

# IOS Zone–Based Firewall: CME/CUE/GW Single Site or Branch Office PSTN Connection Configuration Example

Document ID: 108014

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### IOS Firewall Background

#### Deploying Cisco IOS Zone–Based Policy Firewall

- Considerations for ZFW in VoIP Environments
- IOS Firewall Voice Enhancements 12.4(20)T

### Caveats

- Network Address Translation
- Cisco Unified Presence Client

### CME/CUE/GW Single Site or Branch PSTN Connection

- Scenario Background
- Advantages and Disadvantages
- Data Policies, Zone–Based Firewall, Voice Security, and CCME Configurations

### Provisioning, Management, and Monitoring

### Verify

### Troubleshoot

- Debug Commands

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

Cisco Integrated Service Routers (ISRs) offer a scalable platform to address data and voice network requirements for a wide range of applications. Although the threat landscape of both private and Internet–connected networks is a very dynamic environment, Cisco IOS Firewall offers stateful inspection and Application Inspection and Control (AIC) capabilities to define and enforce a secure network posture, while enabling business capability and continuity.

This document describes design and configuration considerations for firewall security aspects of specific Cisco ISR–based data and voice application scenarios. Configuration for voice services and firewall are provided for each application scenario. Each scenario describes the VoIP and security configurations separately, followed by the entire router configuration. Your network may require other configuration for services such as QoS and VPN to maintain voice quality and confidentiality.

## Prerequisites

### Requirements

There are no specific requirements for this document.

## Components Used

This document is not restricted to specific software and hardware versions.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## IOS Firewall Background

Cisco IOS Firewall is typically deployed in application scenarios that differ from appliance firewalls deployment models. Typical deployments include Teleworker applications, small- or branch-office sites, and retail applications, where low device count, integration of multiple services, and lower performance and security capability depth is desired.

While application of firewall inspection, along with other integrated services in the ISR products, might appear attractive from cost and operational perspective, specific considerations must be evaluated in order to determine if a router-based firewall is appropriate. Application of each additional feature incurs memory and processing costs and will likely contribute to reduced forwarding throughput rates, increased packet latency, and loss of feature capability during periods of peak load if an underpowered integrated router-based solution is deployed.

Follow these guidelines when you decide between a router and an appliance:

- Routers with multiple integrated features enabled are best suited for branch-office or telecommuter sites where less devices offer a better solution.
- High-bandwidth, high-performance applications are typically better addressed with appliances: Cisco ASA and Cisco Unified Call Manager Server should be applied to handle NAT and security policy application and call processing, while routers address QoS policy application, WAN termination, and site-to-site VPN connectivity requirements.

Prior to the introduction of Cisco IOS Software version 12.4(20)T, Classic Firewall and Zone-Based Policy Firewall (ZFW) was unable to fully support capabilities required for VoIP traffic and router-based voice services, requiring large openings in otherwise secure firewall policies to accommodate voice traffic, and offering limited support for evolving VoIP signaling and media protocols.

## Deploying Cisco IOS Zone-Based Policy Firewall

Cisco IOS Zone-Based Policy Firewall, similar to other firewalls, can only offer a secure firewall if the network's security requirements are identified and described by security policy. There are two fundamental approaches to arrive at a security policy: the *trusting* perspective, as opposed to the *suspicious* perspective.

The *trusting* perspective assumes all traffic is trustworthy, except that which can be specifically identified as malicious or unwanted. A specific policy is implemented that denies only the unwanted traffic. This is typically accomplished through the use specific access-control entries, or signature- or behavior-based tools. This approach tends to interfere less with existing applications, but requires a comprehensive knowledge of the threat and vulnerability landscape, and requires constant vigilance to address new threats and exploits as they appear. Additionally, the user community must play a large part in maintaining adequate security. An

environment that allows broad freedom with little control for the occupants offers substantial opportunity for problems caused by careless or malicious individuals. An additional problem of this approach is that it relies much more on effective management tools and application controls that offer sufficient flexibility and performance to be able to monitor and control suspect data in all network traffic. While technology is presently available to accommodate this, the operational burden frequently exceeds the limits of most organizations.

The *suspicious* perspective assumes all network traffic is undesired, except for specifically identified *good* traffic. A policy that is applied which denies all application traffic except that which is explicitly permitted. Additionally, application inspection and control (AIC) may be implemented to identify and deny malicious traffic that is specifically crafted to exploit good applications, as well as unwanted traffic that is masquerading as good traffic. Again, application controls impose operational and performance burdens on the network, although most undesired traffic should be controlled by stateless filters such as access-control lists (ACLs) or Zone-Based Policy Firewall (ZFW) policy, so there should be substantially less traffic that must be handled by AIC, intrusion prevention system (IPS), or other signature-based controls such as flexible packet matching (FPM) or network-based application recognition (NBAR). Thus, if only desired application ports (and dynamic media-specific traffic arising from known control connections or sessions) are specifically permitted, the only unwanted traffic that should be present on the network should fall into a specific, more-easily-recognized subset, which reduces the engineering and operational burden imposed to maintain control over undesired traffic.

This document describes VoIP security configurations based on the *suspicious* perspective; thus, only traffic that is permissible in the voice-network segments is permitted. Data policies tend to be more permissive, as described by notes in each application scenario's configuration.

All security policy deployments must follow a closed-loop feedback cycle; security deployments typically affect capability and functionality of existing applications and must be adjusted to minimize or resolve this impact.

For more information about how to configure the Zone-Based Policy Firewall, refer to Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide.

## Considerations for ZFW in VoIP Environments

The Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide offers a brief discussion for securing the router with the use of security policies to and from the router's *self* zone, as well as alternative capabilities that are provided through various Network Foundation Protection (NFP) features. Router-based VoIP capabilities are hosted within the router's *self* zone, so security policies that protect the router must be aware of the requirements for voice traffic, in order to accommodate the voice signaling and media originated by and destined to Cisco Unified CallManager Express, Survivable Remote-Site Telephony, and Voice Gateway resources. Prior to Cisco IOS Software Version 12.4(20)T, Classic Firewall and Zone-Based Policy Firewall was unable to fully accommodate the requirements of VoIP traffic, so firewall policies were not optimized to fully protect resources. Self-zone security policies that protect router-based VoIP resources rely heavily on capabilities introduced in 12.4(20)T.

## IOS Firewall Voice Enhancements 12.4(20)T

Cisco IOS Software Release 12.4(20)T introduced several enhancements to enable co-resident Zone Firewall and voice capabilities. Three main features apply directly to secure voice applications:

- SIP Enhancements: Application-Layer Gateway and Application Inspection and Control
  - ◆ Updates SIP version support to SIPv2, as described by RFC 3261

- ◆ Broadens SIP signaling support to recognize a wider variety of call flows
- ◆ Introduces SIP Application Inspection and Control (AIC) to apply granular controls to address specific application–level vulnerabilities and exploits
- ◆ Expands self–zone inspection to be able to recognize secondary signaling and media channels resulting from locally–destined/–originated SIP traffic
- Support for Skinny Local Traffic and CME
  - ◆ Updates SCCP support to version 16 (previously supported version 9)
  - ◆ Introduces SCCP Application Inspection and Control (AIC) to apply granular controls to address specific application–level vulnerabilities and exploits
  - ◆ Expands self–zone inspection to be able to recognize secondary signaling and media channels resulting from locally–destined/–originated SCCP traffic
- H.323 v3/v4 Support
  - ◆ Updates H.323 support to v3 and v4 (previously supported v1 and v2)
  - ◆ Introduces H.323 Application Inspection and Control (AIC) to apply granular controls to address specific application–level vulnerabilities and exploits

The router security configurations described in this document include capabilities offered by these enhancements, with explanation to describe the action applied by the policies. For complete details on the voice inspection features, refer to the individual feature documents listed in the Related Information section of this document

## Caveats

In order to reinforce points mentioned earlier, application of Cisco IOS Firewall with router–based voice capabilities must apply the Zone–Based Policy Firewall. Classic IOS Firewall does not include the needed capability to fully support the signaling complexities and behavior of voice traffic.

## Network Address Translation

Cisco IOS network address translation (NAT) is frequently configured concurrently with Cisco IOS Firewall, particularly in cases where private networks must interface with the Internet, or if disparate private networks must connect, particularly if overlapping IP address space is in use. Cisco IOS Software includes NAT application layer gateways (ALGs) for SIP, Skinny, and H.323. Ideally, network connectivity for IP voice can be accommodated without the application of NAT, as NAT introduces additional complexity to troubleshooting and security–policy applications, particularly in cases where NAT overload is used. NAT should only be applied as a last case solution to address network connectivity concerns.

## Cisco Unified Presence Client

This document does not describe configurations that support the use of Cisco Unified Presence Client (CUPC) with IOS Firewall, as CUPC is not yet supported by Zone or Classic Firewall as of Cisco IOS Software Release 12.4(20)T1. CUPC will be supported in a future release of Cisco IOS Software.

## CME/CUE/GW Single Site or Branch PSTN Connection

This scenario introduces secure router–based Voice–over–IP telephony for single–site small–to–medium businesses or for larger multi–site organizations that wish to deploy distributed call processing, maintaining legacy connections to the Public Switched Telephone Network (PSTN). VoIP call control is accommodated through the application of a Cisco Unified Call Manager Express.

PSTN connectivity may be maintained in the long term or may be migrated to a converged voice-and-data IP wide-area network, as described by the application example discussed in the CME/CUE/GW Single Site or Branch Office with SIP Trunk to CCM at HQ or Voice Provider section of this document.

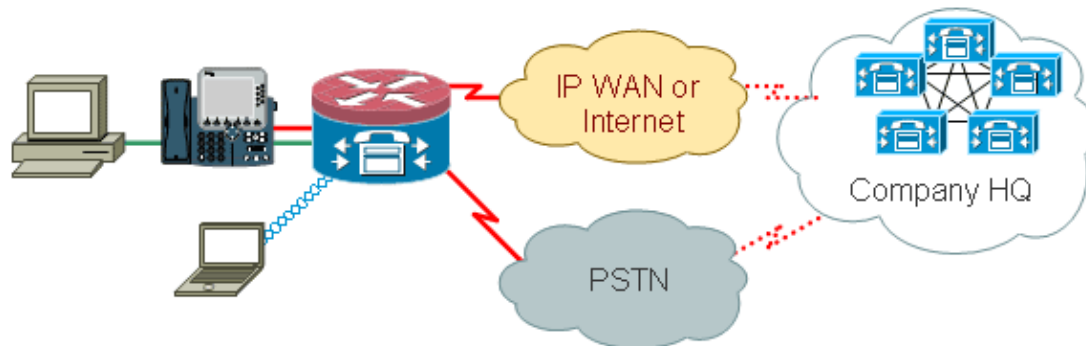
Organizations should consider implementing this type of application scenario for circumstances where disparate VoIP environments are used between sites or if VoIP is impractical due to inadequate WAN data connectivity, or locale-specific restrictions on VoIP usage on data networks. Benefits and best practices of single-site IP Telephony are described in the Cisco Unified CallManager Express SRND.

## Scenario Background

The application scenario incorporates wired phones (voice VLAN), wired PCs (data VLAN), and wireless devices (which include VoIP devices such as IP Communicator).

The security configuration provides:

- Router-initiated signaling inspection between CME and local phones (SCCP and/or SIP)
- Voice-media pinholes for communication between:
  - ◆ Local wired and wireless segments
  - ◆ CME and the local phones for MoH
  - ◆ CUE and the local phones for voice mail
- Apply Application Inspection and Control (AIC) to:
  - ◆ Rate limit invite messages
  - ◆ Assure protocol conformance on all SIP traffic.



## Advantages and Disadvantages

The most obvious benefit of the VoIP aspect of scenario is the migration path offered by integrating existing voice- and data-network infrastructure in an existing POTS/TDM environment, before moving to a converged voice/data network for telephony services to the world beyond the LAN. Phone numbers are maintained for smaller businesses, and existing centrex or DID service can be left in place for larger organizations that desire a staged migration to toll-bypass packet telephony.

Disadvantages include the loss of cost savings that could be realized with toll bypass by moving to a converged voice-and-data network, as well as limitations on calling flexibility and the lack of organization-wide communications integration and portability that could be realized with a fully converged voice-and-data network.

From a security perspective, this type of network environment minimizes VoIP security threats, by avoiding exposure of VoIP resources to the public network or WAN. However, the Cisco Call Manager Express

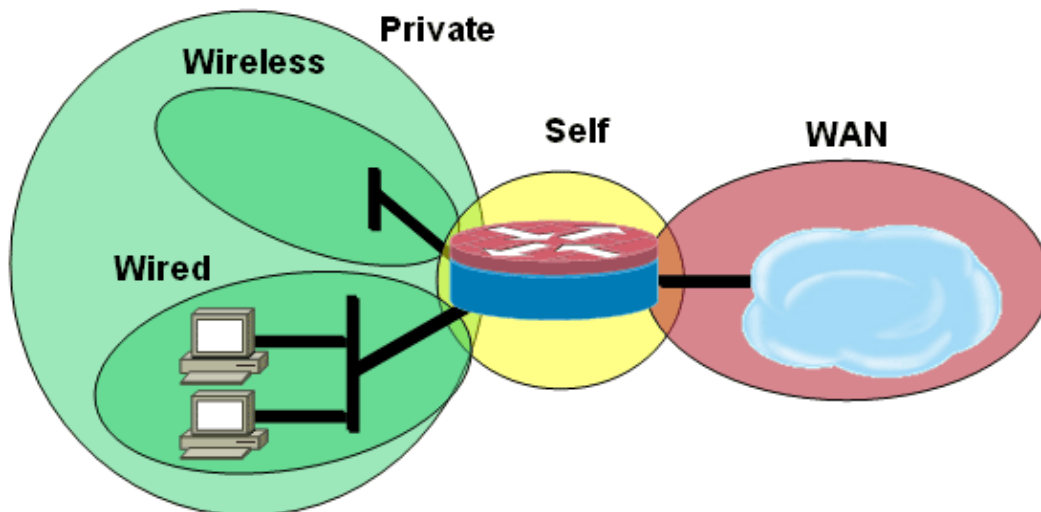
embedded within the router would still be vulnerable to internal threats such as malicious traffic or malfunctioning application traffic. Thus, policy is implemented which allows voice-specific traffic that meets the protocol conformance checks, and specific VoIP actions (i.e. SIP INVITE) are limited so as to reduce the likelihood of malicious or unintentional software malfunctions negatively impacting VoIP resources and usability.

## Data Policies, Zone-Based Firewall, Voice Security, and CCME Configurations

Configuration described here illustrates a 2851 with an Voice Service configuration for CME and CUE connectivity:

```
!
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
!
```

Zone-Based Policy Firewall Configuration, composed of security zones for wired and wireless LAN segments, private LAN (composed of wired and wireless segments), a public WAN segment where untrusted Internet connectivity is reached, and the self zone where the router's voice resources are located.



### Security Configuration

```
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
!
ntp server 172.16.1.1
end

```

## Provisioning, Management, and Monitoring

Provisioning and configuration for both router-based IP Telephony resources and Zone-Based Policy Firewall is generally best accommodated with Cisco Configuration Professional. CiscoSecure Manager does not support Zone-Based Policy firewall or router-based IP telephony.

Cisco IOS Classic Firewall supports SNMP monitoring with the Cisco Unified Firewall MIB. However, Zone-Based Policy Firewall is not yet supported in the Unified Firewall MIB. As such, firewall monitoring must be handled via statistics on the router's command-line interface, or with GUI tools such as Cisco

Configuration Professional.

CiscoSecure Monitoring And Reporting System (CS-MARS) offers basic support for the Zone-Based Policy Firewall, although logging changes that improved log-message correlation to traffic which were implemented in 12.4(15)T4/T5 and 12.4(20)T have not yet been fully supported in CS-MARS.

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

Cisco IOS Zone Firewall provides **show** and **debug** commands to view, monitor, and troubleshoot the firewall s activity. This section provides an introduction to the Zone Firewall **debug** commands that provide detailed troubleshooting information.

## Debug Commands

Debug commands are useful in the event that you use an atypical or unsupported configuration and need to work with the Cisco TAC or other products technical support services to resolve interoperability issues.

**Note:** Application of **debug** commands to specific capabilities or traffic may cause a very large number of console messages, which cause the router console to become unresponsive. In the even that you need to enable debugging, you might want to provide for alternative command-line interface access, such as a telnet window that does not monitor terminal dialogue. You should only enable debug on offline (lab environment) equipment or during a planned maintenance window, as enabling debug might substantially affect router performance.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- **Cisco Unified CallManager Express Solution Reference Network Design Guide**
- **Cisco Unity Express section of Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x**
- **Cisco Unified CallManager Express Security Best Practices**
- **Integrating Cisco Unity Connection with Cisco Unified CME-as-SRST**
- **Cisco Unified Communications Manager Express Command Reference**
- **Cisco CallManager Express/Cisco Unity Express Configuration Example**

- **Cisco CallManager Express 3.4 SNMP MIB Support**
  - **Cisco Unified Communications Manager Express Call Monitoring Interface Guide**
  - **Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide**
  - **Technical Support & Documentation – Cisco Systems**
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 10, 2008

Document ID: 108014

---