Dépanner les abandons de trafic dus à l'inspection du protocole LINA sur FTD

Table des matières

Introduction

Ce document décrit comment identifier si l'inspection de protocole LINA pour Modular Policy Framework (MPF), abandonne le trafic dans le Cisco Secure FTD.

Conditions préalables

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Threat Defense (FTD) virtuel, version 7.4.2
- Cisco Secure Firewall Manager Center (FMC) virtuel, version 7.4.2

The information in this document was created from the devices in a specific lab environment. Tous les dispositifs utilisés dans ce document ont démarré par une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les moteurs d'inspection sont requis dans un pare-feu pour les services qui intègrent des informations d'adressage IP dans le paquet de données utilisateur ou qui ouvrent des canaux secondaires sur des ports attribués dynamiquement.

L'inspection de protocole peut aider à empêcher le trafic malveillant d'entrer dans le réseau en inspectant le contenu des paquets réseau et en bloquant ou en modifiant le trafic en fonction de l'application ou du protocole utilisé.
Par conséquent, les plateformes d'inspection peuvent avoir une incidence sur le débit global. Plusieurs moteurs d'inspection courants sont activés sur le pare-feu par défaut, il peut être nécessaire d'en activer d'autres en fonction du réseau.

Configurations par défaut

Par défaut, la configuration FTD LINA inclut une stratégie qui correspond à tout le trafic d'inspection d'application par défaut.

L'inspection s'applique au trafic sur toutes les interfaces (une politique globale).

Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous pouvez seulement appliquer une stratégie globale, ainsi si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection aux ports non standard, ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut soit la désactiver et en appliquer une nouvelle.

Exécutez la commande show running-config policy-map sur LINA, FTD Command Line Interface (CLI) via le support système diagnostic-cli, pour obtenir les informations.

```
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
!
```

Identifier les pertes de paquets dues à l'inspection du protocole MPF

Même lorsque le trafic s'aligne sur la politique de contrôle d'accès (ACP) attribuée au pare-feu, dans certains scénarios, le processus d'inspection met fin aux connexions en raison d'un comportement de trafic spécifique reçu par le pare-feu, d'une conception non prise en charge, d'une norme d'application ou d'une limitation d'inspection.

Au cours du dépannage du trafic, un processus utile à utiliser est :

- Définissez des journaux de capture en temps réel sur les interfaces à partir desquelles le trafic circule (interfaces d’entrée et de sortie), commande :

```
firepower# capture

        [interface

        ][match

           [port

           ]
```

```
        [port

        ]]
```

À l'aide des captures, vous pouvez inclure l'option packet number X trace detail et elle doit fournir le résultat phase par phase de la connexion, comme le fait une commande packet-tracer, mais avec cette option vous vous assurez qu'il s'agit de trafic en temps réel.

```
firepower# show capture

      packet number X trace detail
```

- Définissez en temps réel Accelerated Security Path (ASP) Drop, le type de capture asp-drop affiche les paquets ou les connexions abandonnés par l'ASP, il y a une liste de raisons que vous pouvez trouver dans les liens associés du document, commande :

```
firepower# capture

      [type

      ] [interface

       ][match
```

```
[port

]

  [port

  ]]
```

Les abandons d'inspection de protocole peuvent être ignorés, comme un résultat allow peut être observé dans les phases packet-tracer. C'est pourquoi il est essentiel de toujours vérifier la raison de l'abandon à l'aide des journaux de capture en temps réel.

Messages d'erreur de rejet courants

La suppression ASP (Accelerated Security Path) est souvent utilisée à des fins de débogage pour aider à résoudre les problèmes réseau. La commande show asp drop est utilisée pour afficher ces paquets ou connexions abandonnés, fournissant des informations sur les raisons des abandons, qui peuvent inclure des problèmes tels que des échecs NAT, des échecs d'inspection ou des refus de règle d'accès.

Points clés sur les abandons ASP :

- Abandons de trame : Il s’agit de abandons liés à des paquets individuels, tels qu’une encapsulation non valide ou l’absence de route vers l’hôte.
- Abandons de flux : Elles sont liées aux connexions, telles que les flux refusés par les règles d'accès ou les échecs NAT.
- Utilisation : La commande est principalement destinée au débogage et le résultat peut

changer.

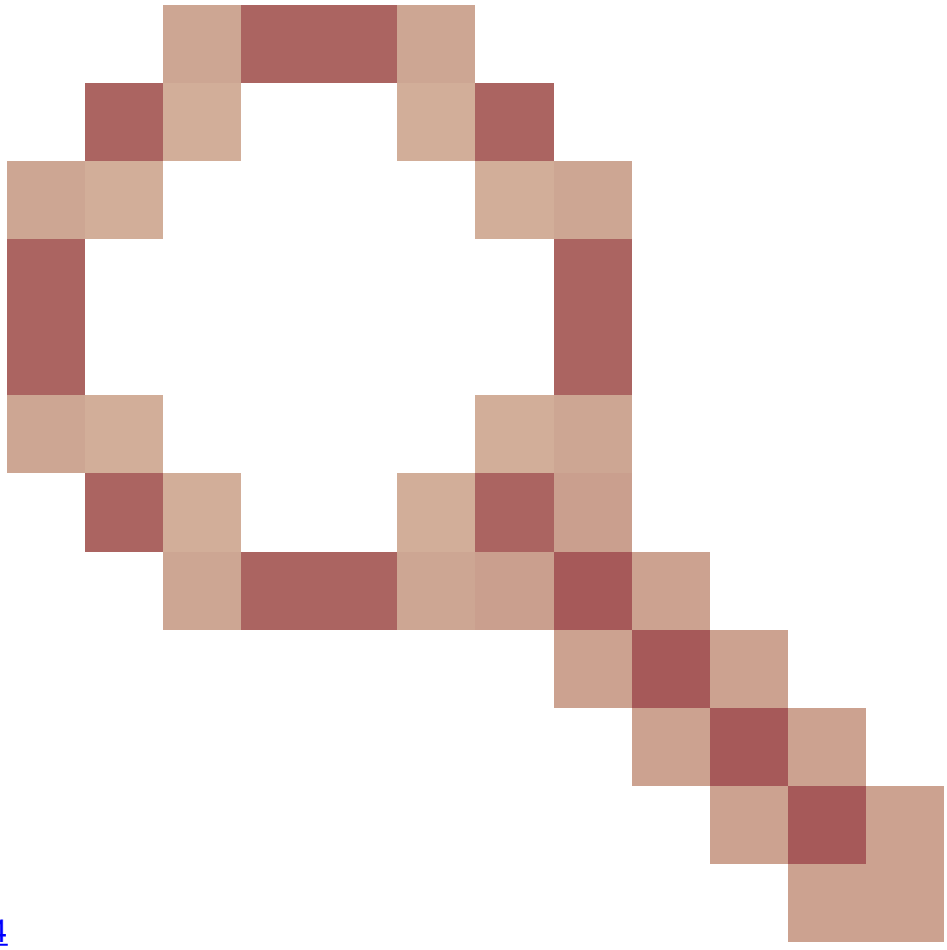
Ces messages d'erreur ou raisons d'abandon sont des exemples que vous pouvez rencontrer lors du dépannage. Ils peuvent différer en fonction du protocole d'inspection utilisé.

Exemple de suppression d'inspection RPC SUN

Ce scénario est pour un proxy FTDv à bras unique dans le déploiement AWS, le trafic RPC encapsulé par Geneve, si l'inspection Sun Rpc est activée, la connexion est abandonnée.

Le résultat montre des abandons ASP pour l'inspection Sun Rpc, Sun Rcp utilise le port 111 comme destination et le dernier paquet est le port d'encapsulation Geneve qui utilise 6081 comme destination. Comme vous pouvez le constater, la raison de l'abandon dans le résultat est « Aucune contiguïté valide »

```
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
```



ID de bogue Cisco [CSCwj00074]

Le proxy FTDv à bras unique abandonne le trafic sans contiguïté avec l'option inspecter sunrpc activée

Le trafic est abandonné en tant que « contiguïté non valide » dans l'ASP du moteur LINA, car les adresses MAC source et de destination sont soudainement remplies entièrement de zéros après le deuxième paquet (SYN/ACK) de la connexion en trois étapes.

Raison de la suppression ASP :

Name : non-contiguïté
Aucune contiguïté valide :
Ce compteur s'incrémente lorsque l'appliance de sécurité reçoit un paquet sur un flux existant qui n'a plus de contiguïté de sortie valide. Cela peut se produire si le saut suivant n'est plus accessible ou si une modification de routage s'est généralement produite dans un environnement de routage dynamique.

Solution : Désactivez l'inspection sunrpc.

Exemple de suppression d'inspection SQL*NET

Ce scénario est pour un proxy FTDv à bras unique dans le déploiement AWS, si l'inspection Sql*Nel est activée, le trafic encapsulé par Geneve est abandonné.

Le résultat est pour les captures de paquets fusionnées (vous pouvez observer le même numéro de paquet) :
Première ligne : Capture de paquets asp-drop non encapsulée, Sql*Net utilise le port 1521 comme destination.
Deuxième ligne : L'interface VNI asp-drop sur LINA, Geneve utilise le port d'encapsulation 6081 comme destination.

Il y a deux raisons différentes de suppression dans le résultat, comme vous pouvez le constater, ils sont "tcp-buffer-timeout" et "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
```

Raison de la suppression ASP :

Name : tcp-buffer-timeout
Délai d'expiration du tampon de paquets TCP en désordre :
Ce compteur est incrémenté et le paquet est abandonné lorsqu'un paquet TCP en file d'attente dans le désordre a été maintenu dans la mémoire tampon pendant trop longtemps.En général, les paquets TCP sont mis en ordre sur les connexions qui sont inspectées par l'appliance de sécurité ou lorsque les paquets sont envoyés au SSM pour inspection. Lorsque le prochain paquet TCP attendu n'arrive pas dans un certain délai, le paquet en panne mis en file d'attente est abandonné.

Recommandations:
Le prochain paquet TCP attendu n'arrive pas en raison d'un encombrement du réseau normal dans un réseau occupé. Le mécanisme de retransmission TCP de l'hôte final doit retransmettre le paquet et la session peut se poursuivre.

Name : tcp-not-syn
Premier paquet TCP non SYN :
A reçu un paquet non SYN comme premier paquet d'une connexion non interceptée et non clouée.

Recommandation :
Dans des conditions normales, ceci peut être observé lorsque l'appliance a déjà fermé une connexion et que le client ou le serveur croit toujours que la connexion est ouverte et continue à transmettre des données. Dans certains cas, cela peut se produire juste après l'émission d'une commande « clear local-host » ou « clear xlate ». En outre, si les connexions n'ont pas été récemment supprimées et que le compteur s'incrémente rapidement, la solution matérielle-logicielle peut être attaquée. Capturez une trace de l'analyseur pour identifier la cause.

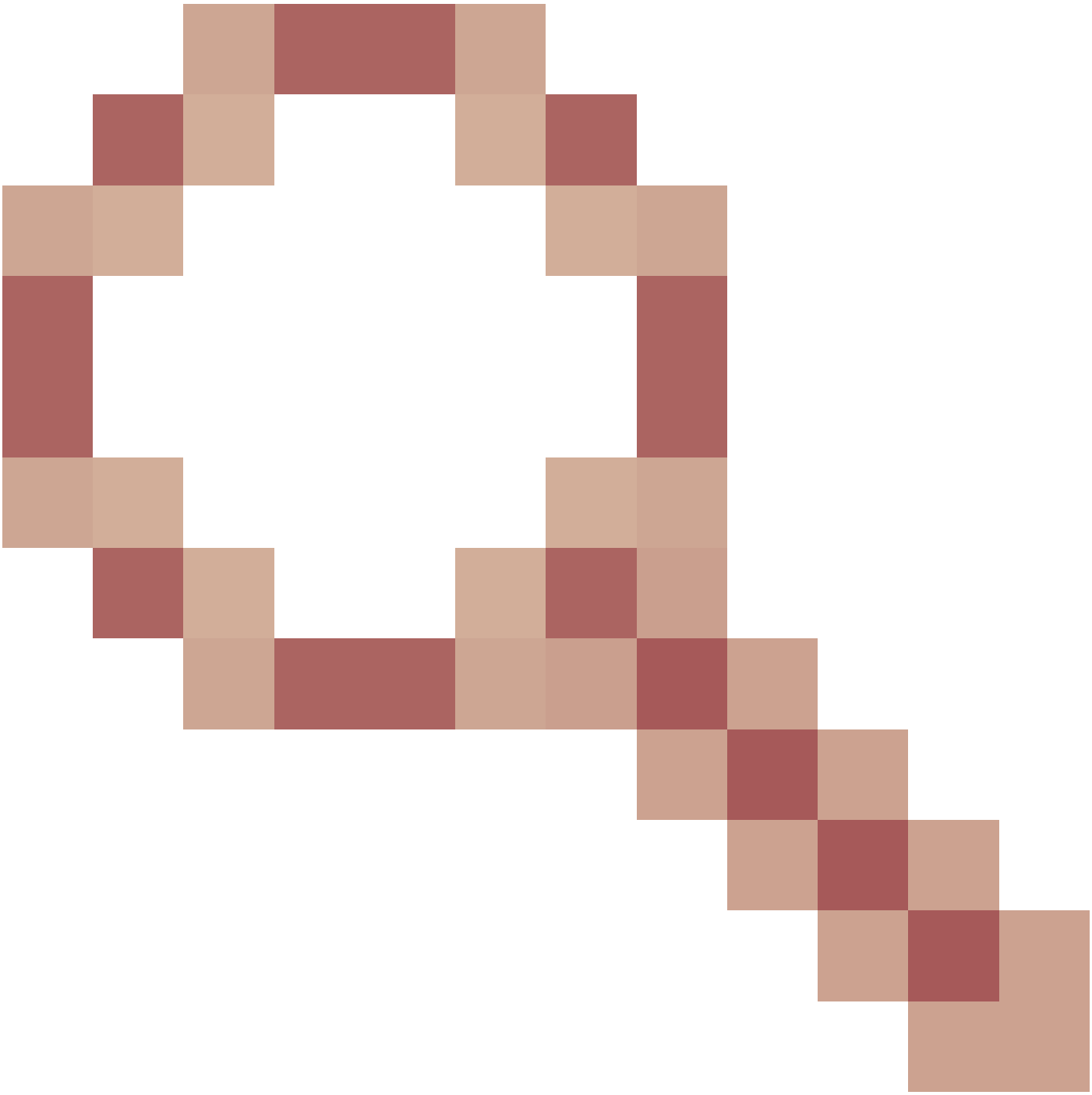
Solution : Désactivez l'inspection SQL*Net lorsque le transfert de données SQL s'effectue sur le même port que le port TCP 1521 du contrôle SQL. L'appliance de sécurité agit en tant que proxy lorsque l'inspection SQL*Net est activée et réduit la taille de la fenêtre du client de 65000 à environ 16000, ce qui entraîne des problèmes de transfert de données.

Exemple de suppression d'inspection ICMP

Ce scénario concerne un environnement de cluster FTD.
L'identificateur ICMP de l'en-tête ICMP peut être utilisé comme port source du 5-tuple dans le flux, de sorte que tous les 5-tuple des paquets ping sont les mêmes, la raison d'abandon ASP est "inspect-icmp-seq-num-not-match" comme vous pouvez l'observer dans cette sortie.

```
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
```

ID de débogage Cisco CSCvb92417



L'ASA de cluster abandonne les réponses ICMP prêtes à l'emploi avec la raison « inspect-icmp-seq-num-not-match »

Raison de la suppression ASP :

Name : inspect-icmp-seq-num-not-match
Le numéro de série d'inspection ICMP ne correspond pas :
Ce compteur doit s'incrémenter lorsque le numéro d'ordre du message de réponse d'écho ICMP ne correspond à aucun message d'écho ICMP transmis précédemment à travers l'appliance sur la même connexion.

Solution : Désactivez l'inspection ICMP. Dans un environnement de cluster : deux ou plusieurs FTD dans le cluster et le trafic ICMP peuvent être asymétriques. On observe qu'il y a un délai pour

la suppression du flux ICMP, la requête ping suivante est envoyée rapidement avant que le flux ping précédent ait été nettoyé. Dans ce cas, des paquets ping consécutifs peuvent être perdus.

Exemple de perte d'inspection SIP

Dans ce scénario, les appels n'ont duré que cinq minutes, puis la connexion est interrompue. Lorsque RTP est utilisé, l'inspection SIP peut interrompre les connexions.
Comme vous pouvez l'observer dans la sortie de capture de paquets sur l'interface pour le trafic VoIP, l'indicateur BYE dans le trafic SIP signifie que l'appel téléphonique est fermé à ce moment-là.

```
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) |
```

Dans cet autre exemple, le syslog montre une adresse IP mappée qui utilise la PAT, l'adresse IP est laissée avec un seul port disponible et la session SIP a atterri sur le même port, SIP a échoué en raison de l'allocation de port. Si la PAT est utilisée, l'inspection SIP peut interrompre la connexion.

La raison de l'abandon ASP est : "Impossible de créer une connexion UDP d'IP/port à IP/port en raison de l'atteinte de la limite de bloc de port PAT par hôte de X" et "terminé par le moteur d'inspection, raison - réinitialisation basée sur la configuration 'service resetinbound'"

```
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
```

Raison de la suppression ASP :

Name : async-lock-queue-limit
Limite de file d'attente de verrouillage asynchrone dépassée :

Chaque file d'attente de travail de verrouillage asynchrone a une limite de 1000. Lorsque d'autres paquets SIP sont tentés d'être expédiés vers la file d'attente de travail, le paquet doit être abandonné.
Recommandation :
Seul le trafic SIP peut être abandonné. Lorsque les paquets SIP ont le même verrou parent et qu'ils peuvent être mis en file d'attente dans la même file d'attente de verrou asynchrone, cela peut entraîner une déplétion des blocs, car un seul coeur gère tous les supports. Si un paquet SIP tente d'être mis en file d'attente lorsque la taille de la file d'attente de verrouillage asynchrone dépasse la limite, le paquet doit être abandonné.

Name : sp-looping-address
adresse de bouclage :
Ce compteur est incrémenté lorsque les adresses source et de destination d'un flux sont identiques. Les flux SIP pour lesquels la confidentialité des adresses est activée sont exclus, car il est normal que ces flux aient les mêmes adresses source et de destination.

Recommandation :
Il existe deux conditions possibles dans lesquelles ce compteur peut s'incrémenter. L'un est lorsque l'appliance reçoit un paquet dont l'adresse source est égale à celle de la destination. Il s'agit d'un type d'attaque DoS. La seconde est lorsque la configuration NAT de l'appliance NAT a une adresse source égale à celle de la destination.

Name : fermé par ses parents
Le flux parent est fermé :
Lorsque le flux parent d'un flux subordonné est fermé, le flux subordonné l'est également. Par exemple, un flux de données FTP (flux subordonné) peut être fermé pour cette raison spécifique lorsque son flux de contrôle (flux parent) est terminé. Cette raison est également donnée lorsqu'un flux secondaire (goupille) est fermé par son application de commande. Par exemple, lorsque le message BYE est reçu, le moteur d'inspection SIP (application de contrôle) doit fermer les flux RTP SIP correspondants (flux secondaire).

Solution : Désactivez l'inspection SIP. En raison des limitations du protocole :

- L'inspection SIP prend uniquement en charge la fonctionnalité de conversation. Le tableau blanc, le transfert de fichiers et le partage d'applications ne sont pas pris en charge. RTC Client 5.0 n'est pas pris en charge.
- Lors de l'utilisation de la PAT, tout champ d'en-tête SIP contenant une adresse IP interne sans port ne peut pas être traduit et par conséquent l'adresse IP interne peut être divulguée à l'extérieur. Si vous voulez éviter cette fuite, configurez NAT au lieu de PAT.
- L'inspection SIP est activée par défaut à l'aide de la carte d'inspection par défaut, qui comprend :
  * Extensions de messagerie instantanée (IM) SIP : Activée.
  * Trafic non SIP sur le port SIP : Abandonné.
  * Masquer les adresses IP des serveurs et des terminaux : Désactivé.
  * Version du logiciel de masque et URI non SIP : Désactivé.
  * Assurez-vous que le nombre de sauts vers la destination est supérieur à 0 : Activée.

* Conformité RTP : Non appliqué.
* Conformité SIP : Ne pas effectuer de contrôle d'état et de validation d'en-tête.

Dépannage

Voici quelques-unes des commandes suggérées pour dépanner les problèmes de trafic liés à l'inspection du protocole MPF LINA.

- Show service-policy affiche les statistiques de politique de service pour les inspections MPF LINA activées.

```
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
```

Cet exemple de sortie de la commande show service-policy inspect http montre les statistiques http :

```
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
```

- Définissez une capture asp-drop sur l'interface à inspecter.

```
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
```

Activation ou désactivation d'inspections d'applications MPF LINA spécifiques

Il s'agit des options disponibles pour activer ou désactiver les inspections d'applications LINA MPF dans Cisco Secure Firewall Threat Defense.

- Configuration sur FlexConfig : Vous avez besoin d'un accès administrateur à l'interface utilisateur FMC, cette modification est permanente sur la configuration.
- Configuration sur CLI FTD : Vous avez besoin d'un accès administrateur à l'interface de ligne de commande FTD, cette modification n'est pas permanente, si un redémarrage ou un nouveau déploiement a lieu, la configuration est supprimée.

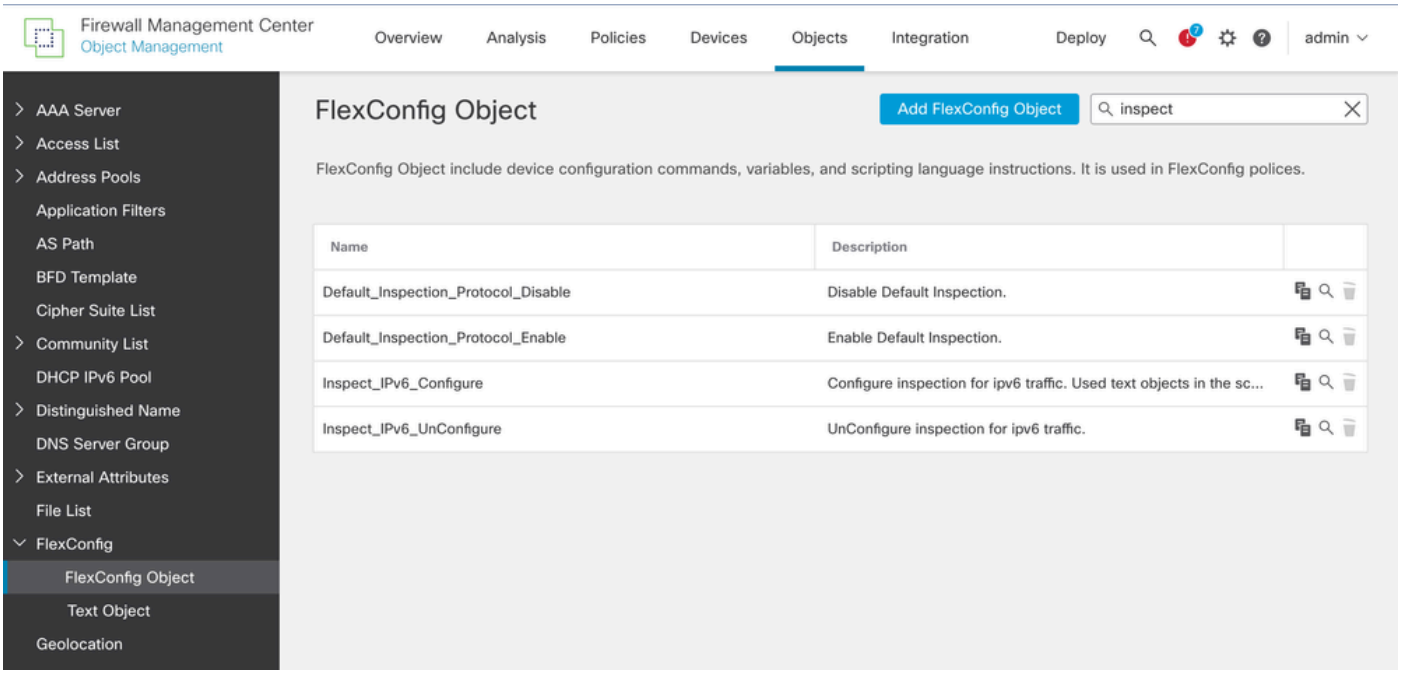
Configuration sur FlexConfig

FlexConfig est une méthode de dernier recours pour configurer des fonctionnalités basées sur ASA qui sont compatibles avec la défense contre les menaces mais qui ne sont pas configurables dans le centre de gestion.

La configuration pour désactiver ou activer l'inspection de manière permanente est sur FlexConfig sur l'interface utilisateur FMC, elle peut être appliquée globalement ou pour un trafic spécifique seulement.

Étape 1.

Dans l'interface utilisateur de FMC, accédez à Objets > Gestion des objets > FlexConfig > FlexConfig Object, là vous pouvez trouver la liste des objets d'inspection de protocole par défaut.



Objets d'inspection du protocole FlexConfig par défaut

Étape 2.

Pour désactiver une inspection de protocole spécifique, vous pouvez créer un objet FlexConfig.

Accédez à Objets > Gestion des objets > FlexConfig > Objet FlexConfig > Ajouter un objet FlexConfig

Dans cet exemple, la configuration pour désactiver l'inspection SIP de la politique globale, la syntaxe doit être :

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

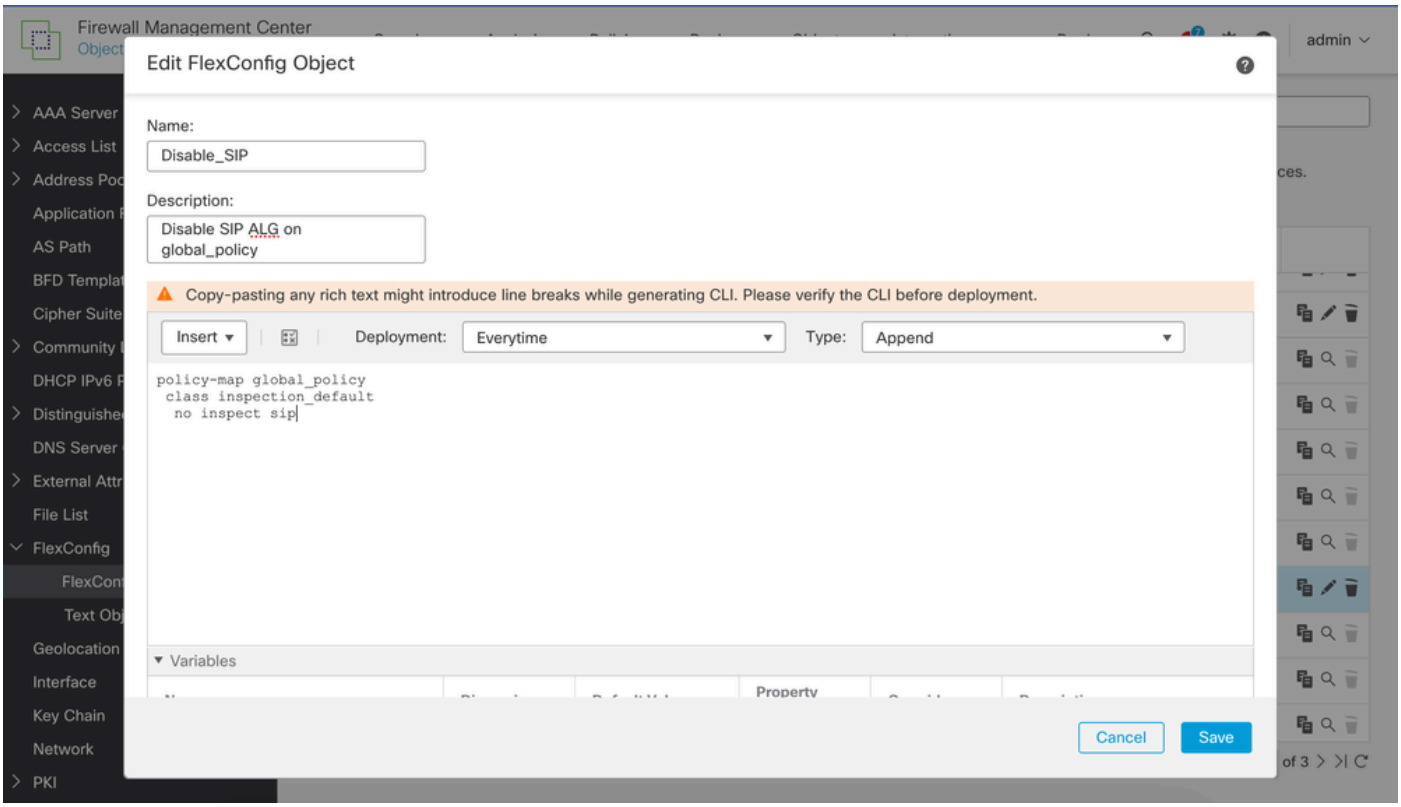
Lors de la configuration d'un objet FlexConfig, vous pouvez choisir la fréquence et le type de déploiement.

Déploiement

- Si l'objet FlexConfig pointe vers des objets gérés par le système tels que des objets réseau ou ACL, choisissez Everytime. Sinon, les mises à jour des objets ne peuvent pas être déployées.
- Utilisez Once si la seule chose que vous faites dans l'objet est d'effacer une configuration. Supprimez ensuite l'objet de la stratégie FlexConfig après le déploiement suivant.

Type

- Append (valeur par défaut). Les commandes de l'objet sont placées à la fin des configurations générées à partir des politiques du centre de gestion. Vous devez utiliser Append si vous utilisez des variables d'objet de stratégie, qui pointent vers des objets générés à partir d'objets gérés. Si les commandes générées pour d'autres stratégies chevauchent celles spécifiées dans l'objet, vous devez sélectionner cette option afin que vos commandes ne soient pas remplacées. C'est l'option la plus sûre.
- Préfixe. Les commandes de l'objet sont placées au début des configurations générées à partir des stratégies du centre de gestion. Vous utiliserez généralement prepend pour les commandes qui effacent ou annulent une configuration.



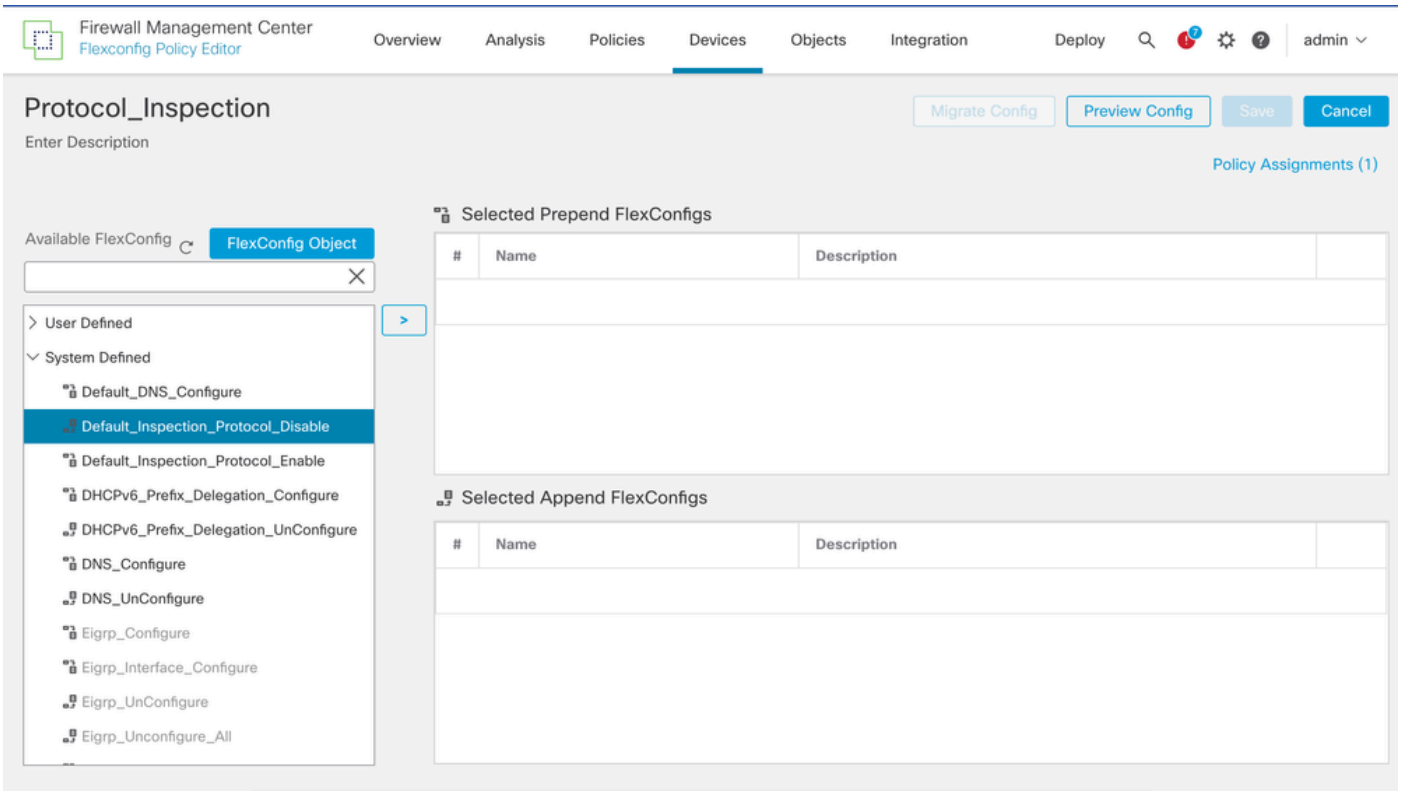
Créer un objet pour désactiver un seul protocole de la politique globale par défaut

Étape 3.

Ajoutez les objets de la stratégie FlexConfig affectés à LINA.

Accédez à Devices > FlexConfig et sélectionnez la stratégie FlexConfig appliquée au pare-feu avec des problèmes de suppression.

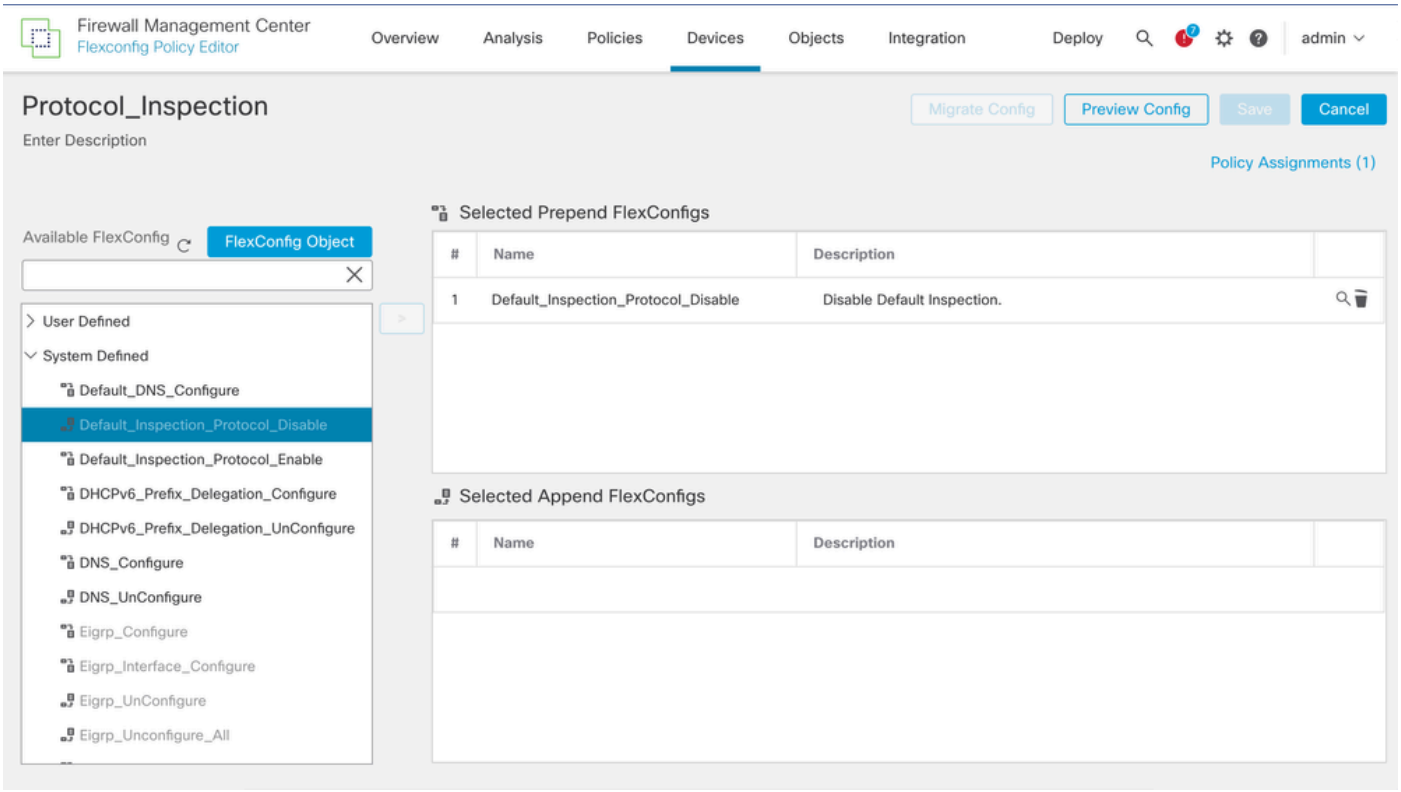
Pour désactiver l'inspection globalement, sélectionnez l'objet Default_Inspection_Protocol_Disable sous System Defined FlexConfig Objects, puis cliquez sur la flèche bleue entre les deux pour l'ajouter à la politique FlexConfig.



Sélectionnez l'objet défini par le système pour désactiver toutes les inspections de protocole

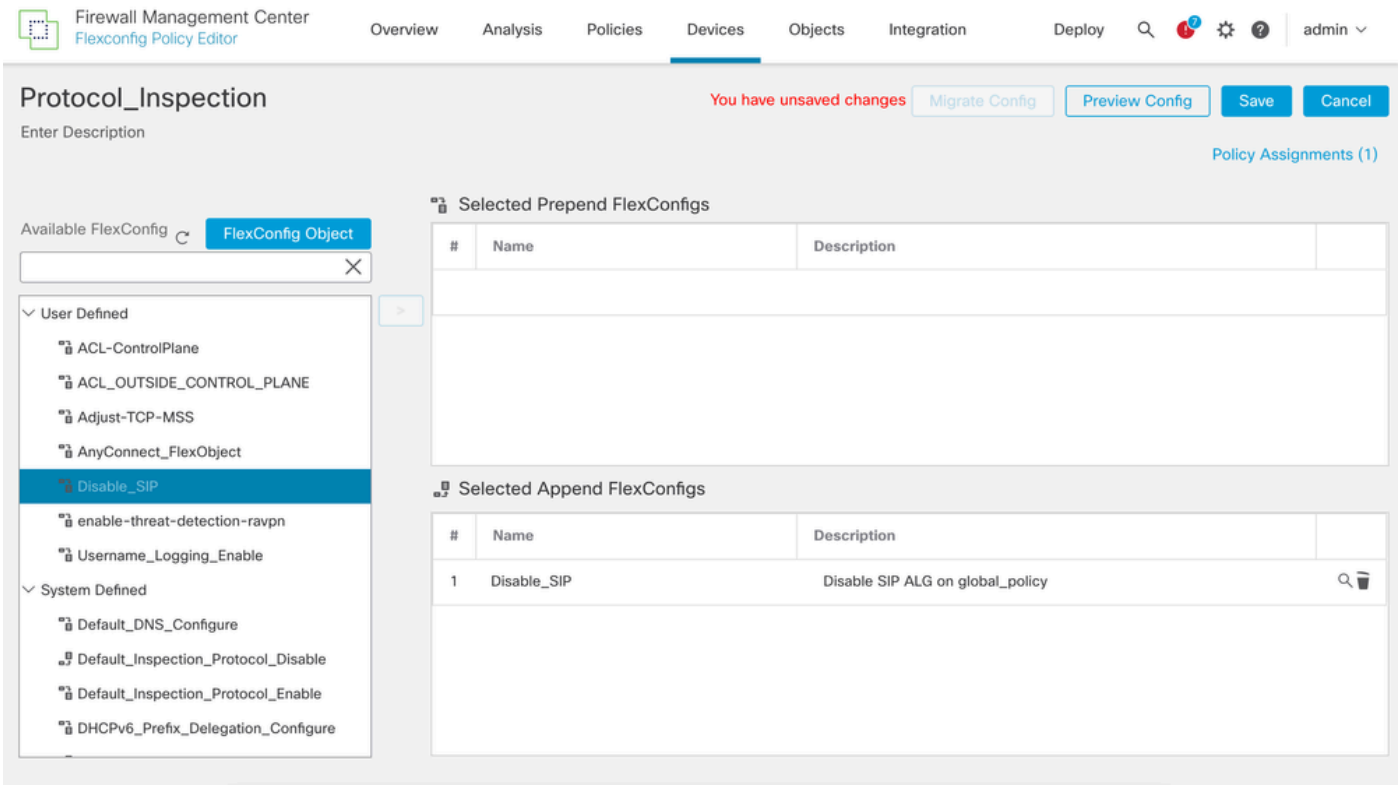
Étape 4.

Une fois sélectionné, confirmez qu'il apparaît dans les bonnes boîtes, n'oubliez pas d'enregistrer et de déployer la configuration pour prendre effet.



Objet sélectionné pour désactiver toutes les inspections de protocole

Étape 5.
Pour désactiver une inspection de protocole unique, sélectionnez l'objet précédemment créé dans la liste définie par l'utilisateur et ajoutez-le à la stratégie à l'aide de la flèche située entre les zones.



Sélectionnez cette option pour désactiver une inspection de protocole unique à partir de la politique globale

Étape 6.

Une fois sélectionné, confirmez qu'il apparaît dans les bonnes boîtes, n'oubliez pas d'enregistrer et de déployer la configuration pour prendre effet.

Configuration à l'aide de FTD CLI

Cette solution peut être appliquée immédiatement à partir de l'interface de ligne de commande FTD pour tester si l'inspection affecte le trafic. Toutefois, la modification de configuration n'est pas enregistrée en cas de redémarrage ou de nouveau déploiement.

La commande doit être exécutée à partir de l'interface de ligne de commande FTD en mode Clish.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Vérifier

Pour vérifier que la désactivation du protocole est effective, exécutez la commande show running-config policy-map. Dans cet exemple, l'inspection SIP est désactivée car elle n'apparaît plus dans la liste des protocoles par défaut.

```
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#
```

Informations connexes

Assistance et documentation techniques - Cisco Systems

- Mise en route de l’inspection du protocole de couche application
- Inspection des protocoles Internet de base
- Utilisation de la commande show ASP Drop

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.