액세스 제어 규칙에 대한 FQDN 기반 개체 구성

목차

```
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>구성</u>
다음을 확인합니다.</u>
문제 해결
```

소개

이 문서에서는 FMC(Firewall Management Center)를 통한 FQDN(Fully Qualified Domain Name) 객체의 컨피그레이션 및 액세스 규칙 생성에서 FQDN 객체를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

• Firepower 기술에 대한 지식

• FMC(FireSIGHT Management Center)에서 액세스 제어 정책 구성 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• 버전 6.3 이상을 실행하는 Firepower Management Center

• 버전 6.3 이상을 실행하는 Firepower Threat Defense

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

구성

1단계. FQDN 기반 개체를 구성하고 사용하려면 먼저 Firepower Threat Defense에서 DNS를 구성 합니다.

FMC에 로그인하여 Devices(디바이스) > Platform Settings(플랫폼 설정) > DNS로 이동합니다.

	ARP Inspection	DNS Resolution Settings									
	Banner	Specify DNS servers grou	Specify DNS servers group and device interfaces to reach them.								
٠	DNS	Z Enable DNS name recol	ution by device								
	External Authentication		action by device								
	Fragment Settings	DNS Server Group*:	Cisco	~ (0						
	НТТР										
	ICMP	Expiry Entry Timer:	1		Rang	e: 1-65535 minutes					
	Secure Shell										
	SMTP Server	Poll Timer:	240	Range: 1-65535 minutes							
	SNMP	Interface Objects									
	SSL	Devices will use specif	ied interface object	ts for conr	necting w	ith DNS Servers.					
	Syslog										
	Timeouts	Available Interface C	Objects 🖒			Selected Interface Obje	ects				
	Time Synchronization	🔍 Search				📩 outside	i				
	UCAPL/CC Compliance	📩 ftd-mamt				servers	1				
		- inside									
		📥 labs									
		- outside									
		a outside		Ad	DI						

📩 outside-nat 👬 postgrad å privileged 📩 research servers 📇 servers-nat 📩 staff

Enable DNS Lookup via diagnostic interface also.

Add

alialia cisco.	Monitoring Policies Objects	Device		> 🖄 🙆	admin Administrator
CISCO. System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Traffic Settings URL Filtering Preferences	Monitoring Policies Objects Device Summary Configure DNS Data Interface Interfaces + ANY DNS Group CiscoUmbrellaDNSServerGroup FQDN DNS SETTINGS Poll Time 240 minu 7 - 65535 SAVE	res 1 7 - 65535	Management Interf DNS Group Filter None CiscoUmbreliaDN Create DNS Group	face	Administrator

	Add DNS (Group			0	×	
E	Name						l
	FQDN-DNS						l
	DNS IP Addresses	s (up to 6)					
	10.10.10.10						
L	Add another DNS IP						
L	Domain Search Na	ame					
l	Retries 2	Timeout 2					
oiry 1				CANCEL	ОК		
65535	5						

참고:DNS를 구성한 후 시스템 정책이 FTD에 적용되는지 확인합니다. (구성된 DNS 서버는 사용할 FQDN을 확인해야 합니다.)

2단계. Objects(개체) > Object Management(개체 **관리) > Add Network(네트워크 추가) > Add Object(개체 추가)로 이동하려면 FQDN 개체를 만듭니다.**

Edit Network	Object				? ×
Name	Test-Server				
Description	Test for FQDN	I			
Network	🔿 Host	🔘 Range	ONetwork	FQDN	
	test.cisco.com	1			
	Note: You can us	e FQDN network obje	cts in access and prefi	ilter rules only	
Lookup:	Resolve within	n IPv4 and IPv6		~	
Allow Overrides					
				Save	Cancel

Add Network Object

D

Name					
FQDN					
Description					
				1.	
Туре					
O Network	◯ Host	FQDN			
 Note: You can us 	e FQDN network	objects in acces	ss rules only.		
Domain Name					
test.cisco.com	I				
e.g. ad.example.co	m				
DNS Resolution					
IPv4 and IPv6		~			
			CANCEL	ок	

0

 \times

3단계. Policies(정책) > Access Control(액세스 제어)로 이동하여 액세스 제어 규칙을 생성합니다.

참고:요구 사항을 기반으로 규칙을 생성하거나 기존 규칙을 수정할 수 있습니다.FQDN 개체 는 소스 및/또는 대상 네트워크에서 사용할 수 있습니다.

Editing Rule - FQDN				? ×
Name FQDN	🗌 Enab	led <u>Move</u>		
Action Allow	🔹 U D 2 🗠 🗖			
Zones Networks VLAN Tags 🛆 Users	Applications Ports	URLs SGT/ISE Attributes	Inspection	Logging Comments
Available Networks 🕏 📀	Source	Networks (0)	Destination Networks	(1)
Search by name or value		Source Original Clier	nt 📄 Test-Server	ĩ
Networks Geolocation	any			
109.236.93.138				
119.161.38.47	Add To Source			
119.161.38.88	Networks			
134.7.248.121	Add to			
134.7.248.137	Destination			
134.7.248.155				
190.61.4.74				
208.76.111.155	Entern	ID address		
Viewing 1-100 of 983	enter al		Enter an IP address	Add
				Save Cancel

Add Access Rul	e					◎ ×		
Order Title 2 Center Rule I	Vame	Action						
Source/Destination Ap	plications URLs Users 9 In	trusion Policy	File policy Logging DESTINATION			_		
ANY	Networks Ports Filter Networks Geolocation F FQDN-Object (FQDN) F Management-Gateway (Host) F OutsidelPv4DefaultRoute (Network) F OutsidelPv4Gateway (Host) F any-ipv4 (Network)		Zones ANY	ANY ANY	Ports/Protocols	+		
Show Diagram					CANCEL	ОК		

컨피그레이션이 완료된 후 정책이 적용되는지 확인합니다.

다음을 확인합니다.

생성된 FQDN 기반 규칙을 트리거할 것으로 예상되는 클라이언트 컴퓨터에서 트래픽을 시작합니 다.

FMC에서 Events > Connection Events로 이동하여 특정 트래픽을 필터링합니다.

Jump to •																				
-	▼ <u>Fir</u>	st Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
4.(2019-	-06-04 16:04:56	2019-06-04 17:05:16	Allow	Intrusion Monitor	21.21.21.101	SA USA	10.123.175.6		servers	outside	61132 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4 (2019-	-06-04 16:04:56		Allow	Intrusion Monitor	21.21.21.101	usa 🔜	10.123.175.6		servers	outside	61132 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4 (2019-	-05-04 12:32:31	2019-06-04 13:32:45	Allow		21.21.21.101	usa 🛄	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4 (2019-	-06-04 12:32:31		Allow		21.21.21.101	SA USA	10.123.175.6		servers	outside	61115 / tcp	22 (ssh) / tcp							FTD-1
4 (2019-	06-04 12:13:13	2019-06-04 12:13:54	Allow	Intrusion Monitor	21.21.21.101	USA USA	10.123.175.6		servers	outside	61097 / tcp	22.(ssh)./.tcp	SSH	SSH client					FTD-1
4 (2019-	-06-04 12:13:13		Allow	Intrusion Monitor	21.21.21.101	usa 🛄	10.123.175.6		servers	outside	61097 / tcp	22 (ssh) / tcp	SSH	SSH client					FTD-1
4 (2019-	-06-04 12:01:40	2019-06-04 12:01:48	Allow	Intrusion Monitor	21.21.21.101	usa 🔜	10.123.175.6		servers	outside	61066 / tcp	22 (ssh) / tcp	SSH SSH	SSH client					FTD-1
4 (2019-	06-04 12:01:40		Allow	Intrusion Monitor	21.21.21.101	SA USA	10.123.175.6		servers	outside	<u>61066 / tcp</u>	22.(ssh)./.tcp	SSH	SSH client					FTD-1
(< Page 1 of 1 >) Displaying rows 1-8 of 8 rows																				
	View	Delete																		
Vi	ew All	Delete All																		

문제 해결

DNS 서버는 FQDN 객체를 확인할 수 있어야 하며, CLI에서 다음 명령을 실행하여 확인할 수 있습니다.

- 시스템 지원 진단 cli
- FQDN 표시

.