PIX/ASA 7.x: Exemplo de Configuração de Serviços de Habilitação de VoIP (SIP, MGCP, H323, SCCP)

Índice

Introdução

Este documento descreve como permitir o tráfego dos protocolos de Voice over IP (VoIP) na interface externa e habilitar a inspeção para cada protocolo nos Cisco PIX/ASA Security Appliances.

Estes são os protocolos:

- **Session Initiation Protocol (SIP)** — O SIP é um protocolo de controle (sinalização) da camada de aplicativos que cria, modifica e encerra sessões com um ou mais participantes. Essas sessões incluem chamadas telefônicas pela Internet, distribuição de multimídia e conferências de multimídia.O SIP, conforme definido pela Internet Engineering Task Force (IETF), possibilita as chamadas de VoIP. O SIP trabalha com o Session Description Protocol

(SDP) para sinalizar chamadas. O SDP especifica os detalhes do fluxo de mídia. O Security Appliance aceita qualquer tipo de gateway de SIP (VoIP) e servidores proxy de VoIP quando o SIP é usado. O SIP e o SDP são definidos nestas RFCs:SIP: Protocolo de iniciação de sessão, RFC 3261SDP: Protocolo session description, RFC 2327Para oferecer suporte às chamadas de SIP via Security Appliance, as mensagens de sinalização para os endereços de conexão de mídia, portas de mídia e conexões embrionárias para a mídia devem ser inspecionadas. Isso acontece porque enquanto a sinalização é enviada por uma porta de destino conhecida (**UDP/TCP 5060**), os fluxos de mídia são alocados dinamicamente. Além disso, o SIP incorpora os endereços IP na área de dados do usuário do pacote IP. A inspeção do SIP aplica o Network Address Translation (NAT) a esses endereços IP incorporados.**Nota:** Se um ponto final remoto tenta se registrar com um proxy do SORVO em uma rede protegida pela ferramenta de segurança, o registro falha sob circunstâncias muito específicas. Essas condições ocorrem quando o Port Address Translation (PAT) está configurado para o ponto final remoto, o servidor registrante do SIP está fora da rede e a porta está ausente do campo de contato na mensagem REGISTER enviada pelo ponto final ao servidor proxy.

- **Media Gateway Control Protocol (MGCP)** — O MGCP é um protocolo de controle de chamadas cliente-servidor baseado em uma arquitetura de controle centralizado. Todas as informações do plano de discagem residem em um agente de chamadas separado. O agente de chamadas, o qual controla as portas do gateway, executa o controle de chamadas. O gateway faz a conversão de mídia entre a rede telefônica pública comutada (PSTN) e as redes VoIP para chamadas externas. Em um ambiente de rede Cisco, os CallManagers funcionam como os agentes de chamadas.O MGCP é um padrão de IETF que seja definido em diversos RFC, que inclui 2705 e 3435 . Os seus recursos podem ser expandidos com o uso de pacotes que incluem, por exemplo, o gerenciamento de tons Dual-Tone Multifrequency (DTMF), RTP seguro, retenção de chamadas e transferência de chamadas.Érelativamente fácil configurar um gateway MGCP. Como a inteligência do roteamento de chamadas está no agente de chamadas, não é necessário configurar o gateway com todos os peers de discagem que de outra forma seriam necessários. Uma desvantagem é que um agente de chamadas deverá estar sempre disponível. Os gateways Cisco MGCP podem usar a Survivable Remote Site Telephony (SRST) e o fallback do MGCP para permitir que o protocolo H.323 assuma e forneça o roteamento de chamadas locais na ausência de um CallManager. Nesse caso, você deverá configurar os peers de discagem no gateway para uso pelo H.323.
- **H.323** — A inspeção de H.323 oferece suporte a aplicativos compatíveis com o H.323, como o Cisco CallManager e o VocalTec Gatekeeper. O H.323 é um conjunto de protocolos definido pela International Telecommunication Union para conferências multimídia em LANs. O Security Appliance oferece suporte até o H.323 Versão 4, o que inclui o recurso de várias chamadas em um canal de sinalização de uma chamada do H.323 v3.Com a inspeção de H.323 permitida, a ferramenta de segurança apoia chamadas múltiplas no canal de sinalização da mesma chamada, uma característica introduzida com versão 3 de H.323. Esta característica reduz o tempo de configuração de chamada e reduz o uso das portas na ferramenta de segurança.As duas principais funções da inspeção de H.323 são:Executar o NAT dos endereços IPv4 incorporados necessários nas mensagens de H.225 e H.245. Como as mensagens de H.323 são codificadas no formato PER, o Security Appliance usa um decodificador ASN.1 para decodificá-las.Alocar dinamicamente as conexões H.245 e RTP/RTCP negociadas.
- **Skinny (ou Simple) Client Control Protocol (SCCP)** — O SCCP é um protocolo simplificado

usado em redes de VoIP. Os Cisco IP Phones que usam o SCCP podem coexistir em um ambiente H.323. Quando usado com o Cisco CallManager, o cliente SCCP pode interoperar com terminais compatíveis com o H.323. As funções da camada de aplicativos no Security Appliance reconhecem o SCCP Versão 3.3 A funcionalidade do software da camada de aplicativos garante que todos os pacotes de sinalização e mídia do SCCP possam cruzar o Security Appliance por meio do NAT dos pacotes de sinalização do SCCP.Há as versões 5 do protocolo de SCCP: 2.4, 3.0.4, 3.1.1, 3.2, e 3.3.2. A ferramenta de segurança apoia todas as versões através da versão 3.3.2. A ferramenta de segurança fornece o apoio da PANCADINHA e NAT para o SCCP. O PAT é necessário quando há um número limitado de endereços IP globais que podem ser usados por telefones IP.O tráfego normal entre o Cisco CallManager e os Cisco IP Phones usa o SCCP e é gerenciado pela inspeção de SCCP sem nenhuma configuração especial. O Security Appliance também oferece suporte às opções 150 e 66 do DHCP, as quais permitem que o Security Appliance envie a localização de um servidor TFTP para os Cisco IP Phones e demais clientes DHCP. Consulte Configurando Serviços de DHCP, DDNS e WCCP para obter mais informações.

Pré-requisitos

Requisitos

Este documento pressupõe que as configurações de VPN necessárias tenham sido feitas em todos os dispositivos e estejam funcionando corretamente.

Refira ASA/PIX: Ferramenta de segurança a um exemplo de configuração do túnel IPSec de LAN para LAN do IOS Router a fim aprender mais sobre a configuração de VPN.

Refira ao PIX/ASA 7.x: Permita uma comunicação entre relações para obter mais informações sobre de como permitir a comunicação entre relações.

Componentes Utilizados

As informações deste documento baseiam-se no Cisco 5500 Series Adaptive Security Appliance (ASA) com a versão 7 do software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração também pode ser usada no Cisco 500 Series PIX Firewall com a versão 7 do software.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

SORVO

A inspeção de SIP aplica NAT às mensagens de texto do SIP, recalcula o comprimento do conteúdo para a porção SDP da mensagem e recalcula o tamanho e a soma de verificação do pacote. Ela abre dinamicamente as conexões de mídia para as portas especificadas na área de SDP da mensagem do SIP como endereços/porta que devem ser escutados pelo ponto final.

A inspeção de SIP possui um banco de dados com índices CALL_ID/FROM/TO da payload do SIP que identifica a chamada, bem como a origem e o destino. Esse banco de dados contém os endereços e portas de mídias que pertenciam aos campos de informação de mídia do SDP e o tipo da mídia. Pode haver vários endereços de mídia e portas para uma sessão. As conexões de RTP/RTCP são abertas entre os dois pontos finais usando-se esses endereços/portas de mídia.

A conhecida porta 5060 deve ser usada na mensagem de estabelecimento inicial da chamada (INVITE). No entanto, as mensagens subseqüentes poderão não ter esse número de porta. O mecanismo de inspeção de SIP abre os pinholes de conexão de sinalização e marca essas conexões como conexões de SIP. Isso é feito para que as mensagens cheguem até o aplicativo SIP e sejam convertidas pelo NAT.

Quando uma chamada é estabelecida, a sessão de SIP é considerada no estado transiente. Esse estado permanecerá até que uma mensagem de resposta seja recebida, o que indica o endereço de mídia RTP e a porta na qual o ponto final de destino escuta. Se houver uma falha no recebimento das mensagens de resposta em até um minuto, a conexão de sinalização será interrompida.

Quando o handshake final é feito, o estado da chamada é alterado para ativo e a conexão de sinalização permanece até o recebimento de uma mensagem BYE.

Se um ponto final interno iniciar uma chamada para um ponto final externo, uma passagem de mídia será aberta para a interface externa a fim de permitir que os pacotes UDP do RTP/RCTP fluam do endereço e da porta de mídia do ponto interno especificados na mensagem INVITE do ponto final interno. Os pacotes UDP do RTP/RTCP não solicitados enviados para uma interface interna não passarão pelo Security Appliance, a menos que a configuração do dispositivo o permita de forma explícita.

As conexões de mídia são interrompidas em até dois minutos após a conexão se tornar ociosa. Este é um timeout configurável e pode ser aumentado ou diminuído.

MGCP

A fim usar o MGCP, você precisa geralmente de configurar pelo menos dois comandos inspect: um para a porta em que o gateway recebe comandos, e um para a porta em que o agente do atendimento recebe comandos. Normalmente, um agente de chamadas envia comandos para a porta de MGCP padrão para gateways, **2427**, e um gateway envia comandos para a porta de MGCP padrão para agentes de chamadas, **2727**.

As mensagens de MGCP são transmitidas via **UDP**. Uma resposta é enviada de volta para o endereço de origem (endereço IP e número da porta IP) do comando, mas a resposta pode não ser originada pelo mesmo endereço para o qual o comando foi enviado. Isso pode ocorrer quando

vários agentes de chamadas são usados em uma configuração de failover e o agente de chamadas que recebeu o comando passou o controle para um agente de backup, o qual enviou a resposta.

H.323

A coleção de protocolos H.323 pode usar em conjunto até duas conexões de TCP e entre quatro e seis conexões de UDP. O FastConnect somente uma conexão de TCP e o Reliability, Availability, and Serviceability (RAS) usa uma única conexão de UDP para registro, admissão e status.

Um cliente H.323 pode inicialmente estabelecer uma conexão de TCP para um servidor H.323 usando a porta 1720 do TCP para solicitar o estabelecimento de uma chamada Q.931. Como parte do processo de estabelecimento da chamada, o terminal H.323 fornece um número de porta para o cliente usar em uma conexão de TCP H.245. Em ambientes em que o gatekeeper H.323 é usado, o pacote inicial é transmitido via UDP.

A inspeção de H.323 monitora a conexão de TCP Q.931 para determinar o número da porta do H.245. Se os terminais H.323 não usarem o FastConnect, o Security Appliance alocará dinamicamente a conexão H.245 com base na inspeção de mensagens do H.225.

Em cada mensagem do H.245, os pontos finais H.323 trocam números de portas que são usadas nos fluxos de dados UDP subseqüentes. A inspeção de H.323 inspeciona as mensagens do H.245 para identificar essas portas e cria dinamicamente conexões para a troca de mídias. O RTP usa o número da porta negociado, enquanto que o RCTP usa o próximo número de porta mais alto.

O canal de controle do H.323 gerencia o H.225 e o H.245 e o RAS H.323. A inspeção de H.323 usa estas portas:

- 1718 — Porta UDP da Gate Keeper Discovery
- 1719 — Porta UDP do RAS
- 1720 — Porta de controle do TCP

Você deve permitir o tráfego para a conhecida porta 1720 do H.323 para a sinalização de chamadas do H.225. No entanto, as portas de sinalização do H.245 são negociadas entre os pontos finais na sinalização do H.225. Quando um gatekeeper de H.323 é usado, o Security Appliance abre uma conexão de H.225 baseada na mensagem de confirmação de admissão (ACF).

Após as mensagens do H.225 serem inspecionadas, o Security Appliance abre o canal H.245 e inspeciona o tráfego enviado pelo canal H.245. Todas as mensagens do H.245 que cruzam o Security Appliance passam pela inspeção de aplicativos do H.245, a qual converte os endereços IP incorporados e abre os canais de mídia negociados nas mensagens do H.245.

O padrão H.323 ITU necessita de um cabeçalho de Transport Protocol Data Unit Packet (TPKT), o qual define o tamanho da mensagem e precede o H.225 e o H.245 antes de ser passado adiante para a conexão confiável. Como o cabeçalho de TPKT não necessariamente precisa ser enviado no mesmo pacote de TCP que as mensagens H.225 e H.245, o Security Appliance deve lembrar do comprimento do TPKT para processar e decodificar as mensagens corretamente. Para cada conexão, o Security Appliance mantém um registro que contém o comprimento do TPKT para a próxima mensagem esperada.

Se o Security Appliance precisar executar o NAT nos endereços IP das mensagens, ele alterará a soma de verificação, o tamanho da UUIE e o TPKT, se ele estiver incluído no pacote de TCP com a mensagem do H.225. Se o TPKT é enviado em um pacote de TCP separado, o proxy do Security Appliance reconhece esse TPKT e anexa um novo TPKT à mensagem do H.245 com o novo tamanho.

SCCP

Nas topologias em que o Cisco CallManager está localizado na interface de segurança mais alta no que diz respeito aos Cisco IP Phones, se houver necessidade de NAT para o endereço IP do Cisco CallManager, o mapeamento deverá ser estático porque o Cisco IP Phone necessita que o endereço IP do Cisco CallManager seja especificado de forma explícita em sua configuração. Uma entrada estática de identidade permite que o Cisco CallManager na interface de segurança mais alta aceite registros dos Cisco IP Phones.

Os Cisco IP Phones necessitam de acesso a um servidor de TFTP a fim de baixar as informações de configuração necessárias para se conectarem ao servidor Cisco CallManager.

Quando os Telefones IP de Cisco estão em uma interface de segurança mais baixa comparada ao servidor TFTP, você deve usar uma lista de acessos a fim conectar ao servidor TFTP protegido na porta 69 UDP. Quando você precisar uma entrada estática para o servidor TFTP, esta não tem que ser uma entrada estática da identidade. Quando o NAT é usado, uma entrada estática de identidade é mapeada no mesmo endereço IP. Quando o PAT é usado, ele é mapeado nos mesmos endereço IP e porta.

Quando os Cisco IP Phones estão em uma interface de segurança mais alta em comparação com o servidor TFTP e o Cisco CallManager, nenhuma lista de acesso ou entrada estática é necessária para permitir que os Cisco IP Phones iniciem a conexão.

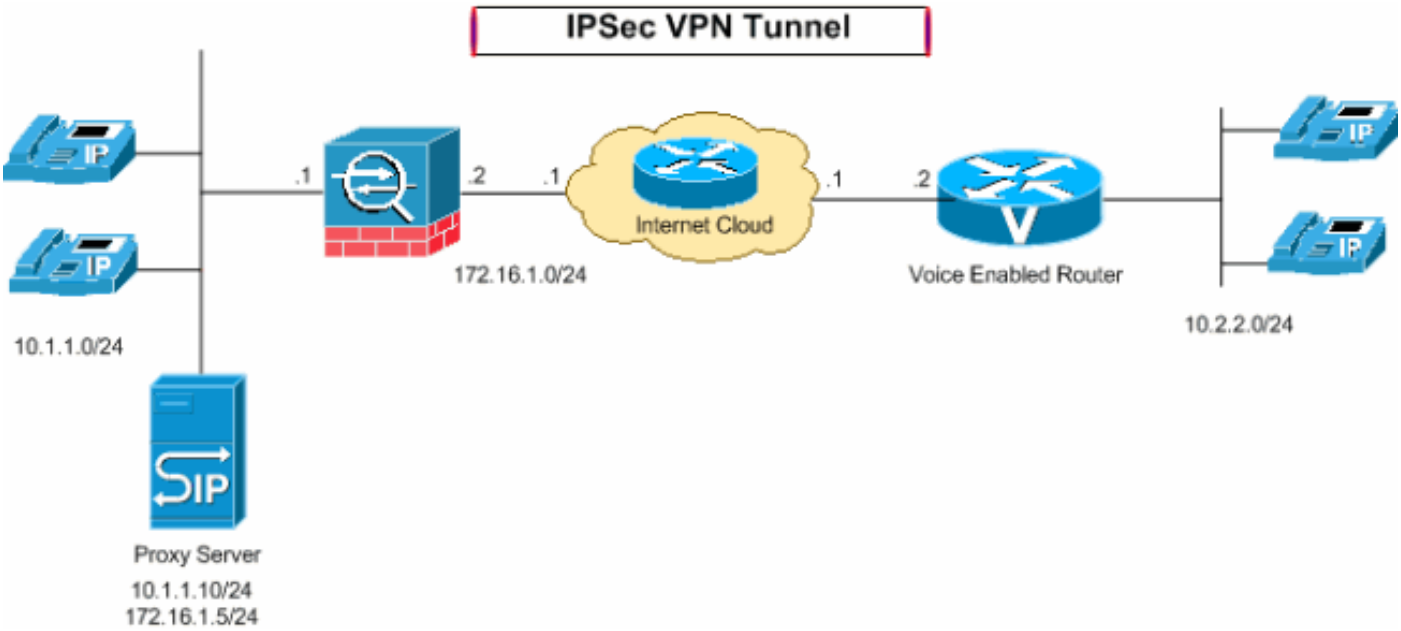
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede do SIP

Essa seção utiliza esta configuração de rede:



Configurações do SIP

Esta seção utiliza as seguintes configurações:

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm. Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas. O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados. Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall. A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego.
- Aplicar inspeções ao tráfego.
- Ativar as inspeções em uma interface.

Configuração da Inspeção Básica do SIP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção 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. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

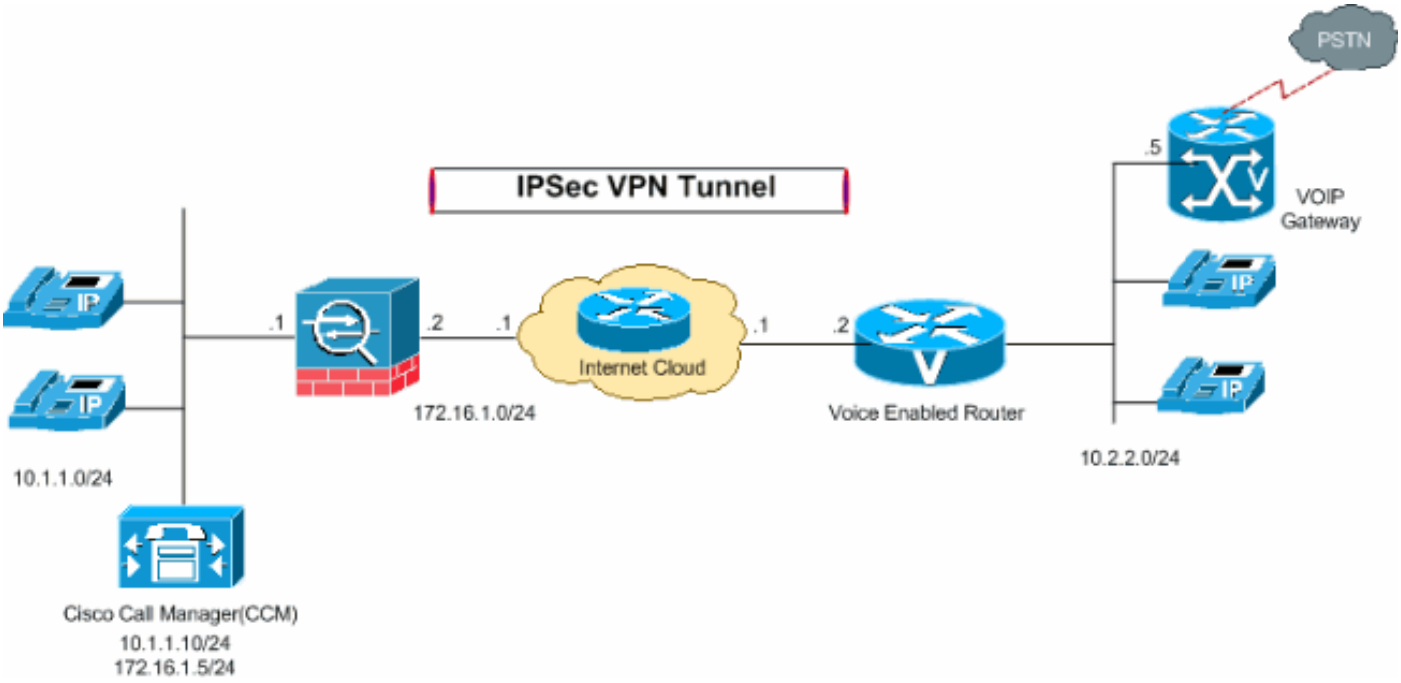
1. Execute o comando **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Execute o comando **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Execute o comando **inspect sip**.`ASA5510(config-pmap-c)#inspect sip`

Configuração de ASA para o SIP
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 Rede do MGCP, H.323 e SCCP

Essa seção utiliza esta configuração de rede:



Configurações do MGCP

Esta seção utiliza as seguintes configurações:

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm. Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas. O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados. Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall. A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego.
- Aplicar inspeções ao tráfego.
- Ativar as inspeções em uma interface.

Configuração da Inspeção Básica do MGCP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção 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. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

1. Execute o comando **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Execute o comando **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Execute o comando **inspect mgcp**.`ASA5510(config-pmap-c)#inspect mgcp`

Configuração de um Mapa de Políticas de Inspeção de MGCP para o Controle de Inspeção Adicional

Se a rede possuir vários agentes de chamadas e gateways para os quais o Security Appliance precisa abrir pinholes, crie um mapa de MGCP. Você poderá então aplicar o mapa de MGCP ao habilitar a inspeção de MGCP. Consulte Configurando a Inspeção de Aplicativos para obter mais informações.

```
!--- 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
```

Configuração de ASA para o 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
```

Configurações do H.323

Esta seção utiliza as seguintes configurações:

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm. Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas. O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados. Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall. A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego.
- Aplicar inspeções ao tráfego.
- Ativar as inspeções em uma interface.

Configuração da Inspeção Básica do H.323

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção 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. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

1. Execute o comando **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Execute o comando **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Execute o comando **inspect h323**.`ASA5510(config-pmap-c)#inspect h323 h225 ASA5510(config-pmap-c)#inspect h323 ras`

Configuração de ASA para o 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#
```

Configurações do SCCP

Esta seção utiliza as seguintes configurações:

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm. Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas. O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados. Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall. A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego.
- Aplicar inspeções ao tráfego.
- Ativar as inspeções em uma interface.

Configuração da Inspeção Básica do SCCP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção 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. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

1. Execute o comando **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Execute o comando **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Execute o comando **inspect skinny**.`ASA5510(config-pmap-c)#inspect skinny`

Configuração de ASA para o 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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

SIP:

Para garantir que a configuração tenha sido implementada com êxito, use o comando **show service-policy** e limite a saída somente à inspeção de SIP usando o comando **show service-policy inspect sip**.

```
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

O comunicador do escritório não pode passar com o ASA, o iPhone registrado sobre o túnel VPN obtém desligado, ou há não audio em Telefones IP através dos túneis VPN.

Solução

O Office Communicator usa no standard SIP e, por padrão, é descartado pelo ASA. Desabilite a inspeção do SORVO, a magro e do H323 a fim resolver estes problema e igualmente `clear xlate` e `host local no` ASA. A mesma solução aplica-se para o IPhones demasiado.

Problema

Atendimentos do vídeo falhados com o `%ASA-4-405102: Incapaz PRE-de atribuir a conexão H245 para o faddr XX.XX.XX.XX ao` Mensagem de Erro de `XX.XX.XX.XX/3239 do laddr`.

Solução

Inspeção de H323 do desabilitação a fim resolver esta edição.

Informações Relacionadas

- PIX/ASA 7.x: Habilitação da Comunicação Entre Interfaces
- Segure o tráfego voip com o PIX Firewall
- Cisco Unified CallManager 5.0 TCP e uso de porta UDP
- Sustentação do produto do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Sustentação do produto do Dispositivos de segurança Cisco PIX série 500
- Suporte por tecnologia do Media Gateway Control Protocol (MGCP)
- Suporte por tecnologia do Skinny Call Control Protocol (SCCP)
- Suporte por tecnologia de H.323
- Suporte Técnico e Documentação - Cisco Systems