FTDのLINAプロトコルインスペクションによるトラフィックドロップのトラブルシューティング

内容

はじめに

このドキュメントでは、モジュラポリシーフレームワーク(MPF)のLINAプロトコルインスペクションがCisco Secure FTDでトラフィックをドロップするかどうかを識別する方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- シスコセキュアファイアウォール脅威対策(FTD)
- Cisco Secure Firewall Manager Center(FMC)。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Virtual Cisco Secure Firewall Threat Defense(FTD)、バージョン7.4.2

- Virtual Cisco Secure Firewall Manager Center(FMC)、バージョン7.4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメント内で使用されているデバイスはすべて、クリアな設定（デフォルト）から作業を始めています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

インスペクションエンジンは、ユーザデータパケットにIPアドレッシング情報を埋め込むサービス、または動的に割り当てられたポートでセカンダリチャネルを開くサービスのファイアウォールに必要です。

プロトコル検査は、ネットワークパケットの内容を検査し、使用されているアプリケーションまたはプロトコルに基づいてトラフィックをブロックまたは変更することで、悪意のあるトラフィックがネットワークに侵入するのを防止するのに役立ちます。
そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。ファイアウォールでは、いくつかの一般的なインスペクションエンジンがデフォルトで有効になっています。ネットワークによっては、他のインスペクションエンジンを有効にする必要がある場合があります。

デフォルト設定

デフォルトでは、FTD LINA設定には、すべてのデフォルトのアプリケーションインスペクショントラフィックに一致するポリシーが含まれています。

インスペクションは、すべてのインターフェイス（グローバルポリシー）のトラフィックに適用されます。

デフォルトのアプリケーション インスペクション トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合、たとえば、非標準ポートにインスペクションを適用したり、デフォルトでは有効にならないインスペクションを追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にしてから新しいポリシーを適用する必要があります。

情報を取得するには、show running-config policy-mapコマンドをLINAで実行し、FTDのコマンドラインインターフェイス(CLI)をシステムサポート診断CLIで実行します。

```
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
!
```

MPFプロトコルインスペクションによるパケットドロップの特定

トラフィックがファイアウォールに割り当てられたアクセスコントロールポリシー(ACP)と一致する場合でも、特定のシナリオでは、ファイアウォールで受信された特定のトラフィック動作、サポートされていない設計、アプリケーション標準、または検査制限のために、検査プロセスによって接続が終了されます。

トラフィックのトラブルシューティング時に使用できる便利なプロセスは次のとおりです。

- 次のコマンドを使用して、トラフィックのフロー元のインターフェイス (入力インターフェイスと出力インターフェイス) にリアルタイムキャプチャログを設定します。

```
firepower# capture

        [interface

        ][match
```

```
          [port

          ]

            [port

            ]]
```

キャプチャを使用する場合は、オプションpacket number X trace detailを含めることができます。また、packet-tracerコマンドと同様に、結果をフェーズごとに接続に使用する必要がありますが、このオプションを使用すると、結果がリアルタイムトラフィックであることを確認できます。

```
firepower# show capture

        packet number X trace detail
```

- Real-time Accelerated Security Path(ASP)Dropを設定すると、キャプチャタイプasp-dropではASPによって廃棄されたパケットや接続が表示されます。この理由のリストは、このドキュメントの「関連リンク」のコマンドに記載されています。

```
firepower# capture
```

```
[type

] [interface

 ][match


    [port

    ]

      [port

      ]]
```

プロトコルインスペクションドロップは、allowの結果がパケットトレーサフェーズで観察されることがあるため、無視できます。そのため、リアルタイムキャプチャログを使用してドロップの理由を常に確認することが重要です。

一般的なドロップエラーメッセージ

Accelerated Security Path(ASP)ドロップは、ネットワークの問題のトラブルシューティングに役立つデバッグ目的でよく使用されます。show asp dropコマンドは、これらのドロップされたパケットや接続を表示し、NAT障害、インスペクション障害、アクセスルール拒否などの問題を含む可能性のあるドロップの理由に関する情報を提供するために使用されます。

ASPドロップに関する重要ポイント：

- フレームドロップ：個々のパケットに関連するドロップ（無効なカプセル化やホストへのルートがないなど）です。
- フロードロップ：アクセスルールによって拒否されたフローやNAT障害などの接続に関連します。
- 使用法：このコマンドは主にデバッグ用で、出力は変わる可能性があります。

これらのエラーメッセージやドロップの原因は、トラブルシューティング中に発生する可能性がある例です。使用されているインスペクションプロトコルによっては遅延が発生する可能性があります。

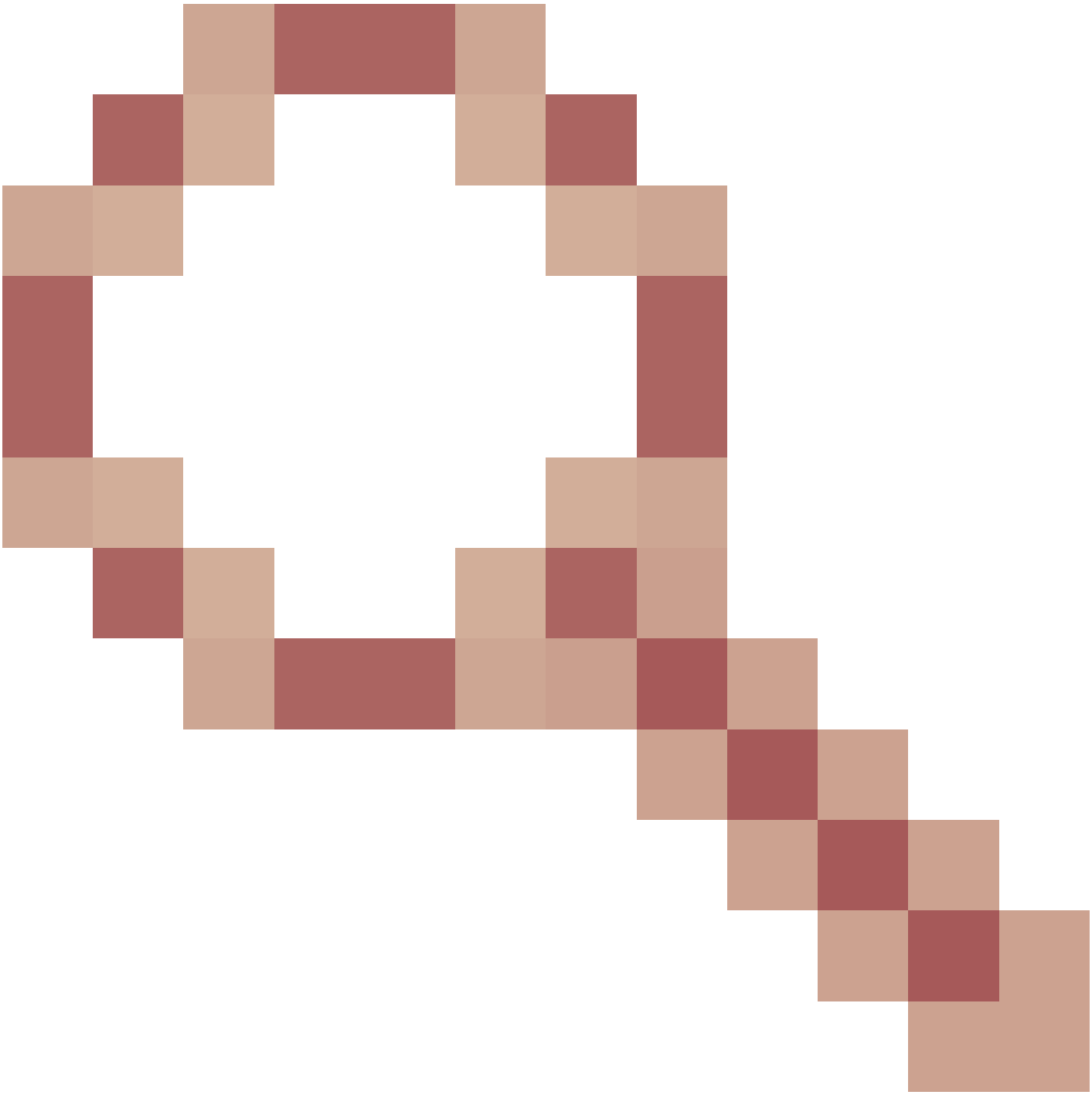
SUN RPCインスペクションドロップの例

このシナリオは、AWSデプロイのシングルアームプロキシFTDv、Geneveによってカプセル化されたRPCトラフィックに対するものです。Sun Rpcインスペクションが有効になっている場合、接続はドロップされます。

出力は、Sun RpcインスペクションのASPドロップを示し、Sun Rcpは宛先としてポート111を使用します。最後のパケットは、宛先として6081を使用するGeneveカプセル化ポートです。出力に「No valid adjacency」というドロップの理由が表示されていることがわかります。

```
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



[inspect sunrpcが有効な場合、FTDvシングルアームプロキシは隣接関係なしでトラフィックをドロップします]

3ウェイハンドシェイクの2番目のパケット(SYN/ACK)の後、送信元と宛先のMACアドレスがすべて突然0に設定されるため、トラフィックはLINAエンジンのASPで「有効な隣接関係がない」としてドロップされます。

ASPドロップの理由：

名前：no-adjacency
有効な隣接関係がありません：
　このカウンタは、セキュリティアプライアンスが、有効な出力隣接関係を持たなくなった既存

のフロー上のパケットを受信すると増加します。これは、ネクストホップが到達不能になった場合、またはルーティングの変更がダイナミックルーティング環境で通常発生した場合に発生する可能性があります。

解決策：sunrpcインスペクションを無効にします。

SQL*NETインスペクションドロップの例

このシナリオは、AWSデプロイのシングルアームプロキシFTDvに対するものです。Sql*Nelインスペクションが有効な場合、Geneveによるカプセル化されたトラフィックはドロップされます。

出力は、マージされたパケットキャプチャのものです（同じパケット番号を確認できます）。
最初の行：asp-dropパケットキャプチャはカプセル化されていません。Sql*Netは宛先として1521ポートを使用します。
2行目：LINAのVNI interface asp-drop、Geneveは宛先としてカプセル化ポート6081を使用します。

出力には2つの異なるドロップの理由があります。それは、「tcp-buffer-timeout」と「tcp-not-syn」であるためです

```
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ドロップの理由：

名前：tcp-buffer-timeout
TCPパケット順序が不正なバッファタイムアウト：
　このカウンタは増加し、キューから外れたTCPパケットがバッファに長期間保持されると、パケットは廃棄されます。通常、セキュリティアプライアンスによって検査される接続または検査のためにSSMにパケットが送信される接続では、TCPパケットが順番通りに配置されます。次に予想されるTCPパケットが一定の期間内に到着しない場合、キューに入れられた順不同のパケットは廃棄されます。

推奨事項：
　ビジー状態のネットワークでは通常、ネットワーク内の輻輳が原因で、次に予想されるTCPパケットが到着しません。エンドホストのTCP再送信メカニズムはパケットを再送信する必要があり、セッションを続行できます。

名前：tcp-not-syn
最初のTCPパケットはSYNではありません。
　代行受信および非固定接続の最初のパケットとして非SYNパケットを受信しました。

推奨事項：
　通常の状況では、アプライアンスがすでに接続を閉じており、クライアントまたはサーバが引き続き接続が開いていると認識してデータを送信し続けている場合に、この現象が発生することがあります。 これが発生する可能性のある例としては、「clear local-host」または「clear xlate」が発行された直後の場合があります。また、接続が最近削除されておらず、カウンタが急速に増加している場合、アプライアンスが攻撃を受けている可能性があります。スニファトレースをキャプチャして、原因の特定に役立てます。

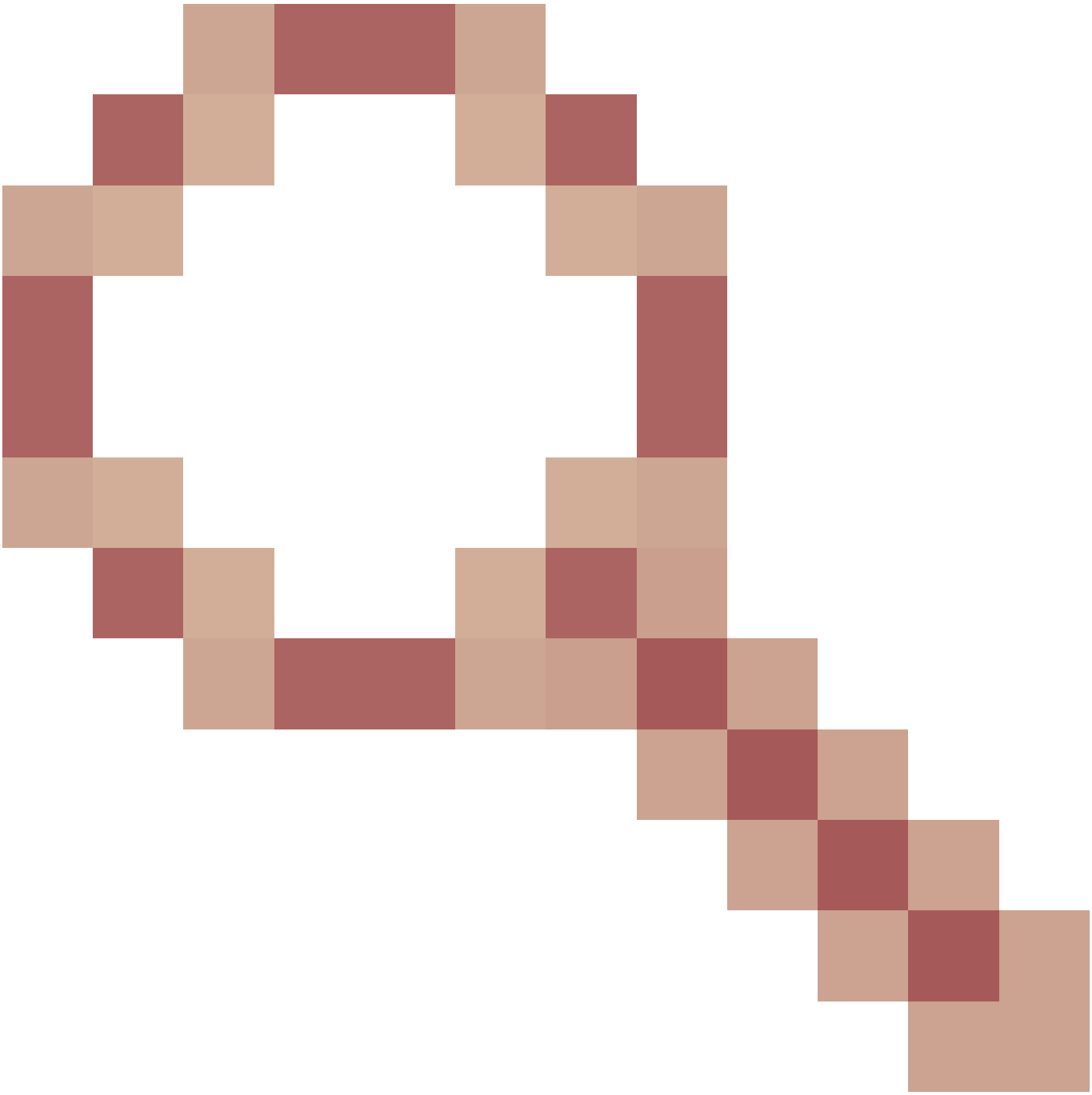
解決策：SQLデータ転送がSQL制御TCPポート1521と同じポートで発生する場合は、SQL*Netインスペクションを無効にします。セキュリティアプライアンスは、SQL*Netインスペクションが有効な場合にプロキシとして機能し、クライアントのウィンドウサイズを65000から約16000に縮小してデータ転送の問題を引き起こします。

ICMPインスペクションドロップの例

このシナリオは、FTDクラスタ環境を対象としています。
ICMPヘッダーのICMP識別子は、フロー内の5タプルの送信元ポートとして使用できるため、pingパケットのすべての5タプルは同じです。この出力で確認できるように、ASPドロップの理由は「inspect-icmp-seq-num-not-matched」です。

```
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-matc
```

Cisco Bug ID CSCvb92417



クラスタASAは、理由「inspect-icmp-seq-num-not-matched」でto-the-box ICMP応答をドロップする

ASPドロップの理由：

名前：inspect-icmp-seq-num-not-matched
ICMP Inspectシーケンス番号が一致しません。
　このカウンタは、ICMPエコー応答メッセージのシーケンス番号が、同じ接続で以前にアプライアンスを通過したICMPエコーメッセージと一致しない場合に増加します。

解決策：ICMPインスペクションを無効にします。クラスタ環境：クラスタ内の2つ以上のFTDとICMPトラフィックが非対称になる場合があります。ICMPフローの削除に遅延が見られます。後続のpingは、前のpingフローがクリーンアップされる前に高速で送信されます。この場合、連続

してpingパケットが失われる可能性があります。

SIPインスペクションドロップの例

このシナリオでは、コールが5分間継続しただけで、接続がドロップされます。RTPを使用すると、SIPインスペクションで接続をドロップできます。
VoIPトラフィックのインターフェイスでのパケットキャプチャの出力からわかるように、SIPトラフィックのBYEフラグは、その時点で電話コールが閉じられたことを意味します。

```
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) |
```

この他の例では、syslogに、PATを使用するマッピングされたIP、使用可能なポートが1つだけのIP、およびポート割り当てのためにSIPセッションが同じポートに固定されたSIPが表示されます。PATが使用中の場合、SIPインスペクションは接続をドロップできます。

ASPドロップの理由は、「ホストごとのPATポートブロック制限Xに達したため、IP/ポートからIP/ポートへのUDP接続を作成できない」および「インスペクションエンジンによる終了、理由 – 「サービスresetinboud」設定に基づくリセット」です。

```
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ドロップの理由：

名前：async-lock-queue-limit
非同期ロックキューの制限を超えました：
　各非同期ロックの作業キューには、1000という制限があります。作業キューにディスパッチするSIPパケットを増やすには、パケットをドロップする必要があります。
推奨事項：

ドロップできるのはSIPトラフィックだけです。SIPパケットに同じ親ロックがあり、それらが同じ非同期ロックキューにキューイングできる場合、すべてのメディアを処理しているのは単一のコアだけなので、ブロックの枯渇が発生する可能性があります。非同期ロックキューのサイズが制限を超えたときにSIPパケットがキューに入れられた場合、そのパケットはドロップされる必要があります。

名前：sp-looping-address
ループアドレス：
このカウンタは、フロー内の送信元アドレスと宛先アドレスが同じ場合に増加します。 アドレスプライバシーが有効になっているSIPフローは、送信元アドレスと宛先アドレスが同じであるのが通常であるため、除外されます。

推奨事項：
このカウンタが増加する場合は、2つの状況が考えられます。1つは、アプライアンスが宛先と同じ送信元アドレスを持つパケットを受信した場合です。これはDoS攻撃のタイプを表します。2つ目は、アプライアンスのNAT設定で、送信元アドレスが宛先のアドレスと同じになるようにNAT処理を行う場合です。

名前：parent-closed
親フローが閉じています：
下位フローの親フローがクローズされると、下位フローもクローズされます。 たとえば、FTPデータフロー（下位フロー）は、制御フロー（親フロー）が終了したときに、この特定の理由でクローズできます。 この理由は、制御アプリケーションによって二次フロー（ピンホール）が閉じられるときにも与えられます。 たとえば、BYEメッセージが受信されると、SIPインスペクションエンジン（制御アプリケーション）は対応するSIP RTPフロー（セカンダリフロー）を閉じる必要があります。

解決策：SIPインスペクションを無効にします。プロトコルの制限により：

- SIPインスペクションは、チャット機能のみをサポートしています。ホワイトボード、ファイル転送、およびアプリケーション共有はサポートされていません。RTC Client 5.0はサポートされていません。
- PATを使用する場合、ポートのない内部IPアドレスを含むSIPヘッダーフィールドは変換できないため、内部IPアドレスが外部にリークされる可能性があります。このリークを回避するには、PATの代わりにNATを設定します。
- SIPインスペクションは、次のようなデフォルトのインスペクションマップを使用してデフォルトで有効になっています。
  * SIPインスタントメッセージング(IM)拡張機能：有効。
  * SIPポートの非SIPトラフィック：ドロップ.
  * サーバーおよびエンドポイントのIPアドレスを非表示にする：無効。
  * マスクソフトウェアバージョンおよび非SIP URI：無効。
  * 宛先までのホップ数が0より大きいことを確認します：有効。
  * RTP準拠：適用されません。
  * SIP準拠：状態チェックとヘッダー検証を実行しません。

トラブルシュート

LINA MPFプロトコルインスペクションに関連するトラフィックの問題をトラブルシューティングするための推奨コマンドを次に示します。

- show service-policy：有効になっているLINA MPFインスペクションのサービスポリシー統計情報を表示します。

```
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
```

次の例はshow service-policy inspect httpコマンドの出力で、httpの統計情報を示しています。

```
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
```

- 検査するインターフェイス上のasp-dropキャプチャを設定します。

```
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
```

特定のLINA MPFアプリケーションインスペクションを有効または無効にする方法

Cisco Secure Firewall Threat DefenseでMPF LINAアプリケーションインスペクションを有効または無効にするには、次のオプションを使用できます。

- FlexConfigでの設定：FMC UIへの管理者アクセスが必要です。この変更は設定に永続的に適用されます。
- FTD CLIを使用した設定：FTD CLIへの管理者アクセスが必要です。この変更は永続的ではありません。リブートや新しい導入が行われると、設定は削除されます。

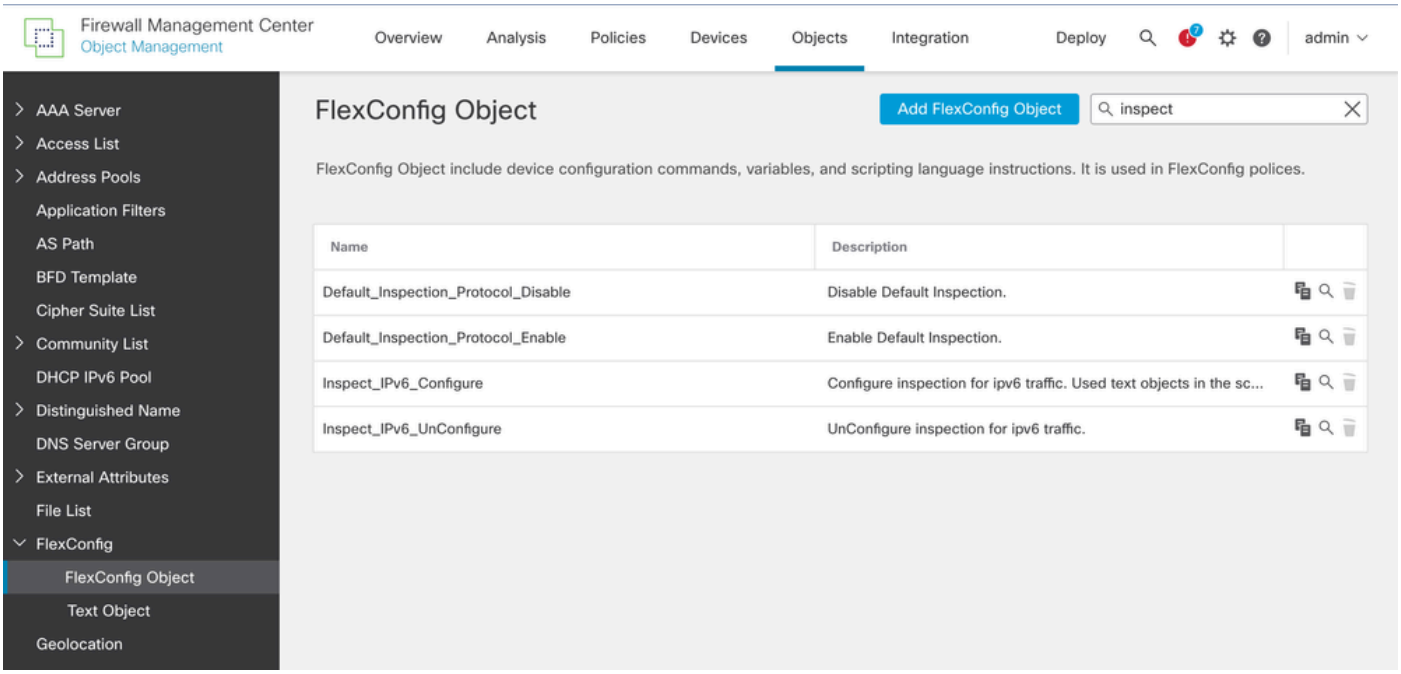
FlexConfigでの設定

FlexConfigは、脅威対策と互換性があるがmanagement centerで特に設定できないASAベースの機能を設定するための最後の手段です。

インスペクションを永続的に無効または有効にする設定は、FMC UIを介したFlexConfigで行います。これは、グローバルに、または特定のトラフィックに対してのみ適用できます。

ステップ 1：

FMCのUIで、Objects > Object Management > FlexConfig > FlexConfig Objectの順に移動すると、デフォルトのプロトコルインスペクションオブジェクトのリストが表示されます。



デフォルトのFlexConfigプロトコルインスペクションオブジェクト

ステップ 2：

特定のプロトコルインスペクションを無効にするには、FlexConfigオブジェクトを作成します。

Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Objectの順に選択します。

この例では、global_policyからSIPインスペクションを無効にする設定の構文は次のようにする必要があります。

```
policy-map global_policy
```

```
class inspection_default
 no inspect sip
```

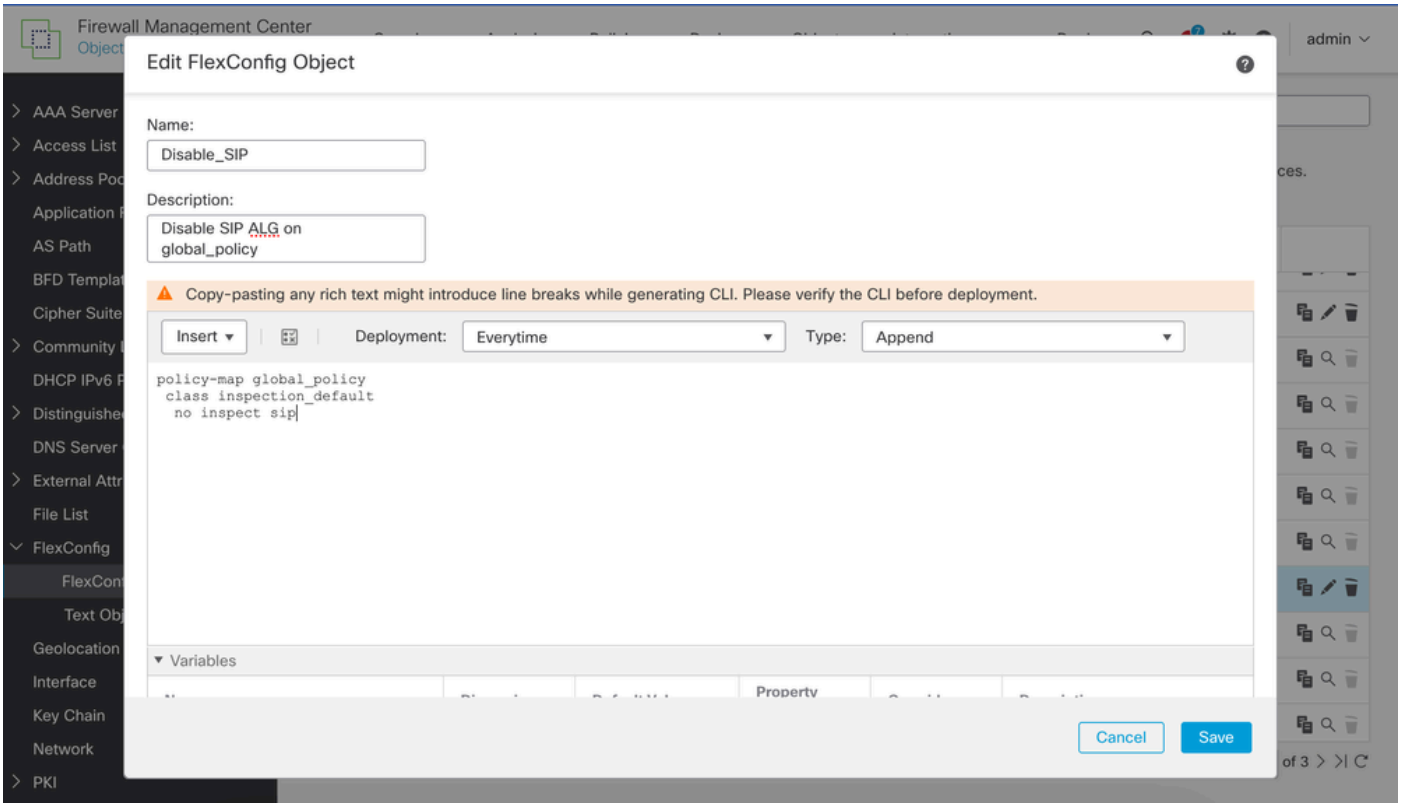
FlexConfigオブジェクトを構成する際に、展開の頻度と種類を選択できます。

導入

- FlexConfigオブジェクトがネットワークやACLオブジェクトなどのシステム管理オブジェクトを指している場合は、Everytimeを選択します。それ以外の場合、オブジェクトの更新を展開できませんでした。
- オブジェクト内で設定のクリアだけが行われる場合は、Onceを使用します。次に、次回の展開後にFlexConfigポリシーからオブジェクトを削除します。

Type

- Append（デフォルト）。 オブジェクト内のコマンドは、management centerポリシーから生成される設定の最後に配置されます。管理対象オブジェクトから生成されたオブジェクトを指すポリシー・オブジェクト変数を使用する場合は、「追加」を使用する必要があります。他のポリシー用に生成されたコマンドがオブジェクトで指定されたコマンドと重複する場合は、コマンドが上書きされないように、このオプションを選択する必要があります。これが最も安全なオプションです。
- プリペンド。 オブジェクト内のコマンドは、management centerポリシーから生成される設定の先頭に配置されます。通常、設定をクリアまたは無効にするコマンドには、prependを使用します。

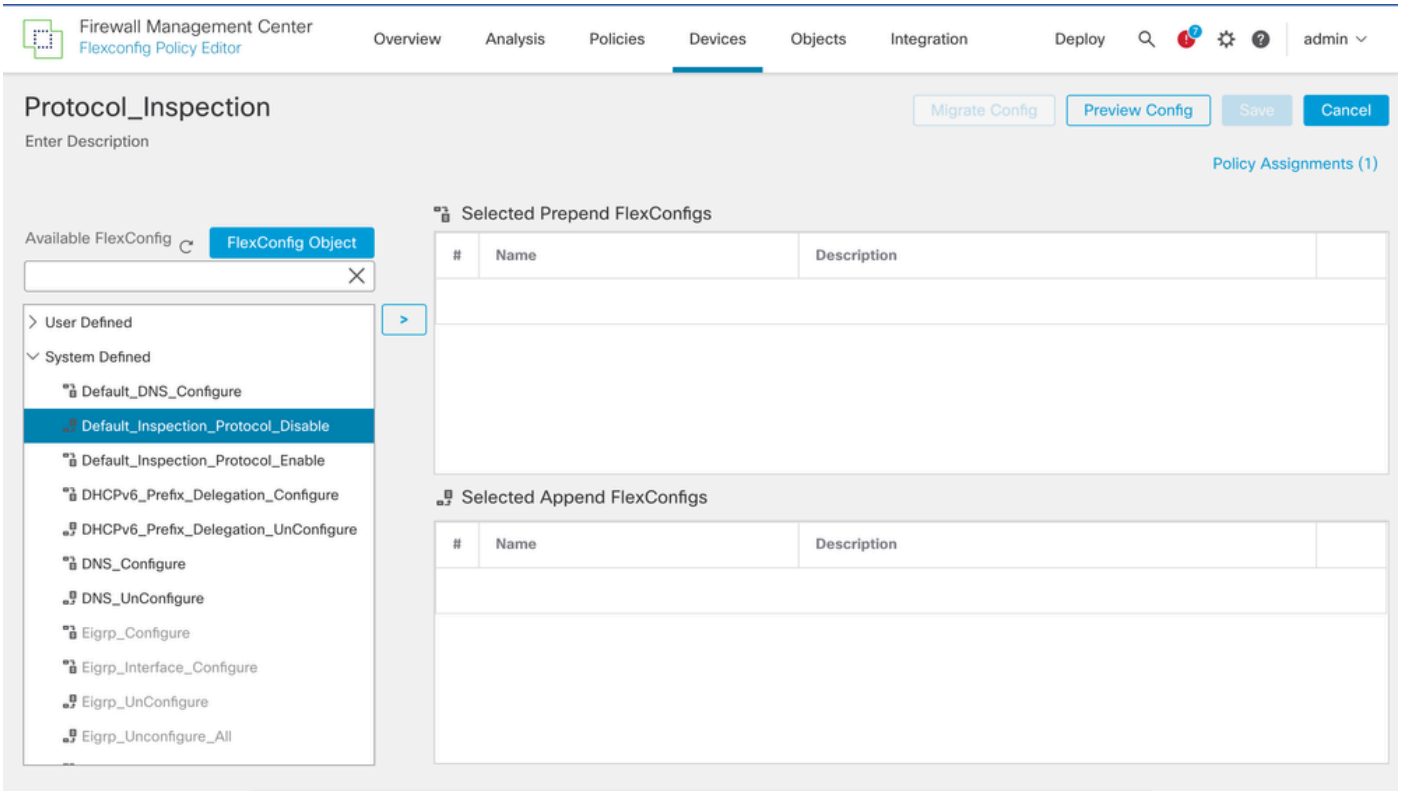


ステップ 3：

LINAに割り当てられたFlexConfigポリシーにオブジェクトを追加します。

Devices > FlexConfigに移動し、ドロップの問題が発生しているファイアウォールに適用されたFlexConfigポリシーを選択します。

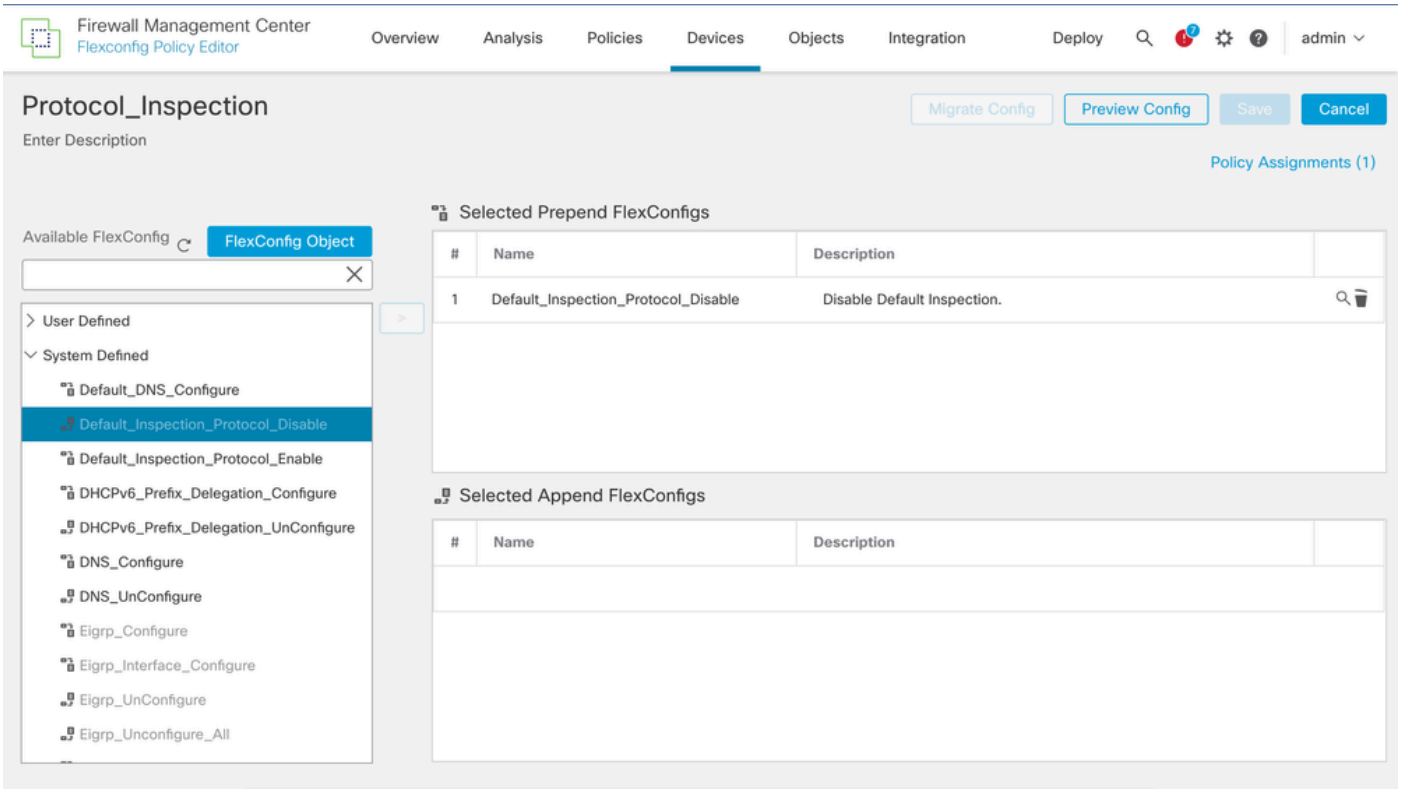
すべてのインスペクションをグローバルに無効にするには、システム定義FlexConfigオブジェクトの下でオブジェクトDefault_Inspection_Protocol_Disableを選択してから、その間の青い矢印をクリックしてFlexConfigポリシーに追加します。



すべてのプロトコルインスペクションを無効にするシステム定義オブジェクトの選択

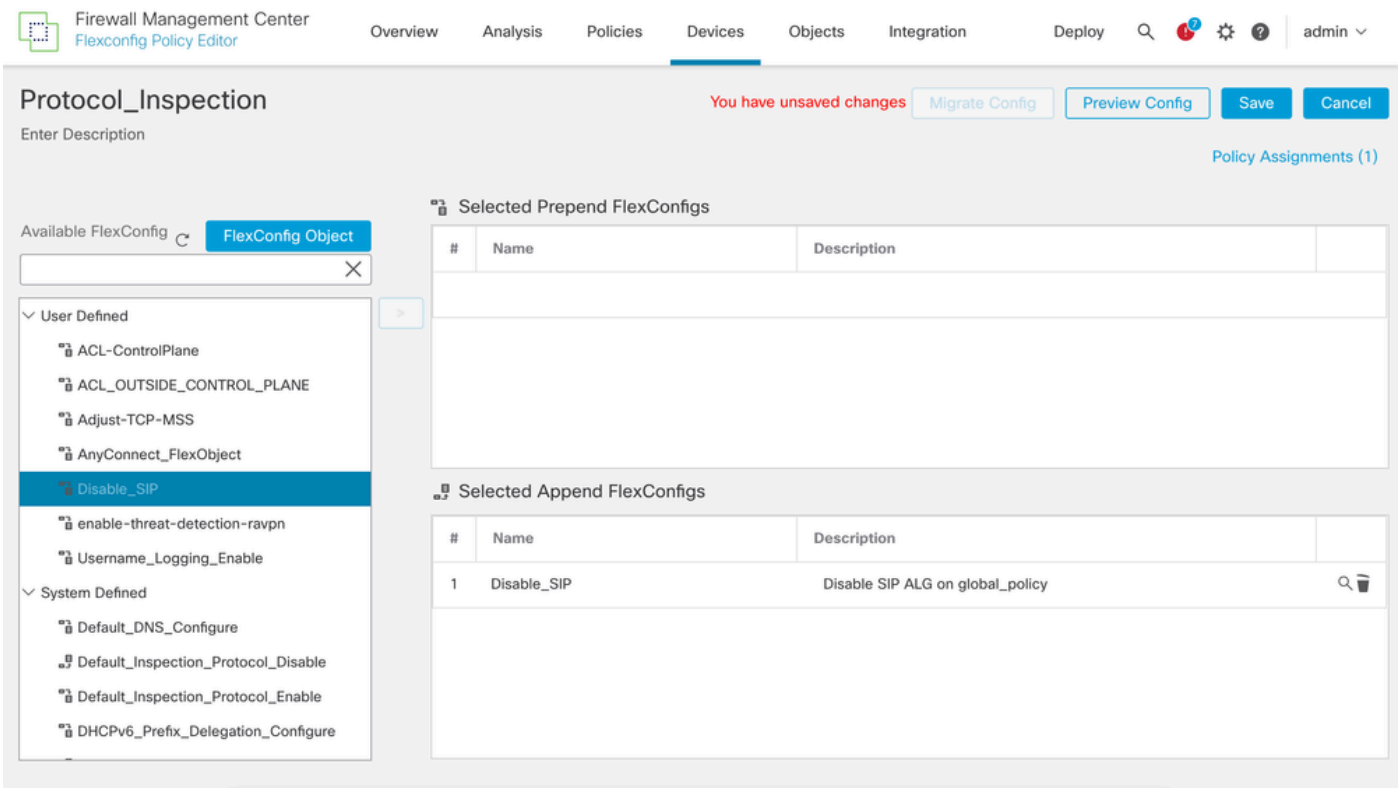
ステップ 4：

選択したら、それが右側のボックスに表示されることを確認します。設定を有効にするために、保存して展開することを忘れないでください。



すべてのプロトコルインスペクションを無効にするために選択したオブジェクト

ステップ 5：
単一のプロトコルインスペクションを無効にするには、前に作成したオブジェクトをユーザ定義リストから選択し、ボックス間の矢印を使用してポリシーに追加します。



global_policyからの単一プロトコルインスペクションを無効にする場合に選択します

手順 6：

選択したら、それが右側のボックスに表示されることを確認します。設定を有効にするために、保存して展開することを忘れないでください。

FTD CLIを使用した設定

このソリューションは、検査がトラフィックに影響しているかどうかをテストするために、FTD CLIからすぐに適用できます。ただし、リブートや新しい導入が発生しても、設定変更は保存されません。

このコマンドは、ClishモードでFTD CLIから実行する必要があります。

```
> configure inspection



        disable

for example
> configure inspection SIP disable
```

確認

プロトコルの無効化が有効であることを確認するには、show running-config policy-mapコマンドを実行します。この例では、SIPインスペクションはデフォルトのプロトコルリストに表示されなくなるため、無効になっています。

```
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#
```

関連情報

テクニカル サポートとドキュメント - Cisco Systems

- アプリケーション層プロトコルインスペクションの概要
- 基本的なインターネットプロトコルの検査
- Show ASP Dropコマンドの使用方法

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。