Advanced Networking Deployments

Planning and Prerequisites

Advanced Networking option

The **Advanced Networking** option needs to be enabled for static NAT or two LAN interfaces. This is available on the Expressway-E (not on the Expressway-C).

Use the LAN2 external interface

In a dual NIC deployment (recommended), configure the **External LAN interface** setting on the IP configuration page to be LAN2.

Note This setting determines where the Expressway-E TURN server allocates TURN relays.

SIP and H.323 Application Layer Gateways (ALGs)

Disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers and firewalls carrying network traffic to or from the Expressway-E. We do not support this functionality on firewalls when deploying an Expressway-E behind a NAT. The Expressway must perform the static network address translation on its own interface (see What About Routers/Firewalls with SIP/H.323 ALG?).

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 through the correct interface.

Requirements for clustered systems

The following additional requirements apply to clustered systems:

- When the peers have **Advanced Networking** enabled, use the LAN1 interface address of each peer to create the cluster.

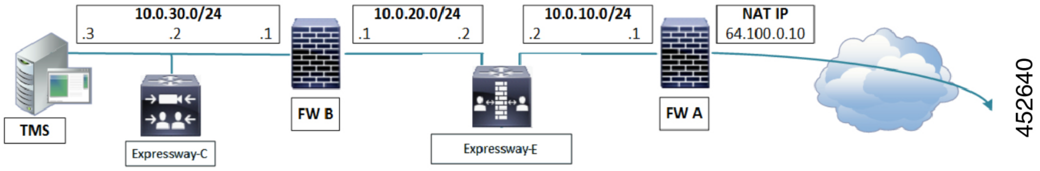
- The LAN interface used for clustering must not have static NAT mode enabled. If static NAT is required, enable it on the LAN2 interface.

Recommended: Dual NIC Static NAT Deployment

The following example illustrates 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 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 1: 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
  - the network interface of the Cisco TMS server – 10.0.30.3
- 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)
- Cisco TMS has Expressway-E added with IP address 10.0.20.2

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 1: Dual Network Interfaces Deployment, 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 (such as 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 can therefore reply to this traffic through its LAN1 interface.

  MRA limitation: Due to Expressway-E security mechanisms, Mobile & Remote Access (MRA) is not compatible with this scenario. If there is source NAT on the packets from Expressway-C then edge login requests will fail (destination NAT is unaffected).

- **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 (such as 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

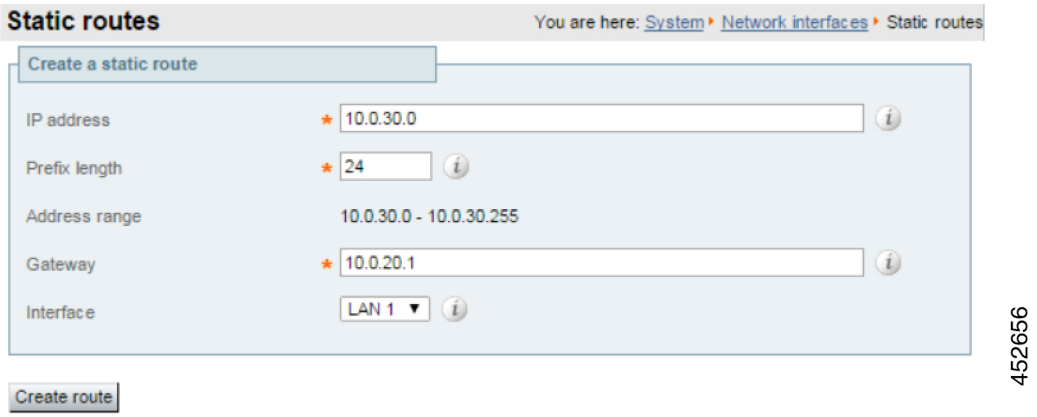
  ```
  xCommand RouteAdd at the CLI
  ```

  If the Expressway-E needs to communicate with other devices behind the internal firewall (for example, to reach 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 (the `Interface` parameter could also be set to `Auto` as the gateway address - 10.0.20.1 - is only reachable via LAN1):

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

Figure 2: The Web UI for Creating a Static Route



Static routes

You are here: System ▸ Network interfaces ▸ Static routes

Create a static route

IP address *	10.0.30.0
Prefix length *	24
Address range	10.0.30.0 - 10.0.30.255
Gateway *	10.0.20.1
Interface	LAN 1 ▼

The `xCommand RouteAdd` command and the equivalent web UI, are detailed 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 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.

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 **Advanced Networking** is enabled on the Expressway-E, the **IP** configuration page (**System** > **Network interfaces** > **IP**) has additional options, allowing you 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.

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. That is, 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 Prerequisites section of this appendix, you should disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a Expressway-E. We do not support this functionality, as, when enabled, it is frequently found to negatively affect the built-in firewall/NAT traversal functionality of the Expressway-E itself.

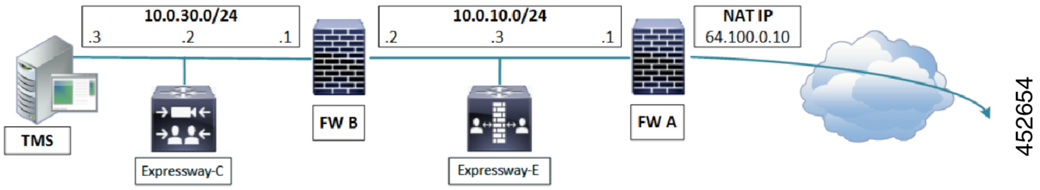
Other Deployment Examples

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. Read Why We Advise Against Using These Types of Deployment.

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.

Figure 3: Single Subnet DMZ - Single LAN Interface and Static NAT



This deployment consists of the following elements:

- Single subnet DMZ (10.0.10.0/24) with the following interfaces:
  - Internal interface of firewall A – 10.0.10.1
  - External interface of firewall B – 10.0.10.2
  - LAN1 interface of Expressway-E – 10.0.10.3
- LAN subnet (10.0.30.0/24) with the following interfaces:
  - Internal interface of firewall B – 10.0.30.1
  - LAN1 interface of Expressway-C – 10.0.30.2
  - Network interface of Cisco TMS – 10.0.30.3

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** is 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.

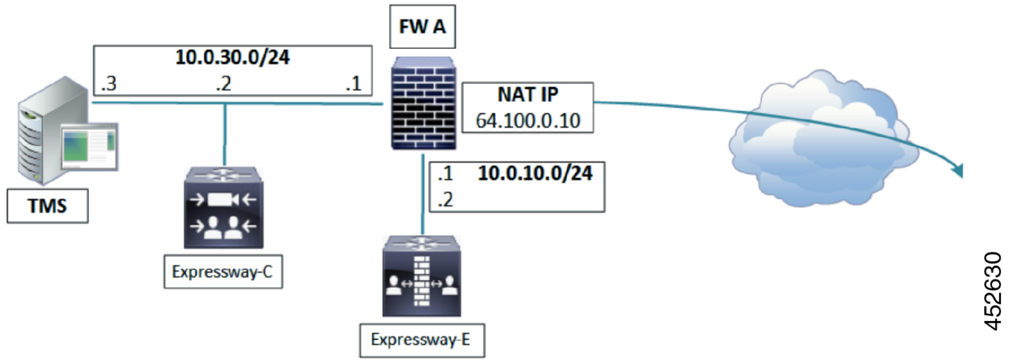
This also means that the external firewall must allow traffic from the Expressway-C to the Expressway-E's external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.

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 through 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, asymmetric routing occurs. Which may or may not work, depending on the firewall capabilities.

The Expressway-E can be added to Cisco TMS using its internal IP address (10.0.10.3). This is because static NAT mode settings on the Expressway-E do not affect Cisco TMS management communications. You could add the Expressway-E's external interface to TMS instead (64.100.0.10 in the diagram) if FW A allows it.

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



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

- DMZ subnet (10.0.10.0/24) with the following interfaces:
  - DMZ interface of firewall A - 10.0.10.1
  - LAN1 interface of Expressway-E - 10.0.10.2
- LAN subnet (10.0.30.0/24) with the following interfaces:
  - LAN interface of firewall A - 10.0.30.1
  - LAN1 interface of Expressway-C – 10.0.30.2
  - Network interface of Cisco TMS – 10.0.30.3

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 is 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.

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.

The Expressway-E can be added to Cisco TMS with the IP address 10.0.10.2 (or with IP address 64.100.0.10 if FW A allows this), since Cisco TMS management communications are not affected by static NAT mode settings on the Expressway-E.

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 4: Media Path in Dual NIC Static NAT Example (Recommended)

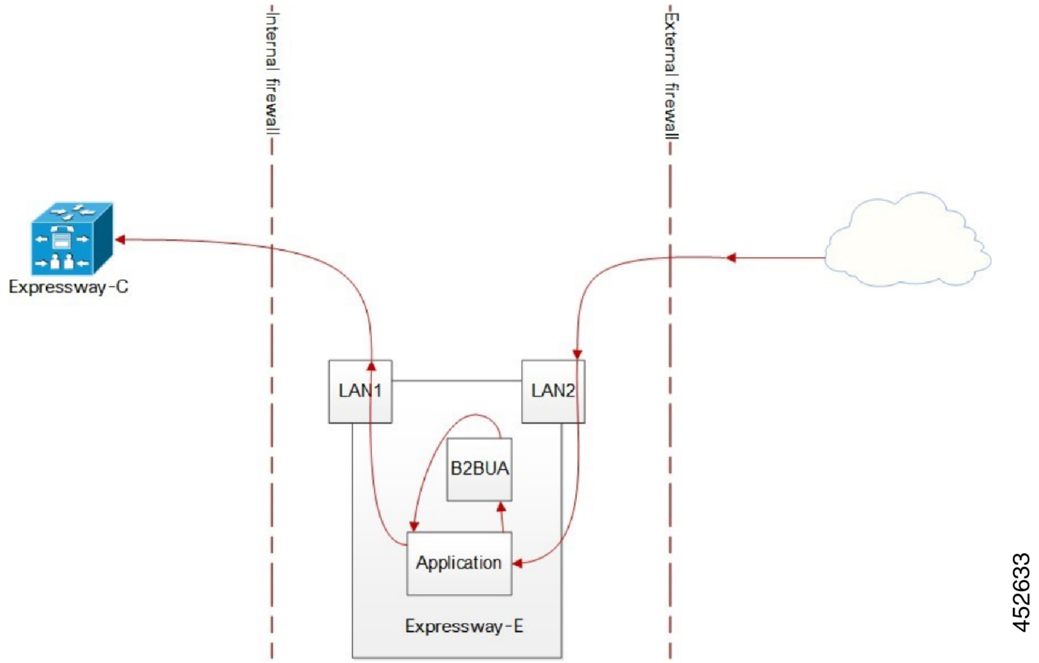


Figure 5: Media Path in Single NIC Static NAT Example

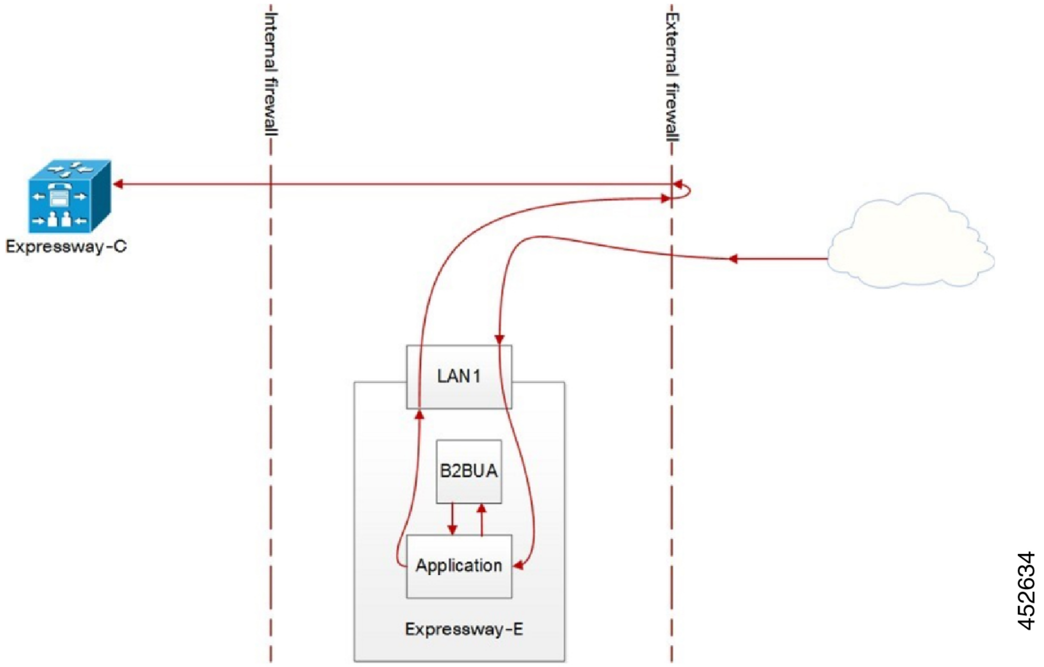
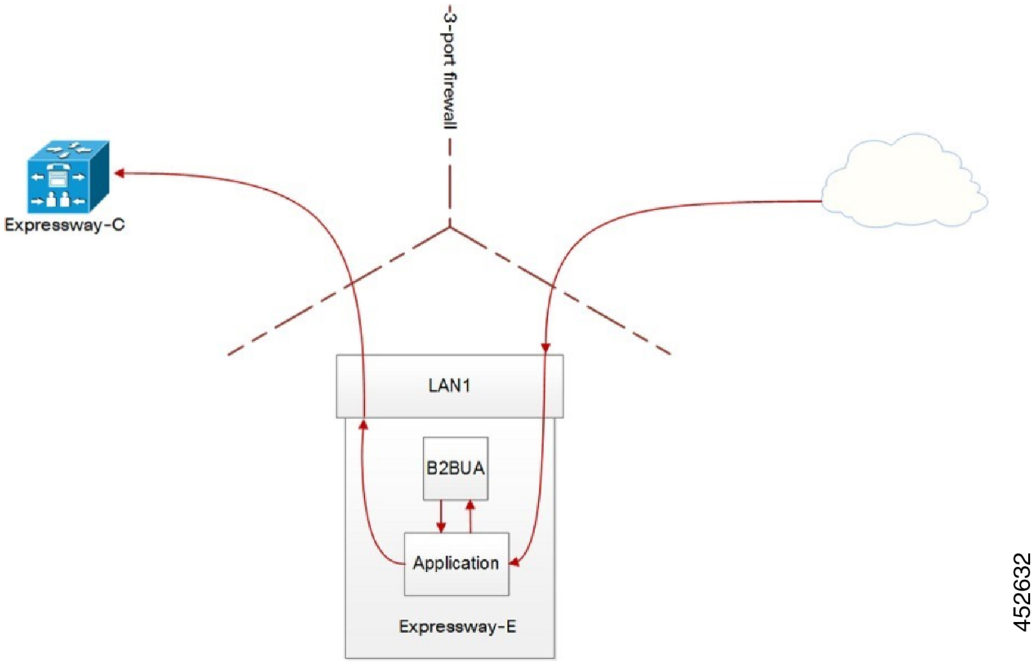


Figure 6: Media Path in 3-port Firewall Static NAT Example



The 3-port Firewall Static NAT diagram, above, shows the traffic flow in the case where a Cisco ASA 8.4 and later series, has been configured to allow traffic to flow from LAN1 through the 3-port firewall.

Other vendors' firewalls may not have a similar configuration option.