Contents

Introduction

This page provides information on how the Cisco ASA 5500 Series Adaptive Security Appliance is configured during Unified Communications system testing when it is deployed in the data center for protecting Unified Communications servers.

The configuration information is based on system testing performed in various test beds during Cisco Unified Communications system releases.

The page does not contain detailed step-by-step procedures; for detailed information about installing, configuring, and administering the Cisco ASA 5500 Series Adaptive Security Appliance, refer to the pointers in the Related Documentation section.

Design

For information on design considerations and guidelines for deploying the Cisco ASA 5500 Series Adaptive Security Appliance in a UC environment, see the Voice Security chapter of the Cisco Unified Communications Manager 8.x Solution Reference Network Design (SRND). For more generic data center security design considerations refer to the Data Center Security Design Guides.

For information on specific deployments and sites where Cisco ASA 5500 Series Adaptive Security Appliance solution testing was performed, see the Tested Deployments and Site Models for IPT Enterprise.

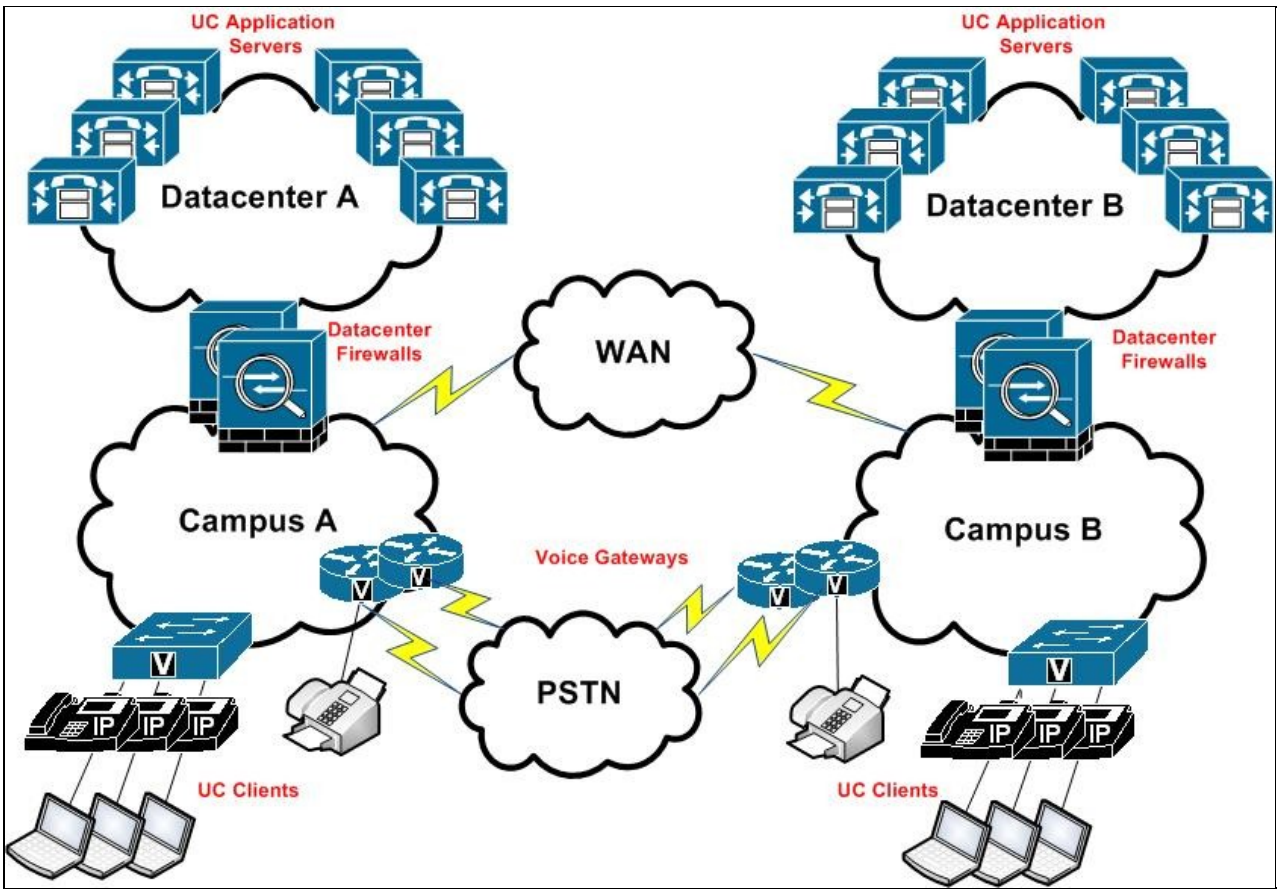
Topologies

This section provides information on where the Cisco ASA 5500 Series Adaptive Security Appliance is located relative to other components when it is used for data center deployments during Cisco Unified Communications solution testing.

The purpose of the data center firewall is to protect the servers in the data center from the rest of the enterprise network. Consequently, the firewall is positioned such that its more trusted ("inside") interface faces the UC servers in the data center and its less trusted ("outside") interface faces the clients. A data center firewall may have more than two interfaces, each with a different security level to distinguish between different trust levels of certain servers and/or clients. Cisco Unified Communications solution testing currently only covers the scenario where the firewall has two interfaces.

An enterprise network may have multiple data centers, in which case the servers in different data centers may need to talk to each other. This can be achieved through a backend connection that does not traverse the firewalls, or through the firewalls themselves. Unified Communications solution testing covers scenarios where the data center to data center traffic flows through the data center firewalls.

Figure 1 provides a schematic overview of this topology.



The above picture shows dual firewalls in front of each data center, for redundancy. For Unified Communications solution testing these firewall pairs are always configured for active/standby operation.

From the Unified Communications perspective the above topology represents two significantly different cases depending on whether the UC servers in the two data centers belong to the same cluster or to two different clusters. Unified Communications solution testing covers both scenarios.

Configuration Details

This section provides the high-level tasks and related information for configuring the Cisco ASA 5500 Series Adaptive Security Appliance as a data center firewall that protects Unified Communications servers.

The following table provide this information:

- **Configuration Tasks**: List of high-level configuration tasks
- **Solution Test Specifics**: Solution test variations from procedures and settings documented in the product documentation.
- **More Information**: Links to product documentation for detailed configuration information related to the high-level tasks.

Table 1: Cisco ASA 5500 Series Adaptive Security Appliance Configuration

Configuration Tasks	Solution Test Specifics	More Information
	N/A	

1. Physical installation and basic system configuration.		Cisco ASA 5500 Series Install and Upgrade Guides Configuring Interfaces Configuring Basic Settings Information About High Availability
2. Unified Communications protocol inspections.	N/A	Configuring Inspection of Voice and Video Protocols TFTP Inspection
3. Access list entries to allow Unified Communications traffic flows.	There are no explicit recommendations on how to configure ACEs for UC traffic. The Access List Examples section contains the ACL template used for solution testing.	ACL Configuration Overview Port Usage for Cisco Unified Communications Manager 8.0 Port Usage for Cisco Unified Presence 8.0 Port Usage for Cisco Unified CCX 8.0
4. Timeout adjustments	There are no explicit recommendations on what timeout values to use, however the design guides are clear that the default 5 minute timeout for H.323 is not sufficient in many cases (see referenced documents for more detail). Solution testing uses a 12 hour timeout for H.323.	Firewalls and H.323 section in the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 7.x Cisco Unified Mobile Agent section in the Cisco Unified Contact Center Enterprise 7.5 SRND Configuring H.323 and H.225 Timeout Values
5. TLS Proxy configuration	N/A	Configuring the TLS Proxy for Encrypted Voice Inspection

Configuration Data

This section contains configuration examples that illustrate how the ASA firewalls are configured in solution testing. The provided examples cover only parts of the firewall configuration; the sum of the examples does not make up a complete configuration. The intention is to provide reference points to a person who is familiar with the ASA firewall. The examples are not a substitute for the configuration and design guides referenced in the Related Documentation section.

Inspection Policy

The following is a typical inspection policy used for solution testing where TLS Proxy is not required:

```
class-map inspection_default
 match default-inspection-traffic
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
!
policy-map type inspect h323 RRQ-RCF-INSPECTION
 parameters
  ras-rcf-pinholes enable
!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect esmtp
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect icmp
  inspect icmp error
  inspect mgcp
  inspect rsh
  inspect sip
  inspect skinny
  inspect tftp
  inspect h323 ras RRQ-RCF-INSPECTION
!
service-policy global_policy global
```

The RRQ-RCF-INSPECTION policy-map is used to turn on a relatively new feature on the ASA that inspects the registration messages H.323 endpoints exchange with gatekeepers. This is useful if the CUCM protected by the ASA has gatekeeper controlled H.225 trunks. For such trunks the CUCM accepts connections on a randomly chosen port and this port is registered with the gatekeeper. Without inspecting the registration messages the ASA would not know where to expect the H.225 connections.

In cases where TLS Proxy is required, the following *additions* are made to the inspection policy:

```
tls-proxy TLS-PROXY
 server trust-point TLS-PROXY-TP
 client ldc issuer LDC-SIGNER-TP
 client ldc key-pair PHONE-COMMON-KEY
 client cipher-suite 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 null-sha1 rc4-sha1
!
class-map SECURE-SIP
 match port tcp range 5061 5062
class-map SECURE-SKINNY
 match port tcp eq 2443
!
policy-map global_policy
 class SECURE-SIP
  inspect sip tls-proxy TLS-PROXY
 class SECURE-SKINNY
  inspect skinny tls-proxy TLS-PROXY
```

Access List Examples

The ASA firewall is capable of applying different access lists on each interface, and separate access lists for traffic entering and leaving an interface. Solution testing is conducted with the same access list (GLOBAL-ACL) applied on both the inside and the outside interface and only to the traffic entering the interfaces:

```
access-group GLOBAL-ACL in interface outside
```

```
access-group GLOBAL-ACL in interface inside
```

We apply an access list to both the inside and the outside interface to increase our chances to discover problems. It is not a technical requirement to have an access list on both interfaces; depending on your security policy, it may be appropriate to not apply any access list to traffic that enters through the "inside" interface.

We chose to apply the same access list to both interfaces to simplify management and to match the global policy described in the previous section. This again is not a technical requirement: you may apply a different access list to each interface.

The ASA 8.3 release introduced the feature of Interface-Independent Access Policies, which will allow us to simplify the above configuration to:

```
access-group GLOBAL-ACL global
```

This has not yet been tested in Unified Communications solution testing.

Object Groups

Another technique to simplify management is the use of object groups. The ASA allows the grouping of both IP addresses and port numbers. Based on prior experience we only group IP addresses into object groups, not port numbers; on the other hand, we do group all IP addresses into object groups. This means that all access list entries refer to the hosts by a descriptive object group name. This makes it easier to remember the purpose of any particular access list entry.

Here are some of the object groups used during solution testing:

```
object-group network 6608-GWS
 description *** 6608 gateways ***
object-group network 6624-GWS
 description *** 6624 gateways ***
object-group network ACCESS-SWITCH
 description *** Access switches for CER ***
object-group network AD-SRVR
 description *** Active Directory Server ***
object-group network ARC-SERVER
 description *** Attendant Console Server ***
object-group network CA-SRVR
 description *** Certificate Authority ***
object-group network LOCAL-CER
 description *** Local Cisco Emergency Response server ***
object-group network REMOTE-CER
 description *** Remote Cisco Emergency Response server (not CoW) ***
object-group network COW-CUCCX
 description *** All remote CUCCX servers belonging to this cluster (leave empty if not doing CoW)
object-group network COW-CUCM
 description *** All remote CUCMs belonging to this cluster (leave empty if not doing CoW) ***
object-group network COW-CUCM-SUB
 description *** Remote CUCM subscribers belonging to this cluster (leave empty if not doing CoW)
object-group network COW-CUCM-TFTP
 description *** Remote CUCM TFTP servers belonging to this cluster (leave empty if not doing CoW)
object-group network CSA-MC
 description *** All CUCM servers at this site ***
object-group network CUCCX
 description *** Contact Center Express Servers ***
object-group network CUCCX-CLIENT
 description *** Contact Center Express Clients ***
object-group network CUCME
```

```
 description *** CallManager Express devices ***
object-group network CUE
 description *** Cisco Unity Express ***
object-group network LOCAL-CUP
 description *** Local Presence Servers ***
object-group network DHCP-SRVR
 description *** DHCP Servers ***
object-group network DNS-SRVR
 description *** DNS Servers ***
object-group network EVERYONE
 description *** All internal IP addresses ***
object-group network EXCHANGE
 description *** Exchange servers ***
object-group network GATEKEEPER
 description *** H.323 Gatekeepers ***
object-group network H323-GWS
 description *** H323 Gateways ***
object-group network IP-PHONES
 description *** IP Phones, including Phone Proxy (not soft clients) ***
object-group network IPSEC-GWS
 description *** IPSec Gateways ***
object-group network LOCAL-CUCM
 description *** All CUCM servers at this site ***
object-group network LOCAL-CUCM-CTFTP
 description *** CUCM Centralized TFTP servers at this site ***
object-group network LOCAL-CUCM-MOH
 description *** CUCM MOH servers at this site ***
object-group network LOCAL-CUCM-PUB
 description *** CUCM publishers at this site ***
object-group network LOCAL-CUCM-SUB
 description *** CUCM subscribers at this site ***
object-group network LOCAL-CUCM-TFTP
 description *** CUCM TFTP servers at this site ***
object-group network MEDIA-RESOURCES
 description *** MTP, Transcoders, Conference Bridges, including SW media resources on CUCM ***
object-group network MGCP-GWS
 description *** MGCP Gateways ***
object-group network MOH-MULTICAST
 description *** Multicast Music-on-Hold addresses ***
object-group network MP-APP-SRVR
 description *** MeetingPlace Application Server ***
object-group network MP-WEB
 description *** MeetingPlace Web Server ***
object-group network NETMGMT-SRVR
 description *** Generic Network Management Servers ***
object-group network NTP-SRVR
 description *** NTP Servers ***
object-group network OCS
 description *** Microsoft Office Communications Server ***
object-group network PC-VLANS
 description *** Soft clients ***
object-group network REMOTE-CUCM
 description *** CUCMs remote sites (not CoW!) ***
object-group network REMOTE-CUCM-SUB
 description *** CUCM subscribers at remote sites (not CoW!) ***
object-group network REMOTE-CUCM-TFTP
 description *** CUCM TFTP servers at remote sites (not CoW!) ***
object-group network REMOTE-CUP
 description *** Remote Presence Servers (not CoW!) ***
object-group network SAMETIME-SRVR
 description *** Sametime server ***
object-group network SCCP-GWS
 description *** SCCP gateways ***
object-group network SIP-GWS
```

```
 description *** SIP gateways, including proxies ***
object-group network SMTP-SRVR
 description *** Email Servers ***
object-group network SYSLOG-SRVR
 description *** Syslog Servers ***
object-group network UMG
 description *** Cisco Unified Messaging Gateway ***
object-group network UNITY
 description *** Unity ***
object-group network UNITY-CONNECTION
 description *** Unity Connection ***
object-group network WCS
 description *** Wireless Control System ***
object-group network WLAN-CONTROLLER
 description *** WLAN Controller ***
```

Note: The following access-list examples are intended as a starting point, not as a guaranteed and complete solution. Unified Communications solution testing does not include explicit test cases to verify the accuracy of these ACL entries. Our aim is to execute test cases that verify Unified Communications functionality (as opposed to security) with these ACL entries and thus provide implicit verification. Accordingly, the ports allowed by these ACL entries allow ports that we believe were needed to execute our test cases. A different Unified Communications environment may require more or fewer open ports.

Cisco Unified Communication Manager and Phones

The following entries allow both SCCP and SIP, and both secure and non-secure phones to register to the CUCM. In a real deployment typically only one or two of these would be needed. Also, these port numbers are configurable. In the above example, port 2443 is used for secure SCCP and port 5061 is used for Secure SIP.

```
access-list GLOBAL-ACL extended permit udp object-group IP-PHONES object-group LOCAL-CUCM-TFTP eq
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq 2
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq 2
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq 2
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM eq 3804
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq s
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq 5
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group IP-PHONES eq s
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group IP-PHONES eq 5
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq 8
access-list GLOBAL-ACL extended permit udp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq s
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group IP-PHONES eq s
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group LOCAL-CUCM-SUB eq c
```

Cisco Unified Communication Manager and Soft Clients

```
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq 24
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM eq 3804
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq si
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq 50
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq 50
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group PC-VLANS eq si
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group PC-VLANS eq 50
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group PC-VLANS eq 50
access-list GLOBAL-ACL extended permit udp object-group PC-VLANS object-group LOCAL-CUCM-TFTP eq t
access-list GLOBAL-ACL extended permit udp object-group PC-VLANS object-group LOCAL-CUCM-SUB eq si
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group PC-VLANS eq si
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group PC-VLANS eq ww
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM eq 8080
```

```
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM eq ctiqbe
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group PC-VLANS eq 8080
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group PC-VLANS eq ctiqbe
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM eq 8443
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUCM eq www
```

Multicast Music on Hold

```
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-MOH object-group MOH-MULTICAST
```

The above line is used where Music on Hold is sent via multicast. The MOH-MULTICAST object group holds the multicast address(es) to which MoH is sent. See also the Media sources in data center section.

Media sources in data center

```
access-list GLOBAL-ACL extended permit udp object-group DC-MEDIA-SOURCES object-group EVERYONE ran
```

This is the solution for the generic problem that sometimes the firewall is not able to inspect the signaling that carries the media port numbers. This usually happens in a Clustering over the WAN setup where the relevant signaling would be the proprietary intracluster communication that the firewall cannot inspect even if it goes through the firewall.

H.323 Gateways and gatekeepers

```
access-list GLOBAL-ACL extended permit tcp object-group H323-GWS object-group LOCAL-CUCM-SUB eq h3
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group H323-GWS eq h3
access-list GLOBAL-ACL extended permit tcp object-group H323-GWS object-group COW-CUCM-SUB eq h323
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM-SUB object-group H323-GWS eq h323
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group GATEKEEPER eq
access-list GLOBAL-ACL extended permit udp object-group COW-CUCM-SUB object-group GATEKEEPER eq 17
access-list GLOBAL-ACL extended permit tcp object-group GATEKEEPER object-group GATEKEEPER eq 1718
access-list GLOBAL-ACL extended permit tcp object-group GATEKEEPER object-group GATEKEEPER eq 1719
access-list GLOBAL-ACL extended permit tcp object-group GATEKEEPER object-group GATEKEEPER eq h323
access-list GLOBAL-ACL extended permit udp object-group GATEKEEPER object-group GATEKEEPER eq 1718
access-list GLOBAL-ACL extended permit udp object-group GATEKEEPER object-group GATEKEEPER eq 1719
access-list GLOBAL-ACL extended permit udp object-group GATEKEEPER object-group GATEKEEPER eq 1720
```

SCCP Gateways

The typical signaling port for SCCP gateways is 2000 for non-secure and 2443 for secure communication. The Catalyst 6608 and 6624 blades have special port requirements, as shown below.

```
access-list GLOBAL-ACL extended permit tcp object-group SCCP-GWS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit tcp object-group SCCP-GWS object-group LOCAL-CUCM-SUB eq 24
access-list GLOBAL-ACL extended permit tcp object-group 6608-GWS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit tcp object-group 6608-GWS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit udp object-group 6608-GWS object-group LOCAL-CUCM-TFTP eq t
access-list GLOBAL-ACL extended permit tcp object-group 6624-GWS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit tcp object-group 6624-GWS object-group LOCAL-CUCM-SUB eq 20
access-list GLOBAL-ACL extended permit tcp object-group SCCP-GWS object-group COW-CUCM-SUB eq 2000
access-list GLOBAL-ACL extended permit tcp object-group 6608-GWS object-group COW-CUCM-SUB eq 2000
access-list GLOBAL-ACL extended permit tcp object-group 6608-GWS object-group COW-CUCM-SUB eq 2001
access-list GLOBAL-ACL extended permit tcp object-group 6624-GWS object-group COW-CUCM-SUB eq 2000
access-list GLOBAL-ACL extended permit tcp object-group 6624-GWS object-group COW-CUCM-SUB eq 2002
```

MGCP Gateways

```
access-list GLOBAL-ACL extended permit udp object-group MGCP-GWS object-group LOCAL-CUCM-SUB eq 24
access-list GLOBAL-ACL extended permit tcp object-group MGCP-GWS object-group LOCAL-CUCM-SUB eq 24
access-list GLOBAL-ACL extended permit udp object-group MGCP-GWS object-group LOCAL-CUCM-TFTP eq t
access-list GLOBAL-ACL extended permit udp object-group MGCP-GWS object-group COW-CUCM-SUB eq 2427
access-list GLOBAL-ACL extended permit tcp object-group MGCP-GWS object-group COW-CUCM-SUB eq 2428
access-list GLOBAL-ACL extended permit udp object-group MGCP-GWS object-group COW-CUCM-TFTP eq tft
```

SIP Gateways

```
access-list GLOBAL-ACL extended permit tcp object-group SIP-GWS object-group LOCAL-CUCM-SUB range
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group SIP-GWS range
access-list GLOBAL-ACL extended permit udp object-group SIP-GWS object-group LOCAL-CUCM-SUB eq sip
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group SIP-GWS eq sip
access-list GLOBAL-ACL extended permit tcp object-group SIP-GWS object-group REMOTE-CUCM-SUB range
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group SIP-GWS range
access-list GLOBAL-ACL extended permit udp object-group SIP-GWS object-group REMOTE-CUCM-SUB eq si
access-list GLOBAL-ACL extended permit udp object-group REMOTE-CUCM-SUB object-group SIP-GWS eq si
```

IPSec Gateways

```
access-list GLOBAL-ACL extended permit esp object-group IPSEC-GWS object-group LOCAL-CUCM
access-list GLOBAL-ACL extended permit esp object-group LOCAL-CUCM object-group IPSEC-GWS
access-list GLOBAL-ACL extended permit udp object-group IPSEC-GWS eq isakmp object-group LOCAL-CUC
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM eq isakmp object-group IPSEC-GW
access-list GLOBAL-ACL extended permit udp object-group IPSEC-GWS object-group EVERYONE range 1638
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group IPSEC-GWS range 1638
```

Media Resources

```
access-list GLOBAL-ACL extended permit tcp object-group MEDIA-RESOURCES object-group LOCAL-CUCM-SU
access-list GLOBAL-ACL extended permit tcp object-group MEDIA-RESOURCES object-group LOCAL-CUCM-SU
```

SIP ICT

```
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group LOCAL-CUCM-SU
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group LOCAL-CUCM-SU
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group REMOTE-CUCM-SU
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group REMOTE-CUCM-SU
access-list GLOBAL-ACL extended permit udp object-group REMOTE-CUCM-SUB object-group LOCAL-CUCM-SU
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group REMOTE-CUCM-SU
```

Extension Mobility Cross Cluster (EMCC)

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group REMOTE-CUCM eq 808
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM object-group LOCAL-CUCM eq 808
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group REMOTE-CUCM eq 844
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM object-group LOCAL-CUCM eq 844
```

H.323 ICT

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group REMOTE-CUCM-SU
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group LOCAL-CUCM-SU
```

SAF

```
access-list GLOBAL-ACL extended permit eigrp object-group SAF-FORWARDERS object-group SAF-FORWARDE
access-list GLOBAL-ACL extended permit tcp object-group SAF-CLIENTS object-group SAF-FORWARDERS eq
```

```
access-list GLOBAL-ACL extended permit tcp object-group SAF-FORWARDERS object-group SAF-CLIENTS eq
```

SIP Trunk to/from CUCME

```
access-list GLOBAL-ACL extended permit tcp object-group CUCME-SIP object-group LOCAL-CUCM-SUB rang
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group CUCME-SIP rang
access-list GLOBAL-ACL extended permit udp object-group CUCME-SIP object-group LOCAL-CUCM-SUB eq s
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group CUCME-SIP eq s
```

H.323 Trunk to/from CUCME

```
access-list GLOBAL-ACL extended permit tcp object-group CUCME-H323 object-group LOCAL-CUCM-SUB eq
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group CUCME-H323 eq
```

Centralized TFTP

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-CTFTP object-group REMOTE-CUCM-
```

SMTP server

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group SMTP-SRVR eq smtp
```

User Access to Cisco Unified Communication Manager

```
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group LOCAL-CUCM-PUB eq ww
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group LOCAL-CUCM-PUB eq 80
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group LOCAL-CUCM-PUB eq ht
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group LOCAL-CUCM-PUB eq 84
```

Cisco Unified Communication Manager Intracluster (Clustering over WAN) Communication

The following entries are only needed if some nodes in of the CUCM cluster are separated from the rest of the cluster by the firewall. This typically happens in Clustering over WAN setups.

```
access-list GLOBAL-ACL extended permit udp object-group COW-CUCM object-group LOCAL-CUCM-PUB eq nt
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq ssh
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 1090
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 1099
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 1500
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 1501
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 1515
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 2552
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 2551
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 2555
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 2556
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 4040
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 5007
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 5555
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 7000
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 7070
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8001
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8002
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8003
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8004
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8005
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8443
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8500
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8888
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM object-group LOCAL-CUCM eq 8889
access-list GLOBAL-ACL extended permit udp object-group COW-CUCM object-group LOCAL-CUCM eq syslog
```

```
access-list GLOBAL-ACL extended permit udp object-group COW-CUCM object-group LOCAL-CUCM eq 8500
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq ssh
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 1090
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 1099
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 1500
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 1501
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 1515
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 2552
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 2551
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 2555
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 2556
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 4040
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 5007
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 5555
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 7000
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 7070
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8001
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8002
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8003
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8004
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8005
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8443
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8500
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8888
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM object-group COW-CUCM eq 8889
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM object-group COW-CUCM eq syslog
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM object-group COW-CUCM eq 8500
```

Intercompany Media Engine (IME)

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group IME-SRVR eq 56
access-list GLOBAL-ACL extended permit tcp object-group IME-ASA-OFFPATH-SIGNALING object-group LOC
access-list GLOBAL-ACL extended permit tcp object-group IME-ASA-OFFPATH-SIGNALING object-group LOC
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group IME-ASA-OFFPAI
access-list GLOBAL-ACL extended permit udp object-group IME-ASA-OFFPATH-MEDIA object-group EVERYON
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group IME-ASA-OFFPATH-MEDI
```

Unity

```
access-list GLOBAL-ACL extended permit tcp object-group UNITY object-group IP-PHONES eq www
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group UNITY eq 120
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group UNITY eq 121
```

Unity Connection

```
access-list GLOBAL-ACL extended permit udp object-group UNITY-CONNECTION object-group SIP-GWS eq s
access-list GLOBAL-ACL extended permit tcp object-group UNITY-CONNECTION object-group CUCME-SIP eq
access-list GLOBAL-ACL extended permit tcp object-group UNITY-CONNECTION object-group CUCME-H323 e
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group UNITY-CONNECTION eq
```

Cisco Unity Express

```
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group LOCAL-CUCM-SUB eq www
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group LOCAL-CUCM-SUB eq ctiqbe
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group LOCAL-CUCM-SUB eq 2789
```

```
access-list GLOBAL-ACL extended permit udp object-group CUE object-group LOCAL-CUCM-SUB eq sip
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCM-SUB object-group CUE eq sip
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group LOCAL-CUCM-SUB eq sip
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group CUE eq sip
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group UNITY-CONNECTION eq www
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group UNITY-CONNECTION eq smtp
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group UNITY eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UNITY-CONNECTION object-group CUE eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UNITY object-group CUE eq smtp
```

Unified Messaging Gateway

```
access-list GLOBAL-ACL extended permit tcp object-group UMG object-group UNITY-CONNECTION eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UMG object-group UNITY eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UMG object-group CUE eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UMG object-group UMG eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UMG object-group UMG eq www
access-list GLOBAL-ACL extended permit tcp object-group UNITY-CONNECTION object-group UMG eq smtp
access-list GLOBAL-ACL extended permit tcp object-group UNITY object-group UMG eq smtp
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group UMG eq smtp
access-list GLOBAL-ACL extended permit tcp object-group CUE object-group UMG eq www
```

Meeting Place

```
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group MP-WEB eq www
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group MP-WEB eq https
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group MP-WEB eq 1503
access-list GLOBAL-ACL extended permit tcp object-group EVERYONE object-group MP-WEB eq 1627
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq www
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq https
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq h323
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq 1503
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq 1627
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq 5003
access-list GLOBAL-ACL extended permit tcp object-group MP-WEB object-group MP-APP-SRVR eq 5005
access-list GLOBAL-ACL extended permit udp object-group MP-WEB object-group MP-APP-SRVR eq ntp
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq www
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq https
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq h323
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq 1503
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq 1627
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq 5003
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group MP-WEB eq 5005
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group LOCAL-CUCM-SUB eq
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCM-SUB object-group MP-APP-SRVR eq
access-list GLOBAL-ACL extended permit tcp object-group MP-APP-SRVR object-group COW-CUCM-SUB eq s
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCM-SUB object-group MP-APP-SRVR eq s
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
access-list GLOBAL-ACL extended permit udp object-group REMOTE-CUCM-SUB object-group MP-APP-SRVR e
```

Contact Center Express Agents

```
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 7
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 8
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 8
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 1
```

```
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 1
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 1
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 4
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 6
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 6
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 8
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 9
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 1
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX rang
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 6
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq h
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS eq 3
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUP eq 844
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUP eq sip
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUP object-group CUCCX-AGENTS eq sip
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX range 24576 32767 object-group
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group LOCAL-CUCCX range 24
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group LOCAL-CUCCX range 32
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX rang
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX rang
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX rang
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 3
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 6
access-list GLOBAL-ACL extended permit udp object-group CUCCX-AGENTS object-group LOCAL-CUCCX rang
access-list GLOBAL-ACL extended permit tcp object-group CUCCX-AGENTS object-group LOCAL-CUCCX eq 1
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS rang
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS eq 6
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS eq 5
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS eq 5
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS eq 5
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group CUCCX-AGENTS rang
```

Contact Center Express Intracluster (Clustering over WAN) Communication

```
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 7
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 7
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1090
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1090
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1099
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1099
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1500
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1500
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1504
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1504
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1515
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1515
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1990
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1990
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1994
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1994
access-list GLOBAL-ACL extended permit udp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1996
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1996
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 2555
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 2555
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 2556
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 2556
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 4040
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 4040
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 4160
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 4160
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 6293
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 6293
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 8080
```

```
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 8080
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 6295
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 6295
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 6999
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 6999
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 8001
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 8001
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 8443
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 8443
access-list GLOBAL-ACL extended permit udp object-group COW-CUCCX object-group LOCAL-CUCCX eq 8500
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX object-group COW-CUCCX eq 8500
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 8500
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 8500
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 9080
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 9080
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 1202
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 1202
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX range 3
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX range 3
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 6553
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 6553
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq ssh
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX range 3
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCCX eq 3016
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX object-group COW-CUCCX eq ntp
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX object-group COW-CUCCX eq 4160
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUCCX object-group COW-CUCCX range 3
access-list GLOBAL-ACL extended permit udp object-group COW-CUCCX object-group LOCAL-CUCCX range 3
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCM eq www
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCM range ct
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCM eq 8443
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCM eq www
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCM range ct
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUCCX object-group COW-CUCM eq 8443
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq ssh
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX range 3
access-list GLOBAL-ACL extended permit tcp object-group COW-CUCCX object-group LOCAL-CUCCX eq 3016
access-list GLOBAL-ACL extended permit udp object-group COW-CUCCX object-group LOCAL-CUCCX eq ntp
access-list GLOBAL-ACL extended permit udp object-group COW-CUCCX object-group LOCAL-CUCCX eq 4160
```

CUCME to CUCCX

```
access-list GLOBAL-ACL extended permit tcp object-group CUCME-SIP object-group LOCAL-CUCCX eq 5062
access-list GLOBAL-ACL extended permit tcp object-group CUCME-H323 object-group LOCAL-CUCCX eq 506
```

Attendant Console

```
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1859
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 11859
access-list GLOBAL-ACL extended permit tcp object-group IP-PHONES object-group ARC-SERVER eq 80
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 80
access-list GLOBAL-ACL extended permit tcp object-group ARC-SERVER object-group IP-PHONES eq 80
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1862
access-list GLOBAL-ACL extended permit tcp object-group ARC-SERVER object-group LOCAL-CUCM-SUB eq
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1433
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1434
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1863
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group ARC-SERVER eq 1864
access-list GLOBAL-ACL extended permit tcp object-group ARC-SERVER object-group CUPS eq 5060
access-list GLOBAL-ACL extended permit tcp object-group CUPS object-group ARC-SERVER eq 5060
```

Presence

```
access-list GLOBAL-ACL extended permit tcp object-group SIP-GWS object-group LOCAL-CUP eq 5060
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUP object-group SIP-GWS eq 5060
access-list GLOBAL-ACL extended permit udp object-group SIP-GWS object-group LOCAL-CUP eq 5060
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CUP object-group SIP-GWS eq 5060
access-list GLOBAL-ACL extended permit tcp object-group SIP-GWS object-group LOCAL-CUP eq 5061
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUP object-group SIP-GWS eq 5062
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 5222
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 8082
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 8083
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 8080
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 8332
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group LOCAL-CUP eq 7335
access-list GLOBAL-ACL extended permit tcp object-group EXCHANGE object-group LOCAL-CUP eq 50020
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUP object-group NETMGMT-SRVR eq 109
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CUP object-group NETMGMT-SRVR eq 109
```

Sametime

```
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group SAMETIME-SRVR eq 153
```

OCS and MOC

```
access-list GLOBAL-ACL extended permit tcp object-group OCS object-group PC-VLANS range sip 5062
access-list GLOBAL-ACL extended permit tcp object-group OCS object-group PC-VLANS eq 8080
access-list GLOBAL-ACL extended permit tcp object-group OCS object-group PC-VLANS eq ctiqbe
access-list GLOBAL-ACL extended permit tcp object-group OCS object-group PC-VLANS eq 5900
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group OCS range sip 5062
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group OCS eq 8080
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group OCS eq ctiqbe
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group OCS eq 5900
```

1040 Sensors

```
access-list GLOBAL-ACL extended permit tcp object-group 1040-SENSOR object-group NETMGMT-SRVR eq 2
access-list GLOBAL-ACL extended permit udp object-group 1040-SENSOR object-group NETMGMT-SRVR eq t
access-list GLOBAL-ACL extended permit udp object-group 1040-SENSOR object-group NETMGMT-SRVR eq 5
access-list GLOBAL-ACL extended permit object-group NETMGMT-SRVR tcp object-group 1040-SENSOR eq 8
```

Wireless

```
access-list GLOBAL-ACL extended permit udp object-group WCS object-group WLAN-CONTROLLER eq snmp
access-list GLOBAL-ACL extended permit udp object-group WLAN-CONTROLLER object-group WCS eq snmptr
```

Cisco Emergency Response

```
access-list GLOBAL-ACL extended permit udp object-group LOCAL-CER object-group ACCESS-SWITCH eq sn
access-list GLOBAL-ACL extended permit udp object-group ACCESS-SWITCH object-group LOCAL-CER eq sn
access-list GLOBAL-ACL extended permit tcp object-group LOCAL-CER object-group REMOTE-CER eq 8443
access-list GLOBAL-ACL extended permit tcp object-group REMOTE-CER object-group LOCAL-CER eq 8443
```

PC's to CVTA port on phone

```
access-list GLOBAL-ACL extended permit tcp object-group PC-VLANS object-group IP-PHONES eq 4224
access-list GLOBAL-ACL extended permit udp object-group PC-VLANS object-group IP-PHONES eq 5445
access-list GLOBAL-ACL extended permit udp object-group IP-PHONES object-group PC-VLANS eq 5445
```

Generic network management access

```
access-list GLOBAL-ACL extended permit udp object-group NETMGMT-SRVR object-group EVERYONE eq snmp
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group NETMGMT-SRVR eq snmp
access-list GLOBAL-ACL extended permit tcp object-group NETMGMT-SRVR object-group EVERYONE eq ssh
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group NETMGMT-SRVR eq tftp
access-list GLOBAL-ACL extended permit tcp object-group NETMGMT-SRVR object-group EVERYONE eq www
access-list GLOBAL-ACL extended permit tcp object-group NETMGMT-SRVR object-group EVERYONE eq 8080
access-list GLOBAL-ACL extended permit tcp object-group NETMGMT-SRVR object-group EVERYONE eq 8443
access-list GLOBAL-ACL extended permit udp object-group EVERYONE object-group NETMGMT-SRVR eq sysl
access-list GLOBAL-ACL extended permit tcp object-group NETMGMT-SRVR object-group EVERYONE eq http
```

Related Documentation

For related information on Cisco ASA 5500 Series Adaptive Security Appliance installation and configuration, see:

1. Cisco ASA 5500 Series Install and Upgrade Guides
2. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3
3. Cisco ASA 5500 Series Configuration Guide using ASDM, 8.3

For design guidelines, see:

1. Voice Security chapter of the Cisco Unified Communications System Release 8.x SRND.
2. Data Center Security Design Guides.

For port usage guidelines for various products, see:

1. Cisco Unified Communications Manager 8.0(2) TCP and UDP Port Usage
2. Cisco Intercompany Media Engine 8.0(2) TCP and UDP Port Usage
3. Port Usage for Cisco Unified Presence Release 8.0
4. Port Utilization Guide for Cisco Unified CCX and Cisco Unified IP IVR, Release 8.0(1)
5. Cisco Unified Business/Department/Enterprise Attendant Console - Design Guide (Page 8-7)
6. Port Usage in Cisco ER

For IP telephony configuration articles and test results, see:

1. IP Telephony Test Results
2. IP Telephony System Configurations