FMC CLI를 사용하여 ACE(Access List Element) 수 계산

목차

소개

이 문서에서는 액세스 제어 정책에서 어떤 규칙이 얼마나 많은 액세스 목록 요소로 확장되는지를 찾는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 기술에 대한 지식
- FMC에서 액세스 제어 정책 구성에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Firepower 위협 방어)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

액세스 제어 규칙은 다음 매개변수 중 하나 또는 여러 조합을 사용하여 생성됩니다.

- IP Address(IP 주소)(Source and Destination)
- 포트(소스 및 대상)
- URL(시스템 제공 범주 및 맞춤형 URL)
- 애플리케이션 탐지기
- VLAN
- 영역

액세스 규칙에서 사용되는 매개변수의 조합에 따라 센서에서 규칙 확장이 변경됩니다. 이 문서에서 는 FMC의 다양한 규칙 조합 및 센서에서 각 관련 확장을 중점적으로 살펴봅니다.

FMC CLI를 사용하여 ACE(Access List Element Count)를 계산하 는 방법

그림과 같이 FMC에서 액세스 규칙의 컨피그레이션을 고려하십시오.

5	Policies / A	I Manager	ment Cen of / Policy Edito	ter	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	Q	p ¢ 🖗	adr	nin ~	-1)- 615	co SE	CUR	E
Port-scan test Try New UI Layout Analyze Hit Counts									Ca	incel										
	Rules Secu	rity Intelligen	ce HTTP	Responses	Logging	Advanced	i			Prefilter Policy	y: Default Pref	filter Policy	Decrypt	Inheritance ion Policy:	Setting: None	l Po Id	licy As lentity	Policy	ents : Non	<u>(1)</u> ie
E	ilter by Device	T Search	n Rules								×	Show R	tule Conflic	ts 🛛 +	Add Cat	egory	-	⊢ Ado	l 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	P6 0	0.	A 🗆	8,	•	¢
\sim	Mandatory - Por	t-scan test (1	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	15 0	\mathbb{I}_{0}^{-}	20	Ē.	• /	Ì
\sim	Default - Port-so	an test (-)																		
Th	There are no rules in this section. Add Pule or Add Category																			

액세스 제어 정책의 규칙 컨피그레이션

FTD CLI에서 이 규칙이 표시되는 경우, 이 규칙이 8개의 규칙으로 확장되었음을 알 수 있습니다.



FMC CLI에서 perl 명령을 사용하여 어떤 규칙이 얼마나 많은 액세스 목록 요소로 확장되고 있는지 확인할 수 있습니다.

<#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



참고: FTD의 액세스 규칙 요소 개수: 14. 여기에는 기본 FTD 규칙 집합(Pre-filter) 및 기본 액세스 제어 규칙도 포함됩니다.

기본 사전 필터 규칙은 FTD CLI에서 확인할 수 있습니다.



High ACE의 영향

- 높은 CPU가 표시됩니다.
- High Memory(높은 메모리)를 확인할 수 있습니다.
- 장치 느림을 관찰할 수 있습니다.
- 구축 실패/구축 시간 연장

OGS(Object Group Search) 활성화 시기 결정

- ACE 수가 디바이스 ACE 제한을 초과합니다.
- OGS를 활성화하면 디바이스 CPU에 부담이 가중되므로 디바이스의 CPU가 아직 높지 않습 니다.
- 비생산 시간 동안 활성화합니다.



주의: OGS를 활성화하기 전에 FTD CLI 클라이언트 모드에서 asp rule-engine transactional-commit access-group을 활성화하십시오. 이는 OGS를 활성화하는 동안 구축 프로세스 도중 및 직후에 트래픽이 삭제되는 것을 방지하도록 구성됩니다.

> > > > asp rule-engine transactional-commit access-group > >

객체 그룹 검색 활성화

현재 OGS를 사용할 수 없습니다.



1. FMC CLI에 로그인합니다. Devices(디바이스) > Device Management(디바이스 관리) > Select the FTD device(FTD 디바이스 선택) > Device(디바이스)로 이동합니다. 고급 설정에서 개체 그룹 검색을 활성화합니다.

Firewall Management C Devices / Secure Firewall Device	enter Overview A Summary	Analysis Policies Devices	s Objects Integration	Deploy Q 🌮 🔅 📀	admin ~
10.70.73.44 Cisco Firepower 2130 Threat Defense Device Routing Interfaces	Inline Sets DHCP SN	MP			
Forward to Short 2		Policy: Initial_	Health_Policy 2021-05-02 02:35:06	Secondary Address:	
		Advanced Settings	G	Status:	0
		Automatic Application Bypass:		Manager Access Interface:	Management Interface
		Dumana Threadwood (ma)	2000		
Inventory Details	¢	bypasa mireanolo (ma).	3000	Advanced Settings	
CPU Type:	CPU MIPS 1200 MHz	Object Group Search:		Application Bypass:	No
CPIL Cores:	1 CPU (12 nores)	Interface Object Optimization:		Bypass Threshold:	3000 ms
Memory:	13701 MB RAM			Object Group Search:	Disabled
Stormon:	N/A		Cancel Save	Interface Object Optimization:	Disabled
Obresis LIDL	N/A	Informative Destination			Disabled
Chassis DRL:	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:			
Humber.		Zero Trust Application Policy			

2. 저장 및 배포를 클릭합니다.

다음을 확인합니다.

OGS를 활성화하기 전:

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
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 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 (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
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://www.access-list.csm.access-
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 (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
firences#

OGS가 활성화된 후:



관련 정보

4

FTD에서 규칙을 확장하는 방법에 대한 자세한 내용은 <u>Firepower</u> 디바이스<u>에서 규칙 확장 이해 문</u> <u>서를 참조하십시오</u>.

FTD 아키텍처 및 문제 해결에 대한 자세한 내용은 FTD(Firepower 위협 방어) 해부를 참조하십시오

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.