Pare-feu basé sur la zone Cisco IOS : Site unique CME/CUE/GW ou filiale avec jonction SIP à CCM au siège

Contenu

Introduction

Les routeurs à services intégrés (ISR) de Cisco offrent une plate-forme évolutive qui répond aux besoins du réseau voix et données pour un large éventail d'applications. Bien que le paysage des menaces des réseaux privés et connectés à Internet soit un environnement très dynamique, le pare-feu Cisco IOS® offre des fonctionnalités d'inspection dynamique et d'inspection et de contrôle des applications (AIC) pour définir et appliquer une position réseau sécurisée, tout en

assurant la continuité et la capacité de l'entreprise.

Ce document décrit les considérations de conception et de configuration pour les aspects de sécurité du pare-feu de scénarios spécifiques d'applications vocales et de données basées sur Cisco ISR. Les configurations des services vocaux et du pare-feu sont fournies pour chaque scénario d'application. Chaque scénario décrit les configurations VoIP et de sécurité séparément, suivies de la configuration complète du routeur. Votre réseau peut nécessiter d'autres configurations pour les services, tels que la QoS et le VPN, afin de préserver la qualité et la confidentialité de la voix.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Informations générales

Arrière-plan du pare-feu IOS

Le pare-feu Cisco IOS est généralement déployé dans des scénarios d'applications qui diffèrent des modèles de déploiement des pare-feu d'appareils. Les déploiements typiques incluent les applications de télétravail, les sites de petites ou de filiales et les applications de vente au détail, où le nombre d'appareils est faible, l'intégration de plusieurs services, et où les performances et les capacités de sécurité sont réduites.

Bien que l'application de l'inspection par pare-feu, ainsi que d'autres services intégrés dans les produits ISR, puisse paraître attrayante du point de vue du coût et du fonctionnement, des considérations spécifiques doivent être évaluées pour déterminer si un pare-feu basé sur un routeur est approprié. L'application de chaque fonctionnalité supplémentaire entraîne des coûts de mémoire et de traitement et peut probablement contribuer à réduire le débit de transfert, à augmenter la latence des paquets et à réduire la capacité des fonctionnalités pendant les périodes de pointe si une solution intégrée sous-alimentée basée sur un routeur est déployée. Respectez ces consignes lorsque vous décidez entre un routeur et une appliance :

- Les routeurs dotés de plusieurs fonctionnalités intégrées sont les mieux adaptés aux sites de filiales ou de télétravailleurs où moins de périphériques offrent une meilleure solution.
- Les applications hautes performances à bande passante élevée sont généralement mieux gérées avec des appliances ; Cisco ASA et Cisco Unified Call Manager Server doivent être appliqués pour gérer la NAT et l'application de stratégie de sécurité et le traitement des

appels, tandis que les routeurs répondent aux besoins en termes d'application de stratégie QoS, de terminaison WAN et de connectivité VPN site à site.

Avant l'introduction de la version 12.4(20)T du logiciel Cisco IOS, les pare-feu classiques et les pare-feu ZFW (Zone-Based Policy Firewall) ne pouvaient pas prendre en charge intégralement les fonctionnalités requises pour le trafic VoIP et les services vocaux basés sur les routeurs, ce qui nécessitait de grandes lacunes dans les politiques de pare-feu par ailleurs sécurisées pour prendre en charge le trafic vocal, et offrait une prise en charge limitée pour les protocoles de signalisation VoIP et les protocoles de support évolutifs.

Déployer le pare-feu de stratégie basé sur les zones Cisco IOS

Le pare-feu Cisco IOS Zone-Based Policy Firewall, similaire aux autres pare-feu, ne peut offrir un pare-feu sécurisé que si les exigences de sécurité du réseau sont identifiées et décrites par la stratégie de sécurité. Il existe deux approches fondamentales pour élaborer une politique de sécurité : la perspective *de confiance*, par opposition à la perspective *suspecte*.

La perspective *de confiance* suppose que tout le trafic est fiable, sauf celui qui peut être spécifiquement identifié comme malveillant ou indésirable. Une politique spécifique est mise en oeuvre qui refuse uniquement le trafic indésirable. Cela se fait généralement au moyen d'entrées de contrôle d'accès spécifiques ou d'outils basés sur les signatures ou les comportements. Cette approche tend à interférer moins avec les applications existantes, mais nécessite une connaissance complète du paysage des menaces et des vulnérabilités et nécessite une vigilance constante pour faire face aux nouvelles menaces et aux nouvelles attaques à mesure qu'elles apparaissent. En outre, la communauté des utilisateurs doit jouer un rôle important dans le maintien d'une sécurité adéquate. Un environnement qui offre une liberté étendue et peu de contrôle aux occupants offre des possibilités substantielles de problèmes causés par des individus négligents ou malveillants. Un autre problème de cette approche est qu'elle repose davantage sur des outils de gestion et des contrôles d'application efficaces qui offrent une flexibilité et des performances suffisantes pour être en mesure de surveiller et de contrôler les données suspectes dans tout le trafic réseau. Bien que la technologie soit actuellement disponible pour y faire face, la charge opérationnelle dépasse souvent les limites de la plupart des organisations.

La perspective *suspecte* suppose que tout le trafic réseau est indésirable, sauf pour le *bon* trafic spécifiquement identifié. Il s'agit d'une stratégie appliquée, qui refuse tout trafic d'application, sauf ce qui est explicitement autorisé. En outre, l'inspection et le contrôle des applications (AIC) peuvent être mis en oeuvre pour identifier et refuser le trafic malveillant spécifiquement conçu pour exploiter de *bonnes* applications, ainsi que le trafic indésirable qui se déguise en *bon* trafic. Là encore, les contrôles d'application imposent des contraintes opérationnelles et de performances au réseau, bien que la plupart du trafic indésirable doive être contrôlé par des filtres sans état, tels que les listes de contrôle d'accès (ACL) ou la politique ZFW (Zone-Based Policy Firewall), de sorte qu'il y a beaucoup moins de trafic qui doit être géré par AIC, le système de prévention des intrusions (IPS) ou d'autres contrôles basés sur les signatures, tels que la technologie FPM (Flexible Packet NBAR) .. Si seuls les ports d'application souhaités (et le trafic spécifique au support dynamique provenant de connexions ou de sessions de contrôle connues) sont spécifiquement autorisés, le seul trafic indésirable présent sur le réseau doit tomber dans un sous-ensemble spécifique, plus facilement reconnu, ce qui réduit la charge d'ingénierie et d'exploitation imposée pour maintenir le contrôle du trafic indésirable.

Ce document décrit les configurations de sécurité VoIP basées sur la perspective *suspecte*, de sorte que seul le trafic autorisé dans les segments de réseau vocal est autorisé. Les politiques de données ont tendance à être plus permissives, comme l'indiquent les notes de configuration de chaque scénario d'application.

Tous les déploiements de stratégie de sécurité doivent suivre un cycle de rétroaction en boucle fermée ; les déploiements de sécurité affectent généralement les capacités et les fonctionnalités des applications existantes et doivent être ajustés pour minimiser ou résoudre cet impact.

Si vous avez besoin d'un arrière-plan supplémentaire pour configurer le pare-feu de stratégie basé sur les zones, consultez le Guide de conception et d'application du pare-feu de zone.

Considérations relatives au ZFW dans les environnements VoIP

Le Guide de conception et d'application du pare-feu de zone propose une brève discussion sur la sécurité des routeurs avec l'utilisation de stratégies de sécurité à destination et en provenance de la zone *autonome* du routeur, ainsi que d'autres fonctionnalités fournies par le biais de diverses fonctions NFP (Network Foundation Protection). Les fonctionnalités VoIP basées sur un routeur sont hébergées dans la zone *autonome* du routeur. Les politiques de sécurité qui protègent le routeur doivent donc être conscientes des exigences du trafic vocal afin de prendre en charge la signalisation vocale et les supports provenant et destinés aux ressources Cisco Unified CallManager Express, Survivable Remote-Site Telephony et Voice Gateway. Avant la version 12.4(20)T du logiciel Cisco IOS, le pare-feu classique et le pare-feu de stratégie basé sur les zones ne pouvaient pas répondre entièrement aux exigences du trafic VoIP, de sorte que les stratégies de pare-feu n'étaient pas optimisées pour protéger pleinement les ressources. Les politiques de sécurité de zone autonome qui protègent les ressources VoIP basées sur les routeurs reposent largement sur les fonctionnalités introduites dans la version 12.4(20)T.

Fonctionnalités vocales du pare-feu IOS

Le logiciel Cisco IOS Version 12.4(20)T a introduit plusieurs améliorations pour permettre les fonctionnalités vocales et de pare-feu de zone corésidents. Trois fonctions principales s'appliquent directement aux applications vocales sécurisées :

- Améliorations SIP : Contrôle et inspection des applications et de la passerelle de couche applicationMet à jour la prise en charge de la version SIP vers SIPv2, comme décrit dans la RFC 3261Étend la prise en charge de la signalisation SIP pour reconnaître une plus grande variété de flux d'appelsIntroduction de SIP Application Inspection and Control (AIC) pour appliquer des contrôles granulaires afin de traiter des vulnérabilités et des exploits spécifiques au niveau des applicationsÉtend l'inspection de zone autonome pour être en mesure de reconnaître les canaux de signalisation et de support secondaires qui résultent du trafic SIP destiné/originaire localement
- Prise en charge du trafic local Skinny et CMEMet à jour la prise en charge de SCCP vers la version 16 (version 9 précédemment prise en charge)Introduit l'inspection et le contrôle des applications (AIC) SCCP afin d'appliquer des contrôles granulaires pour traiter des vulnérabilités et des exploits spécifiques au niveau des applicationsÉtend l'inspection de zone autonome pour être en mesure de reconnaître les canaux de signalisation et de support secondaires qui résultent du trafic SCCP destiné/originaire localement
- Prise en charge H.323 pour les versions 3 et 4Met à jour la prise en charge de H.323 vers les versions 3 et 4 (versions 1 et 2 précédemment prises en charge)Introduit l'inspection et le contrôle des applications (AIC) H.323 pour appliquer des contrôles granulaires afin de traiter des vulnérabilités et des exploits spécifiques au niveau des applications

Les configurations de sécurité des routeurs décrites dans ce document incluent les fonctionnalités offertes par ces améliorations avec des explications pour décrire l'action appliquée par les politiques. Des liens hypertexte vers les documents de chaque fonction sont disponibles dans la

section Informations connexes de ce document si vous souhaitez consulter les détails complets des fonctions d'inspection vocale.

Cavates

Afin de renforcer les points mentionnés précédemment, l'application du pare-feu Cisco IOS Firewall avec des fonctionnalités vocales basées sur un routeur doit appliquer le pare-feu de stratégie basé sur une zone. Le pare-feu IOS classique n'inclut pas la capacité nécessaire pour prendre en charge pleinement la complexité de signalisation ou le comportement du trafic vocal.

Traduction d'adresses réseau (NAT)

La traduction d'adresses de réseau (NAT) Cisco IOS est fréquemment configurée simultanément avec le pare-feu Cisco IOS, en particulier dans les cas où les réseaux privés doivent interagir avec Internet ou si des réseaux privés disparates doivent se connecter, en particulier si l'espace d'adresses IP se chevauche. Le logiciel Cisco IOS inclut des passerelles de couche application NAT (ALG) pour SIP, Skinny et H.323. Idéalement, la connectivité réseau pour la voix IP peut être prise en charge sans application de la NAT, car la NAT introduit une complexité supplémentaire dans les applications de dépannage et de stratégie de sécurité, en particulier dans les cas où la surcharge de la NAT est utilisée. La fonction NAT ne peut être appliquée qu'en dernier recours pour répondre aux problèmes de connectivité réseau.

Client Cisco Unified Presence (CUPC)

Ce document ne décrit pas la configuration qui prend en charge l'utilisation de Cisco Unified Presence Client (CUPC) avec le pare-feu IOS, car CUPC n'est pas encore pris en charge par Zone ou Classic Firewall, depuis la version 12.4(20)T1 du logiciel Cisco IOS. CUPC sera pris en charge dans une prochaine version du logiciel Cisco IOS.

CME/CUE/GW Site unique ou succursale avec liaison SIP vers CCM au siège social ou chez le fournisseur de téléphonie

Ce scénario offre un compromis entre le modèle de traitement des appels à site unique/distribué/RTPC décrit précédemment dans ce document (CME/CUE/GW Single Site ou Branch Office qui se connecte au RTPC) et le réseau voix/données convergé multisite/centralisé défini dans le troisième scénario décrit dans ce document. Ce scénario utilise toujours Cisco Unified CallManager Express local, mais la numérotation longue distance et la téléphonie HQ/remote site sont hébergées principalement par des liaisons SIP site à site, avec numérotation locale et d'urgence via une connexion RTPC locale. Même dans les cas où la majorité des connexions RTPC héritées est supprimée, un niveau de capacité RTPC de base est recommandé pour prendre en charge les défaillances de la numérotation de contournement téléphonique WAN, ainsi que la numérotation locale, comme décrit par le plan de numérotation. En outre, les lois locales exigent généralement qu'une sorte de connectivité RTPC locale soit fournie pour prendre en charge la numérotation d'urgence (911). Ce scénario utilise le traitement distribué des appels, qui offre des avantages et respecte les meilleures pratiques décrites dans la solution Cisco Unified CallManager Express SRND.

Les entreprises peuvent mettre en oeuvre ce type de scénario d'application dans les circonstances suivantes :

- Des environnements VoIP distincts sont utilisés entre les sites, mais la VoIP est toujours souhaitée au lieu du RTPC longue distance.
- L'autonomie site par site est nécessaire pour l'administration du plan de numérotation.
- Une fonctionnalité complète de traitement des appels est nécessaire quelle que soit la disponibilité du WAN.

Arrière-plan du scénario

Le scénario d'application intègre des téléphones filaires (VLAN voix), des PC filaires (VLAN données) et des périphériques sans fil (qui incluent des périphériques VoIP, tels qu'IP Communicator).

La configuration de sécurité fournit les éléments suivants :

1. Inspection de signalisation initiée par le routeur entre CME et les téléphones locaux (SCCP et SIP) et CME et le cluster CUCM distant (SIP).
2. La voix-support identifie les trous de communication entre ceux-ci :Segments filaires et sans fil locauxCME et les téléphones locaux pour la musique d'attenteCUE et les téléphones locaux pour la messagerie vocaleTéléphones et entités d'appel distantes
3. Inspection et contrôle des applications (AIC), qui peuvent être appliqués pour atteindre ces objectifs :Nombre limite de messages d'invitationGarantir la conformité du protocole sur tout le trafic SIP

Avantages/inconvénients

Cette application permet de réduire les coûts, car elle transporte le trafic voix de site à site sur les liaisons de données WAN.

Un inconvénient de ce scénario est que des plans plus détaillés de connectivité WAN sont nécessaires. La qualité des appels de site à site peut être affectée par de nombreux facteurs sur le WAN, tels que le trafic illégitime/indésirable (vers, virus, partage de fichiers peer-to-peer) ou les problèmes de latence difficiles à identifier qui peuvent résulter de l'ingénierie du trafic sur les réseaux de l'opérateur. Les connexions WAN doivent être dimensionnées de manière appropriée pour offrir une bande passante suffisante pour le trafic voix et données ; Le trafic de données moins sensible à la latence, par exemple le trafic de messagerie électronique, de fichiers SMB/CIFS, peut être classé comme trafic de moindre priorité pour QoS afin de préserver la qualité de la voix.

Un autre problème lié à ce scénario est le manque de traitement centralisé des appels et les difficultés qui peuvent survenir lors du dépannage des échecs de traitement des appels. En tant que tel, ce scénario fonctionne le mieux pour les grandes entreprises en tant qu'étape intermédiaire dans une migration vers un traitement centralisé des appels. Les CME Cisco locaux peuvent être convertis pour jouer le rôle de secours SRST complet lorsque la migration vers Cisco CallManager est terminée.

Du point de vue de la sécurité, la complexité croissante de cet environnement rend la mise en oeuvre et le dépannage efficaces de la sécurité plus difficiles, car la connectivité sur un WAN, ou sur un VPN sur l'Internet public, augmente considérablement l'environnement de menace, particulièrement dans les cas où la politique de sécurité nécessite une perspective *de confiance*, où peu de restrictions sont imposées au trafic sur le WAN. Dans cet esprit, les exemples de

configuration fournis par ce document implémentent une stratégie plus *suspecte* qui autorise un trafic stratégique spécifique, qui est ensuite examiné par des contrôles de conformité de protocole. En outre, des actions VoIP spécifiques, à savoir SIP INVITE, sont limitées pour réduire la probabilité de dysfonctionnements logiciels malveillants ou non intentionnels qui ont un impact négatif sur les ressources VoIP et la convivialité.

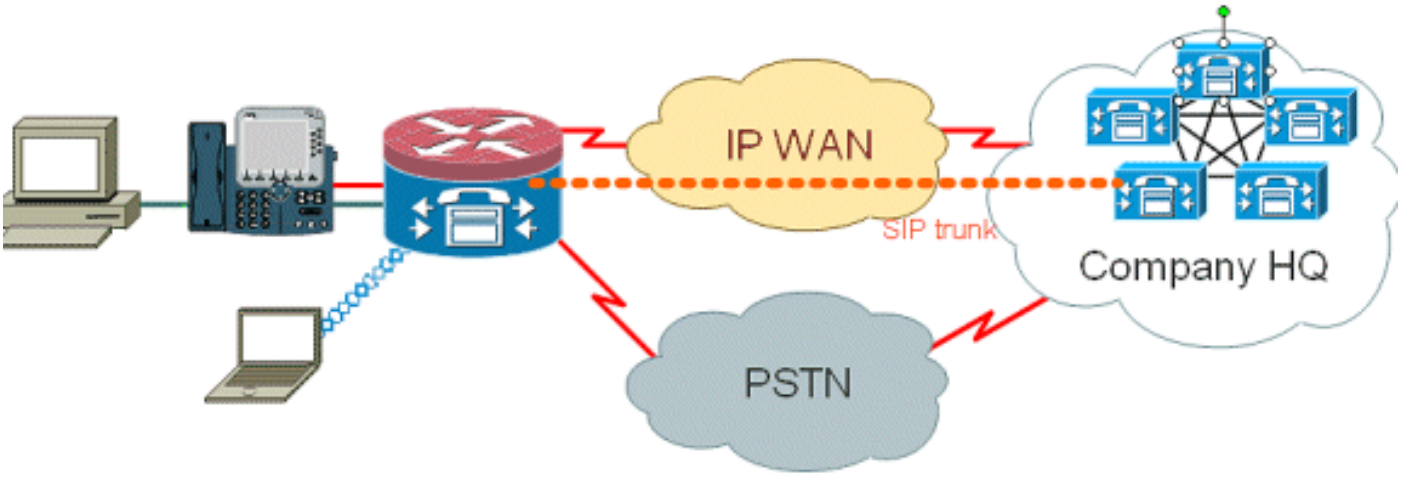
Configuration

Configurations pour les politiques de données, pare-feu basé sur une zone, sécurité vocale, CCME

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

La configuration décrite ici illustre un routeur à services intégrés Cisco 2851.

Ce document utilise les configurations suivantes :

- Configuration du service vocal pour la connectivité CME et CUE
- Configuration du pare-feu de stratégie basé sur les zones
- Configuration de la sécurité

Voici la configuration du service vocal pour la connectivité CME et CUE :

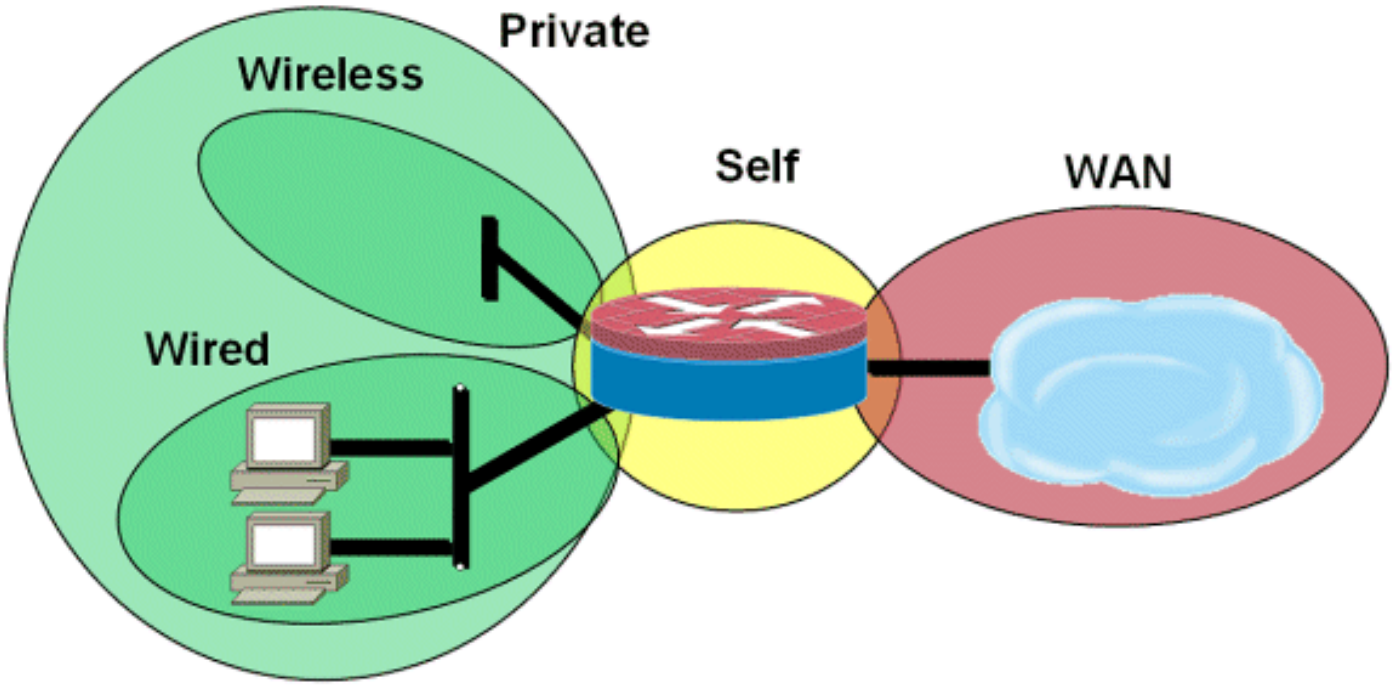
Configuration du service vocal pour la connectivité CME et CUE

```
!
telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
```

```
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp 7960 Jun 10 2008 15:47:13

!
```

Il s'agit de la configuration Zone-Based Policy Firewall, composée de zones de sécurité pour les segments LAN filaires et sans fil, de LAN privé (composé de segments filaires et sans fil), d'un segment WAN où la connectivité WAN fiable est atteinte et de la zone libre où se trouvent les ressources vocales du routeur :



Voici la configuration de sécurité :

Configuration de la sécurité

```
class-map type inspect match-all acl-cmap
match access-group 171
class-map type inspect match-any most-traffic-cmap
match protocol tcp
match protocol udp
match protocol icmp
match protocol ftp
!
!
policy-map type inspect most-traffic-pmap
class type inspect most-traffic-cmap
inspect
class class-default
drop
policy-map type inspect acl-pass-pmap
class type inspect acl-cmap
pass
 !
zone security private
zone security public
zone security wired
zone security wireless
!
```

```
zone-pair security priv-pub source private destination public
service-policy type inspect most-traffic-pmap
zone-pair security priv-vpn source private destination vpn
service-policy type inspect most-traffic-pmap
zone-pair security acctg-pub source acctg destination public
service-policy type inspect most-traffic-pmap
zone-pair security eng-pub source eng destination public
service-policy type inspect most-traffic-pmap
!
!
!
interface GigabitEthernet0/0
ip virtual-reassembly
zone-member security eng

Entire router configuration:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2851-cme2
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring

!
dot11 syslog
ip source-route

!
!
ip cef
no ip dhcp use vrf connected

!
ip dhcp pool pub-112-net
network 172.17.112.0 255.255.255.0
default-router 172.17.112.1
dns-server 172.16.1.22
option 150 ip 172.16.1.43
domain-name bldrtme.com

!

ip dhcp pool priv-112-net
network 192.168.112.0 255.255.255.0
default-router 192.168.112.1
dns-server 172.16.1.22
domain-name bldrtme.com
option 150 ip 192.168.112.1

!
!
ip domain name yourdomain.com

!
```

```
no ipv6 cef
multilink bundle-name authenticated

!
!
!
!

voice translation-rule 1
rule 1 // /1001/

!
!

voice translation-profile default
translate called 1

!
!

voice-card 0
no dspfarm

!
!
!
!
!

interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 172.16.112.10 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto

!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
 !
interface GigabitEthernet0/1.132
encapsulation dot1Q 132
ip address 172.17.112.1 255.255.255.0

!

interface GigabitEthernet0/1.152
encapsulation dot1Q 152
ip address 192.168.112.1 255.255.255.0
ip nat inside
ip virtual-reassembly

!

interface FastEthernet0/2/0

!

interface FastEthernet0/2/1

!
```

```
interface FastEthernet0/2/2

!

interface FastEthernet0/2/3

!

interface Vlan1
ip address 198.41.9.15 255.255.255.0

!

router eigrp 1
network 172.16.112.0 0.0.0.255
network 172.17.112.0 0.0.0.255
no auto-summary
!

ip forward-protocol nd
ip http server ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:/gui

 !!

ip nat inside source list 111 interface
GigabitEthernet0/0 overload

!

access-list 23 permit 10.10.10.0 0.0.0.7
access-list 111 deny
ip 192.168.112.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.112.0 0.0.0.255 any

!
!
!
!
!
!tftp-server flash:/phone/7940-7960/
P00308000400.bin alias P00308000400.bin
tftp-server flash:/phone/7940-7960/
P00308000400.loads alias P00308000400.loads
tftp-server flash:/phone/7940-7960/
P00308000400.sb2 alias P00308000400.sb2
tftp-server flash:/phone/7940-7960/
P00308000400.sbn alias P00308000400.sbn

!

control-plane

!
!
!

voice-port 0/0/0
connection plar 3035452366
description 303-545-2366
```

```
caller-id enable

!

voice-port 0/0/1 description FXO

!

voice-port 0/1/0
description FXS

!

voice-port 0/1/1 description FXS


!
!
!
!
!
dial-peer voice 804 voip
destination-pattern 5251...
session target ipv4:172.16.111.10
!
dial-peer voice 50 pots
destination-pattern A0
port 0/0/0
no sip-register

!
!
!
!

telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp
7960 Jun 10 2008 15:47:13

 !!

ephone-dn 1
number 1001
trunk A0

!
!

ephone-dn 2
number 1002

!
!
ephone-dn 3
number 3035452366
label 2366
trunk A0
```

```
!
!

ephone 1
device-security-mode none
mac-address 0003.6BC9.7737
type 7960
button 1:1 2:2 3:3

!
!
!

ephone 2
device-security-mode none
mac-address 0003.6BC9.80CE
type 7960
button 1:2 2:1 3:3

!
!
!

ephone 5
device-security-mode none

!
!
!

line con 0
exec-timeout 0 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh

line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh

!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp server 172.16.1.1
end
```

Provisionnement, gestion et surveillance

La configuration et la mise en service des ressources de téléphonie IP basées sur les routeurs et du pare-feu de stratégie basé sur les zones sont généralement mieux adaptées à Cisco Configuration Professional. Cisco Secure Manager ne prend pas en charge le pare-feu Zone-Based Policy ni la téléphonie IP basée sur routeur.

Le pare-feu classique Cisco IOS prend en charge la surveillance SNMP avec la MIB de pare-feu

unifié Cisco, mais le pare-feu de stratégie basé sur les zones n'est pas encore pris en charge dans la MIB de pare-feu unifié. En tant que tel, la surveillance du pare-feu doit être gérée à l'aide de statistiques sur l'interface de ligne de commande du routeur ou d'outils d'interface utilisateur graphique, tels que Cisco Configuration Professional.

Cisco Secure Monitoring And Reporting System (CS-MARS) offre une prise en charge de base du pare-feu de stratégie basé sur les zones, bien que les modifications de journalisation qui améliorent la corrélation des messages de journal avec le trafic, mises en oeuvre dans les versions 12.4(15)T4/T5 et 12.4(20)T, n'aient pas encore été entièrement prises en charge dans CS-MARS.

Plans de capacité

Les résultats des tests de performance d'inspection des appels de pare-feu en Inde sont à déterminer.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cisco IOS Zone Firewall fournit des commandes **show** et **debug** pour afficher, surveiller et dépanner l'activité du pare-feu. Cette section décrit l'utilisation des commandes **show** pour surveiller l'activité de base du pare-feu et une introduction aux commandes **debug** du pare-feu Zone pour dépanner votre configuration ou si la discussion avec le support technique nécessite des informations plus détaillées.

Dépannage des commandes

Le pare-feu Cisco IOS Firewall propose plusieurs commandes **show** pour afficher la configuration et l'activité des stratégies de sécurité. Beaucoup de ces commandes peuvent être remplacées par une commande plus courte via l'application de la commande **alias**.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Les commandes de débogage peuvent être utiles si vous utilisez une configuration atypique ou non prise en charge et que vous devez travailler avec le centre d'assistance technique de Cisco ou les services d'assistance technique d'autres produits pour résoudre les problèmes d'interopérabilité.

Remarque : L'application des commandes **debug** à des fonctionnalités ou un trafic spécifiques peut provoquer un très grand nombre de messages de console, ce qui fait que la console du routeur ne répond plus. Dans le même que vous devez déboguer, vous pouvez fournir un autre accès à l'interface de ligne de commande, par exemple une fenêtre Telnet qui ne surveille pas la boîte de dialogue de terminal. Activez uniquement le débogage sur un équipement hors ligne (environnement de laboratoire) ou dans une fenêtre de maintenance planifiée, car le débogage peut affecter considérablement les performances du routeur.

Informations connexes

- Guide de conception du réseau de référence de la solution Cisco Unified CallManager Express
- Meilleures pratiques de sécurité Cisco CallManager Express (CME SRND)
- Intégration de Cisco Unity Connection à Cisco Unified CME-as-SRST
- Référence des commandes de Cisco Unified Communications Manager Express
- Exemple de configuration de Cisco CallManager Express/Cisco Unity Express
- Prise en charge de la MIB SNMP de Cisco CallManager Express 3.4
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Pare-feu Cisco IOS : Améliorations SIP : ALG et AIC
- Logiciel Cisco IOS Firewall H.323
- Prise en charge du pare-feu Cisco IOS pour le trafic local maigre et CME
- Support et documentation techniques - Cisco Systems