# IOS Zone-Based Firewall: Konfigurationsbeispiel für eine PSTN-Verbindung mit CME/CUE/GW an einem Standort oder in einer Zweigstelle

## Inhalt


Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
IOS-Firewall-Hintergrund
Bereitstellen der zonenbasierten Cisco IOS Firewall
Überlegungen zur ZFW in VoIP-Umgebungen
IOS Firewall Voice Enhancements - 12.4(20)T
Hinweise
Network Address Translation
Cisco Unified Presence-Client
CME/CUE/GW PSTN-Verbindung mit einem Standort oder Zweigstelle
Szenario-Hintergrund
Vorteile und Nachteile
Datenrichtlinien, zonenbasierte Firewall, Sprachsicherheit und CCME-Konfigurationen
Bereitstellung, Verwaltung und Überwachung
Überprüfung
Fehlerbehebung
Debugbefehle
Zugehörige Informationen


## Einführung

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 und gleichzeitig Geschäftsfunktionen und Kontinuität zu ermöglichen.

In diesem Dokument werden Design- und Konfigurationserwägungen für Firewall-Sicherheitsaspekte bestimmter Cisco ISR-basierter Daten- und Sprachanwendungen beschrieben. Konfiguration für Sprachservices und Firewall wird für jedes Anwendungsszenario bereitgestellt. Jedes Szenario beschreibt die VoIP- und Sicherheitskonfigurationen separat, gefolgt von der gesamten Router-Konfiguration. Ihr Netzwerk erfordert möglicherweise eine andere Konfiguration für Services wie QoS und VPN, 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.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

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

# IOS-Firewall-Hintergrund

Die Cisco IOS Firewall wird in der Regel in Anwendungsszenarien bereitgestellt, die sich von den Bereitstellungsmodellen von 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 mag, müssen spezifische Überlegungen angestellt werden, um festzustellen, ob eine Router-basierte Firewall geeignet ist. Die Anwendung jeder zusätzlichen Funktion verursacht Speicher- und Verarbeitungskosten und wird wahrscheinlich zu niedrigeren Weiterleitungsdurchsätzen, einer höheren Paketlatenz und einem Verlust von Funktionsmerkmalen während Spitzenlastzeiten beitragen, wenn eine nicht ausgelastete integrierte Router-basierte Lösung bereitgestellt wird.

Befolgen Sie diese Richtlinien, wenn Sie zwischen einem Router und einer Appliance wählen:

- 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 sollten 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. Daher waren große Öffnungen in ansonsten sicheren Firewall-Richtlinien erforderlich, um Sprachdatenverkehr

aufzunehmen, und es wurde nur begrenzte Unterstützung für die Entwicklung von VoIP-Signalisierungs- und Medienprotokollen angeboten.

# Bereitstellen der zonenbasierten Cisco IOS Firewall

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 geht davon aus, 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 beeinträchtigt in der Regel weniger bestehende Anwendungen, erfordert jedoch ein umfassendes Verständnis der Bedrohungs- und Schwachstellenlandschaft und erfordert eine ständige Wachsamkeit, um neue Bedrohungen und Exploits so anzugehen, wie sie auftreten. Darüber hinaus muss die Benutzer-Community eine große Rolle bei der Gewährleistung 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. Eine Richtlinie, die den gesamten Anwendungsdatenverkehr außer dem explizit zulässigen Datenverkehr blockiert. 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 wie Zugriffskontrolllisten (ACLs) oder ZFW-Richtlinien (Zone-Based Policy Firewall) gesteuert werden sollte. Auf diese Weise sollte der Datenverkehr durch AIC, ein Intrusion Prevention System (IPS) oder andere signaturbasierte Kontrollen wie Flexible Packet Matching (FPM) oder netzwerkbasierte Anwendungserkennung (NNIPS) reduziert werden. LEISTE). Wenn also nur gewünschte Anwendungsports (und dynamischer medienspezifischer Datenverkehr, der aus bekannten Steuerungsverbindungen oder Sitzungen entsteht) ausdrücklich zugelassen sind, sollte der einzige unerwünschte Datenverkehr, der im Netzwerk vorhanden sein sollte, in eine spezifische, leichter erkennbare Teilmenge fallen, wodurch der technische und betriebliche Aufwand, der für die Aufrechterhaltung der Kontrolle über unerwünschten Datenverkehr anfällt, verringert wird.

In diesem Dokument werden VoIP-Sicherheitskonfigurationen basierend auf *verdächtigen* Aspekten beschrieben. Somit ist nur der in den Sprachnetzsegmenten zulässige Datenverkehr zulässig. 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 Funktionalität und Funktionalität vorhandener Anwendungen aus und müssen angepasst werden, um diese Auswirkungen zu minimieren oder zu beheben.

Weitere Informationen zum Konfigurieren der zonenbasierten Firewall für Richtlinien finden Sie im Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide.

## Überlegungen zur ZFW in VoIP-Umgebungen

Der Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide bietet eine kurze Erläuterung zur Sicherung des Routers mithilfe von Sicherheitsrichtlinien für die *Selbstzone* des Routers sowie alternativer Funktionen, die über verschiedene Network Foundation Protection (NFP)-Funktionen bereitgestellt werden. Router-basierte VoIP-Funktionen werden in der Self-Zone des Routers gehostet. Sicherheitsrichtlinien zum Schutz des Routers müssen die Anforderungen für Sprachdatenverkehr berücksichtigen, um Sprachsignalisierungen und -medien zu unterstützen, 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, sodass die Firewall-Richtlinien nicht für den vollständigen Schutz der Ressourcen optimiert wurden. Sicherheitsrichtlinien für die Selbstzone, die routerbasierte VoIP-Ressourcen schützen, basieren in hohem Maße auf den in 12.4(20)T eingeführten Funktionen.

## IOS Firewall Voice Enhancements - 12.4(20)T

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 ausgehenden Datenverkehr resultieren
- 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 zu erkennen sind
- H.323 v3/v4-UnterstützungAktualisierungen der H.323-Unterstützung für v3 und v4 (zuvor unterstützte Version 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, die von diesen Erweiterungen angeboten werden, und erläutern, wie die von den Richtlinien

angewendeten Aktionen beschrieben werden. Vollständige Einzelheiten zu den Sprachinspektionsfunktionen finden Sie in den einzelnen Funktionsdokumenten, die im Abschnitt Zugehörige Informationen dieses Dokuments aufgeführt sind.

# 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 erforderliche Funktion zur vollständigen Unterstützung der Komplexität und des Verhaltens von Sprachdatenverkehr bei der Signalisierung.

## Network Address Translation

Cisco IOS Network Address Translation (NAT) wird häufig gleichzeitig mit der Cisco IOS Firewall konfiguriert, insbesondere in Fällen, in denen private Netzwerke mit dem Internet verbunden werden müssen oder in denen unterschiedliche private Netzwerke eine Verbindung herstellen müssen, insbesondere wenn sich überschneidende IP-Adressräume genutzt werden. Die Cisco IOS Software umfasst NAT-Application-Layer-Gateways (ALGs) für SIP, Skinny und H.323. Im Idealfall kann die Netzwerkverbindung für IP-Sprachverbindungen ohne Anwendung von NAT eingerichtet werden, da NAT die Fehlerbehebung und die Anwendung von Sicherheitsrichtlinien zusätzlich vereinfacht, insbesondere bei Verwendung von NAT-Überlastung. NAT sollte nur als letzte Lösung zur Behebung von Netzwerkverbindungsproblemen angewendet werden.

## Cisco Unified Presence-Client

In diesem Dokument werden keine Konfigurationen beschrieben, die die Verwendung von Cisco Unified Presence Client (CUPC) mit der IOS-Firewall unterstützen, da CUPC von der Zone oder der klassischen Firewall 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 PSTN-Verbindung mit einem Standort oder Zweigstelle

Dieses Szenario führt eine sichere, routerbasierte Voice-over-IP-Telefonie für kleine bis mittlere Unternehmen an einem Standort oder für größere Unternehmen an mehreren Standorten ein, die verteilte Anrufverarbeitung bereitstellen und so Legacy-Verbindungen zum Public Switched Telefone Network (PSTN) aufrechterhalten möchten. Die VoIP-Anrufsteuerung wird durch die Anwendung von Cisco Unified Call Manager Express ermöglicht.

Die PSTN-Konnektivität kann langfristig aufrechterhalten werden oder zu einem konvergenten IP-Weitverkehrsnetzwerk für Sprache und Daten migriert werden, wie im Anwendungsbeispiel im Abschnitt CME/CUE/GW Single Site oder in Zweigstellen mit SIP-Trunk zu CCM im Hauptsitz oder im Abschnitt Voice Provider dieses Dokuments beschrieben.

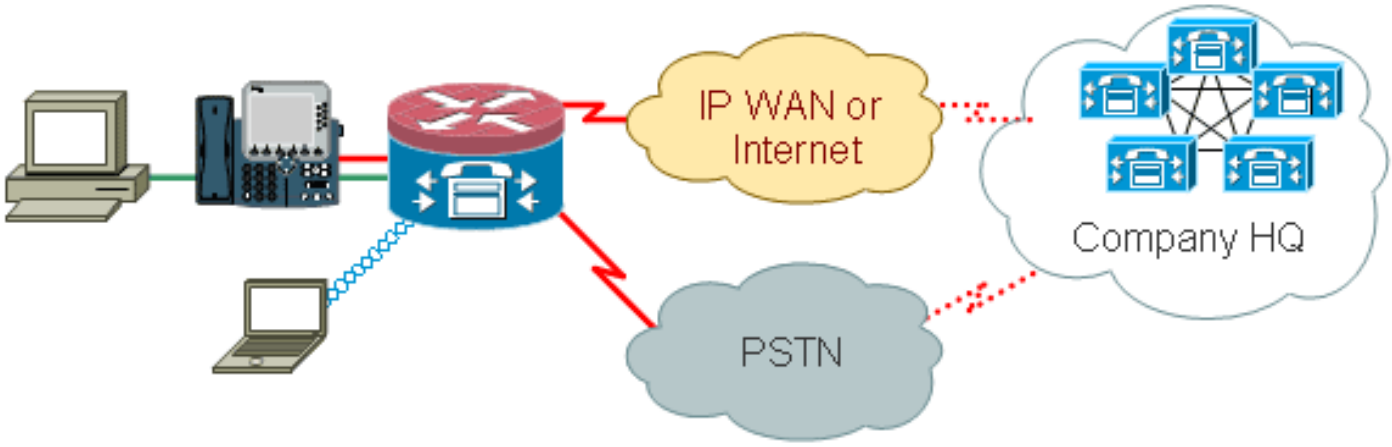
Diese Art von Anwendungsszenario sollte in Erwägung gezogen werden, wenn zwischen den Standorten unterschiedliche VoIP-Umgebungen verwendet werden oder VoIP aufgrund unzureichender WAN-Datenverbindungen oder örtlich begrenzter VoIP-Nutzung in Datennetzwerken nicht praktikabel ist. Die Vorteile und Best Practices für IP-Telefonie an einem Standort werden im Cisco Unified CallManager Express SRND beschrieben.

## 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 Folgendes:

- Vom Router initiierte Signalisierungsprüfung zwischen CME und lokalen Telefonen (SCCP und/oder SIP)
- Sprachmedien-Pinholes für die Kommunikation zwischen:Lokale kabelgebundene und Wireless-SegmenteCME und die lokalen Telefone für WarteschleifenmusikCUE und lokale Telefone für Voicemail
- Application Inspection and Control (AIC) auf:Einladungs-Übertragungsratenlimit für NachrichtenSicherstellen der Protokollkonformität für den gesamten SIP-Datenverkehr




## Vorteile und Nachteile

Der offensichtlichste Vorteil des VoIP-Szenarios ist der Migrationspfad, der durch die Integration der vorhandenen Sprach- und Datennetzwerkinfrastruktur in eine vorhandene POTS/TDM-Umgebung geboten wird, bevor ein konvergentes Sprach-/Datennetzwerk für Telefoniedienste in die Welt außerhalb des LAN verlagert wird. Die Telefonnummern werden für kleinere Unternehmen beibehalten, und für größere Unternehmen, die eine schrittweise Migration zur Telefonie per Umgehung von Telefonaten wünschen, können der vorhandene Centrex- oder DID-Service verbleiben.

Zu den Nachteilen zählen der Verlust von Kosteneinsparungen, die durch die Umstellung auf ein konvergentes Sprach- und Datennetzwerk mit Umgehung von Gebühren realisiert werden könnten, sowie Einschränkungen bei der Anrufflexibilität und fehlende unternehmensweite Kommunikationsintegration und Portabilität, die mit einem vollständig konvergenten Sprach- und Datennetzwerk realisiert werden könnten.

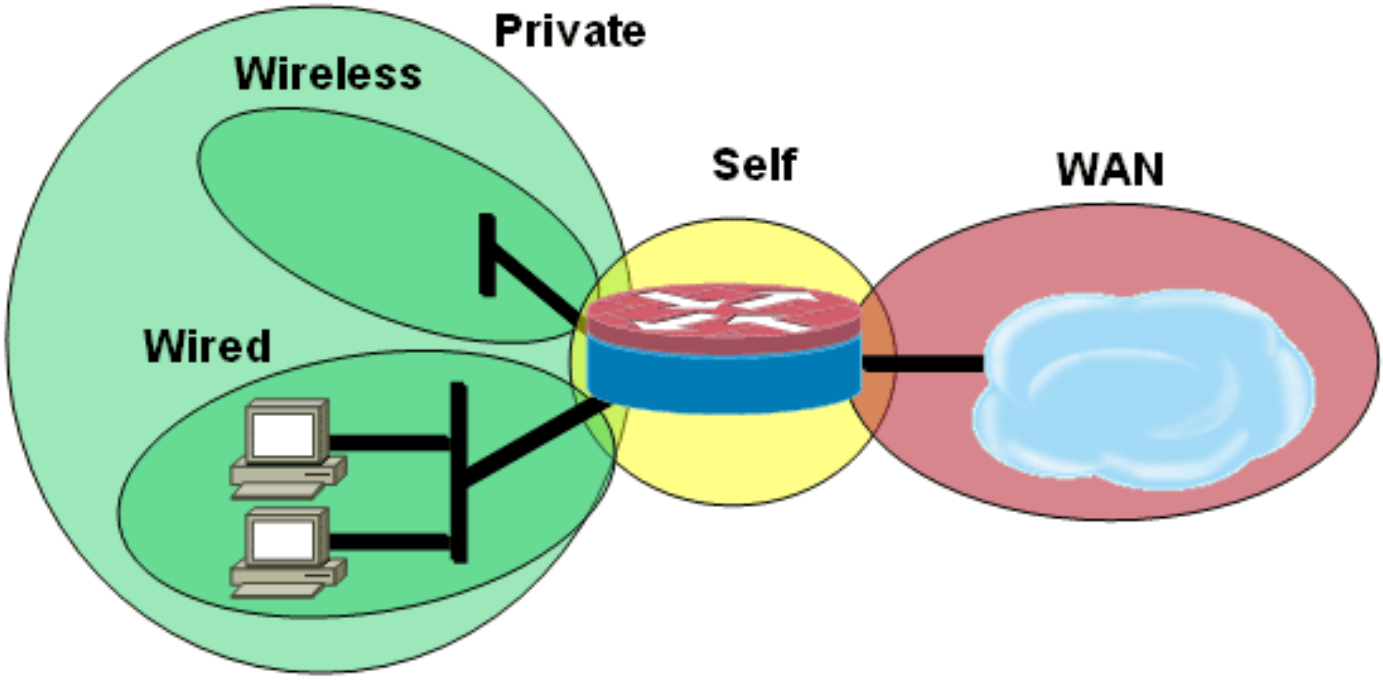
Aus Sicherheitssicht minimiert diese Netzwerkumgebung VoIP-Sicherheitsbedrohungen, da VoIP-Ressourcen nicht dem öffentlichen Netzwerk oder WAN ausgesetzt werden. Der im Router integrierte Cisco Call Manager Express wäre jedoch weiterhin anfällig für interne Bedrohungen wie schädlichen Datenverkehr oder fehlerhaft funktionierenden Anwendungsdatenverkehr. So wird eine Richtlinie implementiert, die Sprachdatenverkehr, der die Protokollkonformitätsprüfungen erfüllt, sowie bestimmte VoIP-Aktionen (z. B. SIP INVITE) begrenzt, um die Wahrscheinlichkeit von bösartigen oder unbeabsichtigten Softwarefehlfunktionen zu verringern, die VoIP-Ressourcen und deren Nutzbarkeit beeinträchtigen.

## Datenrichtlinien, zonenbasierte Firewall, Sprachsicherheit und CCME-Konfigurationen

Die hier beschriebene Konfiguration zeigt einen 2851 mit einer Sprachdienstkonfiguration 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
!
```

Zonenbasierte Firewall-Konfiguration, bestehend aus Sicherheitszonen für kabelgebundene und Wireless-LAN-Segmente, privatem LAN (bestehend aus kabelgebundenen und Wireless-Segmenten), einem öffentlichen WAN-Segment, in dem nicht vertrauenswürdige Internetverbindungen erreicht werden, und der Selbstzone, in der sich die Sprachressourcen des Routers befinden.




**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
```

## Gesamte Routerkonfiguration

```
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
```

# Bereitstellung, Verwaltung 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 Cisco Configuration Professional kompatibel. 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. Zonenbasierte Richtlinien-Firewall wird von der Unified Firewall-MIB jedoch noch nicht unterstützt. Daher muss die Firewall-Überwachung mithilfe von Statistiken über die Befehlszeilenschnittstelle 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. Es protokolliert jedoch Änderungen, die eine verbesserte Log-Message-Korrelation mit Datenverkehr verbesserten, die in 12.4(15)T4/T5 und 12.4(20)T in CS-MARS implementiert wurden.

# 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 Firewall-Aktivitäten bereit. In diesem Abschnitt finden Sie eine Einführung in die Befehle zum **Debuggen** der Zone-Firewall, die detaillierte Informationen zur Fehlerbehebung enthalten.

## Debugbefehle

Debug-Befehle sind nützlich, 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 Konsolenmeldungen ausgegeben wird, wodurch die Router-Konsole nicht mehr reagiert. Auch wenn Sie das Debuggen aktivieren müssen, können Sie einen alternativen Zugriff auf die Befehlszeilenschnittstelle bereitstellen, z. B. ein Telnet-Fenster, das den Terminaldialog nicht überwacht. Sie sollten das Debuggen nur auf Offline-Geräten (Laborumgebung) oder während eines geplanten Wartungsfensters aktivieren, da das Aktivieren des Debuggens die Routerleistung erheblich beeinflussen kann.

# Zugehörige Informationen

- Designleitfaden für das Referenznetzwerk der Cisco Unified CallManager Express-Lösung
- 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
- Technischer Support und Dokumentation für Cisco Systeme