排除FTD上常见的AnyConnect通信问题

目录

简介

本文档介绍当Firepower威胁防御(FTD)使用安全套接字层(SSL)或互联网密钥交换版本2(IKEv2)时，如何对Cisco AnyConnect安全移动客户端(FTD)的一些最常见通信问题进行故障排除。

作者：Angel Ortiz和Fernando Jimenez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco AnyConnect 安全移动客户端.
- 思科FTD。
- 思科Firepower管理中心(FMC)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTD由FMC 6.4.0管理。
- AnyConnect 4.8。

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。本文档中使用的所有设备最初均采用原始（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。

建议的故障排除流程

本指南说明了当FTD用作远程访问虚拟专用网(VPN)网关时，如何排除AnyConnect客户端遇到的一些常见通信问题。 以下各节介绍并解决以下问题：

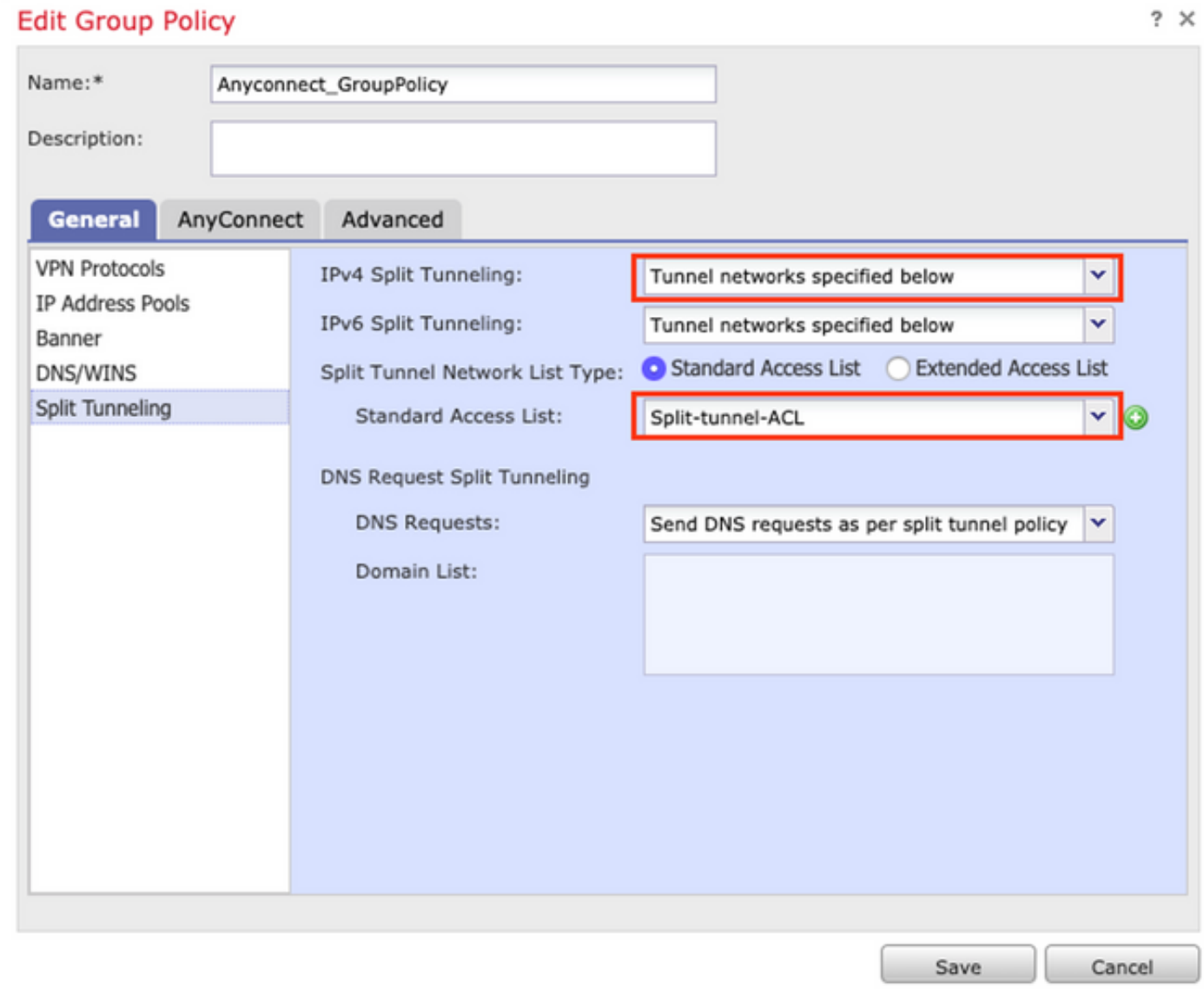
- AnyConnect客户端无法访问内部资源。
- AnyConnect客户端无法访问互联网。
- AnyConnect客户端无法相互通信。
- AnyConnect客户端无法建立电话呼叫。
- AnyConnect客户端可以建立电话呼叫。但是，呼叫上没有音频。

AnyConnect客户端无法访问内部资源

请完成以下步骤：

步骤1.检验拆分隧道配置。

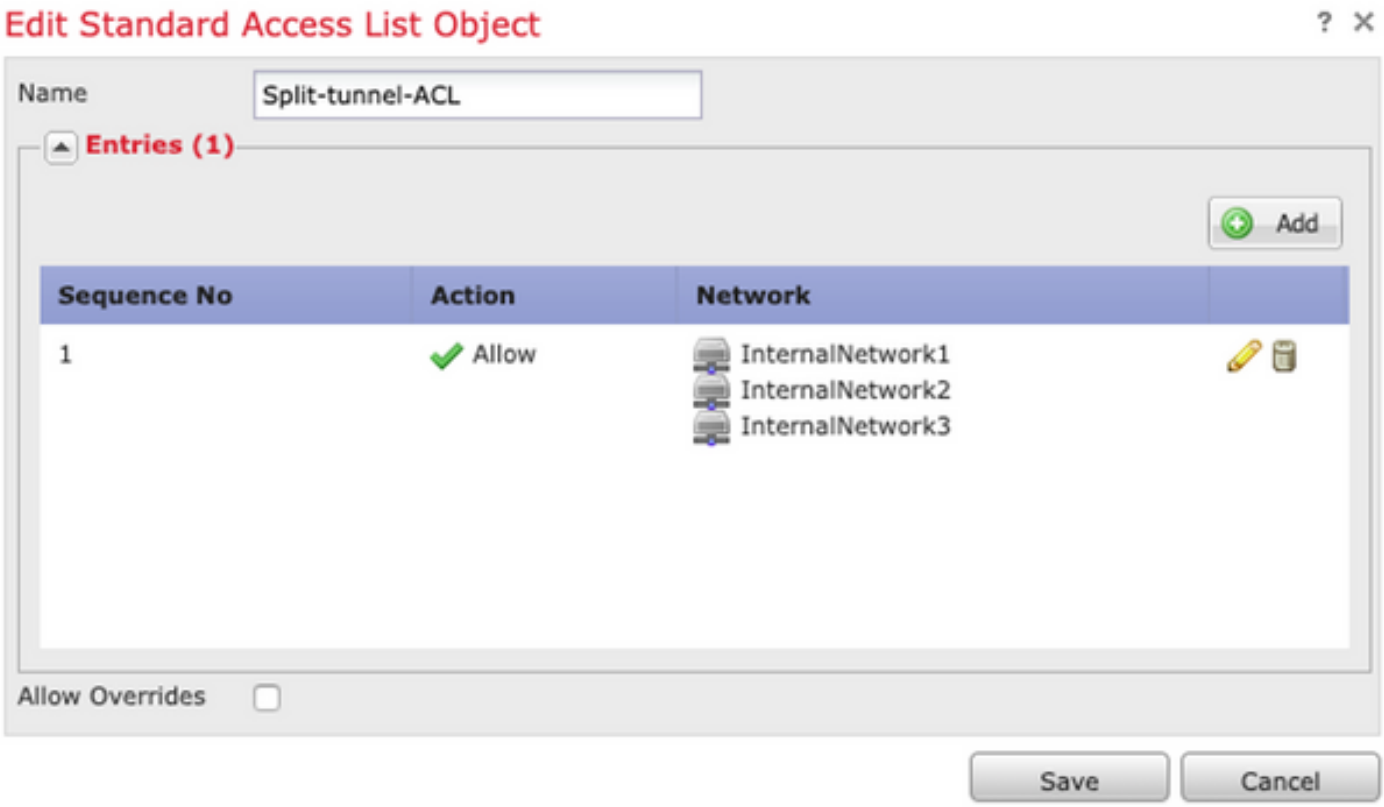
- 导航至AnyConnect客户端连接到的连接配置文件： **设备(Devices)> VPN(VPN)>远程访问(Remote Access)>连接配置文件(Connection Profile)>选择配置文件(Select the Profile)。**
- 导航至分配给该配置文件的组策略：编辑**组策略>常规。**
- 如图所示，检查分割隧道配置。



- 如果它配置为下面**指定的隧**道网络，请验证访问控制列表(ACL)配置：

导航至**Objects > Object Management > Access List > Edit the Access List for Split tunneling。**

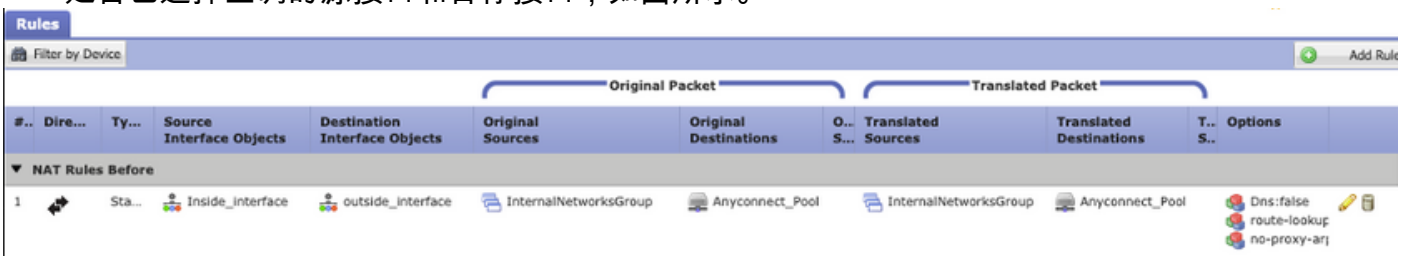
- 确保您尝试从AnyConnect VPN客户端访问的网络列在该访问列表中，如图所示。



第二步： 检验网络地址转换(NAT)免除配置。

请记住，我们必须配置NAT免除规则以避免流量转换为接口IP地址，通常配置为用于互联网访问(使用端口地址转换(PAT))。

- 导航至NAT配置： **设备> NAT。**
- 确保为正确的源（内部）和目标（AnyConnect VPN池）网络配置了NAT免除规则。另请检查是否已选择正确的源接口和目标接口，如图所示。



注意：配置NAT免除规则后，检查**no-proxy-arp并执**行路**由查找**选项作为最佳实践。

步骤3.检验访问控制策略。

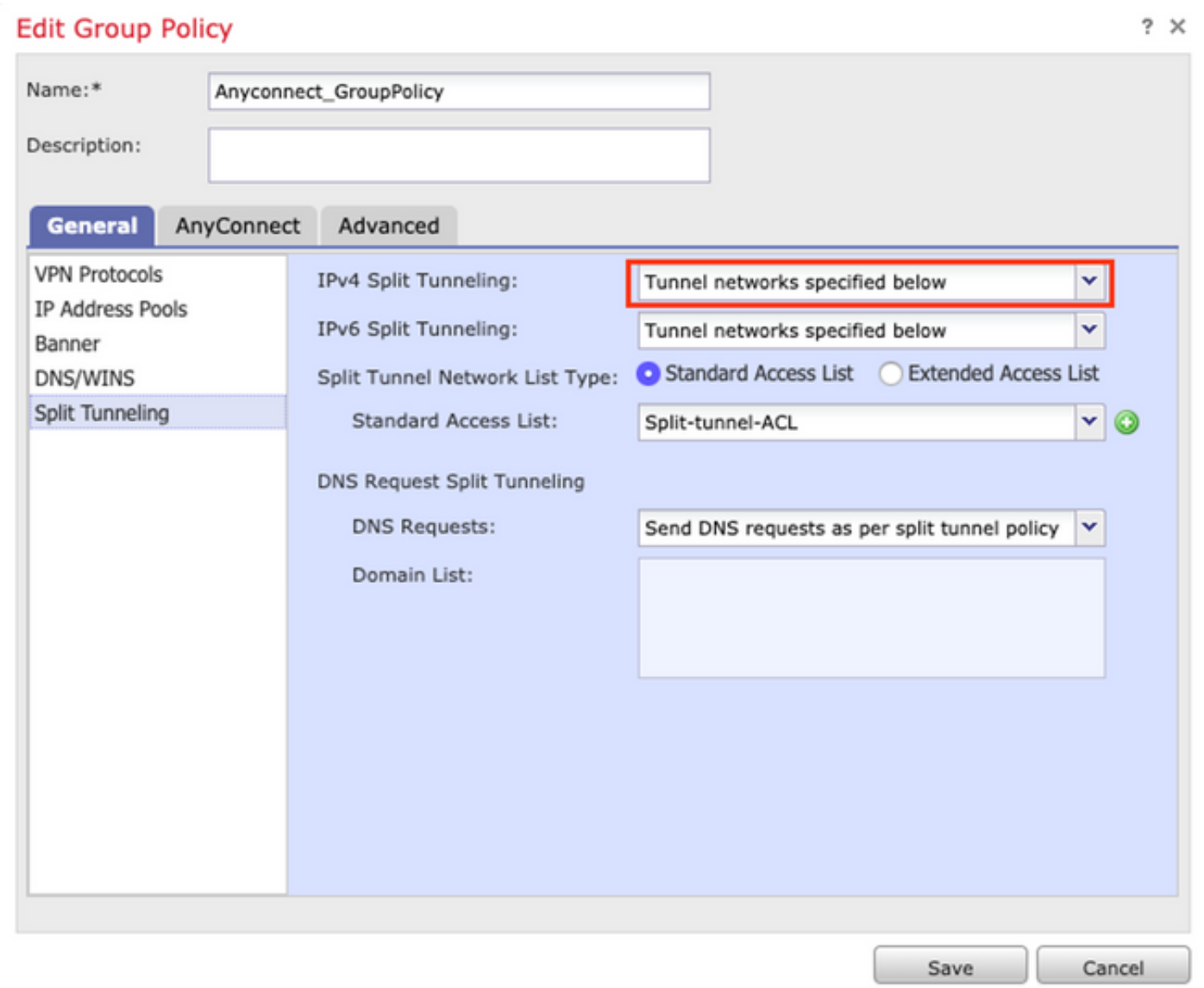
根据您的访问控制策略配置，确保允许来自AnyConnect客户端的流量到达选定的内部网络，如图所示。

AnyConnect客户端无互联网访问

此问题可能有两种情况。

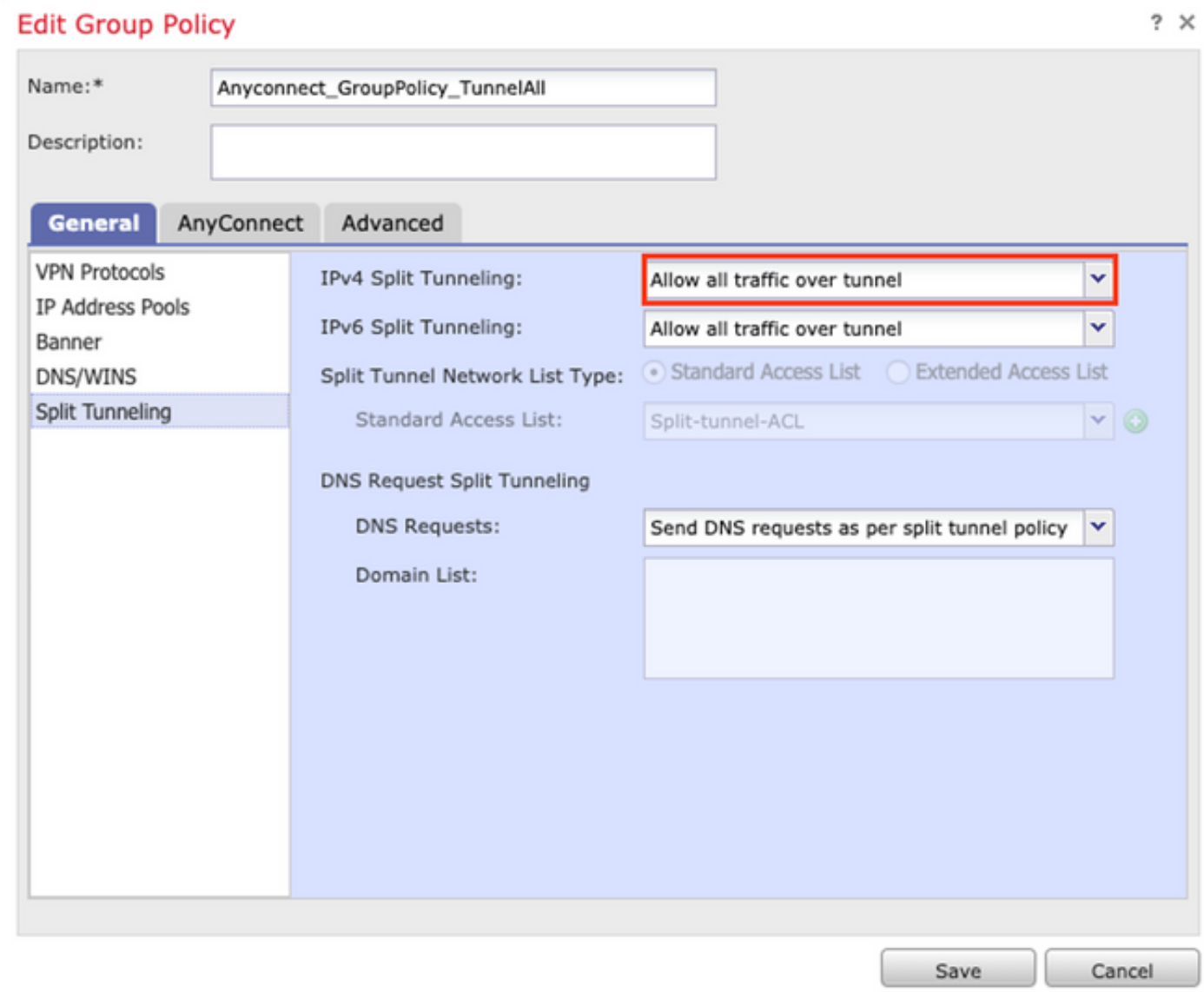
1. 发往互联网的流量不得通过VPN隧道。

确保将组策略配置为分割隧道作为下面指定的**隧道网络，而**不配置为**允许所有通过隧**道的流量，如图所示。



2.发往Internet的流量必须通过VPN隧道。

在这种情况下，分割隧道最常见的组策略配置是选择**允许所有通过隧道的流**量，如图所示。



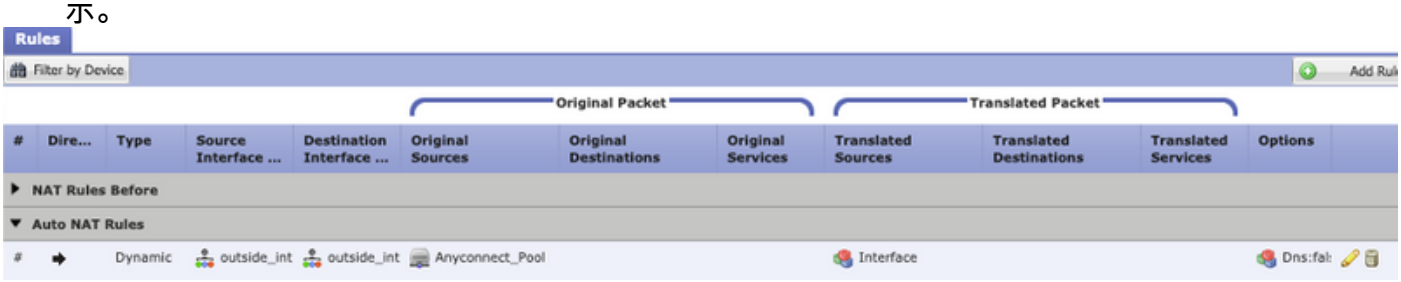
步骤1.检验NAT免除配置以实现内部网络可达性。

请记住，我们仍必须配置NAT免除规则才能访问内部网络。请查看**的第2步 AnyConnect客户端无法访问内部资源** 的下界。

步骤2.检验动态转换的发夹配置。

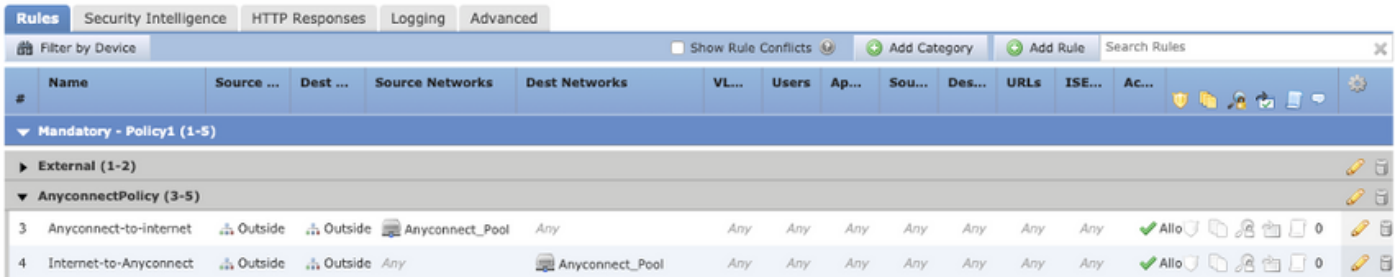
为使AnyConnect客户端能够通过VPN隧道访问互联网，我们需要确保迂回NAT配置正确，以便流量转换到接口的IP地址。

- 导航至NAT配置： **设备> NAT。**
- 确保为正确的接口(互联网服务提供商(ISP)链路)配置动态NAT规则作为源和目标（发夹）。 另请检查是否在原始源和目标接口IP中选择了用于AnyConnect VPN地址池**的网络** 选项，如图所示。



步骤3.检验访问控制策略。

根据您的访问控制策略配置，确保允许来自AnyConnect客户端的流量到达外部资源，如图所示。



AnyConnect客户端无法相互通信

此问题可能存在两种情况：

1. AnyConnect客户端 **允许通过隧道的所有流量** 配置。
2. AnyConnect客户端 **在下面指定的隧道网络** 配置。

1. AnyConnect客户端 **允许通过隧道的所有流量** 配置。

何时 **允许通过隧道的所有流量** 为AnyConnect配置意味着所有内部和外部流量都应转发到AnyConnect头端，当您具有用于公共互联网访问的NAT时，这会成为问题，因为发往另一个AnyConnect客户端的流量会转换为接口IP地址，因此通信失败。

步骤1.检验NAT免除配置。

为了解决此问题，必须配置手动NAT免除规则以允许AnyConnect客户端内的双向通信。

- 导航至NAT配置： **设备> NAT。**
- 确保为正确的源（AnyConnect VPN池）和目标配置NAT免除规则。（AnyConnect VPN池）网络。另外，请检查是否配置了正确的发夹配置，如图所示。

步骤2.检验访问控制策略。

根据您的访问控制策略配置，确保允许来自AnyConnect客户端的流量，如图所示。

2.使用 **在下面指定的隧道网络** 配置。

使用 **在下面指定的隧道网络** 仅为AnyConnect客户端配置的特定流量通过VPN隧道转发到。但是，我们需要确保头端配置正确，以允许AnyConnect客户端内的通信。

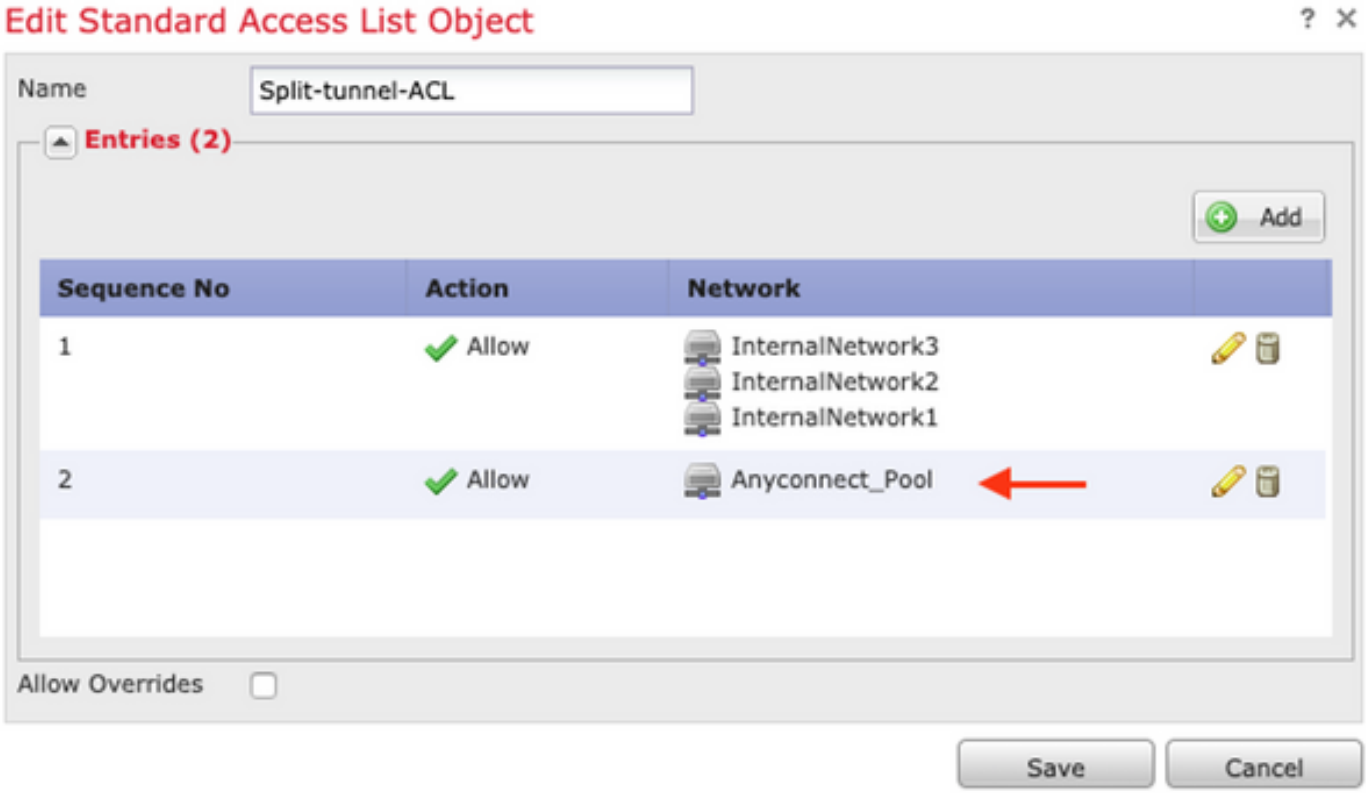
步骤1.检验NAT免除配置。

请在“允**许所有通**过隧道的**流量”部分选中步骤**1。

步骤2.检验分割隧道配置。

要使AnyConnect客户端之间通信，我们需要将VPN池地址添加到分割隧道ACL中。

- 请执行**第**1步 **AnyConnect客户端无法访问内部资源** 的下界。
- 确保AnyConnect VPN池网络列在分割隧道访问列表中，如图所示。



注意：如果AnyConnect客户端有多个IP池，并且需要不同池之间的通信，请确保在分割隧道ACL中添加所有池，并为所需的IP池添加NAT免除规则。

步骤3.检验访问控制策略。

确保允许来自AnyConnect客户端的流量，如图所示。

AnyConnect客户端无法建立电话呼叫

有些情况下，AnyConnect客户端需要通过VPN建立电话呼叫和视频会议。

AnyConnect客户端可以连接到AnyConnect头端，而且无任何问题。它们可以访问内部和外部资源，但无法建立电话呼叫。

对于这种情况，我们需要考虑以下几点：

- 语音的网络拓扑。
- 涉及的协议。即会话初始协议(SIP)、快速生成树协议(RSTP)等
- VPN电话如何连接到Cisco Unified Communications Manager(CUCM)。

默认情况下，FTD和ASA在其全局策略映射中启用应用检测。

在大多数情况下，VPN电话无法与CUCM建立可靠通信，因为AnyConnect头端启用了应用检查，以修改信号和语音流量。

有关可应用应用检测的语音和视频应用的详细信息，请参阅以下文档：

章节：语音和视频协议检测

为了确认应用流量是否被全局策略映射丢弃或修改，我们可以使用**show service-policy**命令，如下所示。

```
firepower#show service-policy

Global policy:
Service-policy: global_policy
Class-map: inspection_default
.

.
Inspect: sip , packet 792114, lock fail 0, drop 10670, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
.
```

在本例中，我们可以看到SIP检测如何丢弃流量。

此外，SIP检测还可以转换负载内的IP地址，而不是IP报头中的IP地址，这会导致不同的问题，因此，建议在我们要通过AnyConnect VPN使用语音服务时禁用它。

要禁用它，我们需要完成后续步骤：

步骤1.进入特权执行模式。

有关如何访问此模式的详细信息，请参阅下一文档：

章节：使用命令行界面(CLI)

步骤2.检验全局策略映射。

运行下一命令并验证是否启用了SIP检测。

```
firepower#show running-config policy-map
.


.
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 xdmcp
 inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect esmtp
```

步骤3.禁用SIP检测。

如果SIP检测已启用，请在clish提示符下关闭运行以下命令：

```
> configure inspection sip disable
```

第四步： 再次验证全局策略映射。

确保从全局策略映射禁用SIP检测：

```
firepower#show running-config policy-map
.
```

.

```
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 xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect esmtp
```

AnyConnect客户端可以建立电话呼叫，但呼叫上没有音频

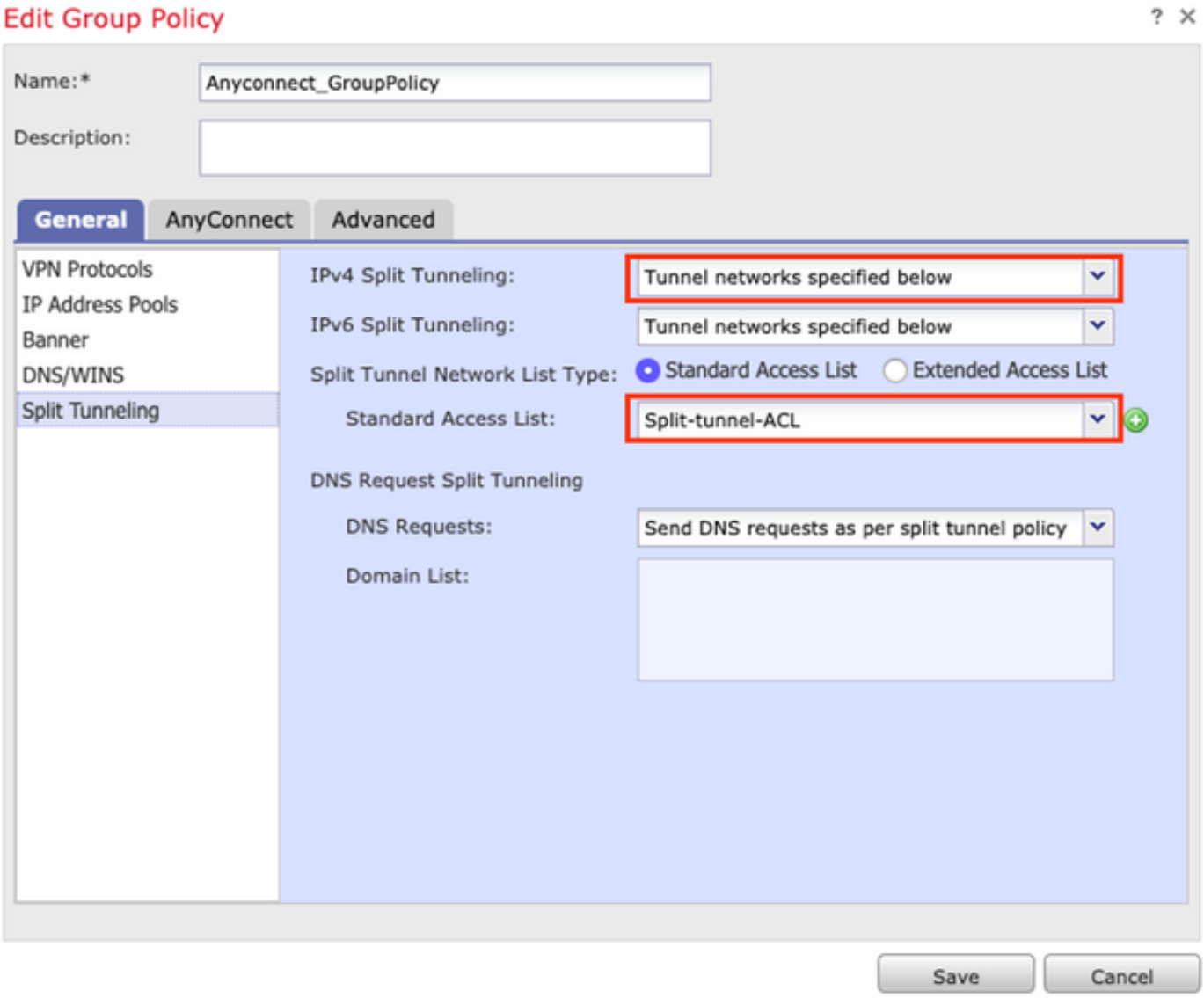
如上节所述，AnyConnect客户端通常需要在连接到VPN时建立电话呼叫。在某些情况下，可以建立呼叫，但客户端可能会遇到音频不足的情况。这适用于下一场景：

- AnyConnect客户端和外部号码之间的呼叫没有音频。
- AnyConnect客户端与另一AnyConnect客户端之间的呼叫没有音频。

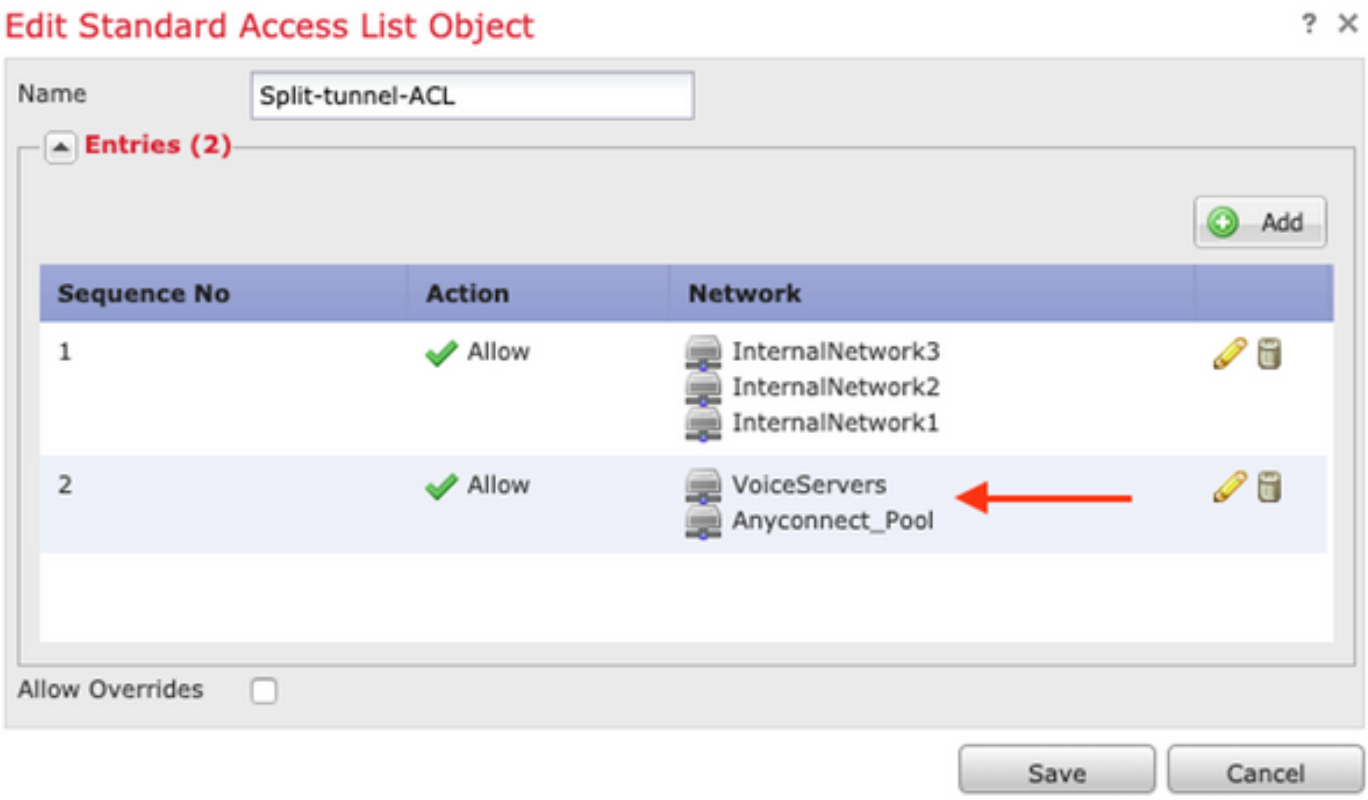
为了修复此问题，我们可以执行以下步骤：

步骤1.检验分割隧道配置。

- 导航至连接配置文件，用于连接到： **设备(Devices)> VPN(VPN)>远程访问(Remote Access)>连接配置文件(Connection Profile)>选择配置文件(Select the Profile)。**
- 导航至分配给该配置文件的组策略：**编辑组策略>常规。**
- 如图所示，检查分割隧道配置。



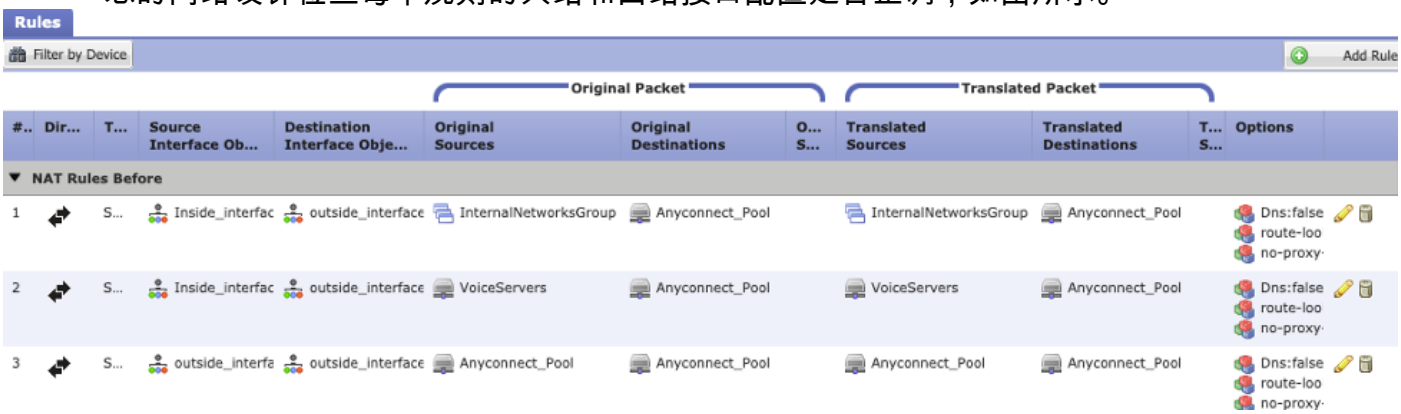
- 如果配置为 **在下面指定的隧道网络**，验证访问列表配置： **对象(Objects)>对象管理(Object Management)>访问列表(Access List)>编辑分割隧道的访问列表(Edit the Access List for Split tunneling)。**
- 确保语音服务器和AnyConnect IP池网络列在分割隧道访问列表中，如图所示。



步骤2.检验NAT免除配置。

必须配置NAT免除规则，以免除从AnyConnect VPN网络到语音服务器网络的流量，并允许AnyConnect客户端内的双向通信。

- 导航至NAT配置： **设备> NAT。**
- 确保为正确的源（语音服务器）和目标（AnyConnect VPN池）网络配置了NAT免除规则，并且AnyConnect客户端与AnyConnect客户端通信的发夹NAT规则已就位。此外，请根据您的网络设计检查每个规则的入站和出站接口配置是否正确，如图所示。

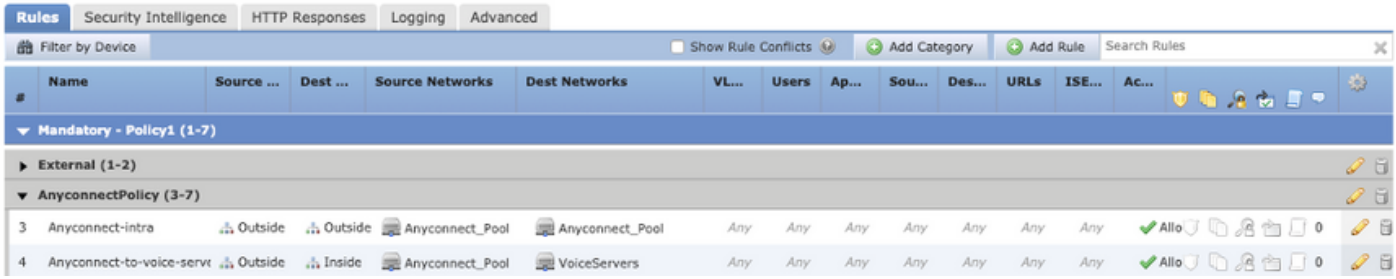


步骤3.检验SIP检测是否已禁用。

请复习上一节 **AnyConnect客户端无法建立电话呼叫** 了解如何禁用SIP检测。

步骤4.检验访问控制策略。

根据您的访问控制策略配置，确保允许来自AnyConnect客户端的流量到达语音服务器和相关网络，如图所示。



相关信息

- 本视频提供了本文档中讨论的不同问题的配置示例。
- 如需其他帮助，请联系技术支持中心(TAC)。需要有效的支持合同： 思科全球支持联系方式.
- 您还可以访问思科VPN社区 这里。