Het aantal toegangslijsten met elementen (ACE) berekenen met behulp van FMC CLI

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Hoe te om het Aantal van het Element van de Toegangslijst (ACE) te berekenen die FMC CLI gebruiken Impact van High ACE Beslissen wanneer het inschakelen van Object Group Search (OGS) Zoeken in objectgroepen inschakelen Verifiëren Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u kunt vinden welke regel in uw toegangscontrolebeleid zich uitbreidt tot hoeveel toegangslijstelementen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER-technologie
- · Kennis over het configureren van het toegangscontrolebeleid op het VCC

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een toegangscontroleregel wordt gecreëerd met het gebruik van een of meer combinaties van deze parameters:

- IP-adres (bron en bestemming)
- Poorten (bron en bestemming)
- URL (door systeem opgegeven categorieën en aangepaste URL's)
- Toepassingsdetectoren
- VLAN's
- Zones

Gebaseerd op de combinatie van parameters die in de toegangsregel worden gebruikt, verandert de regeluitbreiding op de sensor. In dit document worden verschillende combinaties van regels voor het VCC en de bijbehorende uitbreidingen op de sensoren belicht.

Hoe te om het Aantal van het Element van de Toegangslijst (ACE) te berekenen die FMC CLI gebruiken

Overweeg de configuratie van een toegangsregel vanuit het VCC, zoals getoond in de afbeelding:

Firewall Management Center Policies / Access Control / Policy Editor			Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	🌮 🌣 🔞	adm	in ~	cisco S	ECU	RE		
Port-scan test Enter Description Try New UI Layout Analyze Hit Counts Save Cancel																			
Rules Security Intelligence HTTP Responses Logging Advanced Prefiter Policy: Default Prefiter Policy Decryption Policy: None Identity Policy: None																			
Fille	Enter by Device Y Search Rules X Show Rule Conflicts + Add Category + Add Rule																		
#	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	Fo 🛡	6 , <u>2</u>		-	¢
$\sim Ma$	✓ 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	C Allow	₽, ●	B 2	ō 8	0 🌶	Ì
V Default - Port-scan test (-)																			
There are no rules in this section. Add Rule or Add Category																			

Regelconfiguratie in toegangscontrolebeleid

Als je deze regel ziet in FTD CLI, merk je dat deze regel is uitgebreid tot 8 regels.



U kunt controleren welke regel zich uitbreidt in hoeveel toegangslijst-elementen met behulp van de perl-opdracht in FMC CLI:

<#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



Opmerking: elementen in toegangsregels tellen op FTD: 14. Dit omvat ook de standaardset FTD-regels (Pre-filter) en Default Access Control-regels.

De standaard Pre-filter regels zijn te zien in FTD CLI:

firepower# show access-list access-list cached AT log flows: total 0. denied 0. (denu-flow-max 4006)
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 (hitcht=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 rule-id 268454922 (hitcnt=0) 0x46def508
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 (hitcht=0) 0x046f6567
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 (hitcht=0) 0xeced82d1
access-inst CSM_FW_ACL_ time 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-10 268454922 (hitchT=0) 0x16cT4810
access-inst CSM_FW_ACL_ time is advanced permit tcp nost 10.2.2.2. Nost 10.4.4.4.4 eq www rule-10 Z68454922 (http://www.sube-10.2.68454922 (http://www.sube-10.2.6845492 (http://www.sube-10.2.68454922 (http://www.sube-10.2.6845492 (http://www.sube-10.2.6845482 (http://www.sube-10.2.6845482 (http://wwww.sube-10.2
access-list CSM_HW_ALL_ line ii advanced permit tcp object-group FMC_INLINE_src_rule_z68454922 object-group FMC_INLINE_DST_rule_z68454922 ed https rule-id 268454922 (https://www.access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access.com/access
accessite CSN EW ACL line 11 advanced permit ten hert 10 1 1 1 hert 10 2 2 2 en https://doi.org/10.0001620470
access that the final transmission of the first 10.111 host 10.333 eq (https://doi.org/10.0000/000000000000000000000000000000
access that the full of a light and access prime to be the set of
access the Centre and a contract prime contract of the state and a contract of the state access the contract (intenter) Avs60bie17
accession of the later of the l
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

Impact van High ACE

- Hoge CPU is zichtbaar.
- High Memory kan worden gezien.
- Er kan traagheid van het apparaat worden waargenomen.
- Uitval van implementaties/langere implementatietijd.

Beslissen wanneer het inschakelen van Object Group Search (OGS)

- Het aantal ACE-cellen overschrijdt de ACE-grenswaarde van het apparaat.
- De CPU van het apparaat is nog niet hoog omdat OGS meer druk op de CPU van het apparaat legt.
- Schakel dit tijdens niet-productie-uren in.



Waarschuwing: Schakel asp rule-engine transactional-commit access-group in vanuit FTD CLI clish-modus voordat u de OGS inschakelt. Dit is ingesteld om te voorkomen dat het verkeer tijdens en vlak na het implementatieproces daalt terwijl OGS wordt ingeschakeld.



Zoeken in objectgroepen inschakelen

Op dit moment is OGS niet ingeschakeld:



1. Log in bij FMC CLI. Navigeer naar Apparaten > Apparaatbeheer > Selecteer het FTDapparaat > Apparaat. Het zoeken in de objectgroep vanuit geavanceerde instellingen inschakelen:

Firewall Management Center Overview Analysis Policies Devices Objects Integration Depicy Q 🧬 🔅 🔕 admin 🗸 端 SECU											
10.70.73.44 Cisco Firepower 2130 Threat Defense Device Routing Interfaces Inline Sets DHCP SNMP											
Revert to Short 2		Policy: Initial_	Health_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):	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:	ро								
Chassis Module Serial	N/A	QoS Policy:									
Nümber:		Zero Trust Application Policy	6								

2. Klik op Opslaan en implementeren.

Verifiëren

Voordat OGS is ingeschakeld:



Nadat OGS is ingeschakeld:



Gerelateerde informatie

Raadpleeg voor meer informatie over het uitbreiden van regels in het FTD het document <u>Understand the Rule Expansion on FirePOWER Devices</u>.

Raadpleeg <u>FTD</u> (<u>Firepower Threat Defence</u>) voor meer informatie over de FTD-architectuur en probleemoplossing.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.