Configurar e Operar Políticas de Pré-Filtro de FTD

Contents
Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Caso de uso 1 da política de pré-filtro
Ponto principal
Caso de uso 2 da política de pré-filtro
Tarefa 1. Verificar Política de Pré-Filtro Padrão
Requisito da tarefa
Solução
Verificação de CLI (LINA)

Introdução

Este documento descreve a configuração e a operação das Políticas de pré-filtro do Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA5506X que executa o código FTD 6.1.0-195
- FireSIGHT Management Center (FMC) que executa a versão 6.1.0-195
- Dois roteadores 3925 Cisco IOS® com imagens 15.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Uma política de pré-filtro é um recurso introduzido na versão 6.1 e tem três finalidades principais:

- 1. Tráfego correspondente com base nos cabeçalhos internos e externos
- 2. Fornecer controle de acesso antecipado que permita que um fluxo ignore completamente o mecanismo Snort
- 3. Trabalhe como um espaço reservado para Access Control Entries (ACEs) que são migradas da ferramenta de migração do Adaptive Security Appliance (ASA).

Configurar

Caso de uso 1 da política de pré-filtro

Uma Política de Pré-filtro pode usar um Tipo de Regra de Túnel que permite que o FTD filtre com base no tráfego em túnel do cabeçalho IP interno e/ou externo. Na época em que este artigo foi escrito, o tráfego em túnel se refere a:

- Encapsulamento de roteamento genérico (GRE)
- IP em IP
- IPv6 em IP
- Porta 3544 Teredo

Considere um túnel GRE como mostrado na imagem.



Quando você faz ping de R1 para R2 com o uso de um túnel GRE, o tráfego passa pelo Firewall com a aparência mostrada na imagem.

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 wire (1104 bits).	, 138 bytes capt	tured (1	l104 bits)				
■ Ethernet II, Src: CiscoInc_8d:49:81 (c8)	3:4c:75:8d:49:81	L), Dst:	CiscoInc_a1	:2b:f9	(6c:41:6	a:a1:2b:f9)	
Internet Protocol Version 4, Src: 192.1	168.75.39 (192.1	168.75.3	39), Dst: 192	.168.70	5.39 (192	.168.76.39)	duter
Beneric Routing Encapsulation (IP)							
Internet Protocol Version 4, Src: 10.0.	0.1 (10.0.0.1)	, Dst: 1	LO.O.O.2 (10.	0.0.2)		inner	
■ INTERNET CONTROL MESSAGE PROTOCOL							

Se o firewall for um dispositivo ASA, ele verificará o cabeçalho IP externo como mostrado na imagem.

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

Se o firewall for um dispositivo FirePOWER, ele verificará o cabeçalho IP interno como mostrado na imagem.



Com a política de pré-filtro, um dispositivo FTD pode corresponder o tráfego com base nos cabeçalhos internos e externos.

Ponto principal

Dispositivo	Verificações
ASA	IP externo
Snort	IP interno
FTD	Externo (Pré-filtro) + IP Interno (Política de Controle de Acesso (ACP))

Caso de uso 2 da política de pré-filtro

Uma política de pré-filtro pode usar um tipo de regra de pré-filtro que pode fornecer controle de acesso antecipado e permitir que um fluxo ignore completamente o mecanismo Snort, como mostrado na imagem.



Tarefa 1. Verificar Política de Pré-Filtro Padrão

Requisito da tarefa

Verificar a Política de Pré-Filtro padrão

Solução

Etapa 1. Navegue até Policies > Access Control > Prefilter. Uma Política de Pré-filtro padrão já existe, conforme mostrado na imagem.

Overview Analysis	Policies Devices C	bjects	AMP			Deploy) 📀	System	Help 🔻	mikis 🔻
Access Control > Prefilte	r Network Discovery	Applicat	tion Detectors	Correlation	Actions •					
							Obje	ct Manager	nent Acce	ss Control
									O New	Policy
Prefilter Policy			Domain		Last	Modified				
Default Prefilter Policy Default Prefilter Policy w	, vith default action to allow all	tunnels	Global		2016 Modif	04-22 21:43 ied by "admin	:25		D 🖉 (1

Etapa 2. Escolha Editar para ver as configurações da diretiva como mostrado na imagem.

Overview Analysis Policies Devices Objects AMP												
Access Control > Prefilter Network Discovery Application Detectors Correlation									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 cannot add rules to the default Prefilter policy. You can change only default action options.												
Non-	tunneled tra	offic is allowe	ed.	De	efault Action	n: Tunnel Tra	ffic Ar	nalyze all tur	nnel traffic			

Etapa 3. A Política de Pré-filtro já está anexada à Política de Controle de Acesso conforme mostrado na imagem.

Overvi	ew	Analysis	Policies	Devices	Objects	AMP					
Access	Cont	rol • Acces	iscovery	Application D							
ACP_5506-1 Enter Description											
Prefilter F	Prefilter Policy: Default Prefilter Policy										
Rules	Sec	curity Intellige	ence HTT	P Responses	Advance	ed					
Prefilter	r Pol		ø								
Prefilter	Polic	y used before	Default P	refilter Policy							

Verificação de CLI (LINA)

As regras de pré-filtro são adicionadas sobre as ACLs:

<#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
```

Tarefa 2. Bloquear tráfego em túnel com tag

Requisito da tarefa

Bloqueie o tráfego ICMP que é encapsulado dentro do túnel GRE.

Solução

Etapa 1. Se você aplicar esses ACP, poderá ver que o tráfego do Internet Control Message Protocol (ICMP) está bloqueado, independentemente de passar pelo túnel GRE ou não, como mostrado na imagem.

Prefilter Policy: Default Prefilter Policy						SSL Policy: No	0.0			Ident	ity Policy: Nane				
												10	Inheritance S	iettings 🧾 Policy Assignm	ients (1)
Ru	les Security Intellige	ence HTTP F	Responses	Advanced											
Filter by Device Add Category Add								Add Rul	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_SS06	-1 (1-1)											_		
1	Block ICMP	any	any	any	any	any	any	T Fiber: ICM	P any	any	any	any	X Block	V D 2 to 2 o	/ 8
-	Default - ACP_5506-1 ((-)													
The	There are no rules in this section. Add Rule or Add Category														
De	ault Action										Intrusion Prever	ntion: Balanced	Security and	Connectivity *	\$ 🔳

<#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)
```

Nesse caso, você pode usar uma Política de pré-filtro para atender ao requisito da tarefa. A lógica é a seguinte:

- 1. Marque todos os pacotes encapsulados dentro do GRE.
- 2. Crie uma Política de Controle de Acesso que corresponda aos pacotes marcados e bloqueie o ICMP.

Do ponto de vista da arquitetura, os pacotes são verificados em relação às regras de pré-filtro LINA (Linux NAtively), depois às regras de pré-filtro Snort e ACP e, finalmente, o Snort instrui o LINA a descartar. O primeiro pacote passa pelo dispositivo FTD.

Etapa 1. Defina uma tag para tráfego em túnel.

Navegue até Policies > Access Control > Prefilter e crie uma nova Política de pré-filtro. Lembre-se de que a Política de pré-filtro padrão não pode ser editada conforme mostrado na imagem.

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

Dentro da Política de pré-filtro, defina dois tipos de regras:

- 1. Regra de túnel
- 2. Regra de pré-filtro

Você pode pensar nesses dois recursos como totalmente diferentes que podem ser configurados em uma Política de pré-filtro.

Para esta tarefa, é necessário definir uma Regra de túnel como mostrado na imagem.

Add Tunnel Rule			? ×								
1 Tunnel rules perform early handling of non-encrypted encapsulated traffic, using outer IP headers. Fastpathed traffic bypasses access control and QoS.											
Name Tag Tunneled traffic	☑ Enabled	Insert below rule	¥ 1								
Action Analyze	*	Assign Tunnel Tag Inside_the_GRE	Y ◎								
Interface Objects Networks VI Encapsulation Protocols: GRE 3 IP-in-IP IPv6-in-IP Teredo Port (3544)	AN Tags Encapsulation & Ports	2	Comment Logging								

No que se refere às ações:

Ação	Descrição
Analisar	Após LINA, o fluxo é verificado pelo Snort Engine. Opcionalmente, uma tag de túnel pode ser atribuída ao tráfego em túnel.
Bloqueio	O fluxo é bloqueado pelo LINA. O cabeçalho externo deve ser verificado.
Fastpath	O fluxo é manipulado apenas pela LINA sem a necessidade de acionar o mecanismo Snort.

Etapa 2. Defina a Política de Controle de Acesso para o tráfego marcado.

Embora não possa ser muito intuitiva a princípio, a tag de túnel pode ser usada por uma regra de política de controle de acesso como uma zona de origem. Navegue até Policies > Access Control e crie uma Regra que bloqueie o ICMP para o tráfego marcado como mostrado na imagem.

Overvie	w Analysis Policies Devices O	bjects AMP											Deploy
Access	Control + Access Control Network (Discovery Applica	tion Detectors	Correlation	Actions •								
ACP_	ACP_5506-1 Enter Description												
Prefilter Policy: <u>SSR</u> , Policy: <u>SS</u>													
Rules Security Intelligence HTTP Responses Advanced													
db Filter	r by Device											Add Category Ad	d Rule Search
•	Name	Source Zones	best Cones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ESE/SGT Attributes	Action
w Han	datory - ACP_5506-1 (1-1)												
1	Block 1CMP	nside_the_GRE	ery.	any	any	any	any .	3 Filter: DOMP	any	any	any	819	× Block
🐨 Defa	wit - ACP_5506-1 (-)												
There a	There are no rules in this section. Add Rule or Add Category												
Default	Action			_								Intrusion Prevention: Bail	anced Security a

Solutiona de controle de bré-filtro é anexada à Política de controle de acesso.

Verificação

Habilitar captura em LINA e em 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

Em R1, tente fazer ping no ponto final do túnel GRE remoto. O ping falha:

<#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)

A captura CLISH mostra que a primeira solicitação de eco passou pelo FTD e a resposta foi bloqueada:

<#root>

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 18:21:11.75939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.75939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.75939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo 18:21:13.75939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo

A captura LINA confirma isso:

<#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
```

Ative CLISH firewall-engine-debug, limpe os contadores de queda LINA ASP e faça o mesmo teste. A depuração CLISH mostra que, para a Solicitação de Eco, você correspondeu à regra de pré-filtro e, para a Resposta de Eco, a regra 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,

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,

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

A queda de ASP mostra que o Snort descartou os pacotes:

<#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

Em Eventos de conexão, você pode ver a política e a regra de pré-filtro que correspondeu conforme mostrado na imagem.

Ove	Overview Analysis Policies Devices Objects AMP													
Con	itext E	plorer Connectio	ns + Events	Intrusions	Files •	Hosts • Users •	Vulnerabilities •	Correlation • Custo	m • Lookup •	Searc	h			
	Bookmark Th													
Co	Connection Events (switch workflow)													
Con	Connections with Application Details > Table View of Connection Events													
• Se	Search Constraints (Edt Search)													
30	imp to	. •												
	Г	* First Packet ×	Action ×	Initiator ×	Responder ×	Source Port /	Continuation Port	/ × Access Contro	× Access Contro	×	Prefilter ×	Tunnel/Prefilter ×		
				Tb	16	ICMP Type	ICMP Code	Policy	Rule		Policy	Rule		
- 4		2016-05-21 14:27:54	<u>Block</u>	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	np 0/icmp	ACP 5506-1	Block ICMP		Prefilter Policy1	Tag Tunneled traffic		
4		2016-05-21 14:26:51	Block	10.0.0.1	iii <u>10.0.0.2</u>	8 (Echo Request) / icm	ng 0./ icmp	ACP_5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
-1		2016-05-21 14:24:52	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	ng <u>0 / icmp</u>	ACP 5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
4		2016-05-21 14:21:07	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	ng 0./ icmg	ACP_5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
-1		2016-05-21 13:27:04	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	np 0/icmp	ACP 5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
4		2016-05-21 13:24:36	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	np 0./ icmp	ACP_5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
-1		2016-05-21 13:15:26	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icm	np 0/icmp	ACP 5506-1	Block ICMP	П	Prefilter Policy1	Tag Tunneled traffic		
K	< Page	1 of 1 >> Displa	ying rows 1-7	of 7 rows						- 1				

Tarefa 3. Ignorar Mecanismo Snort com Regras de Pré-Filtro Fastpath

Diagrama de Rede



Requisito da tarefa

- 1. Remova as regras atuais de Política de Controle de Acesso e adicione uma regra de Política de Controle de Acesso que Bloqueie todo o tráfego.
- 2. Configure uma regra de Política de Pré-Filtro que ignore o Mecanismo Snort para o tráfego originado na rede 192.168.75.0/24.

Solução

Etapa 1. A política de controle de acesso que bloqueia todo o tráfego é como mostrado na imagem.

	T= Inheritance Settings Policy Assignments (1)															
R	Rules Security Intelligence HTTP Responses Advanced															
đđ	Filter by Device Add Category Add Rule Search Rules										×					
	Name		Source Zones	Dest Zones	Source Netw	Dest Netw	VLAN	Users	Appli	Sourc	Dest	URLs	ISE/ Attrib	Acti	• • <u>•</u> • • •	
-	Mandat	ory -	ACP_550	6-1 (-)												
Th	ere are n	o rule	s in this se	ction. Add	Rule or Add	Category										
-	Default	- AC	P_5506-1	(-)												
Th	There are no rules in this section. Add Rule or Add Category															
D	fault Ac	tion									Access	Control: B	lock All Traf	fic		× 🧾
_																

Etapa 2. Adicione uma regra de pré-filtro com Fastpath como uma ação para a rede de origem 192.168.75.0/24, como mostrado na imagem.

Add Prefilter Rule			? >
Prefilter rules perform early handling of traffic based	on simple network characteristics. Fastpathed tr	affic bypasses access control and	d QoS.
Name Fastpath_src_192.168.75.0/24 Action ➡ Fastpath	✓ Enabled		
Interface Objects Networks VLAN Tags	Ports		Comment Logging
Available Networks 🖒 📀	Source Networks (1)	Destination Net	works (0)
Search by name or value	Add to Source	any	
IPv4-Private-10.0.0-8	Enter an IP address	Add Enter an IP addr	Add

Etapa 3. O resultado é o mostrado na imagem.

Overview	Analysis Policies	Devices Objects	AMP				Deploy	System Help	• mikis •					
Access Cont	rol > Prefilter Netv	work Discovery Ap	oplication Detectors	Correlation Acti	ons •									
Prefilter	Prefilter_Policy1													
Enter Descript	ion													
Rules														
					🔾 Add Tu	nnel Rule 🛛 🔾 Add P	refilter Rule Search	Rules	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-tunnele	d traffic is													

Etapa 4. Salvar e implantar.

Habilitar captura com rastreamento em ambas as interfaces FTD:

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

Tente fazer ping de R1 (192.168.75.39) para R2 (192.168.76.39) através do FTD. O ping falha:

<#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)

A captura na interface interna mostra:

<#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						

O rastreamento do primeiro pacote (solicitação de eco) mostra (pontos importantes destacados):

Spoiler (Realce para ler)

firepower#show capture CAPI packet-number 1 trace

5 pacotes capturados

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: solicitação de eco

Fase: 1

Tipo: CAPTURE

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Lista de Acesso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: ALLOW

Config:

Regra Implícita

Informações adicionais:

Lista de Acesso MAC

Fase: 3

Tipo: ROUTE-LOOKUP

Subtipo: Resolver interface de saída

Resultado: ALLOW

Config:

Informações adicionais:

encontrado próximo salto 192.168.76.39 usa ifc externo de saída

Fase: 4

Tipo: ACCESS-LIST

Subtipo: log

Resultado: 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

Informações adicionais:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: ALLOW

Config:

class-map class-default

corresponder a qualquer

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informações adicionais:

Fase: 6

Tipo: NAT

Subtipo: por sessão

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 7

Tipo: IP-OPTIONS

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 8

Tipo: INSPECT

Subtipo: np-inspect

Resultado: ALLOW

Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

inspect icmp

service-policy global_policy global

Informações adicionais:

Fase: 9

Tipo: INSPECT

Subtipo: np-inspect

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 10

Tipo: NAT

Subtipo: por sessão

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 11

Tipo: IP-OPTIONS

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 12

Tipo: FLOW-CREATION

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Novo fluxo criado com id 52, pacote enviado para o próximo módulo

Fase: 13

Tipo: ACCESS-LIST

Subtipo: log

Resultado: 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

Informações adicionais:

Fase: 14

Tipo: CONN-SETTINGS

Subtipo:

Resultado: ALLOW

Config:

class-map class-default

corresponder a qualquer

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informações adicionais:

Fase: 15

Tipo: NAT

Subtipo: por sessão

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 16

Tipo: IP-OPTIONS

Subtipo:

Resultado: ALLOW Config: Informações adicionais: Fase: 17 Tipo: ROUTE-LOOKUP Subtipo: Resolver interface de saída **Resultado: ALLOW** Config: Informações adicionais: encontrado próximo salto 192.168.76.39 usa ifc externo de saída Fase: 18 Tipo: PESQUISA DE ADJACÊNCIA Subtipo: next-hop e adjacência Resultado: ALLOW Config: Informações adicionais: adjacência Ativa endereço mac do próximo salto 0004.deab.681b atinge 140372416161507 Fase: 19 **Tipo: CAPTURE** Subtipo: Resultado: ALLOW Config: Informações adicionais: Lista de Acesso MAC Resultado: interface de entrada: externo

input-status: ativado input-line-status: ativado interface de saída: externo output-status: up output-line-status: ativado Ação: permitir 1 pacote mostrado

firepower#

firepower# show capture CAPI packet-number 1 trace 5 pacotes capturados 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request 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 Tipo: ROUTE-LOOKUP Subtipo: Resolve Egress Interface Resultado: ALLOW Configuração: Informações Adicionais: localizado próximo salto 192.168.76.39 usa ifc de saída fora Fase: 4 Tipo: ACCESS-LIST Subtipo: log Resultado: ALLOW Configuração: 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 Informações Adicionais: Fase: 5 Tipo: CONN-SETTINGS Subtipo: Resultado: ALLOW Configuração: class-map class-default match any policy global policy class-default set connection advanced-options UM_STATIC TCP_MAP service-policy global policy global Informações adicionais: Fase: 6 Tipo: NAT Subtipo: per-session Resultado: ALLOW Configuração: Informações adicionais: Fase: 7 Tipo: IP-OPTIONS Subtipo: Resultado: ALLOW Configuração: Informações adicionais: Fase: 8 Tipo: INSPECT Subtipo: np-inspect Resultado: ALLOW Configuração: class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy Informações adicionais: Fase: 9 Tipo: INSPECT Subtipo: nnp p-inspect Resultado: ALLOW Configuração: Informações Adicionais: Fase: 10 Tipo: NAT Subtipo: por sessão Resultado: ALLOW Configuração: Informações Adicionais: Fase: 11 Tipo: IP-OPTIONS Subtipo: Resultado: ALLOW Configuração: Informações Adicionais: Fase: 12 Tipo: FLOW-CREATION Subtipo: Resultado: ALLOW Configuração: Informações Adicionais: Novo fluxo criado com id 52, pacote enviado para o próximo módulo Fase: 13 Tipo: ACCESS-LIST Subtipo: log Resultado: ALLOW W 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 Informações Adicionais: Fase: 14 Tipo: CONN-SETTINGS Subtipo: Resultado: ALLOW Configuração: class-map class-default match any policy-map global_policy class-default set connection opções-avançadas UM STATIC TCP MAP service-policy global policy global Informações Adicionais: Fase: 15 Tipo: NAT Subtipo: por sessão Resultado: ALLOW Configuração: Informações Adicionais: Fase: 16 Tipo: IP-OPTIONS Subtipo: Resultado: ALLOW Configuração: Informações Adicionais: Fase:

17 Tipo: ROUTE SUBTIPO DE PESQUISA: Resolver Resultado da Interface de Saída: ALLOW Config: Informações Adicionais: encontrado próximo salto 192.168.76.39 usa ifc de saída fora Fase: 18 Tipo: ADJACENCY-LOOKUP Subtipo: próximo salto e adjacência Resultado: ALLOW Config: Informações Adicionais: adjacência Endereço mac do próximo salto ativo 0004.deab.681b acerta 140372416161507 Fase: 19 Tipo: CAPTURE Subtipo: Resultado: ALALLOOKUP W Config: Informações adicionais: MAC Lista de acesso Resultado: input-interface: outside inputstatus: up input-line-status: up output-interface: outside output-status: up output-line-status: up Ação: permitir 1 pacote mostrado firepower#

A captura na interface externa mostra:

<#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
-							

10 packets shown

O rastreamento do pacote de retorno mostra que ele corresponde ao fluxo atual (52), mas é bloqueado pela ACL:

<#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

Etapa 5. Adicione mais uma regra de pré-filtro para o tráfego de retorno. O resultado é o mostrado na imagem.

Overview Analysis Policies Devices Objects AMP Deploy © System Help • mil													
Access Control > Prefilter Network Discovery Application Detectors Correlation Actions •													
Prefilter_Policy1													
Enter Descriptio	on												
Bulac													
Rules						0	Add Tunnel Rule	Add Drafilter Dula	Search Rules	X			
*	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								Def	ault Action:			

Agora, rastreie o pacote de retorno exibido (pontos importantes destacados):

Spoiler (Realce para ler)

firepower# show capture CAPO packet-number 2 trace

10 pacotes capturados

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: resposta de eco

Fase: 1

Tipo: CAPTURE

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Lista de Acesso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: ALLOW

Config:

Regra Implícita

Informações adicionais:

Lista de Acesso MAC

Fase: 3

Tipo: FLOW-LOOKUP

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Fluxo encontrado com id 62, usa fluxo atual

Fase: 4

Tipo: ACCESS-LIST

Subtipo: log

Resultado: 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

Informações adicionais:

Fase: 5

Tipo: CONN-SETTINGS

Subtipo:

Resultado: ALLOW

Config:

class-map class-default

corresponder a qualquer

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Informações adicionais:

Fase: 6

Tipo: NAT

Subtipo: por sessão

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 7

Tipo: IP-OPTIONS

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Fase: 8

Tipo: ROUTE-LOOKUP

Subtipo: Resolver interface de saída

Resultado: ALLOW

Config:

Informações adicionais:

encontrado próximo salto 192.168.75.39 usa ifc de saída interno

Fase: 9

Tipo: PESQUISA DE ADJACÊNCIA

Subtipo: next-hop e adjacência

Resultado: ALLOW

Config:

Informações adicionais:

adjacência Ativa

endereço mac do próximo salto c84c.758d.4981 atinge 140376711128802

Fase: 10

Tipo: CAPTURE

Subtipo:

Resultado: ALLOW

Config:

Informações adicionais:

Lista de Acesso MAC

Resultado:

interface de entrada: interno

input-status: ativado

input-line-status: ativado

interface de saída: interno

output-status: up

output-line-status: ativado

Ação: permitir

firepower# show capture CAPO packet-number 2 trace 10 pacotes capturados 2: 00:01:38.873123 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 Fase: 3 Tipo: FLOW-LOOKUP Subtipo: Resultado: ALLOW Configuração: Informações Adicionais: Fluxo encontrado com id 62, usa fluxo atual Fase: 4 Tipo: ACCESS-LIST Subtipo: log Resultado: ALLOW Configuração: 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 M 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 Informações adicionais: Fase: 5 Tipo: CONN-SETTINGS Subtipo: Resultado: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM STATIC TCP MAP service-policy global policy global Informações adicionais: Fase: 6 Tipo: NN AT Subtipo: por sessão Resultado: ALLOW Configuração: Informações Adicionais: Fase: 7 Tipo: IP-OPTIONS Subtipo: Resultado: ALLOW Configuração: Informações Adicionais: Fase: 8 Tipo: ROUTE-LOOKUP Subtipo: Resolve Egress Interface Resultado: ALLOW Configuração: Informações Adicionais: encontrado próximo salto 192.168.75.39 usa ifc de saída dentro da Fase: 9 Tipo: ADJACENCY-LOOKUP Subtipo: next-hop e adjacência Resultado: ALLOW Config g: Additional Information: adjacency Ative next-hop mac address c84c.758d.4981 hits 140376711128802 Fase: 10 Tipo: CAPTURE Subtipo: Resultado: ALLOW Config: Additional Information: MAC Access list Resultado: input-interface: inside input-status: up input-line-status: up output-interface: inside output-status: inside output-status: up output-line-status: up output-linestatus: up Ação: allow

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A verificação foi explicada nas respectivas seções de tarefas.

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

• Todas as versões do guia de configuração do Cisco Firepower Management Center podem ser encontradas aqui:

Navegação na documentação do Cisco Secure Firewall Threat Defense

 O Cisco Global Technical Assistance Center (TAC) recomenda enfaticamente este guia visual para conhecimento prático aprofundado sobre as tecnologias de segurança de próxima geração Cisco Firepower, que inclui as mencionadas neste artigo:

Defesa contra ameaças (FTD) do Cisco Firepower

• Para todas as Notas técnicas de configuração e solução de problemas:

Cisco Secure Firewall Management Center

<u>Suporte Técnico e Documentação - Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.