Appendix 3: Firewall and NAT Settings

Internal Firewall Configuration

In many deployments outbound connections (from internal network to DMZ) will be permitted by the NAT/firewall device. If the administrator wants to restrict this further, the following tables provide the permissive rules required. For further information, see Expressway IP Port Usage for Firewall Traversal.

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 Expressway functionality.

Outbound (Internal Network > DMZ)

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Dest.</th>
<th>Source IP</th>
<th>Source port</th>
<th>Transport protocol</th>
<th>Dest. IP</th>
<th>Dest. port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Management computer</td>
<td>EXPe</td>
<td>As required</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>192.0.2.2</td>
<td>80 / 443 / 22 / 23</td>
</tr>
<tr>
<td>SNMP monitoring</td>
<td>Management computer</td>
<td>EXPe</td>
<td>As required</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>161</td>
</tr>
</tbody>
</table>

H.323 traversal calls using Assent

<table>
<thead>
<tr>
<th>Q.931/H.225 and H.245</th>
<th>EXPc</th>
<th>EXPe</th>
<th>Any</th>
<th>15000 to 19999</th>
<th>TCP</th>
<th>192.0.2.2</th>
<th>2776</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Assent</td>
<td>EXPc</td>
<td>EXPe</td>
<td>Any</td>
<td>36002 to 59999 *</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36000 *</td>
</tr>
<tr>
<td>RTCP Assent</td>
<td>EXPc</td>
<td>EXPe</td>
<td>Any</td>
<td>36002 to 59999 *</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36001 *</td>
</tr>
</tbody>
</table>

SIP traversal calls

<table>
<thead>
<tr>
<th>SIP TCP/TLS</th>
<th>EXPc</th>
<th>EXPe</th>
<th>10.0.0.2</th>
<th>25000 to 29999</th>
<th>TCP</th>
<th>192.0.2.2</th>
<th>Traversal zone ports, e.g. 7001</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Assent</td>
<td>EXPc</td>
<td>EXPe</td>
<td>10.0.0.2</td>
<td>36002 to 59999 *</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36000 *</td>
</tr>
<tr>
<td>RTCP Assent</td>
<td>EXPc</td>
<td>EXPe</td>
<td>10.0.0.2</td>
<td>36002 to 59999 *</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36001 *</td>
</tr>
</tbody>
</table>

When ICE is enabled on Expressway-C zones and the Expressway-E is used as the TURN server

<table>
<thead>
<tr>
<th>TURN server control</th>
<th>EXPc</th>
<th>EXPe</th>
<th>Any</th>
<th>&gt;=1024</th>
<th>UDP</th>
<th>192.0.2.2</th>
<th>3478 **</th>
</tr>
</thead>
<tbody>
<tr>
<td>TURN server media</td>
<td>EXPc</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>24000 to 29999</td>
</tr>
</tbody>
</table>

* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at Configuration > Traversal Subzone. In Large Expressway systems the first 12 ports in the range - 36000 to 36011 by default - are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (Configuration > Traversal > Ports). If you choose not to configure a particular pair of ports (Use configured demultiplexing ports = No), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default).
Inbound (DMZ > Internal network)

As Expressway-C to Expressway-E communications are always initiated from the Expressway-C to the Expressway-E (Expressway-E sending messages by responding to Expressway-C’s messages) no ports need to be opened from DMZ to Internal for call handling.

However, if the Expressway-E needs to communicate with local services, such as a Syslog server, some of the following NAT configurations may be required:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Destination</th>
<th>Source IP</th>
<th>Source port</th>
<th>Transport protocol</th>
<th>Dest. IP</th>
<th>Dest. port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>EXPe</td>
<td>Syslog server</td>
<td>192.0.2.2</td>
<td>30000 to 35999</td>
<td>UDP</td>
<td>10.0.0.13</td>
<td>514</td>
</tr>
<tr>
<td>Management</td>
<td>EXPe</td>
<td>Cisco TMS server</td>
<td>192.0.2.2</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>10.0.0.14</td>
<td>80 / 443</td>
</tr>
<tr>
<td>LDAP (for log in, if required)</td>
<td>EXPe</td>
<td>LDAP server</td>
<td>192.0.2.2</td>
<td>30000 to 35999</td>
<td>TCP</td>
<td>389 / 636</td>
<td></td>
</tr>
<tr>
<td>NTP (time sync)</td>
<td>EXPe</td>
<td>Local NTP server</td>
<td>192.0.2.2</td>
<td>123</td>
<td>UDP</td>
<td></td>
<td>123</td>
</tr>
<tr>
<td>DNS</td>
<td>EXPe</td>
<td>Local DNS server</td>
<td>192.0.2.2</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td></td>
<td>53</td>
</tr>
</tbody>
</table>

Traffic destined for logging or management server addresses (using specific destination ports) must 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.

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 Expressway functionality.

Inbound (Internet > DMZ)

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Dest.</th>
<th>Source IP</th>
<th>Source port</th>
<th>Transport protocol</th>
<th>Dest. IP</th>
<th>Dest. port</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 calls using Assent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q.931/H.225 and H.245</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>192.0.2.2</td>
<td>2776</td>
</tr>
<tr>
<td>RTP Assent</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36000</td>
</tr>
<tr>
<td>RTCP Assent</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36001</td>
</tr>
<tr>
<td>H.323 endpoints with public IP addresses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q.931/H.225</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>192.0.2.2</td>
<td>1720</td>
</tr>
<tr>
<td>H.245</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>192.0.2.2</td>
<td>15000 to 19999</td>
</tr>
<tr>
<td>RTP &amp; RTCP</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>192.0.2.2</td>
<td>36002 to 59999</td>
</tr>
<tr>
<td>SIP endpoints using UDP / TCP or TLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP TCP</td>
<td>Endpoint</td>
<td>EXPe</td>
<td>Any</td>
<td>&gt;=1024</td>
<td>TCP</td>
<td>192.0.2.2</td>
<td>5060</td>
</tr>
</tbody>
</table>
**On Large systems you can configure a range of TURN request listening ports. The default range is 3478 - 3483.**

### Outbound (DMZ > Internet)

If you want to restrict communications from the DMZ to the wider Internet, the following table provides information on the outgoing IP addresses and ports required to permit the Expressway-E to provide service to external endpoints.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Dest.</th>
<th>Source IP</th>
<th>Source port</th>
<th>Transport protocol</th>
<th>Dest. IP</th>
<th>Dest. port</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 endpoints with public IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q.931/H.225</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>15000 to 19999</td>
<td>TCP</td>
<td>Any</td>
<td>1720</td>
</tr>
<tr>
<td>H.245</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>15000 to 19999</td>
<td>TCP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>RTP &amp; RTCP</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>36000 to 59999</td>
<td>UDP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>SIP endpoints using UDP / TCP or TLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP TCP &amp; TLS</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>25000 to 29999</td>
<td>TCP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>SIP UDP</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>5060</td>
<td>UDP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>RTP &amp; RTCP</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>36000 to 59999</td>
<td>UDP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>TURN server media</td>
<td>EXPe</td>
<td>Endpoint</td>
<td>192.0.2.2</td>
<td>24000 to 29999</td>
<td>UDP</td>
<td>Any</td>
<td>&gt;=1024</td>
</tr>
<tr>
<td>Other services (as required)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>EXPe</td>
<td>DNS server</td>
<td>192.0.2.2</td>
<td>&gt;=1024</td>
<td>UDP</td>
<td>DNS servers</td>
<td>53</td>
</tr>
<tr>
<td>NTP (time sync)</td>
<td>EXPe</td>
<td>NTP server</td>
<td>192.0.2.2</td>
<td>123</td>
<td>UDP</td>
<td>NTP servers</td>
<td>123</td>
</tr>
</tbody>
</table>
Appendix 4: Advanced Network Deployments

Prerequisites

- Apply an **Advanced Networking** option key on any Expressway-E that needs static NAT or two LAN interfaces. The **Advanced Networking** option is available only on the Expressway-E.
- Disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers/firewalls carrying network traffic to or from the Expressway-E. We strongly recommend disabling this functionality on the firewall/s when deploying an Expressway-E behind a NAT, because our experience shows that they do not handle video traffic properly. You must use the Expressway to perform the static network address translation on its own interface. Read more in What About Routers/Firewalls with SIP/H.323 ALG?, page 47.

Planning Your Deployment

Do Not Overlap Subnets

The recommended deployment of the Expressway-E configures both LAN interfaces. The LAN1 and LAN2 interfaces must be located in non-overlapping subnets to ensure that traffic is sent out the correct interface.

Clustering

- When the peers have the **Advanced Networking** option installed, you must use the LAN1 interface address of each peer to create the cluster.
- The LAN interface that you use for clustering must not have **Static NAT mode** enabled.

For these reasons, we recommend that you use LAN2 as the externally facing interface, and also enable static NAT on LAN2 when it's required.

External LAN Interface Setting

The **External LAN interface** configuration setting, on the IP configuration page, controls where the Expressway-E's TURN server allocates TURN relays. In the recommended dual NIC deployment, you should select the externally-facing LAN interface (LAN2) on the Expressway-E.

Recommended: Dual NIC Static NAT Deployment

The following example demonstrates the recommended deployment. It shows the typical DMZ configuration where the internal and external firewalls cannot route directly to each other, and dual NIC devices such as Expressway-E are required to validate and forward the traffic between the isolated subnets.

The Expressway-E has both NICs enabled, and it has static NAT enabled on its outward-facing LAN interface. The Expressway-C inside the network is a traversal client of the Expressway-E in the DMZ.

**Figure 8** Dual Network Interfaces Deployment
This deployment consists of:

- **DMZ subnet 1 - 10.0.10.0/24,** containing:
  - the internal interface of Firewall A - 10.0.10.1
  - the LAN2 interface of the Expressway-E - 10.0.10.2
- **DMZ subnet 2 - 10.0.20.0/24,** containing:
  - the external interface of Firewall B - 10.0.20.1
  - the LAN1 interface of the Expressway-E - 10.0.20.2
- **LAN subnet - 10.0.30.0/24,** containing:
  - the internal interface of Firewall B - 10.0.30.1
  - the LAN1 interface of the Expressway-C - 10.0.30.2
- **Firewall A** is the outward-facing firewall; it is configured with a NAT IP (public IP) of 64.100.0.10 which is statically NATed to 10.0.10.2 (the LAN2 interface address of the Expressway-E)
- **Firewall B** is the internally-facing firewall
- **Expressway-E LAN1** has static NAT mode disabled
- **Expressway-E LAN2** has static NAT mode enabled with Static NAT address 64.100.0.10
- **Expressway-C** has a traversal client zone pointing to 10.0.20.2 (LAN1 of the Expressway-E)

With the above deployment, there is no regular routing between the 10.0.20.0/24 and 10.0.10.0/24 subnets. The Expressway-E bridges these subnets and acts as a proxy for SIP/H.323 signaling and RTP/RTCP media.

### Static Routes Towards the Internal Network

With a deployment like Figure 8 Dual Network Interfaces Deployment, page 44, you would typically configure the private address of the external firewall (10.0.10.1 in the diagram) as the default gateway of the Expressway-E. Traffic that has no more specific route is sent out from either Expressway-E interface to 10.0.10.1.

- **If the internal firewall (B) is doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the Expressway-E (for example traversal client traffic from Expressway-C), that traffic is recognized as being from the same subnet (10.0.20.0 in diagram) as it reaches LAN1 of the Expressway-E. The Expressway-E will therefore be able to reply to this traffic through its LAN1 interface.

- **If the internal firewall (B) is not doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the Expressway-E (for example traversal client traffic from Expressway-C), that traffic still has the originating IP address (for example, 10.0.30.2 for traffic from Expressway-C in the diagram). You must create a static route towards that source from LAN1 on the Expressway-E, or the return traffic will go to the default gateway (10.0.10.1). You can do this on the web UI (System > Network interfaces > Static routes) or using xCommand RouteAdd at the CLI.

  If the Expressway-E needs to communicate with other devices behind the internal firewall (eg. for reaching network services such as NTP, DNS, LDAP/AD and syslog servers), you also need to add static routes from Expressway-E LAN1 to those devices/subnets.

In this particular example, we want to tell the Expressway-E that it can reach the 10.0.30.0/24 subnet behind the 10.0.20.1 firewall (router), which is reachable via the LAN1 interface. This is accomplished using the following xCommand RouteAdd syntax:

```plaintext
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

In this example, the **Interface** parameter could also be set to **Auto** as the gateway address (10.0.20.1) is only reachable via LAN1.
Figure 9  The Web UI for Creating a Static Route

The xCommand RouteAdd command and syntax, and the equivalent web UI, are described in full in the Expressway help and the Expressway Administrator Guide.

Background Information

The Challenge of NAT for SIP and H.323 Applications

When deploying an Expressway-E for business to business communications, or for supporting home workers and travelling workers, it is usually desirable to deploy the Expressway-E in a NATed DMZ rather than having the Expressway-E configured with a publicly routable IP address.

Network Address Translation (NAT) poses a challenge with SIP and H.323 applications, as with these protocols, IP addresses and port numbers are not only used in OSI layer 3 and 4 packet headers, but are also referenced within the packet payload data of H.323 and SIP messages themselves.

This usually breaks SIP/H.323 call signaling and RTP media packet flows, since NAT routers/firewalls will normally translate the IP addresses and port numbers of the headers, but leave the IP address and port references within the SIP and H.323 message payloads unchanged.

How Does Expressway-E Address This Challenge?

To ensure that call signaling and media connectivity remains functional in scenarios where the Expressway-E is deployed behind a NAT, the Expressway-E will have to modify the parts of SIP and H.323 messages which contain references to its actual LAN2 network interface IP address and replace these with the public NAT address of the NAT router.

This can be achieved by enabling Static NAT mode on selected network interfaces on the Expressway-E. The Static NAT mode feature on the Expressway-E is made available with the Advanced Networking option key.

This option key allows the use of two network interfaces (LAN1 and LAN2) and for Static NAT mode to be enabled on one or both of these interfaces. You do not have to use both interfaces, but we recommend that you do. If you choose to use a single interface, and enable static NAT on that interface, read Why We Advise Against Using These Types of Deployment, page 49.

When static NAT has been enabled on an interface, the Expressway will apply static NAT for all outbound SIP and H.323 traffic for this interface, which means that H.323 and SIP devices have to communicate with this interface using the static NAT address rather than the local interface address.

When the Advanced Networking key is installed on the Expressway-E, the IP configuration page (System > Network interfaces > IP) has additional options, allowing the user to decide whether to Use dual network interfaces, to nominate
which interface is the **External LAN interface**, to enable **Static NAT mode** on selected interfaces and configure an **IPv4 static NAT address** for each interface.

When enabling **IPv4 static NAT mode** on an interface, the Expressway-E will modify the payload of H.323 and SIP messages sent out via this interface, so that references to the LAN2 interface address are replaced with the IPv4 static NAT address configured for this interface. This means that when looking at the payload of SIP and H.323 messages sent out via this interface, it will appear as if the LAN2 interface has a public IP address.

It is important to note that the Expressway-E will not modify the layer 3 source address of outgoing H.323 and SIP packets sent out of this interface, as this will be done by the NAT router.

**What About Routers/Firewalls with SIP/H.323 ALG?**

Some routers and firewalls have SIP and H.323 ALG capabilities. ALG is also referred to as Fixup, Inspection, Application Awareness, Stateful Packet Inspection, Deep Packet Inspection and so forth. This means that the router/firewall is able to identify SIP and H.323 traffic as it passes through and inspect, and in some cases modify, the payload of the SIP and H.323 messages. The purpose of modifying the payload is to help the H.323 or SIP application from which the message originated to traverse NAT, i.e. to perform a similar process to what the Expressway-E does.

The challenge with router/firewall-based SIP and H.323 ALGs is that these were originally intended to aid relatively basic H.323 and SIP applications to traverse NAT, and these applications had, for the most part, very basic functionality and often only supported audio.

Over the years, many H.323 and SIP implementations have become more complex, supporting multiple video streams and application sharing (H.239, BFCP), encryption/security features (H.235, DES/AES), firewall traversal (Assent, H.460) and other extensions of the SIP and H.323 standards.

For a router/firewall to properly perform ALG functions for SIP and H.323 traffic, it is therefore of utmost importance that the router/firewall understands and properly interprets the full content of the payload it is inspecting. Since H.323 and SIP are standards/recommendations which are in constant development, it is not likely that the router/firewall will meet these requirements, resulting in unexpected behavior when using H.323 and SIP applications in combination with such routers/firewalls.

There are also scenarios where the router/firewall normally will not be able to inspect the traffic at all, for example when using SIP over TLS, where the communication is end-to-end secure and encrypted as it passes through the router/firewall.

As per the recommendations in the Introduction section of this appendix, it is highly recommended to disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a Expressway-E, as, when enabled this is frequently found to negatively affect the built-in firewall/NAT traversal functionality of the Expressway-E itself. This is also mentioned in **Appendix 3: Firewall and NAT Settings, page 41**.

**Other Deployment Examples**

**Note:** Using the Expressway-E as shown in these examples could have a serious impact on your network bandwidth, and may contravene your security policy. We strongly recommend that you use the **Recommended: Dual NIC Static NAT Deployment, page 44**. Read **Why We Advise Against Using These Types of Deployment, page 49**.

**Single Subnet DMZ Using Single Expressway-E LAN Interface and Static NAT**

In this case, FW A can route traffic to FW B (and vice versa). Expressway-E allows video traffic to be passed through FW B without pinholing FW B from outside to inside. Expressway-E also handles firewall traversal on its public side.
This deployment consists of:

- a single subnet DMZ - 10.0.10.0/24, containing:
  - the internal interface of firewall A - 10.0.10.1
  - the external interface of firewall B - 10.0.10.2
  - the LAN1 interface of the Expressway-E - 10.0.10.3
- a LAN subnet - 10.0.30.0/24, containing:
  - the internal interface of firewall B - 10.0.30.1
  - the LAN1 interface of the Expressway-C - 10.0.30.2

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of the Expressway-E. **Static NAT mode** has been enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

---

**Note:**

You must enter the FQDN of the Expressway-E, as it is seen from outside the network, as the peer address on the Expressway-C’s secure traversal zone. The reason for this is that in static NAT mode, the Expressway-E requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name.

**This also means that the external firewall must allow traffic from the Expressway-C to the Expressway-E’s external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.**

---

So, in this example, firewall A must allow NAT reflection of traffic coming from the Expressway-C that is destined for the external address, that is 64.100.0.10, of the Expressway-E. The traversal zone on the Expressway-C must have 64.100.0.10 as the peer address.

The Expressway-E should be configured with a default gateway of 10.0.10.1. Whether or not static routes are needed in this scenario depends on the capabilities and settings of FW A and FW B. Expressway-C to Expressway-E communications will be to the 64.100.0.10 address of the Expressway-E; the return traffic from the Expressway-E to Expressway-C might have to go via the default gateway. If a static route is added to the Expressway-E so that reply traffic goes from the Expressway-E and directly through FW B to the 10.0.30.0/24 subnet, this will mean that asymmetric routing will occur and this may or may not work, depending on the firewall capabilities.

### 3-port Firewall DMZ Using Single Expressway-E LAN Interface

- **LAN**
- **Expressway-C**
- **Expressway-E**
- **FW A**

In this deployment, a 3-port firewall is used to create

- a DMZ subnet (10.0.10.0/24), containing:
  - the DMZ interface of firewall A - 10.0.10.1
  - the LAN1 interface of the Expressway-E - 10.0.10.2
a LAN subnet (10.0.30.0/24), containing
  - the LAN interface of firewall A - 10.0.30.1
  - the LAN1 interface of the Expressway-C - 10.0.30.2

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of the Expressway-E. Static NAT mode has been enabled for LAN1 on the Expressway-E, with a static NAT address of 64.100.0.10.

The Expressway-E should be configured with a default gateway of 10.0.10.1. Since this gateway must be used for all traffic leaving the Expressway-E, no static routes are needed in this type of deployment.

---

**Note:** The traversal client zone on the Expressway-C needs to be configured with a peer address which matches the static NAT address of the Expressway-E, in this case 64.100.0.10, for the same reasons as described in *Single Subnet DMZ Using Single Expressway-E LAN Interface and Static NAT, page 47.*

This means that firewall A must allow traffic from the Expressway-C with a destination address of 64.100.0.10. This is also known as NAT reflection, and it should be noted that this is not supported by all types of firewalls.

---

**Why We Advise Against Using These Types of Deployment**

For deployments that use only one NIC on the Expressway-E, but also require static NAT for the public address, the media must “hairpin” or reflect on the external firewall whenever media is handled by the Expressway-E’s back to back user agent (B2BUA).

For all calls coming in on a Unified Communications Traversal Server zone, or another zone where SIP Media encryption mode is not Auto, the Expressway-E’s B2BUA could be engaged to decrypt or encrypt the media packets. In these deployments, the B2BUA sees the public IP address of the Expressway-E instead of its private IP address, so the media stream must go through the network address translator to get to the private IP address.

- Not all firewalls will allow this reflection, and it is considered by some to be a security risk.
- Each call where the B2BUA is engaged will consume three times as much bandwidth as it would using the recommended dual NIC deployment. This could adversely affect call quality.
Figure 10  Media Path in Dual NIC Static NAT Example (Recommended)

Figure 11  Media Path in Single NIC Static NAT Example
Figure 12 Media Path in 3-port Firewall Static NAT Example
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2015</td>
<td>Menu path changes for X8.5. Republished with X8.5.2.</td>
</tr>
<tr>
<td>December 2014</td>
<td>Republished for X8.5.</td>
</tr>
<tr>
<td>August 2014</td>
<td>Correction in firewall appendix.</td>
</tr>
<tr>
<td>June 2014</td>
<td>Republished for X8.2.</td>
</tr>
<tr>
<td>December 2013</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2015 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)