PIX/ASA 7.x : Exemple de configuration de l'activation des services VoIP (SIP, MGCP, H323, SCCP)

Contenu

Introduction

Ce document décrit comment permettre le trafic de protocoles de voix sur IP (VoIP) sur l'interface externe et activer l'inspection pour chaque protocole dans les dispositifs de sécurité Cisco PIX/ASA.

Les protocoles sont les suivants :

- **Protocole d'initiation de session (SIP)** — Le SIP est un protocole de contrôle de la couche applicative (signalisation) qui crée, modifie, arrête des sessions comportant un ou plusieurs participants. Ces sessions incluent des appels téléphoniques via l'Internet, la distribution multimédia et les conférences multimédia.Le SIP, comme défini par l'Internet Engineering Task Force (IETF), active les appels VoIP. Le SIP fonctionne avec le Session Description

Protocol (SDP) pour la signalisation d'appel. Le SDP spécifie les détails concernant le flux multimédia. Le dispositif de sécurité peut prendre en charge toutes les passerelles SIP (VoIP) et tous les serveurs proxy de VoIP quand le SIP est utilisé. Le SIP et le SDP sont définis dans les ces RFC :SIP : protocole SIP (Session Initiation Protocol), RFC 3261SDP : Session Description Protocol, RFC 2327Afin de prendre en charge des appels SIP par le dispositif de sécurité, les messages de signalisation pour les adresses de connexion multimédias, les ports multimédias et les connexions embryonnaires pour le média doivent être inspectés. Ceci car, tandis que la signalisation est envoyée via un port de destination bien connu (**UDP/TCP 5060**), les flux multimédias sont dynamiquement alloués. En outre, le SIP inclut des adresses IP dans la partie données de l'utilisateur du paquet IP. L'inspection SIP applique la traduction d'adresses de réseau (NAT) pour ces adresses IP incluses.**Remarque:** si un périphérique distant essaye de s'enregistrer avec un proxy SIP sur un réseau protégé par le dispositif de sécurité, l'enregistrement échoue dans des conditions très spécifiques. Ces conditions sont quand la traduction d'adresses de port (PAT) est configurée pour le périphérique distant, le serveur de registre SIP est sur le réseau externe, et quand le port manque dans le champ de contact dans le message REGISTER (enregistrement) envoyé par le périphérique au serveur proxy.

- **Media Gateway Control Protocol (MGCP)** — Le MGCP est un protocole de contrôle d'appel client-serveur, construit sur une architecture de contrôle centralisée. Toutes les informations du plan de numérotation résident dans un agent d'appel séparé. L'agent d'appel, qui contrôle les ports sur la passerelle, exécute le contrôle d'appel. La passerelle effectue une traduction des médias entre le réseau téléphonique public commuté (PSTN) et les réseaux VoIP pour des appels externes. Dans un réseau basé sur Cisco, les CallManager fonctionnent en tant qu'agents d'appel.Le MGCP est un standard IETF qui est défini dans plusieurs RFC, incluant 2705 et 3435. Ses capacités peuvent être étendues en utilisant des modules qui incluent, par exemple, le traitement des tons multifréquences deux tons (DTMF), le RTP sécurisé, l'appel en attente et le transfert d'appel.Une passerelle MGCP est relativement facile à configurer. Puisque l'agent d'appel a toute l'intelligence du routage d'appel, vous n'avez pas besoin de configurer la passerelle avec tous les homologues de numérotation dont il aurait besoin autrement. Un inconvénient est qu'un agent d'appel doit toujours être disponible. Les passerelles Cisco MGCP peuvent recourir au Survivable Remote Site Telephony (SRST) et au MGCP pour permettre au protocole H.323 de prendre le relai et de fournir un routage d'appel local en l'absence de CallManager. Dans ce cas, vous devez configurer des homologues de numérotation sur la passerelle que H.323 utilisera.
- **H.323** — L'inspection H.323 fournit la prise en charge d'applications conformes H.323 telles que Cisco CallManager et VocalTec Gatekeeper. H.323 est une suite des protocoles définis par l'Union internationale des télécommunications pour des conférences multimédias par LAN. Le dispositif de sécurité prend en charge le H.323 via la version 4, qui inclut la fonctionnalité Multiple Calls on One Call Signaling Channel du H.323 v3.Lorsque l'inspection H.323 est activée, le dispositif de sécurité prend en charge plusieurs appels sur le même canal de signalisation d'appel, une fonctionnalité introduite avec le H.323 version 3. Cette fonctionnalité réduit la durée d'établissement de l'appel et réduit l'utilisation des ports sur le dispositif de sécurité.Voici les deux fonctions principales de l'inspection H.323 :Traduction d'adresses réseau (NAT) des adresses IPv4 incluses nécessaires dans les messages H.225 et H.245. Les messages H.323 étant encodés dans le format d'encodage PER, le dispositif de sécurité utilise un décodeur ASN.1 pour décoder les messages H.323.Allouer dynamiquement les connexions négociées H.245 et RTP/RTCP.
- **Skinny (ou Simple) Client Control Protocol (SCCP)** — SCCP est un protocole simplifié utilisé

dans des réseaux VoIP. Les téléphones IP Cisco qui utilisent le SCCP peuvent coexister dans un environnement H.323. S'il est utilisé avec Cisco CallManager, le client SCCP peut interopérer avec des terminaux conformes H.323. Les fonctions de couche applicative dans le dispositif de sécurité identifient le SCCP version 3.3. La fonctionnalité du logiciel de la couche applicative assure que toutes les signalisations SCCP et tous les paquets multimédias peuvent traverser le dispositif de sécurité en fournissant le NAT des paquets de signalisation SCCP.Il y a 5 versions du protocole SCCP : 2.4, 3.0.4, 3.1.1, 3.2 et 3.3.2. Le dispositif de sécurité prend en charge toutes les versions via la version 3.3.2. Le dispositif de sécurité fournit la prise en charge de PAT et de NAT pour le SCCP. Le PAT est nécessaire si vous avez des nombres limités d'adresses IP globales à utiliser par des téléphones IP.Le trafic normal entre Cisco CallManager et les téléphones IP Cisco utilise le SCCP et est géré par l'inspection SCCP sans configuration spéciale. Le dispositif de sécurité prend également en charge les options DHCP 150 et 66, qui lui permettent d'envoyer l'emplacement d'un serveur TFTP aux téléphones IP Cisco et à d'autres clients DHCP. Référez-vous à Configurer des services DHCP, DDNS et WCCP pour plus d'informations.

Conditions préalables

Conditions requises

Ce document suppose que la configuration VPN nécessaire est faite sur tous les périphériques et fonctionne correctement.

Reportez-vous à la section ASA/PIX : Exemple de configuration d'un dispositif de sécurité pour tunnel IPsec LAN-à-LAN de routeur IOS afin d'en savoir plus sur la configuration de VPN.

Référez-vous à PIX/ASA 7.x : Activer la communication entre interfaces pour plus d'informations sur la façon d'activer la communication entre interfaces.

Composants utilisés

Les informations de ce document sont basées sur le dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500 qui exécute le logiciel version 7.x.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec le pare-feu PIX de la gamme Cisco 500 qui exécute le logiciel version 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

SIP

L'inspection SIP traduit les adresses réseau des messages textuels SIP, recalcule la longueur du contenu pour la partie SDP du message, et recalcule la longueur du paquet et la somme de contrôle. Elle ouvre dynamiquement des connexions multimédias pour des ports spécifiés dans la partie SDP du message en tant qu'adresse/ports que le périphérique devrait écouter.

L'inspection SIP a une base de données avec des index CALL_ID/FROM/TO de la charge utile SIP qui identifie l'appel, ainsi que la source et la destination. Les adresses et ports multimédias contenus dans cette base de données étaient les contenus des champs d'information multimédia SDP et du type de média. Il peut y avoir plusieurs adresses et ports multimédias pour une session. Des connexions RTP/RTCP sont ouvertes entre les deux périphériques utilisant ces adresses/ports multimédias.

Le port 5060 bien connu doit être utilisé dans le message d'établissement de l'appel initial (INVITE). Cependant, les messages ultérieurs pourraient ne pas avoir ce numéro de port. Le moteur d'inspection SIP ouvre des œilletons de connexion de signalisation et marque ces connexions comme connexions SIP. Ceci est fait pour que les messages atteignent l'application SIP et pour que leurs adresses réseau soient traduites.

Lorsqu'un appel est configuré, la session SIP est considérée comme étant dans un état passager. Cet état demeure jusqu'à ce qu'une réponse soit reçue, indiquant l'adresse et le port multimédias RTP que le périphérique de destination écoute. S'il n'y a pas de message de réponse reçu dans un délai d'une minute, la connexion de signalisation est interrompue.

Une fois que l'établissement final de la liaison est fait, l'état de l'appel passe à actif et la connexion de signalisation reste jusqu'à ce qu'un message de fin (BYE) soit reçu.

Si un périphérique interne lance un appel à un périphérique externe, un passage multimédia est ouvert sur l'interface externe pour permettre aux paquets UDP RTP/RTCP d'atteindre l'adresse et le port multimédias du périphérique interne spécifiés dans le message INVITE du périphérique intérieur. Les paquets UDP RTP/RTCP non sollicités vers une interface interne ne traverseront pas le dispositif de sécurité, à moins que la configuration du dispositif de sécurité le permette spécifiquement.

Les connexions multimédias sont interrompues dans un délai de deux minutes après le début d'inactivité de la connexion. C'est un délai d'attente configurable et peut être paramétré pour un laps de temps plus court ou plus long.

MGCP

Afin d'utiliser MGCP, vous devez généralement configurer au moins deux commandes d'inspection : une pour le port sur lequel la passerelle reçoit des commandes et une pour le port sur lequel l'agent d'appel reçoit des commandes. Normalement, un agent d'appel envoie des commandes au port MGCP par défaut pour des passerelles, **2427**, et une passerelle envoie des commandes au port MGCP par défaut pour des agents d'appel, **2727**.

Les messages MGCP sont transmis via **UDP**. Une réponse est renvoyée à l'adresse source (adresse IP et numéro de port UDP) de la commande, mais la réponse peut ne pas arriver de la

même adresse que celle à partir de laquelle la commande a été envoyée. Ceci peut se produire quand plusieurs agents d'appel sont utilisés dans une configuration de basculement et que l'agent d'appel qui a reçu la commande a passé le contrôle à un agent d'appel de secours, qui envoie ensuite la réponse.

H.323

L'ensemble de protocoles H.323 peut collectivement utiliser jusqu'à deux connexions TCP et de quatre à six connexions UDP. FastConnect utilise seulement une connexion TCP, et le RAS (Reliability, Availability, and Serviceability) utilise une seule connexion UDP pour l'enregistrement, les admissions et l'état.

Un client H.323 client peut initialement établir une connexion TCP à un serveur H.323 en utilisant le port TCP 1720 pour demander l'établissement d'un appel Q.931. En tant qu'élément du processus d'établissement de l'appel, le terminal H.323 fournit un numéro de port au client pour l'utiliser pour une connexion TCP H.245. Dans les environnements où un contrôleur d'accès H.323 est en service, le paquet initial est transmis en utilisant UDP.

L'inspection H.323 surveille la connexion TCP Q.931 pour déterminer le numéro de port H.245. Si les terminaux H.323 n'utilisent pas FastConnect, le dispositif de sécurité alloue dynamiquement la connexion H.245 en se basant sur l'inspection des messages H.225.

Dans chaque message H.245, les périphériques H.323 échangent les numéros de port qui sont utilisés pour les flux de données UDP ultérieurs. L'inspection H.323 inspecte les messages H.245 pour identifier ces ports et crée dynamiquement des connexions pour l'échange multimédia. RTP utilise le numéro de port négocié, alors que RTCP utilise le numéro de port supérieur suivant.

Le canal de contrôle H.323 gère le H.225, le H.245 et le H.323 RAS. L'inspection H.323 utilise ces ports :

- 1718 — port UDP de découverte de contrôleur d'accès
- 1719 — port UDP RAS
- 1720 — port de contrôle TCP

Vous devez autoriser le trafic pour le port H.323 bien connu, 1720, pour la signalisation d'appel H.225. Cependant, les ports de la signalisation H.245 sont négociés entre les périphériques dans la signalisation H.225. Quand un contrôleur d'accès H.323 est utilisé, le dispositif de sécurité ouvre une connexion H.225 basée sur l'inspection du message de confirmation d'admission (ACF).

Une fois les messages H.225 inspectés, le dispositif de sécurité ouvre le canal H.245, puis inspecte le trafic envoyé via le canal H.245. Tous les messages qui passent par le dispositif de sécurité subissent l'inspection de l'application H.245 qui traduit les adresses IP incluses et ouvre les canaux multimédias négociés dans les messages H.245.

La norme H.323 ITU exige qu'un en-tête de paquet d'unité de données de protocole de transport (TPKT), qui définit la longueur du message, précède le H.225 et le H.245, avant d'être transmis à la connexion fiable. Puisque l'en-tête TPKT n'a pas besoin nécessairement d'être envoyé dans le même paquet TCP que les messages H.225 et H.245, le dispositif de sécurité doit se rappeler la longueur du TPKT pour traiter et décoder correctement le message. Pour chaque connexion, le dispositif de sécurité garde un enregistrement qui contient la longueur du TPKT pour le message attendu suivant.

Si le dispositif de sécurité doit exécuter le NAT sur des adresses IP dans des messages, il change la somme de contrôle, la longueur UUIE et le TPKT, s'il est inclus dans le paquet TCP avec le message H.225. Si le TPKT est envoyé dans un paquet TCP distinct, le dispositif de sécurité reçoit les accusés de réception (ACK) de ce TPKT et ajoute un nouveau TPKT au message H.245 avec la nouvelle longueur.

SCCP

Dans les topologies où Cisco CallManager est situé sur l'interface à sécurité plus élevée, en ce qui concerne les téléphones IP Cisco, si le NAT est nécessaire pour l'adresse IP de Cisco CallManager, le mappage doit être statique car un téléphone IP Cisco nécessite que l'adresse IP de Cisco CallManager soit spécifiée explicitement dans sa configuration. Une entrée d'identité statique permet au Cisco CallManager sur l'interface à sécurité plus élevée d'accepter les enregistrements venant de téléphones IP Cisco.

Les téléphones IP Cisco nécessitent l'accès à un serveur TFTP pour télécharger les informations de configuration dont ils ont besoin pour se connecter au serveur Cisco CallManager.

Quand les téléphones IP Cisco sont sur une interface à niveau de sécurité inférieur, comparée au serveur TFTP, vous devez employer une liste d'accès afin de vous connecter au serveur TFTP protégé sur le port UDP 69. Tandis que vous avez besoin d'une entrée statique pour le serveur TFTP, celle-ci n'a pas besoin d'être une entrée d'identité statique. Quand le NAT est utilisé, une entrée d'identité statique effectue le mappage sur la même adresse IP. Quand le PAT est utilisé, il effectue le mappage sur la même adresse IP et le même port.

Quand les téléphones IP Cisco sont sur une interface à sécurité plus élevée, comparée au serveur TFTP et au Cisco CallManager, aucune liste d'accès ou entrée statique n'est nécessaire pour permettre aux téléphones IP Cisco d'initier la connexion.

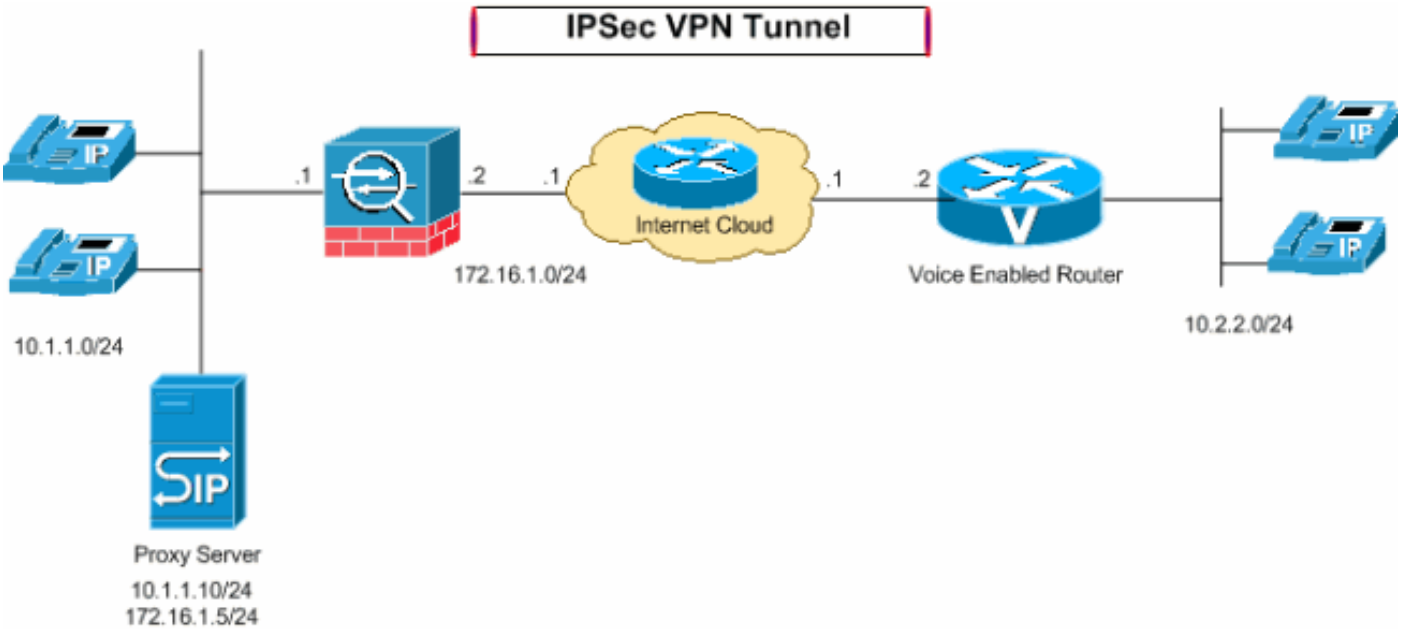
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Schéma de réseau pour SIP

Cette section utilise cette configuration du réseau :



Configurations pour SIP

Cette section utilise ces configurations :

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif. Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide. Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états. Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu. La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic.
- Appliquer des inspections au trafic.
- Activer des inspections sur une interface.

Configurer une inspection SIP de base

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la Stratégie d'inspection par défaut.

1. Émettez la commande **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Émettez la commande **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Émettez la commande **inspect sip**.`ASA5510(config-pmap-c)#inspect sip`

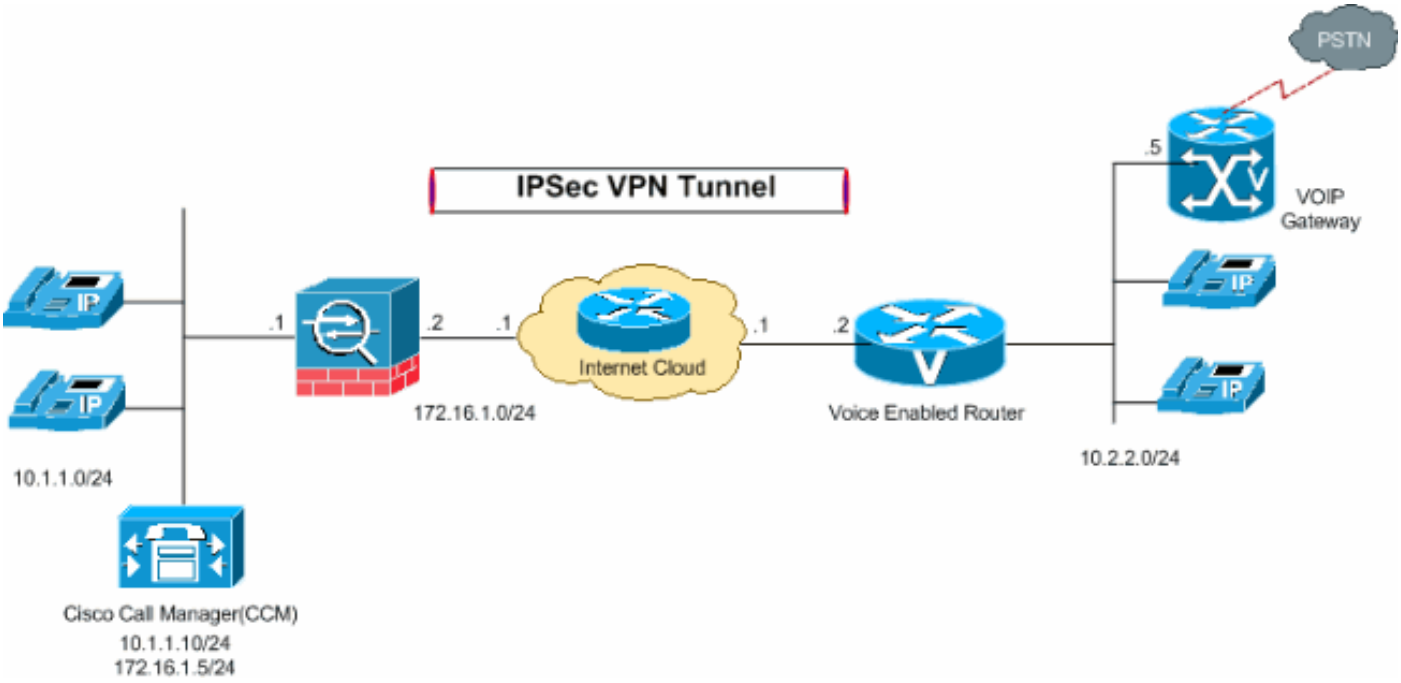
Configuration ASA pour SIP

`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#
```

Schéma de réseau pour MGCP, H.323 et SCCP

Cette section utilise cette configuration du réseau :



Configurations pour MGCP

Cette section utilise ces configurations :

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif. Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide. Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états. Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu. La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic.
- Appliquer des inspections au trafic.
- Activer des inspections sur une interface.

Configurer une inspection MGCP de base

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la Stratégie d'inspection par défaut.

1. Émettez la commande **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Émettez la commande **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Émettez la commande **inspect mgcp**.`ASA5510(config-pmap-c)#inspect mgcp`

Configurer une carte de stratégie d'inspection MGCP pour un contrôle d'inspection supplémentaire

Si le réseau dispose de plusieurs agents d'appel et de passerelles pour lesquelles le dispositif de sécurité a ouvert des œilletons, créez une carte MGCP. Vous pouvez ensuite appliquer la carte MGCP quand vous activez l'inspection MGCP. Référez-vous à Configuration de l'inspection d'applications pour plus d'informations.

```
!--- 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
```

Configuration ASA pour 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
```

Configurations pour H.323

Cette section utilise ces configurations :

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif. Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide. Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états. Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu. La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic.
- Appliquer des inspections au trafic.
- Activer des inspections sur une interface.

Configurer une inspection H.323 de base

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la Stratégie d'inspection par défaut.

1. Émettez la commande **policy-map global_policy**.`ASA5510(config)#policy-map global_policy`
2. Émettez la commande **class inspection_default**.`ASA5510(config-pmap)#class inspection_default`
3. Émettez la commande **inspect h323**.`ASA5510(config-pmap-c)#inspect h323 h225`
   `ASA5510(config-pmap-c)#inspect h323 ras`

Configuration ASA pour 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#
```

Configurations pour SCCP

Cette section utilise ces configurations :

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif. Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide. Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états. Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu. La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic.
- Appliquer des inspections au trafic.
- Activer des inspections sur une interface.

Configurer une inspection SCCP de base

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la Stratégie d'inspection par défaut.

1. Émettez la commande **policy-map global_policy**.`ASA5510(config)#`**`policy-map global_policy`**
2. Émettez la commande **class inspection_default**.`ASA5510(config-pmap)#`**`class inspection_default`**
3. Émettez la commande **inspect skinny**.`ASA5510(config-pmap-c)#`**`inspect skinny`**

Configuration ASA pour 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#
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

SIP :

Afin de s'assurer que la configuration a pris avec succès, utilisez la commande **show service-policy** et limitez la sortie à l'inspection SIP seulement en utilisant la commande **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
```

Dépannez

Problème

L'Office Communicator ne peut pas traverser l'ASA, l'iPhone enregistré au-dessus du tunnel VPN obtient déconnecté, ou il n'y a aucun audio sur des Téléphones IP à travers des tunnels VPN.

Solution

Office Communicator n'a pas de SIP standard, et par défaut, l'ASA l'abandonne. Désactivez les inspections SIP, Skinny et H323 afin de résoudre ce problème et utilisez également clear xlate et local-host dans l'ASA. La même solution s'applique pour l'IPhones aussi.

Problème

Les appels vidéos ont manqué avec le `%ASA-4-405102 : Incapable de préaffecter la connexion H245`

`pour le faddr XX.XX.XX.XX au` message d'erreur de `XX.XX.XX.XX/3239 de laddr.`

Solution

Désactivez l'inspection H323 afin de résoudre ce problème.

Informations connexes

- PIX/ASA 7.x : activer la communication entre interfaces
- Gestion du trafic VoIP avec le pare-feu PIX
- Utilisation des ports TCP et UDP avec Cisco Unified CallManager 5.0
- Assistance produit des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Assistance produit des dispositifs de sécurité de la gamme Cisco PIX 500
- Assistance technique le Media Gateway Control Protocol (MGCP)
- Assistance technique sur le Skinny Call Control Protocol (SCCP)
- Assistance technique sur le H.323
- Support et documentation techniques - Cisco Systems