ConneXium

Product data sheet

ConneXium Tofino Firewall

Description

The ConneXium TCSEFEA Tofino Firewall is a security appliance that provides levels of protection against cyber threats for industrial networks, automation systems, SCADA systems, and process control systems. This Firewall is designed to permit or deny communications between devices connected to the external network connection of the Firewall and the protected devices connected to the internal network connection. The Firewall can restrict network traffic based on user defined rules that would permit only authorized devices, communication types and services.

The ConneXium Tofino Firewall includes built-in security modules and an off-line configuration tool for creating secure zones within an industrial automation environment.

Features

> Built-in Security Modules include:
- Firewall
- Event Logger
- Modbus/TCP Enforcer

> The stateful Firewall Module compares network traffic against a set of user-defined rules and allows or denies traffic based on the rules.

> The Event Logger Module captures security events and alarms, forwarding them to a Syslog server and manual downloading to USB memory.

> The Modbus/TCP Enforcer Module performs detailed content inspection and filtering of Modbus messages. Unauthorized access or incorrectly formatted packets are blocked and alarm message are generated.

> The Tofino Configurator is a menu based tool and designed for the Controls Engineer. It allows the user to easily select:
- Devices to be protected by Firewall
- Unprotected devices with access to protected devices
- Communication protocols allowed
- Types of communication (message types)

> The Tofino Configurator includes templates for Schneider Electric PLC's and over 50 industrial communication protocols

> Supports data packets using the Ethernet II Framing

Schneider Electric

Model

The model number and description of Tofino Firewall is shown below:

TCSEFEA23F3F20	**Tofino Firewall - 10/100BASE TX**

Firewall Overview

- A firewall is an appliance that controls and monitors traffic between networks (or portions of the same network) to help protect computers and devices. It compares the traffic passing through the firewall to a predefined set of rules, discarding traffic that does not meet the rule criteria.
- The ConneXium Tofino Firewall is designed specifically for use in industrial SCADA, automation and control systems. Its capabilities include:
    - Configuration by control engineers, allowing them to specify the devices that can communicate with each other and the protocols they can use.
    - Modbus communication monitoring for correct format.
    - The ability for the user to specify which Modbus commands can be used and what data values can be accessed on each protected Modbus slave device.
    - Physical and logical separation of the control network and plant networks.
    - Division of the control network into security zones based on systems or functions.
    - Ability to hide the network structure and devices of the control system from outside snooping.
    - Conformance to industrial environment standards for continuous operation on the plant floor.
    - Integration with industrial controls and automation protocols, using similar configuration tools

Security Modules

The ConneXium Tofino Firewall is designed to help protect an Industrial Ethernet network from both internal and outside threats. The following is a description of the three built-in Security Modules:

Firewall

Manages rules for stateful monitoring and control of communication traffic passing through the Tofino ConneXium Firewall. Capabilities include:

- Specifying the devices connected to either the external or internal ports on the Tofino ConneXium Firewall.
- Identifying which devices can communicate through the Tofino ConneXium Firewall and to whom.
- Defining the permitted communication initiation direction of each session.
- Selecting the permitted application protocols for any device.
- Defining rate limit controls for traffic type or session.
- Automatically blocking SYN floods and other Denial of Service (DoS) attacks.
- Full stateful inspection of TCP/IP traffic.
- Specifying logging for either allowed or blocked traffic.
- The use of special rules for advanced traffic filtering and vulnerability defense, such as buffer overflow protection.

Modbus/TCP Enforcer A content inspector that checks every Modbus command and response against a list of 'allowed' commands, capabilities include:

- Predefined Read-Only, Read-Write and Programming message type filtering.
- User definable lists of allowed Modbus commands, registers and coils.
- Automatic blocking and reporting of traffic that does not match the rules.
- Protocol 'Sanity Check' blocks any traffic not conforming to the Modbus standard.
- Support for multiple master and slave devices.
- Certified Modbus compliant by Modbus-IDA.
- User-settable options on a per-connection basis:
  - Permitted Modbus function codes
  - Permitted register or coil address range
  - Permitted Modbus unit IDs
  - Sanity check enable/disable
  - Modbus state tracking enable/disable

Event Logger Records security and events alarms to a remote syslog server and locally in the ConneXium Tofino Firewall for added protection. Capabilities include:

- Logging of event messages to internal device memory and external (syslog) monitoring systems.
- Continuous event log back up, even if syslog communications are interrupted.
- Recording of up to 4,000,000 security event records to the ConneXium Tofino Firewall memory for offloading to a USB memory device.
- Providing NERC-CIP standards compliance: Monitoring (CIP 005), Ports & Services (CIP 007), and Security Status Monitoring (CIP 007).
- Enabling ISA IEC 62443[1] compliance when used to create zones of security for devices with similar security requirements.

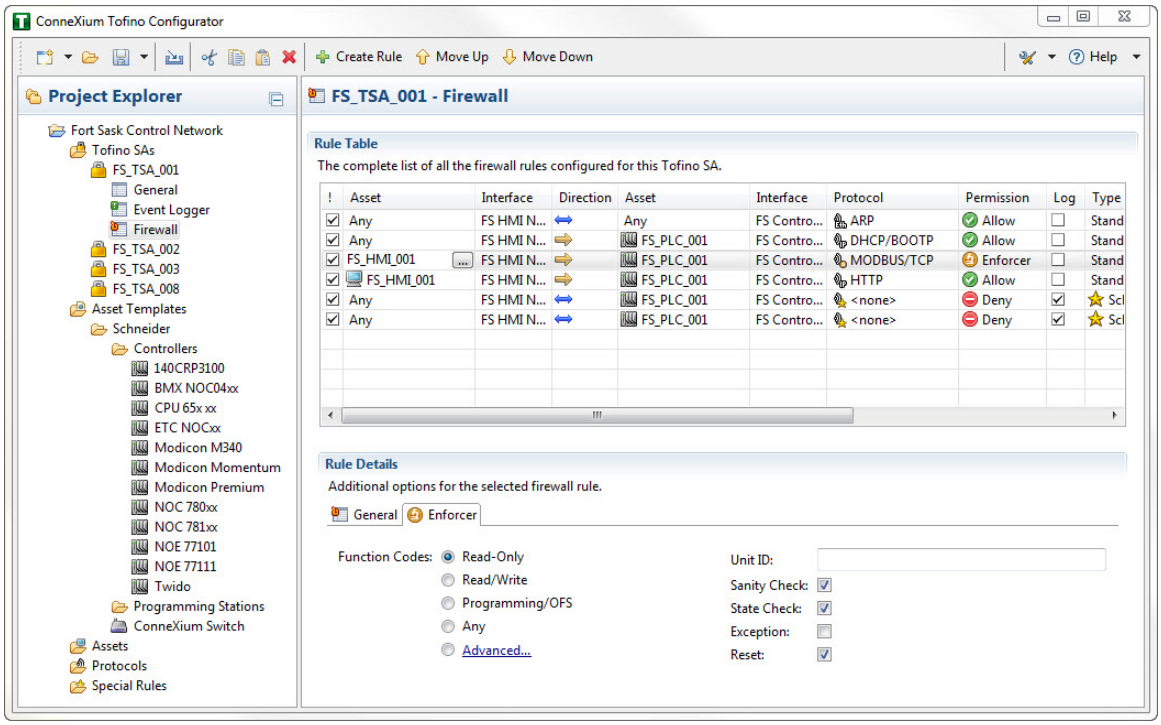
[1] Formerly ANSI/ISA-99 standards

Tofino Configurator

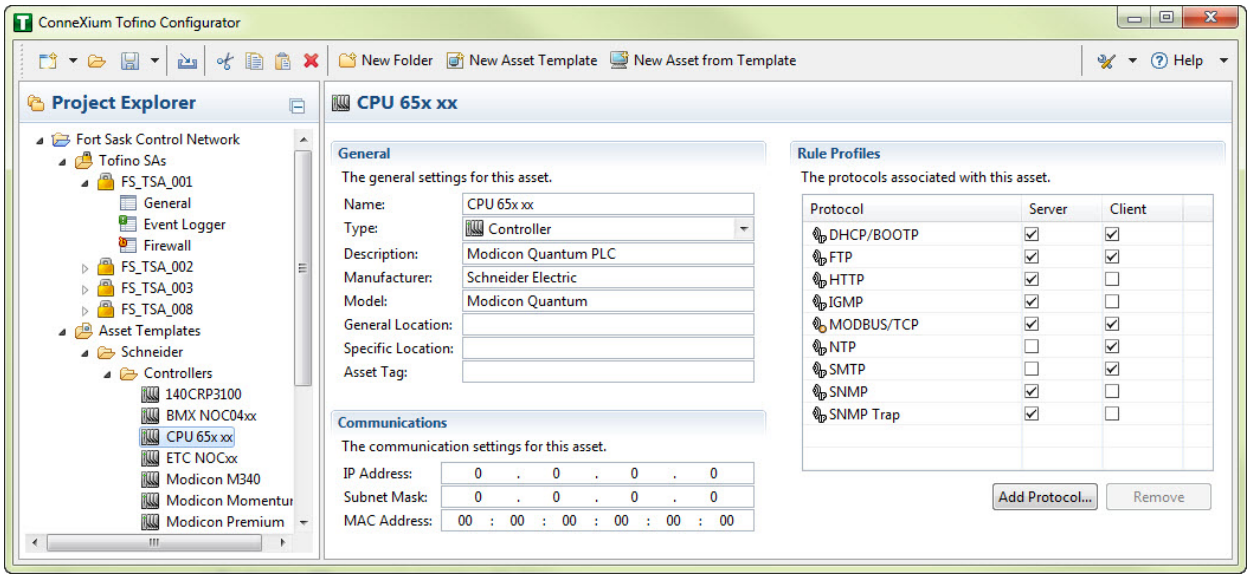
The ConneXium Tofino Configurator is a menu-based software tool that is used to create configuration files for the ConneXium Tofino Firewall. This configurator tool is designed for control engineers and is similar to the configurator interfaces for PLC systems. It does not require an extensive knowledge of networking or cyber security. This configurator includes pre-configured profiles for the major Schneider Electric products and automatic rule-generation, along with the ability to create profiles for other automation and control products. It can import Tofino security profiles or special rules that address newly disclosed vulnerabilities or malware. Protection is immediately effective and does not require any changes to automation equipment or network configurations

The ConneXium Tofino Configurator is included on the CD that is shipped with each firewall. It operates on any PC that supports Windows XP, Windows 2003 Server, Windows 2008 Server or Windows 7 operating systems. Once set-up is complete, use the Configurator to create an off-line configuration file, which is saved to a USB memory device for transfer to the ConneXium Tofino Firewall.

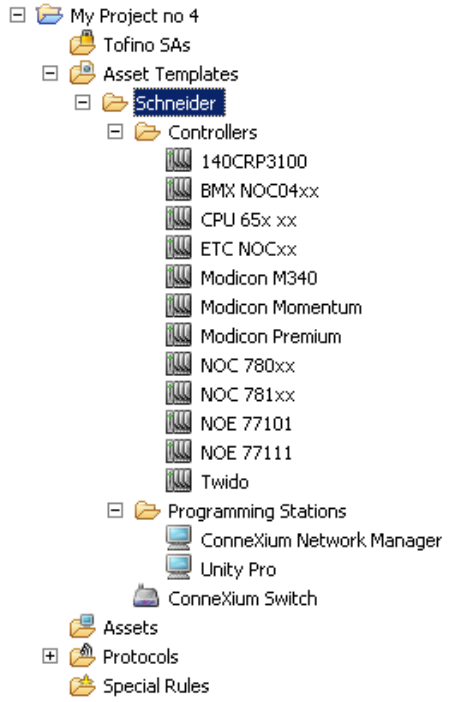
Below is the display for Firewall Security Modules that includes the rule table. In this table you can select the assets to be connected to both sides of the firewall, communication initiation direction, the communication protocol, the permission type, and an option to log denied communications.



The following figure shows a typical asset template for a Quantum Controller, with details such as the communication protocols used by the PLC. This template also includes selections for the model range, description and manufacture, and default Ethernet communication. The menu selections allows you to select additional communication protocols, and enter information for the selected Quantum controller such as IP address, location, and tag number. The templates allow for easy and consistent creation of devices in a project and enables the ConneXium Tofino Configurator to automatically generate the appropriate firewall rules for any product.



The ConneXium Tofino Configurator includes built-in templates for the current Schneider Electric Automation products that include Ethernet communication capability. It also allows a user to create and import templates for other Ethernet enabled devices. The figure below shows the selection Schneider Electric products asset templates.



Technical Specifications

Supply Voltage	12 to 48 Vdc or 24 Vac
Operating Voltage Range	9.6 to 60 Vdc or 18 to 30 Vac
Hold up time	Min 10 ms @ 20.4 Vdc
Power Consumption @ 24 VDC	
TCSEFEA23F3F20	6.9 W Max.
Module Dimension	60 W X 145 H X 123mm D (2.36 X 5.71 X 4.84 in.)
Weight	615g (21.7 oz.)
Operating Temperature	0° to 60° C (32° to 140° F)
Storage Temperature	-40 to 70° C (-40° to + 158° F)
Relative Humidity	10% to 95% non condensing
Protection	IP 20
Pollution Degree	2
Altitude	2000 m (6560 ft.)
Mounting	35 mm DIN Rail
Laser Protection	Class 1, conforming to EN60825-1 (2007)
Shock and Vibration	IEC 60068-2-6, IEC 60068-2-27
EMC Immunity	EN 61000-4-2, -3,-4,-5,-6,-9
EMC Emitted Interference	EN55022 class A / FCC 47 CFR Part 15 class A
Approvals	cUL 508:1988 CE Certificate German Lloyd VI-7-3 Part 1 Ed. 2003
Conformance	RoHS Directive
LED Indicators	Power Supply 1 Power Supply 2 Fault Mode External Port Link Status / Save Operation Internal Port Link Status / Load Operation Serial Port (V.24) Status / Reset Operation
MTBF	240,024 hr. at 25°C GB

Author: Joe Benedetto
October 4, 2012

Accessories

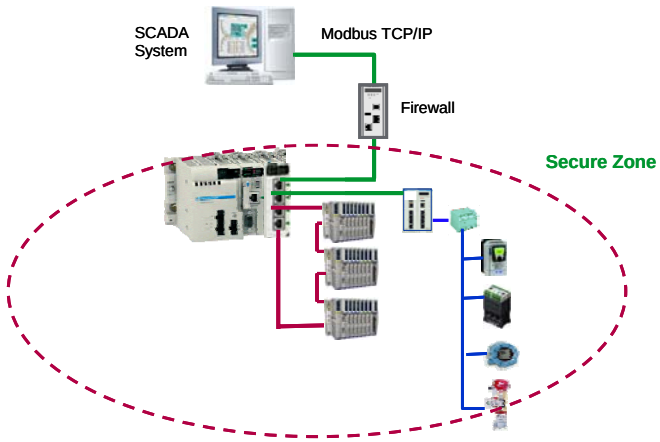
Description	Part No.
Terminal cable – for serial port	490NTRJ11

Use a version 2.0 USB storage devices as the memory back-up adapter for the ConneXium Tofino Firewall. Models that have been tested include the Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar, and the Schneider Electric Model TCSEAM0100.

Network Architectures

A ConneXium Tofino Firewall can be deployed to help protect control systems from unauthorized access through their Ethernet connection. It can also be used to create a secure zone to help protect critical portions of a distributed control system.

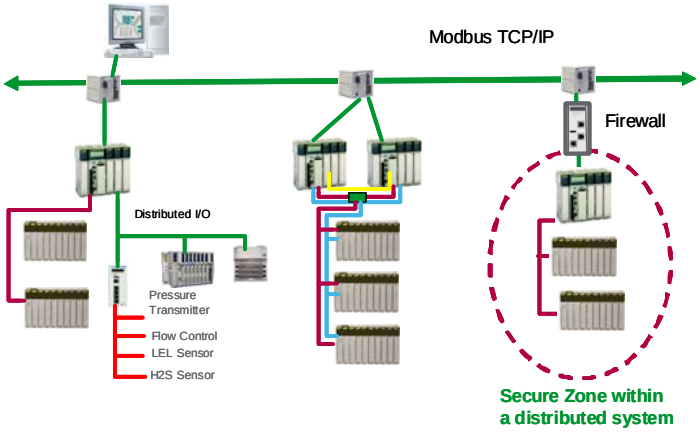
Below are 2 examples of these uses for the ConneXium Tofino Firewalls.



Stand-Alone Control System

Stand-alone systems that are controlling critical operations or infrastructure applications are now being required to meet specified security levels that support continuous operation.

This example shows a system where there is a requirement to limit access to the PLC system. Because of the ConneXium Tofino Firewall and the Modbus/TCP Enforcer module, only the SCADA system can access the PLC. The SCADA system is limited to reading and writing to specified memory locations only.



Secure Zone

In a distributed control architecture, there may be a control system operating a critical process or safety system that requires a higher level of security.

A Firewall can be added to the Ethernet connection to the critical control system or safety system, providing an additional level of security and creating a secure zone.