# PIX/ASA 7.x：启用VoIP (SIP，MGCP，H323，SCCP)服务配置示例

## 目录



## 简介

本文档说明如何允许外部接口的 IP 语音 (VoIP) 协议数据流以及启用 Cisco PIX/ASA 安全设备中每个协议的检查。

协议如下：

- **会话初始化协议 (SIP)** — SIP 是用于创建、修改和终止具有一个或多个参与方的会话的应用层控制（信令）协议。这些会话包括 Internet 电话、多媒体分布和多媒体会议。根据互联网工程任务组 (IETF) 的定义，SIP 可实现 VoIP 呼叫。SIP 与会话描述协议 (SDP) 配合用于呼叫信令。SDP 指定媒体流的详细信息。使用 SIP 时，安全设备可支持所有 SIP (VoIP) 网关和 VoIP 代理服务器。SIP 和 SDP 在以下 RFC 中进行定义：SIP:会话初始化协议，RFC 3261SDP ：会话描述协议，RFC 2327为通过安全设备支持 SIP 呼叫，必须检查信令消息的媒体连接地址、媒体端口和媒体的初期连接。这是因为在通过公认目标端口 (**UDP/TCP 5060**) 发送信令时，将对媒体流进行动态分配。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。SIP 检查

对这些嵌入式 IP 地址应用网络地址转换 (NAT)。**注意：** 如果远程端点尝试注册受安全设备保护的网络中的某个 SIP 代理，在某些非常特殊的情况下注册会失败。这些情况包括：为远程端点配置了端口地址转换 (PAT) 时，SIP 注册服务器位于外部网络中，以及端点向服务器发送的 REGISTER 消息的“contact”字段中缺少端口时。

- **媒体网关控制协议 (MGCP)** — MGCP 是在集中控制体系结构基础上建立的客户端-服务器呼叫控制协议。所有拨号计划信息位于一个单独的呼叫代理中。该呼叫代理控制网关的端口，用于执行呼叫控制。网关针对外部呼叫执行公共交换电话网 (PSTN) 与 VoIP 网络之间的媒体转换。在基于 Cisco 的网络中，将 CallManager 用作呼叫代理。MGCP 是在若干 RFC 中定义的 IETF 标准，其中包括 2705 和 3435 。 通过使用软件包（例如处理 Dual-Tone Multifrequency (DTMF) 声音、安全 RTP、呼叫保留和呼叫转移）可以扩展其功能。MGCP 网关的配置比较简单。由于呼叫代理具有全部呼叫路由智能，因此您不需要为网关配置所需的所有其他拨号对等体。缺点是呼叫代理必须始终可用。Cisco MGCP 网关可使用 Survivable Remote Site Telephony (SRST) 和 MGCP 后退，从而允许 H.323 协议在没有 CallManager 时接管并提供本地呼叫路由。在这种情况下，必须在网关上配置拨号对等体以供 H.323 使用。
- **H.323** — H.323 检查为符合 H.323 的应用程序（如 Cisco CallManager 和 VocalTec 网守）提供支持。H.323 是国际电信联盟针对通过 LAN 进行的多媒体会议定义的一套协议。安全设备支持版本 4 及以下的 H.323，其中包括 H.323 版本 3 中同一呼叫信令信道支持多个呼叫的功能。启用 H.323 检查后，安全设备可支持同一呼叫信令信道中的多个呼叫，这是 H.323 版本 3 中引入的功能。此功能可缩短呼叫建立时间并减少安全设备使用的端口。以下是 H.323 检查的两个主要功能：对 H.225 和 H.245 消息中嵌入的必要的 IPv4 地址执行 NAT。由于 H.323 消息采用 PER 编码格式进行编码，因此安全设备使用 ASN.1 解码器对 H.323 消息进行解码。动态分配协商确定的 H.245 和 RTP/RTCP 连接。
- **精简（或简单）客户端控制协议 (SCCP)** — SCCP 是在 VoIP 网络中使用的一种简化协议。使用 SCCP 的 Cisco IP 电话可以在 H.323 环境中共存。与 Cisco CallManager 一起使用时，SCCP 客户端可以与符合 H.323 的终端进行互操作。安全设备的应用层功能可识别 SCCP 版本 3.3。通过提供 SCCP 信令数据包的 NAT，应用层软件的功能可确保所有 SCCP 信令和媒体数据包均能通过安全设备。以下是 SCCP 协议的 5 个版本：2.4、3.0.4、3.1.1、3.2 和 3.3.2。安全设备支持版本 3.3.2 及以下的所有版本。安全设备为 SCCP 同时提供 PAT 和 NAT 支持。如果可供 IP 电话使用的全局 IP 地址数量有限，则必须使用 PAT。Cisco CallManager 与 Cisco IP 电话之间的正常数据流使用 SCCP 并由 SCCP 检查进行处理，无需进行任何特殊配置。安全设备还支持 DHCP 选项 150 和 66，使安全设备能够向 Cisco IP 电话和其他 DHCP 客户端发送 TFTP 服务器的位置。有关详细信息，请参阅配置 DHCP、DDNS 和 WCCP 服务。

# 先决条件

## 要求

本文档假设所有设备已进行必要的 VPN 配置，且配置可以正常工作。

请参阅 ASA/PIX：安全设备到 IOS 路由器的 LAN 到 LAN IPsec 隧道配置示例。

请参阅 PIX/ASA 7.x：实现接口之间的通信以了解有关如何实现接口之间通信的详细信息。

## 使用的组件

本文档中的信息以运行软件版本 7.x 的 Cisco 5500 系列自适应安全设备 (ASA) 为基准。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 相关产品

此配置也可用于运行软件版本 7.x 的 Cisco 500 系列 PIX 防火墙。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 背景信息

## SIP

SIP 检查对基于 SIP 文本的消息执行 NAT，重新计算消息的 SDP 部分的内容长度，并重新计算数据包长度和校验和。它以动态方式为 SIP 消息中 SDP 部分指定作为端点应监听的地址/端口的端口打开媒体连接。

SIP 检查有一个数据库，其中包含来自 SIP 有效负载的索引 CALL_ID/FROM/TO，用于标识呼叫以及源和目标。此数据库中包含 SDP 媒体信息字段和媒体类型中所含的媒体地址和媒体端口。一个会话可以有多个媒体地址和端口。使用这些媒体地址/端口打开两个端点之间的 RTP/RTCP 连接。

初始呼叫建立 (INVITE) 消息必须使用公认端口 5060。但随后的消息可以不使用此端口号。SIP 检查引擎打开信令连接针孔，将这些连接标记为 SIP 连接。此操作的目的是使消息到达 SIP 应用程序并执行 NAT。

呼叫建立后，便会认为 SIP 会话处于临时状态。在收到指示目标端点监听的 RTP 媒体地址和端口的响应消息之前，将保持这种状态。如果未能在一分钟内收到响应消息，则会切断信令连接。

完成最终握手后，呼叫状态变为活动，并保持信令连接，直到收到 BYE 消息为止。

如果内部端点对外部端点发出呼叫，则会对外部接口打开媒体孔，以允许 RTP/RTCP UDP 数据包流到从内部端点发出的 INVITE 消息中指定的内部端点媒体地址和媒体端口。除非安全设备配置特别允许，否则未经许可进入内部接口的 RTP/RTCP UDP 数据包不会通过安全设备。

在连接变为空闲状态后的两分钟内，将切断媒体连接。这是可配置的超时，可以设置为更短或更长时间。

## MGCP

要使用 MGCP，通常至少需要配置两个检查命令：一个用于网关接收命令的端口，一个用于呼叫代理接收命令的端口。通常情况下，呼叫代理将命令发送到网关的默认 MGCP 端口 **2427**，网关将命令发送到呼叫代理的默认 MGCP 端口 **2727**。

MGCP 消息通过 **UDP** 发送。响应将发送回命令的源地址（IP 地址和 UDP 端口号），但响应不一定来自发送命令的同一个目标地址。如果故障切换配置中使用多个呼叫代理，而收到命令的呼叫代理已将控制移交给备用呼叫代理，后者随后发送响应，便会出现上述情况。

## H.323

H.323 协议集合总共最多可以使用两个 TCP 连接和四到六个 UDP 连接。FastConnect 仅使用一个 TCP 连接，可靠性、可用性和可维护性 (RAS) 使用一个 UDP 连接用于注册、准入和状态。

初始时，H.323 客户端可以使用 TCP 端口 1720 建立与 H.323 服务器的 TCP 连接，以请求建立 Q.931 呼叫。在呼叫建立过程中，H.323 终端为客户端提供用于 H.245 TCP 连接的端口号。在使用 H.323 网守的环境中，使用 UDP 发送初始数据包。

H.323 检查监视 Q.931 TCP 连接以确定 H.245 端口号。如果 H.323 终端不使用 FastConnect，安全设备将根据 H.225 消息的检查动态分配 H.245 连接。

H.323 终端在每个 H.245 消息中交换用于后续 UDP 数据流的端口号。H.323 检查会检查 H.245 消息以标识这些端口，并动态创建用于媒体交换的连接。RTP 使用协商确定的端口号，而 RTCP 使用下一个更高端口号。

H.323 控制信道处理 H.225 和 H.245 及 H.323 RAS。H.323 检查使用下列端口：

- 1718 — 网守发现 UDP 端口
- 1719 — RAS UDP 端口
- 1720 — TCP 控制端口

必须允许 H.225 呼叫信令的数据流通过公认的 H.323 端口 1720。但 H.245 信令端口由 H.225 信令终端协商确定。使用 H.323 网守时，安全设备会根据准入确认 (ACF) 消息的检查打开 H.225 连接。

检查到 H.225 消息后，安全设备打开 H.245 信道，然后检查通过 H.245 信道发送的数据流。所有通过安全设备的 H.245 消息都要经过 H.245 应用检查，以转换嵌入式 IP 地址并打开 H.245 消息中协商确定的媒体信道。

H.323 ITU 标准要求在传递到可靠连接之前，H.225 和 H.245 消息前面必须有定义消息长度的传输协议数据单元数据包 (TPKT) 报头。由于 TPKT 报头不一定在与 H.225 和 H.245 消息相同的 TCP 数据包中发送，因此安全设备必须记住 TPKT 长度以便对消息进行正确的处理和解码。对于每个连接，安全设备会保留一个包含下一个预期消息的 TPKT 长度的记录。

如果安全设备需要对消息中的 IP 地址执行 NAT，它会更改校验和、UUIE 长度和 TPKT（前提是与 H.225 消息一起包括在 TCP 数据包中）。如果 TPKT 在单独的 TCP 数据包中发送，安全设备代理将确认 (ACK) 该 TPKT 并为 H.245 消息附加一个具有新长度的新的 TPKT。

## SCCP

在 Cisco CallManager 所在接口就 Cisco IP 电话而言安全性较高的拓扑中，如果需要对 Cisco CallManager IP 地址执行 NAT，映射必须是静态的，因为 Cisco IP 电话要求在其配置中明确指定 Cisco CallManager IP 地址。标识静态条目使位于安全性较高的接口的 Cisco CallManager 可以接受来自 Cisco IP 电话的注册。

Cisco IP 电话需要访问 TFTP 服务器以下载它们连接到 Cisco CallManager 服务器所需的配置信息。

如果与 TFTP 服务器相比 Cisco IP 电话位于安全性较低的接口，则必须使用访问列表连接到位于 UDP 端口 69 的受保护的 TFTP 服务器。如果确实需要使用 TFTP 服务器的静态条目，则不一定是标识静态条目。使用 NAT 时，标识静态条目映射到相同的 IP 地址。使用 PAT 时，则映射到相同的 IP 地址和端口。

如果与 TFTP 服务器和 Cisco CallManager 相比，Cisco IP 电话位于安全性较高的接口，Cisco IP

电话启动连接时不需要使用访问列表或静态条目。

# 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

## SIP 的网络图

本部分使用以下网络设置：

## SIP 的配置

本部分使用以下配置：

安全设备支持通过自适应安全算法功能进行应用程序检查。通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。实施应用程序检查包括下列操作：

- 标识流量。
- 对流量应用检查。
- 在接口上激活检查。

**配置基本 SIP 检查**

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（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，如果需要改变全局策略（例如，对非标准端口应用检查或添加默认情况下未启用的检查），则需要编辑默认策略或禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 发出 **policy-map global_policy** 命令。`ASA5510(config)#policy-map global_policy`
2. 发出 **class inspection_default** 命令。`ASA5510(config-pmap)#class inspection_default`
3. 发出 **inspect sip** 命令。`ASA5510(config-pmap-c)#inspect sip`

**针对 SIP 的 ASA 配置**

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
```

```
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SIP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq sip pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp !--- Command to enable SIP
inspection. inspect sip inspect xdmcp inspect ftp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

## MGCP、H.323 和 SCCP 的网络图

本部分使用以下网络设置：

## MGCP 的配置

本部分使用以下配置：

安全设备支持通过自适应安全算法功能进行应用程序检查。通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。实施应用程序检查包括下列操作：

- 标识流量。
- 对流量应用检查。
- 在接口上激活检查。

**配置基本 MGCP 检查**

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（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，如果需要改变全局策略（例如，对非标准端口应用检查或添加默认情况下未启用的检查），则需要编辑默认策略或禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 发出 **policy-map global_policy** 命令。ASA5510(config)#**policy-map global_policy**
2. 发出 **class inspection_default** 命令。ASA5510(config-pmap)#**class inspection_default**
3. 发出 **inspect mgcp** 命令。ASA5510(config-pmap-c)#**inspect mgcp**

### 配置用于附加检查控制的 MGCP 检查策略映射

如果网络中有多个需要安全设备为其打开针孔的呼叫代理和网关，则应创建 MGCP 映射。随后可以在启用 MGCP 检查时应用 MGCP 映射。有关详细信息，请参阅配置应用检查。

*!--- Permits inbound 2427 port traffic.* ASA5510(config)#**access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2427** *!--- Permits inbound 2727 port traffic.* ASA5510(config)#**access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2727** ASA5510(config)#**class-map mgcp_port** ASA5510(config-cmap)#**match access-list 100** ASA5510(config-cmap)#exit *!--- Command to create an MGCP inspection policy map.* ASA5510(config)#**policy-map type inspect mgcp mgcpmap** *!--- Command to configure parameters that affect the !--- inspection engine and enters into parameter configuration mode.* ASA5510(config-pmap)#**parameters** *!--- Command to configure the call agents.* ASA5510(config-pmap-p)#**call-agent 10.1.1.10 101** *!--- Command to configure the gateways.* ASA5510(config-pmap-p)#**gateway 10.2.2.5 101** *!--- Command to change the maximum number of commands !--- allowed in the MGCP command queue.* ASA5510(config-pmap-p)#**command-queue 150** ASA5510(config-pmap-p)# exit ASA5510(config)#**policy-map inbound_policy** ASA5510(config-pmap)# **class mgcp_port** ASA5510(config-pmap-c)#**inspect mgcp mgcpmap** ASA5510(config-pmap-c)# exit ASA5510(config)#**service-policy inbound_policy interface outside**

**针对 MGCP 的 ASA 配置**

```
ASA Version 7.2(1)24
!
hostname ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Permits inbound 2427 and 2727 port traffic. access-
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 2427 access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2727 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 !--- Command to
redirect the MGCP traffic received on outside interface
to !--- inside interface for the specified IP address.
static (inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
```

```
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map mgcp_port match access-list 100 class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp inspect mgcp policy-map type inspect
mgcp mgcpmap parameters call-agent 10.1.1.10 101 gateway
10.2.2.5 101 command-queue 150 policy-map inbound_policy
class mgcp_port inspect mgcp mgcpmap ! service-policy
global_policy global service-policy inbound_policy
interface outside prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

## H.323 的配置

本部分使用以下配置：

安全设备支持通过自适应安全算法功能进行应用程序检查。通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。实施应用程序检查包括下列操作：

- 标识流量。
- 对流量应用检查。
- 在接口上激活检查。

### 配置基本 H.323 检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（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，如果需要改变全局策略（例如，对非标准端口应用检查或添加默认情况下未启用的检查），则需要编辑默认策略或禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 发出 **policy-map global_policy** 命令。`ASA5510(config)#`**`policy-map global_policy`**
2. 发出 **class inspection_default** 命令。`ASA5510(config-pmap)#`**`class inspection_default`**
3. 发出 **inspect h323** 命令。`ASA5510(config-pmap-c)#`**`inspect h323 h225`** `ASA5510(config-pmap-c)#`**`inspect h323 ras`**

**针对 H.323 的 ASA 配置**

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
```

```
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming Gate Keeper Discovery UDP port traffic. access-
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 1718 !--- Command to allow the incoming
RAS UDP port. access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 1719 !---
Command to allow the incoming h323 protocol traffic.
access-list 100 extended permit tcp 10.2.2.0
255.255.255.0 host 172.16.1.5 eq h323 pager lines 24 mtu
inside 1500 mtu outside 1500 no failover asdm image
disk0:/asdm-522.bin no asdm history enable arp timeout
14400 !--- Command to redirect the h323 protocol traffic
received on outside interface to !--- inside interface
for the specified IP address. static (inside,outside)
172.16.1.5 10.1.1.10 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.1.1 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map !---
Command to enable H.323 inspection. inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp inspect
ftp ! !--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

## SCCP 的配置

本部分使用以下配置：

安全设备支持通过自适应安全算法功能进行应用程序检查。通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。实施应用程序检查包括下列操作：

- 标识流量。
- 对流量应用检查。
- 在接口上激活检查。

### 配置基本 SCCP 检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（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，如果需要改变全局策略（例如，对非标准端口应用检查或添加默认情况下未启用的检查），则需要编辑默认策略或禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅[默认检查策略](#)。

1. 发出 **policy-map global_policy** 命令。`ASA5510(config)#`**`policy-map global_policy`**
2. 发出 **class inspection_default** 命令。`ASA5510(config-pmap)#`**`class inspection_default`**
3. 发出 **inspect skinny** 命令。`ASA5510(config-pmap-c)#`**`inspect skinny`**

**针对 SCCP 的 ASA 配置**

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SCCP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2000 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp !---
Command to enable SCCP inspection. inspect skinny
inspect esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp inspect ftp ! !--- This
command tells the device to !--- use the "global_policy"
policy-map on all interfaces. service-policy
global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

# 验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

**SIP:**

为确保配置已成功实施，应使用 **show service-policy** 命令，并使用 **show service-policy inspect sip** 命令将输出限制为仅包含 SIP 检查。

```
ASA5510#show service-policy inspect sip Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: sip, packet 0, drop 0, reset-drop 0 ASA5510#
```

**MGCP ：**

```
ASA5510#show service-policy inspect mgcp Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

**H.323 ：**

```
ASA5510(config)#show service-policy inspect h323 h225 Global policy: Service-policy:
global_policy Class-map: inspection_default Inspect: h323 h225 _default_h323_map, packet 0, drop
0, reset-drop 0 h245-tunnel-block drops 0 connection ASA5510(config)#show service-policy inspect
h323 ras Global policy: Service-policy: global_policy Class-map: inspection_default Inspect:
h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0 h245-tunnel-block drops 0 connection
```

**SCCP ：**

```
ASA5510(config)#show service-policy inspect skinny Global policy: Service-policy: global_policy
Class-map: inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

# 故障排除

## 问题

办公室Communicator不能穿过ASA，在VPN通道注册的IP电话断开，或者没有在IP电话的音频在VPN通道间。

## 解决方案

Office Communicator 不使用任何标准 SIP，默认情况下 ASA 会将其丢弃。 禁用 SIP、精简和 H323 检查以解决此问题，并在 ASA 中使用 clear xlate 和 local-host。同一解决方案为IP电话也是适用。

## 问题

视频呼叫失败与`%ASA-4-405102 H245 faddrXX.XX.XX.XXladdr XX.XX.XX.XX/3239`错误消息。

## 解决方案

禁用 H323 检查以解决此问题。

# 相关信息

- PIX/ASA 7.x：实现接口之间的通信
- 使用 PIX 防火墙处理 VoIP 流量
- Cisco Unified CallManager 5.0 TCP 和 UDP 端口使用情况
- Cisco ASA 5500 系列自适应安全设备产品支持
- Cisco PIX 500 系列安全设备产品支持
- Media Gateway Control Protocol (MGCP) 技术支持
- Skinny Call control Protocol (SCCP) 技术支持
- H.323 技术支持
- 技术支持和文档 - Cisco Systems