FTD-clusters configureren op FP9300 (intrachassis)

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram Task 1. Maak de benodigde interfaces voor FTD Cluster Task 2. Maak FTD Cluster Task 3. Registreer FTD Cluster op FMC Task 4. Het configureren van poort-Channel sub-interfaces op FMC Task 5. Controleer de basisconnectiviteit Cluster Capture van Chassis Manager UI Task 6. Verwijdert een Slave-apparaat uit de Cluster. Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de functies van de Cluster op het FPR9300-apparaat kunt configureren en controleren.

Voorzichtig: De in dit document verstrekte informatie heeft betrekking op de eerste installatie/configuratie van het cluster. Dit document is niet van toepassing op de procedure voor vervanging van een eenheid (retourmateriaalmachtiging - RMA)

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

Cisco Firepower 9300 security applicatie voor 1.1(4.95)

- Firepower Threat Defense (FTD) met 6.0.1 (gebouw 1213)
- FireSIGHT Management Center (FMC) van 6.0.1.1 (gebouw 1023)

Tijd voor invullen van het lab: 1 uur.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

- Op de FPR9300 met FTD-apparaat kunt u alle ondersteunde versies configureren binnen het chassis.
- Inter-Chassis clustering werd geïntroduceerd in punt 6.2.
- Poortkanaal 48 wordt gecreëerd als een clustercontrole-link. Voor clustering binnen het chassis gebruikt deze link de FirePOWER 9300 backplane voor clustercommunicatie.
- Individuele gegevensinterfaces worden niet ondersteund, met uitzondering van een beheerinterface.
- De beheersinterface wordt toegewezen aan alle eenheden in het cluster.

Configureren

Netwerkdiagram



Task 1. Maak de benodigde interfaces voor FTD Cluster

Taakeis:

Maak een Cluster, een Management-interface en een Port-Channel-gegevensinterface.

Oplossing:

Stap 1. Maak een poortkanaal-gegevensinterface.

Om een nieuwe interface te maken, moet u inloggen in FPR9300 Chassis Manager en naar het tabblad **Interfaces** navigeren.

Selecteer **Port Channel toevoegen** en maak een nieuwe Port Channel-interface met deze parameters:

| ID van poortkanaal | 5 |
|--------------------|---------------------------|
| Туре | Gegevens |
| inschakelen | Ja |
| Lidstaat | Ethernet1/3, Ethernet 1/4 |

Selecteer **OK** om de configuratie op te slaan zoals in de afbeelding.

| Add Port Cha | nnel | | | | ? × |
|------------------|------------------|---------------|-----------|-----|--------|
| Port Channel ID: | 5 | 🗹 Enable | | | |
| Туре: | Data | • | | | |
| Speed: | 1gbps 🗸 | | | | |
| Interfaces | | _ | | | |
| Ava | ilable Interface | | Member ID | | |
| | Search |] | Ethernet | 1/3 | |
| | Ethernet1/2 | | Ethernet | 1/4 | |
| | Ethernet1/3 | | | | 1 |
| | Ethernet1/4 | | | | |
| | Ethernet1/5 | | | | |
| | Ethernet1/6 | Add Taba from | | | |
| | Ethernet1/7 | Add Interface | | | |
| | Ethernet1/8 | | | | |
| | Ethernet2/1 | | | | |
| | Ethernet2/2 | | | | |
| | Ethernet2/3 | | | | |
| | Ethernet2/4 | | | | |
| | Ethernet3/1 | | | | |
| | Ethernet3/2 | | | | |
| | | | | | |
| | | | | | |
| | | | | ОК | Cancel |

Stap 2. Maak een beheerinterface.

Kies in het tabblad Interfaces de interface, klik op Bewerken en stel de interface Management

Type in.

Klik op **OK** om de configuratie op te slaan zoals in de afbeelding wordt weergegeven.

| Edit Interface - Ethernet1/1 | | | | |
|------------------------------|-------------|--------|--|--|
| Name: | Ethernet1/1 | able | | |
| Type: | mgmt | * | | |
| Speed: | 1gbps | * | | |
| | ок | Cancel | | |

Stap 3. Maak een Cluster-Control Link-interface.

Klik op de knop **Port Channel toevoegen** en maak een nieuwe poortkanaalinterface met deze parameters en zoals in de afbeelding.

| ID van poortkanaal | 48 |
|--------------------|---------|
| Туре | Cluster |
| inschakelen | Ja |
| Lidstaat | - |

| Add Port Cha | annel | | | ? × |
|------------------|-------------------|---------------|-----------|--------|
| Port Channel ID: | 48 | Enable | | |
| Type: | Cluster | · | | |
| Speed: | 1gbps 👻 | • | 1 (C) | |
| Interfaces | | _ | | _ |
| Av | ailable Interface | | Member ID | |
| | Search |] | | |
| | Ethernet1/2 | | | |
| | Ethernet1/5 | | | |
| | Ethernet1/6 | | | |
| | Ethernet1/7 | | | |
| | Ethernet1/8 | Add Interface | | |
| | Ethernet2/1 | Add Internace | | |
| | Ethernet2/2 | | | |
| | Ethernet2/3 | | | |
| | Ethernet2/4 | | | |
| | Ethernet3/1 | | | |
| | Ethernet3/2 | | | |
| | Ethernet3/3 | | | |
| | Ethernet3/4 | | | |
| | | | | |
| | | | | |
| | | | 6 | |
| | | | OK | Cancel |

Task 2. Maak FTD Cluster

Taakeis:

Maak een FTD Cluster unit.

Oplossing:

Stap 1. Navigeer naar Logische apparaten en klik op de knop Toevoegen apparaat.

De FTD-clusters maken als volgt:

| Apparaatnaam | FTD_cluster |
|-------------------|------------------------|
| Siabloon | Cisco Firepower Threat |
| Sjabloon | Defense |
| Afbeeldingsversie | 6.0.1.1213 |
| Apparaatmodus | Cluster |

Als u het apparaat wilt toevoegen, klikt u op OK zoals in de afbeelding.

| Add Device | | | ?× |
|----------------|--------------------------------|---|--------|
| Device Name: | FTD_cluster | | |
| Template: | Cisco Firepower Threat Defense | ~ | |
| Image Version: | 6.0.1.1213 | ~ | |
| Device Mode: | 🔵 Standalone 💿 Cluster | | |
| | | _ | |
| | ОК | | Cancel |

Stap 2. Het FTD Cluster configureren en implementeren.

Nadat u een FTD apparaat hebt gemaakt, wordt u opnieuw gericht naar het Provisioningdevice_name venster.

Klik op het pictogram van het apparaat om de configuratie zoals in de afbeelding te starten.

| 0 | verview Interface | s Logical Device | es Security M | odules Platform Settings | | | System Tools Help admin |
|----------|---|-----------------------------|-----------------|--------------------------|---------|------------------------|-------------------------|
| Pr Ch | rovisioning - FTD_cl ustered Cisco Fireg | uster Jower Threat Defen | se 6.0.1.1213 |] | | | Save Cancel |
| D | ita Ports | | | | | | |
| | themet1/2 | | | | | | |
| 1 | thernet1/5 | | | | | | |
| | thernet1/6 | | | | | | |
| | thernet1/7 | | | | | | |
| | thernet1/8 | | | | | | |
| | thernet2/1 | | | | | | |
| | thernet2/2 | | | | | FTD - 6.0.1.1213 | |
| | (thernet2/3 | | | | | Security Module 1,2,3 | |
| | Ithernet2/4 | | | | | | |
| | thernet3/1 | | | | | | |
| | thernet3/2 | | | | | | |
| | themet3/3 | | | | | | |
| | Inernet3/4 | | | | | | |
| Ľ | ort-onermers | | | | | | |
| | Security Module | Application | Version | Management IP | Gateway | Management Port Status | |
| | Security Module 1 | FTD | 6.0.1.1213 | | | | |
| a | Security Module 2 | FTD | 6.0.1.1213 | | | | |
| | Security Module 3 | FTD | 6.0.1.1213 | | | | |

Het **tabblad** FTD **Cluster Information** met deze instellingen en zoals in de afbeelding weergegeven.

| Cluster-toets | Cisco |
|----------------------|-------------|
| Cluster groepsnaam | FTD_cluster |
| Management-interface | Ethernet1/1 |

| Cisco Firepower Threat Defense - Configuration | | | | | |
|--|-------------------------------------|--|--|--|--|
| Cluster Information Setti | ngs Interface Information Agreement | | | | |
| Security Module(SM) | | | | | |
| Security Module-1,Security M | lodule-2,Security Module-3 | | | | |
| Interface Information | | | | | |
| Cluster Key: | | | | | |
| Cluster Group Name: | FTD_cluster | | | | |
| Management Interface: | Ethernet1/1 | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | OK Cancel | | | | |

Configureer het tabblad FTD **Instellingen** met deze instellingen en zoals in de afbeelding weergegeven.

| Registratiekanaal | Cisco |
|--------------------------|-----------------------------|
| Wachtwoord | Admin123 |
| FireSIGHT Management | 10 62 149 73 |
| Center IP | 10.02.140.75 |
| Zoeken gebieden | cisco.com |
| Firewallmodus | Routed |
| DNS-servers | 173.38.200.100 |
| Volledig gekwalificeerde | keep for 0k 1 1 3 sizes com |
| hostnaam | ksec-ipi9k-1-1-3.cisco.com |
| Interactie uiteindelijk | None |

| Cisco Firepower Three Cluster Information Settings | at Defense - Configu | uration 2× |
|---|---------------------------|------------|
| Registration Key: Password: | ••••• | |
| Firepower Management Center IP: | 10.62.148.73 | |
| Search domains: | cisco.com | |
| Firewall Mode: | Routed | • |
| DNS Servers: | 173.38.200.100 | |
| Fully Qualified Hostname: | ksec-fpr9k-1-1-3.cisco.co | m |
| Eventing Interface: | None | - |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Grand |
| | OK | Cancel |

Het tabblad FTD **Interface Information** met deze instellingen en zoals in de afbeelding weergegeven.

| Type adres A | lleen IPv4 |
|-------------------|----------------|
| Security module 1 | |
| IP-beheer 1 | 0.62.148.67 |
| Netwerkmasker 2 | 55.255.255.128 |
| Gateway 1 | 0.62.148.1 |
| Security module 2 | |
| IP-beheer 1 | 0.62.148.68 |
| Netwerkmasker 2 | 55.255.255.128 |
| Gateway 1 | 0.62.148.1 |
| Security module 1 | |
| IP-beheer 1 | 0.62.148.69 |
| Netwerkmasker 2 | 55.255.255.128 |
| Gateway 1 | 0.62.148.1 |

| Cisco Firepower Threat Defense - Configuration | | | |
|--|---------------------------------|--|--|
| Cluster Information Settings | Interface Information Agreement | | |
| Address Type: | IPv4 only | | |
| Security Module 1 | | | |
| Management IP: | 10.62.148.67 | | |
| Network Mask: | 255.255.255.128 | | |
| Gateway: | 10.62.148.1 | | |
| Security Module 2 | | | |
| Management IP: | 10.62.148.68 | | |
| Network Mask: | 255.255.255.128 | | |
| Gateway: | 10.62.148.1 | | |
| Security Module 3 | | | |
| Management IP: | 10.62.148.69 | | |
| Network Mask: | 255.255.255.128 | | |
| Gateway: | 10.62.148.1 | | |
| | | | |
| | | | |
| | OK Cancel | | |

Accepteer de Overeenkomst op het tabblad Overeenkomst en klik op OK zoals in de afbeelding.

| Cisco Firepower Threat Defense - Configuration 2 Cluster Information Settings Interface Information Agreement | | | | |
|--|--|--|--|--|
| End User License Agreement | | | | |
| IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES | | | | |
| CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE | | | | |
| ✓ Lunderstand and accept the agreement | | | | |
| OK Cancel | | | | |

Stap 3. Wijs de gegevensinterfaces aan de FTD toe.

Vul het gebied met gegevenspoorten uit en klik op elke interface die u aan FTD wilt toewijzen. Selecteer na voltooiing **Opslaan** om een FTD-cluster te maken zoals in de afbeelding.

| c | verview Interface: | Logical Device | Security Modules Pla | tform Settings | | | | System Tools | Help admin |
|-----|---|-----------------------------|----------------------|-------------------|-------------|-----------------|-------------|--------------|------------|
| P | rovisioning - FTD_clu lustered Cisco Firej | uster power Threat Defen | se 6.0.1.1213 | | | | | Save | Cancel |
| D | ata Ports | | | | | | | | |
| | Ethernet1/7 | | | | | | | | |
| I, | Ethernet1/8 | | | | | | | | |
| IJ | Ethernet2/1 | | | | | | | | |
| II, | Ethernet2/2 | | | | | | | | |
| Į, | Ethernet2/3 | _1 | | Port- channel5 | | | | | |
| II. | Ethernet2/4 | _1 | | | | 6 | | | |
| ŀ | Ethernet3/1 | | | | | FTD - 6.0 | 0.1.1213 | | |
| ŀ | Ethernet3/2 | | | But. | | Security M | odule 1,2,3 | | |
| ŀ | Ethernet3/3 | -1 | | channel48 | | | | | |
| ŀ | EthernetJ/4 | | | | | | | | |
| | Port-channel% | | | | | | | | |
| 2 | | | | | | | | | _ |
| | Security Module | Application | Version | Management IP | Gateway | Management Port | Status | | |
| 9 | Security Module 1 | FTD | 6.0.1.1213 | 10.62.148.67 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |
| 9 | Security Module 2 | FTD | 6.0.1.1213 | 10.62.148.68 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |
| ۲ | Security Module 3 | FTD | 6.0.1.1213 | 10.62.148.69 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |

Wacht een paar minuten voordat het cluster wordt ingezet, waarna de algemene verkiezing

plaatsvindt.

Verificatie:

• Van de FPR9300 GUI zoals in de afbeelding.



Van de FPR9300 CLI

| FPR9K-1-A# FPR9K-1-A# scope ssa FPR9K-1-A /ssa # show app-instance | | | | | | |
|--|---------|-------------|-------------------|-----------------|------------|--|
| Application Name | Slot ID | Admin State | Operational State | Running Version | Startup | |
| Version Cluster Oper | State | | | | | |
| | | | | | | |
| ftd | 1 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | |
| In Cluster | | | | | | |
| ftd | 2 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | |
| In Cluster | | | | | | |
| ftd | 3 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | |
| In Cluster | | | | | | |

• Van de LINA (ASA) CLI

firepower# show cluster info

Cluster FTD_cluster: On Interface mode: spanned This is "unit-1-1" in state MASTER ID : 0 Version : 9.6(1)Serial No.: FLM19216KK6 CCL IP : 127.2.1.1 CCL MAC : 0015.c500.016f Last join : 21:51:03 CEST Aug 8 2016 Last leave: N/A Other members in the cluster: Unit "unit-1-3" in state SLAVE ID : 1 Version : 9.6(1)Serial No.: FLM19206H7T CCL IP : 127.2.1.3 CCL MAC : 0015.c500.018f Last join : 21:51:05 CEST Aug 8 2016

Last leave: N/A Unit "unit-1-2" in state SLAVE ID : 2 Version : 9.6(1) Serial No.: FLM19206H71 : 127.2.1.2 CCL IP CCL MAC : 0015.c500.019f Last join : 21:51:30 CEST Aug 8 2016 Last leave: N/A firepower# cluster exec show cluster interface-mode cluster interface-mode spanned cluster interface-mode spanned cluster interface-mode spanned firepower# firepower# cluster exec show cluster history _____ To State From State Reason _____ 21:49:25 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:18 CEST Aug 8 2016 Enabled from CLI DISABLED ELECTION 21:51:03 CEST Aug 8 2016 ELECTION MASTER_POST_CONFIG Enabled from CLI 21:51:03 CEST Aug 8 2016 MASTER_POST_CONFIG MASTER Master post config done and waiting for ntfy _____ _____ To State From State Reason _____ 21:49:44 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:37 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:37 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:41 CEST Aug 8 2016 Received cluster control message ONCALL ELECTION 21:50:41 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:46 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message

21:50:46 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:51 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:51 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:56 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:56 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:51:01 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:04 CEST Aug 8 2016 ONCALL SLAVE_COLD Received cluster control message 21:51:04 CEST Aug 8 2016 SLAVE_COLD SLAVE_APP_SYNC Client progression done 21:51:05 CEST Aug 8 2016 SLAVE CONFIG Slave application configuration sync done SLAVE_APP_SYNC 21:51:17 CEST Aug 8 2016 SLAVE_CONFIG SLAVE_BULK_SYNC Configuration replication finished 21:51:29 CEST Aug 8 2016 SLAVE_BULK_SYNC SLAVE Configuration replication finished _____ _____ To State Reason From State 21:49:24 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:16 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:17 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:21 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:21 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:26 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:26 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message

21:50:31 CEST Aug 8 2016 Received cluster control message ONCALL ELECTION 21:50:31 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:36 CEST Aug 8 2016 Received cluster control message ONCALL ELECTION 21:50:36 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:41 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:41 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:46 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:46 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:51 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:51 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:56 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:56 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:01 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:06 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:06 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:12 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:12 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:17 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:17 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:22 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message

21:51:22 CEST Aug 8 2016

```
ELECTION
                 ONCALL
                                  Received cluster control message
21:51:27 CEST Aug 8 2016
                           Received cluster control message
               ELECTION
ONCALL
21:51:27 CEST Aug 8 2016
                ONCALL
                          Received cluster control message
ELECTION
21:51:30 CEST Aug 8 2016
ONCALL
                SLAVE_COLD Received cluster control message
21:51:30 CEST Aug 8 2016
               SLAVE_APP_SYNC
SLAVE_COLD
                                 Client progression done
21:51:31 CEST Aug 8 2016
SLAVE_APP_SYNC SLAVE_CONFIG Slave application configuration sync done
21:51:43 CEST Aug 8 2016
SLAVE_CONFIG
               SLAVE_BULK_SYNC Configuration replication finished
21:51:55 CEST Aug 8 2016
SLAVE_BULK_SYNC SLAVE
                                    Configuration replication finished
```

firepower#

Task 3. Registreer FTD Cluster op FMC

Taakeis:

Voeg de logische apparaten toe aan het FMC en groepeer ze vervolgens in een cluster.

Oplossing:

Stap 1. Voeg logische apparaten aan het FMC toe. Vanaf FMC versie 6.3 dient u slechts één FTD-apparaat te registreren (aanbevolen als de Master). De rest van de FTD's wordt door het VCC automatisch ontdekt.

Meld u aan bij het FMC en navigeer naar het tabblad **Apparaten >Apparaatbeheer** en klik op **Apparaat toevoegen**.

Voeg het eerste logische apparaat toe met de instellingen zoals aangegeven in de afbeelding.

Klik op Registreren om de registratie te starten.

| Add Device ? × | | | | |
|--|---------------|----|--|--|
| Host: | 10.62.148.67 | | | |
| Display Name: | FTD1 | | | |
| Registration Key: | cisco | | | |
| Group: | None | ~ | | |
| Access Control Policy: | FTD9300 | ~ | | |
| Smart Licensing Malware: | | | | |
| URL Filtering: | | | | |
| Advanced | | | | |
| On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page. | | | | |
| | Register Cano | el | | |

Verificatie vindt u zoals in de afbeelding.

| Cisco Firepower 9000 Series SM-36 Threat Defense Cluster | | | / 6 |
|--|---|---------|-----|
| FTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | |
| FTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 8 |
| FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 6 |

Task 4. Het configureren van poort-Channel sub-interfaces op FMC

Taakeis:

Configureer subinterfaces voor de poortkanaalgegevensinterface.

Oplossing:

Stap 1. Selecteer de knop FTD_cluster Bewerken vanuit de FMC GUI.

Navigeer naar het tabblad Interfaces en klik op het tabblad Add Interfaces > Subinterface zoals in de afbeelding.

| Overview Analysis Policies Devices Obje | ts AMP | | | Deploy | 🔒 System Help 🕶 olga 🕶 |
|--|----------------------|---------------|-----------------------------|------------|------------------------------------|
| Device Management NAT VPN Platform S | ettings | | | | |
| FTD_cluster | | | | | Seve Seve |
| Cisco Firepower 9000 Series SM-36 Threat Defense | | | | | |
| Cluster Devices Routing NAT Interfa | ces Inline Sets DHCP | | | | |
| 2 | | | | | Add Interfaces |
| Interface Logic | l Name Type | Security Zone | Mac Address(Active/Standby) | IP Address | Sub Interface |
| 10 Port-channel5 | EtherChannel | | | | 1 |
| III Port-channel48 | EtherChannel | | | | ۹. |
| Ethernet1/1 diagno | itic Physical | | | | 1 |

Configureer de eerste subinterface met deze details. Selecteer **OK** om de wijzigingen en zoals in de afbeeldingen toe te passen.

| Name | Binnenin |
|------------------|------------------------|
| Algemeen tabblad | |
| Interface | Poortkanaal5 |
| Subinterface-ID | 201 |
| VLAN-id | 201 |
| IPv4-tabblad | |
| IP-type | Statische IP gebruiken |
| IP-adres | 192.168.75.10/24 |

| Add Sub Interface ? × | | | | |
|-----------------------|---------------|------------------|-----------|--|
| Name: Inside | Enabled | Management Only | | |
| Security Zone: | * | - | | |
| Description: | | | | |
| General IPv4 IPv6 | Advanced | | | |
| MTU: | 1500 | (64 - 9000) | | |
| Interface *: | Port-channel5 | Enabled | | |
| Sub-Interface ID *: | 201 | (1 - 4294967295) | | |
| VLAN ID: | 201 | (1 - 4094) | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | OK Cancel | |

| Add Sub Interfac | e ? × | |
|------------------|---|--|
| Name: Insid | de Catalog Management Only | |
| Security Zone: | ~ | |
| Description: | | |
| General IPv4 I | Pv6 Advanced | |
| IP Type: | Use Static IP | |
| IP Address: | eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | OK Cancel | |

Configureer de tweede subinterface met deze details.

| Name | Buiten |
|------------------|------------------------|
| Algemeen tabblad | |
| Interface | Poortkanaal5 |
| Subinterface-ID | 210 |
| VLAN-id | 210 |
| IPv4-tabblad | |
| IP-type | Statische IP gebruiken |
| IP-adres | 192.168.76.10/24 |

Klik op **OK** om de subinterface te maken. Klik op **Opslaan** en voer vervolgens wijzigingen in het FTD_cluster in zoals in de afbeelding.

Verificatie:

| Overview Analysis Policies Devices Objects AMP | | Deploy 🧕 System Help 🔹 olga 🔹 | | | | | | | |
|--|--|-------------------------------|--|--|--|--|--|--|--|
| Device Management NAT VPN Platform Settings | | | | | | | | | |
| FTD_cluster | | | | | | | | | |
| Cisco Firepower 9000 Series SM-36 Threat Defense | | | | | | | | | |
| Cluster Devices Routing NAT Interfaces Inline Sets | DHCP | | | | | | | | |
| 2 | | Add Interfaces • | | | | | | | |
| Interface Logical Name | Type Security Zone Mac Address(Active/Standby) | IP Address | | | | | | | |
| Port-channel5 | EtherChannel | 1 | | | | | | | |
| Port-channel48 | EtherChannel | ٩, | | | | | | | |
| Ethernet1/1 diagnostic | Physical | 1 | | | | | | | |
| Port-channel5.201 Inside | SubInterface | 192.168.75.10/24(Static) | | | | | | | |
| Port-channel5.210 Outside | SubInterface | 192.168.76.10/24(Static) | | | | | | | |

Task 5. Controleer de basisconnectiviteit

Taakeis:

Maak een opname en controleer de connectiviteit tussen twee VM's.

Oplossing:

Stap 1. Maak opnamen op alle clustereenheden.

Navigeer naar LINA (ASA) CLI van Mastereenheid en creëer vangen voor de binnen en buitenkant interfaces.

firepower# firepower# cluster exec capture capi interface inside match icmp any any firepower# firepower# cluster exec capture capo interface outside match icmp any any firepower# Verificatie: firepower# cluster exec show capture capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any

match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any

Stap 2. Voer de ping-test uit van VM1 naar VM2.

Doe de test met 4 pakketten. Controleer de opnametoevoer na de test:

firepower# cluster exec show capture capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any capture capi type raw-data interface Inside [Capturing - 752 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 752 bytes] match icmp any any capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any

firepower#

Start de opdracht om de opnametoevoer op de specifieke eenheid te controleren:

firepower# cluster exec unit unit-1-3 show capture capi

8 packets captured

| 1: | 12:58:36.162253 | 802.1Q | vlan#201 | Р0 | 192.168.75.100 | > | 192.168.76.100 | : icmp: | echo | |
|--------|-----------------|--------|----------|----|----------------|---|----------------|---------|------|-------|
| reques | st | | | | | | | | | |
| 2: | 12:58:36.162955 | 802.1Q | vlan#201 | P0 | 192.168.76.100 | > | 192.168.75.100 | : icmp: | echo | reply |
| 3: | 12:58:37.173834 | 802.1Q | vlan#201 | РO | 192.168.75.100 | > | 192.168.76.100 | : icmp: | echo | |
| reques | st | | | | | | | | | |
| 4: | 12:58:37.174368 | 802.1Q | vlan#201 | P0 | 192.168.76.100 | > | 192.168.75.100 | : icmp: | echo | reply |
| 5: | 12:58:38.187642 | 802.1Q | vlan#201 | РO | 192.168.75.100 | > | 192.168.76.100 | : icmp: | echo | |
| reques | st | | | | | | | | | |
| 6: | 12:58:38.188115 | 802.1Q | vlan#201 | P0 | 192.168.76.100 | > | 192.168.75.100 | : icmp: | echo | reply |
| 7: | 12:58:39.201832 | 802.1Q | vlan#201 | РO | 192.168.75.100 | > | 192.168.76.100 | : icmp: | echo | |
| reques | st | | | | | | | | | |
| 8: | 12:58:39.202321 | 802.1Q | vlan#201 | P0 | 192.168.76.100 | > | 192.168.75.100 | : icmp: | echo | reply |
| 8 pacl | kets shown | | | | | | | | | |

firepower# cluster exec unit unit-1-3 show capture capo

8 packets captured

| 1: | 12:58:36.162543 | 802.1Q | vlan#210 | P0 | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
|--------|---|--------|----------|----|----------------|---|-----------------|-------|------|-------|
| reques | st | | | | | | | | | |
| 2: | 12:58:36.162894 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 3: | 12:58:37.174002 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reques | st | | | | | | | | | |
| 4: | 12:58:37.174307 | 802.1Q | vlan#210 | P0 | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 5: | 12:58:38.187764 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reques | st | | | | | | | | | |
| 6: | 12:58:38.188085 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 7: | 12:58:39.201954 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reques | st | | | | | | | | | |
| 8: | 12:58:39.202290 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 8 pacl | kets shown | | | | | | | | | |
| firepo | firepower# | | | | | | | | | |
| Nada | Vadat u deze taak hebt voltooid, verwijdert u de opname met de volgende opdracht: | | | | | | | | | |

Controleer de uitvoer van de show:

TCP Outside 192.168.76.100:49175 Inside 192.168.75.100:21, idle 0:00:32, bytes 665, flags UIOEN UDP cluster 255.255.255.255.255:49495 NP Identity Ifc 127.2.1.1:49495, idle 0:00:00, bytes 17858058, flags -TCP cluster 127.2.1.3:10844 NP Identity Ifc 127.2.1.1:38296, idle 0:00:33, bytes 5496, flags UI

TCP cluster 127.2.1.3:59588 NP Identity Ifc 127.2.1.1:10850, idle 0:00:33, bytes 132, flags UO

TCP Outside 192.168.76.100:49175 Inside 192.168.75.100:21, idle 0:00:34, bytes 0, flags y
TCP cluster 127.2.1.1:10851 NP Identity Ifc 127.2.1.3:48493, idle 0:00:52, bytes 224, flags UI
.......
TCP cluster 127.2.1.1:64070 NP Identity Ifc 127.2.1.3:10847, idle 0:00:11, bytes 806, flags U0

TCP cluster 127.2.1.1:10851 NP Identity Ifc 127.2.1.2:64136, idle 0:00:53, bytes 224, flags UI TCP cluster 127.2.1.1:15859 NP Identity Ifc 127.2.1.2:10847, idle 0:00:11, bytes 807, flags UO Uitvoer weergeven:

Cluster Capture van Chassis Manager UI

In de volgende afbeelding kunt u een 3-eenheid cluster op FPR9300 met 2 poortkanalen (8 en 48) zien. De logische hulpmiddelen zijn ASA's, maar in het geval van FTD zal hetzelfde concept zijn.Het belangrijkste om te onthouden is dat er weliswaar **3 clustereenheden** zijn, maar dat er vanuit het oogpunt van de vangst slechts **één logisch apparaat** is:

| 0 | ver | view Interfaces | Logical Devices | Security Mod | dules Platform Settir | ngs | | Sys | tem Tools Help admin |
|----|------|---|---------------------------------|--------------|--|---|-----------------|----------|----------------------|
| Lo | gica | l Device List | | | | | | d | Refresh O Add Device |
| | AS | SA C | lustered | Status:ok | | | | | F. 2 E 🔹 |
| l | s | ecurity Module | Application | Version | Management IP | Gateway | Management Port | Status | |
| 6 | s | ecurity Module 1 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 🕶 💱 À |
| | | Ports: Data Interfaces: Cluster Interfaces: | Port-channel8 Port-channel48 | A | ttributes: Cluster Operational Status : Management IP VIRTUAL : Cluster Role : Management URL : Management IP : | : in-cluster 10.111.8.206 master https://10.111.8.206/ 10.111.8.193 | | | |
| G | s | ecurity Module 2 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 💌 🎉 🌧 |
| | | Ports: Data Interfaces: Cluster Interfaces: | Port-channel8 Port-channel48 | A | ttributes: Cluster Operational Status : Management IP VIRTUAL Cluster Role : Management URL : Management IP : | in-cluster 10.111.8.206 slave https://10.111.8.206/ 10.111.8.189 | | | |
| G | s | ecurity Module 3 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 🕶 🎉 |
| | | Ports: Data Interfaces: Cluster Interfaces: | Port-channel8 Port-channel48 | A | ttributes: Cluster Operational Status : Management IP VIRTUAL : Cluster Role : Management URL : Management IP : | in-cluster 10.111.8.206 slave https://10.111.8.206/ 10.111.8.190 | | | |

| Overview Interfaces Logical Devices | Security Modules Platform Settings | Systen | Tools Help admin |
|-------------------------------------|--|---|------------------|
| | Save and Run | Save Cancel | Packet Capture |
| ASA | | Session Name* ARP Selected Interfaces Ethernet1/ | 5 |
| Ethernet1/1 | | Buffer Size 256 MB | ~ |
| Ethernet1/8 (Portchannel48) | | Snap length: 1518 | Bytes |
| Ethernet1/7 (Portchannel48) | | Store Packets Overwr | ite Append |
| Ethernet1/6 (Portchannel48) | | Capture Filter Apply Fi | Iter Capture All |
| Ethernet1/5 (Portchannel48) | ASA | | |
| Ethernet1/4 (Portchannel48) | Ethernet1/9, Ethernet1/10, Ethernet1/11, Ethernet1/12, Ethernet1/13, Ethernet1/14 | | |
| Ethernet1/3 (Portchannel48) | | | |
| Ethernet1/2 (Portchannel48) | | | |
| Ethernet2/2 (Portchannel8) | | | |
| Ethernet2/1 (Portchannel8) | | | |

Task 6. Verwijdert een Slave-apparaat uit de Cluster.

Taakeis:

Log in op het FMC en verwijder de slaveneenheid uit het cluster.

Oplossing:

Stap 1. Meld u aan bij het FMC en navigeer naar het apparaat > Apparaatbeheer.

Klik op het pictogram afval naast de slangeenheid zoals in de afbeelding weergegeven.

| Cisco Firepower 9000 Series SM-36 Threat Defense Cluster | | | <i>s</i> 6 |
|--|---|---------|------------|
| FTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | |
| FTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 8 |
| FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 8 |

Het bevestigingsvenster verschijnt. Selecteer Ja om te bevestigen zoals in de afbeelding.

| Confirm Delete | | | | | | | | |
|---|------|--|--|--|--|--|--|--|
| Device "FTD2" will be deleted from Cluster "FTD_cluster" in Firepower Management Center but will be available in Firepower Security Appliance. Do you want to continue? | | | | | | | | |
| Ye | s No | | | | | | | |

Verificatie:

• Van het FMC zoals in de afbeelding weergegeven.



• Van de FXOS CLI.

| FPR9K-1-A# scope ssa FPR9K-1-A /ssa # show app-instance | | | | | | | | | |
|--|------------------|-------------|-------------------|-----------------|------------|--|--|--|--|
| Application Name Version Cluster Oper | Slot ID State | Admin State | Operational State | Running Version | Startup | | | | |
| | | | | | | | | | |
| ftd | 1 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |
| ftd | 2 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |
| ftd | 3 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |

• Van de LINA (ASA) CLI.

```
firepower# show cluster info
Cluster FTD_cluster: On
    Interface mode: spanned
   This is "unit-1-1" in state MASTER
       ID
             : 0
       Version : 9.6(1)
       Serial No.: FLM19216KK6
       CCL IP : 127.2.1.1
       CCL MAC : 0015.c500.016f
       Last join : 21:51:03 CEST Aug 8 2016
       Last leave: N/A
Other members in the cluster:
   Unit "unit-1-3" in state SLAVE
       ID
           : 1
       Version : 9.6(1)
       Serial No.: FLM19206H7T
       CCL IP : 127.2.1.3
       CCL MAC : 0015.c500.018f
       Last join : 21:51:05 CEST Aug 8 2016
       Last leave: N/A
    Unit "unit-1-2" in state SLAVE
                : 2
       ID
       Version : 9.6(1)
       Serial No.: FLM19206H71
       CCL IP : 127.2.1.2
CCL MAC : 0015.c500.019f
       Last join : 21:51:30 CEST Aug 8 2016
       Last leave: N/A
```

firepower#

Opmerking: Het apparaat is niet geregistreerd bij het FMC, maar is nog steeds een clusterlid op de FPR9300.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De verificatie wordt voltooid en in afzonderlijke taken geregeld.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

• Alle versies van de Cisco Firepower Management Center-configuratiehandleiding zijn hier te vinden:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepowerroadmap.html#id_47280.

• Alle versies van de FXOS Chassis Manager en de CLI configuratiegidsen zijn hier te vinden: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfld-121950</u>.

 Cisco Global Technical Assistance Center (TAC) raadt deze visuele handleiding voor diepgaande praktische kennis van Cisco Firepower Next-generation security technologieën aan, inclusief de technologieën die in dit artikel worden genoemd:

http://www.ciscopress.com/title/9781587144806.

• TechNotes over configuratie en probleemoplossing die betrekking hebben op FirePOWERtechnologieën.

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-serieshome.html.

<u>Technische ondersteuning en documentatie – Cisco Systems</u>