Appendix F: VoIP Deployment Scenarios

H.323 Deployment

The diagram below illustrates an H.323 ETM System deployment.

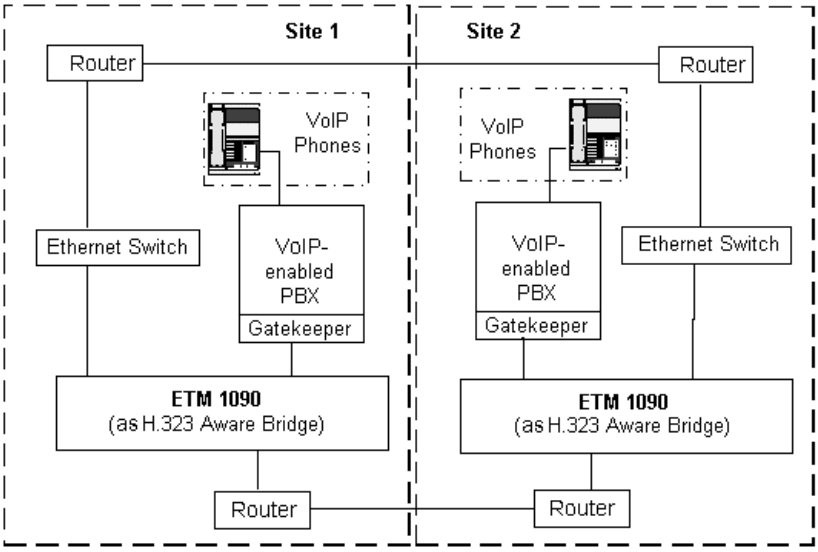

Figure 1 H.323 ETM System Deployment

Non-NAT SIP Deployment

This section describes two scenarios for non-NAT SIP deployment:

- ETM Appliance Directly in Front of a Proxy Server
- ETM Appliance Directly Behind a Firewall

ETM® Appliance Directly in Front of a Proxy Server

The VoIP Span of the ETM Appliance must be configured, via the **Network** tab of the **VoIP Span Configuration** dialog, to operate in bridge mode, not NAT mode. The IP address of the proxy server (PS) must be configured on the **VoIP** tab of the **VoIP Span Configuration** dialog. This deployment will provide protection for the configured proxy server. All call requests to/from the proxy server will be monitored and managed. The firewall component (FW) must be SIP-aware.

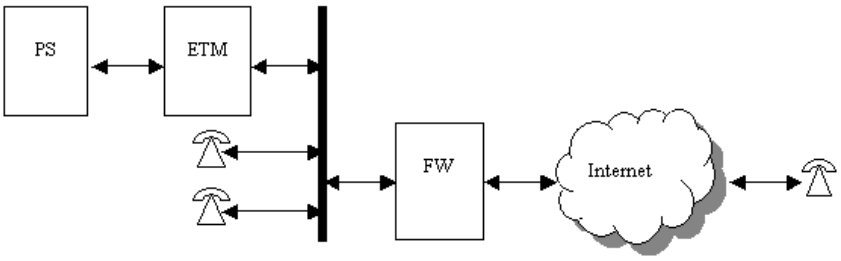

Figure 2 ETM® Appliance in front of Proxy Server

ETM® Appliance Directly Behind a Firewall

The VoIP Span of the ETM Appliance must be configured, via the **Network** tab of the **VoIP Span Configuration** dialog, to operate in bridge mode rather than NAT mode. A list of IP addresses of proxy servers (PS) must be configured via the **VoIP** tab of the **VoIP Span Configuration** dialog. This deployment will provide protection for all proxy servers in the list. All call requests to/from the list of proxy servers from/to external user agents (UA) will be monitored and managed. The firewall component (FW) must be SIP-aware.

SIP NAT Deployment

The ETM System was tested in the following configurations for SIP NAT.

Parallel Deployment

In the Parallel Deployment, the ETM Span's private interface is connected to the enterprise network, and the ETM Span's public interface is connected to the Internet via a network router. The Span receives packets from the managed proxy (located within the Enterprise) and from proxies and/or phones located in the Internet. The Span NATs these packets and their SIP content as they are passed from private to public address space and vice-versa. This deployment scenario has very little impact on the existing Enterprise network and firewall. The managed proxy routes outbound SIP traffic through the Span, and inbound SIP traffic is directed to the Span rather than to the IP firewall.

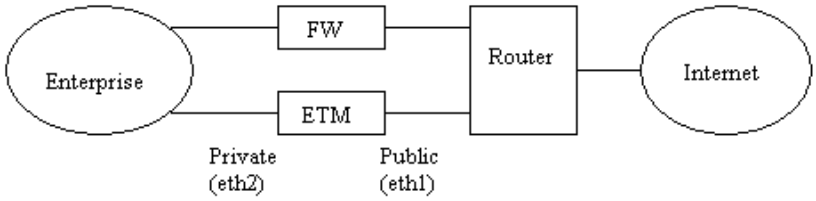

Figure 3 Parallel Deployment

Configuration Activities

The following actions are required to configure ETM Systems operating in the Parallel Deployment scenario:

- Connect the ETM Span's public interface (eth1) directly to an external router or to a network on which the external router is present.
- Assign the private and public addresses and netmasks of the ETM System on the Span's **NAT Configuration** dialog box. The private and public addresses must be valid addresses for sending and receiving packets on the Enterprise and Internet networks. The public address will be mapped to the internal proxy address. For more information on setting the private address, see "Enterprise Configuration" on page 216.
- Set the private and and public signaling ports for the ETM System on the Spans's **NAT Configuration** dialog box. The private signaling port should match the managed proxy's port. The public port can be set as desired, but it is most user friendly to use the default port number. The private and public ports can be set to the same value.

- Set the media port range size and the private and public media port start ports in the Span's **NAT Configuration** dialog box. The media port range size should be set based on the number of expected or allowed simultaneous calls, and typical calls use 2 ports (one for RTP and one for RTCP). The private and public media port ranges can start at the same or different ports.
- Set the default route in the ETM Span's **NAT Configuration** dialog box to use the public-side router as the default gateway. This allows signaling and media packets destined for any remote network to be routed. Note that the default route is specified by setting the destination network to 0.0.0.0 and the netmask to 0.0.0.0. The gateway address is the address of the public-side router and the interface must be eth1.
- Assign a domain name to the SIP proxy server and setup external DNS servers to map this domain name to the ETM Span's public address. This allows inbound calls to be made using the domain name rather than the ETM Span's public address.
- No firewall changes are needed.
- See "Enterprise Configuration" on page 216 to configure the ETM System to work properly in the given enterprise environment.

DMZ Routed Deployment

In a DMZ Routed Deployment, the ETM Span's private interface is connected to the enterprise network, and the ETM Span's public interface is connected to the DMZ port of the IP firewall (or to a DMZ network, to which the DMZ firewall port is also connected). The ETM Span receives packets from the managed proxy (located within the Enterprise) and from proxies and/or phones located in the Internet via the firewall DMZ port. The ETM Span NATs these packets and their SIP content as they are passed from private to public address space and vice-versa. This deployment scenario requires configuration and routing changes at the firewall, but provides the benefit of allowing the firewall to continue to monitor and enforce firewall policy on SIP traffic. The managed proxy routes outbound SIP traffic through the ETM Span which forwards traffic out via the firewall, and inbound SIP traffic is directed to the ETM Span by the firewall.

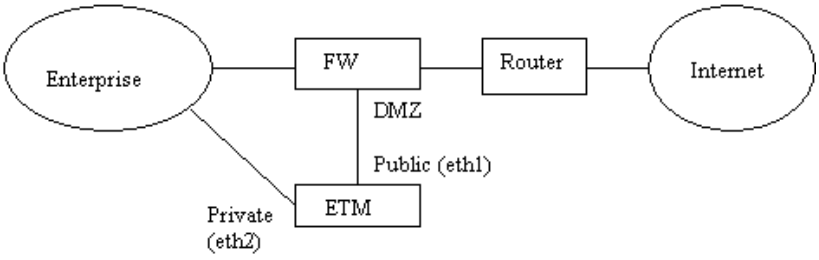

Figure 4 DMZ-Routed Deployment

Configuration Activities

The following actions are required to configure an ETM System operating in the DMZ-Routed Deployment scenario:

- Connect the ETM Span's public interface (eth1) directly to the firewall's DMZ interface or to a network on which the firewall DMZ interface is present.
- Assign the private and public addresses (as well as netmasks) of the ETM System on the Span's **NAT Configuration** dialog box. The private and public addresses must be valid addresses for sending and receiving packets on the Enterprise and Internet networks. The public address will be mapped to the internal proxy address. For more information on setting the private address, see "Enterprise Configuration" below.
- Set the private and and public signaling ports for the ETM System on the Spans's **NAT Configuration** dialog box. The private signaling port should match the managed proxy's port. The public port can be set as desired, but it is most user friendly to use the default port number. The private and public ports can be set to the same value.
- Set the media port range size and the private and public media port start ports in the Span's **NAT Configuration** dialog box. The media port range size should be set based on the number of expected or allowed simultaneous calls, and typical calls use 2 ports (one for RTP and one for RTCP). The private and public media port ranges can start at the same or different ports.
- Set the default route in the ETM Span's **NAT Configuration** dialog box to use the public-side router as the default gateway. This allows signaling and media packets destined for any remote network to be routed. Note that the default route is specified by setting the destination network to 0.0.0.0 and the netmask to 0.0.0.0. The gateway address is the address of the public-side router and the interface must be eth1.
- Assign a domain name to the SIP proxy server and setup external DNS servers to map this domain name to the ETM Span's public address. This allows inbound calls to be made using the domain name rather than the ETM Span's public address.
- Add routing to the firewall to send packets destined for the ETM Span's public address out the firewall's DMZ interface toward the ETM Span.
- Add firewall rules allowing packets to pass through the firewall between the DMZ interface and the public interface. These packets should be limited to ones destined for or originated from the ETM Span's public address and the ETM Span's public signaling port or one of the ETM Span's public media ports. Other firewall rules or rule options can be added as desired, such as limiting the above ETM System traffic to the UDP protocol, etc.

See "Enterprise Configuration" on page 216 to configure the ETM System to work properly in the given Enterprise environment.

Enterprise Configuration

This section applies to both Parallel Deployment and DMZ-Routed Deployment scenarios. The ETM Span's private interface should be connected directly to the subnet on which the managed proxy resides. The proxy directs outbound call signaling to the ETM Span's private interface, and the ETM Span routes inbound call signaling to the proxy using its private interface. Media traffic is routed directly from the phones to the ETM Span's private interface and vice-versa. The following figure shows a possible Enterprise Network configuration.

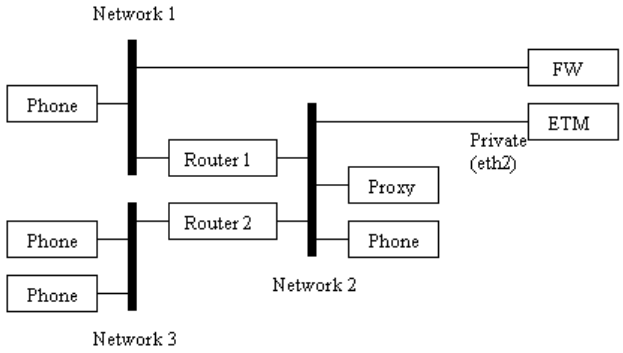

Figure 5 Enterprise Configuration

Configuration Activities

The following actions are required to configure ETM Systems to operate in the local enterprise:

- Connect the ETM Span's private interface to the same subnet on which the managed proxy resides. Note that the managed proxy is the first proxy in the managed proxy list.
- Set the ETM Span's private interface address such that it can send and receive packets on the proxy's subnet. Set the private signaling port to match the proxy's signaling port.
- Add routes in the ETM Span's **NAT Configuration** dialog box to route media packets to enterprise phones not located on the proxy's subnet. For instance, as illustrated above, add a route to Network 1 that uses Router 1 as the gateway, and add a route to Network 2 that uses Router 2 as the gateway. The interface for these routes should be eth2. Add routes for all networks where phones reside other than the local subnet.
- Setup internal DNS servers to map the domain name associated with the proxy to the proxy's internal address. This allows internal phones to make calls using the domain name rather than the proxy's internal address.

- Configure the proxy to use the ETM Span's private address as its default gateway. This allows calls destined for external locations to be routed via the ETM Span.
- Add specific routes to the proxy to allow it to reach specific enterprise machines. This is necessary to allow non-call communications between the proxy and other machines within the enterprise that are not located on the local subnet. For instance, in the above figure, a route can be added to Network 1 using Router 1 as the gateway in order for the proxy to communicate with the firewall.

Use Cases

The following are cases in which you might want to use a SIP NAT deployment:

- To make outbound calls to external phones from within the enterprise, simply dial the destination phone's public SIP address.
- To make inbound calls to internal phones from outside the enterprise, dial the internal user's username at the public domain name or at the ETM Span's public address. For example: "sip:user1@sip.enterprise1.com" or "sip:user1@w.x.y.z" where w.x.y.z is the ETM Span's public address.
- External users can register with the internal proxy to make and receive calls with users in the enterprise.
- Internal users can make outbound calls to external users who are registered with the internal proxy by doing one of the following:
  - Dial the user's username or extension (such as user1 or 1234)
  - Dial "sip:user1@sip.enterprise1.com"
  - Dial "sip:user1@a.b.c.d" where a.b.c.d is the private address of the proxy.
- External users who are registered with the internal proxy can make inbound calls to internal users by doing one of the following:
  - Dial "sip:user1@sip.enterprise1.com"
  - Dial "sip:user1@w.x.y.z" where w.x.y.z is the ETM Span's public address.
- External users who are registered with the internal proxy cannot dial external addresses, including those of other external users who are registered with the internal proxy.
- Parallel forking to multiple external users will not work. After the first Invite is sent out, additional Invites to other locations are blocked.