Resolución de problemas de tráfico descartado debido a la inspección del protocolo LINA en FTD

Contenido

Introducción

Prerequisites

- Componentes Utilizados

Antecedentes

- Configuraciones predeterminadas

Identificación de caídas de paquetes debido a la inspección del protocolo MPF

- Mensajes de error de descarte comunes
  - Ejemplo de descarte de inspección SUN RPC
  - Ejemplo de Borrado de Inspección de SQL*NET
  - Ejemplo de ICMP Inspection Drop
  - Ejemplo de Borrado de Inspección SIP

Troubleshoot

Cómo habilitar o deshabilitar inspecciones específicas de la aplicación LINA MPF

- Configuración sobre FlexConfig
- Configuración mediante la CLI de FTD

Verificación

Información Relacionada

Introducción

Este documento describe cómo identificar si la inspección del protocolo LINA para Modular Policy Framework (MPF) descarta el tráfico en Cisco Secure FTD.

Prerequisites

Cisco le recomendó que tuviera conocimientos sobre los siguientes temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Virtual Cisco Secure Firewall Threat Defence (FTD), versión 7.4.2

- Virtual Cisco Secure Firewall Manager Center (FMC), versión 7.4.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se iniciaron con una configuración sin definir (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los motores de inspección son necesarios en un firewall para los servicios que incorporan información de direccionamiento IP en el paquete de datos del usuario o que abren canales secundarios en puertos asignados dinámicamente.

La inspección de protocolo puede ayudar a evitar que el tráfico malintencionado entre en la red inspeccionando el contenido de los paquetes de red y bloqueando o modificando el tráfico en función de la aplicación o protocolo que se esté utilizando.
Como resultado, los motores de inspección pueden afectar el rendimiento general. Varios motores de inspección comunes están activados en el firewall de forma predeterminada; puede ser necesario para activar otros según la red.

Configuraciones predeterminadas

Por defecto, la configuración de FTD LINA incluye una política que coincide con todo el tráfico de inspección de aplicaciones por defecto.

La inspección se aplica al tráfico en todas las interfaces (una política global).

El tráfico de inspección de aplicaciones predeterminado incluye el tráfico a los puertos predeterminados para cada protocolo. Sólo puede aplicar una política global, por lo que si desea modificar la política global, por ejemplo, para aplicar la inspección a puertos no estándar, o para agregar inspecciones que no están activadas de forma predeterminada, debe editar la política predeterminada o desactivarla y aplicar una nueva.

Ejecute el comando show running-config policy-map en LINA, FTD Command Line Interface (CLI) a través de system support diagnostic-cli, para obtener la información.

```
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
!
```

Identificación de caídas de paquetes debido a la inspección del protocolo MPF

Incluso cuando el tráfico se alinea con la política de control de acceso (ACP) asignada al firewall, en ciertos escenarios, el proceso de inspección finaliza las conexiones debido a un comportamiento de tráfico específico recibido por el firewall, un diseño no compatible, un estándar de aplicación o una limitación de inspección.

Durante la resolución de problemas de tráfico, un proceso útil que se debe utilizar es:

- Establezca registros de captura en tiempo real en las interfaces de las que fluye el tráfico (interfaces de entrada y salida), comando:

```
firepower# capture

        [interface

        ][match


           [port
```

```
]
```

```
[port
```

```
]]
```

Con las capturas, puede incluir la opción packet number X trace detail y debe proporcionar el resultado fase por fase que toma la conexión, como lo hace un comando packet-tracer, pero con esta opción se asegura de que es tráfico en tiempo real.

```
firepower# show capture
```

```
packet number X trace detail
```

- Set real-time Accelerated Security Path (ASP) Drop, el tipo de captura asp-drop muestra los paquetes o conexiones descartados por el ASP, hay una lista de razones que puede encontrar en los enlaces relacionados del documento, comando:

```
firepower# capture
```

```
[type
```

```
] [interface
```

```
][match


   [port

   ]

     [port

     ]]
```

Las caídas de inspección de protocolo se pueden ignorar, ya que un resultado allow se puede observar en las fases packet-tracer. Por eso, es crucial verificar siempre la razón de la caída usando registros de captura en tiempo real.

Mensajes de error de descarte comunes

La eliminación de la ruta de seguridad acelerada (ASP) se utiliza a menudo con fines de depuración para ayudar a solucionar problemas de red. El comando show asp drop se utiliza para mostrar estos paquetes o conexiones caídos, proporcionando información sobre las razones de las caídas, que pueden incluir problemas como fallas de NAT, fallas de inspección o negaciones de reglas de acceso.

Puntos clave sobre las caídas de ASP:

- Descartes de tramas: Se trata de caídas relacionadas con paquetes individuales, como la

encapsulación no válida o la ausencia de ruta al host.
- Caídas de flujo: Éstos están relacionados con las conexiones, como los flujos denegados por las reglas de acceso o los fallos de NAT.
- Uso: El comando es principalmente para la depuración y el resultado puede cambiar.

Estos mensajes de error o motivos de caída son ejemplos que puede encontrar durante la resolución de problemas. Pueden diferir en función del protocolo de inspección que se utilice.

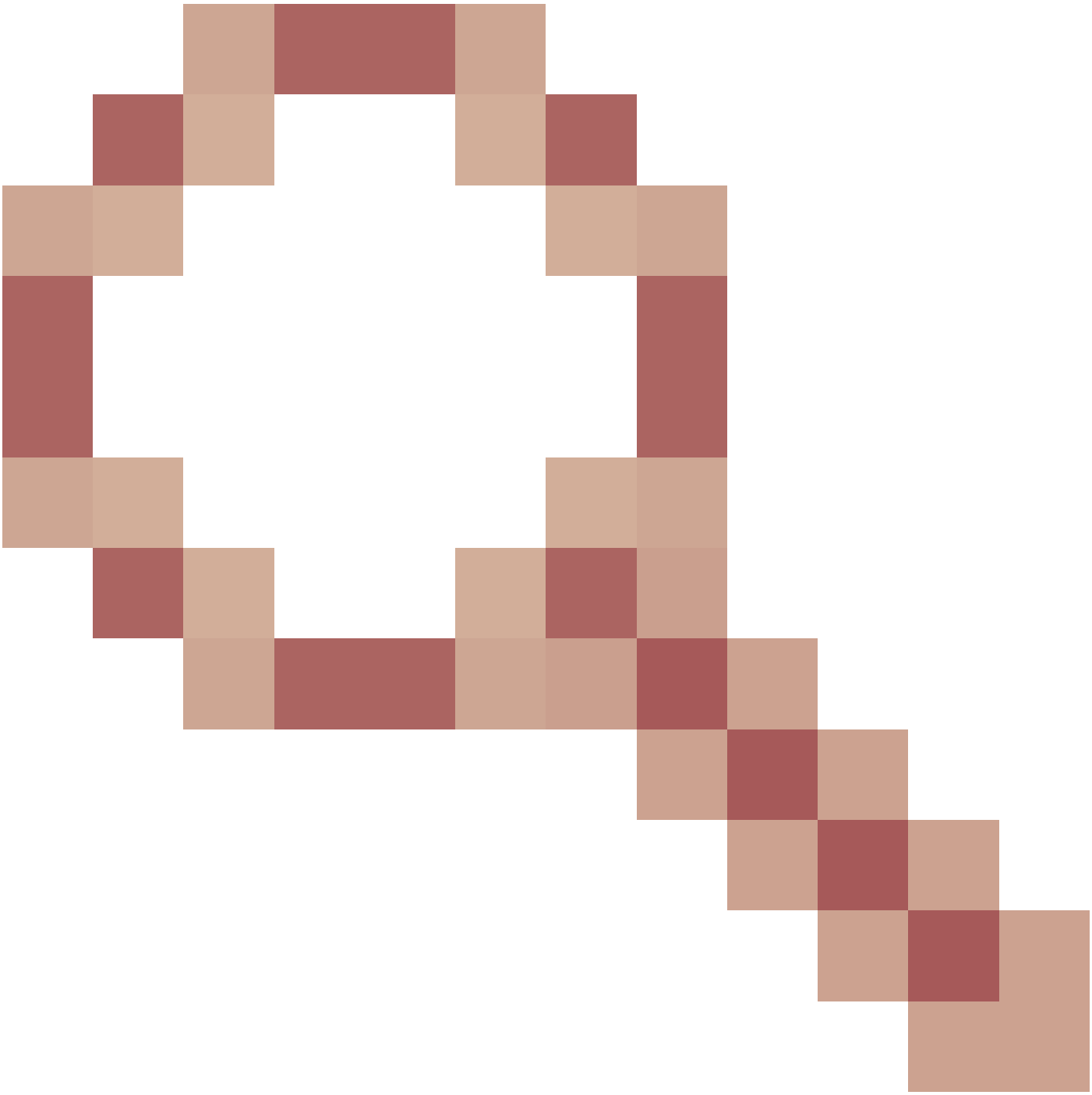
Ejemplo de descarte de inspección SUN RPC

Este escenario es para un FTDv proxy de brazo único en la implementación de AWS, tráfico RPC encapsulado por Geneve, si la inspección de Sun Rpc está habilitada, la conexión se descarta.

El resultado muestra caídas de ASP para la inspección de Sun Rpc, Sun Rcp utiliza el puerto 111 como destino. El último paquete es el puerto de encapsulación Geneve que utiliza 6081 como destino. La razón de la caída en la salida como puede observar es "No hay adyacencia válida"

```
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 bug de Cisco CSCwj00074



[El proxy de brazo único FTDv descarta el tráfico sin adyacencia con la función de inspección sunrpc habilitada]

El tráfico se descarta como 'adyacencia no válida' en el ASP del motor LINA porque las direcciones MAC de origen y destino se llenan repentinamente en ceros después del segundo paquete (SYN/ACK) del intercambio de señales de 3 vías.

Motivo de la eliminación ASP:

Nombre: no-adyacencia
Adyacencia no válida:
Este contador aumenta cuando el dispositivo de seguridad recibe un paquete en un flujo

existente que ya no tiene una adyacencia de salida válida. Esto puede ocurrir si el salto siguiente ya no es alcanzable o si un cambio de ruteo ha ocurrido típicamente en un entorno de ruteo dinámico.

Solución: Inhabilite la inspección sunrpc.

Ejemplo de Borrado de Inspección de SQL*NET

Este escenario es para un FTDv proxy de un solo brazo en la implementación de AWS; si se habilita la inspección de Sql*Nel, el tráfico encapsulado de Geneve se descarta.

El resultado es para las capturas de paquetes combinadas (puede observar el mismo número de paquete):
Primera línea: captura de paquetes de descarte asp no encapsulada, Sql*Net utiliza el puerto 1521 como destino.
Segunda línea: La interfaz VNI asp-drop en LINA, Geneve utiliza el puerto de encapsulación 6081 como destino.

Hay dos razones diferentes de descarte en la salida, como puede observar son "tcp-buffer-timeout" y "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 de la eliminación ASP:

Nombre: tcp-buffer-timeout
Límite de tiempo de búfer de paquetes fuera de orden TCP:
Este contador se incrementa y el paquete se descarta cuando un paquete TCP en cola fuera de orden se ha mantenido en el buffer durante demasiado tiempo. Normalmente, los paquetes TCP se ponen en orden en las conexiones que inspecciona el dispositivo de seguridad o cuando los paquetes se envían al SSM para su inspección. Cuando el siguiente paquete TCP esperado no llega en un período determinado, el paquete en cola fuera de servicio se descarta.

Recomendaciones:
El siguiente paquete TCP esperado no llega debido a una congestión en la red que es normal en una red ocupada. El mecanismo de retransmisión TCP en el host final debe retransmitir el paquete y la sesión puede continuar.

Nombre: tcp-not-syn
Primer paquete TCP no SYN:
Recibió un paquete no SYN como el primer paquete de una conexión no interceptada y no retenida.

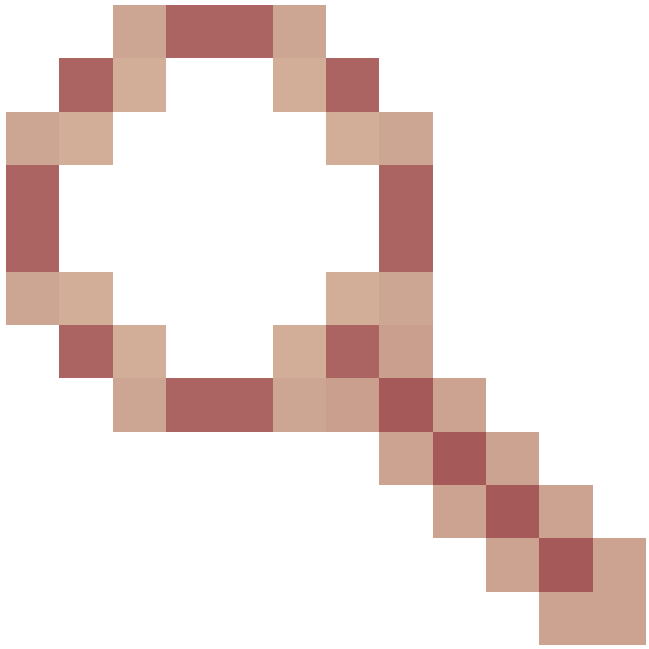
Recomendación:
En condiciones normales, esto puede observarse cuando el dispositivo ya ha cerrado una conexión y el cliente o el servidor aún creen que la conexión está abierta y continúan transmitiendo datos. Algunos ejemplos donde esto puede ocurrir es justo después de que se emita un 'clear local-host' o 'clear xlate'. Además, si las conexiones no se han eliminado recientemente y el contador aumenta rápidamente, el dispositivo puede estar bajo ataque. Capture un rastro del sabueso para ayudar a aislar la causa.

Solución: Desactive la inspección de SQL*Net cuando la transferencia de datos SQL se produzca en el mismo puerto que el puerto TCP 1521 de control SQL. El dispositivo de seguridad actúa como proxy cuando la inspección de SQL*Net está activada y reduce el tamaño de la ventana del cliente de 65000 a aproximadamente 16000, lo que provoca problemas de transferencia de datos.

Ejemplo de ICMP Inspection Drop

Este escenario es para un entorno de clúster FTD.
El identificador ICMP del encabezado ICMP se puede utilizar como el puerto de origen de la 5 tupla en el flujo, por lo que todas las 5 tuplas de los paquetes de ping son iguales, la razón de la caída de ASP es "inspect-icmp-seq-num-not-match", como puede observar en esta salida.

```
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 falla de funcionamiento de Cisco CSCvb92417

[El clúster ASA descarta las respuestas ICMP inmediatas con el motivo "inspect-icmp-seq-num-not-match"]

Motivo de la eliminación ASP:

Nombre: inspect-icmp-seq-num-not-match
Número de secuencia de inspección ICMP no coincidente:
Este contador debe aumentar cuando el número de secuencia del mensaje de respuesta de eco ICMP no coincide con ningún mensaje de eco ICMP que haya pasado a través del dispositivo anteriormente en la misma conexión.

Solución: Desactive la inspección ICMP. En un entorno de clúster: dos o más FTD en el clúster y el tráfico ICMP puede ser asimétrico. Se observa que hay un retraso para la eliminación del flujo ICMP; el ping subsiguiente se envía rápidamente antes de que se haya limpiado el flujo de ping anterior. En este caso, puede ocurrir la pérdida consecutiva de paquetes ping.

Ejemplo de Borrado de Inspección SIP

En este escenario, las llamadas duraron solo cinco minutos y, a continuación, se interrumpe la conexión. Cuando se utiliza RTP, la inspección de SIP puede interrumpir conexiones.
Como puede observar en la salida de captura de paquetes en la interfaz para el tráfico VoIP, el indicador BYE en el tráfico SIP significa que la llamada telefónica está cerrada en ese 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) |
```

En este otro ejemplo, el syslog muestra una IP asignada que utiliza PAT, la IP se queda con un solo puerto disponible y la sesión SIP aterriza en el mismo puerto, el SIP falla debido a la asignación del puerto. Si PAT está en uso, la inspección de SIP puede interrumpir la conexión.

El motivo de la caída de ASP es: "No se puede crear una conexión UDP de IP/puerto a IP/puerto debido a que se ha alcanzado el límite de bloque de puertos PAT por host de X" y "finalizado por el motor de inspección, motivo: restablecimiento basado en la configuración de '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 de la eliminación ASP:

Nombre: async-lock-queue-limit
Se superó el límite de cola de bloqueo asincrónico:
Cada cola de trabajo de bloqueo asíncrono tiene un límite de 1000. Cuando se intentan enviar más paquetes SIP a la cola de trabajo, se debe descartar el paquete.
Recomendación:
Solo se puede descartar el tráfico SIP. Cuando los paquetes SIP tienen el mismo bloqueo principal y se pueden colocar en cola en la misma cola de bloqueo asíncrono, por lo tanto, pueden resultar en la disminución de bloques, porque sólo un núcleo está manejando todos los medios. Si un paquete SIP intenta ponerse en cola cuando el tamaño de la cola de bloqueo asincrónico excede el límite, el paquete debe ser descartado.

Nombre: sp-looping-address
looping-address:
Este contador se incrementa cuando las direcciones de origen y de destino de un flujo son las mismas. Se excluyen los flujos SIP en los que está habilitada la privacidad de direcciones, ya que es normal que esos flujos tengan la misma dirección de origen y de destino.

Recomendación:
Existen dos condiciones posibles en las que este contador puede incrementarse. Una es cuando el dispositivo recibe un paquete con la dirección de origen igual al destino. Esto representa un tipo de ataque DoS. La segunda es cuando la configuración NAT del dispositivo NATs establece una dirección de origen igual a la del destino.

Nombre: cerrado por los padres
El flujo principal está cerrado:
Cuando se cierra el flujo principal de un flujo subordinado, también se cierra el flujo subordinado. Por ejemplo, un flujo de datos FTP (flujo subordinado) se puede cerrar con este motivo específico cuando su flujo de control (flujo principal) finaliza. Esta razón también se da cuando un flujo secundario (pin-hole) es cerrado por su aplicación de control. Por ejemplo, cuando se recibe el mensaje BYE, el motor de inspección SIP (aplicación de control) debe cerrar los flujos RTP SIP correspondientes (flujo secundario).

Solución: Desactive la inspección de SIP. Debido a las limitaciones del protocolo:

- La inspección de SIP solo admite la función de conversación. No se admiten pizarras blancas, transferencia de archivos ni uso compartido de aplicaciones. El cliente RTC 5.0 no es compatible.
- Al utilizar PAT, cualquier campo de encabezado SIP que contenga una dirección IP interna

sin un puerto no se puede traducir y, por lo tanto, la dirección IP interna se puede filtrar fuera. Si desea evitar esta fuga, configure NAT en lugar de PAT.

- La inspección SIP se habilita de forma predeterminada mediante el mapa de inspección predeterminado, que incluye:
  * Extensiones de mensajería instantánea (IM) SIP: Habilitado.
  * Tráfico no SIP en puerto SIP: Suprimidos.
  * Ocultar direcciones IP de servidor y terminal: Inhabilitado.
  * Versión de software de máscara y URI que no son SIP: Inhabilitado.
  * Asegúrese de que el número de saltos hacia el destino sea mayor que 0: Habilitado.
  * Conformidad con RTP: No aplicado.
  * Conformidad con SIP: No realice la comprobación de estado ni la validación de encabezado.

Troubleshoot

Estos son algunos de los comandos sugeridos para resolver problemas de tráfico relacionados con la inspección del protocolo MPF de LINA.

- Show service-policy muestra las estadísticas de política de servicio para las inspecciones de LINA MPF habilitadas.

```
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
```

Este ejemplo de resultado del comando show service-policy inspect http muestra las estadísticas 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
```

- Establezca una captura asp-drop en la interfaz para inspeccionar.

```
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
```

Cómo habilitar o deshabilitar inspecciones específicas de la aplicación LINA MPF

Estas son las opciones disponibles para activar o desactivar las inspecciones de la aplicación MPF LINA en Cisco Secure Firewall Threat Defence.

- Configuración sobre FlexConfig: Necesita acceso de administrador a la interfaz de usuario de FMC; este cambio es permanente en la configuración.
- Configuración sobre CLI de FTD: Necesita acceso de administrador a la CLI de FTD; este cambio no es permanente; si se reinicia o se realiza una nueva implementación, se elimina la configuración.

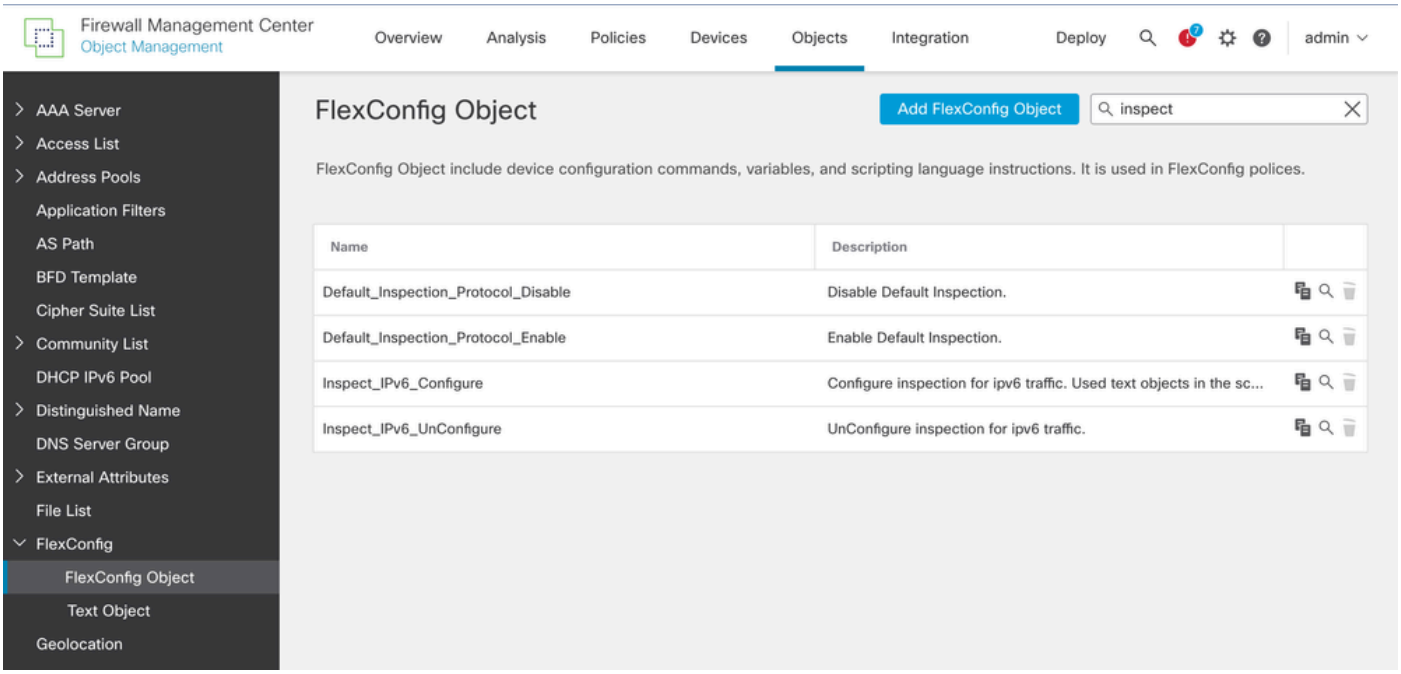
Configuración sobre FlexConfig

FlexConfig es un método de último recurso para configurar las funciones basadas en ASA que son compatibles con Threat Defence pero que no se pueden configurar en el centro de gestión.

La configuración para deshabilitar o habilitar la inspección permanentemente está en FlexConfig en la interfaz de usuario de FMC; se puede aplicar globalmente o solo para tráfico específico.

Paso 1.

En la interfaz de usuario de FMC, navegue hasta Objetos > Administración de objetos > FlexConfig > Objeto FlexConfig, donde puede encontrar la lista de objetos predeterminados de Inspección de protocolo.



Objetos predeterminados de inspección del protocolo FlexConfig

Paso 2.

Para desactivar una inspección de protocolo específica, puede crear un objeto FlexConfig.

Vaya a Objetos > Administración de objetos > FlexConfig > Objeto FlexConfig > Agregar objeto FlexConfig

En este ejemplo, la configuración para inhabilitar la inspección SIP desde global_policy, la sintaxis debe ser:

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

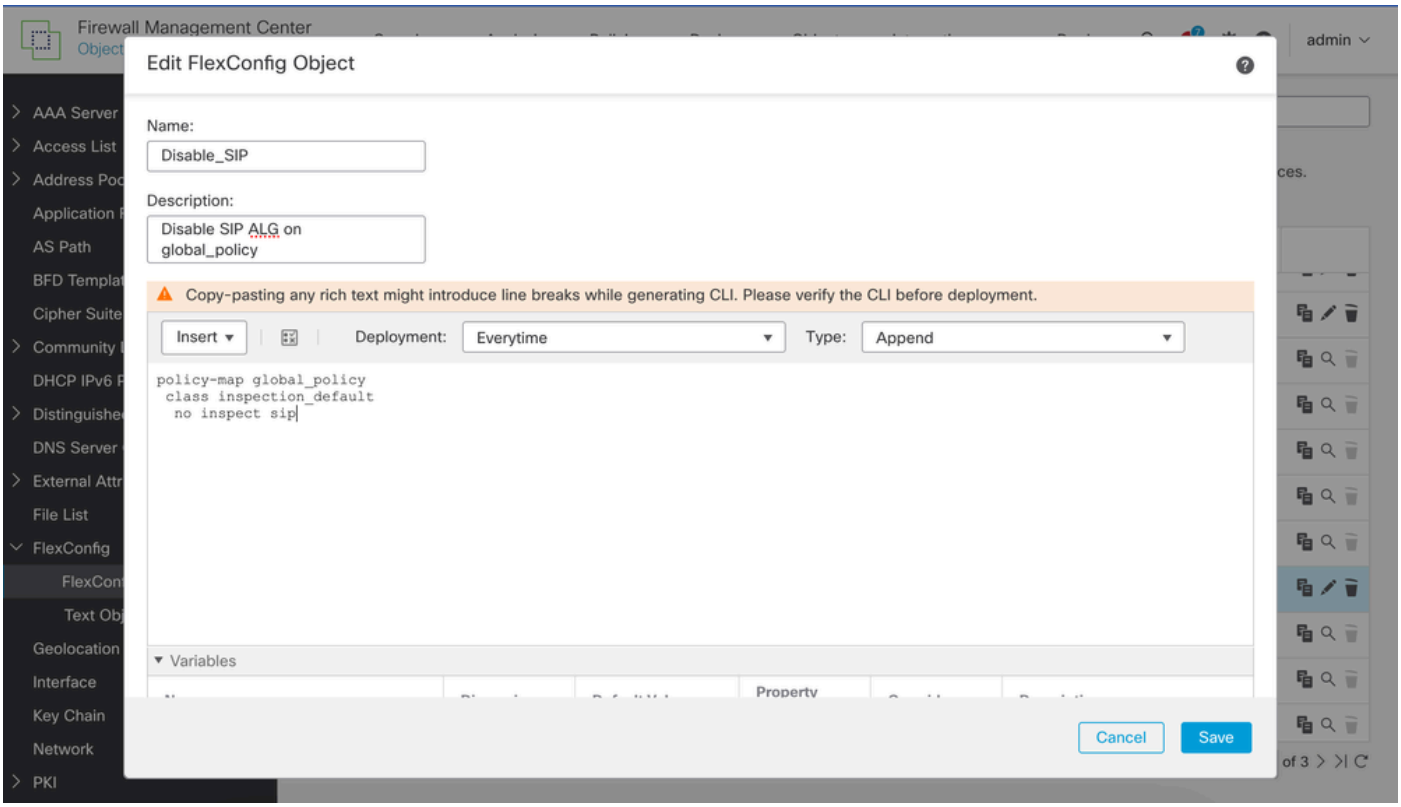
Al configurar un objeto FlexConfig, puede elegir la frecuencia y el tipo de implementación.

Implementación

- Si el objeto FlexConfig apunta a objetos administrados por el sistema, como objetos de red o ACL, seleccione Everytime. De lo contrario, no se podrían implementar las actualizaciones de los objetos.
- Use Once si lo único que hace en el objeto es borrar una configuración. A continuación, quite el objeto de la directiva FlexConfig después de la siguiente implementación.

Tipo

- Append (valor predeterminado). Los comandos del objeto se colocan al final de las configuraciones generadas a partir de las políticas del centro de administración. Debe utilizar Append si utiliza variables de objeto de directiva, que señalan a objetos generados a partir de objetos administrados. Si los comandos generados para otras directivas se solapan con los especificados en el objeto, debe seleccionar esta opción para que los comandos no se sobrescriban. Esta es la opción más segura.
- Anteponer. Los comandos del objeto se colocan al principio de las configuraciones generadas a partir de las políticas del centro de administración. Normalmente utilizaría prepend para los comandos que borran o niegan una configuración.



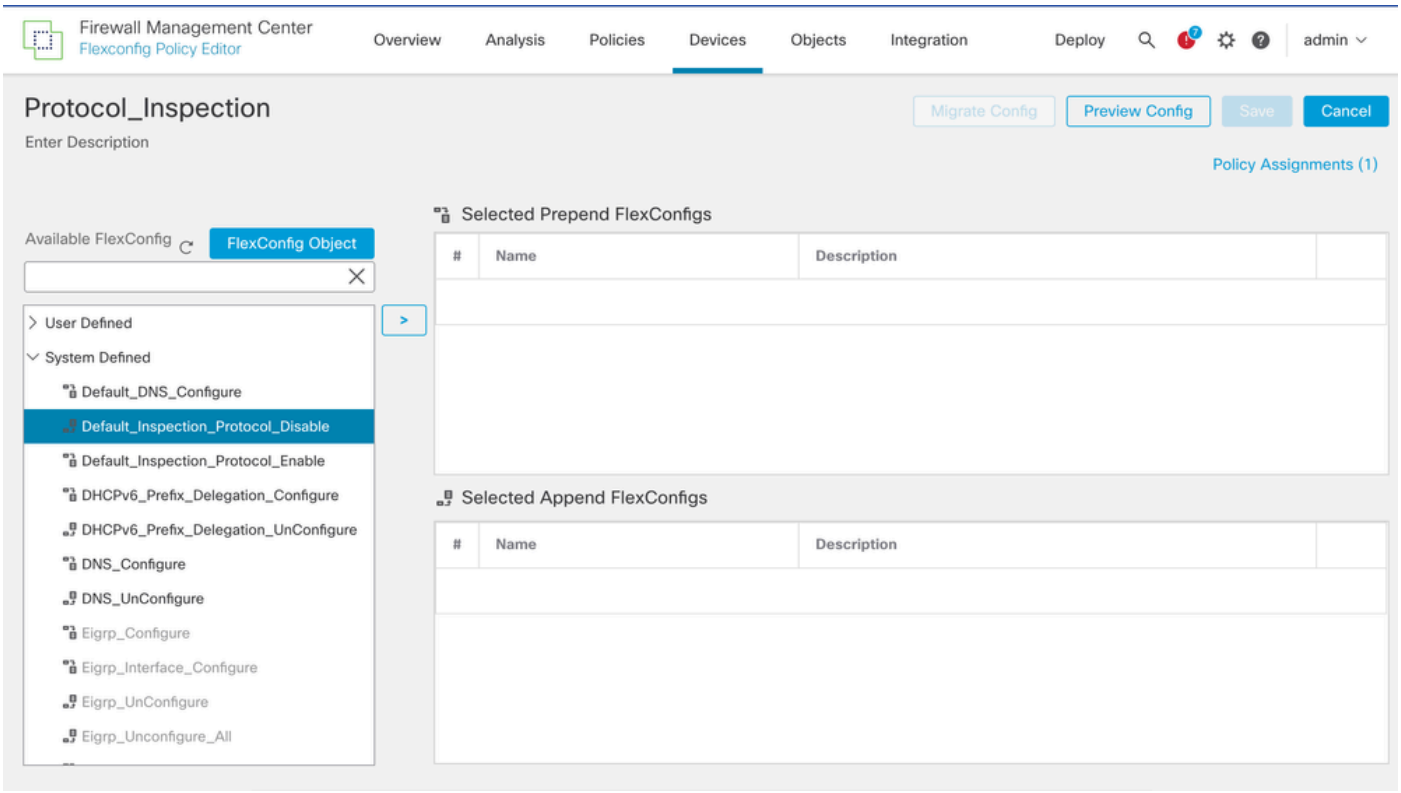
Cree un objeto para inhabilitar un único protocolo desde el global_policy predeterminado

Paso 3.

Agregue los objetos de la política FlexConfig asignados a LINA.

Vaya a Devices > FlexConfig y seleccione la política FlexConfig aplicada al firewall con problemas de caídas.

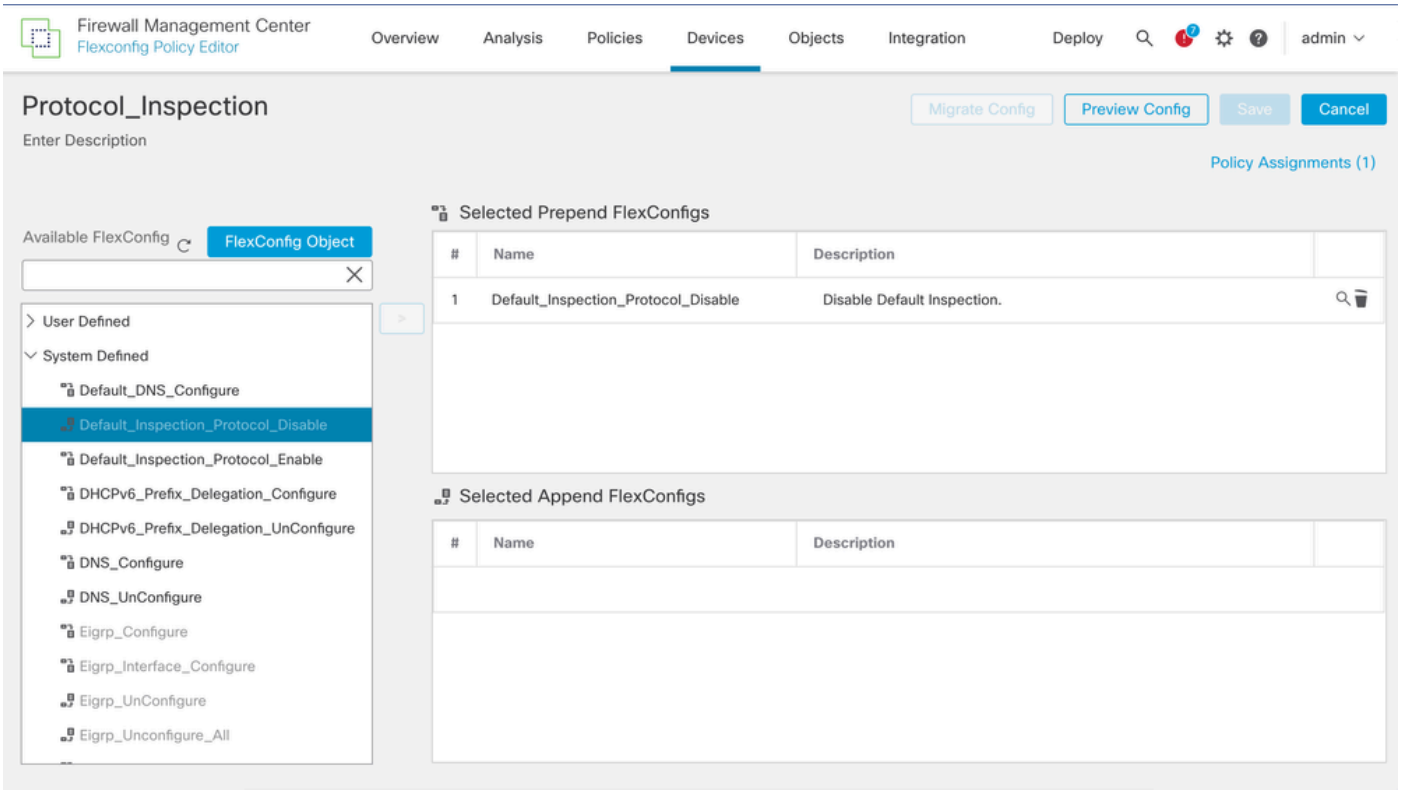
Para desactivar globalmente todas las inspecciones, seleccione el objeto Default_Inspection_Protocol_Disable en Objetos FlexConfig definidos por el sistema y, a continuación, haga clic en la flecha azul intermedia para agregarlo a la política FlexConfig.



Seleccione el objeto definido por el sistema para desactivar toda inspección de protocolo

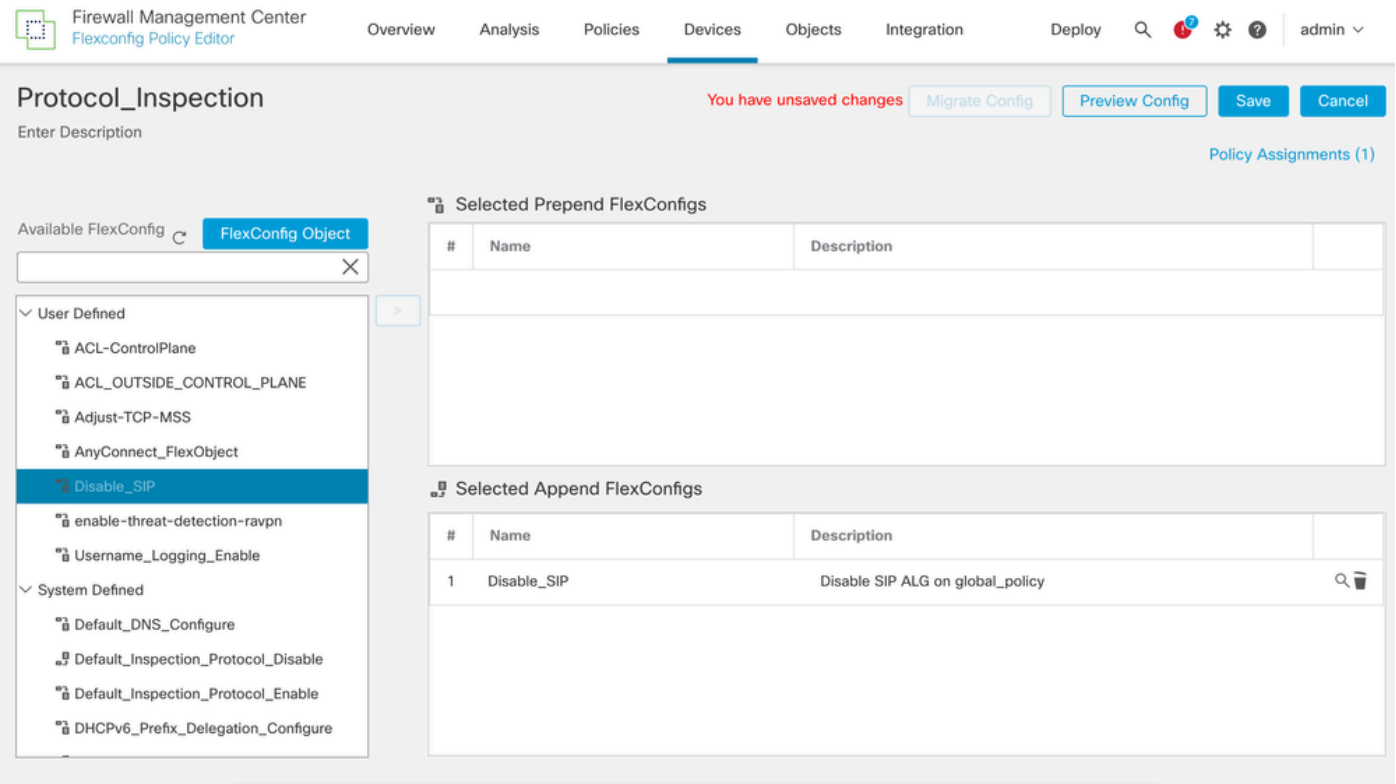
Paso 4.

Una vez seleccionada, confirme que aparece en los cuadros de la derecha, no olvide guardar e implementar la configuración para que surta efecto.



Objeto seleccionado para deshabilitar toda inspección de protocolo

Paso 5.
Para desactivar una inspección de protocolo única, seleccione el objeto creado anteriormente en la lista Definido por el usuario y agréguelo a la directiva mediante la flecha situada entre los cuadros.



Seleccione esta opción para desactivar una inspección de protocolo único desde global_policy

Paso 6.

Una vez seleccionada, confirme que aparece en los cuadros de la derecha, no olvide guardar e implementar la configuración para que surta efecto.

Configuración mediante la CLI de FTD

Esta solución se puede aplicar inmediatamente desde la CLI de FTD para probar si la inspección está afectando al tráfico. Sin embargo, el cambio de configuración no se guarda si se produce un reinicio o una nueva implementación.

El comando debe ejecutarse desde la CLI de FTD en modo de nube.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Verificación

Para verificar que la desactivación del protocolo sea efectiva, ejecute el comando show running-config policy-map. En este ejemplo, la inspección de SIP está inhabilitada porque ya no aparece en la lista de protocolos predeterminados.

```
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#
```

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

- Introducción a la inspección del protocolo de capa de aplicación

- Inspección de los protocolos básicos de Internet
- Show ASP Drop Command Usage

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).