Securing Control Networks with the Tofino™ VPN

Overview

Version 1.4 of the Tofino Industrial Security Solution introduced a new set of Tofino Loadable Security Modules (LSMs) that enable the creation of Virtual Private Network (VPN) connections in control networks. The Tofino VPN is designed specifically for use within an industrial environment, so it has some unique features tailored for use within SCADA and control systems:

- The Tofino VPN is simple to configure and manage without specialized IT knowledge. In addition, the Tofino VPN uses SSL/TLS (Secure Sockets Layer/Transport Layer Security), avoiding the interoperability issues that plague other VPN technologies.
- The Tofino VPN can transport legacy non-IP protocols (such as GOOSE) over IP networks, so low-cost broadband Internet connections may be used to replace expensive dial-up and leased-line services.
- The Tofino VPN can be combined with other security features such as the Tofino Firewall and Modbus TCP Enforcer to ensure only authorized traffic enters and exits the VPN tunnel.

Primary Use Cases for Tofino VPN

The Tofino VPN was designed for three primary use cases:

1. Creating secure 'tunnels' of communication within an existing control or corporate network. This provides an extra layer of isolation and security for critical control traffic that shares network resources with other types of traffic.
2. Enabling remote access for maintenance purposes.
3. Connecting remote plant sites together over a wide-area network (WAN) connection, such as the Internet or SCADA WAN.

This document describes how to use Tofino VPN in Use Case #1 – creating a secure 'tunnel' within an existing corporate network.

Creating a Secure Tunnel in an Existing Corporate Network

The Existing Plant Network

To illustrate the use case, a fictional network has been created and is shown in Figure 1. In this network, we have control traffic passing between an HMI computer and a PLC that is controlling a critical process in the plant. We would like to use the Tofino VPN to isolate this traffic from other devices in the corporate network so they cannot disrupt the operation of our critical PLC. Ideally, we would like to do this without requiring any changes to the PLC, the HMI computer, or the other elements of the network.

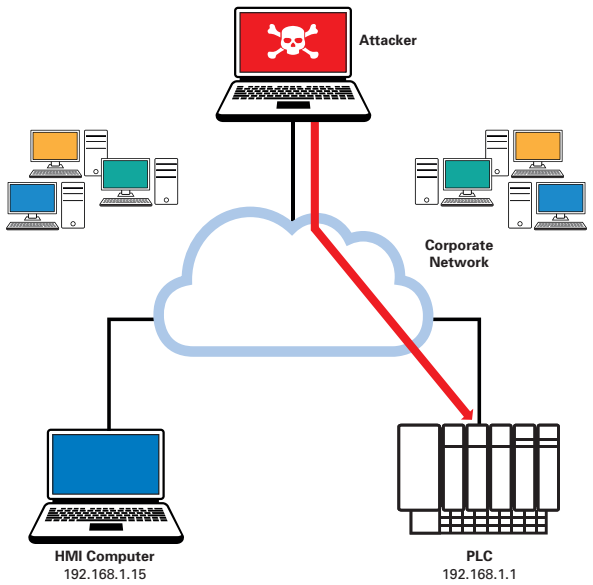


Figure 1: Control Network before Introducing the Tofino Security Appliance

Powering Business Worldwide

Tunnel Control Traffic through a VPN

Figure 2 shows how two Tofino Security Appliances (SAs) have been added to the network to implement a VPN 'tunnel' between the HMI computer and the PLC. In addition, a Windows computer has been added to run the Tofino Central Management Platform (CMP) software to allow configuration and management of the Tofino SAs.

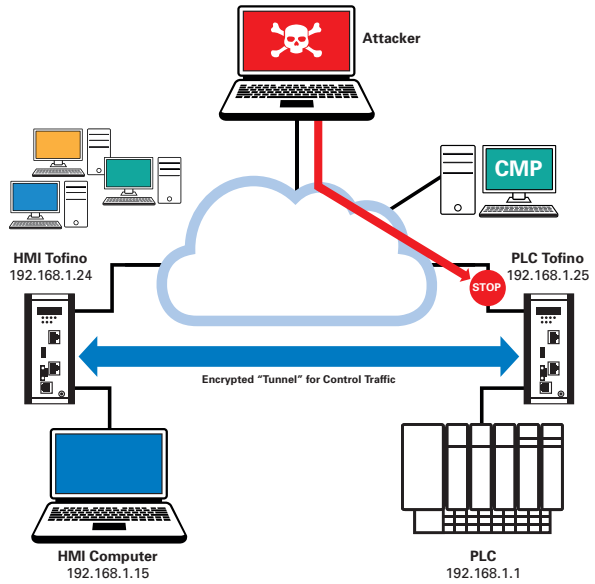


Figure 2: Tunneling Traffic with Tofino VPN

When the VPN tunnel is operational, the Tofino SAs will prevent any traffic from the shared network from reaching the HMI computer or the PLC. At the same time, the HMI and PLC will be connected through an encrypted and authenticated VPN tunnel. Since the Tofino VPN operates at the data link layer (layer 2), this can be achieved without changing the IP addresses or any other network settings on the HMI, PLC or other devices in the network.

Steps to Setting up a VPN

Step 1: Install Tofino Security Appliances

The first step is to connect power to the Tofino SAs and wire them into the appropriate locations in the control network. In their 'factory reset' configuration, the Tofino SAs will transparently bridge all traffic between their two network ports, so they can be installed into the network without disrupting any network traffic.

Each Tofino SA has two network interfaces, so that it can be wired in-line between the device or devices to be protected and the rest of the control network.

The interface labeled with a 'closed padlock' or 'key' icon is called the 'trusted' port; this port should be connected to the device that will be protected by the VPN tunnel (HMI or PLC, as appropriate). The interface labeled with an 'open padlock' or 'globe' icon is called the 'untrusted' port; in the VPN application this interface will be connected to the rest of the plant or corporate network.

Step 2: Install and License the Tofino CMP

The second step is to install the Tofino CMP software on a Windows computer in the corporate network. The Tofino CMP will be used to configure and manage the Tofino SAs.

For best results, this computer should be located at a point in the network where it can connect to the 'untrusted' network interface ('open padlock', or 'globe' icon) on both Tofino Security Appliances.

After the Tofino CMP software is installed, the Tofino CMP and Loadable Security Modules (LSMs) must be licensed before use. This is described in the Tofino CMP Installation and Upgrade Guide.

Step 3: Model the Network in Tofino CMP

Before we can configure the Tofino Security Appliances, we need to build a simple model of the network in the Tofino CMP's Network Editor. A library of icons is available in the Nodes view (top right corner of the Tofino CMP), representing a wide variety of computers, controllers and network devices; these may be added to the network model by simply dragging them from the Nodes view and dropping them at the appropriate location. Figure 3 shows how our example control network can be modeled in the Tofino CMP Network Editor.

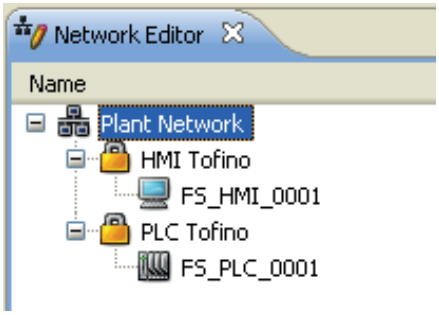


Figure 3: Network Model in the Tofino CMP

The Tofino CMP also offers a 'Tofino Discovery' feature which will scan the control network to discover unconfigured Tofino Security Appliances. Any Tofino SAs discovered in this manner will be presented as a list of icons in the Tofino Discovery view (bottom left view in the Tofino CMP) which can be dragged and dropped into the Tofino CMP Network Editor.

Step 4: Set Tofino Security Appliances to Passive Mode

After the network model is created, the mode of each Tofino Security Appliance should be changed to Passive. Double-click the icon for each Tofino SA, select 'Passive' from the mode pull-down list at the bottom of the view, and click the 'Apply' or 'OK' button.

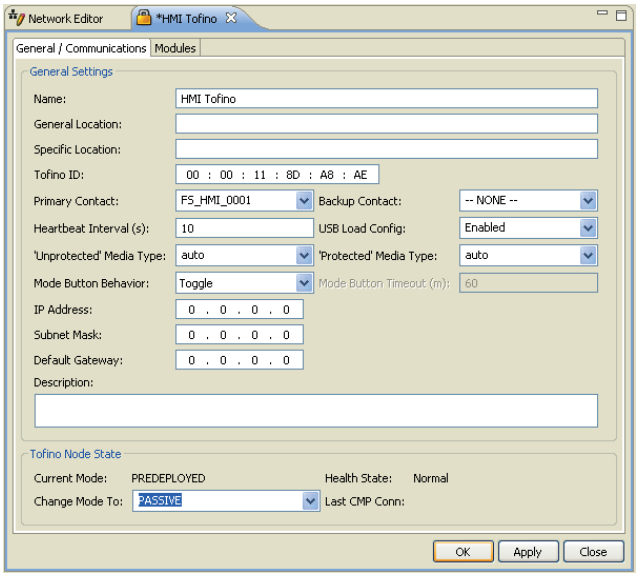


Figure 4: Changing each Tofino SA to Passive mode

If a communications failure occurs, check the Tofino ID and Primary Contact device on this view to make sure they are correct.

Step 5: Assign IP Addresses to each Tofino Security Appliance

By default the Tofino Security Appliance operates with no IP address. However the VPN client and server LSMs require that the Tofino SA have an IP address assigned to it. This is done on the General/Communications settings tab. Set the IP addresses as per the network diagram in Figure 2 (192.168.1.24 for the HMI Tofino, 192.168.1.25 for the PLC Tofino). Refer to Figure 5 for an example.

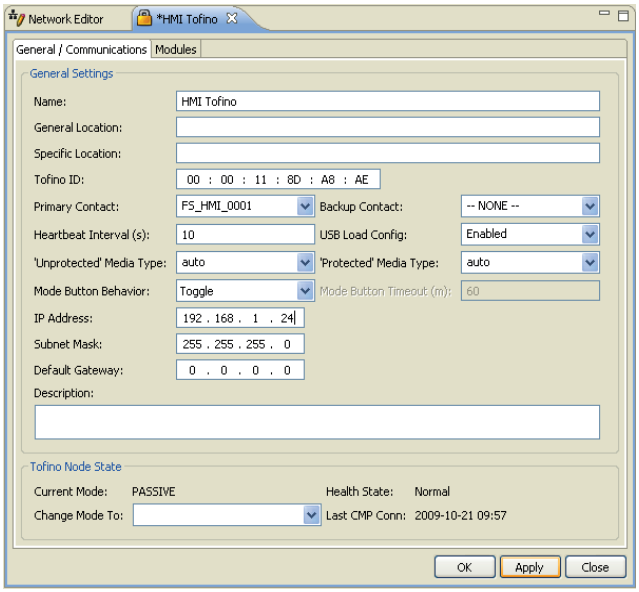


Figure 5: IP address and subnet on HMI Tofino

The subnet mask for both Tofino SAs should be set to 255.255.255.0. No default gateway should be assigned for the Tofino SAs in this example (leave this parameter set to all zeroes).

> Your Tofino SA must have a valid IP address assigned to it before it is configured to act as a VPN Server or Client. Failure to have an address that is reachable from the Tofino CMP may mean loss of all connectivity to that Tofino SA.

Step 6: Install VPN LSMs

Tofino VPN tunnels are point-to-point connections between a VPN client and a VPN server. In this example, the PLC Tofino SA will act as the VPN server and the HMI Tofino SA will act as the VPN client, so we need to install and activate the required Loadable Security Modules (LSMs) on each of the Tofino SAs:

1. Double-click the HMI Tofino SA icon in the Tofino CMP's Network Editor, and select the Modules tab. Highlight the VPN Client LSM and click the 'Activate' button.

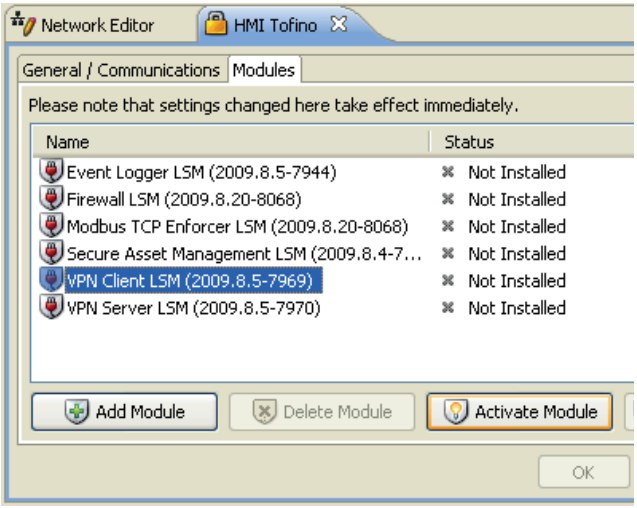


Figure 6: Activating the Tofino VPN Client LSM

2. Double-click the PLC Tofino SA icon in the Tofino CMP's Network Editor, and select the Modules tab. Highlight the VPN Server LSM and click the 'Activate' button.

> Ensure the Tofino SA is in TEST or PASSIVE mode before activating a VPN LSM. We do not recommend attempting to set up a VPN on a Tofino SA that is in OPERATIONAL mode.

Step 7: Configure a VPN tunnel between Tofino Security Appliances

VPN tunnels are configured and managed on the Tofino Security Appliance that has the VPN Server LSM installed.

1. Double-click the PLC Tofino SA icon in the Tofino CMP Network Editor and switch to the VPN Server tab. This will display the current VPN server settings.
2. To create a new VPN tunnel, simply drag the icon of the client Tofino SA from the Network view (top left corner of the Tofino CMP) and drop it on the 'Client List' area of the VPN server tab.

Do not drag and drop the 'HMI' icon onto the VPN server's Client List. The icon representing the Tofino SA that is running the VPN Client should be dropped on the VPN server tab.

At this point the HMI Tofino SA will be displayed in the VPN client list.

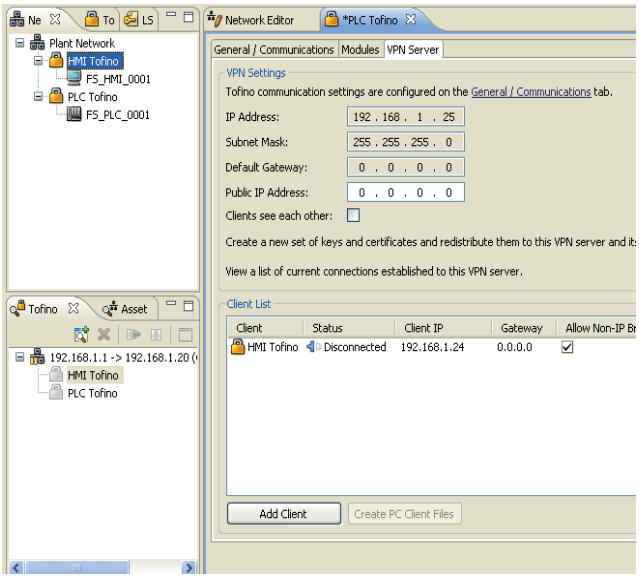


Figure 7: Creating a VPN Tunnel

Step 8: Testing the VPN Tunnel

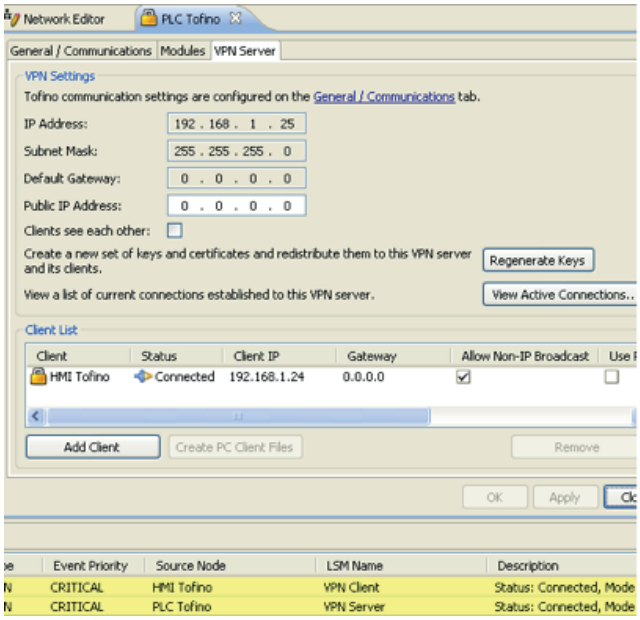
The Tofino Security Appliance features three main operating modes: Passive, Test and Operational.

- In Passive mode the VPN tunnels can be configured, but the Tofino SAs do not set up any VPN tunnels.
- In Test mode, the Tofino SAs will attempt to connect the VPN tunnel, but the tunnel will not be used to pass traffic.
- In Operational mode, VPN tunnels will be connected and will be used to pass traffic.

Test mode may be used to verify that the VPN tunnels can be successfully set up without actually passing traffic through the tunnel. This prevents accidental loss of critical control traffic due to a configuration issue. Both the VPN Server and each VPN Client must be set to Test mode in order for the tunnel to be connected.

After setting both the HMI Tofino SA and the PLC Tofino SA to Test mode, check the VPN Server tab on the PLC Tofino SA to verify that the VPN tunnel is connected. Exception Heartbeats will also show up in the Tofino CMP Event view from each Tofino Security Appliance when the VPN tunnel is connected.

Figure 8: VPN tunnel status shown in the VPN server tab and



as Exception Heartbeats in the Event view

Step 9: Using the VPN to tunnel traffic

Set both the client and server Tofino Security Appliances to Operational mode to cause all network traffic to flow through the VPN tunnel.

When the VPN LSMs are activated and the Tofino SAs are in Operational mode, the Tofino SAs will no longer bridge traffic between their 'trusted' and 'untrusted' network ports. Instead, the VPN tunnel will cause the 'trusted' network interfaces of both the Client and Server Tofino SAs to be bridged together. In our example network this effectively isolates the HMI computer and the PLC from all devices on the 'untrusted' side of the Tofino Security Appliances, but allows these protected devices to continue to communicate with each other as if there was no change in the network. Since the Tofino VPN operates at the datalink layer (layer 2) of the network model, it really is like a virtual 'wire' between the 'trusted' interfaces of each Tofino Security Appliance.

Traffic between the HMI computer and PLC will be blocked until 30-45 seconds after BOTH Tofino SAs have entered Operational mode.

Adding a Firewall to Filter Network Traffic entering the VPN Tunnel

Although the Tofino VPN provides isolation for the control devices, VPN's do not filter any traffic entering or exiting the VPN tunnel. This means that if a device on one end of the VPN tunnel were to become compromised in any way, the VPN tunnel would permit any traffic it generated to reach devices on the other end of the VPN tunnel. For comprehensive security it is vital to combine the VPN tunnel with a firewall. Fortunately, Tofino's modular architecture makes this very simple.

Step 1: Activate the Firewall LSM

First of all, switch both the HMI and PLC Tofino Security Appliances back to Test mode. Once this is done, the Firewall LSM should be activated on both Tofino SAs. While a firewall is required only on the PLC Tofino SA, it is prudent to apply firewall rules on both ends of the VPN tunnel to reduce the potential for a denial of service (DoS) in the tunnel due to traffic overload.

Step 2: Add Firewall Rules to Permit Traffic

We now have a firewall installed on both Tofino Security Appliances, but no firewall rules are in place. This will cause a steady stream of firewall Exception Heartbeats to arrive in the Tofino CMP Event view. Because both Tofino SAs are in Test mode, all traffic will be allowed to pass through them; however before we switch the Tofino SA back to Operational mode, we need to create firewall rules to permit any network traffic that is required by our plant for correct operation.
In our example system, the HMI software uses the Modbus TCP protocol to poll process variables from the PLC; so we will set up a firewall rule to allow Modbus TCP traffic from the HMI to reach the PLC.

1. Double-click the icon for the PLC (FS_PLC_0001) in the Tofino CMP Network Editor and select its Firewall tab.
2. Drag the HMI icon (FS_HMI_0001) from the Network view (top left in the Tofino CMP) and drop it on the 'Talker Rules' item in the PLC's Firewall tab.
3. Drag the "Modbus TCP" protocol from the Tofino CMP's "Protocols" view and drop it on the FS_HMI_0001 icon in the PLC's Firewall tab.

After these steps are complete, the PLC's firewall tab should look like the example in Figure 9.

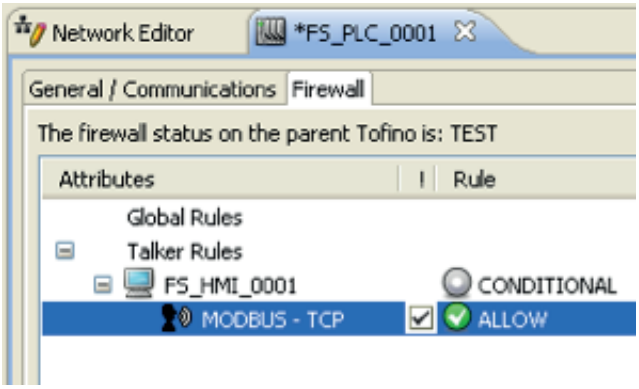


Figure 9: Modbus/TCP traffic between HMI and PLC

Once this rule is in place, click the 'OK' button to save the rule and download it to the PLC Tofino SA. The same rule should also be added to the firewall tab on FS_HMI_0001, by dragging and dropping the PLC (FS_PLC_0001) icon as the talker. Once this is done, there should be no more Exception Heartbeats displayed in the Tofino CMP's Event View for Modbus TCP traffic.

Step 3: Testing Rules before Commissioning

The Tofino Security Appliances may be run in Test mode for a period of time to ensure that all required firewall rules have been set up, and no more firewall Exception Heartbeats. Once this is done, the Tofino Security Appliances may be set to Operational mode to both activate the VPN tunnel and enable the Firewall LSM to filter traffic entering and exiting the tunnel.

Summary: Layered Security – VPN and Firewall

The Tofino VPN solution creates secure 'tunnels' of communication over untrusted networks, such as the Internet or corporate business networks. Unlike other VPNs, the Tofino VPN is easy to deploy, test, and manage. This ensures that good security is not compromised because of configuration errors.
The Tofino VPN supports legacy automation devices and protocols and is industrially hardened. Best of all, it can be combined with other Tofino LSMs, such as the Tofino Firewall LSM or the Tofino Modbus TCP Enforcer LSM, to provide a comprehensive security solution. The combination of VPN and firewall gives control systems the ideal level of security – the VPN secures the critical traffic from external attacks or events and the firewall ensures that internal issues on one side of the VPN can't migrate to the other side.

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-108 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