Pare-feu basé sur la zone IOS : Exemple de configuration de site unique CME/CUE/GW ou connexion PSTN de filiale

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 Firewall 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 permettant 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. La configuration des services vocaux et du pare-feu est fournie 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 des services tels que QoS et 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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Arrière-plan du pare-feu IOS

Le pare-feu Cisco IOS est généralement déployé dans des scénarios d'application qui diffèrent des modèles de déploiement des pare-feu des appliances. 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 afin de 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 contribuera probablement 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.

Suivez les instructions ci-dessous 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 adaptées aux appareils : 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, le pare-feu classique et le pare-feu ZFW (Zone-Based Policy Firewall) n'étaient pas en mesure de prendre pleinement en charge les fonctionnalités requises pour le trafic VoIP et les services vocaux basés sur les routeurs, nécessitant de grandes ouvertures dans des politiques de pare-feu par ailleurs sécurisées pour prendre en charge le trafic voix, et offrant une prise en charge limitée pour la signalisation VoIP et

les protocoles de signalisation et les protocoles multimédias évolutifs.

Déploiement de Cisco IOS Zone-Based Policy Firewall

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 elle nécessite une connaissance approfondie 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 d'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. Stratégie appliquée qui refuse tout le trafic d'application, à l'exception de celle explicitement autorisée. 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 les applications « bonnes », ainsi que le trafic indésirable qui se déguise en trafic bon. 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 doit y avoir 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). Ainsi, 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 qui doit être 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* ; ainsi, seul le trafic autorisé dans les segments de réseau vocal est autorisé. Les politiques de données ont tendance à être plus permissives, comme le décrivent 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.

Pour plus d'informations sur la configuration du pare-feu de stratégie basé sur les zones, reportez-vous au Guide de conception et d'application du pare-feu basé sur les zones de Cisco IOS

Firewall.

Considérations relatives au ZFW dans les environnements VoIP

Le Guide de conception et d'application de Cisco IOS Firewall Zone-Based Policy Firewall propose une brève discussion sur la sécurisation du routeur avec l'utilisation de stratégies de sécurité à destination et en provenance de la zone *libre du* routeur, ainsi que d'autres fonctionnalités fournies par le biais de diverses fonctionnalités de Network Foundation Protection (NFP). Les fonctionnalités VoIP basées sur le routeur sont hébergées dans la zone autonome du routeur. Par conséquent, les politiques de sécurité qui protègent le routeur doivent tenir compte 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 politiques 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.

Améliorations vocales du pare-feu IOS - 12.4(20)T

La version 12.4(20)T du logiciel Cisco IOS a introduit plusieurs améliorations pour activer le pare-feu de zone co-résident et les fonctionnalités vocales. 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 résultant 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 applicationsDéveloppe l'inspection de zone autonome pour être en mesure de reconnaître les canaux de signalisation et de média secondaires résultant du trafic SCCP destiné/originaire localement
- Support H.323 v3/v4Met à jour la prise en charge H.323 vers v3 et v4 (précédemment pris en charge v1 et v2)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 une explication pour décrire l'action appliquée par les politiques. Pour plus de détails sur les fonctions d'inspection vocale, reportez-vous aux documents de fonction individuels répertoriés dans la section Informations connexes de ce document.

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 et le comportement du trafic vocal.

Traduction d'adresses réseau

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 est utilisé. 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 l'application de 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 NAT est utilisée. La fonction NAT ne doit être appliquée qu'en dernier cas pour répondre aux problèmes de connectivité réseau.

Client Cisco Unified Presence

Ce document ne décrit pas les configurations qui prennent 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 à partir de 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 Connexion PSTN site unique ou filiale

Ce scénario introduit la téléphonie VoIP basée sur un routeur sécurisé pour les petites et moyennes entreprises à site unique ou pour les grandes organisations multisites souhaitant déployer un traitement distribué des appels, en conservant les anciennes connexions au réseau téléphonique public commuté (RTPC). Le contrôle des appels VoIP est pris en charge par l'application d'un Cisco Unified Call Manager Express.

La connectivité RTPC peut être maintenue à long terme ou peut être migrée vers un réseau étendu IP voix et données convergé, comme décrit dans l'exemple d'application présenté dans la section CME/CUE/GW Single Site ou Branch Office with SIP Trunk to CCM at HQ ou Voice Provider de ce document.

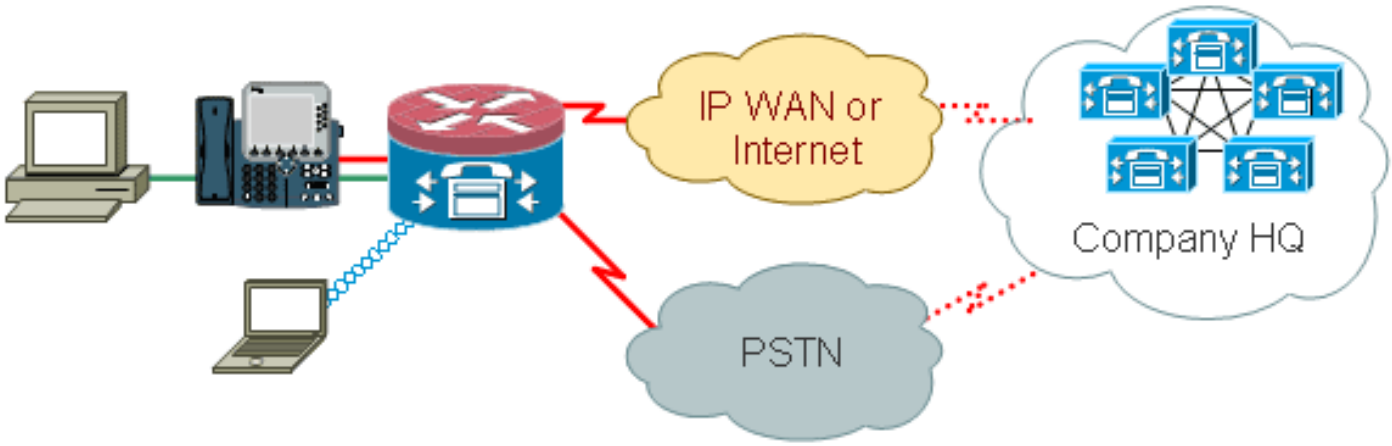
Les entreprises devraient envisager de mettre en oeuvre ce type de scénario d'application dans les cas où des environnements VoIP disparates sont utilisés entre des sites ou si la VoIP est impossible en raison d'une connectivité de données WAN inadéquate ou de restrictions spécifiques aux paramètres régionaux sur l'utilisation de la VoIP sur les réseaux de données. Les avantages et les meilleures pratiques de la téléphonie IP sur un site unique sont décrits dans Cisco Unified CallManager Express SRND.

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 offre :

- Inspection de signalisation initiée par le routeur entre CME et les téléphones locaux (SCCP et/ou SIP)
- Les supports vocaux permettent de détecter les trous de communication entre :Segments filaires et sans fil locauxCME et les téléphones locaux pour la musique d'attenteCUE et les téléphones locaux pour la messagerie vocale
- Appliquer l'inspection et le contrôle des applications (AIC) à :Nombre limite de messages d'invitationGarantir la conformité du protocole sur tout le trafic SIP.



Avantages et inconvénients

L'avantage le plus évident de l'aspect VoIP du scénario est le chemin de migration offert par l'intégration de l'infrastructure de réseau voix et données existante dans un environnement POTS/TDM existant, avant de passer à un réseau voix/données convergé pour les services de téléphonie au monde au-delà du LAN. Les numéros de téléphone sont conservés pour les petites entreprises et les services Centrex ou DID existants peuvent être laissés en place pour les grandes entreprises qui souhaitent une migration intermédiaire vers la téléphonie par paquets de contournement.

Parmi les inconvénients, citons la perte des économies que pourrait réaliser le contournement des interruptions de service en passant à un réseau voix/données convergent, ainsi que les limitations de la flexibilité des appels et le manque d'intégration et de portabilité des communications à l'échelle de l'entreprise qui pourraient être réalisées avec un réseau voix/données entièrement convergé.

Du point de vue de la sécurité, ce type d'environnement réseau réduit les menaces de sécurité VoIP, en évitant l'exposition des ressources VoIP au réseau public ou au WAN. Cependant, Cisco Call Manager Express intégré au routeur reste vulnérable aux menaces internes telles que le trafic malveillant ou le trafic d'applications défaillant. Ainsi, une politique est mise en oeuvre qui autorise le trafic spécifique à la voix qui répond aux contrôles de conformité du protocole, et des actions VoIP spécifiques (i.e. SIP INVITE) sont limitées de manière à réduire la probabilité de dysfonctionnements logiciels malveillants ou non intentionnels affectant négativement les ressources VoIP et la convivialité.

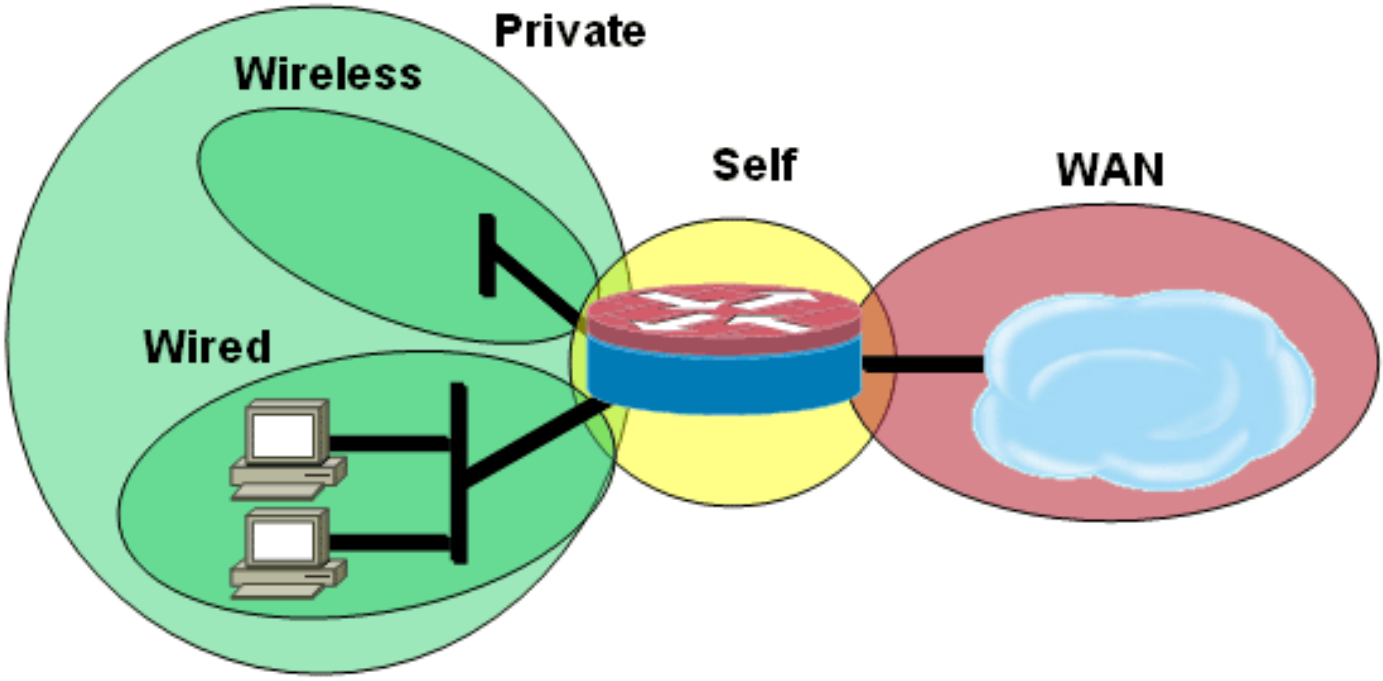
Politiques de données, pare-feu basé sur les zones, sécurité vocale et configurations CCME

La configuration décrite ici illustre un 2851 avec une configuration de 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
!
```

Configuration du pare-feu de stratégie basée sur une zone, 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 public où la connectivité Internet non fiable est atteinte et de la zone libre où se trouvent les ressources vocales du routeur.



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
```

Configuration complète du routeur

```
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
!
ntp server 172.16.1.1
end
```

Provisionnement, gestion et surveillance

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

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

CiscoSecure 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 mis 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.

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 présente les commandes **de débogage** du pare-feu de zone qui fournissent des informations de dépannage détaillées.

Commandes de débogage

Les commandes de débogage sont 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 cas que vous devez activer le débogage, vous pouvez fournir un accès alternatif à l'interface de ligne de commande, tel qu'une fenêtre telnet qui ne surveille pas la boîte de dialogue de terminal. Vous devez uniquement activer le débogage sur un équipement hors ligne (environnement de travaux pratiques) ou pendant une fenêtre de maintenance planifiée, car l'activation du débogage peut affecter considérablement les performances du routeur.

Informations connexes

- Guide de conception du réseau de référence de la solution Cisco Unified CallManager Express
- 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
- Support et documentation techniques - Cisco Systems