APPENDIX D

Firewall and NAT Rules for the Cisco Unified Videoconferencing Solution

Firewall Rules

This section describes firewall rules used for the simplest and most typical firewall configuration.

Table D-1 presents general firewall rules that comply with the guidelines described in the "Firewall Configuration Guidelines" section on page 3-26.

Table D-1 General Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	Any	LAN networks	Any	DMZ net, outside networks	Any	Allowing any kind of traffic from the private network to the DMZ or outside networks (for example, the Internet).
Block	Any	Outside networks	Any	LAN networks, DMZ network	Any	Blocking any kind of traffic to the protected networks (DMZ and internal network).
Block	Any	DMZ network	Any	LAN networks	Any	Blocking any kind of traffic from the DMZ to the private network.

Table D-2 describes rules that you must add to enable connectivity between the Internal Gatekeeper located in the DMZ and the MCU components located on the internal network.

Table D-2 Gatekeeper-to-MCU Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Gatekeeper IP address as it appears in the DMZ	Any	MCU IP address	1025 - 65535	TCP High ports from Gatekeeper to MCU on the LAN. Enables H.245 control signaling channels to be opened.
Pass	TCP	Gatekeeper IP address as it appears in the DMZ	Any	MCU IP address	1720	H.323 signaling to MCU on the LAN. Enables call setup signaling between the Internal Gatekeeper and the MCUs.

Table D-3 describes rules that you must add to enable connectivity between the internal Cisco Unified Videoconferencing Manager located on the DMZ and the Cisco Unified Videoconferencing 3500 MCU located on the internal network.

Table D-3 Cisco Unified Videoconferencing Manager-to-MCU Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco Unified Videoconferencing Manager IP address as it appears on the DMZ	Any	Cisco Unified Videoconferencing Desktop Server IP address	3340	Login (XML) to MCU on the LAN. Enables XML management interface connectivity between the Cisco Unified Videoconferencing Manager and the Cisco Unified Videoconferencing Desktop Server.
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears on the DMZ	Any	Cisco Unified Videoconferencing 3500 MCU IP address	161	SNMP from Cisco Unified Videoconferencing Manager to Cisco Unified Videoconferencing 3500 MCU on the LAN. Enables SNMP management interface connectivity between the Cisco Unified Videoconferencing Manager and the Cisco Unified Videoconferencing 3500 MCU components.

Table D-4 describes a rule that you must add to enable connectivity between the Internal Gatekeeper located on the DMZ and Cisco Unified Videoconferencing 3500 Series Gateway components located on the private network.

Table D-4 Cisco IOS H.323 Gatekeeper-to-gateway Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Gatekeeper IP address as it appears on the DMZ	Any	Cisco Unified Videoconferencing 3500 Series Gateway IP address	1025 - 65535	TCP High ports from Gatekeeper to GW320 on the LAN. Enables H.245 control signaling channels to be opened.

Table D-5 describes rules that you must add to enable a Desktop Client to invite a room system located on the private network.

Table D-5 Gatekeeper-to-endpoint Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Gatekeeper IP address as it appears on the DMZ	Any	Room system IP address as it appears on the private network	1720	H.323 signaling to a room system on the LAN. Enables call setup signaling between the Internal Gatekeeper and room systems.
Pass	TCP	Gatekeeper IP address as it appears on the DMZ	Any	Room system IP address as it appears on the private network	1025 - 65535	TCP High ports from Gatekeeper to room system on the LAN. Enables H.245 control signaling channels to be opened.

Table D-6 describes rules that you must add to enable connectivity between the internal Cisco Unified Videoconferencing Manager located on the DMZ and MCU components located on the internal network.

Table D-6 Cisco Unified Videoconferencing Manager-to-gateway Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	TCP	Cisco Unified Videoconferencing Manager IP address as it appears on the DMZ	Any	GW IP address	1820	H.323 Signaling from Gatekeeper to GW320 on the LAN. Enables call setup signaling between the Internal Gatekeeper and the Cisco Unified Videoconferencing 3500 Series Gateways.
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears on the DMZ	Any	GW IP address	161	SNMP from Cisco Unified Videoconferencing Manager to gateway on the LAN. Enables SNMP management interface connectivity between the Cisco Unified Videoconferencing Manager and the gateway components.

Table D-7 describes rules that you must add to enable connectivity between the internal Cisco Unified Videoconferencing Manager located on the DMZ and MCU components located on the internal network.

Table D-7 Desktop-to-MCU Traffic Firewall Rules

Action	Protocol	Source	Port	Destination	Port	Description
Pass	UDP	Cisco Unified Videoconferencing Manager IP address as it appears on the DMZ	Any	Cisco Unified Videoconferencing Desktop Server IP address	1025-65535	Media connection between the Desktop and MCU. Also open ports between the Cisco Unified Videoconferencing Desktop Server and the EMP. To avoid a conflict with SIP traffic, limit the port range by setting the value opening the range to 10,000 or higher. For operational information about configuring ports, see Configuration Guide for Cisco Unified Videoconferencing Manager.
Pass	UDP	Desktop	Any	MCU	2326-65535	Limit UDP ports opened on the firewall to allow Desktop to send RTP to the internal network (MCU). We recommend that you use a limited range between 2326 and 65535. If this option is used: • Each Client-to-Desktop connection uses 2 UDP ports. • Each Cisco Unified Videoconferencing Desktop Server-to-MCU connection uses UDP ports. Reserve 11 ports per user. To define the range, multiply the number of connections allowed by your license by 11. In addition, 6 UDP ports each are required for: • Every conference with Desktop users. • every recording channel.

NAT Rules

Table D-8 describes static NAT entries in the firewall WAN interface that you must configure to enable connectivity between the Desktop Clients located on the external networks and the Cisco Unified Videoconferencing Desktop Servers located in the DMZ.

Table D-8 NAT Rules defining traffic from Desktop Clients to Web Services

Protocol	External Port Range	NAT IP	Internal Port Range	Description
TCP	80 (HTTP)	Cisco Unified Videoconferencing Desktop Server IP address as it appears on the DMZ	80 (HTTP)	For external Desktop Client web access. Alternatively you can configure the Desktop Clients to connect via TCP port 443. For more information about configuring TCP port 443, see "Configuring Secure Connection Between Cisco Unified Videoconferencing Solution Components" section on page A-1.
TCP	443 (HTTPS)	Cisco Unified Videoconferencing Desktop Server IP address as is appears on the DMZ	443 (HTTPS)	Control connection between Cisco Unified Videoconferencing Desktop Server and Desktop Client (mandatory).
TCP	8080	Cisco Unified Videoconferencing Manager Cisco Unified Videoconferencing Desktop Server IP address as is appears on the DMZ	8080	For external Desktop Client web access to a virtual room configuration. Enables Desktop Client access to Cisco Unified Videoconferencing Manager virtual room settings.

Table D-9 on page D-5 describes a static NAT entry in the firewall WAN interface that you must add to enable connectivity between the Desktop Web Cast clients located on the external networks and the Cisco Unified Videoconferencing Streaming Server located on the DMZ.

Table D-9 NAT Rules defining traffic from Desktop Webcast Clients to the Cisco Unified Videoconferencing Streaming Server

Protocol	External Port Range	NAT IP	Internal Port Range	Description
TCP	7070	Cisco Unified Videoconferencing Streaming Server IP as appears on the DMZ	7070	Streaming tunneling connection enables the Web Cast client to access the streamed conference.

Table D-9 on page D-5 describes a static NAT entry in the firewall WAN interface that you must add to enable connectivity between the Desktop Web Cast clients located on the external networks and the Cisco Unified Videoconferencing Streaming Server located on the DMZ.

Table D-10 NAT Rules defining traffic from Desktop Webcast Clients to the Cisco Unified Videoconferencing Desktop Server

Protocol	External Port Range	NAT IP	Internal Port Range	Description
TCP	Any	Cisco Unified Videoconferencing Desktop Server IP as appears on the DMZ	1025-65535	Media connection between the Desktop Client and Cisco Unified Videoconferencing Desktop Server. If not open, the connection will be tunneled via TCP port 443 effecting performance. To avoid a conflict with SIP traffic, limit the port range by setting the value opening the range to 10,000 or higher. For operational information about configuring ports, see Configuration Guide for Cisco Unified Videoconferencing Manager.