SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M-800 Getting Started

Getting Started

06/2015

C79000-G8900-C337-04

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: C79000-G8900-C337
℗ 07/2015 Änderungen vorbehalten

Vorwort

Zweck

Anhand von Beispielen wird die Projektierung des SCALANCE M gezeigt.

IP-Einstellungen der Beispiele

Hinweis

Die in den Beispielen verwendeten IP-Einstellungen sind frei gewählt.

Im realen Netzverbund müssen Sie diese IP-Einstellungen der Netzwerkumgebung anpassen, um eventuelle Adresskonflikte zu vermeiden.

Allgemeine Benennung

Die Bezeichnung . . . steht für . . .	
SCT	Security Configuration Tool
PST	Primary Setup Tool
CP	CP 343-1 Advanced GX31, CP 443-1 Advanced GX30, CP 1628
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M874	SCALANCE M874-2 SCALANCE M874-3
M876	SCALANCE M876-3 SCALANCE M876-4
M812	SCALANCE M812-1
M816	SCALANCE M816-1
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2

Weiterführende Dokumentation

- Betriebsanleitung "Industrial Remote Communication Remote Networks - SCALANCE M874"

  Dieses Dokument umfasst Informationen, mit denen Sie in der Lage sind, ein Gerät der Produktlinie SCALANCE M874 zu montieren und anzuschließen. Die Konfiguration sowie die Einbindung des Geräts in ein Netzwerk ist nicht Gegenstand dieser Anleitung

- Betriebsanleitung "Industrial Remote Communication Remote Networks - SCALANCE M81x"

  Dieses Dokument umfasst Informationen, mit denen Sie in der Lage sind, ein Gerät der Produktlinie SCALANCE M812, M816 zu montieren und anzuschließen. Die Konfiguration sowie die Einbindung des Geräts in ein Netzwerk ist nicht Gegenstand dieser Anleitung

- Projektierungshandbuch "Industrial Remote Communication Remote Networks - SCALANCE M-800 Web Based Management"

  Dieses Dokument soll Sie in die Lage versetzen das Gerät in Betrieb zu nehmen und zu bedienen. Es vermittelt die notwendigen Kenntnisse über die Konfiguration der Geräte.

- Im Projektierungshandbuch "Industrial Ethernet Security – Grundlagen und Anwendung" erhalten Sie weitere Hinweise zum Arbeiten mit dem SCT (Security Configuration Tool). Sie finden dieses Dokument im Internet unter folgender Beitrags-ID: 56577508 (http://support.automation.siemens.com/WW/view/de/56577508)

- Im Handbuch "SIMATIC NET Industrial Ethernet Netzhandbuch" erhalten Sie Hinweise zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit den Geräten dieser Produktlinie in einem Industrial Ethernet Netzwerk betreiben können. Dort finden Sie u. a. optische Leistungsdaten der Kommunikationspartner, die Sie für den Aufbau benötigen.

  Sie finden dieses Dokument im Internet unter folgender Beitrags-ID: 27069465 (http://support.automation.siemens.com/WW/view/de/27069465)

SIMATIC NET-Handbücher

Die SIMATIC NET-Handbücher finden Sie auf den Internetseiten des Siemens Industry Online Support:

- über die Suchfunktion:

  Link zum Siemens Industry Online Support (http://support.automation.siemens.com/)

  Geben Sie die Beitrags-ID des jeweiligen Handbuchs als Suchbegriff ein.

- über die Navigation auf der linken Seite im Bereich "Industrielle Kommunikation":

  Link zum Bereich "Industrielle Kommunikation" (http://support.automation.siemens.com/WW/view/de/10805878/133400)

  Navigieren Sie zu der gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:
  Register "Beitragsliste", Beitragstyp "Handbücher / Betriebsanleitungen"

Security-Hinweise

Hinweis

Siemens bietet für sein Automatisierungs- und Antriebsproduktportfolio Security-Mechanismen, um einen sicheren Betrieb der Anlage/Maschine zu unterstützen. Unsere Produkte werden auch unter dem Gesichtspunkt Industrial Security ständig weiterentwickelt. Wir empfehlen Ihnen daher, dass Sie sich regelmäßig über Aktualisierungen und Updates unserer Produkte informieren und nur die jeweils aktuellen Versionen bei sich einsetzen. Informationen dazu finden Sie unter:
(http://support.automation.siemens.com)

Hier können Sie sich für einen produktspezifischen Newsletter registrieren.

Für den sicheren Betrieb einer Anlage/Maschine ist es darüber hinaus notwendig, die Automatisierungskomponenten in ein ganzheitliches Industrial Security-Konzept der gesamten Anlage/Maschine zu integrieren, das dem aktuellen Stand der Technik entspricht. Hinweise hierzu finden Sie unter:
(http://www.siemens.com/industrialsecurity)

Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen.

SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection oder Produkt-DVD

  Die DVD liegt einigen SIMATIC NET-Produkten bei.

- Im Internet unter folgender Beitrags-ID:

  50305045 (http://support.automation.siemens.com/WW/view/de/50305045)

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SCALANCE, SINEMA, CP 343-1, CP 443-1, CP 1628, KEY-PLUG, C-PLUG

Inhaltsverzeichnis

SCALANCE M-800 mit WAN verbinden

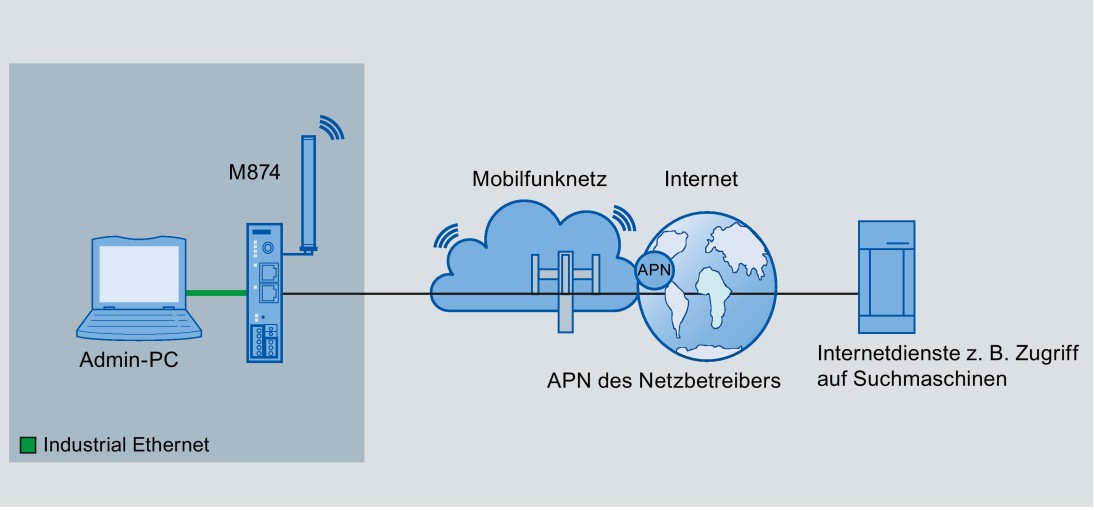
1

1.1 M874 mit dem Mobilfunknetz verbinden

1.1.1 Prinzipielles Vorgehen

In diesem Beispiel wird dem SCALANCE M874, das sich im Zustand der Werkseinstellungen befindet, eine IP-Adresse zugewiesen. Im Anschluss wird das Gerät über das Web Based Management (WBM) konfiguriert.

Aufbau



Erforderliche Geräte/Komponenten

- 1x M874 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
- 1x geeignete Antenne
- 1x SIM-Karte ihres Mobilfunkbetreibers (Die entsprechenden Dienste z. B. Internet sind freigeschaltet)
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmblockstecker
- 1x PC zum Konfigurieren des M874.
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Hinweis

Sie können auch ein SCALANCE M876 verwenden. Die nachfolgend beschriebene Projektierung bezieht sich explizit auf die im Abschnitt "Erforderliche Geräte/Komponenten" erwähnten Komponenten.

Projektierungsschritte

Zum Anbinden eines M874 an das Mobilfunknetz sind folgende Schritte erforderlich:

1. SCALANCE M874 und Netzwerk einrichten (Seite 13).
2. Das Web Based Management starten (Seite 13)
3. Am Web Based Management anmelden (Seite 16)
4. IP-Einstellungen des M874 ändern (Seite 17).
5. SCALANCE M874 konfigurieren.
   - Geräteinformationen festlegen (Seite 19)
   - Zugangsparameter konfigurieren (Seite 19)
   - Uhrzeit einstellen (Seite 22)
   - Zugriff erlauben.

1.1.2 SCALANCE M874 und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Vorgehensweise

1. Packen Sie zunächst das M874 aus und überprüfen Sie den unbeschädigten Zustand.
2. Setzen Sie die SIM-Karte ein.
3. Montieren Sie die Spannungsversorgung.

⚠ WARNUNG

Nur Sicherheitskleinspannung verwenden

Das Gerät SCALANCE M874 ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE M muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

4. Montieren Sie die Antenne.
5. Schließen Sie an einen der beiden Ethernet-Ports (P1, P2) den PC an.
6. Schalten Sie das Gerät an. Nachdem Anschließen leuchtet die Fehler-LED (F) gelb.
7. Schalten Sie jetzt den PC ein.

1.1.3 Das Web Based Management starten

Werkseitig ist das SCALANCE M-800 unter der folgenden IP-Adresse erreichbar:

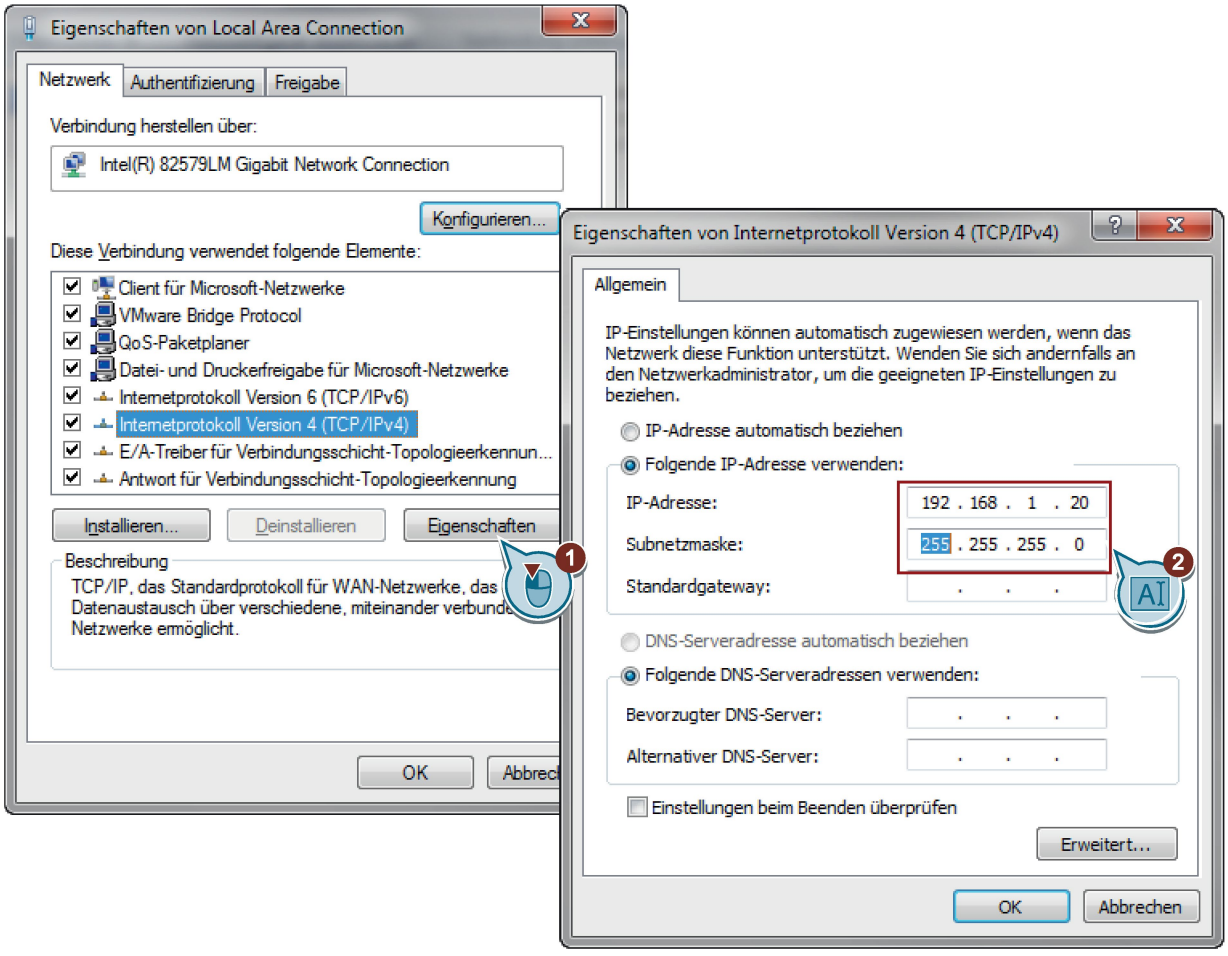
- IP-Adresse: 192.168.1.1
- Subnetzmaske: 255.255.255.0

Der Admin-PC erhält in dieser Beispielkonfiguration folgende IP-Adresseinstellung, um auf das Web Based Management des M-800 zu zugreifen.

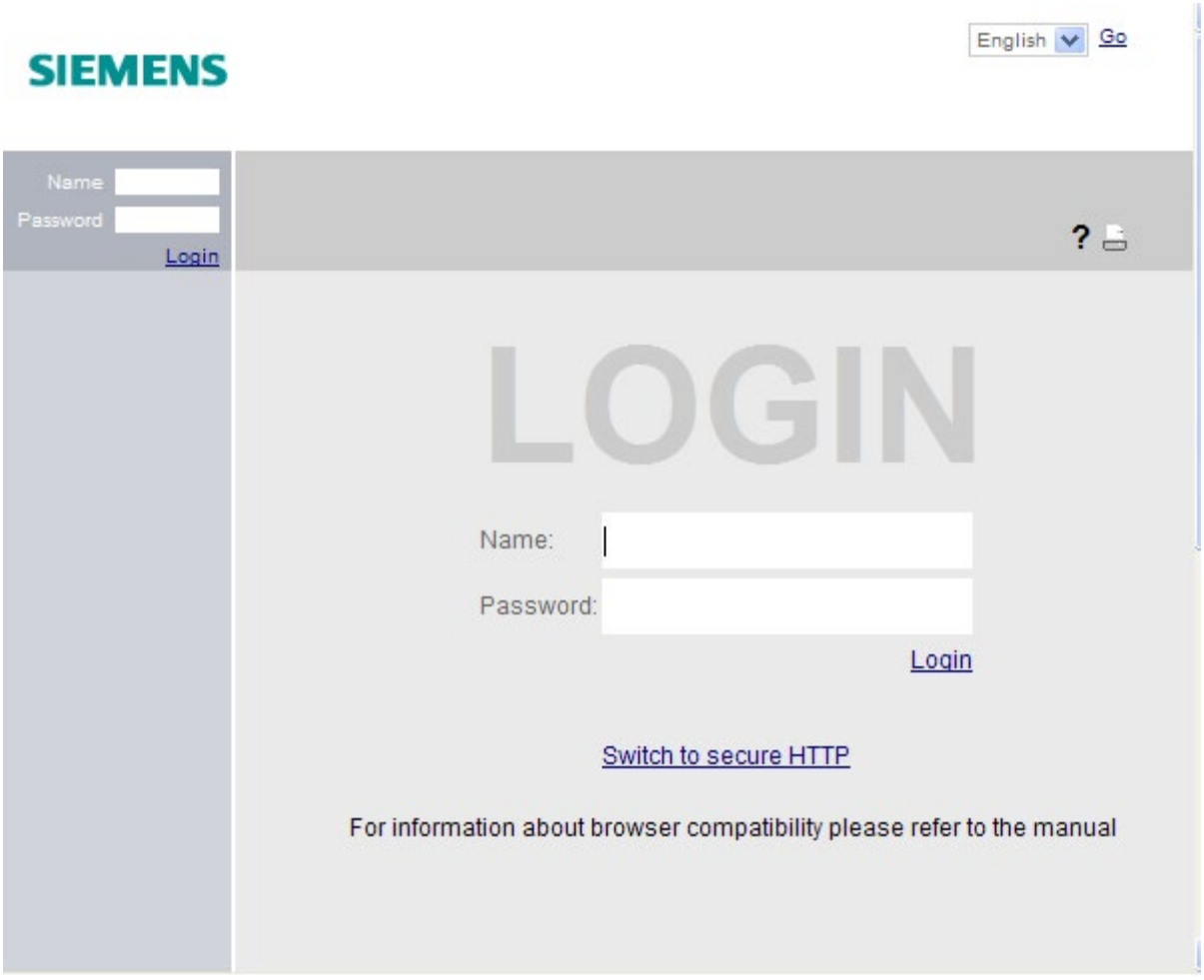
IP-Adresse	Subnetzmaske
192.168.1.20	255.255.255.0

Vorgehensweise

1. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Klicken Sie mit der rechten Maustaste auf das Symbol "LAN-Verbindung" und wählen Sie den Menübefehl "Eigenschaften".
4. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".
5. Geben Sie die dem Admin-PC zugeordneten Werte aus der Tabelle in die dafür vorgesehenen Felder ein.



6. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
7. Geben Sie im Adressfeld des Webbrowsers die IP-Adresse "192.168.1.1" ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

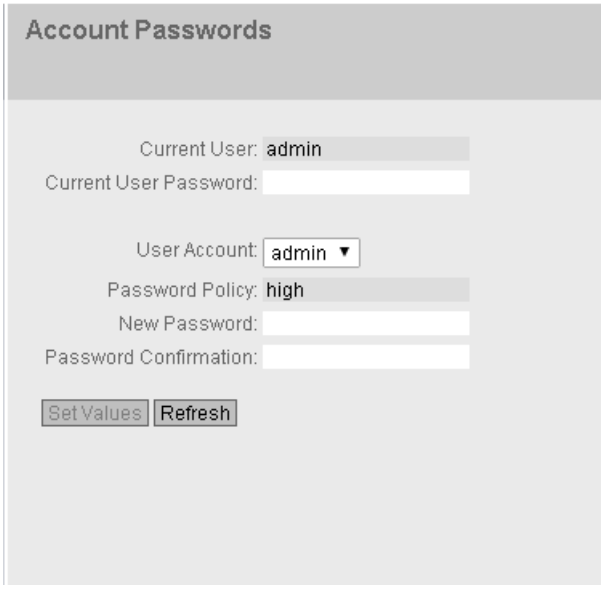


1.1.4 Am Web Based Management anmelden

Vorgehensweise

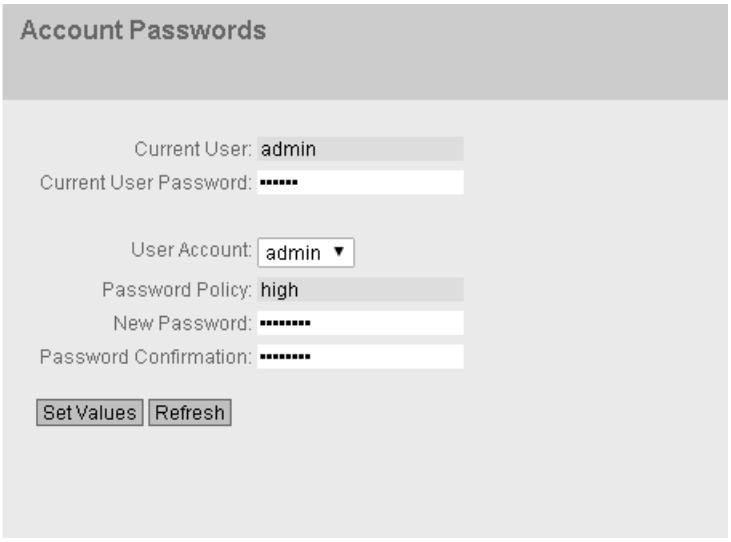
1. Melden Sie sich mit dem Benutzernamen "admin" und dem Passwort "admin" an. Sie werden aufgefordert, das Passwort zu ändern.

2. Bestätigen Sie den Dialog. Automatisch wird die WBM-Seite "Password" geöffnet.



3. Wählen Sie bei "Username" den Benutzer "admin" aus.
4. Tragen Sie bei "Current Admin Password" das Default-Passwort "admin" ein.
5. Legen Sie bei "New Password" das neue Passwort fest.

6. Wiederholen Sie bei "Password Confirmation" das Passwort, um es zu bestätigen. Beide Einträge müssen übereinstimmen.



7. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Das Passwort für den Benutzer "admin" ist geändert. Die Änderungen sind sofort wirksam.

1.1.5 IP-Einstellungen des M874 ändern

Die Geräte erhalten in dieser Beispielkonfiguration folgende IP-Adresseinstellungen:

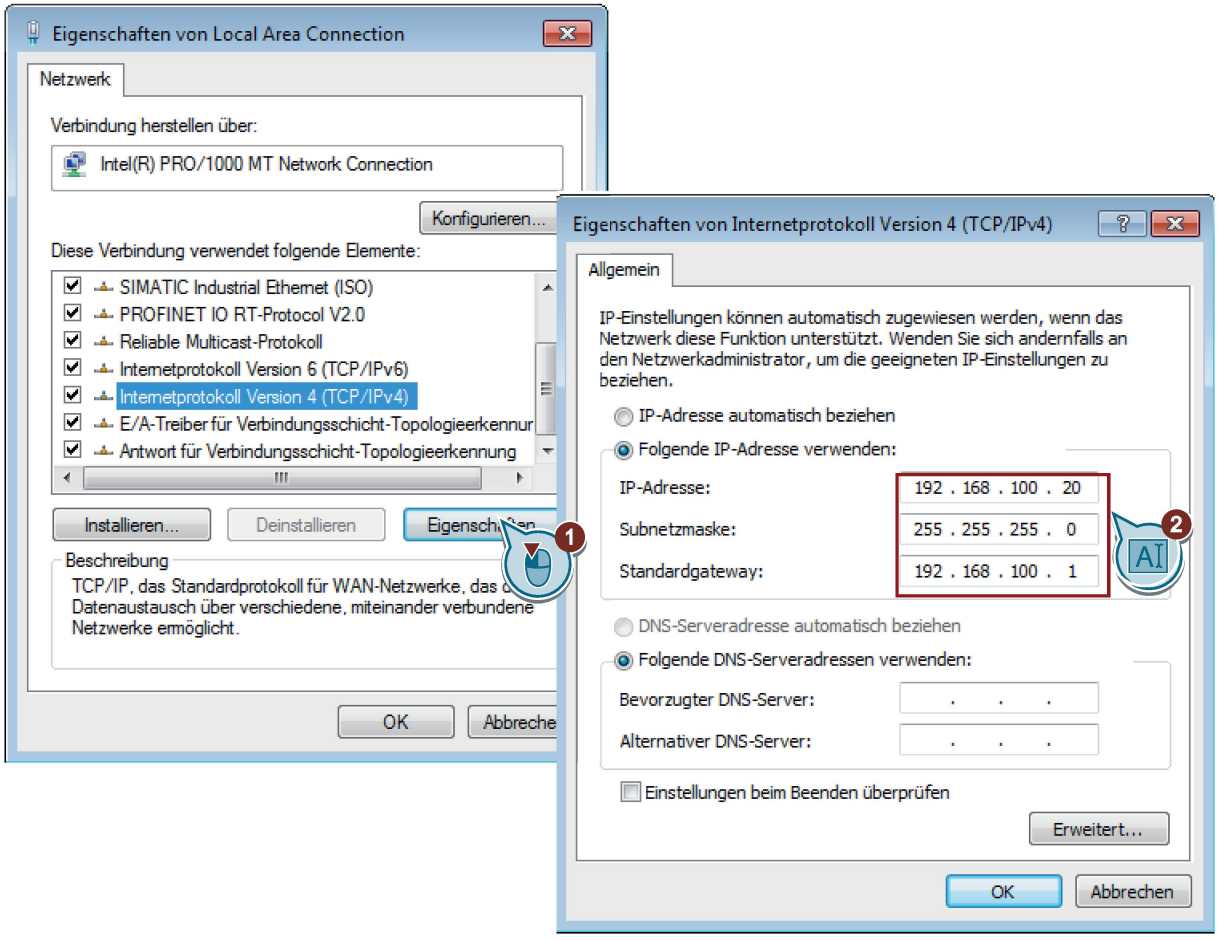
	IP-Adresse	Subnetzmaske
SCALANCE M-800	192.168.100.1	255.255.255.0
Admin-PC	192.168.100.20	255.255.255.0

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "Agent IP".
2. Tragen Sie bei "IP Address" 192.168.100.1 und bei "Subnet Mask" 255.255.255.0 ein.
3. Klicken Sie auf "Set Values".

   In der Adresszeile des Webbrowsers wird die IP-Adresse automatisch angepasst. Der Webbrowser auf dem Admin-PC kann nicht mehr auf das Web Based Management zugreifen, da seine IP-Einstellungen nicht mehr passen.
4. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
5. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".

6. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".
7. Tragen Sie die dem Admin-PC zugeordneten Werte aus der Tabelle in die dafür vorgesehenen Felder ein.



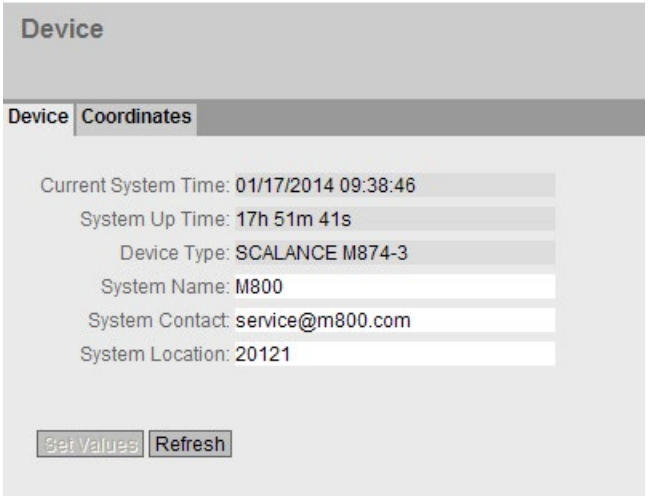
8. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
9. Tragen Sie im Adressfeld des Webbrowsers die IP-Adresse "192.168.100.1" ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).
10. Melden Sie sich mit dem Benutzernamen "admin" und dem geänderten Passwort an.

1.1.6 Geräteinformationen festlegen

Zur besseren Identifikation des SCALANCE M874 legen Sie allgemeine Geräteinformationen fest.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "General" und im Inhaltsbereich auf das Register "Device".
2. Tragen Sie bei "System Name" "M874" als Systemnamen für das Gerät ein.
3. Tragen Sie bei "System Contact" den für das Gerät zuständigen Ansprechpartner ein.
4. Tragen Sie bei "System Location" die Ortsbezeichnung des Aufstellungsorts ein, z.B. die Raumnummer.



5. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Die allgemeinen Geräteinformationen des SCALANCE M874 sind festgelegt.

1.1.7 Zugangsparameter konfigurieren

Voraussetzung

- Die Dienste sind freigeschaltet, z. B. Internet.
- Folgende Daten liegen vor:
  - PIN-Nummer
  - APN
  - Benutzernamen und Passwort für den APN

PIN-Nummer eingeben

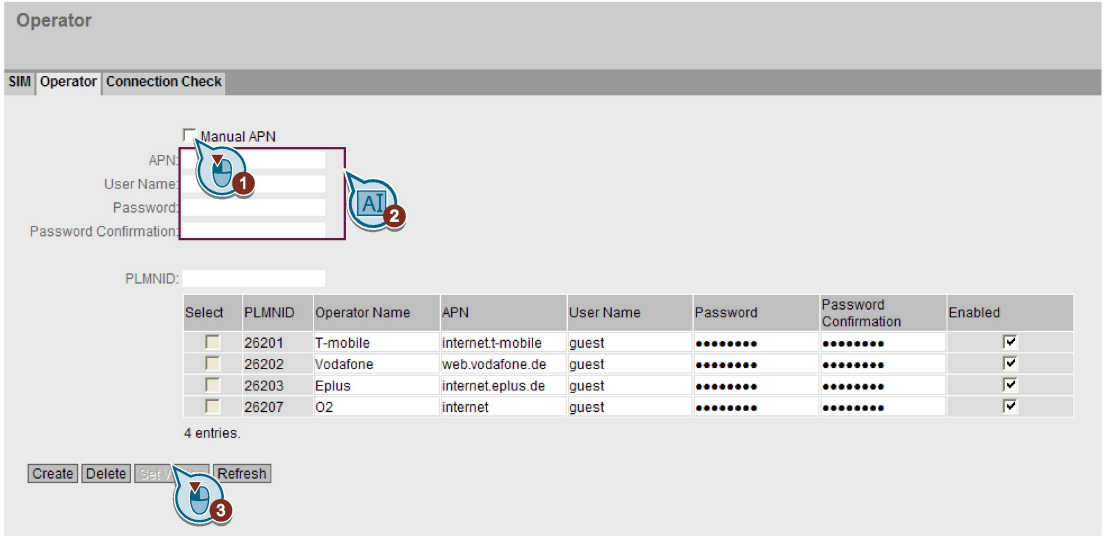
1. Klicken Sie im Navigationsbereich auf "Interfaces" > "Mobile" und im Inhaltsbereich auf das Register "SIM".
2. Geben Sie bei "PIN" die PIN-Nummer ein.
3. Aktivieren Sie "Enable Mobile Networks".
4. Klicken Sie auf "Set Values".

APN konfigurieren

1. Klicken Sie im Inhaltsbereich auf das Register "Operator".
2. Legen Sie die Zugangsdaten für den APN fest.
   - Wenn ihr Mobilfunkanbieter in der Tabelle enthalten ist, ist keine weitere Konfiguration notwendig.

   oder

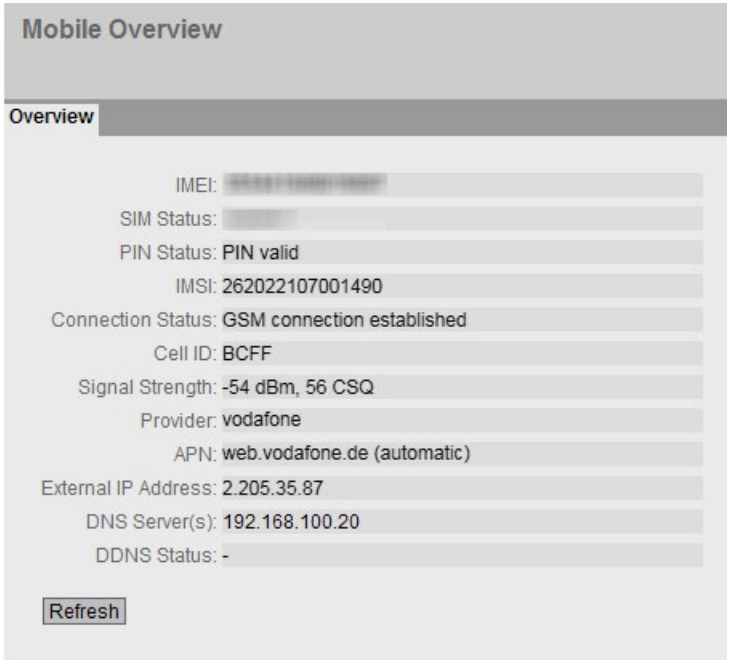
   - Wenn ihr Mobilfunkanbieter nicht in der Tabelle enthalten ist, aktivieren Sie "Manual APN".
   - Tragen Sie den APN, Benutzernamen und Passwort ein. Einige Mobilfunkanbieter verzichten auf die Zugangskontrolle durch ein Passwort. In diesem Fall lassen Sie das Feld leer.



Ergebnis

Die PIN-Nummer und der APN sind konfiguriert. Das M874 verbindet sich nach ca. 30 Sekunden mit dem Mobilfunknetz. Ob die Verbindung aufgebaut ist, können Sie unter "Information" > "Start Page" prüfen.

Detailliertere Informationen zur Verbindung erhalten Sie unter "Information" > "Mobile".



1.1.8 Uhrzeit einstellen

Zur Überprüfung der zeitlichen Gültigkeit von Zertifikaten und für die Zeitstempel von Logbuch-Einträgen werden auf dem SCALANCE M-800 Datum und Uhrzeit geführt. Sie können die Systemzeit selbst manuell einstellen, oder Sie lassen sie mit einem Zeitserver automatisch synchronisieren. Im Internet gibt es eine Reihe von Zeitservern, von denen die aktuelle Uhrzeit präzise bezogen werden kann. Für dieses Beispiel wird der Zeitserver über NTP konfiguriert.

Hinweis

Manuelle Zeiteinstellung - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die Uhrzeit auf Werkseinstellung zurückgesetzt wird, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie erneut die Systemzeit einstellen. Dadurch können Zertifikate ihre Gültigkeit verlieren.

Synchronisation über Zeitserver

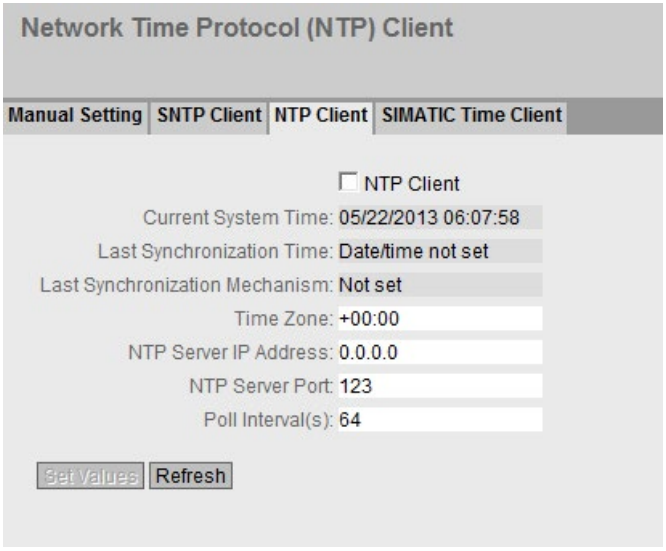
Die Synchronisation der Systemzeit über einen öffentlichen Zeitserver verursacht ein zusätzliches Datenaufkommen auf der Verbindung. Je nach Teilnehmervertrag sind damit erhöhte Kosten verbunden.

Voraussetzung

- Der NTP-Server ist erreichbar.
- Die IP-Adresse des NTP-Servers ist bekannt.
  Für dieses Beispiel wird einer der Zeitserver (z. B. 192.53.103.108) der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig verwendet.

Vorgehensweise

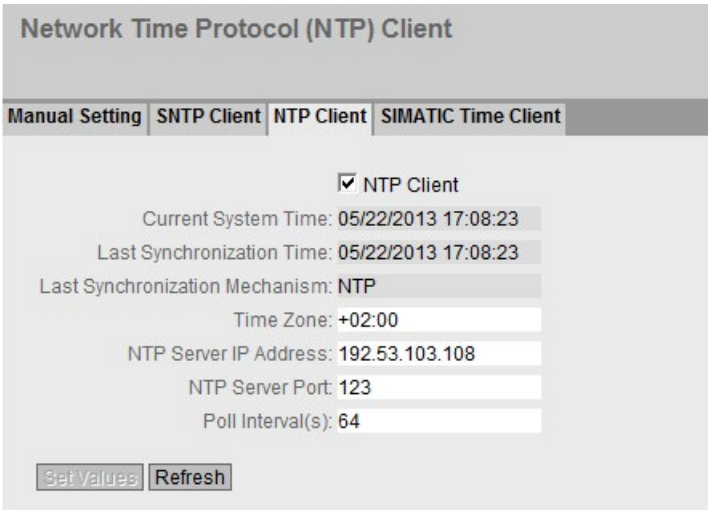
1. Klicken Sie im Navigationsbereich auf "System" > "System Time" und im Inhaltsbereich auf das Register "NTP Client".



2. Tragen Sie bei "Time Zone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Für mitteleuropäische Sommerzeit (MESZ) +02:00.
3. Tragen Sie bei "NTP Server IP Address" die IP-Adresse 192.53.103.108 ein. Die Eingabe der NTP-Adresse als Hostname z. B. timeserver.org ist nicht möglich.
4. Ändern Sie bei Bedarf den Port bei "NTP Server Port". Standardmäßig ist 123 eingestellt.
5. Tragen Sie bei "Poll Interval (s)" den Zeitabstand für die Synchronisation ein. Standardmäßig ist 64 eingestellt.
6. Aktivieren Sie "NTP Client".
7. Klicken Sie auf "Set Values".

Ergebnis

Die Systemzeit über NTP ist eingestellt. Klicken Sie auf "Refresh", um die WBM-Seite zu aktualisieren.



1.1.9 Zugriff erlauben

Es gibt folgende Möglichkeiten den Zugriff zu erlauben:

- Global erlauben

  Hier greifen Sie auf einfache, vordefinierte Firewall-Regeln zurück. Die frei gegebenen Dienste sind für alle Teilnehmer an den entsprechenden Schnittstellen gültig. Für die angegebene Richtung wird der volle Zugriff erlaubt.

  – vlan1: Erlaubt den Zugrff vom internen Netz auf das Gerät

  – ppp0 / usb0: Erlaubt den Zugriff vom externen Netz auf das Gerät

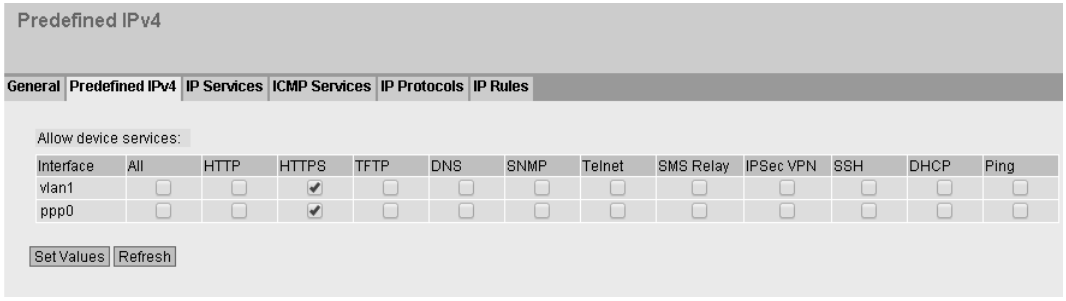
  Die Firewall-Regel für die Gegenrichtung wird mittels zustandsorientierte Paketüberprüfung (stateful packet inspection) erlaubt.

- Bestimmte Dienste erlauben

  Hier definieren Sie Firewall-Regeln, die für einen einzelnen Teilnehmer einzelne Dienste freischaltet oder für den Teilnehmer alle Dienste für den Zugriff auf die Station bzw. das Netz frei geben.
  In diesem Beispiel projektieren Sie die Firewall-Regel, die nur dem Gerät mit der IP-Adresse 192.168.100.20 den Zugriff auf Gerät erlaubt. Für den Zugriff wird der Dienst HTTP (TCP-Port 80) benötigt.

Beispiel 1: HTTPS-Zugriff global erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Aktivieren Sie bei "vlan1" und "ppp0" "HTTPS".
3. Klicken Sie auf "Set Values".



Beispiel 2: HTTPS-Zugriff einem bestimmten Gerät erlauben

Vordefinierte Firewall-Regel abschalten

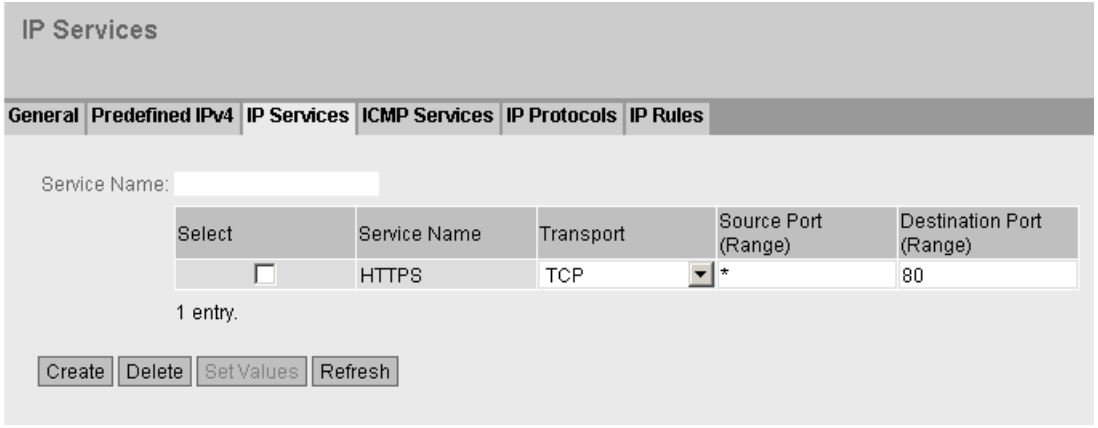
1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Deaktivieren Sie alle Dienste.

IP-Dienst HTTPS anlegen

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Services".
2. Geben Sie bei "Service Name" z. B. "HTTPS" ein und klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
3. Konfigurieren Sie HTTPS mit folgenden Einstellungen:

Transport	TCP
Destination Port (Range)	80 (Standard-Port)

4. Klicken Sie auf "Set Values".

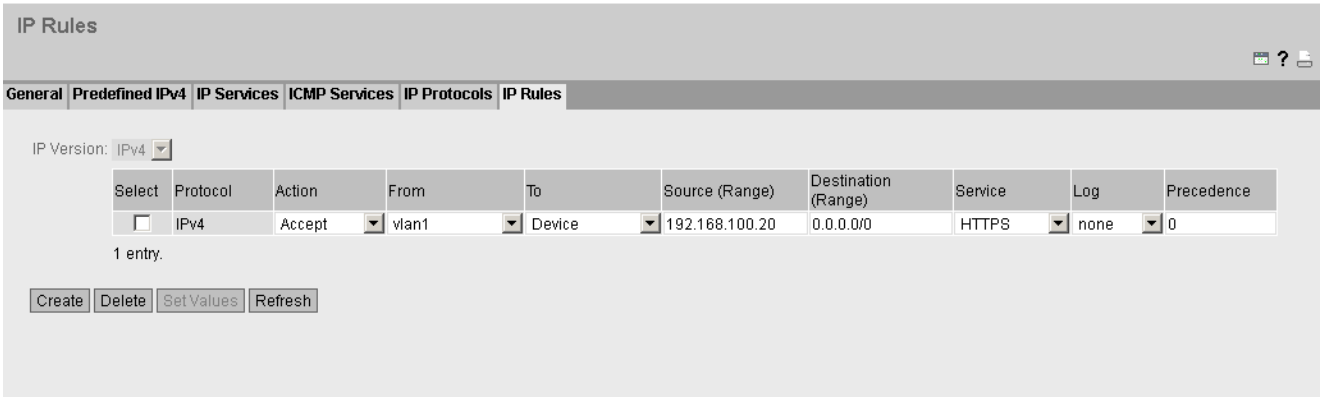


HTTPS-Zugriff nur einem bestimmten Gerät erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
2. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
3. Konfigurieren Sie die Firewall-Regel für den angelegten HTTPS-Dienst mit folgenden Einstellungen:

Action	Accept
From	vlan1
To	Device
Source (Range)	192.168.100.20 (das gewünschte Gerät)
Destination (Range)	0.0.0.0/0 (alle Adressen)
Service	HTTPS

4. Klicken Sie auf "Set Values".



1.1.10 DDNS-Hostnamen einrichten

DDNS steht für "dynamic domain name system". Wenn Sie das SCALANCE M-800 bei einem DDNS-Dienst anmelden, dann ist das Gerät aus dem externen Netz auch unter einem Hostnamen erreichbar, z. B. "example.no-ip.com".

Der DNS-Server des DDNS-Diensts verwaltet die Zuordnung IP-Adresse - Hostnamen. Der Client übermittelt dem DNS-Server seine aktuell zugewiesene IP-Adresse. Der DNS-Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit. Damit ist das SCALANCE M-800 immer über seinen Hostnamen erreichbar.

Voraussetzung

- Benutzernamen und Passwort, dass Sie zur Nutzung des DDNS-Diensts berechtigt
- Registrierter Hostname z. B. example.no-ip.com

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "DNS" und im Inhaltsbereich auf das Register "DDNS Client".
2. Tragen Sie bei "Host" den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip.com
3. Tragen Sie bei "User name" den Benutzernamen und bei "Password / Password confirmation" das Passwort ein, dass Sie zur Nutzung des DDNS-Diensts berechtigt. Ihr DDNS-Anbieter teilt Ihnen diese Angaben mit.
4. Aktivieren Sie "Enable".

5. Klicken Sie auf "Set Values".

Ergebnis

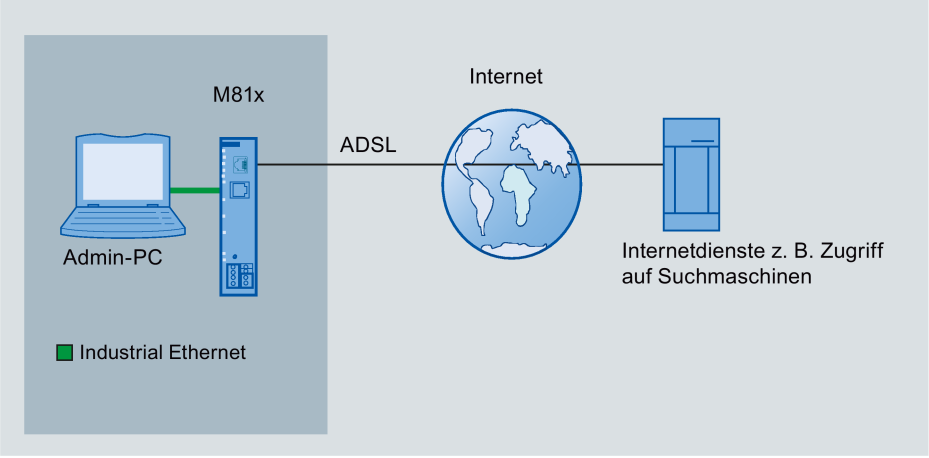
Der DDNS-Client ist aktiviert. Der DDNS-Client auf dem SCALANCE M-800 synchronisiert die zugewiesene IP-Adresse mit dem im DDNS-Dienst registrierten Hostnamen.

1.2 M81x mit ADSL verbinden

1.2.1 Prinzipielles Vorgehen

In diesem Beispiel wird dem SCALANCE M81x, das sich im Zustand der Werkseinstellungen befindet, eine IP-Adresse zugewiesen. Im Anschluss wird das Gerät über das Web Based Management (WBM) konfiguriert.

Aufbau



Erforderliche Geräte/Komponenten

- 1x M812 oder 1x M816 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
- ADSL ist freigeschaltet
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmblockstecker
- 1x PC zum Konfigurieren des Geräts.
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Projektierungsschritte

Zum Anbinden eines M81x an das Festnetz sind folgende Schritte erforderlich:

1. SCALANCE M81x und Netzwerk einrichten (Seite 29).
2. Das Web Based Management starten (Seite 30)
3. Am Web Based Management anmelden (Seite 33)
4. IP-Einstellungen des M81x ändern (Seite 34).
5. SCALANCE M81x konfigurieren.
   - Geräteinformationen festlegen (Seite 36)
   - Zugangsparameter konfigurieren (Seite 37)
   - Uhrzeit einstellen (Seite 39)
   - Zugriff erlauben (Seite 41).

1.2.2 SCALANCE M81x und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Vorgehensweise

1. Packen Sie zunächst das M81x aus und überprüfen Sie den unbeschädigten Zustand.
2. Montieren Sie die Spannungsversorgung.

⚠ WARNUNG

Nur Sicherheitskleinspannung verwenden

Das Gerät SCALANCE M81x ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE M81x muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

3. Verbinden Sie das Gerät mit der DSL-Buchse am Splitter.
4. Schließen Sie das Gerät über die Ethernet-Ports an das lokale Netz an.
5. Schalten Sie das Gerät an. Nachdem Anschließen leuchtet die Fehler-LED (F) rot.
6. Schalten Sie jetzt den PC ein.

1.2.3 Das Web Based Management starten

Werkseitig ist das SCALANCE M-800 unter der folgenden IP-Adresse erreichbar:

- IP-Adresse: 192.168.1.1
- Subnetzmaske: 255.255.255.0

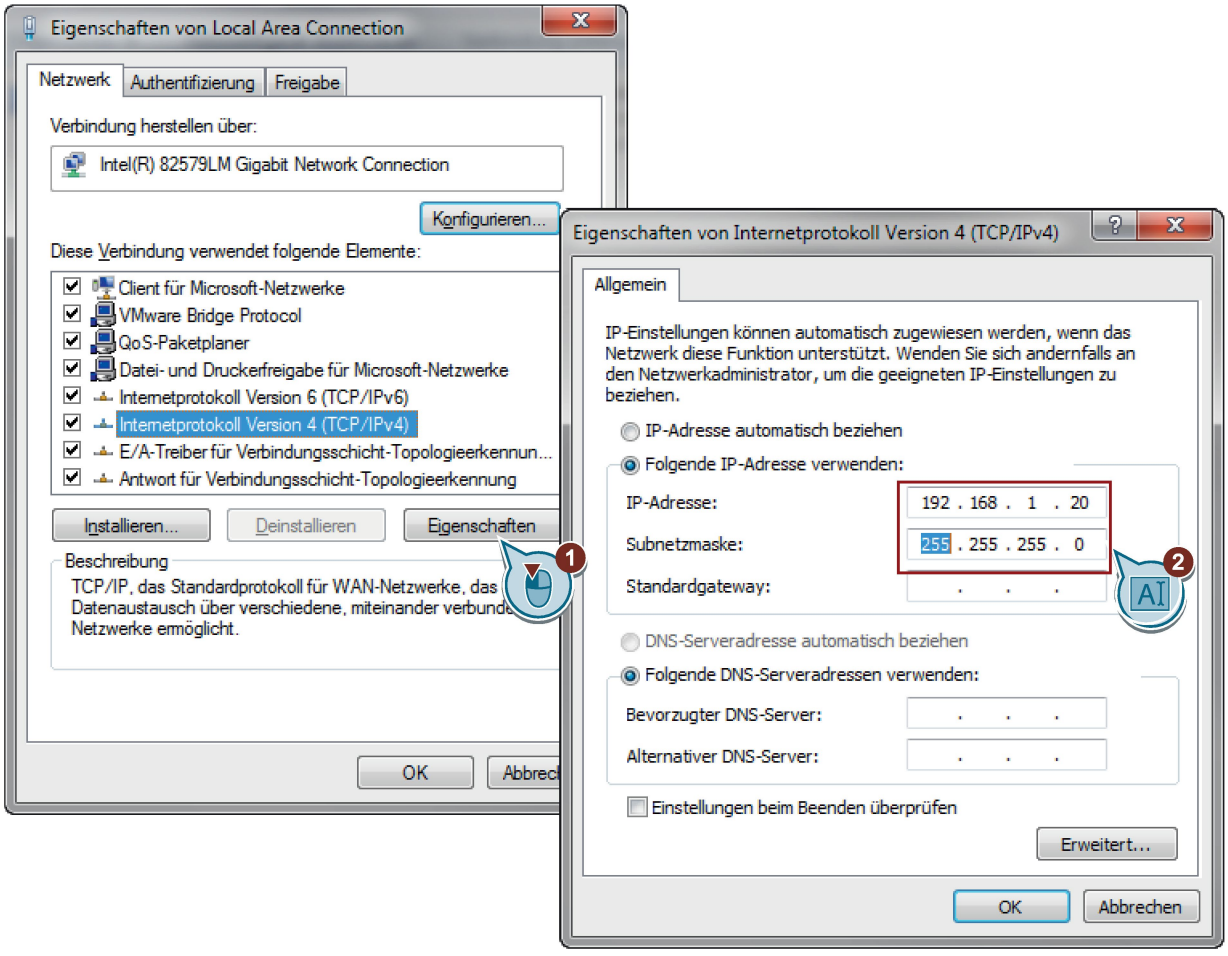
Der Admin-PC erhält in dieser Beispielkonfiguration folgende IP-Adresseinstellung, um auf das Web Based Management des M-800 zu zugreifen.

IP-Adresse	Subnetzmaske
192.168.1.20	255.255.255.0

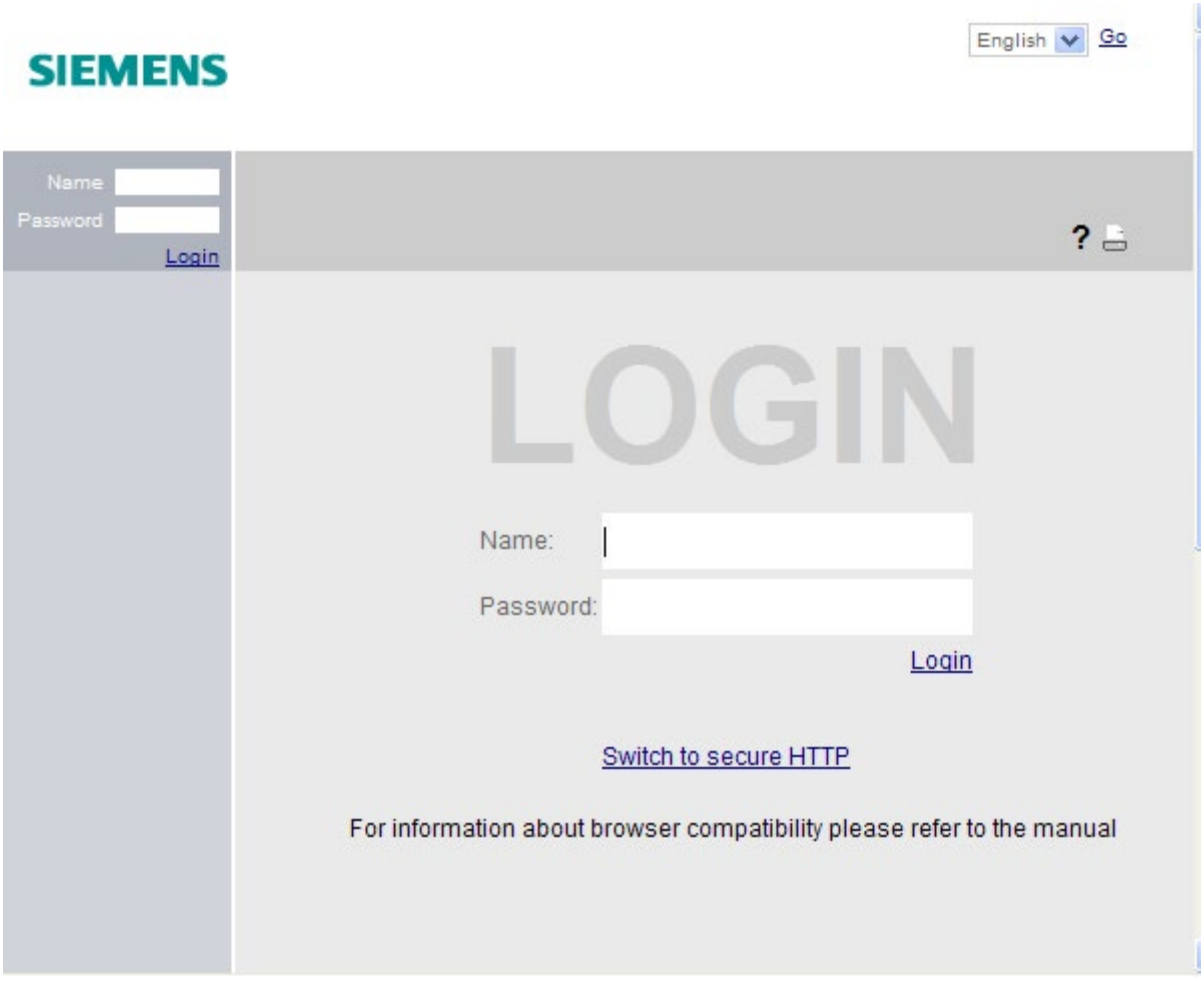
Vorgehensweise

1. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Klicken Sie mit der rechten Maustaste auf das Symbol "LAN-Verbindung" und wählen Sie den Menübefehl "Eigenschaften".
4. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".

5. Geben Sie die dem Admin-PC zugeordneten Werte aus der Tabelle in die dafür vorgesehenen Felder ein.



6. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
7. Geben Sie im Adressfeld des Webbrowsers die IP-Adresse "192.168.1.1" ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

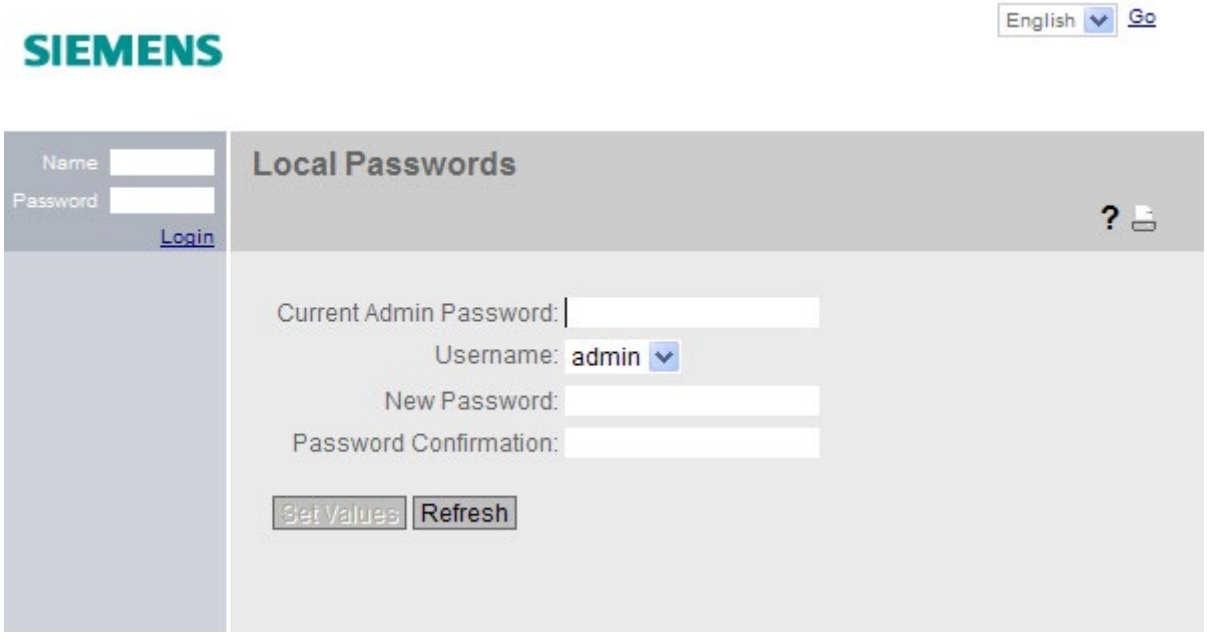


1.2.4 Am Web Based Management anmelden

Vorgehensweise

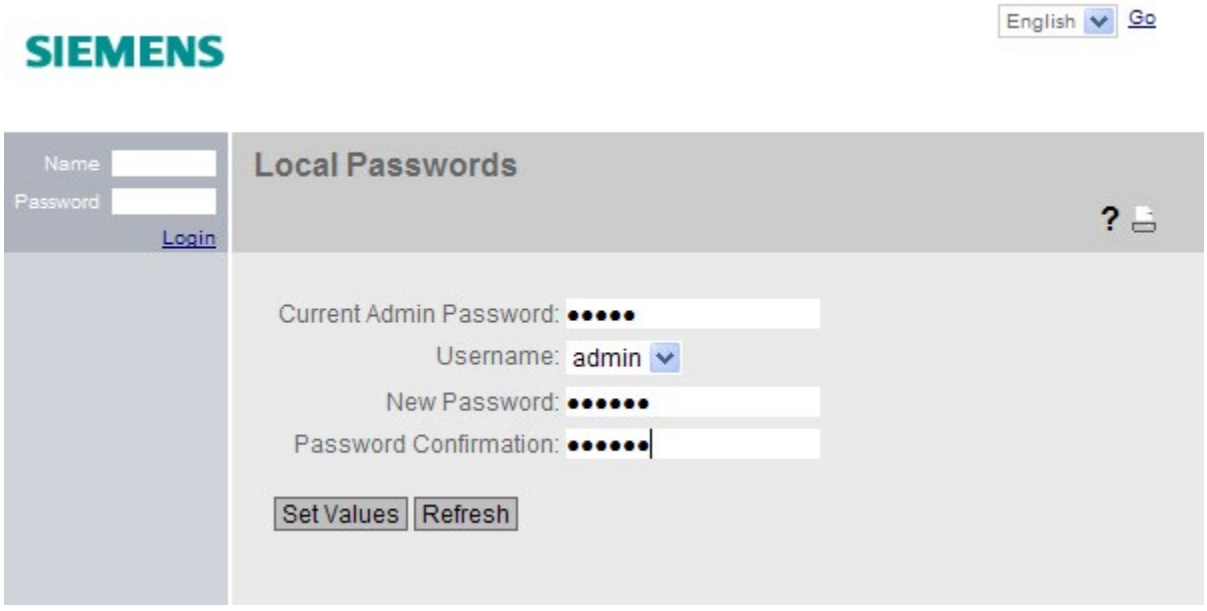
1. Melden Sie sich mit dem Benutzernamen "admin" und dem Passwort "admin" an. Sie werden aufgefordert, das Passwort zu ändern.

2. Bestätigen Sie den Dialog. Automatisch wird die WBM-Seite "Password" geöffnet.



3. Wählen Sie bei "Username" den Benutzer "admin" aus.
4. Tragen Sie bei "Current Admin Password" das Default-Passwort "admin" ein.
5. Legen Sie bei "New Password" das neue Passwort fest.

6. Wiederholen Sie bei "Password Confirmation" das Passwort, um es zu bestätigen. Beide Einträge müssen übereinstimmen.



7. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Das Passwort für den Benutzer "admin" ist geändert. Die Änderungen sind sofort wirksam.

1.2.5 IP-Einstellungen des M81x ändern

Die Geräte erhalten in dieser Beispielkonfiguration folgende IP-Adresseinstellungen:

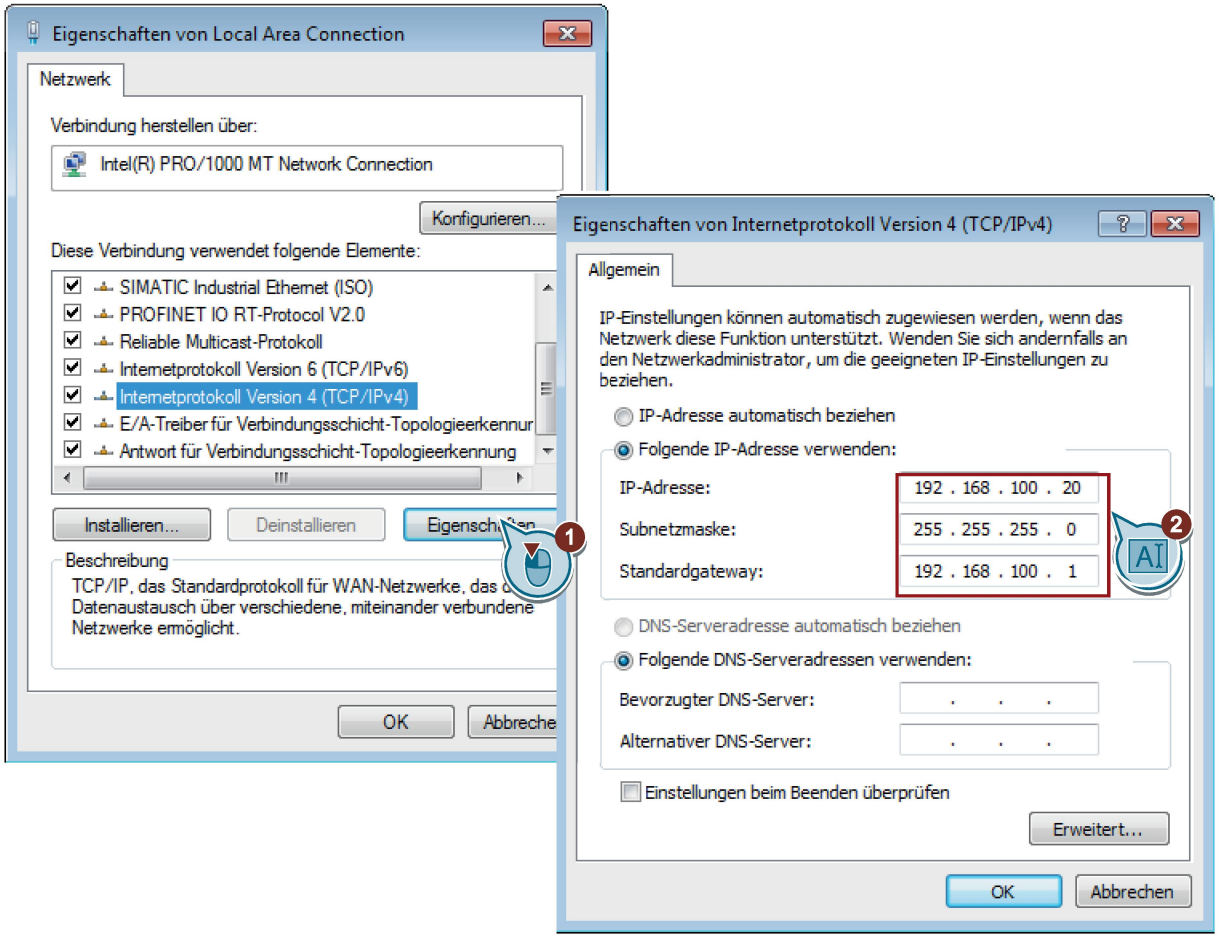
	IP-Adresse	Subnetzmaske
SCALANCE M-800	192.168.100.1	255.255.255.0
Admin-PC	192.168.100.20	255.255.255.0

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "Agent IP".
2. Tragen Sie bei "IP Address" 192.168.100.1 und bei "Subnet Mask" 255.255.255.0 ein.
3. Klicken Sie auf "Set Values".

   In der Adresszeile des Webbrowsers wird die IP-Adresse automatisch angepasst. Der Webbrowser auf dem Admin-PC kann nicht mehr auf das Web Based Management zugreifen, da seine IP-Einstellungen nicht mehr passen.
4. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.

5. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
6. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".
7. Tragen Sie die dem Admin-PC zugeordneten Werte aus der Tabelle in die dafür vorgesehenen Felder ein.



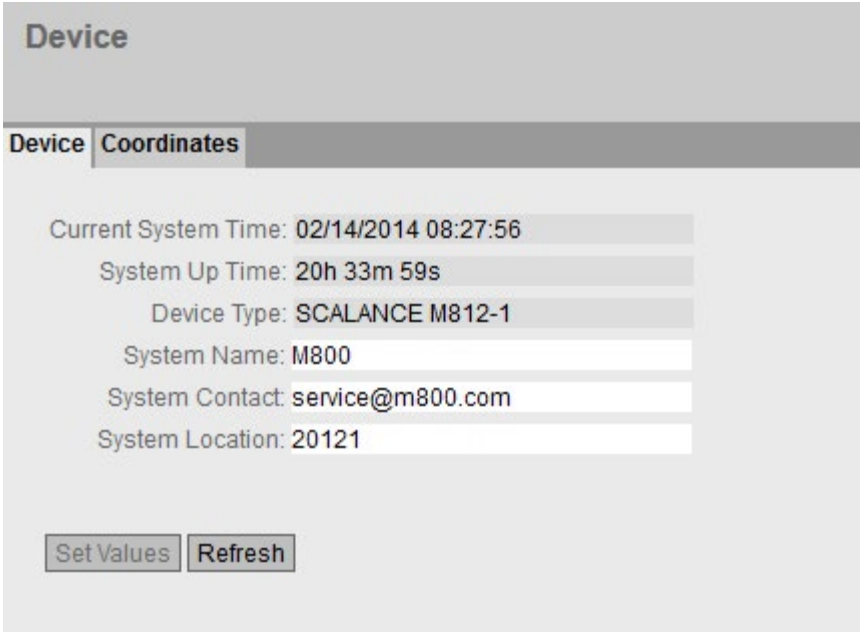
8. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
9. Tragen Sie im Adressfeld des Webbrowsers die IP-Adresse "192.168.100.1" ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).
10. Melden Sie sich mit dem Benutzernamen "admin" und dem geänderten Passwort an.

1.2.6 Geräteinformationen festlegen

Zur besseren Identifikation des SCALANCE M81x legen Sie allgemeine Geräteinformationen fest.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "General" und im Inhaltsbereich auf das Register "Device".
2. Tragen Sie bei "System Name" "M800" als Systemnamen für das Gerät ein.
3. Tragen Sie bei "System Contact" den für das Gerät zuständigen Ansprechpartner ein.
4. Tragen Sie bei "System Location" die Ortsbezeichnung des Aufstellungsorts ein, z.B. die Raumnummer.



5. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Die allgemeinen Geräteinformationen des SCALANCE M81x sind festgelegt.

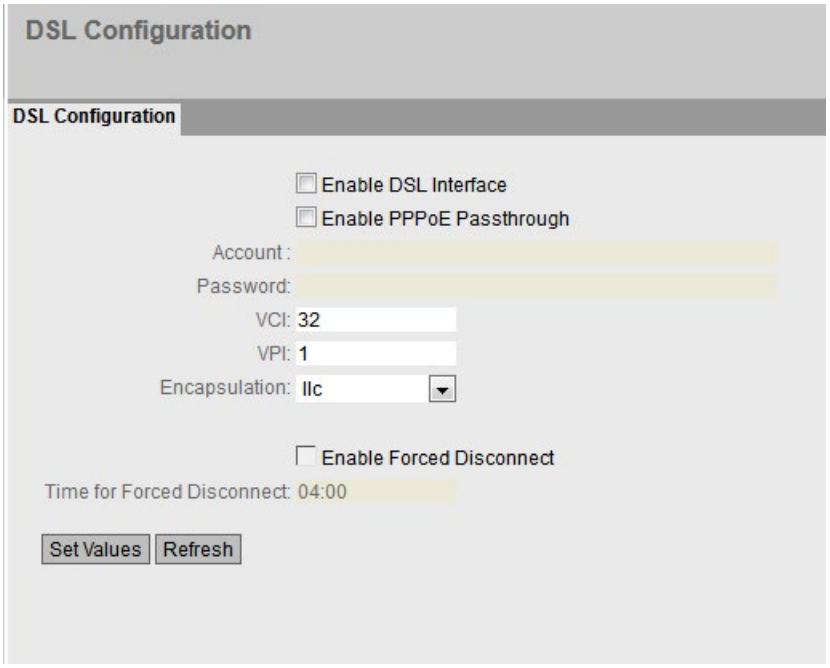
1.2.7 Zugangsparameter konfigurieren

Voraussetzung

- Die Dienste sind freigeschaltet, z. B. Internet.
- Von ihrem DSL-Anbieter sind folgende Zugangsdaten bekannt:
  - Benutzernamen und Passwort für den ADSL-Zugang
  - VCI / VPI
  - Encapsulation

ADSL konfigurieren

1. Klicken Sie im Navigationsbereich auf "Interfaces" > "DSL"



2. Aktivieren Sie "Enable DSL Interface".
3. Deaktivieren Sie "Enable PPPoE Passthrough", um die Zugangsdaten am SCALANCE M81x einzurichten. Die angeschlossenen Geräte können diese DSL-Verbindung nutzen.

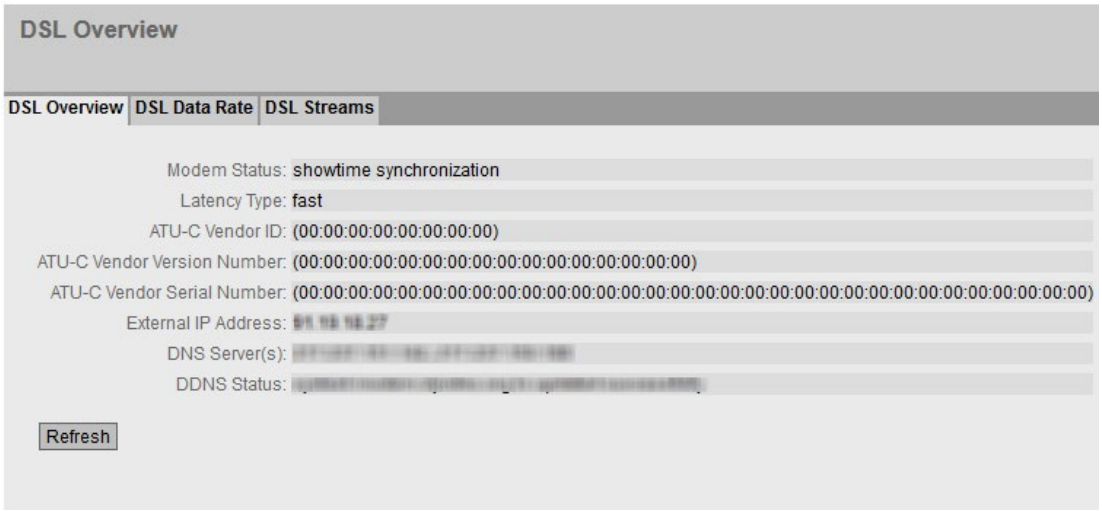
   Wenn "Enable PPPoE Passthrough" aktiviert ist, sind die Zugangsdaten nicht konfigurierbar. In diesem Fall wird das SCALANCE M81x als Modem genutzt. Jedes einzelne angeschlossene Gerät sendet seine Zugangsdaten an das SCALANCE M81x und baut eine eigene Internetverbindung auf.
4. Tragen Sie den Benutzernamen und das Passwort für den ADSL-Zugang ein.
5. Tragen Sie die Einstellungen für VCI / VPI ein. Die Einstellungen erhalten Sie von Ihrem DSL-Anbieter.

6. Wählen Sie bei "Encapsulation" das gewünschte Protokoll aus.
7. Klicken Sie auf "Set Values".

Ergebnis

Die DSL-Verbindung ist eingerichtet. Das Gerät verbindet sich nach ca. 30 Sekunden mit dem Internet. Ob die Verbindung aufgebaut ist, können Sie unter "Information" > "Start Page" prüfen.

Detailliertere Informationen zur Verbindung erhalten Sie unter "Information" > "DSL".



1.2.8 Uhrzeit einstellen

Zur Überprüfung der zeitlichen Gültigkeit von Zertifikaten und für die Zeitstempel von Logbuch-Einträgen werden auf dem SCALANCE M-800 Datum und Uhrzeit geführt. Sie können die Systemzeit selbst manuell einstellen, oder Sie lassen sie mit einem Zeitserver automatisch synchronisieren. Im Internet gibt es eine Reihe von Zeitservern, von denen die aktuelle Uhrzeit präzise bezogen werden kann. Für dieses Beispiel wird der Zeitserver über NTP konfiguriert.

Hinweis

Manuelle Zeiteinstellung - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die Uhrzeit auf Werkseinstellung zurückgesetzt wird, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie erneut die Systemzeit einstellen. Dadurch können Zertifikate ihre Gültigkeit verlieren.

Synchronisation über Zeitserver

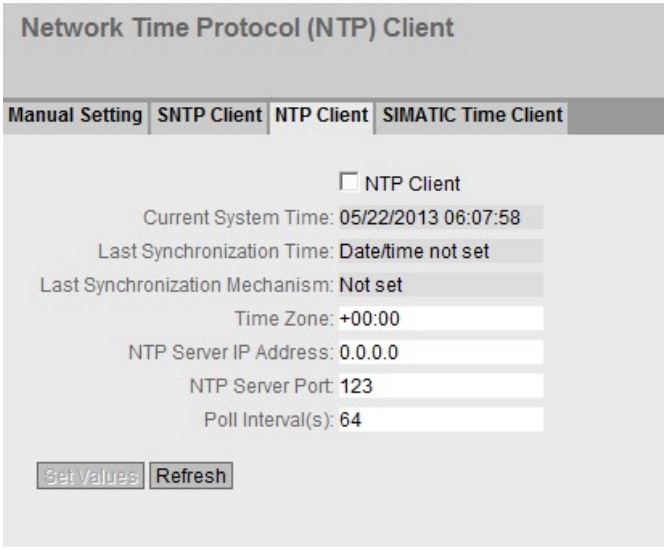
Die Synchronisation der Systemzeit über einen öffentlichen Zeitserver verursacht ein zusätzliches Datenaufkommen auf der Verbindung. Je nach Teilnehmervertrag sind damit erhöhte Kosten verbunden.

Voraussetzung

- Der NTP-Server ist erreichbar.
- Die IP-Adresse des NTP-Servers ist bekannt.
  Für dieses Beispiel wird einer der Zeitserver (z. B. 192.53.103.108) der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig verwendet.

Vorgehensweise

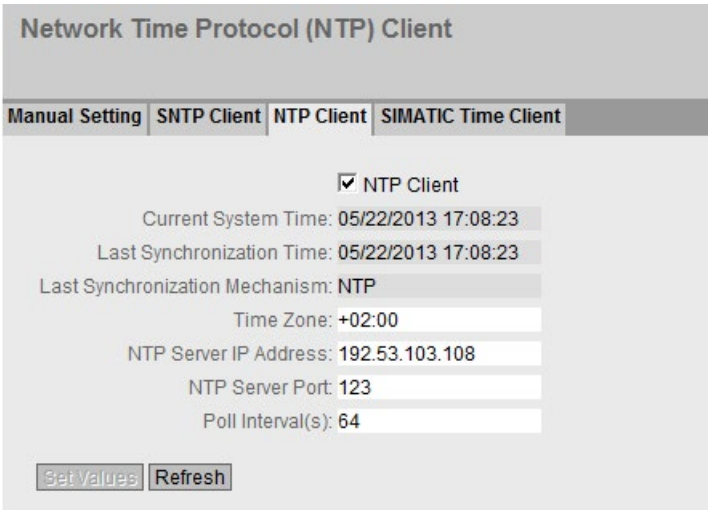
1. Klicken Sie im Navigationsbereich auf "System" > "System Time" und im Inhaltsbereich auf das Register "NTP Client".



2. Tragen Sie bei "Time Zone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Für mitteleuropäische Sommerzeit (MESZ) +02:00.
3. Tragen Sie bei "NTP Server IP Address" die IP-Adresse 192.53.103.108 ein. Die Eingabe der NTP-Adresse als Hostname z. B. timeserver.org ist nicht möglich.
4. Ändern Sie bei Bedarf den Port bei "NTP Server Port". Standardmäßig ist 123 eingestellt.
5. Tragen Sie bei "Poll Interval (s)" den Zeitabstand für die Synchronisation ein. Standardmäßig ist 64 eingestellt.
6. Aktivieren Sie "NTP Client".
7. Klicken Sie auf "Set Values".

Ergebnis

Die Systemzeit über NTP ist eingestellt. Klicken Sie auf "Refresh", um die WBM-Seite zu aktualisieren.



1.2.9 Zugriff erlauben

Die Firewall ist standardmäßig aktiviert. Der Zugriff von intern nach extern ist dabei nicht erlaubt.

Es gibt folgende Möglichkeiten den Zugriff zu erlauben:

- Global erlauben

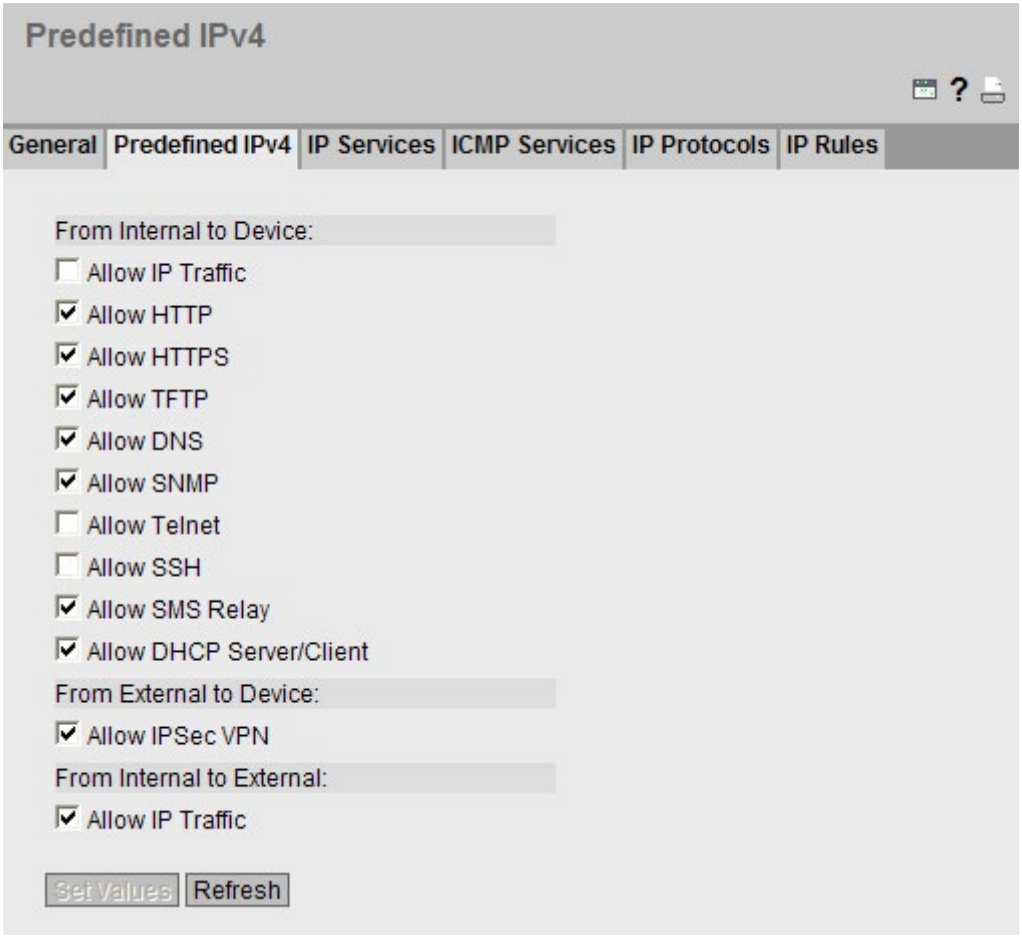
  Hier greifen Sie auf einfache, vordefinierte Firewall-Regeln zurück. Die frei gegebenen Dienste sind für alle Teilnehmer gültig und es wird für die angegebene Richtung der volle Zugriff erlaubt. Die Firewall-Regel für die Gegenrichtung wird mittels zustandsorientierte Paketüberprüfung (stateful packet inspection) erlaubt.

- Bestimmte Dienste erlauben

  Hier definieren Sie Firewall-Regeln, die für einen einzelnen Teilnehmer einzelne Dienste freischaltet oder für den Teilnehmer alle Dienste für den Zugriff auf die Station bzw. das Netz frei geben.
  In diesem Beispiel projektieren Sie die Firewall-Regeln, die nur dem Gerät mit der IP-Adresse 192.168.100.10 den Zugriff auf das gesamte Internet erlaubt. Für den Zugriff werden die Dienste HTTP (TCP-Port 80) und DNS (UDP-Port 53) benötigt.

Zugriff allen erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Aktivieren Sie bei "From Internal to External" "Allow IP Traffic".
3. Klicken Sie auf "Set Values".



Internet-Zugriff einem bestimmten Gerät erlauben

Vordefinierte Firewall-Regel abschalten

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Deaktivieren Sie bei "From Internal to External" "Allow IP Traffic".

IP-Dienste HTTP und DNS anlegen

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Services".
2. Geben Sie bei "Service Name" z. B. "HTTP" ein und klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.

3. Konfigurieren Sie HTTP mit folgenden Einstellungen:

Transport	TCP
Destination Port (Range)	80 (Standard-Port)

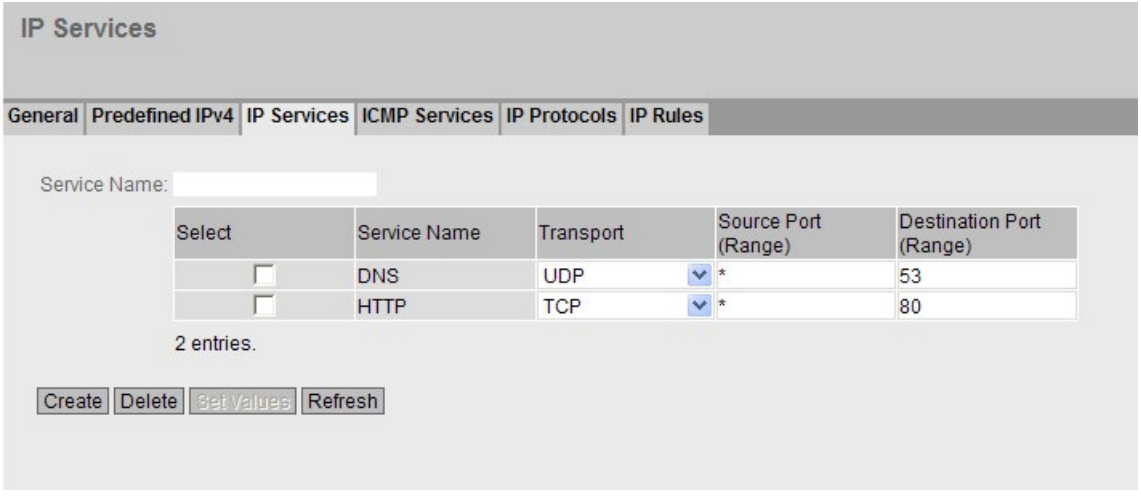
4. In der Tabelle wird ein neuer Eintrag erstellt.

   Geben Sie bei "Service Name" z. B. "DNS" ein und klicken Sie auf "Create".

5. Klicken Sie auf "Set Values".
6. Konfigurieren Sie DNS mit folgenden Einstellungen:

Transport	UDP
Destination Port (Range)	53 (Standard-Port)

7. Klicken Sie auf "Set Values".



IP-Dienst nur einem bestimmten Gerät erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
2. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
3. Konfigurieren Sie die Firewall-Regel für HTTP mit folgenden Einstellungen:

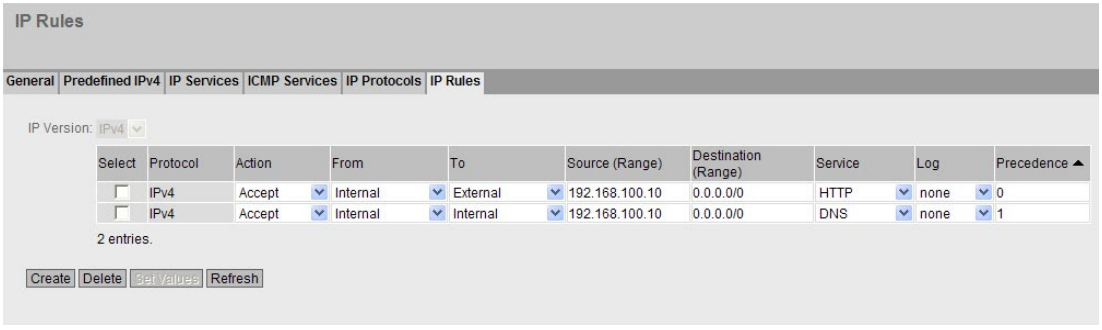
Action	Accept
From	Internal
To	External
Source (Range)	192.168.100.10 (das gewünschte Gerät)
Destination (Range)	0.0.0.0/0 (alle Adressen)
Service	HTTP

4. Klicken Sie auf "Set Values".

5. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
6. Konfigurieren Sie die Firewall-Regel für DNS mit folgenden Einstellungen:

Action	Accept
From	Internal
To	Internal
Source (Range)	192.168.100.10 (das gewünschte Gerät)
Destination (Range)	0.0.0.0/0 (alle Adressen)
Service	HTTP

7. Klicken Sie auf "Set Values".



1.2.10 DDNS-Hostnamen einrichten

DDNS steht für "dynamic domain name system". Wenn Sie das SCALANCE M-800 bei einem DDNS-Dienst anmelden, dann ist das Gerät aus dem externen Netz auch unter einem Hostnamen erreichbar, z. B. "example.no-ip.com".

Der DNS-Server des DDNS-Diensts verwaltet die Zuordnung IP-Adresse - Hostnamen. Der Client übermittelt dem DNS-Server seine aktuell zugewiesene IP-Adresse. Der DNS-Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit. Damit ist das SCALANCE M-800 immer über seinen Hostnamen erreichbar.

Voraussetzung

- Benutzernamen und Passwort, dass Sie zur Nutzung des DDNS-Diensts berechtigt
- Registrierter Hostname z. B. example.no-ip.com

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "DNS" und im Inhaltsbereich auf das Register "DDNS Client".
2. Tragen Sie bei "Host" den Hostnamen ein, den Sie für das Gerät mit Ihrem DDNS-Anbieter vereinbart haben, z. B. example.no-ip.com

3. Tragen Sie bei "User name" den Benutzernamen und bei "Password / Password confirmation" das Passwort ein, dass Sie zur Nutzung des DDNS-Diensts berechtigt. Ihr DDNS-Anbieter teilt Ihnen diese Angaben mit.
4. Aktivieren Sie "Enable".

5. Klicken Sie auf "Set Values".

Ergebnis

Der DDNS-Client ist aktiviert. Der DDNS-Client auf dem SCALANCE M-800 synchronisiert die zugewiesene IP-Adresse mit dem im DDNS-Dienst registrierten Hostnamen.

1.3 M826 mit SHDSL verbinden

1.3.1 Out-of-the-box

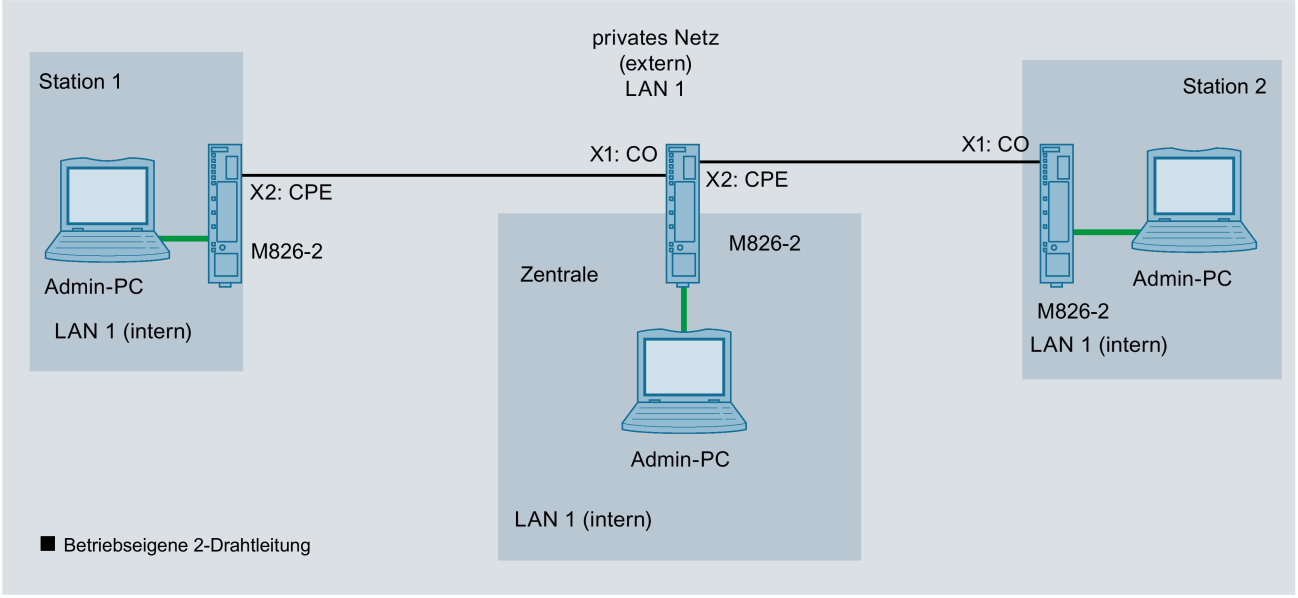
1.3.1.1 Prinzipielles Vorgehen

In diesem Beispiel werden drei SCALANCE M826, die sich im Zustand der Werkseinstellungen befinden, direkt miteinander verbunden.

Voreingestellt sind die SHDSL-Schnittstellen so, dass sie miteinander eine Punkt-zu-Punkt-Verbindung aufbauen können. Für diese Verbindung muss eine SHDSL-Schnittstelle CO und die andere SHDSL-Schnittstelle CPE sein.

Im Auslieferungszustand arbeitet das SCALANCE M826 im Bridge-Modus. Der Unterschied zwischen dem Bridge-Modus und dem Routing-Modus liegt in der Unterteilung in externe und interne Netze. Im Bridge-Modus gibt es keine Unterteilung. Das SCALANCE M826 ist eine transparente Bridge und verbindet Netzknoten, die im selben IP-Subnetz sind. In diesem Modus sind die Sicherheits-Features (IPsec VPN, Firewall, NAT/NAPT) nicht verfügbar.

Aufbau



Die Netzknoten sind im selben IP-Subnetz (LAN1)

Zentrale - Anschluss an SCALANCE M826

- In der Zentrale wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Zentrale
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Station 1 und 2 - Anschluss an SCALANCE M826

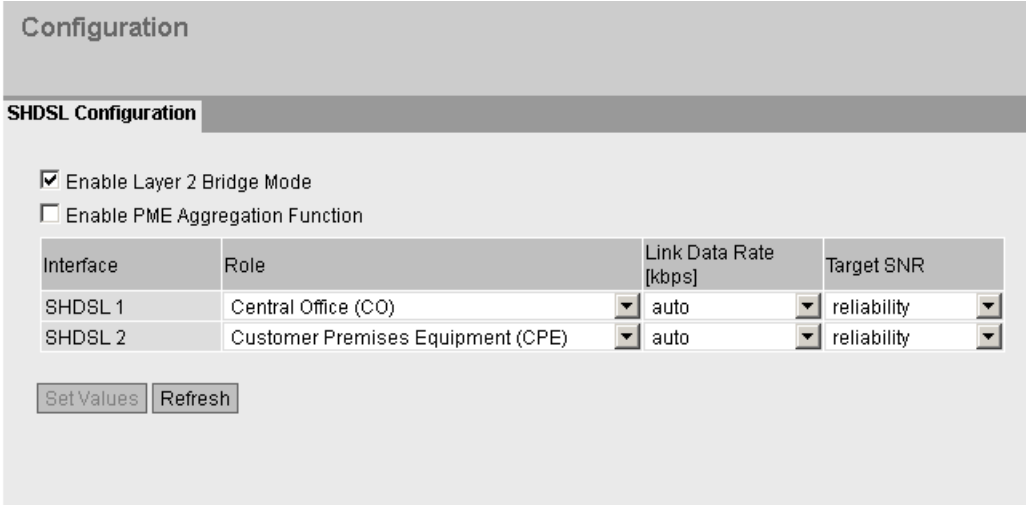
- In der Station wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Station
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Voraussetzung

- Alle Netzknoten sind im selben IP-Subnetz.

Verwendete Einstellungen

Die Geräte verwenden für die Beispielkonfiguration die Werkseinstellungen.



Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an SHDSL
  - 3x M826 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 3x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - 2x 2 Draht-Leitung mit Klemmenblocksteckern
- 3x PC die mit je einem M826 verbunden sind.

Projektierungsschritt

1. SCALANCE M826 und Netzwerk einrichten (Seite 48).

1.3.1.2 SCALANCE M826 und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Voraussetzung

- Alle Netzknoten sind im selben IP-Subnetz.

Vorgehensweise

1. Packen Sie zunächst das M826 aus und überprüfen Sie den unbeschädigten Zustand.
2. Montieren Sie die Spannungsversorgung.

⚠ WARNUNG

Nur Sicherheitskleinspannung verwenden

Das Gerät SCALANCE M826 ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE M826 muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

3. Verdrahten Sie X1 mit X2, siehe Aufbau (Seite 46).
4. Schließen Sie die Geräte über die Ethernet-Ports an das lokale Netz an.

5. Schalten Sie die Geräte an. Nachdem Anschließen leuchtet die Fehler-LED (F) rot
6. Schalten Sie jetzt den PC ein.

Ergebnis

Die SCALANCE M826 sind ohne Konfiguration sofort betriebsbereit. Es kann einige Zeit dauern, bis die Geräte die Verbindungsparameter ausgehandelt haben.

Auf das WBM können Sie nicht zugreifen, da dies eine IP-Adresse voraussetzt. Die IP-Adresse kann mit einem DHCP-Server oder mit dem Primary Setup Tool zugewiesen werden, siehe "SCALANCE M826 mit PST konfigurieren (Seite 52)".

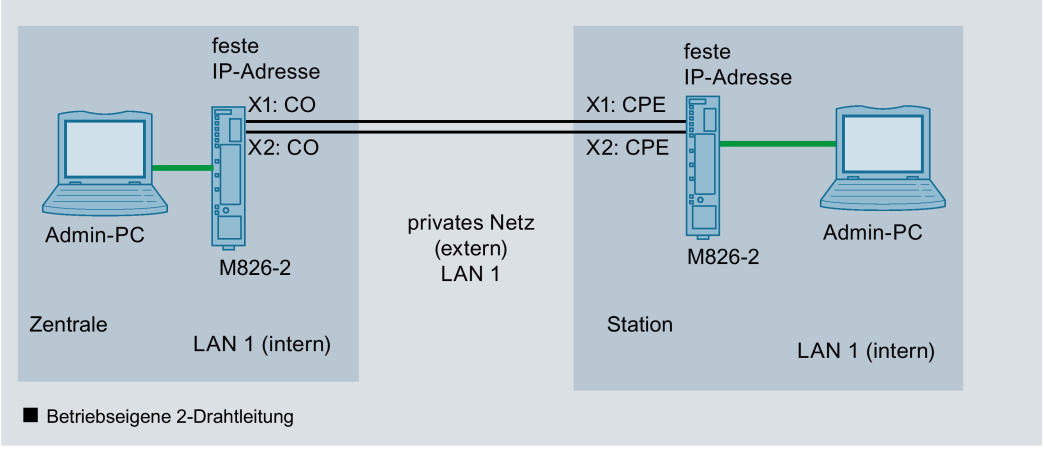
1.3.2 SHDSL im 4-Draht-Betrieb

1.3.2.1 Prinzipielles Vorgehen

In diesem Beispiel werden die beiden SHDSL-Schnittstellen zu einer einzigen Verbindung mit höherer Übertragungsrate zusammengefasst.

Das SCALANCE M826 ist im Bridge-Modus. In diesem Modus sind die Sicherheits-Features (IPsec VPN, Firewall, NAT/NAPT) nicht verfügbar.

Aufbau



Die Netzknoten sind im selben IP-Subnetz

Zentrale - Anschluss an SCALANCE M826

- In der Zentrale wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Zentrale
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Station - Anschluss an SCALANCE M-800

- In der Station wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Station
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an SHDSL
  - 2x M826 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 2x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
- 2x PC die mit je einem SCALANCE M826 verbunden sind.
- PST ist auf dem PC installiert.

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen:

		IP-Adresse
Zentrale	M826	192.168.100.1 255.255.255.0
	Admin-PC	192.168.100.20 255.255.255.0
Station	M826	192.168.100.10 255.255.255.0
	Admin-PC	192.168.100.40 255.255.255.0

Projektierungsschritte

Zum Konfigurieren des 4-Draht-Betriebs sind folgende Schritte erforderlich

1. SCALANCE M826 und Netzwerk einrichten (Seite 51)
2. SCALANCE M826 mit PST konfigurieren (Seite 52)
3. Das Web Based Management starten (Seite 54)
4. Am Web Based Management anmelden (Seite 56)
5. SCALANCE M826 konfigurieren

   Die Schritte gelten für beide Geräte und unterscheiden sich nur in den Einstellungen.

   – Geräteinformationen festlegen (Seite 57)
   – Uhrzeit einstellen (Seite 58)
   – SHDSL konfigurieren (Seite 60)

1.3.2.2 SCALANCE M826 und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Vorgehensweise

1. Packen Sie zunächst das M826 aus und überprüfen Sie den unbeschädigten Zustand.
2. Montieren Sie die Spannungsversorgung.

   ⚠ WARNUNG

   Nur Sicherheitskleinspannung verwenden

   Das Gerät SCALANCE M826 ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

   Das Netzteil für die Versorgung des SCALANCE M826 muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

3. Verdrahten Sie die M826, siehe Aufbau (Seite 49).
4. Schließen Sie das Gerät über die Ethernet-Ports an das lokale Netz an.
5. Schalten Sie das Gerät an. Nachdem Anschließen leuchtet die Fehler-LED (F) rot.
6. Schalten Sie jetzt den PC ein.

1.3.2.3 SCALANCE M826 mit PST konfigurieren

Voraussetzung

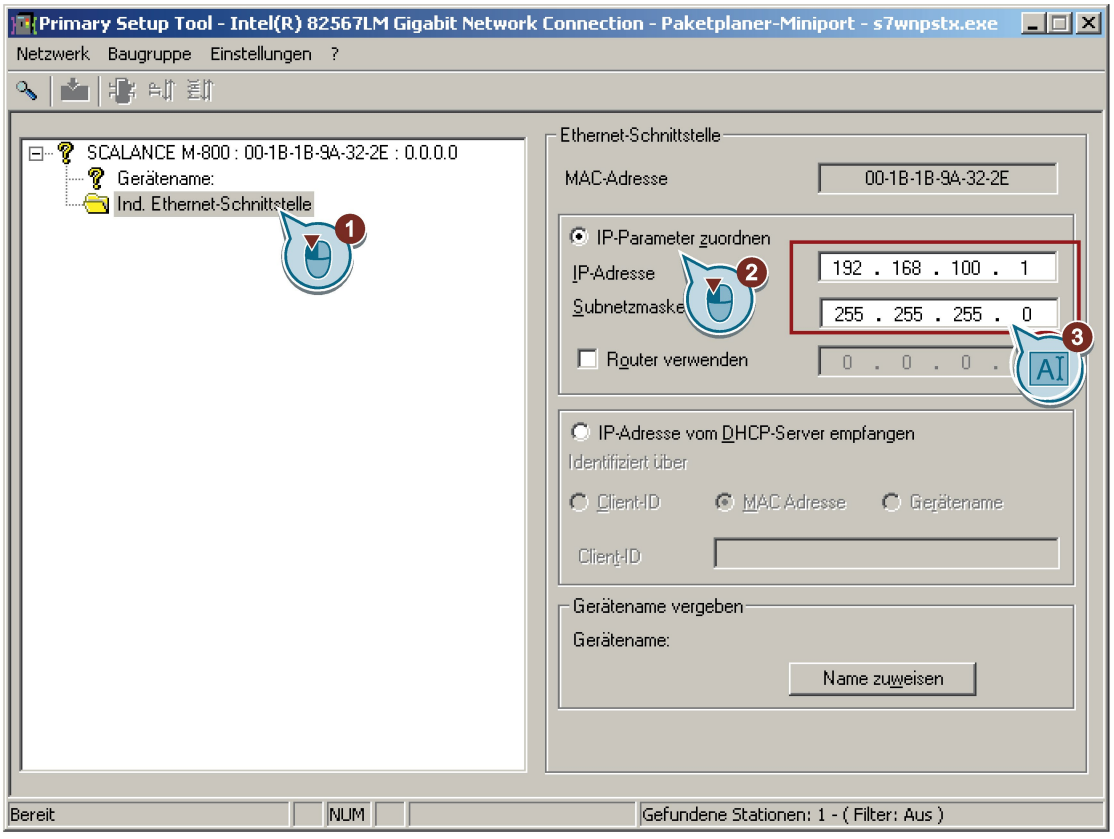
- Die Geräte sind im selben IP-Subnetz.
- Die IP-Adressen sind eindeutig.

Vorgehensweise

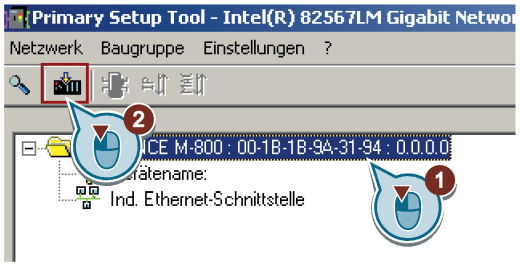
1. Starten Sie das Primary Setup Tool unter "Start > SIMATIC > Primary Setup Tool".

   Wenn am PC mehrere Netzwerkkarten eingebaut sind, wählen Sie unter "Einstellungen >Netzwerkkarte" den Netzwerk-Adapter, der mit M826 verbunden ist.
2. Klicken Sie in der Funktionsleiste auf die Lupe, um den Suchlauf zu starten. Nach dem Suchlauf wird das M826 im PST aufgelistet.

3. Tragen Sie die dem M826 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 49)" ein.



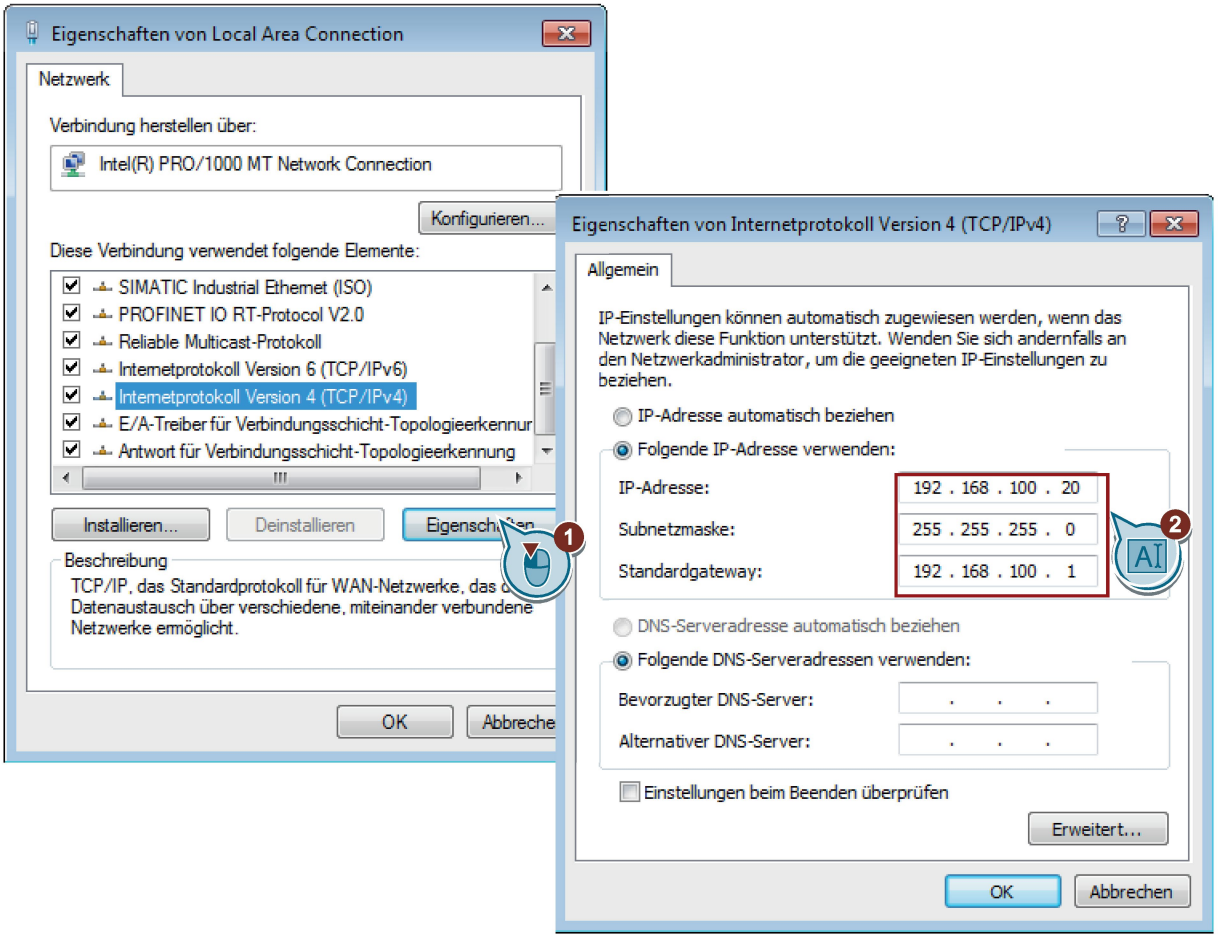
4. Übertragen Sie die IP-Adresse.



1.3.2.4 Das Web Based Management starten

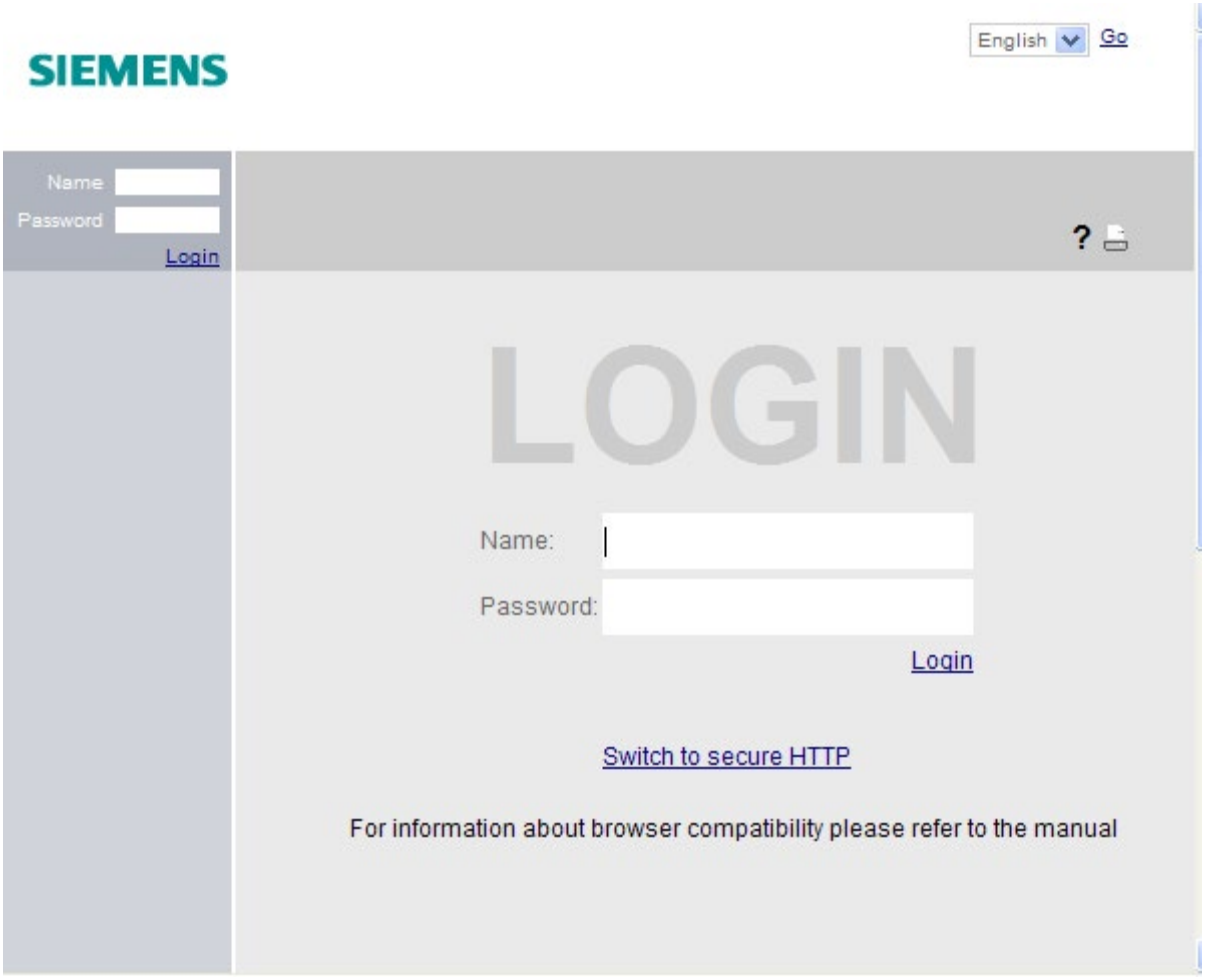
Vorgehensweise

1. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Klicken Sie mit der rechten Maustaste auf das Symbol "LAN-Verbindung" und wählen Sie den Menübefehl "Eigenschaften".
4. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".
5. Tragen Sie die dem Admin-PC zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 49)" ein.



6. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
7. Tragen Sie im Adressfeld des Webbrowsers die dem M826 zugeordnete IP-Adresse aus der Tabelle "Verwendete Einstellungen (Seite 49)" ein. Wenn eine einwandfreie

Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

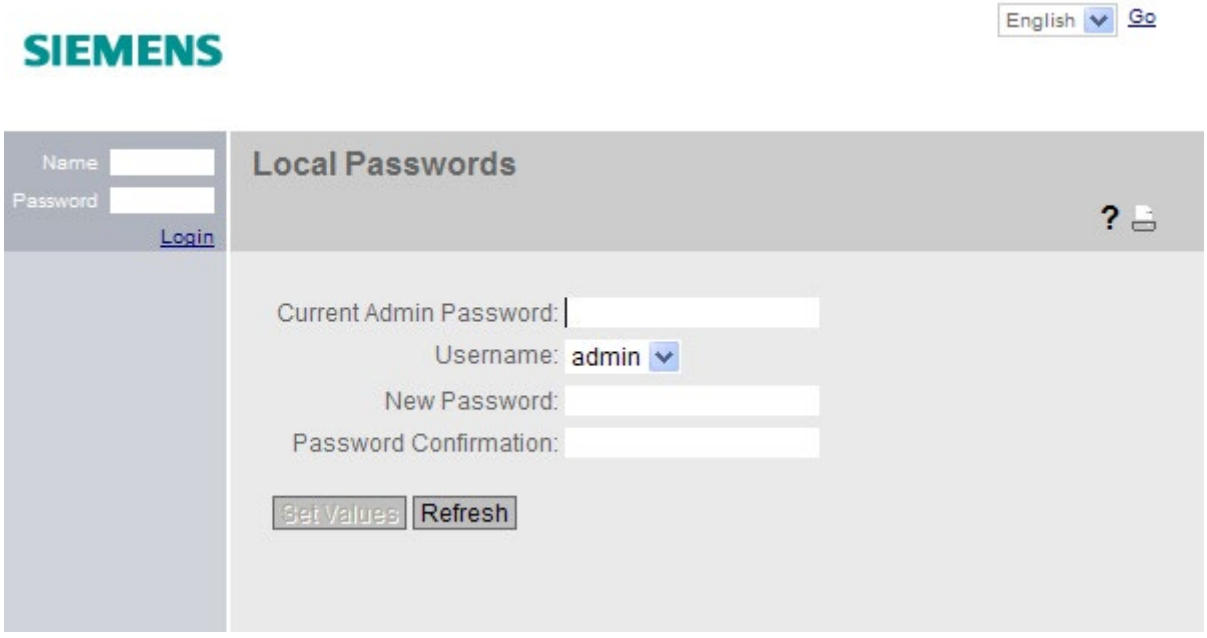


1.3.2.5 Am Web Based Management anmelden

Vorgehensweise

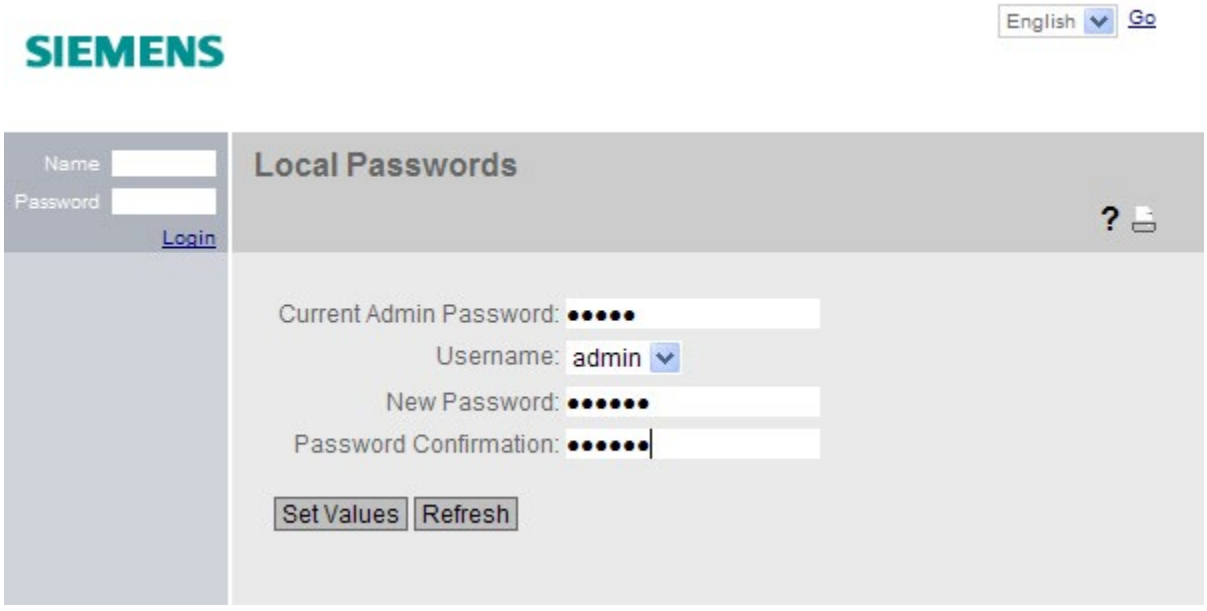
1. Melden Sie sich mit dem Benutzernamen "admin" und dem Passwort "admin" an. Sie werden aufgefordert, das Passwort zu ändern.

2. Bestätigen Sie den Dialog. Automatisch wird die WBM-Seite "Password" geöffnet.



3. Wählen Sie bei "Username" den Benutzer "admin" aus.
4. Tragen Sie bei "Current Admin Password" das Default-Passwort "admin" ein.
5. Legen Sie bei "New Password" das neue Passwort fest.

6. Wiederholen Sie bei "Password Confirmation" das Passwort, um es zu bestätigen. Beide Einträge müssen übereinstimmen.



7. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Das Passwort für den Benutzer "admin" ist geändert. Die Änderungen sind sofort wirksam.

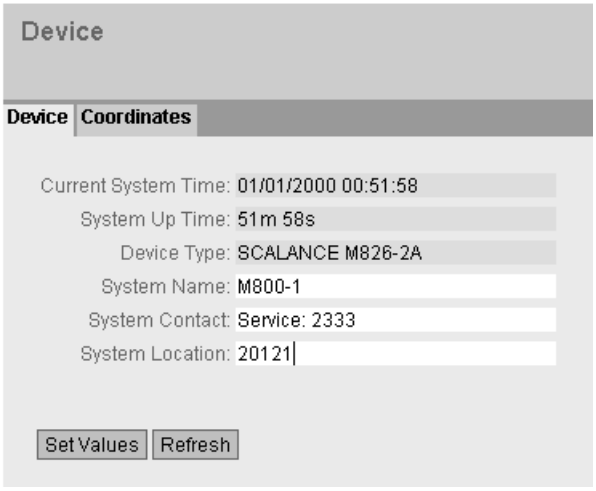
1.3.2.6 Geräteinformationen festlegen

Zur besseren Identifikation der SCALANCE M826 legen Sie allgemeine Geräteinformationen fest.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "General" und im Inhaltsbereich auf das Register "Device".
2. Tragen Sie bei "System Name" einen Systemnamen für das Gerät ein, z. B. "M800-1" für die Zentrale und "M800-2" für die Außenstation.
3. Tragen Sie bei "System Contact" den für das Gerät zuständigen Ansprechpartner ein.

4. Tragen Sie bei "System Location" die Ortsbezeichnung des Aufstellungsorts ein, z.B. die Raumnummer.



5. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Die allgemeinen Geräteinformationen der SCALANCE M826 sind festgelegt.

1.3.2.7 Uhrzeit einstellen

Zur Überprüfung der zeitlichen Gültigkeit von Zertifikaten und für die Zeitstempel von Logbuch-Einträgen werden auf dem SCALANCE M-800 Datum und Uhrzeit geführt. Sie können die Systemzeit selbst manuell einstellen, oder Sie lassen sie mit einem Zeitserver automatisch synchronisieren. Für dieses Beispiel wird der Zeitserver über NTP konfiguriert.

Hinweis

Manuelle Zeiteinstellung - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die Uhrzeit auf Werkseinstellung zurückgesetzt wird, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie erneut die Systemzeit einstellen. Dadurch können Zertifikate ihre Gültigkeit verlieren.

Synchronisation über Zeitserver

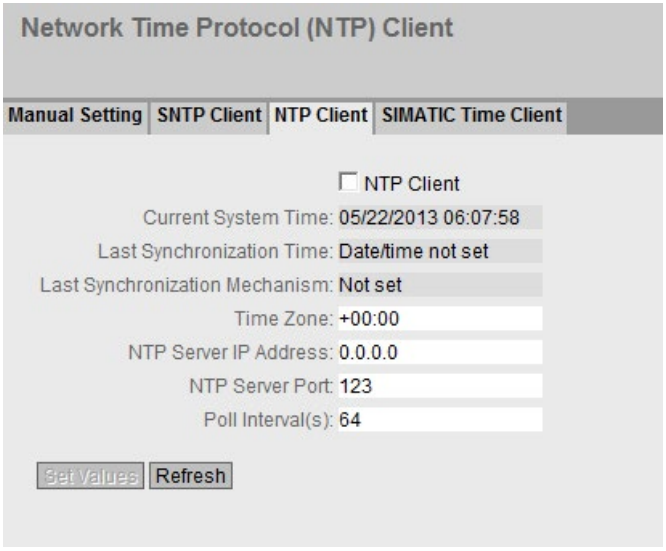
Die Synchronisation der Systemzeit über einen öffentlichen Zeitserver verursacht ein zusätzliches Datenaufkommen auf der Verbindung. Je nach Teilnehmervertrag sind damit erhöhte Kosten verbunden.

Voraussetzung

- Im lokalen Netz ist ein NTP-Server erreichbar.
- Die IP-Adresse des NTP-Servers ist bekannt.
  Für dieses Beispiel wird ein lokaler Zeitserver mit der IP-Adresse 192.168.100.87 verwendet.

Vorgehensweise

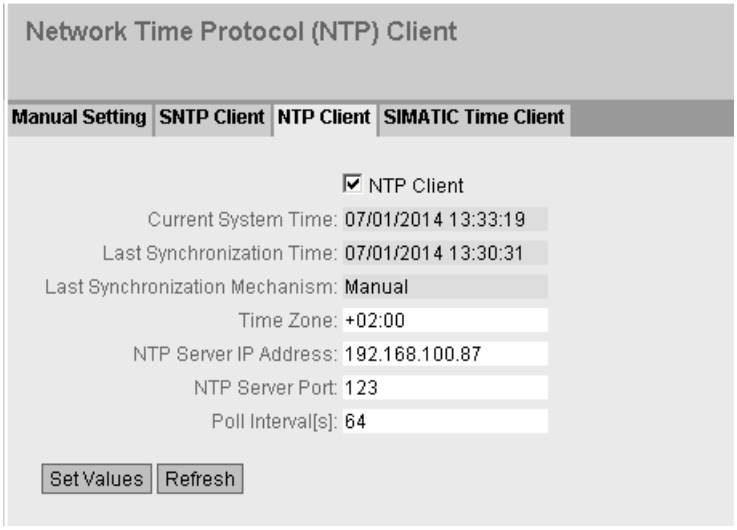
1. Klicken Sie im Navigationsbereich auf "System" > "System Time" und im Inhaltsbereich auf das Register "NTP Client".



2. Tragen Sie bei "Time Zone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Für mitteleuropäische Sommerzeit (MESZ) +02:00.
3. Tragen Sie bei "NTP Server IP Address" die IP-Adresse 192.168.100.87 ein. Die Eingabe der NTP-Adresse als Hostname ist nicht möglich.
4. Ändern Sie bei Bedarf den Port bei "NTP Server Port". Standardmäßig ist 123 eingestellt.
5. Tragen Sie bei "Poll Interval (s)" den Zeitabstand für die Synchronisation ein. Standardmäßig ist 64 eingestellt.
6. Aktivieren Sie "NTP Client".
7. Klicken Sie auf "Set Values".

Ergebnis

Die Systemzeit über NTP ist eingestellt. Klicken Sie auf "Refresh", um die WBM-Seite zu aktualisieren.



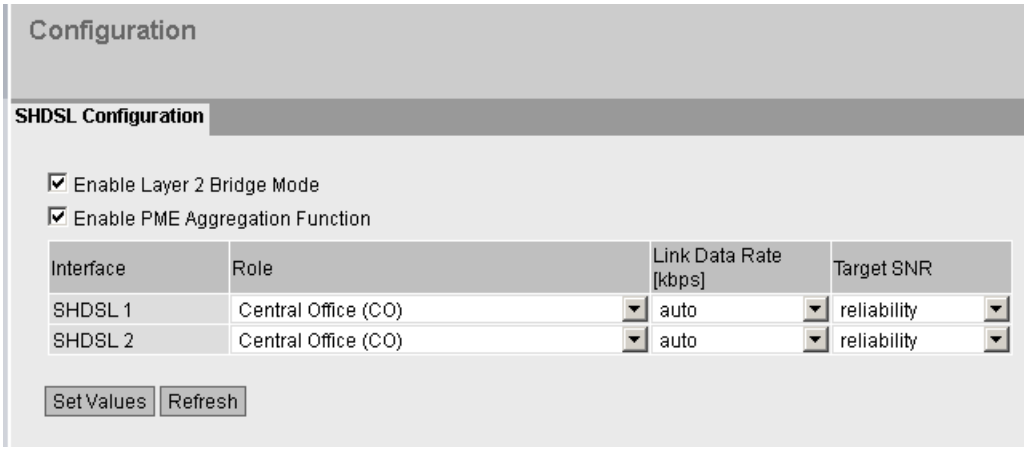
1.3.2.8 SHDSL konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Interfaces" > "SHDSL"
2. Lassen Sie "Enable Layer2 Bridge Mode" aktiviert.
3. Aktivieren Sie "Enable PME Aggregation Function". Wenn aktiviert, werden die SHDSL-Schnittstellen bzw. die 2-Drathleitungen zu einer einzigen Verbindung mit höherer Übertragungsrate zusammengefasst.
4. Legen Sie die Rolle der Schnittstellen fest. Auf beiden Geräten müssen beide Schnittstellen jeweils die gleiche Rolle.

M826 in der Zentrale	X1	Central Office (CO)
	X2	Central Office (CO)
M826 in der Station	X1	Customer Premises Equipment (CPE)
	X2	Customer Premises Equipment (CPE)

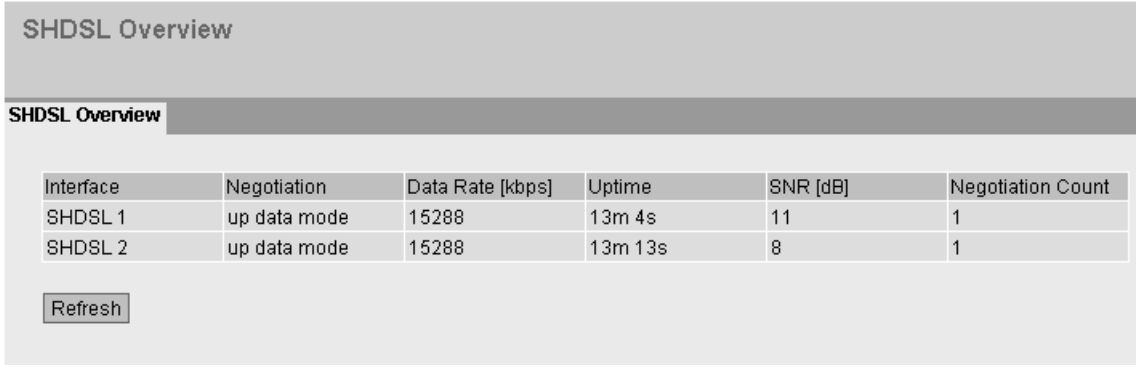
5. Wählen Sie bei "Link Data Rate" "auto" und bei "Target SNR Ration" "reliability".
6. Klicken Sie auf "Set Values".



Ergebnis

Die SHDSL-Verbindung ist eingerichtet. Die Geräte verhandeln die Verbindungsparameter aus. D. h. die Geräte nehmen die Übertragungsrate, bei der zuverlässig die Daten gesendet und empfangen werden können.

Detailliertere Informationen zur Verbindung erhalten Sie unter "Information" > "SHDSL".



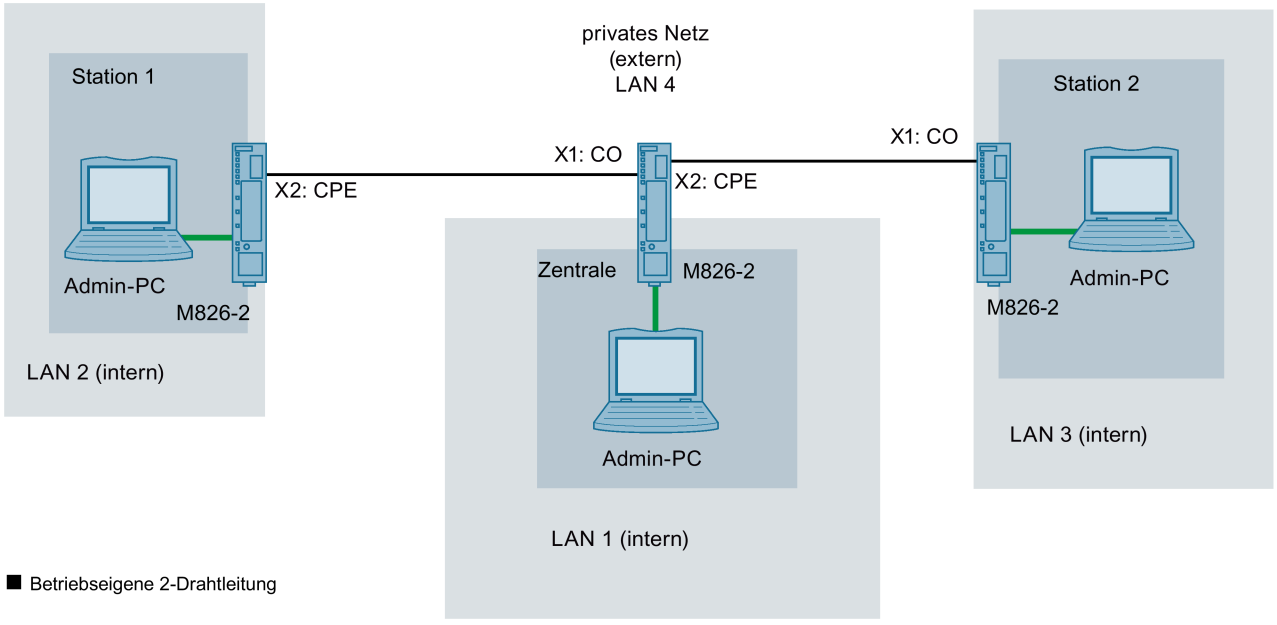
1.3.3 Im Routing-Modus

1.3.3.1 Prinzipielles Vorgehen

In diesem Beispiel sollen drei verschiedene IP-Subnetze über das SCALANCE M826 miteinander verbunden werden. Für diese Verbindung muss jeweils eine SHDSL-Schnittstelle eines Geräts in der Rolle CO sein und die andere in CPE. Da die SCALANCE M826 im Routing-Modus arbeiten, gibt es eine Unterteilung in externe und interne Netze. Somit liegen die SHDSL-Schnittstellen und die Ethernet-Schnittstellen in verschiedenen IP-Subnetzen.

In diesem Modus sind die Sicherheits-Funktionen (IPsec VPN, Firewall, NAT/NAPT) verfügbar.

Aufbau



Die Netzknoten sind in verschiedenen IP-Subnetzen.

Zentrale - Anschluss an SCALANCE M826

- In der Zentrale wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Zentrale
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Station 1 und 2 - Anschluss an SCALANCE M826

- In der Station wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des M826 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer der Station
- Anbindung an das private Netzwerk:
  - Kabelgebunden über die SHDSL-Schnittstelle des M826 an betriebseigene 2-Draht-Leitung.

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an SHDSL
  - 3x M876 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 3x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
- 3x PC die mit je einem M826 verbunden sind.
- PST ist auf dem PC installiert.

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen:

		Interface		IP-Adresse
Zentrale	M826	SHDSL (extern)	Vlan 2	192.168.184.2 255.255.255.0
		Ethernet (intern)	Vlan 1	192.168.100.1 255.255.255.0
	Admin-PC	Ethernet (intern)		192.168.100.20 255.255.255.0
Station 1	M826	SHDSL (extern)	Vlan 2	192.168.184.22 255.255.255.0
		Ethernet (intern)	Vlan 1	192.168.11.2 255.255.255.0
	Admin-PC	Ethernet (intern)		192.168.11.40 255.255.255.0
Station 2	M826	SHDSL (extern)	Vlan 2	192.168.184.42 255.255.255.0
		Ethernet (intern)	Vlan 1	192.168.50.2 255.255.255.0
	Admin-PC	Ethernet (intern)		192.168.50.40 255.255.255.0

Projektierungsschritte

1. SCALANCE M826 und Netzwerk einrichten (Seite 64).
2. SCALANCE M826 mit PST konfigurieren (Seite 65)
3. Das Web Based Management starten (Seite 66)
4. Am Web Based Management anmelden (Seite 69)
5. SCALANCE M826 konfigurieren.

   Die Schritte gelten für alle Geräte und unterscheiden sich nur in den Einstellungen.
   - Geräteinformationen festlegen (Seite 71)
   - Uhrzeit einstellen (Seite 72)
   - IP-Subnetze anlegen (Seite 74)
   - SHDSL konfigurieren (Seite 76)
   - Routen konfigurieren (Seite 77)
   - Zugriff erlauben (Seite 79)

1.3.3.2 SCALANCE M826 und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Vorgehensweise

1. Packen Sie zunächst das M826 aus und überprüfen Sie den unbeschädigten Zustand.
2. Montieren Sie die Spannungsversorgung.

   ⚠ WARNUNG

   Nur Sicherheitskleinspannung verwenden

   Das Gerät SCALANCE M826 ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

   Das Netzteil für die Versorgung des SCALANCE M826 muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.
3. Verdrahten Sie die M826, siehe Aufbau (Seite 62).
4. Schließen Sie das Gerät über die Ethernet-Ports an das lokale Netz an.
5. Schalten Sie das Gerät an. Nachdem Anschließen leuchtet die Fehler-LED (F) rot.
6. Schalten Sie jetzt den PC ein.

1.3.3.3 SCALANCE M826 mit PST konfigurieren

Voraussetzung

- Die IP-Adressen innerhalb des IP-Subnetzes sind eindeutig.

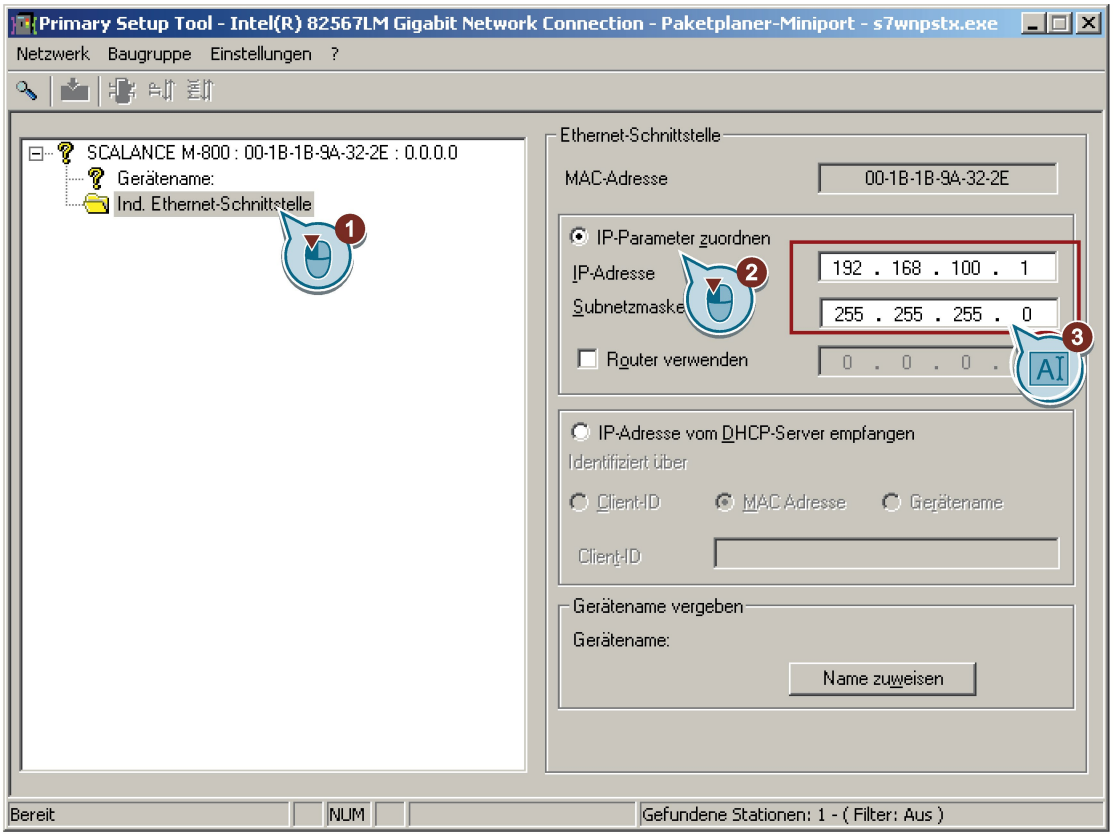
Vorgehenweise

1. Starten Sie das Primary Setup Tool unter "Start > SIMATIC > Primary Setup Tool".

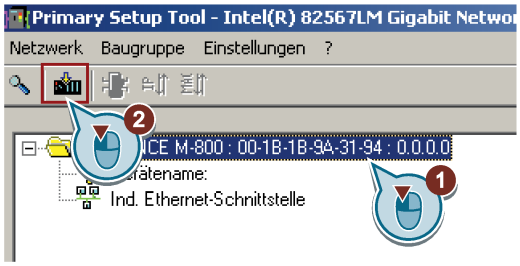
   Wenn am PC mehrere Netzwerkkarten eingebaut sind, wählen Sie unter "Einstellungen >Netzwerkkarte" den Netzwerk-Adapter, der mit M826 verbunden ist.

2. Klicken Sie in der Funktionsleiste auf die Lupe , um den Suchlauf zu starten. Nach dem Suchlauf wird das M826 im PST aufgelistet.

3. Tragen Sie die dem M826 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 62)" ein.



4. Übertragen Sie die IP-Adresse.



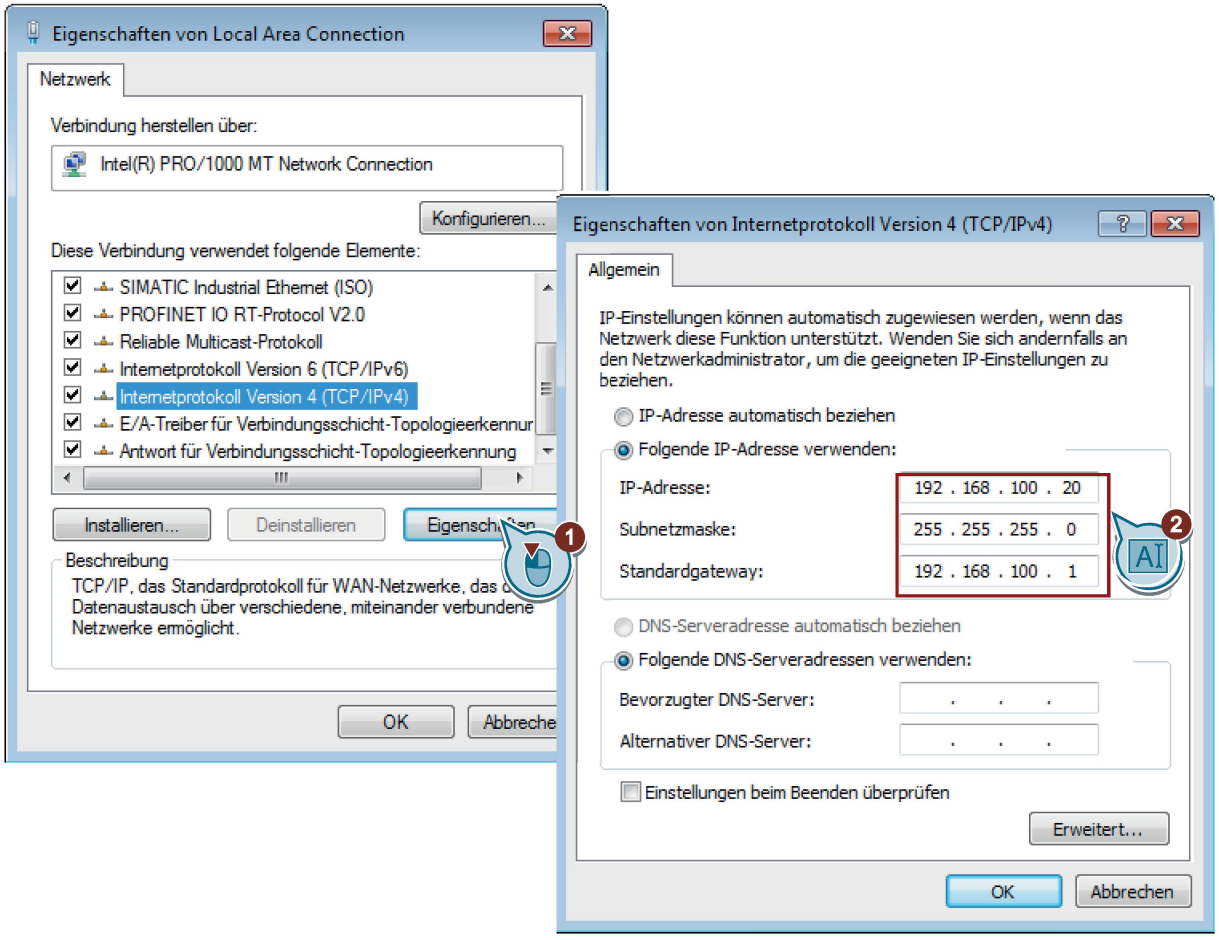
1.3.3.4 Das Web Based Management starten

Vorgehensweise

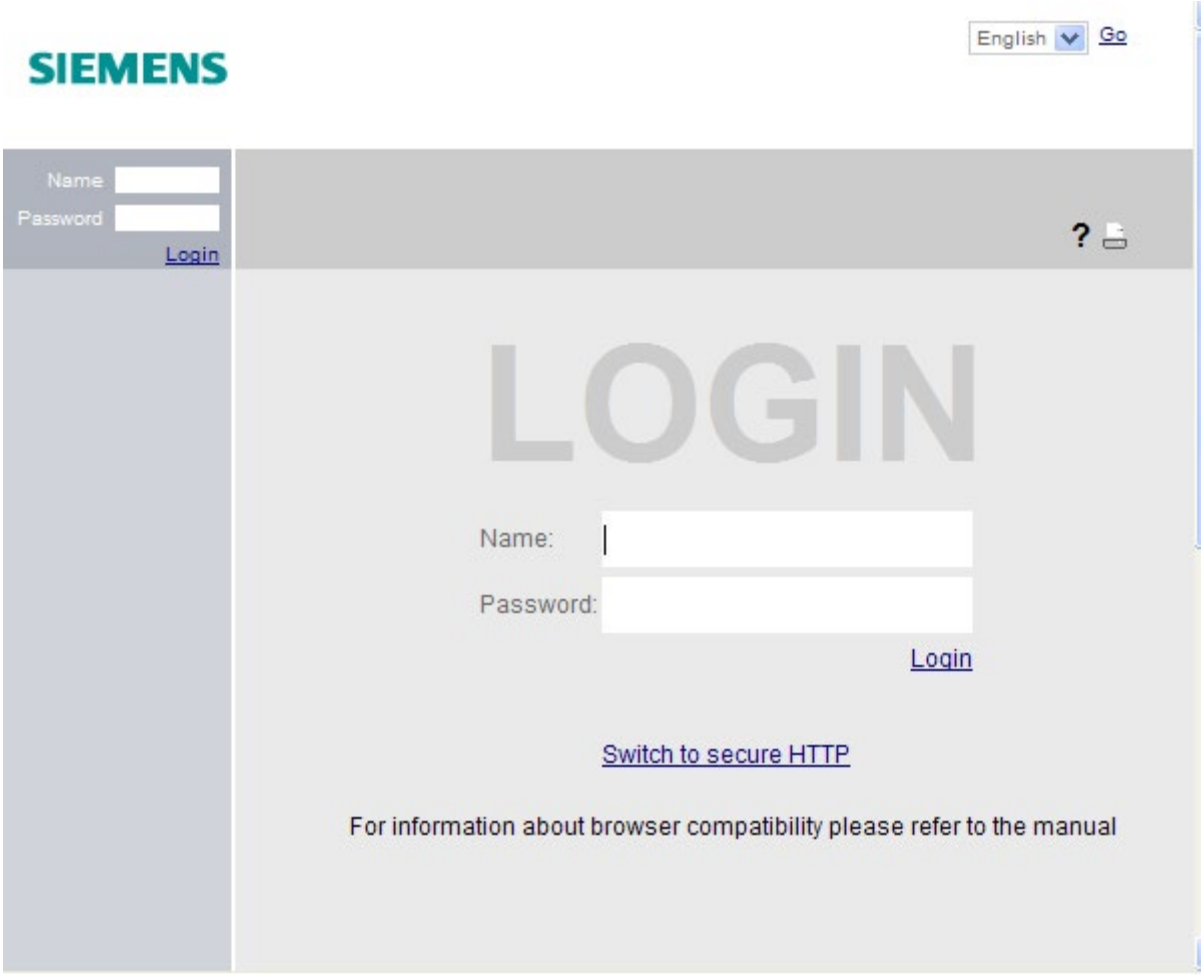
1. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".

4. Tragen Sie die dem Admin-PC zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 62)" ein.

   Als Standardgateway tragen Sie die interne IP-Adresse (Vlan 1) des SCALANCE M826 ein.



5. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
6. Tragen Sie im Adressfeld des Webbrowsers die dem M826 zugeordnete IP-Adresse (vlan 1) aus der Tabelle "Verwendete Einstellungen (Seite 62)" ein. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

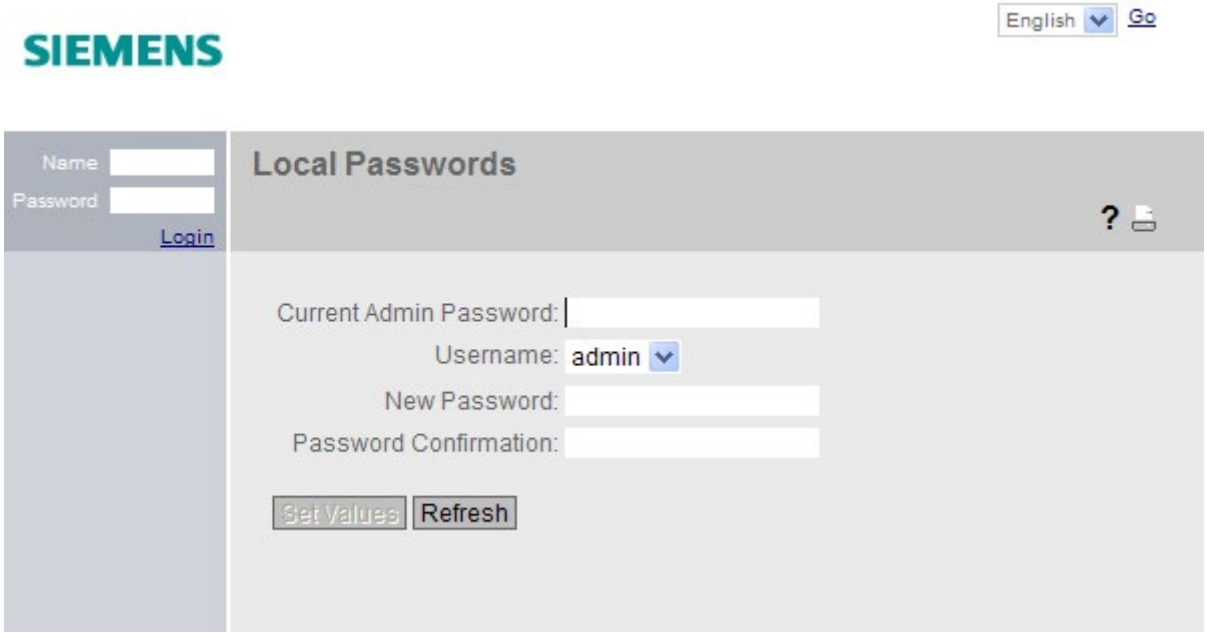


1.3.3.5 Am Web Based Management anmelden

Vorgehensweise

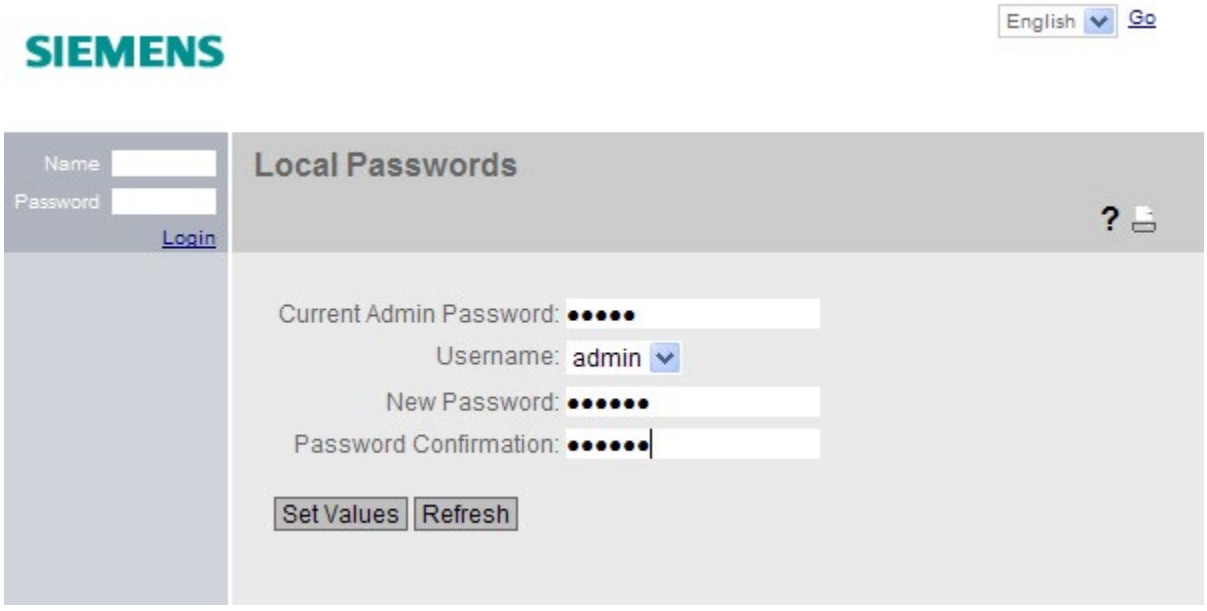
1. Melden Sie sich mit dem Benutzernamen "admin" und dem Passwort "admin" an. Sie werden aufgefordert, das Passwort zu ändern.

2. Bestätigen Sie den Dialog. Automatisch wird die WBM-Seite "Password" geöffnet.



3. Wählen Sie bei "Username" den Benutzer "admin" aus.
4. Tragen Sie bei "Current Admin Password" das Default-Passwort "admin" ein.
5. Legen Sie bei "New Password" das neue Passwort fest.

6. Wiederholen Sie bei "Password Confirmation" das Passwort, um es zu bestätigen. Beide Einträge müssen übereinstimmen.



7. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

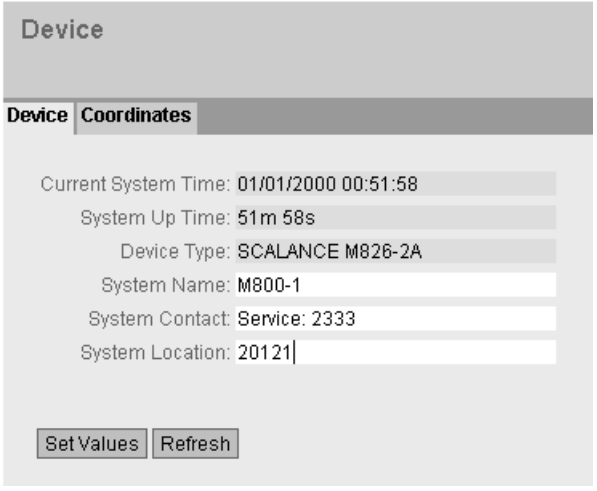
Das Passwort für den Benutzer "admin" ist geändert. Die Änderungen sind sofort wirksam.

1.3.3.6 Geräteinformationen festlegen

Zur besseren Identifikation der SCALANCE M826 legen Sie allgemeine Geräteinformationen fest.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "General" und im Inhaltsbereich auf das Register "Device".
2. Tragen Sie bei "System Name" einen Systemnamen für das Gerät ein, z. B. "M800-1" für die Zentrale und "M800-2" für die Außenstation.
3. Tragen Sie bei "System Contact" den für das Gerät zuständigen Ansprechpartner ein.
4. Tragen Sie bei "System Location" die Ortsbezeichnung des Aufstellungsorts ein, z.B. die Raumnummer.



5. Klicken Sie auf die Schaltfläche "Set Values".

Ergebnis

Die allgemeinen Geräteinformationen der SCALANCE M826 sind festgelegt.

1.3.3.7 Uhrzeit einstellen

Zur Überprüfung der zeitlichen Gültigkeit von Zertifikaten und für die Zeitstempel von Logbuch-Einträgen werden auf dem SCALANCE M-800 Datum und Uhrzeit geführt. Sie können die Systemzeit selbst manuell einstellen, oder Sie lassen sie mit einem Zeitserver automatisch synchronisieren. Für dieses Beispiel wird der Zeitserver über NTP konfiguriert.

Hinweis

Manuelle Zeiteinstellung - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die Uhrzeit auf Werkseinstellung zurückgesetzt wird, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie erneut die Systemzeit einstellen. Dadurch können Zertifikate ihre Gültigkeit verlieren.

Synchronisation über Zeitserver

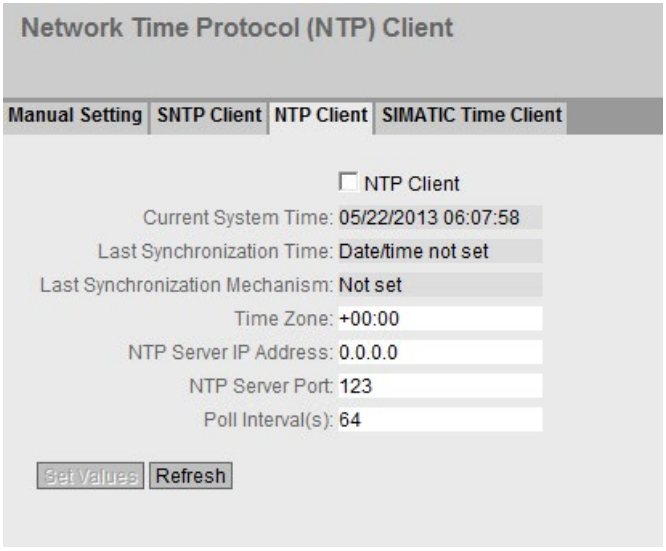
Die Synchronisation der Systemzeit über einen öffentlichen Zeitserver verursacht ein zusätzliches Datenaufkommen auf der Verbindung. Je nach Teilnehmervertrag sind damit erhöhte Kosten verbunden.

Voraussetzung

- Im lokalen Netz ist ein NTP-Server erreichbar.
- Die IP-Adresse des NTP-Servers ist bekannt.
  Für dieses Beispiel wird ein lokaler Zeitserver mit der IP-Adresse 192.168.100.87 verwendet.

Vorgehensweise

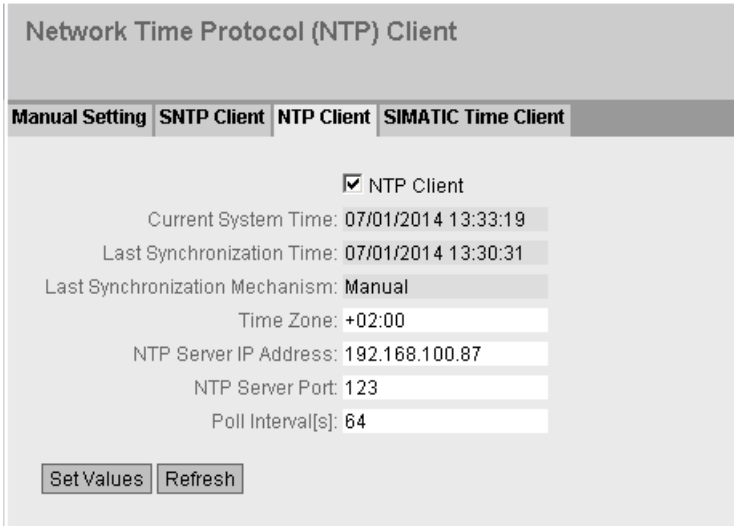
1. Klicken Sie im Navigationsbereich auf "System" > "System Time" und im Inhaltsbereich auf das Register "NTP Client".



2. Tragen Sie bei "Time Zone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Für mitteleuropäische Sommerzeit (MESZ) +02:00.
3. Tragen Sie bei "NTP Server IP Address" die IP-Adresse 192.168.100.87 ein. Die Eingabe der NTP-Adresse als Hostname ist nicht möglich.
4. Ändern Sie bei Bedarf den Port bei "NTP Server Port". Standardmäßig ist 123 eingestellt.
5. Tragen Sie bei "Poll Interval (s)" den Zeitabstand für die Synchronisation ein. Standardmäßig ist 64 eingestellt.
6. Aktivieren Sie "NTP Client".
7. Klicken Sie auf "Set Values".

Ergebnis

Die Systemzeit über NTP ist eingestellt. Klicken Sie auf "Refresh", um die WBM-Seite zu aktualisieren.



1.3.3.8 IP-Subnetz anlegen

Im Routing-Modus werden die Schnittstellen unterschiedlich behandelt.

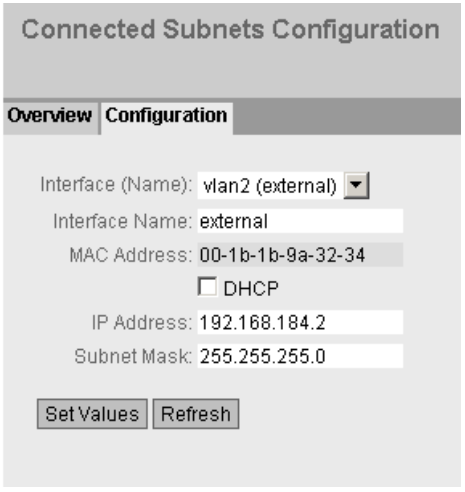
- Ethernet-Schnittstelle: Anbindung des internen IP-Subnetzes (vlan 1)
- SHDSL-Schnittstelle: Anbindung des externen IP-Subnetzes (vlan 2)

Die Ethernet-Schnittstelle bzw. das interne IP-Subnetz wurde bereits mit dem PST konfiguriert. Für dieses Konfigurationsbeispiel ist nur das IP-Subnetz für die SHDSL-Schnittstelle bzw. für das externe IP-Subnetz zu konfigurieren. Die Schritte sind bei allen Geräten durchzuführen.

Vorgehensweise

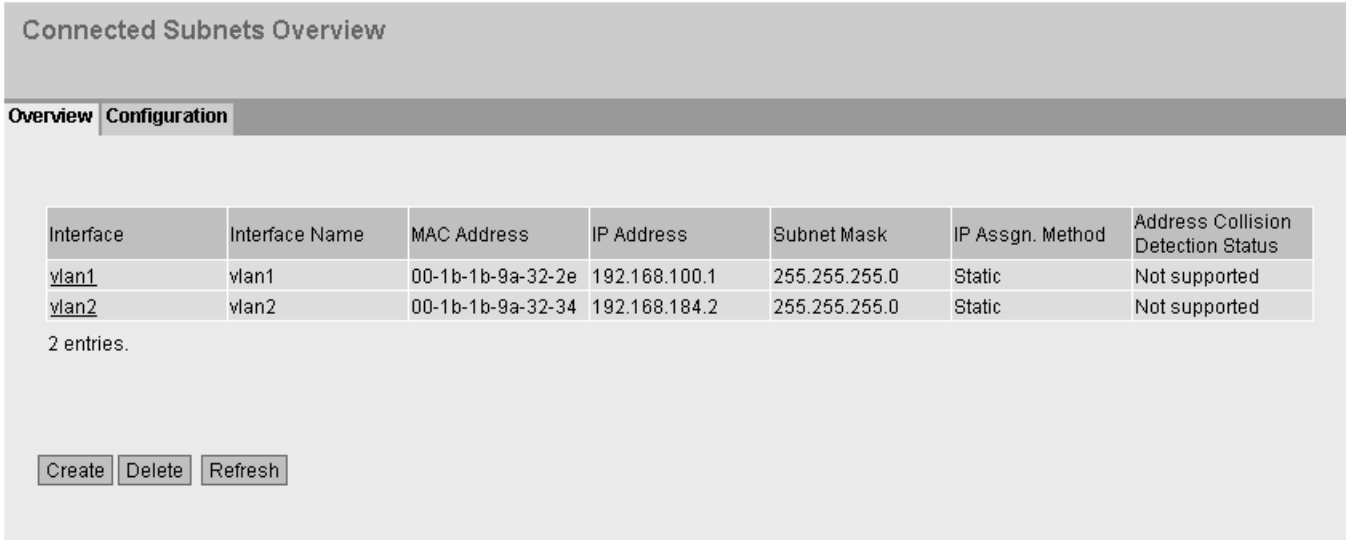
1. Klicken Sie im Navigationsbereich auf "Layer 3" > "Subnets" und im Inhaltsbereich auf das Register "Configuration".
2. Wählen Sie bei "Interface" die "vlan 2" aus.
3. Bei "Interface Name" können Sie einen Namen eingeben.

4. Tragen Sie die dem M826 zugeordneten Wert aus der Tabelle "Verwendete Einstellungen (Seite 62)" ein.
5. Klicken Sie auf "Set Values".



Ergebnis

Die IP-Subnetze sind angelegt. Die IP-Subnetze werden im Register "Overview" angezeigt.



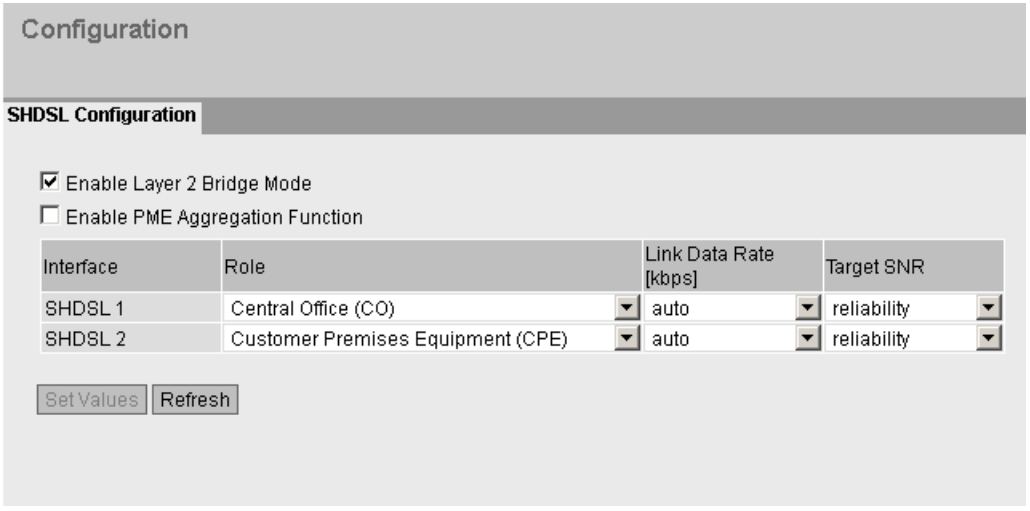
1.3.3.9 SHDSL konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Interfaces " > "SHDSL"
2. Legen Sie die Rolle der Schnittstellen fest

SHDSL 1 (X1)	Central Office (CO)
SHDSL 2 (X2)	Customer Premises Equipment (CPE)

3. Wählen Sie bei "Link Data Rate" "auto" und bei "Target SNR Ration" "reliability".
4. Klicken Sie auf "Set Values".



5. Deaktivieren Sie "Enable Layer2 Bridge Mode", um den Routing-Modus einzustellen. In diesem Modus sind die Sicherheits-Funktionen (IPsec VPN, Firewall, NAT/NAPT) wieder verfügbar.

Ergebnis

Die SHDSL-Verbindung ist eingerichtet. Die Geräte verhandeln die Verbindungsparameter aus. D.h. sie nehmen die Übertragungsrate, bei der zuverlässig die Daten gesendet und empfangen werden können. Detailliertere Informationen zur Verbindung erhalten Sie unter "Information" > "SHDSL".

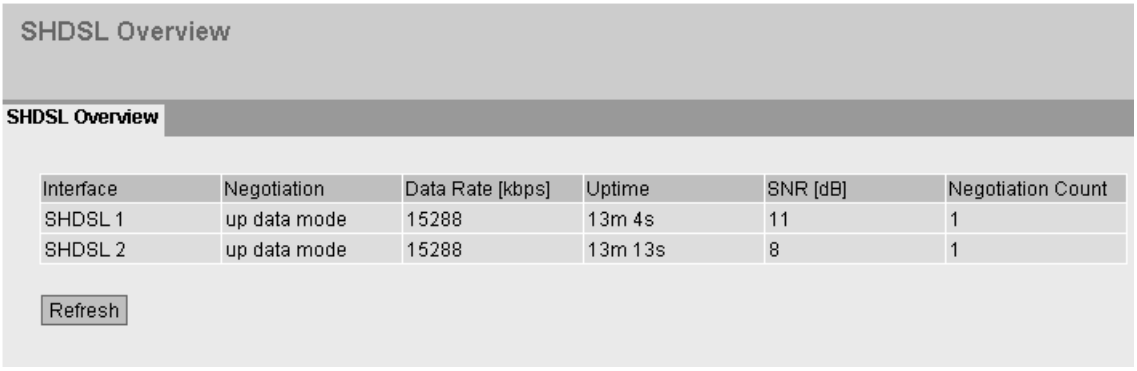


Bild 1-1 Übersicht M826 in der Zentrale

Über Firewall und IPsecVPN können Sie die Datenübertragung zusätzlich schützen.

1.3.3.10 Routen konfigurieren

Die Zentrale und die Stationen sind in verschiedenen IP-Subnetzen. Damit die Zentrale mit den Stationen kommunizieren kann, müssen im M826 die entsprechenden Routen angelegt werden.

M826 in der Zentrale: Routen konfigurieren

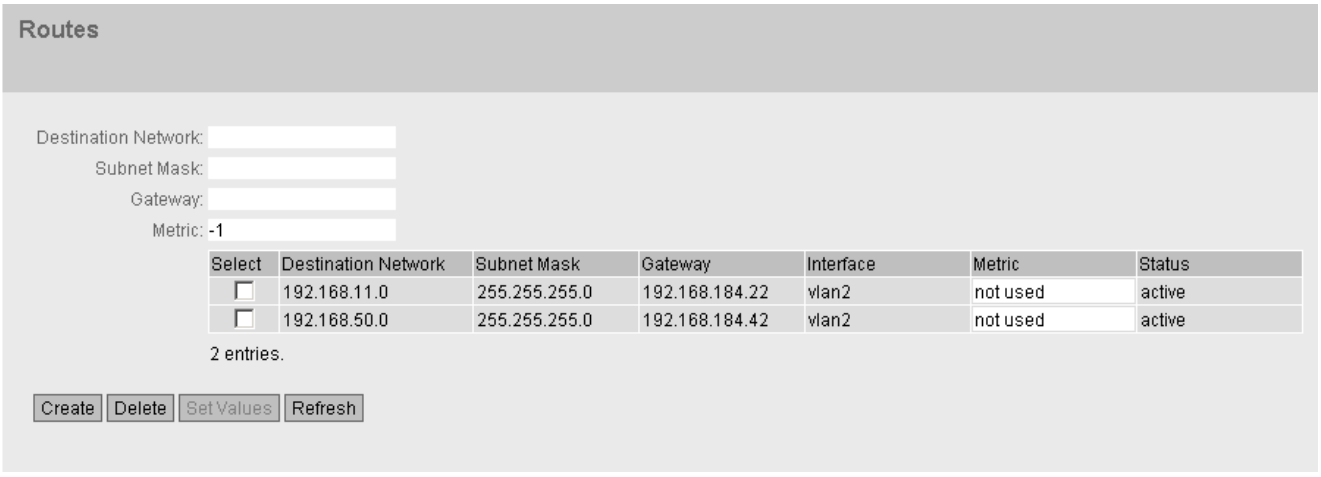
1. Klicken Sie im Navigationsbereich auf "Layer 3" > "Routes".
2. Konfigurieren Sie die Routen mit folgenden Einstellungen:
   - Route zur Station 1

Destination Network	192.168.11.0
Subnetmask	255.255.255.0
Gateway	192.168.184.22 externe IP-Adresse des M826 in der Station 1
Metric	-1

   - Route zur Station 2

Destination Network	192.168.50.0
Subnetmask	255.255.255.0
Gateway	192.168.184.42 externe IP-Adresse des M826 in der Station 2
Metric	-1

3. Wenn Sie die Werte eingetragen haben, klicken Sie auf "Create".
4. Zum Aktualisieren der Anzeige klicken Sie auf "Refresh".



M826 in den Stationen: Routen konfigurieren

1. Klicken Sie im Navigationsbereich auf "Layer 3" >"Routes".
2. Konfigurieren Sie die Route zur Zentrale mit folgenden Einstellungen:

Destination Network	192.168.100.0
Subnetmask	255.255.255.0
Gateway	192.168.184.2 externe IP-Adresse des M826 in der Zentrale
Metric	-1

3. Wenn Sie die Werte eingetragen haben, klicken Sie auf "Create".
4. Zum Aktualisieren der Anzeige klicken Sie auf "Refresh".

Ergebnis

Die Routen sind angelegt. Das SCALANCE M826 in der Zentrale kann mit den Stationen kommunizieren.

Mit der Ping-Funktion lässt sich die Kommunikationsverbindung testen. Ist z. B. vom Admin-PC in der Zentrale der Admin-PC in der Station 1 erreichbar.

1.3.3.11 Zugriff erlauben

Es gibt folgende Möglichkeiten den Zugriff zu erlauben:

- Global erlauben

  Hier greifen Sie auf einfache, vordefinierte Firewall-Regeln zurück. Die frei gegebenen Dienste sind für alle Teilnehmer an den entsprechenden Schnittstellen gültig. Für die angegebene Richtung wird der volle Zugriff erlaubt.

  – vlan1: Erlaubt den Zugrff vom internen Netz auf das Gerät

  – vlan2: Erlaubt den Zugriff vom externen Netz auf das Gerät

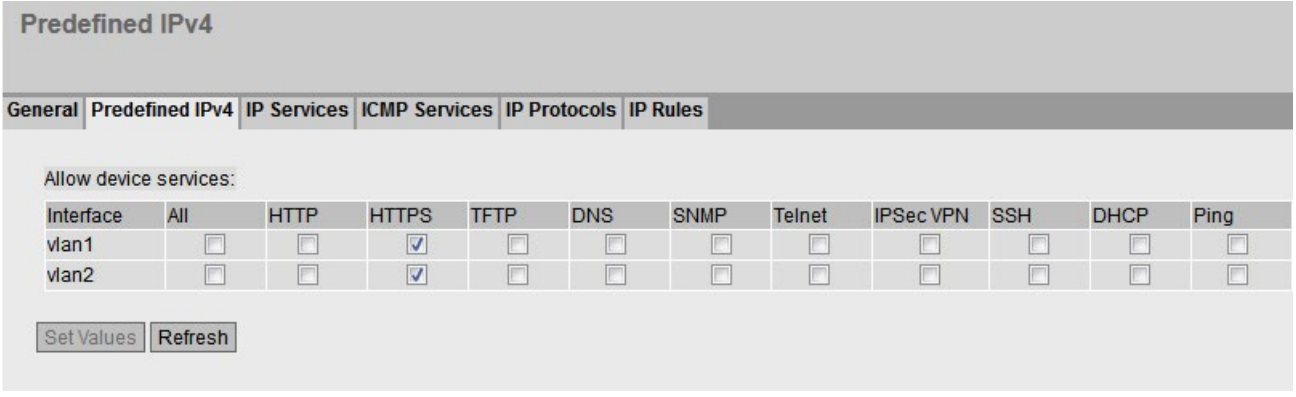
  Die Firewall-Regel für die Gegenrichtung wird mittels zustandsorientierte Paketüberprüfung (stateful packet inspection) erlaubt.

- Bestimmte Dienste erlauben

  Hier definieren Sie Firewall-Regeln, die für einen einzelnen Teilnehmer einzelne Dienste freischaltet oder für den Teilnehmer alle Dienste für den Zugriff auf die Station bzw. das Netz frei geben.
  In diesem Beispiel projektieren Sie die Firewall-Regel, die nur dem Gerät mit der IP-Adresse 192.168.100.20 den Zugriff auf Gerät erlaubt. Für den Zugriff wird der Dienst HTTP (TCP-Port 80) benötigt.

Beispiel 1: HTTPS-Zugriff global erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Aktivieren Sie bei "vlan 1" und "vlan 2" "HTTPS".
3. Klicken Sie auf "Set Values".



Beispiel 2: HTTPS-Zugriff einem bestimmten Gerät erlauben

Vordefinierte Firewall-Regel abschalten

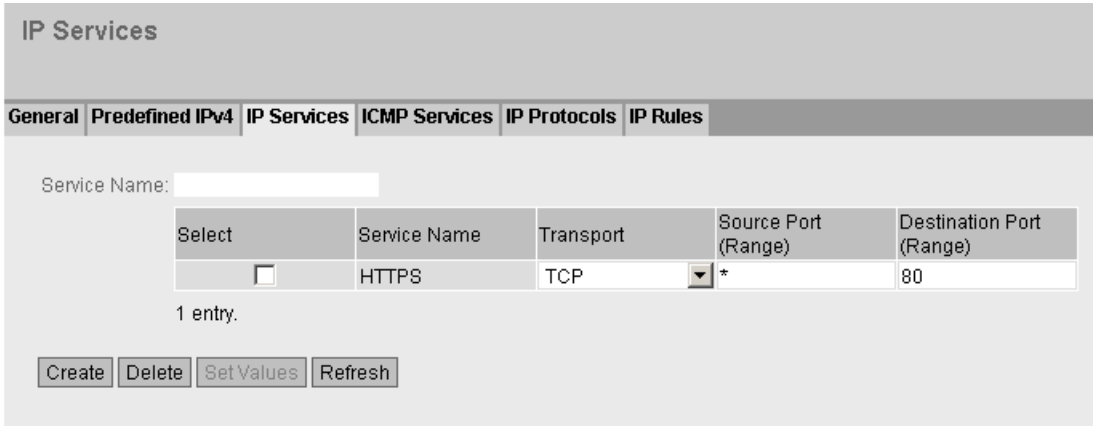
1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "Predefined IPv4".
2. Deaktivieren Sie alle Dienste.

IP-Dienst HTTPS anlegen

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Services".
2. Geben Sie bei "Service Name" z. B. "HTTPS" ein und klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
3. Konfigurieren Sie HTTPS mit folgenden Einstellungen:

Transport	TCP
Destination Port (Range)	80 (Standard-Port)

4. Klicken Sie auf "Set Values".



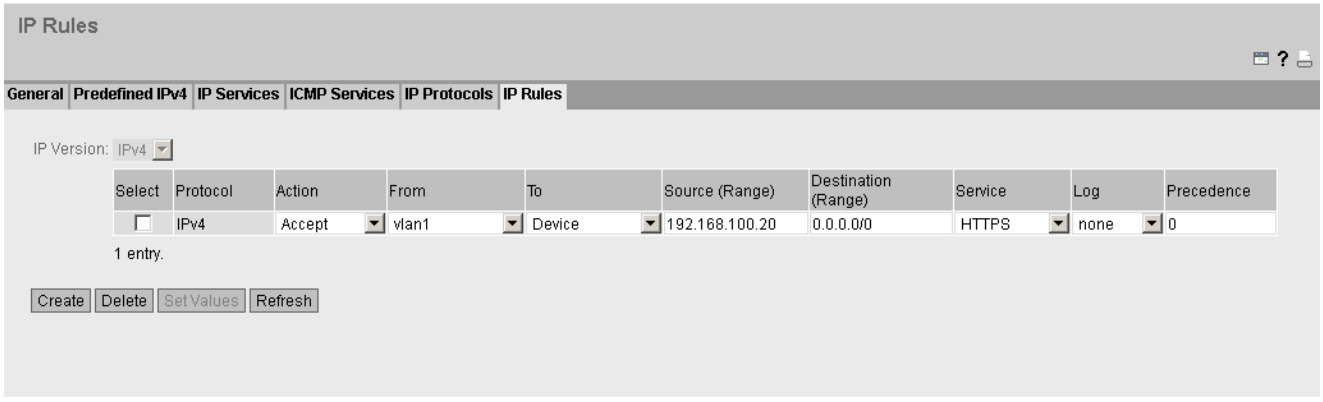
HTTPS-Zugriff nur einem bestimmten Gerät erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
2. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.

3. Konfigurieren Sie die Firewall-Regel für den angelegten HTTPS-Dienst mit folgenden Einstellungen:

Action	Accept
From	vlan1
To	Device
Source (Range)	192.168.100.20 (das gewünschte Gerät)
Destination (Range)	0.0.0.0/0 (alle Adressen)
Service	HTTPS

4. Klicken Sie auf "Set Values".



SCALANCE M-800 als DHCP Server

2

Wenn Sie das Gerät zum Verwalten von Netzwerkkonfiguration verwenden wollen, können Sie das Gerät als DHCP-Server einsetzen. Damit ist es möglich, den am internen Netz angeschlossenen Geräten automatisch IP-Adressen zuzuweisen.

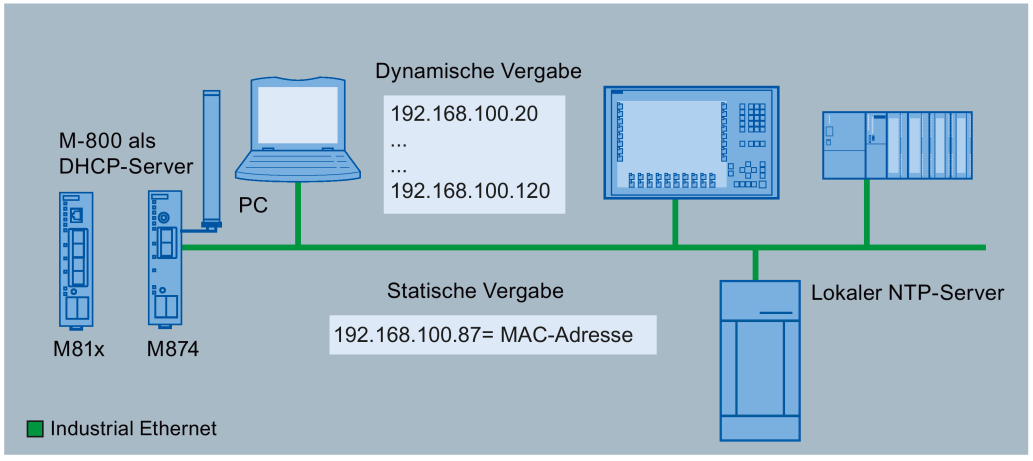
In diesem Beispiel werden die statische und die dynamische IP-Adressvergabe konfiguriert.

Hinweis

DHCP-Client und DHCP-Server

Das Gerät kann entweder nur ein DHCP-Client oder nur ein DHCP-Server sein.

SCALANCE M-800 als DHCP-Server



Erforderliche Geräte/Komponenten

- SCALANCE M-800 als DHCP-Server

  1x M874, 1x M812 oder M816 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmblockstecker
- 1x PC mit dem das SCALANCE M-800 verbunden ist.
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Verwendete Einstellung

Das SCALANCE M-800 erhält für die Beispielkonfiguration die folgende IP-Adresseinstellung:

- IP-Adresse 192.168.100.1
- Subnetzmaske: 255.255.255.0

Voraussetzung

- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

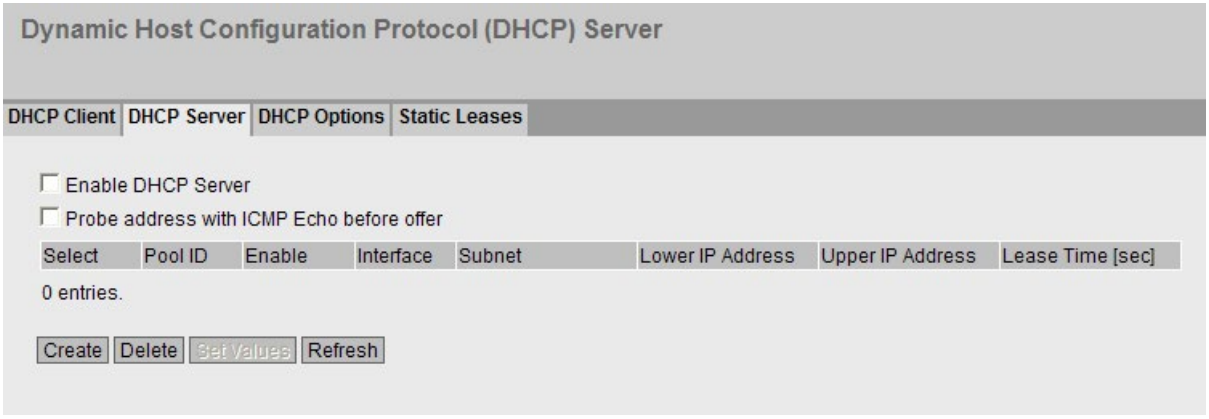
1. Dynamische IP-Adressvergabe projektieren (Seite 85)
2. DHCP-Optionen festlegen (Seite 87)
3. Statische IP-Adressvergabe projektieren (Seite 90)

2.1 Dynamische IP-Adressvergabe projektieren

Die Geräte, deren MAC-Adresse oder deren Client-ID nicht explizit angegeben wurde, erhalten eine beliebige IP-Adresse aus einem vorgegebenen Adressband.

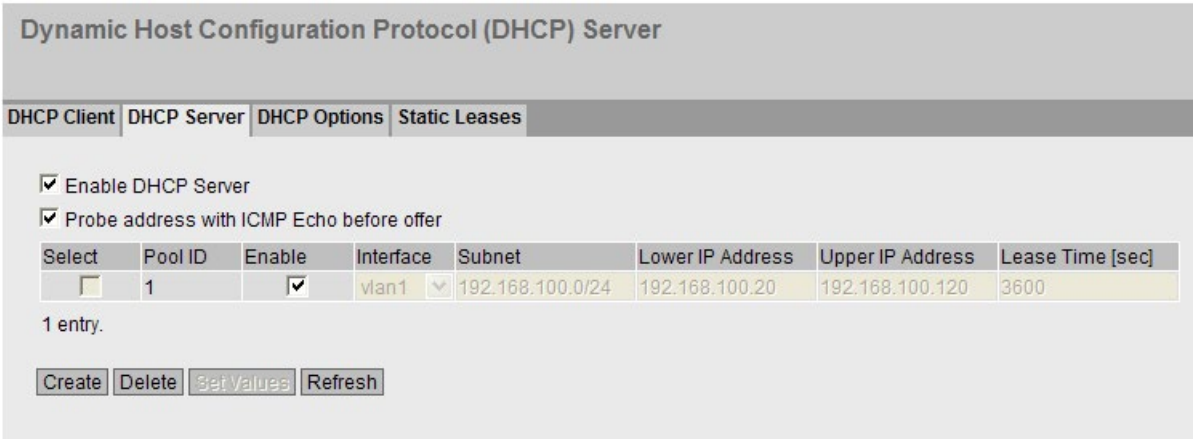
Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "DHCP" und im Inhaltsbereich auf das Register "DHCP Server".



2. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit einer eindeutigen Nummer (Pool ID) angelegt.
3. Tragen Sie bei "Subnet" den Netzadressbereich. Da das verwendete Gerät als Gateway und als DNS-Relay eingesetzt wird, muss die IP-Adresse 192.168.100.1 in den Netzadressbereich gehören. In diesem Beispiel wird die Netzadresse: 192.168.100.0/24 (= 192.168.100.0 / 255.255.255.0) verwendet.
4. Tragen Sie bei "Lower IP Address" die IP-Adresse 192.168.100.20 ein, die den Anfang des dynamischen Adressbands festlegt und im Netzadressbereich liegt.
5. Tragen Sie bei "Upper IP Address" die IP-Adresse 192.168.100.120 ein, die das Ende des dynamischen Adressbands festlegt und im Netzadressbereich liegt.

6. Aktivieren Sie Folgendes:
   - "Enable", um das Adressband zu verwenden
   - "Probe address with ICMP Echo before offer", um die ping-Funktion zu aktivieren. Mit dem ping prüft der DHCP-Server, ob die IP-Adresse schon vergeben ist.
   - "Enable DHCP Server", um den DHCP-Server zu aktivieren.
7. Klicken Sie auf "Set Values".



Ergebnis

Der DHCP-Server kann bis zu 100 IP-Adressen aus einem vorgegebenen Adressband vergeben. Vorausgesetzt, die angeschlossenen Geräte sind so konfiguriert, dass diese die IP-Adresse von einem DHCP-Server beziehen.

2.2 DHCP-Optionen festlegen

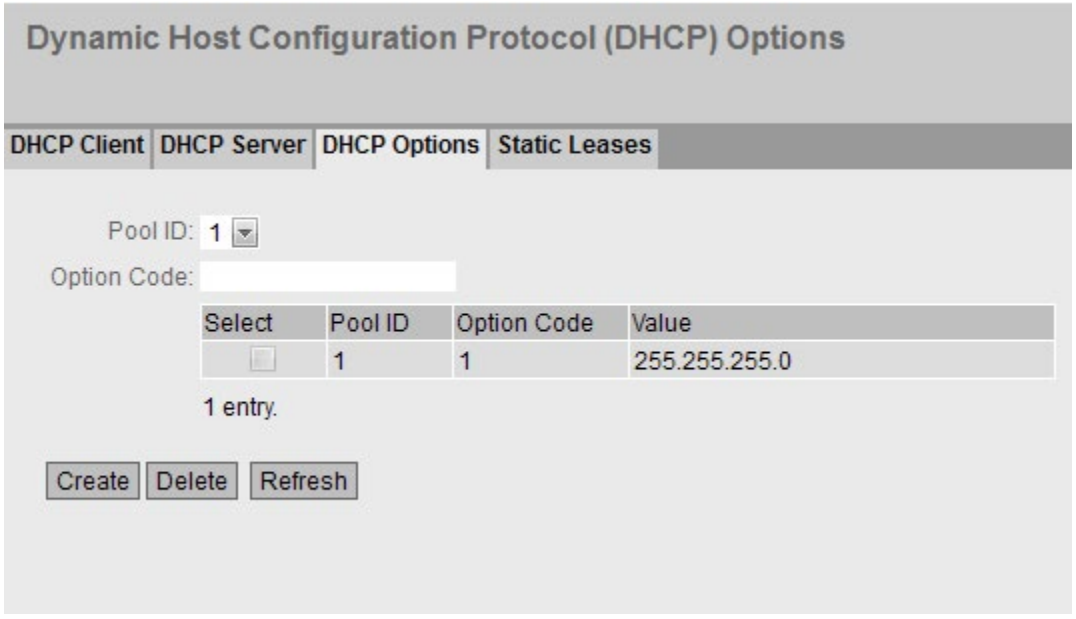
Über DHCP-Optionen lassen sich weitere Informationen an den DHCP-Client übermitteln. Die verschiedenen DHCP-Optionen sind im RFC 2132 definiert.

In diesem Beispiel werden folgende DHCP-Optionen angelegt.

DHCP-Option		Enthaltene Information
1	Netzmaske	Subnetzmaske passend zur IP-Adresse Für dieses Beispiel ist die Subnetzmaske: 255.255.255.0
3	Standard-Gateway	IP-Adresse des Standard-Gateways Ohne diese Information bekommt der DHCP-Client nur eine IP-Adresse vom DHCP-Server zugewiesen und er kann nur mit den Teilnehmern im internen Netz kommunizieren.
6	DNS-Server	IP-Adresse des DNS-Servers Ohne diese Information bekommt der DHCP-Client nicht automatisch einen DNS-Server zugeteilt. Um eine Namensauflösung zu ermöglichen, muss dem DHCP-Client ein DNS-Server bekannt sein. Dieser kann auch manuell konfiguriert werden.
42	NTP-Server	IP-Adresse des NTP-Servers. In diesem Beispiel wird die IP-Adresse des NTP-Servers (192.168.100.87) den DHCP-Clients mitgeteilt. Die IP-Adresse wird in hexadezimaler Schreibweise eingegeben. Die IP-Adresse 192.168.100.87 entspricht "C0A86457". Damit der NTP-Server immer unter dieser IP-Adresse zu erreichen ist, wird die IP-Adresse der MAC-Adresse zugeordnet, siehe Kapitel "Statische IP-Adressvergabe projektieren (Seite 90)".

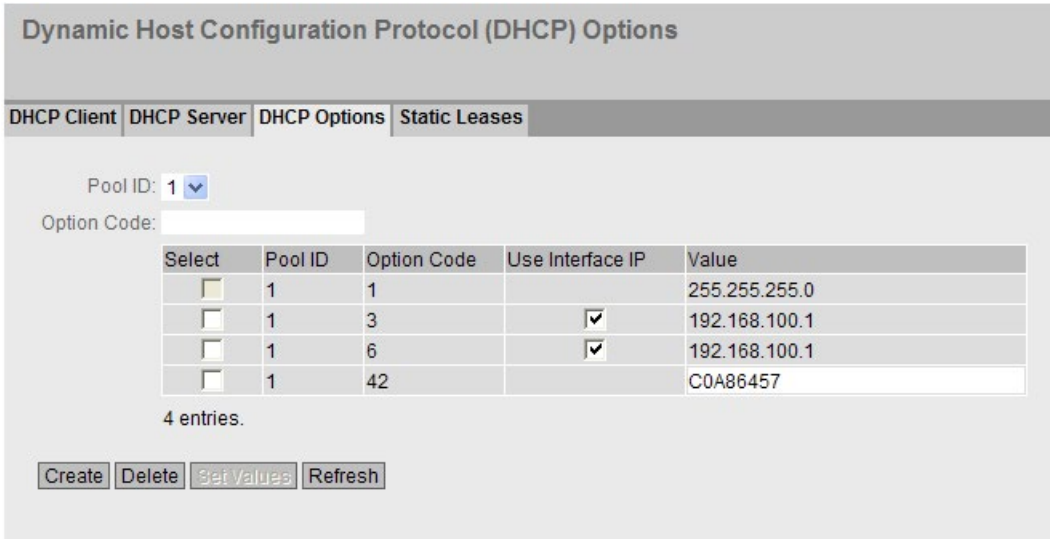
Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "DHCP" und im Inhaltsbereich auf das Register "DHCP Options".



2. Wählen Sie bei "Pool ID" die "1" aus. Tragen Sie bei "Option Code" "1" ein.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt. Automatisch wird die Subnetzmaske 255.255.255.0 eingetragen.
4. Klicken Sie auf "Set Values".
5. Tragen Sie bei "Option Code" "3" ein. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
6. Da das verwendete Gerät als Gateway eingesetzt wird, aktivieren Sie "Use Interface IP". Klicken Sie auf "Set Values". Als Wert wird automatisch die IP-Adresse des Geräts eingetragen.
7. Tragen Sie bei "Option Code" "6" ein. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
8. Da das verwendete Gerät als DNS-Relay eingesetzt wird, aktivieren Sie "Use Interface IP". Klicken Sie auf "Set Values". Als Wert wird automatisch die IP-Adresse des Geräts eingetragen.
9. Tragen Sie bei "Option Code" "42" ein.
10. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
11. Tragen Sie bei "Set Values" die IP-Adresse des NTP-Servers in hexadezimaler Schreibweise ein.

Ergebnis



Die DHCP-Optionen sind konfiguriert. Wenn ein DHCP-Client eine IP-Adresse anfordert, erhält dieser zusätzlich zur Host-IP-Adresse die Informationen, die in den DHCP-Optionen hinterlegt sind.

2.3 Statische IP-Adressvergabe projektieren

Für die Teilnehmer im dauernden Betrieb ist die statische IP-Adresszuweisung vorzuziehen, z. B. für einen lokalen NTP-Server. Die IP-Adresse des NTP-Servers wird in der DHCP-Option verwendet.

Solange der NTP-Server unter der gleichen IP-Adresse erreichbar ist, funktioniert die DHCP-Option. Wenn sich die IP-Adresse ändert, enthält die DHCP-Option eine fehlerhafte Information.

Für das Beispiel wird der MAC-Adresse des NTP-Servers die IP-Adresse zugeordnet. Damit erhält der NTP-Server immer die gleiche IP-Adresse.

Der NTP-Server ist in dieser Beispielkonfiguration unter folgender IP-Adresseinstellung erreichbar:

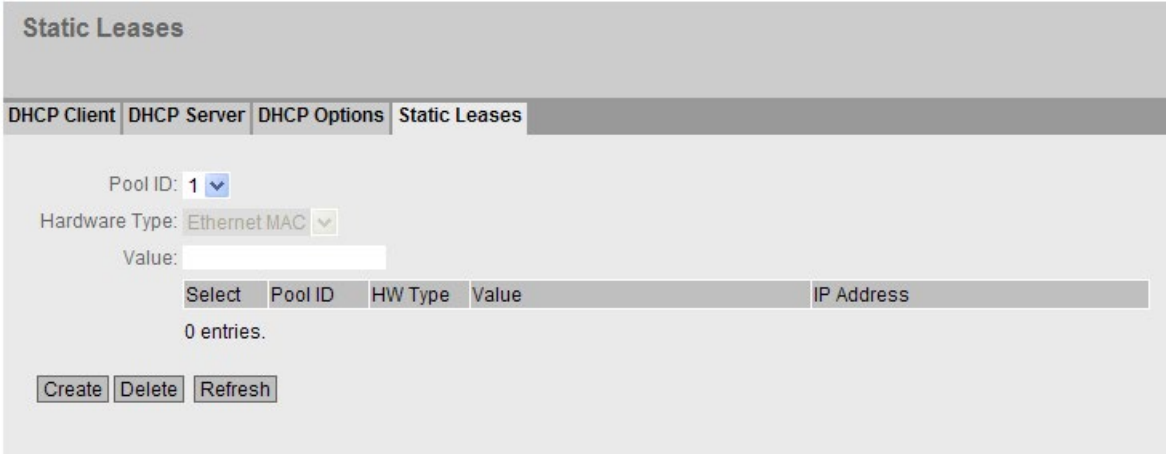
IP-Adresse	Subnetzmaske
192.168.100.87	255.255.255.0

Voraussetzung

- Der NTP-Server bezieht die IP-Adresse von einem DHCP-Server und die Identifikation erfolgt über die MAC-Adresse.

Vorgehensweise

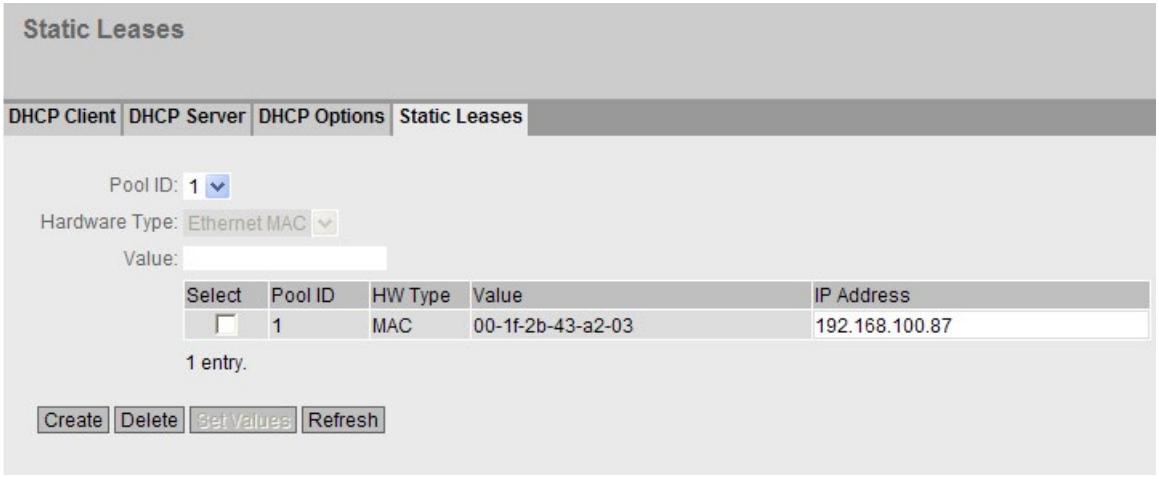
1. Klicken Sie im Navigationsbereich auf "System" > "DHCP" und im Inhaltsbereich auf das Register "Static Leases".



2. Wählen Sie bei "Pool ID" die "1" aus.
3. Wählen Sie bei "Hardware Type" "Ethernet MAC" aus.
4. Tragen Sie bei "Client ID" die MAC-Adresse des NTP-Servers ein.
5. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
6. Tragen Sie bei "IP Address" die IP-Adresse des NTP-Servers ein.
7. Klicken Sie auf "Set Values".

Ergebnis

Der NTP-Server erhält immer die IP-Adresse 192.168.100.87.



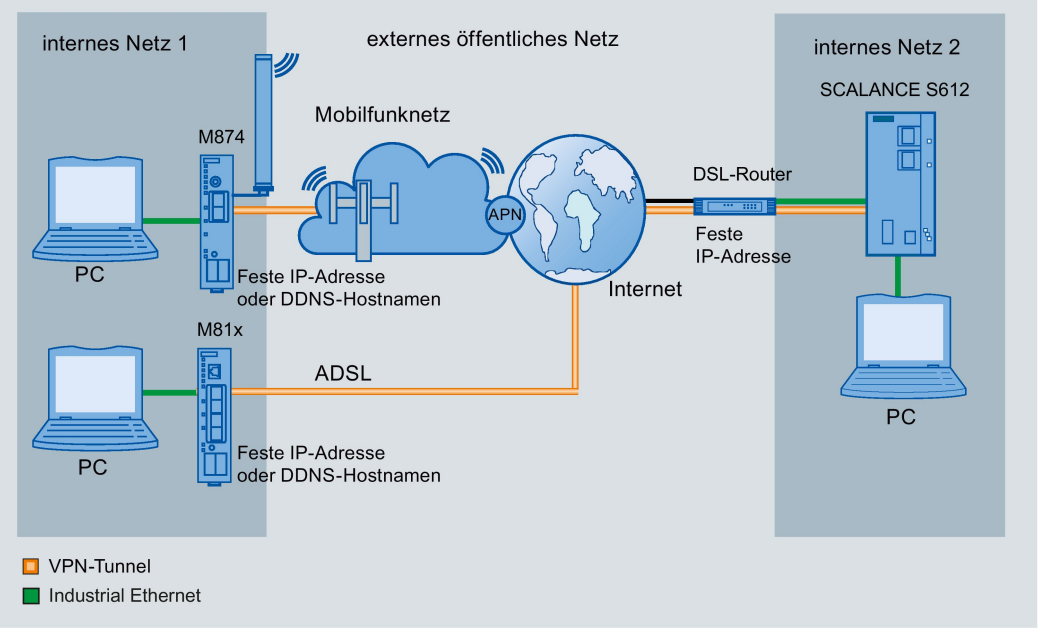
VPN-Tunnel zwischen SCALANCE M-800 und S612 3

3.1 Prinzipielles Vorgehen

In diesen Beispielen wird ein gesicherter VPN-Tunnel zwischen einem SCALANCE M-800 und einem SCALANCE S projektiert.

- Beispiel 1: Gesicherter VPN-Tunnel mit PreShared Keys (PSK)
- Beispiel 2: Gesicherter VPN-Tunnel mit Zertifikaten

Aufbau



Internes Netz 1 - Anschluss an SCALANCE M-800

- Im internen Netz wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des SCALANCE M-800 angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer des internen Netzwerks
  - M-800: SCALANCE M-Modul zum Schutz des internen Netzwerks
- Anbindung an das externe, öffentliche Netzwerk:
  - Drahtlos über die Antenne des M874 an das Mobilfunknetz.
  - Kabelgebunden über die RJ45-Buchse des M81x an ADSL.

Internes Netz 2 - Anschluss an einen internen Port des SCALANCE S

- Im internen Netz wird im Testaufbau der Netzknoten jeweils durch einen PC realisiert, der an den internen Port des Security-Moduls angeschlossen ist.
  - PC: repräsentiert einen Teilnehmer des internen Netzwerks
  - S612: Security-Modul zum Schutz des internen Netzwerks
- Anbindung an das externe, öffentliche Netzwerk über DSL-Router

  Der Zugriff auf das Internet erfolgt über ein DSL-Modem bzw. einen DSL-Router, welche an den externen Port des Security-Moduls angeschlossen wird.

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an das Mobilfunknetz
  - 1x M874 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - 1x geeignete Antenne
  - 1x SIM-Karte ihres Mobilfunkanbieters. Die entsprechenden Dienste z. B. Internet sind freigeschaltet.
- Anbindung an ADSL
  - 1x M812 oder 1x M816 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - ADSL-Zugang ist freigeschaltet
- 1x SCALANCE S612, (zusätzlich optional: eine entsprechend montierte Hutschiene mit Montagematerial)
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
- 1x PC mit dem das SCALANCE M-800 verbunden ist.
- 1x PC mit dem das SCALANCE S612 verbunden und auf dem das Projektierungswerkzeug "Security Configuration Tool" installiert ist.
- 1x DSL-Modem oder DSL-Router
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen

		interne Adresse	externe Adresse
Internes Netz 1	M-800	192.168.100.1 255.255.255.0	Feste IP-Adresse, z. B. 90.90.90.90 Providerabhängig Alternativ kann auch der DDNS-Hostname verwendet werden.
	Admin-PC	192.168.100.20 255.255.255.0	
Internes Netz 2	DSL-Router	192.168.184.254 255.255.255.0	Feste IP-Adresse (WAN-IP-Adresse), z. B. 91.19.6.84
	S612	interner Port 192.168.11.2 255.255.255.0	externer Port 192.168.184.2 255.255.255.0
	PC	192.168.11.100 255.255.255.0	

Voraussetzung

- SCALANCE S612 ist über den DSL-Router mit dem Internet verbunden.

  Im DSL-Router muss das PORT-Forwarding so eingestellt werden, dass die UDP-Pakete vom Internet, welche an die Ports 500 und 4500 des Routers adressiert sind, an die Ports 500 und 4500 des angeschlossenen SCALANCE S 612 (passives Modul) gesendet werden.
- Das SCALANCE M-800 ist mit dem WAN verbunden, siehe "SCALANCE M-800 mit dem WAN verbinden (Seite 11)".
- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

Beispiel 1: Gesicherter VPN-Tunnel mit PSK

VPN-Tunnel mit dem SCT V3.x konfigurieren

1. Projekt und Module anlegen (Seite 97)
2. Tunnelverbindung projektieren (Seite 100)
3. Eigenschaften des S612 konfigurieren (Seite 102)
4. Konfiguration in S612 laden und M-800-Konfiguration abspeichern (Seite 103)

VPN-Tunnel mit dem SCT V4.x konfigurieren

1. Projekt und Module anlegen (Seite 105)
2. Tunnelverbindung projektieren (Seite 108)

3. Eigenschaften des S612 konfigurieren (Seite 110)
4. Konfiguration in S612 laden und M-800-Konfiguration abspeichern (Seite 111)

Das SCALANCE M-800 konfigurieren

1. VPN aktivieren (Seite 112)
2. VPN-Gegenstelle konfigurieren (Seite 113)
3. VPN-Verbindung konfigurieren (Seite 114)
4. VPN-Authentifizierung konfigurieren (Seite 115)
5. Phase 1 und Phase 2 konfigurieren (Seite 116)
6. VPN-Verbindung aufbauen (Seite 117)

Beispiel 2: Gesicherter VPN-Tunnel mit Zertifikaten

VPN-Tunnel mit dem SCT V3.x konfigurieren

1. Projekt und Module anlegen (Seite 119)
2. Tunnelverbindung projektieren (Seite 122)
3. Eigenschaften des S612 konfigurieren (Seite 123)
4. Konfiguration in S612 laden und M-800-Konfiguration abspeichern (Seite 125)

VPN-Tunnel mit dem SCT V4.x konfigurieren

1. Projekt und Module anlegen (Seite 127)
2. Tunnelverbindung projektieren (Seite 130)
3. Eigenschaften des S612 konfigurieren (Seite 132)
4. Konfiguration in S612 laden und M-800-Konfiguration abspeichern (Seite 133)

Das SCALANCE M-800 konfigurieren

1. Zertifikat laden (Seite 134)
2. VPN aktivieren (Seite 136)
3. VPN-Gegenstelle konfigurieren (Seite 137)
4. VPN-Verbindung konfigurieren (Seite 138)
5. VPN-Authentifizierung konfigurieren (Seite 139)
6. Phase 1 und Phase 2 konfigurieren (Seite 139)
7. VPN-Verbindung aufbauen (Seite 141)

3.2 Gesicherter VPN-Tunnel mit PSK

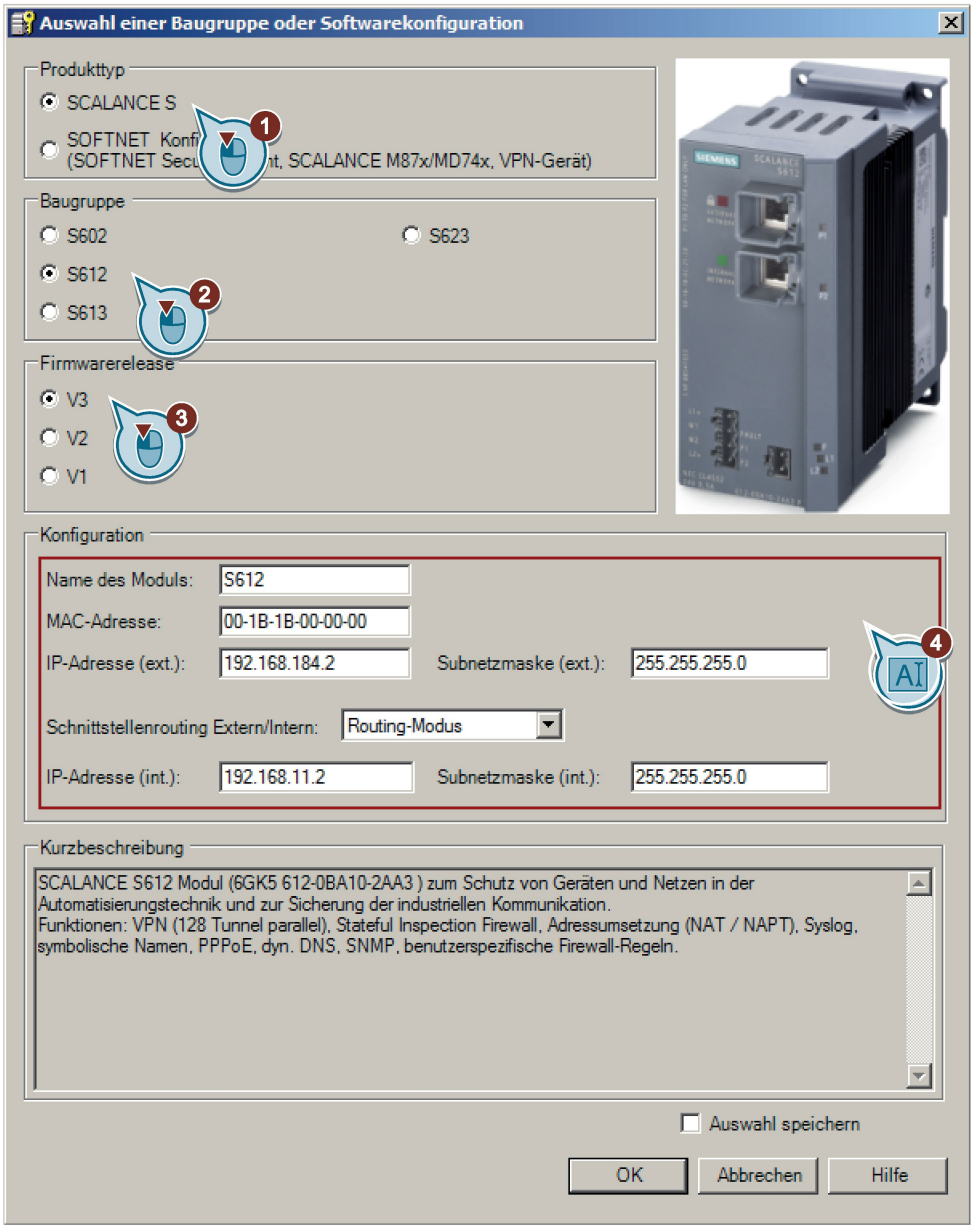
3.2.1 VPN-Tunnel mit dem SCT V3.x konfigurieren

3.2.1.1 Projekt und Module anlegen

Vorgehensweise

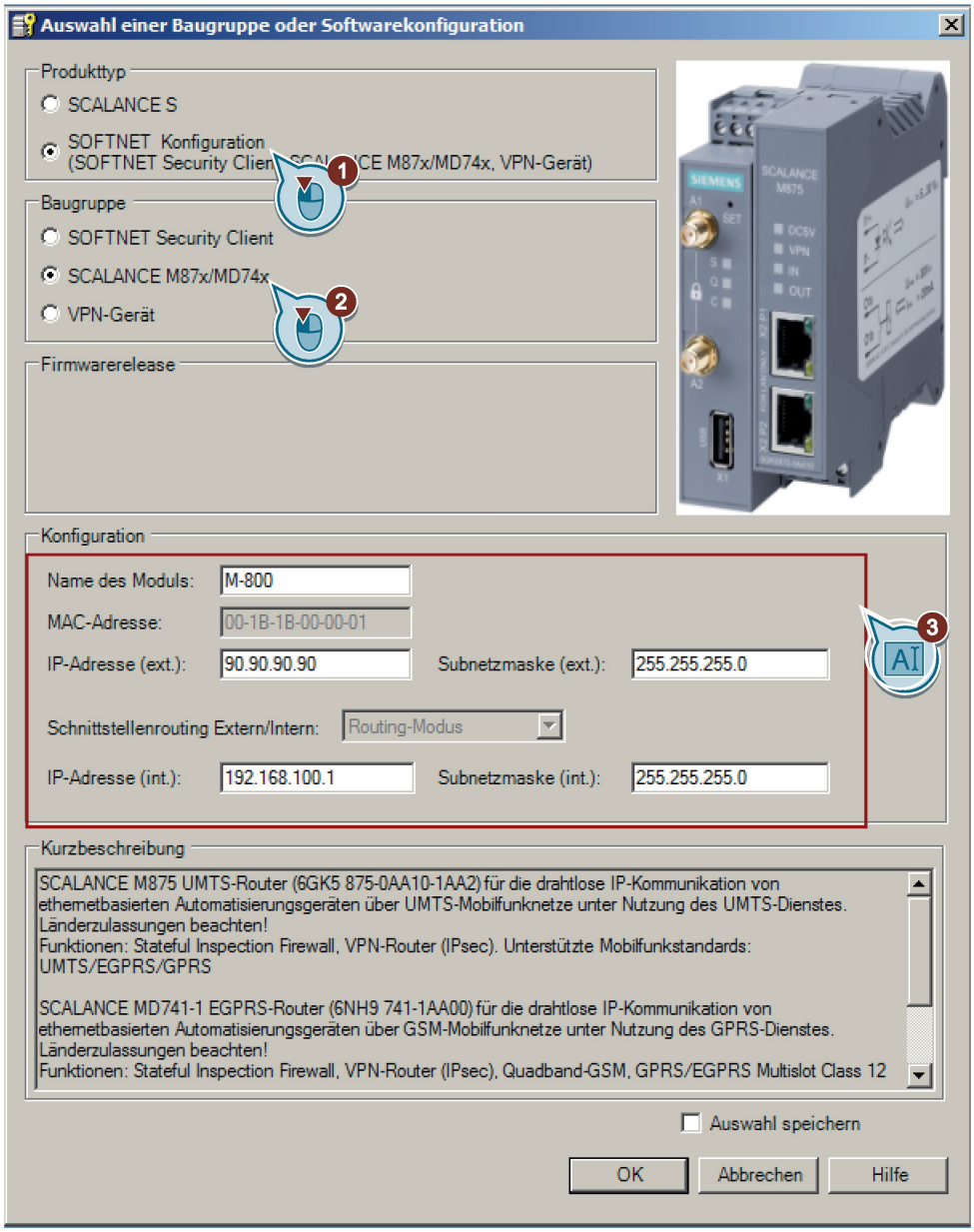
1. Starten Sie die Projektierungssoftware Security Configuration Tool V3.x auf dem PC.
2. Wählen Sie den Menübefehl "Projekt" > "Neu".
3. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an. Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
4. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt und der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" wird geöffnet.

5. Tragen Sie die dem S612 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein. Tragen Sie zusätzlich die MAC-Adresse ein, die auf der Frontseite des Security-Moduls aufgedruckt ist



6. Schließen Sie den Dialog mit "OK".
7. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Modul" ein zweites Modul

8. Tragen Sie die dem M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein.



9. Schließen Sie den Dialog mit "OK".

Ergebnis

Das Security-Modul S612 und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

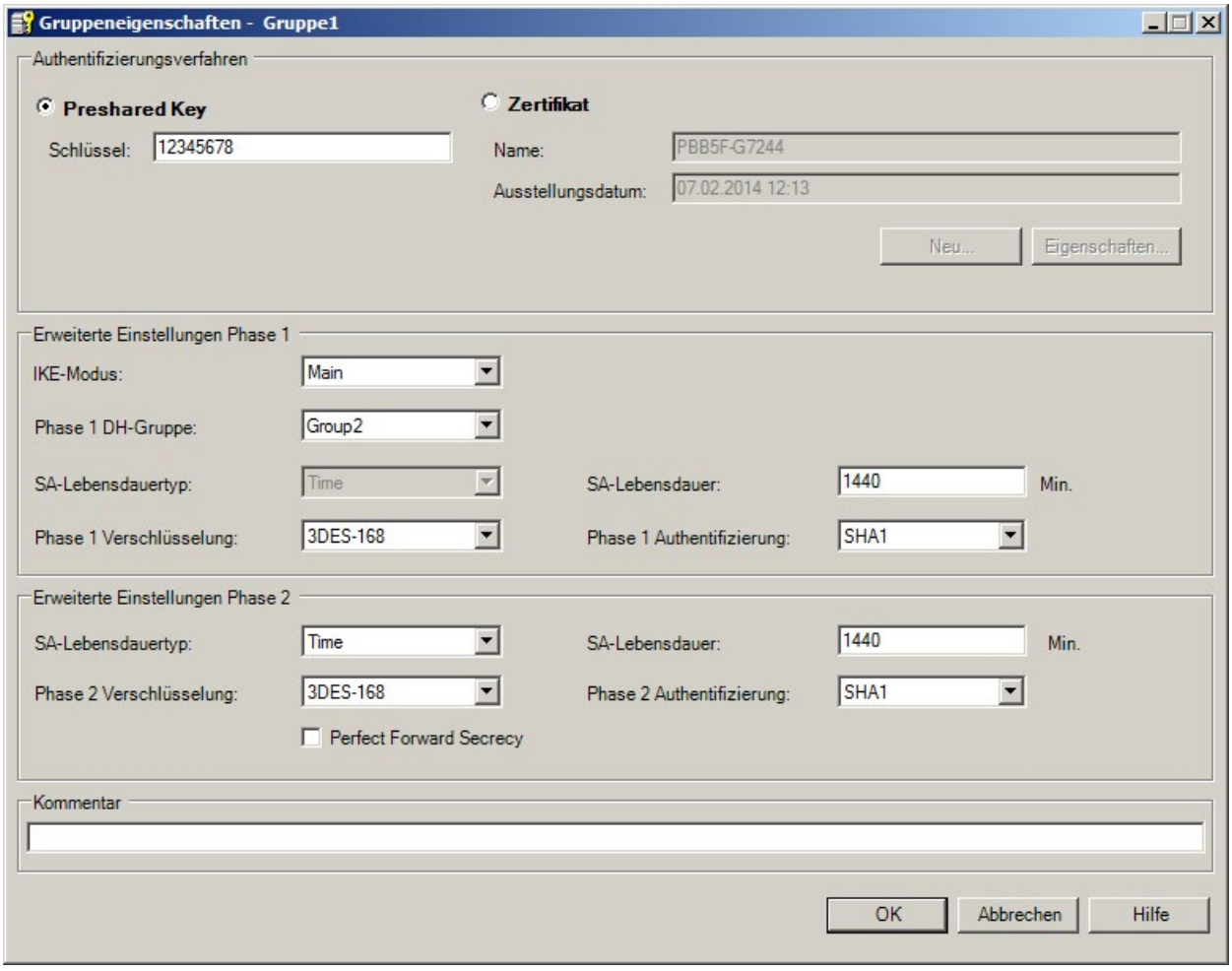
3.2.1.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M-800 und das S612 der gleichen VPN-Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das M-800 und den S612. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.

5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen.
6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

Ergebnis

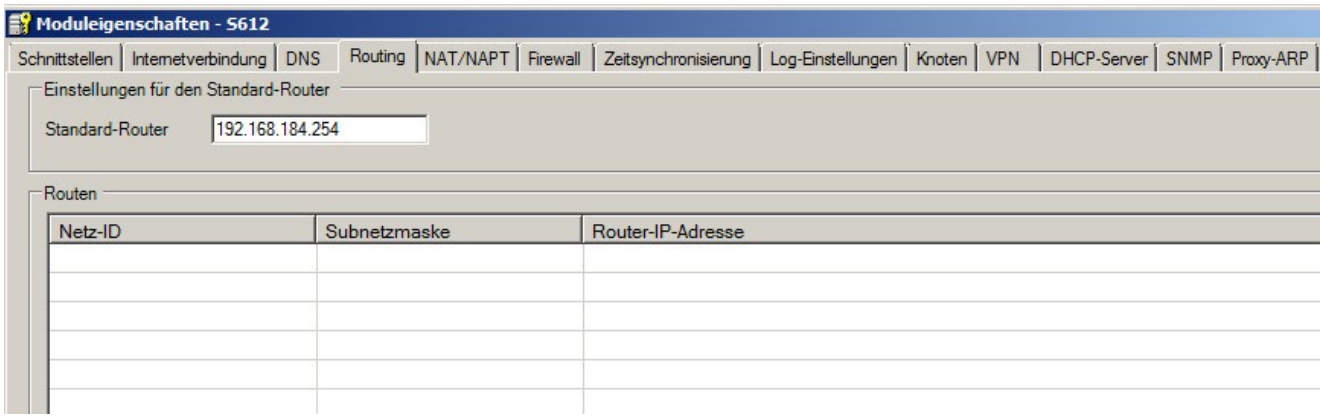
Die Konfiguration der Tunnelverbindung ist abgeschlossen.

3.2.1.3 Eigenschaften des S612 konfigurieren

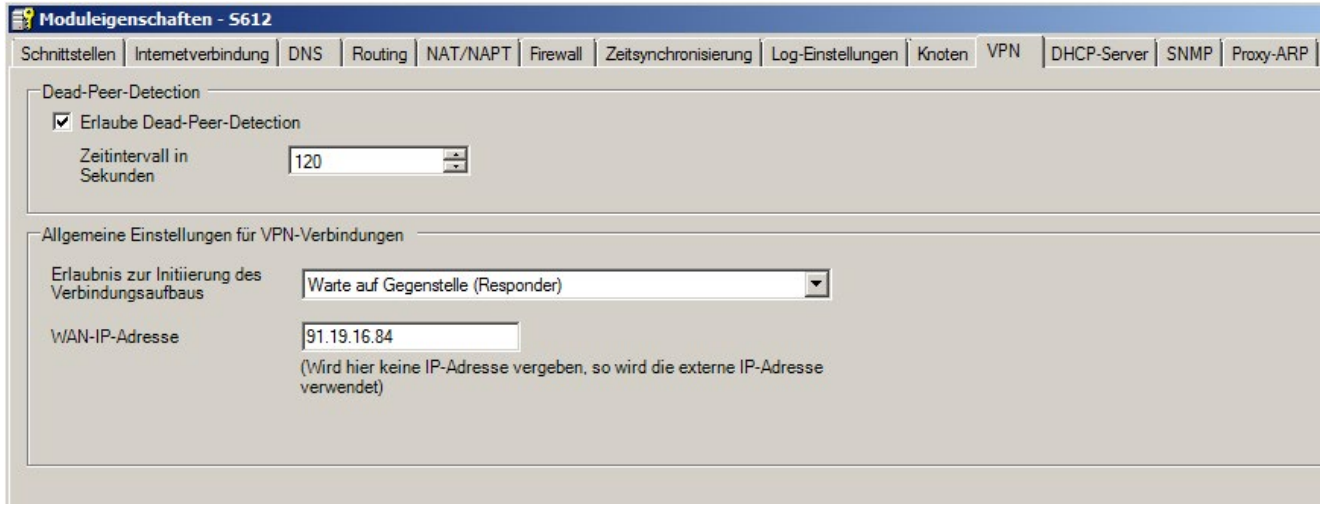
Da der S612 über einen DSL-Router mit dem Internet verbunden ist, sind die Eigenschaften des S612 entsprechend zu konfigurieren.

Vorgehensweise

1. Markieren Sie im Inhaltsbereich den "S612".
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...". Klicken Sie auf das Register "Routing".
3. Tragen Sie bei "Standard-Router" die interne IP-Adresse des DSL-Routers "192.168.184.254" ein. Klicken Sie auf "Übernehmen"



4. Klicken Sie auf das Register "VPN".
5. Wählen Sie bei "Erlaubnis zur Initiierung des Verbindungsaufbaus" den Eintrag "Warte auf Gegenstelle (Responder)" aus.
6. Tragen Sie die WAN-IP-Adresse des DSL-Routers ein, z. B. 91.19.6.84



7. Klicken Sie auf "Übernehmen" und schließen Sie den Dialog mit "OK".
8. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

Ergebnis

Das Security-Projekt ist fertig konfiguriert. Die Einstellungen werden in der Konfigurationsdatei gespeichert:

3.2.1.4 Konfiguration in S612 laden und M-800-Konfiguration abspeichern

Konfiguration in S612 laden

1. Markieren Sie im Inhaltsbereich das Security-Modul "S612" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...". Der folgende Dialog wird geöffnet.

2. Klicken Sie auf "Starten", um den Ladevorgang zu starten.

   Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das Security-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

SCALANCE M-800-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis.

Ergebnis

In das Projektverzeichnis wird folgende Datei abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800.

Konfigurationsdatei	Einstellungen im WBM
IPSec VPN > Verbindungen > VPN Standard Modus - Einstellungen bearbeiten	Security > IPSec VPN > Remote End > Remote Mode: Standard
Adresse des VPN Gateways der Gegenstelle: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentisierungsverfahren: Pre Shared Key	Security > IPSec VPN > Authentication > Authentication: PSK
Pre Shared Key: 12345678	Security > IPSec VPN > Authentication > PSK und PSK Confirmation: 12345678
Remote ID: U28098881@GEA32	Security > IPSec VPN > Authentication > Remote ID nicht benötigt. Im WBM wird externe IP-Adresse des S612 eingetragen. In diesem Beispiel ist das die 192.168.184.2
Lokale ID: U269159D5@GEA32	Security > IPSec VPN > Authentication > Local ID nicht benötigt. Der Eintrag bleibt im WBM leer.
Adresse des gegenüberliegenden Netzes: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Netzmaske des gegenüberliegenden Netzes: 255.255.255.0	
Adresse des lokalen Netzes: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Netzmaske des lokalen Netzes: 255.255.255.0	
IPSec VPN > Verbindungen > IKE Bearbeiten	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA Hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA Modus: Main Mode	--
ISAKMP-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPSec-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPSec-SA Hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPSec-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 2 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--

Konfigurationsdatei	Einstellungen im WBM
DH/PFS-Gruppe: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: An	--
DPD-Verzögerung (Sekunden): 150	--
DPD-Timeout (Sekunden): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD-Maximale Fehlversuche: 5	--

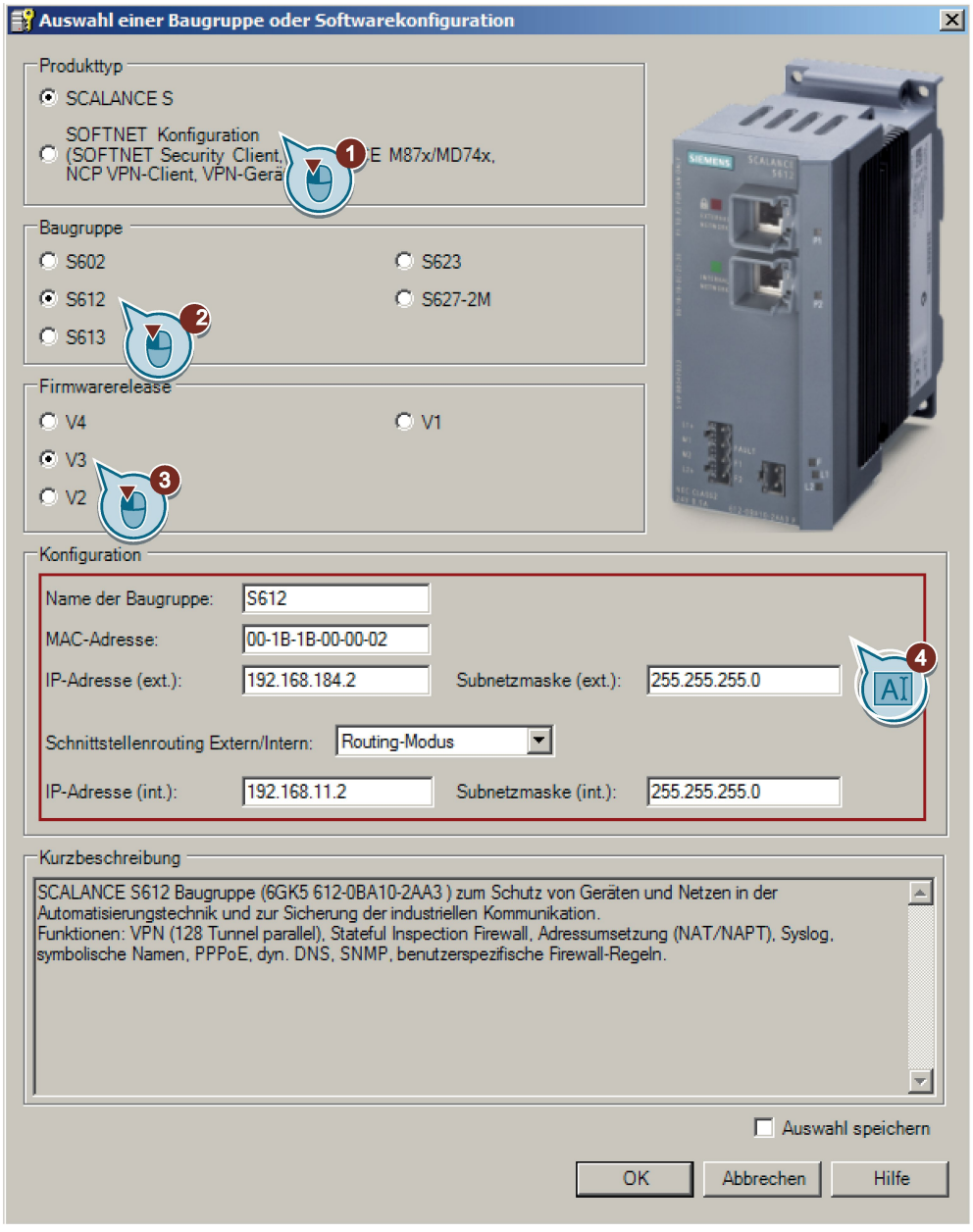
3.2.2 VPN-Tunnel mit dem SCT V4.x konfigurieren

3.2.2.1 Projekt und Module anlegen

Vorgehensweise

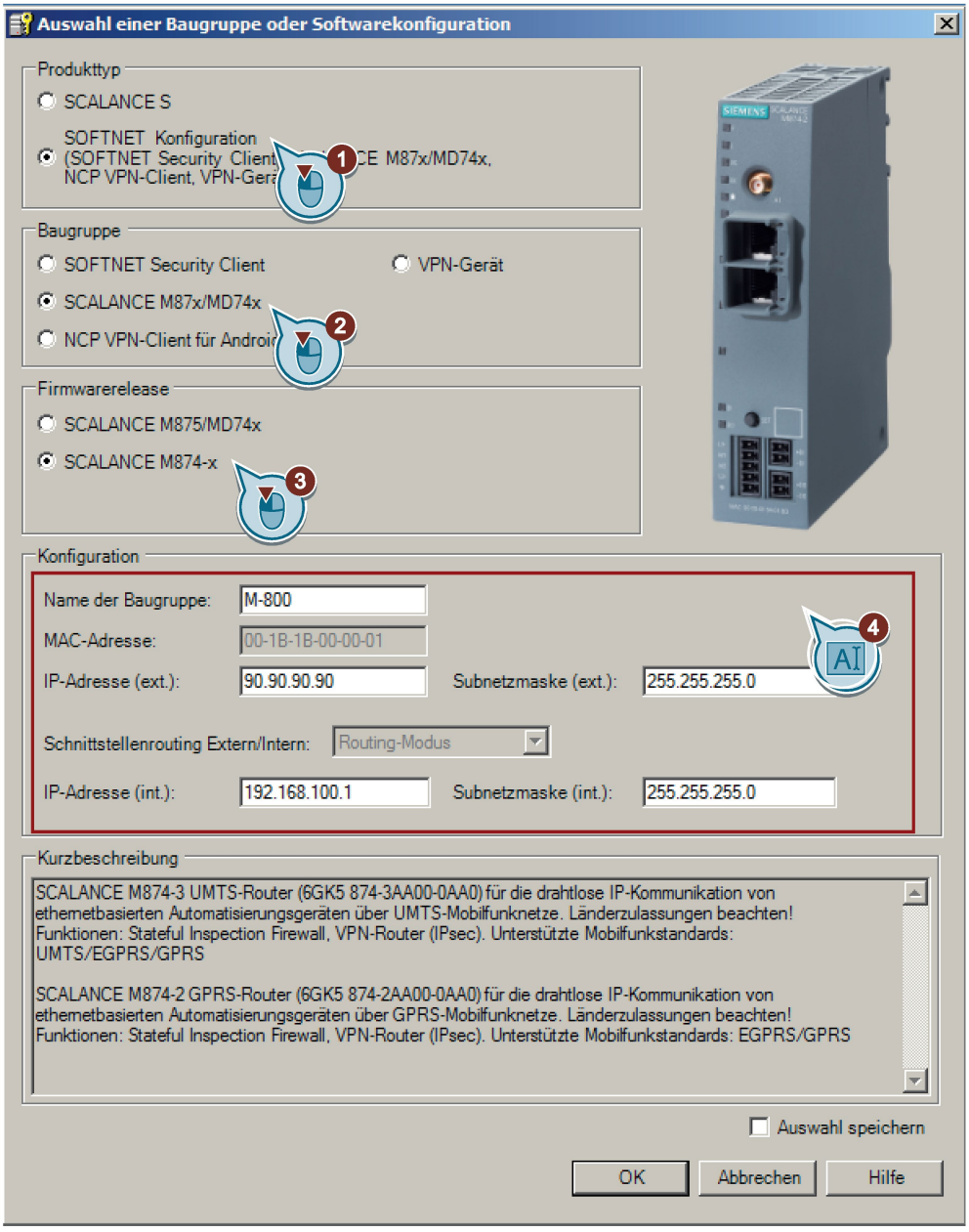
1. Starten Sie die Projektierungssoftware Security Configuration Tool V4.x auf dem PC.
2. Wählen Sie den Menübefehl "Projekt" > "Neu".
3. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an. Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
4. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt und der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" wird geöffnet.

5. Tragen Sie die dem S612 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein. Tragen Sie zusätzlich die MAC-Adresse ein, die auf der Frontseite des Security-Moduls aufgedruckt ist



6. Schließen Sie den Dialog mit "OK".
7. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Baugruppe" ein zweites Modul

8. Tragen Sie die dem M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein.



9. Schließen Sie den Dialog mit "OK".

Ergebnis

Das Security-Modul S612 und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

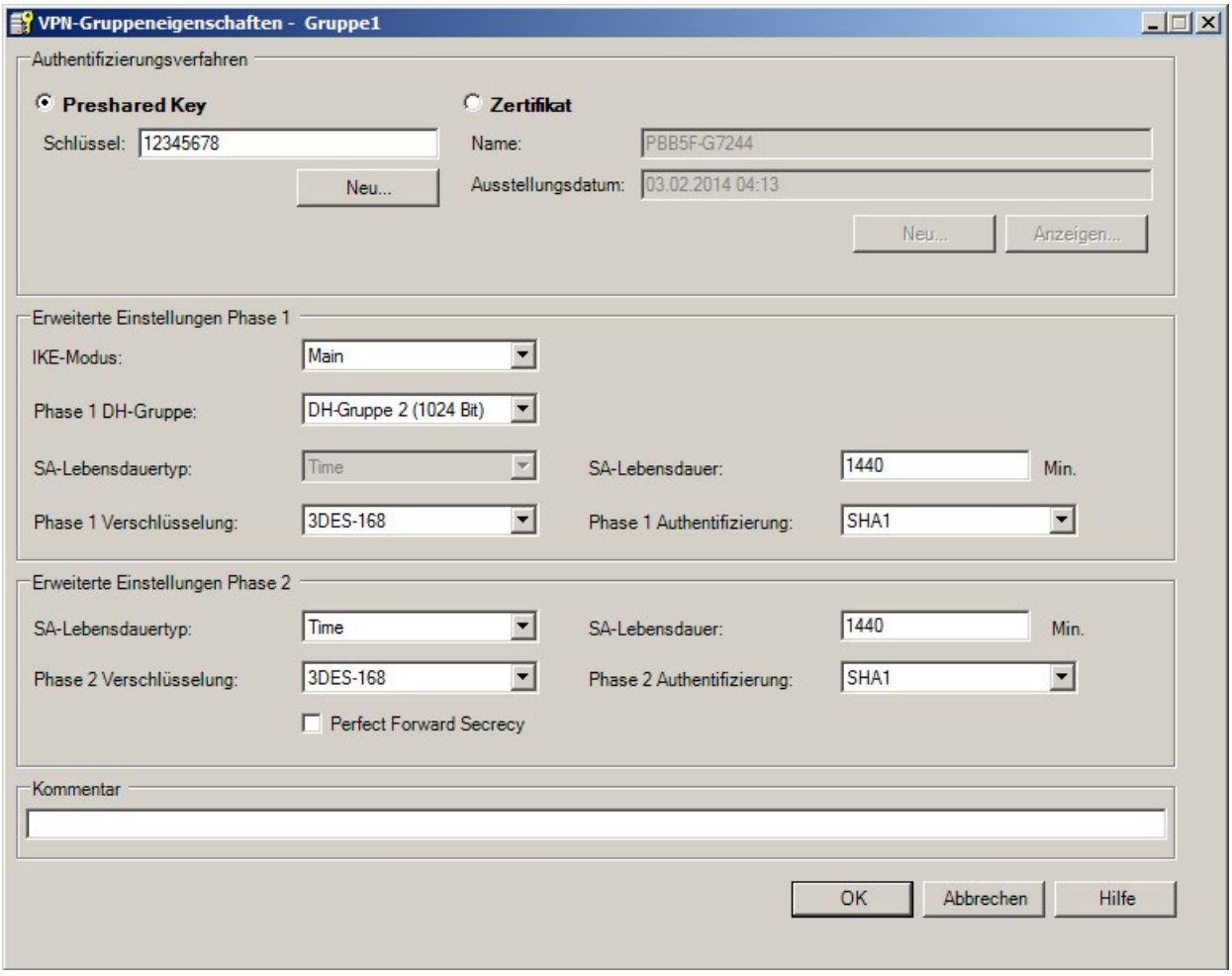
3.2.2.2 Tunnelverbindung projektieren

Nur wenn das M-800 und das S612 der gleichen VPN-Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Baugruppen".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den S612. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Baugruppen sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.

5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen.
6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

Ergebnis

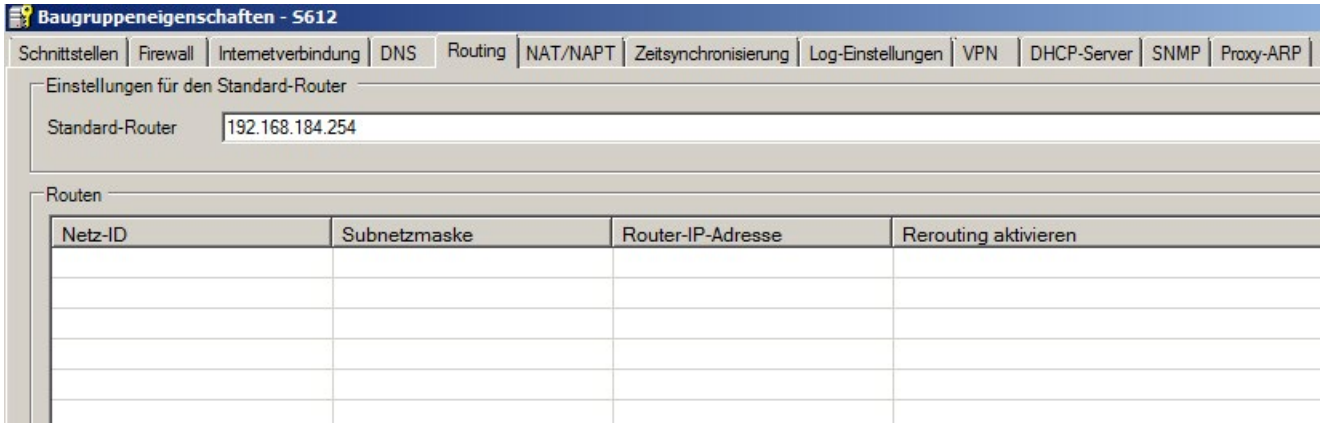
Die Konfiguration der Tunnelverbindung ist abgeschlossen.

3.2.2.3 Eigenschaften des S612 konfigurieren

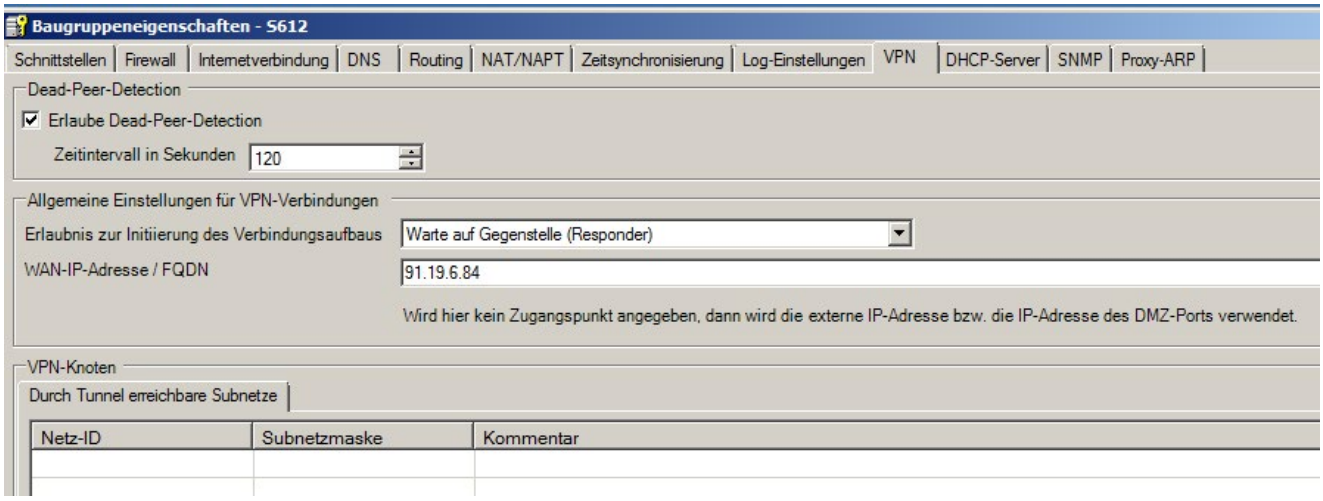
Da der S612 über einen DSL-Router mit dem Internet verbunden ist, sind die Eigenschaften des S612 entsprechend zu konfigurieren.

Vorgehensweise

1. Markieren Sie im Inhaltsbereich den "S612".
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...". Klicken Sie auf das Register "Routing".
3. Tragen Sie bei "Standard-Router" die interne IP-Adresse des DSL-Routers "192.168.184.254" ein. Klicken Sie auf "Übernehmen"



4. Klicken Sie auf das Register "VPN".
5. Wählen Sie bei "Erlaubnis zur Initiierung des Verbindungsaufbaus" den Eintrag "Warte auf Gegenstelle (Responder)" aus.
6. Tragen Sie die WAN-IP-Adresse des DSL-Routers ein, z. B. 91.19.6.84



7. Klicken Sie auf "Übernehmen" und schließen Sie den Dialog mit "OK".
8. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

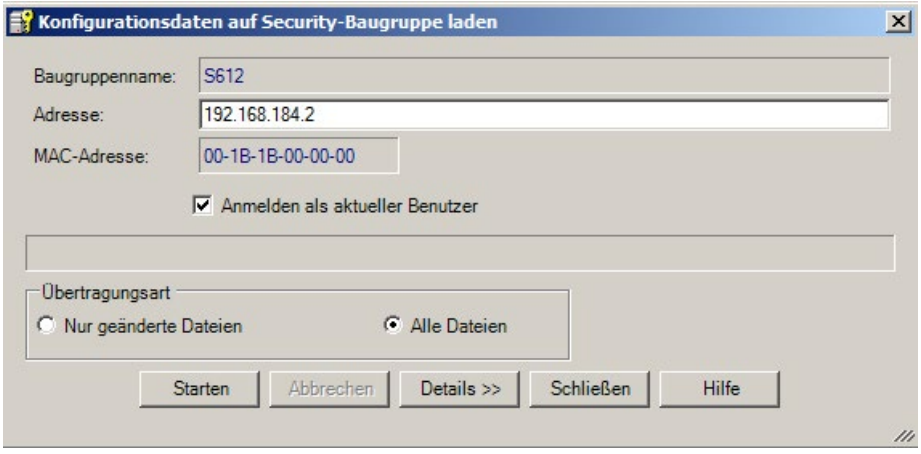
Ergebnis

Das Security-Projekt ist fertig konfiguriert. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

3.2.2.4 Konfiguration in S612 laden und M-800-Konfiguration abspeichern

Konfiguration in S612 laden

1. Markieren Sie im Inhaltsbereich das Security-Modul "S612" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n) ...". Der folgende Dialog wird geöffnet.



2. Klicken Sie auf "Starten", um den Ladevorgang zu starten.

   Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das Security-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

SCALANCE M-800-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n)...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis.

Ergebnis

In das Projektverzeichnis wird folgende Datei abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt

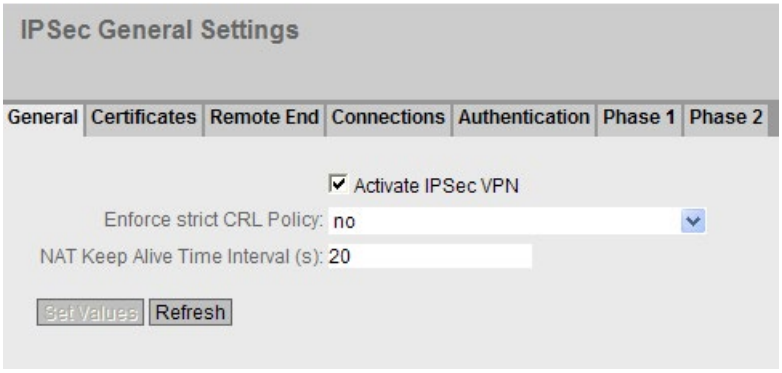
Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800. Folgen Sie den Anweisungen in der Konfigurationsdatei.

3.2.3 SCALANCE M-800 konfigurieren

3.2.3.1 VPN aktivieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN".



3. Klicken Sie auf "Set Values"

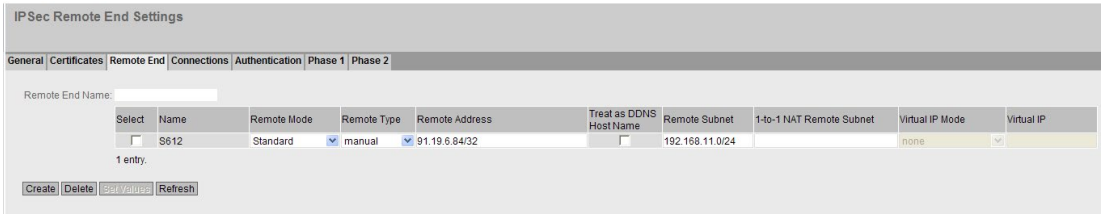
3.2.3.2 VPN-Gegenstelle konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Remote End".
2. Tragen Sie bei "Remote End Name" den Namen der VPN-Gegenstelle (Tunnelendpunkt) ein, z. B. S612.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie die VPN-Gegenstelle mit folgenden Einstellungen aus der Konfigurationsdatei:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN-IP-Adresse des DSL-Routers
Remote Subnet	192.168.11.0/24

5. Klicken Sie auf "Set Values".



3.2.3.3 VPN-Verbindung konfigurieren

Voraussetzung

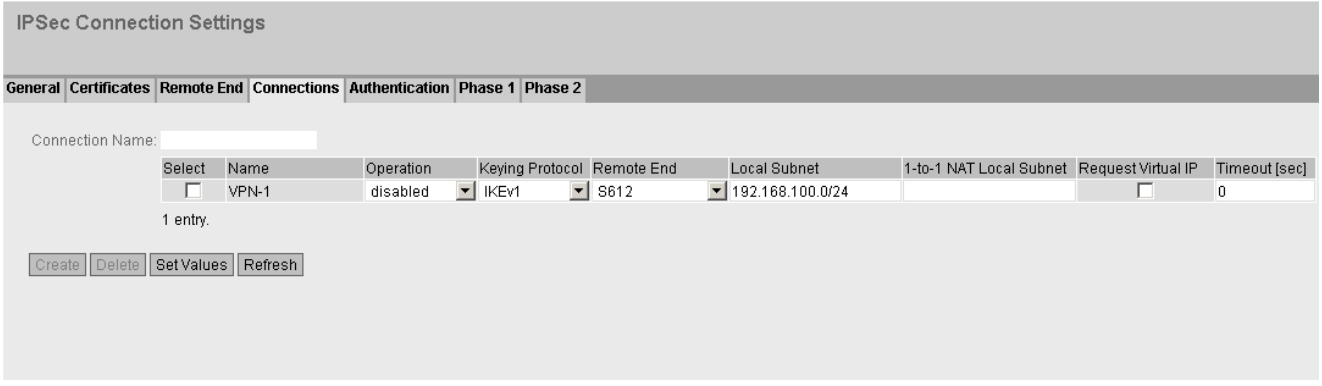
- VPN-Gegenstelle ist angelegt.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Tragen Sie bei "Connection Name" einen Namen für die VPN-Verbindung ein.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie die VPN-Verbindung mit folgenden Einstellungen:

Operation	disabled
Keying Protocol	IKEv1
Remote End	S612 Name der VPN-Gegenstelle
Local Subnet	192.168.100.0/24 Das lokale interne Subnetz 1 in CIDR-Schreibweise.

5. Klicken Sie auf "Set Values".



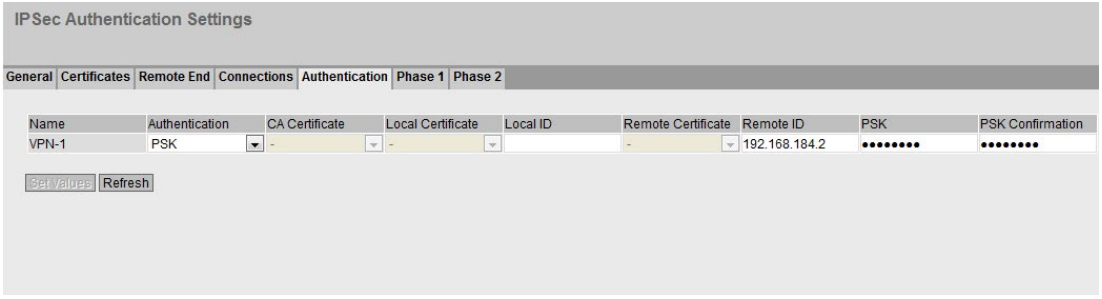
3.2.3.4 VPN-Authentifizierung konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Authentication".
2. Konfigurieren Sie die VPN-Authentifizierung mit folgenden Einstellungen:

Authentication	PSK
Local ID	kein Eintrag notwendig
Remote ID	Externe IP-Adresse des S612, z. B. 162.168.184.2
PSK / PSK Confirmation	12345678 Den Schlüssel, den Sie im SCT projektiert haben.

3. Klicken Sie auf "Set Values".



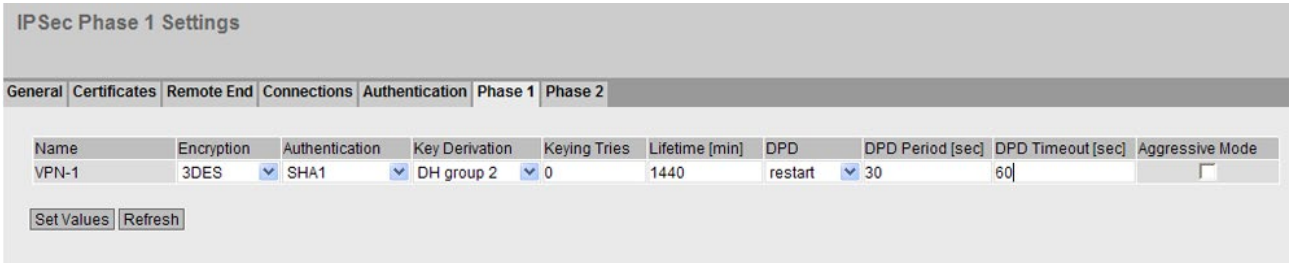
3.2.3.5 Phase 1 und Phase 2 konfigurieren

Phase 1 konfigurieren

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Phase 1".
2. Wählen Sie bei "DPD" "restart" aus.
3. Konfigurieren Sie die Phase 1 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

4. Klicken Sie auf "Set Values".

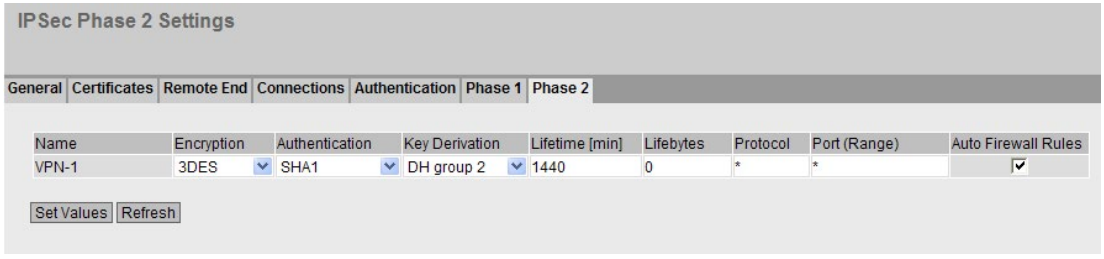


Phase 2 konfigurieren

1. Klicken Sie auf das Register "Phase 2".
2. Konfigurieren Sie für die Phase 2 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

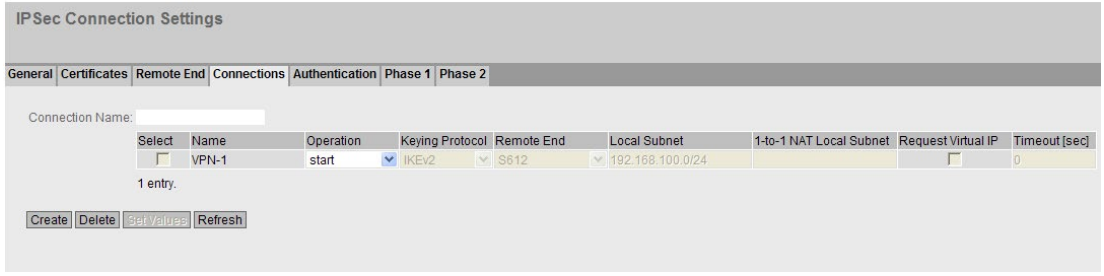
3. Klicken Sie auf "Set Values".



3.2.3.6 VPN-Verbindung aufbauen

Vorgehensweise

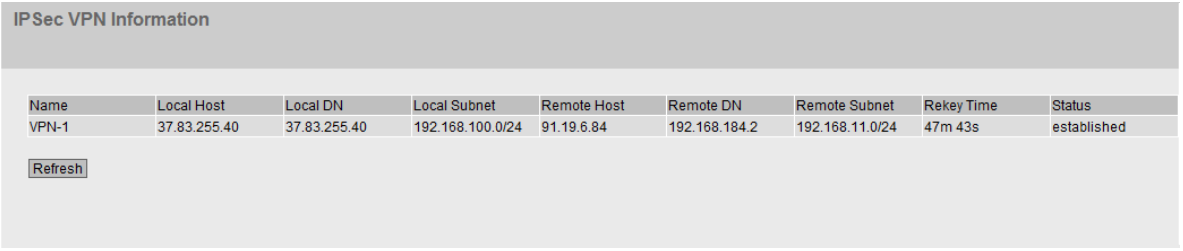
1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Connection".
2. Wählen Sie bei "Operation" "start" aus und klicken Sie auf "Set Values".



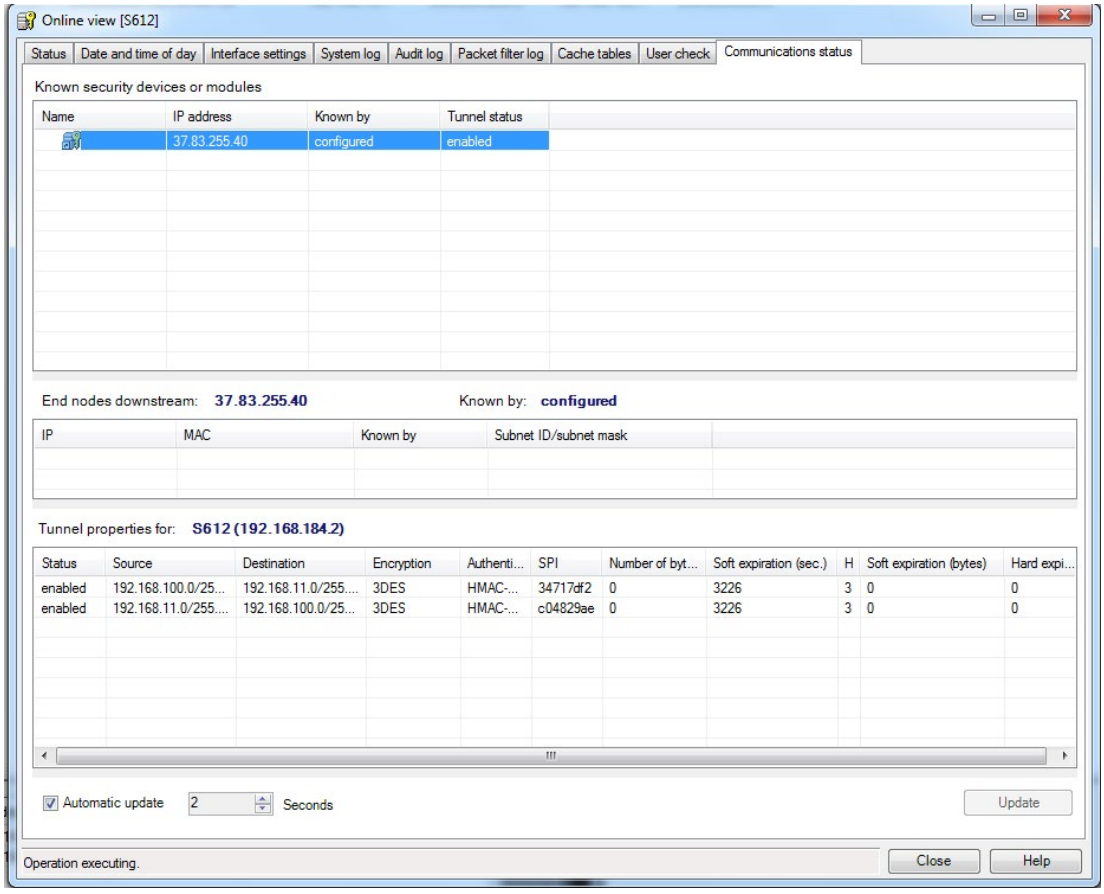
Ergebnis

Das M-800 baut den VPN-Tunnel zum S612 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet am Gerät die LED 🔒 grün.

Weitere Informationen erhalten Sie unter "Information" > "IPSec VPN".



In der Online-Ansicht des SCT können Sie den Kommunikationsstatus am S612 sehen.


Online view [S612]
Status
Date and time of day
Interface settings
System log
Audit log
Packet filter log
Cache tables
User check
Communications status
Known security devices or modules
Name
IP address
Known by
Tunnel status
37.83.255.40
configured
enabled
End nodes downstream: 37.83.255.40
Known by: configured
IP
MAC
Known by
Subnet ID/subnet mask
Tunnel properties for: S612 (192.168.184.2)
Status
Source
Destination
Encryption
Authenti...
SPI
Number of byt...
Soft expiration (sec.)
H
Soft expiration (bytes)
Hard expi...
enabled
192.168.100.0/25...
192.168.11.0/255....
3DES
HMAC-...
34717df2
0
3226
3
0
0
enabled
192.168.11.0/255....
192.168.100.0/25...
3DES
HMAC-...
c04829ae
0
3226
3
0
0
Automatic update
2
Seconds
Update
Operation executing.
Close
Help

3.3 Gesicherter VPN-Tunnel mit Zertifikaten

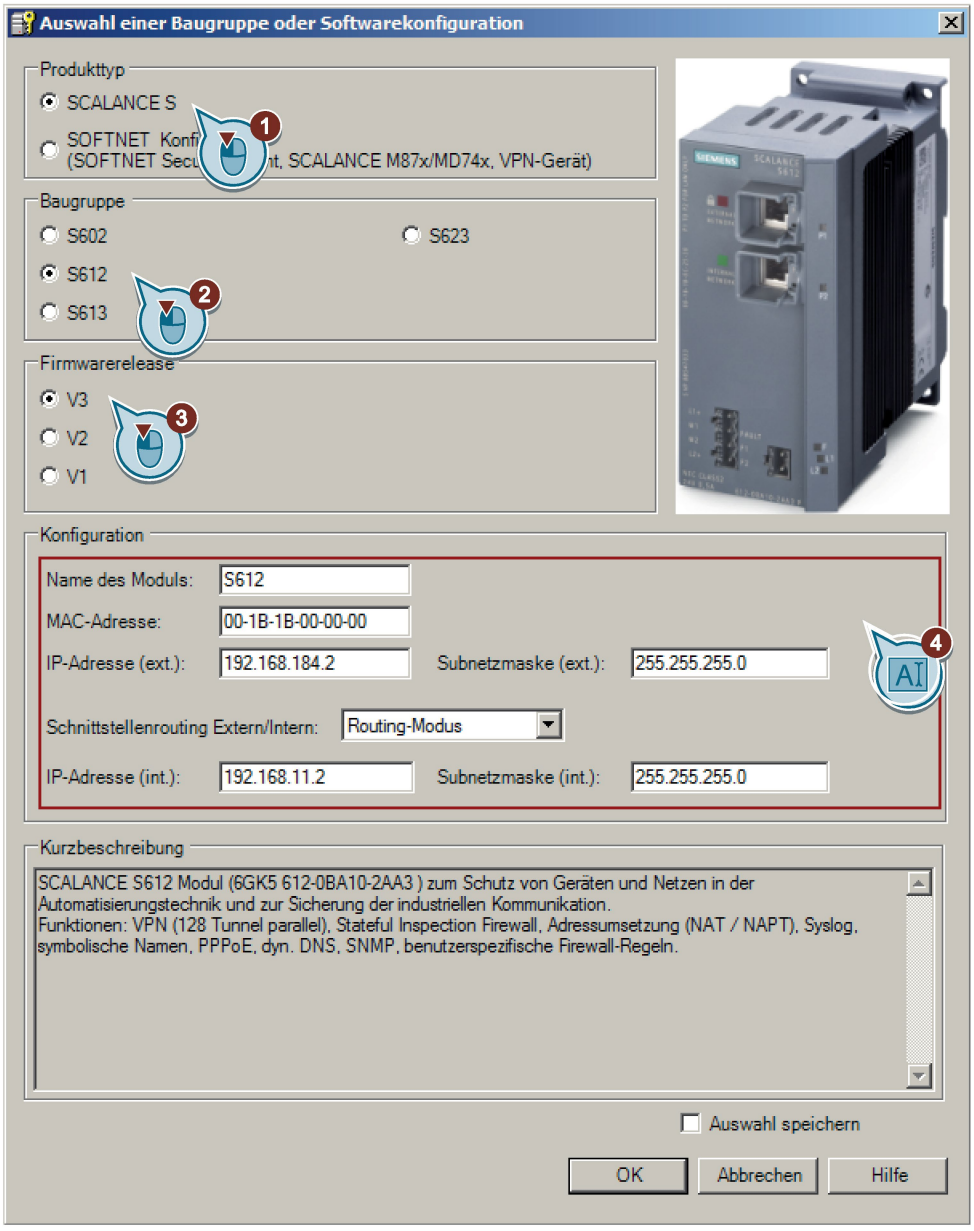
3.3.1 VPN-Tunnel mit dem SCT V3.x konfigurieren

3.3.1.1 Projekt und Module anlegen

Vorgehensweise

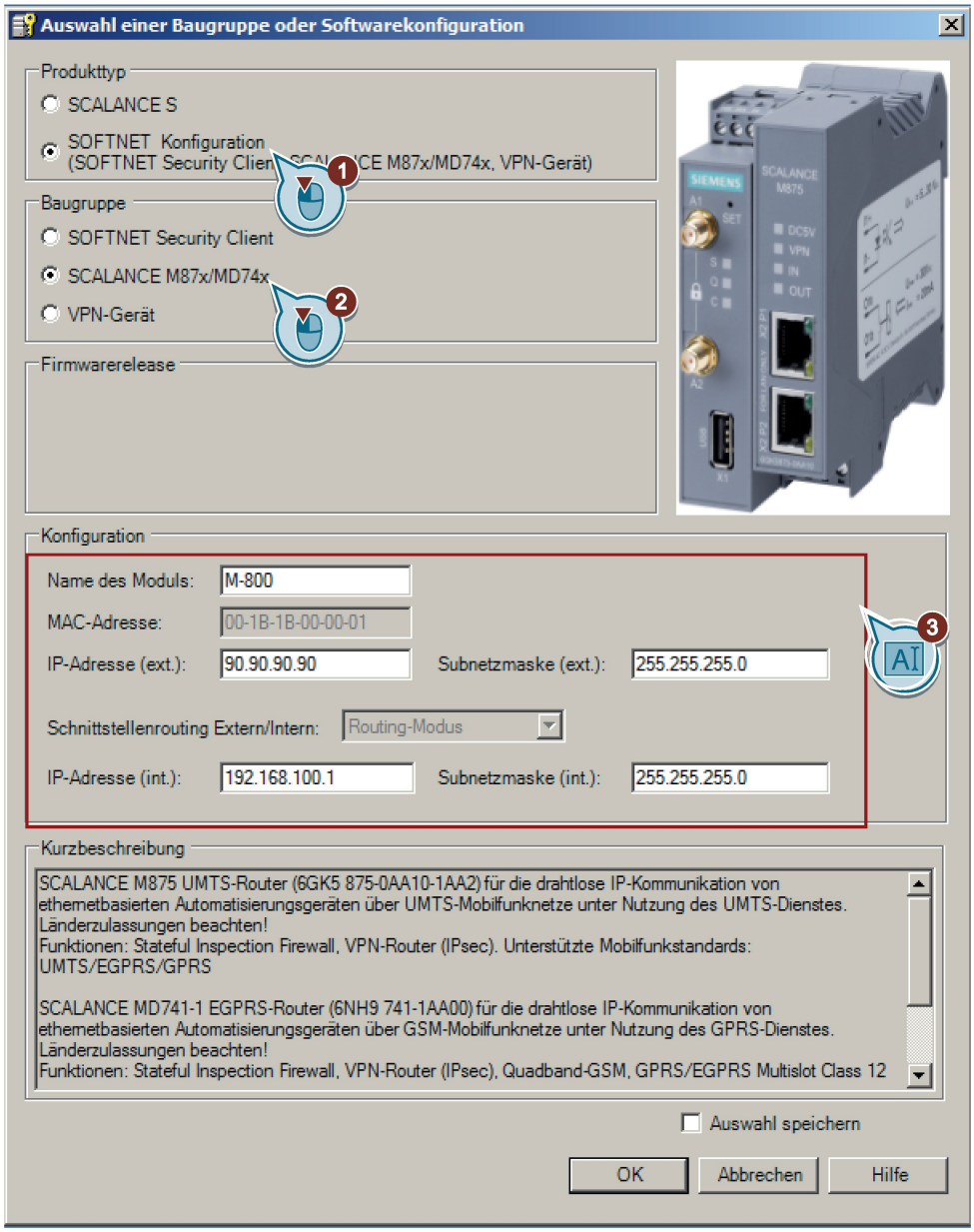
1. Starten Sie die Projektierungssoftware Security Configuration Tool V3.x auf dem PC.
2. Wählen Sie den Menübefehl "Projekt" > "Neu".
3. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an. Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
4. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt und der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" wird geöffnet.

5. Tragen Sie die dem S612 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein. Tragen Sie zusätzlich die MAC-Adresse ein, die auf der Frontseite des Security-Moduls aufgedruckt ist



6. Schließen Sie den Dialog mit "OK".
7. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Modul" ein zweites Modul

8. Tragen Sie die dem M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein.



9. Schließen Sie den Dialog mit "OK".

Ergebnis

Das Security-Modul S612 und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

3.3.1.2 Tunnelverbindung projektieren

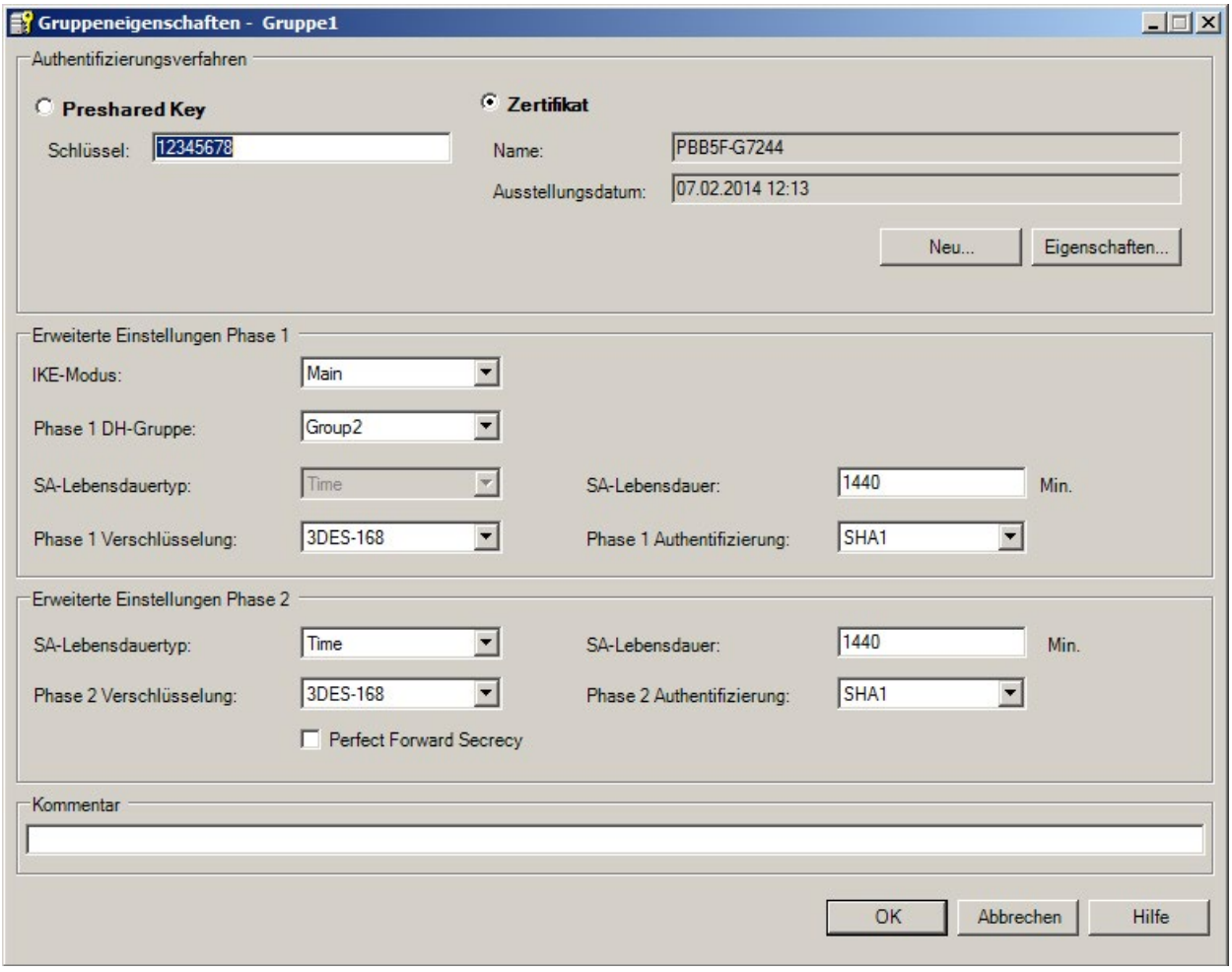
Nur wenn das SCALANCE M-800 und das S612 der gleichen Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den S612. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.

5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen.
6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.

   Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.



Ergebnis

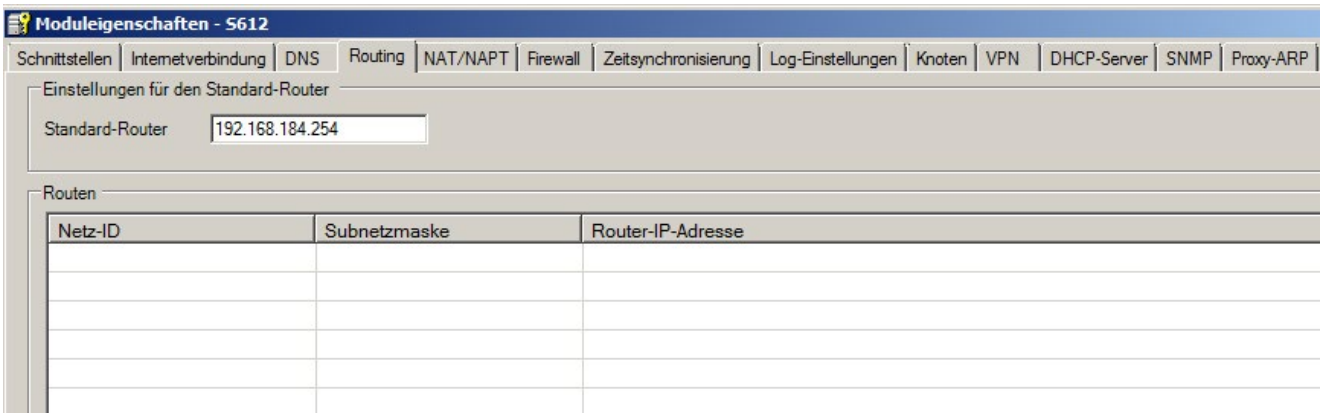
Die Konfiguration der Tunnelverbindung ist abgeschlossen.

3.3.1.3 Eigenschaften des S612 konfigurieren

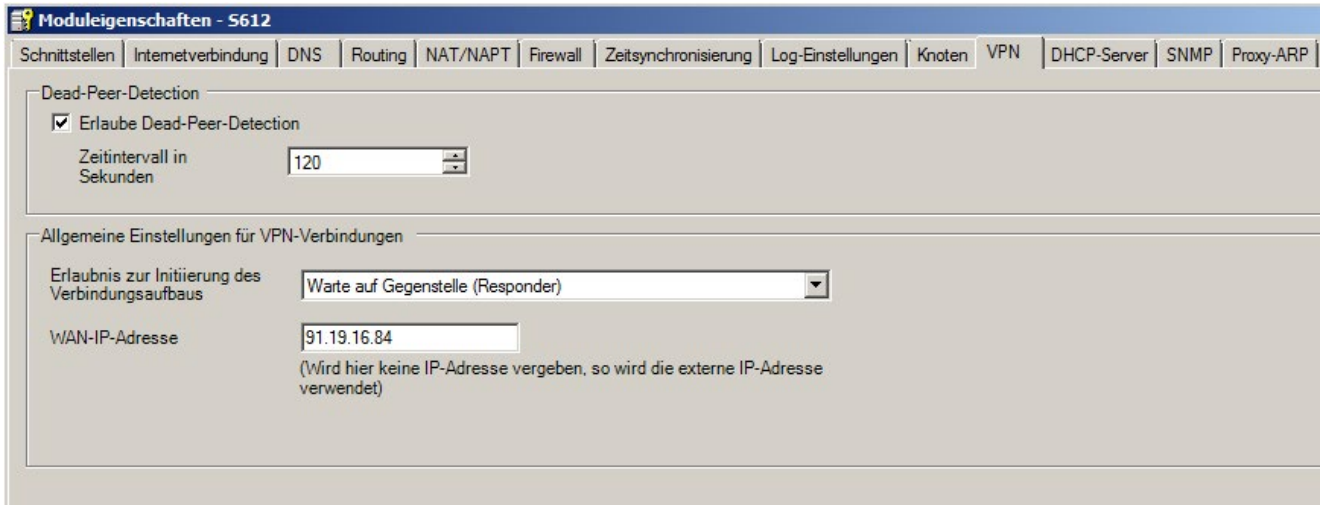
Da der S612 über einen DSL-Router mit dem Internet verbunden ist, sind die Eigenschaften des S612 entsprechend zu konfigurieren.

Vorgehensweise

1. Markieren Sie im Inhaltsbereich den "S612".
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...". Klicken Sie auf das Register "Routing".
3. Tragen Sie bei "Standard-Router" die interne IP-Adresse des DSL-Routers "192.168.184.254" ein. Klicken Sie auf "Übernehmen"



4. Klicken Sie auf das Register "VPN".
5. Wählen Sie bei "Erlaubnis zur Initiierung des Verbindungsaufbaus" den Eintrag "Warte auf Gegenstelle (Responder)" aus.
6. Tragen Sie die WAN-IP-Adresse des DSL-Routers ein, z. B. 91.19.6.84



7. Klicken Sie auf "Übernehmen" und schließen Sie den Dialog mit "OK".
8. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

Ergebnis

Das Security-Projekt ist fertig konfiguriert. Die Einstellungen werden in der Konfigurationsdatei gespeichert:

3.3.1.4 Konfiguration in S612 laden und M-800-Konfiguration abspeichern

Konfiguration in S612 laden

1. Markieren Sie im Inhaltsbereich das Security-Modul "S612" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...".

   Der folgende Dialog wird geöffnet.

2. Klicken Sie auf."Starten", um den Ladevorgang zu starten.

   Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das Security-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

SCALANCE M-800-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats, z. B. Di1S+Xo?.

Ergebnis

In das Projektverzeichnis werden folgende Dateien abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt
- PKCS12-Datei: Projektname.Zeichenfolge.M-800.p12
- Gegenstellenzertifikat: Projektname.Gruppe1.S612.cer

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800 einschließlich einer Information über die zusätzlich erzeugten Zertifikate.

Konfigurationsdatei	Einstellungen im WBM
IPSec VPN > Zertifikate Gegenstellen Zertifikat hochladen: Configuration-1.Gruppe1.S612.cer PKCS12 Datei (.p12) hochladen: Configuration-1.U800CB3FF@G471C.M-800.p12	System > Load&Save > HTTP > IPSecCert : Load
IPSec VPN > Verbindungen > VPN Standard Modus - Einstellungen bearbeiten	Security > IPSec VPN > Remote End > Remote Mode: Standard
Adresse des VPN Gateways der Gegenstelle: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentisierungsverfahren: X.509 Gegenstellenzertifikat	Security > IPSec VPN > Authentication > Authentication: Remote Cert
Gegenstellen Zertifikat: Configuration-1.Gruppe1.S612.cer	Security > IPSec VPN > Authentication > Remote Certificate: Configuration-1.Gruppe1.CP.cer
Remote ID: U5A634732@GC4D8	Security > IPSec VPN > Authentication > Remote ID: U5A634732@GC4D8
Adresse des gegenüberliegenden Netzes: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Netzmaske des gegenüberliegenden Netzes: 255.255.255.0	
Adresse des lokalen Netzes: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Netzmaske des lokalen Netzes: 255.255.255.0	
IPSec VPN > Verbindungen > IKE Bearbeiten	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA Hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA Modus: Main Mode	--
ISAKMP-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPSec-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPSec-SA Hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPSec-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--

Konfigurationsdatei	Einstellungen im WBM
DH/PFS-Gruppe: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: An	--
DPD-Verzögerung (Sekunden): 150	--
DPD-Timeout (Sekunden): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD-Maximale Fehlversuche: 5	--

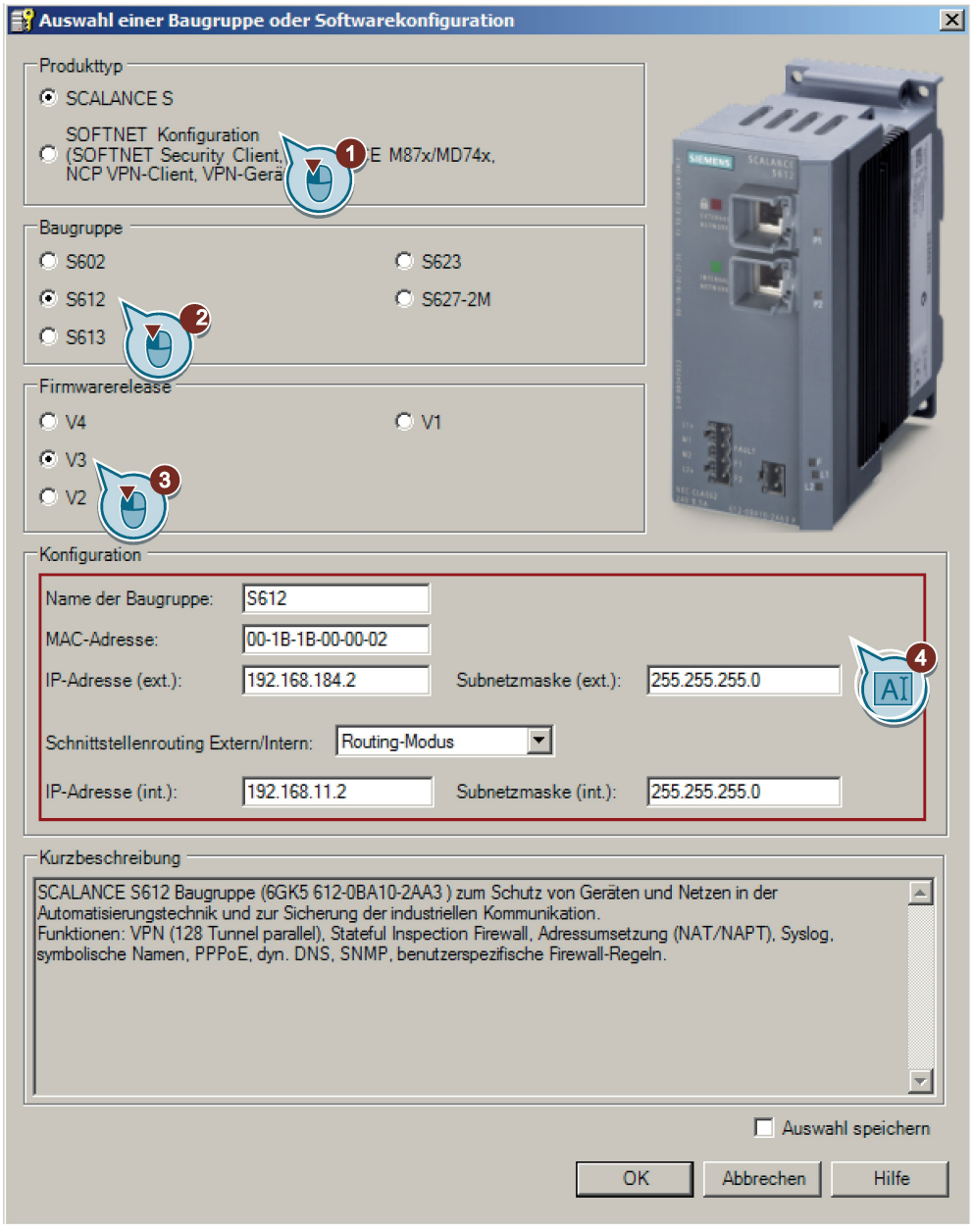
3.3.2 VPN-Tunnel mit dem SCT V4.x konfigurieren

3.3.2.1 Projekt und Module anlegen

Vorgehensweise

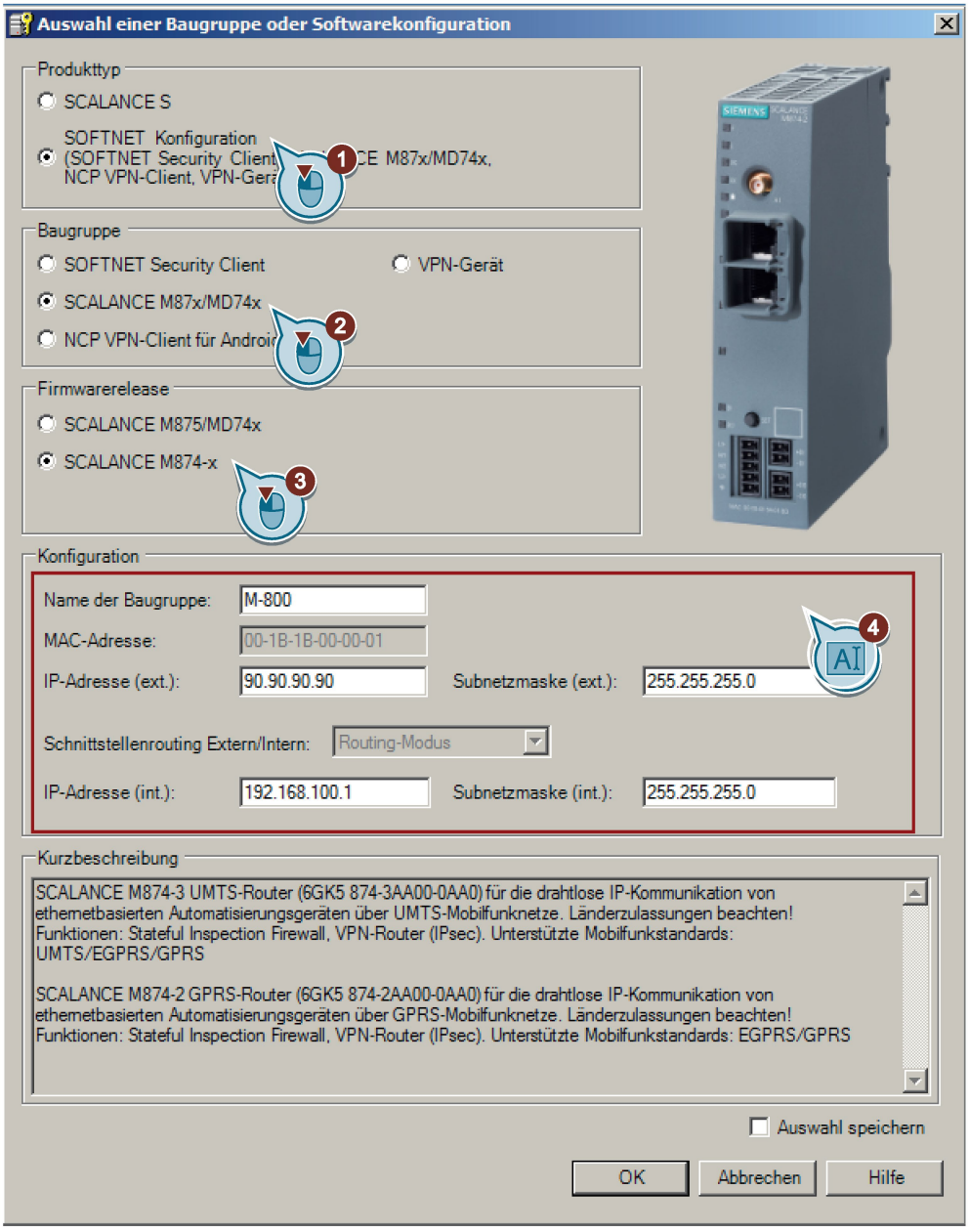
1. Starten Sie die Projektierungssoftware Security Configuration Tool V4.x auf dem PC.
2. Wählen Sie den Menübefehl "Projekt" > "Neu".
3. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an. Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
4. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt und der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" wird geöffnet.

5. Tragen Sie die dem S612 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein. Tragen Sie zusätzlich die MAC-Adresse ein, die auf der Frontseite des Security-Moduls aufgedruckt ist



6. Schließen Sie den Dialog mit "OK".
7. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Baugruppe" ein zweites Modul

8. Tragen Sie die dem M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 93)" ein.



9. Schließen Sie den Dialog mit "OK".

Ergebnis

Das Security-Modul S612 und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

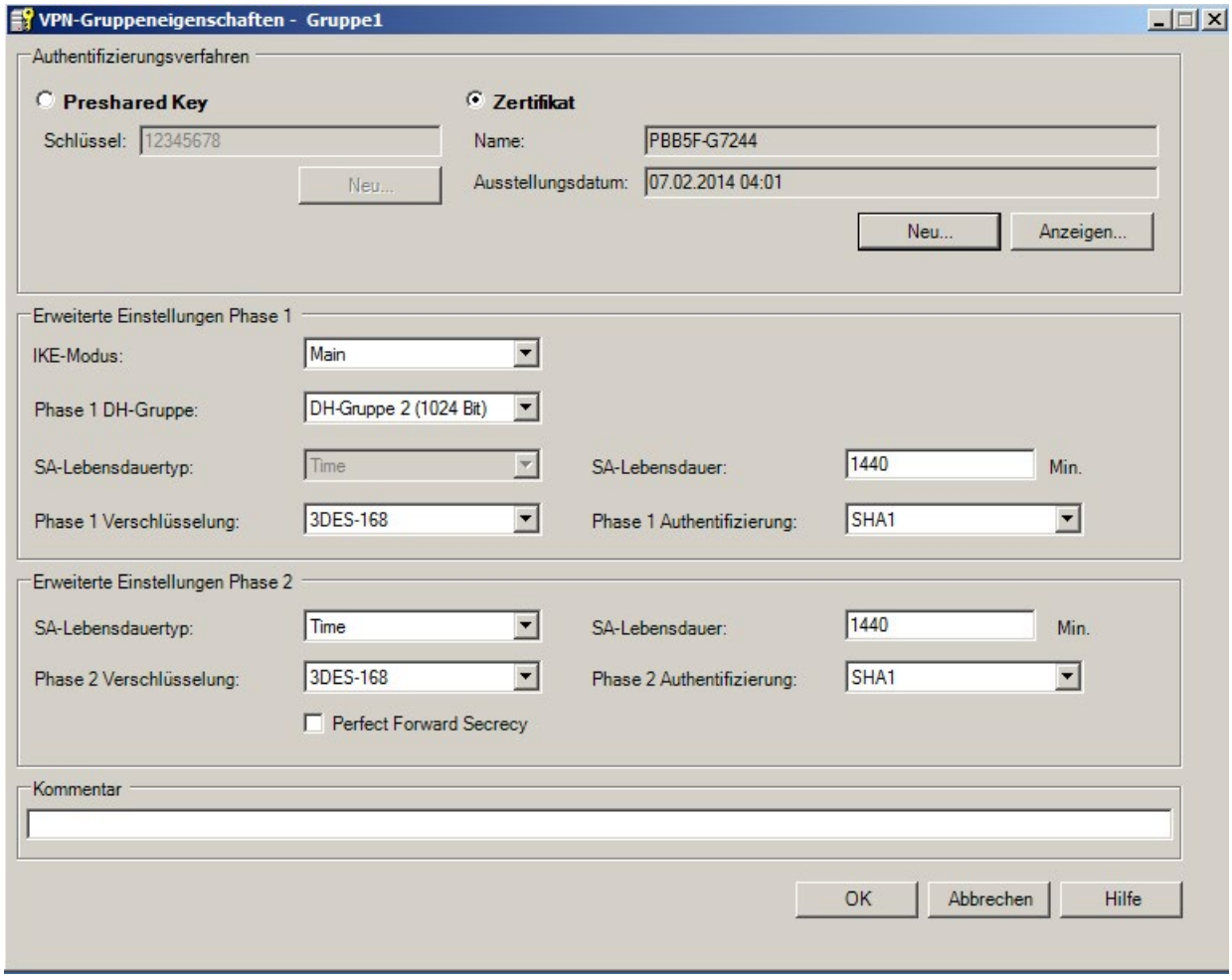
3.3.2.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M und das S612 der gleichen Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das SCALANCE M und den S612. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.

5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen.
6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

Ergebnis

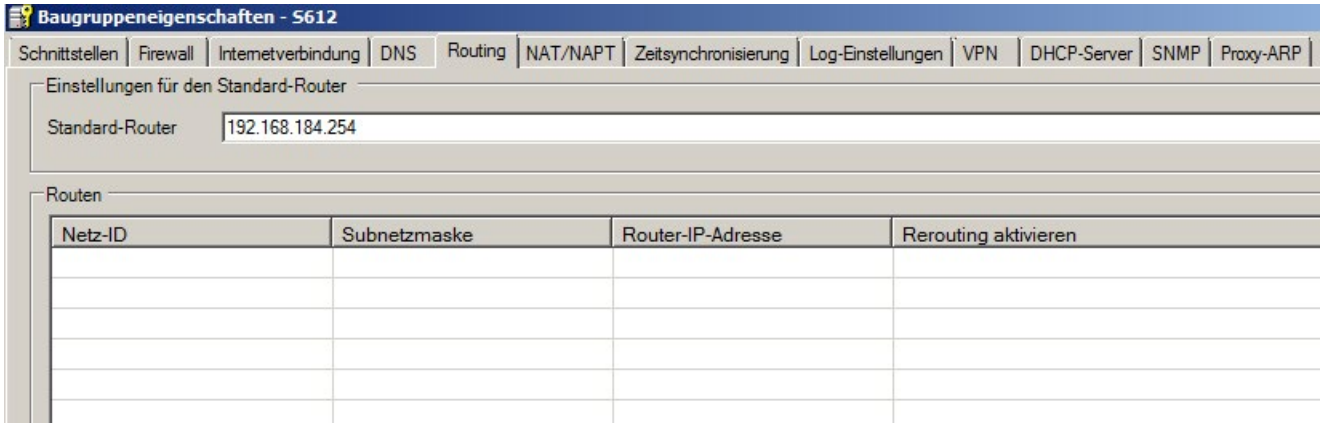
Die Konfiguration der Tunnelverbindung ist abgeschlossen.

3.3.2.3 Eigenschaften des S612 konfigurieren

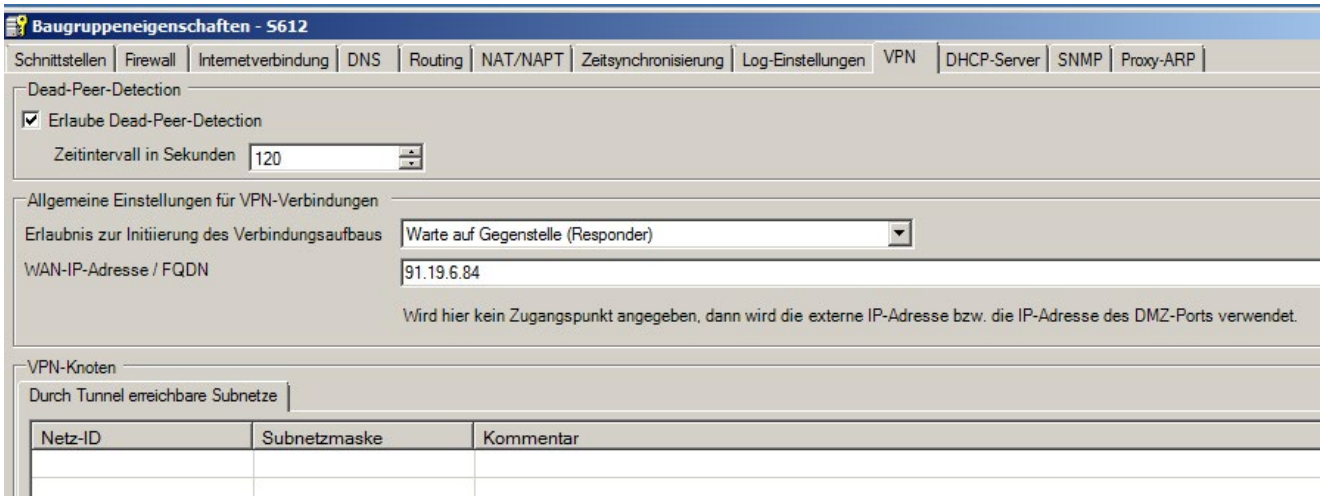
Da der S612 über einen DSL-Router mit dem Internet verbunden ist, sind die Eigenschaften des S612 entsprechend zu konfigurieren.

Vorgehensweise

1. Markieren Sie im Inhaltsbereich den "S612".
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...". Klicken Sie auf das Register "Routing".
3. Tragen Sie bei "Standard-Router" die interne IP-Adresse des DSL-Routers "192.168.184.254" ein. Klicken Sie auf "Übernehmen"



4. Klicken Sie auf das Register "VPN".
5. Wählen Sie bei "Erlaubnis zur Initiierung des Verbindungsaufbaus" den Eintrag "Warte auf Gegenstelle (Responder)" aus.
6. Tragen Sie die WAN-IP-Adresse des DSL-Routers ein, z. B. 91.19.6.84



7. Klicken Sie auf "Übernehmen" und schließen Sie den Dialog mit "OK".
8. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

Ergebnis

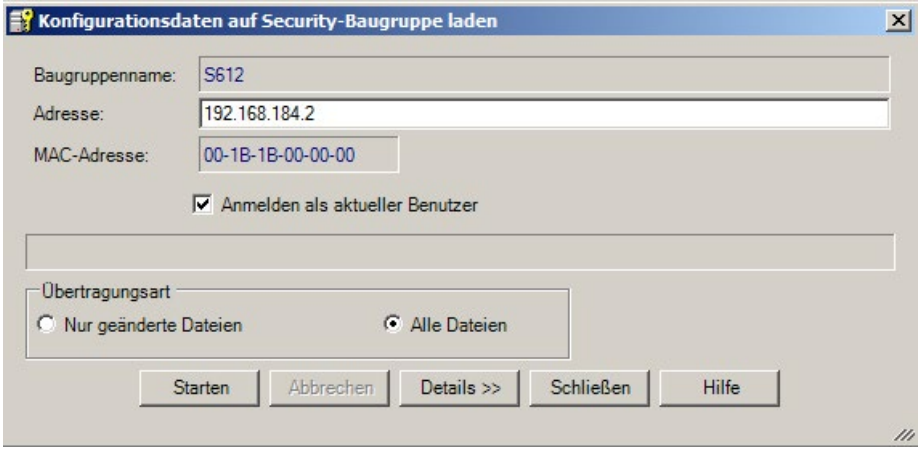
Das Security-Projekt ist fertig konfiguriert. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

3.3.2.4 Konfiguration in S612 laden und M-800-Konfiguration abspeichern

Konfiguration in S612 laden

1. Markieren Sie im Inhaltsbereich das Security-Modul "S612" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n) ...".

   Der folgende Dialog wird geöffnet.



2. Klicken Sie auf."Starten", um den Ladevorgang zu starten.

   Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das Security-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

SCALANCE M-800-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n) ...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats, z. B. Di1S+Xo?.

Ergebnis

In das Projektverzeichnis werden folgende Dateien abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt
- PKCS12-Datei: Projektname.Zeichenfolge.M-800.p12
- Gegenstellenzertifikat: Projektname.Gruppe1.S612.cer

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800 einschließlich einer Information über die zusätzlich erzeugten Zertifikate. Folgen Sie den Anweisungen in der Konfigurationsdatei.

3.3.3 SCALANCE M-800 konfigurieren

3.3.3.1 Zertifikat laden

Voraussetzung

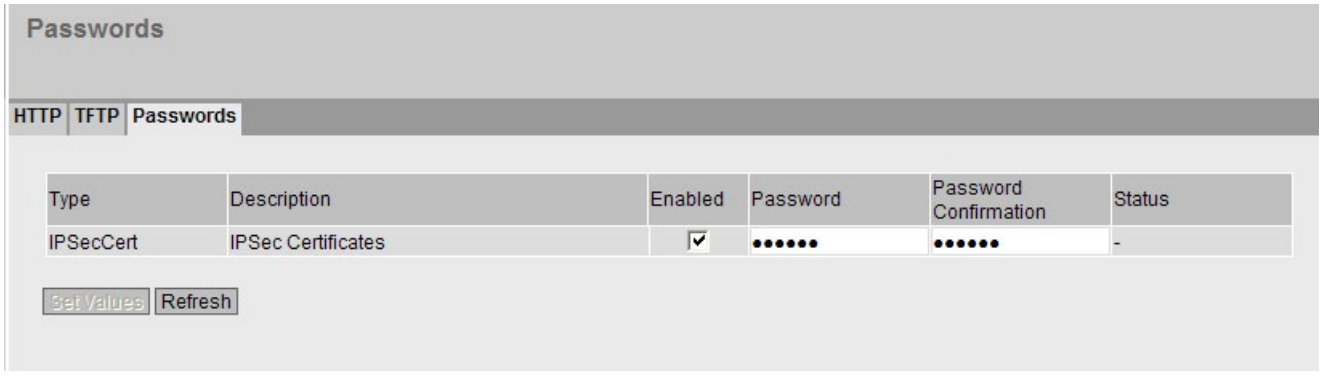
- Auf dem SCALANCE M ist die richtige Uhrzeit eingestellt, siehe Kapitel Uhrzeit einstellen (Seite 22).
- Zertifikate sind vorhanden.

  Die benötigten Zertifikate haben Sie im letzten Kapitel auf dem PC abgespeichert und ein Passwort für den privaten Schlüssel vergeben.

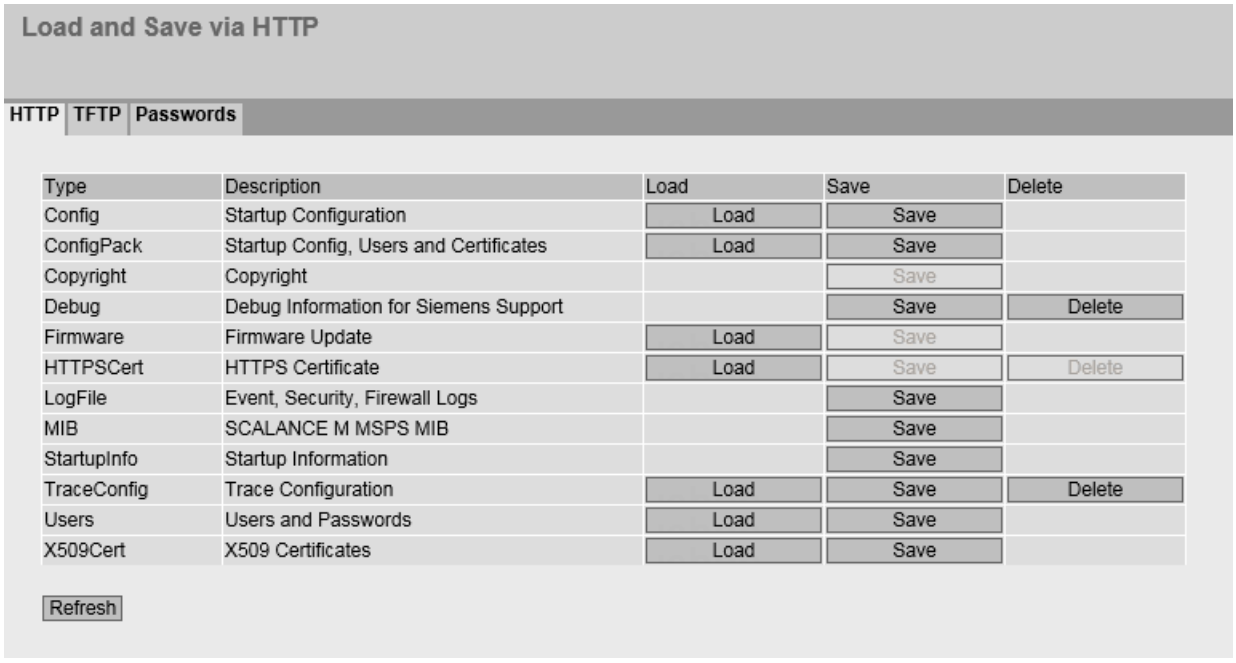
  Übertragen Sie die Zertifikate für das SCALANCE M auf den Admin-PC.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "Load & Save" und im Inhaltsbereich auf das Register "Password".
2. Tragen Sie bei "Password" und bei "Password Confirmation" das Passwort Di1S+Xo? ein, das Sie für die PKCS12-Datei festgelegt haben.
3. Aktivieren Sie "Enabled" und klicken Sie auf "Set Values".



4. Klicken Sie im Inhaltsbereich auf das Register "HTTP".



5. Klicken Sie bei "IPSecCert" oder "X509cert" auf die Schaltfläche "Load". Das Dialogfenster zum Hochladen einer Datei wird geöffnet.

   Navigieren Sie zum Gegenstellenzertifikat.

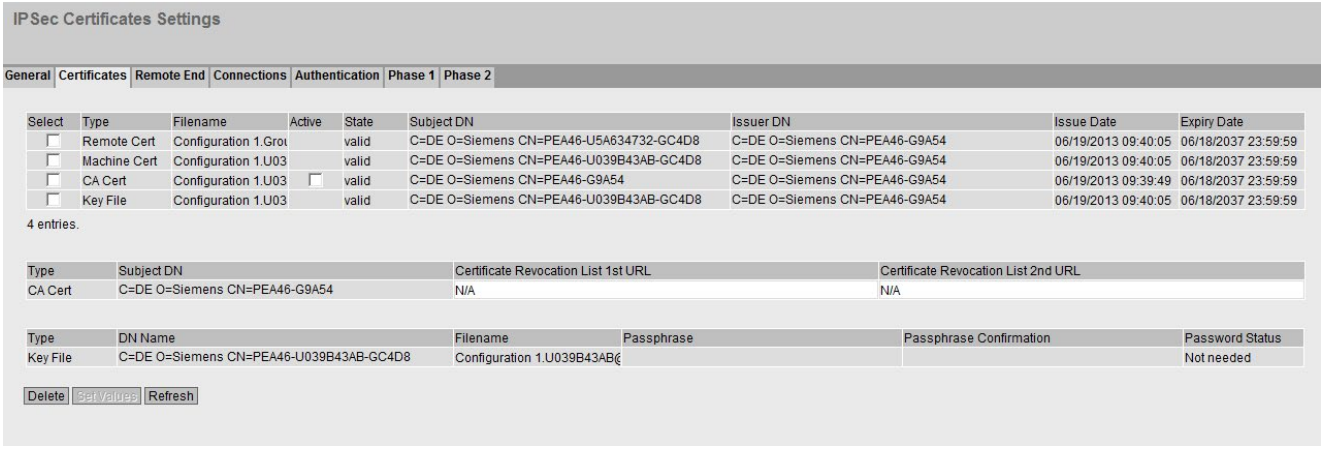
6. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".

   Die Datei wird nun ins Gerät geladen. Nach dem erfolgreichen Laden bestätigen Sie den folgenden Dialog mit "OK".

7. Wiederholen Sie die Schritte 5 und 6 für die PKCS12-Datei.

Ergebnis

Die Zertifikate sind geladen. Unter "Security" > "IPSec VPN" > "Certificates" werden die Zertifikate angezeigt. Die geladenen Zertifikate müssen den Status "valid" besitzen.

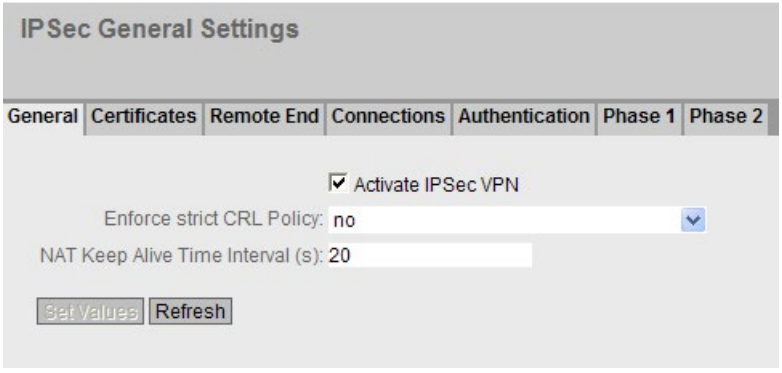


Ab Firmware-Version 4.0 werden die Zertifikate unter "Security" > "Certificates" angezeigt.

3.3.3.2 VPN aktivieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN".



3. Klicken Sie auf "Set Values"

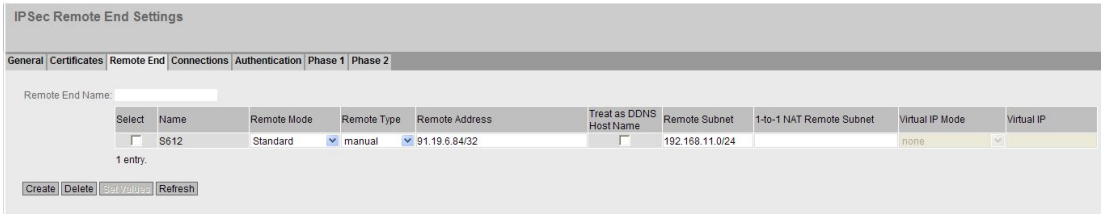
3.3.3.3 VPN-Gegenstelle konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Remote End".
2. Tragen Sie bei "Remote End Name" den Namen der VPN-Gegenstelle (Tunnelendpunkt) ein, z. B. S612.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie die VPN-Gegenstelle mit folgenden Einstellungen aus der Konfigurationsdatei:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN-IP-Adresse des DSL-Routers
Remote Subnet	192.168.11.0/24

5. Klicken Sie auf "Set Values".



3.3.3.4 VPN-Verbindung konfigurieren

Voraussetzung

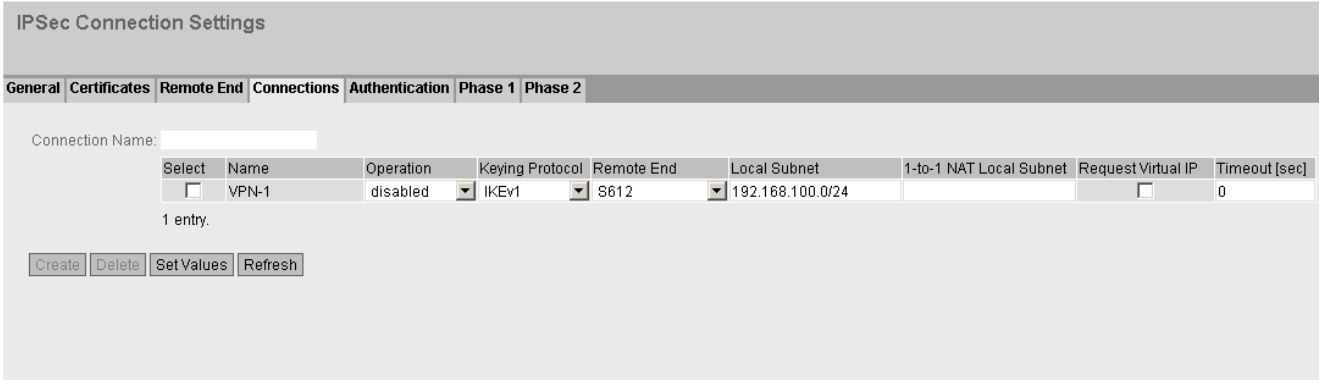
- VPN-Gegenstelle ist angelegt.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Tragen Sie bei "Connection Name" einen Namen für die VPN-Verbindung ein.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie die VPN-Verbindung mit folgenden Einstellungen:

Operation	disabled
Keying Protocol	IKEv1
Remote End	S612 Name der VPN-Gegenstelle
Local Subnet	192.168.100.0/24 Das lokale interne Subnetz 1 in CIDR-Schreibweise.

5. Klicken Sie auf "Set Values".



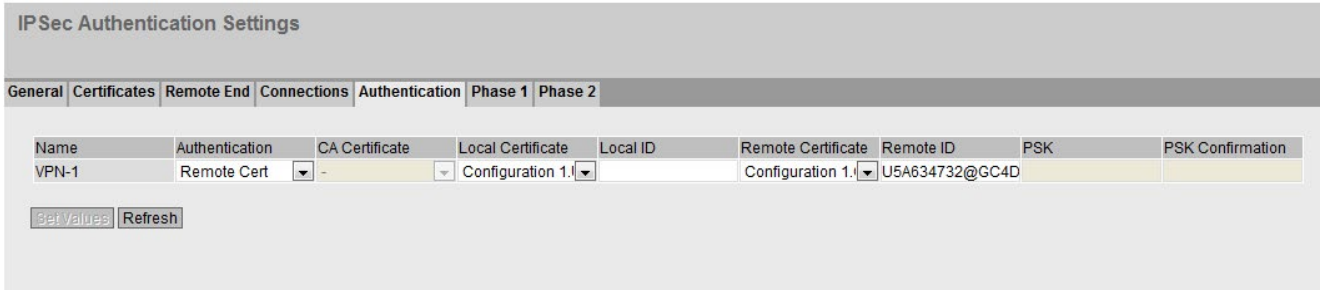
3.3.3.5 VPN-Authentifizierung konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Authentication".
2. Konfigurieren Sie die VPN-Authentifizierung mit folgenden Einstellungen aus der Konfigurationsdatei:

Authentication	Remote Cert
Local Certificate	Projektname.Zeichenfolge.M-800.p12
Remote Certificate	Projektname.Gruppe1.S612.cer
Remote ID	Remote ID aus der Konfigurationsdatei

3. Klicken Sie auf "Set Values".



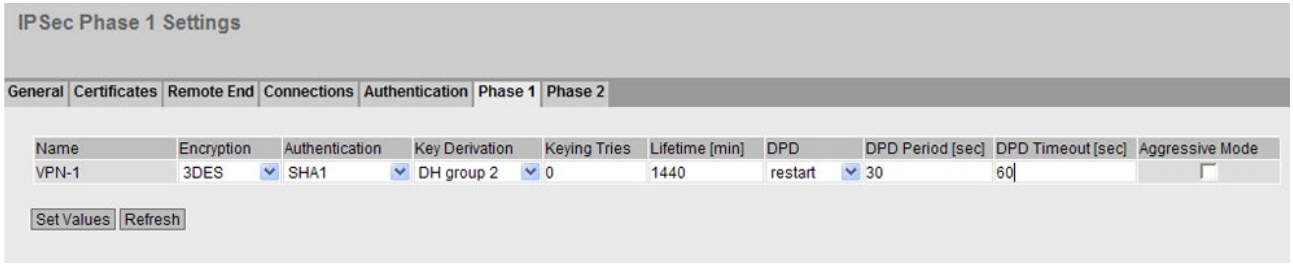
3.3.3.6 Phase 1 und Phase 2 konfigurieren

Phase 1 konfigurieren

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Phase 1".
2. Wählen Sie bei "DPD" "restart" aus.
3. Konfigurieren Sie die Phase 1 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

4. Klicken Sie auf "Set Values".

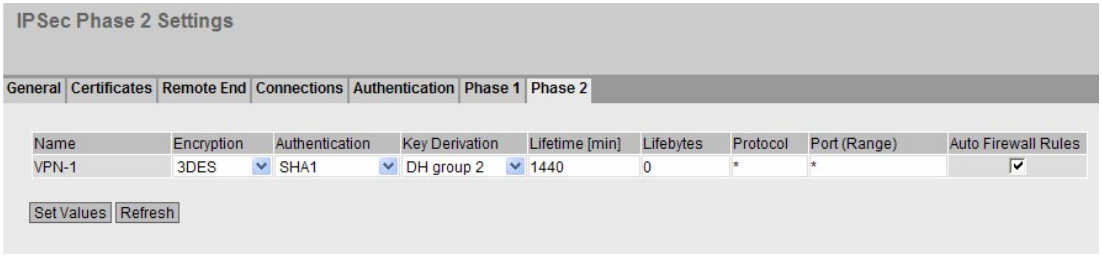


Phase 2 konfigurieren

1. Klicken Sie auf das Register "Phase 2".
2. Konfigurieren Sie für die Phase 2 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

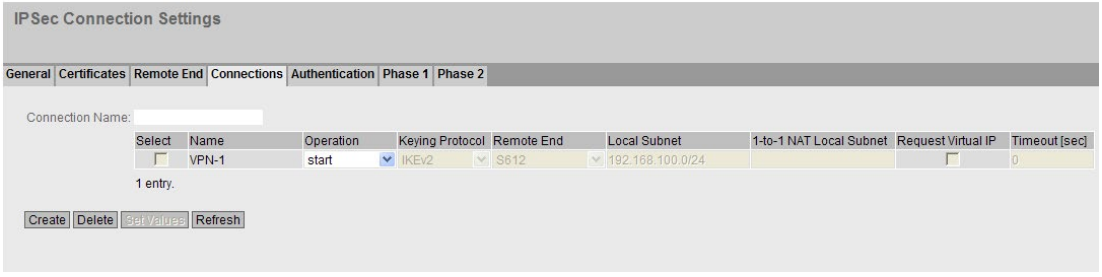
3. Klicken Sie auf "Set Values".



3.3.3.7 VPN-Verbindung aufbauen

Vorgehensweise

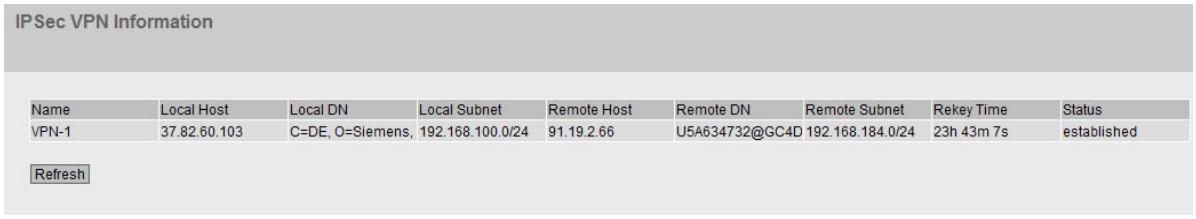
1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Wählen Sie bei "Operation" "start" aus und klicken Sie auf "Set Values".



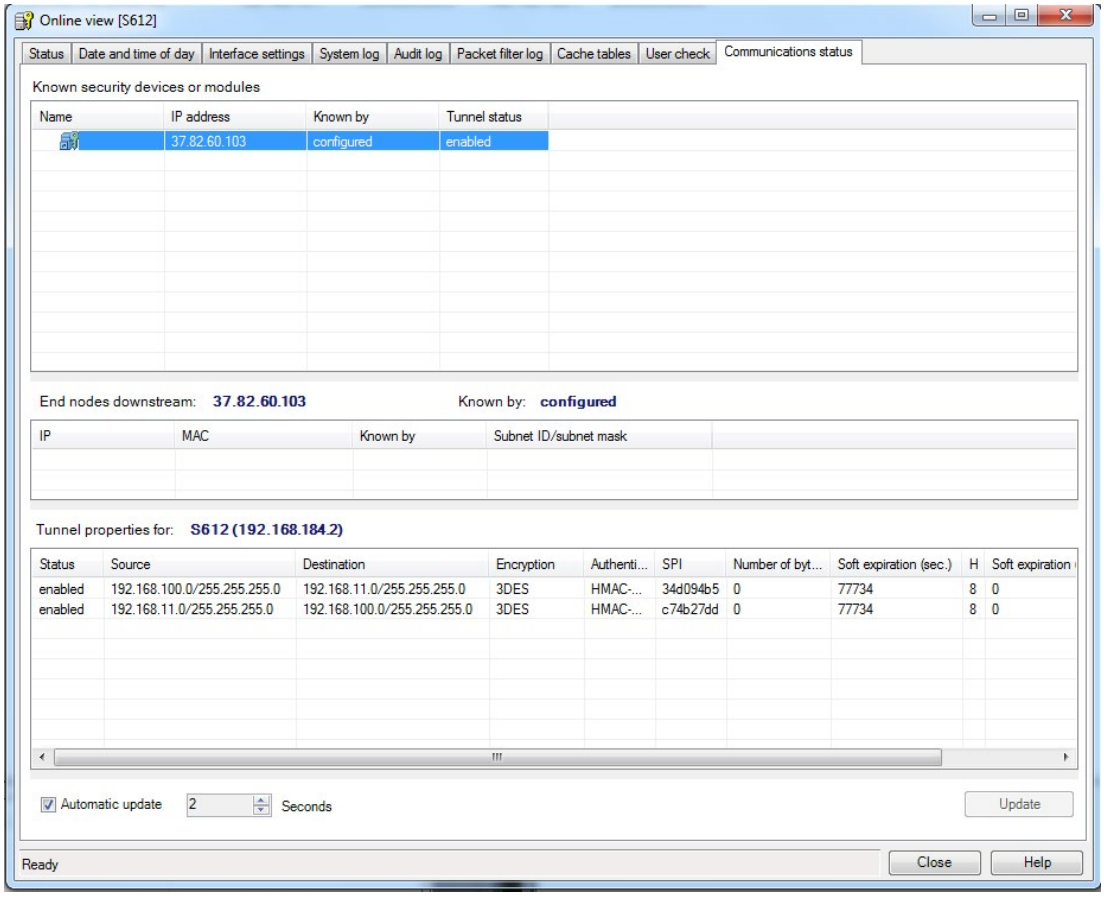
Ergebnis

Das SCALANCE M baut den VPN-Tunnel zum S612 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet am Gerät die LED 🔒 grün.

Weitere Informationen erhalten Sie unter "Information" > "IPSec VPN".



Sie können auch in der Online-Ansicht des SCTs den Status der Tunnelverbindung sehen.


Online view [S612]
Status
Date and time of day
Interface settings
System log
Audit log
Packet filter log
Cache tables
User check
Communications status
Known security devices or modules
Name
IP address
Known by
Tunnel status
37.82.60.103
configured
enabled
End nodes downstream: 37.82.60.103
Known by: configured
IP
MAC
Known by
Subnet ID/subnet mask
Tunnel properties for: S612 (192.168.184.2)
Status
Source
Destination
Encryption
Authenti...
SPI
Number of byt...
Soft expiration (sec.)
H
Soft expiration
enabled
192.168.100.0/255.255.255.0
192.168.11.0/255.255.255.0
3DES
HMAC-...
34d094b5
0
77734
8
0
enabled
192.168.11.0/255.255.255.0
192.168.100.0/255.255.255.0
3DES
HMAC-...
c74b27dd
0
77734
8
0
Automatic update
2
Seconds
Update
Ready
Close
Help

3.4 Firewall bei VPN-Verbindung

Es gibt folgende Möglichkeiten Firewall-Regeln für IPSec anzulegen:

- Automatisch

  Hier werden automatisch die Firewall-Regeln für die spezifizierte VPN-Verbindung angelegt.

- Manuell

  Hier definieren Sie eigene Firewall-Regeln für die spezifizierte VPN-Verbindung.

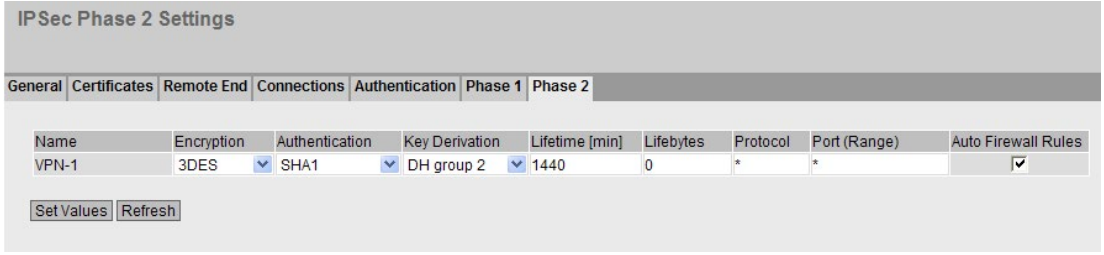
3.4.1 Firewall-Regeln automatisch anlegen

Für das Beispiel wird der VPN-Tunnel verwendet, der im Kapitel "Gesicherter VPN-Tunnel mit Zertifikaten (Seite 170)". Die Geräte haben folgende IP-Adresseinstellung:

		interne Adresse
Internes Netz 1	SCALANCE M-800	192.168.100.1 255.255.255.0
Internes Netz 2	S612	interner Port 192.168.11.2 255.255.255.0

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Phase 2". Die Einstellung "Auto Firewall Rules" ist standardmäßig aktiviert.



Ergebnis

Wenn "Auto Firewall Rule" aktiviert ist, sind folgende Firewall-Regeln aktiv.

Aktion	von / nach	erlaubte Proto-kolle	Für	Quell-IP-Adressen	Ziel-IP-Adressen
Zulas-sen	VPN-Tunnel / Internes Netz 1	TCP / UDP / ICMP	alle Ports bzw. alle ICMP-Pakettypen	192.168.100.0/24	192.168.11.0/24
Zulas-sen	VPN-Tunnel / Internes Netz 2	TCP / UDP / ICMP	alle Ports bzw. alle ICMP-Pakettypen	192.168.11.0/24	192.168.100.0/24
Zulas-sen	internes Netz 2 / VPN-Tunnel	TCP / UDP / ICMP	alle Ports bzw. alle ICMP-Pakettypen	192.168.11.0/24	192.168.100.0/24
Zulas-sen	internes Netz 1 / VPN-Tunnel	TCP / UDP / ICMP	alle Ports bzw. alle ICMP-Pakettypen	192.168.100.0/24	192.168.11.0/24

Durch diese Firewall-Regeln ist der Datenverkehr zwischen dem internen Netz 1 und dem internen Netz 2 uneingeschränkt möglich.

Nicht erlaubt sind HTTP-basierte Zugriffe auf die entfernte VPN-Gegenstelle. Im Kapitel "Firewall-Regeln manuell anlegen (Seite 145)" wird die entsprechende Firewall-Regel angelegt.

3.4.2 Firewall-Regeln manuell anlegen

Voraussetzung

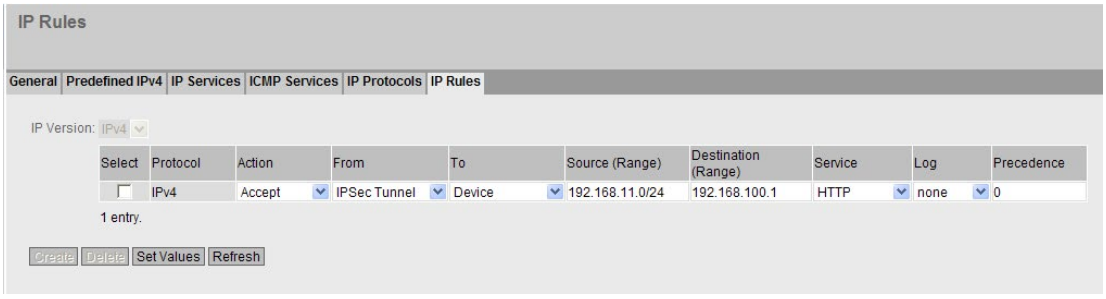
Der IP-Dienst HTTP ist angelegt, siehe Kapitel "Auto-Hotspot".

Allen den HTTP-basierten Zugriff durch den VPN-Tunnel erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
2. Konfigurieren Sie die Firewall-Regel für HTTP mit folgenden Einstellungen:

Action	Accept
From	IPSecTunnel
To	Device
Source (Range)	192.168.11.0/24 (alle Geräte des entfernten internen Netzes 2)
Destination (Range)	192.168.100.1 (auf das gewünschte Gerät)
Service	HTTP

3. Klicken Sie auf "Set Values". Das SCALANCE M ist durch den VPN-Tunnel via HTTP zu erreichen und ist über das WBM konfigurierbar.

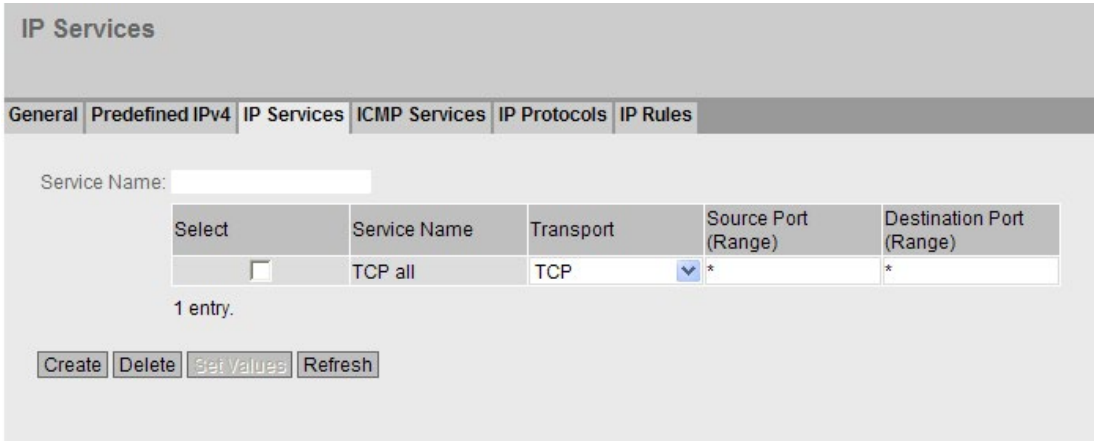


Einem bestimmten Gerät den TCP-basierten Zugriff durch den VPN-Tunnel erlauben

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Services".
2. Tragen Sie bei "Service Name" "TCP all" ein und klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
3. Konfigurieren Sie den Dienst mit folgender Einstellung:

Transport	TCP

4. Klicken Sie auf "Set Values".



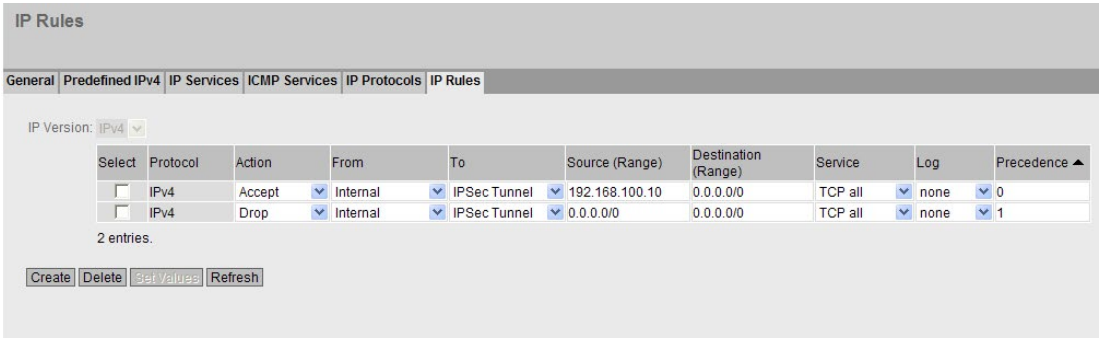
5. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
6. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
7. Konfigurieren Sie die Firewall-Regel mit folgenden Einstellungen:

Action	Accept
From	Internal
To	IPSecTunnel
Source (Range)	192.168.100.10 (nur das Gerät darf vom internen Netz 1 durch den VPN-Tunnel mit TCP kommunizieren)
Destination (Range)	0.0.0.0/0 (auf alle Adressen)
Service	TCP all

8. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.
9. Konfigurieren Sie die zweite Firewall-Regel mit folgenden Einstellungen:

Action	Drop
From	Internal
To	IPSecTunnel
Source (Range)	0.0.0.0/0 (Unterbindet den TCP-Datenverkehr zwischen dem internen Netz und dem, durch den VPN-Tunnel verbundenen, Remote-Netz.)
Destination (Range)	
Service	TCP all

10.Klicken Sie auf "Set Values".



VPN-Tunnel zwischen SCALANCE M-800 und Security-CPs

4

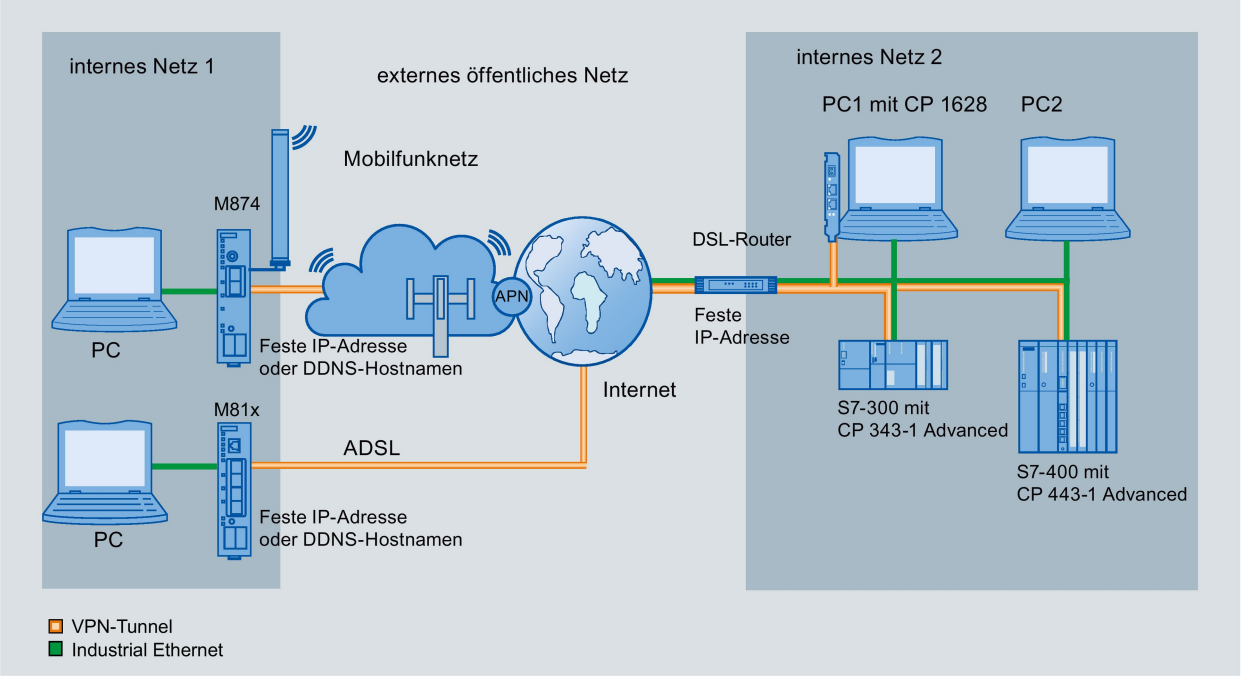
4.1 Prinzipielles Vorgehen

In diesen Beispielen wird ein gesicherter VPN-Tunnel zwischen einem SCALANCE M-800 und dem CP 1628 projektiert.

- Beispiel 1: Gesicherter VPN-Tunnel mit PreShared Keys (PSK)
- Beispiel 2: Gesicherter VPN-Tunnel mit Zertifikaten

Anstelle von CP 1628 kann auch ein CP 343-1 Advanced oder CP 434-1 Advanced verwendet werden.

Aufbau



Internes Netz 1 - Anschluss an SCALANCE M-800

- Im internen Netz wird im Testaufbau ein Netzknoten durch einen Admin-PC realisiert, der an eine Ethernet-Schnittstelle des SCALANCE M angeschlossen ist.
  - Admin-PC: repräsentiert einen Teilnehmer des internen Netzwerks
  - M-800: SCALANCE M-Modul zum Schutz des internen Netzwerks
- Anbindung an das externe, öffentliche Netzwerk.
  - Drahtlos über die Antenne des M874 an das Mobilfunknetz.
  - Kabelgebunden über die RJ45-Buchse des M81x an ADSL.

Internes Netz 2 - Anschluss an einen Port des CP 1628

- Im internen Netz wird im Testaufbau der Netzknoten jeweils durch einen PC realisiert, der an den internen Port des Security-Moduls angeschlossen ist.
  - PC1 mit Security-Modul 1: PC mit CP 1628 zum Schutz des internen Netzwerks
  - PC2: PC mit der Konfigurationssoftware Security Configuration Tool und STEP 7

    Der PC repräsentiert einen Teilnehmer des internen Netzwerks.
- Anbindung an das externe, öffentliche Netzwerk über DSL-Router

  Der Zugriff auf das Internet erfolgt über ein DSL-Modem bzw. einen DSL-Router, welche an einen der beiden Ports des Security-Moduls angeschlossen wird.

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an das Mobilfunknetz
  - 1x M874 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - 1x geeignete Antenne
  - 1x SIM-Karte ihres Mobilfunkanbieters. Die entsprechenden Dienste z. B. Internet sind freigeschaltet.
- Anbindung an ADSL
  - 1x M812 oder 1x M816 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - ADSL-Zugang ist freigeschaltet
- 1x PC mit CP 1628
- 1x PC mit der Konfigurationssoftware Security Configuration Tool und STEP 7.
- 1x DSL-Modem oder DSL-Router
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen

		interne Adresse	externe Adresse
Internes Netz 1	M-800	192.168.100.1 255.255.255.0	Feste IP-Adresse, z. B. 90.90.90.90 Providerabhängig Alternativ kann auch der DDNS-Hostname verwendet werden.
	Admin-PC	192.168.100.20 255.255.255.0	
Internes Netz 2	DSL-Router	192.168.184.254 255.255.255.0	Feste IP-Adresse (WAN-IP-Adresse), z. B. 91.19.6.84
	PC1 mit CP 1628	Für CP 1628: Die IP-Adresse der NDIS-Schnittstelle, z. B. 192.168.184.10. (wird im PC1 projektiert) Für CP 343-1 Advanced oder CP 434-1 Advanced: Die IP-Adresse der PROFINET-Schnittstelle.	Für CP 1628: Die IP-Adresse der Industrial Ethernet-Schnittstelle, z. B. 192.168.184.2. Für CP 343-1 Advanced oder CP 434-1 Advanced: Die IP-Adresse der GBit-Schnittstelle.
	PC2	192.168.184.20 255.255.255.0	

Voraussetzung

- Der CP 1628 ist über den DSL-Router mit dem Internet verbunden.
- In den Eigenschaften des CPs ist die interne IP-Adresse des DSL-Routers als Standard-Gateway konfiguriert.
- Das SCALANCE M-800 ist mit dem WAN verbunden, siehe "SCALANCE M-800 mit dem WAN verbinden (Seite 11)".
- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

Beispiel 1: Gesicherter VPN-Tunnel mit PSK

VPN-Tunnel mit dem SCT V3.x konfigurieren

1. Projekt und Module mit den SCT anlegen (Seite 153)
2. Tunnelverbindung projektieren (Seite 155)
3. Konfiguration in CP laden und M-800-Konfiguration abspeichern (Seite 157)

VPN-Tunnel mit dem SCT V4.x konfigurieren

1. Projekt und Module mit den SCT anlegen (Seite 159)
2. Tunnelverbindung projektieren (Seite 161)
3. Konfiguration in CP laden und M-800-Konfiguration abspeichern (Seite 163)

SCALANCE M-800 konfigurieren

1. VPN aktivieren (Seite 164)
2. VPN-Gegenstelle konfigurieren (Seite 165)
3. VPN-Verbindung konfigurieren (Seite 165)
4. VPN-Authentifizierung konfigurieren (Seite 166)
5. Phase 1 und Phase 2 konfigurieren (Seite 167)
6. VPN-Verbindung aufbauen (Seite 168)

Beispiel 2: Gesicherter VPN-Tunnel mit Zertifikaten

VPN-Tunnel mit dem SCT V3.x konfigurieren

1. Projekt und Module mit den SCT anlegen (Seite 170)
2. Tunnelverbindung projektieren (Seite 172)
3. Konfiguration in CP laden und M-800-Konfiguration abspeichern (Seite 174)

VPN-Tunnel mit dem SCT V3.x konfigurieren

1. Projekt und Module mit den SCT anlegen (Seite 176)
2. Tunnelverbindung projektieren (Seite 178)
3. Konfiguration in CP laden und M-800-Konfiguration abspeichern (Seite 180)

SCALANCE M-800 konfigurieren

1. Zertifikat laden (Seite 181)
2. VPN aktivieren (Seite 183)
3. VPN-Gegenstelle konfigurieren (Seite 184)
4. VPN-Verbindung konfigurieren (Seite 185)
5. VPN-Authentifizierung konfigurieren (Seite 186)
6. Phase 1 und Phase 2 konfigurieren (Seite 187)
7. VPN-Verbindung aufbauen (Seite 189)

4.2 Gesicherter VPN-Tunnel mit PSK

4.2.1 VPN-Tunnel mit dem SCT V3.x konfigurieren

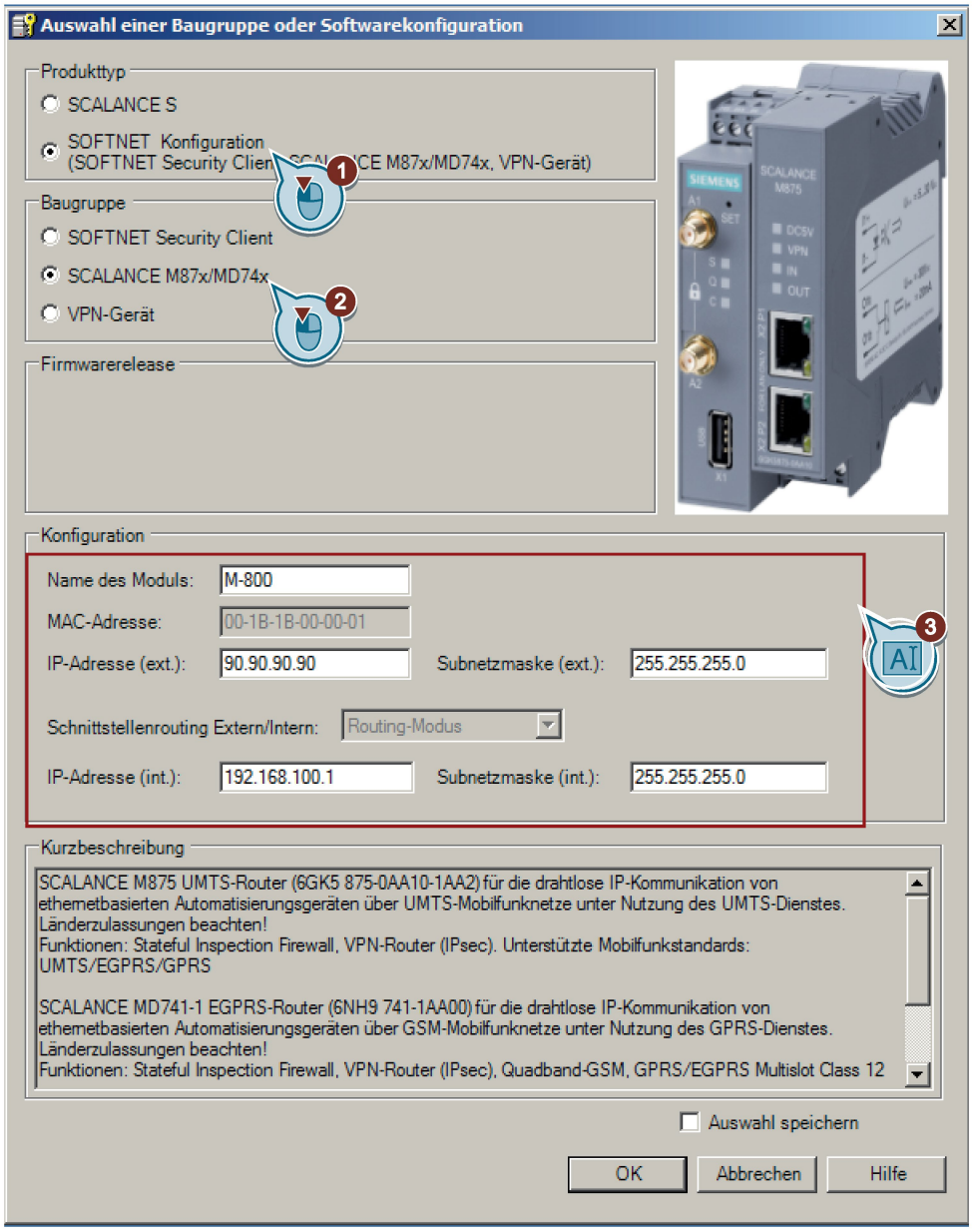
4.2.1.1 Projekt und Module mit den SCT anlegen

Vorgehensweise

1. Aktivieren Sie in den Objekteigenschaften des CP 1628 im Register "Security" das Optionskästchen "Security aktivieren".
2. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an.

   Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
3. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt.
4. Öffnen Sie in HW Konfig das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
   Der angelegte CP wird in der Liste der konfigurierten Module angezeigt.
5. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Modul" ein zweites Modul.

6. Tragen Sie die dem SCALANCE M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 149)" ein.



7. Bestätigen Sie den Dialog mit "OK".

Ergebnis

Der CP und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

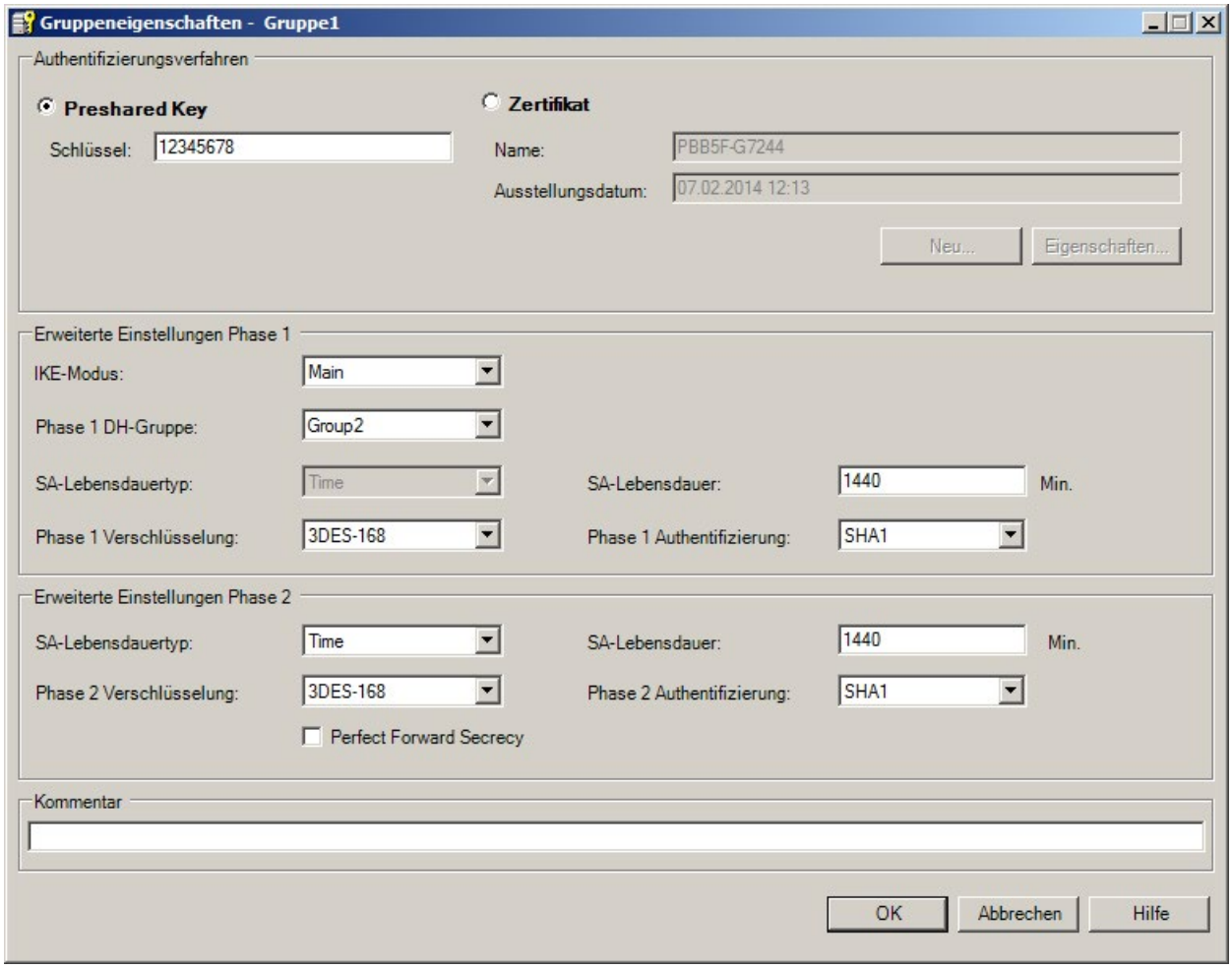
4.2.1.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M-800 und der CP der gleichen VPN-Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den CP. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.
5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen

6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

7. Speichern Sie das Projekt mit dem Menübefehl "Projekt" > "Speichern" ab.

Ergebnis

Die Konfiguration der Tunnelverbindung ist abgeschlossen. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

4.2.1.3 Konfiguration in CP laden und M-800-Konfiguration abspeichern

Konfiguration in CP laden

1. Schließen Sie das Security Configuration Tool.
2. Wählen Sie in HW Konfig das Menü "Station" > "Speichern und Übersetzen".
3. Laden Sie die neue Konfiguration über das Menü "Zielsystem" > "Laden in Baugruppe..." auf das Security-Modul.
   - Für CP 1628: Wurde der Ladevorgang fehlerfrei abgeschlossen, startet das Security-Modul automatisch und die neue Konfiguration ist aktiviert.
   - Für CP 343-1 Advanced oder CP 434-1 Advanced: Starten Sie die S7-CPU nach dem Laden neu, um die neue Konfiguration zu aktivieren

SCALANCE M-800-Konfiguration abspeichern

1. Öffnen Sie in STEP 7 das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
2. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...".
3. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis.

Ergebnis

In das Projektverzeichnis wird folgende Datei abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800.

Konfigurationsdatei	Einstellungen im WBM
IPSec VPN > Verbindungen > VPN Standard Modus - Einstellungen bearbeiten	Security > IPSec VPN > Remote End > Remote Mode: Standard
Adresse des VPN Gateways der Gegenstelle: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentisierungsverfahren: Pre Shared Key	Security > IPSec VPN > Authentication > Authentication: PSK

Konfigurationsdatei	Einstellungen im WBM
Pre Shared Key: 12345678	Security > IPSec VPN > Authentication > PSK und PSK Confirmation: 12345678
Remote ID: U28098881@GEA32	Security > IPSec VPN > Authentication > Remote ID nicht benötigt. Im WBM wird die IP-Adresse der Industrial Ethernet-Schnittstelle eingetragen. In diesem Beispiel ist das die 192.168.184.2
Lokale ID: U269159D5@GEA32	Security > IPSec VPN > Authentication > Local ID nicht benötigt. Der Eintrag bleibt im WBM leer.
Adresse des gegenüberliegenden Netzes: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Netzmaske des gegenüberliegenden Netzes: 255.255.255.0	
Adresse des lokalen Netzes: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Netzmaske des lokalen Netzes: 255.255.255.0	
IPSec VPN > Verbindungen > IKE Bearbeiten	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA Hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA Modus: Main Mode	--
ISAKMP-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPSec-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPSec-SA Hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPSec-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 2 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--
DH/PFS-Gruppe: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: An	--
DPD-Verzögerung (Sekunden): 150	--
DPD-Timeout (Sekunden): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD-Maximale Fehlversuche: 5	--

4.2.2 VPN-Tunnel mit dem SCT V4.x konfigurieren

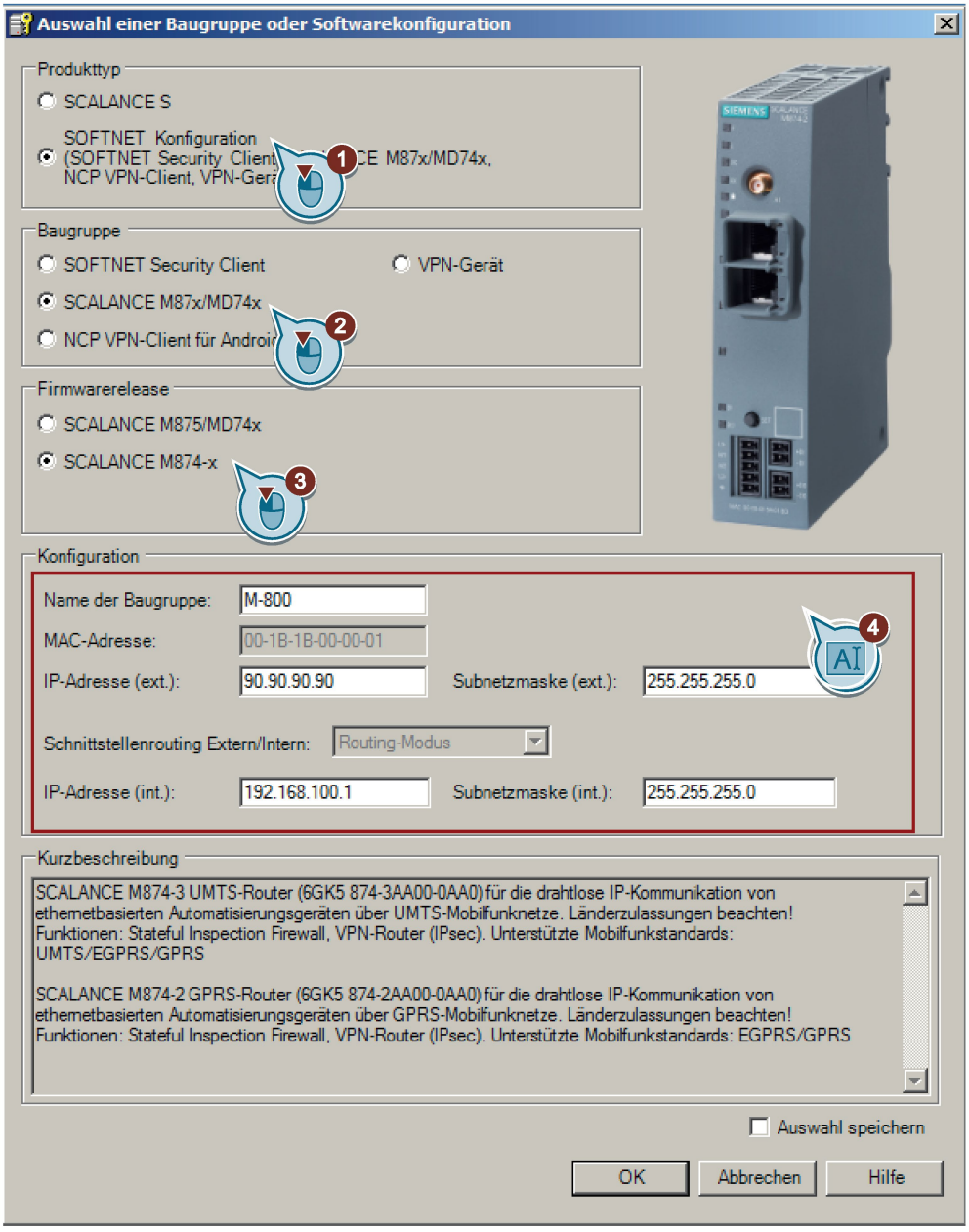
4.2.2.1 Projekt und Module mit den SCT anlegen

Vorgehensweise

1. Aktivieren Sie in den Objekteigenschaften des CP 1628 im Register "Security" das Optionskästchen "Security aktivieren".
2. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an.

   Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
3. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt.
4. Öffnen Sie in HW Konfig das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
   Der angelegte CP wird in der Liste der konfigurierten Module angezeigt.

5. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Baugruppe" ein zweites Modul.



6. Tragen Sie die dem SCALANCE M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 149)" ein.
7. Bestätigen Sie den Dialog mit "OK".

Ergebnis

Der CP und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

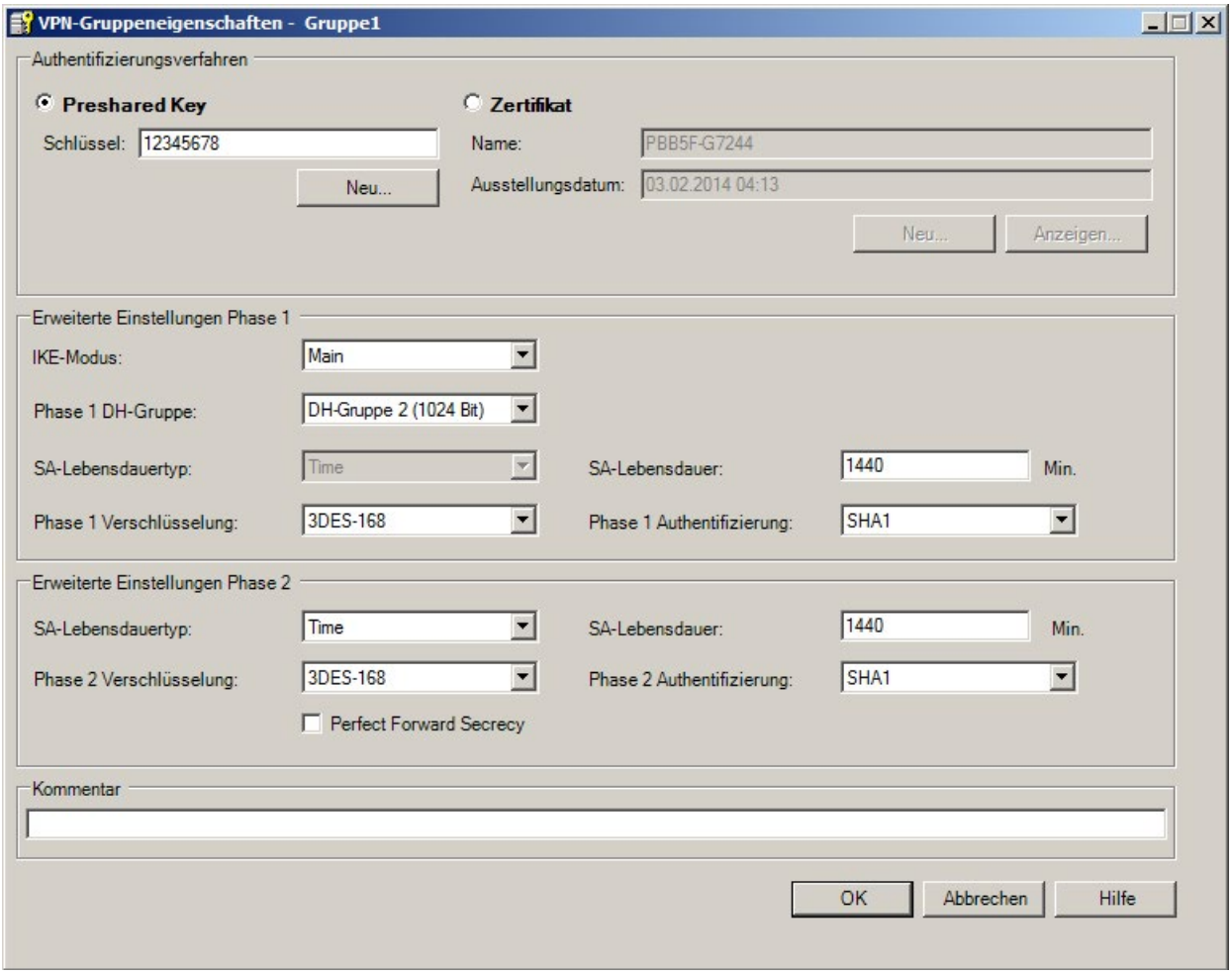
4.2.2.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M-800 und der CP der gleichen VPN-Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden.

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Bauguppen".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den CP. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.
5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen

6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen.



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

7. Speichern Sie das Projekt mit dem Menübefehl "Projekt" > "Speichern" ab.

Ergebnis

Die Konfiguration der Tunnelverbindung ist abgeschlossen. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

4.2.2.3 Konfiguration in CP laden und M-800-Konfiguration abspeichern

Konfiguration in CP laden

1. Schließen Sie das Security Configuration Tool.
2. Wählen Sie in HW Konfig das Menü "Station" > "Speichern und Übersetzen".
3. Laden Sie die neue Konfiguration über das Menü "Zielsystem" > "Laden in Baugruppe..." auf das Security-Modul.
   - Für CP 1628: Wurde der Ladevorgang fehlerfrei abgeschlossen, startet das Security-Modul automatisch und die neue Konfiguration ist aktiviert.
   - Für CP 343-1 Advanced oder CP 434-1 Advanced: Starten Sie die S7-CPU nach dem Laden neu, um die neue Konfiguration zu aktivieren

SCALANCE M-800-Konfiguration abspeichern

1. Öffnen Sie in STEP 7 das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
2. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Modul(e) ...".
3. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis.

Ergebnis

In das Projektverzeichnis wird folgende Datei abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt

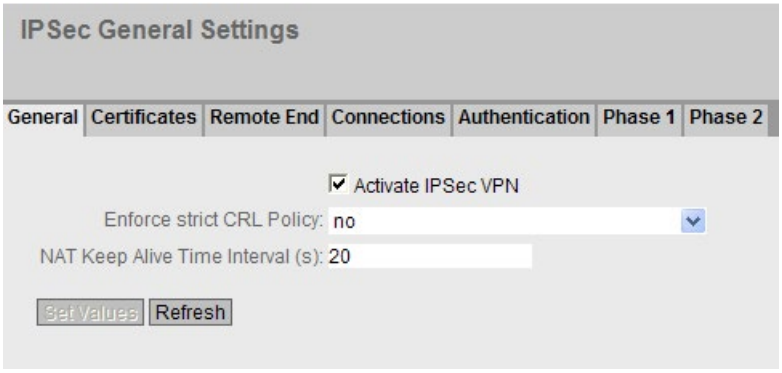
Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800. Folgen Sie den Anweisungen in der Konfigurationsdatei.

4.2.3 SCALANCE M-800 konfigurieren

4.2.3.1 VPN aktivieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN".



3. Klicken Sie auf "Set Values"

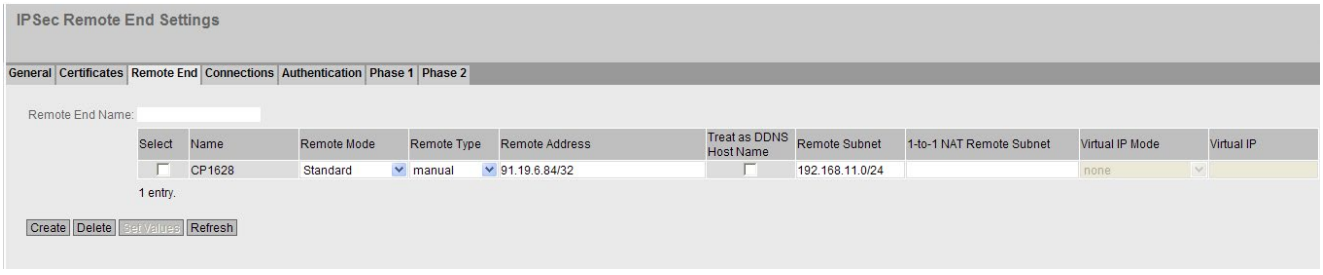
4.2.3.2 VPN-Gegenstelle konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Remote End".
2. Tragen Sie bei "Remote End Name" den Namen der VPN-Gegenstelle (Tunnelendpunkt) ein, z. B. CP1628.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie für die Beispielkonfiguration die VPN-Gegenstelle mit folgenden Einstellungen:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN-IP-Adresse des DSL-Routers
Remote Subnet	192.168.184.0/24

5. Klicken Sie auf "Set Values".



4.2.3.3 VPN-Verbindung konfigurieren

Voraussetzung

- VPN-Gegenstelle ist angelegt.

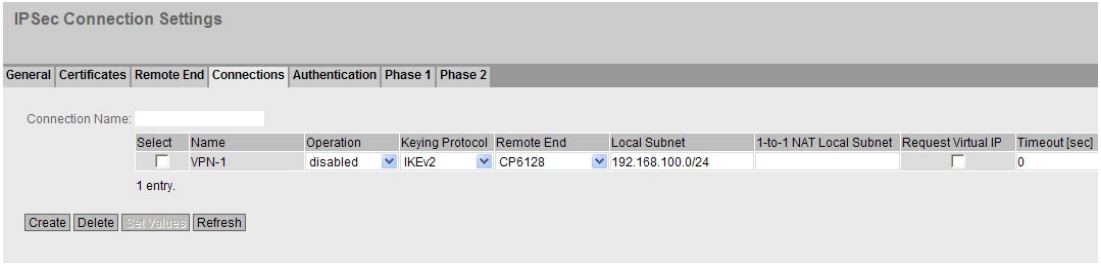
Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Geben Sie bei "Connection Name" einen Namen für die VPN-Verbindung ein.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.

4. Konfigurieren Sie für die Beispielkonfiguration die VPN-Verbindung mit folgenden Einstellungen:

Operation	disabled
Keying Protocol	IKEv1
Remote End	CP1628 Name der VPN-Gegenstelle
Local Subnet	192.168.100.0/24 Das lokale interne Subnetz 1 in CIDR-Schreibweise.

5. Klicken Sie auf "Set Values".



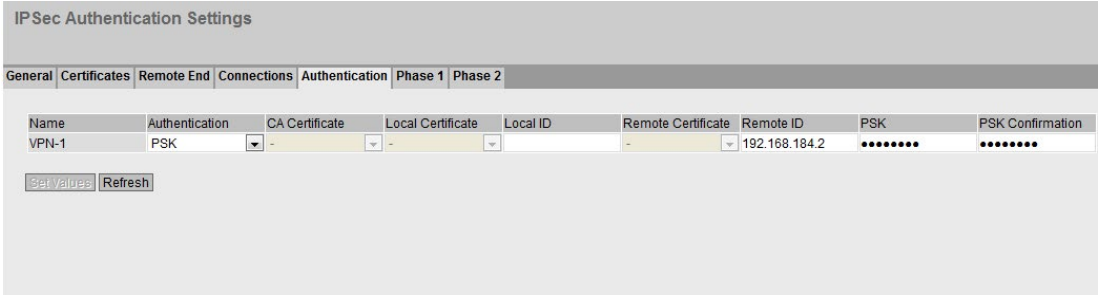
4.2.3.4 VPN-Authentifizierung konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Authentication".
2. Konfigurieren Sie die VPN-Authentifizierung mit folgenden Einstellungen:

Authentication	PSK
Local ID	kein Eintrag notwendig
Remote ID	192.168.184.2 Die IP-Adresse der VPN-Gegenstelle.
PSK / PSK Confirmation	12345678 Den Schlüssel, den Sie im SCT projektiert haben.

3. Klicken Sie auf "Set Values".



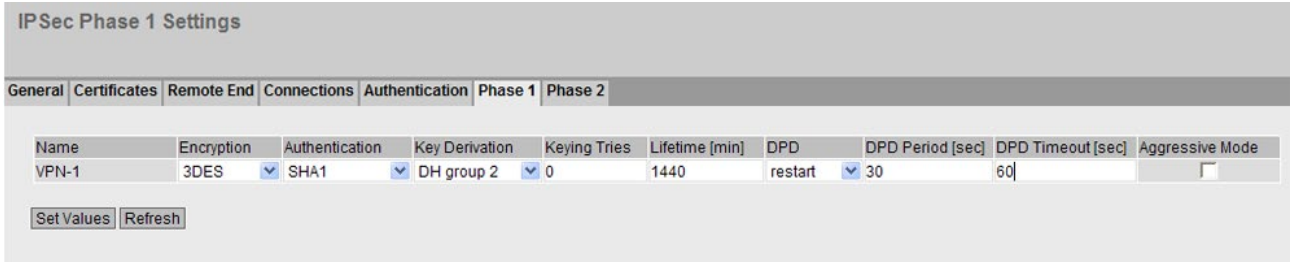
4.2.3.5 Phase 1 und Phase 2 konfigurieren

Phase 1 konfigurieren

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Phase 1".
2. Wählen Sie bei "DPD" "restart" aus.
3. Konfigurieren Sie die Phase 1 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

4. Klicken Sie auf "Set Values".

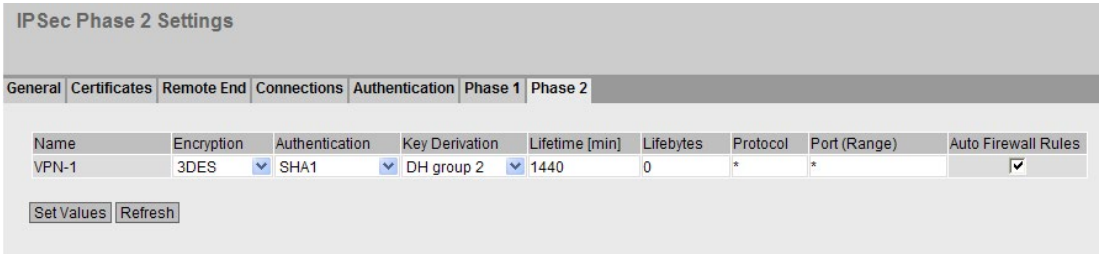


Phase 2 konfigurieren

1. Klicken Sie auf das Register "Phase 2".
2. Konfigurieren Sie für die Phase 2 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

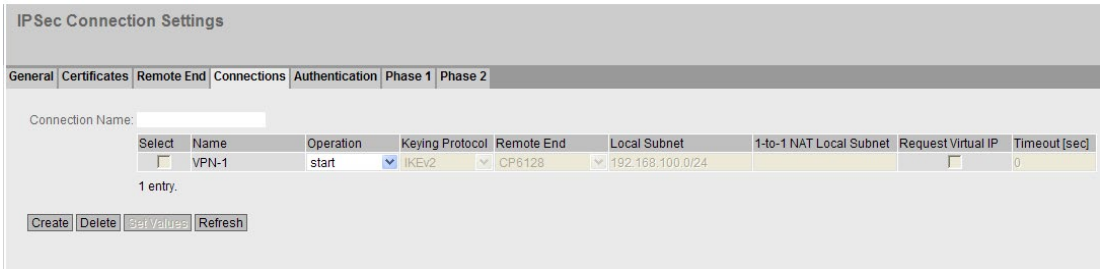
3. Klicken Sie auf "Set Values".



4.2.3.6 VPN-Verbindung aufbauen

Vorgehensweise

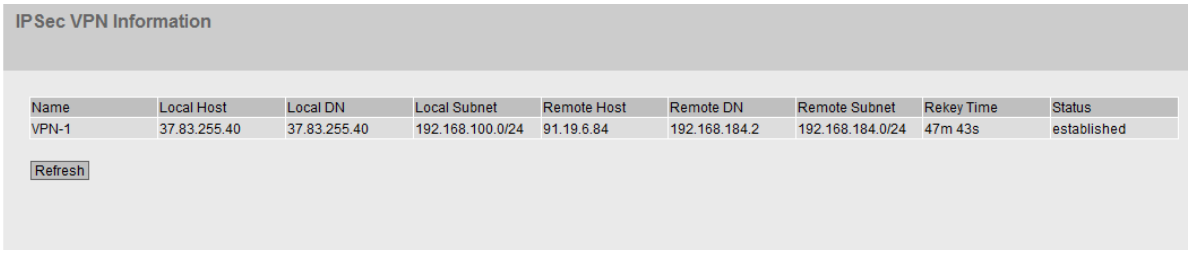
1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Wählen Sie bei "Operation" "start" aus und klicken Sie auf "Set Values".



Ergebnis

Das SCALANCE M-800 baut den VPN-Tunnel zum CP 1628 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet am Gerät die LED grün.

Weitere Informationen erhalten Sie unter "Information" > "IPSec VPN".



4.3 Gesicherter VPN-Tunnel mit Zertifikaten

4.3.1 VPN-Tunnel mit dem SCT V3.x konfigurieren

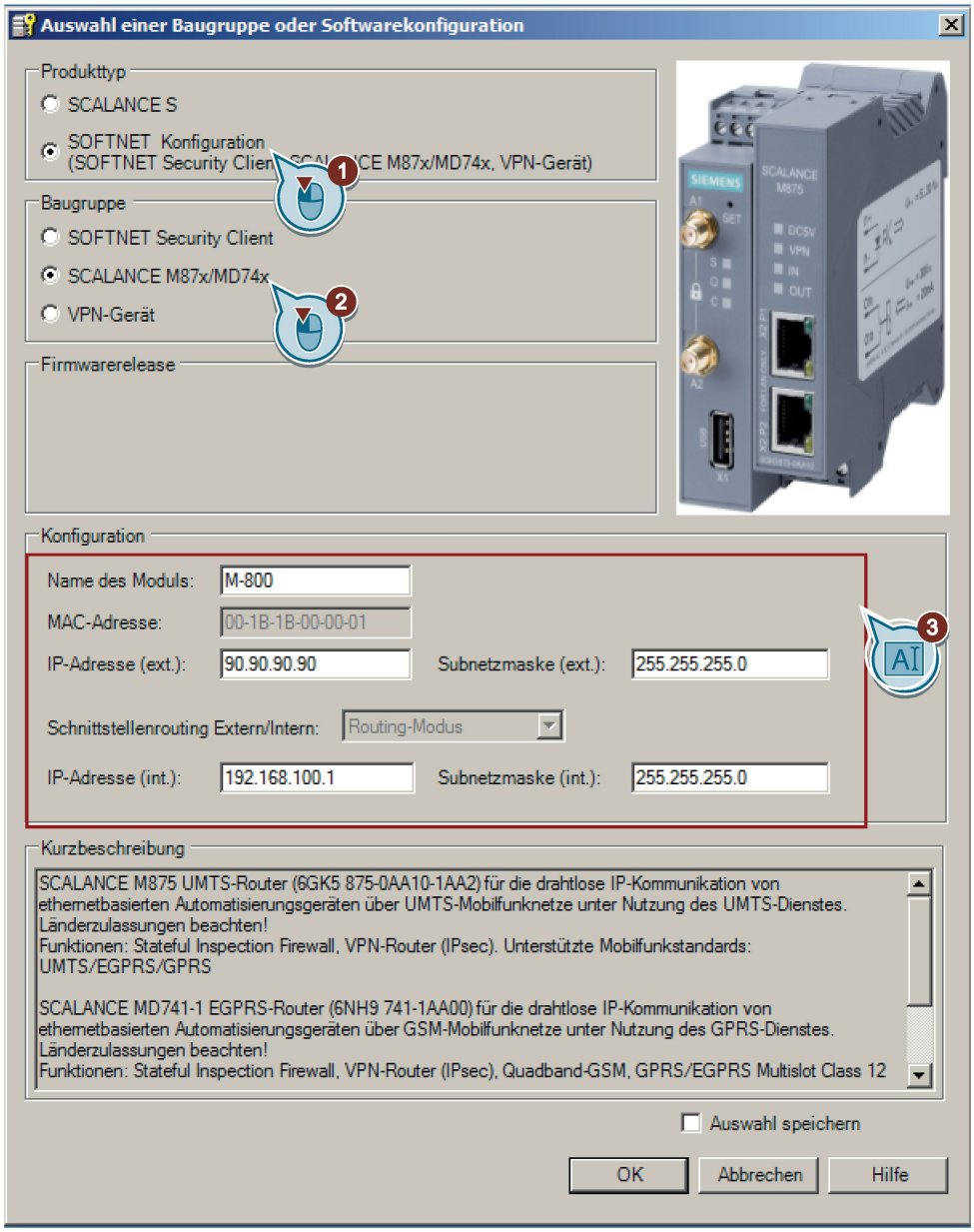
4.3.1.1 Projekt und Module mit den SCT anlegen

Vorgehensweise

1. Aktivieren Sie in den Objekteigenschaften des CP 1628 im Register "Security" das Optionskästchen "Security aktivieren".
2. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an.

   Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
3. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt.
4. Öffnen Sie in HW Konfig das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
   Der angelegte CP wird in der Liste der konfigurierten Module angezeigt.
5. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Modul" ein zweites Modul.

6. Tragen Sie die dem SCALANCE M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 149)" ein.



7. Bestätigen Sie den Dialog mit "OK".

Ergebnis

Der CP und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

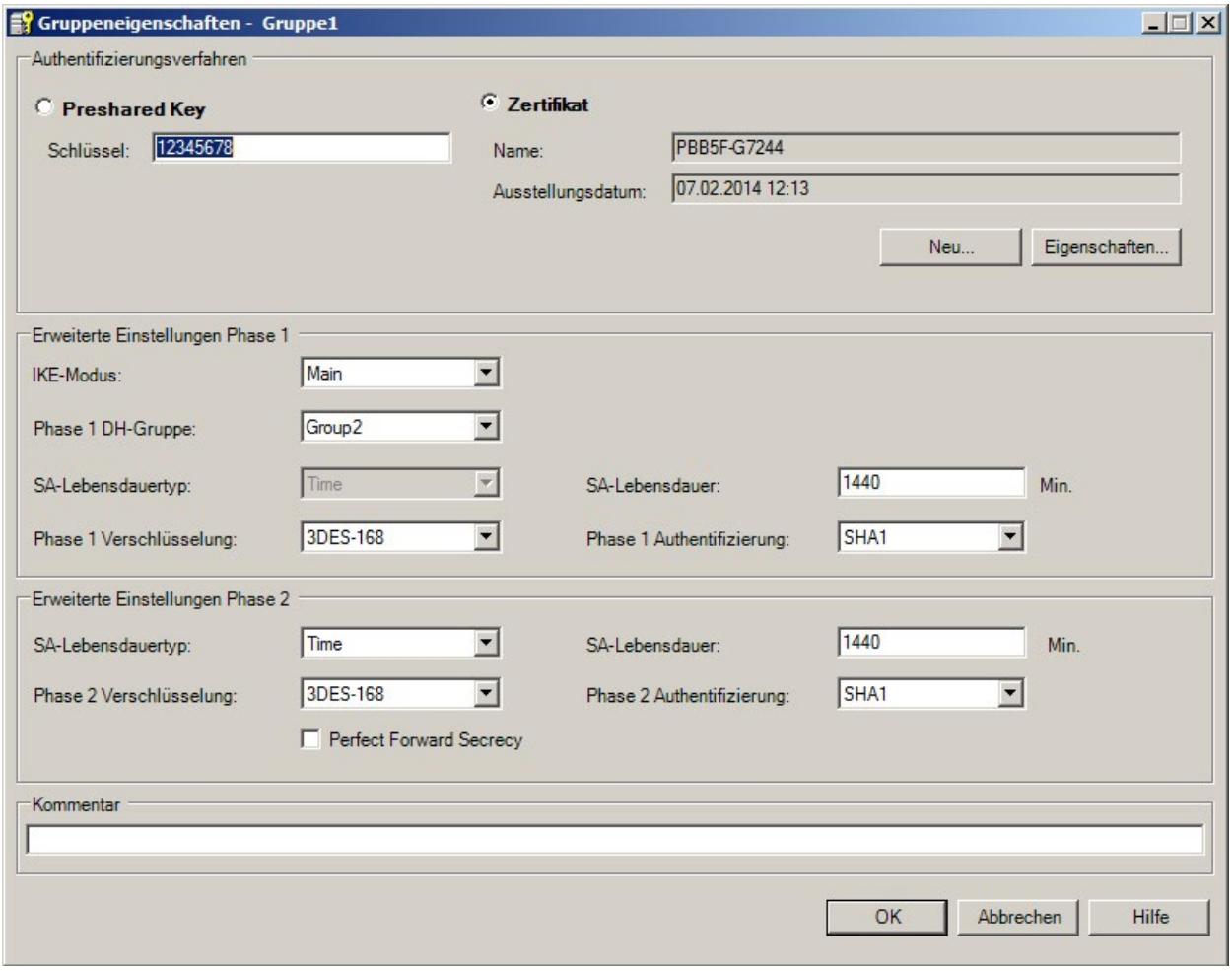
4.3.1.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M-800 und der CP der gleichen Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden..

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den CP. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.
5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen

6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen:



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

7. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

Ergebnis

Die Konfiguration der Tunnelverbindung ist abgeschlossen. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

4.3.1.3 Konfiguration in CP laden und M-800-Konfiguration abspeichern

Konfiguration in CP laden

1. Schließen Sie das Security Configuration Tool.
2. Wählen Sie in HW Konfig das Menü "Station" > "Speichern und Übersetzen".
3. Laden Sie die neue Konfiguration über das Menü "Zielsystem" > "Laden in Baugruppe..." auf das Security-Modul.
   - Für CP 1628: Wurde der Ladevorgang fehlerfrei abgeschlossen, startet das Security-Modul automatisch und die neue Konfiguration ist aktiviert.
   - Für CP 343-1 Advanced oder CP 434-1 Advanced: Starten Sie die S7-CPU nach dem Laden neu, um die neue Konfiguration zu aktivieren.

SCALANCE M-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n) ...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats, z. B. Di1S+Xo?.

Ergebnis

In das Projektverzeichnis werden folgende Dateien abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt
- PKCS12-Datei: Projektname.Zeichenfolge.M-800.p12
- Gegenstellenzertifikat: Projektname.Gruppe1.CP.cer

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800 einschließlich einer Information über die zusätzlich erzeugten Zertifikate.

Konfigurationsdatei	Einstellungen im WBM
IPSec VPN > Zertifikate Gegenstellen Zertifikat hochladen: Configuration-1.Gruppe1.CP.cer PKCS12 Datei (.p12) hochladen: Configuration-1.U800CB3FF@G471C.M-800.p12	System > Load&Save > HTTP > IPSecCert : Load
IPSec VPN > Verbindungen > VPN Standard Modus - Einstellungen bearbeiten	Security > IPSec VPN > Remote End > Remote Mode: Standard
Adresse des VPN Gateways der Gegenstelle: 91.19.6.84	Security > IPSec VPN > Remote End > Remote Address: 91.19.6.84/32
Authentisierungsverfahren: X.509 Gegenstellenzertifikat	Security > IPSec VPN > Authentication > Authentication: Remote Cert
Gegenstellen Zertifikat: Configuration-1.Gruppe1.CP.cer	Security > IPSec VPN > Authentication > Remote Certificate: Configuration-1.Gruppe1.CP.cer

Konfigurationsdatei	Einstellungen im WBM
Remote ID: U5A634732@GC4D8	Security > IPSec VPN > Authentication > Remote ID: U5A634732@GC4D8
Adresse des gegenüberliegenden Netzes: 192.168.184.0	Security > IPSec VPN > Remote End > Remote Subnet: 192.168.184.0/24
Netzmaske des gegenüberliegenden Netzes: 255.255.255.0	
Adresse des lokalen Netzes: 192.168.100.0	Security > IPSec VPN > Connections > Local Subnet: 192.168.100.0/24
Netzmaske des lokalen Netzes: 255.255.255.0	
IPSec VPN > Verbindungen > IKE Bearbeiten	Security > IPSec VPN > Connections > Keying Protocol: IKEv1
Phase 1 - ISAKMP SA	--
ISAKMP-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 1 > Encryption: 3DES
ISAKMP-SA Hash: SHA-1	Security > IPSec VPN > Phase 1 > Authentication: SHA-1
ISAKMP-SA Modus: Main Mode	--
ISAKMP-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Phase 2 - IPSec SA	--
IPSec-SA Verschlüsselung: 3DES-168	Security > IPSec VPN > Phase 2 > Encryption: 3DES
IPSec-SA Hash: SHA-1	Security > IPSec VPN > Phase 2 > Authentication: SHA-1
IPSec-SA Lebensdauer (Sekunden): 86400 In der Textdatei ist der Wert in Sekunden angegeben. Im WBM muss der Wert in Minuten eingegeben werden.	Security > IPSec VPN > Phase 1 > Liftime [min]: 1440
Perfect Forward Secrecy (PFS): Nein	--
DH/PFS-Gruppe: DH-2 1024	Security > IPSec VPN > Phase 1 > Key Derivation: DH group 2 Security > IPSec VPN > Phase 2 > Key Derivation: DH group 2
NAT-T: An	--
DPD-Verzögerung (Sekunden): 150	--
DPD-Timeout (Sekunden): 60	Security > IPSec VPN > Phase 1 > DPD-Timeout [sec]: 60
DPD-Maximale Fehlversuche: 5	--

4.3.2 VPN-Tunnel mit dem SCT V4.x konfigurieren

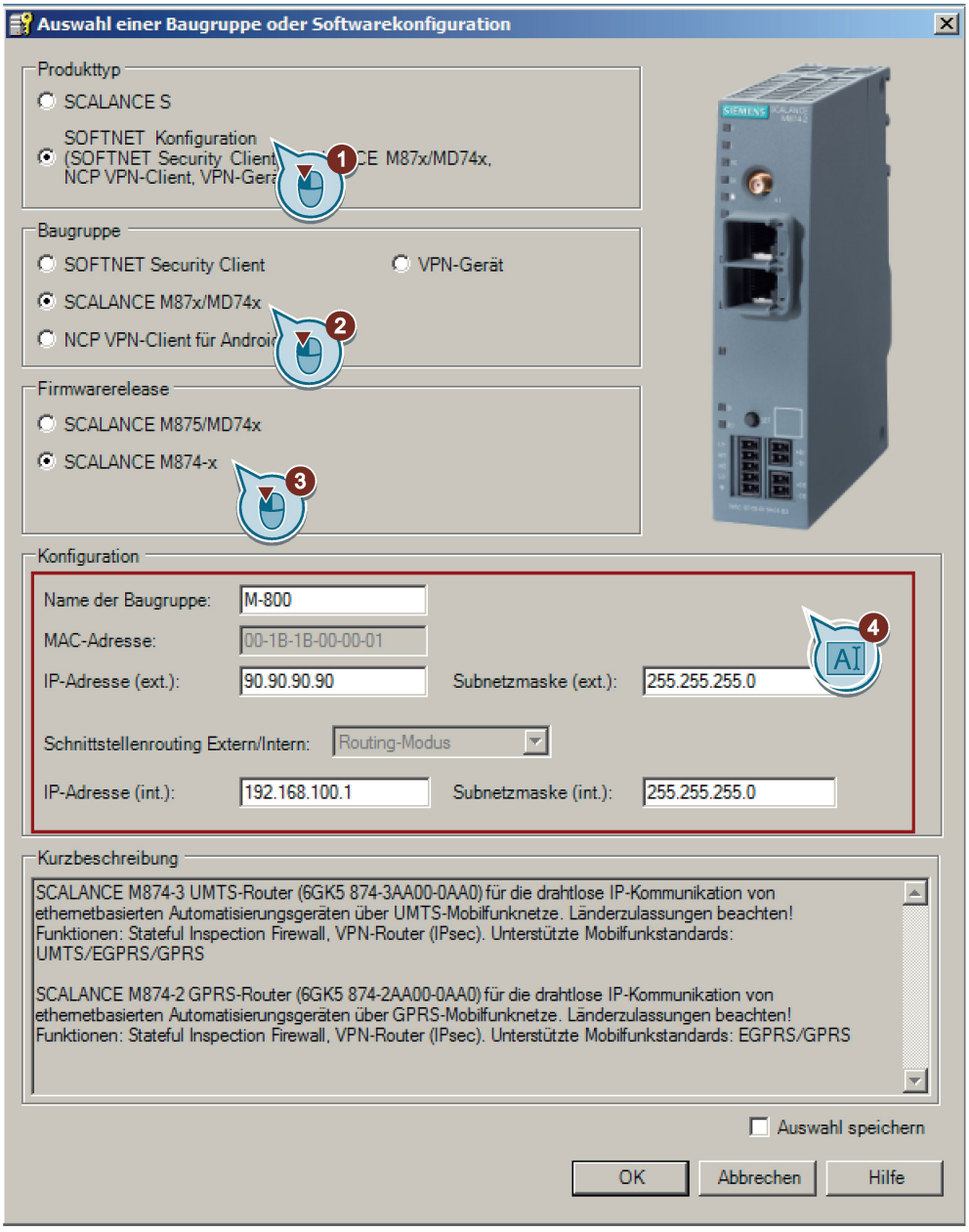
4.3.2.1 Projekt und Module mit den SCT anlegen

Vorgehensweise

1. Aktivieren Sie in den Objekteigenschaften des CP 1628 im Register "Security" das Optionskästchen "Security aktivieren".
2. Legen Sie im folgenden Dialog einen neuen Benutzer mit Benutzernamen und dazugehörigem Passwort an.

   Dem Benutzer wird automatisch die Rolle "Administrator" zugewiesen.
3. Bestätigen Sie den Dialog mit "OK". Ein neues Projekt ist angelegt.
4. Öffnen Sie in HW Konfig das Security Configuration Tool über den Menübefehl "Bearbeiten" > "Security Configuration Tool".
   Der angelegte CP wird in der Liste der konfigurierten Module angezeigt.

5. Erzeugen Sie mit dem Menübefehl "Einfügen" > "Baugruppe" ein zweites Modul.



6. Tragen Sie die dem SCALANCE M-800 zugeordneten Werte aus der Tabelle "Verwendete Einstellungen (Seite 149)" ein.
7. Bestätigen Sie den Dialog mit "OK".

Ergebnis

Der CP und das SCALANCE M-800 werden in der Liste der konfigurierten Module angezeigt.

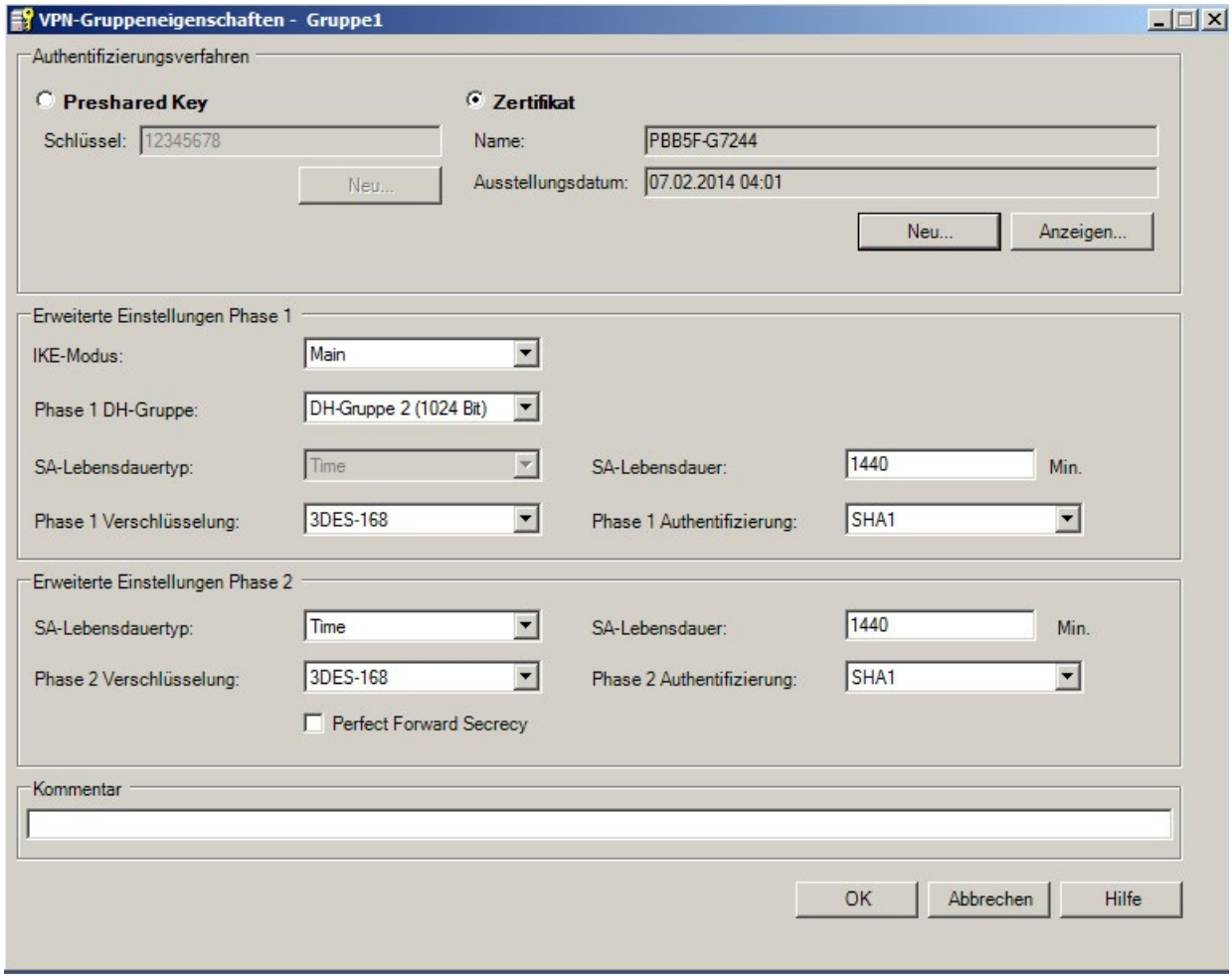
4.3.2.2 Tunnelverbindung projektieren

Nur wenn das SCALANCE M-800 und der CP der gleichen Gruppe zugeordnet sind, kann ein VPN-Tunnel für die gesicherte Kommunikation aufgebaut werden..

Vorgehensweise

1. Selektieren Sie im Navigationsbereich "VPN-Gruppen" und erzeugen Sie mit dem Menübefehl "Einfügen" > "Gruppe" eine neue Gruppe. Die Gruppe erhält automatisch den Namen "Gruppe1".
2. Markieren Sie im Navigationsbereich den Eintrag "Alle Module".
3. Markieren Sie im Inhaltsbereich das SCALANCE M-800 und den CP. Ziehen Sie die Module per Drag&Drop in die "Gruppe1". Beide Module sind nun der "Gruppe 1" zugeordnet.
4. Wechseln Sie mit dem Menübefehl "Ansicht" > "Erweiterter Modus" in den Erweiterten Modus.
5. Öffnen Sie die Gruppeneigenschaften der Gruppe1, indem Sie im Kontextmenü "Eigenschaften ..." auswählen

6. Konfigurieren Sie für diese Beispielkonfiguration die Gruppeneigenschaften mit folgenden Einstellungen:



Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

7. Wählen Sie den Menübefehl "Projekt" > "Speichern". Speichern Sie das Security-Projekt unter dem gewünschten Namen ab.

Ergebnis

Die Konfiguration der Tunnelverbindung ist abgeschlossen. Die Einstellungen werden in der Konfigurationsdatei gespeichert.

4.3.2.3 Konfiguration in CP laden und M-800-Konfiguration abspeichern

Konfiguration in CP laden

1. Schließen Sie das Security Configuration Tool.
2. Wählen Sie in HW Konfig das Menü "Station" > "Speichern und Übersetzen".
3. Laden Sie die neue Konfiguration über das Menü "Zielsystem" > "Laden in Baugruppe..." auf das Security-Modul.
   - Für CP 1628: Wurde der Ladevorgang fehlerfrei abgeschlossen, startet das Security-Modul automatisch und die neue Konfiguration ist aktiviert.
   - Für CP 343-1 Advanced oder CP 434-1 Advanced: Starten Sie die S7-CPU nach dem Laden neu, um die neue Konfiguration zu aktivieren.

SCALANCE M-800-Konfiguration abspeichern

1. Markieren Sie im Inhaltsbereich das "M-800" und wählen Sie den Menübefehl "Übertragen" > "An Baugruppe(n) ...".
2. Speichern Sie die Konfigurationsdatei "Projektname.M-800.txt" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats, z. B. Di1S+Xo?.

Ergebnis

In das Projektverzeichnis werden folgende Dateien abgespeichert:

- Konfigurationsdatei: Projektname.M-800.txt
- PKCS12-Datei: Projektname.Zeichenfolge.M-800.p12
- Gegenstellenzertifikat: Projektname.Gruppe1.CP.cer

Die Konfigurationsdatei enthält die exportierten Konfigurationsinformationen für das SCALANCE M-800 einschließlich einer Information über die zusätzlich erzeugten Zertifikate. Folgen Sie den Anweisungen in der Konfigurationsdatei.

4.3.3 SCALANCE M-800 konfigurieren

4.3.3.1 Zertifikat laden

Voraussetzung

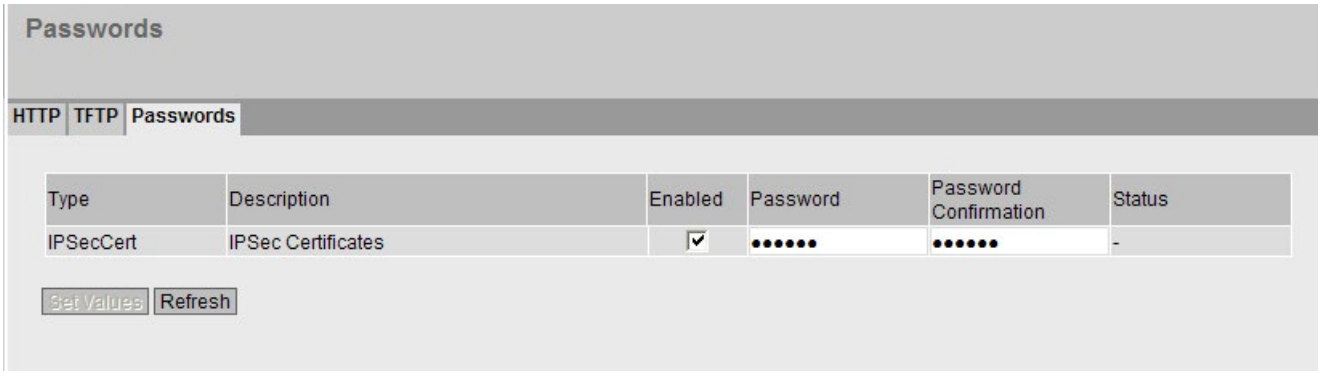
- Auf dem SCALANCE M ist die richtige Uhrzeit eingestellt, siehe Kapitel Uhrzeit einstellen (Seite 22).
- Zertifikate sind vorhanden.

  Die benötigten Zertifikate haben Sie im letzten Kapitel auf dem PC abgespeichert und ein Passwort für den privaten Schlüssel vergeben.

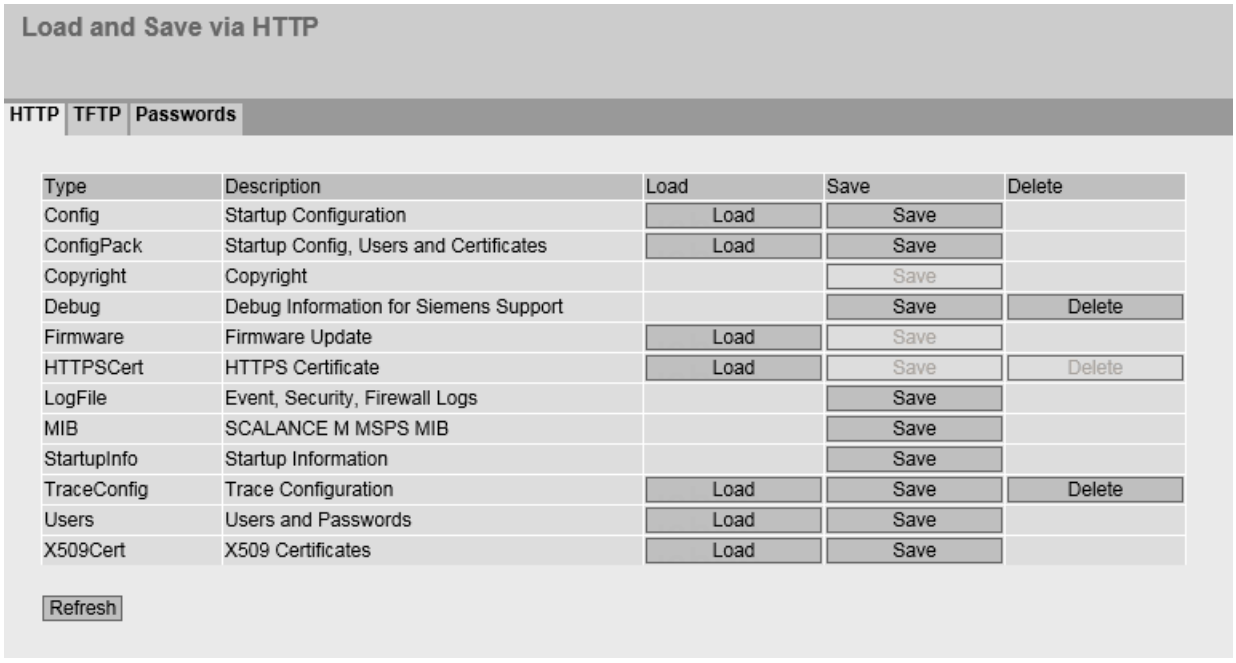
  Übertragen Sie die Zertifikate für das SCALANCE M auf den Admin-PC.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System" > "Load & Save" und im Inhaltsbereich auf das Register "Password".
2. Tragen Sie bei "Password" und bei "Password Confirmation" das Passwort Di1S+Xo? ein, das Sie für die PKCS12-Datei festgelegt haben.
3. Aktivieren Sie "Enabled" und klicken Sie auf "Set Values".



4. Klicken Sie im Inhaltsbereich auf das Register "HTTP".



5. Klicken Sie bei "IPSecCert" oder "X509cert" auf die Schaltfläche "Load". Das Dialogfenster zum Hochladen einer Datei wird geöffnet.

   Navigieren Sie zum Gegenstellenzertifikat.

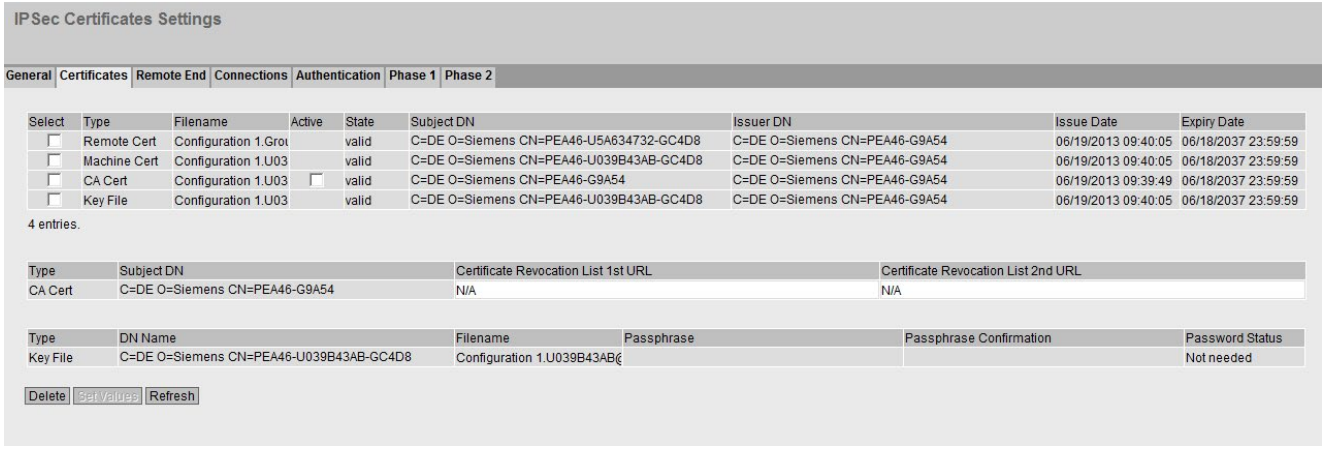
6. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".

   Die Datei wird nun ins Gerät geladen. Nach dem erfolgreichen Laden bestätigen Sie den folgenden Dialog mit "OK".

7. Wiederholen Sie die Schritte 5 und 6 für die PKCS12-Datei.

Ergebnis

Die Zertifikate sind geladen. Unter "Security" > "IPSec VPN" > "Certificates" werden die Zertifikate angezeigt. Die geladenen Zertifikate müssen den Status "valid" besitzen.

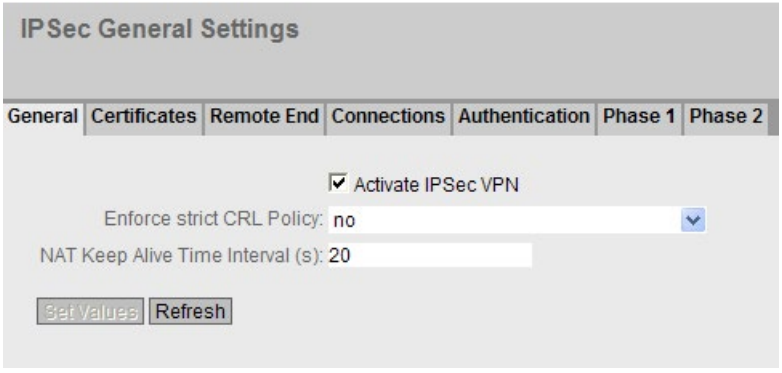


Ab Firmware-Version 4.0 werden die Zertifikate unter "Security" > "Certificates" angezeigt.

4.3.3.2 VPN aktivieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN".



3. Klicken Sie auf "Set Values"

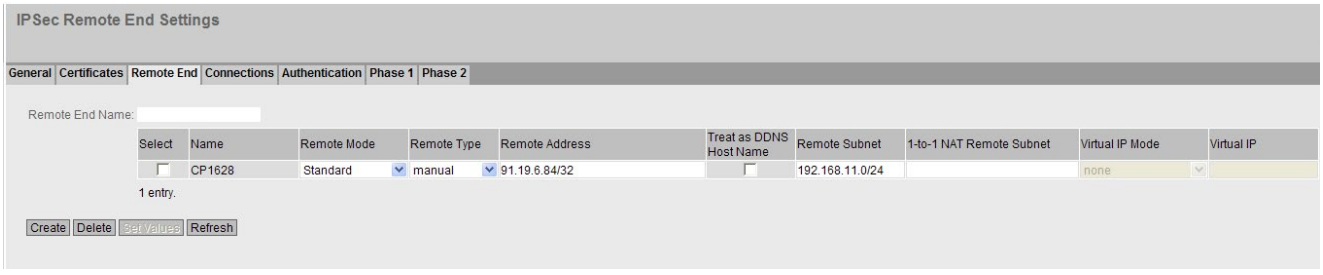
4.3.3.3 VPN-Gegenstelle konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Remote End".
2. Tragen Sie bei "Remote End Name" den Namen der VPN-Gegenstelle (Tunnelendpunkt) ein, z. B. CP1628.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie für die Beispielkonfiguration die VPN-Gegenstelle mit folgenden Einstellungen:

Remote Mode	Standard
Remote Typ	manual
Remote Address	91.19.6.84/32 WAN-IP-Adresse des DSL-Routers
Remote Subnet	192.168.184.0/24

5. Klicken Sie auf "Set Values".



4.3.3.4 VPN-Verbindung konfigurieren

Voraussetzung

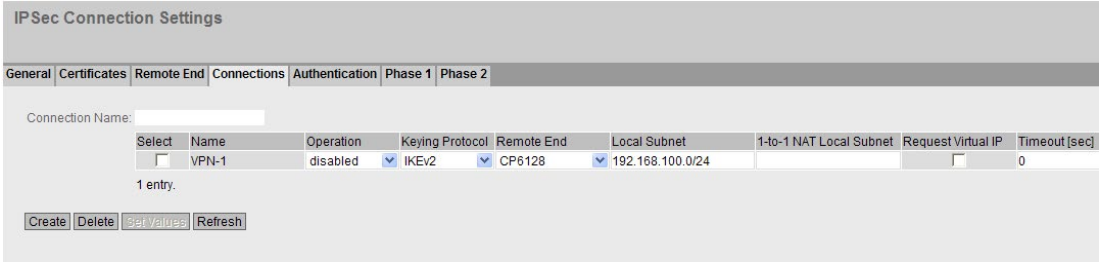
- VPN-Gegenstelle ist angelegt.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".
2. Geben Sie bei "Connection Name" einen Namen für die VPN-Verbindung ein.
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile angelegt.
4. Konfigurieren Sie für die Beispielkonfiguration die VPN-Verbindung mit folgenden Einstellungen:

Operation	disabled
Keying Protocol	IKEv1
Remote End	CP1628 Name der VPN-Gegenstelle
Local Subnet	192.168.100.0/24 Das lokale interne Subnetz 1 in CIDR-Schreibweise.

5. Klicken Sie auf "Set Values".



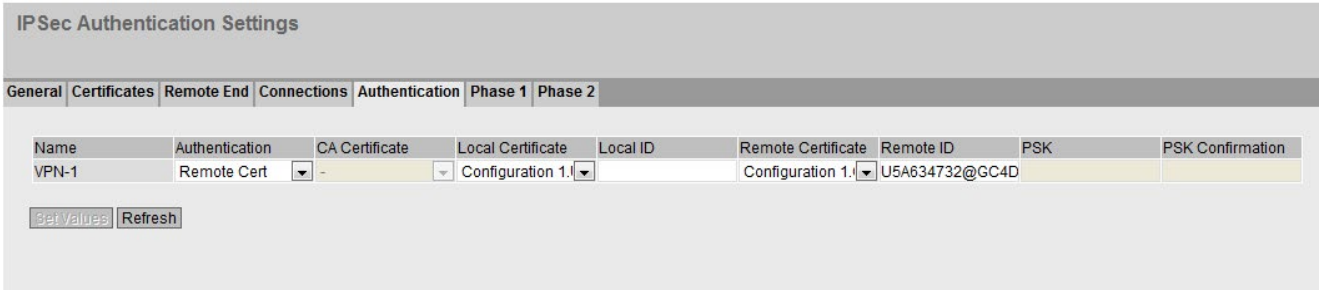
4.3.3.5 VPN-Authentifizierung konfigurieren

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Authentication".
2. Konfigurieren Sie für die Beispielkonfiguration die VPN-Authentifizierung mit folgenden Einstellungen:

Authentication	Remote Cert
Local Certificate	Projektname.Zeichenfolge.M-800.p12
Remote Certificate	Projektname.Gruppe1.CP.cer
Remote ID	Remote ID aus der Konfigurationsdatei

3. Klicken Sie auf "Set Values".



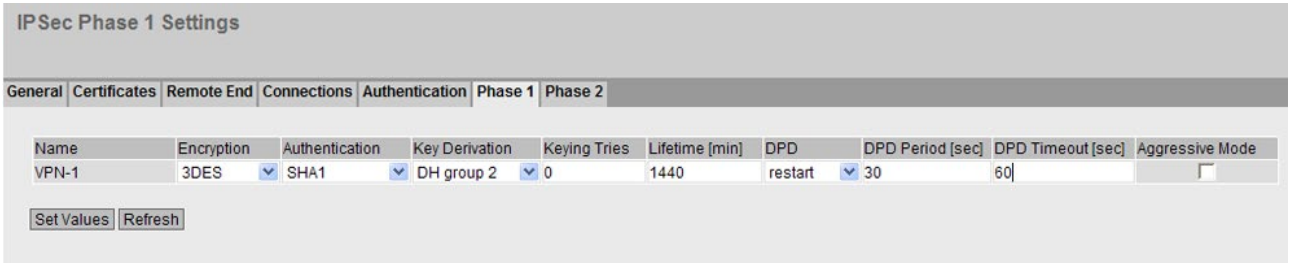
4.3.3.6 Phase 1 und Phase 2 konfigurieren

Phase 1 konfigurieren

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSecVPN" und im Inhaltsbereich auf das Register "Phase 1".
2. Wählen Sie bei "DPD" "restart" aus.
3. Konfigurieren Sie die Phase 1 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

4. Klicken Sie auf "Set Values".

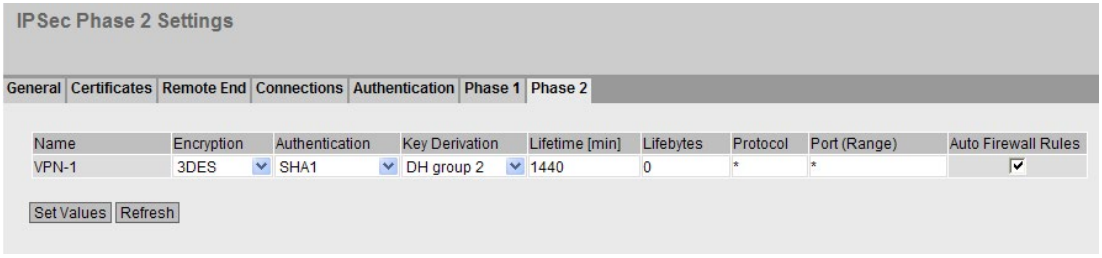


Phase 2 konfigurieren

1. Klicken Sie auf das Register "Phase 2".
2. Konfigurieren Sie für die Phase 2 mit folgenden Einstellungen aus der Konfigurationsdatei:

Encryption	3DES
Authentication	SHA1
IKE Key Derivation	DH group 2
Lifetime [min]	1440

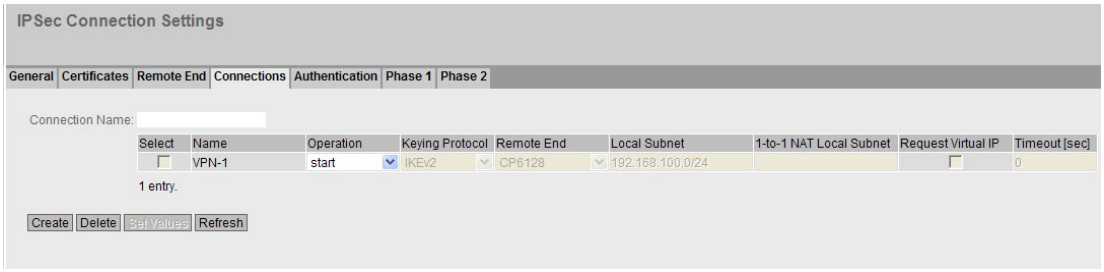
3. Klicken Sie auf "Set Values".



4.3.3.7 VPN-Verbindung aufbauen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "Connection".

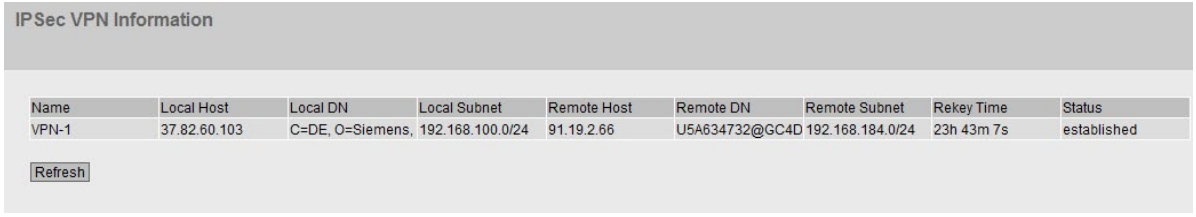


2. Wählen Sie bei "Operation" "start" aus und klicken Sie auf "Set Values".

Ergebnis

Das SCALANCE M-800 baut den VPN-Tunnel zum CP 1628 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet am Gerät die LED 🔒 grün.

Weitere Informationen erhalten Sie unter "Information" > "IPSec VPN".



VPN-Tunnel zwischen SCALANCE M87x und SINEMA RC-Server

5

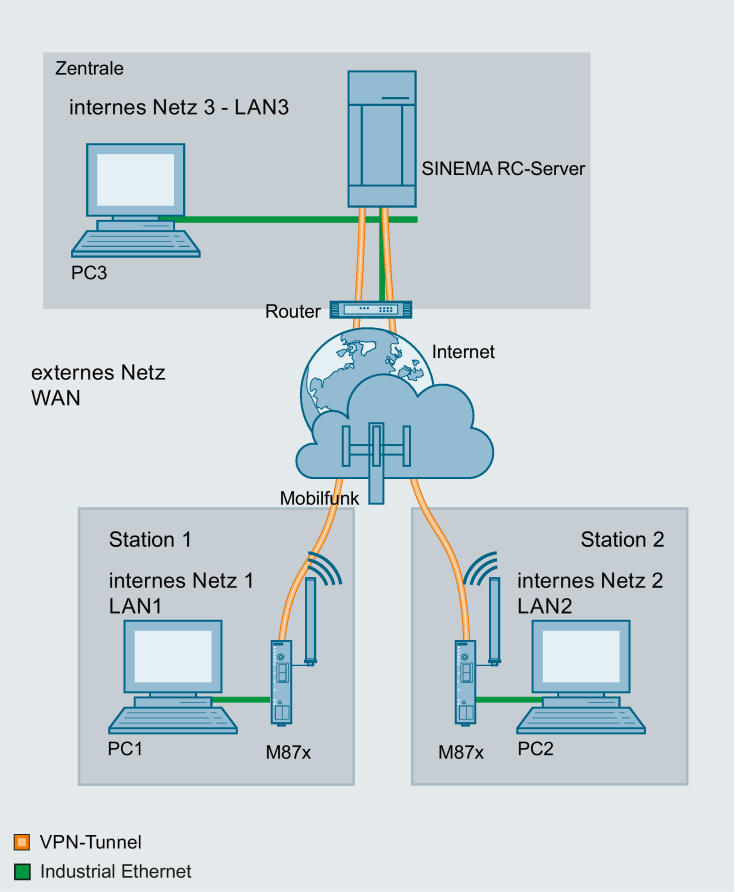
5.1 Prinzipielles Vorgehen

In dieser Beispielkonfiguration sind zwei dezentrale Stationen mithilfe von SCALANCE M87x angeschlossen. Die Geräte kommunizieren über den SINEMA RC-Server, der in der Zentrale steht. Die Adressierung des SINEMA RC erfolgt über eine WAN-IP-Adresse, die von einem Provider bezogen wird. Alternativ können Sie den SINEMA RC-Server auch über einen fest definierten Namen (FQDN) addressieren.

Für die SCALANCE M87x-Geräten wird je ein KEY-PLUG SINEMA Remote Connect benötigt. Mit dem KEY-PLUG wird die Anbindung von SCALANCE M87x an SINEMA RC freigeschaltet.

Dazu müssen sich die Geräte am SINEMA RC-Server anmelden. Erst nach erfolgreicher Authentifizierung wird der VPN-Tunnel zwischen dem Gerät und dem SINEMA RC-Server aufgebaut. Abhängig von den projektierten Kommunikationsbeziehungen und den Sicherheitseinstellungen verschaltet der SINEMA RC Server die einzelnen VPN-Tunnels.

Aufbau



Zentrale - Anschluss an SINEMA RC Server

- Im internen Netz wird im Testaufbau ein Netzknoten durch einen PC realisiert, der an dem LAN-Schnittstelle des SINEMA RC Servers angeschlossen ist.
  - PC: repräsentiert einen Teilnehmer im internen Netzwerk 3
  - SINEMA RC Server
- Anbindung an das externe Netzwerk über einen Router

  Der Zugriff auf das externe Netzwerk erfolgt über einen Router, der an dem WAN-Schnittstelle des SINEMA RC Servers angeschlossen wird.

Station 1 / 2 - Anschluss an SCALANCE M87x

- Im internen Netz wird im Testaufbau ein Netzknoten durch einen PC realisiert, der an die Ethernet-Schnittstelle P1 des M-800 angeschlossen ist.
  - PC: repräsentiert einen Teilnehmer im internen Netzwerk 1/2
  - M-87x: SCALANCE M-Modul zum Schutz des internen Netzwerks 1/2
- Anbindung an das externe, öffentliche Netzwerk
  - Drahtlos über die Antenne des M87x an das Mobilfunknetz. (ab FW 4.0)

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- 2 x M874 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
- 2 x KEY-PLUG SINEMA RC
- 2 x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
- 2 x PC die mit je einem SCALANCE M874 verbunden sind.
- 2 x geeignete Antennen
- 2 x SIM-Karte ihres Mobilfunkanbieters. Die entsprechenden Dienste z. B. Internet sind freigeschaltet.
- 1 x PC, auf dem der SINEMA RC Server installiert ist.
- 1 x PC, der mit dem SINEMA RC Server verbunden ist.
- 1 x Router
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Hinweis

Sie können auch ein SCALANCE M876 verwenden. Die nachfolgend beschriebene Projektierung bezieht sich explizit auf die im Abschnitt "Erforderliche Geräte/Komponenten" erwähnten Komponenten.

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen:

	Name	Schnittstelle	IP-Adresse
Station-1 LAN1	M874-1	LAN-Schnittstelle P1 (vlan1)	192.168.100.1 255.255.255.0
		WAN-Schnittstelle (ppp0)	Dynamische IP-Adresse vom Provider
	PC1	LAN-Schnittstelle	192.168.100.20 255.255.255.0
Station-2 LAN2	M874-2	LAN-Schnittstelle P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN-Schnittstelle (ppp0)	Dynamische IP-Adresse vom Provider
	PC2	Ethernet (LAN 2)	192.168.10.20 255.255.255.0
Zentrale LAN3	SINEMA RC Server	WAN-Schnittstelle	192.168.20.250 255.255.255.0 Die WAN-IP-Adresse, über die der SINEMA RC Server erreichbar ist, ist in diesem Beispiel die WAN-IP-Adresse des Routers. 90.90.90.90 Das Default-Gateway ist die LAN-IP-Adresse des Routers 192.168.20.1 Alternativ kann der SINEMA RC-Server auch über einen definierten Hostnamen (FQDN) addressiert werden.
	PC3	Ethernet (LAN3)	192.168.20.20 255.255.255.0
	Router 3	LAN-Schnittstelle	192.168.20.1 255.255.255.0
		WAN-Schnittstelle	Statische IP-Adresse vom Provider, z. B. 90.90.90.90

Hinweis

Die in der Beispielkonfiguration verwendeten IP-Einstellungen sind frei gewählt.

Im realen Netzverbund müssen Sie diese IP-Einstellungen der Netzwerkumgebung anpassen, um eventuelle Adresskonflikte zu vermeiden.

Voraussetzung

SINEMA RC Server

- Der SINEMA RC Server ist mit dem WAN verbunden. Die Projektierungsschritte finden Sie im Getting Started "SINEMA Remote Connect".

Hinweis

Port-Forwarding am Router

Durch die Nutzung eines Routers als Gateway müssen Sie die folgenden Ports am Router freischalten und die Datenpakete an den SINEMA RC-Server weiterleiten:

- TCP 443
- TCP 5443
- UDP 1194

VPN-fähige Router

Wenn Ihr Router selbst VPN-fähig ist, stellen Sie sicher, dass sich die Ports nicht überschneiden oder diese Funktion deaktiviert ist

Weitereführende Informationen dazu finden Sie in der Dokumentation des Routers.

SCALANCE M874

- Das M874 ist mit dem WAN verbunden, siehe "SCALANCE M874 mit dem WAN verbinden (Seite 11)".

  Die Projektierungsschritte gelten für alle Geräte und unterscheiden sich nur in den Einstellungen, siehe Tabelle "Verwendete Einstellungen (Seite 191)" .
- Das M874 ist über den PC1 bzw. PC2 erreichbar und Sie sind am WBM als "admin" angemeldet.
- Im SCALANCE M ist ein gütliger KEY-PLUG SINEMA Remote Connect gesteckt.

Projektierungsschritte

Zugriff auf den SINEMA RC Servers konfigurieren

Damit der PC über M874 auch auf das WBM des SINEMA RC Servers zugreifen kann, sind auf dem M874 folgende Schritte notwendig:

1. IP-Masquerading aktivieren (Seite 197)
2. Zugriff erlauben (Seite 197)

Fernverbindung auf dem SINEMA RC Server konfigurieren

1. Teilnehmergruppen anlegen (Seite 199)
2. Geräte anlegen (Seite 200)
3. Kommunikationsbeziehungen konfigurieren (Seite 203)

Fernverbindung auf dem M874 konfigurieren

- Gesicherte VPN-Verbindung mit Fingerabdruck (Seite 205)
- Gesicherte VPN-Verbindung mit CA-Zertifikat
  - Zertifikat laden (Seite 208)
  - VPN-Verbindung zum SINEMA RC Server projektieren (Seite 209)

5.2 Zugriff auf den SINEMA RC-Servers konfigurieren

5.2.1 IP-Masquerading aktivieren

IP-Masquerading wird verwendet, damit die internen IP-Adressen extern nicht weitergeleitet werden. Zudem werden keine weiteren Routingeinstellungen im Router benötigt.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3" > "NAT" und im Inhaltsbereich auf das Register "Masquerading".
2. Aktivieren Sie "Enable Masquerading" an der WAN-Schnittstelle.
   - M874, M876-3: ppp0
   - M876-4: usb0
3. Klicken Sie auf "Set Values"

Ergebnis

And der WAN-Schnittstelle ist Masquerading aktiviert. Wenn ein Paket über diese Schnittstelle gesendet wird, wird die Quelladresse auf die dee WAN-Schnittstelle zugewiesenen IP-Adresse umgeschrieben.

5.2.2 Zugriff erlauben

Damit der PC auf den SINEMA RC Server zugreifen kann, wird am Gerät der Zugriff von vlan1 auf die WAN-Schnittstelle freigeschaltet.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "Firewall" und im Inhaltsbereich auf das Register "IP Rules".
2. Klicken Sie auf "Create". In der Tabelle wird ein neuer Eintrag erstellt.

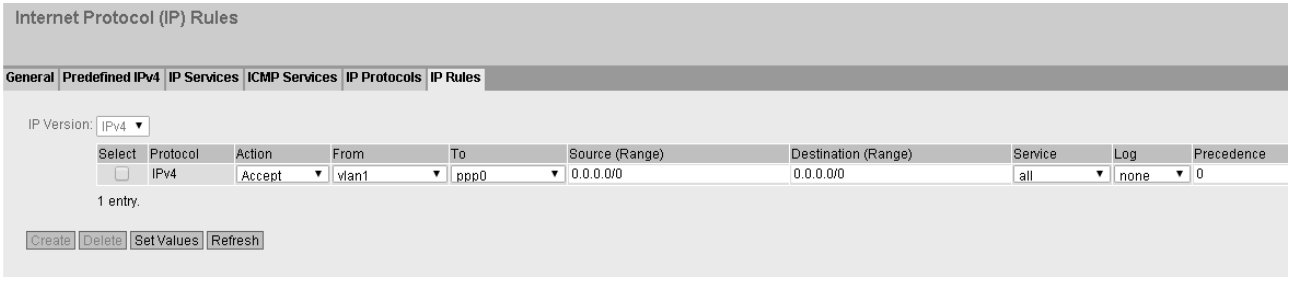
3. Konfigurieren Sie die Firewall-Regel mit folgenden Einstellungen:

Action	Accept
From	vlan1 (intern)
To	extern M874, M876-3: ppp0 M876-4: usb0
Source (Range)	0.0.0.0 (alle IP-Adressen)
Destination (Range)	0.0.0.0 (alle IP-Adressen)
Service	all Der Dienst ist standardmäßig immer verfügbar

4. Klicken Sie auf "Set Values".

Ergebnis

Durch diese Firewall-Regel sind alle Dienste zwischen vlan1 und ppp0 bzw usb0 uneingeschränkt möglich, z. B. HTTPS



5.3 Fernverbindung auf dem SINEMA RC-Server konfigurieren

5.3.1 Teilnehmergruppen anlegen

Benutzer und Geräte lassen sich in Teilnehmergruppen zusammenfassen. Außerdem können Sie festlegen, ob die Kommunikation zwischen den Teilnehmern einer einzelnen Gruppe erlaubt oder verboten ist.

Für diese Beispielkonfiguration werden folgende Gruppen angelegt.

- Station-1
- Station-2
- Service

Voraussetzung

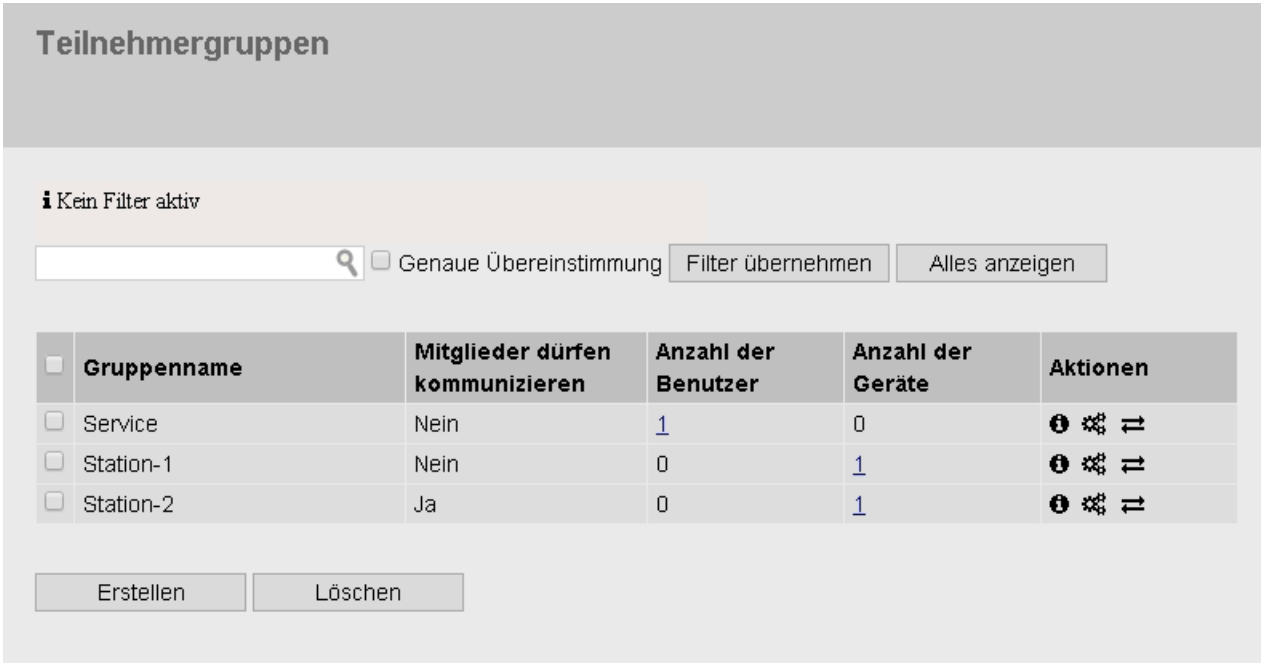
- Der SINEMA RC Server ist mit dem WAN verbunden

Vorgehensweise

1. Geben Sie im Adressfeld des Webbrowsers die WAN-IP-Adresse des SINEMA RC Servers "https://<WAN-IP-Adresse>" ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
2. Melden Sie sich als Benutzer "admin" und dem entsprechenden Passwort an.
3. Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Teilnehmergruppen". Im Inhaltsbereich werden die bereits angelegten Teilnehmergruppen aufgelistet.
4. Klicken Sie auf "Erstellen". Die Seite "Neue Teilnehmergruppe" wird geöffnet.
5. Geben Sie bei Gruppenname "Station-1" ein und klicken Sie auf "Beenden".
6. Wiederholen Sie die Schritte 1 - 3 für die Gruppen "Station-2" und "Service"

Ergebnis

Die Teilnehmergruppen sind angelegt.



5.3.2 Geräte anlegen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Geräte". Im Inhaltsbereich werden die bereits angelegten Geräte aufgelistet.
2. Klicken Sie auf "Erstellen", um ein neues Gerät anzulegen.
3. Geben Sie den Gerätenamen für das Gerät an, z. B. "M874-1" für die Station 1 und "M874-2" für die Station 2.
4. Klicken Sie auf "Weiter"
5. Aktivieren Sie die Option "Verbundene lokale Subnetze".

6. Konfigurieren Sie die Geräte mit folgenden Einstellungen:

Lokale LAN-IP-Adresse	IP-Adresse für vlan1 nach der Tabelle "Verwendete Einstellungen (Seite 191)".
Netzmaske	255.255.255.0

7. Klicken Sie auf "Weiter". Das Register "Gruppenzugehörigkeit" wird angezeigt.
8. Aktivieren Sie die entsprechende Gruppe.

   Beim Gerät "M874-1" die Gruppe "Station-1"

   Beim Gerät "M874-2" die Gruppe "Station-2"
9. Klicken Sie auf "Weiter". Das Register "Passwort " wird angezeigt.
10. Legen Sie das Passwort für den Zugriff fest, z. B. An:t_010 für M874-1 und An:t_020 für M874-2.

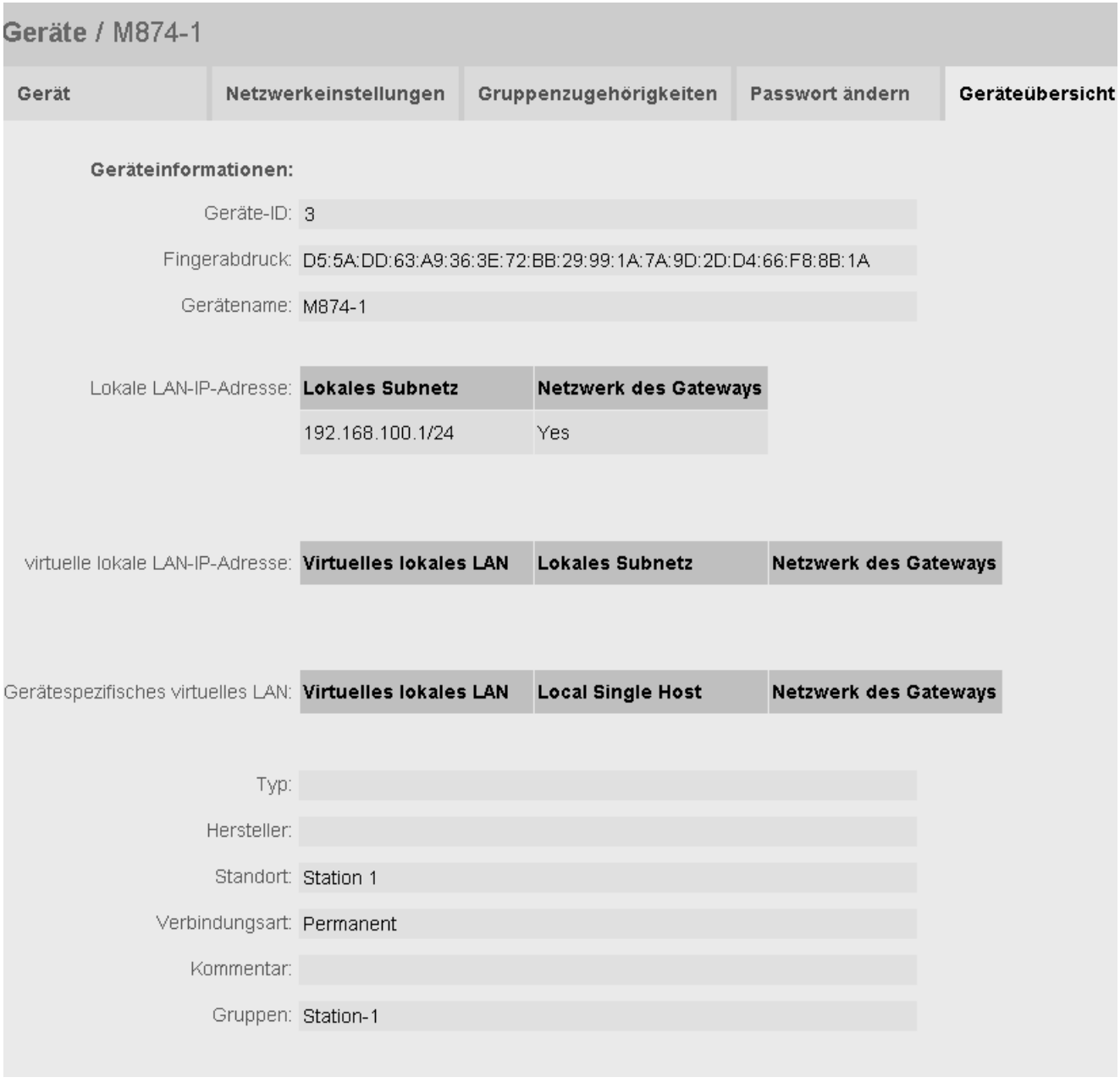
    Das Passwort muss sich aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zusammensetzen.
11. Klicken Sie auf "Beenden".

Ergebnis

Die Geräte werden bei den bereits angelegten Geräten aufgelistet.

- Gerätepasswort
- Geräte-ID
- Fingerabdruck

Die Geräte-ID und den Fingerabdruck finden Sie bei den Geräteinformationen. Klicken Sie auf das Symbol , um die Geräteinformation zu öffnen.



5.3.3 Kommunikationsbeziehungen konfigurieren

Damit die Teilnehmergruppen miteinander kommunizieren können, sind Kommunikationsbeziehungen notwendig. Dabei kann für jede Richtung eine Kommunikationsbeziehung erstellt werden.

Für diese Beispielkonfiguration werden folgende Kommunikationsbeziehungen angelegt:

von Gruppe	zur Zielgruppe
Service	Station-1
	Station-2
Station-1	Station-2

In diesem Konfigurationsbeispiel geht die Kommunikation nur von der Gruppe "Station-1" zur Gruppe "Station-2". In die Gegenrichtung ist keine Kommunikation möglich. Für die Kommunikation von der Gruppe "Station-2" zur Gruppe "Station-1" ist eine weitere Kommunikationsbeziehung notwendig.

Ebenso kann die Gruppe "Service" mit den Gruppen "Station-1" und "Station-2" kommunizieren, aber nicht umgekehrt.

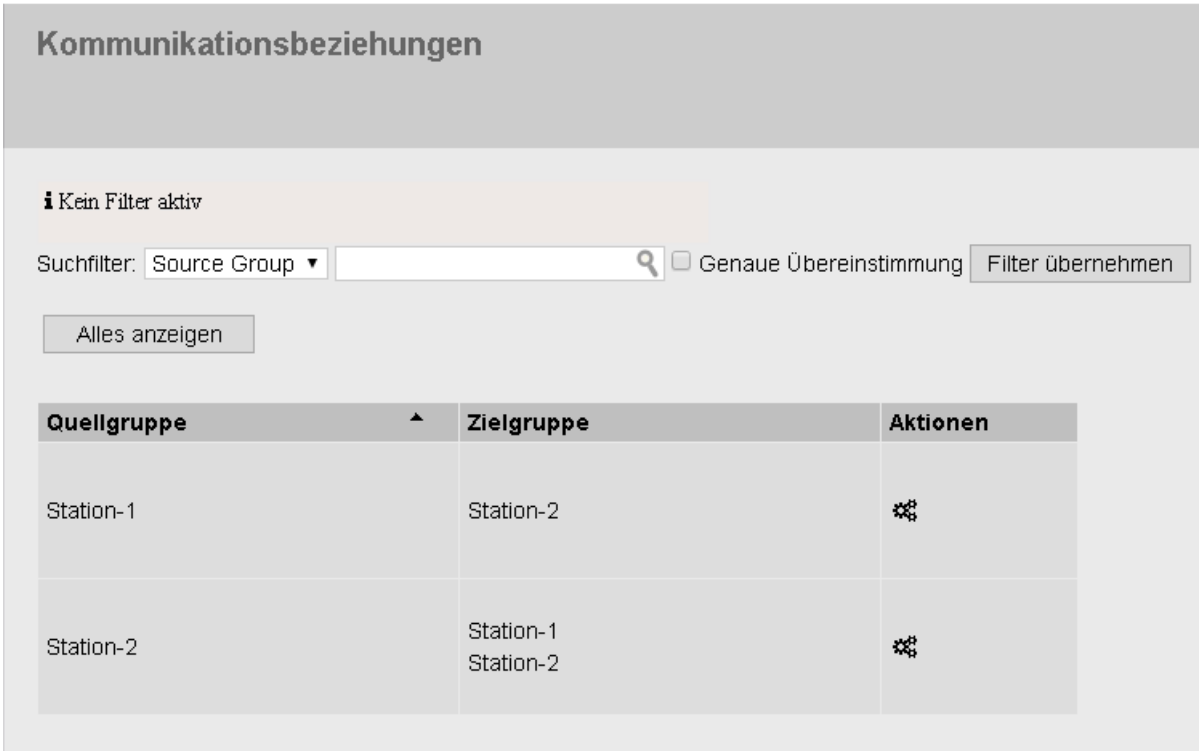
Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Teilnehmergruppen". Im Inhaltsbereich werden die bereits angelegten Teilnehmergruppen aufgelistet.
2. Klicken Sie bei "Station-1" in der Spalte "Aktionen" auf das Symbol ⇄. Die Seite "Zielgruppe" wird geöffnet.
3. Aktivieren Sie "Station-2" und klicken Sie auf "Speichern".
4. Klicken Sie auf "Dialog verlassen".
5. Klicken Sie bei "Service" in der Spalte "Aktionen" auf das Symbol ⇄. Die Seite "Zielgruppe" wird geöffnet.
6. Aktivieren Sie "Station-1" und "Station-2". Klicken Sie auf "Speichern".
7. Klicken Sie auf "Dialog verlassen".

Ergebnis

Die Kommunikationsbeziehungen sind angelegt.

Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Kommunikationsbeziehungen". Im Inhaltsbereich werden die angelegten Beziehungen aufgelistet.



5.4 Fernverbindung auf dem M87x konfigurieren

5.4.1 Gesicherte VPN-Verbindung mit Fingerabdruck

Voraussetzung

- Auf dem PC1/2 sind zwei Webbrowserfenster geöffnet.
- Webbrowser 1:

  Sie sind als Benutzer "admin" am WBM des M874 angemeldet.
- Webbrowser 2:

  Sie sind als Benutzer "service" oder "admin" am WBM des SINEMA RC Servers angemeldet.
- Im M87x ist ein gültiger KEY-PLUG gesteckt.

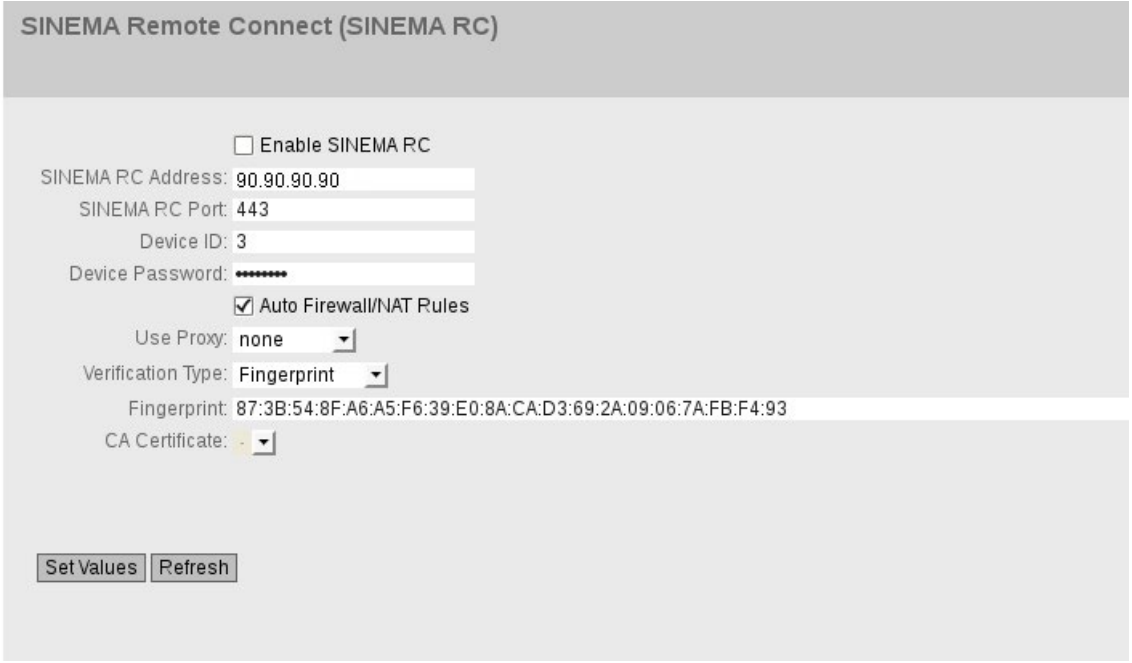
Vorgehensweise

1. Wechseln Sie in den Webbrowser 1.
   - Geben Sie im Adressfeld des Webbrowsers die LAN-IP-Adresse des M874 ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
   - Melden Sie sich als Benutzer "admin" und dem entsprechenden Passwort an.
   - Klicken Sie im Navigationsbereich auf "System" > "SINEMA RC".
   - Geben Sie bei "SINEMA RC Address" die WAN-IP-Adresse des SINEMA RC Servers ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
2. Wechseln Sie in den Webbrowser 2.
   - Geben Sie im Adressfeld des Webbrowsers die WAN-IP-Adresse des SINEMA RC Servers ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
   - Melden Sie sich als Benutzer "admin" und dem entsprechenden Passwort an.
   - Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Geräte".
   - Klicken Sie bei "Aktionen" auf das Symbol , um die Geräteinformation zu öffnen.
   - Markieren Sie mit gedrückter linker Maustaste den Eintrag bei Geräte-ID.
   - Klicken Sie mit der rechten Maustaste auf die Markierung und wählen Sie im Kontextmenü den Befehl zum Kopieren.

3. Wechseln Sie in den Webbrowser 1.
   - Klicken Sie mit der rechten Maustaste in das Eingabefeld von "Device-ID".
   - Wählen Sie im Kontextmenü den Befehl zum Einfügen.
   - Geben Sie bei "Device Password" das Passwort an, das Sie für den Zugriff projektiert haben, An:t_010 für M874-1 und An:t_020 für M874-2.
   - Aktivieren Sie "Auto Firewall / NAT Rules".

     Wenn aktiviert wird, werden automatisch die entsprechenden NAT und Firewallregeln angelegt.

     Wählen Sie bei "Verification Type" "Fingerprint" aus.
4. Wechseln Sie in den Webbrowser 2.
   - Markieren Sie mit gedrückter linker Maustaste den Eintrag bei Fingerabdruck.
   - Klicken Sie mit der rechten Maustaste auf die Markierung und wählen Sie im Kontextmenü den Befehl zum Kopieren.
5. Wechseln Sie in den Webbrowser 1.
   - Klicken Sie mit der rechten Maustaste in das Eingabefeld von "Fingerprint".
   - Wählen Sie im Kontextmenü den Befehl zum Einfügen.
   - Aktivieren Sie "Enable SINEMA RC" und klicken Sie auf "Set Values".



Ergebnis

Das Gerät baut einen VPN-Tunnel zum SINEMA RC Server auf.

Ob die Verbindung erfolgreich ist, können Sie im WBM prüfen.

Webbrowser 1: Klicken Sie im Navigationsbereich auf "Information" > "SINEMA RC".

Webbrowser 2: Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Geräte".

5.4.2 Gesicherte VPN-Verbindung mit CA-Zertifikat

5.4.2.1 Zertifikat laden

Voraussetzung

- Auf dem M874 und auf dem SINEMA RC Server ist die richtige Uhrzeit eingestellt.
- Auf dem PC1/2 sind zwei Webbrowserfenster geöffnet.
- Webbrowser 1:

  Sie sind als Benutzer "admin" am WBM des M874 angemeldet.
- Webbrowser 2:

  Sie sind als Benutzer "admin" am WBM des SINEMA RC Servers angemeldet.

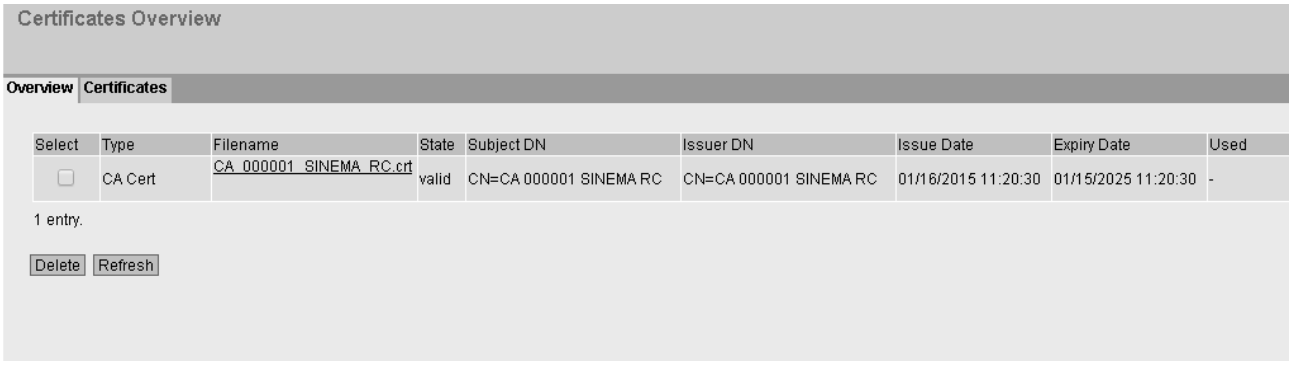
Vorgehensweise

1. Wechseln Sie in den Webbrowser 2.
   - Geben Sie im Adressfeld des Webbrowsers die WAN-IP-Adresse des SINEMA RC Servers ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
   - Melden Sie sich als Benutzer "admin" und dem entsprechenden Passwort an.
   - Klicken Sie im Navigationsbereich auf "Sicherheit" > "Zertifikate".
   - Klicken Sie bei "Aktionen" auf das Symbol  , um das Zertifikate zu exportieren.
2. Wechseln Sie in den Webbrowser 1.
   - Geben Sie im Adressfeld des Webbrowsers die LAN-IP-Adresse des M874 ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
   - Melden Sie sich als Benutzer "admin" und dem entsprechenden Passwort an.
   - Klicken Sie im Navigationsbereich auf "System" > "Load & Save" und im Inhaltsbereich auf das Register "HTTP".
   - Klicken Sie bei "X509Cert" auf die Schaltfläche "Load". Das Dialogfenster zum Hochladen einer Datei wird geöffnet.
   - Navigieren Sie zum exportierten Serverzertifikat. Klicken Sie im Dialogfenster auf die Schaltfläche "Öffnen".

     Die Datei wird nun ins Gerät geladen. Nach dem erfolgreichen Laden bestätigen Sie den folgenden Dialog mit "OK".

Ergebnis

Die Zertifikate sind geladen. Unter "Security" > "Certificates" werden die Zertifikate angezeigt. Die geladenen Zertifikate müssen den Status "valid" besitzen.



5.4.2.2 VPN-Verbindung zum SINEMA RC-Server projektieren

Voraussetzung

- Im M87x ist ein gültiger KEY-PLUG gesteckt.

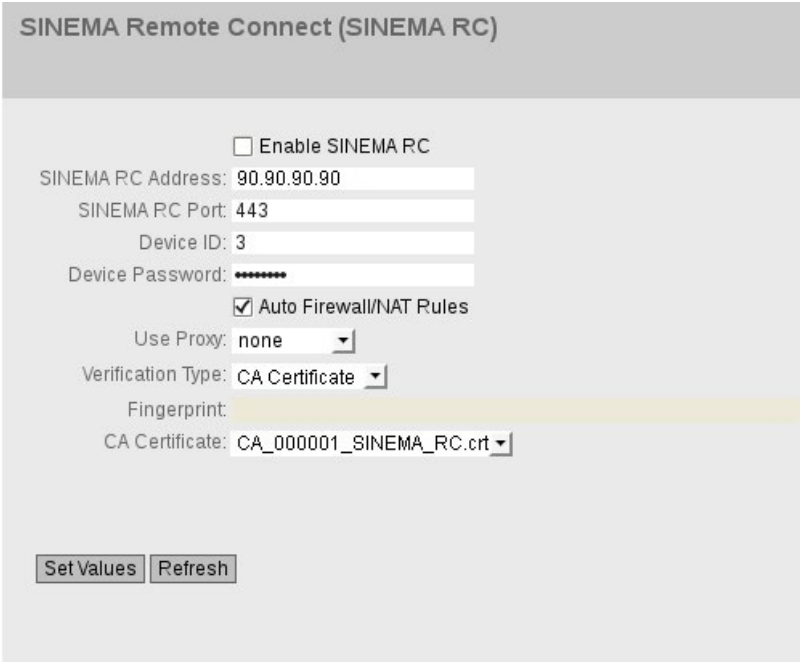
Vorgehensweise

1. Wechseln Sie in den Webbrowser 1.
   - Klicken Sie im Navigationsbereich auf "System" > "SINEMA RC".
   - Geben Sie bei "SINEMA RC Address" die WAN-IP-Adresse des SINEMA RC Servers ein, siehe Tabelle "Verwendete Einstellungen (Seite 191)".
2. Wechseln Sie in den Webbrowser 2.
   - Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Geräte".
   - Klicken Sie bei "Aktionen" auf das Symbol , um die Geräteinformation zu öffnen.
   - Markieren Sie mit gedrückter linker Maustaste den Eintrag bei Geräte-ID.
   - Klicken Sie mit der rechten Maustaste auf die Markierung und wählen Sie im Kontextmenü den Befehl zum Kopieren.

3. Wechseln Sie in den Webbrowser 1.
   - Klicken Sie mit der rechten Maustaste in das Eingabefeld von "Device-ID".
   - Wählen Sie im Kontextmenü den Befehl zum Einfügen.
   - Geben Sie bei "Device Password" das Passwort an, das Sie für den Zugriff projektiert haben, An:t_010 für M874-1 und An:t_020 für M874-2.
   - Aktivieren Sie "Auto Firewall / NAT Rules".

     Wenn aktiviert wird, werden automatisch die entsprechenden NAT und Firewallregeln angelegt.

     Wählen Sie bei "Verification Type "CA Certificate" aus.
   - Wäheln Sie bei "CA Certificate" das Serverzertifikat aus. Nur geladene Zertifikate sind auswählbar.



   - Aktivieren Sie "Enable SINEMA RC" und klicken Sie auf "Set Values".

Ergebnis

Das Gerät baut einen VPN-Tunnel zum SINEMA RC Server auf.

Ob die Verbindung erfolgreich ist, können Sie im WBM prüfen.

Webbrowser 1: Klicken Sie im Navigationsbereich auf "Information" > "SINEMA RC".

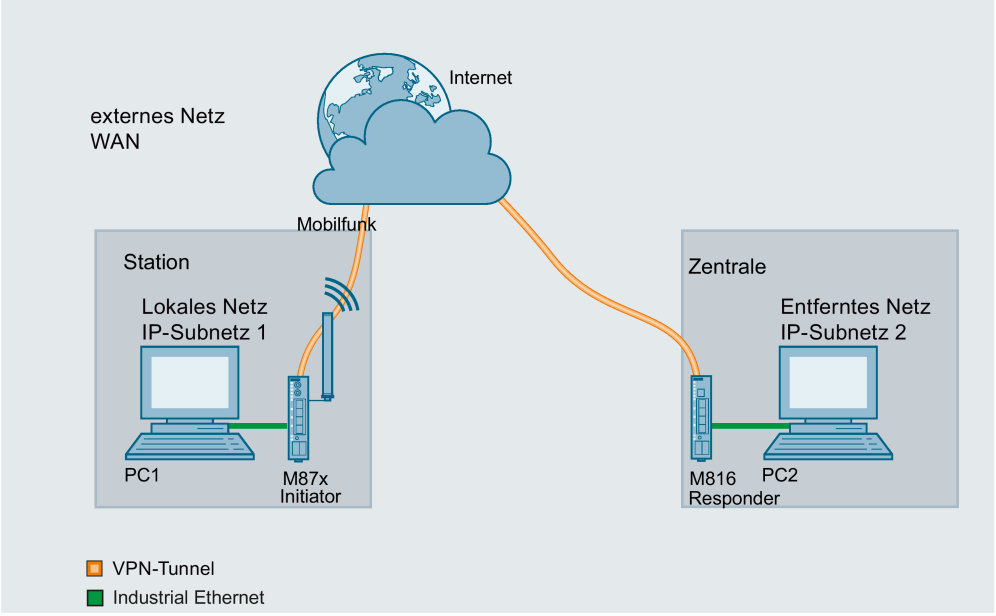
Webbrowser 2: Klicken Sie im Navigationsbereich auf "Fernverbindungen" > "Geräte".

NETMAP mit SCALANCE M-800

6

In diesen Beispielen werden zwei verschiedene IP-Subnetze über SCALANCE M-800 miteinander verbunden. Zwischen beiden SCALANCE M-Geräten ist ein VPN-Tunnel aufgebaut. Die VPN-Verbindung wird vom M876 aus initiiert. Über den aufgebauten VPN-Tunnel werden die Adressen mit NETMAP umgesetzt. Bei dieser Umsetzung wird der Subnetzanteil der IP-Adresse geändert und der Hostanteil bleibt bestehen.

NETMAP kann sowohl die Quell-IP-Adresse als auch die Ziel-IP-Adresse umsetzen.



Lokales Netz - Anschluss an SCALANCE M-800

- Im lokalen Netz wird im Testaufbau ein Netzknoten durch einen PC realisiert, der an eine Ethernet-Schnittstelle des SCALANCE M-800 angeschlossen ist.
  - PC: repräsentiert einen Teilnehmer des lokalen Netzwerks
  - M-800: SCALANCE M-Modul zum Schutz des internen Netzwerks
- Anbindung an das externe, öffentliche Netzwerk:
  - Drahtlos über die Antenne des M87x an das Mobilfunknetz.

Entferntes Netz - Anschluss an M-800

- Im entfernten Netz wird im Testaufbau der Netzknoten jeweils durch einen PC realisiert, der an eine Ethernet-Schnittstelle des SCALANCE M-800 angeschlossen ist.
  - PC: repräsentiert einen Teilnehmer des entfernten Netzwerks
  - M-800: SCALANCE M-Modul zum Schutz des externen Netzwerks
- Anbindung an das externe, öffentliche Netzwerk

  Kabelgebunden über die RJ45-Buchse des M816 an ADSL

Erforderliche Geräte/Komponenten

Für den Aufbau verwenden Sie folgende Komponenten:

- Anbindung an das Mobilfunknetz
  - 1x M876 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - 1x geeignete Antenne
  - 1x SIM-Karte ihres Mobilfunkanbieters. Die entsprechenden Dienste z. B. Internet sind freigeschaltet.
- Anbindung an ADSL
  - 1x M816 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
  - 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
  - ADSL-Zugang ist freigeschaltet
- 2x PCs, die mit den SCALANCE M-800 verbunden sind.
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

---

Hinweis

Sie können auch andere SCALANCE M-800 Geräte verwenden. Die nachfolgend beschriebene Projektierung bezieht sich explizit auf die im Abschnitt "Erforderliche Geräte/Komponenten" erwähnten Komponenten.

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen:

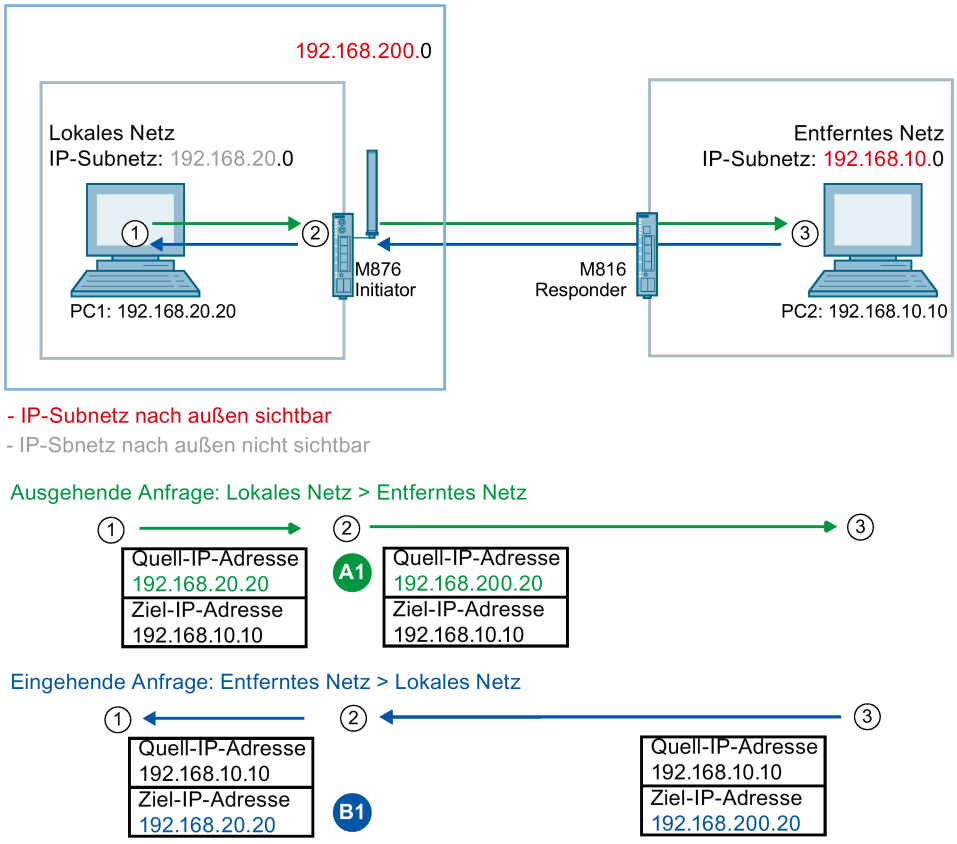
	Name	Schnittstelle	IP-Adresse
Station IP-Subnetz 1	M876	LAN-Schnittstelle P1 (vlan1)	192.168.20.1 255.255.255.0
		WAN-Schnittstelle (ppp0)	Dynamische IP-Adresse vom Provider Das Gerät ist aber über einen dynamischen DNS-Dienst erreichbar, z. B. example.no-ip.com
	PC1	LAN-Schnittstelle	192.168.20.20 255.255.255.0
Zentrale IP-Subnetz 2	M816	LAN-Schnittstelle P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN-Schnittstelle (ppp0)	Feste IP-Adresse (WAN-IP-Adresse), z. B. 91.19.6.84
	PC2	Ethernet (LAN 2)	192.168.10.10 255.255.255.0

Beispiele

Zu NETMAP gibt es folgende Beispiele

1. NETMAP für das lokale Netz (Seite 216)
2. NETMAP für das entfernte Netz (Seite 221)
3. NETMAP für das lokale und das entfernte Netz (Seite 226)

6.1 NETMAP für das lokale Netz



Beim NETMAP des lokalen Netzes wird die Quell-IP-Adresse ① z. B. 192.168.20.20 umgesetzt. Bei dieser Umsetzung wird der Subnetzanteil der IP-Adresse geändert und der Hostanteil bleibt bestehen. In diesem Beispiel ist der Subnetzanteil 192.168.20.0. Dieser Subnetzanteil wird durch 192.168.200.0 ersetzt. Die Quell-IP-Adresse wird vom M876 ② umgesetzt und an das Ziel ③ weitergeleitet.

Bei eingehenden Anfragen ③ wird die Ziel-IP-Adresse 192.168.200.0 durch 192.168.20.0 ersetzt. Die Ziel-IP-Adresse wird vom M876 ② umgesetzt und an das Ziel ① weitergeleitet. Es sind nur die NETMAP-Regeln für die Anfragerichtung notwendig. Die NETMAP-Regeln für die Antworten werden implizit hinzugefügt. Wenn PC1 eine Anfrage an PC2 sendet, wird die Antwort darauf umgesetzt. Das gilt aber nicht für die Anfragen von PC2 an PC1.

Dazu werden auf dem M876 (Initiator) die folgenden NETMAP-Regeln angelegt:

A1 Lokales Netz > Entferntes Netz:
Das Quell-IP-Subnetz 192.168.20.0/24 wird durch 192.168.200.0/24 ersetzt.

B1 Entferntes Netz > Lokales Netz:
Das Ziel-IP-Subnetz 192.168.200.0/24 wird durch 192.168.20.0/24 ersetzt

Zusätzlich kommunizieren die beiden Geräte über einen VPN-Tunnel.

Voraussetzung

- Das SCALANCE M-800 ist mit dem WAN verbunden, siehe "SCALANCE M-800 mit dem WAN verbinden (Seite 83)".
- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

Zum Erstellen der NETMAP-Regeln sind folgende Schritte sind erforderlich:

1. VPN-Verbindung anlegen (Seite 217)
2. NETMAP-Regeln erstellen (Seite 219)

6.1.1 VPN-Verbindung anlegen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN" und klicken Sie auf "Set Values".
3. Klicken Sie im Inhaltsbereich auf das Register "Remote End" und legen Sie die VPN-Gegenstelle mit folgenden Einstellungen an:

	Am M816	**Am M876**
Remote End Name	M876	M816
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Erreichbar über einen dynamischen DNS-Dienst z. B. example.no-ip.com	Feste IP-Adresse (WAN-IP-Adresse) des M816, z. B. 91.19.6.84
Remote Subnet	192.168.200.0/24	192.168.10.0/24

4. Klicken Sie im Inhaltsbereich auf das Register "Connections" und legen Sie die VPN-Verbindung mit folgenden Einstellungen an.

	Am M816	**Am M876**
Connection Name	M816_to_M876	M876_to_M816
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M876	M816
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Klicken Sie im Inhaltsbereich auf das Register "Authentication" und konfigurieren Sie die VPN-Authentifizierung mit folgende Einstellungen.

	Am M816	**Am M876**
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	z. B. 12345678	z. B. 12345678

6. Klicken Sie im Inhaltsbereich auf das Register "Phase 1" und konfigurieren Sie die folgenden Einstellungen.

	M816 / M876
DPD	aktiviert
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

7. Klicken Sie im Inhaltsbereich auf das Register "Phase 2" und konfigurieren Sie die folgenden Einstellungen.

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M816)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Ergebnis

Die VPN-Verbindung auf den Geräten ist konfiguriert. Um die VPN-Verbindung aufzubauen, klicken Sie im Inhaltsbereich auf das Register "Connection".

Wählen Sie bei "Operation" Folgendes aus und klicken auf "Set Values"

	Am M816	**Am M876**
Operation	wait (Responder)	start (Initiator)

Das M876 baut den VPN-Tunnel zum M816 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet an den Geräten die LED 🔒 grün.

6.1.2 NETMAP-Regeln erstellen

Voraussetzung

- Die VPN-Verbindung M876_to_M816 ist konfiguriert, siehe VPN-Verbindung anlegen (Seite 217).

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3" > "NAT" und im Inhaltsbereich auf das Register "NETMAP".
2. Legen Sie die NETMAP-Regel A1 für die ausgehenden Anfragen mit folgenden Einstellungen fest:

Type	Source
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816
Source IP Subnet	192.168.20.0/24
Translated Source IP Subnet	192.168.200.0/24
Destination IP Subnet	192.168.10.0/24

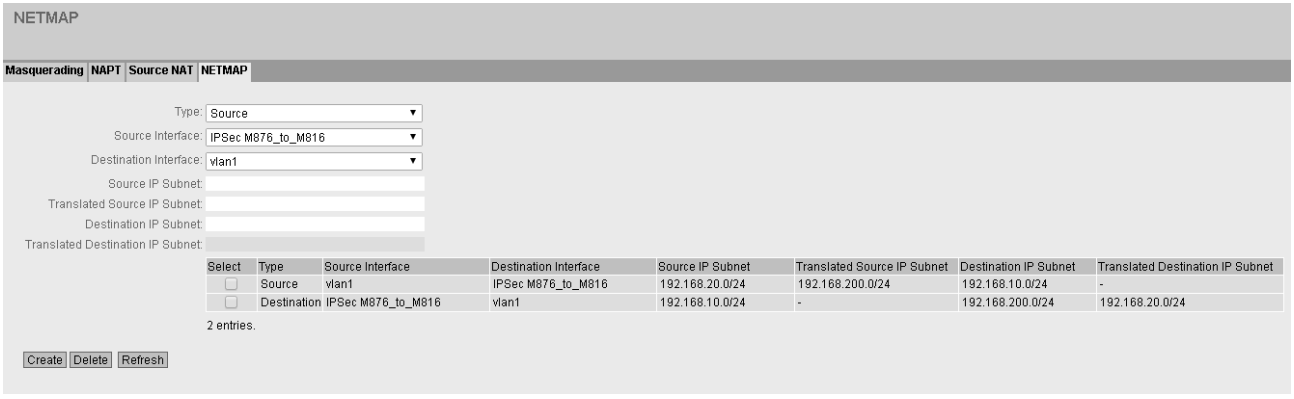
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit den Einstellungen angelegt.
4. Legen Sie die NETMAP-Regel B1 für die eingehenden Anfragen mit folgenden Einstellungen fest:

Type	Destination
Source Interface	IPSec M876_to_M816
Destination Interface	vlan1
Source IP Subnet	192.168.10.0/24
Destination IP Subnet	192.168.200.0/24
Translated Destination IP Subnet	192.168.20.0/24

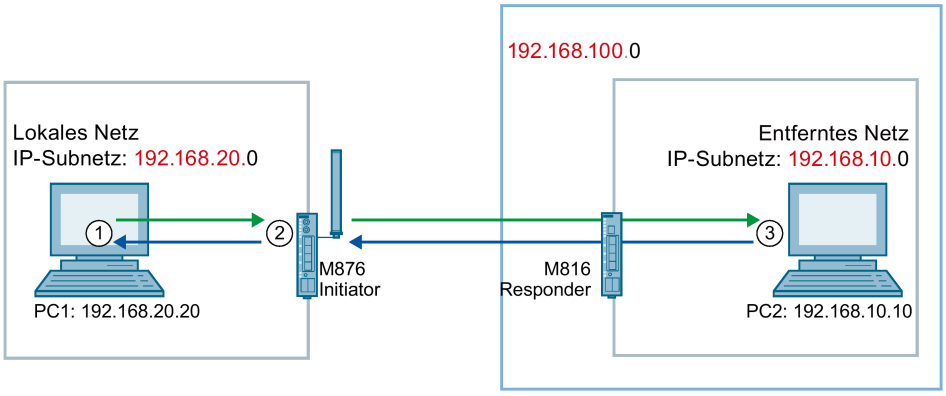
5. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit den Einstellungen angelegt.
6. Klicken Sie auf "Set Values".

Ergebnis

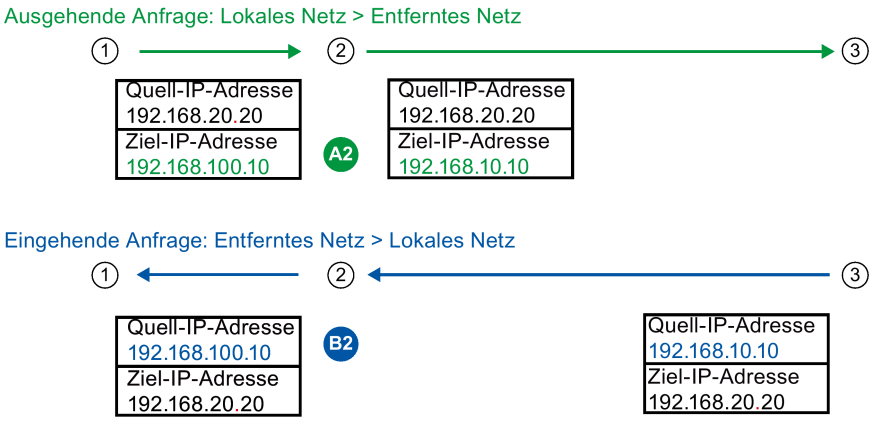
Die Regeln für die aus- und eingehenden Anfragen sind angelegt.



6.2 NETMAP für das entfernte Netz



- IP-Subnetz nach außen sichtbar



Beim NETMAP des entfernten Netzes wird die Ziel-IP-Adresse ① z. B. 192.168.100.10 umgesetzt. In diesem Beispiel ist der Subnetzanteil 192.168.100.0 und wird durch 192.168.10.0 ersetzt. Dadurch ist das entfernte Netz zusätzlich zur 192.168.10.0 auch über die 192.168.100.0 zu erreichen. Die Ziel-IP-Adresse wird vom M876 ② umgesetzt und an das Ziel ③ weitergeleitet.

Bei eingehenden Anfragen ③ wird die Quell-IP-Adresse 192.168.10.0 durch 192.168.100.0 ersetzt. Die Quell-IP-Adresse wird vom M876 ② umgesetzt und an das Ziel ① weitergeleitet.

Es sind nur die NETMAP-Regeln für die Anfragerichtung notwendig. Die NETMAP-Regeln für die Antworten werden implizit hinzugefügt. Wenn PC1 eine Anfrage an PC2 sendet, wird die Antwort darauf umgesetzt. Das gilt aber nicht für die Anfragen von PC2 an PC1.

Dazu werden auf dem M876 (Initiator) die folgenden NETMAP-Regeln angelegt:

- A2 Lokales Netz > Entferntes Netz:
  Das Ziel-IP-Subnetz 192.168.100.0/24 wird durch 192.168.10.0/24 ersetzt.
- B2 Entferntes Netz > Lokales Netz:
  Das Quell-IP-Subnetz 192.168.10.0/24 wird durch 192.168.100.0/24 ersetzt

Zusätzlich sollen die beiden Geräte über einen VPN-Tunnel miteinander kommunizieren.

Voraussetzung

- Das SCALANCE M-800 ist mit dem WAN verbunden, siehe "SCALANCE M-800 mit dem WAN verbinden (Seite 11)".
- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

Folgende Schritte sind erforderlich

1. VPN-Verbindung anlegen (Seite 222)
2. NETMAP-Regeln erstellen (Seite 224)

6.2.1 VPN-Verbindung anlegen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN" und klicken Sie auf "Set Values".
3. Klicken Sie im Inhaltsbereich auf das Register "Remote End" und legen Sie die VPN-Gegenstelle mit folgenden Einstellungen an:

	Am M816	**Am M876**
Remote End Name	M816	M876
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Erreichbar über einen dynamischen DNS-Dienst z. B. example.no-ip.com	Feste IP-Adresse (WAN-IP-Adresse) des M816, z. B. 91.19.6.84
Remote Subnet	192.168.20.0/24	192.168.10.0/24

4. Klicken Sie im Inhaltsbereich auf das Register "Connections" und legen Sie die VPN-Verbindung mit folgenden Einstellungen an.

	Am M816	**Am M876**
Connection Name	M816_to_M876_2	M876_to_M816_2
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M816	M876
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Klicken Sie im Inhaltsbereich auf das Register "Authentication" und konfigurieren Sie die VPN-Authentifizierung mit folgenden Einstellungen.

	Am M816	**Am M876**
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	z. B. 12345678	z. B. 12345678

6. Klicken Sie im Inhaltsbereich auf das Register "Phase 1" und konfigurieren Sie die folgende Einstellungen.

	M816 / M876
DPD	aktiviert
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

7. Klicken Sie im Inhaltsbereich auf das Register "Phase 2" und konfigurieren Sie die folgende Einstellungen.

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Ergebnis

Die VPN-Verbindung auf den Geräten ist konfiguriert. Um die VPN-Verbindung aufzubauen, klicken Sie im Inhaltsbereich auf das Register "Connection".

Wählen Sie bei "Operation" Folgendes aus und klicken auf "Set Values"

	Am M816	**Am M876**
Operation	wait (Responder)	start (Initiator)

Das M876 baut den VPN-Tunnel zum M816 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet an den Geräten die LED 🔒 grün.

6.2.2 NETMAP-Regeln erstellen

Voraussetzung

- Die VPN-Verbindung M876_to_M816_2 ist konfiguriert, siehe VPN-Verbindung anlegen (Seite 222).

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3" > "NAT" und im Inhaltsbereich auf das Register "NETMAP".
2. Legen Sie die NETMAP-Regel A2 für die ausgehenden Anfragen mit folgenden Einstellungen fest:

Type	Destination
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816_2
Source IP Subnet	192.168.20.0/24
Destination IP Subnet	192.168.100.0/24
Translated Destination IP Subnet	192.168.10.0/24

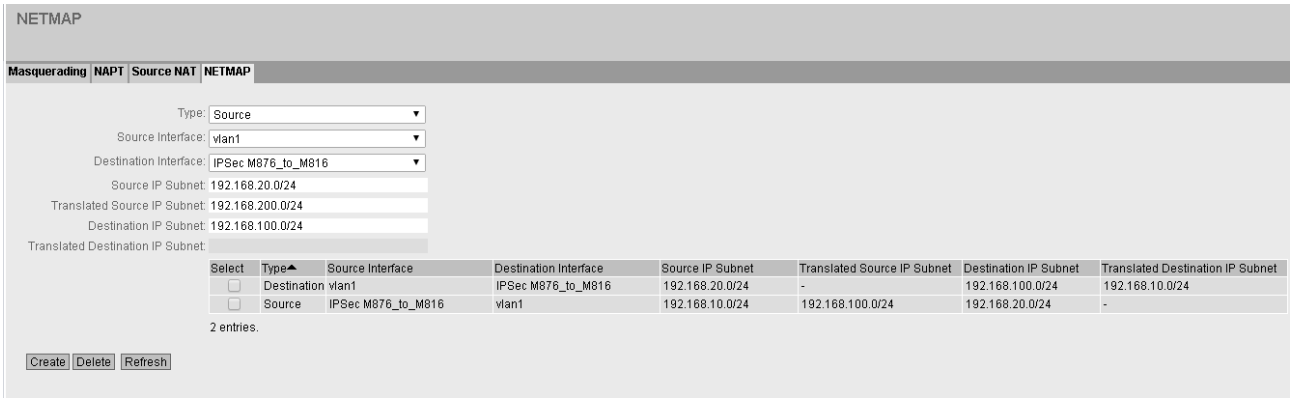
3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit den Einstellungen angelegt.
4. Legen Sie die NETMAP-Regel B2 für die eingehenden Anfragen mit folgenden Einstellungen fest:

Type	Source
Source Interface	IPSec M876_to_M816_2
Destination Interface	vlan1
Source IP Subnet	192.168.10.0/24
Translated Source IP Subnet	192.168.100.0/24
Destination IP Subnet	192.168.20.0/24

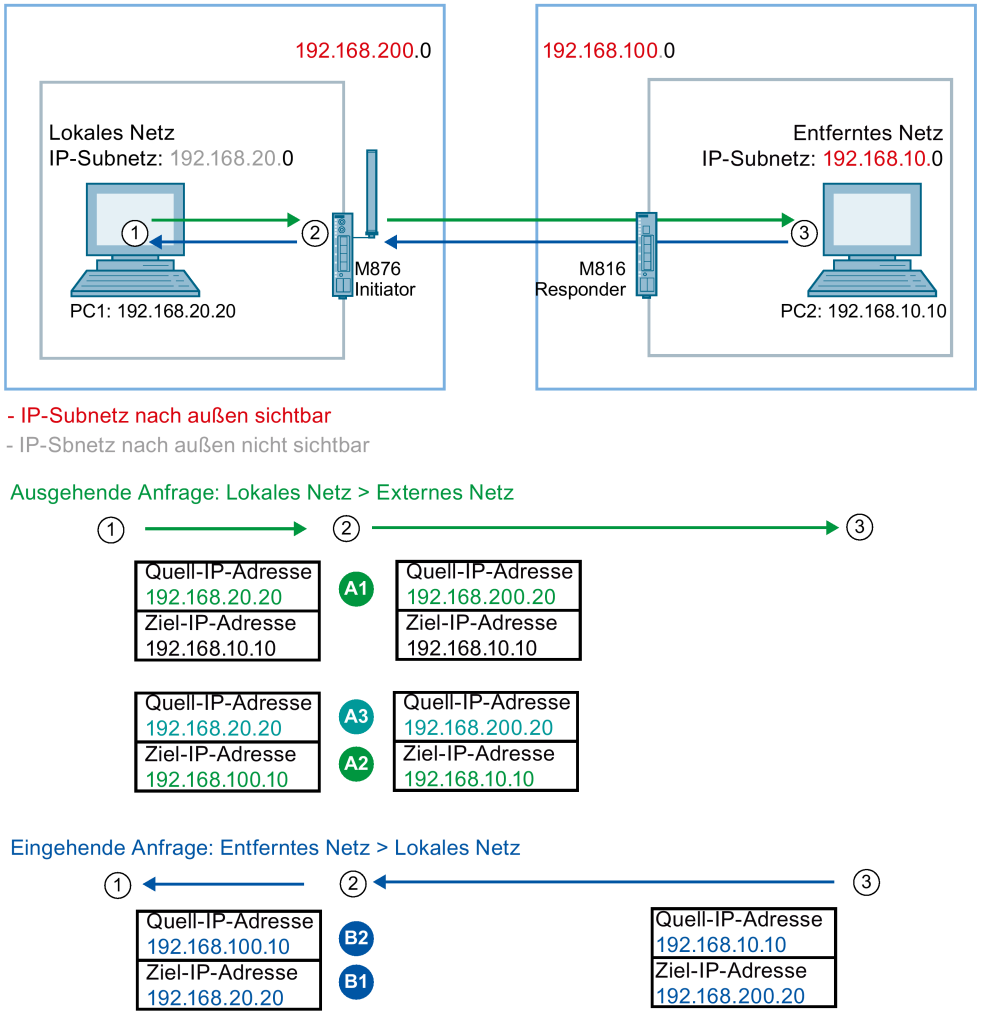
5. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit den Einstellungen angelegt.
6. Klicken Sie auf "Set Values".

Ergebnis

Die Regeln für die aus- und eingehenden Anfragen sind angelegt.



6.3 NETMAP für das lokale und das entfernte Netz



In diesem Beispiel werden die NETMAP-Regeln aus NETMAP für das lokale Netz (Seite 216)und aus NETMAP für das entfernte Netz (Seite 221) kombiniert.

Allerdings gibt es bei den ausgehenden Anfragen eine Besonderheit. Bei ausgehenden Anfragen, deren Quell-IP-Adresse von 192.168.20.0 nach 192.168.200.0 umgesetzt werden, können als Ziel-IP-Adresse sowohl die IP-Adresse 192.168.10.10 als auch die IP-Adresse 192.168.100.10 habe. Für die Regel zum Umsetzen der Ziel-IP-Adresse, ist eine weitere NETMAP-Regel notwendig. Die Adressen werden vom M876 ② umgesetzt und an das Ziel ③ weitergeleitet.

Bei den eingehenden Anfragen werden beide IP-Adressen ausgetauscht.

A1 Lokales Netz > Entferntes Netz:
Das Quell-IP-Subnetz 192.168.20.0/24 wird durch 192.168.200.0/24 ersetzt.

A2 Das Ziel-IP-Subnetz 192.168.100.0/24 wird durch 192.168.10.0/24 ersetzt.

A3 Bei Anfragen mit dem Ziel-IP-Subnetz 192.168.100.0/24 wird das Quell-IP-Subnetz 192.168.20.0/24 wird durch 192.168.200.0/24 ersetzt.

B1 Entferntes Netz > Lokales Netz:
Das Ziel-IP-Subnetz 192.168.200.0/24 wird durch 192.168.20.0/24 ersetzt

B2 Das Quell-IP-Subnetz 192.168.10.0/24 wird durch 192.168.100.0/24 ersetzt

Zusätzlich sollen die beiden Geräte über einen VPN-Tunnel miteinander kommunizieren.

Voraussetzung

- Das SCALANCE M-800 ist mit dem WAN verbunden, siehe "SCALANCE M-800 mit dem WAN verbinden (Seite 11)".
- Das SCALANCE M-800 ist über den Admin-PC erreichbar und Sie sind am WBM als "admin" angemeldet.

Projektierungsschritte

Folgende Schritte sind erforderlich

1. VPN-Verbindung anlegen (Seite 227)
2. NETMAP-Regeln erstellen (Seite 229)

6.3.1 VPN-Verbindung anlegen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Security" > "IPSec VPN" und im Inhaltsbereich auf das Register "General".
2. Aktivieren Sie "Activate IPSec VPN" und klicken Sie auf "Set Values".
3. Klicken Sie im Inhaltsbereich auf das Register "Remote End" und legen Sie die VPN-Gegenstelle mit folgenden Einstellungen an:

	Am M816	**Am M876**
Remote End Name	M876	M816
Remote Mode	Standard	Standard
Remote Typ	manual	manual
Remote Address	Erreichbar über einen dynamischen DNS-Dienst z. B. example.no-ip.com	Feste IP-Adresse (WAN-IP-Adresse) des M816, z. B. 91.19.6.84
Remote Subnet	192.168.200.0/24	192.168.10.0/24

4. Klicken Sie im Inhaltsbereich auf das Register "Connections" und legen Sie die VPN-Verbindung mit folgenden Einstellungen an.

	Am M816	**Am M876**
Connection Name	M816_to_M876	M876_to_M816
Operation	disable	disable
Keyping Protocol	IKv2	IKv2
Remote End Name	M876	M816
Local Subnet	192.168.10.0/24	192.168.20.0/24

5. Klicken Sie im Inhaltsbereich auf das Register "Authentication" und konfigurieren Sie die VPN-Authentifizierung mit folgende Einstellungen.

	Am M816	**Am M876**
Authentication	PSK	PSK
Local ID	-	-
Remote ID	-	-
PSK / PSK Confirmation	z. B. 12345678	z. B. 12345678

6. Klicken Sie im Inhaltsbereich auf das Register "Phase 1" und konfigurieren Sie die folgenden Einstellungen.

	M816 / M876
DPD	aktiviert
Encryption	AES256 CBC (M87x) AES256 (M81x)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440
DPD timeout [sec]	60
Aggressive Mode	nein

7. Klicken Sie im Inhaltsbereich auf das Register "Phase 2" und konfigurieren Sie die folgenden Einstellungen.

	M816 / M876
Encryption	AES256 CBC (M87x) AES256 (M816)
Authentication	SHA512
IKE Key Derivation	DH group 14
Lifetime [min]	1440

Ergebnis

Die VPN-Verbindung auf den Geräten ist konfiguriert. Um die VPN-Verbindung aufzubauen, klicken Sie im Inhaltsbereich auf das Register "Connection".

Wählen Sie bei "Operation" Folgendes aus und klicken auf "Set Values"

	Am M816	**Am M876**
Operation	wait (Responder)	start (Initiator)

Das M876 baut den VPN-Tunnel zum M816 auf. Wenn der VPN-Tunnel aufgebaut ist, leuchtet an den Geräten die LED grün.

6.3.2 NETMAP-Regeln erstellen

Voraussetzung

- Die VPN-Verbindung M876_to_M816_2 ist konfiguriert, siehe VPN-Verbindung anlegen (Seite 227).
- Die NETMAP-Regeln für das lokale Netz (Seite 224)sind angelegt.
- Die NETMAP-Regeln für das entfernte Netz (Seite 219) sind angelegt.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3" > "NAT" und im Inhaltsbereich auf das Register "NETMAP".
2. Legen Sie die NETMAP-Regel A3 für die ausgehenden Anfragen mit folgenden Einstellungen fest:

Type	Source
Source Interface	vlan1
Destination Interface	IPSec M876_to_M816_2
Source IP Subnet	192.168.20.0/24
Destination IP Subnet	192.168.100.0/16
Translated Source IP Subnet	192.168.200.0/24

3. Klicken Sie auf "Create". In der Tabelle wird eine neue Zeile mit den Einstellungen angelegt.
4. Klicken Sie auf "Set Values".

Ergebnis

Die Regeln für die aus- und eingehenden Anfragen sind angelegt.