Cisco IOS Zone-basierte Firewall: CME/CUE/GW Ein Standort oder Zweigstelle mit SIP-Trunk zu CCM im Hauptsitz

Inhalt

Einführung

Die Cisco Integrated Service Router (ISRs) bieten eine skalierbare Plattform für die Erfüllung der Anforderungen von Daten- und Sprachnetzwerken für eine Vielzahl von Anwendungen. Obwohl die Bedrohungslandschaft von privaten und mit dem Internet verbundenen Netzwerken sehr dynamisch ist, bietet die Cisco IOS® Firewall Funktionen für Stateful Inspection und Application Inspection and Control (AIC), um einen sicheren Netzwerkstatus zu definieren und durchzusetzen, während sie Geschäftsfunktionen und Kontinuität ermöglicht.

In diesem Dokument werden Design- und Konfigurationserwägungen für Firewall-Sicherheitsaspekte bestimmter Cisco ISR-basierter Daten- und Sprachanwendungen beschrieben. Die Konfigurationen für Sprachdienste und die Firewall werden für jedes Anwendungsszenario bereitgestellt. Jedes Szenario beschreibt die VoIP- und Sicherheitskonfigurationen separat, gefolgt von der gesamten Router-Konfiguration. Ihr Netzwerk kann möglicherweise eine andere Konfiguration für Services wie QoS und VPN erfordern, um die Sprachqualität und Vertraulichkeit aufrechtzuerhalten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

IOS-Firewall-Hintergrund

Die Cisco IOS Firewall wird in der Regel in Anwendungsszenarien bereitgestellt, die sich von den Bereitstellungsmodellen der Appliance-Firewalls unterscheiden. Typische Bereitstellungen sind Telearbeiter-Anwendungen, Anwendungen für kleine oder Zweigstellen sowie Anwendungen für den Einzelhandel, bei denen eine niedrige Geräteanzahl, die Integration mehrerer Services sowie eine geringere Leistung und Sicherheit gewünscht sind.

Während die Anwendung von Firewall-Inspektionen zusammen mit anderen integrierten Services in den ISR-Produkten aus Kosten- und betrieblicher Sicht attraktiv erscheinen kann, müssen spezifische Überlegungen angestellt werden, um festzustellen, ob eine Router-basierte Firewall geeignet ist. Die Anwendung jeder zusätzlichen Funktion verursacht Speicher- und Verarbeitungskosten und kann wahrscheinlich zu geringeren Weiterleitungsdurchsätzen, einer höheren Paketlatenz und Funktionsverlusten während Spitzenlastzeiten beitragen, wenn eine nicht ausgelastete integrierte Router-basierte Lösung bereitgestellt wird. Beachten Sie bei der Entscheidung zwischen einem Router und einer Appliance die folgenden Richtlinien:

- Router mit mehreren integrierten Funktionen eignen sich am besten für Zweigstellen- oder Telearbeiter-Standorte, bei denen weniger Geräte eine bessere Lösung bieten.
- Hochleistungsanwendungen mit hoher Bandbreite werden in der Regel besser mit Appliances adressiert. Die Cisco ASA und der Cisco Unified Call Manager-Server müssen für die Anwendung von NAT- und Sicherheitsrichtlinien und die Anrufverarbeitung verwendet werden, während die Router die Anforderungen an QoS-Richtlinienanwendung, WAN-Terminierung

und Site-to-Site-VPN-Verbindungen erfüllen.

Vor der Einführung der Cisco IOS Software, Version 12.4(20)T, waren die klassische Firewall und die zonenbasierte Policy Firewall (ZFW) nicht in der Lage, die für VoIP-Datenverkehr und routerbasierte Sprachdienste erforderlichen Funktionen vollständig zu unterstützen. Dies erforderte große Lücken in ansonsten sicheren Firewall-Richtlinien, um Sprachdatenverkehr zu ermöglichen, und bot nur begrenzte Unterstützung für die Entwicklung von VoIP-Signalisierungs- und Medienprotokollen.

Bereitstellung einer zonenbasierten Cisco IOS Firewall für Richtlinien

Cisco IOS Zone-Based Policy Firewall kann, ähnlich wie andere Firewalls, nur dann eine sichere Firewall bereitstellen, wenn die Sicherheitsanforderungen des Netzwerks durch Sicherheitsrichtlinien identifiziert und beschrieben werden. Es gibt zwei grundlegende Ansätze für eine Sicherheitsrichtlinie: die *vertrauensvolle* Perspektive, im Gegensatz zur *verdächtigen* Perspektive.

Die *vertrauensvolle* Perspektive setzt voraus, dass der gesamte Datenverkehr vertrauenswürdig ist, mit Ausnahme des Datenverkehrs, der als schädlich oder unerwünscht identifiziert werden kann. Es wird eine spezifische Richtlinie implementiert, die nur den unerwünschten Datenverkehr blockiert. Dies wird in der Regel mithilfe spezifischer Zugriffskontrolleinträge oder signatur- oder verhaltensbasierter Tools erreicht. Dieser Ansatz stört in der Regel weniger vorhandene Anwendungen, erfordert jedoch ein umfassendes Verständnis der Bedrohungs- und Schwachstellenlandschaft und erfordert ständige Wachsamkeit bei der Bekämpfung neuer Bedrohungen und Exploits, sobald diese auftreten. Darüber hinaus muss die Benutzer-Community eine große Rolle bei der Aufrechterhaltung angemessener Sicherheit spielen. Eine Umgebung, die weit reichende Freiheit und wenig Kontrolle für die Bewohner ermöglicht, bietet erhebliche Möglichkeiten für Probleme, die durch unvorsichtige oder böswillige Personen verursacht werden. Ein weiteres Problem dieses Ansatzes besteht darin, dass er wesentlich stärker auf effektive Verwaltungstools und Anwendungskontrollen angewiesen ist, die genügend Flexibilität und Leistung bieten, um verdächtige Daten im gesamten Netzwerkverkehr überwachen und kontrollieren zu können. Technologie ist zwar derzeit verfügbar, um diesem Problem zu begegnen, der betriebliche Aufwand übersteigt jedoch häufig die Grenzen der meisten Unternehmen.

Die *verdächtige* Perspektive geht davon aus, dass der gesamte Netzwerkverkehr unerwünscht ist, mit Ausnahme des speziell identifizierten *guten* Datenverkehrs. Es handelt sich um eine Richtlinie, die angewendet wird, die den gesamten Anwendungsdatenverkehr blockiert, mit Ausnahme der explizit zulässigen Richtlinien. Zusätzlich kann die Anwendungsinspektion und -kontrolle implementiert werden, um schädlichen Datenverkehr zu identifizieren und zu verweigern, der speziell für die Nutzung *guter* Anwendungen entwickelt wurde, sowie unerwünschten Datenverkehr, der als *guter* Datenverkehr getarnt ist. Auch hier verursachen Anwendungskontrollen betriebliche und leistungsbedingte Belastungen des Netzwerks, obwohl der größte Teil des unerwünschten Datenverkehrs durch Stateless-Filter gesteuert werden muss, wie z. B. Zugriffskontrolllisten (ACLs) oder ZFW-Richtlinien (Zone-Based Policy Firewall). Auf diese Weise muss wesentlich weniger Datenverkehr über AIC, ein Intrusion Prevention System (IPS) oder andere signaturbasierte Kontrollen wie flexibler Paketabgleich (FPM) oder netzwerkbasierte Anwendungserkennung (Network-Erkennung) abgewickelt werden. NBAR). Wenn nur gewünschte Anwendungsports (und dynamischer medienspezifischer Datenverkehr, der aus bekannten Steuerungsverbindungen oder Sitzungen entsteht) ausdrücklich zugelassen sind, muss der einzige unerwünschte Datenverkehr, der im Netzwerk vorhanden ist, in eine bestimmte, leichter erkennbare Teilmenge fallen, wodurch der technische und betriebliche Aufwand für die Aufrechterhaltung der Kontrolle über unerwünschten Datenverkehr verringert wird.

In diesem Dokument werden VoIP-Sicherheitskonfigurationen basierend auf dem *verdächtigen* Aspekt beschrieben, sodass nur der in den Sprachnetzwerksegmenten zulässige Datenverkehr zulässig ist. Datenrichtlinien sind tendenziell permissiver, wie in den Notizen in der Konfiguration der einzelnen Anwendungsszenarien beschrieben.

Bei allen Bereitstellungen von Sicherheitsrichtlinien muss ein Kreislauf-Feedback-Zyklus eingehalten werden. Sicherheitsbereitstellungen wirken sich in der Regel auf die Funktionen und Funktionen vorhandener Anwendungen aus und müssen angepasst werden, um diese Auswirkungen zu minimieren oder zu beheben.

Wenn Sie zusätzliche Hintergrundinformationen zum Konfigurieren der zonenbasierten Firewall benötigen, lesen Sie den Leitfaden zum Design und zur Anwendung der Zonenfirewall.

Überlegungen zur ZFW in VoIP-Umgebungen

Der Design- und Anwendungshandbuch für Zonenfirewall bietet eine kurze Erläuterung der Router-Sicherheit durch die Verwendung von Sicherheitsrichtlinien für die *Selbstzone* des Routers sowie alternativer Funktionen, die über verschiedene NFP-Funktionen (Network Foundation Protection) bereitgestellt werden. Router-basierte VoIP-Funktionen werden in der *Self*-Zone des Routers gehostet. Sicherheitsrichtlinien, die den Router schützen, müssen die Anforderungen für Sprachdatenverkehr berücksichtigen, um die Sprachsignalisierung und die Medien zu integrieren, die von Cisco Unified CallManager Express, Survivable Remote Site Telefony und Voice Gateway-Ressourcen stammen und für diese bestimmt sind. Vor der Cisco IOS Software-Version 12.4(20)T waren die klassische Firewall und die zonenbasierte Firewall nicht in der Lage, die Anforderungen des VoIP-Datenverkehrs vollständig zu erfüllen. Daher wurden Firewall-Richtlinien nicht optimiert, um Ressourcen vollständig zu schützen. Sicherheitsrichtlinien für die Selbstzone, die routerbasierte VoIP-Ressourcen schützen, basieren in hohem Maße auf den in 12.4(20)T eingeführten Funktionen.

IOS Firewall-Sprachfunktionen

In der Cisco IOS Software, Version 12.4(20)T, wurden verschiedene Verbesserungen eingeführt, um gleichzeitig vorhandene Zone-Firewall- und Sprachfunktionen zu ermöglichen. Drei Hauptfunktionen gelten direkt für sichere Sprachanwendungen:

- SIP-Erweiterungen: Gateway und Anwendungsinspektion und -kontrolle auf AnwendungsebeneAktualisierungen der SIP-Versionsunterstützung für SIPv2, wie in RFC 3261 beschriebenUnterstützung für SIP-Signalisierung zur Erkennung einer größeren Vielfalt von AnrufströmenEinführung von SIP Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf AnwendungsebeneErweiterung der Selbstzonenprüfung, um sekundäre Signalisierungs- und Medienkanäle erkennen zu können, die aus lokal bestimmtem/vom SIP-Datenverkehr stammen
- Unterstützung für lokalen Skinny-Datenverkehr und CMEAktualisiert SCCP-Unterstützung auf Version 16 (zuvor unterstützte Version 9)Einführung von SCCP Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf AnwendungsebeneErweiterung der Selbstzonenprüfung, um sekundäre Signalisierungs- und Medienkanäle erkennen zu können, die aus lokal bestimmtem SCCP-Datenverkehr mit Ursprung in der Region stammen
- H.323-Unterstützung für die Versionen 3 und 4Aktualisierung der H.323-Unterstützung für die

Versionen 3 und 4 (zuvor unterstützte Versionen 1 und 2)Einführung von H.323 Application Inspection and Control (AIC) zur Anwendung präziser Kontrollen zur Behebung spezifischer Schwachstellen und Exploits auf Anwendungsebene

Die in diesem Dokument beschriebenen Router-Sicherheitskonfigurationen umfassen Funktionen dieser Erweiterungen sowie Erklärungen zur Beschreibung der von den Richtlinien angewendeten Aktion. Hyperlinks zu den einzelnen Funktionsdokumenten finden Sie im Abschnitt Zugehörige Informationen dieses Dokuments, wenn Sie die vollständigen Details zu den Sprachprüfungsfunktionen überprüfen möchten.

Hinweise

Um die oben genannten Punkte zu untermauern, muss die Anwendung der Cisco IOS Firewall mit routerbasierten Sprachfunktionen die zonenbasierte Firewall anwenden. Die klassische IOS-Firewall bietet nicht die erforderlichen Funktionen zur vollständigen Unterstützung der komplexen Signalisierung oder des Verhaltens von Sprachdatenverkehr.

Network Address Translation (NAT)

Die Cisco IOS Network Address Translation (NAT) wird häufig gleichzeitig mit der Cisco IOS Firewall konfiguriert, insbesondere in Fällen, in denen private Netzwerke eine Verbindung mit dem Internet herstellen müssen oder in denen unterschiedliche private Netzwerke eine Verbindung herstellen müssen, insbesondere wenn sich der IP-Adressbereich überschneidet. Die Cisco IOS Software umfasst NAT-Application-Layer-Gateways (ALGs) für SIP, Skinny und H.323. Im Idealfall können Netzwerkverbindungen für IP-Sprachverbindungen ohne Anwendung von NAT eingerichtet werden, da NAT die Fehlerbehebung und Sicherheitsrichtlinienanwendungen zusätzlich vereinfacht, insbesondere bei Verwendung von NAT-Überlastung. NAT kann nur als Einzelfall-Lösung angewendet werden, um Bedenken hinsichtlich der Netzwerkverbindungen auszuräumen.

Cisco Unified Presence Client (CUPC)

In diesem Dokument wird keine Konfiguration beschrieben, die die Verwendung von Cisco Unified Presence Client (CUPC) mit der IOS-Firewall unterstützt, da CUPC von der Zone oder der klassischen Firewall (ab der Cisco IOS-Softwareversion 12.4(20)T1 noch nicht unterstützt wird. CUPC wird in einer zukünftigen Version der Cisco IOS-Software unterstützt.

CME/CUE/GW Einzel- oder Zweigstelle mit SIP-Trunk zu CCM im Hauptsitz oder Sprachdienstleister

Dieses Szenario bietet einen Kompromiss zwischen dem Modell für die Verarbeitung von Anrufen an einem einzelnen Standort/an einem verteilten Standort/mit einem PSTN verbunden, das zuvor in diesem Dokument beschrieben wurde (CME/CUE/GW Single Site oder Branch Office, das mit dem PSTN verbunden ist), und dem im dritten Szenario dieses Dokuments beschriebenen standortübergreifenden/zentralisierten Anrufverarbeitungs-/konvergenten Sprach- und Datennetzwerk. In diesem Szenario wird weiterhin ein lokaler Cisco Unified CallManager Express verwendet, aber Ferngespräche und Telefonie im Hauptsitz/an einem Remote-Standort werden primär über Site-to-Site-SIP-Trunks ermöglicht, wobei lokale und Notrufe über eine lokale PSTN-Verbindung erfolgen. Selbst in Fällen, in denen die Mehrzahl der Legacy-PSTN-Verbindungen entfernt wird, wird eine grundlegende PSTN-Kapazität empfohlen, um den Ausfall des WAN-

basierten Nummernumgehens sowie des Ortsgesprächs zu bewältigen, wie im Wählplan beschrieben. Darüber hinaus müssen laut lokalen Gesetzen normalerweise lokale PSTN-Verbindungen bereitgestellt werden, um Notrufe (911) zu ermöglichen. In diesem Szenario erfolgt die verteilte Anrufverarbeitung, wobei die Vorteile und Best Practices, wie im Cisco Unified CallManager Express SRND beschrieben, berücksichtigt werden.

Unternehmen können dieses Anwendungsszenario unter folgenden Umständen implementieren:

- Zwischen den Standorten werden unterschiedliche VoIP-Umgebungen verwendet, aber VoIP ist nach wie vor erstrebenswert, anstatt ein PSTN für Fernverbindungen einzurichten.
- Für die Wählplanverwaltung ist eine standortbasierte Autonomie erforderlich.
- Unabhängig von der WAN-Verfügbarkeit ist die vollständige Anrufverarbeitung erforderlich.

Szenario-Hintergrund

Das Anwendungsszenario umfasst kabelgebundene Telefone (Sprach-VLAN), verkabelte PCs (Daten-VLAN) und Wireless-Geräte (darunter VoIP-Geräte wie IP Communicator).

Die Sicherheitskonfiguration bietet folgende Vorteile:

1. Vom Router initiierte Signalisierungsprüfung zwischen CME und lokalen Telefonen (SCCP und SIP) und CME sowie dem Remote-CUCM-Cluster (SIP).
2. Sprachmedien-Engpässe für die Kommunikation zwischen diesen:Lokale kabelgebundene und Wireless-SegmenteCME und die lokalen Telefone für WarteschleifenmusikCUE und lokale Telefone für VoicemailTelefone und Remote-Anrufeinheiten
3. Application Inspection and Control (AIC), mit der folgende Ziele erreicht werden können:Einladungs-Übertragungsratenlimit für NachrichtenProtokollkonformität für den gesamten SIP-Datenverkehr sicherstellen

Vorteile/Nachteile

Diese Anwendung bietet den Vorteil reduzierter Kosten, da sie standortübergreifenden Sprachverkehr auf WAN-Datenverbindungen überträgt.

Ein Nachteil dieses Szenarios ist, dass detailliertere Pläne für die WAN-Konnektivität erforderlich sind. Die Qualität von standortübergreifenden Anrufen kann durch zahlreiche Faktoren im WAN beeinflusst werden, z. B. durch unzulässigen/unerwünschten Datenverkehr (Würmer, Viren, Peer-to-Peer-Dateifreigabe) oder schwer zu identifizierende Latenzprobleme, die durch Traffic Engineering in Betreibernetzwerken entstehen können. WAN-Verbindungen müssen entsprechend dimensioniert sein, um eine ausreichende Bandbreite für Sprach- und Datenverkehr bereitzustellen. weniger latenzanfälliger Datenverkehr, z. B. E-Mail-, SMB-/CIFS-Dateiverkehr, kann zur Wahrung der Sprachqualität als Datenverkehr mit geringerer Priorität für QoS klassifiziert werden.

Ein weiteres Problem bei diesem Szenario sind die fehlende zentrale Anrufbearbeitung und die Schwierigkeiten, die bei der Behebung von Anrufverarbeitungsfehlern auftreten können. Daher eignet sich dieses Szenario am besten für größere Unternehmen als Zwischenschritt bei der Migration zu einer zentralisierten Anrufverarbeitung. Lokale Cisco CMEs können als SRST-Fallback mit vollem Funktionsumfang umgewandelt werden, wenn die Migration zu Cisco CallManager abgeschlossen ist.

Aus sicherheitstechnischer Sicht erschwert die zunehmende Komplexität dieser Umgebung die effektive Implementierung von Sicherheitsmaßnahmen und die Fehlerbehebung, da die Anbindung über ein WAN oder über VPN im öffentlichen Internet die Bedrohungsumgebung erheblich erhöht, insbesondere in Fällen, in denen Sicherheitsrichtlinien eine *vertrauensvolle* Perspektive erfordern, in denen der Datenverkehr über das WAN kaum eingeschränkt wird. Vor diesem Hintergrund implementieren die Konfigurationsbeispiele in diesem Dokument eine *verdächtigere* Richtlinie, die bestimmten geschäftskritischen Datenverkehr zulässt. Anschließend wird dieser durch Protokollkonformitätsprüfungen überprüft. Darüber hinaus sind bestimmte VoIP-Aktionen, also SIP INVITE, darauf beschränkt, die Wahrscheinlichkeit bösartiger oder unbeabsichtigter Softwarefehlfunktionen zu verringern, die sich negativ auf VoIP-Ressourcen und deren Benutzerfreundlichkeit auswirken.

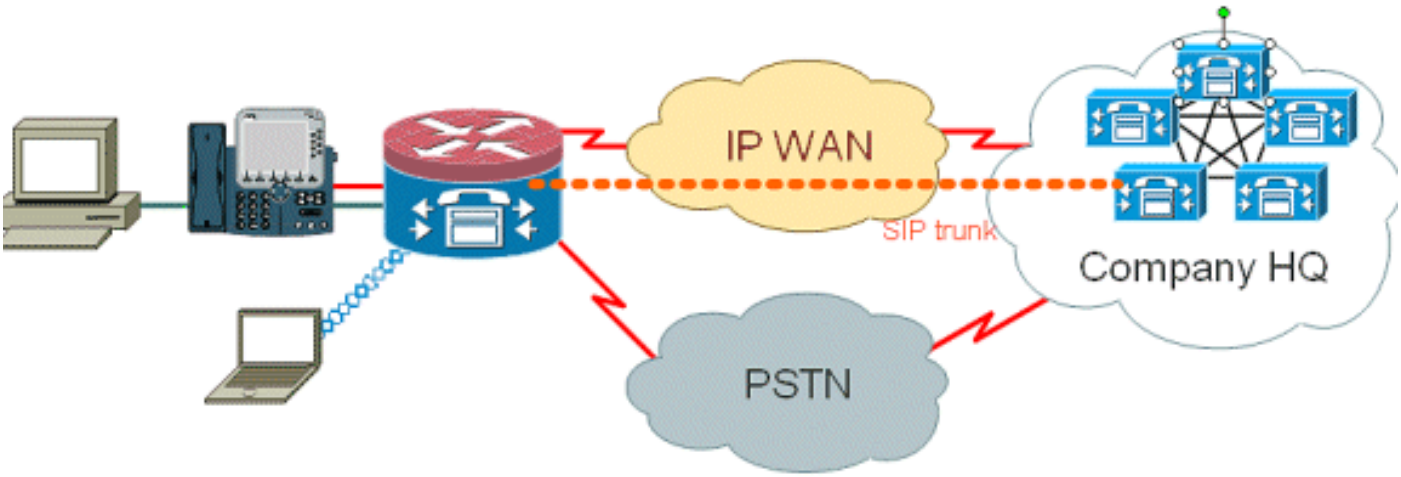
Konfiguration

Konfigurationen für Datenrichtlinien, zonenbasierte Firewall, Sprachsicherheit, CCME

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Die hier beschriebene Konfiguration zeigt einen Cisco 2851 Integrated Services Router.

In diesem Dokument werden folgende Konfigurationen verwendet:

- Konfiguration von Sprachdiensten für CME- und CUE-Verbindungen
- Firewall-Konfiguration für zonenbasierte Richtlinien
- Sicherheitskonfiguration

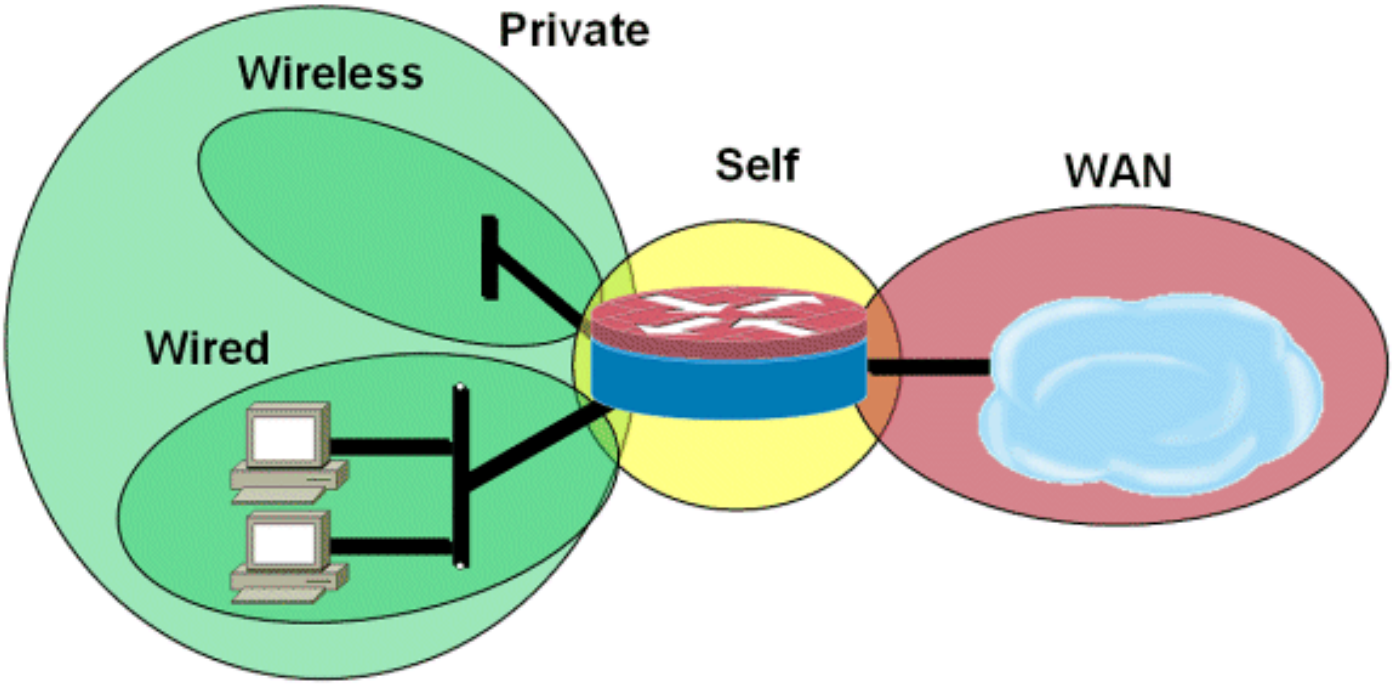
Dies ist die Konfiguration des Sprachdienstes für CME- und CUE-Verbindungen:

Konfiguration von Sprachdiensten für CME- und CUE-Verbindungen

```
!
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

!
```

Dies ist die zonenbasierte Firewall-Konfiguration, die aus Sicherheitszonen für kabelgebundene und Wireless-LAN-Segmente, einem privaten LAN (bestehend aus kabelgebundenen und Wireless-Segmenten), einem WAN-Segment, in dem vertrauenswürdige WAN-Verbindungen erreicht werden, und der Selbstzone besteht, in der sich die Sprachressourcen des Routers befinden:



Dies ist die Sicherheitskonfiguration:

Sicherheitskonfiguration

```
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
```

Bereitstellung, Management und Überwachung

Die Bereitstellung und Konfiguration sowohl für Router-basierte IP-Telefonie-Ressourcen als auch für zonenbasierte Richtlinien-Firewall ist im Allgemeinen am besten mit dem Cisco Configuration Professional kompatibel. Der Cisco Secure Manager unterstützt keine zonenbasierte Firewall oder routerbasierte IP-Telefonie.

Die Cisco IOS Classic Firewall unterstützt die SNMP-Überwachung mit der Cisco Unified Firewall MIB, die zonenbasierte Policy Firewall wird jedoch von der Unified Firewall MIB noch nicht unterstützt. Daher muss die Firewall-Überwachung mithilfe von Statistiken über die Kommandozeilenschnittstelle des Routers oder mithilfe von GUI-Tools wie Cisco Configuration Professional erfolgen.

Das Cisco Secure Monitoring and Reporting System (CS-MARS) bietet grundlegende Unterstützung für die zonenbasierte Policy-Firewall, obwohl Änderungen zur verbesserten Log-Message-Korrelation mit Datenverkehr, die in 12.4(15)T4/T5 und 12.4(20)T implementiert wurden, in CS-MARS noch nicht vollständig unterstützt wurden.

Kapazitätspläne

Die Ergebnisse des Firewall-Leistungstests für Anrufe aus Indien sind noch nicht festgelegt.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Die Cisco IOS Zone Firewall stellt **Anzeige**- und **Debug-**Befehle zum Anzeigen, Überwachen und Beheben der Aktivitäten der Firewall bereit. In diesem Abschnitt wird die Verwendung der **show-**Befehle zur Überwachung der grundlegenden Firewall-Aktivität beschrieben. Außerdem finden Sie eine Einführung in die **Debug-**Befehle der Zone-Firewall zur Fehlerbehebung in Ihrer Konfiguration oder wenn für Gespräche mit dem technischen Support detailliertere Informationen erforderlich sind.

Befehle zur Fehlerbehebung

Die Cisco IOS Firewall bietet mehrere **Show**-Befehle zum Anzeigen der Konfiguration und der Aktivitäten von Sicherheitsrichtlinien. Viele dieser Befehle können mithilfe des **Alias-**Befehls durch einen kürzeren Befehl ersetzt werden.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Debug-Befehle können nützlich sein, wenn Sie eine atypische oder nicht unterstützte Konfiguration verwenden und zur Lösung von Interoperabilitätsproblemen mit dem Cisco TAC oder den technischen Support-Services anderer Produkte zusammenarbeiten müssen.

Hinweis: Die Anwendung von **Debug-**Befehlen auf bestimmte Funktionen oder Datenverkehr kann dazu führen, dass eine sehr große Anzahl von Konsolennachrichten nicht mehr reagiert. Auch wenn Sie debuggen müssen, können Sie einen alternativen Zugriff auf die Kommandozeile bereitstellen, z. B. ein Telnet-Fenster, das den Terminaldialog nicht überwacht. Aktivieren Sie nur

das Debuggen von Offline-Geräten (Laborumgebung) oder innerhalb eines geplanten Wartungsfensters, da das Debuggen die Router-Leistung erheblich beeinflussen kann.

Zugehörige Informationen

- Designleitfaden für das Referenznetzwerk der Cisco Unified CallManager Express-Lösung
- Cisco CallManager Express Security Best Practices (CME SRND)
- Integration von Cisco Unity Connection mit Cisco Unified CME-as-SRST
- Befehlsreferenz für Cisco Unified Communications Manager Express
- Konfigurationsbeispiel für Cisco CallManager Express/Cisco Unity Express
- Cisco CallManager Express 3.4 SNMP MIB-Unterstützung
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Cisco IOS-Firewall: SIP-Erweiterungen: ALG und AIC
- Software Cisco IOS Firewall H.323-Unterstützung
- Unterstützung der Cisco IOS Firewall für lokalen Skinny-Datenverkehr und CME
- Technischer Support und Dokumentation für Cisco Systeme