Configurare il framework di criteri modulare di Firewall Threat Defense

Sommario

Introduzione

Questo documento descrive il framework di criteri modulari (MPF) Firewall Threat Defense (FTD)

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall 3130 Threat Defense versione 10.0.0 (build 140)
- Firewall Management Center (FMC) versione 10.0.0 (build 140)

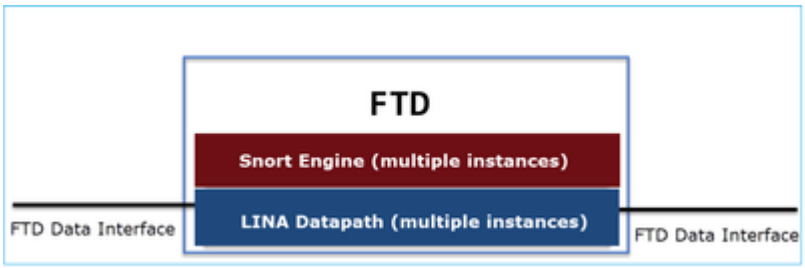
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Panoramica sul piano dati FTD

FTD è un'immagine software unificata costituita da 2 motori principali:

- Datapath (noto anche come LINA)
- Motore Snort



Il datapath LINA e il motore Snort sono le parti principali del piano dati del FTD.

Componenti MPF

MPF utilizza i seguenti componenti:

- class-map corrisponde al traffico interessante.
- policy-map applica azioni al traffico interessante corrispondente alla class-map.
- service-policy applica la mappa dei criteri a livello globale (su tutte le interfacce) o su un'interfaccia specifica.

Direzionalità delle feature

Per quanto riguarda la direzionalità delle funzionalità, consultare la guida alla configurazione dell'ASA:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa924/configuration/firewall/asa-924-firewall-config/inspect-service-policy.html

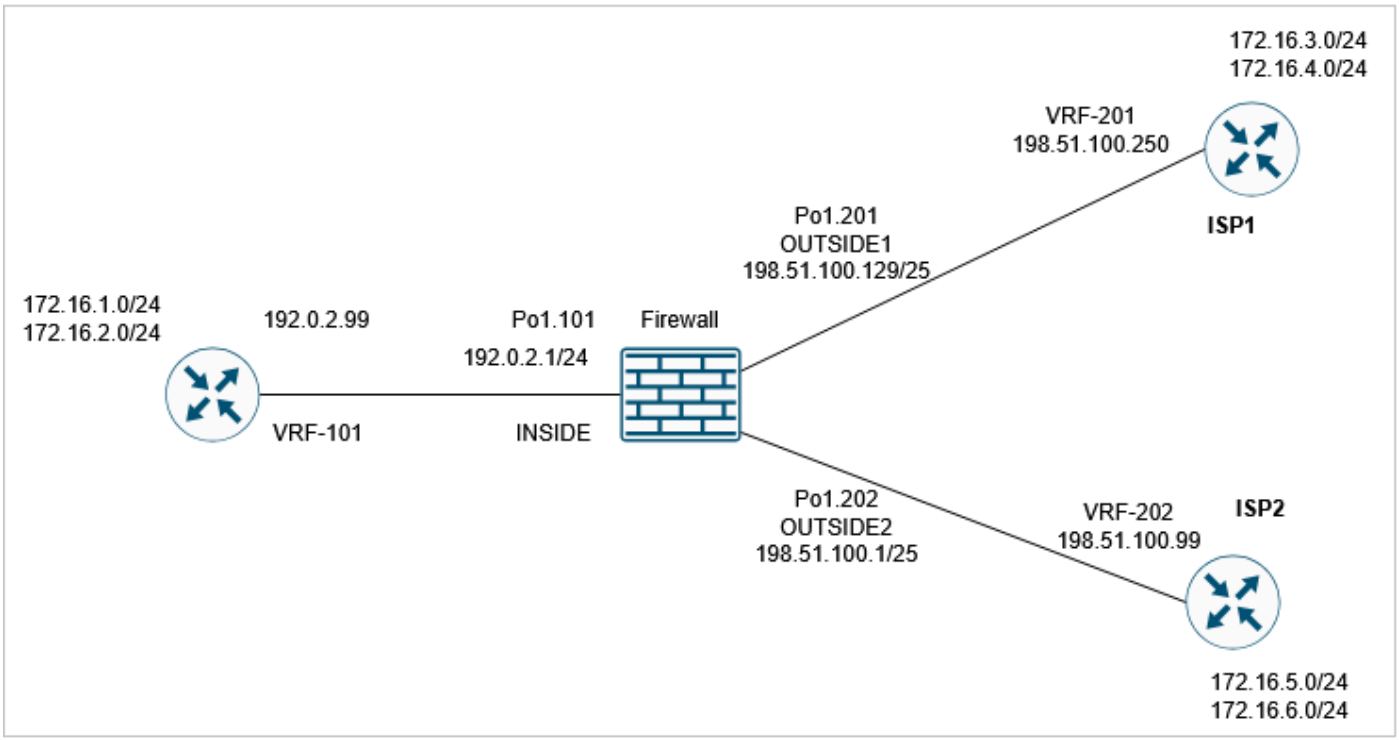
Le funzioni relative all'FTD sono evidenziate:

Table 2. Feature Directionality

Feature	Single Interface Direction	Global Direction
Application inspection (multiple types)	Bidirectional	Ingress
NetFlow Secure Event Logging filtering	N/A	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS standard priority queue	Egress	Egress
TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
TCP normalization	Bidirectional	Ingress
TCP state bypass	Bidirectional	Ingress
User statistics for Identity Firewall	Bidirectional	Ingress

Configurazione

Topologia



La configurazione predefinita di MPF (10.0.0):

<#root>

```
firewall#

show run policy-map

!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
```

```
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP

firewall#
```

show run class-map

```
!
class-map inspection_default
 match default-inspection-traffic
class-map class_snmp
 match port udp eq 4161
!
firewall#
```

show run service-policy

```
service-policy global_policy global
```

Attività 1. Disabilitazione globale dell'ispezione SIP su FTD

Il requisito di questa attività è disabilitare l'ispezione SIP nel motore LINA FTD. Uno dei motivi può essere un requisito politico o un problema software relativo al SIP che influisce sul traffico di transito.

Soluzione

Prima di disabilitare l'ispezione SIP, confermare che sia applicata al traffico di transito:

<#root>

```
firewall#
```

packet-tracer input INSIDE udp 172.16.1.1 5060 172.16.3.1 5060

```
...
Phase: 8
```

Type: INSPECT

Subtype: inspect-sip

Result: ALLOW

Elapsed time: 34788 ns
Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

inspect sip

service-policy global_policy global

Additional Information:
...
Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up

Action: allow

Time Taken: 326018 ns

Esistono due modi per disabilitare l'ispezione SIP a livello globale:

Soluzione 1: Disabilita SIP da CLI FTD CLISH

<#root>

>

configure inspection sip disable

Building configuration...
Cryptochecksum: ef7528dc 7338986d 6714a3a2 4770528e

7818 bytes copied in 0.250 secs
[OK]

Verifica

<#root>

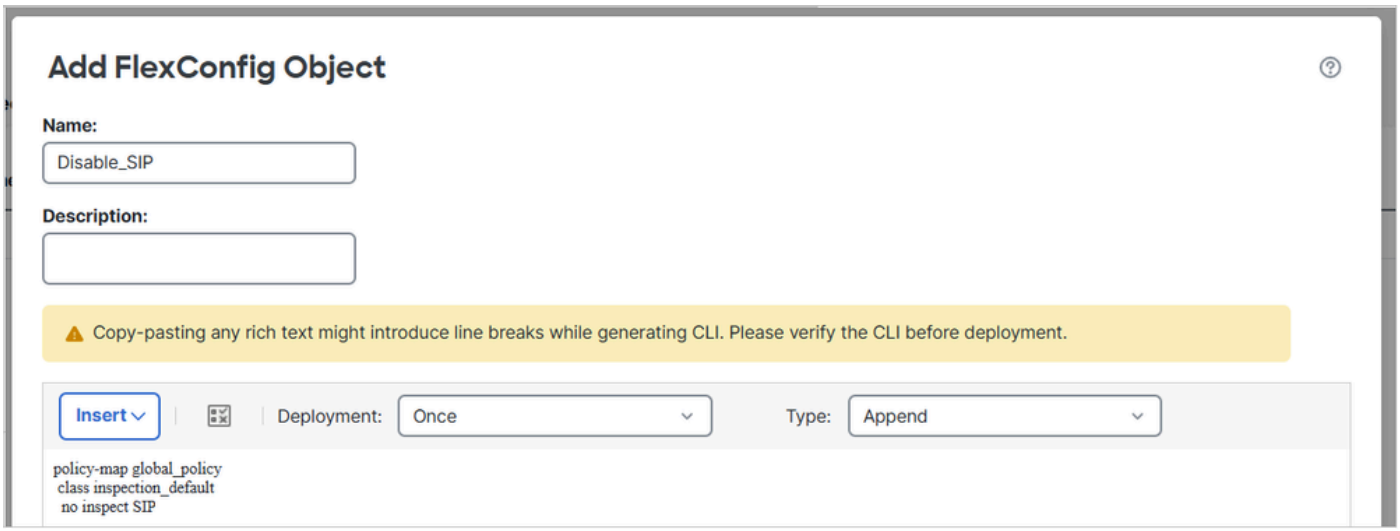
>

show running-config policy-map | include sip

>

Soluzione 2: Disabilita SIP tramite FlexConfig

In FMC selezionare Devices > FlexConfig e creare un oggetto FlexConfig:




```
policy-map global_policy
 class inspection_default
  no inspect sip
```

Applica Usare il criterio FlexConfig e selezionare Preview Config per visualizzarlo in anteprima:

Infine, distribuire il criterio.

Verifica

<#root>

```
firewall#
```

```
show run policy-map | include sip

firewall#
```

Nota: è necessario cancellare la connessione SIP esistente dalla tabella delle connessioni LINA in modo che le connessioni vengano ristabilite senza ispezione SIP. È possibile utilizzare questo comando per verificare le connessioni SIP esistenti:

```
<#root>

firewall#

show conn port 5060
```

Attività 2. Disabilitazione dell'ispezione SIP per host specifici

Per questo task è necessario disabilitare l'ispezione SIP per il traffico tra queste reti:

- SRC: 172.16.1.0/24
- DST 172.16.3.0/24

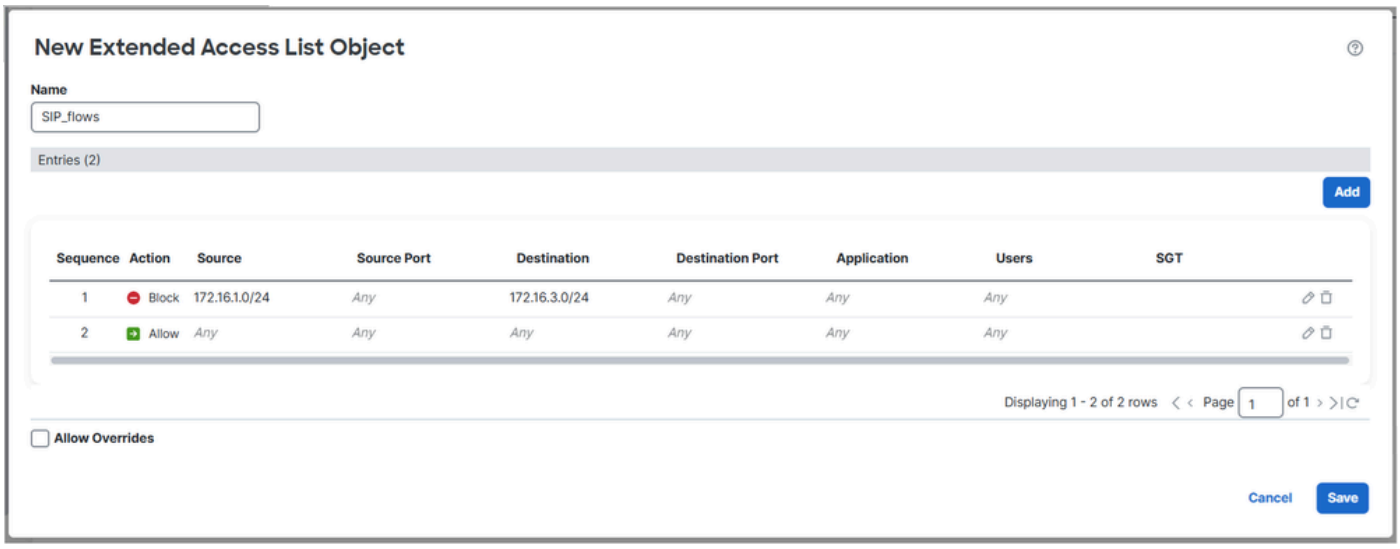
Una delle cause può essere un problema software relativo al SIP che influisce sul traffico di transito

Soluzione

Utilizzare FlexConfig.

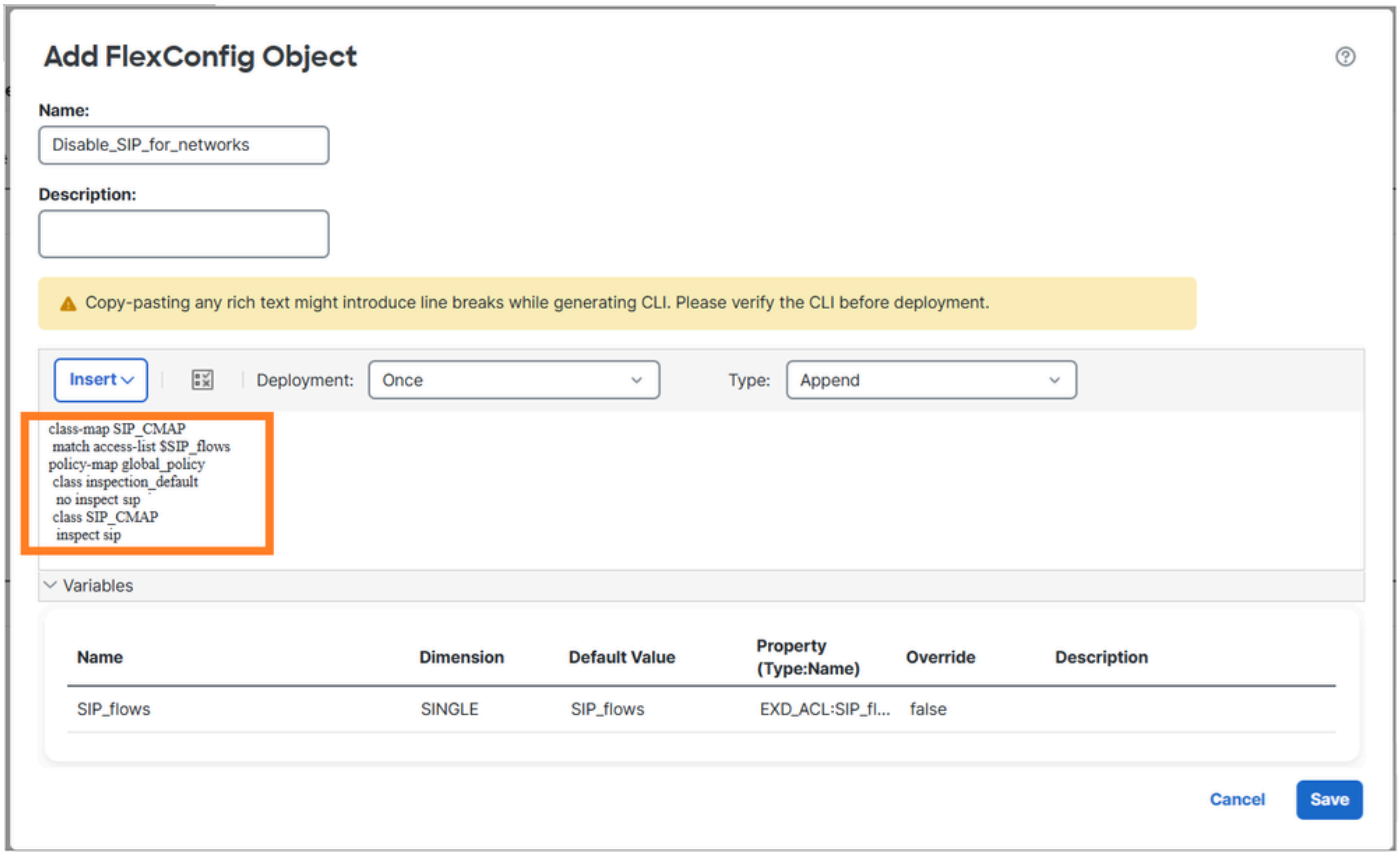
Passaggio 1

Selezionare Oggetti > Elenco accessi > Estesi e creare un elenco degli accessi esteso che corrisponda al traffico interessato. È necessario utilizzare l'azione Blocca poiché l'obiettivo è escludere il traffico specifico. Inoltre, aggiungere una regola Allow (Consenti) per far corrispondere il resto del traffico:



Passaggio 2

Creare un oggetto FlexConfig con una mappa delle classi corrispondente all'elenco di controllo di accesso (ACL) SIP e applicarlo a global_policy:



L'oggetto FlexConfig configurato:

```
class-map SIP_CMAP
 match access-list $SIP_flows
```

```
policy-map global_policy
 class inspection_default
  no inspect sip
 class SIP_CMAP
  inspect sip
```

Nota

Quando si configura l'ACL di autorizzazione, cercare di essere il più possibile specifico (ad esempio, inserire le porte del protocollo) per evitare qualsiasi potenziale impatto sulla CPU. L'esempio di questa attività non specifica le porte di protocollo e può essere evitato in fase di produzione.

Verifica 1

<#root>

```
firewall#
```

show run policy-map | begin global

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
```

class SIP_CMAP

inspect sip

```
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

```
firewall#
```

show run class-map

```
!
```

class-map SIP_CMAP

match access-list SIP_flows

```
class-map inspection_default
 match default-inspection-traffic
class-map class_snmp
 match port udp eq 4161
firewall#
```

show run access-list SIP_flows

```
access-list SIP_flows extended deny ip 172.16.1.0 255.255.255.0 172.16.3.0 255.255.255.0
access-list SIP_flows extended permit ip any any
```

Verifica 2

Il traffico non ispezionato tramite ispezione SIP ha deny=true:

<#root>

```
firewall#
```

packet-tracer input INSIDE udp 172.16.1.1 5060 172.16.3.1 5060 detail | begin INSPECT

Type: INSPECT

Subtype: inspect-sip

```
Result: ALLOW
Elapsed time: 37910 ns
Config:
```

```
class-map SIP_CMAP


 match access-list SIP_flows


policy-map global_policy


 class SIP_CMAP


  inspect sip


service-policy global_policy global


Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x14af42cfa810, priority=70, domain=inspect-sip,

deny=true




hits=1

, user_data=0x000014af4570bea0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0


      src ip/id=172.16.1.0, mask=255.255.255.0, port=0, tag=any




      dst ip/id=172.16.3.0, mask=255.255.255.0, port=0, tag=any,


       dscp=0x0, input_ifc=INSIDE(vrfid:0), output_ifc=any
...
```

Il traffico ispezionato tramite ispezione SIP ha deny=false:

<#root>

```
firewall#

packet-tracer input INSIDE udp 172.16.2.1 5060 172.16.3.1 5060 detail | begin INSPECT



Type: INSPECT



Subtype: inspect-sip


Result: ALLOW
Elapsed time: 34788 ns
Config:
class-map SIP_CMAP
 match access-list SIP_flows
policy-map global_policy
 class SIP_CMAP
  inspect sip
service-policy global_policy global
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x14af459099d0, priority=70, domain=inspect-sip,

deny=false


       hits=1, user_data=0x000014af4570bea0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
       src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
       dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any,
...
```

Verifica 3

Il contatore di ispezione "sip" aumenta quando un pacchetto viene ispezionato dal firewall:

<#root>

```
firewall#

show service-policy inspect sip



Global policy:
  Service-policy: global_policy
```

```
    Class-map: inspection_default
    Class-map: class_snmp
    Class-map: SIP_CMAP
      Inspect: sip ,

packet 2

, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
...
firewall#

packet-tracer input INSIDE udp 172.16.2.1 5060 172.16.3.1 5060



firewall#

show service-policy inspect sip



Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: class_snmp
    Class-map: SIP_CMAP
      Inspect: sip ,

packet 3

, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0



...
```

Attività 3. Configurazione del bypass dello stato TCP per host specifici

Per questa attività, è necessario abilitare il bypass dello stato TCP per il traffico tra queste reti:

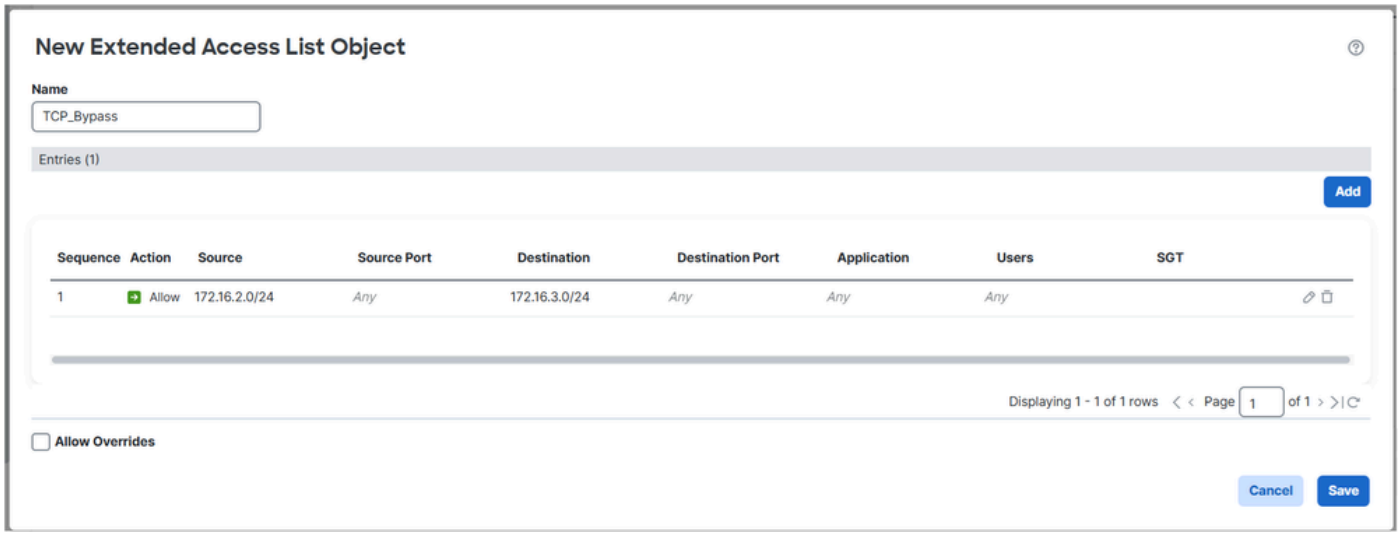
- SRC: 172.16.2.0/24
- DST 172.16.3.0/24

In generale, non è consigliabile utilizzare il bypass dello stato TCP, ma è possibile utilizzarlo come soluzione temporanea per la gestione dei flussi asimmetrici.

Soluzione 1

Passaggio 1

Creare un ACL esteso che corrisponda al traffico interessante:

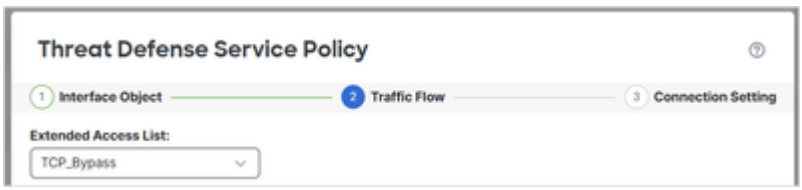


Passaggio 2

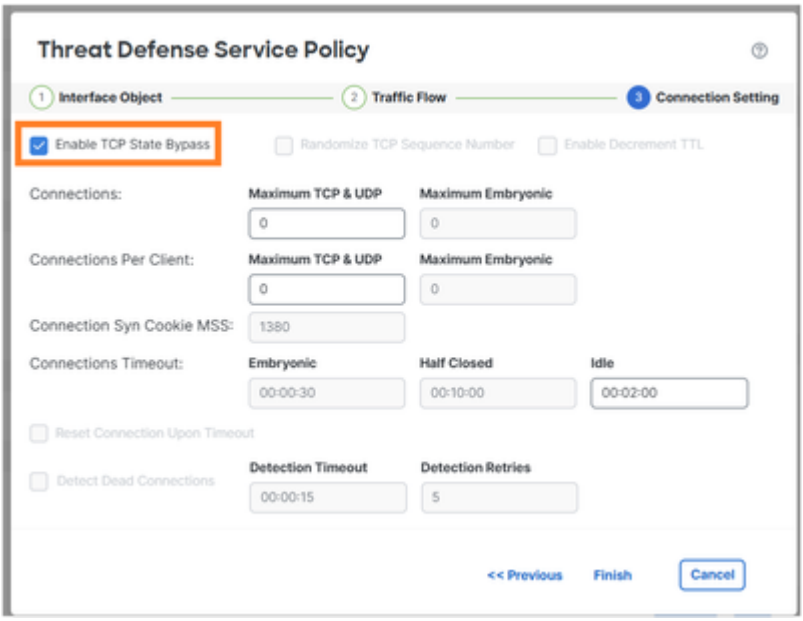
Modificare i criteri di controllo di accesso (ACP) assegnati all'FTD, selezionare la scheda Impostazioni avanzate e modificare i criteri del servizio di difesa delle minacce. Selezionare Aggiungi regola e Avanti.

Passaggio 3

Selezionare l'ACL esteso:



Passaggio 4



Passaggio 5

Selezionare Fine, OK, Salva e Distribuisci.

Il risultato:

<#root>

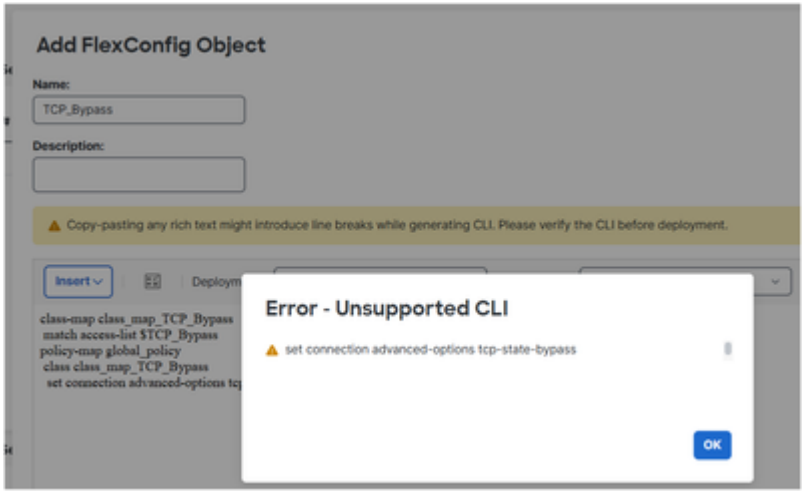
```
firewall#

show run policy-map global_policy


!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP

 class class_map_TCP_Bypass
```

```
  set connection random-sequence-number disable
```

```
  set connection advanced-options tcp-state-bypass
```

```
class class_snmp
 inspect snmp
class class-default
 set connection advanced-options UM_STATIC_TCP_MAP
```

Nota: Nelle versioni precedenti di FMC, ad esempio 6.x, è possibile utilizzare FlexConfig per configurare il bypass dello stato TCP. Nelle versioni più recenti questo non è supportato:



Verifica

<#root>

```
firewall#
```

```
packet-tracer input INSIDE tcp 172.16.2.1 1111 172.16.3.1 80 detail | begin CONN
```

```
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 334 ns
Config:
```

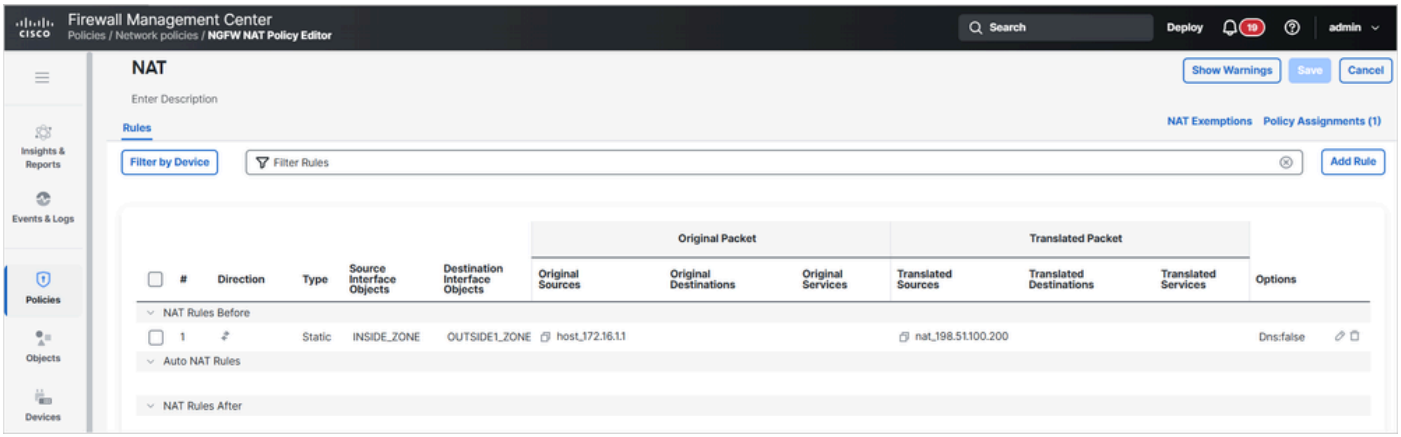
```
class-map class_map_TCP_Bypass
```

```
 match access-list TCP_Bypass


policy-map global_policy


 class class_map_TCP_Bypass


  set connection conn-max 0 embryonic-conn-max 0 random-sequence-number disable syn-cookie-mss 1380


  set connection advanced-options tcp-state-bypass


service-policy global_policy global
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x14af45906b70, priority=7, domain=conn-set, deny=false


hits=1

, user_data=0x000014af45906df0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

       src ip/id=172.16.2.0, mask=255.255.255.0, port=0, tag=any



       dst ip/id=172.16.3.0, mask=255.255.255.0, port=0, tag=any,


       dscp=0x0, input_ifc=INSIDE(vrfid:0), output_ifc=any
...
```

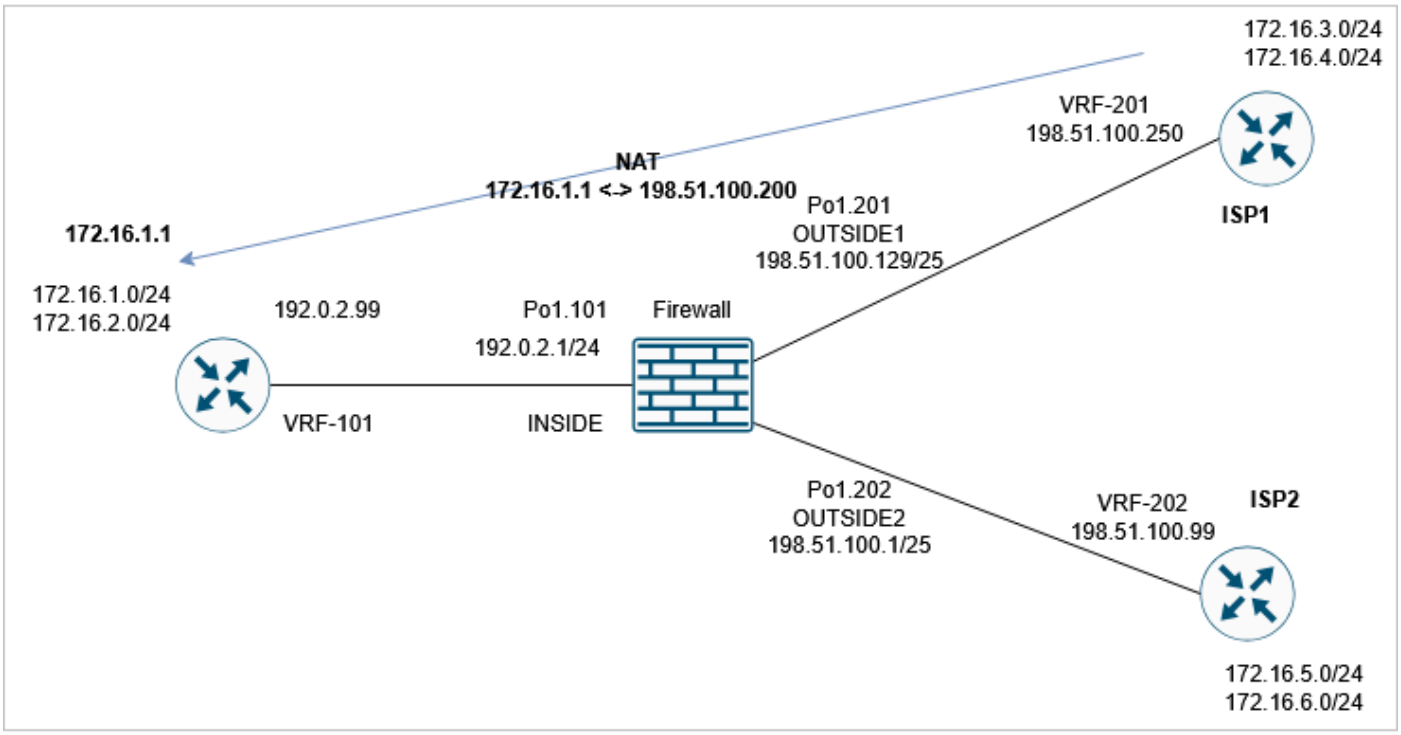
Attività 4. Modifica dell'output di Traceroute

Prerequisito

Configurare il protocollo NAT statico sull'FTD in modo che il protocollo IP 172.16.1.1 situato dietro l'interfaccia INSIDE venga visualizzato come 198.51.100.200 sugli host OUTSIDE1:



Quindi, eseguire un traceroute da ISP1 a 198.51.100.200 (host 172.16.1.1):



<#root>

```
router1#
```

`traceroute vrf VRF-201 198.51.100.200`

```
Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)
```

```
  1 192.0.2.99 1 msec 1 msec *
```

Requisito

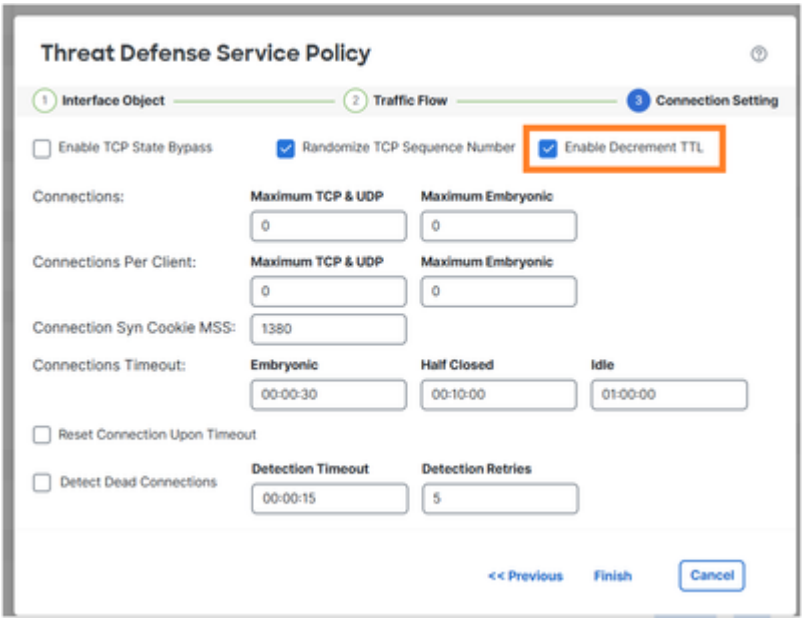
Modificare la configurazione FTD in modo che il traceroute corrisponda a questo output:

<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

  1 198.51.100.129 1 msec 1 msec *



  2 198.51.100.200 1 msec 2 msec *
```

Soluzione

La soluzione include due passaggi di configurazione:
1. Diminuire il valore TTL:

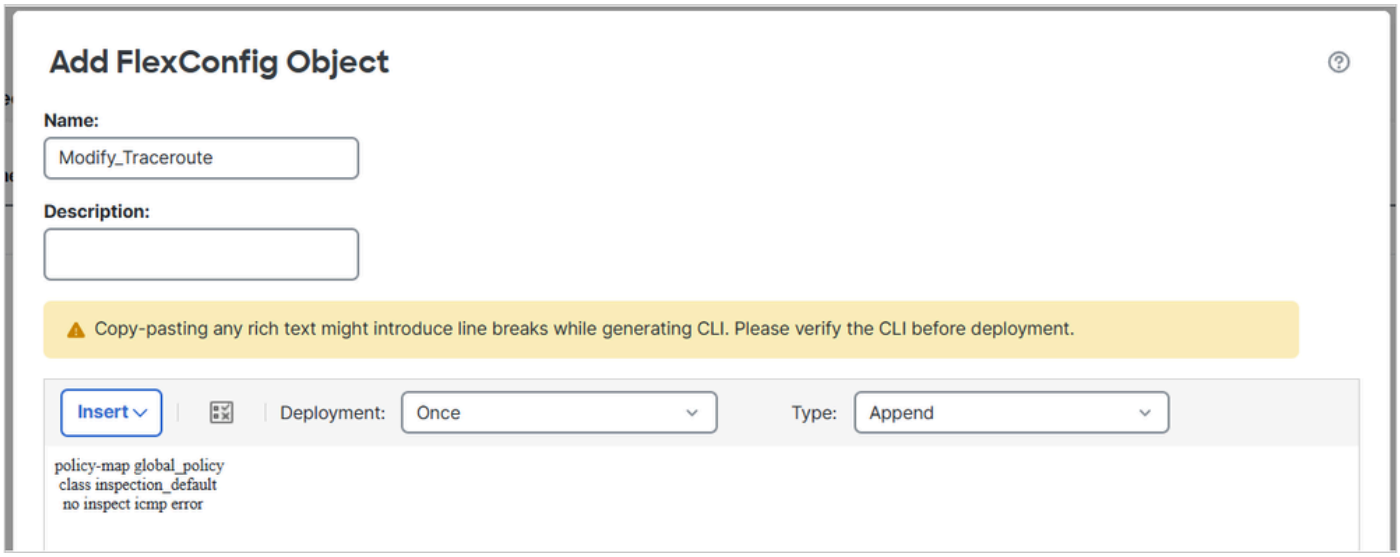


Dopo questa modifica, il traceroute rivela l'hop del firewall:

<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

 1 198.51.100.129 1 msec 1 msec *


  2 192.0.2.99 1 msec 1 msec *
```

2. Disabilitare l'ispezione degli errori ICMP:




```
policy-map global_policy
 class inspection_default
   no inspect icmp error
```

Verifica

Il traceroute mostra l'indirizzo IP NAT convertito dell'host remoto e l'indirizzo IP dell'interfaccia FTD:

<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

  1 198.51.100.129 1 msec 1 msec *



  2 198.51.100.200 1 msec 2 msec *
```

Attività 5. Impostazione dei timeout di connessione

Requisito

Modificare il timeout su 1 settimana per questo flusso:

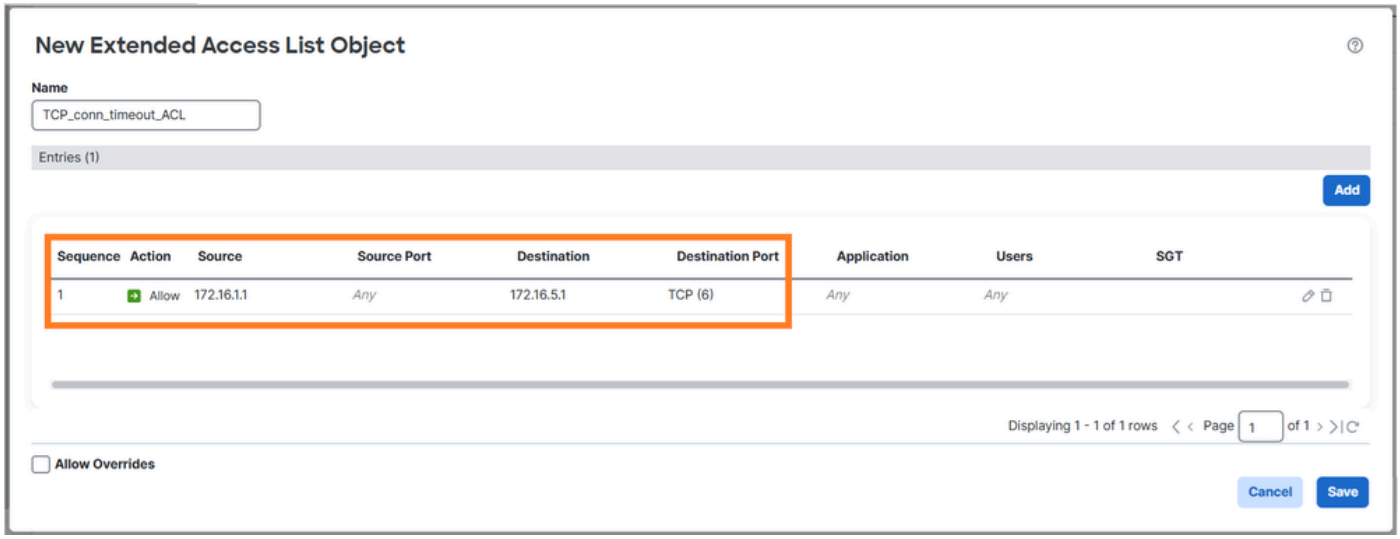
- Protocollo: TCP
- SRC: 172.16.1.1
- DST 172.16.5.1

Soluzione

Per impostare il timeout per flusso, è necessario utilizzare i criteri del servizio.

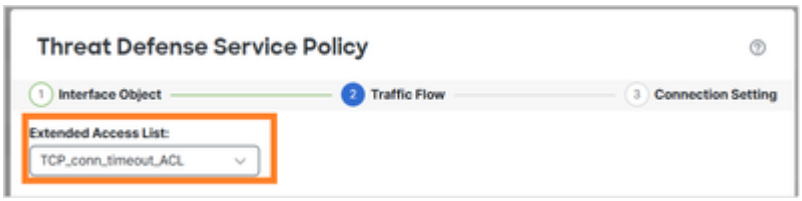
Passaggio 1

Selezionare Oggetti > Elenco accessi e creare un ACL esteso che corrisponda al traffico interessato:

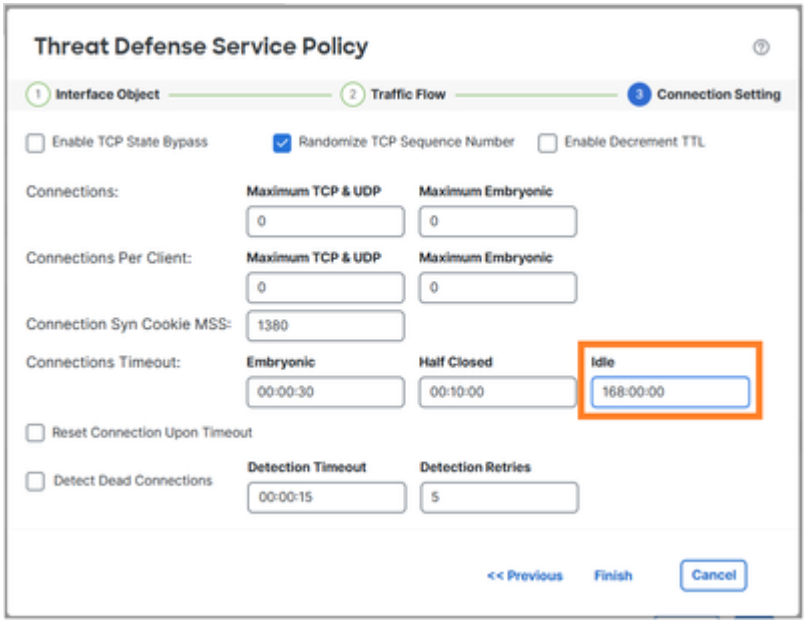


Passaggio 2

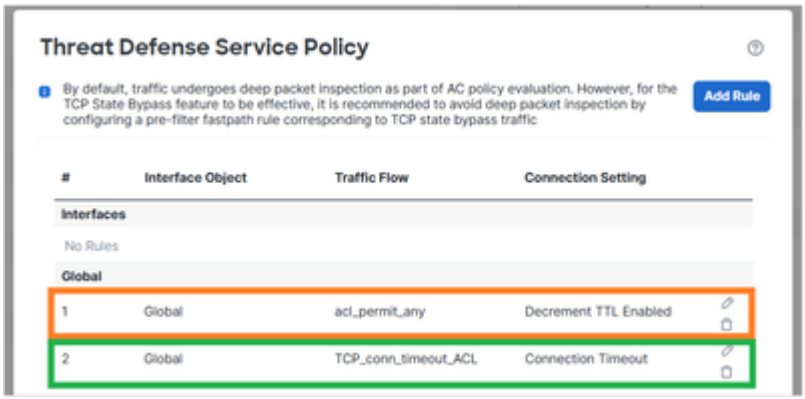
Configurare un criterio MPF che utilizza l'ACL creato nel passaggio 1:



Impostare il timeout di inattività della connessione:



Rimuovere la regola dall'attività precedente poiché si sovrappone al nuovo requisito:



Verifica

La configurazione della mappa dei criteri distribuita:

<#root>

```
policy-map global_policy
 class inspection_default
```

```
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
  inspect icmp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
  inspect sip

 class class_map_TCP_conn_timeout_ACL




  set connection timeout idle 168:00:00



 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

Avviare una nuova connessione TCP da 172.16.1.1 a 172.16.5.1 e controllare la tabella di connessione dell'FTD:

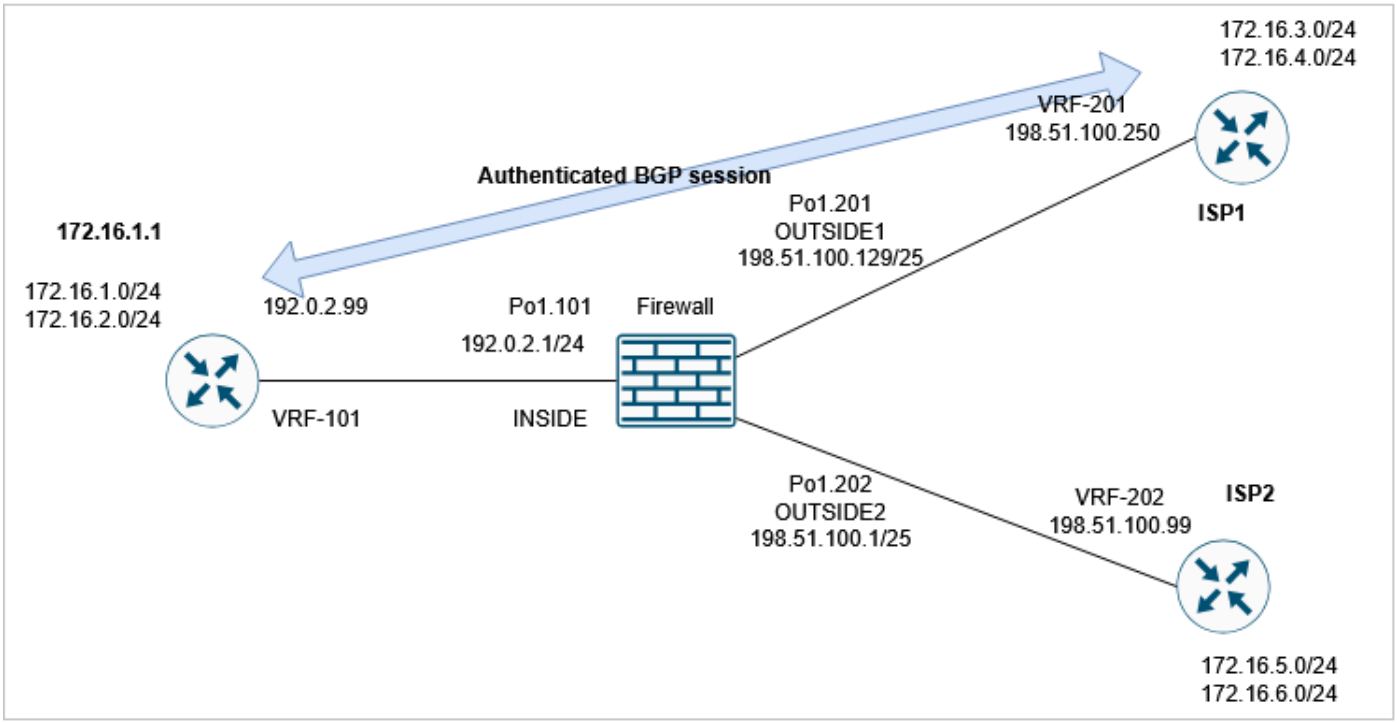
<#root>

```
firewall#

show conn long address 172.16.5.1



...
TCP OUTSIDE2: 172.16.5.1/23 (172.16.5.1/23) INSIDE: 172.16.1.1/29389 (172.16.1.1/29389), flags UIoN1N7,

timeout 7D0h


, bytes 349, flow id 72, Snort id 6, rule id 268439559, Rx-RingNum 27, Internal-Data0/1
Initiator: 172.16.1.1, Responder: 172.16.5.1
Connection lookup keyid: 890
```

Task 6. Autenticazione BGP tramite FTD

Prerequisito

Configurare una sessione BGP tramite FTD. La sessione BGP deve utilizzare l'autenticazione.



Verifica

Con la configurazione FTD predefinita, la sessione BGP non viene stabilita. Sul router è possibile visualizzare:

<#root>

```
router1#
*May 21 07:51:23.595:

%TCP-6-BADAUTH: Invalid MD5 digest

 from 192.0.2.99(24591) to 198.51.100.250(179) tableid - 3
*May 21 07:51:25.595: %TCP-6-BADAUTH: Invalid MD5 digest from 192.0.2.99(24591) to 198.51.100.250(179)
*May 21 07:51:29.595: %TCP-6-BADAUTH: Invalid MD5 digest from 192.0.2.99(24591) to 198.51.100.250(179)
```

Sull'FTD è possibile notare che entrambi i lati non riescono a stabilire la connessione TCP BGP (i flag di connessione indicano che vengono ricevuti solo i pacchetti TCP SYN):

<#root>

```
firewall#

show conn port 179


3 in use, 16 most used
Inspect Snort:
        preserve-connection: 2 enabled, 0 in effect, 15 most enabled, 0 most in effect

TCP OUTSIDE1 198.51.100.250:41090 INSIDE 192.0.2.99:179, idle 0:00:00, bytes 0,

flags aA N1


TCP OUTSIDE1 198.51.100.250:179 INSIDE 192.0.2.99:53629, idle 0:00:02, bytes 0,

flags aA N1
```

Soluzione

Per consentire una sessione BGP autenticata tramite FTD, è necessario che siano soddisfatte le seguenti due condizioni:

1. TCP MD5 (opzione 19) deve essere consentito tramite FTD.
2. È necessario disabilitare l'assegnazione casuale dei numeri di sequenza TCP.

L'opzione TCP MD5 è consentita per impostazione predefinita:

9.6(2)	Default handling of the named options was changed to allow a packet if it contains a single option of a given type, and drop the packet if there are more than one option of that type. Also, the **md5**, **mss**, **allow multiple**, and **mss maximum** keywords were added. The default for the MD5 option was changed from clear to allow.

<#root>

```
firewall#

show run all tcp-map


!
tcp-map UM_STATIC_TCP_MAP
  no check-retransmission
```

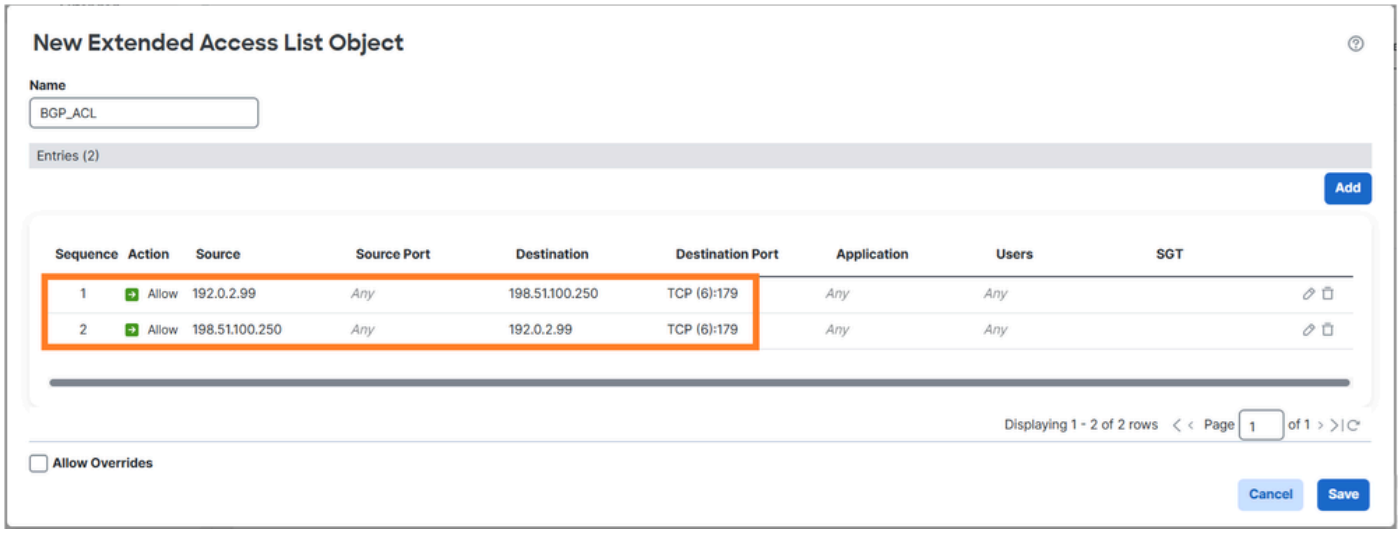
```
  no checksum-verification
  exceed-mss allow
  queue-limit 0 timeout 4
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options mss allow

  tcp-options md5 allow


  ttl-evasion-protection
  urgent-flag allow
  window-variation allow-connection
```

Disabilita in modo globale l'assegnazione casuale del numero di sequenza iniziale TCP (ISDN):

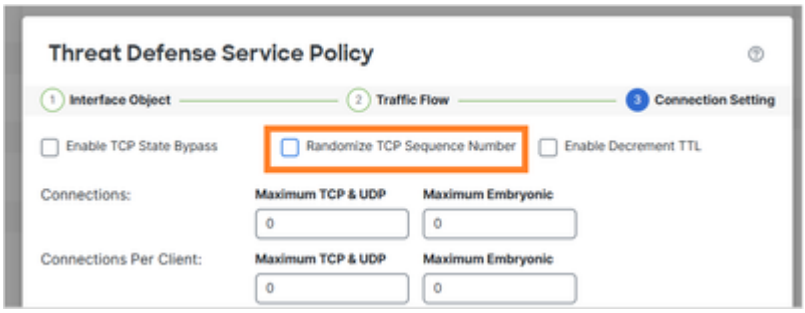
<#root>

```
>

configure tcp-randomization disable


Building configuration...
Cryptochecksum: f8ac5587 7ccc635e bff886a1 bcab820c

8284 bytes copied in 0.260 secs
[OK]
>
```

oppure (metodo preferito) creare un elenco degli accessi esteso che corrisponda alla connessione BGP:



e disabilitare l'assegnazione casuale del numero di sequenza TCP utilizzando i criteri del servizio Threat Defense:



Verifica

La configurazione della mappa dei criteri distribuita:

<#root>

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
```

```
  inspect icmp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
  inspect sip

 class class_map_BGP_ACL



  set connection random-sequence-number disable


 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

La sessione BGP viene stabilita tramite FTD:

<#root>

```
firewall#

show conn long port 179


...

TCP OUTSIDE1: 198.51.100.250/49863 (198.51.100.250/49863) INSIDE: 192.0.2.99/179 (192.0.2.99/179), flags

, idle 44s, uptime 1m40s, timeout 1h0m, bytes 274, flow id 111, Snort id 3, rule id 268439559, Rx-RingN


Initiator: 198.51.100.250, Responder: 192.0.2.99


  Connection lookup keyid: 83487134
```

Suggerimento: È possibile configurare una regola fastpath del prefiltro per il traffico BGP per evitare l'ispezione Snort.

Attività 7. Rilevamento connessioni inattive (DCD)

Requisito

Configurare DCD su FTD per il traffico TCP destinato all'host 172.16.3.1.

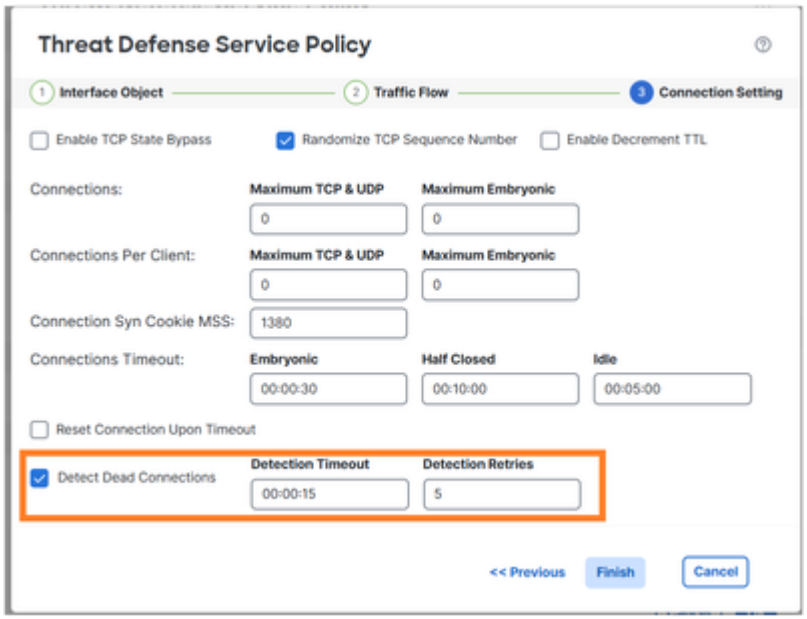
Soluzione

DCD è documentato all'indirizzo:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/advanced-access-service-policies.html#id_71048

1. Passare a Oggetti > Elenco accessi e creare un elenco degli accessi che corrisponda al traffico interessato.

2. Modificare il punto ACP assegnato al firewall, passare alle opzioni avanzate e selezionare Criteri servizio di difesa dalle minacce per abilitare DCD:



La configurazione distribuita:

```
access-list DCD_ACL extended permit object-group ProxySG_ExtendedACL_81604390279 any host 172.16.3.1
!
class-map class_map_DCD_ACL
 match access-list DCD_ACL
policy-map global_policy
 class class_map_DCD_ACL
  set connection timeout dcd
```

Come funziona

Configurare le acquisizioni FTD per visualizzare l'operazione back-end:

```
<#root>
firewall#
capture CAPI interface INSIDE match tcp host 172.16.3.1 any

firewall#
capture CAPO interface OUTSIDE1 match tcp host 172.16.3.1 any
```

Stabilire una connessione TCP attraverso il firewall:

```
<#root>
firewall#
show conn long address 172.16.3.1 | begin 172.16.3.1

TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7
idle 1m18s
, uptime 1m22s,
timeout 5m0s
, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Internal-Data0/1
  Initiator: 192.0.2.99, Responder: 172.16.3.1

  DCD probes sent: Initiator 0, Responder 0 Connection lookup keyid: 76292550
```

Inizialmente, nelle clip del firewall non sono visualizzati pacchetti DCD:

```
<#root>

firewall#

show capture


capture CAPI type raw-data interface INSIDE [

Capturing - 0 bytes


]
  match tcp host 172.16.3.1 any
capture CAPO type raw-data interface OUTSIDE1 [

Capturing - 0 bytes


]
  match tcp host 172.16.3.1 any
```

Quando una connessione inattiva raggiunge il timeout di inattività, l'FTD invia messaggi ACK TCP oggetto di spoofing all'origine e alla destinazione:

```
<#root>

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1


TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 4m59s


, uptime 5m3s, timeout 5m0s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Inte
  Initiator: 192.0.2.99, Responder: 172.16.3.1
  DCD probes sent: Initiator 0, Responder 0 Connection lookup keyid: 76292550

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1


TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 0s


, uptime 5m3s, timeout 15s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Inter
  Initiator: 192.0.2.99, Responder: 172.16.3.1
```

DCD probes sent: Initiator 1

, Responder 0 Connection lookup keyid: 76292550

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1

TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7
  Initiator: 192.0.2.99, Responder: 172.16.3.1

DCD probes sent: Initiator 1, Responder 1

Connection lookup keyid: 76292550

Se entrambi rispondono, il timer di inattività viene reimpostato:

<#root>

firewall#

show capture CAPI

3 packets captured

1: 09:01:30.433952 802.1Q vlan#101 P0 172.16.3.1.23 > 192.0.2.99.23241: . ack 3271882019 win 32757
2: 09:01:30.434334 802.1Q vlan#101 P0

192.0.2.99.23241 > 172.16.3.1.23: . ack 1746306341 win 32746

3: 09:01:30.955654 802.1Q vlan#101 P0 172.16.3.1.23 > 192.0.2.99.23241: . ack 3271882019 win 32757
3 packets shown
firewall#

show capture CAPO

3 packets captured

1: 09:01:30.434364 802.1Q vlan#201 P0 192.0.2.99.23241 > 172.16.3.1.23: . ack 111661490 win 32746
2: 09:01:30.955288 802.1Q vlan#201 P0 192.0.2.99.23241 > 172.16.3.1.23: . ack 111661490 win 32746
3: 09:01:30.955639 802.1Q vlan#201 P0

172.16.3.1.23 > 192.0.2.99.23241: . ack 3875469573 win 32757

```
3 packets shown

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1


TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 1m29s


, uptime 6m33s, timeout 5m0s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Int
  Initiator: 192.0.2.99, Responder: 172.16.3.1
  DCD probes sent: Initiator 1, Responder 1 Connection lookup keyid: 76292550
```

Nota: DCD non funziona con le connessioni scaricate (flag "o").

Informazioni correlate

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/advanced-access-service-policies.html#id_71048

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).