Firewall Configuration

Firewall Configuration

Here are some points to keep in mind when you are configuring your firewalls to permit the connections described in this document:

- If you have a cluster of Expressways, ensure that the destination ports to the public IP address of each Expressway peer are open on the external firewall.
- Sometimes there are different connection types that could be used to achieve the same task. You do not need to always open every port shown in the diagrams and tables. We recommend that you close any that you are not using.

  For example, if your web administration port is TCP 7443 but you only ever use SSH to configure the Expressway, you can close 7443 and leave TCP 22 open. Management ports should only be open to connections originating from inside the network.
- Some firewalls actively close connections that appear inactive, which could interfere with the operation of your video infrastructure.

  For example, TCP port 1720 is used for H.323 call signaling but may be inactive during the call. If this is prematurely closed by the firewall, the H.323 endpoint could interpret that as a dropped call and respond by tearing down the call.

  We recommend extending inactivity timeouts on the known ports to at least two hours, particularly if you are seeing calls fail after a specific duration.
- Firewalls that contain ALG (Application Layer Gateway) for SIP / H.323 protocols may not work as expected with Expressway-E.

  We strongly recommend that you disable SIP or H.323 ALG inspection / awareness on the NAT firewall. We may not be able to support your configuration if you cannot make this change.

  We recommend that you disable UDP inspection on the NAT firewall to avoild media issues.
- In some deployments, media packets can hairpin on the Expressway-E external NIC. Some firewalls cannot allow for hairpinning, and mistrust packets that are destined to their own source.

  We recommend configuring an exception to allow hairpinning on the Expressway-E public interface, if your deployment requires it.

- If you want to use the static NAT feature of Expressway-E, we strongly recommend using two NICs. Dedicating one NIC to the external interface and the other to the internal interface is much better for your network than using one NIC with the static NAT enabled.