramètres de stratégie tels qu'ils apparaissent dans l'image.

Overview Analysis Policies Devices Objects AMP					Deploy					
Acces	s Control)	Prefilter	Network	Discovery	y Application Detectors C			relation	Actions •	
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels Rules										
*	Name	Rule T	Source Interf	Destin Interf	Source Netwo	Destin Netwo	Source Port	Destin Port	VLAN	Action
You ca	You cannot add rules to the default Prefilter policy. You can change only default action options.									
Non-tunneled traffic is allowed Default Action: Tunnel Traffic Analyze all tunnel traffic										

Étape 3. La stratégie de préfiltrage est déjà associée à la stratégie de contrôle d'accès, comme illustré dans l'image.

Overvi	ew	Analysis	Policies	Devices	Objects	AMP
Access	Cont	rol • Acces	s Control	Network D	iscovery	Application D
ACP_ Enter Des	55 criptic	06-1	Iter Policy			
Rules	Sec	curity Intellige	ence HTTF	Responses	Advance	ed
Prefilter Policy Settings						
Prefilter Policy used before access control Default Prefilter Polic						

Vérification CLI (LINA)

Les règles de préfiltrage sont ajoutées en plus des listes de contrôle d'accès :

<#root> firepower# show access-list

PREFILTER POLICY:

```
Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc
```

Tâche 2. Bloquer le trafic tunnelisé avec balise

Exigence de la tâche

Bloquer le trafic ICMP qui est tunnellisé dans le tunnel GRE.

Solution

Étape 1. Si vous appliquez ces ACP, vous pouvez voir que le trafic Internet Control Message Protocol (ICMP) est bloqué, peu importe s'il passe par le tunnel GRE ou non, comme montré dans l'image.

Prefi	ter Policy: Default Pref	iter Policy				SSL Policy: No	ne			Ider	tity Policy: None				
_												10	Inheritance S	ettings 🥂 Policy Assignm	nents (1)
Ru	es Security Intellig	ence HTTP F	Responses	Advanced											
	Filter by Device										Add Category	Add Ru	le Search F	tules	×
•	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio	Source Po	Dest Ports	URLS	ISE/SGT Attributes	Action	• • • • • •	
-	Mandatory - ACP_5506	-1 (1-1)													
1	Block ICMP	any	any	any	any	any	any	CB Filter: ICM	any	any	âñy	any	× Block	00.8020	/ 8
-	Default - ACP_5506-1	(-)													
The	re are no rules in this sec	tion. Add Rule or	Add Category												
De	ault Action										Intrusion Prever	ntion: Balanced	Security and	Connectivity *	S 🔳

<#root>

R1#

```
ping 192.168.76.39
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:
```

• • • • •

Success rate is 0 percent (0/5)

```
R1#
ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Dans ce cas, vous pouvez utiliser une stratégie de préfiltrage pour répondre aux exigences de la tâche. La logique est la suivante :

- 1. Marquez tous les paquets qui sont encapsulés dans GRE.
- 2. Créez une politique de contrôle d'accès qui correspond aux paquets étiquetés et bloque le protocole ICMP.

Du point de vue de l'architecture, les paquets sont vérifiés par rapport aux règles de pré-filtrage LINA (Linux NAtivity), puis aux règles de pré-filtrage Snort et à l'ACP, et enfin Snort ordonne à LINA d'abandonner. Le premier paquet passe par le périphérique FTD.

Étape 1. Définissez une balise pour le trafic tunnelisé.

Accédez à Policies > Access Control > Prefilter et créez une nouvelle stratégie de préfiltrage. N'oubliez pas que la stratégie de préfiltrage par défaut ne peut pas être modifiée comme indiqué dans l'image.

		Object Management Access Control
Last Hod	fied	
New Policy Name: Description:	Prefilter_Policy1	? X

Dans la stratégie de préfiltrage, définissez deux types de règles :

- 1. Règle du tunnel
- 2. Règle de préfiltrage

Vous pouvez les considérer comme des fonctionnalités totalement différentes pouvant être configurées dans une stratégie de préfiltrage.

Pour cette tâche, il est nécessaire de définir une règle de tunnel comme illustré dans l'image.

Add Tunnel R	Rule					? ×
① Tunnel rule	es perform early handling of no	n-encrypted encapsulated traffic, using	outer IP headers. Fast	pathed traffic bypasses acc	ess contr	ol and QoS.
Name	Tag Tunneled traffic	F Enabled	Insert	below rule	¥ 1	
Action	✓ Analyze 1	•	Assign Tunnel Tag	Inside_the_GRE		~ 0
Interface Encapsulation GRE IP-in-IP IPv6-in-IP Teredo Por	Protocols: 3 rt (3544)	N Tags Encapsulation & Ports	2'			Comment Logging

En ce qui concerne les actions :

Action	Description
Analyser	Après LINA, le débit est contrôlé par Snort Engine. Une balise de tunnel peut éventuellement être attribuée au trafic tunnelisé.
Block	Le flux est bloqué par LINA. L'en-tête externe doit être vérifié.
FastPath	Le flux est géré uniquement par LINA sans qu'il soit nécessaire d'utiliser le moteur Snort.

Étape 2. Définissez la politique de contrôle d'accès pour le trafic étiqueté.

Bien qu'elle ne puisse pas être très intuitive au début, la balise de tunnel peut être utilisée par une règle de politique de contrôle d'accès comme zone source. Accédez à Policies > Access Control et créez une règle qui bloque le protocole ICMP pour le trafic étiqueté comme indiqué dans l'image.

01	Overview Analysis Policies Devices Objects AMP Deploy													
Ao	cess Control + Access Control	Network Discovery	Applicat	ion Detectors	Correlation	Actions •								
AC Entr	ACP_5506-1 Enter Description													
R	Pretater Park Cratical Social													
	Filter by Device												Add Category O Ad	Id Rule Search
	Name	Sourc		lest lones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ESE/SGT Attributes	Action
-	Mandatory - ACP_5506-1 (1-1)													
1	Block 3CMP	🐔 in	ide_the_GRE	wy.	879	any.	any	879	S Filter: ICMP	any	819	any	419	× Block
-	▼ Default - ACP_5506-1 (-)													
78	There ere no rules in this section. Add Rule or Add Category													
De	efault Action												Intrusion Prevention: Bal	anced Security a
_														

Remarque : la nouvelle stratégie de préfiltrage est associée à la stratégie de contrôle d'accès.

Vérification

Activez la capture sur LINA et sur CLISH :

<#root>

firepower#

show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes] capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]

<#root>

>

capture-traffic

Please choose domain to capture traffic from: 0 - br1 1 - Router

Selection?

1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

-n

À partir de R1, essayez d'envoyer une requête ping au point de terminaison du tunnel GRE distant. La requête ping échoue :

<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds: Success rate is 0 percent (0/5)

La capture CLISH montre que la première requête d'écho a transité par FTD et que la réponse a été bloquée :

Options: -n 18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo 18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo

La capture LINA le confirme :

<#root>

```
>
```

```
show capture CAPI | include ip-proto-47
102: 18:21:07.767523 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
107: 18:21:09.763739 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
111: 18:21:11.763769 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
115: 18:21:13.763784 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
120: 18:21:15.763830 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
>
show capture CAPO | include ip-proto-47
93: 18:21:07.768133 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
94: 18:21:07.768438 192.168.76.39 > 192.168.75.39: ip-proto-47, length 104
```

Activez CLISH firewall-engine-debug, effacez les compteurs d'abandon LINA ASP et effectuez le même test. Le débogage CLISH montre que pour la requête d'écho, vous avez fait correspondre la règle de préfiltre et pour la réponse d'écho, la règle ACP :

```
<#root>
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
New session
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
uses prefilter rule 268434441 with tunnel zone 1
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, o
icmpType 8, icmpCode 0
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
uses prefilter rule 268434441 with tunnel zone 1
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, o
uses prefilter rule 268434441 with tunnel zone 1
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, o
```

```
icmpType 0, icmpCode 0
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
match rule order 3, 'Block ICMP', action Block
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action
```

L'abandon ASP indique que Snort a abandonné les paquets :

<#root>

>

show asp drop

Frame drop:	
No route to host (no-route)	366
Reverse-path verify failed (rpf-violated)	2
Flow is denied by configured rule (acl-drop)	2
Snort requested to drop the frame (snort-drop)	5

Dans les événements de connexion, vous pouvez voir la stratégie et la règle de préfiltrage que vous avez mises en correspondance, comme illustré dans l'image.

Overview	Analysis Policie	s Devices	Objects /	MP								
Context E	xplorer Connectio	ns + Events	Intrusions •	Files • I	Hosts • Users • Vi	ulnerabilities • Correl	ation • Custom •	Lookup • S	earch			
	Bookmark Th											
Conne	ction Events	switch workflo	ml									
Connection	Connections with Application Details > Table View of Connection Events											
 Search (Search Constraints (Edit Search)											
Jump to												
•	* First Packet ×	Action ×	Initiator × IP	Responder ×	Source Port / × ICMP Type	Destination Port / × ICMP Code	Access Control × Policy	Access Control Rule	× <u>Prefilter</u> × <u>Policy</u>	<u>Tunnel/Prefilter</u> × <u>Rule</u>		
4 🗆	2016-05-21 14:27:54	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP 5506-1	Block ICMP	Prefilter Policy1	Tag Tunneled traffic		
4 🗖	2016-05-21 14:26:51	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0./ icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic		
4 □	2016-05-21 14:24:52	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	<u>0 / icmp</u>	ACP 5506-1	Block ICMP	Prefilter Policy1	Tag Tunneled traffic		
4 🗆	2016-05-21 14:21:07	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	<u>0 / icmp</u>	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic		
4 🗆	2016-05-21 13:27:04	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	<u>0 / icmp</u>	ACP 5505-1	Block ICMP	Prefilter Policy1	Tag Tunneled traffic		
4 🗆	2016-05-21 13:24:36	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	<u>0 / icmp</u>	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic		
4 D	2016-05-21 13:15:26	<u>Block</u>	10.0.0.1	10.0.0.2	8 (Echo Request) / icmp	0 / icmp	ACP 5506-1	Block ICMP	Prefilter Policy1	Tag Tunneled traffic		
K < Page 1 of 1 >> Displaying rows 1-7 of 7 rows												

Tâche 3. Contourner le moteur Snort avec les règles de préfiltre Fastpath

Diagramme du réseau



Exigence de la tâche

- 1. Supprimez les règles de stratégie de contrôle d'accès actuelles et ajoutez une règle de stratégie de contrôle d'accès qui bloque tout le trafic.
- 2. Configurez une règle de stratégie de préfiltrage qui contourne le moteur de détection pour le trafic provenant du réseau 192.168.75.0/24.

Solution

Étape 1. La politique de contrôle d'accès qui bloque tout le trafic est celle illustrée dans l'image.

Advanced	Inheritance Settings 🗒 Policy Assignments (1)										
Rules Security Intelligence HTTP Responses Advanced											
VIAN Hears Appli Sourc Dast HPLs ISE/ Acti											
Attrib											
▼ Mandatory - ACP_5506-1 (-)											
There are no rules in this section. Add Rule or Add Category											
There are no rules in this section. Add Rule or Add Category											
Access Control: Block All Traffic											
Source Zones Dest Netw Netw Dest Netw VLAN Users Appli Sourc Dest URLs ISE/ Acti Acti											

Étape 2. Ajoutez une règle de préfiltrage avec Fastpath comme action pour le réseau source 192.168.75.0/24, comme illustré dans l'image.

Add Prefilter Rule				?
Prefilter rules perform early handling	ng of traffic based on simp	e network characteristics. Fastpath	ned traffic bypasses access control and Qo	s.
Name Fastpath_src_192.168.75	.0/24	F Enabled		
Interface Objects Networks	VLAN Tags Ports	Course Mahurada (4)	Destination Mature	Comment Logging
Available Networks C		Source Networks [1]	Destination Networ	KS (U)
 Scaler by Home of Value any IPv4-Private-All-RFC1918 any-ipv4 any-ipv6 IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast 	Add to Source Add to Destination	22 192.100.73.0/24		
IPv4-Private-10.0.0.0-8		Enter an ID address	Add Enter an 10 address	Add
·		enter an ar address	Enter an 19 address	

Étape 3. Le résultat est tel qu'illustré sur l'image.

	Overview Analysis Policies Devices Objects AMP Deploy System Help • mikis •										
Γ	Access Contro	l ► Prefilter Netw	work Discovery App	plication Detectors	Correlation Actio	ns •					
	Prefilter_Policy1										
	Enter Description										
Rules											
Γ						Add Tu	nnel Rule 🛛 🔾 Add Pr	refilter Rule Search R	ules	2	
	*	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN 1	
	1	Fastpath_src_192.168.	Prefilter	any	any	2 192.168.75.0/24	any	any	any	any	
	Non-tunneled traffic is										

Étape 4. Enregistrer et déployer.

Activez la capture avec trace sur les deux interfaces FTD :

<#root>
firepower#
capture CAPI int inside trace match icmp any any
firepower#
capture CAPO int outsid trace match icmp any any

Essayez d'envoyer une requête ping de R1 (192.168.75.39) vers R2 (192.168.76.39) via le FTD. La requête ping échoue :

<#root>

R1#

.

ping 192.168.76.39

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

Success rate is 0 percent (0/5)

La capture sur l'interface interne montre :

<#root>

firepower#

show capture CAPI

5 packets captured

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request

```
2: 23:35:09.278641 192.168.75.39 > 192.168.76.39: icmp: echo request

3: 23:35:11.279251 192.168.75.39 > 192.168.76.39: icmp: echo request

4: 23:35:13.278778 192.168.75.39 > 192.168.76.39: icmp: echo request

5: 23:35:15.279282 192.168.75.39 > 192.168.76.39: icmp: echo request

5 packets shown
```

La trace du premier paquet (demande d'écho) montre (les points importants sont mis en évidence) :

Déflecteur (Surligner pour lire)

firepower# show capture CAPI packet-number 1 trace

5 paquets capturés

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39 : icmp : requête d'écho

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Liste d'accès MAC

Phase : 2

Type : ACCESS-LIST

Sous-type :

Résultat : ALLOW

Config :

Règle Implicite

Informations supplémentaires:

Liste d'accès MAC

Phase : 3

Type : ROUTE-LOOKUP

Sous-type : Résoudre l'interface de sortie

Résultat : ALLOW

Config :

Informations supplémentaires:

le tronçon suivant trouvé 192.168.76.39 utilise la sortie ifc à l'extérieur

Phase : 4

Type : ACCESS-LIST

Sous-type : log

Résultat : ALLOW

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448 : PREFILTER POLICY : Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448 : RULE : Fastpath_src_192.168.75.0/24

Informations supplémentaires:

Phase : 5

Type : CONN-SETTINGS

Sous-type :

Résultat : ALLOW

Config :

class-map class-default

correspondre à

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informations supplémentaires:

Phase : 6

Type : NAT

Sous-type : par session

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 7

Type : IP-OPTIONS

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 8

Type : INSPECT

Sous-type : np-inspect

Résultat : ALLOW

Config :

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

inspecter icmp

service-policy global_policy global

Informations supplémentaires:

Phase : 9

Type : INSPECT

Sous-type : np-inspect

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 10

Type : NAT

Sous-type : par session

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 11

Type : IP-OPTIONS

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 12

Type : FLOW-CREATION

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Nouveau flux créé avec l'ID 52, paquet envoyé au module suivant

Phase : 13

Type : ACCESS-LIST

Sous-type : log

Résultat : ALLOW

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448 : PREFILTER POLICY : Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448 : RULE : Fastpath_src_192.168.75.0/24

Informations supplémentaires:

Phase : 14

Type : CONN-SETTINGS

Sous-type :

Résultat : ALLOW

Config :

class-map class-default

correspondre à

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informations supplémentaires:

Phase : 15

Type : NAT

Sous-type : par session

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 16

Type : IP-OPTIONS

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 17

Type : ROUTE-LOOKUP

Sous-type : Résoudre l'interface de sortie

Résultat : ALLOW

Config :

Informations supplémentaires:

le tronçon suivant trouvé 192.168.76.39 utilise la sortie ifc à l'extérieur

Phase : 18

Type : RECHERCHE DE CONTIGUÏTÉ

Sous-type : tronçon suivant et contiguïté

Résultat : ALLOW

Config :

Informations supplémentaires:

contiguïté active

l'adresse mac de tronçon suivant 0004.deab.681b atteint 140372416161507

Phase: 19

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Liste d'accès MAC

Résultat :

input-interface : externe

input-status : up input-line-status : up output-interface : externe output-status : actif output-line-status : actif Action : autoriser 1 paquet affiché

firepower#

firepower# show capture CAPI numéro-paquet 1 trace 5 paquets capturés 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39 : icmp : requête d'écho Phase : 1 Type : CAPTURE Sous-type : Résultat : ALLOW Config : Informations supplémentaires : liste d'accès MAC Phase : 2 Type : ACCESS-LIST Sous-type : Résultat : ALLOW Config : Règle implicite Informations supplémentaires : liste d'accès MAC Phase : 3 Type : ROUTE-LOOKUP Sous-type : olve Egress Interface Result : ALLOW Config : Additional Information : found next-hop 192.168.76.39 uses egress ifc outside Phase : 4 Type : ACCESS-LIST Sous-type : log Result : ALLOW Config : access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both access-list CSM ACL remark rule-id 268434448 : PREFILTER POLICY : Prefilter Policy1 access-list CSM FW ACL remark rule-id 268434448 : RULE : Fastpath_src_192.168.75.0/24 Informations supplémentaires : Phase : 5 Type : CONN-SETTINGS Sous-type : Résultat : ALLOW Config : class-map class-default match any policy global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global policy Informations supplémentaires : Phase : 6 Type : NAT Sous-type : par session Résultat : ALLOW Config : Informations supplémentaires : Phase 7 Type : IP-OPTIONS Sous-type : Résultat : ALLOW Config : Informations supplémentaires : Phase : 8 Type : INSPECT Sous-type : np-inspect Résultat : ALLOW Config : class-map inspection_default match defaultinspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy Informations supplémentaires : Phase : 9 Type : INSPECT Sous-type : np-inspect Résultat : ALLOW Config : Informations supplémentaires : Phase : 10 Type : NAT Sous-type : par session Résultat : ALLOW Config : Informations supplémentaires : Phase : 11 Type : IP-OPTIONS Sous-type : : ALLOW Config : Informations supplémentaires : Phase : 12 Type : FLOW-CREATION Sous-type : Résultat : ALLOW Config : Informations supplémentaires : Nouveau flux créé avec l'ID 52, paquet envoyé au module suivant Phase : 13 Type : ACCESS-LIST Sous-type : log Résultat : ALLOW Config : access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both access list CSM_FW_ACL_ remark rule-id 268434448 : PREFILTER POLICY : Prefilter_Policy1 access-list CSM_FW_ACL_ remark rule-id 268434448 : RULE : Fastpath_src_192.168.75.0/24 Informations supplémentaires : Phase : 14 Type : CONN-SETTINGS Sous-type : Résultat : ALLOW Config : class-map class-default match any policy global_policy class-default set connection advancedoptions UM STATIC TCP MAP service-policy global policy global Informations supplémentaires : Phase : 15 Type : NAT Sous-type : per-session ALLOW Config : Additional Information : Phase : 16 Type : IP-OPTIONS Sous-type : Result : ALLOW Config : Additional Information : Phase : 17

Type : ROUTE-LOOKUP Sous-type : Resolve Egress Interface Result : ALLOW Config : Additional Information : found next-hop 192.168.76.39 uses egress ifc outside Phase : 18 Type : ADJACENCY-LOOKUP Sous-type : next-hop and adjacency Result : ALLOW Config : Additional Information : adjacency Active next-hop mac address 0 04.deab.681b hits 140372416161507 Phase : 19 Type : CAPTURE Sous-type : Résultat : ALLOW Config : Informations supplémentaires : MAC Access list Résultat : input-interface : outside input-status : up input-linestatus : up output-interface : outside output-status : up output-line-status : up Action : allow 1 packet show firepower#

La capture sur l'interface externe montre :

<#root>

firepower#

show capture CAPO

10 packets captured

1:	23:35:07.282044	192.168.75.39	>	192.168.76.39:	icmp:	echo	request
2:	23:35:07.282227	192.168.76.39	>	192.168.75.39:	icmp:	echo	reply
3:	23:35:09.278717	192.168.75.39	>	192.168.76.39:	icmp:	echo	request
4:	23:35:09.278962	192.168.76.39	>	192.168.75.39:	icmp:	echo	reply
5:	23:35:11.279343	192.168.75.39	>	192.168.76.39:	icmp:	echo	request
6:	23:35:11.279541	192.168.76.39	>	192.168.75.39:	icmp:	echo	reply
7:	23:35:13.278870	192.168.75.39	>	192.168.76.39:	icmp:	echo	request
8:	23:35:13.279023	192.168.76.39	>	192.168.75.39:	icmp:	echo	reply
9:	23:35:15.279373	192.168.75.39	>	192.168.76.39:	icmp:	echo	request
10:	23:35:15.279541	192.168.76.39	>	192.168.75.39:	icmp:	echo	reply
~	1 . I						

10 packets shown

La trace du paquet de retour indique qu'il correspond au flux actuel (52), mais qu'il est bloqué par la liste de contrôle d'accès :

```
<#root>
firepower#
show capture CAPO packet-number 2 trace
10 packets captured
2: 23:35:07.282227 192.168.76.39 > 192.168.75.39: icmp: echo reply
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id 52, uses current flow Phase: 4 Type: ACCESS-LIST Subtype: log Result: DROP Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1 access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE Additional Information: Result: input-interface: outside input-status: up input-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied by configured rule

Étape 5. Ajoutez une règle de préfiltre supplémentaire pour le trafic de retour. Le résultat est tel qu'illustré sur l'image.

Overview Analysis Policies Devices Objects AMP Deploy © System Help											np • mikis •	
Access Control • Prefilter Network Discovery Application Detectors Correlation Actions •												
Prefilter_Policy1											Cancel	
Enter Descriptio	Enter Description											
Rules	Rules											
							Add Tunnel Rule	Add Prefilter Rule	earch Rules)	
•	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag		Action	
1	Fastpath_src_192.168	Prefilter	any	any	2 192.168.75.0/24	any	any	any	any		🕶 Fastpath	
2	Fastpath_dst_192.168	Prefilter	any	any	any	2 192.168.75.0/24	any	any	any		- Fastpath	
Non-tunneled traffic is allowed Default Act											Action:	

Maintenant, tracez le paquet de retour que vous voyez (points importants mis en évidence) :

Déflecteur (Surligner pour lire)

firepower# show capture CAPO packet-number 2 trace

10 paquets capturés

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39 : icmp : réponse d'écho

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Liste d'accès MAC

Phase : 2

Type : ACCESS-LIST

Sous-type :

Résultat : ALLOW

Config :

Règle Implicite

Informations supplémentaires:

Liste d'accès MAC

Phase: 3

Type : FLOW-LOOKUP

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Débit trouvé avec ID 62, utilise le flux de courant

Phase : 4

Type : ACCESS-LIST

Sous-type : log

Résultat : ALLOW

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 268434450 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434450 : PREFILTER POLICY : Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434450 : RULE : Fastpath_dst_192.168.75.0/24

Informations supplémentaires:

Phase : 5

Type : CONN-SETTINGS

Sous-type :

Résultat : ALLOW

Config :

class-map class-default

correspondre à

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informations supplémentaires:

Phase : 6

Type : NAT

Sous-type : par session

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 7

Type : IP-OPTIONS

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Phase : 8

Type : ROUTE-LOOKUP

Sous-type : Résoudre l'interface de sortie

Résultat : ALLOW

Config :

Informations supplémentaires:

192.168.75.39 de tronçon suivant trouvé utilise la sortie ifc inside

Phase:9

Type : RECHERCHE DE CONTIGUÏTÉ

Sous-type : tronçon suivant et contiguïté

Résultat : ALLOW

Config :

Informations supplémentaires:

contiguïté active

l'adresse mac de tronçon suivant c84c.758d.4981 atteint 140376711128802

Phase : 10

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Config :

Informations supplémentaires:

Liste d'accès MAC Résultat : input-interface : inside input-status : up input-line-status : up output-interface : interne output-status : actif output-line-status : actif

Action : autoriser

firepower# show capture CAPO packet-number 2 trace 10 paquets capturés 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39 : icmp : echo reply Phase : 1 Type : CAPTURE Sous-type : Résultat : ALLOW Config : Informations supplémentaires : Liste d'accès MAC Phase : 2 Type : ACCESS-LIST Sous-type : Résultat : ALLOW Config : Règle implicite Informations supplémentaires : Liste d'accès MAC Phase : 3 Type : FLOW-LOOKUP Sous-type : Résultat : ALLOW Config : Informations supplémentaires : flux trouvé avec l'ID 62, utilise le flux actuel Phase : 4 Type : ACCESS-LIST Sous-type : log Résultat : ALLOW Config : access-group CSM FW ACL global access-list CSM FW ACL advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 268434450 event-log both access-list CSM_FW_ACL_ remark rule-id 268434450 : PREFILTER POLICY : Prefilter_Policy_Policy1 access1 list CSM_FW_ACL_ remark rule-id 268434450 : RULE : Fastpath dst 192.168.75.0/24 Informations supplémentaires : Phase : 5 Type : CONN-SETTINGS Sous-type : Result : ALLOW Config : class-map class-default match any policy-map global policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global Informations supplémentaires : Phase : 6 Type : NAT Sous-type : par session Résultat : ALLOW Config : Informations supplémentaires : Phase : 7 Type : IP-OPTIONS Sous-type : Résultat : ALLOW Config : Informations supplémentaires : 8 Type : ROUTE-LOOKUP Sous-type : Resolve Egress Interface Résultat : ALLOW Config : Additional Information : found next-hop 192.168.75.39 uses egress ifc inside Phase : 9 Type : ADJACENCY-LOOKUP Sous-type : next-hop and adjacency Résultat : ALLOW Config : Additional Information : adjacency Active next-hop mac address c84c.758d.4981 hits 140376711128802 Phase : 10 Type : CAPTURE Sous-type : Result : ALLOW g : Informations supplémentaires : Liste d'accès MAC Résultat : interface d'entrée : état d'entrée interne : up état-ligne-d'entrée : up interface-de-sortie : état-de-sortie interne : up état-ligne-de-sortie : up Action : autoriser

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La vérification a été expliquée dans les sections relatives aux tâches respectives.

Dépannage

Il n'y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

Informations connexes

• Toutes les versions du guide de configuration de Cisco Firepower Management Center sont disponibles ici :

Navigation dans la documentation de Cisco Secure Firewall Threat Defense

• Le Centre d'assistance technique mondial (TAC) de Cisco recommande vivement ce guide visuel pour des connaissances pratiques approfondies sur les technologies de sécurité de nouvelle génération Cisco Firepower, notamment celles mentionnées dans cet article :

Cisco Firepower Threat Defense (FTD)

• Pour toutes les notes techniques de configuration et de dépannage :

Cisco Secure Firewall Management Center

<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.