Configuring firewalls to allow Tofino™ CMP traffic

Introduction

The Tofino Central Management Platform (CMP) is a software application program that allows all Tofino Security Appliances (SAs) in a control network to be managed from a single workstation in the plant.

The Tofino CMP may be located anywhere in the network, as long as it is able to communicate with the Tofino SAs that it manages. If any routers or firewalls are located between the Tofino CMP and a Tofino SA in the network, then each router/firewall device must be configured to allow the Tofino CMP traffic to pass through these devices.

The Tofino CMP uses both TCP and UDP traffic to manage Tofino Security Appliances. There are three types and directions of traffic that must pass between the Tofino CMP and Tofino Security Appliances:

- TCP: Tofino CMP to Tofino SA
- UDP: Tofino CMP to Tofino SA
- UDP: Tofino SA to Tofino CMP computer

Tofino releases, up to and including version 1.4, use port 65000 as the destination port for each type of management traffic. Newer releases will begin to transition to the new IANA assigned port number of 6689.

The requirements for each type of management traffic are listed below.

TCP: Tofino CMP to Tofino Security Appliance

The Tofino CMP computer must be allowed to create TCP connections to each Tofino Security Appliance. For each TCP connection, the Tofino CMP computer is the client and the Tofino SA is the server. Here are the parameters for these TCP connections:

Source IP address

The IP address of the Tofino CMP computer.

Destination IP address

Any of the following IP addresses may be used by the Tofino CMP to contact a specific Tofino Security Appliance:

1. The IP address assigned to the Tofino Security Appliance, if set by the user (Tofino version 1.4 and newer only)
2. Primary contact device
3. Backup contact device
4. The source IP address of the last heartbeat message received from the Tofino Security Appliance
5. Tofino Discovery IP address (the address from which the Tofino SA replied during Tofino Discovery scan)

The Tofino CMP attempts to establish a TCP connection to the appliance at each IP address in the order listed above, until it is successful.

Notes:

- Some of these may resolve to the same IP address.
- Not all of these IP addresses must be configured in Tofino CMP, but management traffic must be able to reach the Tofino SA using at least one of these IP addresses in order to allow successful management of the Tofino SA from the Tofino CMP.
- Not all of these addresses are required to be 'allowed'; however, providing additional IP addresses (such as primary and backup contact devices) provide higher levels of system reliability.

Powering Business Worldwide

Source TCP port

This is the ephemeral (pseudo-random) source port assigned by the Windows OS on the Tofino CMP computer.

Destination TCP port

Two ports should be enabled – port 6689 and port 65000.

Network address and source port number translation is allowed on this traffic if necessary.

UDP: Tofino CMP to Tofino Security Appliance

UDP packets must be allowed to pass from the Tofino CMP computer to each Tofino Security Appliance. Here are the parameters for these UDP packets:

Source IP address

This is the IP address of the Tofino CMP computer.

Destination IP address

Destination IP address for this UDP traffic will be the same as described in 'Destination IP address' for TCP traffic (see page 1).

Source UDP port

Ephemeral source port assigned by the Windows OS of the Tofino CMP computer.

Destination UDP port

Two ports should be enabled – port 6689 and port 65000. Network address and source port number translation is allowed on this traffic if necessary.

UDP: Tofino SA to Tofino CMP computer

UDP packets must be allowed to pass from each Tofino SA to the Tofino CMP computer. Here are the parameters for these UDP packets.

Source IP address

This is the last IP address used by the Tofino CMP computer to connect to the Tofino SA (will be one of the values listed for "Destination IP" in Section 1 above)

Destination IP address

The IP address of the Tofino CMP computer

Source UDP port

The source port will vary depending on the type of message. Firewall rules should be configured to allow any value for the source port.

Destination UDP port

Two ports should be enabled – port 6689 and port 65000.

Network address translation is allowed on this traffic, but port number translation is not allowed. The source and destination UDP port numbers must remain the same when this traffic passes through a router or firewall.

Management of Sequentially-connected Tofino Security Appliances

If Tofino Security Appliances are connected sequentially (i.e. in series), then rules must be added to all the upstream Tofino Security Appliances so that the Tofino CMP traffic can pass through these Tofino SAs and reach the Tofino Security Appliances that are located downstream. There is a protocol available in the Tofino CMP Protocols view called "Tofino CMP" that can be added to the "Global Rules" item on the Firewall tab of each upstream Tofino SA, to allow this traffic to pass to the downstream Tofino Security Appliances.

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 435600 Fax: + 44 (0)1582 422283
www.mtl-inst.com
E-mail: mtlenquiry@eaton.com

Publication No. AN-112 Rev 2 131016
October 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com