Fehlerbehebung bei Datenverkehrsverlusten aufgrund von LINA Protocol Inspection auf FTD

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ermitteln, ob bei der LINA-Protokollüberprüfung für MPF (Modular Policy Framework) Datenverkehr in der Cisco Secure FTD verloren geht.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesen Themen verfügen:

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Manager Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Virtual Cisco Secure Firewall Threat Defense (FTD), Version 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), Version 7.4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Prüfungs-Engines werden in einer Firewall für Services benötigt, die IP-Adressierungsinformationen in das Benutzerdatenpaket einbetten oder sekundäre Kanäle an dynamisch zugewiesenen Ports öffnen.

Die Protokollprüfung kann verhindern, dass schädlicher Datenverkehr in das Netzwerk gelangt, indem der Inhalt der Netzwerkpakete überprüft und Datenverkehr auf Basis der verwendeten Anwendung oder des verwendeten Protokolls blockiert oder geändert wird.
Somit können Prüfungs-Engines den Gesamtdurchsatz beeinflussen. In der Firewall sind standardmäßig mehrere gängige Prüfungs-Engines aktiviert. Diese können je nach Netzwerk zur Aktivierung weiterer Engines erforderlich sein.

Standardkonfigurationen

Standardmäßig enthält die FTD LINA-Konfiguration eine Richtlinie, die mit dem gesamten standardmäßigen Anwendungsinspektionsverkehr übereinstimmt.

Die Prüfung bezieht sich auf den Datenverkehr an allen Schnittstellen (eine globale Richtlinie).

Der standardmäßige Anwendungsinspektionsverkehr beinhaltet Datenverkehr zu den Standardports für jedes Protokoll. Sie können nur eine globale Richtlinie anwenden. Wenn Sie also die globale Richtlinie ändern möchten, z. B. Inspektionen auf nicht standardmäßige Ports anwenden oder Inspektionen hinzufügen möchten, die nicht standardmäßig aktiviert sind, müssen Sie die Standardrichtlinie entweder bearbeiten oder deaktivieren und eine neue anwenden.

Führen Sie den Befehl show running-config policy-map auf LINA, FTD Command Line Interface (CLI) über system support diagnostic-CLI aus, um die Informationen abzurufen.

```
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
!
```

Identifizierung von Paketverlusten aufgrund der MPF-Protokollüberprüfung

Selbst wenn der Datenverkehr mit der der Firewall zugewiesenen Zugriffskontrollrichtlinie (Access Control Policy, ACP) übereinstimmt, werden bei der Überprüfung in bestimmten Szenarien Verbindungen aufgrund eines bestimmten, von der Firewall empfangenen Datenverkehrsverhaltens, eines nicht unterstützten Designs, Anwendungsstandards oder einer Überprüfungseinschränkung beendet.

Bei der Fehlerbehebung für den Datenverkehr empfiehlt sich Folgendes:

- Legen Sie Echtzeit-Erfassungsprotokolle für die Schnittstellen fest, von denen der Datenverkehr fließt (Eingangs- und Ausgangsschnittstellen), Befehl:

```
firepower# capture

        [interface

        ][match



           [port
```

```
          ]

            [port

            ]]
```

Mit den Erfassungen können Sie die Option Paketnummer X Ablaufverfolgungsdetail einschließen und es muss die Ergebnisphase für Phase der Verbindung bereitstellen, wie es ein Paket-Ablaufverfolgungsbefehl tut, aber mit dieser Option stellen Sie sicher, dass es sich um Echtzeit-Datenverkehr handelt.

```
firepower# show capture

        packet number X trace detail
```

- Legen Sie in Echtzeit Accelerated Security Path (ASP) Drop, der Erfassungstyp asp-drop zeigt die Pakete oder Verbindungen, die von der ASP fallen gelassen, gibt es eine Liste von Gründen, die Sie in den Verwandten Links des Dokuments finden, Befehl:

```
firepower# capture

        [type

        ] [interface
```

```
][match


   [port

   ]

     [port

     ]]
```

Protokollprüfungsverluste können ignoriert werden, da in den Paketverfolgungsphasen ein Zulassen-Ergebnis beobachtet werden kann. Aus diesem Grund ist es wichtig, den Grund für das Verwerfen immer mithilfe von Echtzeit-Erfassungsprotokollen zu überprüfen.

Häufige Fehlermeldungen beim Löschen

Der Eintrag Accelerated Security Path (ASP) wird häufig zum Debuggen verwendet, um bei der Behebung von Netzwerkproblemen zu helfen. Der Befehl show asp drop wird verwendet, um diese verworfenen Pakete oder Verbindungen anzuzeigen und Einblicke in die Gründe für die Verwerfungen zu erhalten. Dazu können Probleme wie NAT-Fehler, Inspektionsfehler oder die Verweigerung von Zugriffsregeln gehören.

Wichtige Punkte zu ASP-Drops:

- Frame-Verluste: Hierbei handelt es sich um Löschvorgänge, die sich auf einzelne Pakete

beziehen, z. B. ungültige Kapselung oder keine Route zum Host.
- Flow-Drops: Diese hängen mit Verbindungen zusammen, z. B. Datenflüsse, die von Zugriffsregeln abgelehnt werden, oder NAT-Fehler.
- Verwendung: Der Befehl dient hauptsächlich zum Debuggen, und die Ausgabe kann geändert werden.

Diese Fehlermeldungen oder Abbruchgründe sind Beispiele, die bei der Fehlerbehebung auftreten können. Sie können je nach verwendetem Prüfprotokoll zurückgestellt werden.

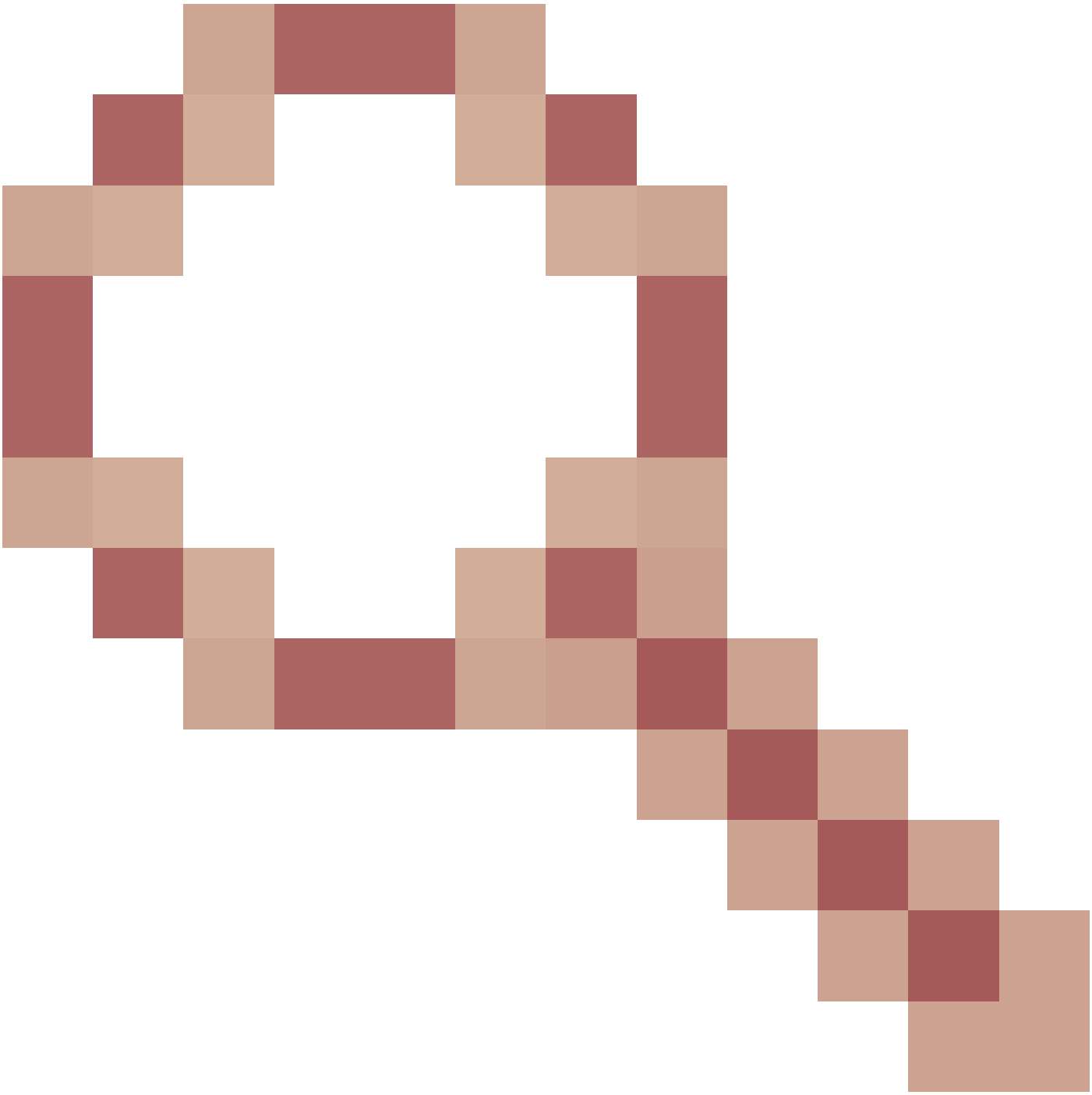
SUN RPC-Inspektion - Fallbeispiel

Dieses Szenario gilt für einen Single-Arm-Proxy FTDv in AWS-Bereitstellung, RPC-Datenverkehr gekapselt von Geneve, wenn die Sun Rpc Inspection aktiviert ist, wird die Verbindung getrennt.

Die Ausgabe zeigt ASP-Drops für die Sun Rpc-Überprüfung, Sun Rcp verwendet Port 111 als Ziel und das letzte Paket ist Geneve Kapselungsport, der 6081 als Ziel verwendet. Wie Sie feststellen können, ist der Grund für das Verwerfen der Ausgabe "Keine gültige Adjacency".

```
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 Bug-ID CSCwj00074



FTDv Single-Arm-Proxy verwirft Datenverkehr ohne Adjacency, wenn inspect sunrpc aktiviert ist

Der Datenverkehr wird im ASP der LINA-Engine als "keine gültige Adjacency" verworfen, da die Quell- und Ziel-MAC-Adresse nach dem zweiten Paket (SYN/ACK) des 3-Wege-Handshakes plötzlich vollständig in Nullen aufgefüllt wird.

Grund für ASP-Löschung:

Name: keine Adjazenz
Keine gültige Adjacency:
Dieser Zähler wird inkrementiert, wenn die Sicherheits-Appliance ein Paket in einem bestehenden Datenstrom empfängt, das keine gültige Ausgabe-Adjacency mehr aufweist. Dies

kann auftreten, wenn der nächste Hop nicht mehr erreichbar ist oder wenn eine Routing-Änderung in der Regel in einer dynamischen Routing-Umgebung stattgefunden hat.

Lösung: Deaktivieren Sie die sunrpc-Inspektion.

SQL*NET-Inspektionslöschbeispiel

Dieses Szenario gilt für einen Single-Arm-Proxy FTDv in einer AWS-Bereitstellung. Wenn die Sql*Nel-Überprüfung aktiviert ist, wird der von Geneve gekapselte Datenverkehr verworfen.

Die Ausgabe gilt für die zusammengeführten Paketerfassungen (Sie können dieselbe Paketnummer beobachten):
Erste Zeile: asp-drop packet capture nicht gekapselt, Sql*Net nutzt den 1521-Port als Ziel.
Zweite Zeile: VNI-Schnittstelle asp-drop auf LINA, Geneve verwenden Kapselungsport 6081 als Ziel.

Es gibt zwei verschiedene Gründe für das Verwerfen der Ausgabe, wie Sie sehen können, sie sind "tcp-buffer-timeout" und "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
```

Grund für ASP-Löschung:

Name: tcp-buffer-timeout
Timeout für TCP-Out-of-Order-Paketpuffer:
Dieser Zähler wird inkrementiert, und das Paket wird verworfen, wenn ein TCP-Paket, das nicht in der Warteschlange enthalten ist, zu lange im Puffer gespeichert wurde. In der Regel werden TCP-Pakete auf Verbindungen, die von der Sicherheits-Appliance geprüft werden, oder wenn Pakete zur Überprüfung an den SSM gesendet werden, in die Reihenfolge gebracht. Wenn das nächste erwartete TCP-Paket nicht innerhalb eines bestimmten Zeitraums ankommt, wird das in der Warteschlange nicht reihenfolgene Paket verworfen.

Empfehlungen:
Das nächste erwartete TCP-Paket kommt aufgrund einer Überlastung im Netzwerk nicht an, was in einem ausgelasteten Netzwerk normal ist. Der TCP-Weiterleitungsmechanismus auf dem End-Host muss das Paket erneut übertragen, und die Sitzung kann fortgesetzt werden.

Name: tcp-not-syn
Erstes TCP-Paket nicht SYN:
Ein Nicht-SYN-Paket wurde als erstes Paket einer nicht abgefangenen und nicht blockierten Verbindung empfangen.

Empfehlung:
Unter normalen Bedingungen ist dies zu sehen, wenn die Appliance bereits eine Verbindung geschlossen hat und der Client oder Server weiterhin glaubt, dass die Verbindung offen ist, und Daten weiter überträgt. Einige Beispiele, in denen dies möglich ist, sind direkt nach der Veröffentlichung eines 'clear local-host' oder 'clear xlate'. Wenn Verbindungen nicht vor kurzem entfernt wurden und der Zähler sich schnell erhöht, kann die Appliance angegriffen werden. Erfassen Sie eine Sniffer-Spur, um die Ursache zu identifizieren.

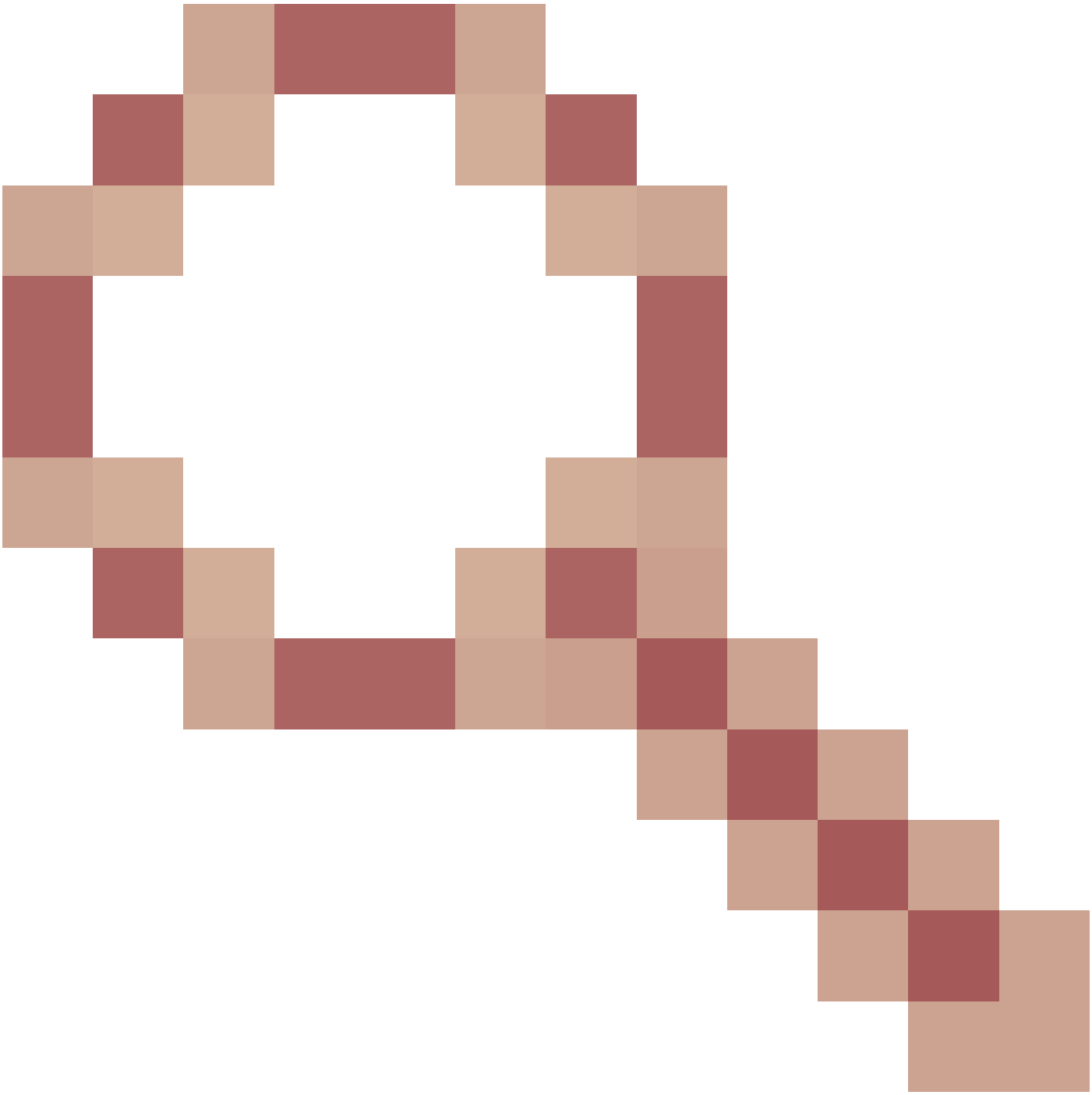
Lösung: Deaktivieren Sie die SQL*Net-Überprüfung, wenn die SQL-Datenübertragung auf demselben Port wie der SQL-Steuerungs-TCP-Port 1521 erfolgt. Die Sicherheits-Appliance agiert als Proxy, wenn die SQL*Net-Überprüfung aktiviert ist, und reduziert die Größe des Client-Fensters von 65000 auf ca. 16000, was zu Problemen bei der Datenübertragung führt.

ICMP-Inspektion - Fallbeispiel

Dieses Szenario gilt für eine FTD-Cluster-Umgebung.
Der ICMP-Bezeichner des ICMP-Headers kann als Quellport des 5-Tupels im Fluss verwendet werden, sodass alle 5-Tupel der Ping-Pakete identisch sind. Der Grund für das ASP-Drop ist "inspect-icmp-seq-num-not matching", wie Sie in dieser Ausgabe sehen können.

```
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 verwirft vorgefertigte ICMP-Antworten mit dem Grund "inspect-icmp-seq-num-not matching"

Grund für ASP-Löschung:

Name: inspect-icmp-seq-num-not-matching
Die ICMP-Untersuchungs-Sequenznummer stimmt nicht überein:
Dieser Zähler muss inkrementiert werden, wenn die Sequenznummer in der ICMP-Echoantwortmeldung mit keiner ICMP-Echomeldung übereinstimmt, die zuvor an die Appliance über dieselbe Verbindung weitergeleitet wurde.

Lösung: Deaktivieren Sie die ICMP-Inspektion. In Clusterumgebung: Zwei oder mehr FTDs im Cluster und der ICMP-Datenverkehr können asymmetrisch sein. Es wird beobachtet, dass die

Löschung des ICMP-Flusses verzögert wird. Der nachfolgende Ping wird schnell gesendet, bevor der vorherige Ping-Fluss bereinigt wurde. In diesem Fall kann es zu einem Verlust eines aufeinander folgenden Ping-Pakets kommen.

SIP-Inspektion - Fallbeispiel

In diesem Szenario dauerten die Anrufe nur fünf Minuten, dann wird die Verbindung unterbrochen. Bei Verwendung von RTP kann die SIP-Inspektion Verbindungen trennen.
Wie Sie in der Ausgabe der Paketerfassung an der Schnittstelle für VoIP-Datenverkehr sehen können, bedeutet das BYE-Flag im SIP-Datenverkehr, dass der Anruf zu diesem Zeitpunkt beendet wird.

```
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 diesem anderen Beispiel zeigt das Syslog eine zugeordnete IP-Adresse, die PAT verwendet. In der IP-Adresse ist nur noch ein Port verfügbar, und die SIP-Sitzung ist auf demselben Port gelandet. SIP ist aufgrund der Port-Zuweisung fehlgeschlagen. Wenn PAT verwendet wird, kann die SIP-Inspektion die Verbindung trennen.

Der Grund für das Verwerfen von ASP ist: "Es konnte keine UDP-Verbindung von IP/Port zu IP/Port hergestellt werden, da der PAT-Port-Blockgrenzwert pro Host von X erreicht wurde" und "Beendet durch Prüfungs-Engine, Grund - Zurücksetzen basierend auf 'service resetinboud'-Konfiguration"

```
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
```

Grund für ASP-Löschung:

Name: async-lock-queue-limit
Grenzwert für asynchrone Sperrwarteschlange überschritten:
Jede Arbeitswarteschlange mit asynchroner Sperre ist auf 1000 beschränkt. Wenn versucht wird, weitere SIP-Pakete an die Arbeitswarteschlange zu senden, muss das Paket verworfen werden.
Empfehlung:
Nur SIP-Datenverkehr kann verworfen werden. Wenn SIP-Pakete die gleiche übergeordnete Sperre haben und in dieselbe asynchrone Sperrwarteschlange gestellt werden können, kann dies zur Blockerschöpfung führen, da alle Medien nur von einem Kern verarbeitet werden. Wenn ein SIP-Paket versucht, in die Warteschlange gestellt zu werden, sobald die Größe der asynchronen Sperrwarteschlange den Grenzwert überschreitet, muss das Paket verworfen werden.

Name: sp-Looping-Adresse
Schleifenadresse:
Dieser Leistungsindikator wird erhöht, wenn die Quell- und Zieladressen in einem Datenfluss identisch sind. SIP-Datenflüsse, bei denen der Adressschutz aktiviert ist, werden ausgeschlossen, da diese Datenflüsse in der Regel dieselbe Quell- und Zieladresse haben.

Empfehlung:
Es gibt zwei mögliche Bedingungen, unter denen dieser Zähler inkrementiert werden kann. Eine ist, wenn die Appliance ein Paket empfängt, dessen Quelladresse dem Ziel entspricht. Dies stellt eine Art von DoS-Angriff dar. Der zweite Fall tritt ein, wenn die NAT-Konfiguration der Appliance-NATs eine Quelladresse enthält, die der des Ziels entspricht.

Name: elterngeschlossen
Übergeordneter Datenfluss ist geschlossen:
Wenn der Elternstrom eines untergeordneten Stromes geschlossen wird, wird auch der untergeordnete Strom geschlossen. Ein FTP-Datenfluss (untergeordneter Fluss) kann beispielsweise aus diesem Grund geschlossen werden, wenn sein Kontrollfluss (übergeordneter Fluss) beendet wird. Dieser Grund ist auch gegeben, wenn eine Sekundärströmung (Stiftloch) durch ihre Steueranwendung geschlossen wird. Wenn beispielsweise die BYE-Nachricht empfangen wird, muss die SIP-Prüfungs-Engine (steuernde Anwendung) die entsprechenden SIP-RTP-Flows (sekundärer Fluss) schließen.

Lösung: Deaktivieren Sie die SIP-Inspektion. Aufgrund von Einschränkungen des Protokolls:

- Die SIP-Inspektion unterstützt nur die Chat-Funktion. Whiteboard, Dateiübertragung und Anwendungsfreigabe werden nicht unterstützt. RTC Client 5.0 wird nicht unterstützt.
- Bei Verwendung von PAT kann kein SIP-Header-Feld, das eine interne IP-Adresse ohne Port enthält, umgewandelt werden, sodass die interne IP-Adresse nach außen durchsickern kann. Wenn Sie diese Leckage vermeiden möchten, konfigurieren Sie NAT anstelle von PAT.
- Die SIP-Inspektion wird standardmäßig mithilfe der Standardinspektionsübersicht aktiviert, die Folgendes umfasst:
  * SIP Instant Messaging (IM)-Erweiterungen: Aktiviert.
  * Nicht-SIP-Datenverkehr an SIP-Port: Verworfen.

* Server- und Endpunkt-IP-Adressen ausblenden: Deaktiviert.
* Maskensoftware und Nicht-SIP-URIs: Deaktiviert.
* Stellen Sie sicher, dass die Anzahl der Hops zum Ziel größer als 0 ist: Aktiviert.
* RTP-Konformität: Nicht erzwungen.
* SIP-Konformität: Führen Sie keine Statusüberprüfung und keine Headervalidierung durch.

Fehlerbehebung

Dies sind einige der empfohlenen Befehle zur Behebung von Datenverkehrsproblemen im Zusammenhang mit der LINA MPF-Protokollprüfung.

- Show service-policy display the service policy statistics for the LINA MPF spections enabled

```
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
```

Diese Beispielausgabe des Befehls show service policy inspect http zeigt die http-Statistik:

```
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
```

- Richtet eine asp-drop-Erfassung für die zu inspizierende Schnittstelle ein.

```
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
```

Aktivieren oder Deaktivieren bestimmter LINA MPF-Anwendungsinspektionen

Mit diesen Optionen können Sie die MPF LINA-Anwendungsinspektionen in Cisco Secure Firewall Threat Defense aktivieren oder deaktivieren.

- Konfiguration über FlexConfig: Sie benötigen Administratorzugriff auf die FMC-Benutzeroberfläche. Diese Änderung gilt dauerhaft für die Konfiguration.
- Konfiguration über FTD CLI: Sie benötigen Administratorzugriff auf die FTD-CLI. Diese Änderung ist nicht dauerhaft. Wenn ein Neustart durchgeführt oder eine neue Bereitstellung durchgeführt wird, wird die Konfiguration entfernt.

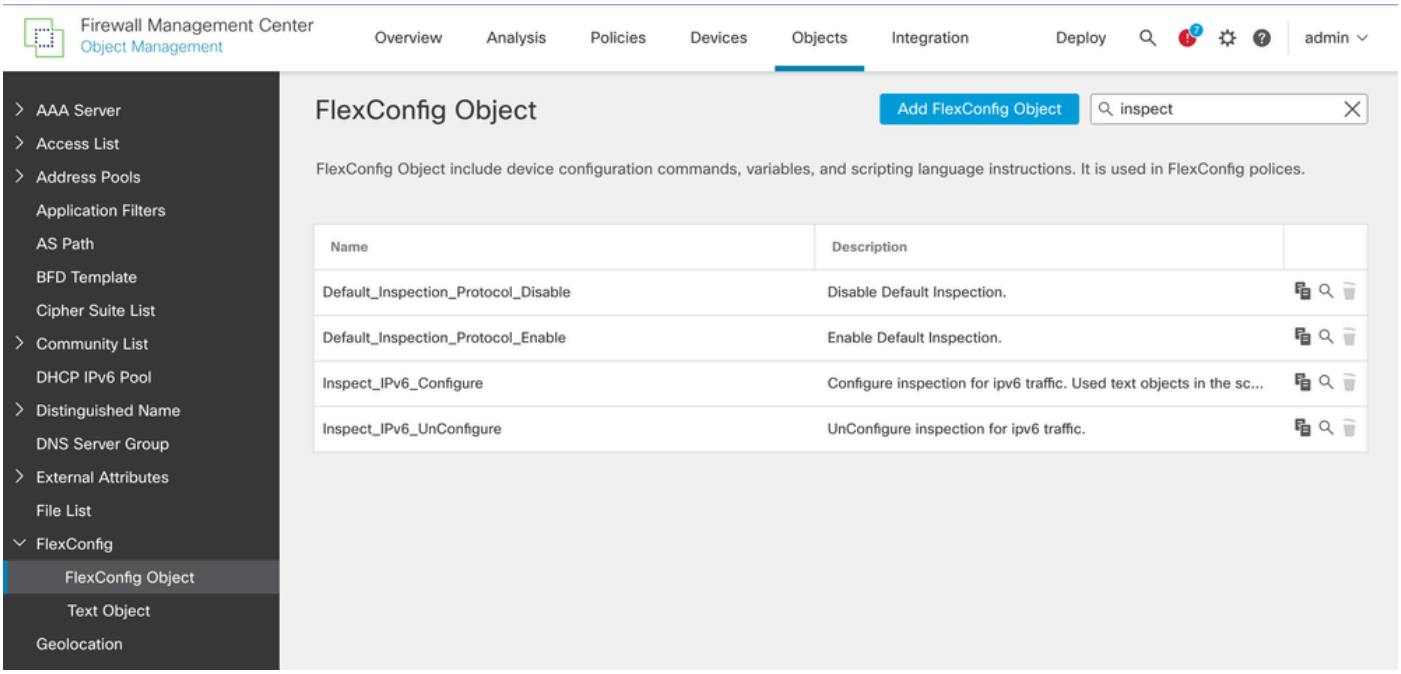
Konfiguration über FlexConfig

FlexConfig ist eine Methode der letzten Instanz zur Konfiguration von ASA-basierten Funktionen, die mit dem Schutz vor Bedrohungen kompatibel sind, aber im Management Center nicht anders konfiguriert werden können.

Die Konfiguration zum permanenten Deaktivieren oder Aktivieren der Überprüfung befindet sich auf FlexConfig über die FMC-Benutzeroberfläche. Sie kann global oder nur für bestimmten Datenverkehr angewendet werden.

Schritt 1:

Navigieren Sie in der FMC-Benutzeroberfläche zu Objects > Object Management > FlexConfig > FlexConfig Object. Dort finden Sie die Liste der standardmäßigen Protokollinspektionsobjekte.



Standard-FlexConfig-Protokollüberprüfungsobjekte

Schritt 2:

Um eine bestimmte Protokollüberprüfung zu deaktivieren, können Sie ein FlexConfig-Objekt erstellen.

Navigieren Sie zu Objekte > Objektverwaltung > FlexConfig > FlexConfig-Objekt > FlexConfig-Objekt hinzufügen

Bei der Konfiguration in diesem Beispiel zum Deaktivieren der SIP-Überprüfung in global_policy muss die Syntax wie folgt lauten:

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

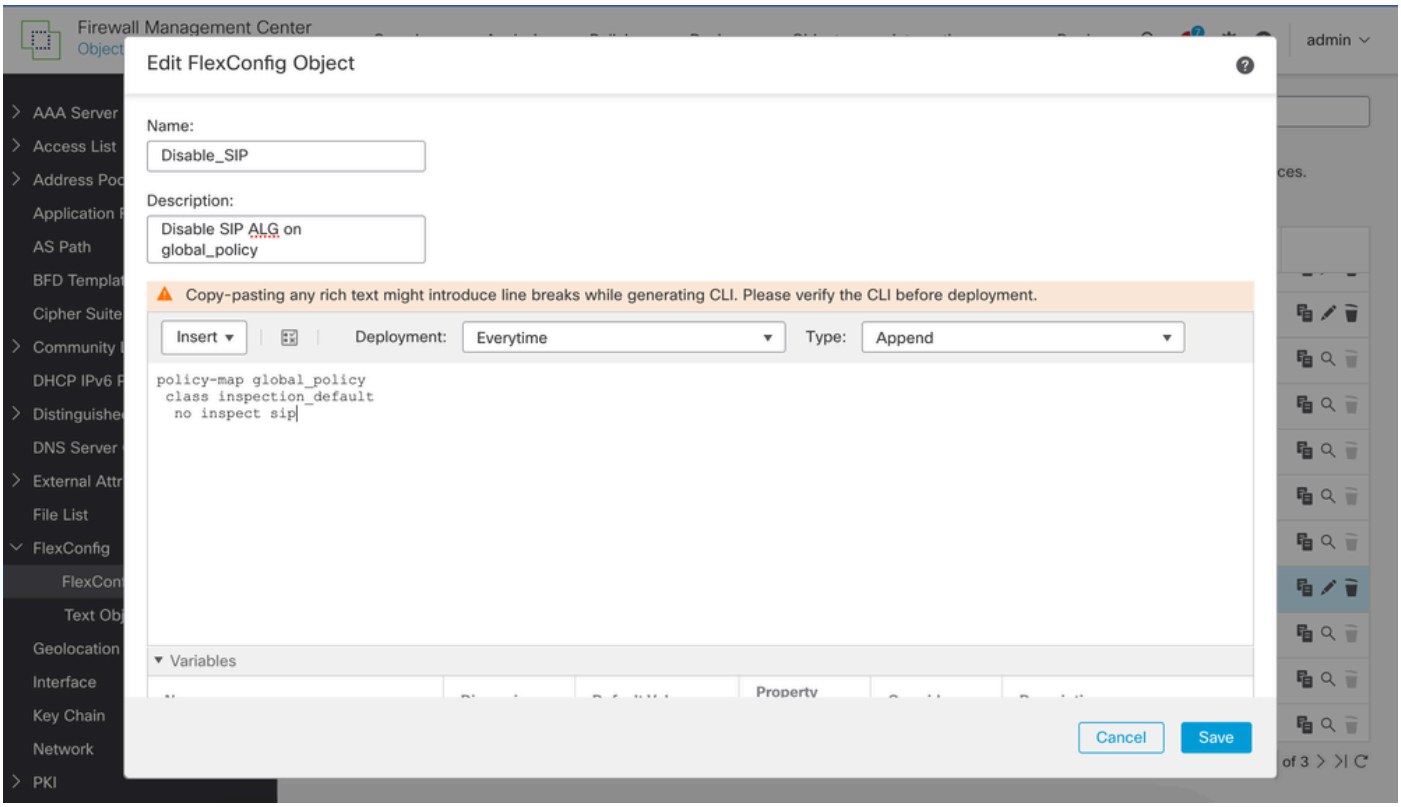
Beim Konfigurieren eines FlexConfig-Objekts können Sie die Bereitstellungshäufigkeit und den Bereitstellungstyp auswählen.

Bereitstellung

- Wenn das FlexConfig-Objekt auf vom System verwaltete Objekte wie Netzwerk- oder ACL-Objekte zeigt, wählen Sie Everytime (Immer). Andernfalls konnten keine Updates für die Objekte bereitgestellt werden.
- Verwenden Sie Once, wenn Sie im Objekt nur eine Konfiguration löschen möchten. Entfernen Sie dann nach der nächsten Bereitstellung das Objekt aus der FlexConfig-Richtlinie.

Typ

- Append (Der Standardwert.) Die Befehle im Objekt werden am Ende der Konfigurationen eingefügt, die aus den Richtlinien des Management Centers generiert wurden. Sie müssen Append verwenden, wenn Sie Richtlinienobjektvariablen verwenden, die auf Objekte verweisen, die von verwalteten Objekten generiert werden. Wenn sich die für andere Richtlinien generierten Befehle mit den im Objekt angegebenen überschneiden, müssen Sie diese Option auswählen, damit die Befehle nicht überschrieben werden. Dies ist die sicherste Option.
- Voranstellen. Befehle im Objekt werden an den Anfang der Konfigurationen gesetzt, die von den Richtlinien des Management Centers generiert werden. In der Regel verwenden Sie das Voranstellen für Befehle, mit denen eine Konfiguration gelöscht oder aufgehoben wird.



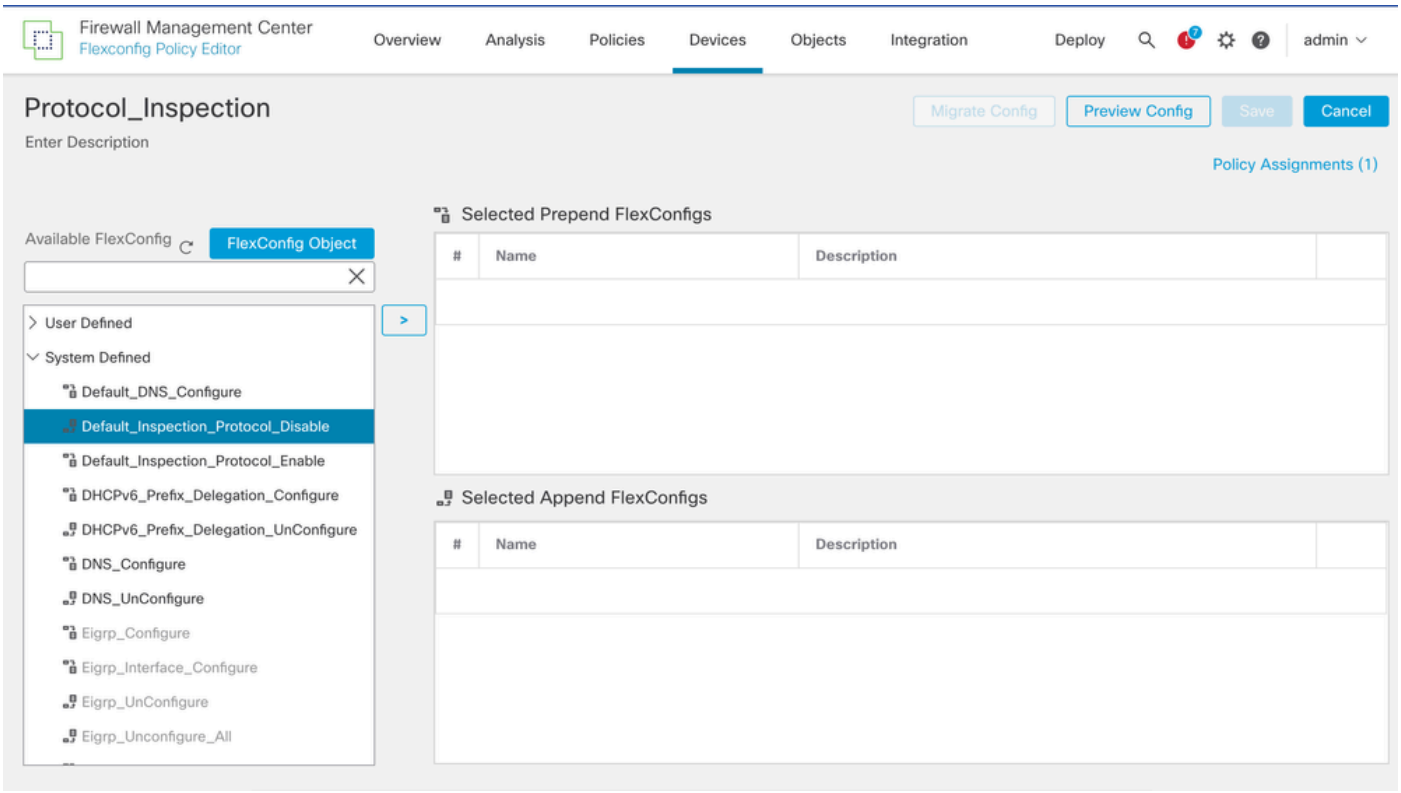
Erstellen Sie ein Objekt, um ein einzelnes Protokoll aus der global_policy-Standardrichtlinie zu deaktivieren.

Schritt 3:

Fügen Sie die Objekte in der LINA zugewiesenen FlexConfig-Richtlinie hinzu.

Navigieren Sie zu Devices (Geräte) > FlexConfig, und wählen Sie die FlexConfig-Richtlinie aus, die bei Problemen mit der Firewall angewendet wird.

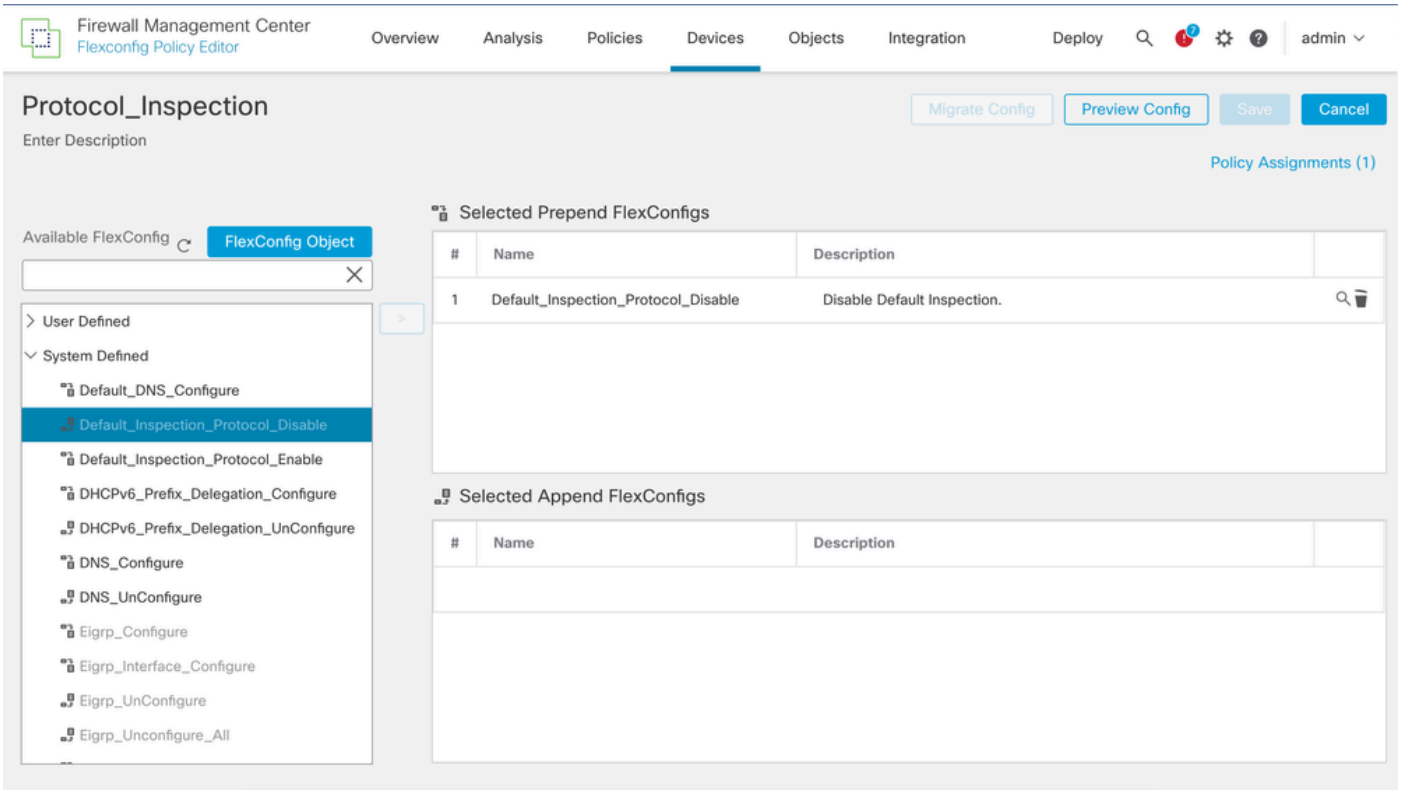
Um die gesamte Inspektion global zu deaktivieren, wählen Sie das Objekt Default_Inspection_Protocol_Disable unter den systemdefinierten FlexConfig-Objekten aus, und klicken Sie dann auf den blauen Pfeil dazwischen, um es der FlexConfig-Richtlinie hinzuzufügen.



Wählen Sie das vom System definierte Objekt aus, um die Protokollüberprüfung zu deaktivieren.

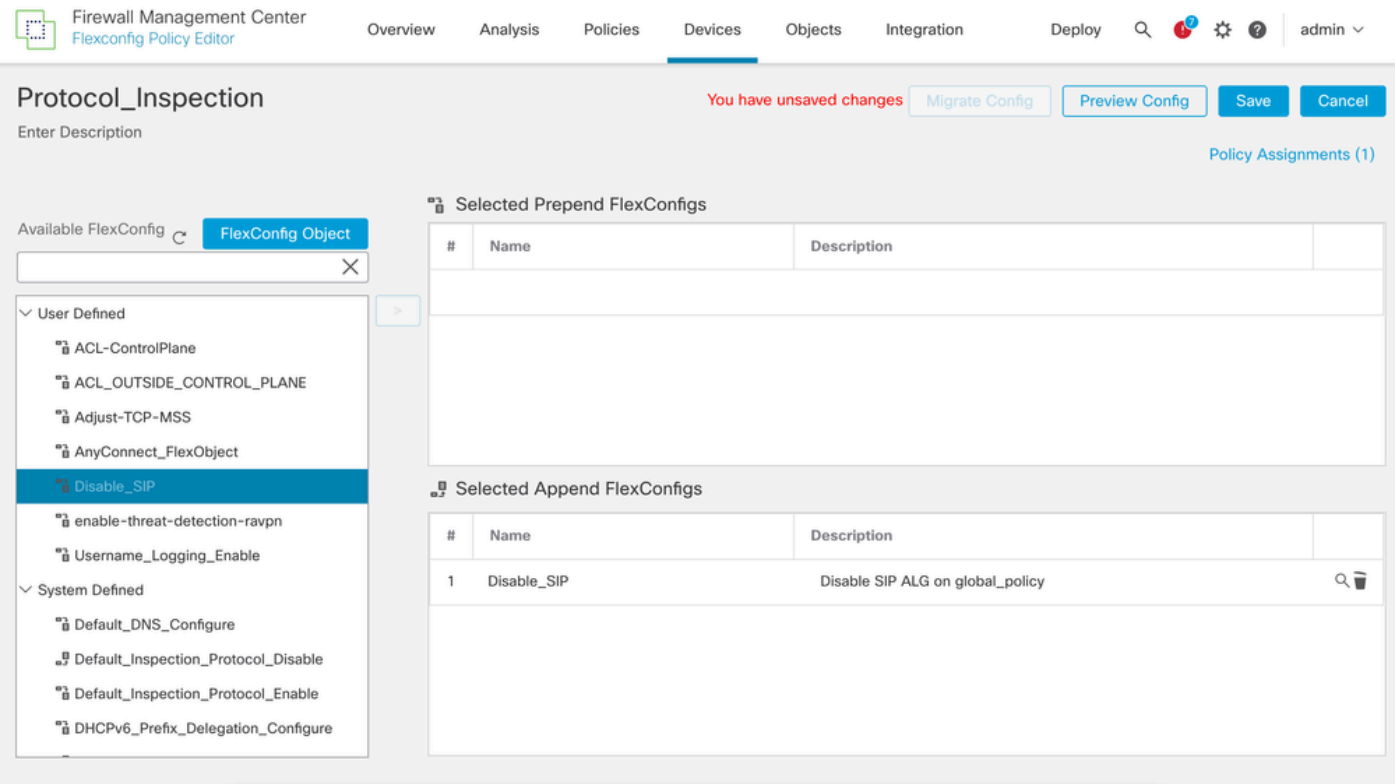
Schritt 4:

Bestätigen Sie nach der Auswahl, dass die Option in den rechten Feldern angezeigt wird. Vergessen Sie nicht, die Konfiguration zu speichern und bereitzustellen, damit sie wirksam wird.



Ausgewähltes Objekt zum Deaktivieren der Protokollüberprüfung

Schritt 5:
Um eine einzelne Protokollüberprüfung zu deaktivieren, wählen Sie das zuvor in der Liste Benutzerdefiniert erstellte Objekt aus, und fügen Sie es der Richtlinie mithilfe des Pfeils zwischen den Feldern hinzu.



Aktivieren Sie diese Option, um die Einzel-Protokollüberprüfung aus global_policy zu deaktivieren.

Schritt 6:

Bestätigen Sie nach der Auswahl, dass die Option in den rechten Feldern angezeigt wird. Vergessen Sie nicht, die Konfiguration zu speichern und bereitzustellen, damit sie wirksam wird.

Konfiguration über FTD CLI

Diese Lösung kann sofort über die FTD-CLI angewendet werden, um zu testen, ob sich die Überprüfung auf den Datenverkehr auswirkt. Die Konfigurationsänderung wird jedoch nicht gespeichert, wenn ein Neustart durchgeführt wird oder eine neue Bereitstellung erfolgt.

Der Befehl muss über die FTD-CLI im Clientmodus ausgeführt werden.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Überprüfung

Führen Sie den Befehl show running-config policy-map aus, um zu überprüfen, ob das deaktivierte Protokoll wirksam ist. In diesem Beispiel ist die SIP-Inspektion deaktiviert, da sie nicht mehr in der Standardprotokollliste angezeigt wird.

```
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#
```

Zugehörige Informationen

Technischer Support und Dokumentation für Cisco Systeme

- Erste Schritte mit der Protokollüberprüfung auf Anwendungsebene

- Überprüfung grundlegender Internet-Protokolle
- Verwendung von ASP-Ablagerungsbefehlen anzeigen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.