Probleemoplossing voor verkeersdruppels als gevolg van LINA Protocol Inspection op FTD

Inhoud

Inleiding

Dit document beschrijft hoe u kunt identificeren als de LINA-protocolinspectie voor Modular Policy Framework (MPF), verkeer laat vallen in Cisco Secure FTD.

Voorwaarden

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Cisco Secure Firewall Threat Defence (FTD).
- Cisco Secure Firewall Manager Center (FMC).

Gebruikte componenten

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

- Virtual Cisco Secure Firewall Threat Defence (FTD), versie 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), versie 7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een uitgeschakelde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De inspectiemotoren zijn vereist in een firewall voor diensten die IP-adresseringsinformatie insluiten in het gebruikerspakket of secundaire kanalen openen op dynamisch toegewezen poorten.

De protocolinspectie kan helpen voorkomen dat kwaadaardig verkeer het netwerk binnenkomt door de inhoud van netwerkpakketten te inspecteren en verkeer te blokkeren of aan te passen op basis van de toepassing of het protocol dat wordt gebruikt.
Hierdoor kunnen inspectiemotoren de totale doorvoersnelheid beïnvloeden. Verschillende veelgebruikte inspectiemotoren zijn standaard ingeschakeld op de firewall, het kan nodig zijn om anderen in te schakelen, afhankelijk van het netwerk.

Standaardconfiguraties

Standaard bevat de FTD LINA-configuratie een beleid dat overeenkomt met al het standaardverkeer voor toepassingsinspectie.

De inspectie geldt voor het verkeer op alle interfaces (een globaal beleid).

Het standaard verkeer van de toepassingsinspectie omvat verkeer aan de standaardhavens voor elk protocol. U kunt slechts één globaal beleid toepassen, dus als u het globale beleid wilt wijzigen, bijvoorbeeld, om inspectie toe te passen op niet-standaard poorten, of om inspecties toe te voegen die niet standaard zijn ingeschakeld, moet u het standaardbeleid bewerken of uitschakelen en een nieuw beleid toepassen.

Laat de opdracht tonen in werking stellen-Config beleid-kaart op LINA, FTD Command Line Interface (CLI) via systeemondersteuning diagnostic-client, om de informatie te krijgen.

```
firepower# show running-config 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
!
```

Identificeer pakketdruppels als gevolg van de MPF-protocolinspectie

Zelfs wanneer het verkeer zich aanpast aan het toegangscontrolebeleid (ACS) dat aan de firewall is toegewezen, worden in bepaalde scenario's de verbindingen beëindigd door specifiek verkeersgedrag dat door de firewall wordt ontvangen, een niet-ondersteund ontwerp, toepassingsnorm of een inspectiebeperking.

Tijdens het oplossen van verkeersproblemen is een handig proces:

- Vastgestelde real-time opnamelogboeken op de interfaces waarvan het verkeer stroomt (in- en uitgangen), opdracht:

```
firepower# capture

        [interface

        ][match

           [port

           ]
```

```
        [port

        ]]
```

Met behulp van de Captures kunt u het optie pakketnummer X sporendetail opnemen en het moet de resultaatfase per fase van de verbinding leveren, zoals een packet-tracer opdracht doet, maar met deze optie zorgt u ervoor dat het real-time verkeer is.

```
firepower# show capture

        packet number X trace detail
```

- Set real-time Accelerated Security Path (ASP) Drop, het opnametype asp-drop toont de pakketten of verbindingen die door het ASP worden gelaten vallen, er is een lijst van redenen die u kunt vinden in de Gerelateerde koppelingen van het document, opdracht:

```
firepower# capture

        [type

        ] [interface
```

```
][match


   [port

   ]


     [port

     ]]
```

Protocolinspectiedruppels kunnen worden genegeerd, aangezien een toegestaan resultaat kan worden waargenomen in de pakkettraceerfasen. Dat is de reden dat het belangrijk is om altijd de reden van de val te verifiëren met behulp van real-time opnamelogboeken.

Veelvoorkomende drop-foutmeldingen

De daling Versnelde van de Veiligheid van de Weg (ASPIS) wordt vaak gebruikt voor het zuiveren doeleinden om het oplossen van netwerkkwesties te helpen. De show asp drop opdracht wordt gebruikt om deze gedropte pakketten of verbindingen te tonen, die inzichten geven in de redenen voor de druppels, die kwesties zoals NAT mislukkingen, inspectiemislukkingen, of toegangsregel ontkenningen kunnen omvatten.

Belangrijkste punten over ASP druppels:

- Frame Drops: Dit zijn druppels gerelateerd aan individuele pakketten, zoals ongeldige inkapseling of geen route naar host.
- Flow Drops: Deze zijn verwant met verbindingen, zoals stromen die door toegangsregels of

NAT mislukkingen worden ontkend.
- Gebruik: Het commando is primair voor debugging en de output kan veranderen.

Deze foutmeldingen of drop redenen zijn voorbeelden die u kunt tegenkomen tijdens het oplossen van problemen. Ze kunnen worden uitgesteld afhankelijk van het gebruikte Inspectie-protocol.

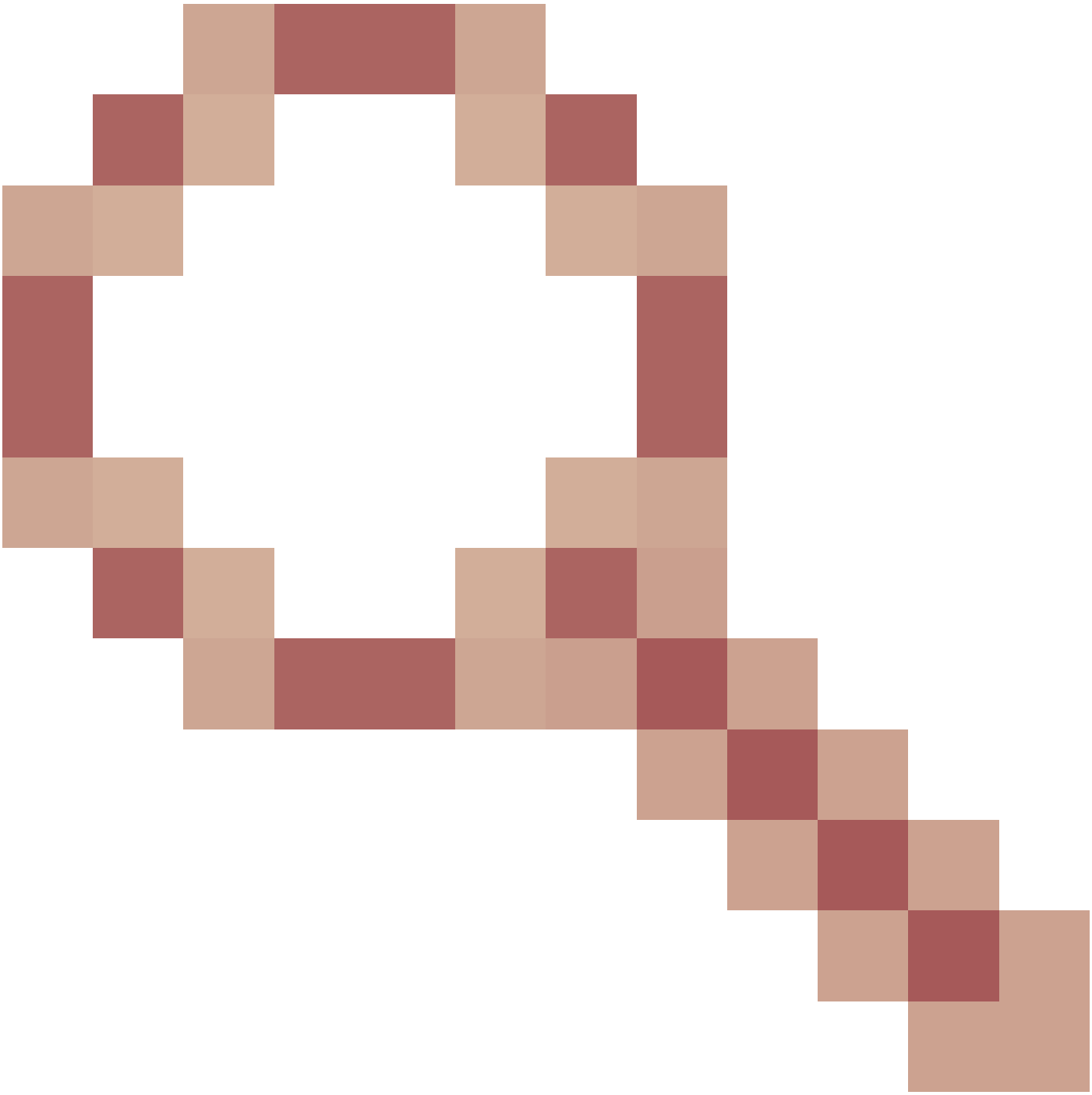
SUN RPC Inspection Drop Voorbeeld

Dit scenario is voor een single-arm proxy FTDv in AWS-implementatie, RPC-verkeer ingekapseld door Geneve, als de Sun Rpc-inspectie is ingeschakeld, wordt de verbinding verbroken.

De output toont ASP daalt voor Sun Rpc inspectie, Sun Rcp gebruik poort 111 als bestemming het laatste pakket is Geneve inkapselingspoort die 6081 als bestemming gebruiken. De reden voor het vallen in de output zoals je kunt zien is "Geen geldige nabijheid"

```
firepower# show capture asp-drop
...
8: 16:23:02.462958 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
9: 16:23:09.769338 10.0.0.5.780 > 172.16.0.3.111: P 1795131583:1795131679(96) ack 526534108 win 29200 D
10: 16:23:10.148658 172.16.0.3.111 > 10.0.0.5.780: . ack 4026726685 win 26880 Drop-reason: (no-adjacenc
11: 16:23:10.463004 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
12: 16:23:26.462729 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
13: 16:23:27.548692 10.79.67.11.60855 > 10.79.67.4.6081: udp 176 [GENEVE segment-id 0 payload-length 13
```

Cisco fout-id CSCwj00074



FTDv single-arm proxy verlaagt verkeer zonder nabijheid met inspect sunrpc ingeschakeld

Het verkeer wordt in de ASP van de LINA-engine als 'geen-geldige nabijheid' weggelaten omdat het mac-adres van de bron en de bestemming plotseling helemaal in nullen wordt ingevuld na het tweede pakket (SYN/ACK) van de 3-voudige handdruk.

ASP Drop reden:

Naam: geen nabijheid
Geen geldige nabijheid:
Deze teller stapelt op wanneer het security apparaat een pakket ontvangt op een bestaande stroom die niet langer een geldige uitvoernabijheid heeft. Dit kan voorkomen als de volgende hop

niet meer bereikbaar is of als een routeringsverandering typisch in een dynamisch routeringsmilieu is voorgekomen.

Oplossing: Schakel sunrpc-inspectie uit.

SQL*NET-inspectiedrop-voorbeeld

Dit scenario is voor een single-arm proxy FTDv in AWS-implementatie, als Sql*Nel-inspectie is ingeschakeld, wordt het ingekapselde verkeer door Geneve verwijderd.

De uitvoer is voor het pakket dat wordt samengevoegd (u kunt hetzelfde pakketnummer waarnemen):
Eerste regel: ASP-drop-pakketopname niet ingekapseld, Sql*Net gebruikt 1521-poort als bestemming.
Tweede regel: VNI interface asp-drop op LINA, Geneve gebruik inkapseling poort 6081 als bestemming.

Er zijn twee verschillende druppelredenen in de output, zoals je kunt zien zijn ze "tcp-buffer-timeout" en "tcp-not-syn"

```
95    2024-12-14 07:55:58.771764    172.16.0.14    10.0.8.2    TCP    251    53905 → 1521 [PSH, ACK] Seq=
95: 07:55:58.771764       10.7.0.3.64056 > 10.7.2.5.6081:  udp 209 [GENEVE segment-id 0 payload-length 169] Drop-

96    2024-12-14 07:55:58.771780    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53905 → 1521 [AC
96: 07:55:58.771780       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length 1432] Dro

99    2024-12-14 07:55:58.997049    172.16.0.14    10.0.8.2    TCP    308    53903 → 1521 [PSH, ACK] Seq=1 Ack=1
99: 07:55:58.997049       10.7.0.3.64056 > 10.7.2.5.6081:  udp 266 [GENEVE segment-id 0 payload-length 226] Drop-

100    2024-12-14 07:55:58.997079    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53903 → 1521 [A
100: 07:55:58.997079       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length 1432] Dr
```

ASP Drop reden:

Naam: TCP-buffer-time-out
Time-out van TCP-out-of-order pakketbuffer:
Deze teller wordt verhoogd en het pakket wordt gelaten vallen wanneer een uit orde geplaatst pakket van TCP te lang in de buffer is gehouden.Typisch, worden de pakketten van TCP in orde op verbindingen geplaatst die door het veiligheidstoestel worden geïnspecteerd of wanneer de pakketten naar SSM voor inspectie worden verzonden. Wanneer het volgende TCP-pakket dat verwacht wordt niet binnen een bepaalde periode aankomt, wordt het in de wachtrij geplaatste pakket dat niet op bestelling is geleverd, verwijderd.

Aanbevelingen:
Het volgende TCP-pakket dat verwacht wordt, komt niet aan vanwege stremming in het netwerk dat normaal is in een druk netwerk. Het TCP-wederuitzendmechanisme in de eindhost moet het pakket opnieuw verzenden en de sessie kan doorgaan.

Naam: TCP niet-syn
Eerste TCP-pakket niet SYN:
Ontving een niet SYN pakket als het eerste pakket van een niet onderschepte en niet genagelde verbinding.

Aanbeveling:
Onder normale omstandigheden is dit te zien wanneer het apparaat al een verbinding heeft gesloten en de client of server nog steeds gelooft dat de verbinding open is en gegevens blijft verzenden. Een paar voorbeelden waar dit kan gebeuren is net nadat een 'duidelijke lokaal-host' of 'duidelijke uitleg' is uitgegeven. Als de aansluitingen bovendien onlangs niet zijn verwijderd en de teller snel groeit, kan het apparaat onder vuur liggen. Leg een snuffelspoor vast om de oorzaak te isoleren.

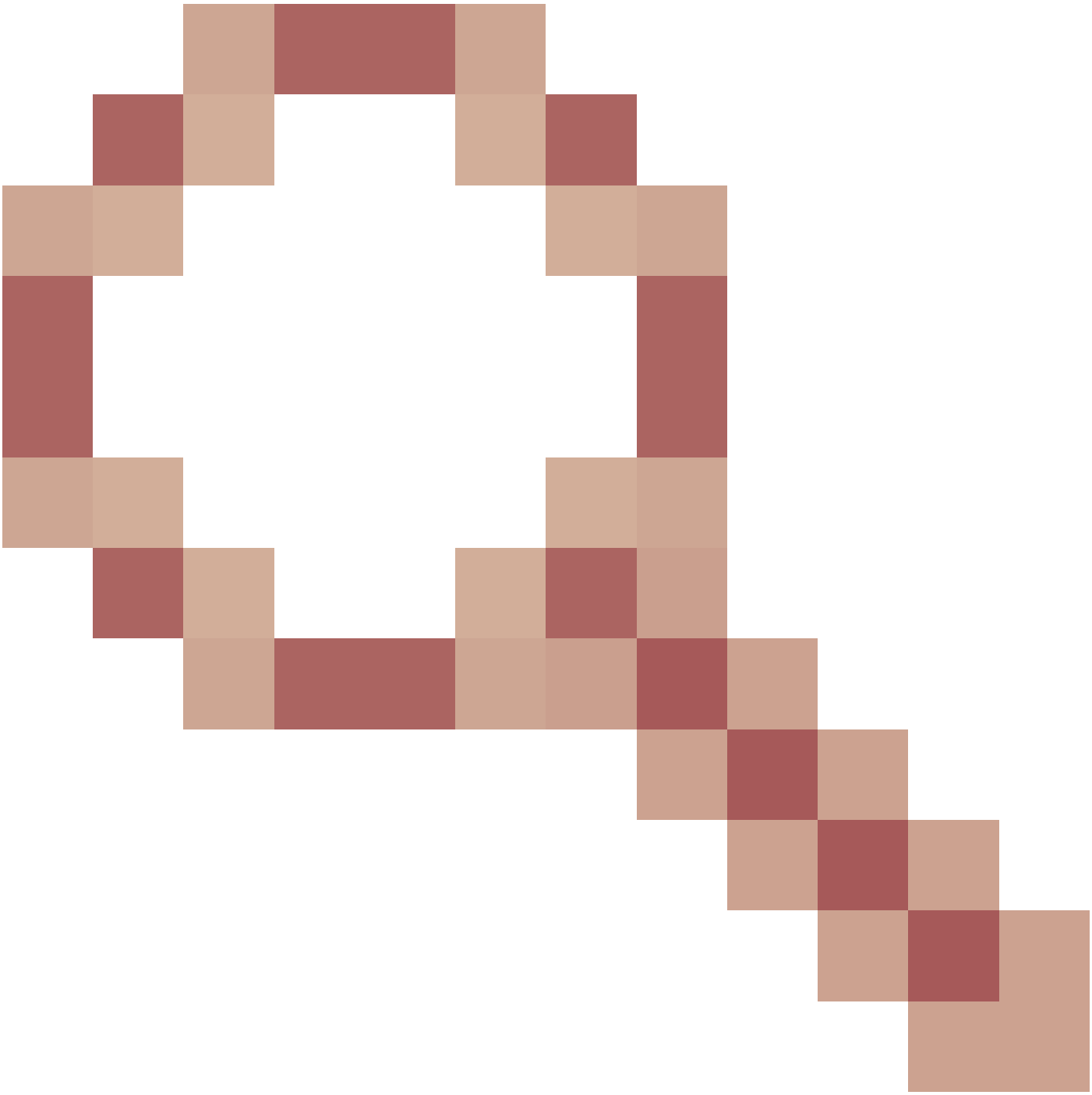
Oplossing: Schakel SQL*Net-inspectie uit als SQL-gegevensoverdracht plaatsvindt via dezelfde poort als de SQL-controle TCP-poort 1521. Het security apparaat fungeert als een proxy wanneer SQL*Net-inspectie is ingeschakeld en verkleint de grootte van het clientvenster van 65000 tot ongeveer 16000 die problemen met gegevensoverdracht veroorzaakt.

Voorbeeld van ICMP-inspectie en drop

Dit scenario is voor een FTD-clusteromgeving.
De ICMP-identificatie van de ICMP-header kan worden gebruikt als de bronpoort van de 5-tuple in de flow, zodat alle 5-tuple van de ping-pakketten hetzelfde zijn, ASP-reden is "inspect-icmp-seq-num-niet-gematched" zoals u kunt waarnemen in deze uitvoer.

```
firepower#show cap asp-drop
 1: 19:47:09.293136 10.0.5.8 > 10.50.0.53 icmp: echo reply Drop-reason: (inspect-icmp-seq-num-not-match
```

Cisco bug-ID CSCvb92417



[Cluster ASA daalt naar de doos ICMP antwoorden met reden "inspect-icmp-seq-num-niet-aangepast"]

ASP Drop reden:

Naam: inspecteren-icmp-seq-num-niet-overeenkomend
ICMP-inspectie volgnummer niet gevonden
Deze teller moet worden verhoogd wanneer het volgnummer in het ICMP-echoantwoordbericht niet overeenkomt met een ICMP-echobericht dat eerder op dezelfde verbinding over het apparaat is doorgegeven.

Oplossing: ICMP-inspectie uitschakelen. In clusteromgeving: twee of meer FTD in cluster en het ICMP-verkeer kan asymmetrisch zijn. Er wordt opgemerkt dat er een vertraging is voor het wissen

van ICMP-stromen, de volgende ping wordt snel verzonden voordat de vorige ping-stroom is opgeruimd. In dit geval kan het opeenvolgende verloren pingpakket gebeuren.

Voorbeeld van SIP-inspectie

In dit scenario duurden de gesprekken slechts vijf minuten, dan is de verbinding verbroken. Wanneer RTP wordt gebruikt, kan SIP-inspectie verbindingen neerzetten.
Aangezien u in de pakketopnameuitvoer op interface voor VoIP-verkeer kunt waarnemen, betekent de BYE-vlag in het SIP-verkeer dat het telefoongesprek op dat moment wordt gesloten.

```
1    2023-10-13 18:39:03.421456    10.6.6.66    172.16.3.77    SIP/SDP    1055    Request: INVITE sip:1
2    2023-10-13 18:39:03.448325    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
3    2023-10-13 18:39:03.525424    172.16.3.77    10.6.6.66    SIP    687    Status: 401 Unauthorized |
4    2023-10-13 18:39:03.525943    10.6.6.66    172.16.3.77    SIP    425    Request: ACK sip:123456789
5    2023-10-13 18:39:03.527331    10.6.6.66    172.16.3.77    SIP/SDP    1343    Request: INVITE sip:1
6    2023-10-13 18:39:03.553544    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
7    2023-10-13 18:39:05.902815    172.16.3.77    10.6.6.66    SIP/SDP    992    Status: 183 Session Pr
8    2023-10-13 18:39:06.091822    172.16.3.77    10.6.6.66    SIP/SDP    967    Status: 180 Ringing |
9    2023-10-13 18:39:13.114435    172.16.3.77    10.6.6.66    SIP/SDP    1063    Status: 200 OK (INVIT
10    2023-10-13 18:39:13.115899    10.6.6.66    172.16.3.77    SIP    560    Request: ACK sip:55663399
11    2023-10-13 18:40:29.206593    172.16.3.77    10.6.6.66    SIP    642    Request: UPDATE sip:FD3a5
12    2023-10-13 18:40:29.207630    10.6.6.66    172.16.3.77    SIP    659    Status: 200 OK (UPDATE) |
13    2023-10-13 18:41:09.940854    10.6.6.66    172.16.3.77    SIP    684    Request: BYE sip:33445566
14    2023-10-13 18:41:10.003066    172.16.3.77    10.6.6.66    SIP    659    Status: 200 OK (BYE) |
```

In dit andere voorbeeld, toont syslog een in kaart gebracht IP die PAT gebruiken, wordt IP verlaten met slechts één beschikbare haven en de zitting van SIP die op zelfde haven wordt geland, SIP ontbrak wegens poorttoewijzing. Als PAT in gebruik is kan SIP-inspectie de verbinding laten vallen.

De reden voor de ASP-daling is: "Kan geen UDP-verbinding maken van IP/poort naar IP/poort omdat de PAT-blokkeringslimiet per host van X is bereikt" en "beëindigd door inspectie-engine, reden - reset gebaseerd op 'service resetinboud'-configuratie"

```
Nov 18 2019 10:19:34: %FTD-6-607001: Pre-allocate SIP Via UDP secondary channel for 3111:10.11.0.13/506
Nov 18 2019 10:19:35: %FTD-6-302022: Built backup stub TCP connection for identity:172.16.2.20/2325 (17
Nov 18 2019 10:19:38: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:38: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
Nov 18 2019 10:19:39: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:39: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
```

ASP Drop reden:

Naam: async-lock-wachtrij-limiet
Maximale asynchrone vergrendelingswachtrij overschreden:
Elke async lock werkrij heeft een limiet van 1000. Wanneer er meer SIP-pakketten naar de

werkwachtrij proberen te worden verzonden, moet het pakket worden gedropt.
Aanbeveling:
Alleen SIP-verkeer kan worden gedropt. Wanneer SIP-pakketten hetzelfde ouderslot hebben en ze in dezelfde async lock wachtrij kunnen worden geplaatst, kan dit resulteren in blokdepletie, omdat slechts één kern alle media verwerkt. Als een SIP-pakket probeert te worden wachtrij wanneer de grootte van de asynchrone vergrendelingswachtrij de limiet overschrijdt, moet het pakket worden gedropt.

Naam: sp-looping-adres
adres van een lus:
Deze teller wordt verhoogd wanneer de bron en bestemmingsadressen in een stroom het zelfde zijn. SIP-stromen waar adresprivacy is ingeschakeld zijn uitgesloten, omdat het normaal is dat die stromen hetzelfde bron- en doeladres hebben.

Aanbeveling:
Er zijn twee mogelijke voorwaarden wanneer deze teller kan stijgen. Een daarvan is wanneer het apparaat een pakket met het bronadres ontvangt dat gelijk is aan de bestemming. Dit vertegenwoordigt een type van de aanval van Dos. De tweede is wanneer de NAT-configuratie van het apparaat NAT's een bronadres is dat gelijk is aan dat van de bestemming.

Naam: door ouder gesloten
Ouderstroom is gesloten:
Wanneer de basisstroom van een ondergeschikte stroom wordt gesloten, wordt de ondergeschikte stroom ook gesloten. Een FTP-gegevensstroom (ondergeschikte stroom) kan bijvoorbeeld worden gesloten met deze specifieke reden wanneer de controlestroom (parent flow) wordt beëindigd. Deze reden wordt ook gegeven wanneer een secundaire stroom (pin-hole) wordt gesloten door de bedieningsapplicatie. Bijvoorbeeld, wanneer het BYE-bericht wordt ontvangen, moet de SIP-inspectie engine (besturingstoepassing) de corresponderende SIP RTP-stromen (secundaire stroom) sluiten.

Oplossing: Schakel SIP-inspectie uit. Vanwege beperkingen op het protocol:

- De SIP-inspectie ondersteunt alleen de Chat-functie. Whiteboard, File Transfer en Application Sharing worden niet ondersteund. RTC-client 5.0 wordt niet ondersteund.
- Wanneer u PAT gebruikt, kan een SIP-headerveld met een intern IP-adres zonder poort niet worden vertaald en kan het interne IP-adres dus buiten worden gelekt. Als u deze lekkage wilt voorkomen, configureert u NAT in plaats van PAT.
- SIP-inspectie is standaard ingeschakeld met behulp van de standaard-inspectiekaart, die het volgende omvat:
  * SIP instant messaging (IM) extensies: Ingeschakeld.
  * Non-SIP verkeer op SIP poort: gevallen.
  * IP-adressen van server- en endpointservers verbergen: Uitgeschakeld.
  * Masker softwareversie en niet-SIP URIs: Uitgeschakeld.
  * Zorg ervoor dat het aantal hop naar de bestemming groter is dan 0: Ingeschakeld.
  * RTP-conformiteit: Niet afgedwongen.
  * SIP-conformiteit: Voer geen statustoetsen en headervalidatie uit.

Problemen oplossen

Dit zijn enkele van de voorgestelde opdrachten om verkeersproblemen op te lossen met betrekking tot de LINA MPF-protocolinspectie.

- Toon dienst-beleid tonen de statistieken van het de dienstbeleid voor de toegelaten inspecties van LINA MPF.

```
firepower# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/s
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
      Inspect: skinny, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp error, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-f
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-
    Class-map: class_snmp
      Inspect: snmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
    Class-map: class-default

      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

Deze steekproefoutput van show service-policy inspect http commando toont de http statistics:

```
firepower# show service-policy inspect http
    Global policy:
      Service-policy: global_policy
        Class-map: inspection_default
          Inspect: http http, packet 1916, drop 0, reset-drop 0
            protocol violations
              packet 0
            class http_any (match-any)
              Match: request method get, 638 packets
              Match: request method put, 10 packets
              Match: request method post, 0 packets
              Match: request method connect, 0 packets
              log, packet 648
```

- Stel een asp-drop-opname in op de te inspecteren interface.

```
Syntax
#Capture


        type asp-drop


         match
```

```
for example
#Capture asp type asp-drop all match ip any any
#Capture asp type asp-drop all match ip any host x.x.x.x
#Capture asp type asp-drop all match ip host x.x.x.x host x.x.x.x
```

Hoe specifieke LINA MPF-toepassingsinspecties in- of uitschakelen

Dit zijn de beschikbare opties om de MPF LINA-toepassingsinspecties in of uit te schakelen in Cisco Secure Firewall Threat Defence.

- Configuratie via FlexConfig: U hebt beheerderstoegang tot de FMC UI nodig, deze verandering is permanent op de configuratie.
- Configuratie via FTD CLI: U hebt beheerderstoegang tot FTD CLI nodig, deze verandering is niet permanent, als een reboot of een nieuwe plaatsing plaatsvindt, wordt de configuratie verwijderd.

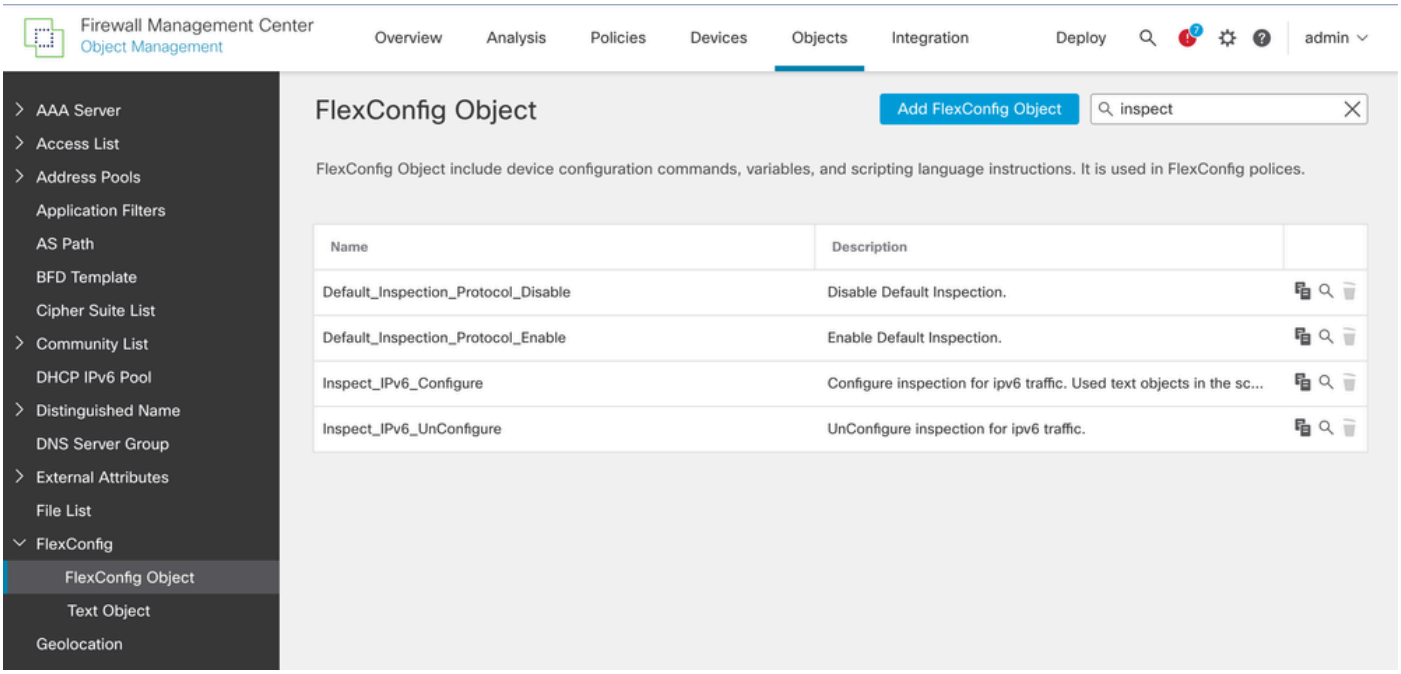
Configuratie via FlexConfig

FlexConfig is een methode van laatste redmiddel om op ASA gebaseerde functies te configureren die compatibel zijn met bedreigingsverdediging maar die niet anderszins in het beheercentrum kunnen worden geconfigureerd.

De configuratie om inspectie permanent uit te schakelen of in te schakelen is op FlexConfig via de FMC UI, kan globaal worden toegepast of alleen voor specifiek verkeer.

Stap 1.

Op FMC UI, navigeer naar Objecten > Objectbeheer > FlexConfig > FlexConfig Object, daar kunt u de lijst met de standaardobjecten van de Protocol Inspectie vinden.



Standaard FlexConfig-protocolinspectieobjecten

Stap 2.

Om een specifieke protocolinspectie uit te schakelen, kunt u een FlexConfig-object maken.

Navigeer naar objecten > Objectbeheer > FlexConfig > FlexConfig-object > Add FlexConfig

In dit voorbeeld, de configuratie om SIP Inspectie van global_policy uit te schakelen, moet de

syntaxis zijn:

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

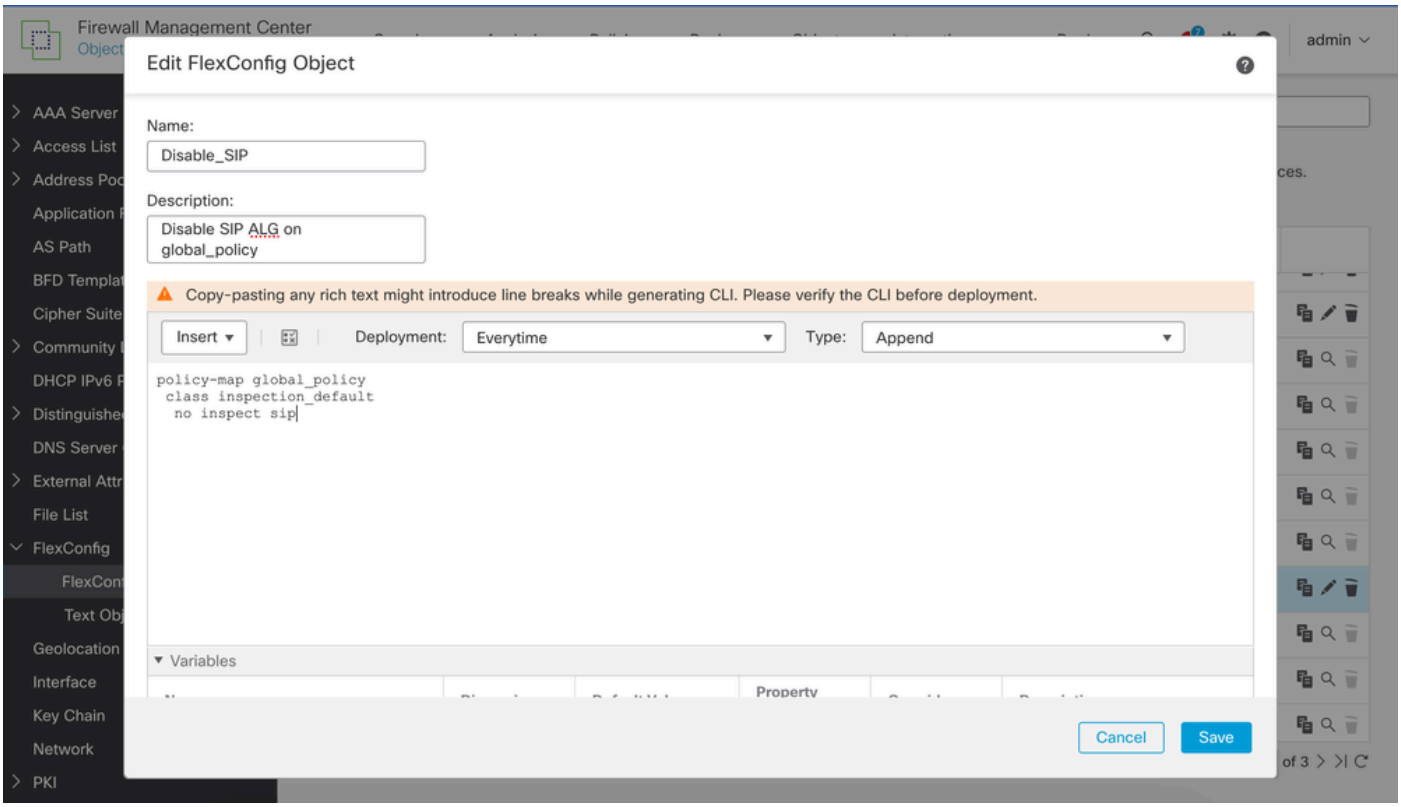
Bij het configureren van een FlexConfig-object kunt u de implementatiefrequentie en het type kiezen.

Implementatie

- Als het FlexConfig-object verwijst naar systeembeheerde objecten zoals netwerk- of ACL-objecten, kiest u Overal. Anders, konden de updates aan de voorwerpen niet worden opgesteld.
- Gebruik Eenmaal als het enige ding dat u in het object doet is om een configuratie te wissen. Verwijder vervolgens het object uit het FlexConfig-beleid na de volgende implementatie.

Type

- Toevoegen (de standaardinstelling) Opdrachten in het object worden aan het einde van de configuraties gezet die zijn gegenereerd op basis van het beleid van het beheercentrum. U moet Toevoegen gebruiken als u beleidsobjectvariabelen gebruikt, die verwijzen naar objecten die van beheerde objecten zijn gegenereerd. Als opdrachten die voor andere beleidsgebieden zijn gegenereerd, overlappen met de opdrachten die in het object zijn opgegeven, moet u deze optie selecteren, zodat uw opdrachten niet worden overschreven. Dit is de veiligste optie.
- Prepend. Opdrachten in het object staan aan het begin van de configuraties die worden gegenereerd op basis van het beleid van het beheercentrum. U zou typisch prepend voor bevelen gebruiken die ontruimen of een configuratie ontkennen.



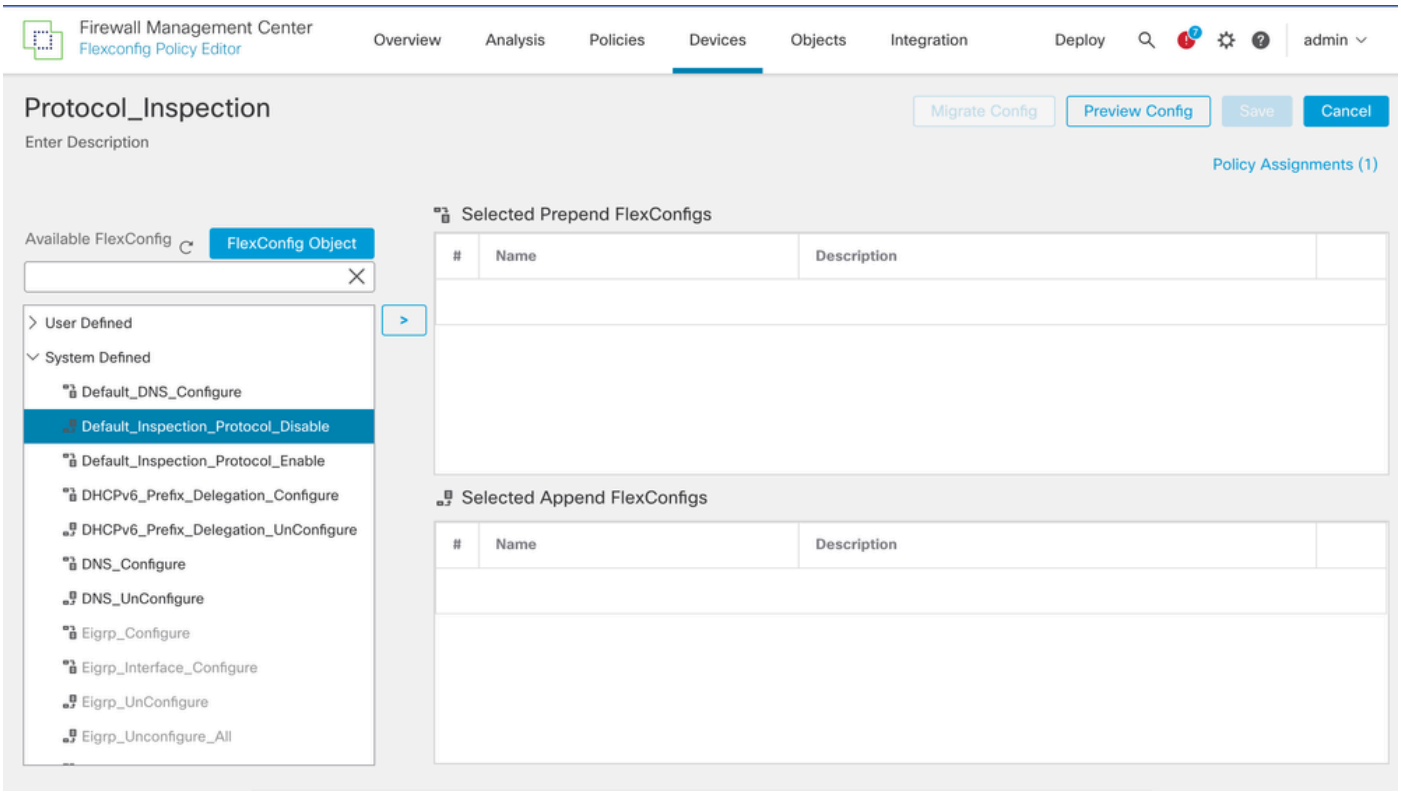
Maak een object om één protocol uit te schakelen vanuit de standaard global_policy

Stap 3.

Voeg de objecten toe in het FlexConfig-beleid dat aan LINA is toegewezen.

Navigeer naar Apparaten > FlexConfig en selecteer het FlexConfig-beleid dat op de firewall is toegepast met problemen met betrekking tot het neerzetten van de firewall.

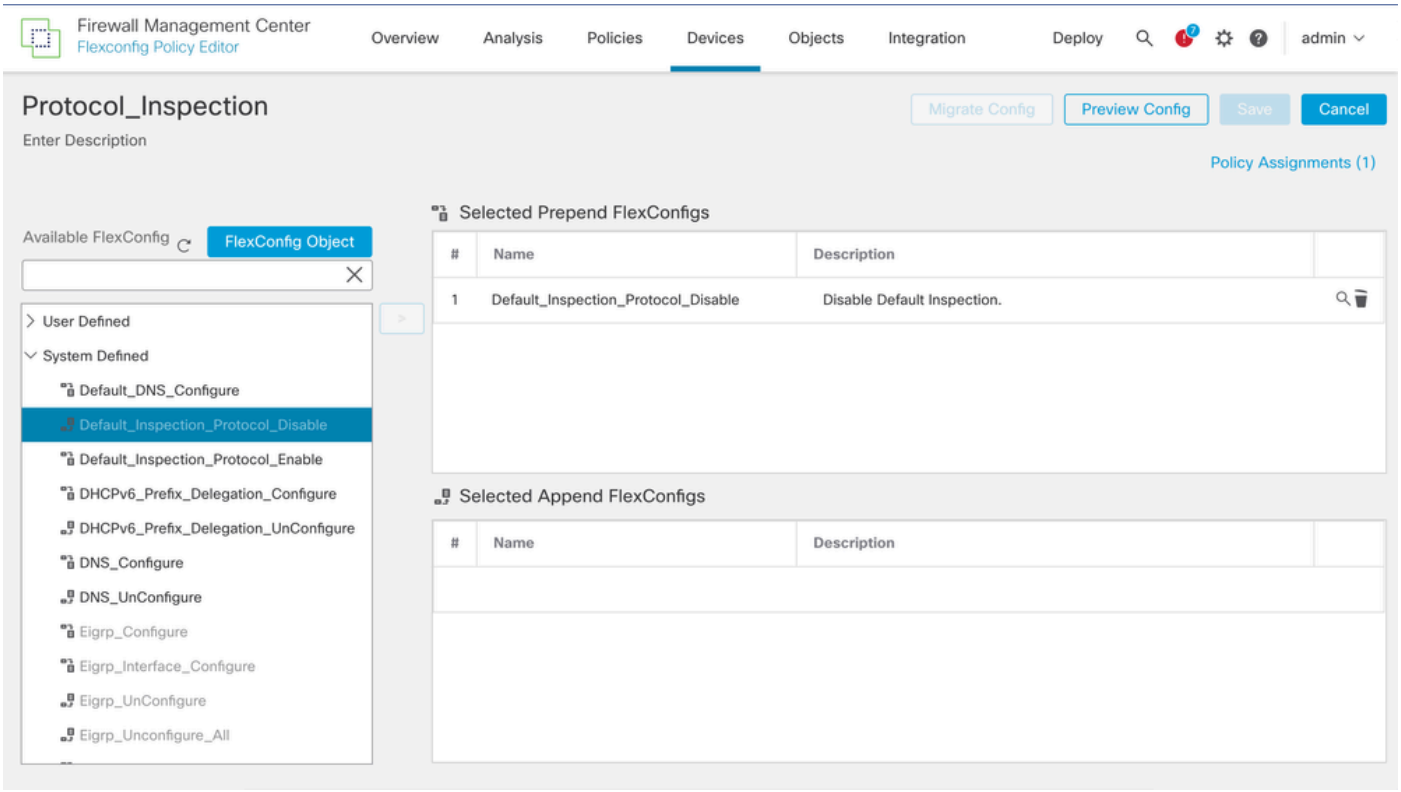
Als u alle inspectie wereldwijd wilt uitschakelen, selecteert u het object Default_Inspection_Protocol_Disable onder de door het systeem gedefinieerde FlexConfig-objecten. Klik vervolgens op de blauwe pijl ertussen om deze aan het FlexConfig-beleid toe te voegen.



Selecteer het systeem gedefinieerde object om alle protocolinspectie uit te schakelen

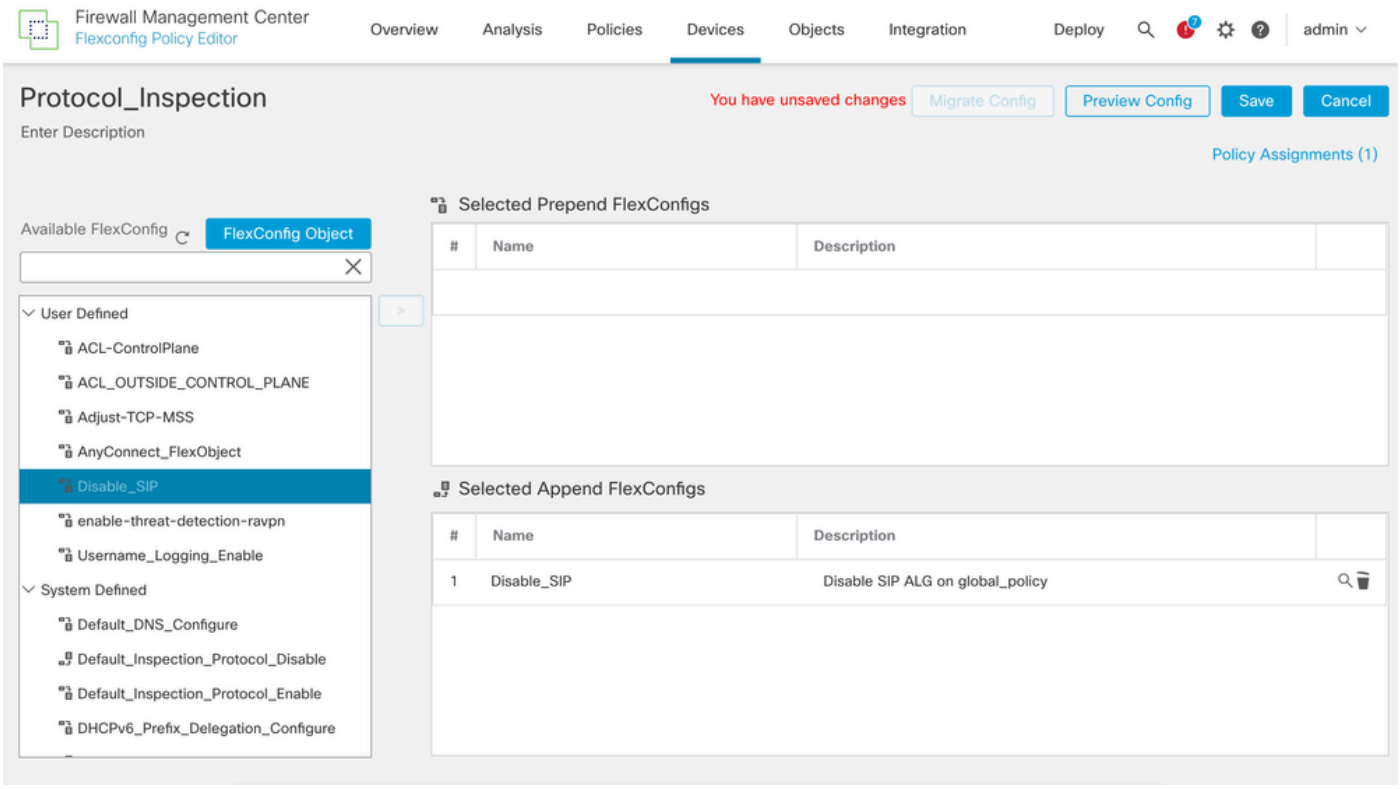
Stap 4.

Zodra geselecteerd, bevestig het in de juiste vakjes verschijnt, vergeet niet om de configuratie op te slaan en op te stellen om van kracht te worden.



Geselecteerd object om alle protocolinspectie uit te schakelen

Stap 5.
Als u één protocolinspectie wilt uitschakelen, selecteert u het object dat eerder door de gebruiker is gedefinieerd en voegt u het toe aan het beleid met de pijl tussen de vakjes.



Selecteer deze optie om één protocolinspectie uit te schakelen van de global_policy

Stap 6.

Zodra geselecteerd, bevestig het in de juiste vakjes verschijnt, vergeet niet om de configuratie op te slaan en op te stellen om van kracht te worden.

Configuratie met behulp van de FTD CLI

Deze oplossing kan direct vanaf de FTD CLI worden toegepast om te testen als de inspectie het verkeer beïnvloedt. De configuratiewijziging wordt echter niet opgeslagen als er opnieuw wordt opgestart of als er een nieuwe implementatie plaatsvindt.

Het commando moet vanuit de FTD CLI in Clish-modus worden uitgevoerd.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Verifiëren

Om te verifiëren dat het protocol onbruikbaar is, voer het bevel uit tonen in werking stelt -in werking stellen-in werking stellen-configuratie beleid-kaart. In dit voorbeeld is SIP-inspectie uitgeschakeld omdat deze niet meer in de standaardprotocollijst staat.

```
firepower# show running-config 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 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
!
firepower#
```

Gerelateerde informatie

Technische ondersteuning en documentatie – Cisco Systems

- Aan de slag met Application Layer Protocol Inspection
- Inspectie van fundamentele internetprotocollen
- Gebruik van ASP Drop Command tonen

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.