When the LAN interface is in a private IP DMZ, you can write the firewall rule-set to restrict the number of hosts the VBP can communicate with to only those devices. This enhances security. You can also do this by using an ACL on a router on the VBP's LAN side.

Implementing a DMZ with a Private IP Space

If the DMZ has private IP space, install the VBP so that its WAN interface is attached outside of the firewall, with a public IP address assigned, while the LAN interface is in the DMZ. You can control access to the WAN port using either ACLs on the upstream router, or the built-in netfilter package on the VBP itself. You can easily configure the VBP to drop any incoming non-H.323 packet (by disabling LAN NAT), as well as accept H.323 packets from only known sources.

You can route the VBP's LAN interface to the enterprise LAN by using the firewall's DMZ and the rule-set outlined in the above guidelines. Again, this is generally sufficient for security policies, since all communications passes through the trusted third-party security device.

Installing the VBP on a public DMZ port to the WAN or Subscriber interfaces must allow the following ports unmodified to the VBP. The VBP itself is the application firewall for H.323 traffic, and with no calls in progress, the VBP will only be listening on TCP port 1720 for incoming calls. The VBP will provide dynamic H.323 application firewall rules to open and close the associated H.225, H.245 and UDP media ports for each call that successfully passes the TCP port 1720 signaling phase. The VBP will embed the public IP assigned to the WAN or Subscriber interface at Layer 5 to the called or calling endpoint. The VBP will also embed the ports below at Layer 5 as they pertain to the H.323 protocol process for H.225 call setup, H.245 media negotiation, and UDP media handling to and from the calling and called endpoints.

Important: For public Internet connectivity, the VBP E or VBP ST series models must have a publicly routable non-NAT'ed IP address assigned to the WAN or Subscriber-side interface.

A firewall must be configured to allow inbound and outbound H.323 protocols to the VBP, as well as other protocols used by the H.323 devices (such as SNTP) and to manage the VBP (such as SSH, HTTP, HTTPS, Telnet).

Since the VBP is a firewall proxy, all H.323 packets will have a source or destination IP address that is the VBP's Subscriber (VBP-S or ST) or WAN (VBP-E) IP address. You can use this to help set up the appropriate firewall rules.

VBP RTP media ports will always be even numbered (for example, 16386, 16388). Odd numbered ports will be used for RTCP (for example, 16387, 16389). The port ranges will be used in a circular hunt from lowest to highest per platform. The VBP 5300 E-10 and E-25 models do not have a reduced port number that equals the bandwidth model. Therefore, a single port range is used for both models.

Using the VBP in a firewall DMZ configuration, the following protocols are required: RAS, Q.931 (H.225), H.245, and RTP, as specified per platform.

Required Ports

This section contains tables that define the ports that are required to implement a VBP with a third-party firewall. Table 1 defines the ports that the VBP could use, depending on the deployment scenario. Tables 2 to 8 list the ports and directional relationship you need to know to configure a DMZ port filtering rules set in various deployment scenarios.

Table 1

In all cases		
FTP	TCP	21 (optional)
HTTP	TCP	80 (optional for management)
HTTPS	TCP	445 (optional for management, this port is adjustable in the “HTTPS Certificate” page)
HTTPS	TCP	443 (Access Proxy)
XMPP	TCP	5222 (Access Proxy)
LDAP	TCP	389 (Access Proxy)
RTP	UDP	16386 - 17286 (200EW,4300T,4350,4350EW) 16386 - 25386 (5300-E/ST10 and E/ST25) 16386 - 34386 (6400-E/ST and E/ST 85
SNMP	UDP	161 (optional for management)
SSH	TCP	22 (optional for management)
Telnet	TCP	23 (optional for management)
TFTP	UDP	69 (optional)
SNTP	TCP	123 (optional)
H.323 Endpoints		
Q.931 (H.225)	TCP	1720
RAS	UDP	1719
H.245	TCP	14085 -15084

VBP-E DMZ required ports to and from the WAN interface

Table 2 shows the ports required for DMZ port filtering policies applied to the VBP-E WAN interface IP.

VBP-E H.323 Endpoints Specific				
Inbound from the Internet to VBP-E WAN Interface IP				
Internet SRC IP	Internet SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 – 65535	VBP WAN IP	TCP – H.225	1720
Any	1024 - 65535	VBP WAN IP	TCP – H.245	14085 - 15084 (contiguous range)
Any	1024 - 65535	VBP WAN IP	UDP - RTP	16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
				16386 - 34386 (6400-E and S85) (contiguous range)
Outbound to the Internet from VBP-E WAN Interface IP				
VBP SRC IP	VBP SRC Port	Internet DST IP	Proto	Internet DST port
VBP WAN IP	1720	Any	TCP – H.225	1024 – 65535 (Typically H.323 endpoints will use the well known H.225 port 1720)
VBP WAN IP	14085-15084	Any	TCP – H.245	1024 – 65535
VBP WAN IP	16386-17286 or 16386-25386 or 16386-34386	Any	UDP - RTP	1024 – 65535 (note: if the DST endpoint can support a limited port range, set to the endpoints DST media range. It is recommended to verify the solution before applying a granular policy on the DMZ firewall)

VBP-E DMZ required ports inbound to the LAN interface

Table 3 shows the ports required for DMZ port filtering policies applied from the LAN H.323 endpoint to the VBP LAN interface IP. Depending on the mode the VBP is configured in, UDP port 1719 will only be required when using the Embedded or Wan Side gatekeeper modes.

Depending on the H.323 endpoints being supported by the VBP there may be configuration options to limit the TCP H.245 and UDP RTP port ranges. Check with each manufactures endpoint to verify these ports before applying a granular policy to the DMZ firewall.

Table 3

VBP-E H.323 Endpoints Specific				
Inbound from the LAN H.323 endpoint to VBP LAN Interface IP				
LAN SRC IP	LAN SRC Port	VBP DST IP	Proto	VBP DST port
Any	1719	VBP LAN IP	UDP - RAS	1719 (needed if the Embedded gatekeeper is enabled)
Any	1720	VBP LAN IP	TCP - H.225	1720
Any	1024 – 65535 (can be limited depending on the endpoint)	VBP LAN IP	TCP - H.245	14085 - 15084 (contiguous range)
Any	1024 – 65535 (can be limited depending on the endpoint)	VBP LAN IP	UDP - RTP	16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
				16386 - 25386 (5300-E/ST10 and E/ST25) (contiguous range)
				16386 - 34386 (6400-E and E85) (contiguous range)

VBP-E DMZ required ports outbound from the LAN interface

Table 4 shows the ports required for DMZ port filtering policies applied from the VBP LAN interface IP to the LAN H.323 endpoint. Depending on the mode the VBP is configured in, UDP port 1719 will only be required when using the Embedded or Wan Side gatekeeper modes.

Depending on the H.323 endpoints being supported by the VBP there may be configuration options to limit the TCP H.245 and UDP RTP port ranges. Check with each manufactures endpoint to verify these ports before applying a granular policy to the DMZ firewall.

Table 4

VBP-E H.323 Endpoints Specific				
Outbound from VBP LAN Interface IP to the LAN H.323 endpoint				
VBP SRC IP	VBP SRC Port	LAN DST IP	Proto	LAN DST port
VBP LAN IP	1719	Any	UDP - RAS	1719 (needed if the Embedded gatekeeper is enabled)
VBP LAN IP	1720	Any	TCP – H.225	1720
VBP LAN IP	14085 - 15084	Any	TCP – H.245	1024 – 65535 (can be limited depending on the endpoint)
VBP LAN IP	16386-17286 or 16386-25386 or 16386-34386	Any	UDP – RTP	1024 – 65535 (can be limited depending on the endpoint)

VBP-ST DMZ required ports inbound from the Internet to the VBP (H.460 support)

In the scenario of a H.460-capable endpoint at a remote location that is registering to the Subscriber interface of a VBP-ST Series for far end NAT traversal using the H.460 protocol, the H.460-capable endpoint must be able to communicate to the Subscriber interface over the defined destination (DST) ports in table 5:

Please ensure that if there is a firewall between the H.460-capable endpoint and the Subscriber interface, the endpoint can communicate over these ports and protocols. Also, note that H.460 as a standard assumes that there is not an “H.323-helper” style service running on the firewall protecting the H.460 endpoint; if there is such a service running on the firewall, please disable it.

Table 6 will describe the reverse port orientation.

Table 5

VBP-ST H.323 with H.460 support				
Inbound from the Internet to VBP-ST Subscriber Interface IP				
Internet SRC IP	Internet SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 – 65535	VBP WAN IP	UDP - RAS	1719
Any	1024 – 65535	VBP WAN IP	TCP – H.225	1720 (alternate port may be configured in the H.323 page, port 1720 is the default)
Any	1024 - 65535	VBP WAN IP	TCP – H.245	14085 - 15084 (contiguous range)
Any	1024 - 65535	VBP WAN IP	UDP - RTP	16386 - 25386 (5300-E/ST10 and E/ST25) (contiguous range)
				16386 - 34386 (6400-E and ST85) (contiguous range)

VBP-ST DMZ required ports outbound from the VBP to the Internet (H.460 support)

Deploying the H.460 protocol for far end NAT traversal will make predicting the source port the NAT router will use almost impossible as these NAT routers could use any port to PAT (Port Address Translation) or source the request from. For this reason it is not recommended to apply a granular port policy for the destination ports regardless if the endpoint supports a limited UDP RTP port range.

Table 6

VBP-ST H.323 with H.460 support				
Outbound to the Internet from VBP-ST Subscriber Interface IP				
VBP SRC IP	VBP SRC Port	Internet DST IP	Proto	Internet DST port
VBP WAN IP	1719	Any	UDP – RAS	1024 – 65535
VBP WAN IP	1720	Any	TCP – H.225	1024 – 65535
VBP WAN IP	14085 - 15084	Any	TCP – H.245	1024 – 65535
VBP WAN IP	16386-25386 or 16386-34386	Any	UDP – RTP	1024 – 65535

VBP-ST DMZ required ports inbound from the Internet to the VBP (H.460 and Access Proxy)

Deploying the VBP-ST to support the Access Proxy feature will require 3 additional ports as referenced in tables 5 and 6 above.

When the Access Proxy configuration is enabled the CMA Desktop or HDX systems installed at the remote locations will be provisioned to authenticate to the VBP-ST Subscriber IP address. The VBP-ST will provide security to the authentication request by inspecting the HTTP header information after decrypting the TLS HTTPS packet, if the packet passes these security checks the VBP-ST system forwards the request to the CMA server on the Provider or more typically called the LAN interface as a destination port 443 request to the CMA server. The CMA server will perform NTLM authentication challenges to verify the endpoints credentials are valid before forwarding the request to the CMA server.

When the CMA server and CMA Desktop or HDX client has successfully authenticated the VBP-ST will build dynamic iptables firewall rules for the IP address discovered in the original authenticated request, this IP address is typically the NAT routers public IP the request can from.

The iptables rules will be added for the source IP address for TCP port 5222 and TCP port 389 for the duration of the session, during this session keep-alive or heartbeat messages are monitored by the VBP to verify the client is still active for each remote client session. When a remote client becomes unresponsive or not actively sending these messages the system will start an aging process and when timed out remove the iptables firewall rules allowing access to the system.

Table 8 will describe the reverse port orientation.

Table 7

VBP-ST H.323 endpoints Specific with Access Proxy services				
Inbound from the Internet to VBP-ST Subscriber Interface IP				
Internet SRC IP	Internet SRC Port	VBP DST IP	Proto	VBP DST port
Any	1024 – 65535	VBP WAN IP	TCP - HTTPS	443 using TLS
Any	1024 – 65535	VBP WAN IP	TCP - XMPP	5222 using TLS
Any	1024 – 65535	VBP WAN IP	TCP - LDAP	389 using TLS
Any	1024 – 65535	VBP WAN IP	UDP - RAS	1719
Any	1024 – 65535	VBP WAN IP	TCP – H.225	1720
Any	1024 – 65535	VBP WAN IP	TCP – H.245	14085 - 15084 (contiguous range)
Any	1024 – 65535	VBP WAN IP	UDP - RTP	16386 - 25386 (5300-ST10 and ST25) (contiguous range)
				16386 - 34386 (6400-ST85) (contiguous range)

VBP-ST DMZ required ports outbound from the VBP to the Internet (H.460 and Access Proxy)

Table 8

VBP-ST H.323 endpoints Specific with Access Proxy services				
Outbound to the Internet from VBP-ST WAN/Subscriber Interface IP				
VBP SRC IP	VBP SRC Port	Internet DST IP	Proto	Internet DST port
VBP WAN IP	443 using TLS	Any	TCP - HTTPS	1024 - 65535
VBP WAN IP	5222 using TLS	Any	TCP - XMPP	1024 - 65535
VBP WAN IP	389 using TLS	Any	TCP – LDAP	1024 - 65535
VBP WAN IP	1719	Any	UDP – RAS	1024 – 65535
VBP WAN IP	1720	Any	TCP – H.225	1024 – 65535
VBP WAN IP	14085 - 15084	Any	TCP – H.245	1024 - 65535
VBP WAN IP	16386-25386 or 16386-34386	Any	UDP - RTP	1024 – 65535

VBP-ST DMZ required ports inbound from the LAN gatekeeper (H.323 and Access Proxy)

When the Access Proxy configuration is enabled the CMA Desktop or HDX systems installed at the remote locations will be provisioned to authenticate to the VBP-ST Subscriber IP address. The VBP-ST will provide security to the authentication request by inspecting the HTTP header information after decrypting the TLS HTTPS packet, if the packet passes these security checks the VBP-ST system forwards the request to the CMA server on the Provider or more typically called the LAN interface as a destination port 443 request to the CMA server. The CMA server will perform NTLM authentication challenges to verify the endpoints credentials are valid.

The VBP will not source this request as port 443, it will dynamically assign the source port, however the VBP will source the request as the Layer 3 IP address configured as the Provider IP.

Use the below chart to configure the VBP-ST in a DMZ port filtering on the LAN side; this is sometimes required for IT departments that want to monitor traffic going to/from the Provider or LAN interface of the VBP.

When deploying this scenario a routed gatekeeper model is required, this allows the dynamic provisioning ports (Access Proxy) and H.323 signaling to go direct between the VBP and the CMA. The UDP RTP media will go direct to/from the VBP to/from the LAN H.323 endpoint, if the LAN H.323 endpoints can support a fixed UDP RTP media range the DMZ filter policy can be reduced from the below ranges discussed. When deploying these scenario’s it is advised to not apply a strict DMZ policy when installing the system for the first time. When the system is installed and test calls for all features are successful in both directions, then apply a more granular DMZ firewall policy for only the required ports.

Table 10 will describe the reverse port orientation.

Table 9

VBP-ST H.323 endpoints Specific with Access Proxy services				
Inbound from the LAN H.323 gatekeeper or endpoint to VBP-ST Provider Interface IP				
LAN SRC IP	LAN SRC Port	VBP DST IP	Proto	VBP DST port
CMA IP	443 using TLS	VBP LAN IP	TCP – HTTPS	1024 – 65535
CMA IP	5222 using TLS	VBP LAN IP	TCP – XMPP	1024 – 65535
CMA IP	389 using TLS	VBP LAN IP	TCP – LDAP	1024 – 65535
CMA or gatekeeper IP	1719	VBP LAN IP	UDP – RAS	1719
CMA or gatekeeper IP	1720	VBP LAN IP	TCP – H.225	1720
CMA or gatekeeper IP	1024 - 65535	VBP LAN IP	TCP – H.245	14085 - 15084 (contiguous range)
LAN H.323 endpoint IP or subnet	1024 - 65535	VBP LAN IP	UDP - RTP	16386 - 25386 (5300-ST10 and ST25) (contiguous range)
				16386 - 34386 (6400-ST85) (contiguous range)

VBP-ST DMZ required ports outbound to the LAN gatekeeper (H.323 and Access Proxy)

Table 10

VBP-ST H.323 endpoints Specific with Access Proxy services				
Outbound from the VBP-ST Provider Interface IP to the LAN H.323 gatekeeper or endpoint				
LAN SRC IP	LAN SRC Port	VBP DST IP	Proto	VBP DST port
VBP LAN IP	1024 – 65535	CMA IP	TCP – HTTPS	443 using TLS
VBP LAN IP	1024 – 65535	CMA IP	TCP – XMPP	5222 using TLS
VBP LAN IP	1024 – 65535	CMA IP	TCP – LDAP	389 using TLS
VBP LAN IP	1719	CMA or gatekeeper IP	UDP – RAS	1719
VBP LAN IP	1720	CMA or gatekeeper IP	TCP – H.225	1720
VBP LAN IP	14085 - 15084	CMA or gatekeeper IP	TCP – H.245	1024 - 65535
VBP LAN IP	16386-25386 or 16386-34386	LAN H.323 endpoint IP	UDP - RTP	1024 - 65535