排除由于FTD上的LINA协议检查导致的流量丢弃故障

目录

简介

本文档介绍如何识别模块化策略框架(MPF)的LINA协议检测是否丢弃思科安全FTD中的流量。

先决条件

思科建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)。
- 思科安全防火墙管理器中心(FMC)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 虚拟思科安全防火墙威胁防御(FTD)，版本7.4.2
- 虚拟思科安全防火墙管理器中心(FMC)，版本7.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。用于本文的所有设备始于初始（默认

）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

防火墙中需要检查引擎来提供以下服务：在用户数据包中嵌入IP寻址信息，或在动态分配的端口上打开辅助信道。

协议检测可通过检测网络数据包的内容并根据所使用的应用或协议阻止或修改流量来帮助防止恶意流量进入网络。
因此，检测引擎可能会影响整体吞吐量。防火墙上默认启用多个常用检测引擎，可能需要启用其他检测引擎，具体取决于网络。

默认配置

默认情况下，FTD LINA配置包含与所有默认应用检测流量匹配的策略。

检测适用于所有接口上的流量（全局策略）。

默认应用程序检查流量包括到每个协议的默认端口的流量。只能应用一个全局策略。因此，如果要改变全局策略（例如，对非标准端口应用检查，或者添加默认情况下未启用的检查），则需要编辑默认策略，或者禁用默认策略并应用新的策略。

通过system support diagnostic-cli在LINA、FTD Command Line Interface(CLI)上运行show running-config policy-map命令以获取信息。

```
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
!
```

识别由于MPF协议检测导致的数据包丢弃

即使流量与分配给防火墙的访问控制策略(ACP)一致，在某些场景中，检查过程也会因防火墙接收的特定流量行为、不受支持的设计、应用标准或检查限制而终止连接。

在流量故障排除期间，一个有用的流程是：

- 在流量流经的接口（入口和出口接口）上设置实时捕获日志，命令：

```
firepower# capture

        [interface

        ][match


           [port

           ]


             [port

             ]]
```

使用捕获时，可以包括packet number X trace detail选项，它必须提供连接所经过的逐阶段结果，与packet-tracer命令相同，但使用此选项可以确保它是实时流量。

```
firepower# show capture

        packet number X trace detail
```

- 设置实时加速安全路径(ASP)丢弃(Set real-time Accelerated Security Path [ASP] Drop)，捕获类型asp-drop显示ASP丢弃的数据包或连接，在文档的相关链接中有一个原因列表，命令：

```
firepower# capture

        [type

        ] [interface

         ][match


            [port

            ]

              [port

              ]]
```

可以忽略协议检测丢弃，因为allow结果可以在Packet Tracer阶段观察到。因此，务必使用实时捕获日志来验证丢弃原因。

常见丢弃错误消息

加速安全路径(ASP)丢弃通常用于调试目的，以帮助排除网络问题。show asp drop命令用于显示这些丢弃的数据包或连接，从而提供对丢弃原因的见解，这可能包括NAT故障、检测故障或访问规则拒绝等问题。

有关ASP丢弃的要点：

- 帧丢弃:这些是与单个数据包相关的丢弃，例如封装无效或没有到主机的路由。
- 流丢弃:这些与连接相关，例如访问规则拒绝的流或NAT故障。
- 使用率:该命令主要用于调试，输出可能会改变。

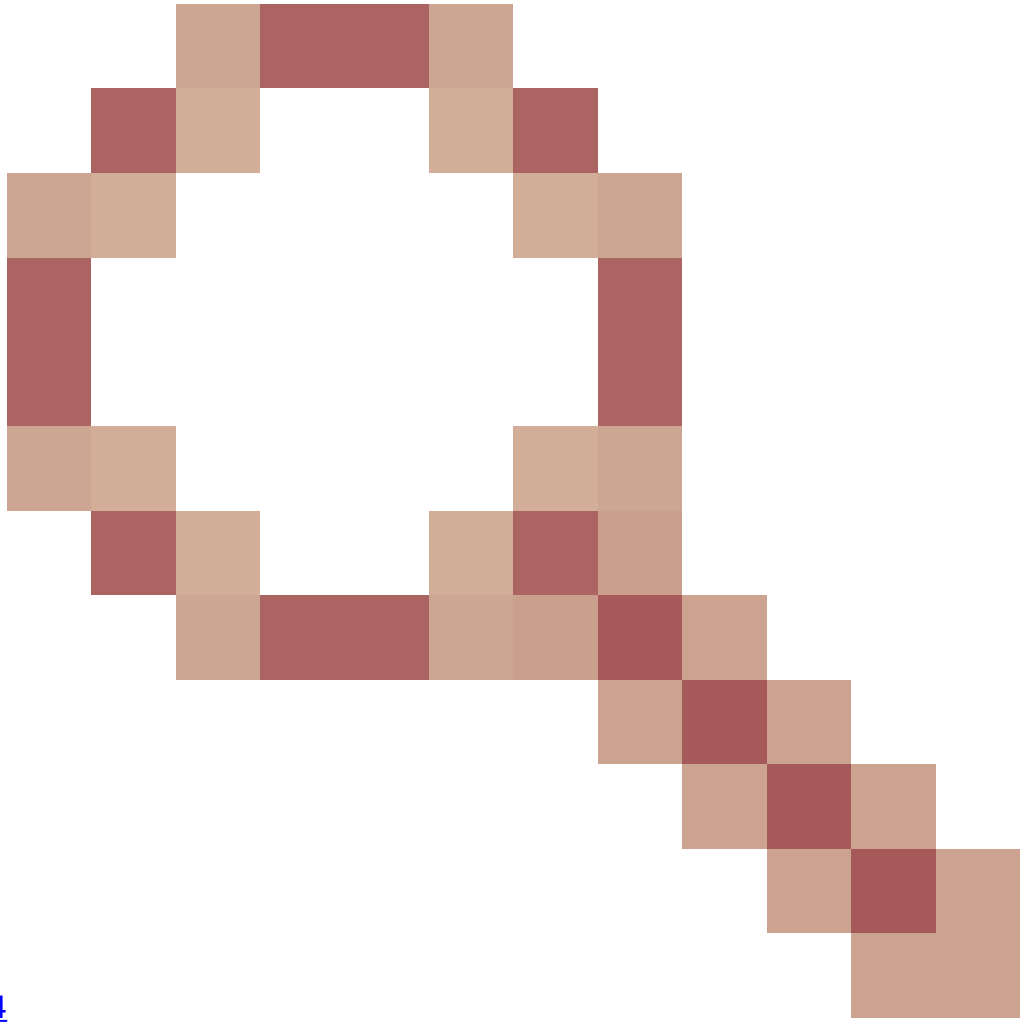
这些错误消息或丢弃原因都是您在故障排除过程中遇到的示例。它们可以根据正在使用的检测协议进行延迟。

SUN RPC检测丢弃示例

此场景适用于AWS部署中的单臂代理FTDv，即Geneve封装的RPC流量，如果启用Sun Rpc检查，则连接会断开。

输出显示用于Sun Rpc检测的ASP丢弃，Sun Rcp使用端口111作为目标最后一个数据包是使用6081作为目标的Geneve封装端口。您可以观察到，输出中的丢弃原因为“无有效邻接关系”

```
firepower# show capture asp-drop
...
8: 16:23:02.462958 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
9: 16:23:09.769338 10.0.0.5.780 > 172.16.0.3.111: P 1795131583:1795131679(96) ack 526534108 win 29200 D
10: 16:23:10.148658 172.16.0.3.111 > 10.0.0.5.780: . ack 4026726685 win 26880 Drop-reason: (no-adjacenc
11: 16:23:10.463004 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
12: 16:23:26.462729 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
13: 16:23:27.548692 10.79.67.11.60855 > 10.79.67.4.6081: udp 176 [GENEVE segment-id 0 payload-length 13
```



Cisco Bug ID CSCwj00074

FTDv单臂代理在启用了inspect sunrpc的情况下丢弃无邻接的流量

在LINA引擎的ASP中，流量被丢弃为“无效邻接”，因为源和目标MAC地址在三次握手的第二个数据包(SYN/ACK)之后突然填充为全部为零。

ASP删除原因：

名称：无邻接关系
无有效邻接关系：
　当安全设备收到不再具有有效输出邻接关系的现有流上的数据包时，此计数器增加。如果下一跳不再可访问，或者通常在动态路由环境中发生了路由更改，则会发生这种情况。

解决方案：禁用sunrpc检测。

SQL*NET检测丢弃示例

此场景适用于AWS部署中的单臂代理FTDv，如果启用了Sql*Nel检测，Geneve封装的流量将被丢弃。

输出适用于合并的数据包捕获（您可以观察相同的数据包编号）：
第一行：asp-drop数据包捕获未封装，Sql*Net使用1521端口作为目标。

第二行：LINA上的VNI接口asp-drop，Geneve使用封装端口6081作为目标。

输出中有两个不同的丢弃原因，因为您可以观察它们是“tcp-buffer-timeout”和“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
```

ASP删除原因：

名称：TCP缓冲区超时
TCP无序数据包缓冲区超时：
　当队列无序的TCP数据包在缓冲区中保留时间过长时，此计数器将递增并丢弃数据包。通常，TCP数据包在安全设备检查的连接上或数据包发送到SSM进行检查时按顺序排列。当下一个期望的TCP数据包在一段时间内未到达时，排队的无序数据包将被丢弃。

建议：
　下一个预期的TCP数据包不会到达，因为网络拥塞在繁忙网络中是正常的。终端主机中的TCP重新传输机制必须重新传输数据包，会话才能继续。

名称：tcp-not-syn
第一个TCP数据包不是SYN:
　收到一个非SYN数据包，作为第一个未拦截且未固定的连接数据包。

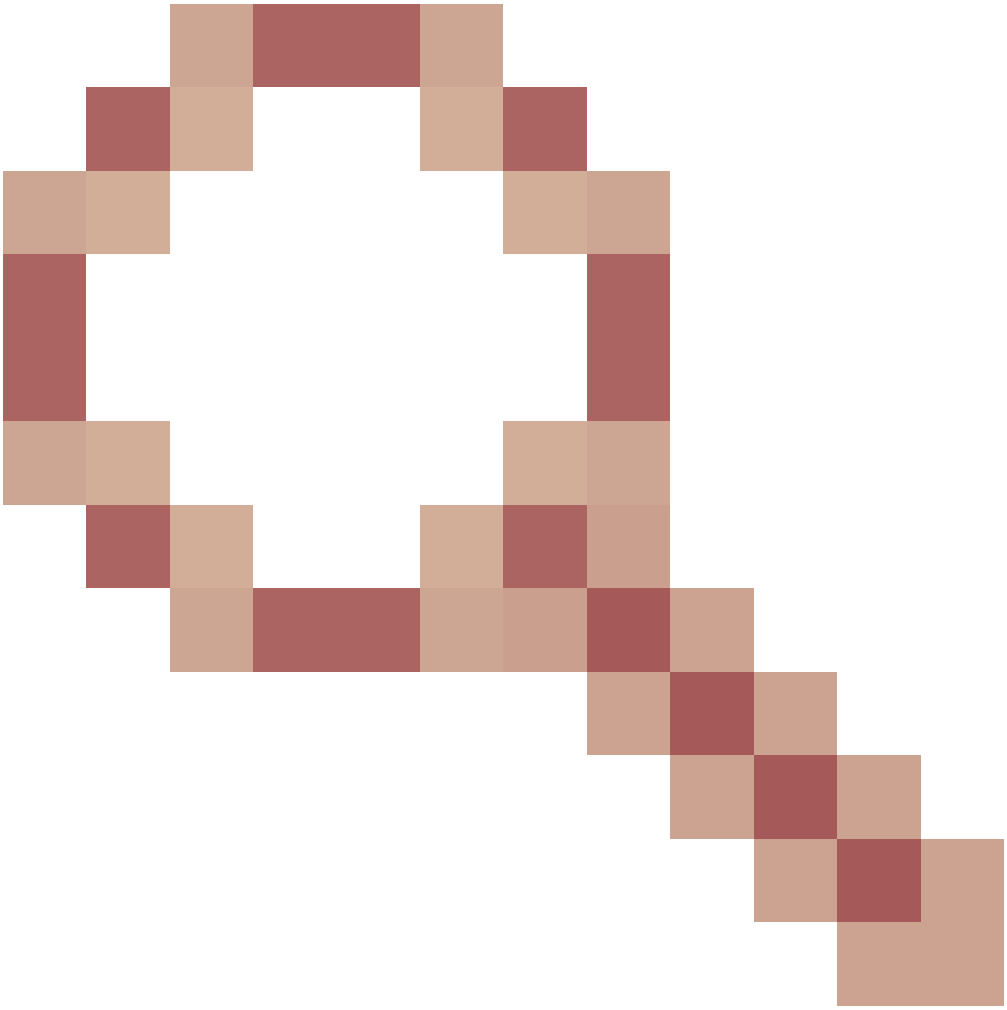
建议：
　在正常情况下，当设备已关闭连接，并且客户端或服务器仍认为连接已打开并继续传输数据时，可以看到这种情况。 有些示例可能发生在发出“clear local-host”或“clear xlate”之后。此外，如果最近未删除连接，并且计数器快速增加，则设备可能受到攻击。捕获嗅探器踪迹以帮助查明原因。

解决方案：当SQL数据传输与SQL控制TCP端口1521发生在同一端口上时，禁用SQL*Net检查。启用SQL*Net检查时，安全设备充当代理，并将导致数据传输问题的客户端窗口大小从65000减小到16000。

ICMP检测丢弃示例

此方案适用于FTD集群环境。
ICMP报头的ICMP标识符可用作流中5元组的源端口，因此ping数据包的所有5元组都是相同的，ASP丢弃原因为“inspect-icmp-seq-num-not-matched”，正如您在此输出中所看到的。

```
firepower#show cap asp-drop
 1: 19:47:09.293136 10.0.5.8 > 10.50.0.53 icmp: echo reply Drop-reason: (inspect-icmp-seq-num-not-matc
```



Cisco Bug ID CSCvb92417

集群ASA丢弃具有原因“inspect-icmp-seq-num-not-matched”的现成ICMP应答

ASP删除原因：

名称：inspect-icmp-seq-num-not-matched
ICMP检查序列号不匹配：
　当ICMP回应应答消息中的序列号与之前在同一连接上通过设备的任何ICMP回应消息都不匹配时，此计数器必须递增。

解决方案：禁用ICMP检测。在群集环境中：集群中的两个或多个FTD，并且ICMP流量可以是非对称的。观察到ICMP流删除存在延迟，后续ping会在前一个ping流清理完成之前快速发送。在这种情况下，可能会发生连续ping数据包丢失。

SIP检测丢弃示例

在这种情况下，呼叫仅持续五分钟，然后连接断开。使用RTP时，SIP检测可以丢弃连接。
正如您在接口上有关VoIP流量的数据包捕获输出中所看到的，SIP流量中的BYE标志表示电话呼叫在当时已关闭。

```
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) |
```

在此其他示例中，系统日志显示使用PAT的映射IP，该IP仅有一个可用端口，并且SIP会话位于同一端口，SIP由于端口分配而失败。如果正在使用PAT，则SIP检测可以断开连接。

ASP丢弃原因如下："由于达到每主机PAT端口块限制X而无法创建从IP/端口到IP/端口的UDP连接"和"被检查引擎终止，原因 — 根据'service resetinboud'配置重置"

```
Nov 18 2019 10:19:34: %FTD-6-607001: Pre-allocate SIP Via UDP secondary channel for 3111:10.11.0.13/506
Nov 18 2019 10:19:35: %FTD-6-302022: Built backup stub TCP connection for identity:172.16.2.20/2325 (17
Nov 18 2019 10:19:38: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:38: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
Nov 18 2019 10:19:39: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:39: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
```

ASP删除原因：

名称：async-lock-queue-limit
超出异步锁定队列限制：
每个异步锁定工作队列的限制为1000。当尝试向工作队列分派更多SIP数据包时，必须丢弃数据包。
建议：
只能丢弃SIP流量。当SIP数据包具有相同的父锁定且可以排队到相同的异步锁定队列中时，可能导致块耗尽，因为只有单个核心处理所有媒体。如果异步锁定队列的大小超过限制时SIP数据包尝试排队，则必须丢弃该数据包。

名称：sp循环地址
循环地址：
当流中的源地址和目的地址相同时，此计数器递增。 启用了地址隐私的SIP流被排除，因为这些流具有相同的源和目标地址是正常的。

建议：
此计数器可能会增加两个条件。一种是设备收到源地址等于目标的数据包时。这表示一种DoS攻击。 第二种情况是，设备的NAT配置将源地址转换为与目标地址相同的源地址。

名称：父关闭
父流已关闭：
当从属流的父流关闭时，从属流也关闭。 例如，当FTP数据流（从属流）的控制流（父流）终止时，可以使用此特定原因关闭FTP数据流。 当二次流（针孔）被其控制应用关闭时，也给出了这个原因。 例如，当收到BYE消息时，SIP检测引擎（控制应用）必须关闭相应的SIP RTP流（辅助流）。

解决方案：禁用SIP检测。由于协议的限制：

- SIP检测仅支持聊天功能。不支持白板、文件传输和应用共享。不支持RTC客户端5.0。
- 使用PAT时，包含不带端口的内部IP地址的任何SIP报头字段都不能转换，因此内部IP地址可能会泄露到外部。如果要避免此泄漏，请配置NAT而不是PAT。
- 默认情况下，使用默认检测映射启用SIP检测，包括：
  * SIP即时消息(IM)扩展：启用.
  * SIP端口上的非SIP流量：已丢弃.
  *隐藏服务器和终端IP地址：禁用.
  *屏蔽软件版本和非SIP URI:禁用.
  *确保到目标的跳数大于0:启用.
  * RTP一致性：未执行。
  * SIP一致性：请勿执行状态检查和报头验证。

故障排除

以下是对LINA MPF协议检查相关的流量问题进行故障排除的一些建议命令。

- Show service-policy显示启用的LINA MPF检查的服务策略统计信息。

```
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
```

show service-policy inspect http命令的输出示例显示http统计信息：

```
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
```

- 在要检查的接口上设置asp-drop捕获。

```
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
```

如何启用或禁用特定LINA MPF应用检测

这些选项可用于在思科安全防火墙威胁防御中启用或禁用MPF LINA应用检测。

- 通过FlexConfig进行配置：您需要具有对FMC UI的管理员访问权限，此更改对配置是永久性的。
- FTD CLI上的配置：您需要具有对FTD CLI的管理员访问权限，此更改不是永久的，如果发生重新启动或新部署，配置将被删除。

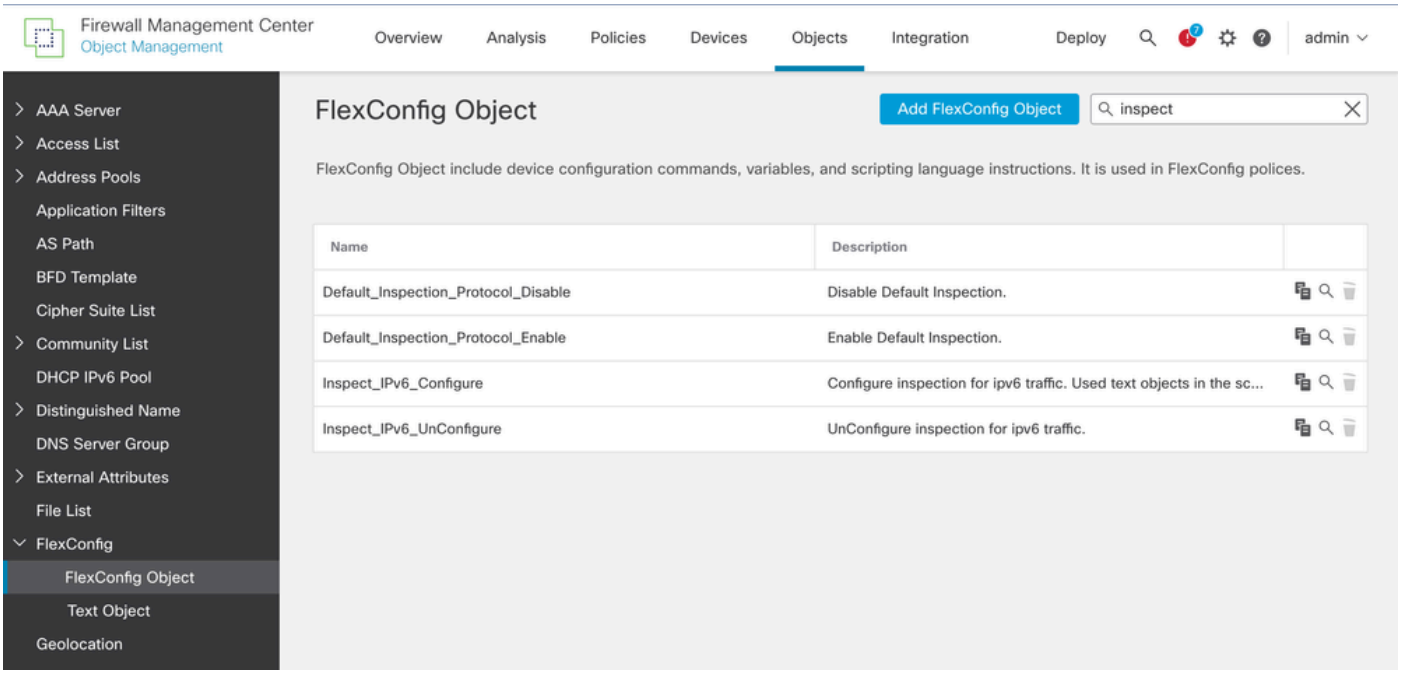
通过FlexConfig配置

FlexConfig是一种最后选用方法，用于配置基于ASA的功能，这些功能与威胁防御兼容，但在管理中心中无法以其他方式进行配置。

永久禁用或启用检测的配置位于FMC UI上的FlexConfig上，可以全局应用该配置，也可以仅应用于特定流量。

步骤1:

在FMC UI上，导航到对象>对象管理> FlexConfig > FlexConfig对象，在那里可以找到默认协议检测对象的列表。



默认FlexConfig协议检测对象

Step 2.

要禁用特定协议检测，可以创建FlexConfig对象。

导航到对象>对象管理> FlexConfig > FlexConfig对象>添加FlexConfig对象

在本示例中，要从global_policy禁用SIP检测，其语法必须是：

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

配置FlexConfig对象时，可以选择部署频率和类型。

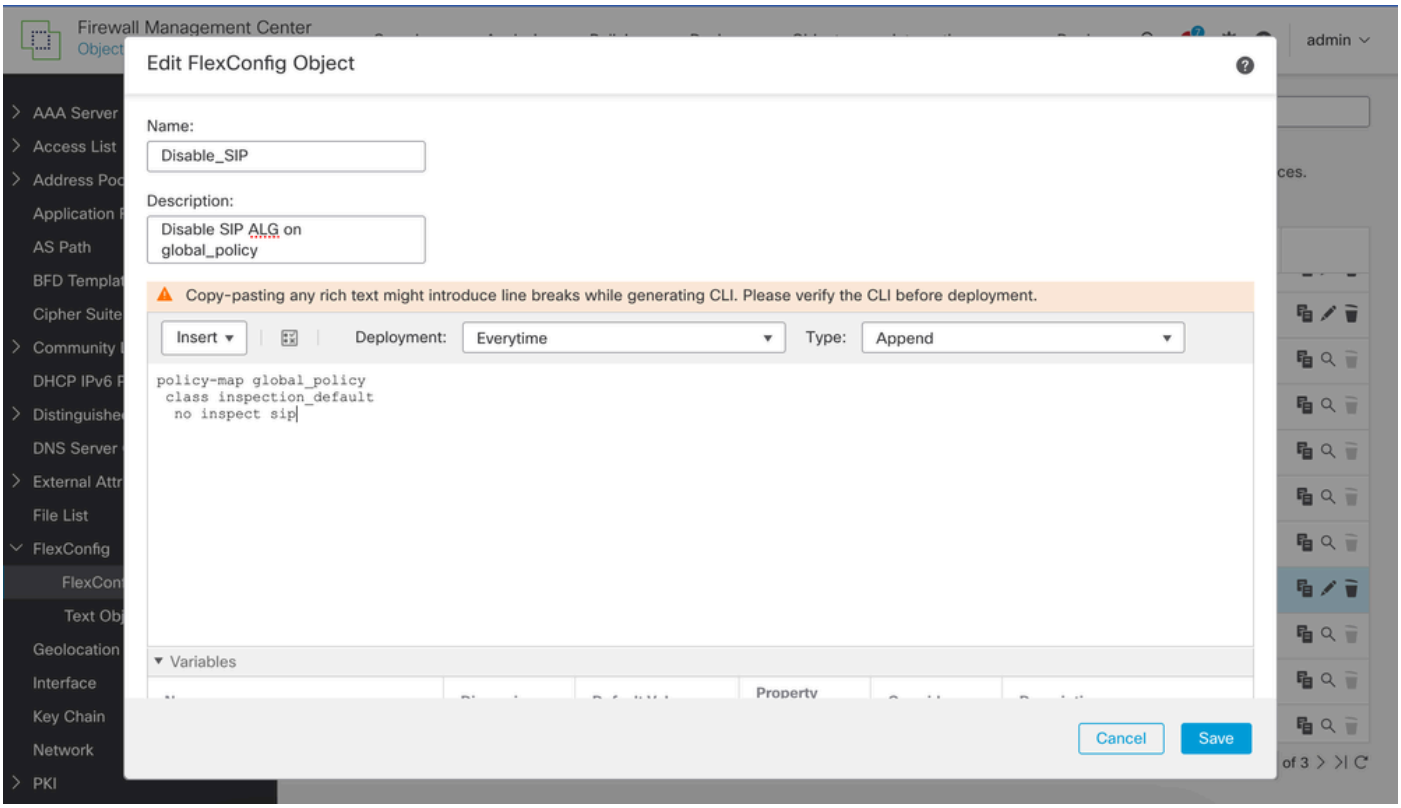
部署

- 如果FlexConfig对象指向系统管理的对象，例如网络或ACL对象，请选择Everytime。否则，无法部署对象的更新。
- 如果对象中唯一要清除的配置时，请使用一次。然后，在下次部署后从FlexConfig策略中删除对象。

类型

- Append（默认值。）对象中的命令放置在管理中心策略生成的配置的末尾。如果使用策略对象变量（指向从受管对象生成的对象），则必须使用Append。如果为其他策略生成的命令与对象中指定的命令重叠，则必须选择此选项，以便命令不会被覆盖。这是最安全的选项。

- 预置。对象中的命令放置在管理中心策略生成的配置的开头。您通常使用prepend命令来清除或否定配置。



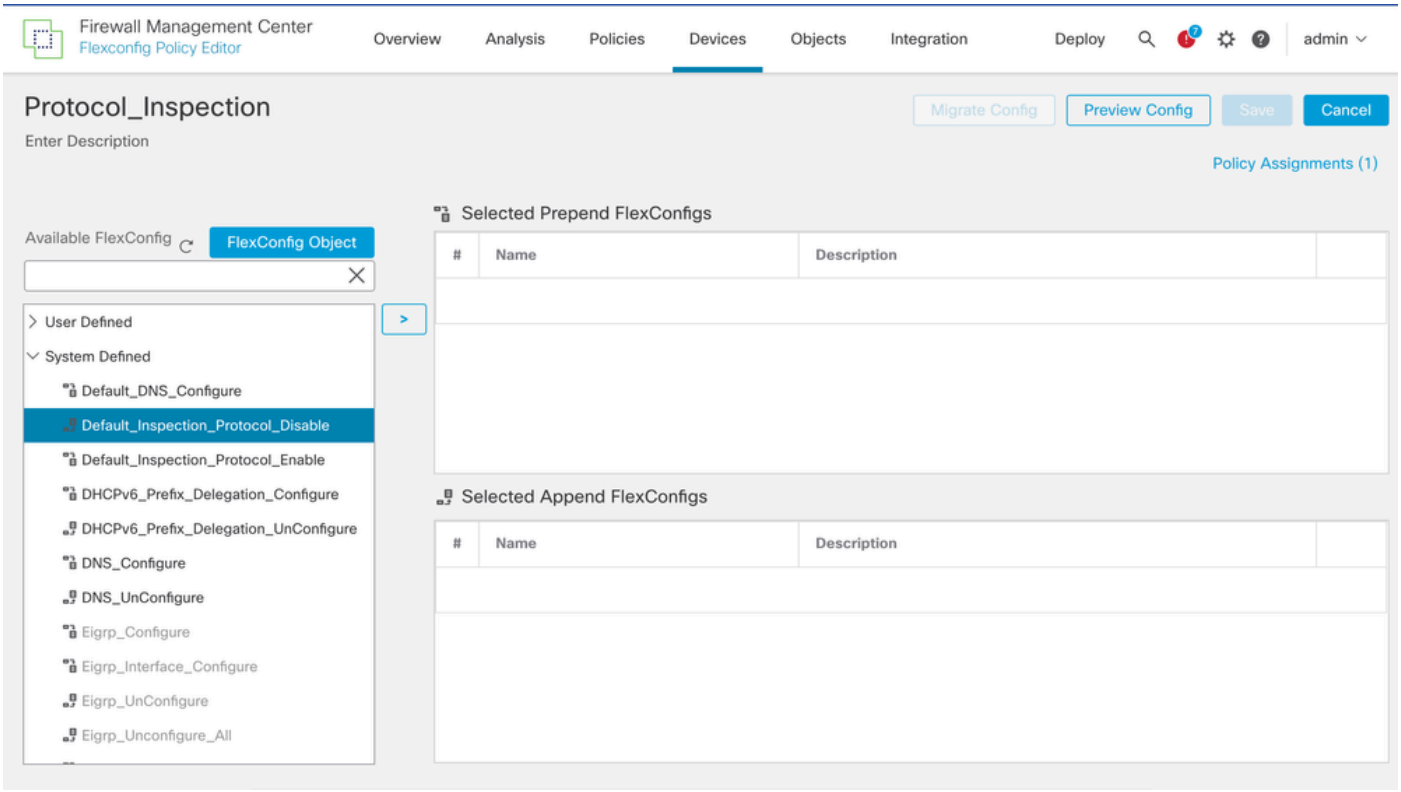
创建对象以禁用默认global_policy中的单个协议

第 3 步：

在分配给LINA的FlexConfig策略中添加对象。

导航到Devices > FlexConfig，选择应用于防火墙的FlexConfig策略，同时解决丢弃问题。

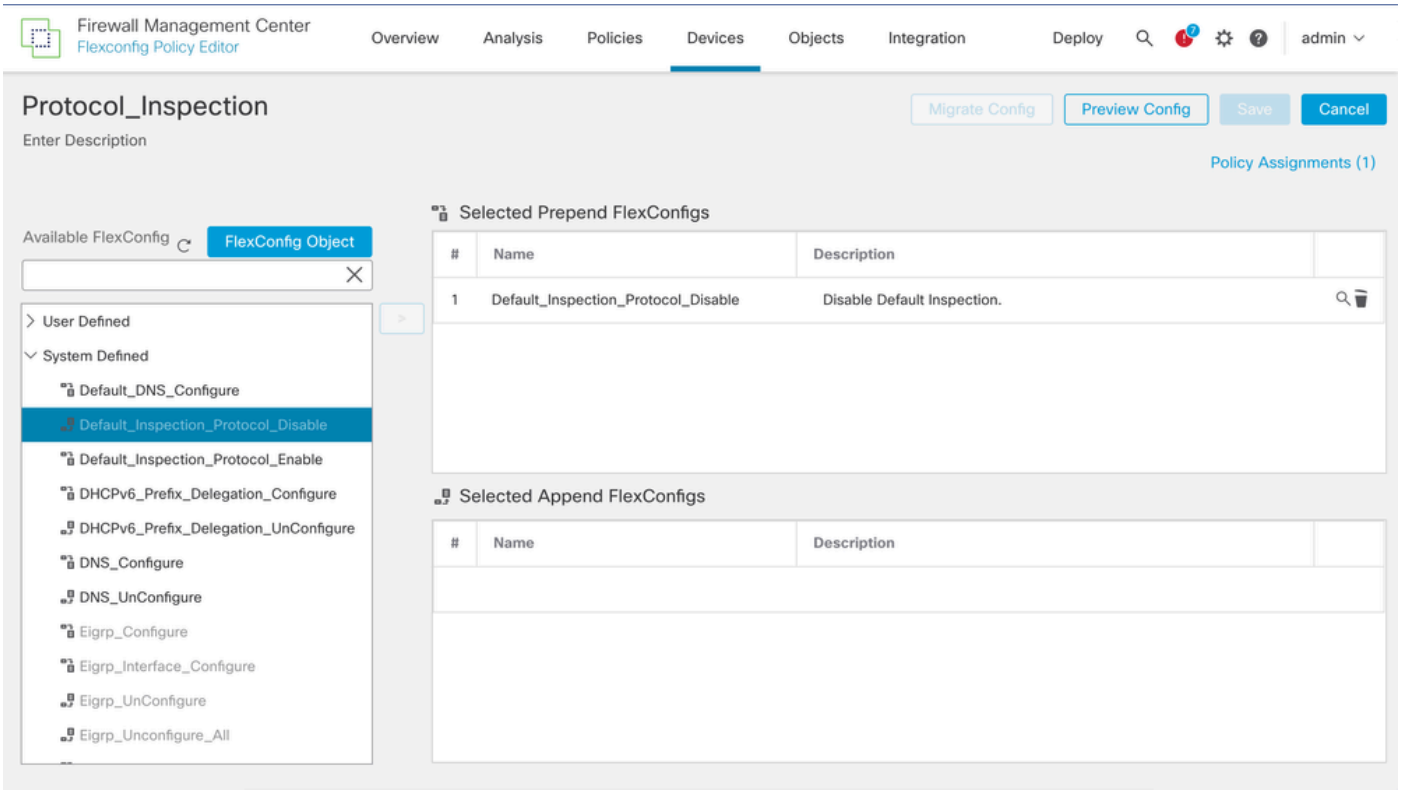
要全局禁用所有检查，请选择System Defined FlexConfig Objects下的Object Default_Inspection_Protocol_Disable，然后点击其间的蓝色箭头将其添加到FlexConfig Policy。



选择System defined Object以禁用所有协议检查

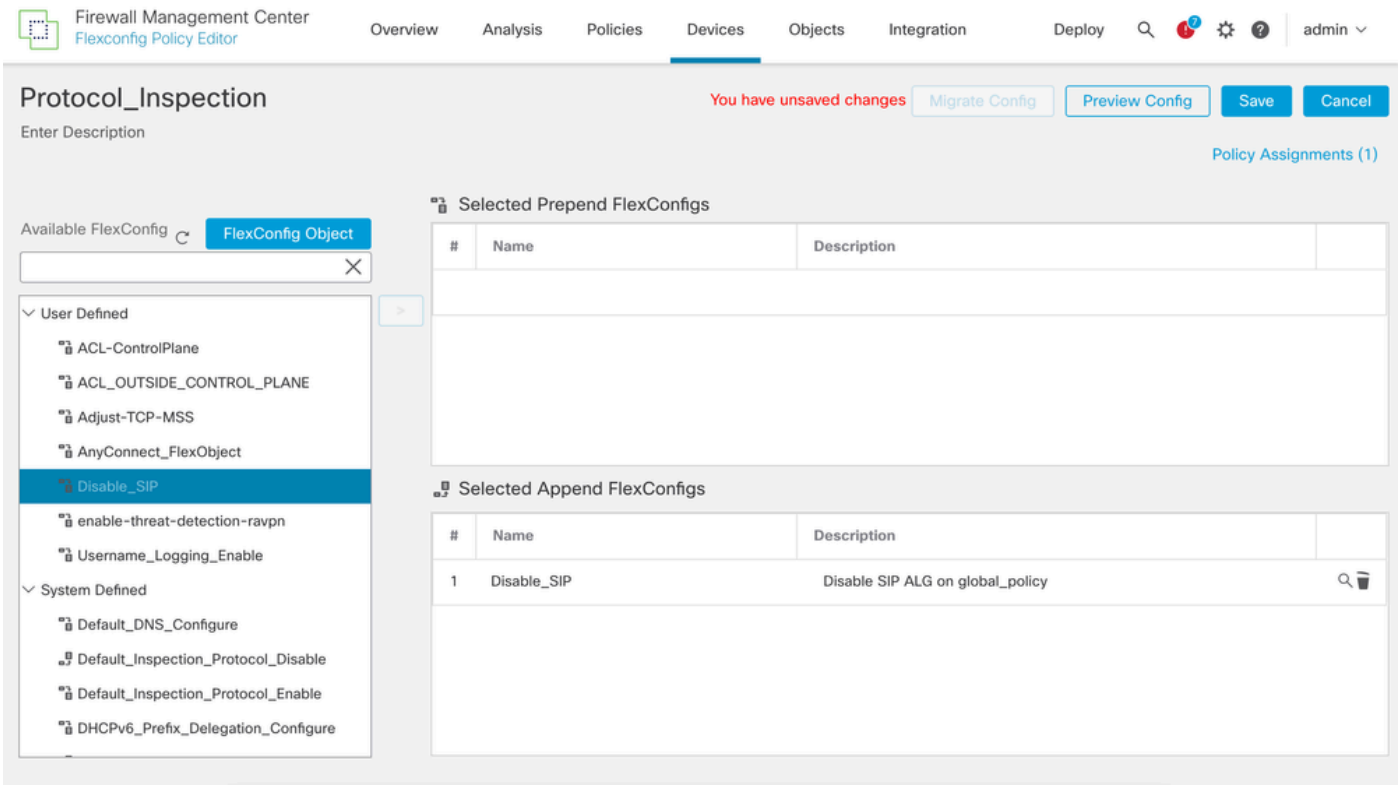
第 4 步：

选中后，请确认它显示在右框中，不要忘记保存并部署配置以生效。



禁用所有协议检测的选定对象

第 5 步：
要禁用单个协议检测，请从User defined列表中选择之前创建的对象，然后使用框之间的箭头将其添加到策略中。



选择以从global_policy禁用单个协议检测

第六步：

选中后，请确认它显示在右框中，不要忘记保存并部署配置以生效。

使用FTD CLI进行配置

可以立即从FTD CLI应用此解决方案，以测试检查是否影响流量。但是，如果发生重新启动或新部署，则不会保存配置更改。

该命令必须从FTD CLI以清洁模式执行。

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

验证

要验证协议禁用是否有效，请执行show running-config policy-map命令。在本示例中，SIP检测被禁用，因为它不再显示在默认协议列表中。

```
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#
```

相关信息

技术支持和文档 - Cisco Systems

- 应用层协议检测入门
- 基本Internet协议检测
- Show ASP Drop命令用法

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。