ConneXium

TCSEFEA Tofino Firewall
Benutzerhandbuch

S1B76072.00

www.schneider-electric.com

Schneider Electric

Inhalt

Sicherheitshinweise

Wichtige Informationen

Beachten Sie: Lesen Sie diese Anweisungen gründlich durch und machen Sie sich mit dem Gerät vertraut, bevor Sie es installieren, in Betrieb nehmen oder warten. Die folgenden Hinweise können an verschiedenen Stellen in dieser Dokumentation enthalten oder auf dem Gerät zu lesen sein. Die Hinweise warnen vor möglichen Gefahren oder machen auf Informationen aufmerksam, die Vorgänge erläutern bzw. vereinfachen.

Erscheint dieses Symbol zusätzlich zu einem Warnaufkleber, bedeutet dies, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung des Hinweises Verletzungen zur Folge haben kann.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine unmittelbar gefährliche Situation aufmerksam, die bei Nichtbeachtung **unweigerlich** einen schweren oder tödlichen Unfall zur Folge hat.

⚠ WARNUNG

WARNUNG verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – Tod oder schwere Verletzungen **zur Folge haben** kann.

⚠ VORSICHT

VORSICHT verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – leichte Verletzungen **zur Folge haben** kann.

Bitte beachten: Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, gewartet und instand gesetzt werden.
Schneider Electric haftet nicht für Schäden, die aufgrund der Verwendung dieses Materials entstehen.

Über dieses Handbuch

Gültigkeitsbereich
Die in diesem Buch enthaltenen Daten und Abbildungen sind nicht verbindlich. Wir behalten uns das Recht vor, unsere Erzeugnisse im Rahmen unserer Strategie der ständigen Produktentwicklung zu ändern. Die Informationen in dieser Unterlage können ohne Ankündigung geändert werden und dürfen nicht als für Schneider Electric verbindlich ausgelegt werden.

Produktbezogene Informationen
Schneider Electric übernimmt keine Verantwortung für Fehler, die gegebenenfalls in dieser Unterlage auftreten. Falls Sie Anregungen für Verbesserungen oder Ergänzungen haben oder Fehler in dieser Veröffentlichung gefunden haben, dann verständigen Sie uns bitte.

Kein Teil dieser Unterlage darf in irgendeiner Form oder auf irgendeine Weise elektronisch oder mechanisch vervielfältigt werden, einschließlich von Fotokopien, ohne ausdrückliche schriftliche Genehmigung von Schneider Electric.

Alle einschlägigen staatlichen, regionalen und lokalen Sicherheitsbestimmungen müssen beim Installieren und Anwenden dieses Produkts beachtet werden. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemdaten zu gewährleisten, darf nur der Hersteller Reparaturen an den Teilen vornehmen.

Bei Einsatz der Geräte für Anwendungen mit technischen Sicherheitsanforderungen bitte die einschlägigen Anweisungen beachten.

Das Unterlassen der Verwendung von Schneider Electric-Software oder freigegebener Software zusammen mit unseren Hardware-Erzeugnissen kann zu falschen Arbeitsergebnissen führen.

Das Unterlassen der Beachtung dieser produktbezogenen Warnung kann zu Verletzungen oder Gerätebeschädigungen führen.

Benutzerkommentar
Ihre Anmerkungen und Hinweise sind uns jederzeit willkommen. Senden Sie sie einfach an unsere E-mail-Adresse: techpub@schneider-electric.com

Weiterführende Dokumentation

Titel	Referenznummer
Anwender-Handbuch TCSEFEA ConneXium Tofino Firewall	S1B76072
Installationsanleitung TCSEFEA ConneXium Tofino Firewall	S1B69360

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Hinweis:	Ein Hinweis betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in Bedienoberfläche

1 Einführung in den ConneXium Tofino Configurator

Bei der industriellen Sicherheitslösung ConneXium Tofino handelt es sich um ein umfassendes Paket zur Sicherung industrieller Leitsysteme, insbesondere im Bereich lokaler Netze (LANs). Das System besteht aus drei Kernkomponenten:

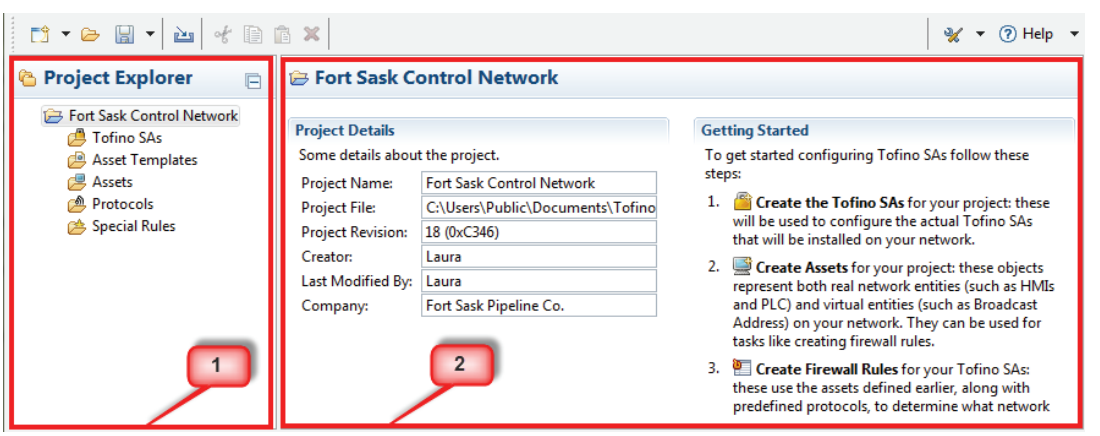
- ConneXium Tofino Firewall; diese wird im vorliegenden Handbuch als Tofino Sicherheitsvorrichtung (Tofino Security Appliance) oder als Tofino SA bezeichnet. Hierbei handelt es sich um industriell gehärtete Geräte, die vor schutzbedürftigen (einzelnen bzw. Gruppen von) Mensch-Maschine-Schnittstellen (HMIs), verteilten Prozessleitsystemen (DCS), speicherprogrammierbaren Steuerungen (SPS) oder Fernbedienungsterminals (RTUs) installiert werden.
- LSM: ladbare Tofino-Sicherheitsmodule; hierbei handelt es sich um Software-Module, die Sicherheitsdienste bereitstellen, etwa in Form einer Firewall oder eines Ereignisprotokolls (Event Logger). Jedes LSM wird auf den betreffenden Tofino SAs aktiviert. Je nach Anforderungen des Leitsystems können Sie so die Sicherheitsfunktionen der Firewalls bedarfsgerecht anpassen. Die LSMs von ConneXium-Systemen werden werkseitig vorinstalliert.
- ConneXium Tofino Configurator - ein Windows-basiertes, netzunabhängiges Management-System zum Konfigurieren der einzelnenTofino SAs.

Verwenden Sie den ConneXium Tofino Configurator auf einem netzunabhängigen Rechner, um Konfigurationsdaten für jede Tofino SA in Ihrem Betrieb festzulegen. Wenn Sie die Konfiguration fertiggestellt haben, können Sie eine Kopie der Konfigurationsdaten auf ein USB-Speichermedium sichern. Mit dem Speichermedium können Sie die Konfiguration dann in die betreffenden Tofino SAs laden. Sie können auch Konfigurationsdaten von einer Tofino SA abrufen und diese zurück in denConneXium Tofino Configurator laden, um zu verifizieren, dass im Feldbereich die richtige Konfiguration verwendet wird.

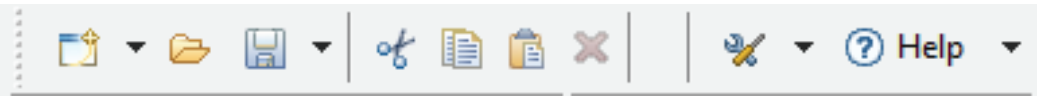
1.1 Navigieren durch den ConneXium Tofino Configurator

Hinsichtlich Gestaltung und Bedienung ist der ConneXium Tofino Configurator an den Windows Explorer angelehnt, den Sie auf Ihrem Rechner zum Navigieren zwischen Dateien und Ordnern verwenden. Sie können den ConneXium Tofino Configurator daher umgehend benutzen.

- 1 - Das Menüfenster „Projekt-Explorer“, wo die Tofino SAs, Ressourcenvorlagen, Ressourcen, Protokolle und Sonderregeln in einem Baumformat angezeigt werden (vergleichbar mit der Darstellung von Dateien im Windows Explorer). Sie können alle Objekte im Menüfenster „Projekt-Explorer“ anklicken und sich die entsprechenden Einzelheiten im Menüfenster „Details“ ansehen. Wenn Sie den Wurzelordner anklicken, wird eine Tabelle mit den definierten Objekten des jeweiligen Typs angezeigt. Wenn Sie z. B. auf den Ordner „Ressourcen“ (Assets) klicken, wird eine Tabelle mit den bereits definierten Ressourcen des Projektes angezeigt.
- 2 - Das Menüfenster „Details“, wo die spezifischen Informationen zu den im Projekt-Explorer ausgewählten Objekten angezeigt werden. Hier können Sie einzelne Werte für ein Objekt editieren.



Der ConneXium Tofino Configurator verfügt über eine Werkzeugleiste, mit der Sie unterschiedliche Aktionen an Objekten in einem Projekt durchführen können.



Die Werkzeugleiste enthält 3 Abschnitte:

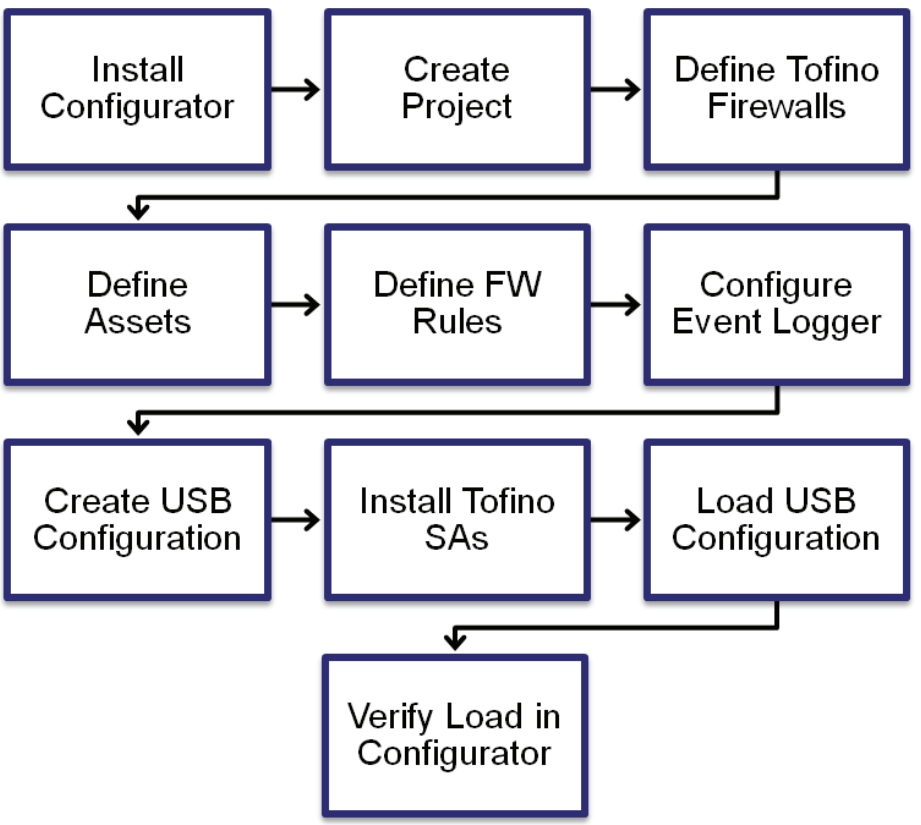
- Projekt editieren (Project Edit commands) - Dieser Bereich wird links außen in der Werkzeugleiste angezeigt und enthält Befehle für die Verwaltung von Projektdateien und den zugehörigen Daten: Er beinhaltet folgende Optionen:
  - Erzeugen von neuen Projekten, Ressourcen, Ressourcen-Vorlagen, Protokollen oder Tofino SAs unter Verwendung eines Assistenten;
  - Ein bestehendes Projekt öffnen;
  - Ein Projekt speichern;
  - Vordefinierte Ressourcen-Vorlagen, Protokolle, Sonderregeln und Sicherheitsprofile importieren
  - Objekte und Felder ausschneiden, kopieren, einfügen und löschen.

- Kontextbefehle (Context commands) - Dieser Bereich wird in der Mitte der Werkzeugleiste angezeigt und enthält Befehle, die sich auf die aktuell bearbeiteten Inhalte beziehen. Je nach Art des im Project Explorer selektierten Objekttyps erscheint hier eine andere Befehlsliste.

- Hilfe und Konfiguration (Help and Configuration commands) - Dieser Bereich wird rechts außen in der Werkzeugleiste angezeigt und stellt folgende Funktionen zur Verfügung:
  - Prüfprotokolle (Audit Logs): Aufrufen und Verwalten des Prüfsystems
  - Einstellungen (Preferences): Bearbeiten von Konfigurationen (wie z. B. den Speicherort der Prüfdatei)
  - Befehle des Hilfemenüs (Abwärtspfeil rechts von „Hilfe“) einschließlich der Menüpunkte „About (Über dieses Programm)“ und „Display Help (Hilfe anzeigen)“.

2 10 Schritte zu einem sicheren Leitsystem

Der ConneXium Tofino Configurator ist so konzipiert, dass er Ihnen die Installation von Sicherheits-Firewalls in einem industriellen Leitsystem so leicht wie möglich macht. Führen Sie die folgenden Schritte aus, um die industrielle Sicherheitslösung ConneXium Tofino zu installieren und zu konfigurieren.



☐ Installieren Sie den ConneXium Tofino Configurator auf Ihrem Rechner.
☐ Erzeugen Sie ein Tofino ConneXium-Projekt.
☐ Definieren Sie die Tofino SAs für Ihr Projekt: Anhand dieser Informationen konfigurieren Sie dann die tatsächlichen Tofino SAs, die in Ihrem Netz installiert werden.

- ☐ Definieren Sie Ressourcen für Ihr Projekt: Diese Objekte stellen sowohl physische Netzinstanzen innerhalb Ihres Netzes dar (z. B. HMIs und PLCs) als auch virtuelle Instanzen (z. B. Broadcast-Adressen). Sie verwenden diese, um unterschiedliche Aufgaben (wie das Erzeugen von Firewall-Regeln) einfacher zu bewerkstelligen.
- ☐ Definieren Sie Firewall-Regeln für die Tofino SAs: Diese verwenden die von Ihnen erzeugten Ressourcen sowie die mit dem ConneXium Tofino Configurator ausgelieferten vordefinierten Protokolle und Sonderregeln, um festzulegen, welchen Netzverkehr die jeweilige Tofino SA zulässt oder blockiert. Über die Auswahl der Firewall haben Sie Zugriff auf den „Modbus TCP Enforcer“.
- ☐ Konfigurieren Sie den Event Logger (optional): Geben Sie die Adressdaten des Systemprotokollservers ein, an den die Alarm- und Event-Meldungen der Tofino SA gesendet werden sollen. Alternativ können Sie die Tofino SA so konfigurieren, dass die Protokolle lokal in der Tofino SA gepeichert werden. Sie können diese dann später auf ein USB-Speichermedium übertragen.
- ☐ Erzeugen Sie eine Konfiguration auf einem USB-Speichermedium: Hierdurch erstellen Sie verschlüsselte Konfigurationsdateien auf dem USB-Speichermedium, welche Sie in die Tofino SAs laden können.
- ☐ Installieren Sie die Tofino SA-Hardware in Ihrem Netz, und zwar zwischen einem oder mehreren zu schützenden Geräten und dem Rest des Netzes.
- ☐ Laden Sie die Konfiguration in die Tofino SAs: Stecken Sie das USB-Speichermedium mit den Konfigurationsdateien in den USB-Port der entsprechenden Tofino SA und laden Sie die Konfiguration dort ein.
- ☐ Überprüfen Sie die Konfiguration: Mit dem entsprechenden Befehl rufen Sie die Konfigurations-Ladeprotokolle von dem USB-Speichermedium ab, mit dem Sie Konfigurationen in eine oder mehrere Tofino SAs geladen haben. Hierdurch können Sie die Konfigurationen der Tofino SAs im Feldbereich aufzeichnen und in Ihrem Projekt speichern.

Sie haben nun die industrielle Sicherheitslösung ConneXiumTofino installiert und damit die Sicherheit Ihres Prozesssteuerungsnetzes erheblich verbessert.

Hinweis: Während der Erstkonfiguration oder während der Aktualisierung der Konfiguration lässt die Tofino SA den Netzverkehr ohne Einschränkungen passieren. Die Firewall-Regeln werden erst dann wirksam, wenn Sie die Erstkonfiguration oder die Aktualisierung der Tofino SA abgeschlossen haben; d. h. der Netzbetrieb wird erst dann beeinflusst, wenn Sie den vollständigen Regelsatz geladen haben. Das Laden einer durchschnittlichen Konfiguration dauert etwa 30 Sekunden.

3 Installation des ConneXium Tofino Configurators

Dieser Abschnitt enthält detaillierte Informationen zur Installation des ConneXium Tofino Configurator auf einem Rechner, auf dem bislang noch kein ConneXium Tofino Configuratorinstalliert war.
Führen Sie die nachstehenden Schritte aus, um eine neue Version des ConneXium Tofino Configurator zu installieren:

☐ Führen Sie das Installationsprogramm für den ConneXium Tofino Configurator aus.
☐ Geben Sie den entsprechenden Lizenz-Aktivierungsschlüssel ein. Sie finden diesen auf der Hülle der CD, die mit der ConneXium Tofino Firewall ausgeliefert wird.

Erste vorbereitende Schritte

Halten Sie zur Installation der ConneXium Tofino Configurator-Software folgendes bereit:

- die Installations-CD für den ConneXium Tofino Configurator;
- den Lizenz-Aktivierungsschlüssel (eine Zeichenfolge aus 25 Buchstaben und Ziffern, wie z. B. X4QP9-RMNRQ-B59SD-AG5H6-KSFRW).

Ausführen der Installation des ConneXium Tofino Configurators

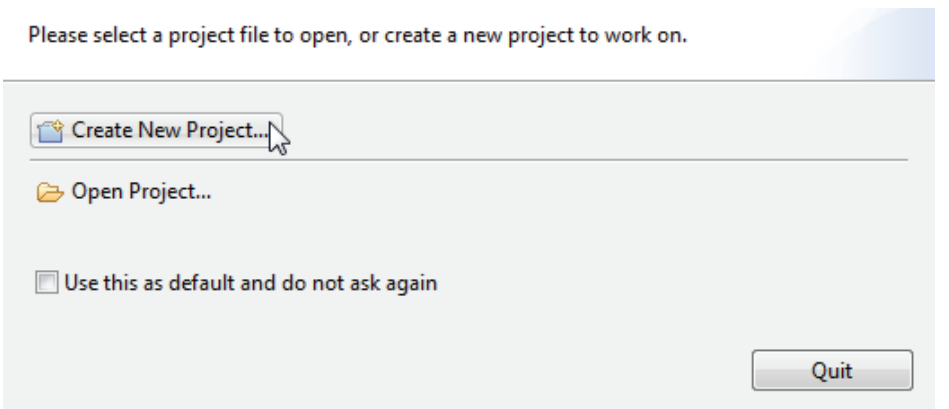
☐ Starten Sie das Installationsprogramm für den ConneXium Tofino Configurator von der CD.
☐ Folgen Sie den Bildschirmanweisungen, um den ConneXium Tofino Configurator zu installieren.
☐ Geben Sie im Bildschirm-Menü `Lizenz aktivieren (Activate Your License)` Ihren Lizenzschlüssel und die sonstigen benötigten Daten ein.

4 Projekte erzeugen

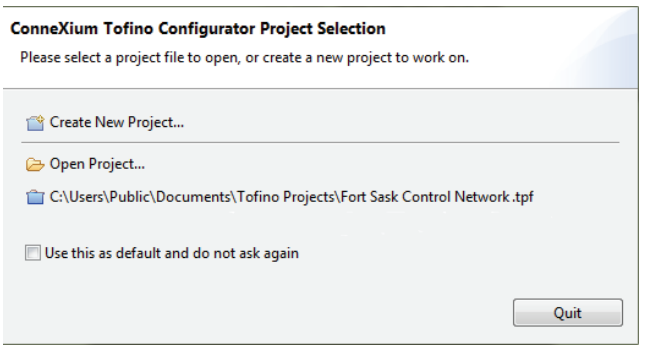
Der ConneXium Tofino Configurator verwendet Projektdateien, um eine oder mehrere Tofino SAs zu koordinieren, die zusammen in einer Anlage oder in einem Projekt eingesetzt werden. Jede Projektdatei enthält die Konfigurationen der von ihr verwaltetenTofino SAs und außerdem sonstige Daten wie Netzressourcen und gemeinsame Protokolle.

Wenn Sie den ConneXium Tofino Configuratorzum ersten Mal starten, können Sie zwischen zwei Möglichkeiten wählen:

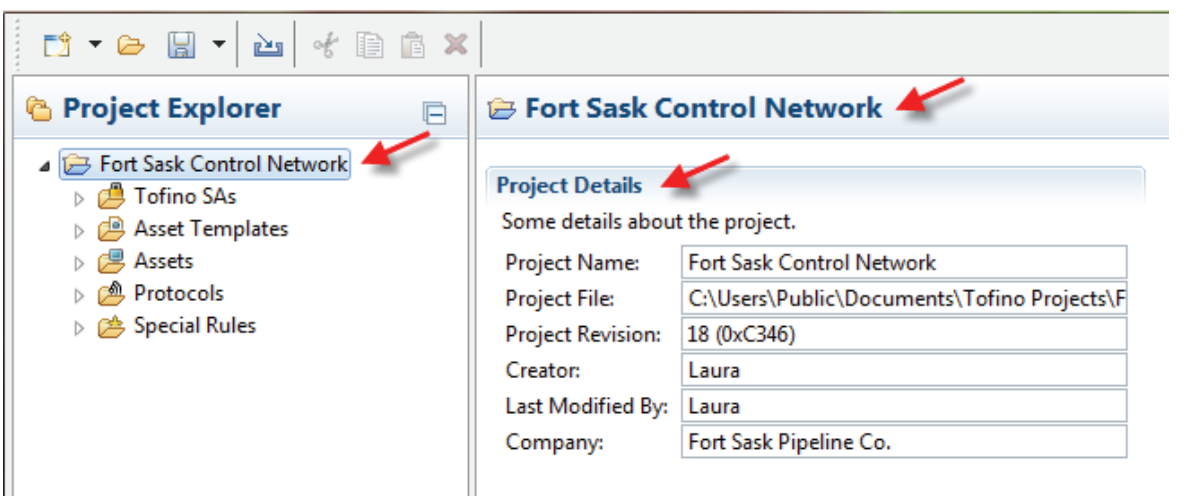
- Informationen zum Erstellen eines neuen Projektes finden Sie unter „Ein neues Projekt erzeugen“.
- Ein bestehendes Projekt öffnen.



Wenn Sie eine Projektdatei bearbeitet haben, wird diese anschließend im Startfenster angezeigt und kann mit einem Klick geöffnet werden. Sie können auch eine bestimmte Projektdatei als Standardprojekt definieren, das bei jedem Start des ConneXium Tofino Configurator automatisch geöffnet wird. Im Menü „Projekteinstellungen“ (Project Preferences) können Sie das Standardprojekt entfernen oder ändern. Siehe hierzu auch „Einstellungen“.

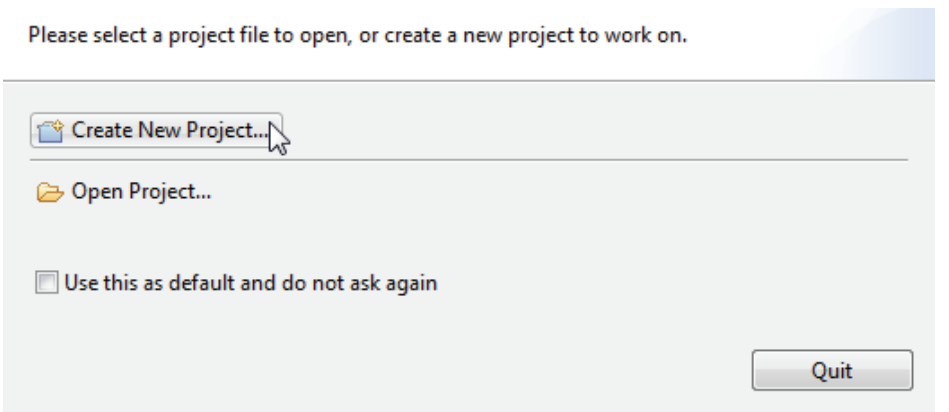


Nachdem das Projekt geöffnet ist, können Sie durch Auswählen des oberen Ordners im Projekt-Explorer die Projektdetails im Menüfenster „Details“ aufrufen. Diese beinhalten Informationen wie den Projektnamen, den Speicherort der Projektdatei auf dem Rechner, den Revisionsstand des Projektes sowie den Ersteller der Datei und den Firmennamen.

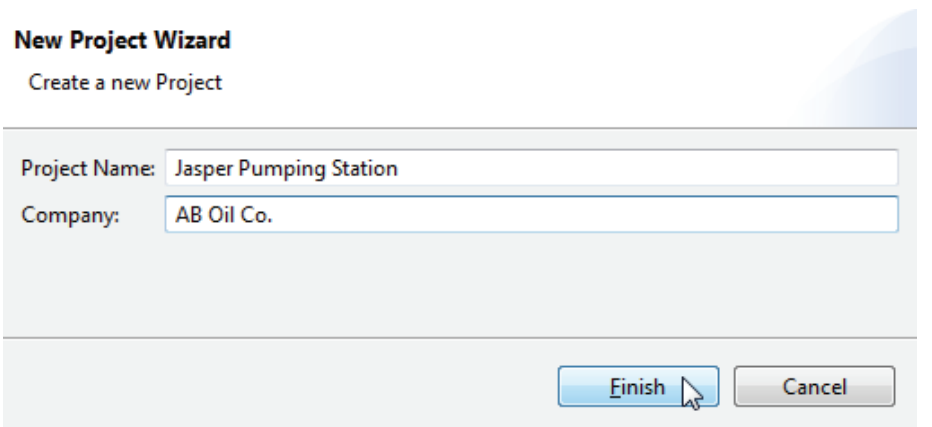


4.1 Ein neues Projekt erzeugen

Erzeugen Sie bei der ersten Verwendung des ConneXium Tofino Configurators ein Projekt. Um den Assistenten „Neues Projekt“ aufzurufen, wählen Sie auf dem Startbildschirm `Neues Projekt erzeugen (Create a New Project)`. (Sie können ein neues Projekt auch über den Projekt-Explorer erzeugen. Klicken Sie hierfür auf die Schaltfläche `Neu (New)` und wählen Sie `Projekt (Project)`).



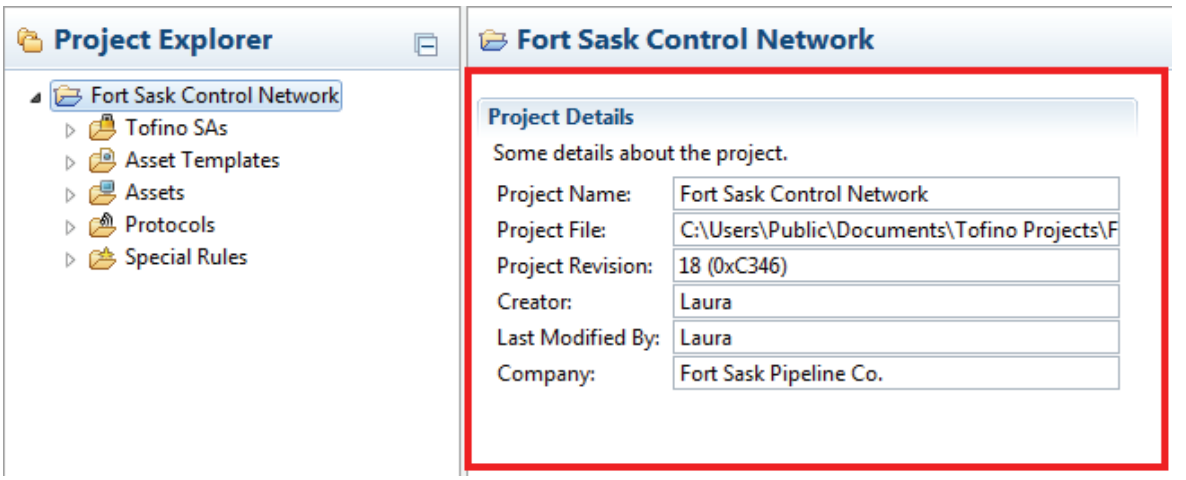
Wenn Sie den Assistenten aufrufen, werden Sie aufgefordert, zwei Felder auszufüllen: `Projektname (Project Name)` und `Firma (Company)`.



4.2 Ein Projekt anzeigen und editieren

Wenn Sie in der Projekt-Explorer-Ansicht auf den Projektnamen klicken, öffnet sich das Menüfenster mit den Details zum Projekt (Project Details). Hier können Sie einzelne Punkte editieren und sich die Projektversion, den Ersteller der Datei und den bzw. die Bearbeiter anzeigen lassen.

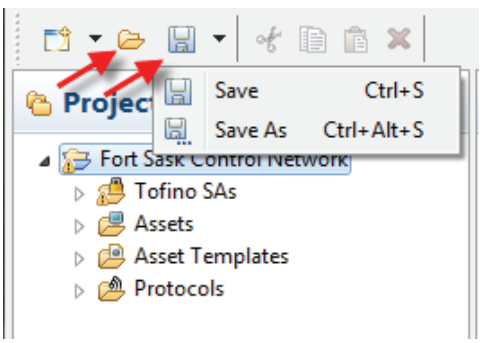
- Projektname (Project Name) - ein benutzerdefinierter Projektname. Die Voreinstellung lautet „Mein Projekt“ (My Project).
- Projektdatei (Project File) - der Name der Datei sowie der Speicherort, von dem die Datei geladen bzw. an dem sie zuletzt gespeichert wurde. Dies ist zugleich der Ort, an dem die Datei beim nächsten Speichervorgang gespeichert wird. Bei neuen, noch nicht gespeicherten Projekten erscheint hier „<ungespeichert>“ (unsaved).
- Projektrevision (Project Revision) - die aktuelle Versionsnummer des Projektes sowie eine spezielle Prüfsumme (Hash-Code), welche die Wahrscheinlichkeit verringert, dass Revisionsnummern versehentlich doppelt vergeben werden. Bei jedem Speichern des Projektes wird die Revisionsnummer hochgezählt.
- Erstellt von (Creator) - verwendet den Windows-Benutzernamen, der bei der Erstellung des Projektes angemeldet war.
- Zuletzt geändert von (Last Modified By) - verwendet den Windows-Benutzernamen, der beim letzten Speichern des Projektes angemeldet war.
- Company - ein benutzerdefinierter Firmenname.


Project Explorer
Fort Sask Control Network
Tofino SAs
Asset Templates
Assets
Protocols
Special Rules
Fort Sask Control Network
Project Details
Some details about the project.
Project Name: Fort Sask Control Network
Project File: C:\Users\Public\Documents\Tofino Projects\F
Project Revision: 18 (0xC346)
Creator: Laura
Last Modified By: Laura
Company: Fort Sask Pipeline Co.

4.3 Projektdateien verwalten

Sie können Projektdateien ebenso wie sonstige Windows-Dateien verwalten. Mit dem ConneXium Tofino Configurator können Sie folgende Aktionen durchführen:

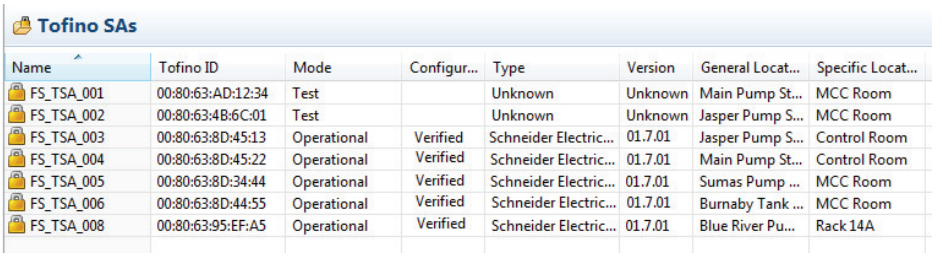
- Open - Eine bestehende Projektdatei öffnen.
- Save - Das aktuelle Projekt in der Projektdatei speichern.
- Save As - Das aktuelle Projekt unter neuem Namen in einer anderen Projektdatei speichern.



Sie können eine Projektdatei – so wie andere Dateien auch – ganz regulär mit dem Windows Explorer löschen.

5 Definieren von Tofino SA-Konfigurationen

Mit den Verwaltungsfunktionen der Tofino SA können Sie die Konfigurationsdaten für mehrereTofino SAs eines einzelnen Projektes erstellen, editieren und löschen.



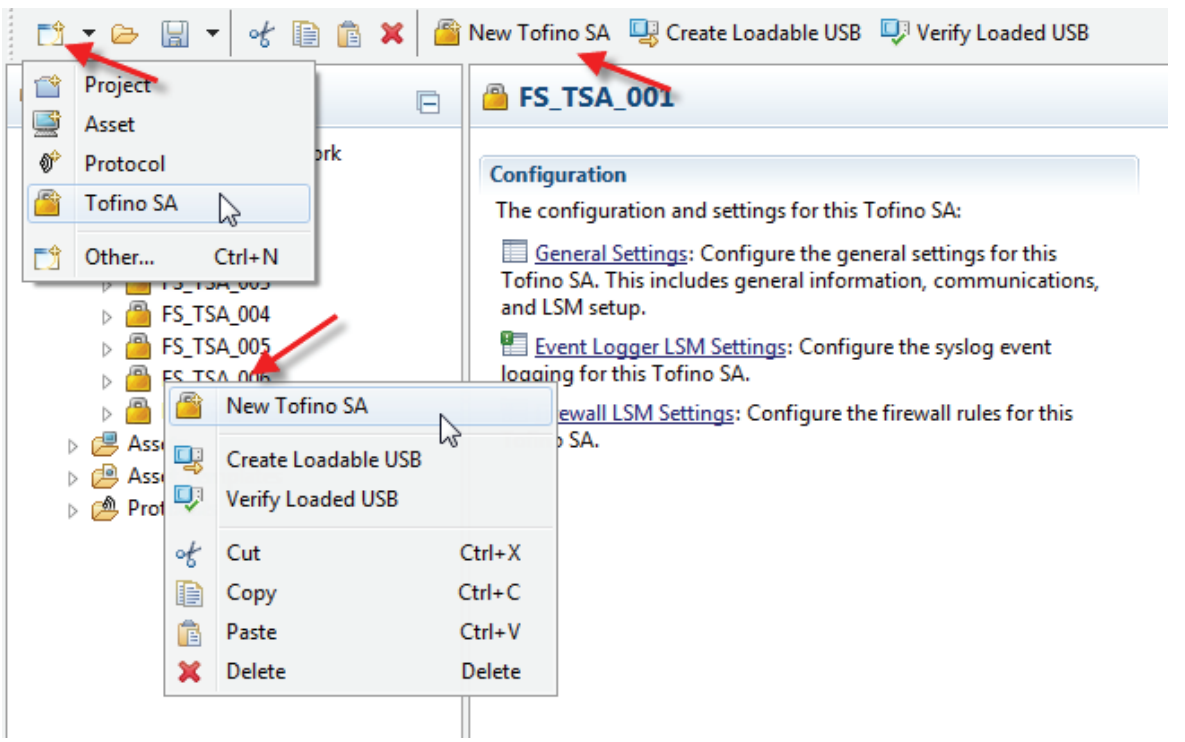
Wenn Sie in der Projekt-Explorer-Ansicht eine bestimmte Tofino SA auswählen, haben Sie folgende Möglichkeiten:

- ☐ Eine neue Tofino SA erzeugen.
- ☐ Die Konfiguration der Tofino SA aufrufen und editieren.
- ☐ Eine portable Konfigurationsdatei erzeugen und diese auf einem USB-Speichermedium sichern. Sie haben anschließend die Möglichkeit, das USB-Speichermedium an eineTofino SA anzuschließen und die Konfigurationsdatei zu laden.
- ☐ Das Ladeprotokoll des USB-Speichermediums gegenprüfen, das Sie zum Laden der Konfiguration verwendet haben. Auf diese Weise können Sie erfolgreiche USB-Ladevorgänge aufzeichnen und bei Bedarf überprüfen.

5.1 Erzeugen einer neuen Tofino SA

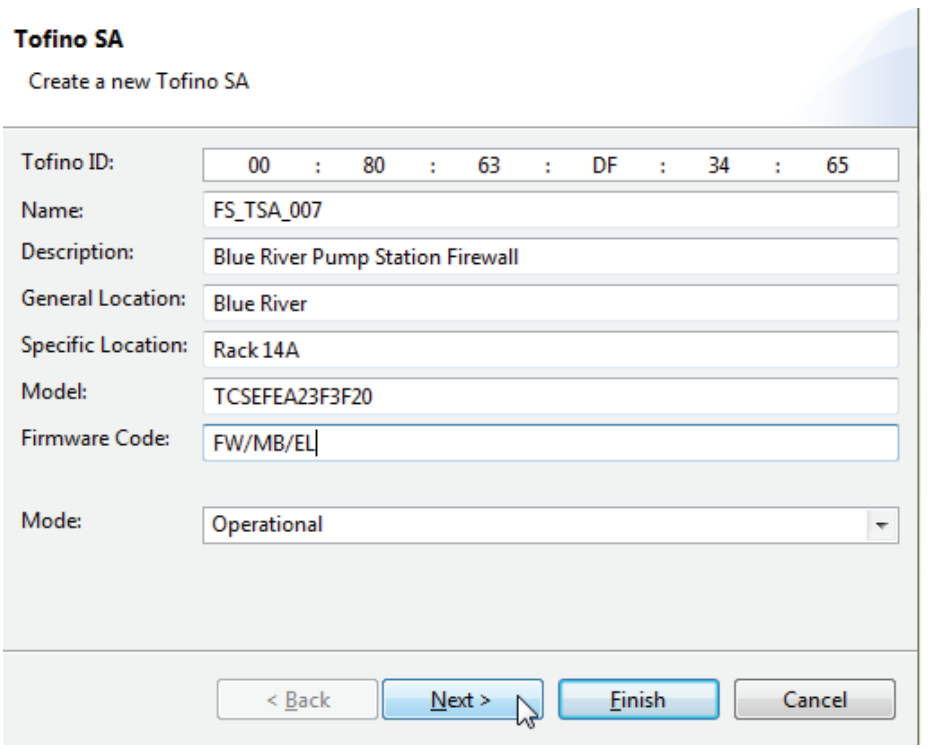
Mit dem Tofino SA-Assistenten können Sie eine neue Tofino SA erzeugen. Dabei stehen Ihnen drei Möglichkeiten zur Verfügung, um den Tofino SA-Assistenten aufzurufen:

- ☐ Klicken Sie auf die Schaltfläche `Neu (New)` und wählen Sie `Tofino SA` aus.
- ☐ Klicken Sie im mittleren Bereich der Werkzeugleiste auf die Schaltfläche `Neue Tofino SA (New Tofino SA)`.
- ☐ Führen Sie einen Rechtsklick auf eine bestehende Tofino SA aus und wählen Sie `Neue Tofino SA`.

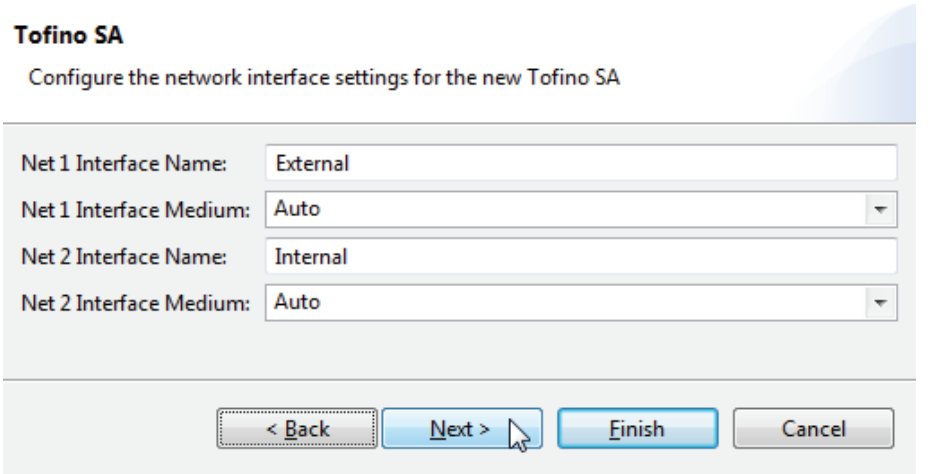


Assistent „Neue Tofino SA“

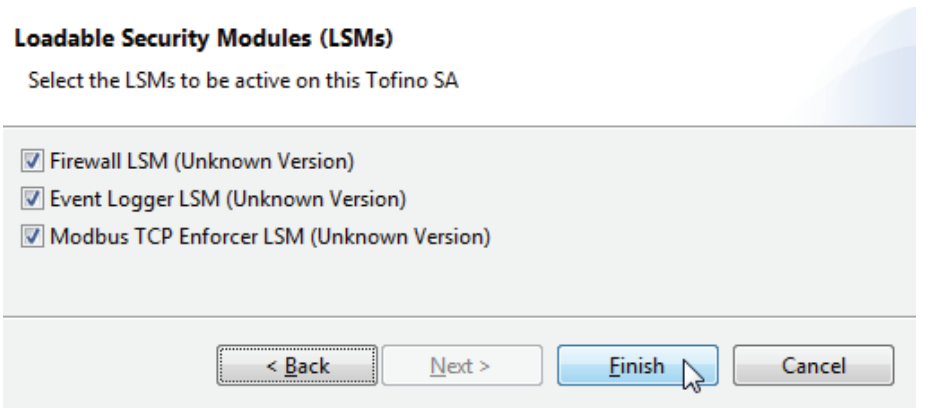
Wenn Sie den Assistenten aufrufen, werden Sie aufgefordert, die Tofino-ID, den Namen, die Beschreibung, den allgemeinen und spezifischen Standort sowie den Modelltyp einzugeben. Der Firmware-Code wird anhand der von Ihnen eingegebenen Modellnummer automatisch berechnet. Wählen Sie zuletzt noch den Modus (Betriebs- oder Test-modus) aus, in dem die Tofino SA nach dem Laden der Konfiguration ausgeführt werden soll.



Auf der zweiten Seite des Assistenten können Sie die Schnittstellen der jeweiligenTofino SA benennen und die zugehörige Konfiguration festlegen.



Auf der zweiten Seite des Assistenten können Sie schließlich die LSMs auswählen, die auf der betreffenden Tofino SA aktiviert werden sollen.



Weitere Informationen zu diesen Feldern finden Sie unter „Allgemeine Einstellungen einer Tofino SA“.

5.2 Eine Tofino SA aufrufen und editieren.

Wenn Sie in der Projekt-Explorer-Ansicht auf den Namen der Tofino SA klicken, öffnet sich das Menüfenster mit denTofino SA-Details. Hier können Sie durch die Konfigurationsseiten navigierenTofino SA und Assistenten für unterschiedliche Aktionen aufrufen (z. B. um eine Konfiguration auf einem USB-Speichermedium zu speichern).

Die für eine Tofino SA verfügbaren Optionen für Konfiguration und Einstellungen hängen von den zuvor gewählten LSMs ab. In der Regel können Sie folgende Einstellungen vornehmen:

- Allgemeine Einstellungen (General Settings) - zum Konfigurieren der allgemeinen Einstellungen der ausgewählten Tofino SA. Hierzu gehören allgemeine Informationen, Kommunikationsparameter und die Auswahl der LSMs.
- Einstellungen für LSM „Event Logger“ - zum Konfigurieren der Warnmeldungen und Ereignisprotokolle der ausgewählten Tofino SA.
- Einstellungen für LSM „Firewall“ - zum Konfigurieren der Firewall-Regeln der ausgewählten Tofino SA.

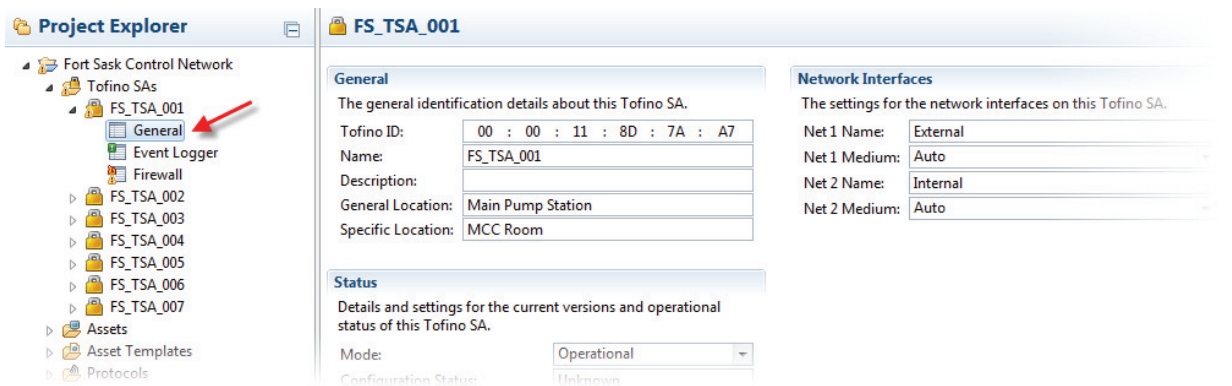
Für die ausgewählte Tofino SA können Sie unter anderem folgende Aktionen durchführen:

- Portable USB-Konfiguration erzeugen (Create Loadable USB Drive) - Mit diesem Befehl erzeugen Sie eine portable Konfiguration, die Sie auf einem ausgewählten USB-Speichermedium speichern können. Sie können dieses Speichermedium dann in einen USB-Port der ausgewählten Tofino SA stecken und die Konfiguration dort einladen.

- USB-Laufwerk prüfen (Verify Loaded USB Drive) - Dieser Befehl ruft den Konfigurationsbericht von dem USB-Laufwerk ab, von dem Sie eine Konfiguration in die ausgewählte Tofino SA geladen haben. Auf diese Weise können Sie erfolgreiche USB-Ladevorgänge aufzeichnen und bei Bedarf überprüfen.

5.3 Allgemeine Einstellungen einer Tofino SA

Im Menüfenster „Allgemeine Einstellungen“ (General Settings) der Tofino SA können Sie die generellen Einstellungen der ausgewählten Tofino SA anzeigen und konfigurieren. Hierzu gehören allgemeine Informationen, Kommunikationsparameter, der Status und die Auswahl der LSMs.



Allgemein.

- Tofino-ID:
  Die Kennung, die rechts auf der Vorderseite der Tofino SA angebracht ist. Anhand dieser Nummer bestätigen Sie, dass Sie eine Konfiguration in die richtige Tofino SA laden.
- Name:
  Geben Sie hier eine eindeutige Bezeichnung bzw. Kennung für die Tofino SA ein (z. B. Pumpwerk Neustadt oder JP-TFN-001). Aus Gründen der Übersichtlichkeit und für eine unkomplizierte Verwendung benötigt jede Tofino SA eine eindeutige Bezeichnung.
- Beschreibung (Description):
  Ein Textfeld, in dem Sie z. B. die Funktion dieser Tofino SA beschreiben können.

- Allgemeiner Standort (General Location):
  Dieses Textfeld dient als Referenz.
- Genauer Standort (Specific Location):
  Dieses Textfeld dient als Referenz.

Netzschnittstellen

- Name Netz 1 (Net 1 Name):
  Ein Name bzw. ein Bezeichner, mit dem der obere Ethernet-Port in der Tofino SA beschrieben wird. Sie können diesen z. B. anhand des angeschlossenen Netzes (wie etwa „Unternehmensnetz“) oder anhand der funktionalen Eigenheiten auswählen (wie etwa „Nicht vertrauenswürdig“).
- Medium Netz 1 (Net 1-Medium):
  Hiermit konfigurieren Sie die Einstellungen für die Schnittstelle am oberen Ethernet-Port. Die Tofino SA unterstützt die automatische Verhandlung bei beiden Ethernet-Ports. Automatische Verhandlung (auto-negotiation) bedeutet konkret, dass die Tofino SA die Verbindungs- und Übertragungsparameter automatisch mit dem angeschlossenen Switch oder Gerät aushandelt. Abhängig vom Kabelmedium in der Tofino SA können Sie die Ethernet-Ports manuell auf folgende Werte setzen:
  – Auto (Auto-Verhandlung)
  – 10baseT-HD (Twisted-Pair, 10 Mb/s, Halbduplex)
  – 10baseT-FD (Twisted-Pair, 10 Mb/s, Vollduplex)
  – 100baseTX-HD (Twisted-Pair, 100 Mb/s, Halbduplex)
  – 100baseTX-FD (Twisted-Pair, 100 Mb/s, Vollduplex)

  Der voreingestellte Wert ist „Auto“.

- Name Netz 2 (Net 2 Name):
  Ein Name bzw. ein Bezeichner, mit dem der untere Ethernet-Port in der Tofino SA beschrieben wird. Sie können diesen z. B. anhand des angeschlossenen Netzes (wie etwa „Steuerungsnetz“) oder anhand der funktionalen Eigenheiten auswählen (wie etwa „vertrauenswürdig“).
- Medium Netz 2 (Net 1-Medium):
  Hiermit konfigurieren Sie die Einstellungen für die Schnittstelle am unteren Ethernet-Port. Die Tofino SA unterstützt automatische Verhandlungen bei beiden Ethernet-Ports. Automatische Verhandlung (auto-negotiation) bedeutet konkret, dass die Tofino SA die Verbindungs- und Übertragungsparameter automatisch mit dem angeschlossenen Switch oder Gerät aushandelt. Abhängig vom Kabelmedium können Sie die Ethernet-Ports auch manuell auf folgende Werte setzen:
  – Auto (Auto-Verhandlung)
  – 10baseT-HD (Twisted-Pair, 10 Mb/s, Halbduplex)
  – 10baseT-FD (Twisted-Pair, 10 Mb/s, Vollduplex)
  – 100baseTX-HD (Twisted-Pair, 100 Mb/s, Halbduplex)
  – 100baseTX-FD (Twisted-Pair, 100 Mb/s, Vollduplex)

  Der voreingestellte Wert ist „Auto“.

Status

- Modus (Mode):
  Sie können die Tofino SA auf einen der beiden folgenden Modi einstellen:
  – Test:
    Die Tofino SA ist vollständig betriebsbereit und verarbeitet Datenverkehr, verwirft jedoch keinen Netzverkehr. Mit diesem Modus können Sie die ordnungsgemäße Konfiguration der Tofino SA testen, bevor Sie sie für die Filterung des Verkehrs im Leitsystem einsetzen.
  – Betriebsbereit (Operational):
    Die Tofino SA stellt eine vollständige Verarbeitung der Datenpakete und sämtliche Schutzfunktionen bereit.

- Konfigurationsstand (Configuration Status):
  Zeigt den aktuellen Status der tatsächlichen Tofino SA im Feldbereich an. Dieser wird anhand der letzten USB-Prüfung bestimmt:
  - Unbekannt (Unknown):
    Die Konfiguration ist entweder nicht in die Tofino SA geladen oder nicht überprüft worden.
  - Geprüft (Verified):
    Eine USB-Konfiguration wurde erfolgreich in die Tofino SA geladen; der Befehl „USB-Konfiguration prüfen“ (Verify Loaded USB) wurde ausgeführt, um das betreffende Ergebnis an den ConneXium Tofino Configurator zu übermitteln.
  - Fehler (Failed):
    Wie das Resultat des Befehls „USB-Konfiguration prüfen“ zeigt, ist der Ladevorgang an dieser Tofino SA bei der letzten Ausführung des Befehls „USB laden“ gescheitert.
- Letzte Konfigurationsrevision (Latest Configuration Revision):
  Zeigt die die aktuelle Versionsnummer der Tofino SA-Konfiguration in der betreffenden Projektdatei an und darüber hinaus eine spezielle Prüfsumme (Hash-Code), welche die Wahrscheinlichkeit verringert, dass Revisionsnummern versehentlich doppelt vergeben werden. Die Revisionsnummer wird jedes Mal hochgezählt, wenn Sie die Einstellungen derTofino SA verändern und das Projekt speichern. Der ConneXium Tofino Configurator berechnet diese Revisionsnummer getrennt von der Revisionsnummer des Projektes.
- Überprüfte Konfigurationsrevision (Verified Configuration Revision):
  Die letzte Versionsnummer dieserTofino SA-Konfiguration; wie die Überprüfung durch den Befehl „USB-Konfiguration prüfen“ ergeben hat, wurde die Konfiguration in der Tofino SA installiert. Ebenfalls angezeigt wird eine spezielle Prüfsumme (Hash-Code), welche die Wahrscheinlichkeit verringert, dass Revisionsnummern versehentlich doppelt vergeben werden. Wenn sich der Wert im Feld „Überprüfte Konfigurationsrevision“ von dem im Feld „Letzte Konfigurationsrevision“ unterscheidet, besteht die Möglichkeit, dass die Tofino SA eine veraltete Konfiguration enthält.
- Gerätetyp (Hardware Type):
  Dieses Feld wird durch den Befehl „USB-Konfiguration prüfen“ aktualisiert, und zwar anhand des von der Tofino SA gemeldeten Tofino-Typs.
- Modell (Model):
  Dieses Feld wird durch den Befehl „USB-Konfiguration prüfen“ aktualisiert, und zwar anhand des von der Tofino SA gemeldeten Modelltyps.

- Firmware-Code:
  Dieses Feld zeigt die verfügbaren und in diesem Produkt vorinstallierten LSMs an.
- Firmware-Version:
  Dieses Feld wird durch den Befehl „USB-Konfiguration prüfen“ aktualisiert, und zwar anhand der von der Tofino SA gemeldeten Firmware-Version.

Ladbare Sicherheitsmodule (Loadable Security Modules) (LSMs):

Hier können Sie die LSMs auswählen, die während des USB-Ladevorgangs auf der Tofino SA aktiviert werden sollen. Dies sind beispielsweise:

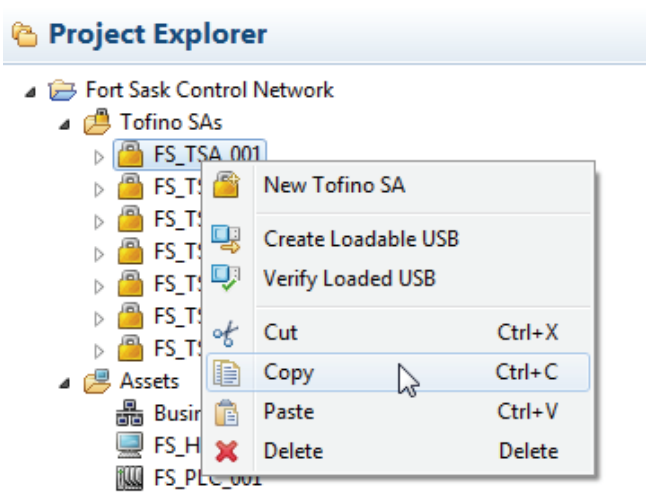
- LSM „Firewall“
- LSM „Event Logger“
- LSM „Modbus TCP Enforcer“

Wenn Sie ein LSM ausgewählt haben, können unterhalb des Tofino SA-Ordners zusätzliche Unterordner erscheinen. Mit diesen können Sie die jeweilige LSM konfigurieren. Beachten Sie, dass sich die Einstellungen für die „Enforcer“-LSMs im Unterordner „Firewall“ befinden.

5.4 Verwalten von Tofino SAs

Sie können eine Tofino SA wie ein normales Windows-Objekt verwalten. Wenn Sie eine Tofino SA mit der rechten Maustaste anklicken oder alternativ die Werkzeugleiste verwenden, haben Sie folgende Möglichkeiten:

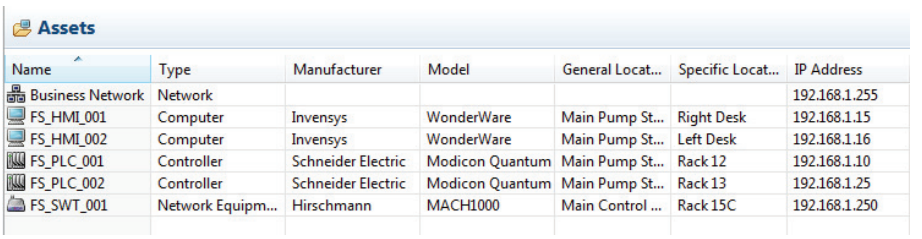
- Neue Tofino SA - der Assistent „Neue Tofino SA“ wird gestartet.
- Portable USB-Konfiguration erzeugen (Create Loadable USB) - Erzeugt eine portable Konfigurationsdatei, die Sie auf ein USB-Speichermedium speichern können. Sie können das Speichermedium der dann in einen USB-Port der Tofino SA stecken und die Konfiguration dort einladen.
- USB-Konfiguration prüfen (Verify Loaded USB) - Prüft das Ladeprotokoll des USB-Speichermediums, das Sie zum Laden der Konfiguration verwendet haben. Auf diese Weise können Sie erfolgreiche USB-Ladevorgänge aufzeichnen und bei Bedarf überprüfen.
- Ausschneiden (Cut) - Entfernt die markierte Tofino SA aus dem Projekt und speichert sie in die Zwischenablage. Sie können sie dann an einem anderen Speicherort wieder einfügen.
- Kopieren (Copy) - Erzeugt eine Kopie der markierten Tofino SA des Projektes und speichert sie in die Zwischenablage. Sie können sie dann an einem anderen Speicherort wieder einfügen.
- Einfügen (Paste) - Fügt den Inhalt der Zwischenablage in das Projekt ein.
- Löschen (Delete) - Entfernt die markierte Tofino SA aus dem Projekt.



6 Definieren von Ressourcen

Der ConneXium Tofino Configurator verwaltet sog. Ressourcen (Assets). Zu diesen zählen zum einen physische Geräte wie SPS-Einheiten, Rechner und Netzgeräte; zum anderen auch „virtuelle Ressourcen“ wie ein Broadcast-Adressbereich, ein Netz oder eine Multicast-Adresse. Dies ermöglicht Ihnen eine flexible Gestaltung der Firewall-Regeln.

Die Ressourcenverwaltung ermöglicht Ihnen das Erstellen, Editieren und Löschen von Ressourcen, die tatsächliche Geräte und Systeme im Steuerungsnetz repräsentieren. Mit Hilfe von Ressourcenvorlagen können Sie zudem Standardvorlagen für häufig verwendete Ressourcen erstellen.


Assets

Name	Type	Manufacturer	Model	General Locat...	Specific Locat...	IP Address
Business Network	Network					192.168.1.255
FS_HMI_001	Computer	Invensys	WonderWare	Main Pump St...	Right Desk	192.168.1.15
FS_HMI_002	Computer	Invensys	WonderWare	Main Pump St...	Left Desk	192.168.1.16
FS_PLC_001	Controller	Schneider Electric	Modicon Quantum	Main Pump St...	Rack 12	192.168.1.10
FS_PLC_002	Controller	Schneider Electric	Modicon Quantum	Main Pump St...	Rack 13	192.168.1.25
FS_SWT_001	Network Equipm...	Hirschmann	MACH1000	Main Control ...	Rack 15C	192.168.1.250

Wenn Sie in der Projekt-Explorer-Ansicht eine bestimmte Ressource auswählen, haben Sie folgende Möglichkeiten:

- Eine neue Ressource oder einen neuen Ordner erzeugen.
- Die Details der Ressource aufrufen und editieren.
- Eine Ressource löschen.
- Ressourcen ausschneiden, kopieren und einfügen.

Rechner, Controller, Geräte und Netzvorrichtungen als Ressourcen

Bei den meisten im ConneXium Tofino Configurator verwendeten Ressourcen handelt es sich um physische Geräte. Diese verwenden üblicherweise sog. Unicast-Nachrichten. Bei Unicast-Nachrichten handelt es sich um Netzverkehr, der von einem bestimmten Gerät zu einem anderen bestimmten Gerät übermittelt wird. Wenn Sie einen Rechner, einen Controller, ein Gerät oder eine sonstige Netzvorrichtung als Ressource definieren, geht der ConneXium Tofino Configurator davon aus, dass es sich um ein physisches Gerät im Netz handelt und unterstützt Sie bei der Erstellung geeigneter Regeln für den jeweiligen Gerätetyp.

Netzressourcen

Bei Netzressourcen handelt es sich um virtuelle Nachbildungen der in einem bestimmten Netz bzw. Subnetz enthaltenen Geräte. Wenn Sie ein Netz als Ressource definieren, geht der ConneXium Tofino Configurator davon aus, dass es sich um eine Anzahl von Geräten im Netz handelt, die zu einer Gruppe von IP-Adressen gehören, welche einem Subnetz zugeordnet sind. Wenn Sie demgemäß eine Netzressource in einer Regel verwenden, unterstützt Sie der ConneXium Tofino Configurator bei der Erstellung von Regeln, mit denen Verkehr von dem entsprechenden Adressbereich zugelassen oder blockiert wird.

Broadcast- und Multicast-Ressourcen

In den meisten Netzen kommen Nachrichten vor, die an eine allgemeine Adresse gesendet werden und von allen Teilnehmern des Netzes empfangen werden sollen. Diese werden als Broadcast- bzw. Multicast-Nachrichten bezeichnet. Für den Umgang mit solchen Nachrichten verfügt der ConneXium Tofino Configurator über spezielle Ressourcen.

- Broadcast:
  Diese Ressource stellt eine Adresse dar, die für IP-Broadcast-Nachrichten verwendet wird. Broadcast-Pakete sind ein normaler Bestandteil des Netzverkehrs. Ein Gerät überträgt sie an eine Broadcast-Adresse, nach der viele Geräte „lauschen“. So nutzen IP-Netze Broadcast-Pakete, um Netzadressen unter Verwendung des Protokolls ARP (Address Resolution Protocol) aufzulösen. Die genaue Broadcast-Adresse hängt von der Subnetzmaske ab, die für das jeweilige Netz

festgelegt wurde. Wenn eine Knoten die Adresse 192.168.1.1 hat, könnte die Broadcast-Adresse 192.168.1.255 lauten (je nach Subnetzmaske des Knotens). Sie benötigen eine solche Ressource, wenn Sie Broadcast-Filterregeln im LSM „Firewall“ bereitstellen möchten.

- Multicast:
  Diese Ressource stellt eine Adresse dar, die für IP-Multicast-Nachrichten verwendet wird. Multicast-Paket werden an eine Multicast-Adresse gesendet, nach der eine Anzahl von Geräten „lauscht“. Üblicherweise sind dies IP-Adressen im Bereich von 224.0.0.0 bis 239.255.255.255, die vom Hersteller der Controller-Hardware, den verwendeten Protokollen und der Netz-Konfiguration abhängen. So wird die Adresse 239.192.22.121 oft in EtherNet/IP-Netzen verwendet, die Adresse 234.5.6.7 oft in fehlertoleranten Ethernet-Systemen. Dies ist erforderlich, wenn Sie Multicast-Filterregeln im LSM „Firewall“ bereitstellen möchten.

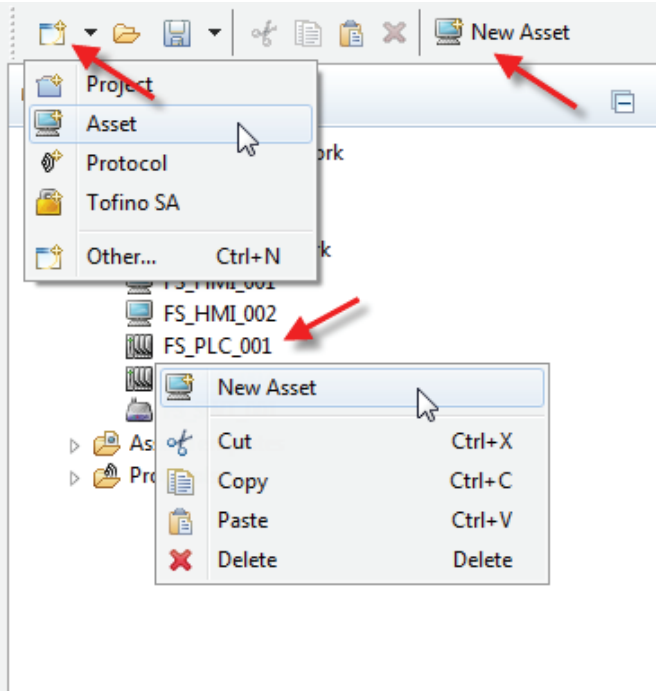
6.1 Eine Ressource erzeugen

Sie erzeugen neue Protokolle mit Hilfe des Assistenten „Neue Ressource (New Asset)“. Dabei stehen Ihnen vier Möglichkeiten zur Verfügung, um den Assistenten „Neue Ressource“ aufzurufen:

- Klicken Sie auf die Schaltfläche `Neu (New)` und wählen Sie `Ressource (Asset)` aus.
- Klicken Sie im mittleren Bereich der Werkzeugleiste auf die Schaltfläche `Neue Ressource (New Asset).`
- Führen Sie einen Rechtsklick auf eine bestehende Ressource aus und wählen Sie `Neue Ressource (New Asset).`
- Erzeugen einer Ressource aus einer Ressourcenvorlage.

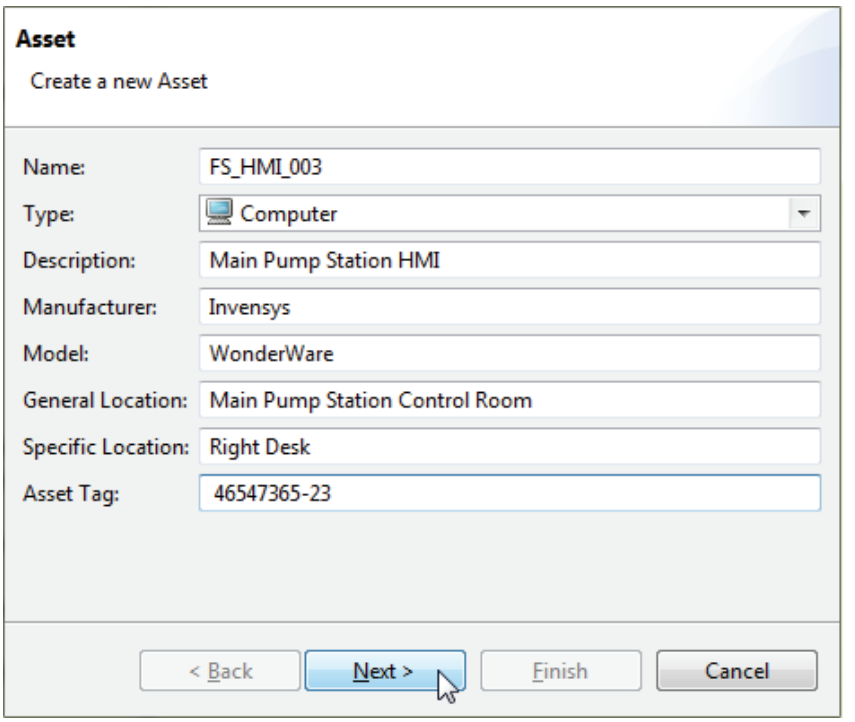
Die vierte Methode steht Ihnen zur Verfügung, wenn Sie den Ordner „Ressourcenvorlagen“ (Asset Template) ausgewählt haben.

Sie haben auch die Möglichkeit, bestehende Ressourcen oder Ressourcenvorlagen in den Ressourcenordner zu kopieren. Hierdurch rufen Sie jedoch nicht den Assistenten auf. Es ist daher erforderlich, dass Sie die entsprechenden Felder wie „Name“ oder „IP-Adresse“ manuell editieren.

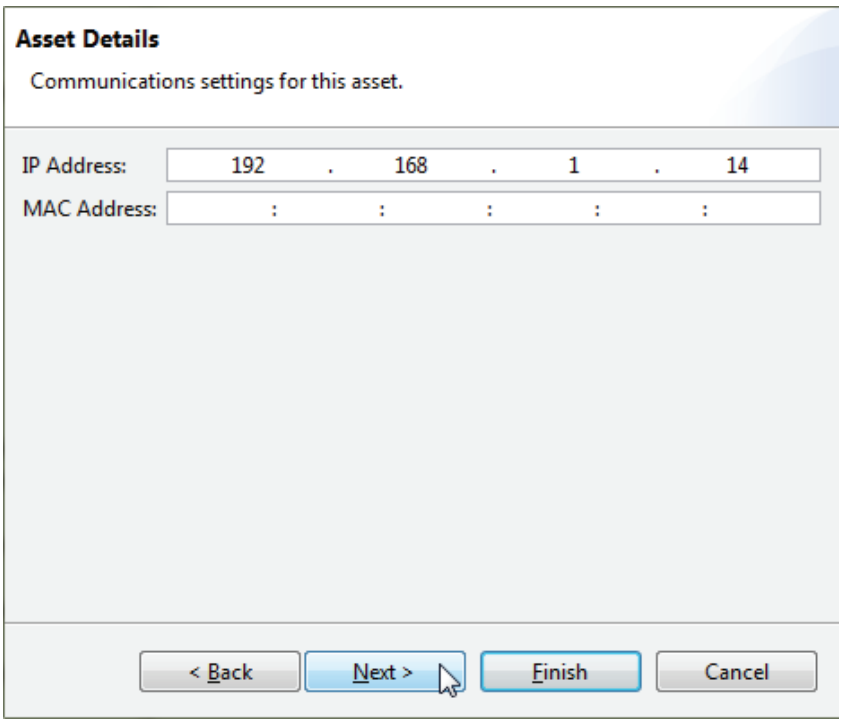


Assistent „Neue Ressource“

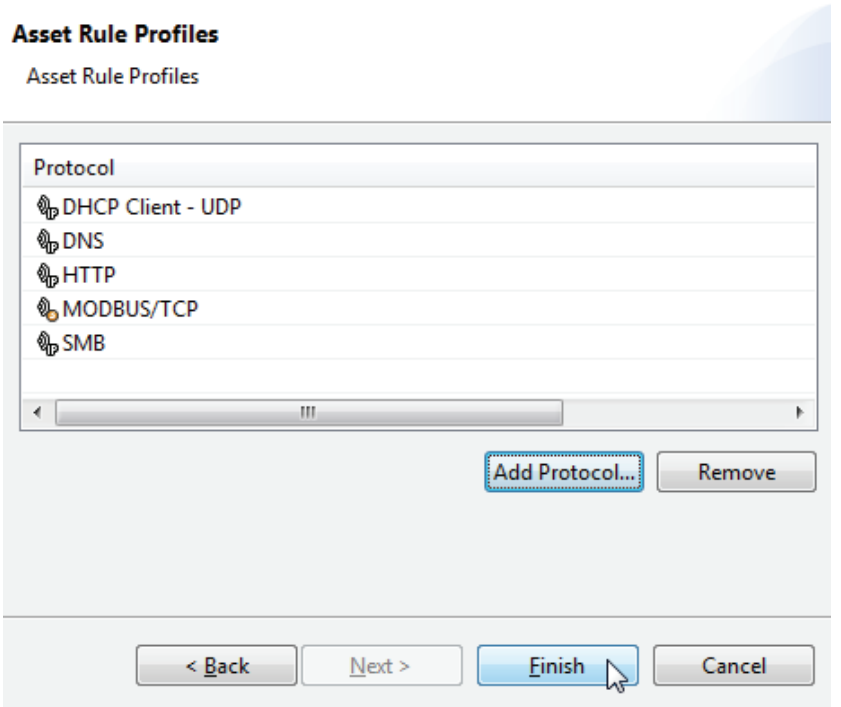
Wenn Sie den Assistenten aufrufen, werden Sie aufgefordert, den Namen, den Ressourcentyp und einige optionale Felder einzugeben. Weitere Informationen zu diesen Feldern finden Sie unter „Ressourcen aufrufen und editieren“



Auf der zweiten Seite des Assistenten haben Sie die Möglichkeit, die Adressdaten für die Ressource einzugeben. Der ConneXium Tofino Configurator verwendet diese Informationen beim Erstellen von Firewall-Regeln für diese Ressource.



Auf der dritten Seite des Assistenten können Sie Regelprofile definieren, indem Sie Protokolle auswählen, welche die Ressource üblicherweise für die Kommunikation verwendet. Beim Erzeugen von Firewall-Regeln verwendet das Gerät diese Regelprofile, um mögliche Regeln vorzuschlagen.



6.2 Ressourcenvorlagen

Mit Hilfe der Ressourcenvorlagen können Sie zügig mehrere Ressourcen erzeugen. Sie enthalten vordefinierte Felder, mit deren Hilfe Sie zügig ähnliche Ressourcen erzeugen können. Wenn in Ihrem Werk beispielsweise 10 SPS ähnlicher Bauart installiert sind, können Sie zur Abbildung dieses SPS-Typs eine Ressourcenvorlage erzeugen oder eine bestehende Ressourcenvorlage verwenden. Daraus können Sie auf die Schnelle Ressourcen erzeugen, welche die 10 SPS abbilden. Bei jeder Verwendung des Tools `Neue Ressource aus Vorlage (New Asset From Template)` wird dann eine neue Ressource erzeugt, bei der die Eingabefelder (mit Ausnahme von Name, Standort und Adresse) bereits ausgefüllt sind.

Der ConneXium Tofino Configurator wird mit einer Anzahl von Vorlagen ausgeliefert, die für Schneider Automation Produkte vorinstalliert sind. Sie können neue Vorlagen auch über den Befehl „Import“ importieren oder eigene Vorlagen erzeugen.

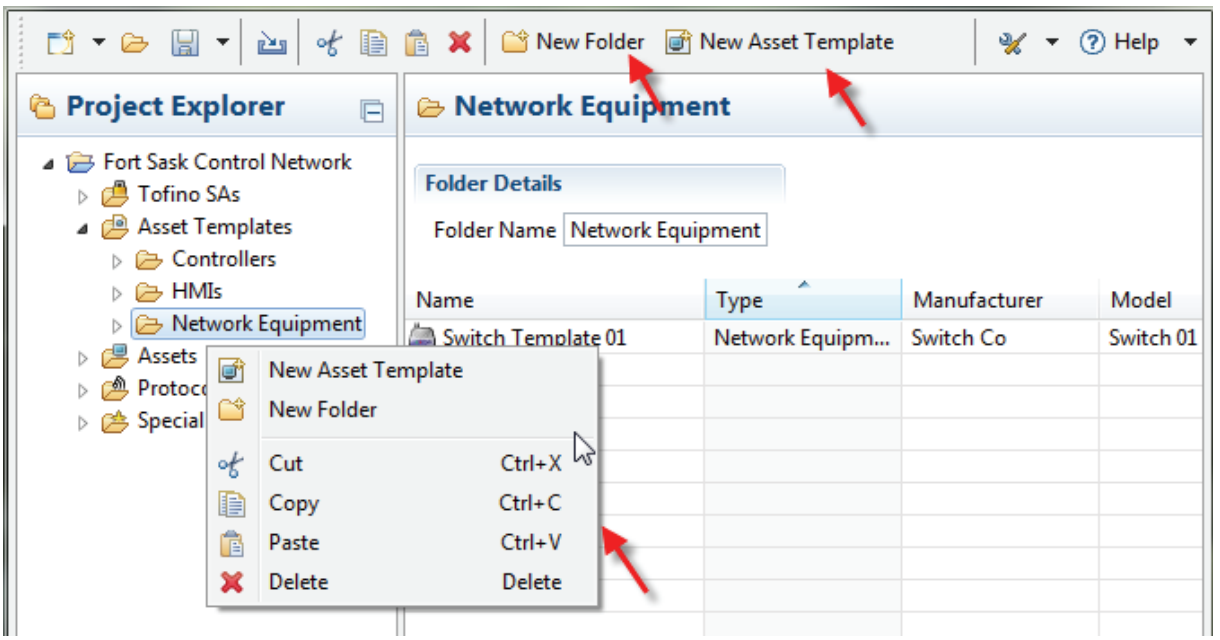
Zudem können Sie Ressourcenvorlagen auch dadurch erzeugen, dass Sie eine bestehende Ressource in den Ordner „Ressourcenvorlagen“ (Asset Template) kopieren.

Wenn Sie in der Projekt-Explorer-Ansicht eine bestimmte Ressourcenvorlage auswählen, haben Sie folgende Möglichkeiten:

- Eine neue Ressourcenvorlage oder einen neuen Ressourcenordner erzeugen.
- Eine neue Ressource auf Basis der ausgewählten Vorlage erzeugen;
- Die Details der Ressourcenvorlage aufrufen und editieren.
- Eine Ressource löschen.
- Ressourcenvorlagen ausschneiden, kopieren und einfügen.

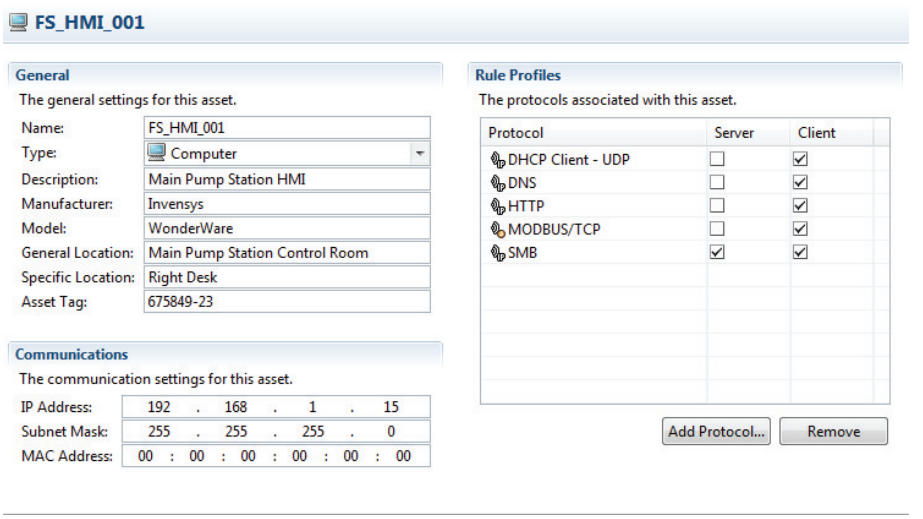
Einige Vorlagen sind werkseitig voreingestellt. Sie haben keine Möglichkeit, diese auszuschneiden oder zu löschen.

Um eine Ressourcenvorlage als Grundlage für eine Ressource zu verwenden, wählen Sie die gewünschte Vorlage aus und betätigen die Schaltfläche `Neue Ressource aus Vorlage (New Asset From Template)`. Dies ruft den Assistenten „Neue Ressource“ auf, wobei die meisten Felder dann bereits ausgefüllt sind.


New Folder
New Asset Template
Help
Project Explorer
Network Equipment
Fort Sask Control Network
Tofino SAs
Asset Templates
Controllers
HMIs
Network Equipment
Assets
Folder Details
Folder Name
Network Equipment
Name
Type
Manufacturer
Model
Switch Template 01
Network Equipm...
Switch Co
Switch 01
New Asset Template
New Folder
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Delete Delete

6.3 Ressourcen aufrufen und editieren

Wenn Sie in der Projekt-Explorer-Ansicht auf den Namen einer Ressource klicken, öffnet sich das Menüfenster mit den Details zur Ressource (Asset Details). In diesem Menüfenster können Sie die Einstellungen für die ausgewählte Ressource ansehen und konfigurieren. Hierzu gehören allgemeine Informationen und Kommunikationsparameter.



Allgemeines

- Name:
  Geben Sie hier eine eindeutige Bezeichnung bzw. Kennung für die Ressource ein (z. B. SPS Pumpwerk Neustadt oder JP-SPS-001). Um etwaige Verwechslungen möglichst auszuschließen, benötigt jede Ressource eine eindeutige Bezeichnung.
- Typ (Type):
  Wählen Sie einen Ressourcentyp. Die zur Verfügung stehenden Eingabefelder werden von der ausgewählten Ressource bestimmt. Ressourcen können einem der folgenden Typen zugeordnet werden:
  - Rechner
  - Controller
  - Gerät
  - Netz
  - Netzvorrichtung
  - Broadcast
  - Multicast
- Beschreibung (Description):
  Ein Textfeld, in dem Sie die Funktion dieser Ressource beschreiben können.
- Hersteller (Manufacturer):
  Das herstellende Unternehmen oder das Fabrikat einer Ressource (z. B. Schneider Electric)
- Modell (Model):
  Das Modell der betreffenden Ressource (z. B. Quantum)
- Allgemeiner Standort (General Location):
  Dieses Textfeld dient als Referenz.
- Genauer Standort (Specific Location):
  Dieses Textfeld dient als Referenz.
- Ressourcen-Kennzeichnung (Asset Tag):
  Ein benutzerdefiniertes Feld für Kennzeichnungen von Firmen-Ressourcen.

Kommunikation

- IP-Adresse:
  Bezeichnet die IP-Adresse der Ressource. Achten Sie darauf, eine korrekte Adresse einzugeben, damit die Firewall-Regeln ordnungsgemäß funktionieren.
- Subnetz-Maske:
  Die Tofino SA verwendet die Subnetzmaske in Verbindung mit der IP-Adresse, um Rechner oder Geräte zu identifizieren, die Teil eines lokalen Netzes oder eines Subnetzes sind. Bei einer Subnetzmaske handelt es sich um eine 32-Bit-Zahl, deren Schreibweise durch vier mittels Punkten getrennte Zahlen zwischen 0 und 255 gekennzeichnet ist. In Subnetzmasken wird üblicherweise eine der Zahlen 255 oder 0 verwendet (wie z. B. 255.255.255.0). In besonderen Fällen können jedoch auch andere Zahlen eingesetzt werden.
- MAC-Adresse (MAC Address):
  Bezeichnet die Ethernet-MAC-Adresse oder die physische Adresse der Ressource. Bei den meisten Ressourcen ist das ein optionales Feld, das Sie leer lassen sollten. Wenn Sie jedoch Regeln für nicht IP-basierte Protokolle wie GOOSE erstellen, geben Sie hier eine MAC-Adresse ein.

Regelprofile

Beim Erzeugen einer Ressource können Sie auch die Protokolle festlegen, welche die Ressource üblicherweise verwendet. Zudem können Sie bestimmen, ob die Ressource diese Protokolle als Client verwendet (d. h. die Kommunikation initiiert) oder als Server (d. h. auf Anfragen von Clients reagiert). Der Assistent „Neue Firewall-Regel“ kann diese Informationen verwenden, um automatisch Regeln für die Ressource zu erzeugen.

- Protokoll (Protocol):
  Eine Liste mit Protokollen, welche diese Ressource für die Netzkommunikation verwenden kann.

  Hinweis: Wenn Sie ein Protokoll für die Anwendungsschicht (wie Modbus oder HTTP) auswählen, besteht keine Notwendigkeit, die Protokolle für die unteren Schichten (wie Ethernet, TCP und IP) auszuwählen.

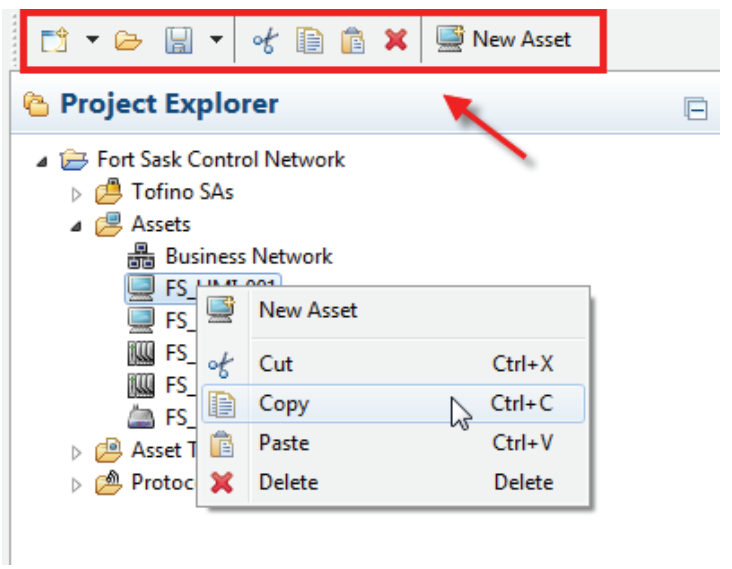
- Server:
  Wenn Sie dieses Kästchen anklicken, fungiert die Ressource als Server und antwortet auf Anfragen von Clients. Anwendungsbeispiel: Sie definieren einen Web-Server oder ein Modbus-Slave-Gerät (z. B. eine SPS) als Server.
- Client:
  Wenn Sie dieses Kästchen anklicken, fungiert die Ressource als Client und initiiert Anfragen an Server. Anwendungsbeispiel: Sie definieren einen Web-Browser oder ein Modbus-Client-Gerät (z. B. eine HMI) als Client.

Bei Bedarf können Sie die zu einer Ressource gehörenden Protokolle sowohl Clients wie auch Servern zuordnen. So kann z. B. ein Rechner sowohl Web-Server-Software wie auch Web-Browser-Software enthalten und somit zugleich als HTTP-Client wie auch als HTTP-Server bestimmt werden.

6.4 Ressourcen verwalten

Sie können eine Ressource wie ein normales Windows-Objekt verwalten. Wenn Sie eine Ressource mit der rechten Maustaste anklicken oder alternativ die Werkzeugleiste verwenden, haben Sie folgende Möglichkeiten:

- Neue Ressource (New Asset) - ruft den Assistenten „Neue Ressource“ auf.
- Neuer Ordner (New Folder) - erzeugt einen neuen Ordner für die Organisation Ihrer Ressourcen.
- Ausschneiden (Cut) - Entfernt die markierte Ressource aus dem Projekt und speichert sie in die Zwischenablage. Sie können sie dann an einem anderen Speicherort wieder einfügen.
- Kopieren (Copy) - Erzeugt eine Kopie der markierten Ressource des Projektes und speichert sie in die Zwischenablage. Sie können sie dann an einem anderen Speicherort wieder einfügen.
- Einfügen (Paste) - Fügt den Inhalt der Zwischenablage in das Projekt ein.
- Löschen (Delete) - Entfernt die markierte Ressource aus dem Projekt.



7 Definieren von Firewall-Regeln

Was ist eine Firewall?

Eine Firewall ist ein Mechanismus, mit dem Sie den Verkehr zwischen zwei Netzen (bzw. zwei Bereichen desselben Netzes) regeln und überwachen können, um so die einzelnen Komponenten des Netzes mit einem Schutz zu versehen. Der Mechanismus vergleicht den durch die Firewall geleiteten Verkehr mit einer Reihe von vordefinierten Regeln und verwirft den Verkehr, der den Regelkriterien nicht entspricht. Der aktivierte Mechanismus arbeitet als Filter: Er blockiert ungewollten Netzverkehr und begrenzt Art und Menge der Kommunikationsvorgänge, die zwischen schutzbedürftigen Geräten oder Netzen und anderen Systemen ablaufen - wie dem Unternehmensnetz oder anderen Bereichen des Steuerungsnetzes eines Standortes.

Bei der Tofino Firewall handelt es sich um eine LSM, die zwecks Verarbeitung des Datenverkehrs in der Tofino SA aktiviert wird. Diese Firewall arbeitet zustandsabhängig und stellt eine umfassende Paketüberprüfung bereit (stateful deep-packet inspection firewall).

Was ist ein Enforcer?

Eine Enforcer ist eine fortgeschrittene Firewall für spezifische SCADA- und ICS-Protokolle. Sie ermöglicht es Ihnen, Datenverkehr anhand von bestimmten Funktions-Codes und Nachrichteninhalten zu filtern. Enforcer sind als Add-Ons für die reguläre Tofino Firewall-LSM konzipiert. Zu den Enforcern gehören:

- Modbus TCP Enforcer:
  Dieses LSM bietet diverse Sicherheitsfunktionen zur Verwaltung des Modbus-TCP-Verkehrs:
  - Es prüft, ob die einzelnen Modbus-Pakete der Protokollspezifikation entsprechen. Je nach Resultat lässt es das Paket zu oder lehnt es ab.
  - Sie können Modbus-Funktionen festlegen, welche die Tofino SA zulassen oder ablehnen soll.
  - Es überwacht den Status der Modbus-TCP-Verbindungen und kann so eingehende Nachrichten feststellen und deren Reihenfolge untersuchen.

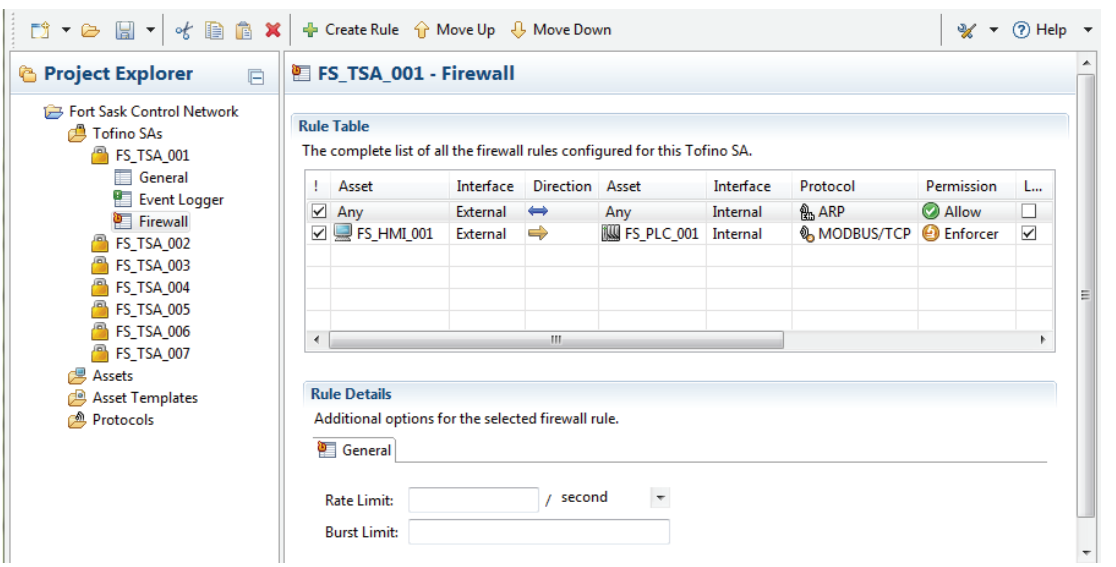
7.1 Firewall-Regeln verwalten

Das Menüfenster „Firewall“ enthält eine Liste der für die ausgewählte Tofino SA konfigurierten Firewall-Regeln. Sie können zudem:

- Eine neue Firewall-Regel erzeugen.
- Eie Regeln aufrufen und editieren.
- Regeln umordnen.
- Regeln ausschneiden, kopieren und einfügen.
- Regeln löschen.

Bei der Verwendung der Befehle „Ausschneiden“, „Kopieren“, „Einfügen“ und „Löschen“ können Sie mehrere Firewall-Regeln auswählen und Massenoperationen durchführen. So können Sie etwa einen Satz Regeln von einer Tofino SA kopieren und in eine andere einfügen.

Wenn Sie eine Regel auswählen, erscheint der Abschnitt „Regeldetails“ (Rule Details) mit weiteren Optionen für die jeweilige Regel bzw. das jeweilige Protokoll.

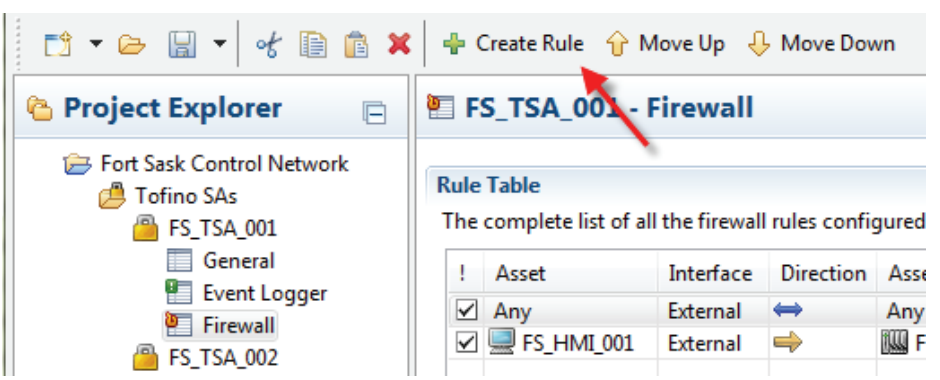


Firewall-Regeln erzeugen

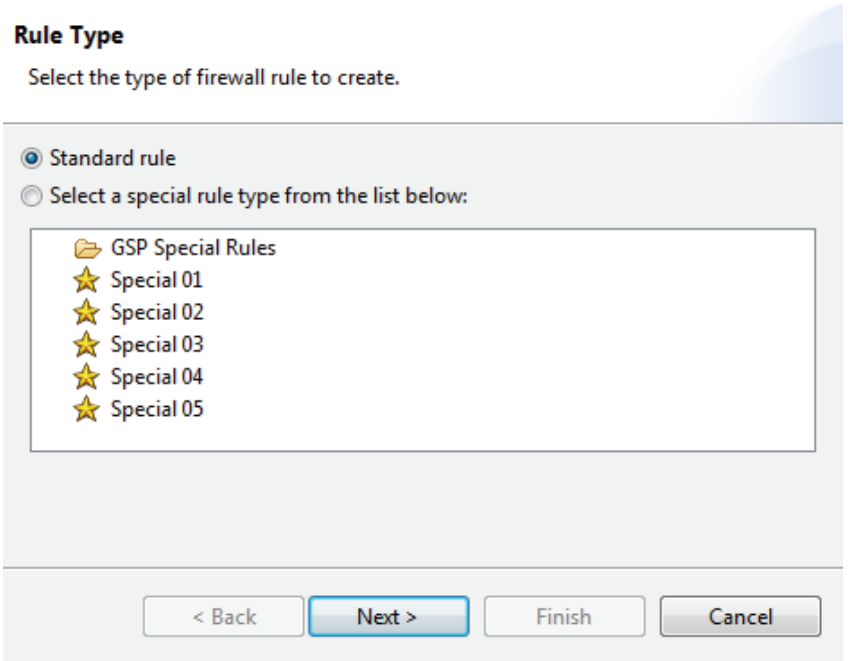
Die ConneXium Tofino Configurator bietet Ihnen die Möglichkeit, zwei Arten von Firewall-Regeln zu erstellen:

- Standardmäßige Firewall-Regeln sind so konzipiert, dass sie spezifische Protokolle, welche die Firewall passieren, entweder zulassen oder ablehnen. Mit ihrer Hilfe können Sie Quelle, Ziel, Richtung, Genehmigungsstatus und Ratenbegrenzung für den Datenverkehr eines bestimmten Protokolltyps festlegen. Wenn Sie beispielsweise den Modbus/TCP-Verkehr zwischen zwei Geräten zulassen wollen, können Sie eine Standardregel einsetzen. Verwenden Sie Standardregeln für den Großteil Ihrer Anwendungen.
- Bei Sonderregeln handelt es sich um höchst komplexe Regeln, die weit über ein einfaches Zulassen oder Ablehnen hinausgehen. Sie könnten eine Sonderregel z. B. verwenden, um eine Teilmenge eines bestimmten Verkehrstyps zu blockieren. Die verfügbaren Sonderregeln können Sie sich im gleichnamigen Ordner ansehen. Solche Regeln sollten Sie ausschließlich in Ausnahmefällen verwenden.

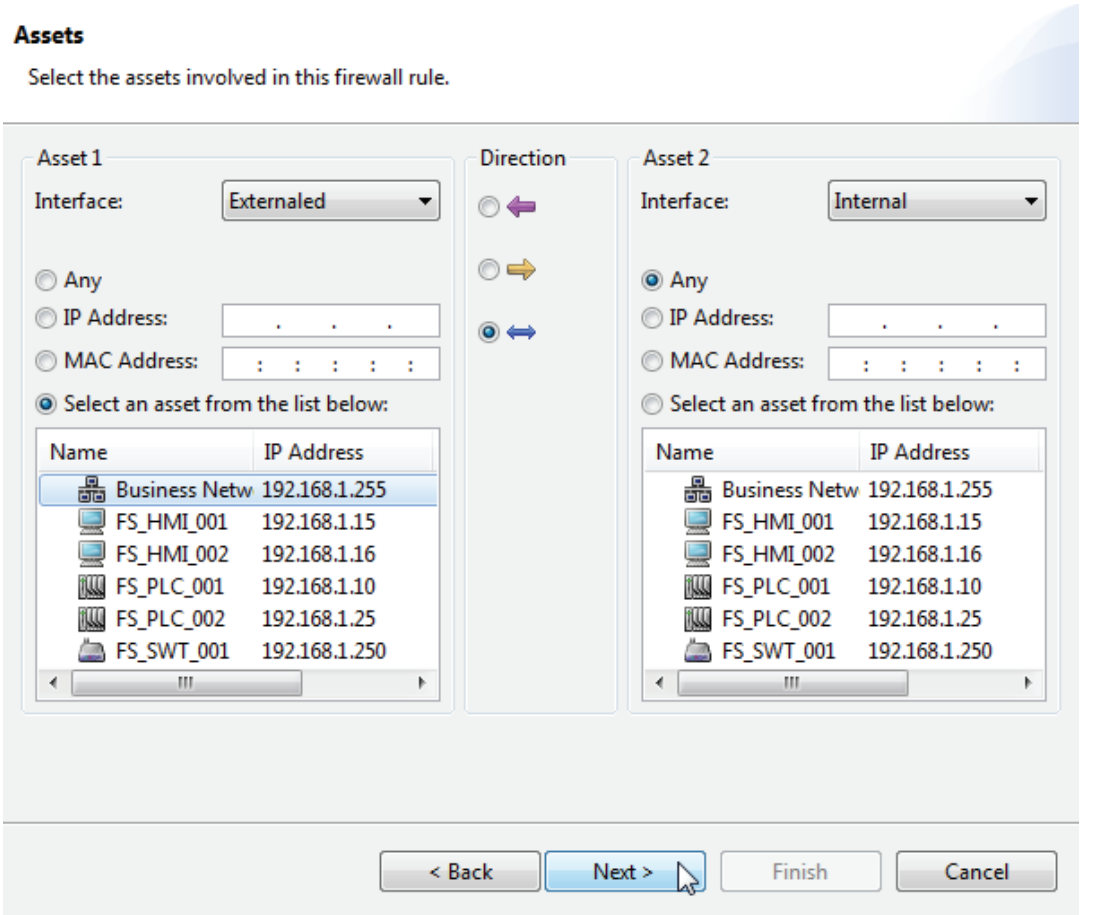
Sie erzeugen neue Regeln mit Hilfe des Assistenten „Neue Firewall-Regel (New Firewall Rule)“. Den Assistenten können Sie wie folgt aufrufen: Wählen Sie das Menüfenster „Firewall“ bei der Tofino SA aus, für die Sie eine Regel erzeugen wollen. Klicken Sie dann auf die Schaltfläche `Regel erzeugen (Create Rule)` im mittleren Bereich der Werkzeugleiste.



Wenn Sie den Assistenten aufrufen, werden Sie gefragt, ob Sie die neue Regel auf Basis einer Standard-Regel oder einer Sonderregel erzeugen möchten. Wenn Sie hier Sonderregel (Special Rule) auswählen, fordert Sie der Assistent auf, eine Regel aus einer Liste verfügbarer Sonderregel-Vorlagen auszuwählen.



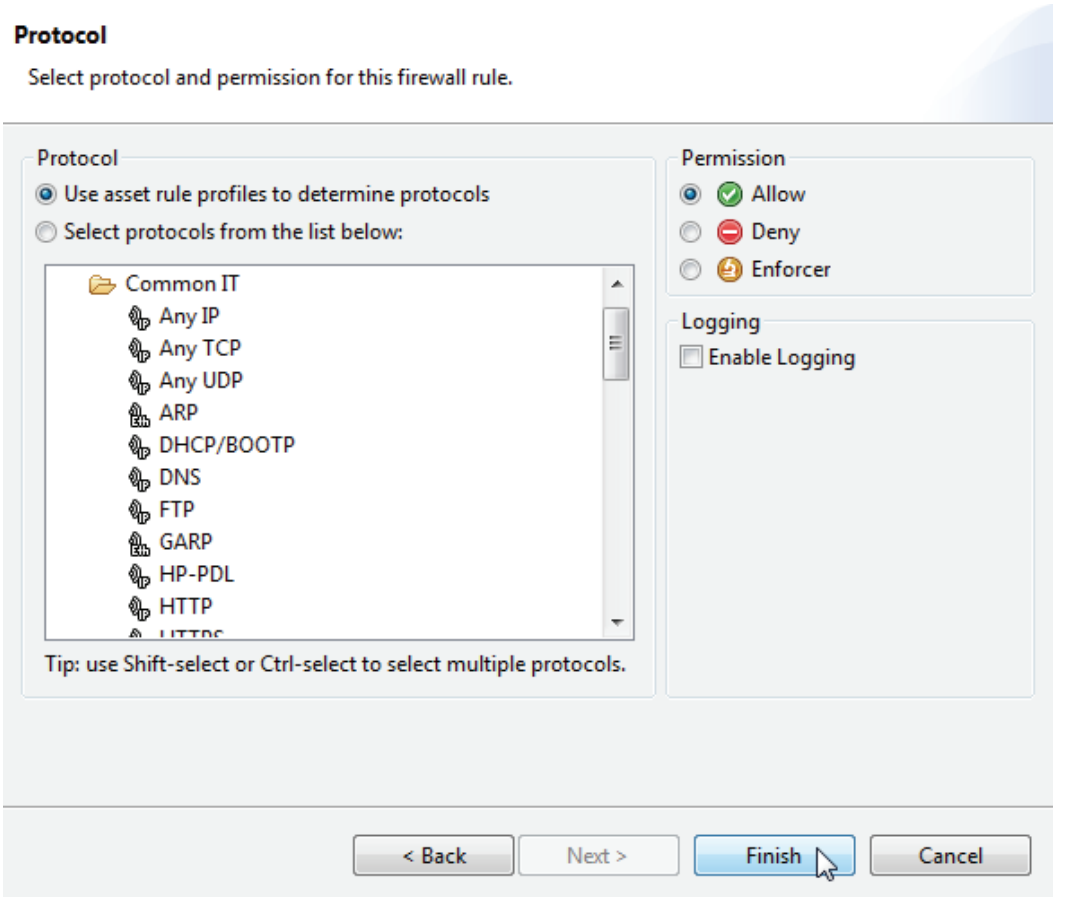
Im nächsten Schritt werden Sie aufgefordert, die Schnittstellen, die Richtung und entweder Ressourcen oder Adressen einzugeben. Weitere Informationen zu diesen Feldern finden Sie unter „Firewall-Regeln aufrufen und editieren“



Auf der zweiten Seite des Assistenten werden Sie aufgefordert, ein oder mehrere Protokolle für die Regeln auszuwählen. Mit Hilfe des Assistenten können Sie:

- Die Regelprofile verwenden, die zu den Ressourcen gehören, welche Sie zum automatischen Erzeugen der Regeln ausgewählt haben.
- Eine manuelle Auswahl der Protokolle treffen, für die Sie Regeln erstellt haben möchten. Wenn Sie mehr als ein Protokoll ausgewählt haben, wird eine Regel für jedes Protokoll erstellt.

Schlussendlich wählen Sie den Genehmigungsstatus aus (z. B. Zulassen, Ablehnen oder Enforcer) und legen fest, ob bei jedem Auslösen dieser Regel ein Protokoll erzeugt werden soll.

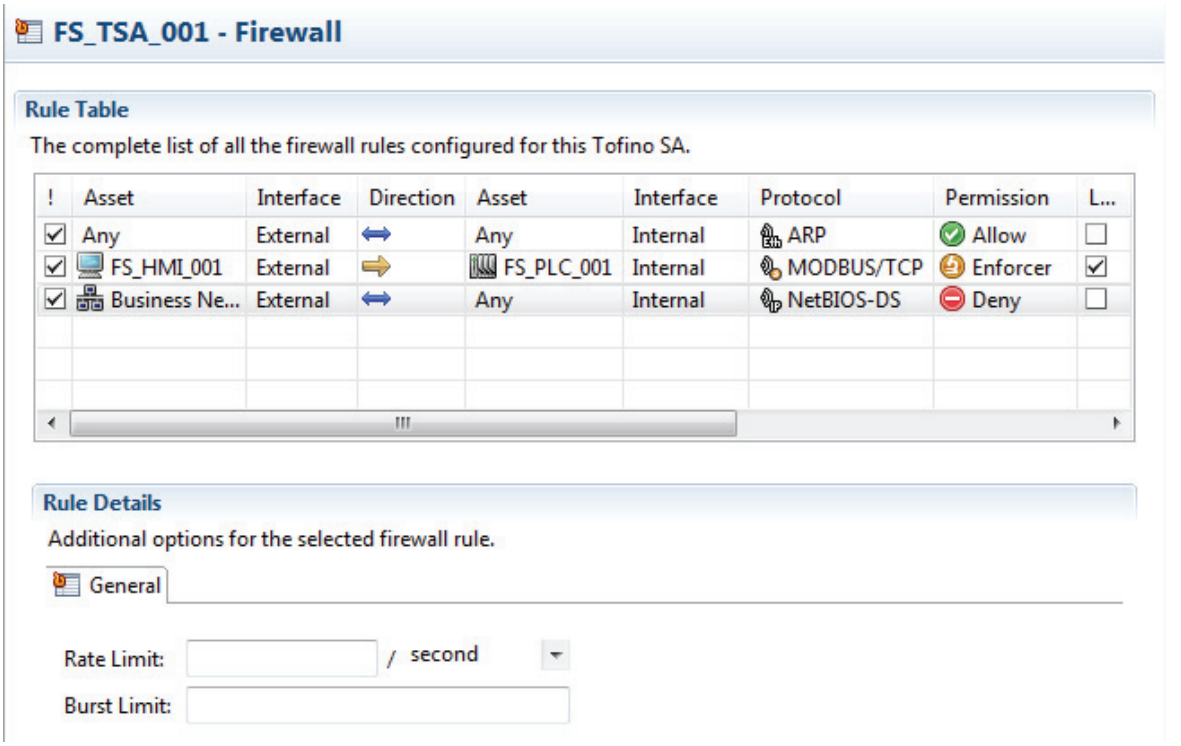


Hinweis: Wenn Sie die automatische Regelerzeugung ausgewählt haben, überprüft der ConneXium Tofino Configurator beide zuvor im Assistenten ausgewählten Ressourcen auf Protokolle, die in den Regelprofilen aufgeführt sind. Die automatische Regelerzeugung erzeugt dann eine Regel für jedes Protokoll, das die beiden Ressourcen gemeinsam haben. In folgenden Fällen wird eine Warnmeldung gesendet: Wenn die beiden Ressourcen kein gemeinsames Protokoll aufweisen; wenn die zwei Ressourcen zwar ein gemeinsames Protokoll aufweisen, aber beide entweder Clients oder Server sind.

7.2 Firewall-Regeln aufrufen und editieren

Wenn Sie in der Projekt-Explorer-Ansicht auf den Unterordner „Firewall“ der Tofino SA klicken, öffnet sich das Menüfenster mit den Details zur Firewall (Firewall Details). Hier können Sie die Firewall-Regeln für die jeweilige Tofino SA nebst entsprechenden Regeldetails ansehen und editieren (siehe „Einzelheiten zu Firewall-Regeln“). Sie können auch die Reihenfolge ändern, in der Regeln ausgewertet werden (siehe „Reihenfolge der Firewall-Regeln“). Der ConneXium Tofino Configurator fordert Sie auch auf, Firewall-Regeln zu erstellen, die er für notwendig erachtet (siehe „Assistierte Erstellung von Firewall-Regeln“).

Firewall-Regeln editieren



- ! : Über das Kontrollkästchen „Aktive Regel“ (Active Rule) können Sie die jeweilige Regel aktivieren (Häkchen gesetzt) oder deaktivieren (kein Häkchen gesetzt). Wenn Sie kein Häkchen gesetzt haben, wird die Regel nicht in die Firewall geladen. Dies bietet Ihnen die Möglichkeit, im Vorhinein Regeln zu erzeugen, die Sie erst zu einem späteren Zeitpunkt aktivieren möchten. Zudem können Sie zu Testzwecken Regeln kurzfristig deaktivieren, ohne diese zu löschen.
- Ressource (Asset) (#1):
  Eine Ressource oder Adresse, auf welche die Regel anzuwenden ist. Folgende Einträge sind gültig:
  – Beliebig
  – Ein festgelegter Ressourcen-Name
  – IP- oder MAC-Adresse
    Beachten Sie, dass bestimmte Protokolle einen bestimmten Adresstyp oder eine vordefinierte Adresse benötigen.
- Interface:
  Hier handelt es sich um die Tofino SA-Schnittstelle, bei der die links aufgeführte Ressource oder Adresse zu finden ist.

- Richtung (Direction):
  Die Richtung, mit der eine Sitzung eingeleitet wird (siehe „Rechts versus links versus bidirektional“). In der Tabelle können Sie zwischen drei möglichen Werten auswählen:
  – Rechts
  – Links
  – Bidirektional
- Ressource (Asset) (#2):
  Eine Ressource oder Adresse, auf welche die Regel anzuwenden ist. Folgende Einträge sind gültig:
  – Beliebig
  – Ein festgelegter Ressourcen-Name
  – IP- oder MAC-Adresse
    Beachten Sie, dass bestimmte Protokolle einen bestimmten Adresstyp oder eine vordefinierte Adresse benötigen.
- Interface:
  Hier handelt es sich um die Tofino SA-Schnittstelle, bei der die richtige Ressource oder Adresse zu finden ist.
- Protokoll (Protocol)
  Das Protokoll, das Sie beim Erstellen der Firewall-Regel im ConneXium Tofino Configurator definiert haben. Im Ordner „Protokolle“ finden Sie eine Liste mit Protokollen.
- Erlaubnis (Permission):
  Gibt an, wie die Firewall anhand der festgelegten Regeln mit einem Paket verfährt. Es gibt drei Möglichkeiten:
  – Zulassen (Allow): Der der Regel entsprechende Verkehr darf die Tofino SA passieren.
  – Ablehnen (Deny): Die Tofino SA blockiert den der Regel entsprechenden Verkehr.
  – Enforcer: Verkehr, der der Regel in der Tofino SA entspricht, wird anhand der Einstellungen der umfassenden Paketüberprüfung genauer untersucht und gefiltert. Diese Option steht für Protokolle wie Modbus zur Verfügung, bei denen das LSM „Enforcer“ installiert ist.

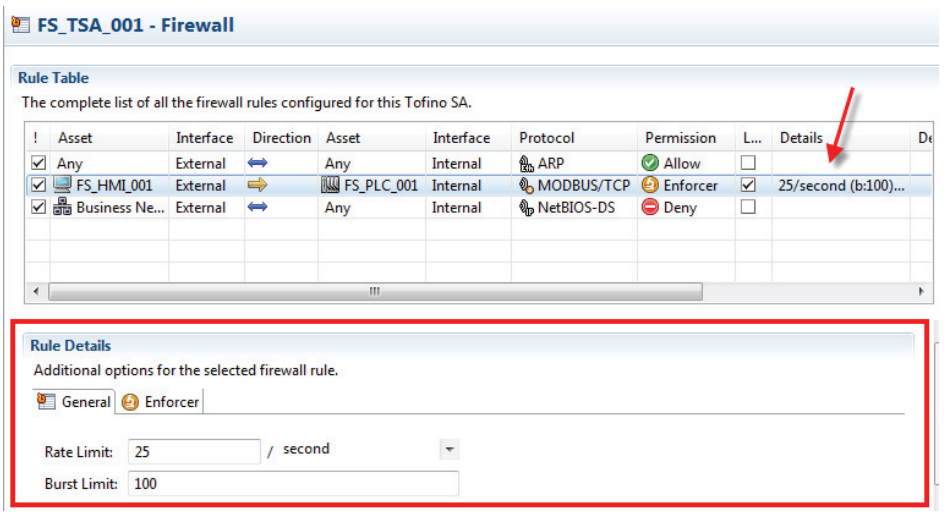
- Typ (Type):
  - Standard: Diese Regeln sind so konzipiert, dass sie spezifische Protokolle, welche die Firewall passieren, entweder zulassen oder ablehnen. Mit ihrer Hilfe kann ein Nutzer Quelle, Ziel, Richtung und Genehmigungsstatus für den Datenverkehr eines bestimmten Protokolltyps festlegen. Wenn ein Nutzer z. B. den Modbus/TCP-Verkehr zwischen zwei Geräten zulassen will, kann er eine Standardregel einsetzen.
  - Speziell (Special): Hier handelt es sich um höchst komplexe Regeln, die weit über ein einfaches Zulassen oder Ablehnen hinausgehen. Sie könnten eine Sonderregel z. B. verwenden, um eine Teilmenge eines bestimmten Verkehrstyps zu blockieren. Die verfügbaren Sonderregeln können Sie sich im gleichnamigen Ordner ansehen.
- Log:
  Ein Kontrollkästchen, um die Protokollierung für eine Regel zu aktivieren

  Hinweis: Standardmäßig werden abgelehnte Pakete protokolliert, zugelassene Pakete jedoch nicht. Wenn Sie bei einer „Zulassen“-Regel die Protokollierung auswählen, werden die Nachrichten des zugelassenen Datenverkehrs protokolliert. Wenn Sie bei einer „Ablehnen“-Regel die Protokollierung abwählen, wird der blockierte Datenverkehr verworfen, ohne dass eine Protokollierung stattfindet. Diese Option ist sinnvoll, um Broadcast-Verkehr zu blockieren, der zu übermäßigen Fehlalarmen führen kann.

- Details:
  Hier finden Sie eine kurze Zusammenfassung von Einzelheiten zu Firewall-Regeln, wie bspw. „RO“ für „Modbus Read-Only“.
- Beschreibung (Description):
  In diesem zweckmäßigen Feld kann ein Steuerungsingenieur Textangaben ergänzen und so die Regeln dokumentieren, die Sie in der Tofino SA eingerichtet haben.

Einzelheiten zu Firewall-Regeln

Bei vielen Firewall-Regeln können Sie die erweiterten Einstellungen anpassen (wie z. B. die Ratenbegrenzung des Verkehrs). Die Einstellungen für eine ausgewählte Regel werden in einem oder in mehreren Reitern unterhalb der Regeltabelle im ConneXium Tofino Configurator angezeigt. Zudem finden Sie eine Zusammenfassung dieser Regeln in der Spalte „Details“ der Firewall-Tabelle.

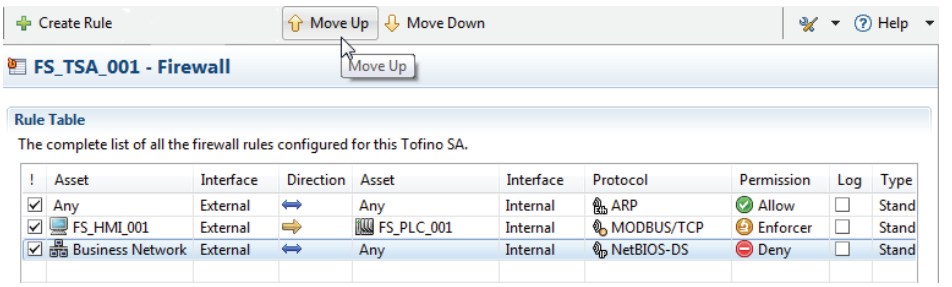


Reihenfolge der Firewall-Regeln

Die Tofino SA überprüft die Pakete nacheinander, d. h. entsprechend der Reihenfolge, in der die Regeln in der Tabelle der Firewall-Regeln angezeigt werden. Wenn Sie dieselben Regeln in einer anderen Reihenfolge anordnen, kann dies den Umgang der Tofino SA mit dem Datenverkehr drastisch verändern.

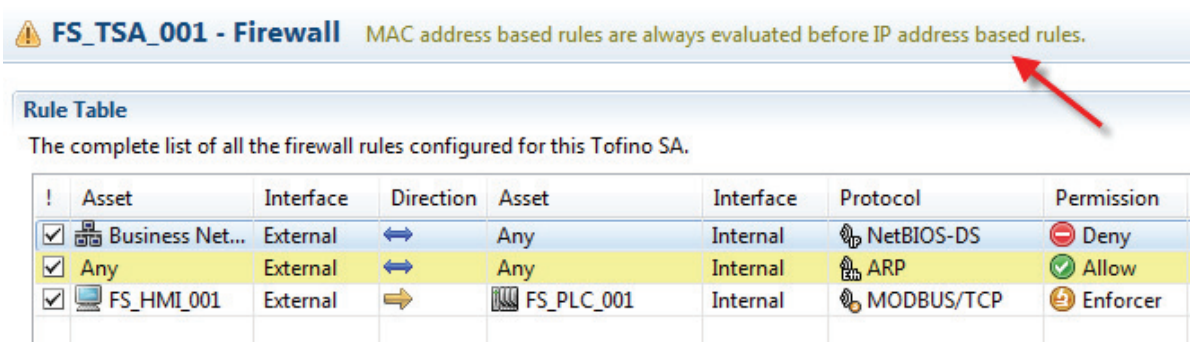
Wenn die Tofino SA ein Paket empfängt, vergleicht sie dieses zunächst mit der ersten Regel, dann mit der zweiten, der dritten usw. Wenn sie eine passende Regel findet, beendet sie die Überprüfung und wendet diese Regel an. Wenn sie das Paket mit allen Regeln vergleicht, ohne eine passende Regel zu finden, wird das Paket abgelehnt.

Sie können Regeln manuell umordnen: Wählen Sie hierzu eine Regel aus und verschieben Sie diese durch Betätigen der Schaltfläche `Nach oben (Move Up)` bzw. `Nach unten (Move Down)` in der mittleren Werkzeugleiste.



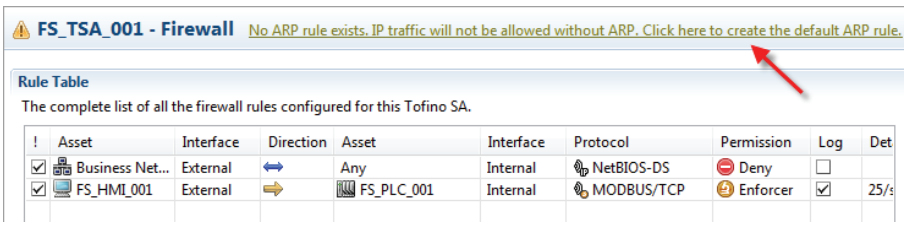
Bitte beachten Sie, dass die erste zutreffende Regel in der Tofino SA auf das Paket angewendet wird, nicht die am besten passende. Setzen Sie daher die eher spezifischen Regeln oben auf die Liste und platzieren Sie die allgemeineren darunter. So können Sie vermeiden, dass eine allgemeine Regel noch vor der spezifischeren Regel auf das Paket angewendet wird.

Es gibt jedoch gewisse Ausnahmen für diese Vorgehensweise. Dies gilt etwa, wenn Regeln, die MAC-Adressen verwenden, vor den Regeln ausgewertet werden sollen, die IP-Adressen verwenden. Falls dies erforderlich ist, gibt die ConneXium Tofino Configurator eine entsprechende Meldung aus.



Assistierte Erstellung von Firewall-Regeln

Einige Firewall-Regeln sind für das ordnungsgemäße Funktionieren anderer Regeln erforderlich. So ist z. B. eine ARP-Zulassen-Regel erforderlich, damit eine TCP-Regel funktioniert. Das liegt daran, dass die Geräte, die das TCP-Protokoll verwenden, das ARP-Protokoll zum Bestimmen der Adresse des jeweils anderen verwenden. Die Tofino SA stellt fest, wenn eine zusätzliche Regel benötigt wird und fordert Sie dazu auf, diese einzufügen.



Übertragungsbegrenzung mit der Firewall

Die Firewall-Regeln beinhalten drei erweiterte Einstellungen, mit denen Sie die Übertragungsbegrenzung konfigurieren können. Diese Einstellungen legen die Rate fest, mit der Pakete, welche die anderen Kriterien für eine bestimmte Regel erfüllt haben, die Firewall passieren dürfen. Die Übertragungsbegrenzung verwendet einen Token-Bucket-Filter-Algorithmus mit drei Einstellungen:

- Ratenbegrenzung (Rate Limit): Die zulässige durchschnittliche Paketübertragungsrate in einer festgelegten Zeitspanne
- Intervall (Interval): Die für die Übertragungsbegrenzung verwendete Zeitspanne (in Sekunden, Minuten oder Stunden)
- Paketbegrenzung (Burst Limit): Die maximale anfängliche Zahl zugelassener Pakete. Diese ist größer oder gleich der Ratenbegrenzung.

Um das Prinzip der Token-Bucket-Filterung besser zu verstehen, können Sie sich einen „Eimer“ (engl. bucket) voller Sendezeichen (engl. tokens) vorstellen. Die Firewall benötigt ein Sendezeichen, um ein Datenpaket weiterzuleiten. Wenn sich im „Eimer“ keine Sendezeichen mehr befinden, werden die von der Firewall solange verworfen, bis sich wieder Sendezeichen im „Eimer“ befinden. Die Anzahl der Sendezeichen (und somit die Anzahl der weitergeleiteten Pakete) wird durch zwei Einstellungen gesteuert – die Ratenbegrenzung und die Paketbegrenzung.

Die Ratenbegrenzung bezeichnet die Geschwindigkeit, mit der der „Eimer“ wieder mit Sendezeichen befüllt wird. Die Ratenbegrenzung wird anhand eines Intervalls berechnet, welches der Benutzer festlegt (z. B. pro Sekunde oder pro Minute). Wenn also die Ratenbegrenzung den Wert 50 aufweist und das Intervall auf „pro Sekunde“ eingestellt ist, werden 50 Sendezeichen pro Sekunde in den „Eimer“ gefüllt und 50 Pakete pro Sekunde durch die Firewall gelassen. Beachten Sie, dass das Wiederbefüllen des Eimers schrittweise während des Intervalls vor sich geht, anstatt in einem Zug am Beginn des Intervalls.

Bei der Paketbegrenzung handelt es sich zum einen um die anfängliche Zahl von Sendezeichen im „Eimer“, zum anderen um die maximale Anzahl von Sendezeichen, die der „Eimer“ aufnehmen kann. Anders gesagt, trägt dieser Parameter dazu bei, dass sich in Zeiten mit geringem Datenverkehr keine Anhäufung von Sendezeichen ergibt.

Die Firewall lässt umgehend jede Anhäufung von Paketen passieren, deren Anzahl der Anzahl von Sendezeichen im „Eimer“ entspricht. Wenn der Eimer leer ist, kann die Firewall Datenpakete nur analog zur Wiederbefüllung und mit der durch die Ratenbegrenzung festgelegten Geschwindigkeit weiterleiten. Wenn die Paketrate die Ratenbegrenzung übersteigt, leert sich der Eimer mit der Geschwindigkeit der Paketrate. Die Wiederbefüllung des Eimers wird dann durch die Ratenbegrenzung beschränkt. Anders formuliert: Wenn Sie die Paketbegrenzung auf 100 und die Ratenbegrenzung auf 25 pro Sekunde setzen und 1000 Pakete zur Firewall senden, werden die ersten 100 Pakete durchgelassen und im Anschluss daran 25 Pakete pro Sekunde. Alle anderen Pakete werden verworfen.

Rechts versus links versus bidirektional

Viele Firewall-Regeln sind mit einer bestimmten Richtung verknüpft. Diese angezeigte Pfeilrichtung gibt an, welches Gerät die Verbindung zwischen den zwei Knoten aufbaut. Sie bezieht sich nicht auf den Paketfluss. Wenn z. B. eine Mensch-Maschine-Schnittstelle (HMI) Modbus/TCP verwendet, um Daten von einer speicherprogrammierbaren Steuerung (SPS) anzufordern, ist die HMI dasjenige Gerät, das die Kommunikationsverbindung einrichtet. Sobald die Verbindung hergestellt ist, fließen die Pakete in beide Richtungen.

Sie können sich dies auch wie ein normales Telefonsystem vorstellen. Die Person, die die Rufnummer wählt (Person 1) ist diejenige, welche die Verbindung einrichtet (d. h. erstellt). Sobald die andere Person (Person 2) das Gespräch annimmt, kann die Sprache in beide Richtungen fließen.

Mit dem LSM „Tofino Firewall“ können Sie beim Einrichten einer Verbindung zwischen drei Möglichkeiten wählen:

- Rechts: Verbindungen können – gemäß Festlegung in der Regeltabelle – nur von der linken Ressource erstellt werden und fließen in Richtung rechts. So könnte es sich bei der linken Ressource um die HMI und bei der rechten um die SPS handeln; die Verbindungsrichtung wäre auf „rechts“ gesetzt. Die HMI dürfte dann die Verbindung initiieren. Die SPS dürfte antworten, hätte jedoch keine Genehmigung, eine Sitzung zu initiieren.

- Links: Verbindungen können – gemäß Festlegung in der Regeltabelle – ausschließlich von der rechten Ressource erstellt werden und fließen in Richtung links. So könnte es sich bei der rechten Ressource um eine Arbeitsstation mit einem Browser-Client und bei der linken um einen Web-Server handeln; die Verbindungsrichtung wäre auf „links“ gesetzt. Die Arbeitsstation dürfte dann die Verbindung initiieren. Der Web-Server dürfte antworden, hätte jedoch keine Genehmigung, eine Sitzung zu initiieren.

- Bidirektional: Verbindungen können von beiden Geräten hergestellt werden.

Denken Sie daran, dass der Datenverkehr in beide Richtungen fließen kann, sobald die Verbindung hergestellt ist – unabhängig von der in der Regel definierten Richtung.

7.3 Verwenden von „Modbus TCP Enforcer“-Regeln

Beim LSM „Modbus TCP Enforcer“ handelt es sich um eine Firewall, die eine umfassende Paketüberprüfung für das Modbus-TCP-Protokoll bietet. Diese ermöglicht es Ihnen, Datenverkehr anhand von bestimmten Modbus-Funktions-Codes, Registerbereichen und der Gültigkeit von Modbus-Nachrichten zu filtern. Beim LSM „Modbus TCP Enforcer“ handelt es sich um ein Sicherheits-Software-Modul für die reguläre ConneXium Tofino Firewall.

Aktivieren des LSMs „Modbus TCP Enforcer“

Um die Funktionsmerkmale des „Modbus TCP Enforcer“ nutzen zu können, aktivieren Sie im Bereich „Allgemeine Einstellungen einer Tofino SA“ der Tofino SA die LSMs „Firewall“ und „Modbus TCP Enforcer“.

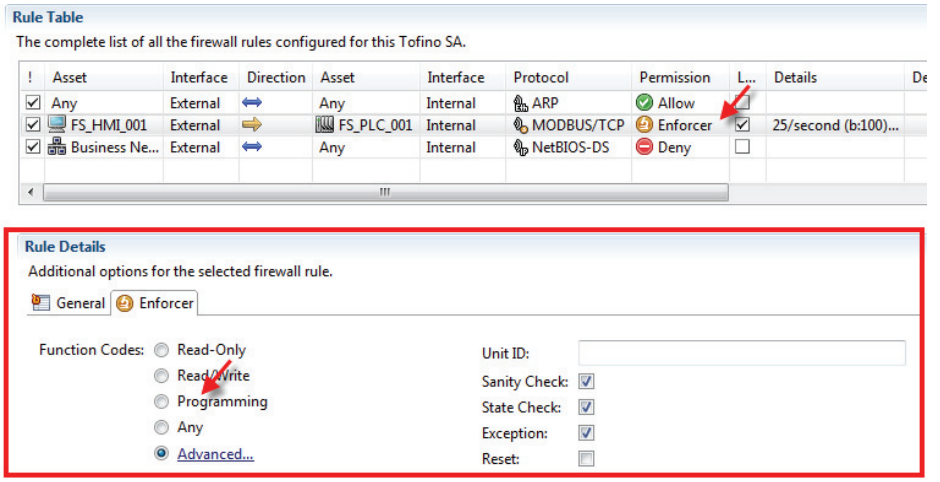
Regeln für den „Modbus TCP Enforcer“ erstellen

Führen Sie die folgenden Schritte aus, um eine Firewall-Regel für den „Modbus TCP Enforcer“ zu erstellen:

- ☐ Erzeugen Sie eine Firewall-Regel zwischen zwei Ressourcen.
- ☐ Stellen Sie das Protokoll entweder auf Modbus TCP oder auf Modbus UDP ein.
- ☐ Stellen Sie die Richtung für die Regel so ein, dass sie VOM Modbus-Master ZUM Modbus-Slave wirkt. (Bedenken Sie, dass keine Möglichkeit besteht, die Option „Bidirektional“ mit dem LSM „Modbus TCP Enforcer“ zu verwenden.)
- ☐ Setzen Sie den Parameter „Erlaubnis“ (Permission) auf „Enforcer“.

  Hinweis: Wenn Sie „Zulassen“ oder „Ablehnen“ auswählen, erlaubt bzw. blockiert die Tofino SA den Modbus-Verkehr entsprechend, ohne den „Modbus TCP Enforcer“ hierfür heranzuziehen.

Wenn Sie eine Regel für den „Modbus TCP Enforcer“ erstellen, ist es erforderlich, diese im nächsten Schritt zu konfigurieren.



Regeln für den „Modbus TCP Enforcer“ konfigurieren

Führen Sie die folgenden Schritte aus, um die von Ihnen erstellte Firewall-Regel für den „Modbus TCP Enforcer“ zu konfigurieren:

☐ Klicken Sie auf den Reiter „Enforcer Details“.
☐ Konfigurieren Sie die nachfolgenden Felder gemäß Ihren Bedürfnissen:

- Funktions-Codes: Setzen Sie diese auf einen der folgenden Werte:

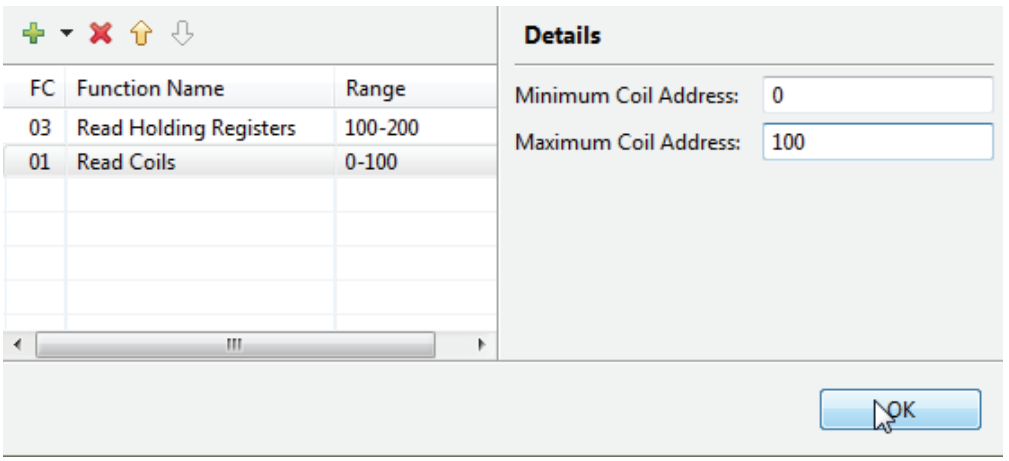
  Nur lesen (Read-Only): Es sind nur Funktions-Codes zulässig, bei denen es sich um Datenlesebefehle handelt.
  Lesen/Schreiben (Read/Write): Es sind nur Funktions-Codes zulässig, bei denen es sich entweder um Datenlese- oder um Datenschreibbefehle handelt.
  Programmierung/OFS (Programming/OFS): Es sind nur Funktions-Codes zulässig, bei denen es sich entweder um Daten-Lese/Schreib-Befehle oder um Programmierbefehle handelt.
  Beliebig (Any): Alle Modbus-Funktions-Codes sind zulässig.
  Erweitert (Advanced): Öffnet ein neues Fenster, in welchem Sie Funktions-Codes und -Bereiche individuell auswählen können.

- Geräte-ID (Unit ID):
  Die Tofino SA verwendet den sog. „Unit Identifier“, um über Geräte (wie Bridges, Router und Gateways) zu kommunizieren, die mit einer einzigen IP-Adresse mehrere unabhängige Modbus-Endgeräte unterstützen. Bei den meisten Modbus-TCP-Anwendungen sollten Sie diesen Wert auf 0 oder 1 setzen. Wenn Sie keine Überprüfung der Geräte-ID möchten, löschen Sie die Angaben in diesem Feld.
- Plausibilitätsprüfung (Sanity Check):
  Bei den bekannten Modbus-Befehlen (1-6, 15, 16, 20-24) kann die Tofino SA prüfen, ob die Nachrichten wohlgeformt sind und der Modbus-Spezifikation entsprechen. Sollte dies nicht der Fall sein, blockiert die Tofino SA die betreffenden Nachrichten. Wenn z. B. der Modbus-Befehl „Mehrere Register schreiben“ (Funktions-Code 16) einen Wert in seinem Längenfeld enthält, der entweder unzulässig ist oder nicht der gesendeten Datenmenge entspricht, wird die betreffende Nachricht verworfen. Bei Modbus-Geräten, die

nicht der Spezifikation Modbus/TCP 1.1b entsprechen, kann es notwendig sein, dass Sie diese Option deaktivieren. (Beachten Sie, dass die Plausibilitätsprüfung des „Modbus Application Header“ (MBAP) unabhängig von Ihrer hier vorgenommenen Einstellung durchgeführt wird.)

- Zustandsüberprüfung (State Check): Wenn Sie hier ein Häkchen setzen, blockiert die Tofino SA alle Modbus-Befehle und -Antworten, die im Hinblick auf den aktuellen Verbindungsstatus in einer falschen Abfolge gesendet werden. Drei Beispiele verdeutlichen das Prinzip einer Kommunikation mit falscher Abfolge: 1) Ein Master-Gerät gibt zwei Befehle aus, ohne dass das Slave-Gerät dazwischen eine Antwort sendet. 2) Ein Slave-Gerät gibt einen Befehl an ein Master-Gerät aus. 3) Ein Master-Gerät gibt eine Antwort an ein Slave-Gerät aus. Wenn Sie hier kein Häkchen setzen, findet keine Blockierung solcher falsch ablaufenden Befehle und Antworten durch die Tofino SA statt.
- Ausnahme (Exception): Wenn Sie hier ein Häkchen setzen, sendet die Tofino SA gegebenenfalls eine Modbus-TCP-Ausnahmeantwort an das Modbus-Gerät, das die blockierte Nachricht erzeugt hat. Bitte beachten Sie, dass einige unzulässige Modbus-TCP-Nachrichten eine definierte Ausnahmeantwort enthalten.
  Bei Modbus-UDP empfiehlt es sich, kein Häkchen bei „Ausnahme“ zu setzen und die Option „Zurücksetzen“ anzuklicken bzw. auszuwählen.
- Zurücksetzen (Reset): Wenn Sie dieses Kontrollkästchen anklicken, sendet die Tofino SA beim Blockieren einer Nachricht eine „TCP Reset“-Nachricht an beide Modbus-Geräte. Hierdurch können Sie das Sperren von Sitzungen bei bestimmten, mangelhaft gestalteten Modbus-Produkten vermeiden.

☐ Wenn Sie für den betreffenden Funktions-Code „Erweitert“ (Advanced) auswählen, öffnet sich das Fenster für die erweiterte Filterung der Modbus-TCP-Funktions-Codes (Advanced Modbus TCP Function Code Filtering). Hier können Sie die Funktions-Codes sowie die Register- und Ausgangsbereiche festlegen, die Sie für die betreffende Regel zulassen möchten. Klicken Sie hierfür in der Werkzeugleiste auf die Schaltfläche `Funktions-Code hinzufügen (Add Function Code)` . Wählen Sie dann den zu erlaubenden Funktions-Code aus und fügen Sie optional einen Register- oder Ausgangsbereich hinzu. Sie können so viele Funktions-Codes wie benötigt hinzufügen. Allerdings sollten Sie den betreffenden Funktions-Code nur einmal pro Regel eingeben.


FC
Function Name
Range
03
Read Holding Registers
100-200
01
Read Coils
0-100
Details
Minimum Coil Address:
0
Maximum Coil Address:
100
OK

8 Konfigurieren von Ereignisprotokollen

Das Sicherheitsmodul „Event Logger“ können Sie einsetzen, um für die Tofino SA externe Alarm-Meldungen und die Versendung von Ereignisprotokollen zu einem Systemprotokollserver bereitzustellen. Es bietet Ihnen zwei Möglichkeiten, um Ereignisprotokolle zu speichern:

- Über das Systemprotokoll: Ausnahmeereignisse der Tofino SA werden an einen entfernten Systemprotokollserver weitergeleitet.
- Über die Speicherung von Ausnahmeereignissen in den Langzeitspeicher der Tofino SA und die Übertragung der Daten auf ein USB-Speichermedium.

Aktivieren des LSMs „Event Logger“

Damit Ihnen die Funktionen des Event Loggers zur Verfügung stehen, aktivieren Sie das LSM „Event Logger“ in derTofino SA unter „Allgemeine Einstellungen einer Tofino SA“.

Einrichten des LSMs „Event Logger“

Sie können den „Event Logger“ konfigurieren, wenn Sie in der Projektansicht auf den entsprechend bezeichneten Ordner klicken.

- IP-Adresse Syslog-Server (Syslog Server IP Address):
  Hier geben Sie die Adresse des Systemprotokollservers ein, an den Sie die Protokolle senden möchten. Setzen Sie alle Felder auf Null, wenn Sie die Fernprotokollierung deaktivieren möchten.
- Standard-Gateway (Default Gateway):
  Hier handelt es sich um die IP-Adresse des weiterleitenden Routers des Netzes, in dem sich die Tofino SA befindet. Diese Angabe ist nur dann erforderlich, wenn sich der Systemprotokollserver in einem **anderen** Netz als die Tofino SA befindet. Wenn Sie die Systemprotokollierung nicht nutzen oder wenn sich die Tofino SA und der Systemprotokollserver auf demselben Subnetz befinden, schreiben Sie Nullen in dieses Feld.
- Ziel-Port (Destination Port):
  Hier handelt es sich um die Nummer des UDP-Ports, an dem Ihr Systemprotokollserver nach Protokollmeldungen „lauscht“ (üblicherweise Port 514). Lassen Sie das Feld leer, wenn Sie die Systemprotokollierung deaktivieren möchten.
- Kleinste protokollierte Priorität (Lowest Priority Logged):
  Hier legen Sie die kleinste Protokollierungsstufe fest, ab der die Tofino SA aufzeichnen soll. Wenn Sie die Priorität auf 0 setzen, werden nur Notfallereignisse aufgezeichnet. Wenn Sie die Priorität auf 7 setzen, wird jedes ermittelte Ereignis aufgezeichnet. Die Voreinstellung beträgt 5.

	Niedrigste zu protokollierende Meldung mit Priorität
0	Notfall: Das System ist unbrauchbar.
1	Alarm: Sofortige Maßnahmen sind erforderlich.
2	Kritisch: bei kritischen Situationen
3	Fehler: bei fehlerhaften Zuständen
4	Warnung: bei Situationen, die eine Warnmeldung erforderlich machen
5	Hinweis: bei normalen, aber bedeutsamen Situationen
6	Information: informative Meldungen
7	Debug: Debug-Meldungen

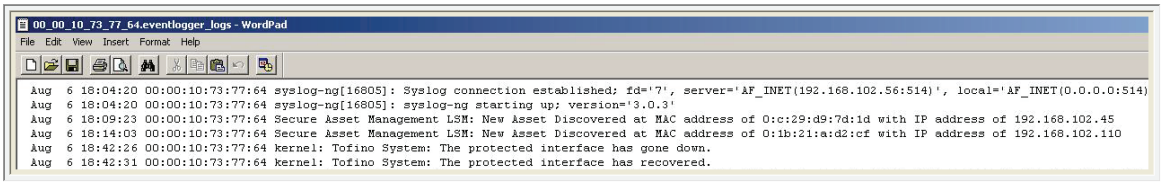
Tab. 1: Einstellmöglichkeiten beim Event Logger in Bezug auf die niedrigste zu protokollierende Meldung mit Priorität

Hinweis: Bedenken Sie, dass die Tofino SA keine IP-Adresse benötigt, um mit einem entfernten Systemprotokollserver zu kommunizieren. Die Tofino SA verwendet eine spezielle „Tarnkappentechnik“, um ohne IP-Adresse kommunizieren zu können. Für den Systemprotokollserver stellen sich die Quelladressen entweder als 0.0.0.0 oder als 169.254.2.2 dar.

Protokolle von einem USB-Speichermedium abrufen

Um die auf der Tofino SA gespeicherten Protokolle abzurufen, schließen Sie ein USB-Speichermedium am USB-Port der Tofino SA an und starten Sie den USB-Speichervorgang. Weitere Informationen finden Sie unter: „USB-Speichervorgänge mit Ihrer Tofino SA“

Wenn Sie die Protokolle auf das USB-Speichermedium übertragen haben, schließen Sie dieses an einen Rechner an. Auf dem Speichermedium finden Sie nun die Dateien mit den Protokollen. Die Protokolle werden in den Dateien <tofino id>_evt.log sowie <tofino id>_evt.<X>.gz gespeichert. Die mit evt.log bezeichneten Dateien enthalten die aktuellsten Ereignisse und sind unkomprimiert. Die mit evt.X.gz bezeichneten Dateien sind komprimiert und enthalten ältere Ereignisprotokolle. Sie können die mit evt.log bezeichneten Dateien mit einem Systemprotokoll-Viewer oder (wegen der besseren Formatierung) mit WordPad öffnen. Die mit evt.X.gz bezeichneten Dateien können Sie mit einer Software entpacken, die das GZIP-Format beherrscht (z. B. WinRAR oder 7-Zip). Nachstehend finden Sie ein Beispiel für eine mit Microsoft WordPad geöffnete Protokolldatei.



9 Konfigurationen laden und überprüfen

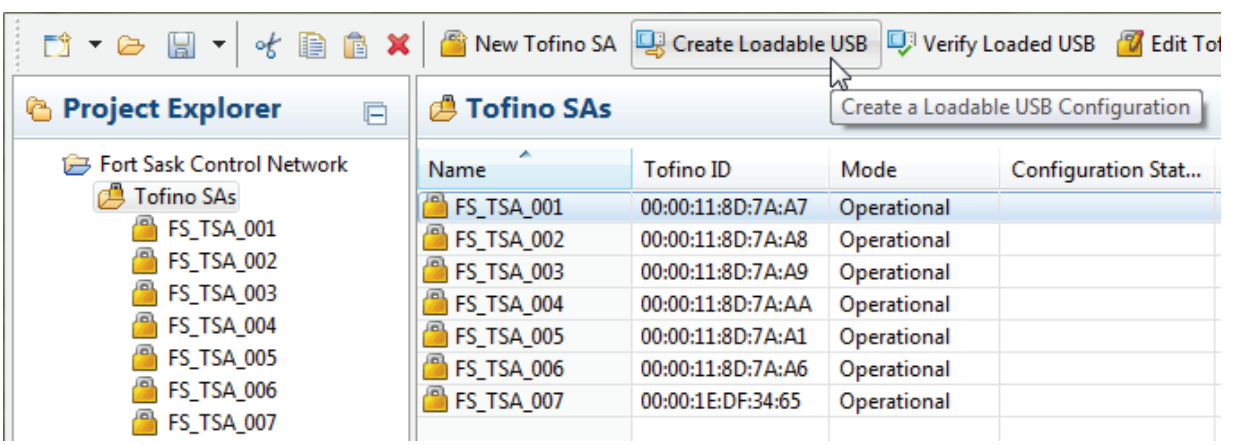
Nachdem Sie die Tofino SAs im ConneXium Tofino Configurator konfiguriert haben, übertragen Sie diese Konfigurationen an die Tofino SAs im Feldbereich. Dabei handelt es sich um einen Vorgang in drei Schritten:

- ☐ Erzeugen Sie eine Konfiguration auf einem USB-Speichermedium: Hierdurch erstellen Sie verschlüsselte Konfigurationsdateien auf dem USB-Speichermedium, welche Sie in die Tofino SAs laden können.
- ☐ Übertragen Sie die Konfiguration an die Tofino SAs: Stecken Sie das USB-Speichermedium mit den Konfigurationsdateien in den USB-Port der entsprechenden Tofino SA und laden Sie die Konfiguration dort ein.
- ☐ Überprüfen Sie die auf dem USB-Speichermedium befindliche Konfiguration: Mit dem entsprechenden Befehl rufen Sie die Konfigurations-Ladeprotokolle von dem USB-Speichermedium ab, mit dem Sie Konfigurationen in eine oder mehrere Tofino SAs geladen haben. Hierdurch können Sie die Konfigurationen der Tofino SAs im Feldbereich aufzeichnen und überprüfen und diese in Ihrem Projekt speichern.

9.1 Eine USB-Konfiguration erzeugen

Verwenden Sie den Befehl `Portable USB-Konfiguration erzeugen (Create Loadable USB Drive)` im ConneXium Tofino Configurator, um eine Tofino SA im Feldbereich zu konfigurieren. Dieser Befehl erzeugt eine ladbare Konfiguration für eine Tofino SA die Sie auf einem ausgewählten USB-Speichermedium speichern können. Sie können dieses Speichermedium dann in einen USB-Port der entsprechenden Tofino SA stecken und die Konfiguration dort einladen.

☐ Wählen Sie die Tofino SAs aus, für die Sie eine USB-Konfiguration erzeugen wollen. Sie können mehrere Tofino SA-Konfigurationen auf demselben USB-Speichermedium speichern.
☐ Klicken Sie in der mittleren Werkzeugleiste auf die Schaltfläche `Portable USB-Konfiguration erzeugen (Create Loadable USB)`.



☐ Wählen Sie das USB-Speichermedium aus, auf das Sie die Konfigurationsdateien speichern wollen.

Sie haben die Möglichkeit, eine ladbare USB-Konfigurationsdatei zu erstellen, wenn die folgenden Bedingungen erfüllt sind:

- Die Konfiguration der Tofino SA enthält keine Fehler.
- Sie haben Schreibzugriff auf die Projektdatei.
- Sie haben Änderungen am Projekt gespeichert.

Durch die Erfordernis für einen Schreibzugriff können Sie verhindern, dass Benutzer ohne ausreichende Berechtigung die im Feldbereich befindlichen Tofino SAs modifizieren.

Mittels der letzten Anforderung können Sie die Wahrscheinlichkeit verringern, dass sich die Konfiguration, die in die Tofino SAs im Feldbereich geladen wird, von der Konfiguration in der Projektdatei unterscheidet.

9.2 USB-Ladevorgänge mit Ihrer Tofino SA

Die Schaltfläche „Speichern/Laden/Reset“ an der Tofino SA stellt drei Funktionen bereit. Diese hängen davon ab, wie oft Sie auf die Schaltfläche drücken.

- Einmal: Speichert Diagnose- und Protokolldateien auf ein USB-Speichermedium.
- Zweimal: Lädt Konfigurationsdateien von einem USB-Speichermedium.
- Dreimal: Setzt die Tofino SA auf den werksseitigen Lieferzustand zurück.

Über die USB-Ladefunktion können Sie entweder die vom ConneXium Tofino Configurator erzeugten Konfigurationsdateien oder Firmware-Aktualisierungen in die Tofino SA einladen. Verwenden Sie hierzu ein USB-Speichermedium (siehe „Eine USB-Konfiguration erzeugen“).

Hinweis: Erfahrungsgemäß funktionieren folgende USB 2.0-Speichermedien-Fabrikate: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar sowie Schneider TCSEAM0100. Andere Fabrikate und Modelle funktionieren möglicherweise, wurden jedoch nicht getestet.

⚠ WARNUNG

NICHT VORGESEHENER BETRIEB DES GERÄTES

Führen Sie die nachstehenden Schritte zum Laden der Konfiguration sorgfältig durch.

- ☐ Schalten Sie dieTofino SA an und warten Sie mindestens eine Minute.
- ☐ Schließen Sie das USB-Speichermedium mit den vorbereiteten Dateien an einen der USB-Ports des Gerätes an.
- ☐ Klicken Sie zweimal auf die Schaltfläche „Speichern/Laden/Reset (Save Load Reset)“.
- ☐ Die Anzeigen 1/S sowie 2/L leuchten auf und zeigen einen Ladevorgang an.
- ☐ Nach einigen Sekunden läuft eine Blink-Sequenz von rechts nach links und zeigt einen laufenden USB-Ladevorgang an.
- ☐ Entfernen Sie das USB-Speichermedium, wenn die Blink-Sequenz beendet ist.

Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.

Wenn der Ladevorgang erfolgreich war, erlischt die Fehler-LED der Tofino SA.

Nach einem erfolgreichen Ladevorgang per USB sollten sich pro Tofino SA mindestens fünf Dateien auf dem USB-Speichermedium befinden (<tofino id> wird dabei durch die tatsächliche Kennung der Tofino SA ersetzt):

- <tofino id>_tc_data
  „USB-Überprüfung“-Daten, die anzeigen, ob die Konfiguration erfolgreich oder fehlerhaft war.
- <tofino id>_diagnostics.txt
  Diagnosedaten zur Tofino SA (siehe „Diagnosefunktionen der Tofino SA“).
- <tofino id>_evt.log sowie <tofino id>_evt.<X>.gz
  Ereignisprotokolle der Tofino SA (siehe „Konfigurieren von Ereignisprotokollen“).

- <tofino id>_kernel_evt.enc:
  Verschlüsselte Informationen zur Diagnose des Kernels (ausschließlich zur werkseitigen Fehlersuche und -behebung).
- <tofino id>_diagnostics.enc
  Verschlüsselte Informationen zur Diagnose des Moduls (ausschließlich zur werkseitigen Fehlersuche und -behebung).

Hinweis: Während der Erstkonfiguration oder während der Aktualisierung der Konfiguration lässt die Tofino SA den Netzverkehr ohne Einschränkungen passieren. Die Firewall-Regeln werden erst dann wirksam, wenn Sie die Erstkonfiguration oder die Aktualisierung der Tofino SA abgeschlossen haben; d. h. der Netzbetrieb wird erst dann beeinflusst, wenn Sie den vollständigen Regelsatz geladen haben. Das Laden einer durchschnittlichen Konfiguration dauert etwa 30 Sekunden.

9.3 USB-Speichervorgänge mit Ihrer Tofino SA

Die Schaltfläche „Speichern/Laden/Reset“ an der Tofino SA stellt drei Funktionen bereit. Diese hängen davon ab, wie oft Sie auf die Schaltfläche drücken.

- Einmal: Speichert Diagnose- und Protokolldateien auf ein USB-Speichermedium.
- Zweimal: Lädt Konfigurationsdateien von einem USB-Speichermedium.
- Dreimal: Setzt die Tofino SA auf den werksseitigen Lieferzustand zurück.

Die USB-Speicherfunktion kopiert Diagnose- und Validierungsdateien von der Tofino SA auf ein USB-Speichermedium. Sie können diese Dateien dann mit Hilfe der Funktion „USB-Konfiguration prüfen“ des ConneXium Tofino Configurators validieren oder sie zur Analyse an den technischen Support senden.

Zum Erzeugen dieser Dateien ist es erforderlich, dass Sie eine Speicherung via USB durchführen. Bitte beachten Sie, dass durch einen USB-Ladevorgang auch ein USB-Speichervorgang ausgeführt wird. Dies dient dem Zweck, die Ergebnisse des Ladevorgangs und den Status der Tofino SA nach Abschluss des Vorgangs aufzuzeichnen.

- ☐ Schalten Sie die Tofino SA an und warten Sie mindestens eine Minute.
- ☐ Schließen Sie das USB-Speichermedium an einen der USB-Ports des Gerätes an.
- ☐ Klicken Sie einmal auf die Schaltfläche „Speichern/Laden/Reset (Save Load Reset)“.
- ☐ Die Anzeige 1/S leuchtet auf.
- ☐ Nach einigen Sekunden läuft eine Blink-Sequenz von links nach rechts und zeigt einen laufenden USB-Speichervorgang an.
- ☐ Entfernen Sie das USB-Speichermedium, wenn die Blink-Sequenz beendet ist.
- ☐ Bei erfolgreicher Speicherung kehren die LEDs der Tofino SA wieder in den Status zurück, den sie vor dem Speichervorgang hatten.

Hinweis: Erfahrungsgemäß funktionieren folgende USB 2.0-Speichermedien-Fabrikate: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar sowie Schneider TCSEAM0100. Andere Fabrikate und Modelle funktionieren möglicherweise, wurden jedoch nicht getestet.

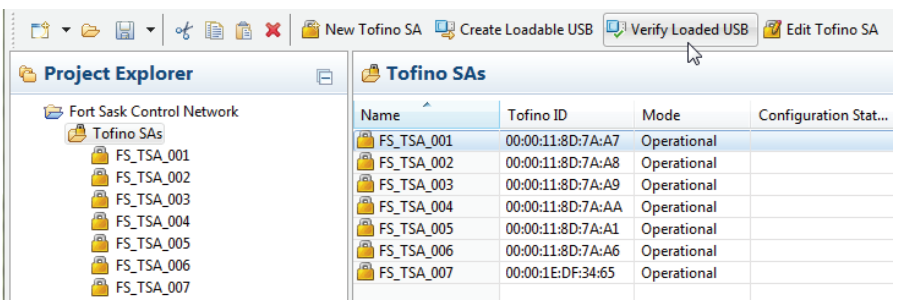
Nach einem erfolgreichen Speichervorgang per USB sollten sich pro Tofino SA mindestens fünf Dateien auf dem USB-Speichermedium befinden. Hierbei handelt es sich um folgende Dateien (wobei <tofino id> durch die tatsächliche Kennung der Tofino SA ersetzt wird):

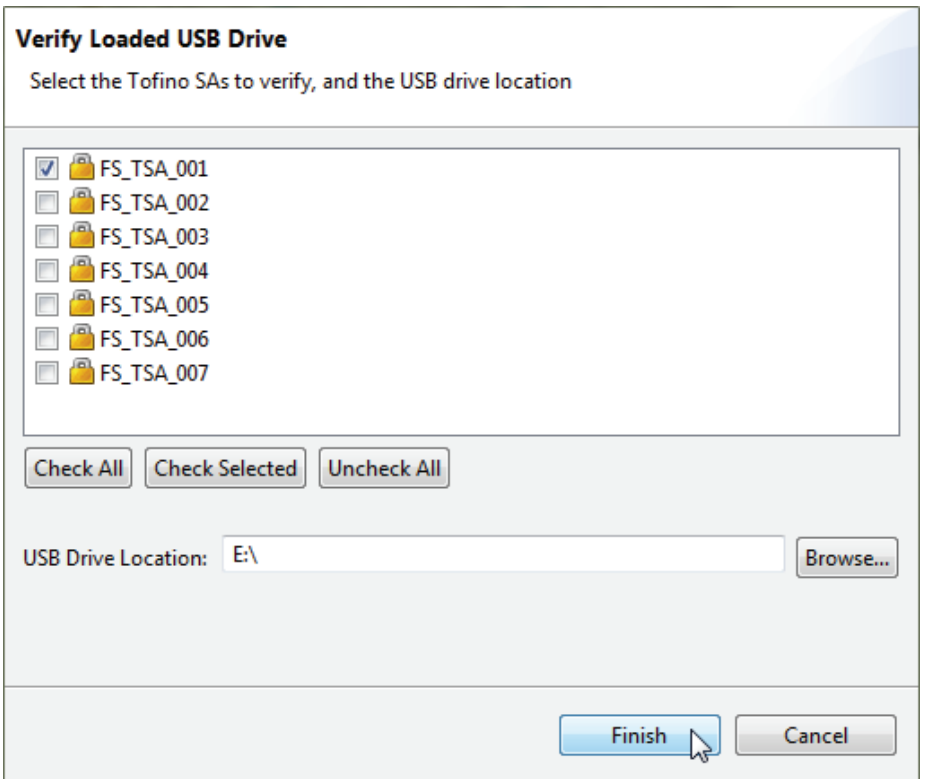
- <tofino id>_tc_data
  „USB-Überprüfung“-Daten, die anzeigen, ob die Konfiguration erfolgreich oder fehlerhaft war.
- <tofino id>_diagnostics.txt
  Diagnosedaten zur Tofino SA (siehe „Diagnosefunktionen der Tofino SA“).
- <tofino id>_evt.log sowie <tofino id>_evt.<X>.gz
  Ereignisprotokolle der Tofino SA (siehe „Konfigurieren von Ereignisprotokollen“).
- <tofino id>_kernel_evt.enc
  Verschlüsselte Informationen zur Diagnose des Kernels (ausschließlich zur werkseitigen Fehlersuche und -behebung).
- <tofino id>_diagnostics.enc
  Verschlüsselte Informationen zur Diagnose des Moduls (ausschließlich zur werkseitigen Fehlersuche und -behebung).

9.4 USB-Überprüfung

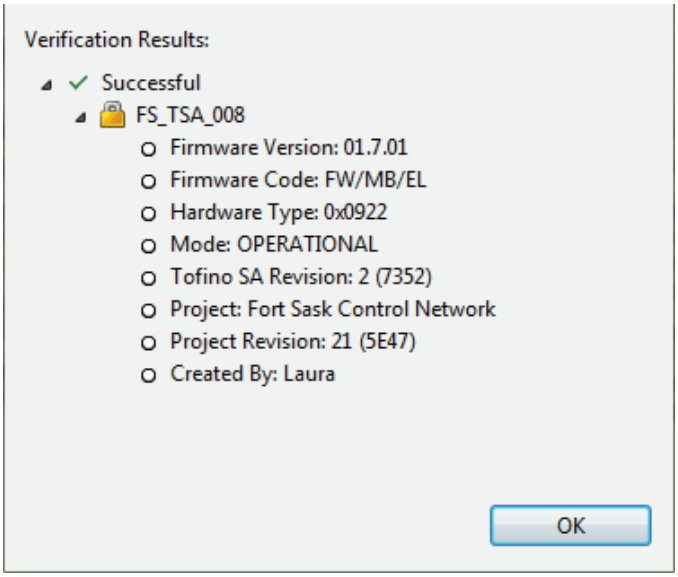
Verwenden Sie die Funktion `USB-Konfiguration prüfen`, um die Konfiguration einer oder mehrerer Tofino SAs zu überprüfen. Mit diesem Befehl rufen Sie die Konfigurations-Ladeprotokolle von dem USB-Speichermedium ab, mit dem Sie Konfigurationen in eine oder mehrereTofino SAs geladen haben. Hierdurch können Sie die Konfigurationen der Tofino SAs im Feldbereich aufzeichnen und überprüfen.

- ☐ Schließen Sie das die Daten enthaltende USB-Speichermedium an Ihren Rechner an.
- ☐ Wählen Sie eine oder mehrere Tofino SAs aus, die Sie prüfen möchten.
- ☐ Klicken Sie in der mittleren Werkzeugleiste auf die Schaltfläche`USB-Konfiguration prüfen (Verify Loaded USB)`. Es erscheint ein Assistent, der Sie durch die Überprüfung der Konfiguration auf dem ausgewählten USB-Laufwerk führt.
- ☐ Wählen Sie die Tofino SA aus, die Sie prüfen möchten.
- ☐ Wählen Sie den Speicherort auf dem USB-Laufwerk aus.





Der ConneXium Tofino Configurator zeigt die Prüfdaten an und protokolliert sie. Die Konfigurationsrevision, der Gerätetyp und die Firmware-Version der überprüften Tofino SAs werden in der Projektdatei aktualisiert. Sie können sich die Prüfdaten auch im Ordner „Allgemeine Einstellungen einer Tofino SA“ der jeweiligen Tofino SA ansehen.

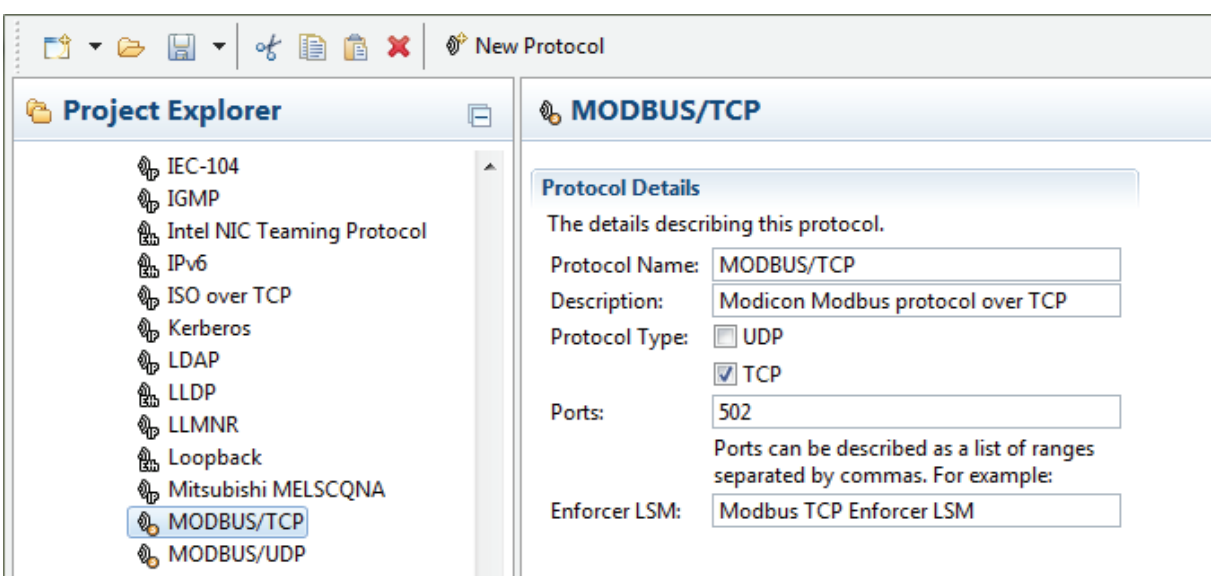

Verification Results:
Successful
FS_TSA_008
Firmware Version: 01.7.01
Firmware Code: FW/MB/EL
Hardware Type: 0x0922
Mode: OPERATIONAL
Tofino SA Revision: 2 (7352)
Project: Fort Sask Control Network
Project Revision: 21 (5E47)
Created By: Laura
OK

10 Weiterführender Themenbereich - Erzeugen und Verwalten von Protokollen

Im ConneXium Tofino Configurator definiert der Bereich „Protokolle“ (Protocols) die einzelnen Dienste, die zwischen Geräten im Netz kommuniziert werden. So erfordert die Nutzung von Internet-Verkehr in einem Netz das HTTP-Protokoll für die Kommunikation zwischen einem Web-Server und einem Web-Client. Analog hierzu könnte ein HMI das Modbus-TCP-Protokoll verwenden, um mit einer SPS zu kommunizieren.

Die Tofino SA ist mit einem vollständigen Satz vordefinierter Protokolle ausgestattet. In besonderen Fällen kann es jedoch erforderlich sein, neue Protokolle für besondere Gerätetypen oder Situationen zu erstellen.

Mit den Funktionen der Protokollverwaltung können Sie Protokolle erstellen, editieren und löschen. Der ConneXium Tofino Configurator wird mit einer Anzahl vordefinierter Protokolle ausgeliefert, die in vielen industriellen Systemen gebräuchlich sind. Diese werkseitig voreingestellten Protokolle können Sie weder ausschneiden noch löschen.



Wenn Sie in der Projekt-Explorer-Ansicht ein bestimmtes Protokoll auswählen, haben Sie folgende Möglichkeiten:

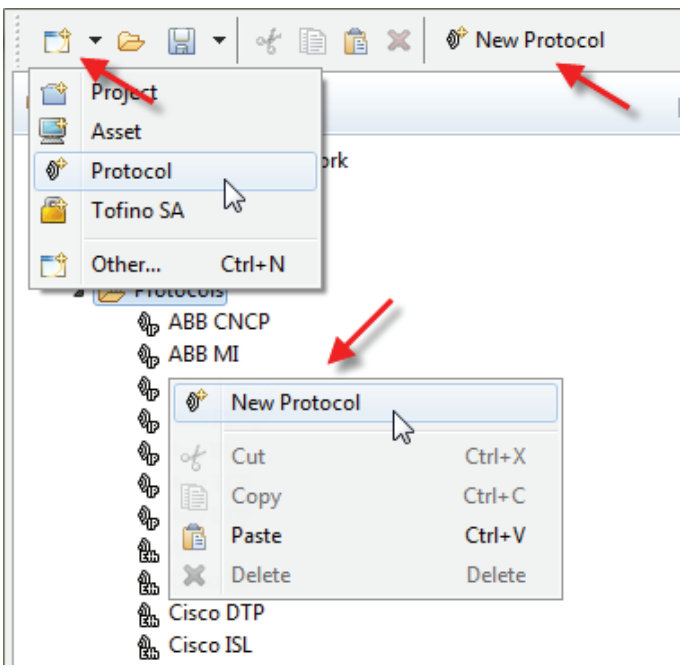
- Ein neues Protokoll oder einen neuen Ordner erzeugen.
- Die Einzelheiten des Protokolls aufrufen und editieren.
- Ein Protokoll löschen.
- Protokolle ausschneiden, kopieren und einfügen.

Einige Protokolle sind werkseitig voreingestellt. Sie haben keine Möglichkeit, diese zu bearbeiten, auszuschneiden oder zu löschen.

10.1 Ein Protokoll erzeugen

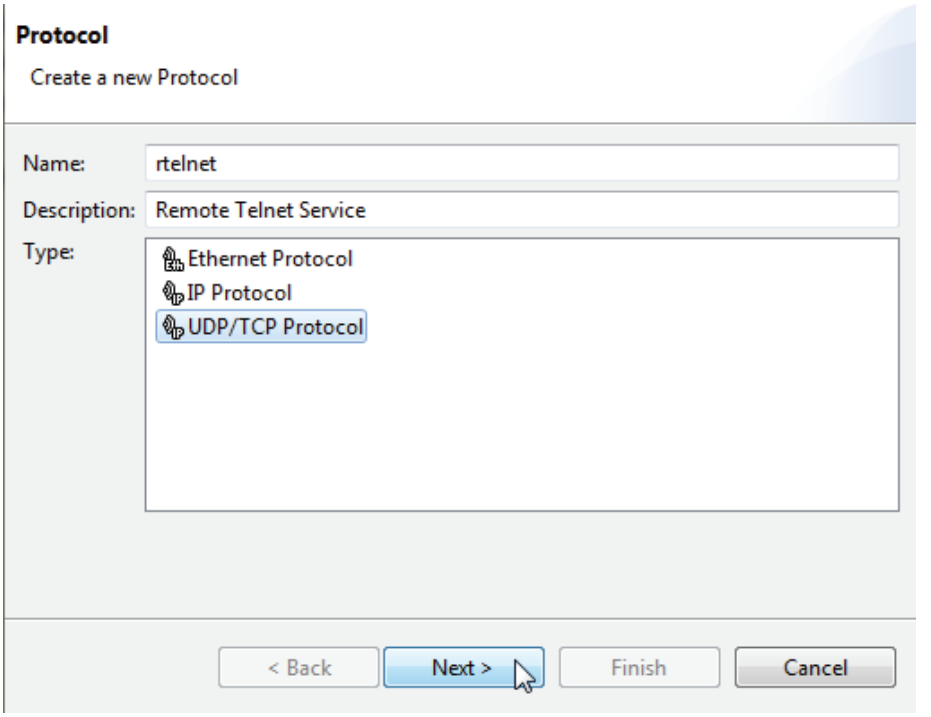
Sie erzeugen neue Protokolle mit Hilfe des Assistenten „Neues Protokoll“ (New Protocol). Dabei stehen Ihnen drei Möglichkeiten zur Verfügung, um den Assistenten „Neues Protokoll“ aufzurufen.

- Klicken Sie auf die Schaltfläche `Neu (New)` und wählen Sie `Protokoll (Protocol)` aus.
- Klicken Sie im mittleren Bereich der Werkzeugleiste auf die Schaltfläche `Neues Protokoll (New Protocol)`.
- Führen Sie einen Rechtsklick auf ein bestehendes Protokoll aus und wählen Sie `Neues Protokoll (New Protocol)`.

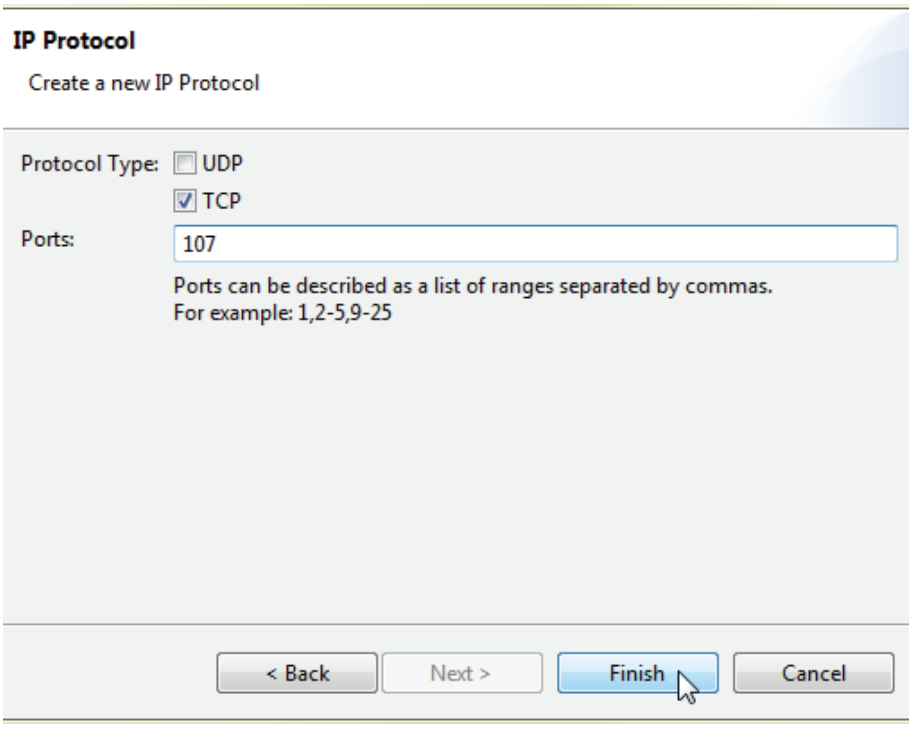


Assistent „Neues Protokoll“

Wenn Sie den Assistenten aufrufen, fordert Sie der Assistent auf, einen Namen und eine Beschreibung einzugeben und den Protokolltyp auszuwählen.



Auf der zweiten Seite des Assistenten haben Sie die Möglichkeit, spezifische Einzelheiten für das Protokoll einzugeben. Die auf dieser Seite angezeigten Details hängen von dem auf der ersten Seite ausgewählten Protokolltyp ab.

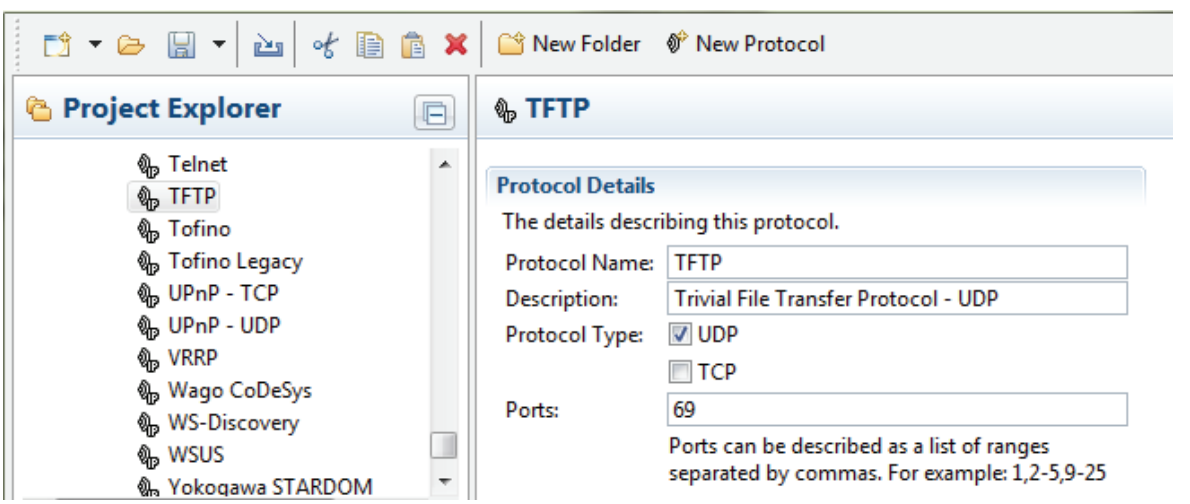


Weitere Informationen zu diesen Feldern finden Sie unter „Ein Protokoll anzeigen und editieren“.

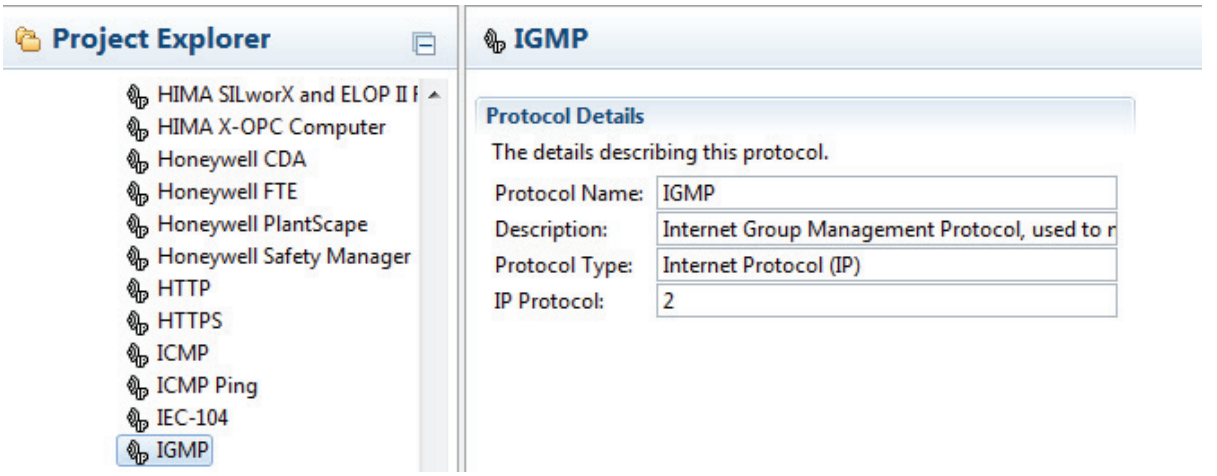
10.2 Ein Protokoll anzeigen und editieren

Wenn Sie in der Projekt-Explorer-Ansicht auf den Namen eines Protokolls klicken, öffnet sich das Menüfenster mit den Details zum Protokoll (Protocol Details). In diesem Menüfenster können Sie die Einstellungen für das ausgewählte Protokoll ansehen und konfigurieren. Hierzu gehören allgemeine Informationen und einzelne Parameter. Die Details hängen von dem ausgewählten Protokolltyp ab. Nachstehend sehen Sie drei typische Protokolle unterschiedlichen Typs.

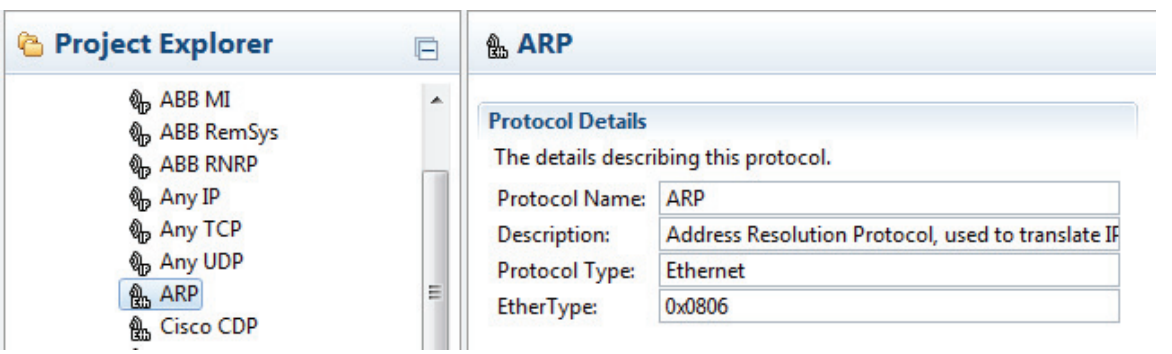
UDP/TCP-Protokoll



IP-Protokoll



Ethernet-Protokoll



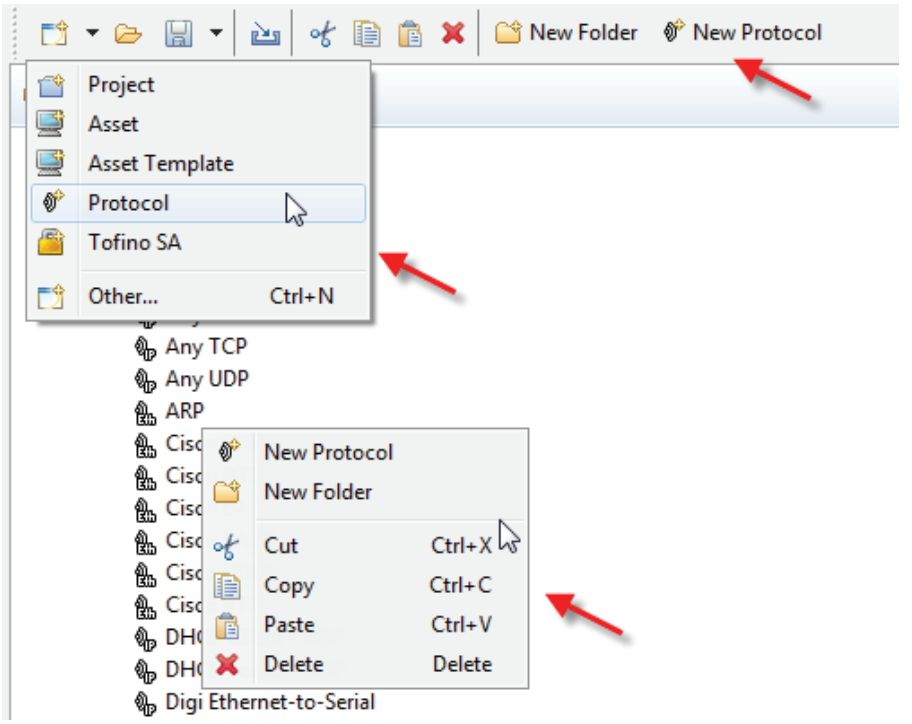
Allgemeines

- Protokollname (Protocol Name): Geben Sie hier eine eindeutige Bezeichnung bzw. Kennung für das Protokoll ein. Denken Sie daran, jedes Protokoll eindeutig zu bezeichnen, um etwaige Verwechslungen möglichst auszuschließen.
- Beschreibung (Description): Dieses Textfeld dient zur Referenz. Sie können hier die Funktion dieses Protokolls beschreiben.
- Protokolltyp (Protocol Type): Hier legen Sie die allgemeine Klassifizierung des Protokolls und die zugehörigen Eingabefelder fest. (UDP, TCP, IP oder Ethernet).
- Ports: Trennen Sie bei der Eingabe einzelne Port-Nummern durch Kommas und kennzeichnen Sie Bereiche von Port-Nummern durch Bindestriche. Wenn das Protokoll z. B. die TCP-Ports 5000 bis 5004 verwendet, können Sie diese entweder in der Form <5000, 5001, 5002, 5003, 5004> oder als <5000-5004> eingeben. Verwenden Sie hierzu ausschließlich die Zahlen 0 bis 9, Kommas und Bindestriche.
- IP-Protokoll (IP Protocol): Die Nummer des IP-Protokolls (im Hexadezimalformat).
- Typfeld (EtherType): Die Nummer des Typfeldes (im Hexadezimalformat). Weitere Informationen finden Sie unter http://www.iana.org/assignments/ethernet-numbers überwachen/ignorieren.

10.3 Protokolle verwalten

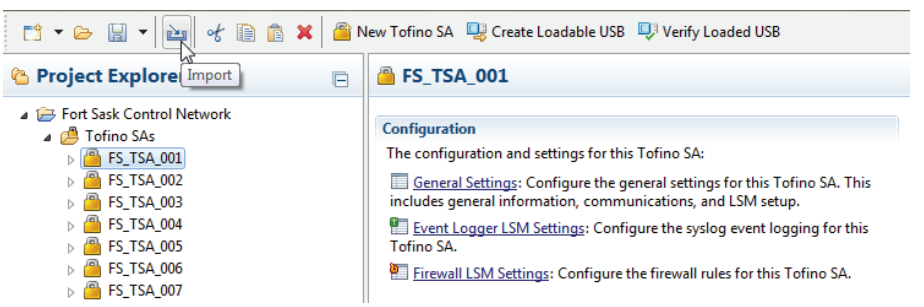
Sie können ein Protokoll wie ein normales Windows-Objekt verwalten. Wenn Sie ein Protokoll mit der rechten Maustaste anklicken oder alternativ die Werkzeugleiste verwenden, haben Sie folgende Möglichkeiten:

- Neues Protokoll (New Protocol) - ruft den Assistenten „Neues Protokoll“ auf.
- Neuen Ordner erzeugen (Create New Folder) - erzeugt einen neuen Ordner für die Organisation Ihrer Protokolle.
- Ausschneiden (Cut) - Entfernt das markierte Protokoll aus dem Projekt und speichert es in die Zwischenablage. Sie können es dann an einem anderen Speicherort wieder einfügen.
- Kopieren (Copy) - Erzeugt eine Kopie des markierten Protokolls des Projektes und speichert sie in die Zwischenablage. Sie können sie dann an einem anderen Speicherort wieder einfügen.
- Einfügen (Paste) - Fügt den Inhalt der Zwischenablage in das Projekt ein.
- Löschen (Delete) - Entfernt das markierte Protokoll aus dem Projekt. Beachten Sie, dass Sie bestimmte vordefinierte Protokolle ausschließlich lesen können. Sie haben keine Möglichkeit, diese zu verschieben oder zu löschen.


New Folder
New Protocol
Project
Asset
Asset Template
Protocol
Tofino SA
Other... Ctrl+N
Any TCP
Any UDP
ARP
New Protocol
New Folder
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Delete Delete
Digi Ethernet-to-Serial

11 Weiterführender Themenbereich - Vorlagen und Sicherheitsprofile importieren

Der ConneXium Tofino Configurator ermöglicht Ihnen den Import vordefinierter Objekte, die Sie als Bausteine für Ihr Sicherheitskonzept verwenden können. Sie können folgende Objekttypen importieren:



- Ressourcenvorlagen
- Protokolle
- Sonderregeln
- Sicherheitsprofile

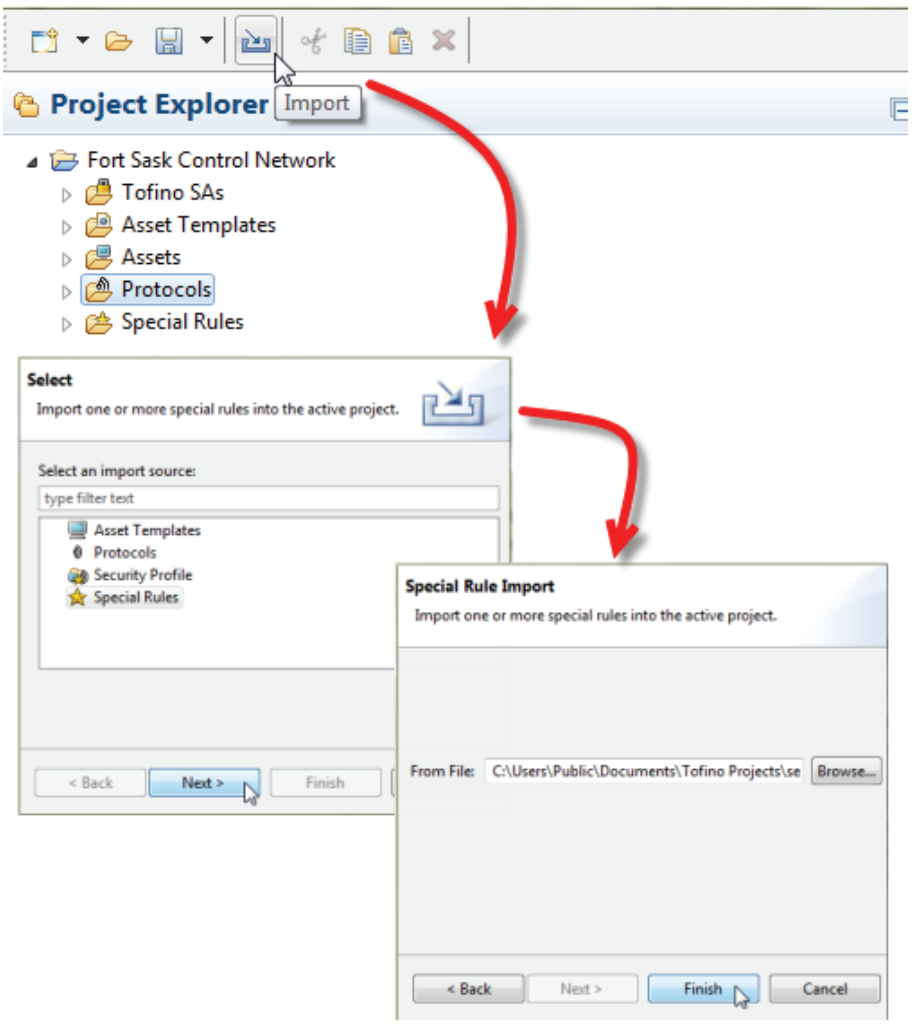
Über den Import von Ressourcenvorlagen, Protokollen oder Sonderregeln können Sie bestehende Definitionen aktualisieren oder Ihrem Projekt neue Definitionen hinzufügen. Wenn Sie neue Versionen von Ressourcenvorlagen, Protokollen oder Sonderregeln importieren, findet keine automatische Aktualisierung der Regeln Ihrer Firewall statt.

Bei Sicherheitsprofilen handelt es sich um vordefinierte Kombinationen aus Ressourcenvorlagen, Sonderregeln und Protokolldefinitionen, die zu einer einzelnen Sicherheitsprofil-Datei (im Format .tsp) zusammengefasst sind. Diese ermöglichen es Ihnen, zugehörige Objekte, welche Sie zum Schutz von speicherprogrammierbaren Steuerungen (SPS), verteilten Prozessleitsystemen (DCS) oder sonstigen Geräten vor veröffentlichten Sicherheitslücken benötigen, in Form einer einzigen Datei zu importieren.

Hinweis: Wenn die Ressourcenvorlagen oder Sicherheitsprofile in einer zu importierenden Datei auf Protokolle oder Sonderregeln verweisen, werden letztere während des Importvorgangs mit importiert.

Um ein vordefiniertes Objekt zu importieren, führen Sie die folgenden Schritte aus:

☐ Klicken Sie auf die Schaltfläche `Import`.
☐ Wählen Sie den zu importierenden Objekttyp aus.
☐ Wählen Sie die betreffende Objektdatei aus.
☐ Klicken Sie auf `Fertig stellen (Finish)`.


Project Explorer
Import
Fort Sask Control Network
Tofino SAs
Asset Templates
Assets
Protocols
Special Rules
Select
Import one or more special rules into the active project.
Select an import source:
type filter text
Asset Templates
Protocols
Security Profile
Special Rules
< Back
Next >
Finish
Special Rule Import
Import one or more special rules into the active project.
From File:
C:\Users\Public\Documents\Tofino Projects\se
Browse...
< Back
Next >
Finish
Cancel

12 Weiterführender Themenbereich - Einstellungen des ConneXium Tofino Configurators

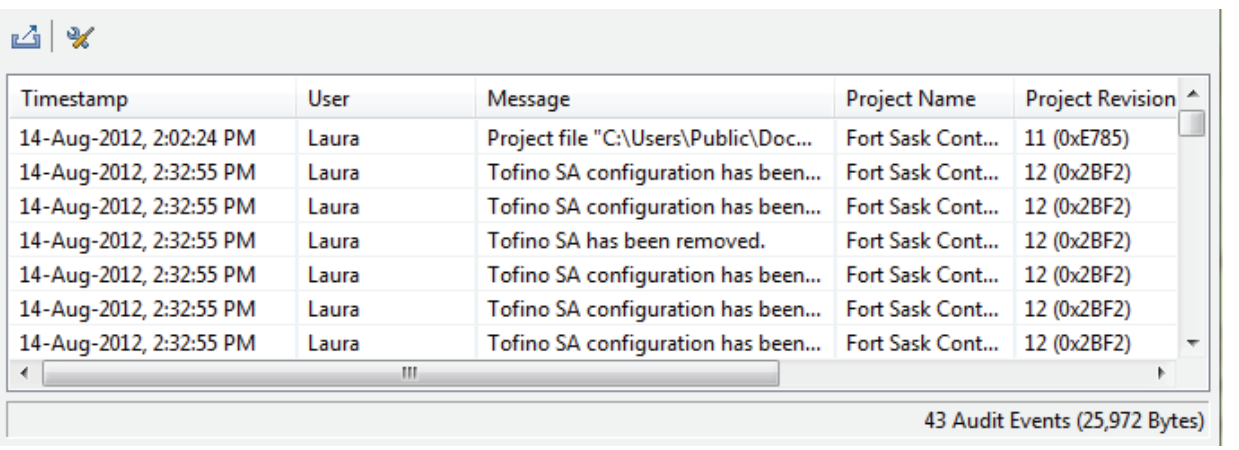
Mit Hilfe der nachstehend aufgeführten, erweiterten Einstellungen können Sie Anpassungen am ConneXium Tofino Configurator vornehmen:

- ☐ Informationen zum Konfigurieren von Prüfeinstellungen und Projekteinstellungen finden Sie unter „Einstellungen“.
- ☐ Informationen zum Festlegen von Benutzerverwaltungsrechten finden Sie unter „Benutzerverwaltung“.

12.1 Benutzerverwaltung

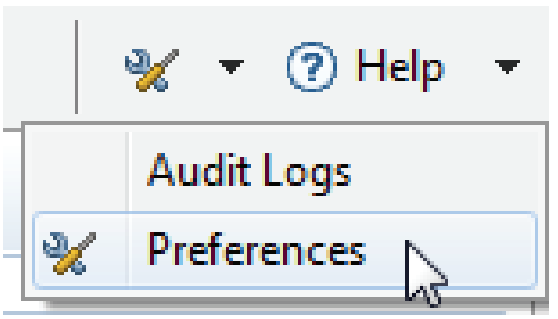
Die Benutzeridentifikation und die Verwaltung für den ConneXium Tofino Configurator ist an die Kontoverwaltung von Windows angelehnt. Wenn Sie Änderungen an einem Projekt vornehmen, wird für alle durchgeführten Aktionen mit dem ConneXium Tofino Configurator der jeweils aktive Windows-Benutzername aufgezeichnet. Der ConneXium Tofino Configurator zeichnet diesen Benutzernamen und die von ihm durchgeführten Änderungen am Projekt in den Prüfprotokollen auf.

Die Benutzerzugriffssteuerung für ein ConneXium Tofino Configurator-Projekt ist ähnlich gelagert: Sie basiert auf den Sicherheitseinstellungen der Windows-Dateiverwaltung für die jeweilige Projektdatei. Wenn eine Person beispielsweise ausschließlich lesenden Zugriff auf den Ordner hat, der die Projektdatei enthält, gewährt der ConneXium Tofino Configurator dieser Person ebenfalls ausschließlich einen Lesezugriff auf Projektaufgaben. Diese Einstellungen gehen über die grundlegende Dateiverwaltung hinaus. Sie können hiermit z. B. unterbinden, dass ein nicht autorisierter Benutzer eine USB-Konfiguration in die Tofino SA lädt.



12.2 Einstellungen

Mit dem Befehl „Einstellungen“ (Preferences) können Sie Einstellungen aufrufen und editieren, die keinem bestimmten Projekt zugeordnet sind.



- Prüfung (Audit) - Speicherort und Größe der Prüfdatei.
- Projekt (Project) - Hiermit legen Sie das bei Programmaufruf geöffnete Standardprojekt fest.

Einstellungen für Prüfung (Audit Preferences)

Auf dieser Seite des Menüs „Einstellungen“ (Preferences) können Sie den Speicherort und die maximale Größe der Prüfdatei einstellen.

Hilfe

Auf dieser Seite des Menüs „Einstellungen“ (Preferences) können Sie auswählen, auf welche Art und Weise die Hilfe zum ConneXium Tofino Configurator auf Ihrem Rechner angezeigt wird. So können Sie festlegen, ob die Hilfe in einem Fenster des ConneXium Tofino Configurators oder in einem externen Browser dargestellt wird.

Projekteinstellungen

In diesem Abschnitt des Menüs „Einstellungen“ (Preferences) können Sie das Standardprojekt konfigurieren, das beim Programmaufruf geöffnet wird.

13 Fehlersuche

13.1 Diagnosefunktionen der Tofino SA

Eine Tofino SA bietet Ihnen die Möglichkeit, Diagnosedateien zu Zwecken der Fehlersuche und -behebung auf ein USB-Speichermedium zu speichern. Zum Erzeugen dieser Dateien benötigen Sie eine Speicherung via USB. Sie können diese Dateien auch mit einem normalen Texteditor betrachten oder sie zur Analyse an den technischen Support senden.

Zum Erzeugen dieser Dateien benötigen Sie eine Speicherung via USB.

- ☐ Schalten Sie die Tofino SA an und warten Sie mindestens eine Minute.
- ☐ Schließen Sie das USB-Speichermedium an einen der USB-Ports des Gerätes an.
- ☐ Klicken Sie einmal auf die Schaltfläche „Speichern/Laden/Reset (Save Load Reset)“.
- ☐ Die Anzeige 1/S leuchtet auf.
- ☐ Nach einigen Sekunden läuft eine Blink-Sequenz von links nach rechts und zeigt einen laufenden USB-Speichervorgang an.
- ☐ Entfernen Sie das USB-Speichermedium, wenn die Blink-Sequenz beendet ist.
- ☐ Bei erfolgreicher Speicherung kehren die LEDs der Tofino SA wieder in den Status zurück, den sie vor dem Speichervorgang hatten.
- ☐ Schicken Sie Kopien dieser Dateien zur Analyse an den technischen Support.

Hinweis: Erfahrungsgemäß funktionieren folgende USB 2.0-Speichermedien-Fabrikate: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar sowie Schneider TCSEAM0100. Andere Fabrikate und Modelle funktionieren möglicherweise, wurden jedoch nicht getestet.

Diagnosedateien auswerten

Bei erfolgreicher Speicherung der Diagnosedaten finden sich drei oder vier Dateien auf dem USB-Speichermedium, die wie folgt oder ähnlich bezeichnet sind:[1]

- **<tofino id>_tc_data**: „USB-Überprüfung“ Daten der, die anzeigen, ob die Konfiguration erfolgreich oder fehlerhaft war.
- **<tofino id>_diagnostics.txt:** Diagnosedaten zur Tofino SA..
- **<tofino id>_evt.log sowie <tofino id>_evt.<X>.gz:** Ereignisprotokolle der Tofino SA (siehe „Konfigurieren von Ereignisprotokollen“).
- **<tofino id>_kernel_evt.enc:** Verschlüsselte Informationen zur Diagnose des Kernels (ausschließlich zur werkseitigen Fehlersuche und -behebung).
- **<tofino id>_diagnostics.enc:** Verschlüsselte Informationen zur Diagnose des Moduls (ausschließlich zur werkseitigen Fehlersuche und -behebung).

Wenn Sie die auf .txt endende Datei mit einem normalen Texteditor wie WordPad untersuchen, sollten Sie in etwa folgenden Inhalt vorfinden:

```
==================================================================
2  Tofino Version information:
3    Tofino Firmware version: Tofino Linux: 1.7.0
4  Tofino Hardware Info:
5    Hardware : Schneider ConneXium Development Platform
6    Processor : XScale-IXP42x Family rev 2 (v5b)
7    Flash Type: P-Flash
8    Tofino ID:  00:80:63:73:77:649
==================================================================
10  Network Statistics
11    unsecured IF ifconfig
12  eth0      Link encap:Ethernet  HWaddr 00:80:63:73:77:64
13          inet6 addr: fe80::280:66ff:fe04:652c/64 Scope:Link
14          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
15          RX packets:2776 errors:0 dropped:0 overruns:0 frame:0
16          TX packets:3900 errors:0 dropped:0 overruns:0 carrier:0
17          collisions:0 txqueuelen:100
18         RX bytes:419084 (409.2 KiB)  TX bytes:586268 (572.5 KiB)
19
20    secured IF ifconfig
21  eth1      Link encap:Ethernet  HWaddr 00:80:63:73:77:65
22          inet6 addr: fe80::280:66ff:fe04:652d/64 Scope:Link
23          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
24          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
```

1. Das Präfix des Dateinamens entspricht der Tofino-ID.

```
25          TX packets:716 errors:0 dropped:0 overruns:0 carrier:0
26          collisions:0 txqueuelen:100
27          RX bytes:846 (846.0 B)  TX bytes:95002 (92.7 KiB)
28
29    unsecured IF Settings
30  Basic registers of MII PHY #0:  1000 782d 0013 7a11 01e1 45e1
0005 6001.
31 The autonegotiated capability is 01e0.
32 The autonegotiated media type is 100baseTx-FD.
33 Basic mode control register 0x1000: Auto-negotiation enabled.
34 You have link beat, and everything is working OK.
35 Your link partner advertised 45e1: Flow-control 100baseTx-FD
100baseTx 10baseT-FD 10baseT, w/ 802.3X flow control.
36   End of basic transceiver information.
37
38     secured IF Settings
39 Basic registers of MII PHY #1:  1000 782d 0013 7a11 01e1 45e1 0005
6001.
40 The autonegotiated capability is 01e0.
41 The autonegotiated media type is 100baseTx-FD.
42 Basic mode control register 0x1000: Auto-negotiation enabled.
43 You have link beat, and everything is working OK.
44 Your link partner advertised 45e1: Flow-control 100baseTx-FD
100baseTx 10baseT-FD 10baseT, w/ 802.3X flow control.
45   End of basic transceiver information.
46
47
=================================================================
48 Memory
49           total       used       free     shared    buffers     cached
50 Mem:         62952      17952      45000          0        140       9060
51 -/+ buffers/cache:        8752      54200
52 Swap:             0          0          0
53-----------------------------------------------------------------
54 MemTotal:         62952 kB
55 MemFree:          44992 kB
56 Buffers:            140 kB
57 Cached:            9060 kB
58 SwapCached:           0 kB
59 Active:            9288 kB
60 Inactive:          1996 kB
61 SwapTotal:            0 kB
62 SwapFree:             0 kB
63 Dirty:                0 kB
64 Writeback:            0 kB
65 AnonPages:         2100 kB
66 Mapped:            1744 kB
67 Slab:              3176 kB
68 SReclaimable:       752 kB
69 SUnreclaim:        2424 kB
70 PageTables:         260 kB
71 NFS_Unstable:         0 kB
72 Bounce:               0 kB
```

```
73 WritebackTmp:         0 kB
74 CommitLimit:      31476 kB
75 Committed_AS:      5200 kB
76 VmallocTotal:    958464 kB
77 VmallocUsed:      33436 kB
78 VmallocChunk:    917500 kB
79
================================================================
80 Flash
81 Filesystem                Size      Used Available Use% Mounted on
82 rootfs                    31.5M       8.1M     23.4M  26% /
83
================================================================
```

Die auf .enc endenden Dateien sind verschlüsselt. Sie sollten diese an den technischen Produkt-Support senden.

Bei den auf .evt.log sowie <tofino id>_evt.<X>.gz endenden Dateien handelt es sich um vom LSM „Event Logger“ erzeugte Protokolldateien. Sie können diese mit jeder Software für Ereignisprotokolle öffnen und anschauen (siehe „Konfigurieren von Ereignisprotokollen“).

13.2 Firewall blockiert keinen Verkehr

Wenn das LSM „Tofino Firewall“ den spezifizierten Datenverkehr nicht wie geplant blockiert, prüfen Sie zunächst folgende Details:

- Den Status des LSMs „Tofino Firewall“: Ist das LSM aktiviert (siehe „Allgemeine Einstellungen einer Tofino SA“?
- Den Modus der Tofino SA. Ist die Tofino SA betriebsbereit? Die Status-LED der Tofino SA sollte dauerhaft leuchten.
- Entspricht die Konfiguration der Tofino SA TATSÄCHLICH dem, was im ConneXium Tofino Configurator gespeichert ist? Falls Sie diesbezüglich Zweifel haben, überprüfen Sie dies mit der Funktion „USB-Konfiguration prüfen“ (siehe „USB-Überprüfung“).

Überprüfen Sie anschließend die Regeln im Menüfenster „Firewall“ der Tofino SA auf folgende Fragestellungen hin (siehe „Firewall-Regeln verwalten“):

- Sind die IP-Adressen des Gerätes korrekt?
- Stimmen die Protokolle und die Übertragungsrichtung?
- Gibt es widersprüchliche Regeln? Haben Sie der Tofino SA beispielsweise zugleich eine Regel „Alle zulassen“ und eine protokollspezifische Regel zugeordnet?
- Haben Sie die Geräteverbindung hergestellt, BEVOR Sie die Regel geladen haben? Die Tofino SA unterbricht keine bestehende Verbindung zwischen zwei Geräten. Falls Sie davon ausgehen, dass die Verbindung bereits vor dem Laden der Regel bestand, versuchen Sie die Verbindung zu unterbrechen, indem Sie eines der Geräte neu starten.

13.3 Empfehlungen zu USB-Speichermedien

Sofern bei Ihnen Schwierigkeiten auftreten, wenn Sie über USB laden bzw. speichern, überprüfen Sie zunächst, ob Sie ein Speichermedium verwenden, das kompatibel zu USB 2.0 ist. Die Tofino SA funktioniert nicht mit Speichermedien, die lediglich zu USB 1.1 kompatibel sind. Die Fehler-LED der Tofino SA leuchtet zweimal auf, wenn das Gerät ein unzulässiges USB 1.1-Speichermedium erkennt.

Die getestet und freigegebenen USB-Speichermedien sind: Kingston Data Traveler, SanDisk Cruzer, Sony Microvault, Lexar, Schneider TCSEAM0100.

Anzahl Blinkzeichen	Während des Ladens	Während des Speicherns
2	Entweder ist kein USB-Speichermedium angeschlossen oder das Dateisystem des Speichermediums ist nicht mit FAT16 oder FAT32 formatiert.	Das Dateisystem des Speichermediums ist nicht mit FAT16 oder FAT32 formatiert.
3	Die Dateien auf dem USB-Speichermedium sind ungültig.	Das Gerät konnte keine Diagnosedateien laden. Bitte wenden Sie sich an den für Sie zuständigen technischen Support.
4	Das Gerät konnte die Konfigurationsdateien nicht verschlüsseln. Möglicherweise wurden die Dateien während des Kopiervorgangs beschädigt. Wiederholen Sie den Kopiervorgang. Wenn der Fehler weiter besteht, wenden Sie sich an den für Sie zuständigen technischen Support.	Das Gerät konnte die Diagnosedateien nicht verschlüsseln. Bitte wenden Sie sich an den für Sie zuständigen technischen Support.
5	Das Gerät konnte die Dateien nicht laden. Möglicherweise wurden die Dateien während des Kopiervorgangs beschädigt. Wiederholen Sie den Kopiervorgang. Wenn der Fehler weiter besteht, wenden Sie sich an den für Sie zuständigen technischen Support.	Das Gerät konnte die verschlüsselten Diagnosedateien nicht auf das USB-Speichermedium kopieren. Möglicherweise ist das Speichermedium voll.
6	Das Gerät konnte die USB-Verbindung nicht deaktivieren. Bitte wenden Sie sich an den für Sie zuständigen technischen Support.	Das Gerät konnte die USB-Verbindung nicht deaktivieren. Bitte wenden Sie sich an den für Sie zuständigen technischen Support.
7		Das Dateisystem des Gerätes verfügt über keine ausreichende Speicherkapazität, um die Dateien vor dem Kopieren auf das USB-Speichermedium zwischenzuspeichern. Bitte wenden Sie sich an den für Sie zuständigen technischen Support.

Tab. 2: Aktivität der Fehler-LED beim Laden und Speichern

13.4 Zurücksetzen Ihrer Tofino SA auf die Werkseinstellungen

Sie können die Tofino SA anhand der folgenden Schritte auf den werksseitigen Lieferzustand zurückzusetzen:

- ☐ Stellen Sie sicher, dass die Tofino SA eingeschaltet und die Einschaltinitialisierung abgeschlossen ist.
- ☐ Betätigen Sie die Taste „Speichern/Laden/Reset (Save Load Reset)“ und lassen Sie sie anschließend wieder los. Führen Sie dies insgesamt dreimal durch, bis die drei LEDs aufleuchten. Bei der ersten Betätigung leuchtet die Anzeige „1/S“ auf, bei der zweiten die Anzeige „ 2/L“ und bei der dritten die Anzeige „V.24/R“.
- ☐ Nach einigen Sekunden beginnt die Tofino SA mit dem Zurücksetzen auf die Werkseinstellungen. Während des Zurücksetzens blinken die Anzeigen „1/S“, „2/L“, „V.24/R“, „Mode“ sowie „Fault“ gleichzeitig.

Wenn das Zurücksetzen abgeschlossen ist, erlöschen die Anzeigen „1/S“, „2/L“, „V.24/R“, „Mode“ und „Fault“ wieder. Dieses LED-Muster liefert die Bestätigung, dass dieTofino SA passiv ist und den Datenverkehr ohne Filterung durchlässt. Wenn die Anzeige „Mode“ aufleuchtet, wiederholen Sie die Schritte 1 bis 3. Wenn die LEDs sich anders verhalten als oben geschildert, wenden Sie sich an den technischen Support.

14 Glossar

ACL	Access Control List (Zugangskontrollliste): Eine Liste mit Regeln, welche die Zugriffsberechtigungen zu Netzressourcen festlegt
ARG	Assisted Rule Generation (Unterstützte Erzeugung von Regeln): Diese Funktion unterstützt Sie beim Erstellen von Firewall-Regeln, damit Sie Geräte innerhalb des Netzes schützen können. Die entsprechende Funktion ist Bestandteil des LSMs „Secure Asset Management“.
Children	Die auch als „Kinder“ (Children) bezeichneten Kindknoten sind Netzknoten, die sich in einem Netzbaum unterhalb der „Eltern“ bzw. Elternknoten befinden.
CIP	Common Industrial Protocol: Bei CIP handelt es sich um einen offenen Standard für industrielle Netztechnologien. Er wird von der ODVA, der „Open DeviceNet Vendor Association“, gepflegt und weiterentwickelt.
CSP	Client-Server-Protokoll: Ein Protokoll des Unternehmens Allen-Bradley, das für die Kommunikation mit speicherprogrammierbaren Steuerungen über TCP/IP eingesetzt wird.
DCOM	Distributed Component Object Model (Objektmodell für die Verteilung von Software-Komponenten): Hierbei handelt es sich um eine Erweiterung des von Microsoft entwickelten „Component Object Model (COM)“, welches die Kommunikation zwischen Objekten auf unterschiedlichen Rechnern eines Netzes unterstützt.
DCS	Distributed Control System (verteiltes Prozessleitsystem): Ein verteiltes Prozessleitsystem ermöglicht die entfernte Überwachung und Steuerung von Feldgeräten von einzelnen oder mehreren Betriebsstationen aus.
DMZ	Demilitarized Zone (entmilitarisierte Zone): Ein kleines Netz, das als „neutrale Zone“ zwischen einem vertrauenswürdigen privaten Netz und einem externen, nicht vertrauenswürdigen Netz eingefügt wird.
DNP3	Distributed Network Protocol 3 (Protokoll für verteilte Netze): Ein Protokoll, das zwischen Komponenten in Prozessautomatisierungssystemen verwendet wird
DNS	Domain Name System (Domänennamensystem): Ein verteiltes Datenbanksystem, um für Menschen lesbare Namen in Internet-Protokoll-Adressen aufzulösen.
DPI	Deep Packet Inspection (umfassende Paketüberprüfung)
Firewall	Eine Zusammenstellung von Sicherheitsregelungen und -komponenten, mit denen der Zugriff von nicht autorisierten Personen oder Geräten auf geschützte Knoten eines Netzes unterbunden wird. Im Wesentlichen arbeitet eine Firewall als Kontrollpunkt, an dem unzulässige Verbindungen zu Knoten hinter der Firewall blockiert werden, während vertrauenswürdige Kommunikationsübertragungen ohne Beeinträchtigungen passieren dürfen.
FTP	File Transfer Protocol (Datenübertragungsprotokoll)
GUI	Graphical User Interface (grafische Benutzeroberfläche): Eine grafische Schnittstelle zum Computer (im Gegensatz zur textbasierten Schnittstelle)
HMI	Human Machine Interface (Mensch-Maschine-Schnittstelle): Diese Schnittstelle ermöglicht die Interaktion zwischen Mensch und Maschine.

HTML	Hypertext Markup Language (Hypertext-Auszeichnungssprache): Hierbei handelt es sich um die für das Internet verwendete Autorensprache zur Erstellung von Dokumenten.
HTTP	Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll): Das Protokoll, das für die Übertragung von Web-Dokumenten von einem Server zu einem Browser verwendet wird.
HTTPS	Hypertext Transfer Protocol over SSL: Ein Protokoll, mittels dessen Web-Dokumente verschlüsselt von einem Server zu einem Browser übertragen werden.
IDS	Intrusion Detection System (System zur Erkennung von Eindringversuchen): Hierbei handelt es sich um ein System, das verdächtige Muster im Netzverkehr aufspürt und meldet.
IP	Internet-Protokoll: Das Standardprotokoll des Internets. Es definiert das Format von Datagrammen und sichert eine bestimmte (minimale) Dienstgüte für die Auslieferung von Datenpaketen zu.
IT	Informationstechnik: Die Entwicklung, Installation und Implementierung von Rechnersystemen und Anwendungen.
LAN	Local Area Network (lokales Netz): Ein Netz, in dem Rechner innerhalb eines begrenzten Bereiches (Haus, Büro, Labor, Fabrik) miteinander verbunden sind.
LDAP	Lightweight Directory Access Protocol: Ein Protokoll für den Zugriff auf Verzeichnisdienste.
LSM	Ladbares Sicherheitsmodul: Hierbei handelt es sich um Software-Plug-ins, die Sicherheitsdienste wie eine Firewall, ein System zur Erkennung von Eindringversuchen (IDS) oder ein Diagnoseprogramm bereitstellen.
Modbus	Ein von der Fa. Modicon Incorporated entwickeltes Kommunikationsprotokoll zur Verwendung mit den firmenspezifischen SPS-Geräten.
MySQL	Eine relationale Datenbankverwaltung (RDBMS; relational database management system), die als Server fungiert und einen Mehrbenutzerzugang zu einzelnen oder mehreren Datenbanken bereitstellt.
NETBEUI	NetBIOS Extended User Interface: Eine erweiterte Version des NetBIOS-Protokolls.
NetBIOS	Network Basic Input Output System: Ein Quasi-Standard von IBM, den Anwendungen für die Kommunikation in einem lokalen Netz verwenden.
Asset	Bezeichnet die Objekte, welche die in Ihrem Leitsystem installierten Gerätschaften darstellen. Diese können in sieben Kategorien unterteilt werden: Rechner, Controller, Geräte, Netze, Netzvorrichtungen, Broadcast und Multicast.
OLE	Object Linking and Embedding (Objekt-Verknüpfung und -Einbettung): Dieser Vorläufer von COM ermöglicht es Anwendungen, Daten zu teilen und geteilte Daten zu manipulieren.
OPC	OLE for Process Control: Ein auf OLE, COM und DCOM basierender Standard, der den Zugriff auf Prozesssteuerungsdaten über Microsoft Windows-Systeme ermöglicht.
Parent	Ein Elternknoten ist ein übergeordneter Netzknoten, an den andere Knoten (sog. „Kinder“) angeschlossen sind.
PCN	Process Control Network (Prozesssteuerungsnetz): Ein Kommunikationsnetz, mit dem Befehle und Daten zur Steuerung von Geräten und sonstigen industriellen Vorrichtungen übertragen werden.

PLC	Programmable Logic Controller (speicherprogrammierbare Steuerung, SPS): Eine SPS ist ein kleiner, anwendungsspezifischer Rechner, der zur Steuerung bzw. Regelung von industriellen Anlagen oder Verfahren eingesetzt wird.
Protokoll	Ein Abkommen oder Standard, das bzw. der die Verbindung, die Kommunikation und den Datentransfer zwischen zwei Rechnern/Endgeräten steuert und ermöglicht. In seiner einfachsten Form kann ein Protokoll als eine Anzahl von Regeln definiert werden, welche die Syntax, die Wortbedeutung und die Synchronisation der Kommunikation bestimmen. Protokolle lassen sich mittels Hardware, Software oder einer Verbindung dieser implementieren. Auf der untersten Stufe definiert ein Protokoll das Verhalten einer Hardware-Verbindung.
RPC	Remote Procedure Call (Entfernter Prozeduraufruf): Ein Standard zum Aufrufen von Code auf einem externen Rechner innerhalb eines Netzes.
SA	Security Appliance (Sicherheitsvorrichtung): Eine industriell gehärtete Sicherheitsvorrichtung, die zur Installation vor (einzelnen bzw. einem Verbund von) schutzbedürftigen Mensch-Maschine-Schnittstellen (HMIs), verteilten Prozessleitsystem (DCS), speicherprogrammierbaren Steuerungen (SPS) oder Fernbedienungsterminals (RTUs) ausgelegt ist.
SCADA	Supervisory Control And Data Acquisition (Überwachung, Steuerung, Datenerfassung): Ein System zur industriellen Steuerung, das aus mehreren Fernbedienungsterminals (RTUs), einer Kommunikationsinfrastruktur sowie einem oder mehreren Steuerungsrechnern besteht.
SNMP	Simple Network Management Protocol (einfaches Netzverwaltungsprotokoll): Ein Protokoll zur Verwaltung von Geräten wie Router, Switche und Hosts.
SQL	Eine Computersprache für Datenbanken zur Verwaltung von Daten in relationalen Datenbankverwaltungen.
SSL	Secure Socket Layer: Ein von Netscape Incorporated entwickelter Quasi-Standard für verschlüsselte Kommunikation.
TCP	Transmission Control Protocol (Übertragungssteuerungsprotokoll): Ein Protokoll auf Transportebene, das einen verbindungsorientierten Dienst für Datenströme bereitstellt.
TFTP	Trivial File Transfer Protocol (einfaches Dateiübertragungsprotokoll)
Tofino Security Appliance	Eine industriell gehärtete Sicherheitsvorrichtung, die zur Installation vor (einzelnen bzw. einem Verbund von) schutzbedürftigen Mensch-Maschine-Schnittstellen (HMIs), verteilten Prozessleitsystem (DCS), speicherprogrammierbaren Steuerungen (SPS) oder Fernbedienungsterminals (RTUs) ausgelegt ist.
UDP	User Datagram Protocol: Ein verbindungsloses Protokoll für den Netztransport
URL:	Uniform Resource Locator (einheitlicher Quellenanzeiger): Die Adresse einer Quelle im Internet
XML	eXtensible Markup Language: Eine allgemeine Auszeichnungssprache zum Erstellen von Auszeichnungssprachen für besondere Zwecke, welche unterschiedlichste Datenarten beschreiben können.