고가용성을 보장하는 보안 방화벽 위협 방어의 결 함 있는 유닛 교체

목차

소개

이 문서에서는 HA(고가용성) 설정에 속하는 결함이 있는 Secure Firewall Threat Defense 모듈을 교체하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FXOS(Firepower eXtensible 운영 체제)
- Cisco FTD(Secure Firewall Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower 4110은 FXOS v2.12(0.498)를 실행합니다.
- 논리적 디바이스에서 Cisco Secure Firewall v7.2.5 실행
- Secure Firewall Management Center 2600 실행 버전 7.4
- SCP(Secure Copy Protocol) 지식

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

이 절차는 어플라이언스에서 지원됩니다.

- Cisco Secure Firewall 1000 Series 어플라이언스
- Cisco Secure Firewall 2100 Series 어플라이언스
- Cisco Secure Firewall 3100 Series 어플라이언스
- Cisco Secure Firewall 4100 Series 어플라이언스
- Cisco Secure Firewall 4200 Series 어플라이언스
- Cisco Secure Firewall 9300 어플라이언스
- Cisco Secure Firewall Threat Defense for VMWare

시작하기 전에

이 문서에서는 동일한 FXOS 및 FTD 버전으로 새 유닛을 구성해야 합니다.

결함 유닛 식별

FTD-HA High Availability						1
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD 7.2	.5 EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	¢Þ	:
FTD-02(Secondary, Failed) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD 7.2	.5 EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	¢	:

이 시나리오에서 보조 유닛(FTD-02)은 실패 상태입니다.

결함이 있는 유닛을 백업으로 교체

이 절차를 사용하여 기본 또는 보조 유닛을 교체할 수 있습니다. 이 설명서에서는 교체하려는 결함 유닛에 대한 백업이 있는 것으로 가정합니다.

1단계. FMC에서 백업 파일을 다운로드합니다. System > Tools > Restore > Device Backups로 이 동하고 올바른 백업을 선택합니다. Download(다운로드)를 클릭합니다.

Firewall Management Center System / Tools / Backup/Restore / Backup Managemen	Overview A	Analysis Poli	icies Devices	Objects	Integration	Deploy	Q 🔮	¢ 0	admin ~	cisco S	ECURE
										Remote	Storage
Backup Management Backup Profiles											
				C	Firewall Managemer	nt Backup	Manage	ed Device	Backup	Upload Ba	ackup
Firewall Management Backups											
System Information Date Created	File Name	VDB V	/ersion	Location	Size (MB)	Config	gurations		Events	TI	D
Restore Download Delete Move	2					ţ	Storage Lo	cation: /\	/ar/sf/backup	/ (Disk Usa	ge: 8%)
System Information	Date Created	File Name			VDB Version	Location	Size (MB)	Con	figurations	Events	TID
Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:48:04	FTD-02_Seco	ondary_20230926234	646.tar	build 365	Local	53		Yes	No	No
Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:47:57	FTD-01_Prim	ary_2023092623463	7.tar	build 365	Local	52		Yes	No	No
4											
Source Delete Move											

2단계. 새 FTD의 /var/sf/backup/ 디렉토리에 FTD 백업을 업로드합니다.

2.1 test-pc(SCP 클라이언트)에서 /var/tmp/ 디렉토리 아래의 FTD에 백업 파일을 업로드합니다.

@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/

2.2 FTD CLI expert 모드에서 백업 파일을 /var/tmp/에서 /var/sf/backup/ 로 이동합니다.

root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/

3단계. 다음 명령을 클릭 모드에서 적용하여 FTD-02 백업을 복원합니다.

>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense

This Device Model :: Cisco Firepower 4110 Threat Defense Backup Details ***** Model = Cisco Firepower 4110 Threat Defense Software Version = 7.2.5Serial = FLM22500791 Hostname = firepower Device Name = FTD-02_Secondary IP Address = 10.88.171.89 Role = SECONDARY VDB Version = 365SRU Version = FXOS Version = 2.12(0.498)Manager IP(s) = 10.88.243.90Backup Date = 2023-09-26 23:46:46 Backup Filename = FTD-02_Secondary_20230926234646.tar ***** Verify that you are restoring a valid backup file. Make sure that FTD is installed with same software version and matches versions from backup manifest be Restore operation will overwrite all configurations on this device with configurations in backup. If this restoration is being performed on an RMA device then ensure old device is removed from network ***** Are you sure you want to continue (Y/N)Y Restoring device Added table audit_log with table_id 1 Added table health_alarm_syslog with table_id 2 Added table dce_event with table_id 3 Added table application with table_id 4 Added table rna_scan_results_tableview with table_id 5 Added table rna_event with table_id 6 Added table ioc_state with table_id 7 Added table third_party_vulns with table_id 8 Added table user_ioc_state with table_id 9 Added table rna_client_app with table_id 10 Added table rna_attribute with table_id 11 Added table captured_file with table_id 12 Added table rna_ip_host with table_id 13 Added table flow_chunk with table_id 14 Added table rua_event with table_id 15 Added table wl_dce_event with table_id 16 Added table user_identities with table_id 17 Added table whitelist_violations with table_id 18 Added table remediation_status with table_id 19 Added table syslog_event with table_id 20 Added table rna_service with table_id 21 Added table rna_vuln with table_id 22 Added table SRU_import_log with table_id 23 Added table current_users with table_id 24 Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023): The system is going down for reboot NOW!



참고: 복구가 완료되면 디바이스는 CLI에서 로그아웃하고 재부팅하며 FMC에 자동으로 연 결합니다. 이 때 디바이스는 최신 상태가 아닙니다.

4단계. HA 동기화를 다시 시작합니다. FTD CLI에서 다음과 같이 configure high-availability resume을 입력합니다.

>configure high-availability resume

FTD 고가용성 컨피그레이션이 완료되었습니다.

V FTD-HA High Availability							11
 FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed 	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	4D	:
FTD-02(Secondary, Standby) Snort 3 10.88 171 89 - Routed	Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	~Q>	:

백업하지 않고 결함이 있는 유닛 교체

실패한 디바이스의 백업이 없는 경우 이 가이드를 계속 진행할 수 있습니다. 기본 또는 보조 유닛을 교체할 수 있습니다.이 프로세스는 디바이스가 기본 디바이스인지 보조 디바이스인지에 따라 달라 집니다. 이 설명서에서 설명하는 모든 단계는 결함이 있는 보조 유닛을 복원하는 것입니다. 오류가 발생한 기본 유닛을 복원하려면 5단계에서 등록 과정에서 기존 보조/액티브 유닛을 기본 디바이스 로, 교체 디바이스를 보조/스탠바이 디바이스로 사용하여 고가용성을 구성합니다.

1단계. Device(디바이스) > Device Management(디바이스 관리)로 이동하여 고가용성 컨피그레이 션의 스크린샷(백업)을 작성합니다. 올바른 FTD HA 쌍(연필 아이콘 클릭)을 편집한 다음 High Availability(고가용성) 옵션을 클릭합니다.

FTD-HA Cisco Firepower 4110 Threat Defense Summary High Availability D	evice Routing	Interfaces Inline Set	s DHCP VTEP								Cancel
High Availability Configuration	n										
High Availability Link					State Link						
Interface			Etherne	1/5	Interface					Eth	ernet1/5
Logical Name			FA-	INK	Logical Name						FA-LINK
Primary IP			10.10.	10.1	Primary IP					10	.10.10.1
Secondary IP			10.10.	10.2	Secondary IP					10	.10.10.2
Subnet Mask			255.255.255	252	Subnet Mask					255.255.	255.252
IPsec Encryption			Disa	bled	Statistics						Q
Monitored Interfaces											
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6			Active Link-Local IF	V6	Standby Link-Loca	l IPv6	Monitoring	
Inside	192.168.30.1									•	1
diagnostic										•	/
Outside	192.168.16.1									•	/
Failover Trigger Criteria				1	Interface MAC Addre	esses					+
Failure Limit			Failure	of 1 ices	Physical Interface		Active Mac Add	ress	Standby Mac A	ddress	
Peer Poll Time 1 sec			sec	No records to display							
Peer Hold Time			15	sec							
Interface Poll Time			5	sec							
Interface Hold Time			25	sec							

2.1 Devices(디바이스) > Device Management(디바이스 관리)로 이동한 다음 오른쪽 상단의 세 개 의 점 메뉴를 클릭합니다. 그런 다음 Break 옵션을 클릭합니다.



2.2. 대기 피어가 응답하지 않을 경우 강제 중단을 선택합니다. 옵션:

Collapse All						Download Devi	ce List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)	Confirm Break						
FTD-HA High Availability	Breaking the except the provided operation m	e High Availa Access Contr ight also res	bility pair "FTD-HA" will erase al rol and Flex Config policy from si tart Snort processes of primary a	I configuration tandby peer. This and secondary			1
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Fit Force break, it	nporarily cau air? standby pee	sing traffic interruption. Are you er does not respond	Base-ACP	49	:	
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Fir			Base-ACP	49	:	



참고: 장치가 응답하지 않으므로 HA를 강제로 해제해야 합니다. 고가용성 쌍을 해제하면 활성 장치는 배포된 모든 기능을 유지합니다. 스탠바이 디바이스는 장애 조치 및 인터페이 스 컨피그레이션을 상실하며 독립형 디바이스가 됩니다.

3단계. 결함이 있는 FTD를 삭제합니다. 교체할 FTD를 확인한 다음 3점 메뉴를 클릭합니다. 삭제를 클릭합니다.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rolli	Back
✓ Ungrouped (2)							
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«D	11
FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«9	Delete
							Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot Files

4단계. 새 FTD를 추가합니다.

4.1. Devices > Device Management > Add로 이동한 다음 Device를 클릭합니다.

View By: Group 🔻						Migrate C	Deployment History
All (1) • Error (0) • Warning (1) • Offline (0)	Normal (0) Oe	ployment Pe	nding (1) • Upgrade (0)	 Snort 3 (1) 		Q Search Devic	ce Add 🔻
Collapse All						Do	Device High Availability
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rolli	Chassis
Ungrouped (1)							Group
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	(۵)	11

4.2. 프로비전 방법을 선택합니다. 이 경우 등록 키, 호스트 구성, 표시 이름, 등록 키. 액세스 제어 정 책을 구성하고 등록을 누릅니다.

Add Device

Select the Provisioning Method:

Registration Key
 Serial Number

CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

.....

Group:

None

Access Control Policy:*

Base-ACP	•
----------	---

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click here for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

v

Select a recommended Tier	•
Carrier	
Malware Defense	
IPS IPS	
URL	
Advanced	
Unique NAT ID:†	
Transfer Packets	

Cancel

8

5단계. HA를 생성합니다.

5.1 Devices(디바이스) > Device Management(디바이스 관리) > Add(추가)로 이동하여 High Availability(고가용성) 옵션을 클릭합니다.

View By	Group									Migrate	Deployment History
All (2) • Error (0)	 Warning (0) 	Offline (0)	Normal (2)	 Deployment Pending (0) 	 Upgrade (0) 	 Snort 3 (2) 			Q, Search Dev	ice Add 🔻
Collapse	All									Do	Device High Availability
	Nama				Model	Version	Charala	Licenses	Access Control Policy	Auto Poll	Cluster
	rearing .				model	10150011	0105515	Licenses	meets control roley	2000 101	Group
	 Ungrouped (2) 										
	FTD-01 Snort : 10.88.171.87 -	3 Routed			Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«ڳ	1
	FTD-02 Snort : 10.88.171.89 -	3 Routed			Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base~ACP	«Ø	Z :

5.2. Add High Availability Pair(고가용성 추가 쌍)를 구성합니다. Name(이름), Device Type(디바이 스 유형)을 구성하고 FTD-01을 Primary Peer(기본 피어)로, FTD-02를 Secondary Peer(보조 피어)로 선택한 다음 Continue(계속)를 클릭합니다.

View By: Group						Migrate Deployme	ent History
All (2) • Error (0) • Warning (0) • Offline (0) • Normal (2)	Deployment Pending (0) • Upgrade (0)	 Snort 3 (2) 			Q, Search Device	Add 🔻
Collarse All						Download Dev	ce List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (2)		Add High Availa	bility Pair 🛛 🕑				
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	Name:* FTD-HA		Essentials	Base-ACP	e?>	1
FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	Device Type: Firewall Threat Def	lense 💌	Essentials	Base-ACP	4S	1
		Primary Peer: FTD-01	•				
		Secondary Peer:	•				
		 Threat Defense F configuration. Lic converted to their on both peers. 	ligh Availability pair will have primary enses from primary peer will be r high availability versions and applied				
			Cancel				



참고: 기본 유닛을 컨피그레이션이 아직 있는 디바이스로 선택해야 합니다(이 경우 FTD-01).

5.3. HA 생성을 확인한 다음 Yes(예)를 클릭합니다.

	Add High Availability Pair	
FTD	Name:* FTD-HA	Essenti
FTD	Warning	Essenti
	This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption. Do you want to continue?	
	Do not display this message again No Yes	
	converted to their high availability versions and applied on both peers.	
	Cancel Continue	



참고: 고가용성을 구성하면 두 유닛의 snort 엔진이 다시 시작되며 이로 인해 트래픽이 중단 될 수 있습니다.

5.4. 2단계에서 고가용성 매개변수를 구성한 다음 Add(추가) 옵션을 클릭합니다.

Firewall Management Center Overview Analysis Devices / Device Management	Policies Devices Objects Integration		Deploy Q 💕	🗘 🙆 admin 🗸 🔐	SECURE
View By: Group • All (2) • Error (0) • Warning (0) © Offline (0) • Normal (2)	Deployment Pending (0) Upgrade (0) Sin	ort 3 (2)		Migrate Deployme	nt History Add 💌
Collague All				Download Devi	e List Report
Name	Add High Availability Pair	0	Access Control Policy	Auto RollBack	
	High Availability Link	State Link			
FTD-01 Snort 3 10.88.171.87 - Routed	Interface: Ethernet1/5 v Logical Name: FA-LINK	Interface: Same as LAN Failover Link Logical Name:* FA-LINK	Base-ACP	Q+	1
FTD-02 Snort 3 10.88.171.89 - Routed	Primary IP: 10.10.10.1	Primary IP:* 10.10.10.1	Base-ACP	<0	1
	Secondary IP: 10.10.10.2 Subnet Mask: 255.255.255.252	Secondary IP:* 10.10.10.2 Subnet Mask:* 255.255.252			
	IPsec Encryption				
	Enabled Key Generation: Auto v	_			
	LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.				
		Cancel			

6. FTD 고가용성 컨피그레이션이 완료되었습니다.

FTD-HA High Availability							1
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«Þ	:
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	4Q	:



참고: 가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터의 ARP 테이블을 지워 기본 장 치 교체 시 트래픽 흐름을 복원해야 합니다. 자세한 내용은 고가용성의 <u>MAC 주소 및 IP 주</u> 소를 참조하십시오.

관련 정보

• <u>Cisco 기술 지원 및 다운로드</u>

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.