Risoluzione dei problemi di perdita di traffico a causa dell'ispezione del protocollo LINA su FTD

Sommario

- Introduzione
- Prerequisiti
  - Componenti usati
- Premesse
  - Configurazioni predefinite
- Identificazione delle perdite di pacchetti causate dall'ispezione del protocollo MPF
  - Messaggi di errore comuni da eliminare
    - Esempio di drop di ispezione RPC SUN
    - Esempio di eliminazione di SQL*NET Inspection
    - Esempio di eliminazione di un'ispezione ICMP
    - Esempio di rilascio per ispezione SIP
- Risoluzione dei problemi
- Come abilitare o disabilitare le ispezioni specifiche dell'applicazione LINA MPF
  - Configurazione su FlexConfig
  - Configurazione con la CLI FTD
- Verifica
- Informazioni correlate

Introduzione

Questo documento descrive come identificare se l'ispezione del protocollo LINA per Modular Policy Framework (MPF), scarta il traffico nell'FTD Cisco Secure.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

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

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

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

Premesse

I motori di ispezione sono richiesti in un firewall per i servizi che incorporano le informazioni sull'indirizzo IP nel pacchetto dati dell'utente o che aprono i canali secondari sulle porte assegnate dinamicamente.

L'ispezione del protocollo può contribuire a impedire l'ingresso di traffico dannoso nella rete ispezionando il contenuto dei pacchetti di rete e bloccando o modificando il traffico in base all'applicazione o al protocollo in uso.
Di conseguenza, i motori di ispezione possono influire sul throughput complessivo. Diversi motori di ispezione comuni sono abilitati sul firewall per impostazione predefinita, può essere necessario abilitarne altri a seconda della rete.

Configurazioni predefinite

Per impostazione predefinita, la configurazione LINA FTD include una policy che corrisponde a tutto il traffico di ispezione dell'applicazione predefinito.

L'ispezione si applica al traffico su tutte le interfacce (una politica globale).

Il traffico di ispezione delle applicazioni predefinito include il traffico verso le porte predefinite per ogni protocollo. È possibile applicare un solo criterio globale, pertanto se si desidera modificare il criterio globale, ad esempio per applicare l'ispezione a porte non standard o per aggiungere ispezioni non abilitate per impostazione predefinita, è necessario modificare il criterio predefinito oppure disabilitarlo e applicarne uno nuovo.

Per ottenere le informazioni, eseguire il comando show running-config policy-map su LINA, FTD Command Line Interface (CLI) tramite system support diagnostic-cli.

```
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
!
```

Identificazione delle perdite di pacchetti causate dall'ispezione del protocollo MPF

Anche quando il traffico è in linea con i criteri di controllo di accesso (ACP, Access Control Policy) assegnati al firewall, in alcuni scenari il processo di ispezione interrompe le connessioni a causa di uno specifico comportamento del traffico ricevuto dal firewall, di una progettazione non supportata, di uno standard di applicazione o di una limitazione relativa all'ispezione.

Durante la risoluzione dei problemi relativi al traffico, è utile eseguire una delle seguenti operazioni:

- Impostare i log di acquisizione in tempo reale sulle interfacce da cui scorre il traffico (interfacce in entrata e in uscita), con il comando:

```
firepower# capture

        [interface

        ][match



           [port
```

```
          ]

            [port

            ]]
```

Usando le acquisizioni, è possibile includere l'opzione packet number X trace detail e fornire il risultato fase per fase della connessione, come fa un comando packet-tracer, ma con questa opzione si assicura che si tratti di traffico in tempo reale.

```
firepower# show capture

        packet number X trace detail
```

- Set real-time Accelerated Security Path (ASP) Drop, il tipo di acquisizione asp-drop mostra i pacchetti o le connessioni scartate da ASP, c'è un elenco di motivi che si possono trovare nei collegamenti correlati del documento, comando:

```
firepower# capture

        [type

        ] [interface
```

```
][match


   [port

   ]


     [port

     ]]
```

Le cadute dall'ispezione del protocollo possono essere ignorate, in quanto il risultato consentito può essere osservato nelle fasi di tracciamento dei pacchetti. Per questo motivo, è fondamentale verificare sempre il motivo della perdita utilizzando i log di acquisizione in tempo reale.

Messaggi di errore comuni da eliminare

L'eliminazione del percorso di protezione accelerata (ASP) viene spesso utilizzata a scopo di debug per facilitare la risoluzione dei problemi di rete. Il comando show asp drop viene usato per visualizzare i pacchetti o le connessioni ignorati, fornendo informazioni sui motivi delle perdite, che possono includere problemi come errori NAT, errori di ispezione o rifiuti delle regole di accesso.

Punti chiave sulle interruzioni ASP:

- Perdite di fotogrammi: Si tratta di perdite relative a singoli pacchetti, ad esempio incapsulamento non valido o nessuna route verso l'host.
- Perdite di flusso: Sono correlate alle connessioni, ad esempio flussi negati da regole di accesso o errori NAT.

- Utilizzo: Il comando viene utilizzato principalmente per il debug e l'output può variare.

Questi messaggi di errore o motivi di eliminazione sono esempi che si possono verificare durante la risoluzione dei problemi. Possono differire a seconda del protocollo di ispezione utilizzato.

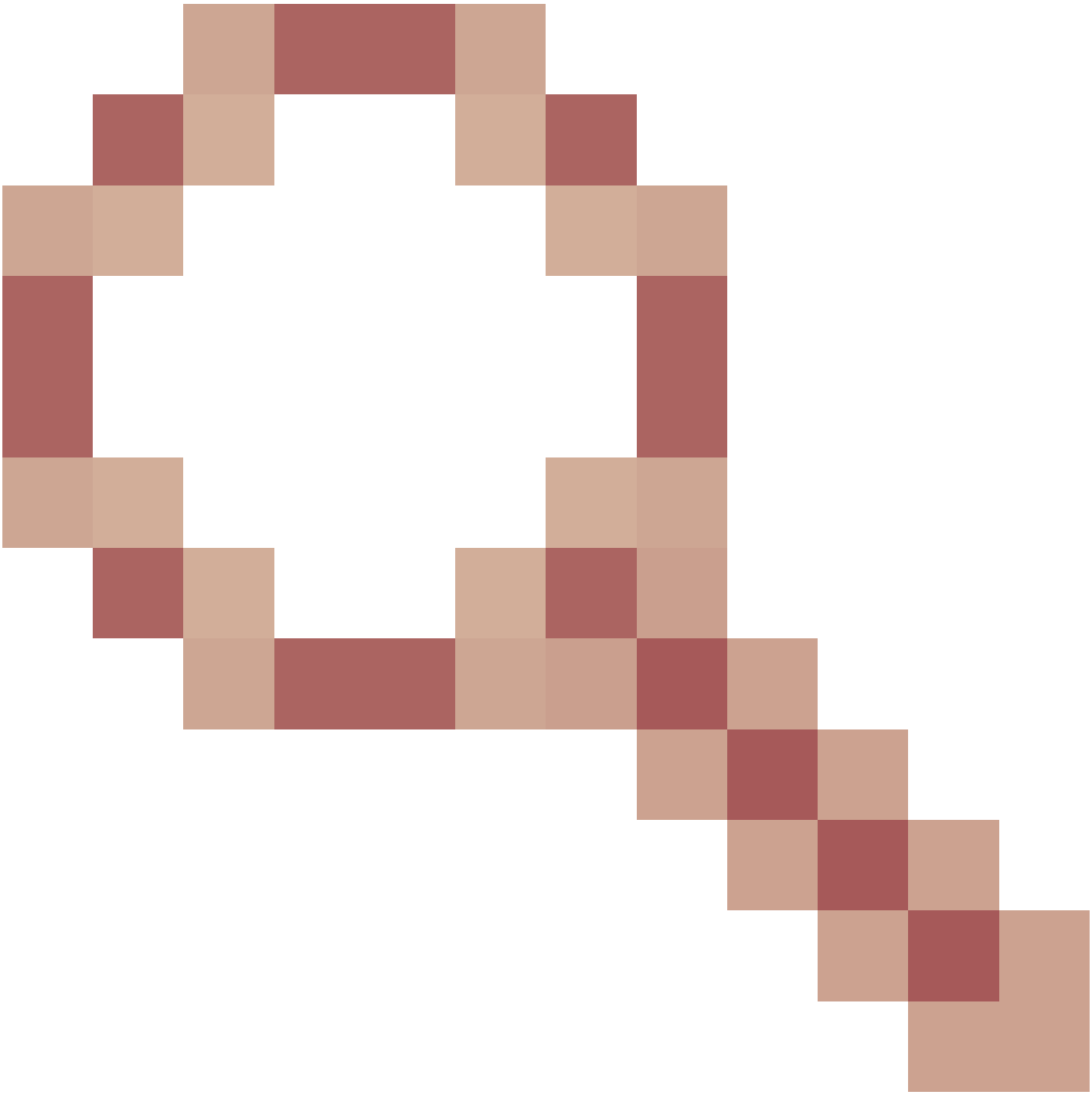
Esempio di drop di ispezione RPC SUN

Questo scenario riguarda un proxy FTDv a braccio singolo nella distribuzione AWS, traffico RPC incapsulato da Geneve, se l'ispezione Rpc Sun è abilitata la connessione viene interrotta.

L'output mostra le cadute ASP per l'ispezione di Sun Rpc, Sun Rcp utilizza la porta 111 come destinazione. L'ultimo pacchetto è la porta di incapsulamento Geneve, che utilizza 6081 come destinazione. Il motivo di caduta nell'output come si può osservare è "Nessuna adiacenza valida"

```
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 bug Cisco CSCwj0074



[Il proxy FTDv a braccio singolo interrompe il traffico senza adiacenze con l'opzione inspect sunrpc abilitata]

Il traffico viene scartato come 'adiacenza non valida' nell'ASP del motore LINA perché gli indirizzi MAC di origine e destinazione vengono improvvisamente popolati tutti in zero dopo il secondo pacchetto (SYN/ACK) dell'handshake a 3 vie.

Motivo eliminazione ASP:

Nome: non adiacenza
Nessuna adiacenza valida:
Questo contatore viene incrementato quando l'accessorio di sicurezza riceve un pacchetto in un

flusso esistente che non ha più una adiacenza di output valida. Questa condizione si può verificare se l'hop successivo non è più raggiungibile o se una modifica del routing si è verificata in genere in un ambiente di routing dinamico.

Soluzione: Disabilita ispezione sunrpc.

Esempio di eliminazione di SQL*NET Inspection

Questo scenario si riferisce a un proxy FTDv a braccio singolo nella distribuzione AWS; se l'ispezione Sql*Nel è abilitata, il traffico incapsulato da Geneve viene scartato.

L'output viene generato per le acquisizioni di pacchetti unite (è possibile osservare lo stesso numero di pacchetto):
Prima riga: L'acquisizione dei pacchetti asp-drop non è incapsulata. Sql*Net utilizza la porta 1521 come destinazione.
Seconda riga: VNI interface asp-drop su LINA, Geneve usa la porta di incapsulamento 6081 come destinazione.

L'output ha due diverse cause di perdita, come si può notare, sono "tcp-buffer-timeout" e "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
```

Motivo eliminazione ASP:

Nome: tcp-buffer-timeout
Timeout buffer pacchetti TCP non in ordine:
Questo contatore viene incrementato e il pacchetto viene scartato quando un pacchetto TCP fuori coda è stato mantenuto nel buffer troppo a lungo. In genere, i pacchetti TCP vengono ordinati sulle connessioni ispezionate dall'appliance di sicurezza o quando i pacchetti vengono inviati all'SSM per l'ispezione. Quando il successivo pacchetto TCP previsto non arriva entro un certo periodo, il pacchetto non in ordine inserito in coda viene scartato.

Consigli:
Il successivo pacchetto TCP previsto non arriva a causa di una congestione della rete normale in una rete occupata. Il meccanismo di ritrasmissione TCP nell'host finale deve ritrasmettere il pacchetto e la sessione può continuare.

Nome: tcp-not-syn
Primo pacchetto TCP non SYN:
Ricevuto un pacchetto non SYN come primo pacchetto di una connessione non intercettata e non bloccata.

Consiglio:
In condizioni normali è possibile verificare se la connessione è già stata chiusa e se il client o il server continua a ritenere che la connessione sia aperta e a trasmettere i dati. Alcuni esempi di situazioni in cui questo problema si verifica sono le situazioni successive all'emissione di un'istruzione 'clear local-host' o 'clear xlate'. Inoltre, se le connessioni non sono state rimosse di recente e il contatore aumenta rapidamente, l'accessorio potrebbe essere soggetto a attacchi. Acquisire una traccia sniffer per isolare la causa.

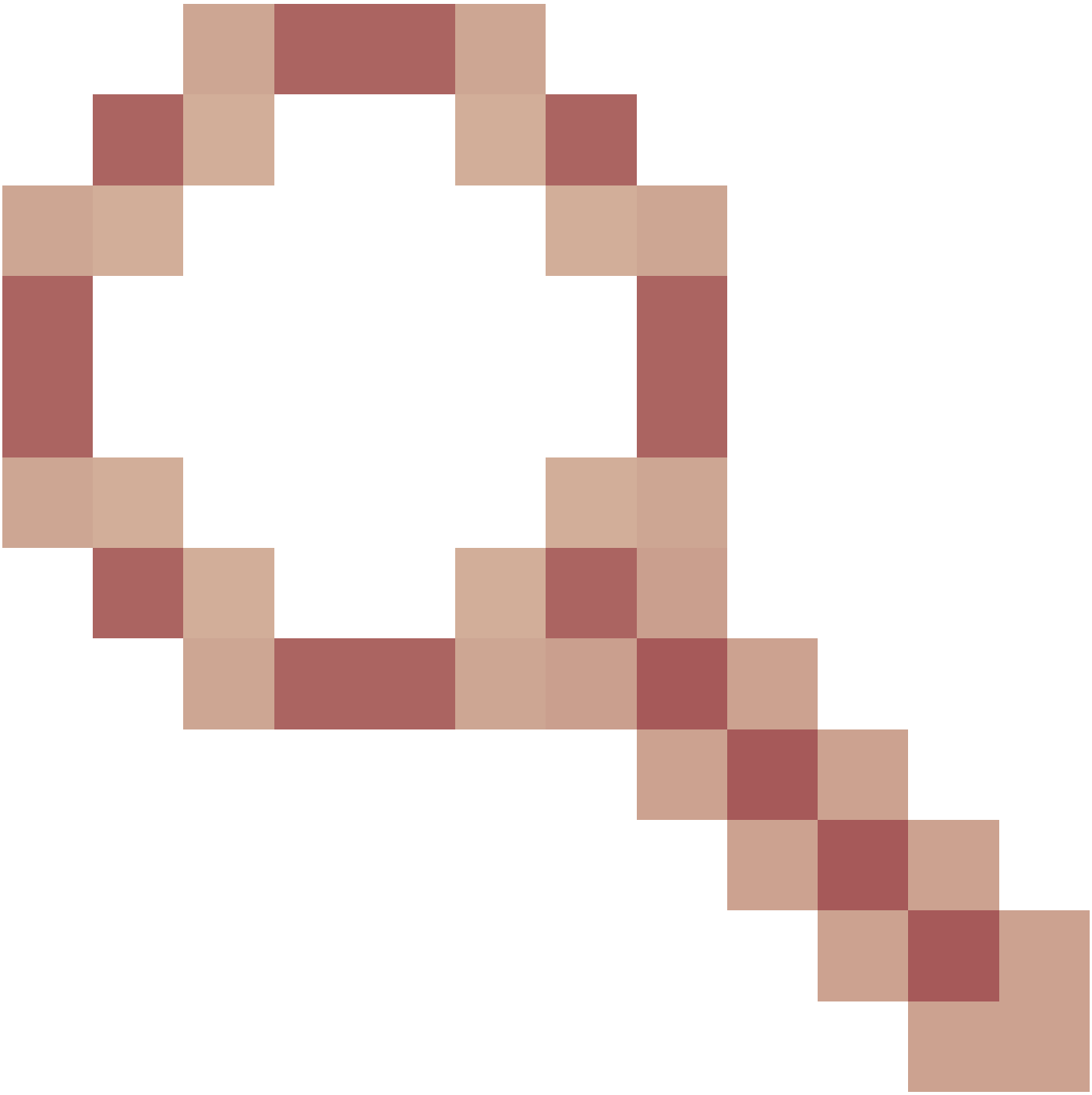
Soluzione: Disabilitare l'ispezione SQL*Net quando il trasferimento dei dati SQL avviene sulla stessa porta della porta TCP 1521 del controllo SQL. L'appliance di sicurezza funge da proxy quando l'ispezione SQL*Net è abilitata e riduce le dimensioni della finestra del client da 65.000 a circa 16.000, causando problemi di trasferimento dei dati.

Esempio di eliminazione di un'ispezione ICMP

Questo scenario è relativo a un ambiente cluster FTD.
L'identificatore ICMP dell'intestazione ICMP può essere usato come porta di origine della 5-tupla nel flusso, quindi tutte le 5-tuple dei pacchetti ping sono uguali, il motivo del rilascio ASP è "inspect-icmp-seq-num-not-matched" come si può osservare in questo output.

```
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 bug Cisco CSCvb92417



[L'ASA del cluster ignora le risposte ICMP predefinite con il motivo "inspect-icmp-seq-num-not-matched"]

Motivo eliminazione ASP:

Nome: inspect-icmp-seq-num-not-matched
Numero di sequenza ICMP Inspect non corrispondente:
Il contatore deve aumentare quando il numero di sequenza nel messaggio di risposta echo ICMP non corrisponde ad alcun messaggio echo ICMP passato precedentemente sull'accessorio sulla stessa connessione.

Soluzione: Disabilitare l'ispezione ICMP. In ambiente cluster: due o più FTD nel cluster e il traffico ICMP può essere asimmetrico. Si è verificato un ritardo nell'eliminazione del flusso ICMP. Il ping

successivo viene inviato rapidamente prima della pulizia del flusso ping precedente. In questo caso, si può verificare una perdita consecutiva del pacchetto ping.

Esempio di rilascio per ispezione SIP

In questo scenario, le chiamate sono durate solo cinque minuti, quindi la connessione viene interrotta. Quando si usa il protocollo RTP, l'ispezione SIP può interrompere le connessioni. Come si può osservare nell'output di acquisizione dei pacchetti sull'interfaccia per il traffico VoIP, il flag BYE nel traffico SIP indica che la chiamata telefonica è chiusa in quel momento.

```
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) |
```

Nell'altro esempio, il syslog mostra un IP mappato che usa PAT, l'IP rimane con una sola porta disponibile e la sessione SIP è atterrata sulla stessa porta, il SIP non è riuscito a causa dell'allocazione della porta. Se PAT è in uso, l'ispezione SIP può interrompere la connessione.

Motivo dell'eliminazione ASP: "Impossibile creare la connessione UDP da IP/porta a IP/porta a causa del raggiungimento del limite di X per il blocco della porta PAT per host" e "terminato dal motore di ispezione, motivo - reimpostazione in base alla configurazione '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
```

Motivo eliminazione ASP:

Nome: async-lock-queue-limit
Limite coda di blocco asincrono superato:
Ogni coda di lavoro di blocco asincrono ha un limite di 1000. Quando si tenta di inviare alla coda di lavoro più pacchetti SIP, il pacchetto deve essere scartato.

Consiglio:
È possibile eliminare solo il traffico SIP. Quando i pacchetti SIP hanno lo stesso blocco padre e possono essere inseriti nella stessa coda di blocco asincrono, si può verificare una riduzione del numero di blocchi, in quanto solo un core singolo gestisce tutti i supporti. Se un pacchetto SIP tenta di essere accodato quando le dimensioni della coda di blocco asincrona superano il limite, il pacchetto deve essere eliminato.

Nome: indirizzo SP ciclico
indirizzo ciclico:
Questo contatore viene incrementato quando gli indirizzi di origine e di destinazione in un flusso sono uguali. I flussi SIP in cui è abilitata la privacy degli indirizzi vengono esclusi, in quanto è normale che tali flussi abbiano lo stesso indirizzo di origine e di destinazione.

Consiglio:
Esistono due possibili condizioni in cui questo contatore può aumentare. La prima si verifica quando l'accessorio riceve un pacchetto il cui indirizzo di origine corrisponde alla destinazione. Si tratta di un tipo di attacco DoS. La seconda si verifica quando la configurazione NAT dell'accessorio utilizza un indirizzo di origine uguale a quello di destinazione.

Nome: chiuso da padre
Il flusso padre è chiuso:
Quando il flusso padre di un flusso subordinato viene chiuso, anche il flusso subordinato viene chiuso. Ad esempio, un flusso di dati FTP (flusso subordinato) può essere chiuso con questo motivo specifico quando il relativo flusso di controllo (flusso padre) viene terminato. Questo motivo è indicato anche quando un flusso secondario (foro a perno) viene chiuso dall'applicazione di controllo. Ad esempio, quando si riceve il messaggio BYE, il motore di ispezione SIP (applicazione di controllo) deve chiudere i corrispondenti flussi RTP SIP (flusso secondario).

Soluzione: Disabilita ispezione SIP. A causa dei limiti del protocollo:

- L'ispezione SIP supporta solo la funzione Chat. La lavagna, il trasferimento di file e la condivisione di applicazioni non sono supportati. RTC Client 5.0 non è supportato.
- Quando si utilizza PAT, non è possibile convertire alcun campo dell'intestazione SIP contenente un indirizzo IP interno senza porta e quindi l'indirizzo IP interno può essere perso all'esterno. Per evitare queste perdite, configurare NAT anziché PAT.
- Per impostazione predefinita, l'ispezione SIP è abilitata utilizzando la mappa di ispezione predefinita, che include:
  * Estensioni di messaggistica immediata SIP: Attivato.
  * Traffico non SIP sulla porta SIP: Eliminato.
  * Nascondere gli indirizzi IP di server ed endpoint: Disabled.
  * Maschera la versione del software e gli URI non SIP: Disabled.
  * Accertarsi che il numero di hop verso la destinazione sia maggiore di 0: Attivato.
  * Conformità RTP: Non applicato.
  * Conformità SIP: Non eseguire il controllo dello stato e la convalida dell'intestazione.

Risoluzione dei problemi

Questi sono alcuni dei comandi suggeriti per risolvere i problemi di traffico relativi all'ispezione del protocollo LINA MPF.

- Mostra criteri di servizio visualizza le statistiche dei criteri di servizio per le ispezioni di LINA MPF abilitate.

```
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
```

In questo output di esempio del comando show service-policy inspect http vengono visualizzate le statistiche 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
```

- Impostare un'acquisizione asp-drop sull'interfaccia da ispezionare.

```
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
```

Come abilitare o disabilitare le ispezioni specifiche dell'applicazione LINA MPF

Queste sono le opzioni disponibili per abilitare o disabilitare le ispezioni dell'applicazione MPF

LINA in Cisco Secure Firewall Threat Defense.

- Configurazione su FlexConfig: È necessario disporre dell'accesso come amministratore all'interfaccia utente di FMC. Questa modifica è permanente nella configurazione.
- Configurazione su CLI FTD: È necessario l'accesso amministrativo alla CLI FTD. Questa modifica non è permanente. Se viene eseguito un riavvio o una nuova distribuzione, la configurazione viene rimossa.

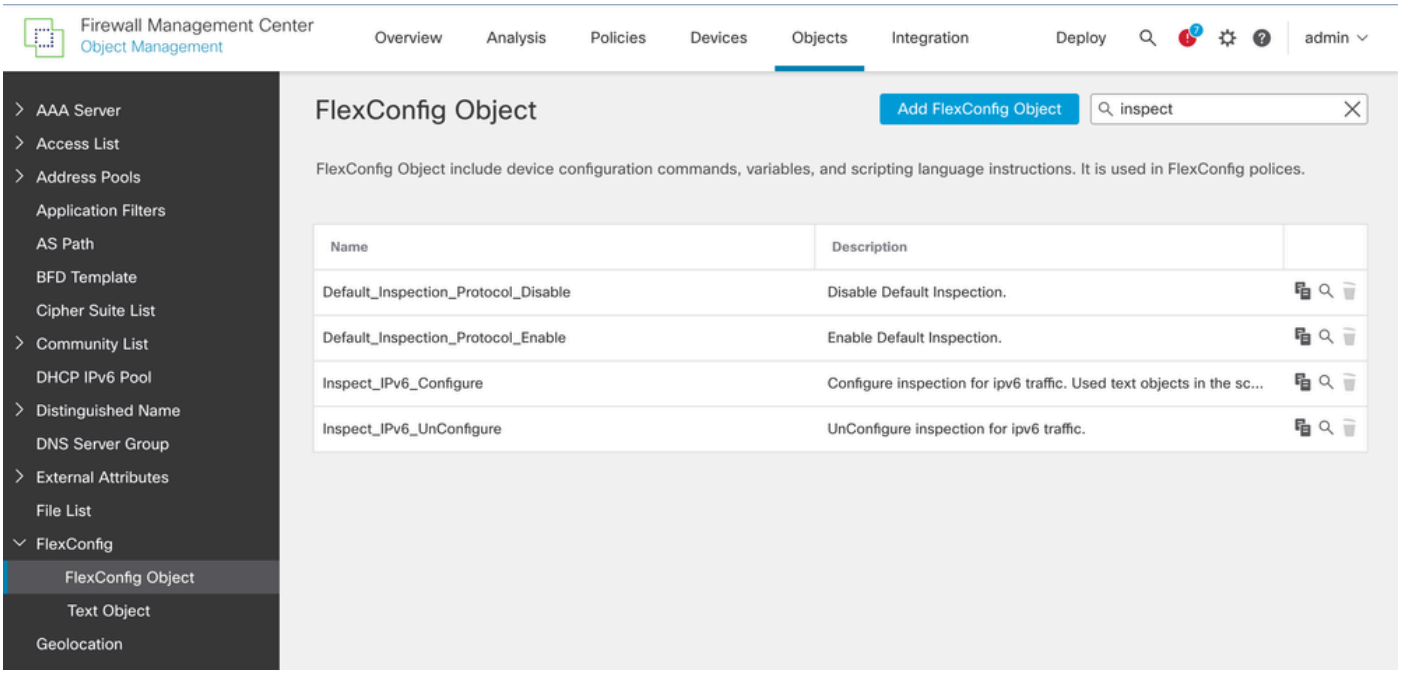
Configurazione su FlexConfig

FlexConfig è un metodo di ultima istanza per configurare le funzionalità basate su ASA che sono compatibili con la difesa dalle minacce, ma che non sono altrimenti configurabili nel centro di gestione.

La configurazione per disabilitare o abilitare l'ispezione in modo permanente è su FlexConfig nell'interfaccia utente di FMC e può essere applicata globalmente o solo per il traffico specifico.

Passaggio 1.

Nell'interfaccia utente di FMC, selezionare Oggetti > Gestione oggetti > FlexConfig > Oggetto FlexConfig, dove è possibile trovare l'elenco degli oggetti Ispezione protocollo predefiniti.



Oggetti ispezione protocollo FlexConfig predefinito

Passaggio 2.

Per disattivare una specifica ispezione del protocollo, è possibile creare un oggetto FlexConfig.

Selezionare Oggetti > Gestione oggetti > FlexConfig > Oggetto FlexConfig > Aggiungi oggetto FlexConfig

In questo esempio, per disabilitare l'ispezione SIP da global_policy, la sintassi deve essere:

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

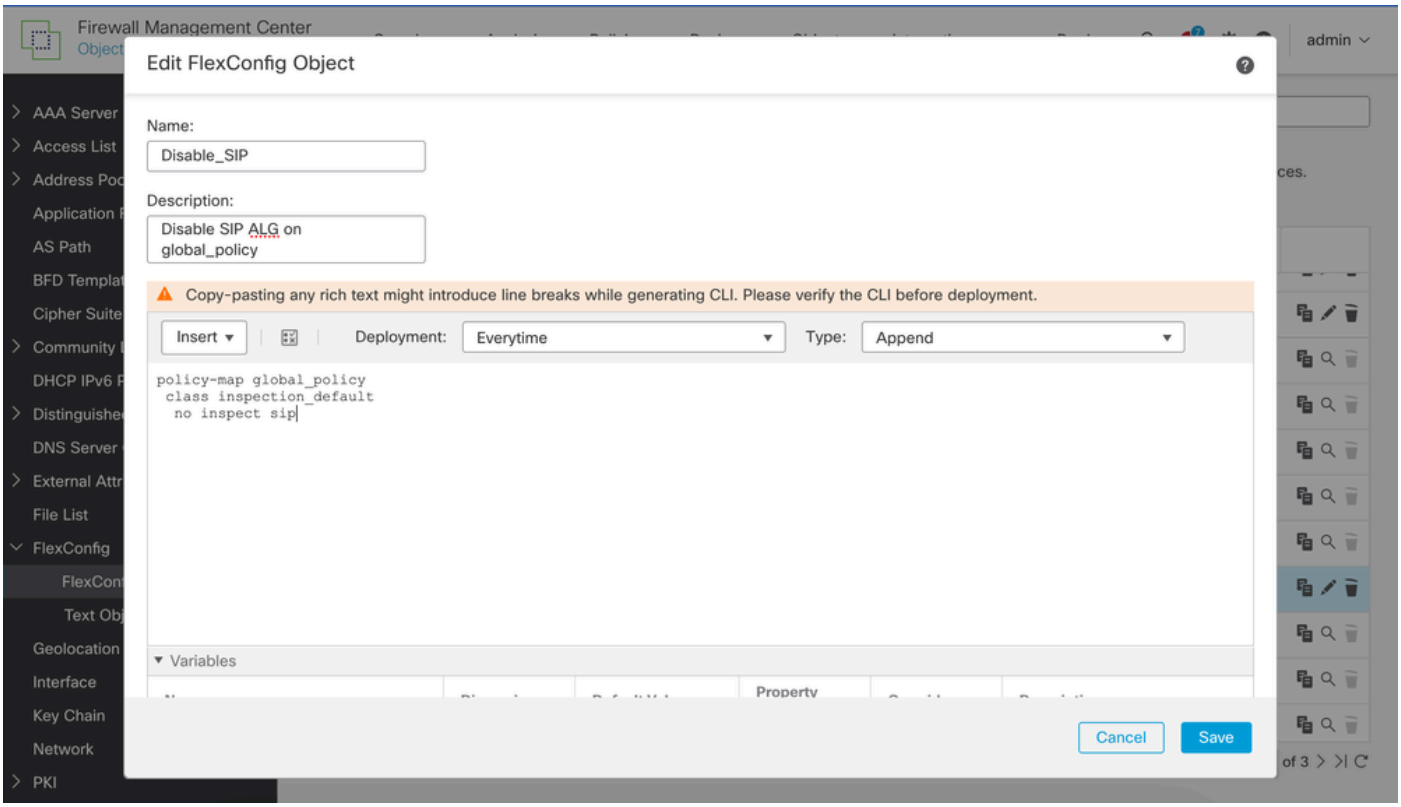
Quando si configura un oggetto FlexConfig, è possibile scegliere la frequenza e il tipo di distribuzione.

Implementazione

- Se l'oggetto FlexConfig punta a oggetti gestiti dal sistema come oggetti di rete o ACL, scegliere Everytime. In caso contrario, non sarà possibile distribuire gli aggiornamenti agli oggetti.
- Utilizzare Una volta se l'unica operazione da eseguire sull'oggetto è cancellare una configurazione. Quindi, rimuovere l'oggetto dal criterio FlexConfig dopo la distribuzione successiva.

Tipo

- Append (Impostazione predefinita). I comandi nell'oggetto vengono inseriti alla fine delle configurazioni generate dai criteri del centro di gestione. È necessario utilizzare Aggiungi se si utilizzano variabili oggetto criterio che fanno riferimento a oggetti generati da oggetti gestiti. Se i comandi generati per altri criteri si sovrappongono a quelli specificati nell'oggetto, è necessario selezionare questa opzione in modo che i comandi non vengano sovrascritti. Questa è l'opzione più sicura.
- Anteponi. I comandi nell'oggetto vengono inseriti all'inizio delle configurazioni generate dai criteri del centro di gestione. In genere, si utilizza prepend per i comandi che cancellano o negano una configurazione.



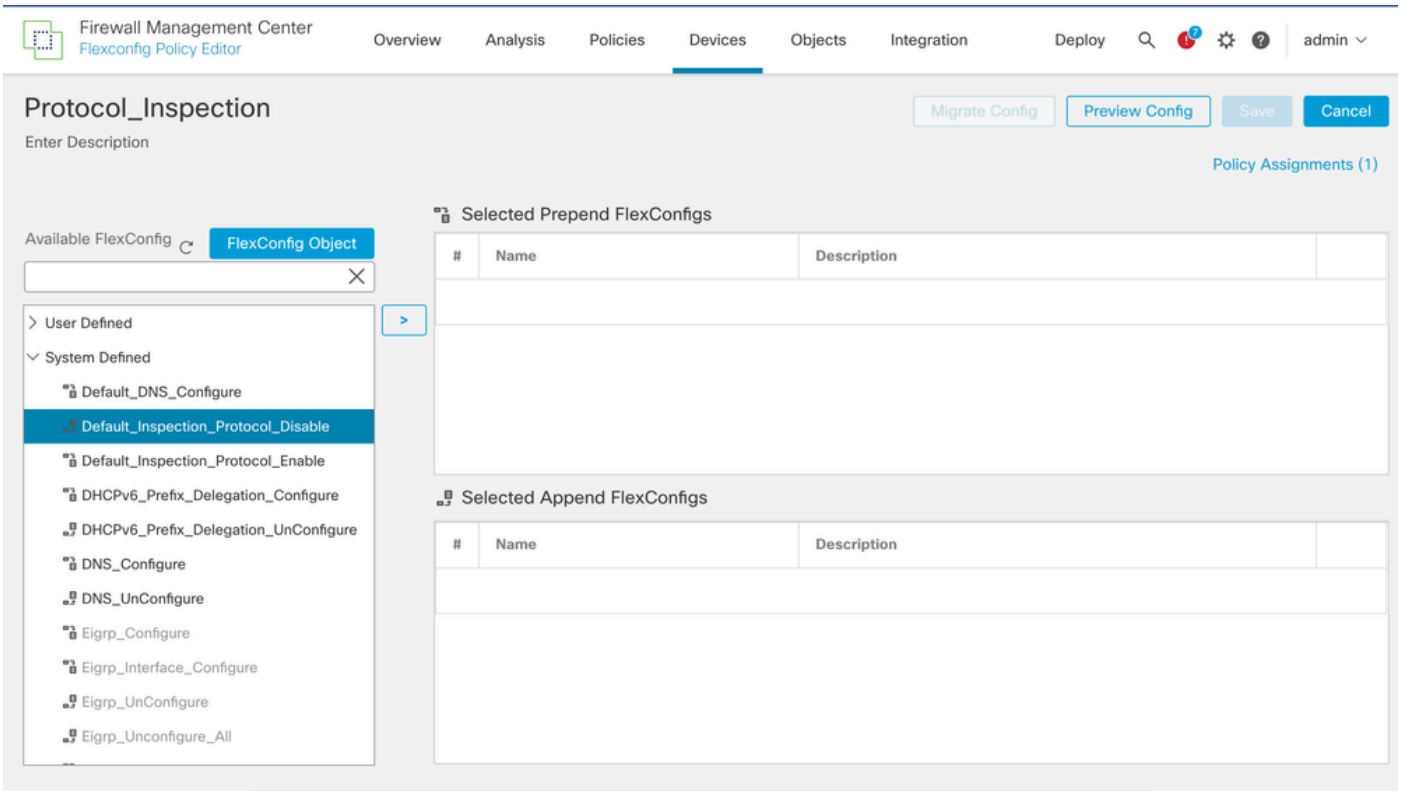
Creare un oggetto per disabilitare un singolo protocollo dal valore predefinito global_policy

Passaggio 3.

Aggiungere gli oggetti nel criterio FlexConfig assegnato a LINA.

Passare a Dispositivi > FlexConfig e selezionare il criterio FlexConfig applicato al firewall con problemi di rilascio.

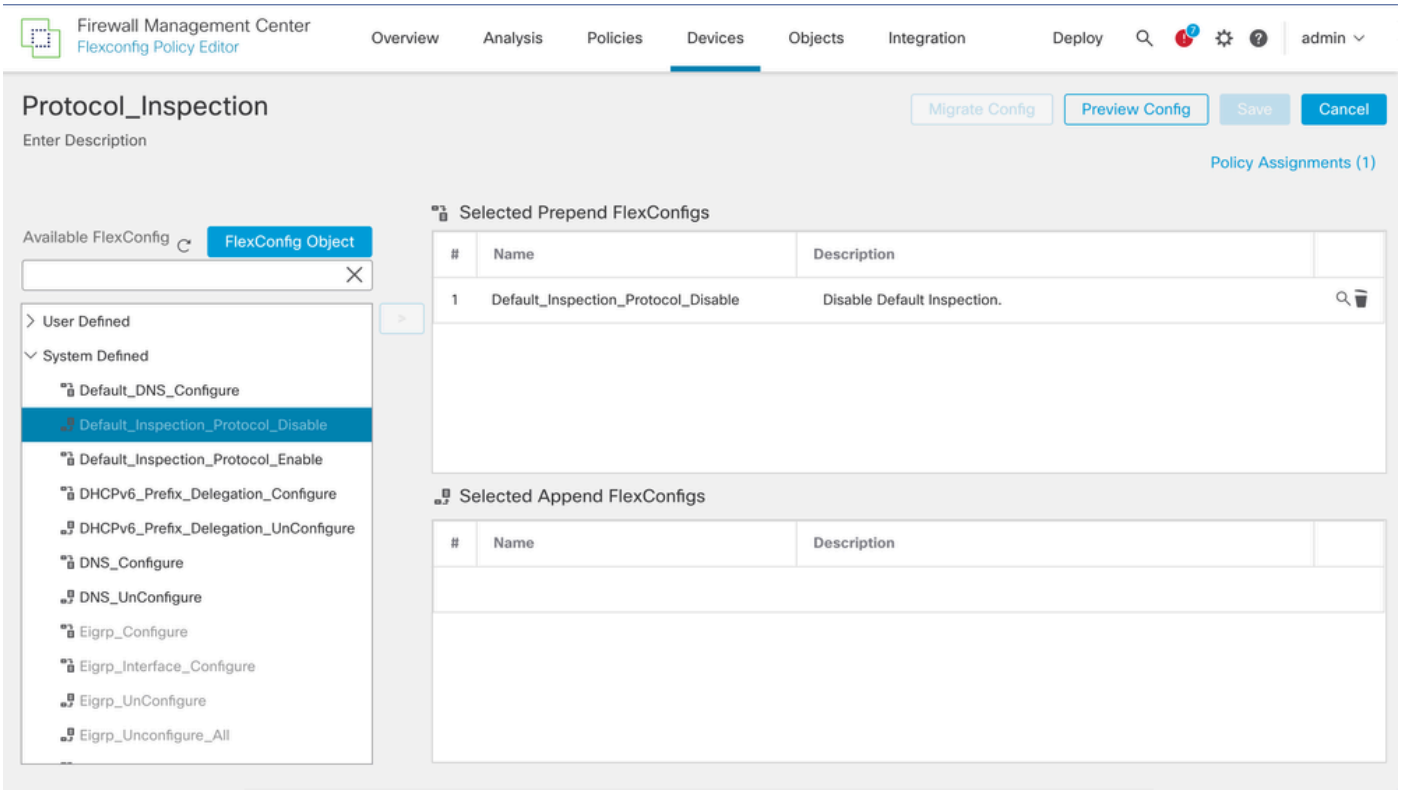
Per disabilitare tutte le ispezioni a livello globale, selezionare l'oggetto Default_Inspection_Protocol_Disable in Oggetti FlexConfig definiti dal sistema, quindi fare clic sulla freccia blu in mezzo per aggiungerlo al criterio FlexConfig.



Selezionare l'oggetto definito dal sistema per disabilitare tutte le funzioni di ispezione del protocollo

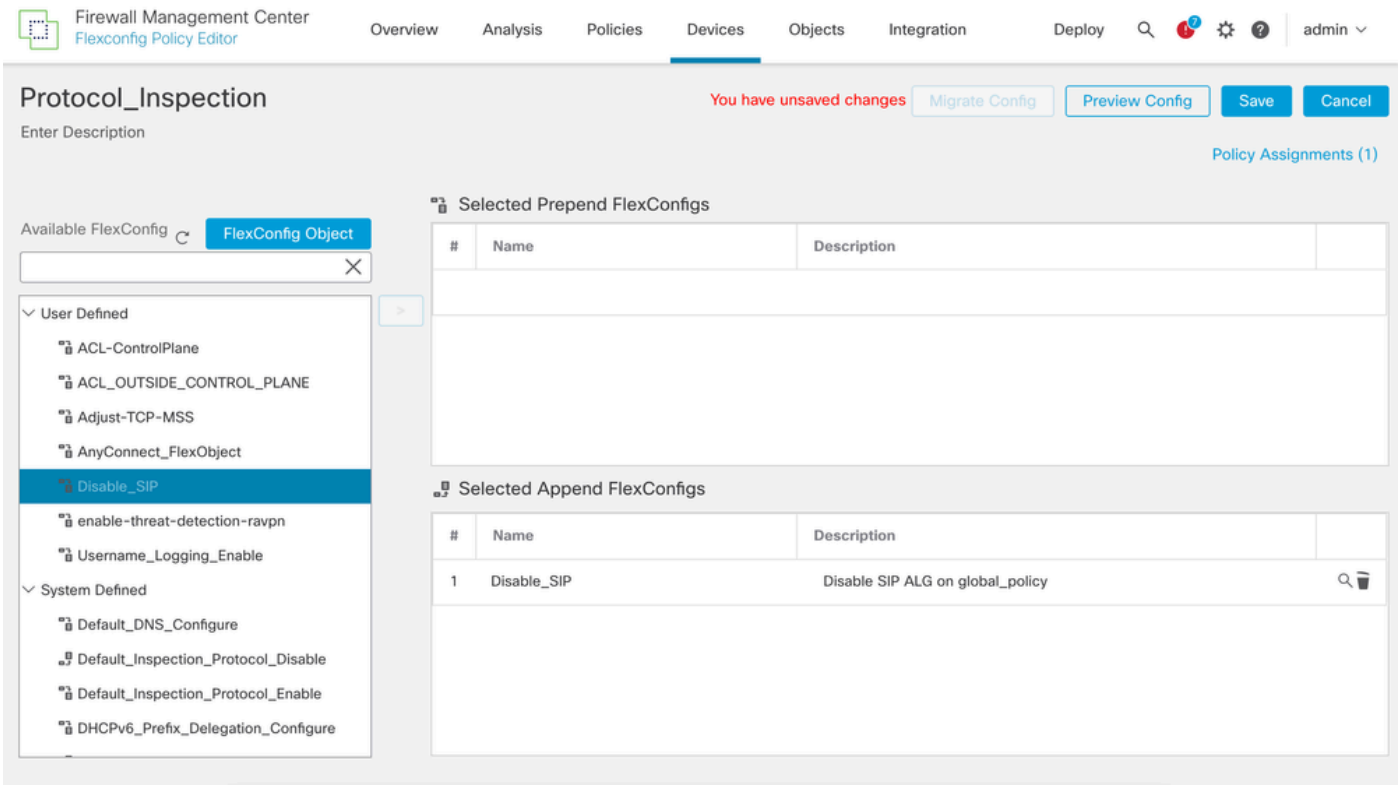
Passaggio 4.

Dopo aver selezionato la configurazione, confermarne la visualizzazione nelle caselle appropriate. Non dimenticare di salvare e distribuire la configurazione per renderla effettiva.



Oggetto selezionato per disabilitare tutte le funzioni di ispezione del protocollo

Passaggio 5.
Per disattivare una singola ispezione del protocollo, selezionare l'oggetto precedentemente creato dall'elenco Definito dall'utente e aggiungerlo al criterio utilizzando la freccia presente tra le caselle.



Selezionare questa opzione per disabilitare l'ispezione di un singolo protocollo da global_policy

Passaggio 6.

Dopo aver selezionato la configurazione, confermarne la visualizzazione nelle caselle appropriate. Non dimenticare di salvare e distribuire la configurazione per renderla effettiva.

Configurazione con la CLI FTD

Questa soluzione può essere applicata immediatamente dalla CLI dell'FTD per verificare se l'ispezione incide sul traffico. Tuttavia, la modifica della configurazione non viene salvata se si verifica un riavvio o una nuova distribuzione.

il comando deve essere eseguito dalla CLI FTD in modalità clish.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Verifica

Per verificare che la disabilitazione del protocollo sia effettiva, eseguire il comando show running-config policy-map. Nell'esempio, l'ispezione SIP è disabilitata perché non viene più visualizzata nell'elenco dei protocolli predefiniti.

```
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#
```

Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems

- Guida introduttiva a Controllo protocollo livello applicazione
- Controllo dei protocolli Internet di base
- Mostra utilizzo comando di rilascio ASP

Informazioni su questa traduzione

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