Beleid voor FTD-voorfilter configureren en gebruiken

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Prefilter Policy Use Case 1 Pre-filter Policy Use Case 2 Taak 1. Controleer het standaardbeleid voor het filter CLI (LINA)-verificatie

Inleiding

In dit document worden de configuratie en werking van het beleid voor het voorfilteren van FirePOWER Threat Defence (FTD) beschreven.

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:

- ASA 5506X die FTD-code 6.1.0-195 gebruikt
- FireSIGHT Management Center (FMC) met 6.1.0-195
- Twee 3925 Cisco IOS®-routers die 15.2 afbeeldingen uitvoeren

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 Prefilter Policy is een functie die in versie 6.1 is geïntroduceerd en dient drie hoofddoelen:

- 1. Match traffic op basis van zowel de binnen- als de buitenkop
- 2. Verstrek vroege toegangscontrole die een stroom toestaat om snort motor volledig te omzeilen
- 3. Werk als plaatsaanduiding voor toegangscontrolevermeldingen (ACE's) die zijn gemigreerd vanuit de migratietool Adaptieve security applicatie (ASA).

Configureren

Prefilter Policy Use Case 1

Een prefilterbeleid kan een tunnelregeltype gebruiken waarmee FTD kan filteren op basis van zowel binnen als buiten IP-headerverkeer. Toen dit artikel werd geschreven, verwijst tunnelverkeer naar:

- Generic Routing Encapsulation (GRE)
- IP-in-IP
- IPv6-in-IP
- Teredo-poort 3544

Beschouw een GRE-tunnel zoals in de afbeelding.



Wanneer u van R1 naar R2 pingelt met behulp van een GRE-tunnel, gaat het verkeer door de Firewall zoals in de afbeelding.

| 1 2016-05-31 02:15:15.10.0.0.1 | 10.0.0.2 | ICMP | 138 Echo | (ping) | request | id=0x0013, | seq=0/0, |
|--|-----------------|-----------|--------------|---------|-----------|-------------|----------|
| 2 2016-05-31 02:15:15.10.0.0.2 | 10.0.0.1 | ICMP | 138 Echo | (ping) | reply | id=0x0013, | seq=0/0, |
| < | | | | | | | |
| ■ Frame 1: 138 bytes on wire (1104 bits), | 138 bytes capt | tured (11 | LO4 bits) | | | | |
| ■ Ethernet II, Src: CiscoInc_8d:49:81 (c8) | :4c:75:8d:49:81 | l), Dst: | CiscoInc_a1 | :2b:f9 | (6c:41:6 | a:a1:2b:f9) | |
| Internet Protocol Version 4, Src: 192.1 | 68.75.39 (192.1 | 68.75.39 | 9), Dst: 192 | .168.70 | 5.39 (192 | .168.76.39) | duter |
| Generic Routing Encapsulation (IP) | | | | | | | |
| ■ Internet Protocol Version 4, Src: 10.0. | 0.1 (10.0.0.1), | , Dst: 10 |).0.0.2 (10. | 0.0.2) | | inner | |
| Internet Control Message Protocol | | | | | | | |

Als de firewall een ASA-apparaat is, controleert hij de externe IP-header zoals in de afbeelding.

| L2 Header | Outer IP Header src=192.168.75.39 dst=192.168.76.39 | GRE Header | Inner IP Header src=10.0.0.1 dst=10.0.0.2 | L7 |
|--------------|--|---------------|--|----|
|--------------|--|---------------|--|----|

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

, idle 0:00:17, bytes 520, flags

Als de firewall een FirePOWER-apparaat is, controleert hij de interne IP-header zoals in de afbeelding.

| L2 (Header H | Duter IP Header src=192.168.75.39 dst=192.168.76.39 | GRE Header | Inner IP Header src=10.0.0.1 dst=10.0.0.2 | L7 |
|------------------|--|---------------|--|----|
|------------------|--|---------------|--|----|

Met prefilterbeleid kan een FTD-apparaat verkeer koppelen op basis van zowel binnen- als buitenkoppen.

Belangrijkste punt:

| Apparaat | Controles |
|----------|---|
| ASA | Buitenste IP |
| Snort | Binnenste IP |
| FTD | Buitenzijde (voorfilter) + Binnenste IP (Toegangscontrolebeleid (ACS)) |

Pre-filter Policy Use Case 2

Een Prefilterbeleid kan een Prefilter Regel Type gebruiken dat vroege toegangscontrole kan verstrekken en een stroom toestaan om de Snort motor volledig zoals getoond in het beeld te mijden.



Taak 1. Controleer het standaardbeleid voor het filter

Taakvereiste:

Controleer het standaard prefilterbeleid

Oplossing:

Stap 1. Ga naar **Beleid > Toegangsbeheer > Prefilter**. Er bestaat al een standaardbeleid voor voorfilters, zoals in de afbeelding.

| Overview Analysis Polici | es Devices O | bjects | AMP | | | Deploy |) 📀 | System | Help 🔻 | mikis 🔻 |
|--|-------------------------|-----------|---------------|-------------|------------------|-----------------------------|------|------------|--------------|------------|
| Access Control > Prefilter N | etwork Discovery | Applicati | ion Detectors | Correlation | Actions • | | | | | |
| | | | | | | | Obje | ct Manager | nent Acce | ss Control |
| | | | | | | | | | 🔘 New I | Policy |
| | | | | | | | | | | |
| Prefilter Policy | | | Domain | | Last M | lodified | | | | |
| Default Prefilter Policy Default Prefilter Policy with defa | ult action to allow all | tunnels | Global | | 2016- Modifie | 04-22 21:43 ed by "admin | :25 | | D 🖉 E | 1 |

Stap 2. Kies Bewerken om de beleidsinstellingen te zien zoals in de afbeelding.

| Overview Analysis Policies Devices Objects AMP | | | | | | | | | | |
|--|-------------|-----------------|------------------|------------------|-----------------|-----------------|----------------|----------------|------------------|--------|
| Acce | ss Control | Prefilter | Network | c Discovery | Applicat | tion Detecto | rs Corr | relation | Actions • | |
| Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels Rules | | | | | | | | | | |
| | | | | | | | | | | |
| * | Name | Rule T | Source Interf | Destin Interf | Source Netwo | Destin Netwo | Source Port | Destin Port | VLAN | Action |
| You cannot add rules to the default Prefilter policy. You can change only default action options. | | | | | | | | | | |
| Nor | -tunneled t | raffic is allow | ed | De | fault Actior | n: Tunnel Traf | ffic Ar | nalyze all tur | nel traffic | |

Stap 3. Het prefilterbeleid is al gekoppeld aan het toegangscontrolebeleid zoals in de afbeelding.



CLI (LINA)-verificatie

Voorfilterregels worden bovenop ACL's toegevoegd:

<#root>

firepower#

show access-list

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 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc
```

Taak 2. Blok tunnelverkeer met tag

Taakvereiste:

Blokkeer ICMP-verkeer dat is getunneld binnen GRE-tunnel.

Oplossing:

Stap 1. Als u deze ACS toepast, kunt u zien dat ICMP-verkeer wordt geblokkeerd, ongeacht of het door de GRE-tunnel gaat of niet, zoals in de afbeelding.

| P | refil | er Policy: Default Prefi | ter Policy | | | | SSL Policy: No | 08 | | | Identity Policy: None | | | | | |
|---|----------------------------|----------------------------|-------------------|---------------|--------------------|------------------|----------------|-------|----------------|-----------|-----------------------|-----------------|-----------------------|--------------|---------------------------|------------|
| | Devi | Constitution interfere | | 0 | thunsed | | | | | | | | Te . | Inheritance | Settings 🧾 Policy Assig | nments (1) |
| | | iter hy Device | SIGE HITPI | Responses | Advanced | | | | | | | a Add Category | 0 444 80 | la Search | Rules | × |
| | - | inter by better | | | | | | | | | | g Hod Category | 0 100 10 | | | ~ |
| | • | Name | Source Zones | Dest Zones | Source Networks | Dest Networks | VLAN Tags | Users | Applicatio | Source Po | Dest Ports | URLS | ISE/SGT Attributes | Action | | |
| | • 1 | tandatory - ACP_SS06 | -1 (1-1) | | | | | | | | | | | | | |
| | 1 | Block ICMP | any | any | any | any | any | any | C3 Filter: ICM | P any | any | any | any | X Block | 00.802 | / 8 |
| | ▼ Default - ACP_SS06-1 {-} | | | | | | | | | | | | | | | |
| | The | e are no rules in this sec | tion. Add Rule or | Add Category | | | | | | | | | | | | |
| | Def | sult Action | | | | | | | | | | Intrusion Preve | ntion: Balanced | Security and | d Connectivity | ¥ \$ 📘 |

<#root>

R1#

ping 192.168.76.39

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
<#root>
R1#
ping 10.0.0.2
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

In dit geval kunt u een Prefilterbeleid gebruiken om aan de taakvereiste te voldoen. De logica is als volgt:

- 1. U labelt alle pakketten die zijn ingekapseld in GRE.
- 2. U maakt een beleid voor toegangscontrole dat overeenkomt met de gelabelde pakketten en blokkeert ICMP.

Vanuit architectuuroogpunt worden de pakketten gecontroleerd aan de hand van de Linux NAvely (LINA) voorfilterregels, vervolgens Snort voorfilterregels en ACP, en ten slotte geeft Snort LINA de opdracht te drogen. Het eerste pakket maakt het door het FTD-apparaat.

Stap 1. Definieer een tag voor tunnelverkeer.

Navigeer naar **Beleid > Toegangsbeheer > Prefilter** en maak een nieuw Prefilterbeleid. Onthoud dat het standaard voorfilterbeleid niet kan worden bewerkt zoals in de afbeelding.

| | | Object Management Access Control |
|--------------|-------------------|----------------------------------|
| | | New Policy |
| Last Mod | ified | |
| New Policy | | ? × |
| Name: | Prefilter_Policy1 | |
| Description: | | |
| _ | | Save Cancel |

Binnen het Prefilterbeleid kunt u twee soorten regels definiëren:

- 1. Tunnelregel
- 2. Prefilterregel

U kunt deze twee als totaal verschillende functies die kunnen worden geconfigureerd in een Prefilter-beleid.

Voor deze taak is het noodzakelijk om een tunnelregel te definiëren zoals in de afbeelding.

| Add Tunn | el Rule | | | | | | ? × |
|--|---|--------------------|----------------------------|--------------------------|-----------------------|-----------------------|---------------|
| () Tunne | al rules perform early handlin | g of non-encrypted | encapsulated traffic, usin | g outer IP headers. Fast | pathed traffic bypass | es access control and | i QoS. |
| Name | Tag Tunneled traffic | | ✓ Enabled | Insert | below rule | ۲ 1 | |
| Action | ✓ Analyze 1 | * | | Assign Tunnel Tag | Inside_the_GRE | | × 0 |
| Interf Encapsula GRE IP-in-I IPv6-in Teredo | face Objects Networks ation Protocols: 3 IP n-IP o Port (3544) | VLAN Tags E | ncapsulation & Ports | 2 | | Co | mment Logging |

Wat de acties betreft:

| Actie | Beschrijving |
|-------------------|---|
| Analyseren | Na LINA wordt de stroom gecontroleerd door Snort Engine. Naar keuze kan een tunneltag worden toegewezen aan het tunnelverkeer. |
| Block (blokkeren) | De stroom wordt geblokkeerd door LINA. De kop aan de buitenkant moet worden gecontroleerd. |
| Fast Path | De stroom wordt alleen afgehandeld door LINA zonder de noodzaak om de Snort- motor te starten. |

Stap 2. Bepaal het Toegangsbeheerbeleid voor het gelabelde verkeer.

Alhoewel het in eerste instantie niet erg intuïtief kan zijn, kan de Tunnel Tag door een Access Control Policy Rule gebruikt worden als een Source Zone. Navigeer naar **Beleid > Toegangsbeheer** en maak een regel die ICMP voor het gelabelde verkeer blokkeert zoals in de afbeelding.

| Over | new Analysis Policies Devices C | bjects AMP | | | | | | | | | | | Deploy |
|----------------|--|-----------------------|----------------|--------------------|------------------|-----------|-------|----------------|--------------|------------|------|---------------------------|------------------|
| Acces | s Control + Access Control Network | Siscovery Application | tion Detectors | Correlation | Actions • | | | | | | | | |
| ACP Enter S | ACP_5506-1 Enter Description | | | | | | | | | | | | |
| Prefik | Prefilter Policy Intelligence UTD Responses Advanced | | | | | | | | | | | | |
| at r | ter by Device | | | | | | | | | | | Add Category Ad | d Rule Search |
| | Name | Source Zones | lest Iones | Source Networks | Dest Networks | VLAN Tags | Users | Applications | Source Ports | Dest Ports | URLs | ISE/SGT Attributes | Action |
| - 11 | andatory - ACP_5506-1 (1-1) | | | | | | | | | | | | |
| 1 | Block 3CHP | 🗟 Inside_the_GRE | ety. | any | any | any | any. | 3 Filter: JCMP | any | any | any | any | X Block |
| - | ▼ Default - ACP_5506-1 (-) | | | | | | | | | | | | |
| There | There are no rules in this section. Add Rule or Add Category | | | | | | | | | | | | |
| Defa | alt Action | | | | | | | | | | | Intrusion Prevention: Bal | anced Security a |
| | | | | | | | | | | | | | |

Opmerking: het nieuwe prefilterbeleid is gekoppeld aan het toegangscontrolebeleid.

Verificatie:

Opname op LINA en op CLISH inschakelen:

<#root>

firepower#

show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]

<#root>

>

capture-traffic

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection?
1
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
-n
```

Van R1, probeer om het verre GRE tunneleindpunt te pingelen. Het pingelen mislukt:

<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

```
• • • • •
```

```
Success rate is 0 percent (0/5)
```

De CLISH-opname laat zien dat het eerste echoverzoek door FTD is gegaan en dat het antwoord is geblokkeerd:

<#root>

```
Options: -n

18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo I

18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo I

18:21:15.759939 IP
```

De LINA Capture bevestigt dit:

<#root>

>

show capture CAPI | include ip-proto-47

102: 18:21:07.767523 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104 107: 18:21:09.763739 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104 111: 18:21:11.763769 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104

```
115: 18:21:13.763784 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
120: 18:21:15.763830 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
>
show capture CAPO | include ip-proto-47
93: 18:21:07.768133 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
94: 18:21:07.768438 192.168.76.39 > 192.168.75.39: ip-proto-47, length 104
```

Schakel CLISH-firewall-engine-debug in, wis LINA ASP drop-tellers en voer dezelfde test uit. De CLISH debug toont aan dat voor de Echo-request u de prefilterregel en voor de Echo-Reply de ACS-regel heeft aangepast:

<#root>

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

New session

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, g

icmpType 8, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId 10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, q

5

icmpType 0, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

match rule order 3, 'Block ICMP', action Block

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action

De ASP-drop laat zien dat Snort de pakketten liet vallen:

<#root>

>

show asp drop

| Frame drop: | |
|--|-----|
| No route to host (no-route) | 366 |
| Reverse-path verify failed (rpf-violated) | 2 |
| Flow is denied by configured rule (acl-drop) | 2 |
| | |

Snort requested to drop the frame (snort-drop)

In de Verbindingsgebeurtenissen kunt u het Prefilterbeleid en de -regel zien die u hebt aangepast zoals in de afbeelding.

| Ove | Overview Analysis Policies Devices Objects AMP | | | | | | | | | | | |
|-------------------------------------|--|---------------------|---------------|-------------|-------------|------------------------------|-----------------------------------|----------------------------|----------------|-----------------------|--|--|
| Con | text E | xplorer Connectio | ns ► Events | Intrusions | Files • I | Hosts • Users • \ | Vulnerabilities • Corr | elation • Custom • | Lookup • Se | arch | | |
| | Bookmark Th | | | | | | | | | | | |
| Connection Events (switch workflow) | | | | | | | | | | | | |
| Con | Connections with Application Details > Table View of Connection Events | | | | | | | | | | | |
| • Se | Search Constraints (Edit Search) | | | | | | | | | | | |
| Ju | mp to | | | | | | | | | _ | | |
| | Г | • First Packet × | Action × | Initiator × | Responder × | Source Port / × ICMP Type | Destination Port / X ICMP Code | Access Control × Policy | Access Control | Prefilter × Policy | <u>Tunnel/Prefilter</u> × <u>Rule</u> | |
| 4 | | 2016-05-21 14:27:54 | Block | 10.0.0.1 | il 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP 5505-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 14:26:51 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP_5506-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 14:24:52 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP 5505-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 14:21:07 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP_5506-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 13:27:04 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP 5505-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 13:24:36 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0./ icmp | ACP_5506-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 4 | | 2016-05-21 13:15:26 | Block | 10.0.0.1 | 10.0.0.2 | 8 (Echo Request) / icmp | 0 / icmp | ACP_5505-1 | Block ICMP | Prefilter Policy1 | Tag Tunneled traffic | |
| 14 | (Page | 1 of 1 >> Display | ying rows 1-7 | of 7 rows | | | | | | | | |

Taak 3. Bypass Snort Engine met FastPath Prefilter Regels

Netwerkdiagram

| | | FTD | | |
|----|-----------------|-----|-----------------|----|
| R1 | 192.168.75.x/24 | | 192.168.76.x/24 | R2 |
| | .39 | | .39 | |
| | inside | | outside | |

Taakvereiste:

- 1. Verwijder de huidige regels van het Toegangsbeheer en voeg een regel van het Toegangsbeheer toe die al verkeer blokkeert.
- 2. Configureer een beleidsregel Prefilter die de Snortengine voor verkeer omzeilt vanuit het 192.168.75.0/24-netwerk.

Oplossing:

Stap 1. Toegangscontrolebeleid dat alle verkeer blokkeert, is zoals in de afbeelding wordt weergegeven.

| | Rulas Sequrity Intelligence HTTP Responses Advanced | | | | | | | | | | | | | | |
|--|---|-----------------|---------------|----------------|--------------|------|-------|-------|-------|-----------------------------------|------|----------------|------|-------------|-----|
| in the second se | Advanced Advanced Image: Filter by Device Image: Advanced Image: Filter by Device Image: Advanced | | | | | | | | | | | | | | |
| | Name | Source Zones | Dest Zones | Source Netw | Dest Netw | VLAN | Users | Appli | Sourc | Dest | URLs | ISE/ Attrib | Acti | • • • • • • | |
| - | Mandatory | - ACP_550 | 6-1 (-) | | | | | | | | | | | | |
| Th | ere are no ru | les in this se | ection. Add | Rule or Add | Category | | | | | | | | | | |
| - | Default - A | CP_5506-1 | (-) | | | | | | | | | | | | |
| Th | There are no rules in this section. Add Rule or Add Category | | | | | | | | | | | | | | |
| De | fault Action | | | | | | | | | Access Control: Block All Traffic | | | | | × 🔳 |
| _ | | | | | | | | | | | | | | | |

Stap 2. Voeg een Prefilterregel toe met Fastpath als een actie voor bronnetwerk 192.168.75.0/24 zoals in de

afbeelding.

| Add Prefilter Rule | | | | | ? X |
|--|---|-------------------------------------|---------------------------|----------------------|---------|
| Prefilter rules perform early handlin | g of traffic based on simple | network characteristics. Fastpath | ed traffic bypasses acces | s control and QoS. | |
| Name Fastpath_src_192.168.75. Action ➡ Fastpath | 0/24 | Enabled | | | |
| Interface Objects Networks | VLAN Tags Ports | | | Comment | Logging |
| Available Networks | O | Source Networks (1) | Dest | ination Networks (0) | |
| Search by name or value any PV4-Private-All-RFC1918 any-ipv4 any-ipv6 IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast | Add to Source Add to Destination | <pre>>> 192.168.75.0/24</pre> | any any | | |
| IPv4-Private-10.0.0.0-8 | | Enter an IP address | Add Ente | r an IP address | Add |

Stap 3. Het resultaat is zoals in de afbeelding.

| Overview | Analysis Policies | Devices Objects | AMP | | | | Deploy |)System Help 🔻 | mikis v | |
|--------------------------------------|---|-------------------|---------------------|-------------------|----------|----------------------|------------------------|----------------|---------|--|
| Access Con | trol • Prefilter Netv | vork Discovery Ap | plication Detectors | Correlation Actio | ns 🔻 | | | | | |
| Prefilter Enter Descrip | Prefilter_Policy1 Enter Description Rules | | | | | | | | | |
| Rules | | | | | O Add Tu | nnel Rule 🛛 🔾 Add Pr | refilter Rule Search R | ules | × | |
| | Name | Rule Type | Source | Destination | Source | Destination | Source | Destination | VLAN 1 | |
| | | and the | Interface Objects | Interface Objects | Networks | Networks | Port | Port | | |
| 1 Fastpath_src_192.168. Prefilter an | | any | any | 2 192.168.75.0/24 | any | any | any | any | | |
| Non-tunnel | ed traffic is | | | | | | | | | |

Stap 4. Opslaan en implementeren.

Opname met spoor op beide FTD-interfaces inschakelen:

<#root> firepower# capture CAPI int inside trace match icmp any any firepower# capture CAPO int outsid trace match icmp any any

Probeer via het FTD van R1 (192.168.75.39) naar R2 (192.168.76.39) te pingen. Pingen mislukt:

<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

```
Success rate is 0 percent (0/5)
```

Capture on the inside interface toont:

<#root>

.

firepower#

show capture CAPI

5 packets captured

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request 2: 23:35:09.278641 192.168.75.39 > 192.168.76.39: icmp: echo request 3: 23:35:11.279251 192.168.75.39 > 192.168.76.39: icmp: echo request 4: 23:35:13.278778 192.168.75.39 > 192.168.76.39: icmp: echo request 5: 23:35:15.279282 192.168.75.39 > 192.168.76.39: icmp: echo request 5 packets shown

Sporen van eerste pakket (echo-verzoek) toont (belangrijke gemarkeerde punten):

Spoiler (Markeren om te lezen)

FirePOWER# geeft opnamekaart CAPI-pakketnummer 1 weer

5 opgenomen pakketten

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo verzoek

Fase: 1

Type: OPNAME

Subtype:

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

MAC-toegangslijst

Fase: 2

Type: TOEGANGSLIJST

Subtype:

Resultaat: TOESTAAN

Config:

impliciete regel

Aanvullende informatie:

MAC-toegangslijst

Fase: 3

Type: ROUTE-LOOKUP

Subtype: Uitgaande interface oplossen

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

gevonden next-hop 192.168.76.39 gebruikt egress ifc buiten

Fase: 4

Type: TOEGANGSLIJST

Subtype: log

Resultaat: TOESTAAN

Config:

access-group CSM_FW_ACL_global

access-list CSM_FW_ACL_ geavanceerde vertrouwen ip 192.168.75.0 255.255.255.0 elke regel-id 268434448 gebeurtenislogboek beide

access-list CSM_FW_ACL_ remark regel-id 268434448: PREFILTER BELEID: Prefilter_Policy1

toegangslijst CSM_FW_ACL_ remark regel-id 268434448: REGEL: Fastpath_src_192.168.75.0/24

Aanvullende informatie:

Fase: 5

Type: CONN-INSTELLINGEN

Subtype:

Resultaat: TOESTAAN

Config:

class-map class-default

overeenkomen met een willekeurig

policy-map global_policy class class-default geavanceerde opties voor verbinding instellen UM_STATIC_TCP_MAP service-policy global_policy global Aanvullende informatie: Fase: 6 Type: NAT Subtype: per sessie Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 7 **Type: IP-OPTIES** Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 8 Type: INSPECTEREN Subtype: np-inspecteren Resultaat: TOESTAAN Config: class-map inspection_default verkeer met standaardinspectie vergelijken policy-map global_policy class inspection_default **ICMP** inspecteren service-policy global_policy global Aanvullende informatie:

Fase: 9

Type: INSPECTEREN Subtype: np-inspecteren Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 10 Type: NAT Subtype: per sessie Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 11 **Type: IP-OPTIES** Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 12 Type: FLOW-CREATIE Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: Nieuwe stroom die met id 52 is gemaakt, pakket verzonden naar volgende module Fase: 13 Type: TOEGANGSLIJST Subtype: log

Resultaat: TOESTAAN

Config:

access-group CSM_FW_ACL_global

access-list CSM_FW_ACL_ geavanceerde vertrouwen ip 192.168.75.0 255.255.255.0 elke regel-id 268434448 gebeurtenislogboek beide

access-list CSM_FW_ACL_ remark regel-id 268434448: PREFILTER BELEID: Prefilter_Policy1

toegangslijst CSM_FW_ACL_ remark regel-id 268434448: REGEL: Fastpath_src_192.168.75.0/24

Aanvullende informatie:

Fase: 14

Type: CONN-INSTELLINGEN

Subtype:

Resultaat: TOESTAAN

Config:

class-map class-default

overeenkomen met een willekeurig

policy-map global_policy

class class-default

geavanceerde opties voor verbinding instellen UM_STATIC_TCP_MAP

service-policy global_policy global

Aanvullende informatie:

Fase: 15

Type: NAT

Subtype: per sessie

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

Fase: 16

Type: IP-OPTIES

Subtype:

Resultaat: TOESTAAN

Config: Aanvullende informatie: Fase: 17 Type: ROUTE-LOOKUP Subtype: Uitgaande interface oplossen Resultaat: TOESTAAN Config: Aanvullende informatie: gevonden next-hop 192.168.76.39 gebruikt egress ifc buiten Fase: 18 Type: ADJACENCY-LOOKUP Subtype: volgende hop en nabijheid Resultaat: TOESTAAN Config: Aanvullende informatie: nabijheid Actief Next-hop mac-adres 0004.deab.681b hits 140372416161507 Fase: 19 Type: OPNAME Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: MAC-toegangslijst **Resultaat:** input-interface: buiten invoerstatus: omhoog inline-status: omhoog uitvoer-interface: buiten

uitvoerstatus: omhoog

uitvoerstatus: omhoog

Actie: toestaan

1 getoond pakket

vuurkracht#

FirePOWER# toont Capi-pakketnummer 1 spoor 5 pakketten opgenomen 1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo aanvraag Fase: 1 Type: CAPTURE Subtype: CAPTURE Subtype: Resultaat: TOESTAAN Config: Extra informatie: MAC-toegangslijst Fase: 2 Type: ACCESS-LIST Subtype: Resultaat: TOESTAAN Config: Impliciet Regel Aanvullende informatie: MAC-toegangslijst Fase: 3 Type: ROUTE-LOOKUP Subtype: Resultaat van de interface: STA Config toe: Aanvullende informatie: gevonden next-hop 192.168.76.39 gebruikt uitgaande ifc buiten fase: 4 Type: ACCESS-LIST Subtype: log Resultaat: STA Config toe: access-group CSM_FW_ACL_global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.0 elke regel-id 268434448 event-log zowel access-list CSM FW ACL remark-id: PREMARK-268434448 FILTERBELEID: Prefilter Policy1 access-list CSM FW ACL remark rule-id 268434448: REGEL: Fastpath_src_192.168.75.0/24 Aanvullende informatie: Fase: 5 Type: CONN-INSTELLINGEN Subtype: Resultaat: STA Config: class-map class-default match any policy-map global policy class-class-default set connection geavanceerde-opties UM STATIC TCP MAP servicepolicy global_policy global_policy global Aanvullende informatie: Fase: 6 Type: NAT Subtype: NAT Resultaat: PERSESSION Config: Aanvullende informatie: Fase: 8 Type: INSPECT Subtype: np-inspect Resultaat: STA Config toe: class-map inspection_default match default-inspection-traffic policy-map global policy class inspection default inspect icmp-service-policy global policy global Aanvullende informatie: Fase: 9 Type: INSPECT Subtype: np-inspect Resultaat: STA Config toe: Extra informatie: Fase: 11 Type: NAT Subtype: per-sessie Resultaat: STA Config toe: Extra informatie: Fase: 11 Type: IP-OPTIONS Subtype: Resultaat: STA Config: Extra informatie: Subtype: 12 Type: type: Resultaat: STA Config toe: Aanvullende informatie: Nieuwe stroom die is aangemaakt met id 52, pakket verzonden naar volgende module Fase: 13 Type: ACCESS-LIST Subtype: log Resultaat: STA Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 willekeurige regel-id 268434448 event-log beide access-list CSM_FW_ACL_ remark regel-id 268434448: PREFILTER BELEID1 CSM_FW_ACL_ remark regel-id 268434448: REGEL: Fastpath_src_192.168.75.0/24 Aanvullende informatie: Fase: 14 Type: CONN-INSTELLINGEN Subtype: Resultaat: STA Config toe: class-map class-default match om het even welke policy-map global_policy class-class-default set-verbinding geavanceerde opties UM_STATIC_TCP_MAP service-policy global_policy global Aanvullende informatie: Fase: 15 Type: NAT Subtype: per-sessie Resultaat: STA Config toe: Extra informatie: Fase: 16 Type: IP-OPTIONS Subtype: Resultaat: STA Config: 17 Type: ROUTE-LOOKUP Subtype: Resolve Uitgang Interface Resultaat: STA Config toe: Aanvullende informatie: gevonden volgende-hop 192.168.76.39 gebruikt uitgang ifc buiten fase: 18 Type: ADJACENCY-LOOKUP Subtype: volgende-hop en nabijheid Resultaat: STA Config toe: Aanvullende informatie: nabijheid Actief volgende-hop mac-adres 0004.deab.681b hits 140372416161507 Phase: 19 Type: CAPTURE Subtype: Resultaat: STA Config toe: ult: input-interface: buiten input-status: omhoog input-line-status: omhoog output-interface: buiten output-status: omhoog output-line-status: omhoog Actie: laat 1 pakket getoond vuurkracht# toe

De opname op de buiteninterface toont:

<#root>

firepower#

show capture CAPO

10 packets captured

| 1: | 23:35:07.282044 | 192.168.75.39 | > | 192.168.76.39: | icmp: | echo | request |
|-----|-----------------|---------------|---|----------------|-------|------|---------|
| 2: | 23:35:07.282227 | 192.168.76.39 | > | 192.168.75.39: | icmp: | echo | reply |
| 3: | 23:35:09.278717 | 192.168.75.39 | > | 192.168.76.39: | icmp: | echo | request |
| 4: | 23:35:09.278962 | 192.168.76.39 | > | 192.168.75.39: | icmp: | echo | reply |
| 5: | 23:35:11.279343 | 192.168.75.39 | > | 192.168.76.39: | icmp: | echo | request |
| 6: | 23:35:11.279541 | 192.168.76.39 | > | 192.168.75.39: | icmp: | echo | reply |
| 7: | 23:35:13.278870 | 192.168.75.39 | > | 192.168.76.39: | icmp: | echo | request |
| 8: | 23:35:13.279023 | 192.168.76.39 | > | 192.168.75.39: | icmp: | echo | reply |
| 9: | 23:35:15.279373 | 192.168.75.39 | > | 192.168.76.39: | icmp: | echo | request |
| 10: | 23:35:15.279541 | 192.168.76.39 | > | 192.168.75.39: | icmp: | echo | reply |
| | 1 | | | | | | |

10 packets shown

Spoor van het retourpakket toont aan dat het overeenkomt met de huidige stroom (52), maar het wordt geblokkeerd door de ACL:

<#root>

firepower#

show capture CAPO packet-number 2 trace

10 packets captured

2: 23:35:07.282227 192.168.76.39 > 192.168.75.39: icmp: echo reply

Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list

Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list

Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information:

Found flow with id 52, uses current flow

Phase: 4

Type: ACCESS-LIST

```
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Stap 5. Voeg nog een prefilterregel toe voor het retourverkeer. Het resultaat is zoals in de afbeelding.

| Overview / | Analysis Policies | Devices Objects | s AMP | | | | | Depl | oy 🛛 s | System H | elp • mikis • |
|-------------------|----------------------|-----------------|-----------------------------|----------------------------------|--------------------|-------------------------|-----------------|---------------------|--------------|----------|---------------|
| Access Contr | ol • Prefilter Net | work Discovery | Application Detectors | Correlation Actio | ns 🔻 | | | | | | |
| Prefilter_Policy1 | | | | | | | | | | | |
| | | | | | | | Add Tunnel Rule | Add Prefilter Rule | Search Rules | | 3 |
| • | Name | Rule Type | Source Interface Objects | Destination Interface Objects | Source Networks | Destination Networks | Source Port | Destination Port | VLAN Tag | | Action |
| 1 | Fastpath_src_192.168 | Prefilter | any | any | 2 192.168.75.0/24 | any | any | any | any | | 🕶 Fastpath |
| 2 | Fastpath_dst_192.168 | . Prefilter | any | any | any | 2 192.168.75.0/24 | any | any | any | | 👐 Fastpath |
| Non-tunneled | I traffic is allowed | | | | | | | | | Defaul | t Action: |

Vind nu het retourpakket dat u ziet (belangrijke punten gemarkeerd):

Spoiler (Markeren om te lezen)

FirePOWER# geeft opnamekaart CAPO pakketnummer 2 weer

10 opgenomen pakketten

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo antwoord

Fase: 1

Type: OPNAME

Subtype:

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

MAC-toegangslijst

Fase: 2

Type: TOEGANGSLIJST

Subtype:

Resultaat: TOESTAAN

Config:

impliciete regel

Aanvullende informatie:

MAC-toegangslijst

Fase: 3

Type: FLOW-LOOKUP

Subtype:

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

Gevonden stroom met id 62, gebruikt huidige stroom

Fase: 4

Type: TOEGANGSLIJST

Subtype: log

Resultaat: TOESTAAN

Config:

access-group CSM_FW_ACL_global

access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.255.0 regel-id 268434450 event-log

access-list CSM_FW_ACL_ remark regel-id 268434450: PREFILTER BELEID: Prefilter_Policy1

toegangslijst CSM_FW_ACL_ remark regel-id 268434450: REGEL: Fastpath_dst_192.168.75.0/24

Aanvullende informatie:

Fase: 5

Type: CONN-INSTELLINGEN

Subtype:

Resultaat: TOESTAAN

Config:

class-map class-default overeenkomen met een willekeurig policy-map global_policy class class-default geavanceerde opties voor verbinding instellen UM_STATIC_TCP_MAP service-policy global_policy global Aanvullende informatie: Fase: 6 Type: NAT Subtype: per sessie Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 7 **Type: IP-OPTIES** Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: Fase: 8 Type: ROUTE-LOOKUP Subtype: Uitgaande interface oplossen Resultaat: TOESTAAN Config: Aanvullende informatie: gevonden next-hop 192.168.75.39 gebruikt egress ifc binnenkant Fase: 9 Type: ADJACENCY-LOOKUP

Subtype: volgende hop en nabijheid

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

nabijheid Actief

Next-hop mac adres c84c.758d.4981 hits 140376711128802

Fase: 10

Type: OPNAME

Subtype:

Resultaat: TOESTAAN

Config:

Aanvullende informatie:

MAC-toegangslijst

Resultaat:

ingang-interface: binnen

invoerstatus: omhoog

inline-status: omhoog

uitvoer-interface: binnen

uitvoerstatus: omhoog

uitvoerstatus: omhoog

Actie: toestaan

FirePOWER# toont Capo-pakketnummer 2 spoor 10 pakketten opgenomen 2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: icmp: echo antwoord Fase: 1 Type: CAPTURE Subtype: CAPTURE Subtype: Resultaat: TOESTAAN Config: Extra informatie: MAC-toegangslijst Fase: 2 Type: ACCESS-LIST Subtype: Resultaat: TOESTAAN Config: Impliciete regel STA Config toe: Aanvullende informatie: Gevonden stroom met id 62, gebruikt de huidige fase van de stroom: 4 Type: ACCESS-LIST Subtype: log Resultaat: STA Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.0 regel-id 268434450 event-log beide access-list CSM_FW_ACL_remark regel-id 268434450: PREFILTER_Policy1 regel-id 268434450: REGEL: Fastpath_dst_192.168.75.0/24 Aanvullende informatie: Fase: 5 Type: CONN-SETTINGS Subtype: Resultaat: STA Config: class-map class-default match om het even welke policy-map global_policy global Aanvullende informatie: Fase: 6 Type: NAT Subtype: per-sessie Resultaat: STA Config: Extra informatie: Fase: 7 Type: IP-OPTIONS Subtype: Resultaat: STA Config: Extra informatie: 8 Type: ROUTE-LOOKUP Subtype: Resultaat van de interface: STA Config toe: Extra Informatie: gevonden volgende-hop 192.168.75.39 gebruikt uitgaande ifc binnen Fase: 9 Type: ADJACENCY-LOOKUP Subtype: volgende-hop en nabijheid Resultaat: STA Config toe: Aanvullende informatie: nabijheid Actief volgende-hop mac adres c84c.758d.4981 hits 140376711128802 Fase: 10 Type: CAPTURE Subtype: Resultaat: STA Config: Extra informatie: MAC Access list Resultaat: input-interface: input-line status: input-line status:: omhoog output-interface: binnen output-status: omhoog output-lijn-status: omhoog Actie: toestaan

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De verificatie is toegelicht in de respectieve taakonderdelen.

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

• Alle versies van de Cisco Firepower Management Center-configuratiehandleiding vindt u hier:

Navigatie in de documentatie voor Cisco Secure Firewall Threat Defence

• Cisco Global Technical Assistance Center (TAC) raadt deze visuele gids ten zeerste aan voor diepgaande praktische kennis over Cisco Firepower Security Technologies van de volgende generatie, die de in dit artikel genoemde technologieën omvat:

Cisco Firepower Threat Defence (FTD)

• TechNotes voor alle configuratie en probleemoplossing:

Cisco Secure Firewall Management Center

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

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.