Calcule a contagem de elementos da lista de acesso (ACE) usando a CLI do FMC

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Como calcular a ACE (Access List Element Count, contagem de elementos da lista de acesso) usando a CLI do FMC Impacto da alta ACE Decidir Quando Ativar a Pesquisa de Grupos de Objetos (OGS) Ativando a Pesquisa de Grupos de Objetos Verificar Informações Relacionadas

Introdução

Este documento descreve como você pode localizar qual regra em sua política de controle de acesso está se expandindo para quantos elementos da lista de acesso.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- · Conhecimento da tecnologia Firepower
- Conhecimento sobre a configuração das políticas de controle de acesso no FMC

Componentes Utilizados

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

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower

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 regra de controle de acesso é criada com o uso de uma ou várias combinações destes parâmetros:

- Endereço IP (origem e destino)
- Portas (origem e destino)
- URL (Categorias fornecidas pelo sistema e URLs personalizadas)
- Detectores de aplicativos
- VLANs
- Zonas

Com base na combinação de parâmetros usados na regra de acesso, a expansão da regra muda no sensor. Este documento destaca várias combinações de regras no FMC e suas respectivas expansões associadas nos sensores.

Como calcular a ACE (Access List Element Count, contagem de elementos da lista de acesso) usando a CLI do FMC

Considere a configuração de uma regra de acesso do FMC, como mostrado na imagem:

Ę	Policies / /	I Manage Access Contro	ment Cen of / Policy Edito	ter	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	6 ⁰⁰ ¢0	adm	in ~	cisco	SEC	URE
•	Port-scan test Enter Description Try New UI Layout D Analyze Hit Counts Save Cancel																		
Rules Security Intelligence HTTP Responses Logging Advanced Prefiter Policy: Default Prefiter Policy Decryption Policy: None Identity Policy: None Eilter by Device Search Rules Search Rules X Search Rules Add Category 4 Add Rules																			
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destina Dynamic Attributes	Action	F0 \$	G , <i>R</i>			¢
~ 1	✓ Mandatory - Port-scan test (1-1)																		
1	Rule 1	Any	Any	10.1.1.1 10.2.2.2	10.3.3.3 10.4.4.4	Any	Any	Any	Any	TCP (6):80 TCP (6):443	Any	Any	Any	Allow	P5 🖤	B 2		0	/1
V Default - Port-scan test (-)																			
The	There are no rules in this section. Add Rule or Add Category																		

Configuração de Regra na Política de Controle de Acesso

Se você vir essa regra na CLI de FTD, perceberá que essa regra foi expandida em 8 Regras.



Você pode verificar qual regra está se expandindo para quantos elementos da lista de acesso usando o comando perl na CLI do FMC:

<#root>

perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

root@firepower:/Volume/home/admin# perl /var/opt/CSC0px/bin/access_rule_expansion_count.pl

Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

Access Control Rule Expansion Computer

Enter FTD UUID or Name:

> 10.70.73.44

Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

Access Control Rule Expansion Computer

Device:

UUID: 93cc359c-39be-11d4-9ae1-f2186cbddb11

Name: 10.70.73.44

Access Control Policy:

UUID: 005056B9-F342-0ed3-0000-292057792375

Name: Port-scan test

Description:

Intrusion Policies:

UUID	NAME		I
Date: 2024-Jul-17 at 06:51:55 UTC			
NOTE: Computation is done on per rule b	basis. Count from shadow rule	es will not b	pe applicable on device
Run "Rule Conflict Detection" tool on A	AC Policy for specified devic	ce to detect	and optimise such rul
	NAME	 I	COUNT
005056B9-F342-0ed3-0000-000268454919	Rule 1	 	8
TOTAL: 8			
Access Rule Elements Count on FTD: 14			

>>> My JVM PID : 19417



Nota: Elementos da Regra de Acesso Contam no FTD: 14. Isso também inclui o conjunto padrão de regras de FTD (pré-filtro) e a regra de controle de acesso padrão.

As regras de pré-filtro padrão podem ser vistas na CLI do FTD:

access light period (d) los (lows tatel & dealed & (dealed & (dealed & (dealed &)
access-tist cached Act tog flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list CSM_FM_ACL_; 14 elements; name hash: 0x4a69e3t3
access-inst CSM_FM_ACL_ line I remark rule-id 9998: PKEFILTER POLICY: Default funnel and Priority Policy
access-inst CSM_FW_ACL_ the 2 remark rule-10 9998; RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FM_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcht=0) 0x15559766
access-list CSM_FM_ACL_ Line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (httcht=0) 0x4607839e
access-tist CSM_FM_ALL_ time 5 advanced permit uop any range 1025 05335 any ed 3544 fule=10 3938 (http://www.artidsaas
access-tist CSR_FM_ACL_ time 6 advanced permit 41 any any rule-id 9986 (http://www.sweessada
access-tist CSA_FM_ACLtime / advanced permit gree any any rule=10 grads (nitcht=0) 0522/ad060
access-tist CSA_FM_ACL time & remark rule=10 200494222 ACCESS FOLCES. FOTC-SCAR LESC - Mandatory
access-tist CSA_TM_ACL_ time 5 femant Futerio 200494922. F. Roter A Mile 1 Decess-tist CSA_TM_ACL_ time 5 femant Futerio 200494922. F. Roter A Mile 1 and A Mile
access-tist CSA_TA_CC_ time to auvaiced permit CCP OUPCLER OUP TALLETS : _ ute_zood94522 OUPCTRUE TALLETS C_ Ute_zood94522 et www.ilete-to 200454522 (inclite-o) 0x40001500
access-tist CSM_tm_RCL_ time to advance permit tup host 10.1.1.1 host $10.3.1.3$ eq www rule=10.2004/922 (hitratis) 0x04010031
accessitist CSM Figure 1 advanced permit top host 10.2.2.2 host 10.3.3.3 en www rule=1d 268450422 (hitcht=0) 0x6cf6481d
access-list CSM FW 4CL line 10 advanced parmit to host 10.2.2.2 host $10.4.4.4$ or www rule-id 268454922 (hitchiel) 0x9d098336
access-list CSM_EM_ACL_line 11 advanced permit to phiet-group EMC TNLTNE stc rule 268454922 object-group EMC TN
access-list CSM FW ACL line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
access-list CSM FW ACL line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcht=0) 0x837a795d
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eg https rule-id 268454922 (hitcht=0) 0x42a0ae77
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a

Impacto da alta ACE

- Pode-se ver uma CPU alta.
- A memória alta pode ser vista.
- A lentidão do dispositivo pode ser observada.
- Falha nas implantações/Tempo de implantação mais longo.

Decidir Quando Ativar a Pesquisa de Grupos de Objetos (OGS)

- A contagem de ACEs está excedendo o limite de ACEs do dispositivo.
- A CPU do dispositivo ainda não está alta, pois a ativação de OGS aumenta a pressão sobre a CPU do dispositivo.
- Habilite-o durante horas que não sejam de Produção.



Cuidado: habilite o asp rule-engine transactional-commit access-group do modo de clish FTD CLI antes de habilitar o OGS. Isso é configurado para evitar quedas de tráfego durante e logo após o processo de implantação ao habilitar o OGS.



Ativando a Pesquisa de Grupos de Objetos

No momento, o OGS não está habilitado:



1. Faça login na CLI do FMC. Navegue até Devices > Device Management > Select the FTD device > Device. Ative a Pesquisa de grupo de objetos nas Configurações avançadas:

Firewall Management C Devices / Secure Firewall Device	<mark>enter</mark> Overview A Summary	Analysis Policies Devices	Objects Integration	Deploy 🔍 🎸 🥸	admin ~ cisco SECURE
10.70.73.44 Cisco Firepower 2130 Threat Defense Device Routing Interfaces	Inline Sets DHCP SN	MP .			
Revent to Short 2		Policy: Initial_Heal	Ith_Policy 2021-05-02 02:35:06	Secondary Address:	
		Advanced Settings	0	Status:	0
				Manager Access Interface:	Management Interface
		Automatic Application Bypass:			
		Bypass Threshold (ms): 3	3000		
Inventory Details	c	Object Group Search: 🗸		Advanced Settings	/
CPU Type:	CPU MIPS 1200 MHz	Interface Object Optimization:		Application Bypass:	No
CPU Cores:	1 CPU (12 cores)			Bypass Threshold:	3000 ms
Memory;	13701 MB RAM			Object Group Search:	Disabled
Storage:	N/A	Cancel Save		Interface Object Optimization:	Disabled
Chassis URL:	N/A	Identity Policy:			
Chassis Serial Number:	N/A	NAT Policy:	Port-scan test		
Chassis Module Number:	N/A	Platform Settings Policy:	po		
Chassis Module Serial	N/A	QoS Policy:			
Number:		Zero Trust Application Policy:			

2. Clique em Salvar e implantar.

Verificar

Antes de o OGS ser habilitado:

firepower# show access-list	
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)	
alert-interval 300	
access-list CSM_FW_ACL_; 14 elements; name hash: 0x4a69e3f3	
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: 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 udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e	
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5	
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba	
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066	
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory	
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1	
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www_ule-id 2	
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57	
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xeced82d1	
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf481d	
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d098336	Expanding
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq http_rule_1	
	to O Dullas
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78	to 8 Rules.
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x837a795d	
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77	
access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17	
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default	
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE	
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a	
firenower#	

Depois que o OGS for habilitado:

<pre>firepower# show access-list access-list cached ACL Ug flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 309 access-list CSM_PM_ACL_; line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_PM_ACL_, line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_PM_ACL_, line 2 aremark rule-id 9998: REFEAULT TUNNEL ACTION RULE access-list CSM_PM_ACL_, line 3 advanced permit udp any rule-id 9998 (hitcnt=0) 0x/56597d6 access-list CSM_PM_ACL_ line 6 advanced permit 10 any rule-id 9998 (hitcnt=0) 0x/567866 access-list CSM_PM_ACL_ line 6 advanced permit 11 any any rule-id 9998 (hitcnt=0) 0x3614 access-list CSM_PM_ACL_ line 6 advanced permit 14 any any rule-id 9998 (hitcnt=0) 0x36278666 access-list CSM_PM_ACL_ line 6 advanced permit top object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq www.rule-id 68454922 (hitcnt=0) 0x1071fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-1-acce access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-1-acce access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-1-acce access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-1-acce access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-1-acce access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454923 (2147483648) v4-</pre>		
access-list CSM_PM_ACL_line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 288453888: L4 RULEs DFFAULT ACTION RULE access-list CSM_PM_ACL_line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 288453888: L4 RULEs PC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 288453888: L4 RULEs PC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 288454922 eq https: rule-id 288454		
alert-interval 300 access-list GSH_PM_ACL, line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list GSH_PM_ACL, line 2 aremark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list GSH_PM_ACL, line 3 advanced permit upd any rule-id 9998 (hitcatt=0) 0xf5b597d6 access-list CSH_PM_ACL, line 4 advanced permit upd any rule-id 9998 (hitcatt=0) 0xf5b597d6 access-list CSH_PM_ACL, line 6 advanced permit upd any rule-id 9998 (hitcatt=0) 0xf5b597d6 access-list CSH_PM_ACL, line 6 advanced permit upd any rule-id 9998 (hitcatt=0) 0x52c7a066 access-list CSH_PM_ACL, line 6 advanced permit upd 9998 (hitcatt=0) 0x52c7a066 access-list CSH_PM_ACL, line 10 advanced permit top bolet-group FMC_INLINE_src_rule_268454922 (bitcatt=0) 0x65454922 (hitcatt=0) 0x65454922 (hitcatt=0) 0x62f45422 = compression for the 10 advanced permit top bolet-group FMC_INLINE_src_rule_268454922 (bitcatt=0) 0x071fd2 access-list CSH_PM_ACL, line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule=14 access-list CSM_PM_ACL, line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule=14 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule=14 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule=14 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_26845 access-list CSM_PM_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 13 advan	access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)	
access-list CSM_PM_ACL_ ine 1 memorts; name hash: 8/4a599a3/3 access-list CSM_PM_ACL_ line 1 memorts; name hash: 8/4a599a3/3 access-list CSM_PM_ACL_ line 2 memorts rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_PM_ACL_ line 3 advanced permit tipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6 access-list CSM_PM_ACL_ line 4 advanced permit up any eq 3544 any range 1025 65335 rule-1d 9998 (hitcnt=0) 0x46d7839e access-list CSM_PM_ACL_ line 5 advanced permit up any eq 3544 any range 1025 65335 rule-1d 9998 (hitcnt=0) 0x46d7839e access-list CSM_PM_ACL_ line 6 advanced permit up any range 1025 65335 rule-1d 9998 (hitcnt=0) 0x46d7839e access-list CSM_PM_ACL_ line 7 advanced permit up any range 1025 65335 rule-1d 9998 (hitcnt=0) 0x3f1d5aa5 access-list CSM_PM_ACL_ line 8 memork rule-id 268454922: l7 RULE: Rule 1 access-list CSM_PM_ACL_ line 10 advanced permit top object-group FMC_INLINE_acc.rule_268454922 (bject-group FMC_INLINE_dst_rule_268454922 eq www rule-id 58454922 (hitcnt=0) 0x1071fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top object-group FMC_INLINE_src_rule_268454922 (bject-group FMC_INLINE_dst_rule_268454922 eq https: rule- 268454922 (hitcnt=0) 0x1071fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (bject-group FMC_INLINE_dst_rule_268454922 eq https: rule- 268454922 (hitcnt=0) 0x04349953 access-list CSM_FM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 (x 268454922 (hitcnt=0) 0x04349953 access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: ACEESS POLICY: Port=acan test - Default access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: ACEESS POLICY: Port=acan test - Default access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: ACEESS POLICY: Port=acan test - Default access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: L4 RUL		
access-list CSM_PM_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_PM_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_PM_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xfsb597d6 access-list CSM_PM_ACL_ line 4 advanced permit upinip any any rule-id 9998 (hitcnt=0) 0xfsb597d6 access-list CSM_PM_ACL_ line 5 advanced permit upinip any any rule-id 9998 (hitcnt=0) 0xfsb597d6 access-list CSM_PM_ACL_ line 6 advanced permit upinip any any rule-id 9998 (hitcnt=0) 0xfsb597d6 access-list CSM_PM_ACL_ line 6 advanced permit upinip any any rule-id 9998 (hitcnt=0) 0x66095aba access-list CSM_PM_ACL_ line 7 advanced permit upinip u	access-list CSM_FW_ACL_; 8 elements; name hash: 0x4a69e3f3	
access-list CSM_PM_ACL_ line 3 advanced permit upt any eq 3544 any range 1025 65535 rule-1d 9998 (hitcht=0) 0xf5b597d6 access-list CSM_PM_ACL_ line 4 advanced permit upt any rule-id 9998 (hitcht=0) 0xf5b597d6 access-list CSM_PM_ACL_ line 4 advanced permit upt any range 1025 65535 rule-1d 9998 (hitcht=0) 0xaf1d5aa5 access-list CSM_PM_ACL_ line 5 advanced permit upt any rule-id 9998 (hitcht=0) 0x5627a066 access-list CSM_PM_ACL_ line 7 advanced permit upt any rule-id 9998 (hitcht=0) 0x5627a066 access-list CSM_PM_ACL_ line 8 remark rule-id 268454922: LT RULE: Rule 1 access-list CSM_PM_ACL_ line 10 advanced permit top object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www.rule-id 168454 access-list CSM_PM_ACL_ line 10 advanced permit top object-group FMC_INLINE_src_rule_268454922 (bitcht=0) 0x1671fd22 access-list CSM_PM_ACL_ line 11 advanced permit top vobject-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-12-26845 2222(222) (hitcht=0) 0x1671fd22 2268454922 (hitcht=0) 0x1671fd23 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-12-26845 2268454922 (hitcht=0) 0x0671fd23 2268454922 (hitcht=0) 0x067480955 access-list CSM_PM_ACL_ line 11 advanced permit top V4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454928 (22147483648) v4-object-group FMC_INLINE_dst_rule_268454988 v4022 (2147483648)	access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy	
access-list CSM_FM_ACL_ line 3 advanced permit ipinip any any rule-id 9988 (hitcht=0) 0xf5b597d6 access-list CSM_FM_ACL_ line 4 advanced permit udp any range 1025 65535 rule-id 9998 (hitcht=0) 0x46d7839e access-list CSM_FM_ACL_ line 5 advanced permit udp any range 1026 65535 any eq 3544 rule-id 9998 (hitcht=0) 0x46d7839e access-list CSM_FM_ACL_ line 5 advanced permit udp any rule-id 9986 (hitcht=0) 0x66095aba access-list CSM_FM_ACL_ line 7 advanced permit udp any rule-id 9986 (hitcht=0) 0x527a666 access-list CSM_FM_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory access-list CSM_FM_ACL_ line 10 advanced permit tcp bdject=group FMC_INLINE_src_rule_268454922 (bdject-group FMC_INLINE_dst_rule_268454922) eq www rule-id 268454922 (bdject-group FMC_INLINE_dst_rule_268454922) eq www rule-id 268454922 (bdject-group FMC_INLINE_src_rule_268454922) advanced permit tcp bdject=group FMC_INLINE_src_rule_268454922 (bdject-group FMC_INLINE_dst_rule_268454922) eq https: rule-id 268454922 (cdframe=1) advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (bdject-group FMC_INLINE_dst_rule_268454922) eq https: rule-id 268454922 (cdframe=1) advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922) eq https: rule-id 268454922 (cdframe=1) advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (cdframe=1) advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 268454922 (cdframe=1) advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https: rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_FM_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_scan test - Default access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: IA RUE: DEFAULT ACTION RUE access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: IA RUE: DEFAULT ACTIO	access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE	
access-list CSM_PM_ACL_ line 4 advanced permit udp any range 1025 65353 srule-1d 9998 (hitcht=0) 0x66095aba access-list CSM_PM_ACL_ line 5 advanced permit 41 any any rule-1d 9998 (hitcht=0) 0x52678066 access-list CSM_PM_ACL_ line 6 advanced permit gre any any rule-1d 9998 (hitcht=0) 0x52678066 access-list CSM_PM_ACL_ line 7 meark rule-id 268454922: CT RULE: Rule 1 access-list CSM_PM_ACL_ line 10 advanced permit top object-group FMC_INLINE_src_rule_268454922 (pict-group FMC_INLINE_dst_rule_268454922 eq www.rule-id 168454 9222 (hitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pict-group FMC_INLINE_dst_rule_268454922 eq https:rule-1-26845 9222 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x10971fdd2 access-list CSM_PM_ACL_ line 11 advanced permit top v4-object-group FMC_INLINE_src_rule_268454922 (pitcht=0) 0x0430953 access-list CSM_PM_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 14 advanced deny ip any any rule-id 2684538888 (hitcht=0) 0x07a021a frequences	access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6	
access-list CSM_PM_ACL_line 5 advanced permit udp any range 1025 6535 any eq 3544 rule-1d 9988 (hitcht=0) 0xaf1d5aa5 access-list CSM_PM_ACL_line 6 advanced permit 1 any any rule-1d 9988 (hitcht=0) 0x66095bab access-list CSM_PM_ACL_line 8 remark rule-1d 268454922: XCCESS POLICY: Port-scan test - Mandatory access-list CSM_PM_ACL_line 9 remark rule-1d 268454922: XCCESS POLICY: Port-scan test - Mandatory access-list CSM_PM_ACL_line 1 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922: eq www rule-1d 668454 access-list CSM_PM_ACL_line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-1d 668454 access-list CSM_PM_ACL_line 11 advanced permit tcp vd-object-group FMC_INLINE_scc_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp vd-object-group FMC_INLINE_src_rule_268454922 (2147483648) vd-object-group FMC_INLINE_dst_rule_26845922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp vd-object-group FMC_INLINE_src_rule_268454922 (2147483648) vd-object-group FMC_INLINE_dst_rule_26845922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp vd-object-group FMC_INLINE_src_rule_268454922 (2147483648) vd-object-group FMC_INLINE_dst_rule_26845922 eq https rule-1 268454922 (hitcht=0) 0x304499545 access-list CSM_PM_ACL_line 12 remark rule-id 268453888: ACCES5 POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 13 remark rule-id 268453888 (httcnt=0) 0x97a9021a freepower8	access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e	
access-list CSM_PM_ACL_ line 6 advanced permit 41 any any rule-id 9988 (hitchtte) 0x562593ba access-list CSM_PM_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitchtte) 0x52c73066 access-list CSM_PM_ACL_ line 8 remark rule-id 268454922: LT RULE: Rule 1 access-list CSM_PM_ACL_ line 9 remark rule-id 268454922: LT RULE: Rule 1 access-list CSM_PM_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_PM_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_FM_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_FM_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_FM_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_FM_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex ex exact list CSM_FM_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_FM_ACL_ line 13 remark rule-id 268453888: AR ULE: DEFAULT ACTION RULE access-list CSM_FM_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcht=0) 0x97aa021a frequences	access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5	
access-list CSM_PM_ACL_line 12 advanced permit gre any any rule-1d 9998 (hitchtel) 0x5273066 access-list CSM_PM_ACL_line 9 remark rule-id 268454922: ACESS POLICY: Port-scan test - Mandatory access-list CSM_PM_ACL_line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 8845922 (hitchtel) 8x1071fd2 access-list CSM_PM_ACL_line 11 advanced permit tcp vobject-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp vobject-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp v0-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-1 access-list CSM_PM_ACL_line 11 advanced permit tcp v0-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-1 268454922 (hitchte)) 0x94499950 access-list CSM_FM_ACL_line 12 advanced permit tcp 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_FM_ACL_line 13 remark rule-id 268453888 (hitchte) 0x97a9021a frepower#	access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba	
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1 access-list CSM_FW_ACL_ Line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id for the source of the sourc	access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066	
access-list CSM_FW_ACL_ line 19 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 68454 access-list CSM_FW_ACL_ line 10 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 68454 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 68454 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex eq https rule-id 268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex eq https rule-id 268454922 ex	access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory	
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 66454 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 66454 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 66454 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 ex access-list CSM_FW_ACL_ line 12 remark rule-id 268453888 : ACCESS POLICY: Port-scan test - Default access-list CSM_FW_ACL_ line 13 remark rule-id 268453888 : L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a ffrepower#	access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1	
access-list CSM_FW_ACL_ line 10 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_268454922(3 Expanding to access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 en https rule-10 for an access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 en https rule-10 for an access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 en https rule-10 for an access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 en https rule-10 for an access-list CSM_FW_ACL_ line 12 remark rule-11 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_268454922 en https rule-11 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_26845492 en https rule-12 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 en https rule-12 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 en https rule-12 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 en https rule-12 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 en https rule-12 for advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 en https rule-12 for advanced permit en h	access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454	
S8454922 (hitcht=0) 0x1071fdd2 access=list CSM_FW_ACL_ line 11 advanced permit tcp object-group FWC_INLINE_src_rule_268454922 object-group FWC_INLINE_dst_rule_268454922 eq https rule=1 advanced permit tcp v4-object-group FWC_INLINE_src_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_src_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454923(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454922(2147483648) v4-object-group FWC_INLINE_dst_rule_268454923(2147483648) v4-object-group FWC_INLINE_dst_rule_26845388(hitcht=0) 0x97aa021a frepowers	access-list CSM_FW_ACL_ line 10 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_268454922(2	Expanding to
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-15-3644 access-list CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922 (2147483648) v4-object-group FMC_INLINE_dst_rule_26845 922(1 268454922 (nitcnt:e0) 0x944a995a access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: A RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a ffrepomer#	68454922 (hitcht=0) 0x1071fdd2	Experient8 to
access-list CSM_PW_ACL_ line 11 advanced permit top V4-object-group FMC_INLINE_src_rule_268454922(2147483648) V4-object-group FMC_INLINE_dst_rule_268454922(2 268454922 (hitchted) 8x944a995a access-list CSM_PM_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PM_ACL_ line 13 remark rule-id 268453888: AL RULE: DEFAULT ACTION RULE access-list CSM_PM_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcht=0) 8x97aa821a frepomer#	access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-i	only 2 Rules.
access-list CSM_FW_ACL_ line 11 advanced permit tcp V4-object-group FWC_INLINE_src_rule_268454922(2147483648) V4-object-group FWC_INLINE_dst_rule_268451922(2 268454922 (1intcnte) 0 W20449953 access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a firepower#		only 2 mateou
26843922 (http://doi.org/1016127993) access-list CSM_PACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_PALAL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_FALACL_ line 14 advanced deny ip any any rule-id 268453888 (hitch:0) 0x97aa021a Hrepomer#	access-List CSM_FW_ACL_ line 11 advanced permit tcp v4-object-group FMC_INLINE_src_rule_268454922(2147483648) v4-object-group FMC_INLINE_dst_rule_26845	
access-list CSM_EW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default access-list CSM_EM_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_EM_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a firepower#	268454922 (hitcht=0) 0x944a995a	
uccess-list CSM_PM_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE access-list CSM_PM_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a firepower≇ ∎	access-list CSM_FW_ACL_ line 12 remark rule-1d 2684538888: ACCESS POLICY: Port-scan test - Default	
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcht=0) 0x97aa021a firepower# 📲	access-list CSM_FW_ACL_ line 13 remark rule-1d 2684538888: L4 RULE: DEFAULT ACTION RULE	
f1repower#	access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcht=0) 0x97aa021a	
	F1repower#	

Informações Relacionadas

Para obter informações mais detalhadas sobre como as regras são expandidas no FTD, consulte o documento <u>Compreender a expansão de regras em dispositivos FirePOWER</u>.

Para obter mais informações sobre a arquitetura e a solução de problemas do FTD, consulte <u>Dissecting (FTD) Firepower Threat Defense</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.