Solucionar problemas de quedas de tráfego devido à inspeção de protocolo LINA no FTD

Contents

Introdução

Este documento descreve como identificar se a inspeção de protocolo LINA para Modular Policy Framework (MPF), gera descarte de tráfego no Cisco Secure FTD.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os mecanismos de inspeção são necessários em um firewall para serviços que incorporam informações de endereçamento IP no pacote de dados do usuário ou que abrem canais secundários em portas atribuídas dinamicamente.

A inspeção de protocolo pode ajudar a evitar que o tráfego mal-intencionado entre na rede, inspecionando o conteúdo dos pacotes de rede e bloqueando ou modificando o tráfego com base no aplicativo ou protocolo que está sendo usado.
Como resultado, os mecanismos de inspeção podem afetar o throughput geral. Vários mecanismos de inspeção comuns são ativados no firewall por padrão; pode ser necessário ativar outros, dependendo da rede.

Configurações padrão

Por padrão, a configuração LINA do FTD inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão.

A inspeção se aplica ao tráfego em todas as interfaces (uma política global).

O tráfego de inspeção de aplicativos padrão inclui o tráfego para as portas padrão para cada protocolo. É possível aplicar somente uma política global. Assim, se desejar alterar a política global, por exemplo, para aplicar inspeção a portas não padrão ou adicionar inspeções que não são habilitadas por padrão, você deverá editar a política padrão ou desabilitá-la e aplicar uma nova política.

Execute o comando show running-config policy-map no LINA, FTD Command Line Interface (CLI) via system support diagnostic-cli, para obter as informações.

```
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
!
```

Identificar quedas de pacotes devido à inspeção de protocolo do MPF

Mesmo quando o tráfego se alinha com a política de controle de acesso (ACP) atribuída ao firewall, em determinados cenários, o processo de inspeção encerra conexões devido ao comportamento de tráfego específico recebido pelo firewall, um design sem suporte, padrão de aplicativo ou uma limitação de inspeção.

Durante a solução de problemas de tráfego, um processo útil a ser usado é:

- Defina logs de captura em tempo real nas interfaces das quais o tráfego flui (interfaces de entrada e saída), comando:

```
firepower# capture

        [interface

        ][match

           [port

           ]
```

```
        [port

        ]]
```

Usando as capturas, você pode incluir a opção packet number X trace detail e deve fornecer o resultado fase por fase que a conexão leva, como faz um comando packet-tracer, mas com esta opção você garante que seja tráfego em tempo real.

```
firepower# show capture

      packet number X trace detail
```

- Set real-time Accelerated Security Path (ASP) Drop, o tipo de captura asp-drop mostra os pacotes ou conexões eliminados pelo ASP, há uma lista de razões que você pode encontrar nos links relacionados do documento, comando:

```
firepower# capture

      [type

      ] [interface
```

```
][match


   [port

   ]

     [port

     ]]
```

Os descartes de inspeção de protocolo podem ser ignorados, pois um resultado de permissão pode ser observado nas fases do packet-tracer. Por isso, é crucial sempre verificar o motivo da queda usando registros de captura em tempo real.

Mensagens de erro comuns de queda

A queda do caminho de segurança acelerado (ASP) é frequentemente usada para fins de depuração para ajudar a solucionar problemas de rede. O comando show asp drop é utilizado para exibir esses pacotes ou conexões descartados, fornecendo insights sobre os motivos dos descartes, que podem incluir problemas como falhas de NAT, falhas de inspeção ou recusas de regras de acesso.

Pontos principais sobre quedas de ASP:

- Quedas de quadros: São descartes relacionados a pacotes individuais, como encapsulamento inválido ou nenhuma rota para o host.
- Quedas de fluxo: Elas estão relacionadas a conexões, como fluxos negados por regras de

acesso ou falhas de NAT.
- Uso: O comando é principalmente para depuração e a saída pode mudar.

Essas mensagens de erro ou motivos para soltar são exemplos que você pode encontrar durante a solução de problemas. Eles podem adiar dependendo do protocolo de Inspeção que está sendo usado.

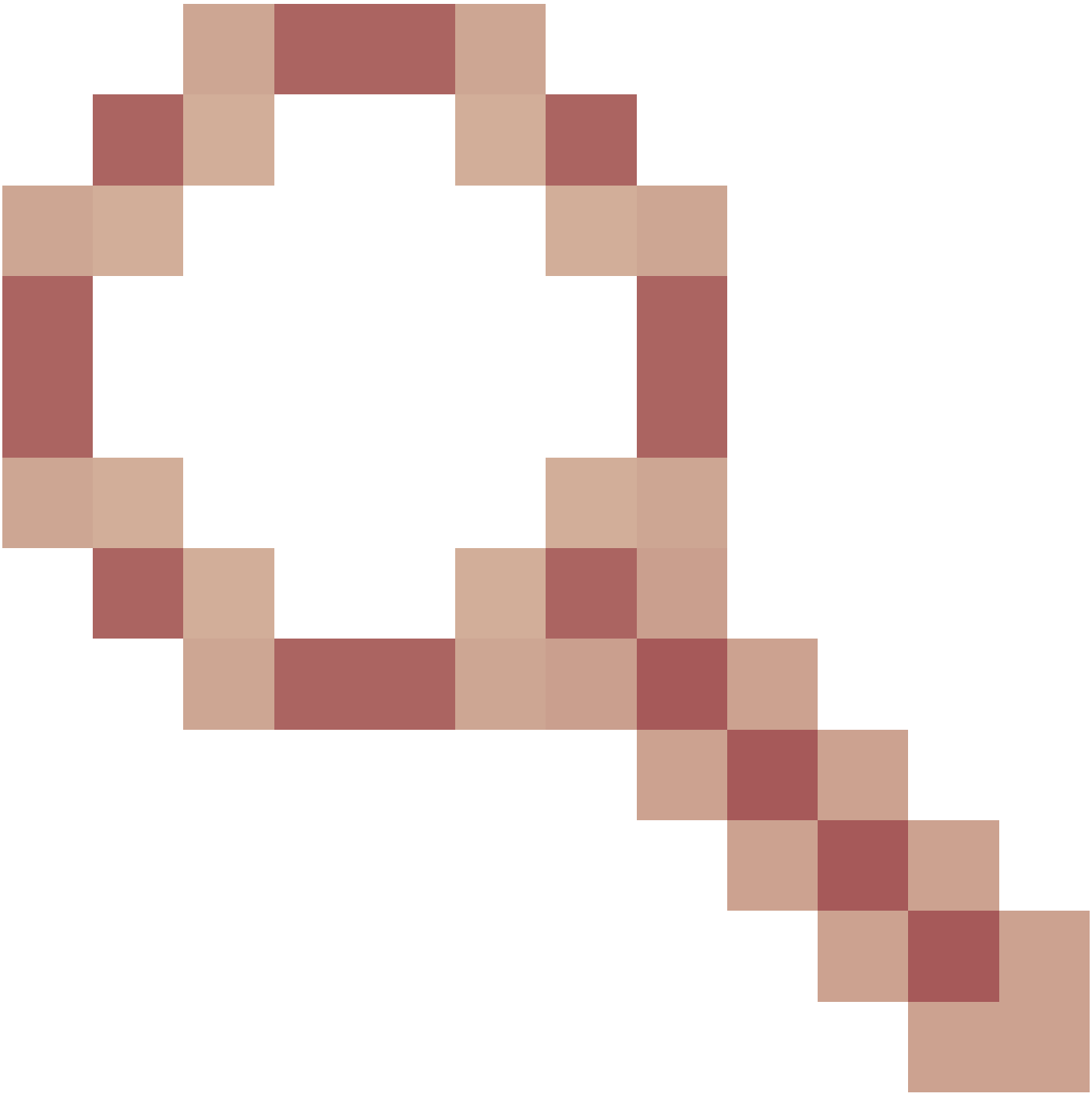
Exemplo de Descarte de Inspeção SUN RPC

Este cenário é para um FTDv de proxy de braço único na implantação AWS, tráfego RPC encapsulado por Geneve, se a inspeção Rpc da Sun estiver habilitada, a conexão será descartada.

A saída mostra quedas de ASP para inspeção de Rpc da Sun, o Rcp da Sun usa a porta 111 como destino. O último pacote é a porta de encapsulamento de Geneve que usa 6081 como destino. A razão de queda na saída, como você pode observar, é "Sem adjacência 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 da Cisco CSCwj00074



[O proxy de braço único de FTDv descarta o tráfego sem adjacência com o inspect sunrpc habilitado]

O tráfego é descartado como "adjacência não válida" no ASP do mecanismo LINA porque o endereço mac origem e destino são subitamente preenchidos com apenas zeros após o segundo pacote (SYN/ACK) do handshake triplo.

Motivo da queda de ASP:

Nome: no-adjacency
Nenhuma adjacência válida:
Esse contador é incrementado quando o Security Appliance recebe um pacote em um fluxo

existente que não tem mais uma adjacência de saída válida. Isso pode ocorrer se o próximo salto não estiver mais acessível ou se uma alteração de roteamento tiver ocorrido normalmente em um ambiente de roteamento dinâmico.

Solução: Desabilite a inspeção de sunrpc.

Exemplo de Eliminação de Inspeção do SQL*NET

Este cenário é para um FTDv de proxy de braço único na implantação AWS, se a inspeção Sql*Nel estiver habilitada, o tráfego encapsulado por Geneve será descartado.

A saída é para as capturas de pacotes mescladas (você pode observar o mesmo número de pacote):
Primeira linha: captura de pacote de queda de asp não encapsulada, o Sql*Net usa a porta 1521 como destino.
Segunda linha: Interface VNI asp-drop em LINA, Geneve usa a porta de encapsulamento 6081 como destino.

Há dois motivos de descarte diferentes na saída, pois eles são "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] Se
95: 07:55:58.771764       10.7.0.3.64056 > 10.7.2.5.6081:  udp 209 [GENEVE segment-id 0 payload-length 1

96    2024-12-14 07:55:58.771780    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53905 -
96: 07:55:58.771780       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length

99    2024-12-14 07:55:58.997049    172.16.0.14    10.0.8.2    TCP    308    53903 → 1521 [PSH, ACK] Se
99: 07:55:58.997049       10.7.0.3.64056 > 10.7.2.5.6081:  udp 266 [GENEVE segment-id 0 payload-length 2

100    2024-12-14 07:55:58.997079    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53903
100: 07:55:58.997079       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length
```

Motivo da queda de ASP:

Nome: tcp-buffer-timeout
Tempo limite de buffer de pacote TCP fora de ordem:
Esse contador é incrementado e o pacote é descartado quando um pacote TCP fora de ordem enfileirado é mantido no buffer por muito tempo. Normalmente, os pacotes TCP são colocados em ordem nas conexões que são inspecionadas pelo Security Appliance ou quando os pacotes são enviados ao SSM para inspeção. Quando o próximo pacote TCP esperado não chegar dentro de um certo período, o pacote fora de serviço enfileirado será descartado.

Recomendações:
O próximo pacote TCP esperado não chega devido ao congestionamento na rede, que é normal em uma rede ocupada. O mecanismo de retransmissão TCP no host final deve retransmitir o pacote e a sessão pode continuar.

Nome: tcp-not-syn
Primeiro pacote TCP não SYN:
Recebido um pacote não SYN como o primeiro pacote de uma conexão não interceptada e não pregada.

Recomendação:
Em condições normais, isso pode ser visto quando o equipamento já fechou uma conexão e o cliente ou servidor ainda acredita que a conexão está aberta e continua a transmitir dados. Alguns exemplos em que isso pode ocorrer são apenas depois que um 'clear local-host' ou 'clear xlate' é emitido. Além disso, se as conexões não tiverem sido removidas recentemente, e o contador estiver aumentando rapidamente, o dispositivo pode estar sob ataque. Capture um farejador de rastreamento para ajudar a isolar a causa.

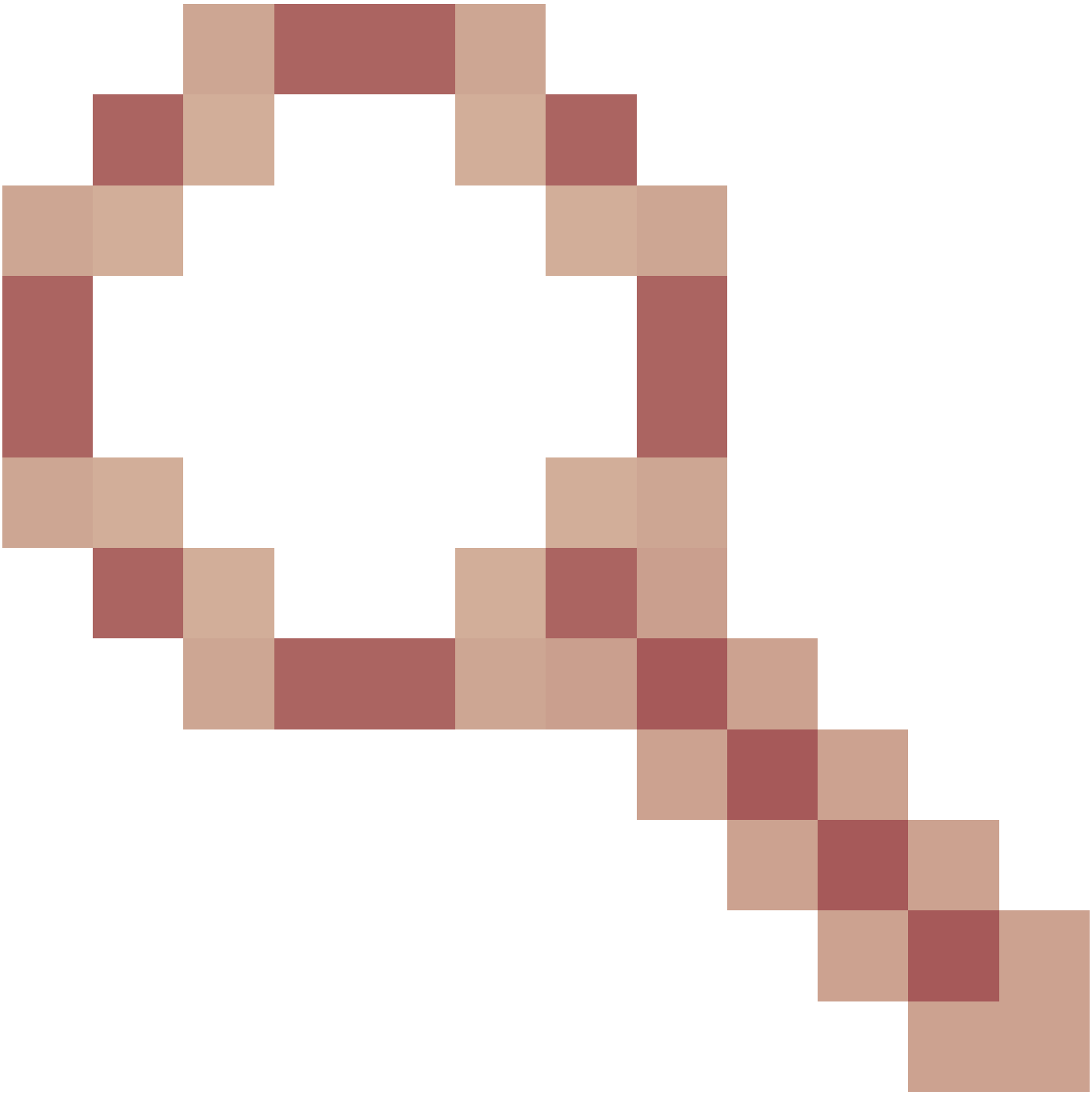
Solução: Desative a inspeção do SQL*Net quando a transferência de dados SQL ocorrer na mesma porta da porta TCP 1521 do controle SQL. O Security Appliance atua como um proxy quando a inspeção do SQL*Net está ativada e reduz o tamanho da janela do cliente de 65000 para sobre 16000 causando problemas de transferência de dados.

Exemplo de Descarte de Inspeção ICMP

Este cenário é para um ambiente de cluster FTD.
O identificador ICMP do cabeçalho ICMP pode ser usado como a porta origem da 5 tupla no fluxo, de modo que todas as 5 tuplas dos pacotes de ping sejam iguais, a razão de queda ASP é "inspect-icmp-seq-num-not-matched", como você pode observar nesta saída.

```
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 bug da Cisco CSCvb92417



O ASA do cluster cai para a caixa ICMP responde com o motivo "inspect-icmp-seq-num-not-matched"

Motivo da queda de ASP:

Nome: inspect-icmp-seq-num-not-matched
Número de sequência de inspeção ICMP não correspondido:
Esse contador deve ser incrementado quando o número de sequência na mensagem de resposta de eco ICMP não corresponder a nenhuma mensagem de eco ICMP que tenha passado pelo aplicativo anteriormente na mesma conexão.

Solução: Desative a Inspeção ICMP. Em ambiente de cluster: dois ou mais FTD em cluster e o tráfego ICMP pode ser assimétrico. É observado que há um atraso para a exclusão do fluxo

ICMP, o ping subsequente é enviado rapidamente antes que o fluxo de ping anterior tenha sido limpo. Nesse caso, pode ocorrer a perda consecutiva de um pacote de ping.

Exemplo de queda de inspeção de SIP

Nesse cenário, as chamadas duraram apenas cinco minutos e a conexão é interrompida. Quando o RTP é usado, a Inspeção de SIP pode descartar conexões.
Como você pode observar na saída da captura de pacotes na interface para tráfego VoIP, a flag BYE no tráfego SIP significa que a chamada telefônica está fechada nesse 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) |
```

Neste outro exemplo, o syslog mostra um IP mapeado que usa PAT, o IP é deixado com apenas uma porta disponível e a sessão SIP aterrou na mesma porta, o SIP falhou devido à alocação de porta. Se o PAT estiver em uso, a inspeção do SIP poderá descartar a conexão.

O motivo da queda do ASP é: "Não é possível criar uma conexão UDP de IP/porta para IP/porta porque o limite de bloco de porta PAT por host de X foi atingido" e "foi encerrado pelo mecanismo de inspeção, motivo - redefinição com base na configuração de 'serviço redefinido'"

```
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 da queda de ASP:

Nome: async-lock-queue-limit
Limite de fila de bloqueio assíncrono excedido:
Cada fila de trabalho de bloqueio assíncrono tem um limite de 1000. Quando mais pacotes SIP tentam ser despachados para a fila de trabalho, o pacote deve ser descartado.

Recomendação:
Somente o tráfego SIP pode ser descartado. Quando os pacotes SIP têm o mesmo bloqueio pai e podem ser enfileirados na mesma fila de bloqueio assíncrono, isso pode resultar em esgotamento de blocos, pois apenas um único núcleo está manipulando todas as mídias. Se um pacote SIP tentar ser enfileirado quando o tamanho da fila de bloqueio assíncrono exceder o limite, o pacote deverá ser descartado.

Nome: sp-looping-address
endereço de loop:
Esse contador é incrementado quando os endereços de origem e destino em um fluxo são os mesmos. Os fluxos SIP onde a privacidade de endereço está habilitada são excluídos, pois é normal que esses fluxos tenham os mesmos endereços de origem e destino.

Recomendação:
Há duas condições possíveis quando esse contador pode ser incrementado. Uma é quando o equipamento recebe um pacote com o endereço origem igual ao destino. Isso representa um tipo de ataque DoS. A segunda é quando a configuração NAT do dispositivo faz NAT de um endereço de origem igual ao do destino.

Nome: pai-fechado
O fluxo pai está fechado:
Quando o fluxo-pai de um fluxo subordinante é fechado, o fluxo subordinante também é fechado. Por exemplo, um fluxo de dados FTP (fluxo subordinante) pode ser fechado com esse motivo específico quando seu fluxo de controle (fluxo pai) é encerrado. Esta razão também é dada quando um fluxo secundário (orifício de pino) é fechado por sua aplicação de controle. Por exemplo, quando a mensagem BYE é recebida, o mecanismo de inspeção SIP (aplicativo de controle) deve fechar os fluxos RTP SIP correspondentes (fluxo secundário).

Solução: Desabilite a Inspeção SIP. Devido a limitações no protocolo:

- A inspeção SIP suporta apenas o recurso Bate-papo. O quadro de comunicações, a transferência de arquivos e o compartilhamento de aplicativos não são suportados. O RTC Client 5.0 não é suportado.
- Ao usar o PAT, qualquer campo do cabeçalho SIP que contenha um endereço IP interno sem uma porta não pode ser convertido e, portanto, o endereço IP interno pode vazar para fora. Se desejar evitar esse vazamento, configure NAT em vez de PAT.
- A inspeção SIP é ativada por padrão usando o mapa de inspeção padrão, que inclui:
  * Extensões de mensagens instantâneas (IM) SIP: Habilitado.
  * Tráfego não SIP na porta SIP: Descartado.
  * Ocultar endereços IP do servidor e do ponto de extremidade: Desabilitado.
  * Mascarar a versão do software e os URIs não SIP: Desabilitado.
  * Verifique se o número de saltos até o destino é maior que 0: Habilitado.
  * Conformidade RTP: Não aplicado.
  * Conformidade com SIP: Não executar verificação de estado e validação de cabeçalho.

Troubleshooting

Estes são alguns dos comandos sugeridos para solucionar problemas de tráfego relacionados à inspeção do protocolo LINA MPF.

- Show service-policy exibe as estatísticas de política de serviço para as inspeções 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 exemplo de saída do comando show service-policy inspect http mostra as estatísticas 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
```

- Defina uma captura asp-drop na interface a ser inspecionada.

```
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
```

Como ativar ou desativar inspeções específicas de aplicativos LINA MPF

Estas são as opções disponíveis para ativar ou desativar as inspeções do aplicativo MPF LINA no Cisco Secure Firewall Threat Defense.

- Configuração sobre FlexConfig: Você precisa de acesso de administrador à interface do usuário do FMC; essa alteração é permanente na configuração.
- Configuração sobre CLI de FTD: Você precisa de acesso de administrador à CLI do FTD; essa alteração não é permanente; se uma reinicialização ou uma nova implantação ocorrer, a configuração será removida.

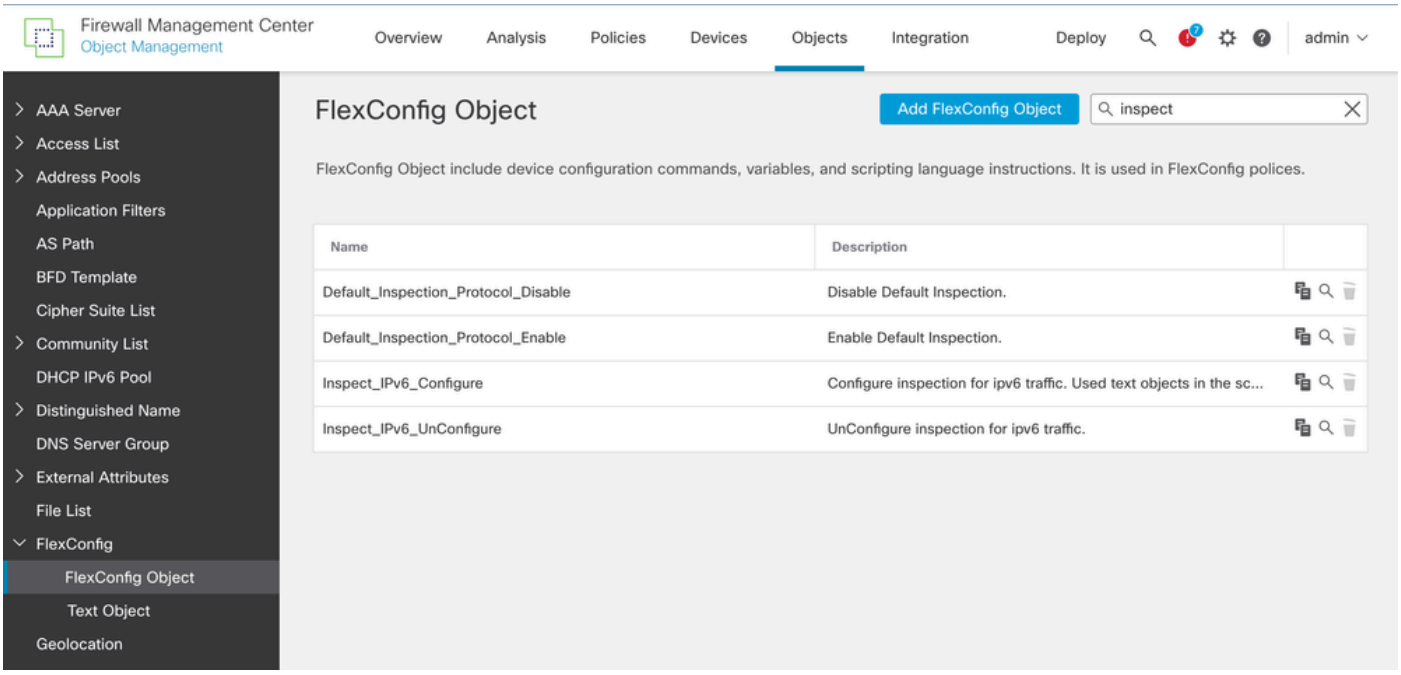
Configuração sobre FlexConfig

O FlexConfig é um método de último recurso para configurar recursos baseados em ASA que são compatíveis com a defesa contra ameaças, mas que não podem ser configurados no centro de gerenciamento.

A configuração para desabilitar ou habilitar a inspeção permanentemente está no FlexConfig pela interface do usuário do FMC, ela pode ser aplicada globalmente ou apenas para tráfego específico.

Etapa 1.

Na interface do usuário do FMC, navegue até Objects > Object Management > FlexConfig > FlexConfig Object, onde você poderá encontrar a lista dos objetos padrão de Protocol Inspection.



Objetos de inspeção de protocolo FlexConfig padrão

Etapa 2.

Para desativar uma inspeção de protocolo específica, você pode criar um Objeto FlexConfig.

Navegue até Objetos > Gerenciamento de objetos > FlexConfig > Objeto FlexConfig > Adicionar objeto FlexConfig

Neste exemplo, a configuração para desativar a Inspeção SIP da global_policy, a sintaxe deve ser:

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

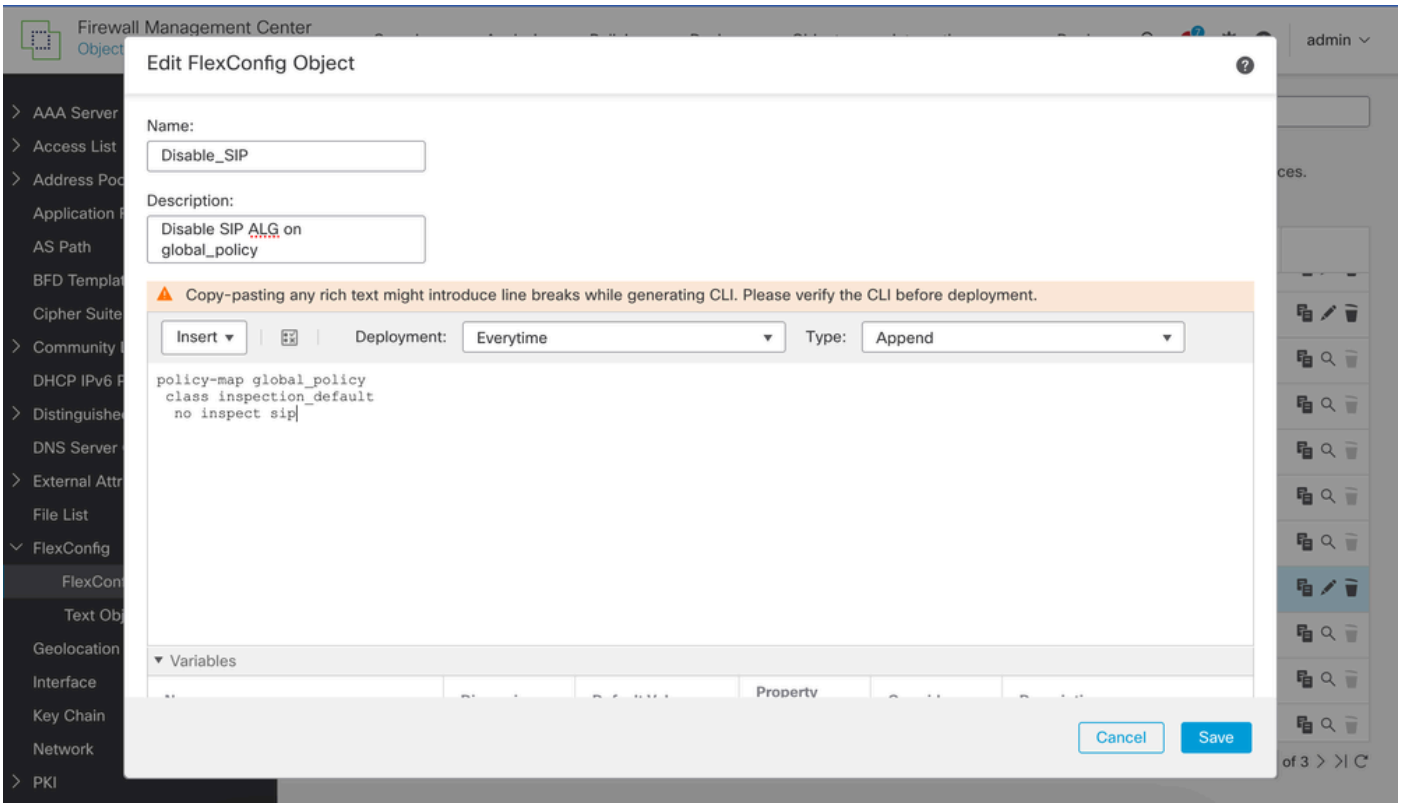
Ao configurar um objeto FlexConfig, você pode escolher a frequência e o tipo de implantação.

Implantação

- Se o objeto FlexConfig apontar para objetos gerenciados pelo sistema, como objetos de rede ou ACL, escolha Everytime. Caso contrário, as atualizações dos objetos não poderiam ser implantadas.
- Use Once se a única coisa que você fizer no objeto for limpar uma configuração. Em seguida, remova o objeto da política FlexConfig após a próxima implantação.

Tipo

- Append (O padrão.) Os comandos no objeto são colocados no final das configurações geradas das políticas do centro de gerenciamento. Você deve usar Anexar se usar variáveis de objeto de política, que apontam para objetos gerados a partir de objetos gerenciados. Se os comandos gerados para outras políticas se sobrepõem àqueles especificados no objeto, você deve selecionar essa opção para que seus comandos não sejam substituídos. Essa é a opção mais segura.
- Preceder. Os comandos no objeto são colocados no início das configurações geradas a partir das políticas do centro de gerenciamento. Normalmente, você usaria prepend para comandos que limpam ou negam uma configuração.



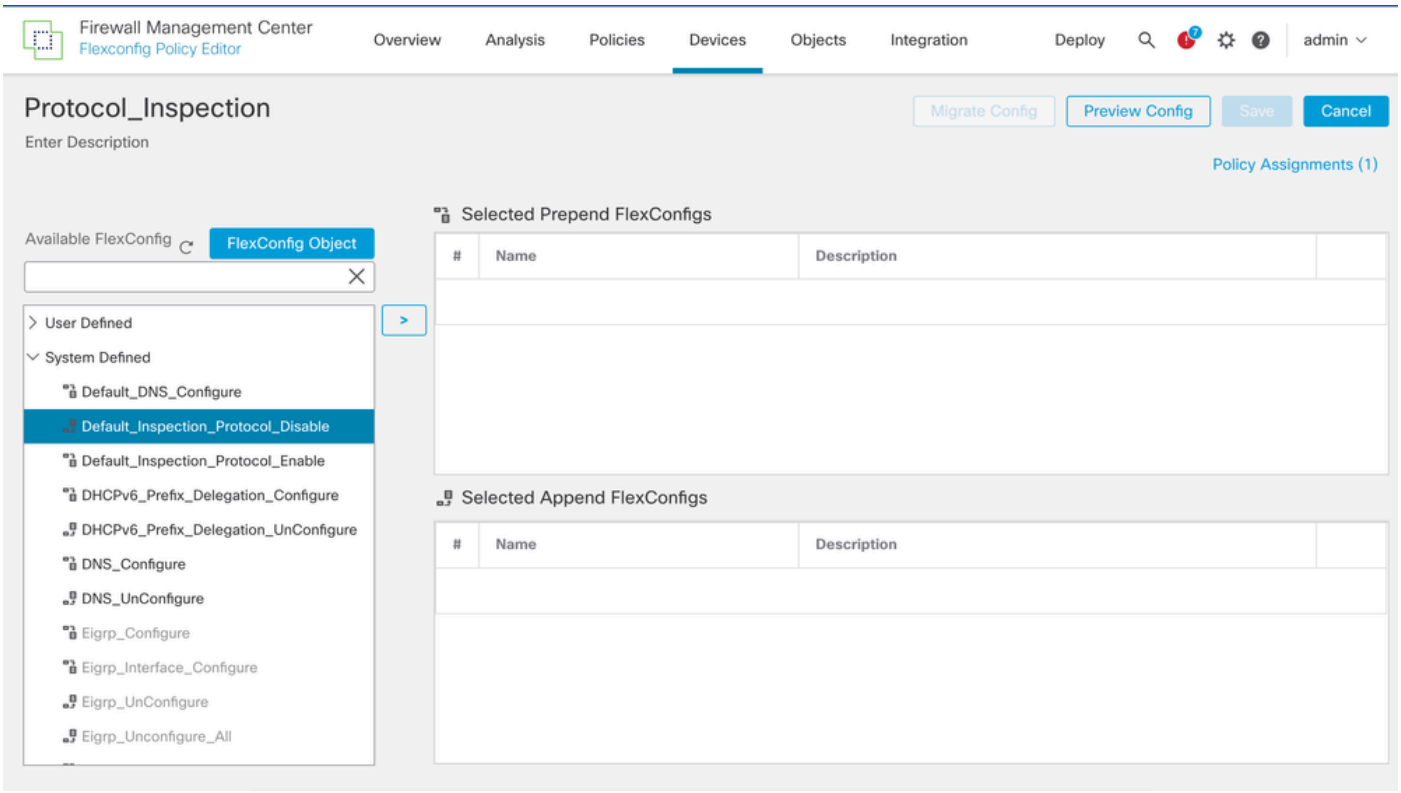
Crie um objeto para desativar um único protocolo da global_policy padrão

Etapa 3.

Adicione os objetos na política FlexConfig atribuída ao LINA.

Navegue até Devices > FlexConfig e selecione a política FlexConfig aplicada ao firewall com problemas de remoção.

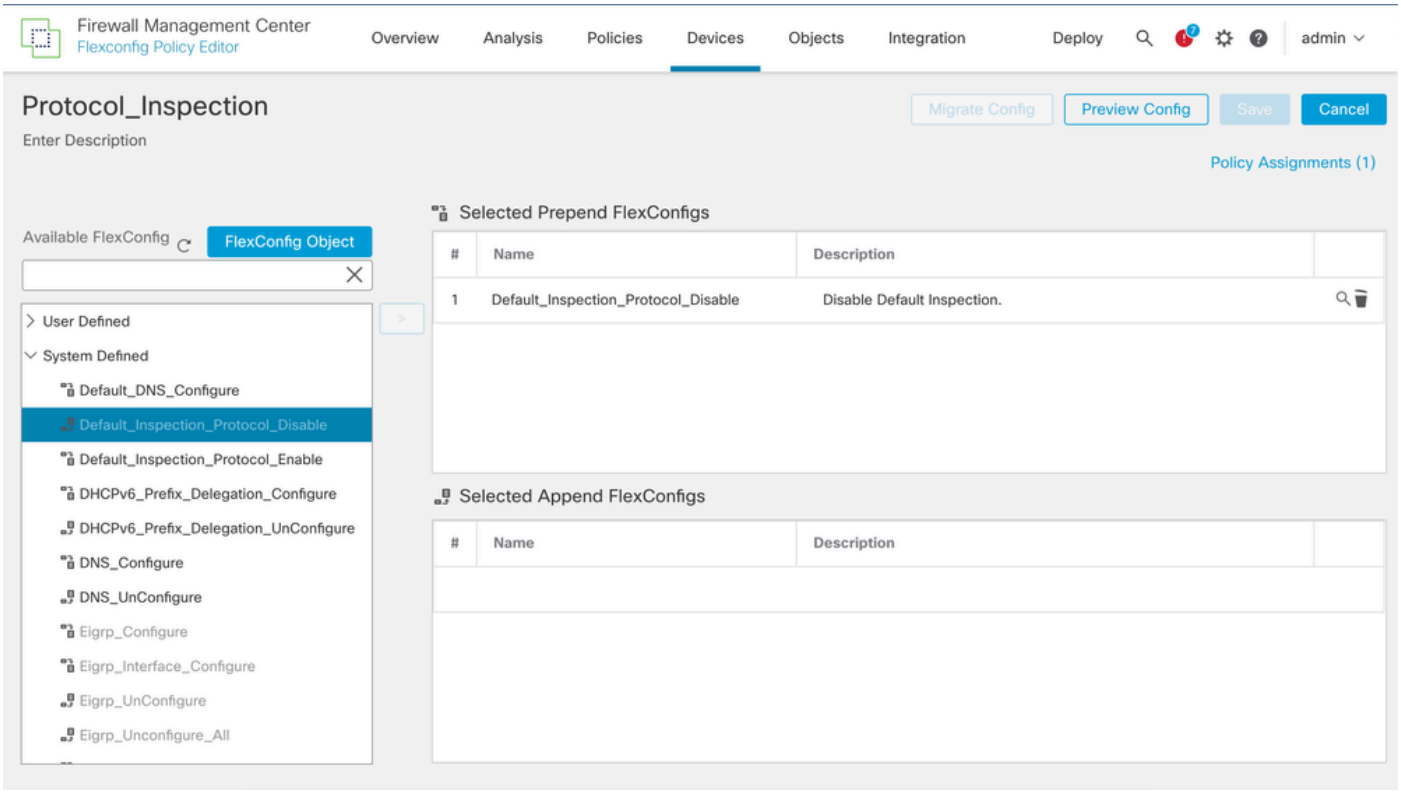
Para desativar toda a inspeção globalmente, selecione o Objeto Default_Inspection_Protocol_Disable em Objetos FlexConfig Definidos pelo Sistema e clique na seta azul no meio para adicioná-lo à Política FlexConfig.



Selecione o objeto definido pelo sistema para desativar toda a inspeção de protocolo

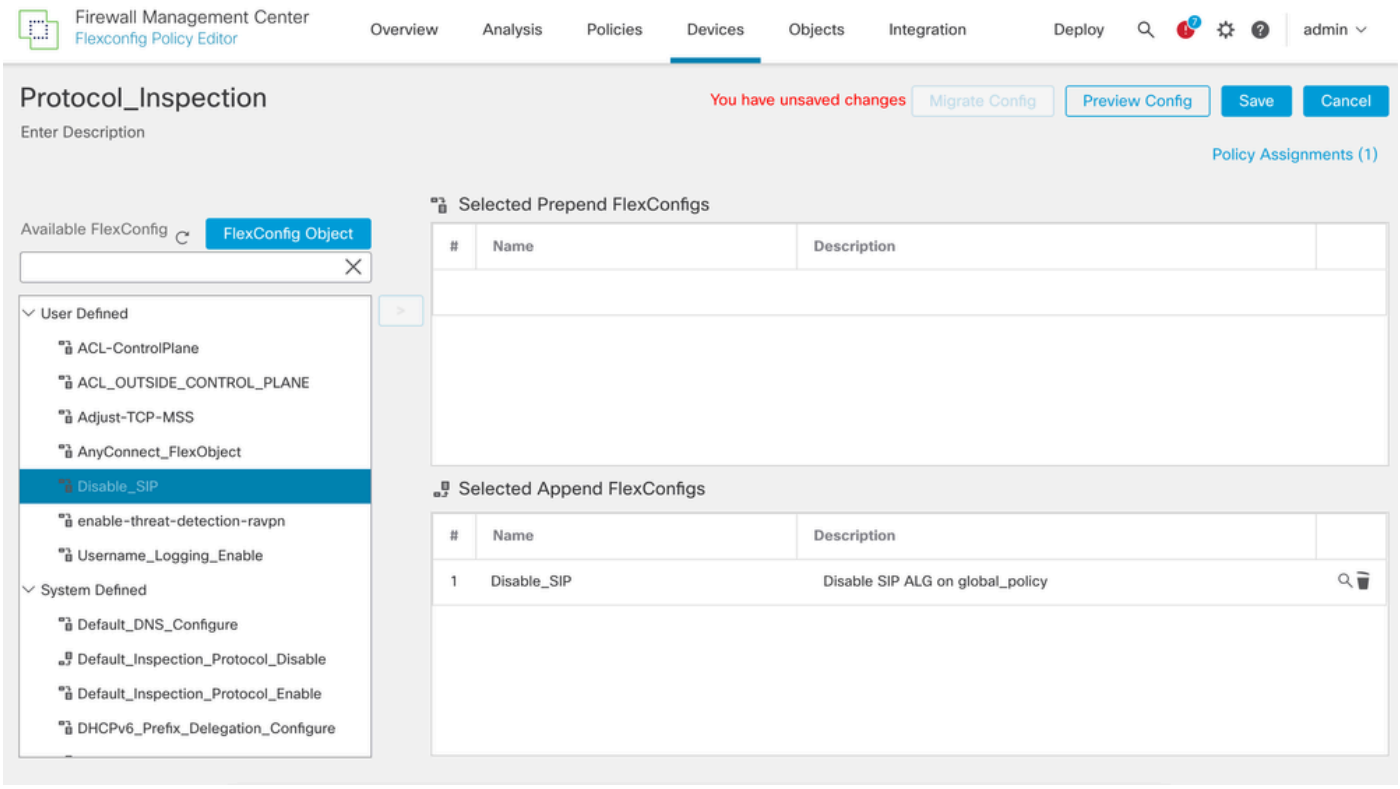
Etapa 4.

Depois de selecionada, confirme se ela aparece nas caixas à direita. Não se esqueça de salvar e implantar a configuração para entrar em vigor.



Objeto selecionado para desativar toda a inspeção de protocolo

Etapa 5.
Para desativar uma única inspeção de protocolo, selecione o objeto criado anteriormente na lista Definido pelo usuário e adicione-o à política usando a seta entre as caixas.



Selecione para Desativar uma Inspeção de Protocolo Único na global_policy

Etapa 6.

Depois de selecionada, confirme se ela aparece nas caixas à direita. Não se esqueça de salvar e implantar a configuração para entrar em vigor.

Configuração usando a CLI de FTD

Essa solução pode ser aplicada imediatamente a partir da CLI do FTD para testar se a inspeção está afetando o tráfego. No entanto, a alteração de configuração não será salva se ocorrer uma reinicialização ou uma nova implantação.

O comando deve ser executado a partir da CLI do FTD no modo de Clicar.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

Verificar

Para verificar se a desabilitação do protocolo é efetiva, execute o comando show running-config policy-map. Neste exemplo, a inspeção de SIP é desativada, pois não aparece mais na lista de protocolos padrão.

```
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#
```

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

- Introdução à Inspeção de Protocolo da Camada de Aplicação
- Inspeção de protocolos básicos da Internet
- Mostrar Uso do Comando Drop do ASP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.