

Appendix 3 – NAT & firewall configuration

NAT device configuration requirement

For more information regarding port usage refer to the Cisco VCS Deployment Guide - Cisco VCS IP port usage for firewall traversal (X4 and X5) or the Cisco VCS Administrator Guide for port usage information.

Internal firewall configuration

In this example, it is assumed that outbound connections (from internal network to DMZ) are all permitted by the NAT device.

As Cisco VCS Control to Cisco VCS Expressway communications are always initiated from Cisco VCS Control to Cisco VCS Expressway (Cisco VCS Expressway sending messages by responding to Cisco VCS Control's messages) no ports need to be opened from DMZ to Internal for call handling.

Note: ensure that any SIP or H.323 'fixup' ALG or awareness functionality is disabled on the NAT firewall – if enabled this will adversely interfere with the Cisco VCS functionality.

If a Syslog logging server and a Cisco TMS server are deployed (see the Optional configuration steps section) then the following NAT configuration will be required:

Inbound (DMZ > Internal network)

Purpose	Source	Destination	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Logging	VCSe	Syslog server	192.0.2.2	40000 to 49999	UDP	10.0.0.13	514
Management	VCSe	TMS server	192.0.2.2	>=1024	TCP	10.0.0.14	80/443

Note: traffic destined for the Logging and Management server addresses (using specific destination ports) needs to be routed to the internal network.

External firewall configuration requirement

In this example it is assumed that outbound connections (from DMZ to external network) are all permitted by the Firewall device.

Note: ensure that any SIP or H.323 'fixup' ALG or awareness functionality is disabled on the NAT firewall – if enabled this will adversely interfere with the Cisco VCS functionality.

Inbound (Internet > DMZ)

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 Endpoints registering with Assent							
RAS Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	1719
Q.931/H.225 and H.245	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	2776
RTCP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	2777
RTP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	2776
SIP Endpoints registering using UDP / TCP or TLS							
SIP TCP	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	5060
SIP TLS	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	5061
RTP & RTCP	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	50000 to 52399

Note: it is assumed that remote H.323 devices are registering using the Assent protocol. If the devices are registering using H.460 18/19 please refer to the Cisco VCS Deployment Guide - Cisco VCS IP port usage for firewall traversal (X4 and X5) or the Cisco VCS Administrator Guide for port usage information.