FTDプレフィルタポリシーの設定と運用

内容

 はじめに

 前提条件

 要件

 使用するコンボーネント

 背景説明

 設定

 プレフィルタボリシーの使用例1

 主要なポイント

 プレフィルタボリシーの使用例2

 タスク 1.デフォルトのプレフィルタポリシーの確認

 タスクの要件

 解決方法

 CLI(LINA)の検証

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)プレフィルタポリシーの設定と動作について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDコード6.1.0-195が稼働するASA5506X
- 6.1.0-195が稼働するFireSIGHT Management Center(FMC)
- ・ 15.2イメージを実行する2台の3925 Cisco IOS®ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

プレフィルタポリシーは6.1バージョンで導入された機能で、主に次の3つの目的に使用されます。

- 1. 内部ヘッダーと外部ヘッダーの両方に基づいてトラフィックを照合する
- 2. フローがSnortエンジンを完全にバイパスできる早期アクセス制御を提供
- 適応型セキュリティアプライアンス(ASA)移行ツールから移行されるアクセスコントロール エントリ(ACE)のプレースホルダとして機能します。

設定

プレフィルタポリシーの使用例1

PrefilterポリシーではTunnel Rule Typeを使用でき、これによりFTDは内部と外部の両方のIPヘッ ダートンネリングトラフィックに基づいてフィルタリングできます。この記事の執筆時点では、 トンネルトラフィックとは次の意味を持っています。

- 総称ルーティングカプセル化(GRE)
- IP-in-IP
- IPv6-IP
- Teredo ポート 3544

図に示すように、GREトンネルを検討します。



GREトンネルを使用してR1からR2にpingを実行すると、トラフィックはファイアウォールを通 過し、図のように見えます。

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,
Image: A state of the state							
■ Frame 1: 138 bytes on wire (1104 bits),	138 bytes capt	tured (1	104 bits)				
■ Ethernet II, Src: CiscoInc_8d:49:81 (c8)	:4c:75:8d:49:83	1), Dst:	CiscoInc_a1	:2b:f9	(6c:41:6	a:a1:2b:f9)	
Internet Protocol Version 4, Src: 192.1	.68.75.39 (192.1	168.75.3	39), Dst: 192	.168.70	5.39 (192	.168.76.39)	duter
Generic Routing Encapsulation (IP)							
Internet Protocol Version 4, Src: 10.0.	0.1 (10.0.0.1)	, Dst: 1	0.0.0.2 (10.	0.0.2)		inner	
Internet Control Message Protocol							

ファイアウォールがASAデバイスの場合は、図に示すように、外部IPヘッダーを確認します。

L2 HeaderOuter IP HeaderGRE HeaderInner IP Headersrc=192.168.75.39 dst=192.168.76.39GRE HeaderHeader src=10.0.0.1 dst=10.0.02L	7
--------------------------------------------------------------------------------------------------------------------------------------------------------	---

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

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

ファイアウォールがFirePOWERデバイスの場合、図に示すように、内部IPヘッダーがチェックさ れます。



プレフィルタポリシーを使用すると、FTDデバイスは内部ヘッダーと外部ヘッダーの両方に基づ いてトラフィックを照合できます。

主要なポイント

デバイス	チェック
ASA	外部IP
Snort	内部IP
FTD	外部(プレフィルタ)+内部IP(アクセス コントロールポリシー(ACP))

プレフィルタポリシーの使用例2

プレフィルタポリシーは、早期アクセス制御を提供し、フローが図のようにSnortエンジンを完全 にバイパスできるプレフィルタルールタイプを使用できます。



タスク 1.デフォルトのプレフィルタポリシーの確認

タスクの要件

デフォルトのプレフィルタポリシーの確認

解決方法

ステップ 1 : Policies > Access Control > Prefilterの順に移動します。図に示すように、デフォル トのプレフィルタポリシーがすでに存在します。

Overview Analysis	Policies Devices O	bjects AMF	P			Deploy) 📀	System	Help 🔻	mikis 🔻
Access Control > Prefilter	Network Discovery	Application De	etectors	Correlation	Actions •					
							Objec	ct Manager	nent Acce	ss Control
				O New I	Policy					
								_		
Prefilter Policy			Domain		Last	Modified				
Default Prefilter Policy Default Prefilter Policy w	tunnels	Global 20 Mo			-04-22 21:43 fied by "admin	25		D 🖉 6	1	

ステップ2:Editを選択し、図に示すようなポリシー設定を表示します。

Overview Analysis Policies Devices Objects AMP														
Acce	ss Contro	l ► Prefilter	Network	k Discovery	Applica	tion Detecto	rs Corr	relation	Actions •					
Defaul Defaul	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	You cannot add rules to the default Prefilter policy. You can change only default action options.													
Non	-tunneled	traffic is allow	ed	De	fault Action	n: Tunnel Trat	ffic Ar	nalyze all tur	nnel traffic					

ステップ 3 : プレフィルタポリシーは、図に示すように、アクセスコントロールポリシーにすで に割り当てられています。



CLI(LINA)の検証

プレフィルタルールはACLの上に追加されます。

<#root>

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

タスク 2.タグ付きトンネルトラフィックのブロック

タスクの要件

GREトンネル内でトンネリングされるICMPトラフィックをブロックします。

解決方法

ステップ1:これらのACPを適用すると、図に示すように、Internet Control Message Protocol(ICMP;インターネット制御メッセージプロトコル)トラフィックが、GREトンネルを 通過するかどうかにかかわらず、ブロックされていることがわかります。

Prefilter Policy: Default Prefilter Policy						SSL Policy: No	08			Ident	satity Policy: None				
_												10	Inheritance S	ettings 🧾 Policy Assignm	nents (1)
Ru	ules Security Intelligence HTTP Responses Advanced														
	🖹 Filter by Device 🔹 🗘 Add Category 🖏 Add Rule Search Rules 🗙										×				
	Name	Source	Dest	Source	Dest	MAN Trees	Brees	Indicatio	Francis Da	Devil Devile		-	Author		
	Name	zones	zones	Networks	Networks	VLAN Tags	users	Аррисано	Source Po	Dest Ports	UKLS	Attributes	Action	🙂 🍋 🔏 👘 🔳 🖷	
-	Mandatory - ACP_5506	-1 (1-1)											_		
1	Block ICMP	any	any	any	any	any	any	E Filter: ICM	P any	any	any	any	× Block	00.8 ± 20	/8
-	Default - ACP_5506-1	(-)													
775	ere are no rules in this sec	tion. Add Rule or	Add Category												
De	fault Action										Intrusion Preve	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)

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)

この場合、プレフィルタポリシーを使用してタスク要件を満たすことができます。ロジックは次 のとおりです。

- 1. GRE内にカプセル化されているすべてのパケットにタグを付けます。
- 2. タグ付きパケットに一致し、ICMPをブロックするアクセスコントロールポリシーを作成し ます。

アーキテクチャの観点からは、パケットはLInux NAatively(LINA)プレフィルタルールに照らして チェックされ、次にSnortプレフィルタルールとACPがチェックされ、最後にSnortからLINAに廃 棄が指示されます。最初のパケットはFTDデバイスを経由します。

ステップ1:トンネルトラフィックのタグを定義します。

Policies > Access Control > Prefilterの順に移動し、新しいプレフィルタポリシーを作成します。 図に示すように、デフォルトのプレフィルタポリシーは編集できないことに注意してください。

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

プレフィルタポリシー内で、次の2種類のルールを定義します。

1. トンネル規則

2. プレフィルタルール

これら2つは、プレフィルタポリシーで設定できる完全に異なる機能と考えることができます。 この作業では、図に示すようにトンネル規則を定義する必要があります。

R1#

Add Tunne	l Rule						? ×					
O Tunnel	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		¥ 0					
Interfa Encapsulati IP GRE IP-in-IP IPv6-in- Teredo I	ice Objects Networks	VLAN Tags E	ncapsulation & Ports	2'			Comment Logging					

アクションに関して

アクション	説明
分析	LINAの後、フローはSnortエンジンによってチェックされます。必要に応じて、 トンネルタグをトンネルトラフィックに割り当てることができます。
Block	フローがLINAによってブロックされています。外側のヘッダーをチェックする必 要があります。
高速パス	Snortエンジンを使用せずに、フローを処理できるのはLINAだけです。

ステップ2:タグ付きトラフィックのアクセスコントロールポリシーを定義します。

最初はあまり直感的ではありませんが、アクセスコントロールポリシールール(ACL)で送信元ゾ ーンとしてトンネルタグを使用できます。Policies > Access Controlの順に移動し、図に示すよう に、タグ付きトラフィックのICMPをブロックするルールを作成します。

_													
Ove	rview Analysis Policies De	vices Objects	АМР										Deploy
Acce	ss Control + Access Control	Network Discovery	Application Detector	Correlation	Actions •								
ACI	ACP_5506-1 Enter Description												
Prefi	Verefilter Policy Intelligence SSR. Policy I												
Rub	Rales Security Intelligence HITIP Responses Advanced												
	Fiber by Device	_	_									Add Category O Ad	Id Rule Search
•	Name	Source Zones	lest	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attributes	Action
	tandatory - ACP_5586-1 (1-1)												
1	Block ICHP	🖑 Inside,	the_GRE MY	any	877	any	any	3 Filter: ICMP	817	any .	any	any	X Block
-	Default - ACP_5506-1 (-)		_										
The	re are no rules in this section. Add Rul	le or Add Category											
Def	ault Action											Intrusion Prevention: Bal	anced Security a
_													

💊 注:新しいプレフィルタポリシーがアクセスコントロールポリシーに適用されます。

検証

LINAおよびCLISHでキャプチャを有効にします。

<#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

R1から、リモートGREトンネルのエンドポイントにpingを実行してみます。pingが失敗します。

<#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)

CLISHキャプチャは、最初のエコー要求がFTDを通過し、応答がブロックされたことを示してい ます。

<#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 18:21:11.759939 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

LINAキャプチャによってこれを確認します。

<#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
```

CLISH firewall-engine-debugを有効にし、LINA ASP dropカウンタをクリアして、同じテストを実 行します。CLISHデバッグは、エコー要求に対してプレフィルタルールに一致し、エコー応答に 対してACPルールが一致したことを示しています。

<#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 \text{ AS } 1 \text{ 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

ASPドロップは、Snortによってパケットがドロップされたことを示します。

<#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

Connection Eventsでは、次の図に示すように、一致したプレフィルタポリシーとルールを確認できます。

Ove	Overview Analysis Policies Devices Objects AMP												
Cor	text E	xplorer Connectio	ns + Events	Intrusions	Files • F	losts • Users •	Vulnerabilities • Co	rrelation • Custom •	Lookup • S	iearo	h		
	Bookmark Th												
Co	nne	ction Events	witch workflo	m)									
Con	Connections with Application Details > Table View of Connection Events												
• S	Search Constraints (<u>Edit Search</u>)												
30	Jump to 🔹												
	Г	* First Packet ×	Action ×	Initiator ×	Responder ×	Source Port / ×	Destination Port /	× Access Control ×	Access Control	×	Prefilter ×	Tunnel/Prefilter ×	
	-			IE .	IE.	ICHP LYPE	ICHP CODE	FORCY	BARE	H	FORCY	EARC	
+		2016-05-21 14:27:54	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icms	2 <u>0 / icmp</u>	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) / icms	<u>9 / icmp</u>	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) / icms	<u>0 / icmp</u>	ACP 5505-1	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) / icms	<u>9 / 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) / icms	<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) / icms	<u>9 / icmp</u>	ACP_5506-1	Block ICMP		Prefilter Policy1	Tag Tunneled traffic	
4		2016-05-21 13:15:26	Block	10.0.0.1	10.0.0.2	8 (Echo Request) / icms	<u>0 / icmp</u>	ACP 5506-1	Block ICMP		Prefilter Policy1	Tag Tunneled traffic	
1.C	< Page	1 of 1 >>> Disolar	ving rows 1-7	of 7 rows									

タスク 3.FastpathプレフィルタルールによるSnortエンジンのバ イパス

ネットワーク図



タスクの要件

- 1. 現在のアクセスコントロールポリシールールを削除し、すべてのトラフィックをブロックす るアクセスコントロールポリシールールを追加します。
- 2. 192.168.75.0/24ネットワークから送信されたトラフィックのSnortエンジンをバイパスする プレフィルタポリシールールを設定する。

解決方法

ステップ1:すべてのトラフィックをブロックするアクセスコントロールポリシーを図に示しま す。

	Enterity Intelligences VITID Responses Advanced														
in the second se	Rules Security intelligence HTTP Responses Advanced Tilter by Device Add Category										×				
# Name Source Zones Dest Zones Source Netw Dest Netw VLAN Users Appli Sourc Dest URLs ISE/ Acti															
-	▼ Mandatory - ACP_5506-1 (-)														
Th	ere are no ru	les in this se	ction. Add	Rule or Add	Category										
-	▼ Default - ACP_5506-1 (-)														
Th	There are no rules in this section. Add Rule or Add Category														
De	Default Action								Access Control: Block All Traffic				× 🧾		

ステップ 2:図に示すように、ソースネットワーク192.168.75.0/24のアクションとして Fastpathを使用するプレフィルタルールを追加します。

Add Prefilter Rule			? ×								
O Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and 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 Networks	(0)								
 Search by name or value any IPv4-Private-All-RFC1918 any-ipv4 any-ipv6 IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast 	2 192.168.75.0/24	any									
IPv4-Private-10.0.0.0-8	Enter an IP address Add	Enter an IP address	Add								

ステップ3:結果は図のようになります。

Overview	Analysis Policies	Deploy	🔉 System Help	• mikis •									
Access Control > Prefilter Network Discovery Application Detectors Correlation Actions •													
Prefilter Policy1													
Enter Description													
Rules													
Add Tunnel Rule Add Prefilter Rule Search Rules													
•	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-tunne	Non-tunneled traffic is												

ステップ4:保存して展開します。

両方のFTDインターフェイスでトレースによるキャプチャを有効にします。

<#root>

firepower#

capture CAPI int inside trace match icmp any any

firepower#

capture CAPO int outsid trace match icmp any any

FTDを介してR1(192.168.75.39)からR2(192.168.76.39)へのpingを試みます。pingが失敗します。

<#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)

内部インターフェイスのキャプチャは次のように表示されます。

<#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

最初のパケットのトレース(エコー要求)は、次のように表示されます(重要なポイントは強調 表示されています)。

スポイラー(参照用に強調表示)

firepower# show capture CAPIパケット番号1トレース

5 packets captured

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp:エコー要求

フェーズ:1

タイプ:CAPTURE

Subtype:

結果: ALLOW

Config:

Additional Information:

MAC Access list

フェーズ:2

タイプ:ACCESS-LIST

Subtype:

結果:ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

フェーズ:3

タイプ:ROUTE-LOOKUP

サブタイプ:出力インターフェイスの解決

結果:ALLOW

Config:

Additional Information:

ネクストホップ192.168.76.39が出力ifc外部を使用していることが判明しました

フェーズ:4

タイプ:ACCESS-LIST

サブタイプ:ログ

結果: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: プレフィルタポリシー: Prefilter_Policy1

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

Additional Information:

フェーズ:5

タイプ: CONN-SETTINGS

Subtype:

結果:ALLOW

Config:

クラスマップクラスデフォルト

match any

policy-map global_policy

class class-default

接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ:6

タイプ:NAT

サブタイプ:セッションごと

結果: ALLOW

Config:

Additional Information:

フェーズ:7

タイプ: IP-OPTIONS

Subtype:

結果: ALLOW

Config:

Additional Information:

フェーズ:8

タイプ:INSPECT

サブタイプ: np-inspect

結果: ALLOW

Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

インスペクションICMP

service-policy global_policy global

Additional Information:

フェーズ:9

タイプ:INSPECT

サブタイプ: np-inspect

結果:ALLOW

Config:

Additional Information:

フェーズ: 10

タイプ:NAT

サブタイプ:セッションごと

結果: ALLOW

Config:

Additional Information:

フェーズ:11

タイプ: IP-OPTIONS

Subtype:

結果: ALLOW

Config:

Additional Information:

フェーズ:12

タイプ:FLOW-CREATION

Subtype:

結果: ALLOW

Config:

Additional Information:

ID 52で作成された新しいフロー、次のモジュールにパケットがディスパッチされました

フェーズ:13

タイプ:ACCESS-LIST

サブタイプ:ログ

結果: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: プレフィルタポリシー: Prefilter_Policy1

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

Additional Information:

フェーズ:14

タイプ: CONN-SETTINGS

Subtype:

結果: ALLOW

Config:

クラスマップクラスデフォルト

match any

policy-map global_policy

class class-default

接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ:15

タイプ:NAT

サブタイプ:セッションごと

結果:ALLOW

Config:

Additional Information:

フェーズ:16

タイプ: IP-OPTIONS

Subtype:

結果:ALLOW

Config:

Additional Information:

フェーズ:17

タイプ:ROUTE-LOOKUP

サブタイプ:出力インターフェイスの解決

結果: ALLOW

Config:

Additional Information:

ネクストホップ192.168.76.39が出力ifc外部を使用していることが判明しました

フェーズ:18

タイプ: ADJACENCY-LOOKUP

サブタイプ:ネクストホップと隣接関係

結果:ALLOW

Config:

Additional Information:

隣接関係アクティブ

ネクストホップmacアドレス0004.deab.681bが140372416161507にヒット

フェーズ:19

タイプ:CAPTURE

Subtype:

結果: ALLOW

Config:

Additional Information:

MAC Access list

Result:

入力インターフェイス:外部

入力ステータス:アップ

input-line-status:up(入力回線ステータス:アップ)

出力インターフェイス:外部

出力ステータス:アップ

出力回線ステータス:アップ

アクション:許可

1 packet shown

firepower#

firepower# show capture CAPI packet-number 1 trace 5キャプチャされたパケット1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request Phase: 1タイプ: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2タイ プ: ACCESS-LIST Subtype: Result: ALLOW Config: ImPLICIT Rule AdDITIONAL Information: MAC Access Information: フェーズ: 3タイプ: ROUTE-LOOKUPサブタイプ: 出力インターフ エイスの解決結果:許可する構成:追加情報:検出されたネクストホップ192.168.76.39は出力 ifc外部を使用しますフェーズ: 4タイプ: ACCESS-LISTサブタイプ: ログ結果: ALLOW構成: access-group CSM FW ACL global access-list CSM FW ACL advanced trust ip 192.168.75.05 5.255.255.0 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追加情報: Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map-class-match any policy map global-policy class default-class-class default connection advanced-options UM STATIC TCP MAP service-policy global_policy global追加情報:フェーズ: 6タイプ: NATサブタイプ:セッション単位の結果 :許可設定:追加情報:フェーズ: 7タイプ: IP-OPTIONSサブタイプ:許可設定:追加情報 :フェーズ: 8タイプ: INSPECTサブタイプ: np-inspect結果: ALLOW Config: class-map inspection_default match-inspection-policy global_policy class inspect icmp service-policy global_policy情報:フェーズ: 9タイプ: INSPECTサブタイプ: np-inspect結果:許可 Config:追加情報:フェーズ: 10タイプ: NATサブタイプ:セッションごとの結果:許可 Config:追加情報:フェーズ: 11タイプ: IP-OPTIONSサブタイプ:結果: ALLOW Config:追 加情報:フェーズ: 12タイプ: FLOW-CREATIONサブタイプ:結果: ALLOW Config:追加情 報:新しいフローがID 52で作成され、次のモジュールにディスパッチされたフェーズ:13 Type: ACCESS-LIST Subtype: 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 268434448 event-log both access-list CSM FW ACL remark rule-id: PREFILTER POLICY: Prefilter_Policy access-list CSM 268434448: RULE: Fastpath_src_192.168.75.0/24追加情報:フェ ーズ: 14タイプ: CONN-SETTINGSサブタイプ: 結果: ALLOW Config: class-map classdefault match any policy-map global policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global追加情報:フェーズ: 15タイプ: NATサブタイプ: per-session結果: ALLOW Config:追加情報:フェーズ: 16タイプ: IP-OPTIONSサブタイプ:結果:許可Config:追加情報:フェーズ: 17タイプ: ROUTE-

LOOKUPサブタイプ:解決Egressインターフェイス結果:許可Config:追加情報: found nexthop 192.168.76.39 uses egress ifc outsideフェーズ: 18タイプ: ADJACENCY-LOOKUPサブタ イプ:ネクストホップおよびアジャセンシー結果:許可Config:追加情報:アジャセンシー関係 Activeアドレスmac 0004.deab.681b hits 140372416161507 Phase: 19タイプ: CAPTUREサブタ イプ:結果: ALLOW Config:追加情報: MACアクセスリスト結果: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: upアクション: allow 1パケットが表示されたfirepower#

Outsideインターフェイスのキャプチャは次のように表示されます。

<#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						

10 packets shown

戻りパケットのトレースには、現在のフロー(52)と一致することが示されますが、ACLによって ブロックされています。

<#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

ステップ 5 : リターントラフィック用にプレフィルタルールをもう1つ追加します。結果は図のようになります。

Overview Analysis Policies Devices Objects AMP Deploy © System Hel										
Access Control • Prefilter Network Discovery Application Detectors Correlation Actions •										
Prefilter_Policy1										
Kures							Add Tunnel Rule	Add Prefilter Rule	learch Rules	3
•	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	Festpeth_dst_192.168	Prefilter	any	any	any	2 192.168.75.0/24	any	any	any	👐 Fastpath
Non-tunneled traffic is allowed Default Ac										

次に、表示された戻りパケットをトレースします(重要な点が強調表示されています)。

<u>スポイラー</u>(参照用に強調表示)

firepower# show capture CAPO packet-number 2トレース

10 packets captured

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp:エコー応答

フェーズ:1

タイプ:CAPTURE

Subtype:

結果: ALLOW

Config:

Additional Information:

MAC Access list

フェーズ:2

タイプ:ACCESS-LIST

Subtype:

結果: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

フェーズ:3

タイプ:FLOW-LOOKUP

Subtype:

結果:ALLOW

Config:

Additional Information:

ID 62のフローが見つかりました。現在のフローを使用します

フェーズ:4

タイプ:ACCESS-LIST

サブタイプ:ログ

結果: 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:プレフィルタポリシー: Prefilter_Policy1

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

Additional Information:

フェーズ:5

タイプ: CONN-SETTINGS

Subtype:

結果: ALLOW

Config:

クラスマップクラスデフォルト

match any

policy-map global_policy

class class-default

接続の詳細設定オプションUM_STATIC_TCP_MAPを設定する

service-policy global_policy global

Additional Information:

フェーズ:6

タイプ:NAT

サブタイプ:セッションごと

結果: ALLOW

Config:

Additional Information:

フェーズ:7

タイプ: IP-OPTIONS

Subtype:

結果: ALLOW

Config:

Additional Information:

フェーズ:8

タイプ:ROUTE-LOOKUP

サブタイプ:出力インターフェイスの解決

結果:ALLOW

Config:

Additional Information:

ネクストホップ192.168.75.39が内部で出力ifcを使用していることが判明しました

フェーズ:9

タイプ: ADJACENCY-LOOKUP

サブタイプ:ネクストホップと隣接関係

結果:ALLOW

Config:

Additional Information:

隣接関係アクティブ

ネクストホップmacアドレスc84c.758d.4981が140376711128802にヒット

フェーズ: 10

タイプ:CAPTURE

Subtype:

結果:ALLOW

Config:

Additional Information:

MAC Access list

Result:

入力インターフェイス:内部

入力ステータス:アップ

input-line-status:up(入力回線ステータス:アップ)

出力インターフェイス:内部

出力ステータス:アップ

出力回線ステータス:アップ

アクション:許可

firepower# show capture CAPO packet-number 2 trace 10キャプチャされたパケット2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo reply Phase: 1タイプ: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2タイプ: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Information: MAC アクセスリストフェーズ: 3タイプ: FLOW-LOOKUPサブタイプ: 結果: ALLOW Config:追加情報: ID 62のフローが見つかりました。現在のフローを使用しています。 フェーズ: 4タイプ: ACCESS-LISTサブタイプ: ログ結果: ALLOW Config: access-group CSM FW ACL global access-list CSM FW ACL advanced trust ip any 192.168.75.0 255.255.0 rule-id 268434450 -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追加情報: Phase: 5タイプ: CONN-SETTINGSサブタイプ:結果 :許可する構成: class-map class-default match any-policy-map global_policy class-default set connection advanced-options UM STATIC TCP-MAP policy global policy global追加情報: Phase: 6タイプ: NATサブタイプ: per-session結果: ALLOW Config:追加情報: Phase: 7タ イプ: IP-OPTIONSサブタイプ: Result: ALLOW Config:追加情報: Phase: 8タイプ: ROUTE-LOOKUPサブタイプ: Resolve Egressインターフェイス結果: ALLOW Config:追加情 報: found next-hop 192.168.75.39 uses egifc inside Phase: 9タイプ: ADJACENCY LOOKUPサ ブタイプ:ネクストホップとアジャセンシー結果:許可Config:追加情報:アジャセンシー関係 アクティブなネクストホップmacアドレスc84c.758d.4981ヒット140376711128802フェーズ :10タイプ:CAPTUREサブタイプ:結果:許可Config:追加情報:MACアクセスリスト結果 :入力インターフェイス:内部input-status:up入力ラインステータス:up出力インターフェイス :内部output-status:up出力ラインステータス:upアクション:許可

確認

ここでは、設定が正常に機能しているかどうかを確認します。

検証については、それぞれのタスクセクションで説明しています。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

Cisco Firepower Management Center(FMC)コンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

<u>Cisco Secure Firewall Threat Defenseに関するドキュメントの参照</u>

 Cisco Global Technical Assistance Center(TAC)では、このドキュメントで説明されている 内容を含む、Cisco Firepower次世代セキュリティテクノロジーに関する詳細で実用的な知 識を得るために、このビジュアルガイドを強く推奨しています。

<u>Cisco Firepower Threat Defense (FTD)</u>

・設定とトラブルシューティングに関するすべてのテクニカルノート:

<u>Cisco Secureファイアウォール管理センター</u>

• <u>テクニカル サポートとドキュメント - Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。