# PIX/ASA 7.x: Ejemplo de configuración de los servicios del permiso VoIP (SORBO, MGCP, H323, SCCP)

## Contenido



## Introducción

Este documento describe cómo permitir el tráfico de los protocolos de la voz sobre IP (VoIP) en la interfaz exterior y habilitar el examen para cada protocolo en los dispositivos de seguridad del PIX/ASA de Cisco.

Éstos son los protocolos:

- **Session Initiation Protocol (SIP)** — El SORBO es un protocolo del control de la capa de la aplicación (señalización) que crea, modifica, y termina las sesiones con uno o más participantes. Estas sesiones incluyen las llamadas telefónicas de Internet, la distribución de las multimedias, y las conferencias de las multimedias.SORBA, según lo definido por la Fuerza de tareas de ingeniería en Internet (IETF) (IETF), las llamadas VoIP de los permisos.

SORBA los trabajos con el protocolo session description (SDP) para la señalización de llamada. El SDP especifica los detalles de la secuencia de medios. El dispositivo de seguridad puede soportar cualquier gateway del SORBO (VoIP) y los servidores proxy VoIP cuando se utiliza el SORBO. El SORBO y el SDP se definen en estos RFC:SORBO: Session Initiation Protocol, RFC 3261SDP: Protocolo session description, RFC 2327Para soportar las llamadas del SORBO a través del dispositivo de seguridad, los mensajes de señalización para los direccionamientos de la conexión de medios, los puertos de los media, y las conexiones embrionarias para los media deben ser examinados. Esto es porque mientras que la señalización se envía sobre un puerto de destino conocido (**UDP/TCP 5060**), las secuencias de medios se afectan un aparato dinámicamente. También, el SORBO integra los IP Addresses en la porción de los useres data del paquete del IP. El examen del SORBO aplica el Network Address Translation (NAT) para estos IP Address incluidos.**Nota:** Si un punto final remoto intenta registrarse con un proxy del SORBO en una red protegida por el dispositivo de seguridad, el registro falla bajo condiciones muy específicas. Estas condiciones son cuando el Port Address Translation (PAT) se configura para el punto final remoto, el secretario del SORBO que el servidor está en la red externa, y cuando el puerto falta en el campo del contacto en el mensaje del REGISTRO enviado por el punto final al servidor proxy.

- **Media Gateway Control Protocol (MGCP)** — El MGCP es un protocolo del Control de llamadas del servidor del cliente, empleado la arquitectura del control centralizado. Toda la información del Plan de marcado reside en un agente de la llamada diferentes. El agente de la llamada, que controla los puertos en el gateway, realiza el Control de llamadas. El gateway hace la traducción de medios entre el Public Switched Telephone Network (PSTN) y las redes VoIP para las llamadas externas. En una red basada en Cisco, los CallManageres funcionan como los agentes de la llamada.El MGCP es una norma de IETF que se define en varios RFC, que incluye 2705 y 3435 . Sus capacidades se pueden ampliar por el uso de los paquetes que incluyen, por ejemplo, la dirección de los tonos del Multifrecuencia de tono dual (DTMF), del RTP seguro, del control de la llamada, y de la transferencia de llamada.Un gateway MGCP es relativamente fácil de configurar. Porque el agente de la llamada tiene toda la inteligencia del Call Routing, usted no necesita configurar el gateway con todos los dial peer que necesitaría de otra manera. Una desventaja es que un agente de la llamada debe siempre estar disponible. Los gatewayes de Cisco MGCP pueden utilizar el Survivable Remote Site Telephony (SRST) y el repliegue soporte de MGCP para permitir que el protocolo de H.323 asuma el control y proporcione la encaminamiento de la Llamada local en ausencia de un CallManager. En ese caso, usted debe configurar a los dial peer en el gateway para uso de H.323.
- **H.323** — El examen de H.323 proporciona el soporte para las aplicaciones compatibles de H.323 tales como Cisco CallManager y portero de VocalTec. H.323 es un conjunto de protocolos definido por la Unión Internacional de Telecomunicaciones para las conferencias de las multimedias sobre los LAN. El dispositivo de seguridad soporta H.323 a través de la versión 4, que incluye las varias llamadas de la característica del v3 de H.323 en un canal de señalización de llamada.Con el examen de H.323 habilitado, el dispositivo de seguridad soporta las varias llamadas en el canal de señalización de la misma llamada, una característica introducida con la versión 3 de H.323. Esta característica reduce el tiempo de configuración de llamada y reduce el uso de los puertos en el dispositivo de seguridad.Éstas son las dos funciones principales del examen de H.323:NAT que el IPv4 integrado necesario dirige en los mensajes H.225 y H.245. Porque los mensajes de H.323 se codifican adentro POR el formato de codificación, el dispositivo de seguridad utiliza un decodificador ASN.1 para decodificar los mensajes de H.323.Afecte un aparato dinámicamente las conexiones

negociadas H.245 y RTP/RTCP.

- **El protocolo del control de cliente flaco (o simple) (SCCP)** — SCCP es un protocolo simplificado usado en las redes VoIP. Los Teléfonos IP de Cisco que utiliza el SCCP pueden coexistir en un entorno de H.323. Cuando está utilizado con el Cisco CallManager, el cliente SCCP puede interoperar con las terminales H.323-compliant. Las funciones de la capa de la aplicación en el dispositivo de seguridad reconocen la versión 3.3 del SCCP. Las funciones del software de la capa de la aplicación se aseguran de que toda la señalización y paquetes de medios del SCCP puedan atravesar el dispositivo de seguridad proporcionando al NAT del SCCP que señala los paquetes.Hay 5 versiones del protocolo SCCP: 2.4, 3.0.4, 3.1.1, 3.2, y 3.3.2. El dispositivo de seguridad soporta todas las versiones a través de la versión 3.3.2. El dispositivo de seguridad proporciona el soporte de la PALMADITA y NAT para el SCCP. La PALMADITA es necesaria si usted tiene números limitados de IP Address globales para uso de los Teléfonos IP.El tráfico normal entre el Cisco CallManager y los Teléfonos IP de Cisco utiliza el SCCP y es dirigido por el examen del SCCP sin ninguna configuración especial. El dispositivo de seguridad también soporta las opciones DHCP 150 y 66, que permiten que el dispositivo de seguridad envíe la ubicación de un servidor TFTP a los Teléfonos IP de Cisco y a otros clientes DHCP. Refiera a configurar los servicios del DHCP, DDNS, y WCCP para más información.

# prerrequisitos

## Requisitos

Este documento asume que la configuración VPN necesaria está hecha en todos los dispositivos y trabaja correctamente.

Refiérase ASA/PIX: Dispositivo de seguridad a un ejemplo de configuración del router IOS túnel ipsec de LAN a LAN para aprender más sobre la configuración VPN.

Consulte PIX/ASA 7.x: Habilite la comunicación entre las interfaces para más información sobre cómo habilitar la comunicación entre las interfaces.

## Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) que funciona con la versión de software 7.x.

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 pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Productos Relacionados

Esta configuración se puede también utilizar con el firewall PIX de las Cisco 500 Series que funciona con la versión de software 7.x.

## Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

# Antecedentes

## SORBO

SORBA el examen NAT los mensajes basados texto del SORBO, recalcula la longitud contenta para la porción SDP del mensaje, y recalcula la Longitud del paquete y la suma de comprobación. Abre dinámicamente las conexiones de medios para los puertos especificadas en la porción SDP del mensaje del SORBO como el direccionamiento/puertos en los cuales el punto final debe escuchar.

El examen del SORBO tiene una base de datos con los índices CALL_ID/FROM/TO del payload del SORBO que identifique la llamada, así como la fuente y el destino. Se contienen dentro de esta base de datos los direccionamientos de los media y los puertos de los media que fueron contenidos en los campos de información de los media SDP y el tipo de media. Puede haber direccionamientos y puertos de los medios múltiples para una sesión. Las conexiones RTP/RTCP se abren entre los dos puntos finales usando estos direccionamientos/puertos de los media.

El puerto conocido 5060 se debe utilizar en el mensaje de la configuración de llamada inicial (INVITE). Sin embargo, los mensajes subsiguientes no pudieron tener este número del puerto. El motor del examen del SORBO abre los agujeritos de la conexión de la señalización, y marca estas conexiones como conexiones del SORBO. Esto se hace para que los mensajes alcancen la aplicación del SORBO y sean NATed.

Mientras que se configura una llamada, la sesión del SORBO se considera en el estado transitorio. Sigue habiendo este estado hasta que se reciba un mensaje de respuesta que indica el direccionamiento y el puerto de los media RTP en los cuales el punto final de destino escucha. Si hay un error recibir los mensajes de respuesta en el plazo de un minuto, se derriba la conexión de la señalización.

Una vez que se hace el apretón de manos final, mueven al estado de la llamada al active y sigue habiendo la conexión de la señalización hasta que se reciba un mensaje del ADIÓS.

Si un punto final interior inicia una llamada a un punto final exterior, un agujero de los media se abre en la interfaz exterior para permitir que los paquetes UDP RTP/RTCP fluyan al direccionamiento de los media del punto final y al puerto interiores de los media especificado en el mensaje INVITE (Invitar) del punto final interior. Los paquetes UDP no solicitados RTP/RTCP a una interfaz interior no atravesarán el dispositivo de seguridad, a menos que la configuración del dispositivo de seguridad lo permita específicamente.

Las conexiones de medios se derriban dentro dos minutos después de que la conexión llega a estar ociosa. Esto es un descanso configurable y se puede fijar por un período de tiempo más corto o más largo.

## MGCP (Protocolo de control de gateway de medios)

Para utilizar el MGCP, usted necesita generalmente configurar por lo menos dos comandos inspect: uno para el puerto en el cual el gateway recibe los comandos, y uno para el puerto en el cual el agente de la llamada recibe los comandos. Normalmente, un agente de la llamada envía

los comandos al puerto del valor por defecto MGCP para los gatewayes, **2427**, y un gateway envía los comandos al puerto del valor por defecto MGCP para los agentes de la llamada, **2727**.

Los mensajes MGCP se transmiten sobre el **UDP**. Una respuesta se devuelve a la dirección de origen (dirección IP y número del puerto UDP) del comando, pero la respuesta no pudo llegar del mismo direccionamiento al cual el comando fue enviado. Esto puede ocurrir cuando los agentes de las varias llamadas se utilizan en una configuración de failover y el agente de la llamada que recibió el comando ha pasado el control a un agente de la llamada de backup, que entonces envía la respuesta.

## H.323

La colección de H.323 de protocolos puede utilizar colectivamente hasta dos conexión TCP y cuatro a seis conexiones UDP. El FastConnect utiliza solamente una conexión TCP, y la confiabilidad, la Disponibilidad, y la utilidad (RAS) utiliza una sola conexión UDP para el registro, las admisiones, y el estatus.

Un cliente de H.323 puede establecer inicialmente una conexión TCP a un servidor de H.323 usando el puerto TCP 1720 para pedir la configuración de la llamada del q.931. Como parte del proceso de configuración de llamada, la terminal de H.323 suministra un número del puerto al cliente para utilizar para una conexión TCP H.245. En los entornos donde está funcionando el portero de H.323, el paquete inicial se transmite usando el UDP.

El examen de H.323 monitorea la conexión TCP del q.931 para determinar el número del puerto H.245. Si los Terminales H.323 no utilizan el FastConnect, el dispositivo de seguridad afecta un aparato dinámicamente la conexión H.245 basada en el examen de los mensajes H.225.

Dentro de cada mensaje H.245, los puntos finales de H.323 intercambian los números del puerto que se utilizan para las secuencias de datos subsiguientes UDP. El examen de H.323 examina los mensajes H.245 para identificar estos puertos y crea dinámicamente las conexiones para el intercambio de los media. El RTP utiliza el número del puerto negociado, mientras que el RTCP utiliza el número del puerto más alto siguiente.

El canal de control de H.323 dirige H.225 y H.245 y H.323 RAS. El examen de H.323 utiliza estos puertos:

- 1718 — Puerto de la detección UDP del encargado de puerta
- 1719 — Puerto RAS UDP
- 1720 — Puerto de control TCP

Usted debe permitir el tráfico para el puerto bien conocido 1720 de H.323 para la señalización de llamada H.225. Sin embargo, los puertos de la señalización H.245 se negocian entre los puntos finales en la señalización H.225. Cuando utilizan a un portero de H.323, el dispositivo de seguridad abre una conexión H.225 basada en el examen Confirmación de admisión (ACF) del mensaje.

Después de que se examinen los mensajes H.225, el dispositivo de seguridad abre el canal H.245 y después examina el tráfico enviado sobre el canal H.245. Todos los mensajes H.245 que pasan a través del dispositivo de seguridad experimentan la Inspección de la aplicación H.245, que traduce los IP Address incluidos y abren los canales de los media negociados en los mensajes H.245.

El estándar de ITU de H.323 requiere que una encabezado del paquete de la unidad de datos del

Transport Protocol (TPKT), que define la longitud del mensaje, preceda el H.225 y el H.245, antes de ser pasado encendido a la conexión confiable. Porque la encabezado TPKT no necesita necesariamente ser enviada en el mismo paquete TCP que los mensajes H.225 y H.245, el dispositivo de seguridad debe recordar la longitud TPKT para procesar y para decodificar los mensajes correctamente. Para cada conexión, el dispositivo de seguridad guarda un expediente que contenga la longitud TPKT para el mensaje previsto siguiente.

Si el dispositivo de seguridad necesita realizar el NAT en los IP Addresses en los mensajes, cambia la suma de comprobación, la longitud UUIE, y el TPKT, si se incluye en el paquete TCP con el mensaje H.225. Si el TPKT se envía en un paquete TCP separado, los acuses de recibo del proxy del dispositivo de seguridad (ACK) ese TPKT y añaden un nuevo TPKT al final del fichero al mensaje H.245 con la nueva longitud.

### SCCP

En las topologías donde el Cisco CallManager está situado en la interfaz de mayor seguridad en cuanto a los Teléfonos IP de Cisco, si el NAT se requiere para la dirección IP del Cisco CallManager, la asignación debe ser estática mientras que un Cisco IP Phone requiere la dirección IP del Cisco CallManager ser especificado explícitamente en su configuración. Una Entrada estática de la identidad permite que el Cisco CallManager en la interfaz de mayor seguridad valide los registros de los Teléfonos IP de Cisco.

Los Teléfonos IP de Cisco requieren el acceso a un servidor TFTP para descargar la información de la configuración que necesitan conectar con el Cisco Callmanager server.

Cuando los Teléfonos IP de Cisco están en una interfaz de menor seguridad comparada al servidor TFTP, usted debe utilizar una lista de acceso para conectar con el servidor TFTP protegido en el puerto 69 UDP. Mientras que usted necesita una Entrada estática para el servidor TFTP, esto no tiene que ser una Entrada estática de la identidad. Cuando se utiliza el NAT, una Entrada estática de la identidad asocia a la misma dirección IP. Cuando se utiliza la PALMADITA, asocia a la misma dirección IP y puerto.

Cuando los Teléfonos IP de Cisco están en una interfaz de mayor seguridad comparada al servidor TFTP y al Cisco CallManager, no se requiere ninguna lista de acceso o Entrada estática para permitir que los Teléfonos IP de Cisco inicien la conexión.

## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

### Diagrama de la red para el SORBO

Esta sección utiliza esta configuración de red:

### Configuraciones para el SORBO

Esta sección usa estas configuraciones:

El dispositivo de seguridad soporta la Inspección de la aplicación con la función del algoritmo de seguridad adaptable. Con la Inspección de la aplicación stateful usada por el algoritmo de seguridad adaptable, el dispositivo de seguridad sigue cada conexión que atraviese el Firewall y se asegura de que son válidos. El Firewall, con la inspección con estado, también monitorea el estado de la conexión para compilar la información para colocar en una tabla de estado. Con el uso de la tabla de estado además de las reglas administrador-definidas, las decisiones de filtración se basan en el contexto que es establecido por los paquetes pasajeros previamente con el Firewall. La implementación de las Inspecciones de la aplicación consiste en estas acciones:

- Identifique el tráfico.
- Aplique los exámenes al tráfico.
- Active los exámenes en una interfaz.

### Configure el examen básico del SORBO

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global. Por lo tanto, si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar o para agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el **comando policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Publique el **comando class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Publique el comando del **sorbo de la inspección**.`ASA5510(config-pmap-c)#inspect sip`

**Configuración ASA para el SORBO**

```
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#
```

## Diagrama de la red para el MGCP, H.323 y el SCCP

Esta sección utiliza esta configuración de red:

## Configuraciones para el MGCP

Esta sección usa estas configuraciones:

El dispositivo de seguridad soporta la Inspección de la aplicación con la función del algoritmo de seguridad adaptable. Con la Inspección de la aplicación stateful usada por el algoritmo de seguridad adaptable, el dispositivo de seguridad sigue cada conexión que atraviese el Firewall y se asegura de que son válidos. El Firewall, con la inspección con estado, también monitorea el estado de la conexión para compilar la información para colocar en una tabla de estado. Con el uso de la tabla de estado además de las reglas administrador-definidas, las decisiones de filtración se basan en el contexto que es establecido por los paquetes pasajeros previamente con el Firewall. La implementación de las Inspecciones de la aplicación consiste en estas acciones:

- Identifique el tráfico.
- Aplique los exámenes al tráfico.
- Active los exámenes en una interfaz.

### Configure el examen básico MGCP

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global. Por lo tanto, si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar o para agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el **comando policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Publique el **comando class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Publique el **comando mgcp de la inspección**.`ASA5510(config-pmap-c)#inspect mgcp`

### Configure una correspondencia de políticas del examen MGCP para el control adicional del examen

Si la red tiene los agentes y gatewayes de las varias llamadas para los cuales el dispositivo de seguridad tiene que abrir los agujeritos, cree una correspondencia MGCP. Usted puede entonces aplicar la correspondencia MGCP cuando usted habilita el examen MGCP. Refiera a configurar la Inspección de la aplicación para más información.

```
!--- 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
```

**Configuración ASA para el MGCP**

```
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
```

## Configuraciones para H.323

Esta sección usa estas configuraciones:

El dispositivo de seguridad soporta la Inspección de la aplicación con la función del algoritmo de seguridad adaptable. Con la Inspección de la aplicación stateful usada por el algoritmo de seguridad adaptable, el dispositivo de seguridad sigue cada conexión que atraviese el Firewall y se asegura de que son válidos. El Firewall, con la inspección con estado, también monitorea el estado de la conexión para compilar la información para colocar en una tabla de estado. Con el uso de la tabla de estado además de las reglas administrador-definidas, las decisiones de filtración se basan en el contexto que es establecido por los paquetes pasajeros previamente con el Firewall. La implementación de las Inspecciones de la aplicación consiste en estas acciones:

- Identifique el tráfico.
- Aplique los exámenes al tráfico.
- Active los exámenes en una interfaz.

### Configure el examen básico de H.323

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global. Por lo tanto, si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar o para agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el **comando policy-map global_policy**.`ASA5510(config)#`**`policy-map global_policy`**
2. Publique el **comando class inspection_default**.`ASA5510(config-pmap)#`**`class inspection_default`**
3. Publique el **comando h323 de la inspección**.`ASA5510(config-pmap-c)#`**`inspect h323 h225`**
   `ASA5510(config-pmap-c)#`**`inspect h323 ras`**

**Configuración ASA para H.323**

```
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#
```

## Configuraciones para el SCCP

Esta sección usa estas configuraciones:

El dispositivo de seguridad soporta la Inspección de la aplicación con la función del algoritmo de seguridad adaptable. Con la Inspección de la aplicación stateful usada por el algoritmo de seguridad adaptable, el dispositivo de seguridad sigue cada conexión que atraviese el Firewall y se asegura de que son válidos. El Firewall, con la inspección con estado, también monitorea el estado de la conexión para compilar la información para colocar en una tabla de estado. Con el uso de la tabla de estado además de las reglas administrador-definidas, las decisiones de filtración se basan en el contexto que es establecido por los paquetes pasajeros previamente con

el Firewall. La implementación de las Inspecciones de la aplicación consiste en estas acciones:

- Identifique el tráfico.
- Aplique los exámenes al tráfico.
- Active los exámenes en una interfaz.

### Configure el examen básico del SCCP

Por abandono, la configuración incluye una directiva que haga juego todo el tráfico del examen de la aplicación predeterminada y aplique el examen al tráfico en todas las interfaces (una política global). El tráfico del examen de la aplicación predeterminada incluye el tráfico a los puertos predeterminados para cada protocolo. Usted puede aplicar solamente una política global. Por lo tanto, si usted quiere alterar la política global, por ejemplo, para aplicar el examen a los puertos no estándar o para agregar los exámenes que no se habilitan por abandono, usted necesita editar la política predeterminada o inhabilitarla y aplicar un nuevo. Para una lista de todos los puertos predeterminados, refiera a la directiva predeterminada del examen.

1. Publique el **comando policy-map global_policy**.`ASA5510(config)#`**`policy-map global_policy`**
2. Publique el **comando class inspection_default**.`ASA5510(config-pmap)#`**`class inspection_default`**
3. Publique el comando **flaco de la inspección**.`ASA5510(config-pmap-c)#`**`inspect skinny`**

**Configuración ASA para el SCCP**

```
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#
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

### SORBO:

Para asegurar la configuración ha tomado, utiliza el **comando service-policy de la demostración** y limita con éxito la salida al examen del SORBO solamente, usando la servicio-**directiva de la demostración examina el** comando del **sorbo**.

```
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
```

# Troubleshooting

### Problema

El comunicador de la oficina no puede pasar con el ASA, el iPhone registrado sobre el túnel VPN consigue disconnected, o hay no audio en los Teléfonos IP a través de los túneles VPN.

### Solución

El comunicador de la oficina no utilizó ningún SORBO estándar , y por abandono, el ASA lo cae. Inhabilite el SORBO, flaco y el examen H323 para solucionar este problema y también `clear xlate`

y `host local` en el ASA. La misma solución solicita el IPhones también.

### Problema

Llamadas del vídeo falladas con el `%ASA-4-405102: Incapaz de reservar la conexión H245 para el faddr XX.XX.XX.XX al` mensaje de error de `XX.XX.XX.XX/3239 del laddr`.

### Solución

Examen de la neutralización H323 para resolver este problema.

## Información Relacionada

- PIX/ASA 7.x: Comunicación del permiso entre las interfaces
- Tráfico de VoIP de la manija con el firewall PIX
- Cisco Unified CallManager 5.0 TCP y uso del puerto UDP
- Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte de productos del Dispositivos de seguridad Cisco PIX de la serie 500
- Soporte de tecnología del Media Gateway Control Protocol (MGCP)
- Soporte de tecnología del Skinny Call Control Protocol (SCCP)
- Soporte de tecnología de H.323
- Soporte Técnico y Documentación - Cisco Systems