TECHDOCS

Handbuch

WAGO-I/O-SYSTEM 750

750-8xxx(/xxx-xxx)

PFC100/200

Cyber Security für Controller PFC100/PFC200

Version 1.2.1

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Tel.: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technischer Support

Tel.: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich Fehler, trotz aller Sorgfalt, nie vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: documentation@wago.com

Inhaltsverzeichnis

1 Hinweise zu dieser Dokumentation 6
1.1 Urheberschutz 6
1.2 Symbole 7
1.3 Darstellung der Zahlensysteme 8
1.4 Schriftkonventionen 8

2 Wichtige Erläuterungen 9
2.1 Rechtliche Grundlagen 9
2.1.1 Änderungsvorbehalt 9
2.1.2 Personalqualifikation 9
2.1.3 Bestimmungsgemäße Verwendung der Serie 750 9
2.1.4 Technischer Zustand der Geräte 10

3 Einleitung 11
3.1 Abkürzungen 13

4 Standardkonfiguration 15
4.1 Physikalische Schnittstellen 15
4.2 Netzwerkdienste 16
4.2.1 Gerätespezifische Dienste 18
4.3 Benutzer und Passwörter 18
4.3.1 WBM-Benutzer 18
4.3.2 Linux®-Benutzer 18
4.3.3 SNMP-Benutzer 19
4.3.4 CODESYS und *e!RUNTIME*-Webvisualisierung 19

5 Bedrohungen für industrielle Steuerungssysteme 20
5.1 Defense-in-Depth-Prinzip 21
5.2 Spezifische Bedrohungen anhand einer Referenzarchitektur 23
5.2.1 Physikalische Schnittstellen am WAGO-Controller 25
5.2.1.1 Reset-Taster 26
5.2.1.2 Betriebsartenschalter 26
5.2.1.3 ETHERNET-Schnittstellen (X1 / X2) 26
5.2.1.4 Service-Schnittstelle 27
5.2.1.5 Serielle Schnittstelle (RS-232) 27
5.2.1.6 Speicherkartensteckplatz 27
5.2.1.7 GSM/3G-Modem-Schnittstelle 27
5.2.2 Zugänge über das Netzwerk 29
5.2.2.1 Softwarekomponenten 29
5.2.2.2 „Man-in-the-Middle-Attacken“ 29
5.2.2.3 Netzwerk-Schnittstellen und Protokolle 29
5.2.2.4 Firewalls 30
5.2.3 Zugänge über Benutzer und Passwörter 30

6 Hardening 32
6.1 Physikalischen Zugang einschränken 32
6.1.1 Service-Schnittstelle deaktivieren 32
6.1.2 Linux®-Konsole auf der seriellen Schnittstelle deaktivieren 33
6.2 Netzwerkzugänge sichern 34

6.2.1 Verschlüsselt kommunizieren 34
6.2.1.1 Webserverauthentifizierung 34
6.2.1.2 TLS-Verschlüsselung 34
6.2.1.3 Diffie-Hellman-Parameter erzeugen 35
6.2.1.3.1 Diffie-Hellman-Parameter für den Webserver austauschen 36
6.2.1.4 SSH-Zugang „härten“ 37
6.2.1.4.1 Anmeldung über Passworteingabe deaktivieren 40
6.2.1.4.2 Anmeldung per Root-Login verweigern 41
6.2.1.4.3 Server-Schlüssel austauschen 41
6.2.1.5 Zertifikate erstellen und austauschen 43
6.2.1.5.1 Vorlage für die Zertifikate erstellen 43
6.2.1.5.2 Root-CA-Zertifikat erstellen 47
6.2.1.5.3 Gerätezertifikat erstellen 49
6.2.1.5.4 Zertifikate exportieren 54
6.2.1.5.5 Zertifikate auf dem Client und auf dem Gerät installieren 55
6.2.1.5.6 Zertifikatsperrliste anlegen 56
6.2.2 Zugriff über offene Netzwerkschnittstellen einschränken 59
6.2.2.1 WAGO-Service-Kommunikation deaktivieren 59
6.2.2.2 Standard-Netzwerkports ändern 59
6.2.2.3 Unverschlüsselten Zugang auf das WBM sperren 60
6.2.2.4 Zugang zur CODESYS Laufzeitumgebung deaktivieren 61
6.2.2.5 Direktzugriff auf die CODESYS Webvisualisierung sperren 61
6.2.2.6 Zugriff auf die Laufzeitumgebung *e!RUNTIME* sperren 62
6.3 Passwörter ändern 63
6.3.1 Passwörter im Web-Based-Management ändern 63
6.3.2 Linux®-Passwörter über die Linux®-Konsole ändern 64
6.4 Firewall konfigurieren 66
6.4.1 Firewall im Web-Based-Management konfigurieren 67
6.4.1.1 White List für bestimmte IP-Adressen anlegen 68
6.4.1.2 White List für Netzwerke anlegen 71
6.4.2 MAC-Adressenfilter 74
6.4.2.1 MAC-Adressen im Web-Based-Management konfigurieren 74

7 Erweiterte Sicherheitsmaßnahmen 76

7.1 VPN – Virtual Private Network 76
7.1.1 Allgemein 76
7.1.2 Zertifikate erzeugen 78
7.1.3 „IP Forwarding“ aktivieren 78
7.1.4 OpenVPN 79
7.1.4.1 Benutzer und Gruppe für den OpenVPN-Dienst einrichten 79
7.1.4.2 Firewall konfigurieren 80
7.1.4.3 Routing konfigurieren 81
7.1.4.4 Konfigurationsdateien erstellen 83
7.1.4.4.1 Host-to-Host-VPN 83
7.1.4.4.2 Site-to-Site-VPN 87
7.1.4.5 Konfiguration auf den Controller übertragen 90
7.1.5 IPsec 92
7.1.5.1 Sicherheitsprotokolle 92
7.1.5.2 Internet Key Exchange Protokoll (IKE) 93
7.1.5.3 Security Policy Database (SPD) 93

7.1.5.4 Security Association (SA) und Security Parameter Index (SPI) ...93
7.1.5.5 Konfigurationsdateien erstellen ...95
7.1.5.5.1 Host-to-Host-VPN ...95
7.1.5.5.2 Site-to-Site-VPN...97
7.1.5.6 Firewall konfigurieren ...101
7.1.5.7 Konfiguration auf den Controller übertragen ...103
7.2 Port-Authentisierung gemäß IEEE 802.1X...105
7.2.1 Port-Authentisierung mittels Benutzername und Kennwort gemäß EAP-MD5...107
7.2.1.1 EAP-MD5-Port-Authentisierung einrichten...108
7.2.2 Port-Authentisierung mittels Zertifikaten (EAP-TLS)...109
7.2.2.1 EAP-TLS-Port-Authentisierung einrichten...111
7.2.3 Automatische Port-Authentisierung während des Boot-Vorgangs ..112
7.3 Simple Certificate Enrollement Protocol (SCEP)...114
7.3.1 Automatische Bearbeitung der Anfrage...115
7.3.2 Manuelle Bearbeitung ...115
7.3.2.1 SCEP-Prozess einrichten ...116

8 Anhang ...118

8.1 FAQ zu IPsec ...118
8.1.1 Zusätzliche IPsec-Fehler- bzw. Statusanalyse ...119

Abbildungsverzeichnis ...121

Tabellenverzeichnis ...123

1 Hinweise zu dieser Dokumentation

Hinweis

Dokumentation aufbewahren!
Diese Dokumentation ist Teil des Produkts. Bewahren Sie deshalb die Dokumentation während der gesamten Nutzungsdauer des Produkts auf. Geben Sie die Dokumentation an jeden nachfolgenden Benutzer des Produkts weiter. Stellen Sie darüber hinaus sicher, dass gegebenenfalls jede erhaltene Ergänzung in die Dokumentation mit aufgenommen wird.

Die vorliegende Dokumentation gilt für die Standardausführungen sowie alle Varianten der Controller PFC100/PFC200.

1.1 Urheberschutz

1.2 Symbole

GEFAHR

Warnung vor Personenschäden!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

GEFAHR

Warnung vor Personenschäden durch elektrischen Strom!
Kennzeichnet eine unmittelbare Gefährdung mit hohem Risiko, die Tod oder schwere Körperverletzung zur Folge haben wird, wenn sie nicht vermieden wird.

WARNUNG

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit mittlerem Risiko, die Tod oder (schwere) Körperverletzung zur Folge haben kann, wenn sie nicht vermieden wird.

VORSICHT

Warnung vor Personenschäden!
Kennzeichnet eine mögliche Gefährdung mit geringem Risiko, die leichte oder mittlere Körperverletzung zur Folge haben könnte, wenn sie nicht vermieden wird.

ACHTUNG

Warnung vor Sachschäden!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

ESD

Warnung vor Sachschäden durch elektrostatische Aufladung!
Kennzeichnet eine mögliche Gefährdung, die Sachschaden zur Folge haben könnte, wenn sie nicht vermieden wird.

Hinweis

Wichtiger Hinweis!
Kennzeichnet eine mögliche Fehlfunktion, die aber keinen Sachschaden zur Folge hat, wenn sie nicht vermieden wird.

Information

Weitere Information
Weist auf weitere Informationen hin, die kein wesentlicher Bestandteil dieser Dokumentation sind (z. B. Internet).

1.3 Darstellung der Zahlensysteme

Tabelle 1: Darstellungen der Zahlensysteme

Zahlensystem	Beispiel	Bemerkung
Dezimal	100	Normale Schreibweise
Hexadezimal	0x64	C-Notation
Binär	'100' '0110.0100'	In Hochkomma, Nibble durch Punkt getrennt

1.4 Schriftkonventionen

Tabelle 2: Schriftkonventionen

Schriftart	Bedeutung
kursiv	Namen von Pfaden und Dateien werden kursiv dargestellt z. B.: *C:\Programme\WAGO Software*
Menü	Menüpunkte werden fett dargestellt z. B.: **Speichern**
>	Ein „Größer als“- Zeichen zwischen zwei Namen bedeutet die Auswahl eines Menüpunktes aus einem Menü z. B.: **Datei > Neu**
Eingabe	Bezeichnungen von Eingabe- oder Auswahlfeldern werden fett dargestellt z. B.: **Messbereichsanfang**
„Wert“	Eingabe- oder Auswahlwerte werden in Anführungszeichen dargestellt z. B.: Geben Sie unter **Messbereichsanfang** den Wert „4 mA“ ein.
[Button]	Schaltflächenbeschriftungen in Dialogen werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[Eingabe]**
[Taste]	Tastenbeschriftungen auf der Tastatur werden fett dargestellt und in eckige Klammern eingefasst z. B.: **[F5]**

2 Wichtige Erläuterungen

Dieses Kapitel beinhaltet ausschließlich eine Zusammenfassung der wichtigsten Sicherheitsbestimmungen und Hinweise. Diese werden in den einzelnen Kapiteln wieder aufgenommen. Zum Schutz vor Personenschäden und zur Vorbeugung von Sachschäden an Geräten ist es notwendig, die Sicherheitsrichtlinien sorgfältig zu lesen und einzuhalten.

2.1 Rechtliche Grundlagen

2.1.1 Änderungsvorbehalt

Die WAGO Kontakttechnik GmbH & Co. KG behält sich Änderungen vor. Alle Rechte für den Fall der Patenterteilung oder des Gebrauchsmusterschutzes sind der WAGO Kontakttechnik GmbH & Co. KG vorbehalten. Fremdprodukte werden stets ohne Vermerk auf Patentrechte genannt. Die Existenz solcher Rechte ist daher nicht auszuschließen.

2.1.2 Personalqualifikation

Sämtliche Arbeitsschritte, die an den Geräten des WAGO-I/O-SYSTEMs 750 durchgeführt werden, dürfen nur von Elektrofachkräften mit ausreichenden Kenntnissen im Bereich der Automatisierungstechnik vorgenommen werden. Diese müssen mit den aktuellen Normen und Richtlinien für die Geräte und das Automatisierungsumfeld vertraut sein.

Alle Eingriffe in die Steuerung sind stets von Fachkräften mit ausreichenden Kenntnissen in der SPS-Programmierung durchzuführen.

2.1.3 Bestimmungsgemäße Verwendung der Serie 750

Feldbuskoppler, Controller und I/O-Module des modularen WAGO-I/O-SYSTEMs 750 dienen dazu, digitale und analoge Signale von Sensoren aufzunehmen und an Aktoren auszugeben oder an übergeordnete Steuerungen weiterzuleiten. Mit den Controllern ist zudem eine (Vor-)Verarbeitung möglich.

Die Geräte sind für ein Arbeitsumfeld entwickelt, welches der Schutzart IP20 genügt. Es besteht Fingerschutz und Schutz gegen feste Fremdkörper ≥ 12,5 mm, jedoch kein Schutz gegen Wasser. Der Betrieb der Geräte in nasser und staubiger Umgebung ist nicht gestattet, sofern nicht anders angegeben.

Der Betrieb von Geräten des WAGO-I/O-SYSTEMs 750 im Wohnbereich ist ohne weitere Maßnahmen nur zulässig, wenn diese die Emissionsgrenzen (Störaussendungen) gemäß EN 61000-6-3 einhalten. Entsprechende Angaben finden Sie im Kapitel „Gerätebeschreibung“ > „Normen und Richtlinien“ im Handbuch zum eingesetzten Feldbuskoppler oder Controller.

Für den Betrieb des WAGO-I/O-SYSTEMs 750 in explosionsgefährdeten Bereichen ist ein entsprechender Gehäuseschutz gemäß der Richtlinie 2014/34/EU erforderlich. Zusätzlich ist zu beachten, dass eine Baumusterprüfbescheinigung erwirkt werden muss, die den korrekten Einbau des Systems im Gehäuse bzw. Schaltschrank bestätigt.

Die Realisierung von Sicherheitsfunktionen wie NOT-HALT-Einrichtungen oder Schutztürüberwachungen darf nur von den F-I/O-Modulen des modularen WAGO-I/O-SYSTEMs 750 ausgeführt werden. Nur diese sicheren F-I/O-Module gewährleisten funktionale Sicherheit gemäß den aktuellen internationalen Normen. Rückwirkungsfreie Ausgangsmodule von WAGO können von der Sicherheitsfunktion angesteuert werden.

2.1.4 Technischer Zustand der Geräte

Die Geräte werden ab Werk für den jeweiligen Anwendungsfall mit einer festen Hard- und Softwarekonfiguration ausgeliefert. Sie enthalten keine durch den Anwender zu wartenden oder zu reparierenden Teile. Folgende Handlungen bewirken den Haftungsausschluss der WAGO Kontakttechnik GmbH & Co. KG:

- Reparaturen,
- Veränderungen an der Hard- oder Software, die nicht in der Bedienungsanleitung beschrieben sind,
- nicht bestimmungsgemäßer Gebrauch der Komponenten.

Weitere Einzelheiten ergeben sich aus den vertraglichen Vereinbarungen. Wünsche an eine abgewandelte bzw. neue Hard- oder Softwarekonfiguration richten Sie bitte an die WAGO Kontakttechnik GmbH & Co. KG.

3 Einleitung

Durch die Vernetzung industrieller Anlagen mit dem Internet sind Steuerungssysteme, wie das WAGO-I/O-SYSTEM, anfälliger für Cyberangriffe. Um Sicherheitsbedrohungen zu minimieren und wirtschaftliche Schäden zu vermeiden, gibt es drei wesentliche Sicherheitsziele, die von einem System erfüllt werden sollten:

- **Verfügbarkeit**:
  Die Daten und Funktionen eines Systems sollten zeit- und bedarfsgerecht zur Verfügung stehen.
- **Integrität**
  Die Korrektheit und Vollständigkeit von schützenswerten Daten sowie die korrekte Funktionsweise des Systems sollten gewährleistet sein.
- **Vertraulichkeit**
  Schützenswerte Daten und Informationen sollten nur Personen zugänglich sein, die dazu berechtigt sind.

Die vorliegende Dokumentation beschreibt potenzielle Sicherheitsbedrohungen und hat zum Ziel diese Sicherheitsbedrohungen mit wirksamen und angemessenen Maßnahmen abzuwehren.

Zu den Grundsätzen eines sicheren Systemdesigns gehören:

- **Minimale Privilegien/Minimales Need-to-know-Prinzip:**
  Benutzer- und Systemkomponenten verfügen nur über minimale Privilegien und Zugriffsrechte, die zur Erfüllung einer bestimmten Aktion erforderlich sind.
- **Gestaffelte Sicherheitsebenen/„Defense-in-Depth Prinzip“:**
  Sicherheitsbedrohungen werden nicht nur durch eine einzige Gegenmaßnahme abgeschwächt, sondern durch mehrere gestaffelte und sich ergänzende Sicherheitsmaßnahmen.
- **Redundanzprinzip:**
  Systeme sind so ausgelegt, dass ein Fehler an einer Komponente die Funktionen der Sicherheitssysteme nicht beeinträchtigt. Die Wahrscheinlichkeit und die Schwere der Probleme (z. B. Denial-of-Service-Angriffe), die durch einen übermäßigen Verbrauch von Systemressourcen verursacht werden, müssen dementsprechend minimiert werden.

Die ETHERNET-basierenden WAGO-Produkte sind auf den Betrieb innerhalb eines geschlossenen industriellen Kommunikationsnetzwerks ausgerichtet. Sofern die Geräte nicht nur innerhalb geschlossener, industrieller Netzwerke eingesetzt werden sollen, gilt es seitens des Integrators und des Betreibers weitere Sicherheitsmaßnahmen zur optimalen Nutzung der Produkte zu treffen.

Sind die industriellen Netzwerke öffentlich zugänglich (z. B. durch frei zugängliche Netzwerkschnittstellen innerhalb des in sich geschlossenen, industriellen Netzwerkes) oder öffentlich erreichbar (z. B. durch Datenverbindungen über den öffentlichen Datenverkehr (Internet)), dann müssen organisatorische und technische Sicherheitsmaßnahmen ergriffen werden, um

das interne Netzwerk zu schützen und die Sicherheitsziele sicherzustellen. Die zu ergreifenden Sicherheitsmaßnahmen hängen dabei von dem zu erwartenden Risiko durch eine potenzielle, äußere Einflussnahme ab.

Die Controller PFC100 und PFC200 bieten umfangreiche Sicherheitsfunktionen, wie z.B. TLS, SSH, VPN und eine hostbasierte Firewall. Ein integrierter Passwortschutz und eine gesicherte Kommunikation schützen vor Zugriffen auf Funktionen, Programminhalte und vor dem Einschleusen von Schadsoftware.

Diese und weitere Schutzmaßnahmen, die in diesem Handbuch empfohlen werden, helfen Ihnen dabei, das Angriffsrisiko durch bestimmte Bedrohungen auf Maschinen und Anlagen zu minimieren und den oben beschriebenen Sicherheitszielen näherzukommen. Zusätzlich zu den Empfehlungen werden gemeldete, potenzielle Sicherheitslücken durch WAGO untersucht, bewertet und behoben, sofern eine Behebung nicht die generelle Funktionsweise des Produktes beeinträchtigt. Die Informationen in diesem Handbuch werden nach Bedarf kontinuierlich aktualisiert.

3.1 Abkürzungen

Tabelle 3: Abkürzungen

Abkürzung	Bedeutung	Beschreibung
AH	Authentication Header	Das AH-Protokoll sorgt innerhalb von IPsec (VPN) für die Authentizität der zu übertragenen Daten und die Authentifizierung des Senders. Mit AH wird die Integrität und Echtheit der Daten sichergestellt. Die Nutzdaten werden jedoch nicht verschlüsselt und sind damit für jeden lesbar.
BSI	Bundesamt für Sicherheit in der Informationstechnik	Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.
ESP	Encapsulating Security Payload	Das ESP-Protokoll ist für die Sicherstellung der Authentizität, Integrität und Vertraulichkeit der zu übertragenen IP-Pakete zuständig. Im Unterschied zum AH-Protokoll verschlüsselt das ESP-Protokoll zusätzlich die Nutzdaten.
IKE	Internet key exchange	Das IKE ist ein Schlüsselprotokoll zum Austausch der Schlüssel des Internet Protocol Security (siehe Kapitel „IPsec“).
IPsec	Internet Protocol Security	IPsec ist eine Erweiterung des Internet-Protokolls (IP). Mit erweiterten Verschlüsselungs- und Authentifizierungs-mechanismen können IP-Pakete kryptografisch gesichert über öffentliche und unsichere Netze transportiert werden.
PSK	Pre-Shared Key	Pre-Shared Key bedeutet, dass die Schlüssel zur Authentifizierung und Verschlüsselung vorab zwischen den Teilnehmern ausgetauscht werden.
ROOT-CA	Wurzel-zertifizierungsstelle	Die Root-CA signiert ihr eigenes Zertifikat selbst. Das Wurzelzertifikat bildet damit den gemeinsamen Vertrauensanker aller ihm untergeordneter Zertifikate.
SA	Security Association	Eine Security Association (dt. Sicherheitsvereinbarung) ist die grundlegende Basis jeder IPsec-Verbindung. Sie beschreibt, wie zwei miteinander kommunizierende Parteien in Rechnernetzen sicher miteinander kommunizieren können. Diese Sicherheitsvereinbarungen werden für den Authentication Header (AH) und den Encapsulated Security Payload (ESP) jeweils individuell getroffen.

Tabelle 3: Abkürzungen

Abkürzung	Bedeutung	Beschreibung
SCEP	Simple Certificate Enrollment Process	SCEP vereinfacht das Anfordern und Ausstellen von Zertifikaten in internen vertrauenswürdigen Netzwerken. Die Idee dabei ist, dass jeder Standardnetzwerk-Benutzer sein digitales Zertifikat auf elektronischem Wege selbstständig holen kann.
SPI	Security Parameter Index	Der SPI ist eine Nummer, die gemeinsam mit der IP-Zieladresse und einem Sicherheitsprotokoll, eine bestimmte Sicherheitsvereinbarung (SA) identifiziert.
VPN	Virtual Private Network	Ein virtuelles privates Netzwerk ist ein in sich geschlossenes logisches Netzwerk, bei dem die Teilnehmer räumlich voneinander getrennt über einen VPN-Tunnel verbunden sind.
WBM	Web-Based-Management	Über das Web-Based-Management können WAGO-Geräte per Webbrowser konfiguriert und administriert werden.

4 Standardkonfiguration

Nachfolgend wird die Standardkonfiguration der Controller aufgeführt. Mögliche Sicherheitsrisiken über netzwerkbasierte oder physikalische Zugriffe werden im Kapitel „Bedrohungsszenarien“ dargestellt. Daraus resultierende notwendige Maßnahmen zur Vermeidung dieser Sicherheitsrisiken werden im Kapitel „Hardening“ beschrieben.

4.1 Physikalische Schnittstellen

Die Controller verfügen über die in der nachfolgenden Tabelle aufgelisteten physikalischen Schnittstellen.

Gerät	Bedeutung
Speicherkarten-Steckplatz	Steckplatz für SD-Speicherkarte
RS-232/-485	Kommunikationsanschluss
RJ-45 (ETHERNET)	Netzwerkanschluss für ETHERNET
Service-Schnittstelle	Serieller Anschluss für Service-Tätigkeiten an WAGO-Geräten
Reset-Taster	Kurzhubtaster mit unterschiedlichen Funktionen, abhängig von der Position des Betriebsartenschalters
Betriebsartenschalter	Unterschiedliche Funktionen (RUN, STOP, RESET), abhängig vom Zustand des Gerätes
ETHERNET-Schnittstellen X1/X2	Netzwerkanschlüsse
3G-Modem	Internes Mobilfunkmodem (nur bei 750-8207)

Folgende Feldbussysteme werden unterstützt:

- CANopen,
- PROFIBUS DP,
- Modbus TCP/UPD/RTU

Hinweis

Nähere Informationen finden Sie in den Produkthandbüchern!
Nähere Informationen zu den physikalischen Schnittstellen und Feldbussen finden Sie in den entsprechenden Handbüchern der jeweiligen Controller!

4.2 Netzwerkdienste

Die standardmäßig unterstützten Protokolle bzw. Dienste der Controller sind nachfolgend aufgelistet. Zusätzlich zu diesen Diensten sind im Abschnitt „Gerätespezifische Dienste“ die Dienste aufgeführt, die nur von bestimmten Geräten unterstützt werden.

Hinweis

Aktive Ports können angezeigt werden!
Sie können sich die aktuell geöffneten aktiven Ports anzeigen lassen, indem Sie den Befehl „netstat -tulp“ als Benutzer „root“ auf der Linux®-Konsole ausführen!

Tabelle 4: Basiskonfiguration Server

Port	Protokoll	Beschreibung	Programm
20/TCP 21/TCP	FTP (File Transfer Protocol)	Protokoll zur Dateiübertragung[2)]	pure-ftpd
20/TCP 21/TCP	FTPS (File Transfer Protocol over SSL)	Verschlüsseltes Protokoll zur Dateiübertragung[2)]	pure-ftpd
22/TCP	SSH (Secure Shell)	Verschlüsseltes Netzwerkprotokoll für den Fernzugriff[1)]	dropbear
22/TCP	SFTP (Secure File Transfer Protocol)	Verschlüsseltes Protokoll zur Dateiübertragung[1)]	sftp-server
23/TCP	Telnet	Netzwerkprotokoll für den Fernzugriff[2)]	busybox
53/TCP 53/UDP	DNS (Domain Name System)	Protokoll für die Namensauflösung[2)]	dnsmasq
67/UDP	DHCP (Dynamic Host Configuration Protocol)	Protokoll zur Geräteparameterierung[2)]	dnsmasq
69/UDP	TFTP (Trivial File Transfer Protocol)	Protokoll zur Dateiübertragung[2)]	tftpd
80/TCP	HTTP (Hyper Text Transfer Protocol)	Protokoll zum Laden von Webseiten[1)]	lighttpd
161/UDP 162/UDP (Trap)	SNMP v1 (Simple Network Management Protocol v1)	Protokoll für die Steuerung und Überwachung von Netzwerkelementen[2)]	net-smnp
161/UDP 162/UDP (Trap)	SNMP v2c (Simple Network Management Protocol v2c)	Protokoll für die Steuerung und Überwachung von Netzwerkelementen[2)]	net-smnp
161/UDP 162/UDP (Trap)	SNMP v3 (Simple Network Management Protocol v3)	Protokoll für die Steuerung und Überwachung von Netzwerkelementen[2)]	net-smnp
443/TCP	HTTPS (Hyper Text Transfer Protocol over SSL)	Protokoll zum sicheren Übertragen von Webseiten[1)]	lighttpd
4500/UDP	IPsec (Internet Protocol Security)	Protokoll zum Verbinden von zwei vertrauenswürdigen Geräten/Netzwerken über ein nicht vertrauenswürdiges Netzwerk, z.B. das Internet	ipsec
500/UDP	IKEv2 (Internet-Key-Exchange-Protokoll)	Protokoll zum automatischen Schlüsselaustausch für IPsec	charon
502/TCP 502/UDP	Modbus	Protokoll für den Prozessdatenaustausch (***e!****RUNTIME*)[1)]	codesys3
502/TCP 502/UDP	Modbus	Protokoll für den Prozessdatenaustausch (CODESYS V2)[1,5)]	plclinux_rt
514/UDP	Syslog	Protokoll für die Übertragung von Log-Meldungen[1,4)]	syslog-ng

Tabelle 4: Basiskonfiguration Server

Port	Protokoll	Beschreibung	Programm
1194/UDP	OpenVPN	Protokoll zum Verbinden von zwei Geräten/Netzwerke über ein nicht vertrauenswürdiges Netzwerk, z.B. das Internet.	openvpn
1740/UDP	PLC Handler	***e!****RUNTIME*-Laufzeitumgebung[1,2)]	codesys3
2159/TCP	GDB remote serial protocol	Protokoll für das Debuggen von Remote Targets	gdbserver
2455/TCP	PLC Handler	CODESYS Laufzeitumgebung[1,3,5)]	plclinux_rt
4840/TCP	OPC UA (OPC Unified Architecture)	Protokoll zum Datenaustausch[3)]	codesys3
6626/TCP	I/O-Check	Proprietäres Protokoll von WAGO zur Geräteparametrierung[1,4)]	iocheckd
8080/TCP	HTTP (Hyper Text Transfer Protocol)	***e!****RUNTIME*-Webserver[2,3)]	codesys3
8080/TCP	HTTP (Hyper Text Transfer Protocol)	CODESYS Webserver[2,3,5)]	plclinux_rt
11740/TCP	PLC Handler	***e!****RUNTIME* Laufzeitumgebung[3)]	codesys3
UDP		Durch ***e!****RUNTIME* geöffneter Port ohne Funktion[3)]	codesys3

[1)] Dienst ist im Auslieferungszustand aktiv
[2)] Dienst muss durch den Benutzer aktiviert werden oder wird aktiviert sobald eine (CODESYS/***e!****RUNTIME*-)Applikation auf dem Gerät gestartet wird
[3)] Dienst/Port ist abhängig von der verwendeten Laufzeitumgebung
[4)] Dienst/Port ist an den Local Host gebunden und von außen nicht erreichbar
[5)] Nur beim PFC200 verfügbar

Tabelle 5: Basiskonfiguration Client

Port	Protokoll	Beschreibung	Programme
52/TCP 52/UDP	DNS (Domain Name System	Protokoll zur Namensauflösung	-
68/UDP	DHCP (Dynamic Host Configuration Protocol)	Protokoll zur Geräteparameterierung	busybox
69/UDP	TFTP (Trivial File Transfer Protocol)	[2)]	busybox
123/UDP	SNTP/NTP (Network Time Protocol)	Protokoll zur Zeitsynchronisierung in einem Netzwerk	ntpclient
1883/TCP 8883/TCP	MQTT (Message Queue Telemetry Transport)	Protokoll für Machine-to-Machine-Kommunikation	dataagent
4500/UDP	IPsec (Internet Protocol Security)	Protokoll zum Verbinden von zwei vertrauenswürdigen Geräten/Netzwerken über ein nicht vertrauenswürdiges Netzwerk, z.B. das Internet	Ipsec
514/UDP	Syslog	Protokoll für die Übertragung von Log-Meldungen[1,4)]	syslog-ng
1194/UDP	OpenVPN	Protokoll zum Verbinden von zwei Geräten/Netzwerke über ein nicht vertrauenswürdiges Netzwerk, z.B. das Internet	openvpn

[1)] Client ist im Auslieferungszustand aktiv
[2)] Client muss durch den Benutzer aktiviert werden oder wird aktiviert sobald eine (CODESYS/***e!****RUNTIME*-)Applikation auf dem Gerät gestartet wird
[3)] Client ist abhängig von der verwendeten Laufzeitumgebung
[4)] Client ist an den Local Host gebunden und von außen nicht erreichbar

4.2.1 Gerätespezifische Dienste

Tabelle 6: Anwendungen für PFC100/PFC200

Gerät	Port	Protokoll	Beschreibung	Programm
PFCx00	102/TCP	IEC 61850	Übertragungsprotokoll zwischen Leitsystemen und Fernbedienungsterminals (Fernwirktechnik)	CODESYS V2.3
PFCx00	2404/TCP 2404/UDP	IEC 60870-5-104		
PFCx00	20000/TCP 20000/UDP	DNP3 (Distributed Network Protocol)		

4.3 Benutzer und Passwörter

In den folgenden Kapiteln werden die voreingestellten Benutzer der verschiedenen Dienste des Controllers beschrieben.

4.3.1 WBM-Benutzer

Das WBM hat eine eigene Benutzerverwaltung. Die hier verwendeten Benutzer sind aus Sicherheitsgründen von den übrigen Benutzergruppen im System isoliert. Es können keine neuen Benutzer angelegt werden; die vorhandenen Benutzer sind fest in der Anwendung hinterlegt. Hinweise zum Ändern der Passwörter finden Sie im Kapitel „Hardening“ > … > „Passwörter im Web-Based-Management ändern“.

Tabelle 7: WBM-Benutzer

Benutzer	Rechte	Standardpasswort
admin	Alle (Administrator)	wago
user	Eingeschränkt	user
guest	Nur Anzeige	Kein Login möglich. Wird verwendet, wenn keine Anmeldung erfolgt ist.

4.3.2 Linux®-Benutzer

Die Gruppe der Linux®-Benutzer umfasst die Benutzer des Betriebssystems. Dienste, die von dem Gerät angeboten werden, werden jeweils unter einem eigenen Benutzer ausgeführt, welcher für einen Login gesperrt ist. Weitere Benutzer können hinzugefügt werden.

Hinweis

Passwörter für Dienstbenutzer
Dienstbenutzer, wie z. B. www, messagebus, rpcuser, nobody oder opc, sind für einen Login gesperrt. Bitte ändern Sie diese Passwörter nicht!

Benutzer	Besonderheit	Standardpasswort
root	Administrator	wago
admin	CODESYS Runtime-Benutzer	wago
user	Benutzer	user

Hinweise zum Ändern der Passwörter finden Sie im Kapitel „Hardening“ > … > „Linux®-Passwörter über die Linux®-Konsole ändern“.

4.3.3 SNMP-Benutzer

Der SNMP-Dienst verwaltet seine eigenen Benutzer. Hier sind im Auslieferungszustand keine Benutzer hinterlegt.

Information

Weitere Information finden Sie im Produkthandbuch!
Weitere Informationen zu SNMP-Diensten finden Sie im Handbuch des entsprechenden Controllers unter www.wago.com!

4.3.4 CODESYS und *e!RUNTIME*-Webvisualisierung

Für die CODESYS und ***e!****RUNTIME*-Webvisualisierung kann je Projekt ein Passwort für unterschiedliche Arbeitsgruppen eingestellt werden.

Information

Benutzer und Passwörter werden nicht automatisch angelegt!
Die Benutzer und Passwörter für die CODESYS und die ***e!****RUNTIME*-Webvisualisierung müssen vom Endanwender angelegt werden!

5 Bedrohungen für industrielle Steuerungssysteme

In diesem Kapitel werden potenzielle Bedrohungsszenarien beschrieben, die sich bei einer Vernetzung mit einem öffentlichen Netzwerk, z. B. dem Internet, ergeben können. Des Weiteren werden auf Basis der beschriebenen Szenarien Lösungsansätze (Defense-in-Depth) und konkrete Maßnahmen für die Controller empfohlen.

Die nachfolgende Aufzählung des BSI gibt einen Überblick über die, aus seiner Sicht, kritischsten Bedrohungen für industrielle Steuerungssysteme. Innerhalb dieses Kapitels liegt der Fokus auf den unmittelbaren Bedrohungen für die Controller.

- Social Engineering und Phishing
- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware*
- Infektion mit Schadsoftware über Internet und Intranet*
- Einbruch über Fernwartungszugänge
- Menschliches Fehlverhalten und Sabotage
- Internetverbundene Steuerungskomponenten*
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Extranet und Cloud-Komponenten
- (D)DoS-Angriffe*
- Kompromittierung von Smartphone im Produktionsumfeld

* Unmittelbare Bedrohungen für die Controller

Um ein Schutzniveau zu erreichen, das dem größten Teil der Bedrohungen entgegenwirkt, muss ein ganzheitlicher Ansatz gemäß des Defense-in-Depth-Prinzips verfolgt werden.

Hinweis

Beachten Sie für weiterführende Informationen die BSI-Empfehlung!
Beachten Sie für weiterführende Informationen die Empfehlung „IT in der Produktion“ vom Bundesamt für Sicherheit in der Informationstechnik > „Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen 2016“.

5.1 Defense-in-Depth-Prinzip

Der Betreiber einer Infrastruktur muss die vom BSI aufgelisteten Bedrohungen für industrielle Steuerungssysteme ganzheitlich betrachten. Eine sichere Infrastruktur ist nur dann gegeben, wenn sowohl organisatorische als auch technische Sicherheitsmaßnahmen gestaffelt implementiert werden und sich gegenseitig ergänzen. Somit soll verhindert werden, dass durch das Überwinden einer Sicherheitsmaßnahme ein komplettes System bzw. eine Anlage kompromittiert werden kann. Das Defense-in-Depth-Prinzip kann sowohl für die gesamte Architektur eines Betreibers als auch für einen einzelnen Controller angewendet werden.

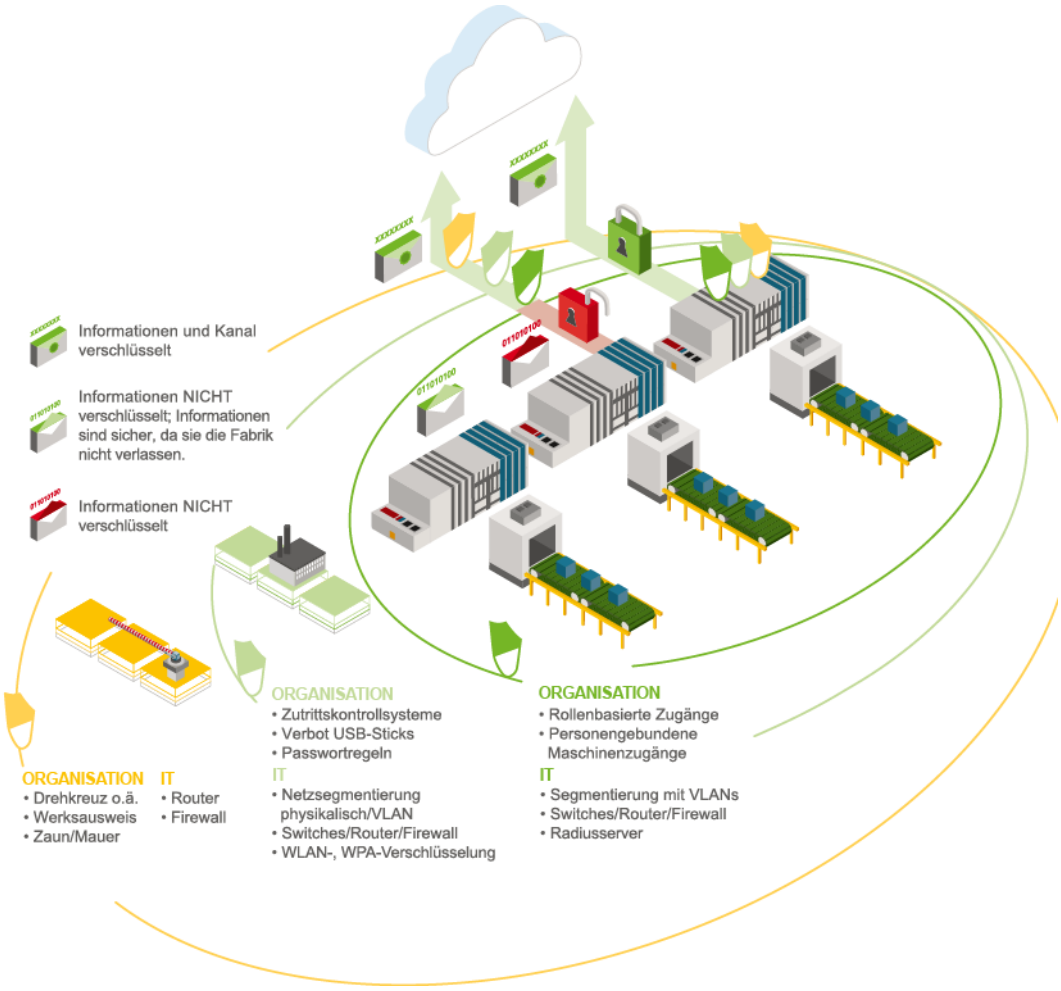

Abbildung 1: Zwiebelschalenmodell

Die Abbildung „Zwiebelschalenmodell“ zeigt exemplarisch eine Infrastruktur, die mit gestaffelten Sicherheitsmaßnahmen geschützt wird. In der äußersten Schicht (gelb) wird der physische Zugangsschutz in Form von Zutrittskontrollen dargestellt. Der physische Zugangsschutz sorgt dafür, dass Unbefugte nicht ohne Weiteres die kritischen Anlagen betreten können. In der mittleren Schicht (hellgrün) werden Richtlinien und Prozesse in Kombination mit technischen Maßnahmen für die Netzwerksicherheit dargestellt. Diese Maßnahmen stellen zusätzliche Hürden für einen potenziellen Angreifer dar. Wenn ein Angreifer dennoch bis zu den Steuerungen durchdringt, können durch Sicherheitsmaßnahmen auf Steuerungsebene die Risiken einer

Kompromittierung weiter minimiert werden (dunkelgrüne Schicht). Nachfolgend werden ausschließlich die Bedrohungen und potenziellen Sicherheitsmechanismen auf Steuerungsebene betrachtet.

Hinweis

Weitere Informationen zu Cyber-Security in Produktionsanlagen!
Detaillierte Maßnahmen zur Umsetzung der Cyber-Security in der Produktion sind im White Paper „IT Sicherheit in Produktionsanlagen“ beschrieben. Dieses White Paper können Sie unter https://www.wago.com/ downloads anfordern.

5.2 Spezifische Bedrohungen anhand einer Referenzarchitektur

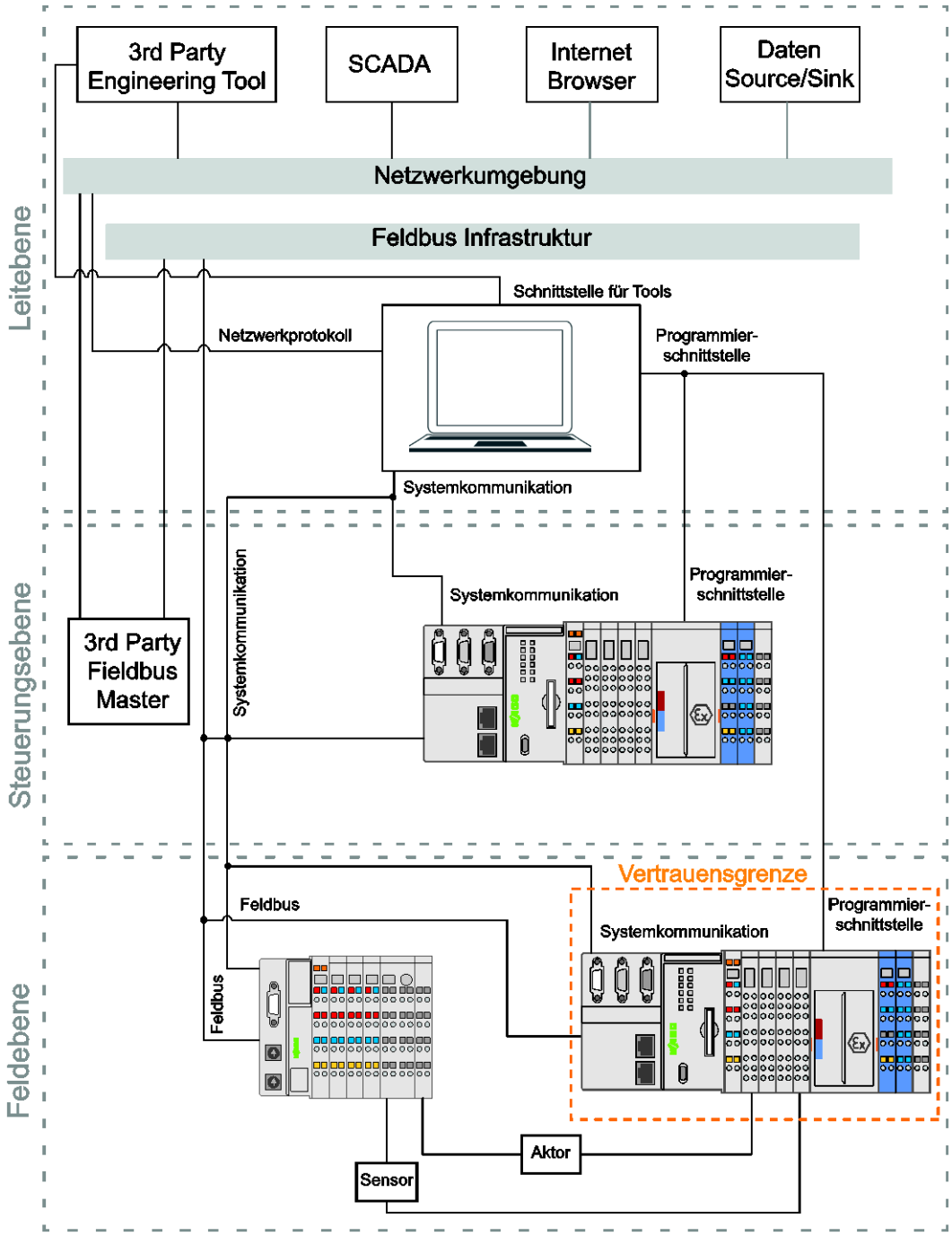

Abbildung 2: Referenzarchitektur

Die Referenzarchitektur stellt eine klassische Anwendungsumgebung dar, in der Steuerungssysteme von WAGO zum Einsatz kommen.

Die sogenannte Vertrauensgrenze stellt den Übergang von einem vertrauenswürdigen in einen nicht-vertrauenswürdigen Bereich dar und trennt damit die unterschiedlichen Sicherheitsniveaus. Die Vertrauensgrenze hat einen besonderen Stellenwert, da sich bei dem Übergang von oder zu einem anderen Bereich mögliche Angriffsvektoren ergeben können. Die unterschiedlichen

Schnittstellen, die die Steuerung zur Verfügung stellt, um mit anderen Systemen zu kommunizieren, stellen potenzielle Bedrohungen für den Controller dar.

Nachfolgend werden Szenarien möglicher Cyberangriffe beschrieben, die sowohl über den physikalischen als auch über den netzwerkbasierten Zugang zum Controller stattfinden können. Sofern ein Angreifer physischen Zugriff auf den Controller hat, kann eine Interaktion über die Schnittstellen durch zusätzlich angeschlossene Eingabegeräte erfolgen.

5.2.1 Physikalische Schnittstellen am WAGO-Controller

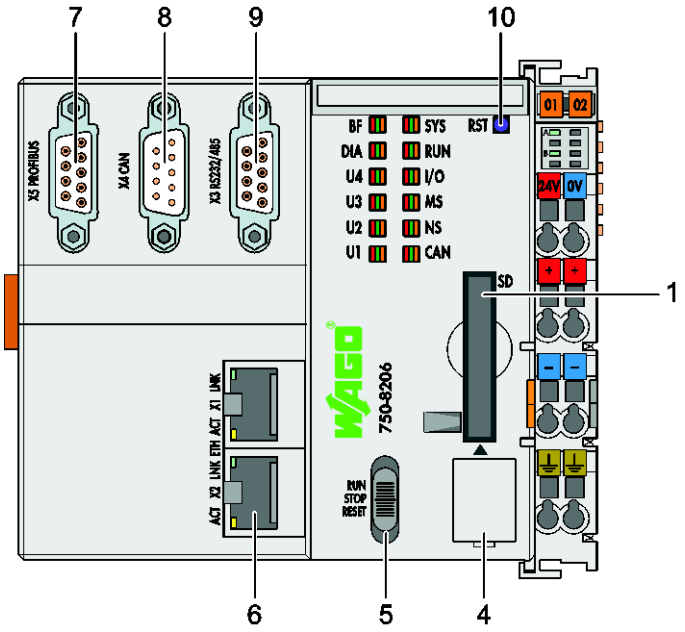

Abbildung 3: Physikalische Schnittstellen am WAGO-Controller

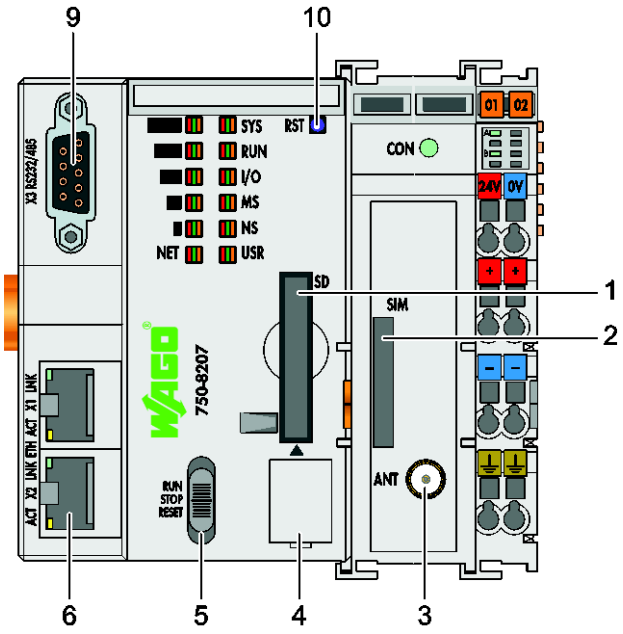

Abbildung 4: Physikalische Schnittstellen am WAGO-Controller mit GSM/3G-Modem-Schnittstelle

1 Speicherkartensteckplatz
2 SIM-Kartensteckplatz
3 Antenne
4 Service-Schnittstelle
5 Betriebsartenschalter
6 ETHERNET-Schnittstellen
7 Feldbusanschluss – PROFIBUS DP
8 Feldbusanschluss – CANopen
9 Serielle Schnittstelle (RS-232)
10 Reset-Taster

Hinweis

Produkthandbücher WAGO-Controller!
Detailinformationen zu den Controllern finden Sie in den entsprechenden Produkthandbüchern unter www.wago.com.

5.2.1.1 Reset-Taster

Mit dem Reset-Taster (**10**) können abhängig von der Position des Betriebsartenschalters unterschiedliche Funktionen ausgeführt werden. Um zu vermeiden, dass das Gerät auf Werkseinstellungen zurückgesetzt wird und damit der Passwortschutz obsolet wird, sollte der Zugang zum Reset-Taster auf den autorisierten Personenkreis beschränkt werden.

Hinweis

Zugang zu dem Schaltschrank beschränken!
Montieren Sie den Controller in einem Schaltschrank und sorgen Sie dafür, dass nur ein beschränkter Personenkreis Zugang zu dem Schaltschrank hat!

Netzwerkeinstellungen und folgende Passwörter werden zurückgesetzt:
- „admin“ (Linux),
- „admin“ (WBM)
- „user“ (WBM)

Folgende Passwörter werden nicht zurückgesetzt:
- „root“ (Linux)
- „user“ (Linux)

5.2.1.2 Betriebsartenschalter

Mit dem Betriebsartenschalter (**5**) kann zwischen den Betriebsarten STOP, RUN und RESET gewählt werden. Um zu vermeiden, dass hiermit ein Denial-of-Service-Angriff (DoS) auf eine laufende CODESYS oder ***e!****RUNTIME*-Applikation ausgeführt wird, sollte der Zugang zum Betriebsartenschalter auf den befugten Personenkreis beschränkt werden.

Hinweis

Zugang zum Schaltschrank beschränken!
Montieren Sie den Controller in einem Schaltschrank und sorgen Sie dafür, dass nur ein beschränkter Personenkreis Zugang zu dem Schaltschrank hat!

5.2.1.3 ETHERNET-Schnittstellen (X1 / X2)

Die beiden ETHERNET-Schnittstellen (**6**) des Controllers können wahlweise im Switch- oder im Separated-Modus betrieben werden. Im Auslieferungszustand ist der Switch-Modus eingeschaltet. Eine Übersicht über die Netzwerkdienste finden Sie im Kap. „Standardkonfiguration“ > „Netzwerkdienste“.

Wenn die ETHERNET-Schnittstellen nicht genutzt werden, können Sie diese in ihrer Funktion über die Konfiguration einschränken, siehe Kapitel „Hardening“ > … > „Zugriff über offene Netzwerkschnittstellen einschränken“.

Hinweis

Beachten Sie die Security-Hinweise zu ETHERNET-basierten Geräten!
Beachten Sie die Security-Hinweise von WAGO zu ETHERNET-basierten Geräten unter https://www.wago.com/de/automatisierungstechnik/security.

5.2.1.4 Service-Schnittstelle

Die Service-Schnittstelle (**4**) ist für die Nutzung des WAGO-Service-Protokolls vorgesehen. Hierüber kann das System z. B. mit der Software „WAGO Ethernet Settings“, „WAGO-I/O-*Check*“ oder ***e!****COCKPIT* konfiguriert werden.

Wenn die Service-Schnittstelle nicht genutzt wird, sollte sie aus Sicherheitsgründen deaktiviert werden, um die Angriffsmöglichkeiten zu reduzieren, siehe „Hardening“ > … „Service-Schnittstelle deaktivieren“.

5.2.1.5 Serielle Schnittstelle (RS-232)

Der Kommunikationsanschluss RS-232 (**9**) ist standardmäßig nicht belegt und für die Nutzung der Laufzeitumgebungen CODESYS oder ***e!****RUNTIME* vorgesehen.

Wenn die serielle Schnittstelle nicht genutzt wird, sollte diese nicht zugewiesen sein (unassigned), siehe Kapitel „Hardening“ > … > Linux®-Konsole auf der seriellen Schnittstelle deaktivieren“.

Hinweis

Kommunikationsanschluss RS-232 ist nicht immer verfügbar!
Beachten Sie, dass die Schnittstelle RS-232 nicht auf allen Geräten vorhanden ist!

5.2.1.6 Speicherkartensteckplatz

Die Controller verfügen über einen Speicherkartensteckplatz (**1**). Ein potenzieller Angreifer könnte mithilfe einer präparierten SD-Karte das System von der SD-Karte aus starten. Sobald eine SD-Karte installiert ist, bootet der Controller grundsätzlich von der SD-Karte. Die Daten auf dem internen Flash-Speicher können auf diesem Weg manipuliert werden oder es kann direkt in die Steuerungsapplikation eingegriffen werden. Eine Manipulation kann nur schwer oder gar nicht festgestellt werden.

Hinweis

Zugang zum Schaltschrank beschränken!
Montieren Sie den Controller in einem Schaltschrank und sorgen Sie dafür, dass nur ein beschränkter Personenkreis Zugang zu dem Schaltschrank hat!

5.2.1.7 GSM/3G-Modem-Schnittstelle

Bestimmte Controller verfügen über ein zusätzliches Modem-Modul mit einem SIM-Kartensteckplatz (**2**) und eine SMA-Buchse für die Antenne (**3**) zur Nutzung der Mobilfunkfunktionalität. Die SIM-Karte sollte durch einen PIN-Schutz vor unerlaubtem Zugriff geschützt werden.

Hinweis

Zugang zum Schaltschrank beschränken!
Montieren Sie den Controller in einem Schaltschrank und sorgen Sie dafür, dass nur ein beschränkter Personenkreis Zugang zu dem Schaltschrank hat!

Hinweis

Das Antennensignal kann im Schaltschrank zu schwach sein!
Stellen Sie sicher, dass das Antennensignal ausreichend ist, wenn Sie das Gerät im Schaltschrank verstauen. Ist das Antennensignal zu schwach, besteht kein Zugang zum mobilen Netz!

5.2.2 Zugänge über das Netzwerk

In diesem Kapitel werden potenzielle netzwerkbasierte Cyberangriffe beschrieben, die z. B. über lokale Netzwerke erfolgen können. Durch die zunehmende Komplexität und Vernetzung der Kommunikationsteilnehmer innerhalb mehrschichtiger Netzwerke (siehe Abbildung „Referenzarchitektur“), können Cyberkriminelle in vielerlei Hinsicht die Systemsicherheit gefährden. Da industrielle Steuerungen zunehmend mit Firmennetzwerken vernetzt werden, stellen sie einen zusätzlichen Angriffsvektor dar.

5.2.2.1 Softwarekomponenten

Schwachstellen in der verwendeten Software stellen eine potenzielle Bedrohung dar, da hierdurch z.B. das Einschleusen von schadhaftem Code oder die Ausführung von DoS-Angriffen begünstigt wird.

Um diesen Bedrohungen entgegenzuwirken, wird empfohlen, dass Sie die Software des Controllers auf dem aktuellsten Stand halten (z.B. durch ein Firmware-Update). Aktualisieren Sie Ihr System regelmäßig mittels Patches, die von WAGO Kontakttechnik GmbH & Co. KG bereitgestellt werden. Führen Sie zusätzlich Härtungsmaßnahmen durch, die den Controller sicherer machen.

Um eine aktuelle Auflistung der Linux®-Pakete Ihres Controllers zu bekommen, können Sie den folgenden Befehl auf der Linux®-Konsole ausführen:

„ipkg list“.

5.2.2.2 „Man-in-the-Middle-Attacken“

Man-in-the-Middle-Attacken sind Angriffe auf den Kommunikationskanal zwischen zwei Kommunikationspartnern. Der Angreifer gibt sich dabei als eine vertrauenswürdige Quelle aus, sodass die beiden Kommunikationspartner nicht feststellen können, dass sie mit dem Angreifer kommunizieren. Der Angreifer ist so in der Lage, alle übertragenen Informationen zu lesen und zu manipulieren.

Für eine optimale Sicherheit der Controller wird empfohlen, die TLS-Konfiguration von „Standard“ auf „Strong“ zu ändern, siehe Kapitel „Hardening“ > … > „TLS-Verschlüsselung“. Weiterhin wird empfohlen, das generische TLS-Zertifikat auszutauschen, siehe Kapitel „Hardening“ > … > Zertifikate erstellen und austauschen.

5.2.2.3 Netzwerk-Schnittstellen und Protokolle

Portscanner können von Cyberkriminellen dazu genutzt werden, fremde Rechner auf Zugangsmöglichkeiten über offene Schnittstellen zu überprüfen. Jede offene Schnittstelle stellt eine potenzielle Bedrohung dar, da über nicht benötigte Netzwerkdienste ein Zugriff auf das System erfolgen kann.

Um bestimmte Netzwerkschnittstellen/-protokolle zu blockieren, die in einer spezifischen Anwendungsumgebung nicht benötigt werden, kann eine Firewall

verwendet werden. Nähere Informationen hierzu finden Sie im Kapitel „Hardening“ < … > „Firewall-Konfiguration“.

Eine Übersicht über alle Netzwerkdienste, die standardmäßig von WAGO eingesetzt werden, finden Sie im Kapitel „Standardkonfiguration“ … > „Netzwerkdienste“.

Hinweis

Beachten Sie die Security-Hinweise für netzwerkbasierte WAGO-Steuerungen!
Security-Hinweise für netzwerkbasierte WAGO-Steuerungen finden Sie unter https://www.wago.com/de/automatisierungstechnik/security

5.2.2.4 Firewalls

Mithilfe einer Firewall können Sie eine Schutzmaßnahme gegen unsichere und/oder schädigende Verbindungen einrichten. Eine Firewall-Regel sollte stets restriktiv konfiguriert werden, um den Zugriff auf eine bestimmte Netzwerk-Schnittstelle zu beschränken. Der Zugriff auf die Netzwerk-Schnittstelle sollte nur auf einzelne Computer oder Subnetze beschränkt werden, die auf den Dienst zugreifen müssen. Weitere Informationen zu den Firewall-Regeln finden Sie im Kapitel „Hardening“ > Firewall konfigurieren“.

5.2.3 Zugänge über Benutzer und Passwörter

Hinweis

Passwörter ändern
Die im Auslieferungszustand eingestellten Standardpasswörter für alle Benutzer sind in dieser Betriebsanleitung dokumentiert und bieten keinen hinreichenden Schutz! Ändern Sie die Passwörter entsprechend Ihren Erfordernissen bei der Erstinbetriebnahme!

Ein Passwortschutz mit Standardpasswörtern oder mit Passwörtern geringer Komplexität bietet keinen ausreichenden Schutz. So kann ein potenzieller Angreifer den Passwortschutz leicht umgehen und Zugriff auf das betroffene Benutzerkonto mit den entsprechenden Berechtigungen erhalten.

Die nachfolgend aufgelisteten Dienste haben jeweils ihre eigene Benutzerverwaltung mit Benutzerkonten:

- Web-Based-Management (WBM)
- Linux®
- SNMP
- CODESYS-Webvisualisierung
- ***e!****RUNTIME*-Webvisualisierung

Empfehlungen für sichere Passwörter:

- Ändern Sie Ihr Passwort regelmäßig.
- Verwenden Sie mindestens acht Zeichen.
- Speichern Sie Ihr Passwort nicht im Klartext auf Ihrer Festplatte.

- Verwenden Sie möglichst viele unterschiedliche Zeichen, Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern.
- Ihr Passwort sollte keinen persönlichen Bezug enthalten - zum Beispiel keine Namen oder Geburtstage.

Information

Weitere Informationen finden Sie beim „National Institute of Standards and Technology“ (NIST)!
Das NIST gibt in der „NIST Special Publication 800-63B“ im Abschnitt „Authenticator and Verifier Requirements“ Hinweise für sichere Passwörter! (https://pages.nist.gov/800-63-3/sp800-63b.html)

6 Hardening

Hardening (Härtung) bedeutet, die Sicherheit eines Systems durch eine Reihe von Maßnahmen zu erhöhen und es damit besser vor Bedrohungen zu schützen, siehe Kapitel „Bedrohungen für industrielle Steuerungssysteme“.

Die WAGO-Controller sind Linux®-basierte PCs. Das Linux®-Betriebssystem bietet zahlreiche Netzwerk-Services an, die nicht für jedes System und jeden Benutzer zugänglich sein sollten. Es sollten nur die notwendigen Prozesse mit minimalen Rechten aktiv sein. Im Folgenden werden einige Maßnahmen beschrieben, die dazu beitragen, Ihr System auf ein Minimum sicherheitskritischer Aspekte zu reduzieren.

Hinweis

Dieses Dokument erhebt nicht den Anspruch auf Vollständigkeit!
Sorgen Sie dafür, dass eine sicherheitstechnische Überprüfung Ihrer Anwendung in Bezug auf Ihre Anforderungen erfolgt!

6.1 Physikalischen Zugang einschränken

6.1.1 Service-Schnittstelle deaktivieren

Die Service-Schnittstelle wird unter anderem für die Kommunikation mit der Software WAGO-I/O-*CHECK* und WAGO-ETHERNET-Settings genutzt. Wenn die Service-Schnittstelle nicht dauerhaft genutzt wird, sollte sie deaktiviert werden, siehe auch Kapitel „Bedrohungen für industrielle Steuerungssysteme“ > „Spezifische Bedrohungen anhand einer Referenzarchitektur“.

Hinweis

Service-Schnittstelle kann nur als Administrator deaktiviert werden!
Für die Deaktivierung der Service-Schnittstelle benötigen Sie Admin-Berechtigungen!

1. Wählen Sie im WBM den Menüpunkt **Administration** > **Service Interface** um die Service-Schnittstelle zu deaktivieren.

Abbildung 5: Service-Schnittstelle deaktivieren

2. Aktivieren Sie im Bereich „Assign Owner of Service Interface“ das Kontrollfeld **Unassigned.**
Hiermit wählen Sie aus, dass die serielle Schnittstelle keiner Applikation zugewiesen wird und frei ist, damit beispielsweise ein CODESYS-Programm über Funktionsbausteine darauf zugreifen kann.

3. Betätigen Sie die Schaltfläche **[Change Owner].**

4. Starten Sie den Controller erneut, um die Änderung zu übernehmen.

6.1.2 Linux®-Konsole auf der seriellen Schnittstelle deaktivieren

Der Controller verfügt über eine serielle RS-232-Schnittstelle, die für verschiedene Funktionen konfiguriert werden kann. Im Auslieferungszustand ist sie nicht zugewiesen und kann von Anwendungen, wie z. B. CODESYS, genutzt werden. Alternativ kann die serielle Schnittstelle auch Linux® zugewiesen werden, sodass eine Linux®-Kommandozeile bereitgestellt wird. Mit dieser Einstellung kann die serielle Schnittstelle für die Kommunikation mit der Linux®-Konsole verwendet werden.

Wird die serielle Schnittstelle für andere Anwendungen konfiguriert, ist sie für den Zugriff auf eine Konsole blockiert. Wenn die serielle Schnittstelle nicht regelmäßig für den Zugriff auf die Konsole genutzt werden soll, ist es ratsam, die Bindung des seriellen Anschlusses an die Konsole zu deaktivieren.

Hinweis

Linux®-Konsole kann nur als Administrator deaktiviert werden!
Für die Deaktivierung der Linux®-Konsole benötigen Sie Admin-Berechtigungen!!

1. Wählen Sie im WBM den Menüpunkt **Administration** > **Serial Interface** um den Zugriff auf die Linux®-Konsole zu deaktivieren.

2. Wählen Sie das Kontrollfeld **Unassigned**.
   Hiermit stellen Sie sicher, dass die serielle Schnittstelle keiner Kommandozeile zugewiesen wird.

Abbildung 6: Linux®-Konsole deaktivieren

3. Betätigen Sie die Schaltfläche **[Change Owner]** um die Änderung zu übernehmen.

6.2 Netzwerkzugänge sichern

6.2.1 Verschlüsselt kommunizieren

6.2.1.1 Webserverauthentifizierung

Die WBM-Seiten des Controllers können wahlweise mit dem Webprotokoll HTTP oder HTTPS geöffnet werden. HTTPS sollte bevorzugt verwendet werden, da es das TLS-Protokoll einsetzt. Das TLS-Protokoll sichert die Kommunikation durch Verschlüsselung und Authentifizierung.

Die Standardeinstellung des Controllers ermöglicht starke Verschlüsselung, nutzt aber nur einfache Authentifizierungsverfahren. Da eine Authentifizierung für alle sicheren Kommunikationskanäle eine zentrale Rolle spielt, ist dringend angeraten, eine sicherere Authentifizierung durchzuführen. Basis der Authentifizierung bildet das auf dem Controller gespeicherte Sicherheitszertifikat. Der Standardablageort des Sicherheitszertifikats ist: /etc/lighttpd/https-cert.pem.

Im Auslieferzustand verwendet der Controller ein generisches Sicherheitszertifikat im x509-Format. Um eine sicherere Authentifizierung zu ermöglichen, müssen Sie dieses generische Sicherheitszertifikat durch ein spezifisches für das individuelle Gerät ersetzen.

6.2.1.2 TLS-Verschlüsselung

Beim Aufbau einer HTTPS-Verbindung handeln der Webbrowser und der Webserver aus, welche TLS-Version und welches kryptografische Verfahren zu benutzen ist.

Über die Gruppe „TLS Configuration“ der WBM-Seite „Security“ können die bei HTTPS erlaubten kryptografischen Verfahren und die benutzbaren TLS-Versionen umgeschaltet werden.

Es sind die Einstellungen „Strong“ und „Standard“ möglich.
Mit der Einstellung „Strong“ erlaubt der Webserver nur die TLS-Version 1.2 und starke Algorithmen. Ältere Software und ältere Betriebssysteme unterstützen eventuell TLS 1.2 und die Verschlüsselungsalgorithmen nicht.
Mit der Einstellung „Standard“ sind TLS 1.0, TLS 1.1, TLS 1.2 und auch kryptografische Verfahren erlaubt, die heute nicht mehr als sicher angesehen werden. Eine Verwendung wird nur für die Abwärtskompatibilität mit älteren Systemen empfohlen.

Information

Technische Richtlinie TR-02102 des BSI
Die Regeln für die Einstellung „Strong“ richten sich nach der technischen Richtlinie TR-02102 des Bundesamtes für Sicherheit in der Informationstechnik.
Die Richtlinie finden Sie im Internet unter: https://www.bsi.bund.de > „Publikationen“ > „Technische Richtlinien“.

Information

Leitfaden des BSI zur Migration auf TLS 1.2
Der Leitfaden des Bundesamtes für Sicherheit in der Informationstechnik zur Migration auf TLS 1.2 enthält „Kompatibilitätsmatrizen“, die darstellen, welche Software kompatibel zu TLS 1.2 ist.
Den Leitfaden finden Sie im Internet unter: https://www.bsi.bund.de > „Themen“ > „Standards und Kriterien“ > „Mindeststandards“.

Für eine optimale Sicherheit wird empfohlen die TLS-Konfiguration im Web-Based-Management von „Standard“ auf „Strong“ zu ändern.

1. Navigieren Sie im WBM zum Menü **Security** > **TLS Configuration**.

2. Aktivieren Sie das Kontrollfeld **Strong**.

Abbildung 7: TLS Configuration

3. Klicken Sie auf die Schaltfläche **[Submit]** um die Änderung zu übernehmen.

6.2.1.3 Diffie-Hellman-Parameter erzeugen

Das Diffie-Hellman-Verfahren ist eine Methode zur Vereinbarung eines gemeinsamen digitalen Schlüssels. Dabei wird nicht der geheime Sitzungsschlüssel, sondern nur das Ergebnis einer Rechenoperation übertragen. So können zwei Kommunikationsteilnehmer sicher über ein öffentliches Netz kommunizieren. Sie verwenden eine Verschlüsselungsmethode ihrer Wahl, die den mit dem Diffie-Hellman-Verfahren vereinbarten gemeinsamen Schlüssel nutzt.

Sie können die Diffie-Hellman-Parameter über die Schlüsselverwaltungssoftware XCA erzeugen.

1. Öffnen Sie die Software XCA und wählen Sie unter dem Menü **Extra** das Untermenü **DH Parameter erstellen.**

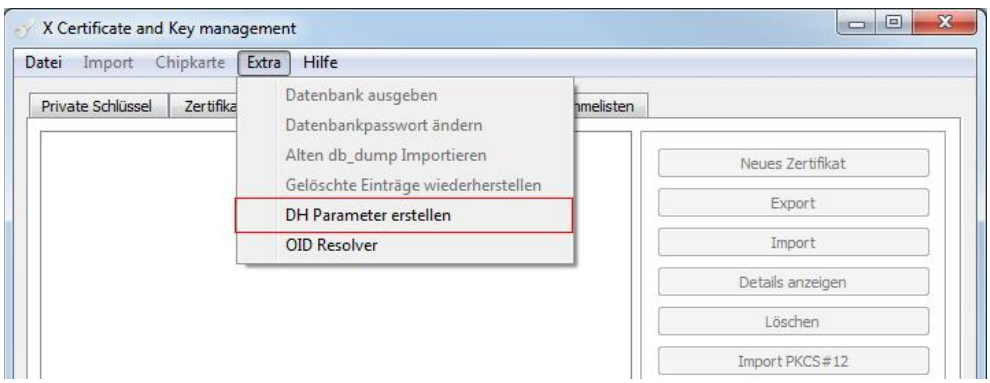

Abbildung 8: Diffie-Hellmann-Parameter erstellen

2. Wählen Sie eine Schlüssellänge von mindestens 2000 Bit.

Hinweis

Beachten Sie die Vorgaben zur Schlüssellänge!
Bei einem geplanten Einsatz nach dem Jahr 2022 sollte die Schlüssellänge mindestens 3000 Bit haben, siehe BSI TR 02102-1, Seite 56/57, „7.2.1. Diffie-Hellman“!

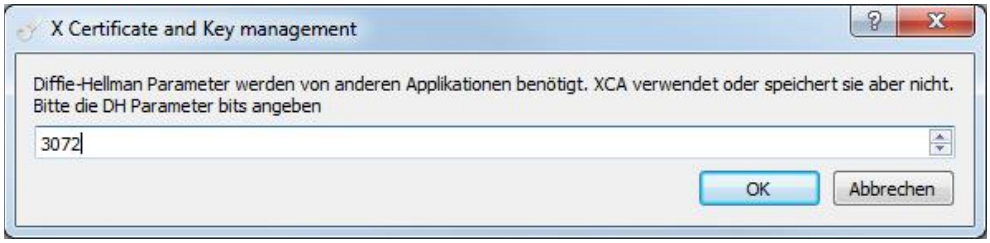

Abbildung 9: Schlüssellänge, DH Parameter

Hinweis

Erstellung der Parameter kann eine längere Zeit in Anspruch nehmen!
Je nachdem welche Schlüsselgröße gewählt wird, kann die Erstellung der DH-Parameter sehr lange dauern!

Im Hintergrund werden die Parameter „p“ und „g“ erstellt. Nach Fertigstellung öffnet sich ein Dialogfenster zum Speichern der Parameter. Die Parameter „p“ und „g“ müssen nicht geheim bleiben und können über eine unsichere Verbindung übertragen werden. Beim Schlüsselaustausch nach dem Diffie-Hellman-Verfahren wählen die zwei Kommunikationspartner zusätzlich zu den Parametern „p“ und „g“ jeweils eine geheime Zahl. Aus den öffentlichen und der geheimen Zahl wird jeweils eine neue Zahl berechnet. Die neuen Zahlen werden wieder ausgetauscht, um damit den gemeinsamen, geheimen Schlüssel „k“ zu erzeugen, der für Dritte nicht zugänglich ist.

Der Diffie-Hellman-Schlüsselaustausch wird für SSL/TLS-Verbindungen genutzt, siehe Kapitel „OpenVPN“ sowie für den Webserver, siehe nachfolgendes Kapitel.

6.2.1.3.1 Diffie-Hellman-Parameter für den Webserver austauschen

Sie können die erzeugten Diffie-Hellman-Parameter (siehe Kapitel „Diffie-Hellman-Parameter erzeugen“) für den Webserver gegen Ihre eigenen austauschen:

1. Laden Sie die erzeugten Parameter per SCP/FTPS/SFTP auf den Controller in den folgenden Ordner:
   /etc/lighttpd/

2. Die Parameterdatei müssen Sie in den Konfigurationsdateien „tls-strong.conf“ und „tls-standard.conf“ in dem Schlüssel „ssl.dh-file“ angeben:
   ssl.dh-file = „/etc/lighttpd/<Name Ihrer DH Parameter Datei>“

3. Starten Sie abschließend den Webserver neu:
   /etc/init.d/lighttpd stop
   /etc/init.d/lighttpd start

6.2.1.4 SSH-Zugang „härten“

SSH unterstützt neben der Authentifizierung mittels Benutzernamen und Kennwort auch Authentifizierungen, die auf einem Schlüsselpaar (privat/öffentlich) basieren. Erstellen Sie die Schlüssel z. B. über das kostenlose Windows-Programm „Putty Key Generator“ (Putty v0.68 oder aktueller, Schritt 1-10). Darüber hinaus sollte der Login für den Benutzer „root“ gesperrt werden (siehe Kapitel „SSH-Zugang „härten“ > „Anmeldung per root login verweigern“) und der Standardport verändert werden (siehe Kapitel „Standard-Netzwerkports ändern“).

1. Laden Sie PuTTYgen von der Website https://the.earth.li/~sgtatham/putty/latest/w64/puttygen.exe.

2. Starten Sie das PuTTY-Hilfsprogramm PuTTYgen:

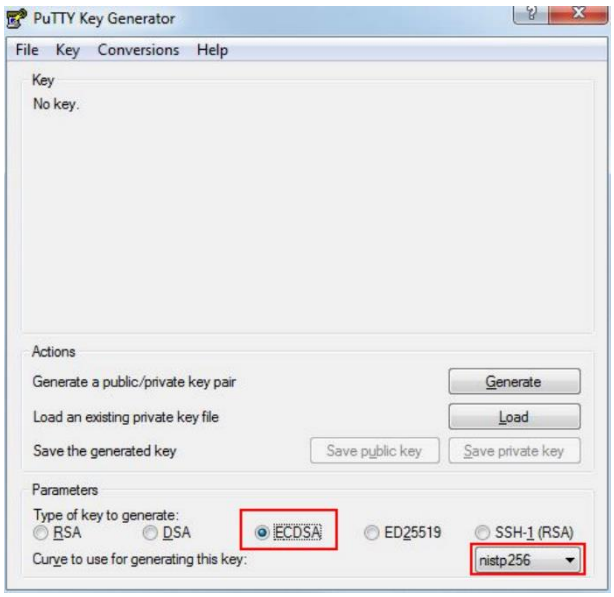

Abbildung 10: PuTTYgen starten

3. Wählen Sie die Art des zu erzeugenden Schlüssels (ECDSA)und die elliptische Kurve (nistp 256).

Hinweis

Beachten Sie die Empfehlungen bei kryptografischen Verfahren!
Entsprechend den technischen Richtlinien des BSI TR-02102-4 (Version 2017-01) wird bei ECDSA eine Schlüssellänge von mindestens 250 Bit vorgegeben!

4. Betätigen Sie danach die Schaltfläche [**Generate**], um mit der Schlüsselerzeugung zu beginnen.

5. Bewegen Sie die Maus während der Schlüsselerzeugung so lange willkürlich im Fenster, bis die Fortschrittsanzeige das Ende erreicht hat. PuTTYgen generiert die für die Schlüsselerzeugung notwendigen Zufallszahlen unter anderem aus den Bewegungen des Mauszeigers.

Nach Abschluss der Erzeugung werden die Schlüsseldaten im Fenster angezeigt:

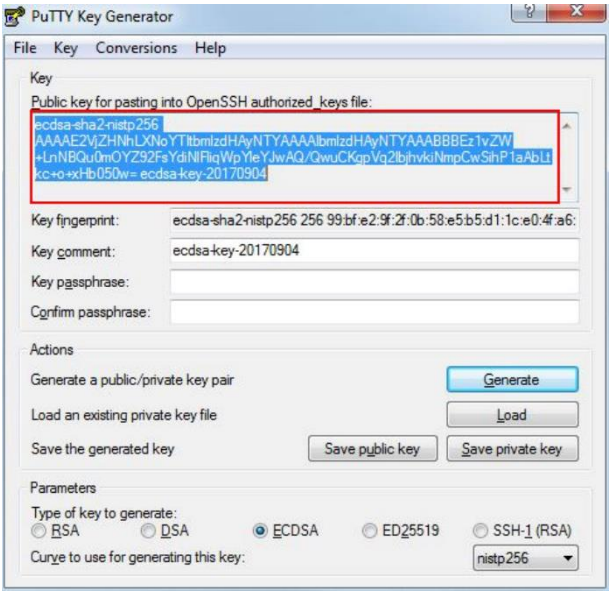

Abbildung 11: PuTTYgen Schlüsselerzeugung

6. Klicken Sie auf die Schaltflächen [**Save public key**] und [**Save private key**] um Ihr Schlüsselpaar zu speichern.

7. Vergeben Sie im Eingabefeld **Key passphrase** noch ein Passwort für den privaten Schlüssel.

8. Bestätigen Sie das Passwort im Eingabefeld **Confirm passphrase**.

9. Speichern Sie den privaten Schlüssel an einem sicheren Ort, damit sich kein Unbefugter mit dem Schlüssel am Gerät authentifizieren kann.

Der öffentliche Schlüssel muss auf der Steuerung im Home-Verzeichnis des Benutzers hinterlegt werden, der sich mit dem Schlüssel authentifizieren soll (z. B. /home/user). Dort muss zunächst ein Unterordner „.ssh“ sowie die Datei „authorized_keys“ erstellt werden, siehe nachfolgende Beschreibung.

Hinweis

Beachten Sie die Dateiberechtigungen!
Das Verzeichnis „.ssh“ muss die Linux®-Berechtigung **rwx------ (700)** und die Datei „authorized_keys“ muss die Linux®-Berechtigung **rw------- (600)** haben; andernfalls wird der Schlüssel nicht akzeptiert!

10. Legen Sie das Verzeichnis „.ssh“ an:
```
user@PFC200-40ED7D:~ pwd
/home/user
user@PFC200-40ED7D:~mkdir .ssh && chmod 700 .ssh
```

11. Kopieren Sie den öffentlichen Schlüssel aus dem PuTTY-Key-Generator, siehe Abbildung „PuTTYgen Schlüsselerzeugung“.

12. Fügen Sie den Schlüssel in die Datei „authorized_keys“ ein:
```
user@PFC200-40ED7D:~ pwd
```

```
/home/user
user@PFC200-40ED7D:~ cat << 'EOF' >.ssh/authorized_keys
  > Public key (ecdsa-sha2-nistp256AAAAE2V … ecdsa-key-
20170904)
  >EOF
user@PFC200-40ED7D:~ chmod 600 .ssh/authorized_keys
user@PFC200-40ED7D:~ ls -l .ssh/authorized_keys
-rw-------    1 user     user             261 Jan 24 08:39
.ssh/authorized_keys
```

Hinweis

Achten Sie beim Einfügen der Schlüssel auf die Syntax!
Jeder Schlüssel muss in der Datei „authorized_keys“ in eine Zeile geschrieben werden!

13. Testen Sie den Zugang über Ihren privaten Schlüssel bevor Sie die Anmeldung per Passworteingabe deaktivieren.

PuTTY-Konfiguration

Damit Sie den Schlüssel zum Authentifizieren nutzen können, müssen Sie den Schlüssel Ihrem SSH Client bekanntgeben. Nachfolgend ist ein Beispiel für PuTTY beschrieben (andere Clients sind analog zu konfigurieren):

1. Starten Sie das PuTTY-Hilfsprogramm. Es öffnet sich das Dialogfenster „PuTTY Configuration“.

2. Navigieren Sie in der Verzeichnisstruktur zum Menü **Connection** > **SSH** > **AUTH.** Es öffnet sich das Dialogfenster für die SSH-Authentifizierungsoptionen.

3. Wählen Sie im Bereich „Authentication parameters“ Ihren privaten Schlüssel aus.

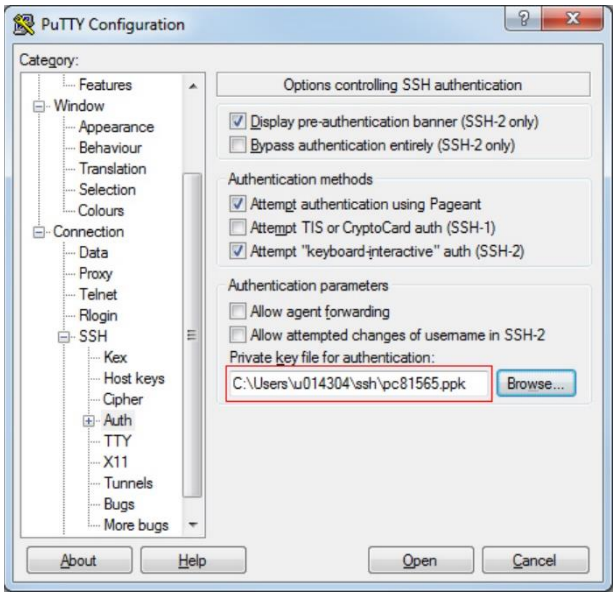

Abbildung 12: PuTTY-Konfiguration

4. Wechseln Sie in der Verzeichnisstruktur zum Menü **Session**.

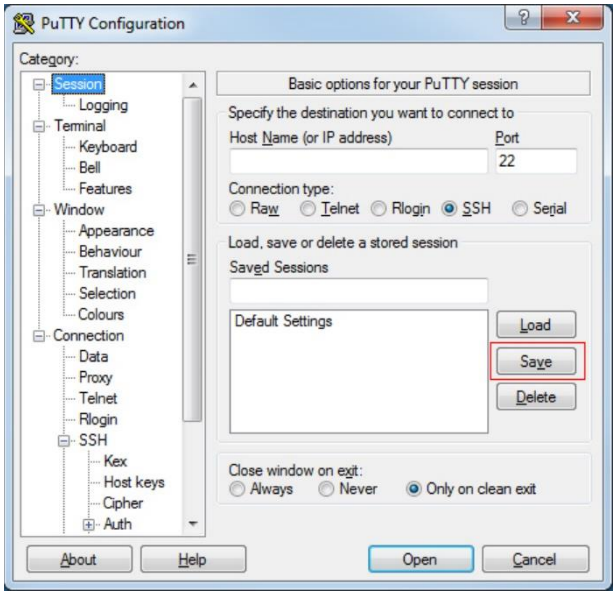

Abbildung 13: PuTTY Konfiguration speichern

5. Speichern Sie die Konfiguration mit der Schaltfläche [**Save**].

6.2.1.4.1 Anmeldung über Passworteingabe deaktivieren

Zwei Möglichkeiten stehen Ihnen zur Verfügung:

Konfigurationsdatei:

1. Setzen Sie „`PASSWORD_LOGIN`“ auf „false“ (default = true). Die Konfigurationsdatei finden Sie unter: /etc/dropbear/dropbear.conf.

2. Starten Sie den Dienst neu.

WBM:

1. Navigieren Sie im WBM zum Menü **Ports and Services** > **SSH**.

2. Entfernen Sie den Haken für das Kontrollfeld **Allow password login**.

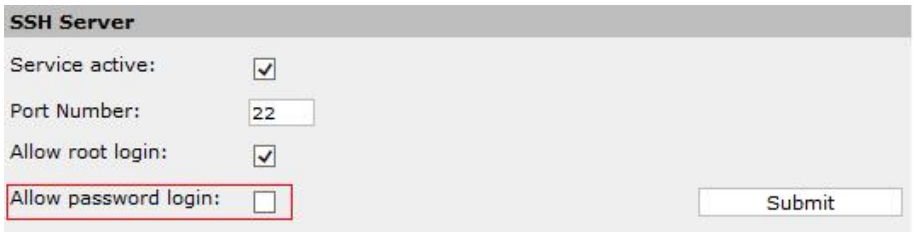

Abbildung 14: Anmeldung über Passworteingabe deaktivieren

3. Speichern Sie die Einstellung mit der Schaltfläche [**Submit**].

Bei Änderungen über das WBM wird der Dienst automatisch neu gestartet.

6.2.1.4.2 Anmeldung per Root-Login verweigern

Hinweis

Sorgen Sie vorher dafür, dass Sie sich nicht vom System aussperren!
Richten Sie vorher ein Benutzerkonto ein, das mit den gleichen Zugriffsrechten ausgestattet ist, wie das Root-, bzw. das Superuser-Konto! Mit den Befehlen `su` und `sudo` können Sie einzelnen Benutzern Administratorrechte geben.

Zwei Möglichkeiten stehen Ihnen zur Verfügung:

Konfigurationsdatei:

1. Setzen Sie „`ROOT_LOGIN`“ auf „false“ (default = true). Die Konfigurationsdatei finden Sie unter: /etc/dropbear/dropbear.conf.

2. Starten Sie den Dienst neu.

WBM:

1. Navigieren Sie im WBM zum Menü **Ports and Services** > **SSH**.

2. Entfernen Sie den Haken für das Kontrollfeld **Allow root login**.

Abbildung 15: Anmeldung per root login verweigern

3. Speichern Sie die Einstellung mit der Schaltfläche [**Submit**].

Bei Änderungen über das WBM wird der Dienst automatisch neu gestartet.

6.2.1.4.3 Server-Schlüssel austauschen

Im Auslieferzustand verwendet der Controller einen generischen Schlüssel, der durch einen individuellen Schlüssel ersetzt werden muss.

Die Geräte 750-8202 - 750-8207 sind nicht mit einem Hardwarezufallszahlengenerator ausgerüstet und müssen daher mit externen Zufallszahlen initialisiert werden. Für die Einrichtung aller anderen Geräte kann direkt mit Punkt 3 begonnen werden.

Die Schlüssel werden auf dem Gerät neu generiert.

1. Stellen Sie eine Verbindung zur Linux®-Konsole via SSH her.

2. Kopieren Sie Zufallszahlen von Ihrem Host auf den Controller:

Linux via SSH:

```
openssl rand 1024 | ssh root@192.168.1.72 'cat >
/dev/urandom'
```

Windows via PuTTYgen:

- Erstellen Sie die Zufallszahlen, wie im Kap. „SSH-Zugang „härten““ beschrieben (Punkt 1.-5.).
- Kopieren Sie die im Fenster angezeigten Schlüsseldaten in die Zwischenablage.
- Stellen Sie eine Verbindung zur Linux®-Konsole via SSH her.
- Starten Sie auf dem Controller den Befehl „cat > /dev/urandom“.
- Fügen Sie die Schlüsseldaten aus der Zwischenablage ein.
- Drücken Sie nacheinander die Tasten ENTER und STRG-D, um die Eingabe zu beenden.

3. Melden Sie sich am Controller an:
   ```
   ssh root@192.168.1.17
   ```

4. Generieren Sie auf dem Controller die neuen Schlüssel:
   ```
   cd /etc/dropbear
   rm -f dropbear_ecdsa_host_key && dropbearkey -t ecdsa -s 521
   -f dropbear_ecdsa_host_key
   rm -f dropbear_dss_host_key && dropbearkey -t dss -s 1024 -f
   dropbear_dss_host_key
   rm -f dropbear_rsa_host_key && dropbearkey -t rsa -s 2048 -f
   dropbear_rsa_host_key
   ```

5. Sichern Sie die Schlüssel und starten Sie den Controller neu:
   ```
   sync && reboot
   ```

Linux via SSH:

Nach dem Neustart weist eine Warnung in der Kommandozeile darauf hin, dass der veränderte Server-Schlüssel auf eine Man-in-the-Middle-Attacke hindeuten könnte, z. B. wie folgt:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:CSD8j+LxPxE4mtLIPzgyTbKozoCPYZNBvPEQVfrpVws.
```

6. Löschen Sie den in der Fehlermeldung genannten Schlüssel aus dem Unterordner „.ssh/known_hosts“ des Home-Verzeichnisses auf Ihrem Host.

Windows via PuTTY:

Nach dem Neustart erscheint die folgende Warnmeldung:

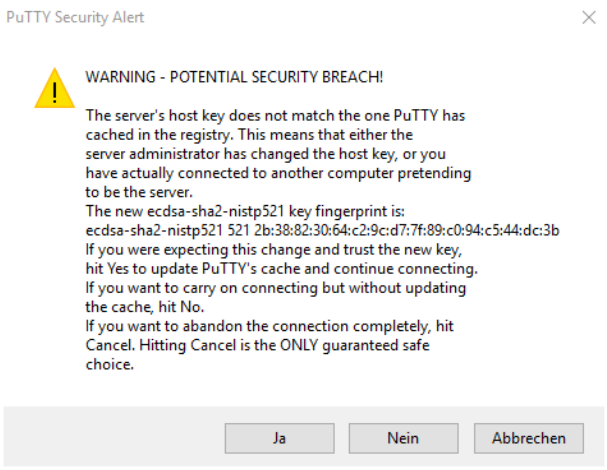

Abbildung 16: Neustart Putty

6. Klicken Sie [**Ja**], um den Cache zu aktualisieren und die Verbindung fortzusetzen.

Weitere Informationen hierzu finden Sie im Kapitel „Hardening > … > „Zertifikate erstellen und austauschen“.

6.2.1.5 Zertifikate erstellen und austauschen

Ein Zertifikat ermöglicht eine gesicherte Verbindung für die Netzwerkkommunikation und wird für die Authentifizierung des Remote Host genutzt. Das grüne Schlosssymbol im Browser weist darauf hin, dass diese Website über ein gültiges und vertrauenswürdiges Zertifikat verfügt und die Verbindung gesichert ist.

Es wird empfohlen, die standardmäßig mitgelieferten WAGO-Zertifikate durch eigene Zertifikate auszutauschen, da der private Schlüssel für alle Geräte, Kunden und jede Firmware identisch ist und damit nicht als geheim gelten kann. Eigens erstellte Zertifikate müssen von einer Zertifizierungsstelle (sog. Root-CA) unterzeichnet werden. Das Root-Zertifikat bildet den gemeinsamen Vertrauensanker aller ihm untergeordneten Zertifikate und muss im lokalen Trust Store des Browsers oder Clients gespeichert werden.

In den folgenden Kapiteln wird beispielhaft die Erstellung von Schlüsseln und Zertifikaten mit der Schlüsselverwaltungssoftware XCA beschrieben. Mit der kostenlosen Software ist es möglich, Zertifikate selbst zu erstellen. Die Zertifikate/Schlüssel werden in einer lokalen Datenbankdatei gespeichert. Die Datenbank, welche unter anderem private Schlüssel enthält, wird dabei mit einem Passwort geschützt.

6.2.1.5.1 Vorlage für die Zertifikate erstellen

1. Öffnen Sie die Software XCA und wählen Sie unter dem Menü **Datei** das Untermenü **Neue Datenbank**.

2. Wählen Sie einen Speicherort und einen passenden Namen für die Datenbank.

3. Geben Sie ein Passwort für die Sicherung der Datenbank ein. Danach wird die neu erstellte Datenbank automatisch geöffnet:

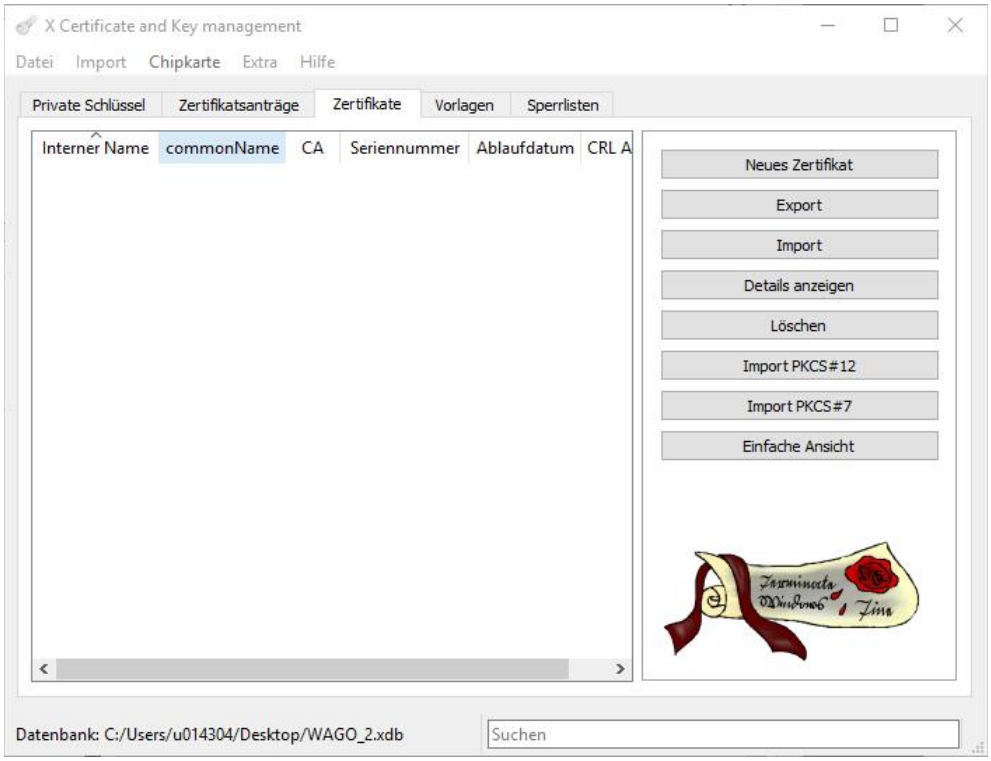

Abbildung 17: Datenbank XCA

4. Wählen Sie in der Registerkarte **Vorlagen** die Schaltfläche [**Neue Vorlage**].

5. Wählen Sie in dem sich öffnenden Dialogfenster „Vorlagenwerte voreinstellen“ die Einstellung „[default] Leere Vorlage“.

6. Bestätigen Sie die Auswahl mit [**OK**].

7. Wechseln Sie im sich öffnenden Dialogfenster „XCA Vorlage ändern“ zur Registerkarte „Inhaber“:

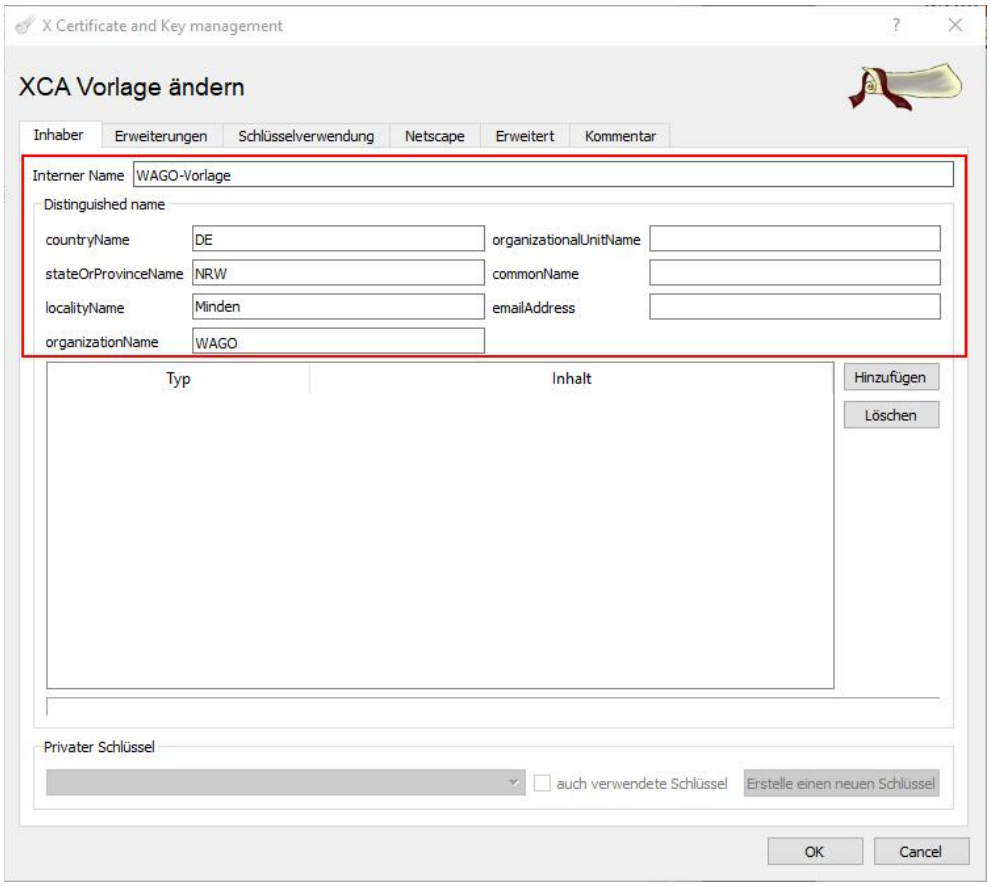

Abbildung 18: Vorlage anlegen, Register „Inhaber“

Tabelle 8: Registerkarte „Inhaber“

Eingabefeld	Bedeutung
Interner Name	Der Wert in diesem Feld dient als interne Referenz und sollte das Zertifikat eindeutig identifizieren.
countryName	Ländercode (z. B. DE für Deutschland)
stateOrProvinceName	Bundesland (z. B. NRW)
localityName	Ausstellungsort des Zertifikats
organizationName	Name der Organisation, die das Zertifikat ausgestellt hat
organizationUnitName	Abteilungsbezeichner
commonName	Hier kann ein allgemeiner Bezeichner hinterlegt werden.
emailAddress	Hier kann eine E-Mail-Adresse hinterlegt werden.

8. Füllen Sie die markierten Eingabefelder im oberen Bereich aus.
   Das Feld „commonName“ wird in der Vorlage leer gelassen und später ausgefüllt.

9. Bestätigen Sie Ihre Eingaben mit [**OK**]

Nachdem die Vorlage erstellt wurde, wird sie im Fenster angezeigt.

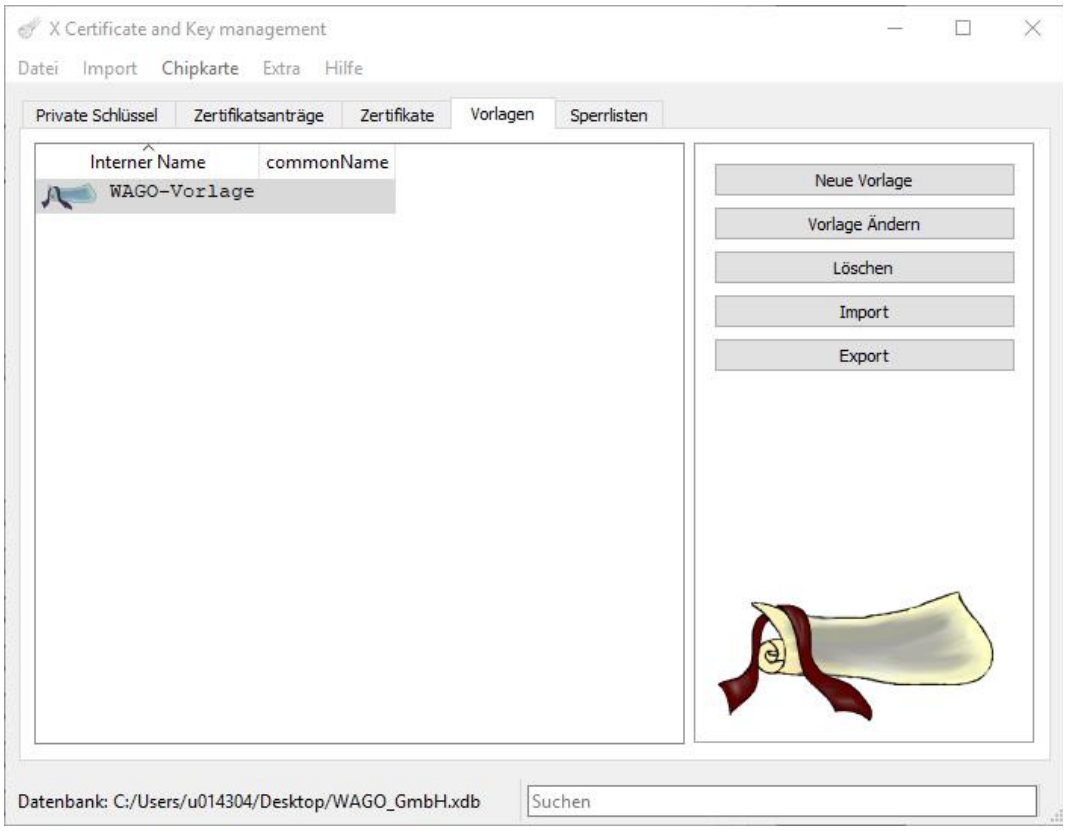

Abbildung 19: Vorlage erstellt

6.2.1.5.2 Root-CA-Zertifikat erstellen

1. Wechseln Sie zur Registerkarte „Zertifikate“, um das Root-CA-Zertifikat zu erstellen.

2. Wählen Sie die Schaltfläche [**Neues Zertifikat**]. Das folgende Dialogfenster öffnet sich:

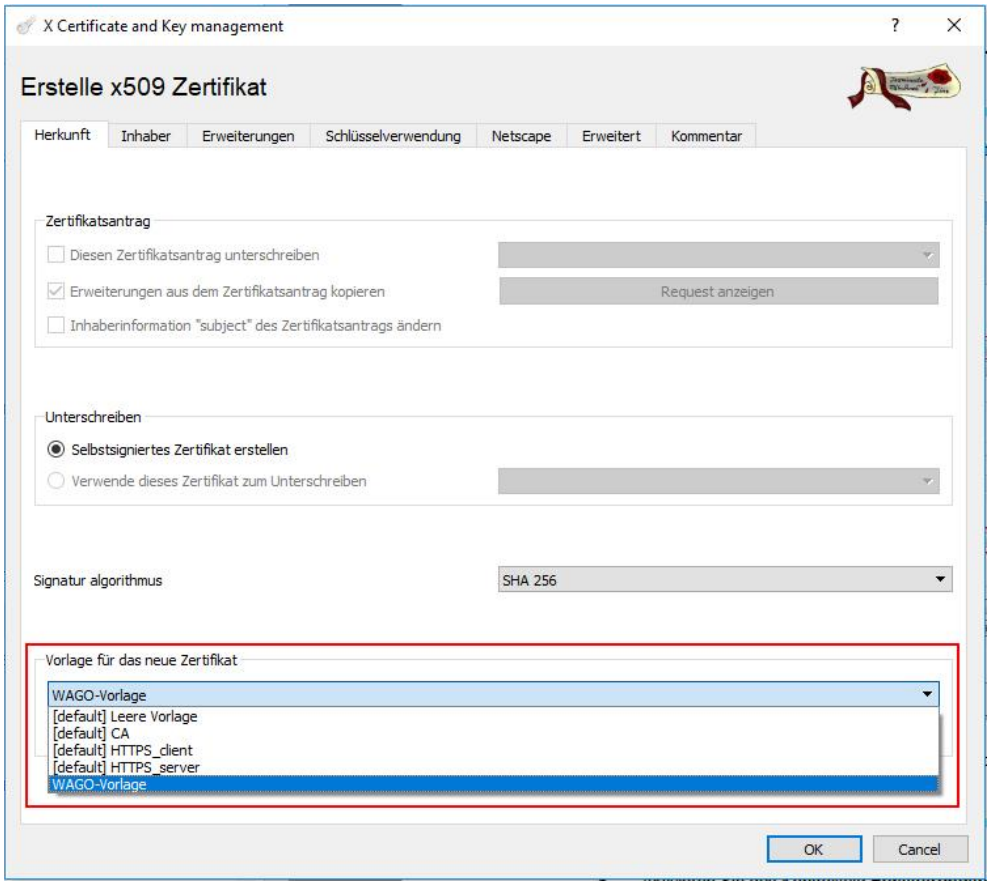

Abbildung 20: Zertifikat erstellen

3. Wählen Sie aus dem Auswahlfeld „Vorlage für das neue Zertifikat“ Ihre erstellte Vorlage aus.

4. Wählen Sie die Schaltfläche [**Subject übernehmen**].

5. Wählen Sie aus dem Auswahlfeld „Vorlage für das neue Zertifikat“ die Vorlage „[default] CA“ aus.

6. Wählen Sie die Schaltfläche [**Erweiterungen übernehmen**].

7. Wechseln Sie zur Registerkarte „Inhaber“.

8. Geben Sie einen Bezeichner in das Eingabefeld „CommonName“ ein. (z. B. „RootCA“).

9. Wählen Sie die Schaltfläche [**Erstelle einen neuen Schlüssel**].

Abbildung 21: Neuen Schlüssel anlegen

10. Stellen Sie Schlüsseltyp und Schlüssellänge für die Root-CA ein. Der Name ist voreingestellt.
    Die Vergabe ist abhängig davon, ob der Schlüssel für die Root-CA oder für den Controller generiert wird (für empfohlene Schlüssellängen siehe technische Richtlinien des BSI TR-02102-2).

11. Wählen Sie die Schaltfläche [**Erstellen**], um den Schlüssel zu erstellen.

12. Beenden Sie das Dialogfenster über **[OK],** nach der Mitteilung über die erfolgreiche Schlüsselerstellung.

Das erstellte Zertifikat wird in der Registerkarte „Zertifikate“ angezeigt:

Abbildung 22: Neues Zertifikat angelegt

6.2.1.5.3 Gerätezertifikat erstellen

1. Wechseln Sie zur Registerkarte „Zertifikate“, um das Gerätezertifikat zu erstellen.

2. Wählen Sie die Schaltfläche [**Neues Zertifikat**]. Das folgende Dialogfenster öffnet sich:

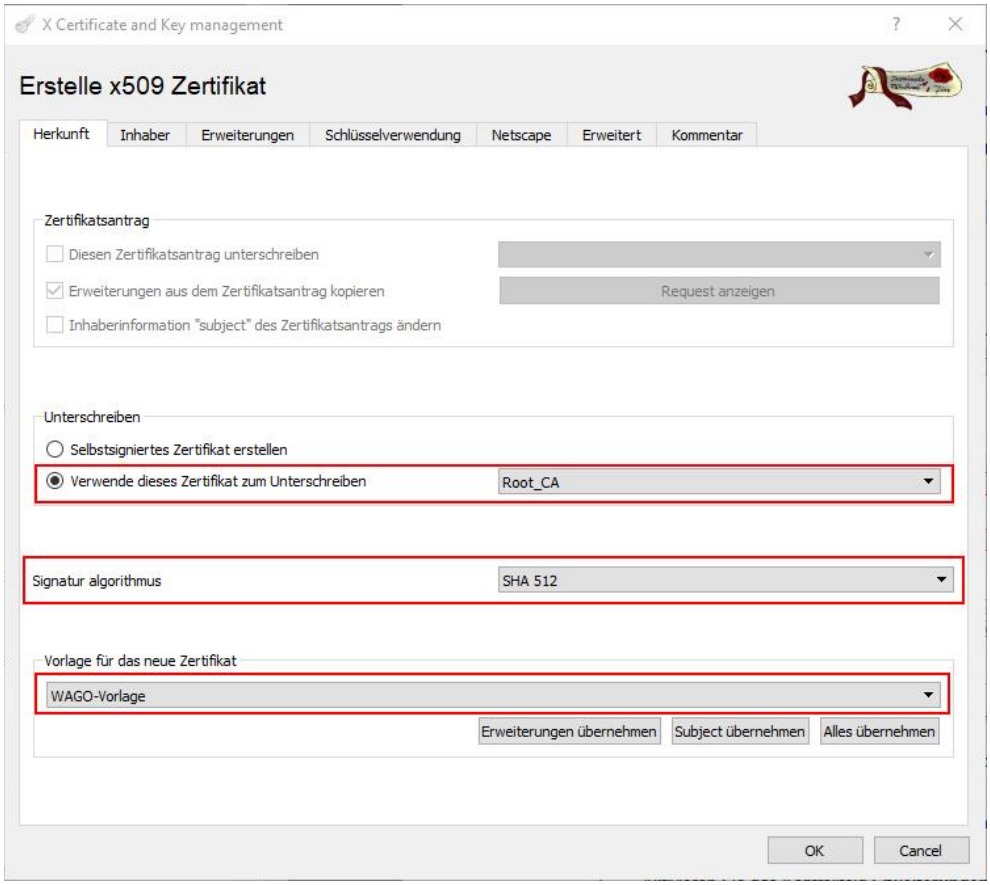

Abbildung 23: Neues Gerätezertifikat erstellen

3. Aktivieren Sie das Kontrollfeld **Verwende dieses Zertifikat zum Unterschreiben** und wählen Sie Ihr erstelltes Root_CA-Zertifikat aus.

4. Wählen Sie im Auswahlfeld **Signatur algorithmus** den Wert „SHA 512“ (siehe technische Richtlinien des BSI TR-02102).

5. Wählen Sie im Auswahlfeld **Vorlage für das neue Zertifikat** Ihre erstellte Vorlage aus.

6. Wählen Sie die Schaltfläche [**Subject übernehmen**].

7. Wählen Sie im Auswahlfeld „Vorlage für das neue Zertifikat“ die Vorlage „[default] HTTPS_server“ aus.

8. Wählen Sie die Schaltfläche [**Erweiterungen übernehmen**].

9. Wechseln Sie zur Registerkarte „Inhaber“.

10. Geben Sie die IP-Adresse Ihres Gerätes in das Eingabefeld „CommonName“ ein.

11. Wählen Sie die Schaltfläche [**Erstelle einen neuen Schlüssel**].

Abbildung 24: Neuen Schlüssel anlegen

12. Stellen Sie Schlüsseltyp und Schlüssellänge für die Root-CA ein. Der Name ist voreingestellt.
Die Vergabe ist abhängig davon, ob der Schlüssel für die Root-CA oder für den Controller generiert wird (für empfohlene Schlüssellängen siehe technische Richtlinien des BSI TR-02102-2).

13. Wählen Sie die Schaltfläche [**Erstellen**], um den Schlüssel zu erstellen.

14. Wechseln Sie zur Registerkarte „Erweiterungen“.

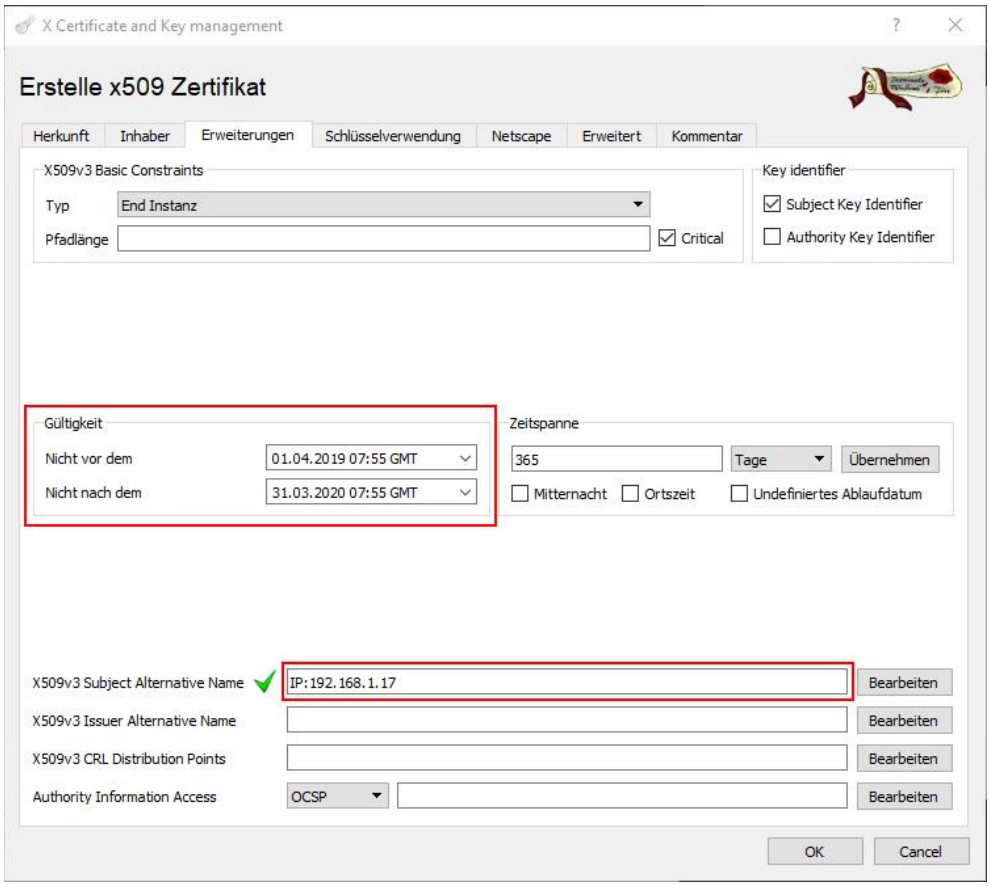

Abbildung 25: Registerkarte Erweiterungen

15. Stellen Sie die Gültigkeit des Gerätezertifikats ein. Beachten Sie dabei die Empfehlungen der „technischen Richtlinien des BSI TR-02102-2“.

16. Fügen Sie in dem Eingabefeld **X509v3 Subject Alternative Name** ebenfalls die IP-Adresse und/oder den Hostname hinzu.

Hinweis

Der Wert im Eingabefeld „X509v3 Subject Alternative Name“ muss identisch mit der Adresszeile sein!
Die IP-Adresse bzw. der Hostname wird von den Browsern genutzt, um die Identität festzustellen. Wenn der im Eingabefeld „**X509v3 Subject Alternative Name**“ eingetragene Wert von dem Wert in der Adresszeile abweicht, wird das Zertifikat als nicht gültig erkannt!

17. Wählen Sie dazu die Schaltfläche **[Bearbeiten]**. Folgendes Eingabefenster öffnet sich:

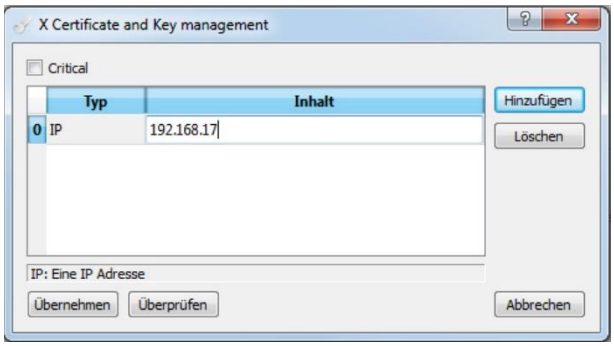

Abbildung 26: X509v3 Subject Alternative Name, IP-Adresse eingeben

18. Wählen Sie die Schaltfläche [**Hinzufügen**].

19. Wählen Sie im Auswahlfeld **Typ** entweder „IP“ für IP-Adresse oder „DNS“ für Hostname.

20. Geben Sie den entsprechenden Wert in das Eingabefeld “Inhalt“ ein.

21. Wechseln Sie wieder zurück zur Registerkarte „Schlüsselverwendung“, um die Nutzung der Zertifikate einzuschränken.

22. Tragen Sie die in der Abbildung markierten Werte ein.

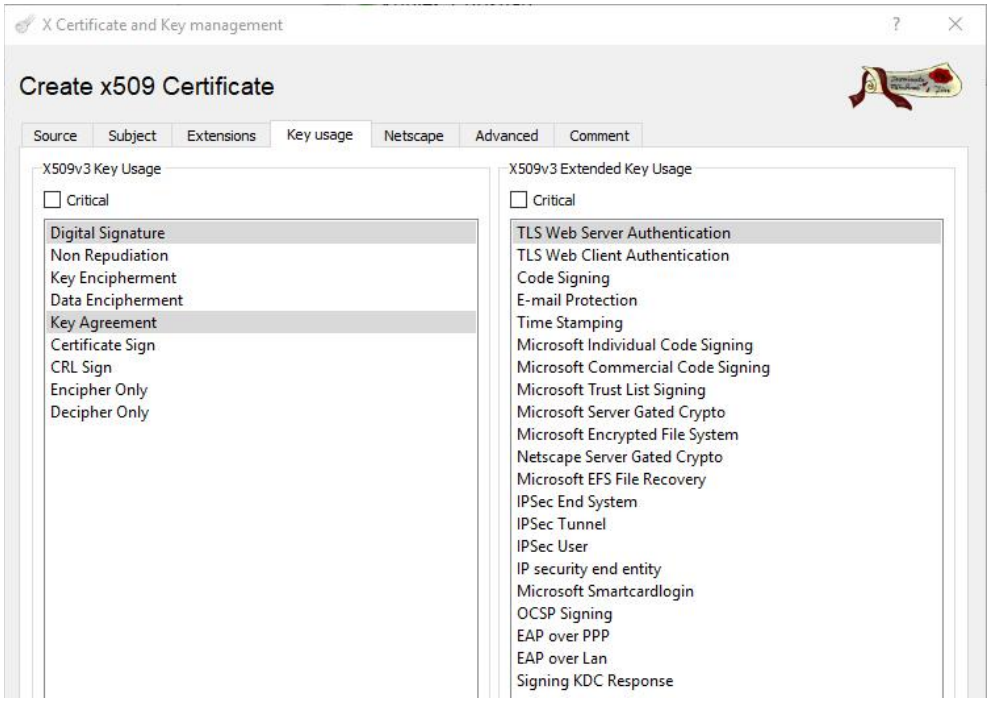

Abbildung 27: Neuer Zertifikatsantrag, Schlüsselverwendung Client

Hinweis

Bei der Serverauthentifizierung andere Werte eintragen!
Beachten Sie, dass bei der Serverauthentifizierung im rechten Feld der Eintrag „TLS Web Server Authentication“ eingetragen wird. Im linken Feld werden die Werte „Digital Signature“ und „Key Encipherment“ oder alternativ „Key Agreement“ eingetragen. Ansonsten ist das Verfahren der Zertifikatserstellung für Sever/Client identisch!

23. Bestätigen Sie Ihre Eingaben mit [**OK**].
Das neue Zertifikat wird in der Registerkarte „Zertifikate“ unterhalb des Root-CA-Zertifikats angezeigt.

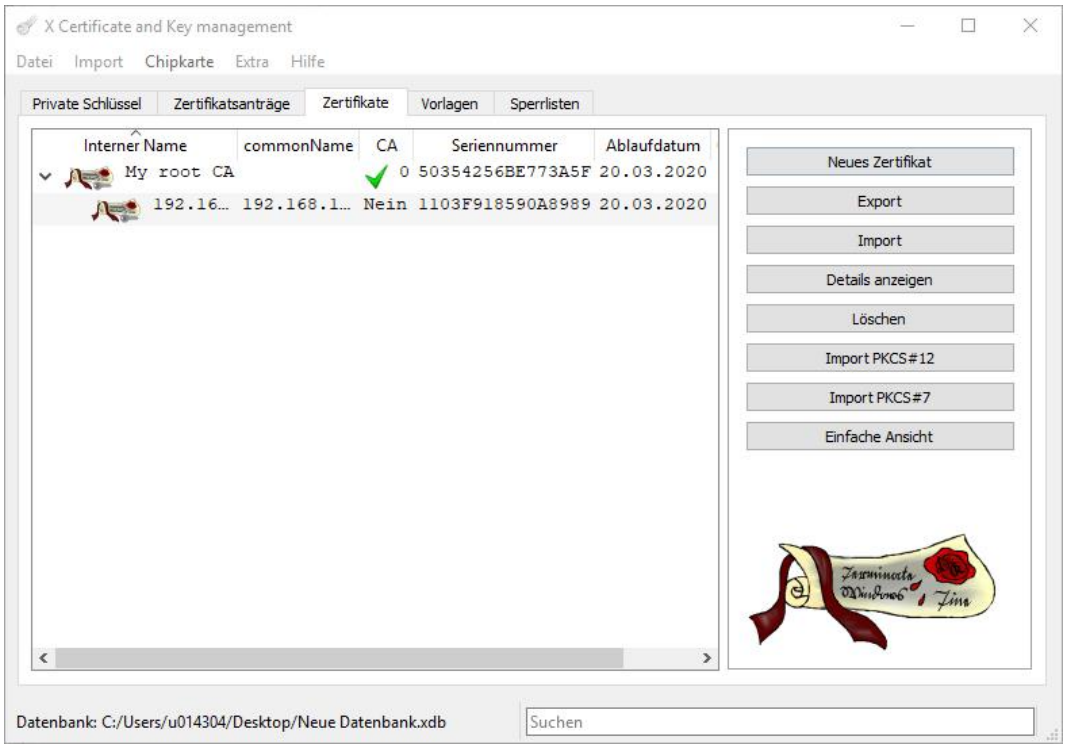

Abbildung 28: Gerätezertifikat erstellt

6.2.1.5.4 Zertifikate exportieren

1. Wechseln Sie im Hauptfenster in die Registerkarte „Zertifikate“ und klappen Sie die Baumstruktur ganz auf.

2. Markieren Sie Ihr Root-CA-Zertifikat und öffnen Sie über Rechtsklick das Kontextmenü.

3. Wählen Sie **Export** > **Datei**.

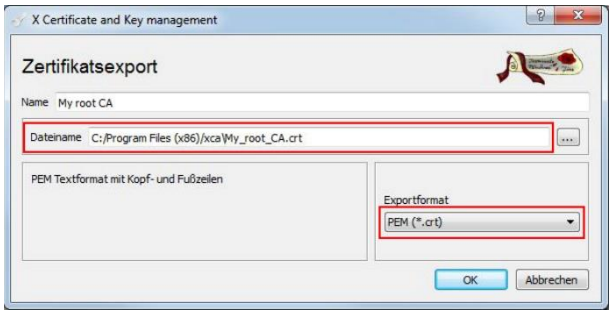

Abbildung 29: Root-CA-Zertifikat exportieren

4. Wählen Sie über die Schaltfläche [**…**] den Speicherort aus.

5. Wählen Sie in der Auswahlliste **Exportformat** den Eintrag „PEM ohne Schlüssel“ aus.

6. Bestätigen Sie mit [**OK**].

7. Markieren Sie Ihr Controller-Zertifikat und öffnen Sie über Rechtsklick das Kontextmenü.

8. Wählen Sie **Export** > **Datei**.

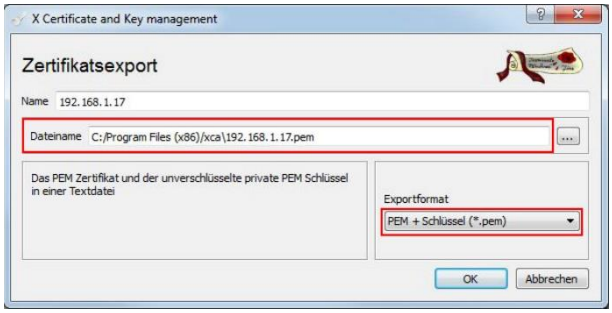

Abbildung 30: Controller-Zertifikat exportieren

9. Wählen Sie über die Schaltfläche [**…**] einen Speicherort aus.

10. Wählen Sie in der Auswahlliste **Exportformat** den Eintrag „PEM mit Schlüssel“ aus.

11. Bestätigen Sie mit [**OK**].

6.2.1.5.5 Zertifikate auf dem Client und auf dem Gerät installieren

Hinweis

Neues Gerätezertifikat bei Änderungen von IP-Adresse/Hostname erforderlich!
Wenn die IP-Adresse oder der Hostname geändert wurden, muss das Zertifikat für den Controller mit der korrekten IP-Adresse oder dem korrekten Hostname neu erstellt werden (siehe Kapitel „Gerätezertifikat erstellen“!

1. Importieren Sie Ihr Root-CA-Zertifikat in den Browser.
   Das Vorgehen hängt vom verwendeten Browser ab!

2. Übertragen Sie die Zertifikate via FTPS/SCP auf den Controller.

3. Legen Sie das PFC Zertifikat unter „/etc/lighttpd/“ ab und benennen Sie es um in „https-cert.pem“.

4. Übertragen Sie das Root-CA-Zertifikat via FTPS/SCP auf den Controller.

5. Legen Sie das Root-CA-Zertifikat unter „/etc/lighttpd/“ ab und benennen Sie es um in „root-ca.pem“.

6. Öffnen Sie die Datei tls.conf (/etc/lighttpd/tls.conf).

7. Fügen Sie die Zeile „ssl.ca-file“ ein und tragen Sie dort den Ablageort ein: „/etc/lighttpd/root-ca.pem“.

Abbildung 31: Ablageort „/etc/lighttpd/root-ca.pem“

8. Starten Sie den Webserver neu mithilfe des Tools: „/etc/config-tools/restart_webserver“. Alternativ kann das Gerät neu gestartet werden.

Sobald – je nach Browser – vor oder hinter Ihrer Webadresse ein grünes Schlosssymbol erscheint, ist die Aktion erfolgreich verlaufen und Ihre Verbindung von jetzt an gesichert. Die Browser zeigen häufig in der Adresszeile an, wie vertrauenswürdig eine Verbindung ist. Firefox z. B. zeigt ein grünes Schloss an, wenn das Zertifikat von einer vertrauenswürdigen Root-CA signiert ist.

Abbildung 32: Grünes Schloss im Browser (Firefox)

6.2.1.5.6 Zertifikatsperrliste anlegen

Hinweis

Zertifikatssperrlisten nur bei OpenVPN und IPsec!
Auf den Controllern werden Zertifikatssperrlisten aktuell ausschließlich bei OpenVPN- und IPsec-Verbindungen genutzt.

Eine Zertifikatssperrliste (Certificate Revocation List, CRL) beinhaltet Zertifikate, die innerhalb des Gültigkeitszeitraums gesperrt, ungültig, falsch oder widerrufen sind. Das ist sinnvoll für den Fall, dass ein privater Schlüssel verloren geht oder einem Client das Vertrauen entzogen werden soll. Wenn bspw. ein Mitarbeiter aus dem Unternehmen ausscheidet, möchte man in der Regel dessen Zertifikat vorzeitig für ungültig erklären, um den Zugang zum Firmennetzwerk zu verhindern.

Ein Eintrag für ein gesperrtes Zertifikat kann temporär erfolgen. Die Zertifikatsperrliste wird auf dem Server angelegt.

Hinweis

Sie können zunächst eine leere Liste anlegen!
Sie können zunächst eine leere Zertifikatsperrliste anlegen, um zu vermeiden, dass ein VPN-Dienst bei einer Aktualisierung neu gestartet werden muss. Eine leere Liste kann auch im laufenden Betrieb aktualisiert werden!

Sie können eine Zertifikatsperrliste über die Schlüsselverwaltungssoftware XCA erzeugen.

1. Öffnen Sie die Software XCA und wählen Sie die Registerkarte „Zertifikate“**.**
2. Markieren Sie das Zertifikat, das Sie der Sperrliste hinzufügen möchten.
3. Wählen Sie über die rechte Maustaste das Menü **Rücknahme**.

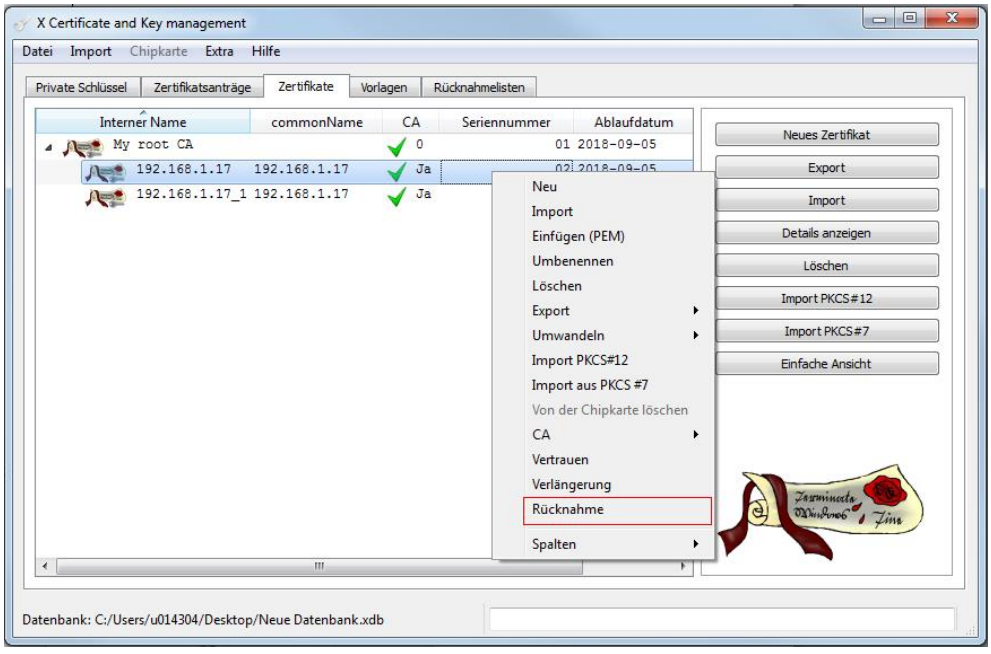

Abbildung 33: Zertifikatsperrliste anlegen

4. In dem sich öffnenden Fenster können Sie einen Grund für den Entzug des Vertrauens angeben und das Datum, ab welchem das Zertifikat ungültig ist.

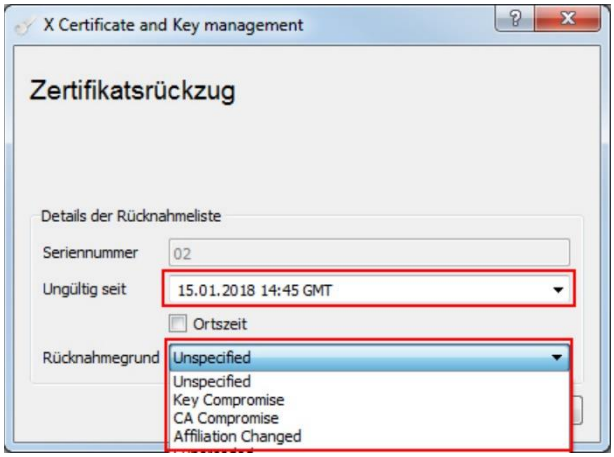

Abbildung 34: Zertifikatsrückzug

5. Wiederholen Sie die Schritte 2 … 4 bei Bedarf.

6. Wechseln Sie zur Registerkarte „Rücknahmelisten“.

7. Wählen Sie über die rechte Maustaste das Menü **Neu**.

In dem sich öffnenden Fenster brauchen Sie keine weiteren Einstellungen vornehmen; XCA fügt die gesperrten Zertifikate automatisch der Liste hinzu. Optional können Sie das Update-Intervall festlegen und den Signaturalgorithmus anpassen.

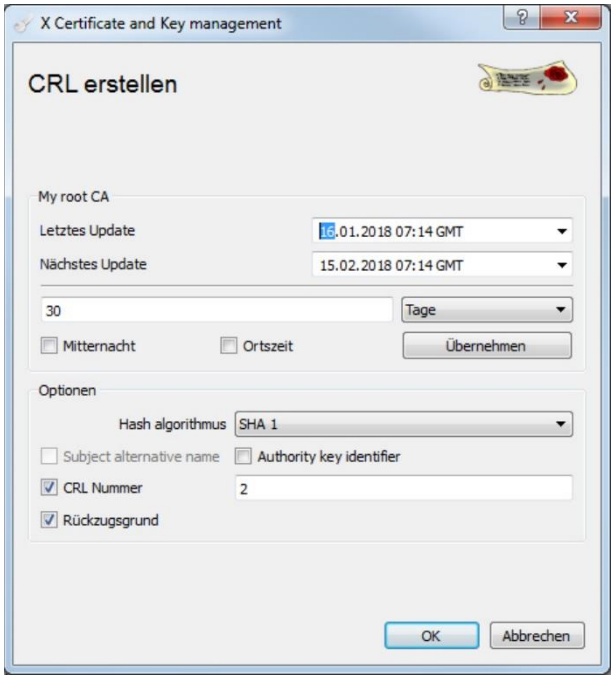

Abbildung 35: CRL erstellen

8. Wählen Sie die Schaltfläche **[OK]**. Anschließend wird die Zertifikatssperrliste in der Registerkarte „Rücknahmelisten“ angezeigt.

9. Wählen Sie die Zertifikatssperrliste aus und wählen Sie die Schaltfläche **[Export].**

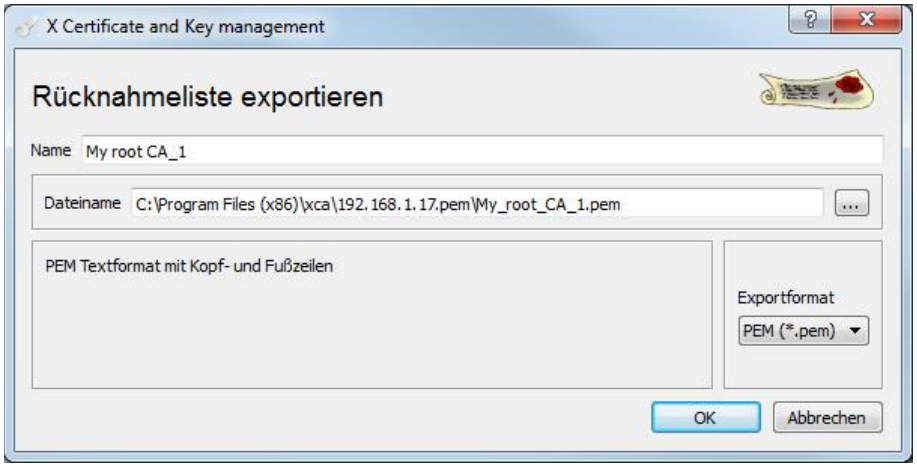

Abbildung 36: Rücknahmeliste exportieren

10. Speichern Sie die Zertifikatssperrliste.

11. Wählen Sie die Schaltfläche **[OK]**.

Hinweis

Beachten Sie die Ablagestruktur!
Wenn Sie ein OpenVPN-Netzwerk einrichten, muss die Zertifikatssperrliste in dem für OpenVPN spezifizierten Verzeichnis gespeichert werden (siehe Kap. „OpenVPN“ > „Konfigurationsdateien erstellen“, Server Konfiguration „crl-verify“)!

Hinweis

Beachten Sie die Ablageorte für Zertifikatssperrlisten bei OpenVPN!
Bei OpenVPN muss vorab die Konfigurationsdatei für OpenVPN angelegt werden, da dort die Ablageorte definiert werden, siehe Kap. „OpenVPN“ > „Konfigurationsdateien erstellen“!

Hinweis

Der VPN-Dienst muss auf die Zertifikatssperrliste zugreifen können!
Stellen Sie sicher, dass der VPN-Dienst auf die Zertifikatssperrliste zugreifen kann, auch wenn er keine Root-Privilegien besitzt. Übertragen Sie dazu entweder den Dateibesitz auf den OpenVPN-User:
`chown openvpn:openvpn <Datei>`
oder legen Sie die Datei so an, dass sie „world-readable“ ist:
`chmod 644 <Datei>`
(Die Datei enthält keine geheimen Informationen).

6.2.2 Zugriff über offene Netzwerkschnittstellen einschränken

Alle Dienste bzw. Netzwerkschnittstellen, die nicht genutzt oder für die aktuelle Anwendung nicht benötigt werden, können ein unnötiges Gefahrenpotenzial darstellen. Es sollte daher im Einzelfall überprüft werden, welche Dienste und Netzwerkschnittstellen benötigt und welche deaktiviert werden können. Bei Produktivsystemen sollte aber im Vorfeld getestet werden, welche Auswirkungen das Deaktivieren auf das System hat.

In den nachfolgenden Kapiteln wird beschrieben, wie standardmäßig aktive Dienste deaktiviert werden können. Des Weiteren kann der Zugriff auf einen Dienst auch auf eine bestimmte Schnittstelle beschränkt werden. Dieses Vorgehen wird empfohlen, wenn ein Dienst benötigt wird und daher nicht abgeschaltet werden kann. Durch diese Beschränkung kann die Angriffsfläche für einen Cyberangriff weiter reduziert werden. Details hierzu finden Sie im Kapitel „Hardening“ > „Firewall konfigurieren“.

Hinweis

Nutzen Sie stets sichere Protokolle!
Nutzen Sie stets sichere Protokolle, wie z. B. HTTPS anstelle von HTTP und SNMPv3 anstelle von SNMPv1 etc.!

6.2.2.1 WAGO-Service-Kommunikation deaktivieren

Wenn die WAGO-Service-Kommunikation nicht verwendet wird, bzw. die Entwicklungswerkzeuge WAGO-I/O-*Check*, ETHERNET-Settings oder ***e!****COCKPIT* nicht benötigt werden, sollte diese deaktiviert werden.

1. Wählen Sie im WBM den Menüpunkt **Ports and Services > Network Services**, um die WAGO Service-Kommunikation zu deaktivieren.

2. Deaktivieren Sie im Bereich „I/O-Check“ das Kontrollfeld **Service active**.

Abbildung 37: WAGO-Service-Kommunikation deaktivieren

3. Klicken Sie auf die Schaltfläche **[Submit]** um die Änderung zu übernehmen.

6.2.2.2 Standard-Netzwerkports ändern

Die Mehrzahl der automatisierten Login-Attacken auf Netzwerkdienste, wie z. B. SSH, erfolgt auf dem Standard-Netzwerkport 22. Eine einfache und effektive Methode sich davor zu schützen besteht darin, den SSH Port zu ändern. Die verwendeten Standard-Netzwerkports für CODESYS und SSH können über das Web-Based-Management geändert werden.

1. Navigieren Sie zum Menü **Ports and Services** > **PLC Runtime Services**.

2. Tragen Sie im Bereich „CODESYS“ im Eingabefeld **Communication Port Number** bevorzugt einen Port aus dem Bereich der „Dynamic Port Numbers“ ein.

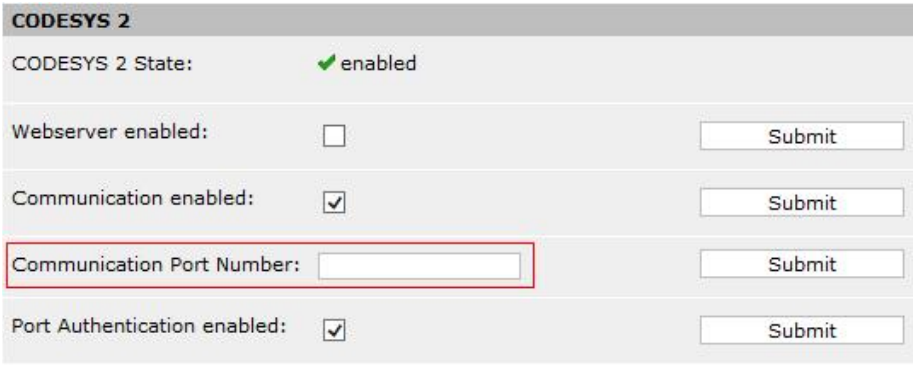

Abbildung 38: Standard-Netzwerkports ändern

Jeder Netzwerkport kann auf einem System nur einmal verwendet werden. Stellen Sie daher sicher, dass der Port nicht von einer anderen Applikation genutzt wird, da es sonst zu Verbindungsproblemen kommen kann. Ebenfalls sollten keine reservierten Ports anderer Dienste genutzt werden.

Hinweis

Dynamic Port Numbers (dynamische Portnummern)
Die Verwendung der „Dynamic Port Numbers“ stellt nur eine Empfehlung dar, um Kollisionen mit bereits verwendeten Ports zu vermeiden!

Die „Dynamic Port Numbers“ werden auch als private Portnummern bezeichnet. Es handelt sich um Portnummern, die **jede** Anwendung für die Kommunikation mit **jeder** anderen Anwendungen über die Internetprotokolle TCP oder UDP nutzen kann! Mehr Informationen unter: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

3. Betätigen Sie die Schaltfläche **[Submit],** um die Änderung zu übernehmen.

4. Wiederholen Sie die Schritte 2 … 3 im Menü **Ports and Services** > **SSH** im Bereich **„**SSH Server“, um dort den Port zu ändern.

Hinweis

Externe Firewalls müssen entsprechend konfiguriert werden!
Wenn Sie eine externe Firewall verwenden, müssen Sie ggf. die verwendeten Ports freigeben!

6.2.2.3 Unverschlüsselten Zugang auf das WBM sperren

Im Auslieferungszustand des Controllers wird der Port TCP/80 für das WBM und eine ggf. vorhandene Webvisualisierung genutzt. Bei einem Zugriff per HTTP wird der Browser automatisch auf die verschlüsselte Verbindung umgeleitet. Es wird empfohlen diesen Port über das WBM abzuschalten.

1. Öffnen Sie das WBM und navigieren Sie zum Menü **Ports and Services** > **Network Services.**

2. Deaktivieren Sie das Kontrollfeld **Service active** im Bereich „http“**.**

Abbildung 39: Unverschlüsselten Zugang auf das WBM sperren

3. Klicken Sie auf die Schaltfläche [**Submit**]. Die angepassten Einstellungen werden übernommen.

6.2.2.4 Zugang zur CODESYS Laufzeitumgebung deaktivieren

Hinweis

e!*RUNTIME*-**Laufzeitumgebung lässt sich nicht deaktivieren!**
Die Deaktivierung des Zugangs zur Laufzeitumgebung ist nur für CODESYS, nicht aber für ***e!****RUNTIME* möglich!

Der Controller verfügt über eine CODESYS Laufzeitumgebung, über die der Controller programmiert werden kann.

Das CODESYS Programm wird in der Regel über die ETHERNET-Schnittstellen heruntergeladen. Die zwei ETHERNET-Schnittstellen des Controllers können für verschiedene Funktionen konfiguriert werden. Wenn die Programmierung, bzw. die Erstinbetriebnahme abgeschlossen ist, kann der CODESYS Zugang auf das Gerät deaktiviert werden, um einen unerwünschten Zugriff zu verhindern.

1. Wählen Sie im WBM den Menüpunkt **Ports and Service** > **PLC Runtime Services** um den CODESYS Zugang zu deaktivieren.

2. Deaktivieren Sie im Bereich „CODESYS“ das Kontrollfeld **Communication enabled**.

Abbildung 40: Zugang zur CODESYS Laufzeitumgebung deaktivieren

3. Klicken Sie auf die Schaltfläche **[Submit]** um die Änderung zu übernehmen.

6.2.2.5 Direktzugriff auf die CODESYS Webvisualisierung sperren

Die Webvisualisierung von CODESYS kann via Webserver über die folgenden Ports erreicht werden:

- Port TCP/80 und/oder TCP/443
- Port TCP/8080

Es wird empfohlen in den Firewall-Einstellungen den direkten Zugriff über Port TCP/8080 zu sperren, da hier nur eine unverschlüsselte Verbindung möglich ist.

1. Wählen Sie im WBM den Menüpunkt **Firewall** > **General Configuration**.

2. Deaktivieren Sie im Bereich „Firewall Parameter Interface X1/X2 > Service enabled“ das Kontrollfeld **PLC WebVisu – direct link (port 8080)**“.

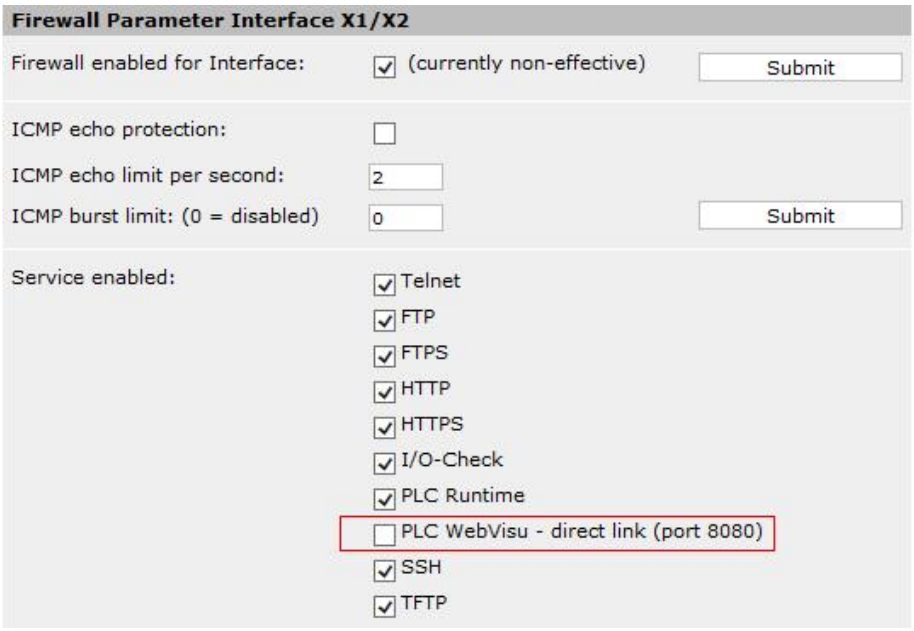

Abbildung 41: Direktzugriff auf die CODESYS Webvisualisierung sperren

3. Klicken Sie auf die Schaltfläche **[Submit],** um die Änderung zu übernehmen.

4. Wiederholen Sie Schritt 2 und 3 im Menü **Firewall** > **General Configuration** > **Firewall Parameter Interface VPN**, wenn Sie ein „Virtual Private Network“ nutzen.

Hinweis

X1 und X2 können als getrennte Schnittstellen betrieben werden!
Wenn Sie die beiden ETHERNET-Schnittstellen X1 und X2 als getrennte Netzwerk-Schnittstellen betreiben, müssen die o. g. Schritte 1 … 3 jeweils für die Schnittstellen X1 und X2 durchgeführt werden.

6.2.2.6 Zugriff auf die Laufzeitumgebung *e!RUNTIME* sperren

Aktivieren Sie zunächst die Firewall, falls diese noch nicht aktiviert ist, siehe Kapitel „Firewall konfigurieren“ > „Firewall im Web-Based-Management konfigurieren“.

1. Wählen Sie im WBM den Menüpunkt **Firewall** > **General Configuration**.

2. Deaktivieren Sie die Kontrollfelder **PLC Runtime** in den Bereichen „Firewall Parameter Interface X1/X2“ und **„**Firewall Parameter Interface VPN“.

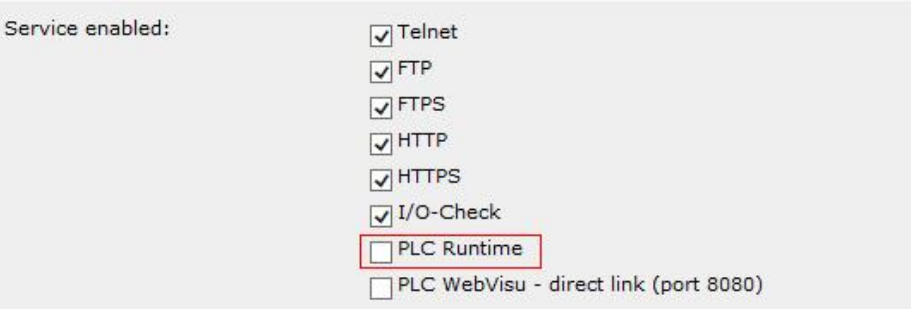

Abbildung 42: Zugriff auf die Laufzeitumgebung ***e!****RUNTIME* sperren

3. Klicken Sie auf die Schaltfläche **[Submit]** um die Änderung zu übernehmen.

Hierdurch wird der Zugriff auf den Port 11740/TCP oder auf den Port 2455/TCP gesperrt, je nachdem, welche Laufzeitumgebung verwendet wird. Alternativ können Sie einen Benutzerfilter für den Port 11740/TCP (***e!****Runtime*) oder für den Port 2455/TCP (CODESYS) anlegen. Details hierzu siehe Kapitel „Firewall im Web-Based-Management konfigurieren“ >“White List für bestimmte IP-Adressen anlegen“.

Port 1740/UDP (*e!Runtime*) schließen

1. Löschen Sie den Link im Dateisystem:
   /usr/lib/cds3-custom-components/libCmpBlkDrvUdp.so
2. Starten Sie die ***e!****RUNTIME* neu.

```
root@PFC200-40ED7D:~ rm /usr/lib/cds3-custom-components/libCmpBlkDrvUdp.so
root@PFC200-40ED7D:~ /etc/init.d/runtime stop
Terminate eRUNTIME...done
root@PFC200-40ED7D:~ /etc/init.d/runtime start
Starting eRUNTIME...done.
```

6.3 Passwörter ändern

Hinweis

Standardpasswörter ändern!
Die im Auslieferungszustand eingestellten Standardpasswörter sind in dieser Betriebsanleitung dokumentiert und bieten so keinen hinreichenden Schutz! Ändern Sie die Passwörter entsprechend Ihren Erfordernissen; Sie benötigen dafür allerdings Administrator-Berechtigungen!

6.3.1 Passwörter im Web-Based-Management ändern

Um das Web-Based-Management zu öffnen, geben Sie die IP-Adresse oder den Hostname Ihres Controllers in die Adresszeile Ihres Browsers ein. Die erforderlichen Einstellungen hierzu finden Sie im Handbuch des entsprechenden Controllers.

Hinweis

Anmeldung erforderlich!
Um voreingestellte Parameter zu ändern, ist zunächst eine Anmeldung erforderlich. Geben Sie dazu folgende Zugangsdaten ein:
Benutzername: admin
Passwort: wago

1. Wählen Sie im WBM den Menüpunkt **Administration** > **Users** um ein Passwort zu ändern.

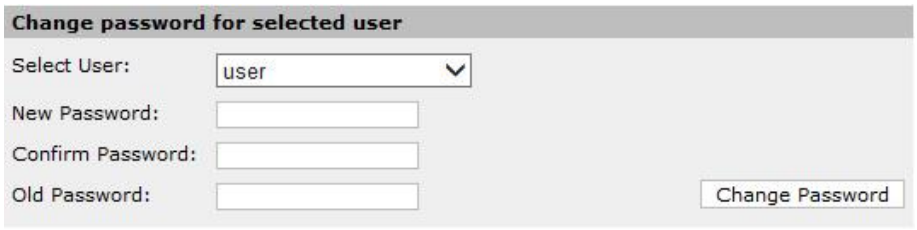

Abbildung 43: Passwörter im Web-Based-Management ändern

2. Wählen Sie den Benutzer („user“ oder „admin“) aus, für den Sie ein neues Passwort vergeben wollen.
3. Geben Sie das neue Passwort in das Eingabefeld **New Password** ein.
4. Bestätigen Sie das neue Passwort im Eingabefeld **Confirm Password**.
5. Klicken Sie auf die Schaltfläche **[Change Password]** um die Änderung zu übernehmen.

Hinweis

Beachten Sie die zulässigen Zeichen für Passwörter!
Zulässige Zeichen für das Passwort sind folgende ASCII-Zeichen: a … z, A … Z, 0 … 9, Leerzeichen und die Sonderzeichen:
]!"#$%&'()*+,./:;<=>?@[\^_`{|}~-

Werden außerhalb des WBM (z. B. über CBM) Passwörter mit unzulässigen Zeichen für das WBM eingestellt, ist ein Zugriff auf die WBM-Seiten nicht mehr möglich!

6.3.2 Linux®-Passwörter über die Linux®-Konsole ändern

Eine Verbindung zur Linux®-Konsole kann über verschiedene Zugänge hergestellt werden:

- Via Konsole über die RS-232-Schnittstelle
- Via SSH über ETHERNET

Die WAGO-Controller werden mit verschiedenen Benutzernamen und Standardpasswörtern ausgeliefert:

- root/wago
- admin/admin
- user/user

Bei der Eingabe neuer Passwörter beachten Sie bitte die Empfehlungen für sichere Passwörter im Kapitel: „Bedrohungsszenarien“ > … > „Zugänge über Benutzer und Passwörter“. Jeder Benutzer kann sein eigenes Passwort ändern, der Benutzer „root“ kann die Passwörter für alle anderen Benutzer ändern.

1. Stellen Sie eine Verbindung zur Linux®-Konsole her, entweder via Konsole über die RS-232-Schnittstelle oder via SSH über den ETHERNET-Port.
2. Ändern Sie die Passwörter mit dem Linux®-Tool „passwd“:

```
root@PFC200-40ED7D:~ passwd <Benutzer>
Changing password for <Benutzer>
New password: <Neues Passwort eingeben>
Retype password: <Neues Passwort wiederholen>
Password for <Benutzer> changed by root
```

Hinweis

Für den aktuellen Benutzer kann der Benutzername entfallen!
Wenn das Passwort nur für den aktuellen Benutzer geändert werden soll, kann die Angabe des Benutzernamens entfallen.

Das Passwort für den Benutzer „admin“ können Sie alternativ auch über das WBM ändern.

1. Wählen Sie im WBM den Menüpunkt **Ports and Services** > **PLC Runtime Services** > **General Configuration**.

Abbildung 44: Passwort für den Benutzer „admin“ ändern

2. Tragen Sie im Eingabefeld **Port Authentication Password** Ihr Passwort ein.
3. Bestätigen Sie Ihr Passwort im Eingabefeld **Confirm Password**.
4. Betätigen Sie die Schaltfläche [**Submit**], um das Passwort zu übernehmen.

6.4 Firewall konfigurieren

Damit Sie Ihr Netzwerk gegen Angriffe von außen sichern können, ist es wichtig, dass Sie Ihre Firewall mit einem Regelsatz konfigurieren, der Ihrer Anwendung entspricht.

ACHTUNG

Sorgen Sie für einen Notzugang zum System!
Richten Sie sich vor dem Konfigurieren der Firewall immer einen Notzugang ein, z. B. eine Verbindung über eine serielle Verbindung. So sorgen Sie dafür, dass Sie sich nicht durch einen Fehler selbst von Ihrem System aussperren können!

Der Controller hat eine eingebaute hostbasierte Firewall, die auf dem Linux®-Programm „iptables“ basiert. Die Firewall arbeitet als White-List-Filter, d. h. Pakete welche nicht explizit über die White List erlaubt werden, werden durch die Firewall blockiert. Die Filter werden in sogenannten Ketten (Chains) abgearbeitet; die Reihenfolge innerhalb der Ketten legt die Abarbeitungsreihenfolge fest.

Der Controller unterstützt das Anlegen von eigenen Filterregeln mit den folgenden Aktionen:

Tabelle 9: Aktionen für Filterregeln

Aktion	Beschreibung
ACCEPT	Das Paket wird akzeptiert und angenommen
DROP	Das Paket wird nicht angenommen; der Sender erhält keine Nachricht.

Eigene Filter können im WBM angelegt werden, siehe Kapitel „Firewall im Web-Based-Management konfigurieren“.

Im Anschluss an eine ACCEPT-, oder eine DROP-Aktion werden keine weiteren Regeln abgearbeitet.
Wenn keine Regel auf ein Paket angewendet werden kann, wird eine vordefinierte Regel für das Paket ausgeführt. Der Controller wendet als vordefinierte Regel eine DROP-Aktion für eingehenden Netzwerkverkehr an, mit Ausnahme von bereits bestehenden Verbindungen.
Vom Benutzer neu angelegte Filter werden sofort wirksam und vor den vordefinierten Regeln abgearbeitet. Informationen zu den vordefinierten Regeln finden Sie im Handbuch des entsprechenden Controllers unter www.wago.com.
Pakete, die von einem Benutzerfilter akzeptiert werden (Aktion ACCEPT), werden direkt an den entsprechenden Dienst weitergeleitet, ohne dass diese die vordefinierten Regeln passieren.

6.4.1 Firewall im Web-Based-Management konfigurieren

Unter dem Menüpunkt **Firewall** > **General Configuration** konfigurieren Sie die Einstellungen für die Firewall.

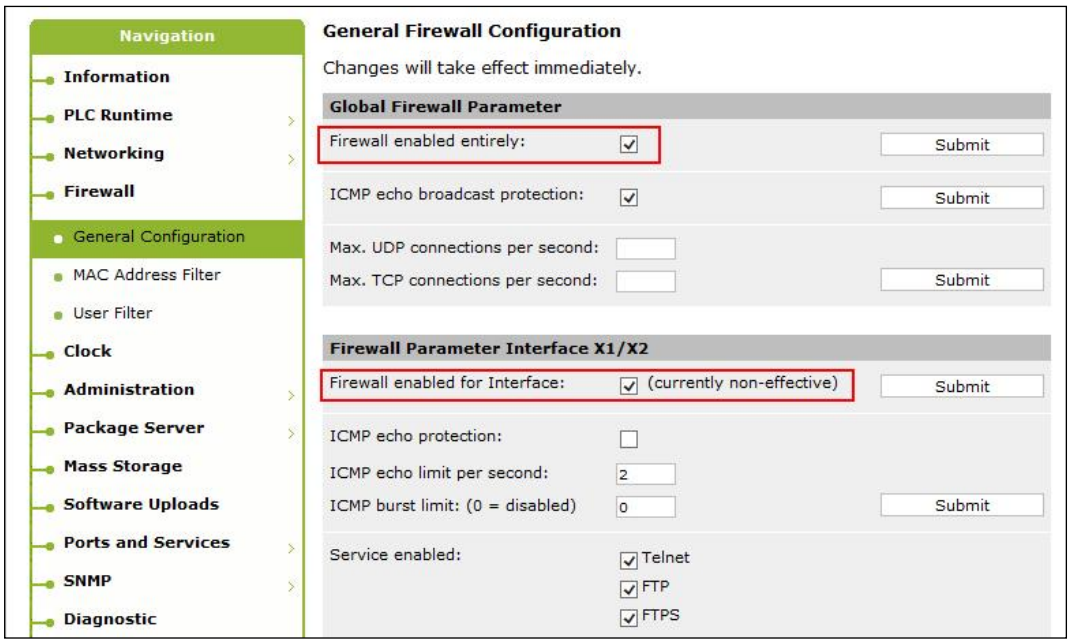

Abbildung 45: Firewall-Konfiguration im WBM

Um die Firewall zu aktivieren, müssen die folgenden Einstellungen vorgenommen werden:

1. Aktivieren Sie das Kontrollfeld **Firewall enabled entirely** (standardmäßig deaktiviert).
2. Klicken Sie auf die Schaltfläche **[Submit]**. Die angepassten Einstellungen werden übernommen.
3. Aktivieren Sie das Kontrollfeld **Firewall enabled for Interface**.
4. Klicken Sie auf die Schaltfläche **[Submit]**. Die angepassten Einstellungen werden übernommen.

Hinweis

Erlauben Sie nur den Zugriff aus vertrauenswürdigen Netzwerken!
Die Firewall kann auch nur für eine ausgewählte Schnittstelle aktiviert werden. Bitte beachten Sie dazu die Netzwerkstruktur und das Security-Konzept für Ihre Anwendung. Erlauben Sie nur den Zugriff aus vertrauenswürdigen Netzwerken auf Ihr Gerät!

Hinweis

Die Firewall-Regeln gelten sowohl für IPsec als auch für OpenVPN!
Die Konfiguration der Firewall-Regeln für ein VPN über das WBM (**Firewall Parameter Interface VPN**) ist unabhängig von der verwendeten VPN-Technologie (IPsec oder OpenVPN).
Im Auslieferungszustand sind IPsec-Standardregeln für das Modem-Interface (wwan) und Standardregeln für OpenVPN (tun+ und tap+) definiert. Die vordefinierten Regeln können Sie sich über die Linux®-Konsole mit dem Befehl „iptables-save“ anzeigen lassen.

6.4.1.1 White List für bestimmte IP-Adressen anlegen

Sie können eine White List anlegen, mit der Sie definierten IP-Adressen den Zugriff auf Dienste erlauben, die von Ihrem System angeboten werden.

ACHTUNG

DROP-Aktion immer erst NACH einer ACCEPT-Aktion anlegen!
Legen Sie immer erst eine ACCEPT-Regel für Ihre eigene IP-Adresse an, da sonst die Gefahr besteht, dass Sie sich selbst aussperren!

Hinweis

Benutzerdefinierte Filterregeln haben Vorrang!
Bitte beachten Sie, das benutzerdefinierte Filterregeln **vor** den im Controller vordefinierten Regeln ausgeführt werden. Nach einer ACCEPT-Aktion werden die vordefinierten Regeln nicht mehr angewendet. Aus diesem Grund sollten Sie immer einen Port unter „Destination Port“ angeben, um nicht versehentlich Vollzugriff auf alle Ports in Ihrem System zu gewähren!

Um eine White List anzulegen, werden zuerst alle IP-Adressen der White List hinzugefügt, die auf den Dienst des Systems zugreifen dürfen. Danach wird ein Filter mit einer DROP-Aktion angelegt, welcher alle anderen Zugriffe blockiert.

Nachfolgend wird beispielhaft die IP-Adresse 192.168.147.1 für den Zugriff auf SSH freigeschaltet (siehe Schritte 1 … 8). Alle anderen IP-Adressen werden für den Zugriff gesperrt (siehe Schritte 9 … 16).

ACCEPT-Aktion

1. Wechseln Sie zum Menü **Firewall > User Filter**.
2. Aktivieren Sie im Bereich „Add new user filter > Policy“ das Kontrollfeld **Accept**.
3. Tragen Sie im Eingabefeld **Source IP adress** die IP-Adresse ein, der sie einen Zugang erlauben möchten.
4. Tragen Sie im Eingabefeld **Source netmask** die Netzmaske „255.255.255.255“ ein, wenn Sie **ausschließlich** der angegebenen IP-Adresse Zugang erlauben möchten.
5. Tragen Sie im Eingabefeld **Destination port** den Port der Anwendung ein, die freigeschaltet werden soll.

6. Aktivieren Sie das Kontrollfeld **TCP oder UDP,** abhängig von dem Protokoll, das Sie freischalten möchten.

7. Aktivieren Sie das Kontrollfeld **Any, X1** oder **VPN** um die Regel für die jeweilige Schnittstelle anzuwenden.

Hinweis

Die Schnittstelle X2 steht im Switch-Modus nicht zur Verfügung!
Die beiden ETHERNET-Schnittstellen X1 und X2 können wahlweise im Switch-Modus oder als getrennte Netzwerk-Schnittstellen betrieben werden. Wenn Sie beide Netzwerk-Schnittstellen verwenden, müssen Sie die Regel für die Schnittstelle X2 kopieren.

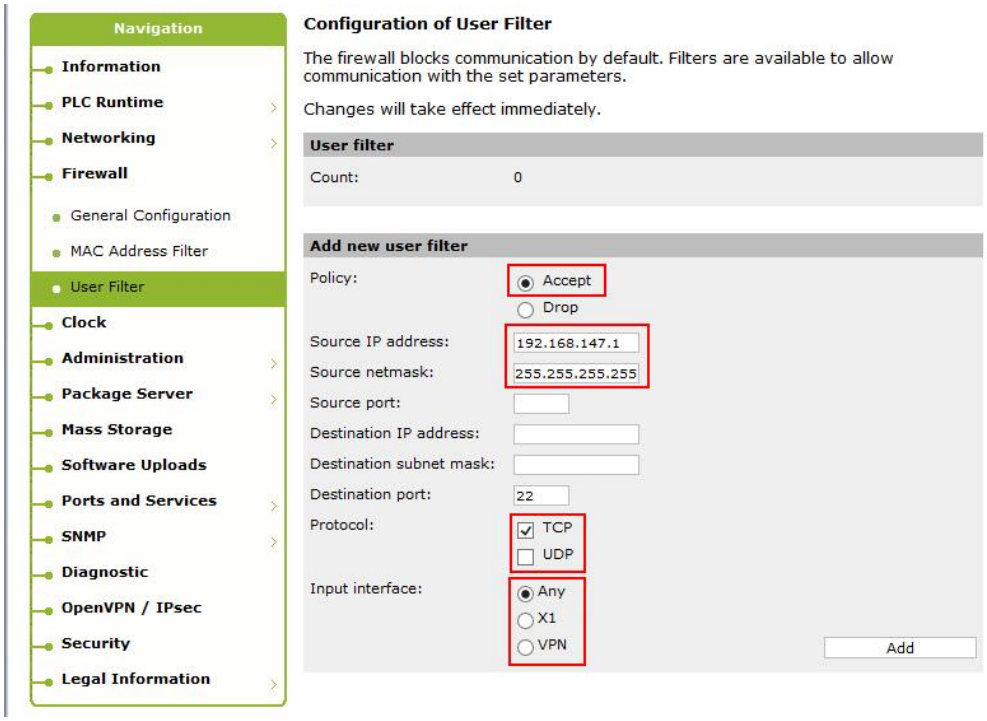

Abbildung 46: User-Filter: White List anlegen

8. Klicken Sie auf die Schaltfläche **[Add]**. Die Regel wird übernommen.

Drop-Aktion

9. Wechseln Sie zum Menü **Firewall > User Filter**.

10. Aktivieren Sie im Bereich „Add new user filter > Policy“ das Kontrollfeld **Drop**.

11. Lassen Sie das Eingabefeld **Source IP adress** leer.

12. Lassen Sie das Eingabefeld **Source netmask** leer.

13. Tragen Sie im Eingabefeld **Destination port** den Port der Anwendung ein, die freigeschaltet werden soll, z. B. „22“ für SSH.

14. Aktivieren Sie das Kontrollfeld **TCP oder UDP,** abhängig von dem Protokoll, das Sie freischalten möchten.

15. Aktivieren Sie das Kontrollfeld **Any** um die Regel für jede Schnittstelle anzuwenden.

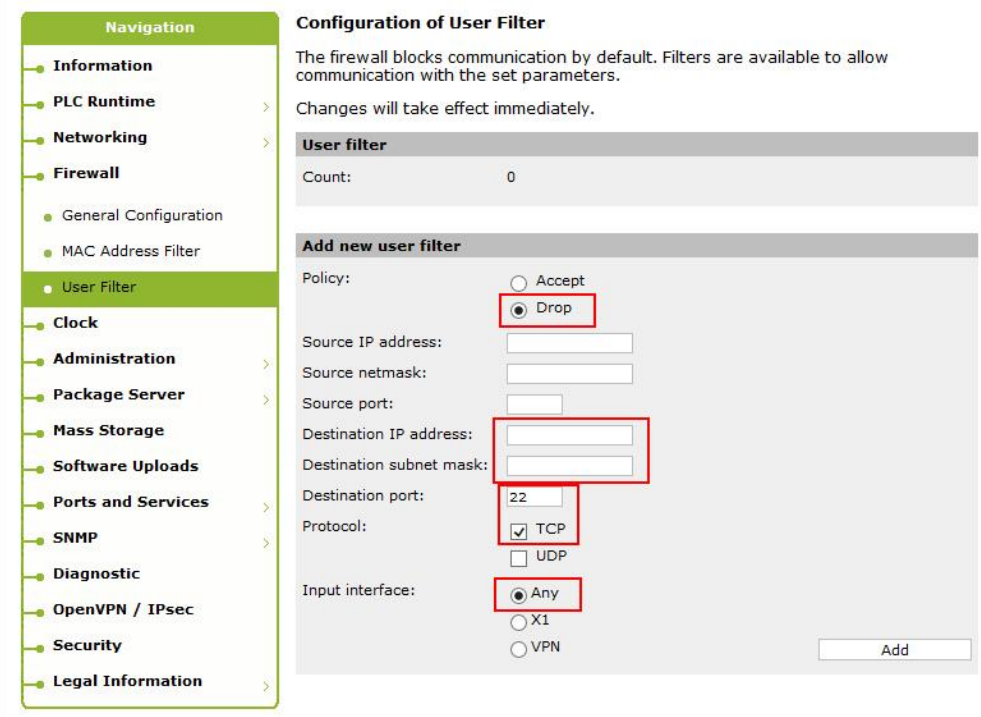

Abbildung 47: Anlegen einer Black List für alle Zugriffe

16. Klicken Sie auf die Schaltfläche [**Add**]. Die Regel wird übernommen.

Die Filter werden abschließend in der angezeigten Reihenfolge ausgeführt:

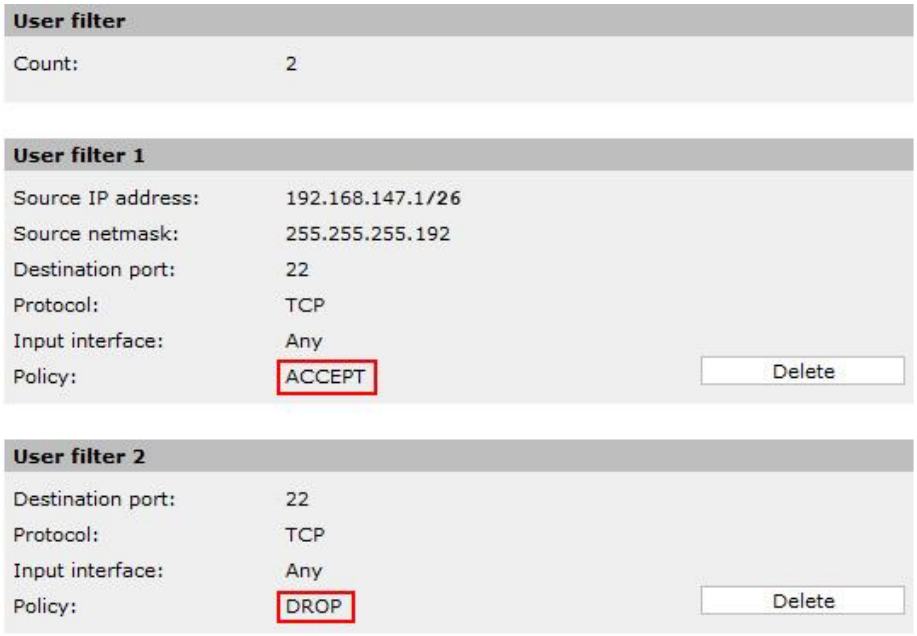

Abbildung 48: Reihenfolge der Filterregeln

6.4.1.2 White List für Netzwerke anlegen

Wenn eine White List für ein Netzwerk oder mehrere Netzwerke angelegt werden soll, müssen diese zunächst per ACCEPT-Aktion frei gegeben werden. Anschließend muss der Zugang für alle anderen Netzwerke per DROP-Aktion blockiert werden, analog zur Freigabe von einer einzelnen IP-Adresse. Die Filterregeln, die Sie unter „Firewall“ > „General Configuration“ aktiviert haben, werden dadurch außer Kraft gesetzt. Spezifizieren Sie daher den Port für den Dienst, den Sie freigeben möchten.

ACHTUNG

DROP-Aktion immer erst NACH einer ACCEPT-Aktion anlegen!
Bevor Sie bestimmten IP-Adressen oder Netzwerken den Zugang verwehren, müssen Sie immer erst die White List anlegen, da diese sonst unter Umständen nicht mehr angewendet werden. Der Zugang zum Netzwerk kann so unerwünschter Weise gesperrt werden!

Nachfolgend wird beispielhaft das Netzwerk 192.168.147.1/26 für den Zugriff auf SSH freigeschaltet (siehe Schritte 1 … 8). In den dargestellten Beispielen wird jeglicher Zugriff für andere Netzwerkteilnehmer gesperrt (siehe Schritte 9 … 16).

ACCEPT-Aktion

1. Wechseln Sie zum Menü **Firewall > User Filter**.
2. Aktivieren Sie im Bereich „Add new user filter > Policy“ das Kontrollfeld **Accept**.
3. Tragen Sie im Eingabefeld S**ource IP adress** die IP-Adresse ein, der sie einen Zugang erlauben möchten.
4. Tragen Sie im Eingabefeld **Source netmask** die Netzmaske „255.255.255.192“ ein.
5. Tragen Sie im Eingabefeld **Destination port** den Port der Anwendung ein, die freigeschaltet werden soll.
6. Aktivieren Sie das Kontrollfeld **TCP oder UDP,** abhängig von dem Protokoll, das Sie freischalten möchten.
7. Aktivieren Sie das Kontrollfeld **Any, X1** oder **VPN** um die Regel für die jeweilige Schnittstelle anzuwenden.

Hinweis

Die Schnittstelle X2 steht im Switch-Modus nicht zur Verfügung!
Die beiden ETHERNET-Schnittstellen X1 und X2 können wahlweise im Switch-Modus oder als getrennte Netzwerk-Schnittstellen betrieben werden. Wenn Sie beide Netzwerk-Schnittstellen verwenden, müssen Sie die Regel für die Schnittstelle X2 kopieren.

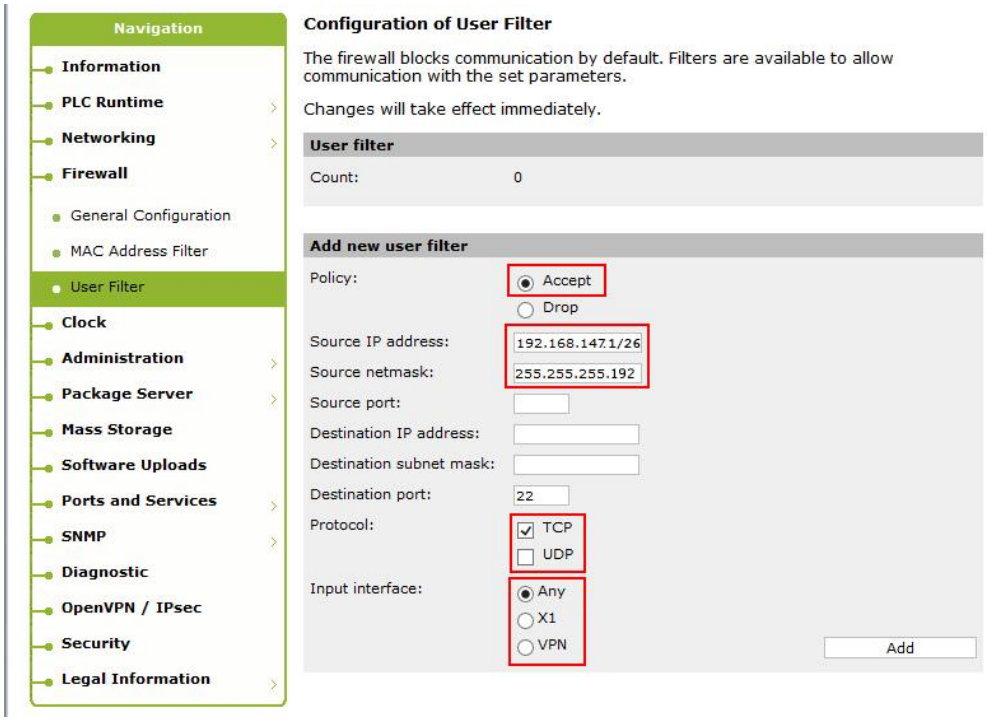

Abbildung 49: User Filter: White List für Netzwerke anlegen

8. Klicken Sie auf die Schaltfläche **[Add]**. Die Regel wird übernommen.

Drop-Aktion

9. Wechseln Sie zum Menü **Firewall > User Filter**.

10. Aktivieren Sie im Bereich „Add new user filter > Policy“ das Kontrollfeld **Drop**.

11. Lassen Sie das Eingabefeld **Source IP adress** leer.

12. Lassen Sie das Eingabefeld **Source netmask** leer.

13. Tragen Sie im Eingabefeld **Destination port** den Port der Anwendung ein, die freigeschaltet werden soll, z. B. „22“ für SSH.

14. Aktivieren Sie das Kontrollfeld **TCP oder UDP,** abhängig von dem Protokoll, das Sie freischalten möchten.

14. Aktivieren Sie das Kontrollfeld **Any** um die Regel für jede Schnittstelle anzuwenden.

15. Klicken Sie auf die Schaltfläche [**Add**]. Die Regel wird übernommen.

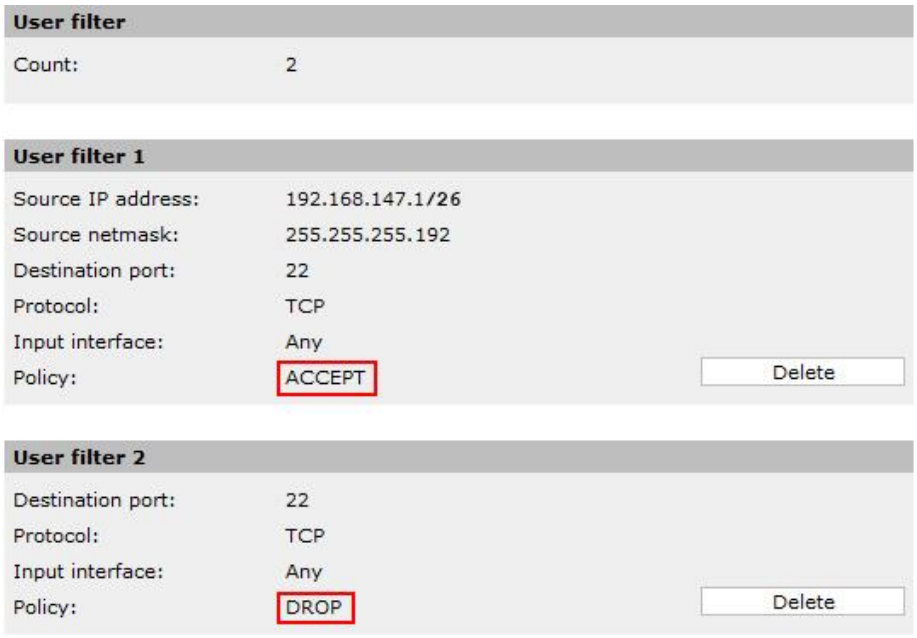

Abbildung 50: Freigabe von definierten Netzwerken

In dem dargestellten Beispiel ist das Netzwerk 192.168.147.1/26 für den Zugriff auf SSH freigeschaltet worden. Das beinhaltet die IP-Adressen 192.168.147.1 … 192.168.147.62 und die Broadcast-Adresse 192.168.147.1.63.

6.4.2 MAC-Adressenfilter

MAC-Adressen eines Geräts können einfach gefälscht werden. Die Filterung von MAC-Adressen ist daher als einzige Sicherheitsmaßnahme unzureichend. MAC-Adressen werden auf der ETHERNET-Schicht genutzt und bedingen einen physikalischen Zugriff auf das lokale Netzwerk (Local Area Network (LAN)). Es können also keine Zugriffe von außen, z. B. über einen Router verhindert werden. Wenn über einen Router auf das System zugegriffen wird, sieht der Controller nur die MAC-Adresse des Routers. Daher wird empfohlen, die Filterung von MAC-Adressen mit weiteren Schutzmechanismen zu kombinieren.

Im Auslieferungszustand der Controller ist standardmäßig ein „White-Listing“ für alle WAGO-MAC-Adressen, basierend auf der Herstellerkennung OUI (Organizationally Unique Identifier) eingetragen, aber nicht aktiv. Dieser Filter sollte gelöscht und durch Filter ersetzt werden, die zu den Gegebenheiten in Ihrem Netzwerk passen.

1. Ziehen Sie immer MAC-Adressen anderer, vertrauenswürdiger Netzwerkteilnehmer anstelle der Herstellerkennung vor. Über die Herstellerkennung werden alle MAC-Adressen eines Herstellers freigeschaltet; das ist in vielen Fällen nicht gewünscht.

2. Schalten Sie vor dem Aktivieren des MAC-Adressenfilters die MAC-Adresse Ihres PCs oder die des Zugangs zum Gerät frei (z. B. Router, Proxy etc.), um sich selbst nicht auszusperren!

6.4.2.1 MAC-Adressen im Web-Based-Management konfigurieren

Unter dem Menüpunkt **Firewall** > **MAC Address Filter** können Sie den MAC-Adressenfilter aktivieren und konfigurieren:

Zunächst werden die MAC-Adressen aller Geräte eingetragen, die mit dem Gerät kommunizieren dürfen.

1. Tragen Sie im Feld **MAC address** im Bereich **MAC address filter whitelist** die MAC-Adresse ein, die freigeschaltet werden soll.

2. Tragen Sie im Eingabefeld **MAC mask** im Bereich „MAC address filter whitelist“ den Wert „ff:ff:ff:ff:ff:ff“ ein.

Hinweis

MAC-Maske für den neuen Listeneintrag
Der Eintrag im Eingabefeld **MAC mask** bestimmt die Bits, die geprüft werden, wenn eine bestimmte MAC-Adresse freigeschaltet werden soll.

3. Aktivieren Sie das Kontrollfeld **Filter enabled.**

Abbildung 51: MAC-Adressen eintragen

4. Betätigen Sie die Schaltfläche **[Add]**. Die eingetragene MAC-Adresse wird freigeschaltet.

Hinweis

Die Anzahl der Listeneinträge ist begrenzt!
Es können maximal 10 Filter für MAC-Adressen eingegeben werden.

Nachdem alle MAC-Adressen eingetragen wurden, muss der MAC-Adressenfilter aktiviert werden.

5. Aktivieren Sie das Kontrollfeld **Filter enabled** im Bereich **„**Global MAC address filter state**“,** um den globalen MAC-Adressenfilter zu aktivieren.

6. Betätigen Sie die Schaltfläche **[Submit]**. Die angepassten Einstellungen werden übernommen.

7. Aktivieren Sie das Kontrollfeld **Filter enabled** im Bereich „MAC address filter state X1/X2“**,** um den MAC-Adressenfilter für die jeweilige Schnittstelle zu aktivieren.

8. Betätigen Sie die Schaltfläche **[Submit]**. Die angepassten Einstellungen werden übernommen.

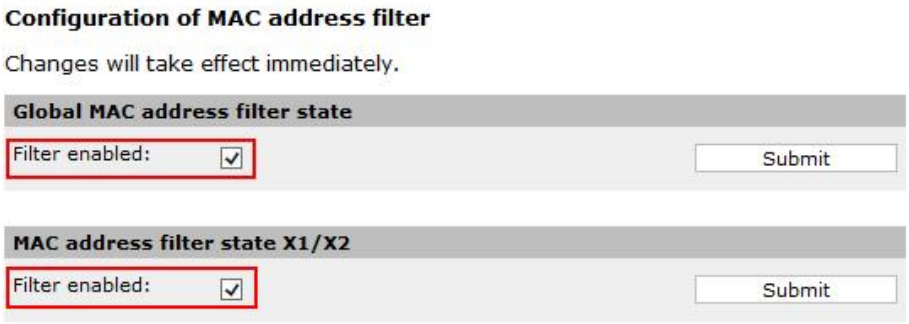

Abbildung 52: MAC-Adressenfilter aktivieren

7 Erweiterte Sicherheitsmaßnahmen

In diesem Kapitel werden zusätzliche Sicherheitsmaßnahmen beschrieben, die mit dem PFC100/200 realisiert werden können und dazu beitragen Ihre Systemsicherheit zu erhöhen.

7.1 VPN – Virtual Private Network

7.1.1 Allgemein

Der Begriff „Virtual Private Network“ steht für eine Reihe von Technologien (z. B. IPsec), die ein virtuelles privates Netzwerk innerhalb eines öffentlich zugänglichen Netzwerks erstellen können. Innerhalb dieses geschlossenen VPNs können nur die verbundenen und autorisierten Teilnehmer gesichert miteinander kommunizieren.

Für die Authentifizierung stehen im Wesentlichen zwei Verfahren zur Verfügung; entweder zertifikatsbasiert oder über einen vorab installierten statischen Schlüssel (Pre-shared Key).

- **Zertifikatsbasiert**: Bei der zertifikatsbasierten Authentifizierung wird die Identität eines VPN-Endpunkts mittels eines digitalen Zertifikats geprüft bzw. bestätigt. Ein digitales Zertifikat basiert auf einem individuellen Schlüsselpaar, das sich aus einem privaten und einem öffentlichen Schlüssel zusammensetzt. Wenn das digitale Zertifikat eines VPN-Endpunktes kompromittiert wird, muss das Zertifikat gesperrt und auf dem betroffenen Gerät ausgetauscht werden, siehe Kapitel „Hardening“ > … > „Zertifikatssperrliste anlegen“.
- **Pre-shared Key**: Beim Pre-shared-Key-Verfahren wird ein gemeinsamer statischer Schlüssel für alle VPN-Endpunkte verwendet. Im Falle einer Kompromittierung des gemeinsamen Schlüssels, muss der Schlüssel manuell bei allen VPN-Endpunkten ausgetauscht werden.

Hinweis

Beachten Sie die Empfehlungen bei kryptografischen Verfahren!
Die zusätzliche Sicherung der Datenpakete durch Verschlüsselung führt zu einer zeitlichen Verzögerung und somit zu einer längeren Paketlaufzeit. Achten Sie auf die Wahl der Schlüssellängen für die kryptografischen Verfahren, entsprechend den technischen Richtlinien des BSI TR-02102-4 (Version 2017-01)!

Nachfolgend werden typische Basisszenarien für den Aufbau eines VPNs dargestellt:

Site-to-Site-VPN

Abbildung 53: Site-to-Site-VPN

Bei einem Site-to-Site-VPN werden zwei oder mehrere lokale Netzwerke miteinander zu einem virtuellen logischen Netzwerk über das Internet verbunden, siehe Abbildung „Site-to-Site-VPN“. Die gesicherte Kommunikation erfolgt dabei zwischen den beiden Gateways (z.B. VPN-Gateway oder Router).

Host-to-Site-VPN

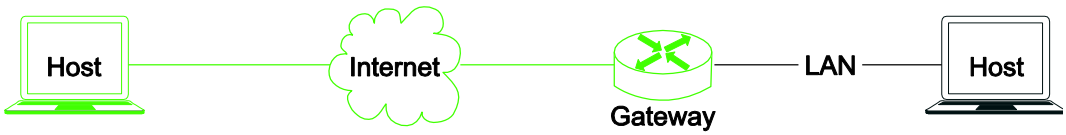

Abbildung 54: Host-to-Site-VPN

Das Host-to-Site-VPN ermöglicht es bestimmten Anwendern (z. B. im Home-Office oder mobil), sicher auf ein entferntes Netzwerk zuzugreifen, siehe Abbildung „Host-to-Site-VPN“. Die gesicherte Kommunikation erfolgt dabei vom Endsystem des Anwenders (Host) bis zum Gateway des entfernten Netzwerks (z.B. VPN-Gateway oder Router).

Host-to-Host-VPN

Abbildung 55: Host-to-Host-VPN bzw. Remote-Desktop-VPN

Das Host-to-Host-VPN ermöglicht eine gesicherte VPN-Verbindung zwischen zwei Endsystemen (Ende-zu-Ende-Sicherung), siehe Abbildung „Host-to-Host-VPN“. Somit wird die vollständige Kommunikation zwischen den beteiligten Endsystemen gesichert.

In den folgenden Kapiteln werden exemplarisch die beiden Szenarien „Site-to-Site“ und „Host-to-Host“ für die Controller beschrieben.

7.1.2 Zertifikate erzeugen

Für die gegenseitige zertifikatsbasierte Authentifizierung benötigen die VPN-Endpunkte jeweils ein Zertifikat, welches von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurde. Beachten Sie beim Erstellen der Zertifikate die Hinweise am Ende dieses Abschnitts.

Eine Anleitung zum Erstellen von Zertifikaten und Schlüsseln finden Sie im Kapitel „Hardening“ > … > „Zertifikate erstellen und austauschen“.

Hinweis

Bei TLS-basierten VPNs (OpenVPN) wird für ein Client-Zertifikat eine andere Vorlage als für ein Server-Zertifikat benötigt!
Beachten Sie, wenn Sie einen Antrag für ein Client-Zertifikat erstellen, dass Sie in der Registerkarte **Herkunft** im Auswahlfeld **Vorlage für das neue Zertifikat** den Eintrag **[default] HTTPS_client** auswählen. Siehe Kapitel „Hardening“ > … > „Antrag für ein Gerätezertifikat erstellen“. In der Beschreibung wird die Vorlage **[default] HTTPS_client** ausgewählt!

Hinweis

Achten Sie darauf, dass die Uhrzeit auf allen Systemen gleich ist!
Wenn Sie Zertifikate nutzen, muss die Uhrzeit auf allen Systemen identisch sein. Es kann sonst zu Problemen kommen, wenn Zertifikate z. B. von einem System als noch nicht gültig oder als schon abgelaufen angesehen werden!

7.1.3 „IP Forwarding“ aktivieren

Für ein Site-to-Site-VPN müssen die Endpunkte des VPNs als Router konfiguriert werden. Hierfür muss die Funktion „IP Forwarding“ im Controller aktiviert werden. Diese Einstellung ist standardmäßig deaktiviert, damit ein- und ausgehende Datenpakete in und aus einem dahinter liegenden Netzwerk weitergeleitet werden.
Aktivieren Sie „IP Forwarding“ auf dem Controller wie folgt:

1. Wählen Sie im WBM den Menüpunkt **Networking** > **Routing,** um die Funktion „IP Forwarding“ zu aktivieren.

2. Aktivieren Sie das Kontrollfeld **Routing enabled entirely** im Bereich „General Routing Configuration“.

Abbildung 56: „IP Forwarding“ aktivieren

3. Betätigen Sie die Schaltfläche **[Submit]** um die Einstellung zu speichern.

Alternativ können Sie die Funktion „IP Forwarding“ aktivieren, indem Sie die folgende Zeile in die Datei „etc/sysctl.conf“ eintragen oder einen eventuell vorhandenen Eintrag anpassen:

```
net.ipv4.ip_forward = 1
```

7.1.4 OpenVPN

Mit der freien Software OpenVPN kann ein Virtuelles Privates Netzwerk (VPN) über eine TLS-Verbindung aufgebaut werden. Es werden zwei Betriebsmodi unterstützt:

- **Routing-Modus**: Hiermit wird ein verschlüsselter Tunnel hergestellt, in dem ausschließlich IP-Pakete (OSI-Schicht 3) weitergeleitet werden.
- **Bridging-Modus**: Hiermit wird ein vollständiges Tunneln von ETHERNET-Frames (OSI-Schicht 2) ermöglicht, sodass der Einsatz beliebiger Netzwerkprotokolle möglich ist.

In den nachfolgenden Kapiteln wird die Konfiguration einer OpenVPN-Verbindung schrittweise beschrieben.

7.1.4.1 Benutzer und Gruppe für den OpenVPN-Dienst einrichten

Zunächst müssen ein dedizierter Benutzer und eine Gruppe für den OpenVPN-Dienst angelegt werden:

1. Melden Sie sich über SSH am Controller an.
2. Legen Sie eine Gruppe „openvpn“ an:

```
addgroup -S openvpn
```

3. Legen Sie einen Benutzer „openvpn“ an und fügen Sie diesen Benutzer in die zuvor erstellte Gruppe „openvpn“ ein:

```
adduser -G openvpn -S -D -H openvpn
```

Hinweis

Schreiben Sie den angelegten Benutzer in die OpenVPN-Konfigurationsdatei!
OpenVPN muss so konfiguriert werden, dass der Benutzer nach dem Initialisieren zu dem oben angelegten, nicht privilegierten Benutzer wechselt, siehe Kapitel „Host-to-Host-VPN“, Abschnitt „Minimale Rechte“!

7.1.4.2 Firewall konfigurieren

Hinweis

In der Firewall muss OpenVPN auf dem Server freigegeben werden!
Sie müssen auf dem Server eine Ausnahmeregel für die OpenVPN-Verbindung erstellen, da die Firewall die Verbindung für das VPN nicht automatisch freigibt!

1. Wählen Sie im WBM den Menüpunkt **Firewall** > **User Filter,** um eine Ausnahmeregel für OpenVPN zu erstellen.

2. Füllen Sie die Felder im Bereich „Add new user filter“ aus, wie in der Abbildung dargestellt:

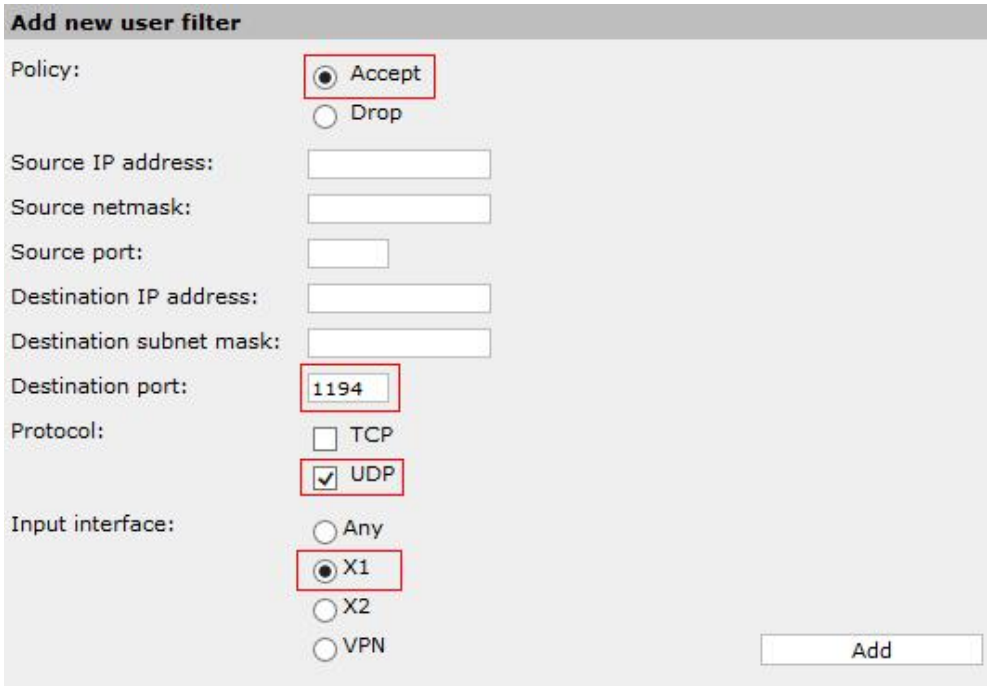

Abbildung 57: Firewall Konfiguration – OpenVPN

Hinweis

Achten Sie auf den richtigen Port-Eintrag!
Achten Sie darauf, dass der Eintrag unter „Destination port“ identisch zu Ihrem konfigurierten Port ist!

3. Betätigen Sie die Schaltfläche **[Add],** um den Filter anzuwenden.

Alternativ können Sie die Firewall mit dem nachfolgenden Befehl über die Linux®-Konsole konfigurieren:

```
firewall iptables --add-filter on X1 udp - - - - - 1194 accept --apply
```

7.1.4.3 Routing konfigurieren

Routing ermöglicht die Kommunikation über Netzwerkgrenzen hinweg. Wenn sich zwei Hosts nicht in einem Netzwerk befinden, müssen die Daten über einen Router geleitet werden, welcher die beiden Netzwerke miteinander verbindet. Im Fall von großen Netzwerken, wie z. B. dem Internet, können es auch mehrere Router sein.

Routen definieren den logischen Weg innerhalb eines Netzwerks zum Zielhost. Beim Anlegen von Routen wird immer nur der nächste Host auf dem Weg zum Zielhost angegeben und nicht die vollständige Route. Wenn die Daten über mehrere Router transportiert werden, müssen auf den dazwischen liegenden Routern ebenfalls Routen zum nachfolgenden Router angelegt werden. In großen Netzwerken, wie dem Internet, wird dies automatisch gesteuert, bis der Zielhost erreicht wird (z. B. über das „Border Gateway Protocol“ (BGP)).

Nachfolgend wird das Anlegen von Routen auf dem Controller beschrieben. Für andere Systeme informieren Sie sich bitte über das Handbuch zu Ihrem Gerät und/oder Ihrem Betriebssystem.

Für die nachfolgend beschriebene Routing-Konfiguration wird die folgende Netzwerktopologie als Beispiel verwendet:

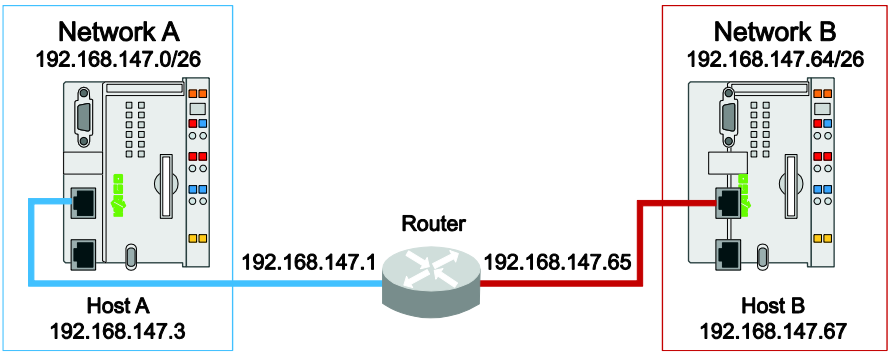

Abbildung 58: Netzwerktopologie, Routing

Host A soll mit Host B Daten austauschen. Hierfür müssen die Daten von Host A über den Router geleitet werden, der die Daten von Netzwerk A in das Netzwerk B weiterleitet. Um das gewünschte Verhalten zu erreichen, wird zunächst Host A mittels einer Route mitgeteilt, dass das Netzwerk B, in dem sich Host B befindet, über den Router (192.168.147.1) erreichbar ist.

Sie können diese Route über Config-Tools aufrufen:

```
/etc/config-tools/config_routing -a static state=enabled dest=192.168.147.64 dest-
mask=255.255.255.192 gw=192.168.147.1 metric=20
```

Alternativ können Sie die Route bei einem Controller über das WBM hinzufügen:

1. Wählen Sie im WBM den Menüpunkt **Networking** > **Routing**.

2. Aktivieren Sie im Bereich „General Routing Configuration“ das Kontrollfeld **Routing enabled entirely**.

Abbildung 59: Routing enabled

3. Aktivieren Sie im Bereich „Static Routes“ das Kontrollfeld **Enabled**.

4. Tragen Sie im Eingabefeld **Destination Address** die Zieladresse des Netzwerks B ein.

5. Tragen Sie im Eingabefeld **Destination Mask** die Netzwerkmaske des Netzwerks B ein.

6. Tragen Sie im Eingabefeld **Gateway Address** die IP-Adresse des Routers ein.

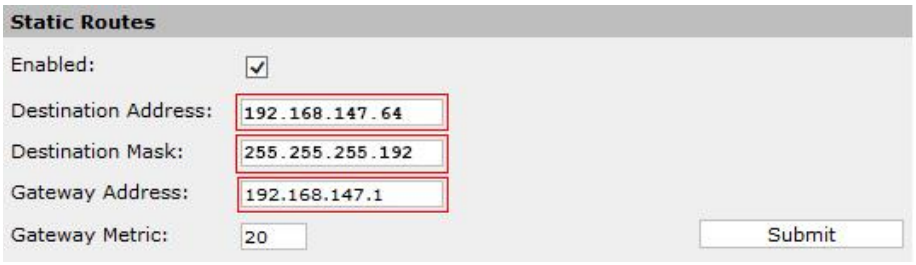

Abbildung 60: Static Routes

7. Speichern Sie die Einstellung mit der Schaltfläche [**Submit**].

8. Wiederholen Sie das Routing für Host B.

Hinweis

Routen müssen in beide Richtungen angelegt werden!
Auf Host B muss ebenfalls eine Route angelegt werden, um Host B mitzuteilen, dass das Netzwerk A über den Router (192.168.147.65) erreichbar ist. Wenn die Route nur in eine Richtung angelegt wird, würden die Daten z. B. von Host A bei Host B ankommen; dieser könnte aber keine Daten zurückschicken!

7.1.4.4 Konfigurationsdateien erstellen

Im Folgenden werden zwei Konfigurationsdateien für ein Host-to-Host- und für ein Site-to-Site-VPN dargestellt. Die beispielhaften Konfigurationen können Sie 1:1 kopieren und für Ihre VPN-Konfiguration übernehmen. Lediglich Ihre spezifischen Werte müssen angepasst werden.

Voraussetzung:

- Zertifikate und Schlüssel sind generiert, siehe Kapitel „Zertifikate erstellen und austauschen“ und „Diffie-Hellman-Parameter erzeugen“.
- Die Zertifikate sind in dem Ordner /etc/certificates/ abgelegt. Der private Schlüssel ist in dem Ordner /etc/certificates/keys/ abgelegt. Beide Pfade müssen Sie auch in der OpenVPN-Konfigurationsdatei angeben, siehe in der Serverkonfiguration „Spezifikation der Ablageorte für Zertifikate und Schlüssel“!
  Informationen hierzu finden Sie im Kapitel „Konfiguration auf den Controller übertragen“.

7.1.4.4.1 Host-to-Host-VPN

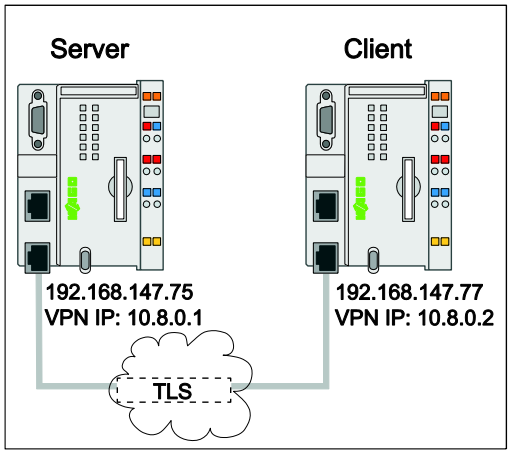

Abbildung 61: Host-to-Host-Verbindung

In der folgenden Beispielkonfiguration wird angenommen, dass der Server unter der IP-Adresse 192.168.147.75 und der Client unter der IP-Adresse 192.168.147.77 erreichbar ist. Ändern Sie diese Werte entsprechend Ihren Gegebenheiten!

Legen Sie die nachfolgenden Konfigurationen für Client und Server für ein Host-to-Host-VPN an.

Serverkonfiguration

```
###################
#    Allgemein    #
###################

# Multi-Client Serverkonfiguration
mode server

##################
#    Netzwerk    #
##################

# Auf welchem Interface soll der OpenVPN-Dienst angeboten werden?
# Spezifizieren Sie hier die IP-Adresse des jeweiligen Interfaces oder lassen
# Sie den Eintrag weg, wenn auf allen Interfaces der Dienst angeboten werden soll.

local 192.168.147.75

# Auf welchem Port soll der OpenVPN-Dienst angeboten werden
# Der Standardport ist 1194, diesen sollten Sie aber vermeiden um automatischen
# Scans im Internet aus dem Wege zu gehen.
port 1194

# UDP als Übertragungsprotokoll nutzen
proto udp

# Wir nutzen den Tunnelmodus, nur OSI-Schicht 3 Protokolle werden übertragen.
dev tun

# Welche Topologie nutzen wir innerhalb des VPN-Netzwerks?
topology subnet

# Clients bekommen aus dem folgenden Adresspool eine IP zugewiesen.
# Diesen Adressbereich dürfen Sie nicht in Ihrem Netzwerk verwenden,
# da es ansonsten zu Problemen führt und das VPN nicht aufgebaut werden kann.

server 10.8.0.0 255.255.255.0

# OpenVPN verschickt regelmäßig Keep-Alive Pakete, mit dem Schlüssel „keepalive"
# Sie können die Frequenz einstellen und ab wie viel Sekunden ein Client/Server
als nicht
# mehr erreichbar gilt.
keepalive 10 120

######################
#    Kryptografie    #
######################

# Spezifikation der Ablageorte für Zertifikate und Schlüssel
# Halten Sie den privaten Schlüssel geheim!
ca /etc/certificates/my_root-ca.crt
cert /etc/certificates/my_openvpn_server.crt
key /etc/certificates/keys/my_openvpn_server.key

# Ablageort der CRL
crl-verify /etc/certificates/my_root-ca_crl.pem

# Diffie-Hellman Parameter
dh /etc/certificates/dh2048.pem

# Zusätzlich zum Zertifikat benötigt der Client einen statischen Schlüssel. Dies
# ist eine Vorsichtsmaßnahme gegen DoS Attacken.
# Den Schlüssel können Sie mit folgendem Befehl erzeugen:
#      openvpn --genkey --secret /etc/openvpn/static.key
tls-auth static.key 0

# Cipher welcher standardmäßig genutzt werden soll. In diesem Fall AES 256
# im CBC (Cipher Block Chaining) Modus
```

```
cipher AES-256-CBC

#########################
#    Minimale Rechte    #
#########################

# Der Dienst sollte mit minimalen Rechten laufen, hier wird die Gruppe und der
Benutzer
# konfiguriert welcher für die Ausführung genutzt wird – dieser Benutzer muss ggf.
vorher
# angelegt werden. Siehe hierzu <Benutzer für OpenVPN anlegen>.
user openvpn
group openvpn

# Spezieller Modus, sodass nach einem Neustart die Verbindung wieder
# aufgebaut werden kann ohne „root"-Berechtigungen
persist-key
persist-tun

#################
#    Logging    #
#################

# Datei, in der der aktuelle Status im Minutenintervall geschrieben wird
status /var/log/openvpn-status.log

# Verbosity des Servers. Für die Fehlersuche kann hier ein höherer Wert gesetzt
# werden, so dass mehr Meldungen gespeichert werden.
verb 4
```

Clientkonfiguration

```
###################
#    Allgemein    #
###################

# Clientkonfiguration
client

#################
#    Netzwerk    #
#################

# Hier muss das Gleiche stehen wie beim Server. In diesem Fall
# „tun", da OpenVPN im Tunnel-Modus betrieben werden soll
dev tun

# Ident zu der Serverkonfiguration, alternativ ist auch TCP möglich
proto udp

# Hier wird der OpenVPN-Server und der Port spezifiziert. Der Port muss
# identisch zu dem auf dem Server konfigurierten sein
remote 192.168.147.75 1194

# Der Client versucht ständig sich mit dem Server zu verbinden. Es gibt
# keinen Timeout ab welchem die Verbindungsversuche abgebrochen werden.
resolv-retry infinite

# Es ist kein Bind auf ein Netzwerkinterface nötig
nobind

#########################
#    Minimale Rechte    #
#########################

# Mit welchem Benutzer und welcher Gruppe der OpenVPN-Client laufen soll.
user openvpn
group openvpn
```

```
# Spezieller Modus, sodass nach einem Neustart des OpenVPN-Dienstes eine
Verbindung auch mit minimalen Rechten aufgebaut
# werden kann.
persist-key
persist-tun

######################
#    Kryptografie    #
######################

# Spezifikation der Ablageorte für Zertifikate und Schlüssel
# Halten Sie den privaten Schlüssel geheim!
ca /etc/certificates/my_root-ca.crt
cert /etc/certificates/my_openvpn_client.crt
key /etc/certificates/keys/my_openvpn_client.key

# Um MitM Angriffe mittels Client Zertifikaten zu verhindern, wird der Client
# angewiesen den Verwendungszweck der Zertifikate zu überprüfen. Achten Sie
# daher beim Erstellen von Zertifikaten darauf, dass Sie die korrekten
# Verwendungen eintragen.
remote-cert-tls server

# Zusätzlich zum Zertifikat braucht der Client einen zusätzlichen Schlüssel.
# Dieser ist auf allen Systemen identisch und dient nur dazu DoS Angriffe zu
# vermeiden.
tls-auth static.key 1

# Standardmäßig eingesetzter Cipher. In diesem Fall AES-256 im CBC (Cipher
# Block Chaining) Modus. Mittels folgenden Befehls können Sie sich weitere
# unterstützte Cipher anzeigen lassen:
#    openvpn --show-ciphers
cipher AES-256-CBC

#################
#    Logging    #
#################

# Datei, in der der aktuelle Status im Minutenintervall geschrieben wird.
status /var/log/openvpn-status.log

# Speicherort für die Log Datei, diese wird immer neu angelegt. Wenn Sie
# ein kontinuierliches Speichern wünschen, ersetzen Sie den Schlüssel „log“
# durch „log-append“.
log /var/log/openvpn.log

# Verbosity des Servers. Für die Fehlersuche kann hier ein höherer Wert gesetzt
# werden, sodass mehr Meldungen gespeichert werden.
verb 4
```

7.1.4.4.2 Site-to-Site-VPN

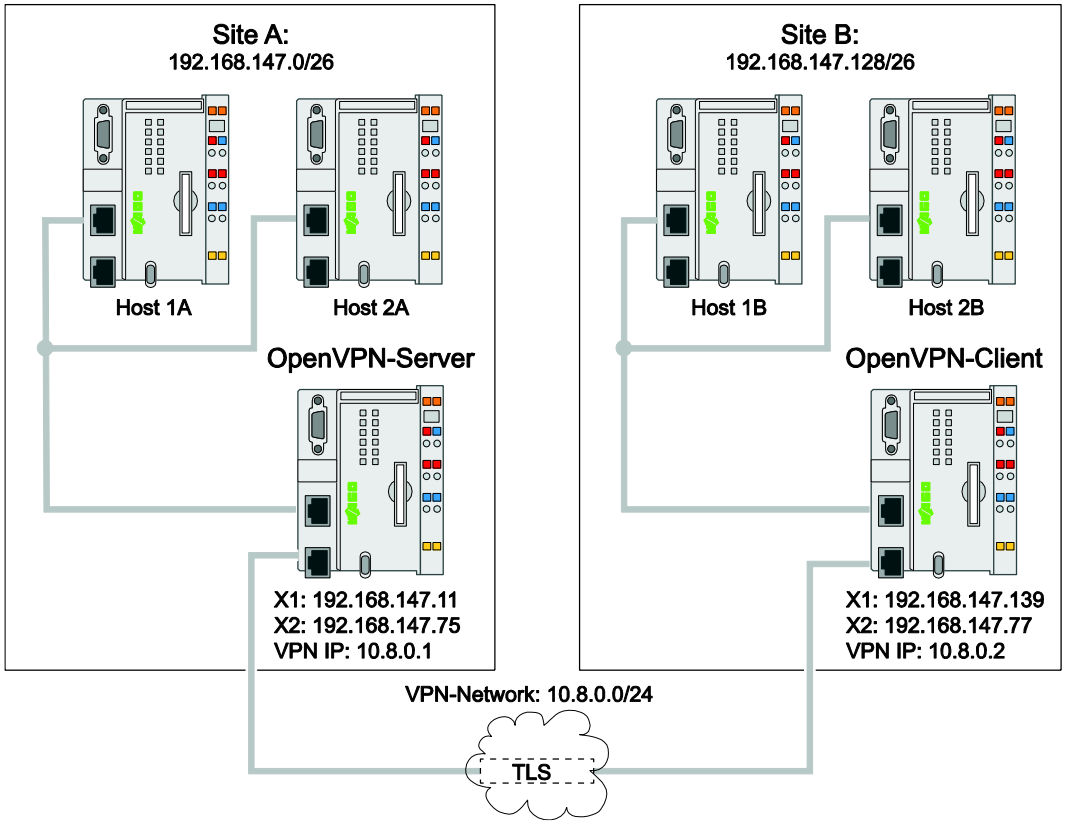

Abbildung 62: Site-to-Site-VPN

Site-to-Site bedeutet, dass zwei oder mehrere Netzwerke miteinander verbunden werden und auf einen Host hinter dem Verbindungspartner (OpenVPN-Server oder -Client) zugegriffen werden kann. Für ein Site-to-Site-VPN erweitern Sie die zuvor aufgeführte Host-to-Host-Konfiguration um die nachfolgend beschriebenen Einstellungen. Es werden an dieser Stelle nur die Unterschiede aufgeführt; die gesamte Konfiguration wird nicht wiederholt.

OpenVPN-Serverkonfiguration

1. Aktivieren Sie auf dem OpenVPN-Server das „IP Forwarding“, damit Sie von den OpenVPN-Clients auf das Netzwerk hinter dem OpenVPN-Server zugreifen können, siehe Kap. „IP Forwarding aktivieren“.

Der OpenVPN-Server dient als Router für das Netzwerk (Site A) und leitet die Netzwerkpakete an die Hosts weiter.

2. Legen Sie auf den Hosts im Netzwerk hinter dem OpenVPN-Server (Site A) eine Route für das VPN-Netzwerk an (siehe Kapitel „Routing konfigurieren“).

Mithilfe der Route wird das VPN-Netzwerk 10.8.0.0/24 über den Host 192.168.147.11 erreichbar.

3. Fügen Sie den folgenden Teil in die Serverkonfiguration unterhalb der Netzwerkeinstellungen ein, um den Zugriff auf das Netzwerk hinter dem OpenVPN-Server zu ermöglichen:

```
# Erstellen Sie ein Verzeichnis, unterhalb des OpenVPN
# Konfigurationsverzeichnisses für die Client Konfiguration(en)
client-config-dir ccd
```

4. Legen Sie eine Konfigurationsdatei für jeden Client unterhalb des zuvor erstellten Verzeichnisses an (siehe Serverkonfiguration „client-config-dir“).

Die Datei muss genauso wie der „commonName“ im Client-Zertifikat benannt sein, siehe Kapitel „Antrag für ein Gerätezertifikat erstellen“.

Hinweis

OpenVPN-Benutzer oder -Gruppe muss Zugriff auf die Datei haben!
Achten Sie darauf, dass der Benutzer „openvpn“ und/oder die Gruppe „openvpn“, die Sie in der Serverkonfiguration für ein Host-to-Host-VPN angelegt haben, lesenden Zugriff auf die Datei hat!

```
# Jeder OpenVPN-Client bekommt eine fixe IP aus dem zuvor konfigurierten IP
# Adress Pool für das VPN.
ifconfig-push 10.8.0.2 255.255.255.0

# Die Route für das Netzwerk hinter dem Server muss dem OpenVPN-Client bekannt
# gemacht werden.
push "route 192.168.147.0 255.255.255.192 10.8.0.1"
```

Mit dieser Konfiguration können OpenVPN-Clients auf das Netzwerk hinter dem OpenVPN-Server zugreifen.

Hinweis

Diese Einstellung ist Client-spezifisch!
Beachten Sie, dass für jeden OpenVPN-Client eine eigene Konfiguration, analog wie zuvor beschrieben, erstellt werden muss. Ersetzen Sie in dieser die IP-Adresse für den jeweiligen Client!

OpenVPN-Client-Konfiguration

1. Aktivieren Sie auf dem OpenVPN-Client das IP Forwarding, damit Sie auf das Netzwerk hinter dem OpenVPN-Client zugreifen können, siehe Kap. „IP Forwarding aktivieren“.

Damit die Hosts hinter dem OpenVPN-Server auf die Hosts hinter dem OpenVPN-Client zugreifen können, muss dem OpenVPN-Server das Netzwerk hinter dem OpenVPN-Client bekannt gemacht werden.

2. Fügen Sie eine Route hinzu, indem Sie die serverseitige Client-Konfiguration um die folgenden Einstellungen erweitern:

```
# Netzwerk hinter dem Client dem OpenVPN-Server bekanntmachen.
iroute 192.168.147.128 255.255.255.192
```

Hinweis

Diese Einstellung ist Client-spezifisch!
Die Route ist spezifisch für jeden Host und das entsprechende Netzwerk hinter dem OpenVPN-Client. Sie müssen die Route daher für jeden Host extra anpassen!

3. Legen Sie auf den Hosts im Netzwerk hinter dem OpenVPN-Client (Site B) eine Route an (siehe Kapitel „Routing konfigurieren“).

Mithilfe dieser Route sollen Netzwerkpakete aus dem Netzwerk A (192.168.147.0/26) über den OpenVPN-Client (192.168.147.139) an Hosts aus dem Netzwerk B weitergeleitet werden.

4. Legen Sie zusätzlich auf den Hosts im Netzwerk hinter dem OpenVPN-Server (Site A) eine Route an (siehe Kapitel „Routing konfigurieren“).

Mit dieser Route soll die Kommunikation mit den Hosts aus dem Netzwerk B (192.168.147.128/26) über den OpenVPN Server (192.168.147.11) ermöglicht werden.

Multi-Client-Konfiguration

Wenn mehrere Clients mit dem OpenVPN-Server oder wenn mehrere Netzwerke (Site C, D usw.) miteinander verbunden sind, müssen die Clients untereinander kommunizieren können. In diesem Fall müssen Sie Ihre OpenVPN-Konfiguration um die nachfolgend beschriebenen Einstellungen erweitern.

1. Fügen Sie den nachfolgenden Konsolenbefehl in Ihre OpenVPN-Konfiguration ein:

```
# Client zu Client Kommunikation erlauben
client-to-client
```

Mit dieser Konfiguration können die Clients untereinander kommunizieren. Damit die Hosts aus den verbundenen Netzwerken ebenfalls miteinander kommunizieren können, müssen Sie entsprechende Routen anlegen.

2. Fügen Sie in der serverseitigen Client-Konfiguration eine Route hinzu:

```
# Netzwerk dem OpenVPN-Server bekanntmachen.
iroute 192.168.147.128 255.255.255.192
```

3. Legen Sie auf den Hosts im Netzwerk hinter dem OpenVPN-Client und -Server jeweils Routen für das Netzwerk an, auf welches Sie zugreifen möchten (siehe Kapitel „Routing konfigurieren“).

Mit diesen Routen können die Hosts aus dem Netzwerk die Datenpakete über den OpenVPN-Client bzw. -Server senden.

7.1.4.5 Konfiguration auf den Controller übertragen

Sie können den Controller konfigurieren, wenn Sie die folgenden Tätigkeiten ausgeführt haben:

- OpenVPN-Dienst auf dem Controller eingerichtet
- Zertifikate und Diffie-Hellman-Schlüssel erzeugt
- OpenVPN-Konfigurationsdateien erstellt

1. Öffnen Sie das WBM und melden Sie sich als Administrator („admin“) an.

2. Navigieren Sie zum Menü **OpenVPN** / **IPsec.**

3. Wählen Sie im Bereich „OpenVPN“ die Konfigurationsdatei aus, die Sie auf das Gerät übertragen wollen.

Abbildung 63: WBM, Konfigurationsdatei auswählen

Hinweis

Namenskonvention und Ablageort der Konfigurationsdatei!
Die Datei muss nicht openvpn.conf heißen, wird aber nach dem Übertragen in „openvpn.conf“ umbenannt und in dem Ordner /etc/openvpn/ abgelegt!

4. Wählen Sie im Bereich „Certificate Upload“ im Eingabefeld **New Certificate** die entsprechenden Zertifikate. (Root-CA-Zertifikat und Zertifikat für Client oder Server). Für den Server können Sie auch die Diffie-Hellman-Parameter laden, die vom Server bereitgestellt werden.

5. Wählen Sie im Bereich „Certificate Upload“ im Eingabefeld **New Private Key** Ihren privaten Schlüssel.

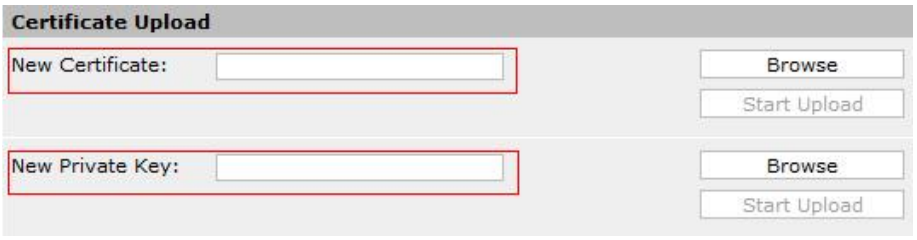

Abbildung 64: WBM, Zertifikate auswählen

Hinweis

Ablageorte der Zertifikate und Schlüssel!
Die Zertifikate werden nach dem Übertragen in dem Ordner /etc/certificates/ abgelegt. Der private Schlüssel wird in dem Ordner /etc/certificates/keys/ abgelegt. Beide Pfade müssen Sie auch in der OpenVPN-Konfiguration angeben!

6. Aktivieren Sie im Bereich „OpenVPN“ das Kontrollfeld **OpenVPN enabled**, damit der OpenVPN-Dienst nach einem Neustart zur Verfügung steht.

Abbildung 65: OpenVPN-Dienst aktivieren

6. Starten Sie den OpenVPN-Dienst mittels Config-Tools:

```
/etc/config-tools/vpncfg ovpn --start
```

Alternativ können Sie das Gerät neu starten.

7.1.5 IPsec

IPsec ist eine Erweiterung des IP-Protokolls, das um die Sicherheitsziele Vertraulichkeit, Authentisierung und Integrität ergänzt wurde. Dadurch ist es möglich, IP-Pakete kryptografisch zu sichern, wodurch eine gesicherte Kommunikation über unsichere Netze realisiert wird. Die Sicherung der Pakete erfolgt auf Layer-3 (siehe OSI-Modell, Vermittlungsschicht). Bei IPsec wird zwischen den folgenden Übertragungsmodi unterschieden:

- **Tunnelmodus:** Im Tunnelmodus wird das komplette IP-Paket (inklusive des IP-Headers) gekapselt und mit einem neuen, zusätzlichen IP-Header versehen. Der Vorteil in diesem Modus, gegenüber dem Transportmodus, liegt in dem Verbergen der Quell- bzw. Zieladresse. Die Identität der eigentlichen Kommunikationspartner bleibt so verborgen. Der Tunnelmodus kann in den Basisszenarien „Host-to-Host“, „Host-to-Site“ und „Site-to-Site“ verwendet werden.
- **Transportmodus:** Im Transportmodus wird kein neuer IP-Header hinzugefügt, sodass die notwendigen Informationen für die Übertragung der Netzwerkpakete aus dem ursprünglichen IP-Header verwendet werden. In diesem Übertragungsmodus ist es nicht möglich verschiedene Netzwerke miteinander zu koppeln. Dieser Modus kann lediglich für das Szenario „Host-to-Host“ verwendet werden.

7.1.5.1 Sicherheitsprotokolle

IPsec stellt die beiden Sicherheitsprotokolle „Authentication Header“ (AH) und „Encapsulating Security Payload“ (ESP) bereit:

- **Authentication Header (AH):** Mit dem „Authentication Header“ (AH) wird die Integrität und Authentizität der zu übertragenen Daten sichergestellt. AH bietet keinen Schutz der Vertraulichkeit; alle Daten werden im Klartext übertragen.
- **Encapsulating Security Payload (ESP):** Durch „Encapsulating Security Payload“ (ESP) wird, analog zum Sicherheitsprotokoll AH, die Integrität und die Authentizität sichergestellt. Im Unterschied zu AH wird zusätzlich die Vertraulichkeit durch Verschlüsselung der zu übertragenden Daten gewährleistet.

Die Sicherheitsprotokolle ESP und AH können, je nach Sicherheitsanforderungen, getrennt oder gemeinsam verwendet werden. Die Verschlüsselungs- und Authentisierungsverfahren können entsprechend konfiguriert werden, siehe Kapitel „Erweiterte Sicherheitsmaßnahmen“ > … > „Konfigurationsdateien erstellen“.

7.1.5.2 Internet Key Exchange Protokoll (IKE)

Das IKE-Protokoll ist für den Austausch von Verbindungsparametern zuständig, die für den Aufbau eines gesicherten Kommunikationskanals zwischen den IPsec-Endpunkten benötigt werden. Es werden unter anderem die folgenden Parameter ausgetauscht:

- Art der gesicherten Übertragung
- Verschlüsselungsalgorithmus
- Kryptografische Schlüssel
- Dauer der Gültigkeit der kryptografischen Schlüssel

In der vorliegenden Dokumentation wird in den Testszenarien ausschließlich IKEv2 betrachtet (siehe Kapitel „Host-to-Host-VPN und Kapitel Site-to-Site-VPN).

7.1.5.3 Security Policy Database (SPD)

In der „Security Policy Database“ sind Regelsätze (Security Policy) definiert, die den Umgang mit den ein- und ausgehenden Datenpaketen spezifiziert. Dabei wird zwischen den drei Grundfunktionen unterschieden:

- Paket wird sofort verworfen (DISCARD).
- Paket wird ohne Änderung weitergeleitet (BYPASS).
- Paket wird durch IPsec verarbeitet (PROTECT).

Der Umgang mit den Datenpaketen erfolgt über bestimmte Auswahlkriterien (Selektoren), die in der Konfigurationsdatei „ipsec.conf“ aufgeführt sind. Diese sind zum Beispiel:

- Quell- oder Ziel-IP-Adresse
- Transport-Layer-Protokoll: TCP/UDP
- Identitätsname des Zertifikats

7.1.5.4 Security Association (SA) und Security Parameter Index (SPI)

Damit die IPsec-Endpunkte die kryptografisch gesicherten Netzwerkpakete gemäß Security Policy verarbeiten können (Entschlüsselung/Integritätsprüfung), müssen die notwendigen Informationen bzw. Parameter bereitgestellt werden. Diese notwendigen Informationen werden in einer Datenbank den jeweiligen IPsec-Endpunkten zur Verfügung gestellt, um den zusätzlichen Daten-Overhead pro Netzwerkpaket möglichst gering zu halten.

Eine eindeutige Zuordnung auf die zu verwendenden kryptografischen Parameter und Algorithmen erfolgt innerhalb der Datenbank mithilfe

- des „Security Parameter Index“ (SPI), der für jedes IPsec-Paket zusätzlich übertragen wird,
- der übertragenden IP-Zieladresse und
- dem verwendeten Sicherheitsprotokoll (ESP/AH).

Diese Zuordnung wird als Sicherheitsvereinbarung bzw. „Security Association“ (SA) bezeichnet. Sie regelt die Kommunikation zwischen den IPsec-Endpunkten.

Da die IPsec-Endpunkte sowohl senden als auch empfangen können, wird je IPsec-Endpunkt eine SA pro Kommunikationsrichtung benötigt. Die Verwaltung der ausgehandelten SAs erfolgt in der „Security Association Database“ (SAD), in der alle SAs aufgeführt sind. Die Aushandlung der SAs erfolgt über das „Internet Key Exchange Protokoll“ (IKE).

Für die Überprüfung der Authentizität der IPsec-Endpunkte, während des Aufbaus einer SA, werden unter anderem die folgenden Authentisierungsverfahren bereitgestellt:

- PSK – Pre Shared Keys
- X.509-Zertifikate

Bei der Identifizierung der VPN-Gegenstellen mittels Zertifikat ist eine zusätzliche Angabe in Form eines „Identifiers“ notwendig. Der Identifier kann z. B. in Form einer IP-Adresse, eines DNS-Namen (FQDN) oder einer E-Mail-Adresse (FQUN) erfolgen.

Hinweis

Führen Sie den Identifier bei strongSwan entweder im „Subject Alternative Name“ und/oder im Common Name (CN) auf!
Es wird empfohlen, den Identifier (z.B. DNS-Name oder IP-Adresse) im Feld „Subject Alternative Name“ des Zertifikats aufzuführen. Für weitere Informationen bezüglich der Zertifikate bei strongSwan siehe: https://wiki.strongswan.org/projects/strongswan/wiki/SimpleCA!

Um eine erfolgreiche Verbindung über IPSec aufzubauen, müssen die Teilnehmer folgende Informationen besitzen:

- IP-Adresse der Gegenstelle
- Subnetzmaske des Netzwerks
- Tunnelname
- Authentisierungsverfahren
- Verwendetes Verschlüsselungs- und Authentisierungsverfahren
- Schlüssel der kryptografischen Verfahren

7.1.5.5 Konfigurationsdateien erstellen

Im Folgenden werden zwei Konfigurationsdateien für eine Host-to-Host- und für eine Site-to-Site-Verbindung dargestellt. Die beispielhaften Konfigurationen können Sie 1:1 kopieren und für Ihre VPN-Konfiguration übernehmen. Lediglich Ihre spezifischen Werte müssen angepasst werden. Es ist möglich, innerhalb der Konfigurationsdateien die ESP- bzw. AH-Verfahren explizit anzugeben.

Hinweis

Unterstützte Cipher-Suites bei der IPsec-Applikation strongSwan!
Eine Übersicht der unterstützten Cipher-Suites bei der IPsec-Applikation strongSwan erhalten Sie unter dem folgenden Link: https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites“.

7.1.5.5.1 Host-to-Host-VPN

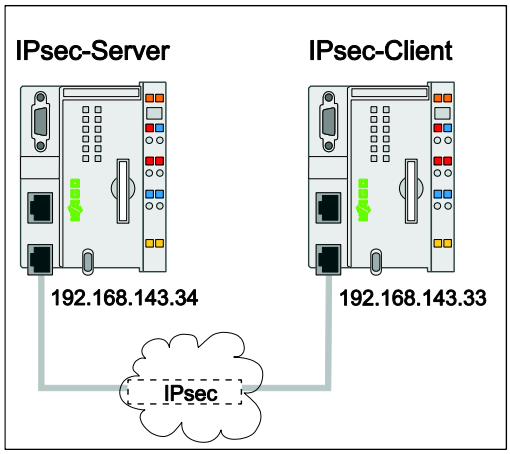

Abbildung 66: Host-to-Host-Verbindung, IPsec

In der folgenden Beispielkonfiguration wird angenommen, dass der IPsec-Server unter der IP Adresse 192.168.143.34 und der IPsec-Client unter der IP-Adresse 192.168.143.33 erreichbar ist. Ändern Sie diese Werte entsprechend Ihrer Gegebenheiten!

Zusätzlich zu der Konfigurationsdatei „ipsec.conf“ muss auch eine Datei „ipsec.secrets“ erstellt werden, in welcher das Authentisierungsgeheimnis aufgeführt wird. Beide Dateien finden Sie in den nachfolgenden Beispielkonfigurationen. Im Falle einer zertifikatsbasierten Authentisierung wird der „Private Key“ aufgeführt. Beim PSK-Verfahren wird der gemeinsame Schlüssel „Shared Secret“ aufgeführt.

Transportmodus mit X.509 Zertifikaten

Konfiguration für IPsec-Client

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
   ikelifetime=60m
   keylife=20m
   rekeymargin=3m
   keyingtries=1
   mobike=no
   keyexchange=ikev2
   ike=aes128-sha256-modp2048
   esp=aes128-sha256-modp2048

conn host-host
   left=192.168.143.33
   leftcert=PFC1Cert.pem
   leftid=@PFC1.wago.org
   leftfirewall=yes
   right=192.168.143.34
   rightid=@PFC2.wago.org
   type=transport
   auto=start

# /etc/ipsec.secrets - strongSwan IPsec secrets file
: RSA PFC1Cert.pem
```

Konfiguration für IPsec-Server

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
   ikelifetime=60m
   keylife=20m
   rekeymargin=3m
   keyingtries=1
   mobike=no
   keyexchange=ikev2
   ike=aes128-sha256-modp2048
   esp=aes128-sha256-modp2048

conn host-host
   left=192.168.143.34
   leftcert=PFC2Cert.pem
   leftid=@PFC2.wago.org
   leftfirewall=yes
   right=192.168.143.33
   rightid=@PFC1.wago.org
   type=transport
   auto=start

# /etc/ipsec.secrets - strongSwan IPsec secrets file
: RSA PFC2Cert.pem
```

Hinweis

Beachten Sie die Informationen zu den Konfigurationsparametern!
Die Beschreibung der einzelnen Konfigurationsparameter kann auf der strongSwan-Hompage eingesehen werden:
https://wiki.strongswan.org/projects/strongswan/wiki/IpsecConf!

Tunnelmodus mit X.509-Zertifikaten

Hinweis

Für den Tunnelmodus sind nur minimale Änderungen notwendig!
Für den Tunnelmodus müssen Sie dem Parameter „type“ in der Konfigurationsdatei „ipsec.conf“ den Wert „tunnel“ zuweisen. Alternativ kann der Parameter „type“ entfernt werden, da der Standardmodus dem Wert „tunnel“ entspricht.

7.1.5.5.2 Site-to-Site-VPN

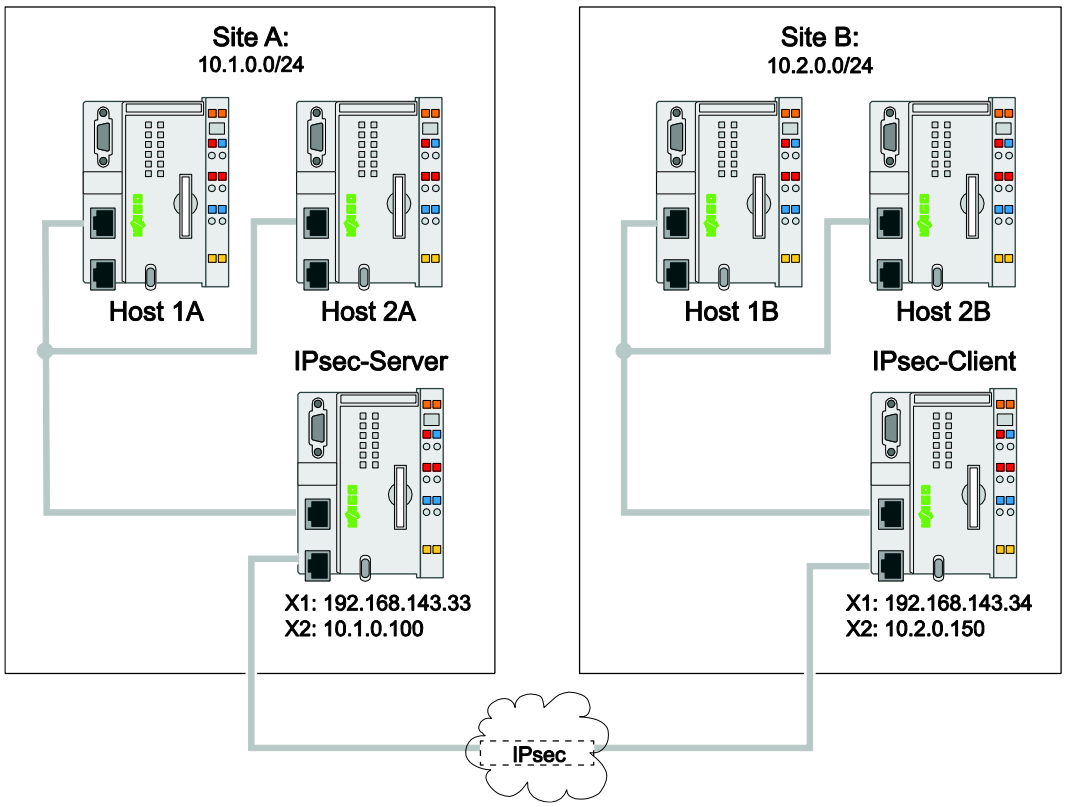

Abbildung 67: Site-to-Site-VPN, IPsec

Site-to-Site-VPN bedeutet, dass auch auf Systeme hinter dem Verbindungspartner (IPsec-Server oder IPsec-Client) zugegriffen werden kann. Für ein Site-to-Site-VPN können Sie die nachfolgende Beispielkonfiguration übernehmen und Ihre spezifischen Werte entsprechend anpassen. Die Datei „ipsec.secret“ kann aus dem vorherigen Beispiel übernommen werden.

Konfiguration für IPsec-Client

```
# /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
   ikelifetime=60m
   keylife=20m
   rekeymargin=3m
   keyingtries=1
   keyexchange=ikev2
   mobike=no
   ike=aes128-sha256-modp2048
   esp=aes128-sha256-modp2048
conn net-net
   left=192.168.143.33
   leftcert=PFC1Cert.pem
   leftid=@PFC1.wago.org
   leftsubnet=10.1.0.0/24
   leftfirewall=yes
   right=192.168.143.34
   rightid=@PFC2.wago.org
   rightsubnet=10.2.0.0/24
   auto=start
```

Konfiguration für IPsec-Server

```
  # /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
   ikelifetime=60m
   keylife=20m
   rekeymargin=3m
   keyingtries=1
   keyexchange=ikev2
   mobike=no
   ike=aes128-sha256-modp2048
   esp=aes128-sha256-modp2048

conn net-net
   left=192.168.143.34
   leftcert=PFC2Cert.pem
   leftid=@PFC2.wago.org
   leftsubnet=10.2.0.0/24
   leftfirewall=yes
   right=192.168.143.33
   rightid=@PFC2.wago.org
   rightsubnet=10.1.0.0/24
   auto=add
```

Hinweis

Beachten Sie die Informationen zu den Konfigurationsparametern!
Die Beschreibung der einzelnen Konfigurationsparameter kann auf der strongSwan-Hompage eingesehen werden:
https://wiki.strongswan.org/projects/strongswan/wiki/IpsecConf!

Zugriff der Clients (Site A) auf ein Netzwerk hinter dem IPsec-Client (Site B)

1. Aktivieren Sie auf dem IPsec-Server und auf dem IPsec-Client das „IP Forwarding“, damit der Zugriff auf das dahinter liegende Netzwerk möglich wird. Siehe Kapitel „Zusätzliche Sicherheitsmaßnahmen“ > … > „IP Forwarding aktivieren“.

Zusätzlich muss auf den Systemen im Netzwerk hinter dem IPsec-Server eine Route erstellt werden, sodass die Pakete für die Netzwerk-Clients (Site A) an den IPsec-Server weitergeleitet werden. Der IPsec-Server leitet die Pakete dann an den entsprechenden IPsec-Client weiter.

Sie können die Route über das WBM hinzufügen:

2. Wählen Sie im WBM den Menüpunkt **Networking** > **Routing**.

3. Tragen Sie im Bereich „Static Routes“ im Eingabefeld **Gateway Address** die IP-Adresse Ihres Servers ein.

4. Speichern Sie die Einstellung mit der Schaltfläche [**Submit**].

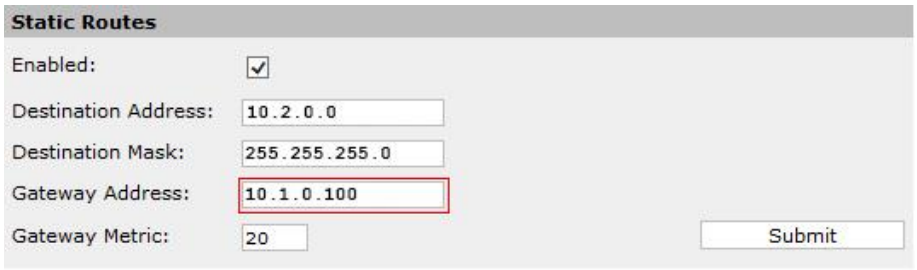

Abbildung 68: Static Routes, Zugriff der Clients auf ein Netzwerk hinter dem IPsec-Client

Zugriff der Clients (Site B) auf ein Netzwerk hinter dem IPsec-Server (Site A)

Auf den Systemen im Netzwerk hinter dem IPsec-Cient muss eine Route erstellt werden, sodass die Pakete an den vorgeschalteten IPsec-Client weitergeleitet werden. Der IPsec-Client leitet die Pakete dann als Router an den IPsec-Server weiter.

Sie können die Route über das WBM hinzufügen:

5. Wählen Sie im WBM den Menüpunkt **Networking** > **Routing**.

6. Tragen Sie im Bereich „Static Routes“ im Eingabefeld **Gateway Address** die IP-Adresse Ihres Servers ein.

7. Speichern Sie die Einstellung mit der Schaltfläche [**Submit**].

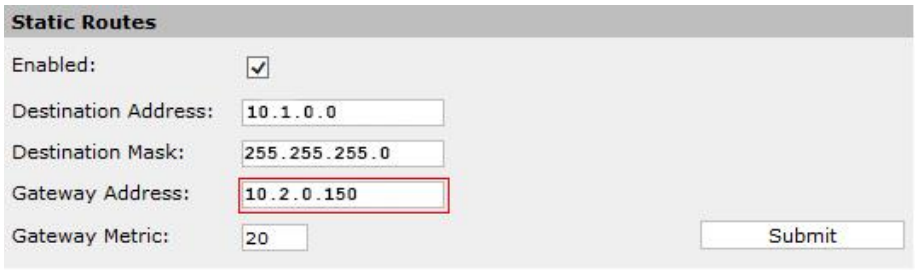

Abbildung 69: Static Routes , Zugriff der Clients auf ein Netzwerk hinter dem IPsec-Server

7.1.5.6 Firewall konfigurieren

Hinweis

In der Firewall muss IPsec explizit für X1 und X2 freigegeben werden!
Sie müssen für beide IPsec-Gegenstellen Ausnahmeregeln für die IPsec-Verbindung erstellen, da die Firewall das IPsec-VPN nicht automatisch über die Schnittstelle X1 bzw. X2 freigibt. Es existieren lediglich vordefinierte IPsec-Ausnahmeregeln für das Modem-Interface (wwan)!

Das Hinzufügen der IPsec-Ausnahmeregeln für die Schnittstelle X1 erfolgt über die folgenden Schritte (analog auch für Schnittstelle X2):

1. Verbinden Sie sich mit der Linux®-Konsole des Controllers über SSH oder die serielle Schnittstelle.

2. Editieren Sie die Datei „params.xml“ unter dem Pfad /etc/firewall/, z. B. mithilfe der Linux®-Applikation „nano“:

```
nano /etc/firewall/params.xml
```

In der nachfolgenden Abbildung sehen Sie die modifizierte Datei „params.xml“, wie sie für den Aufbau einer IPsec-Verbindung über die Schnittstelle X1 notwendig ist:

```
<?xml version="1.0" encoding="utf-8"?>
<firewall xmlns="http://www.wago.com/security/firewall"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://www.wago.com/security/firewall params.xsd">

    <parameters>
        <interfaces>
            <!-- In case any names ('name' and 'rname' tags) should be changed
                 please amend validate_if.sh script accordingly! -->
            <interface name="X1"  rname="br0"   ethernet="yes" ipsec_srv="yes"/>
            <interface name="X2"  rname="br1"   ethernet="yes"/>
            <interface name="WAN" rname="wwan0" ethernet="yes" ipsec_srv="yes"/>
            <interface name="VPN" rname="wwan0" ethernet="no"  ipsec="yes"/>
            <interface name="VPN" rname="tun+"  ethernet="no" />
            <interface name="VPN" rname="tap+"  ethernet="yes"/>
            <interface name="VPN"  rname="br0"   ethernet="no" ipsec="yes"/>
        </interfaces>
    </parameters>

</firewall>
```

Beschreibung des Parameters „ipsec_srv="yes“

Mithilfe des zusätzlichen Parameters „ipsec_srv="yes"“ werden beim Neustart der Firewall die folgenden persistenten Ausnahmebehandlungen für das Interface X1 (br0) automatisch hinzugefügt:

- Freischaltung der Ports 500/UDP (IKE) und 4500/UDP (NAT)
- Freischaltung des IPsec-Sicherheitsprotokolls ESP

Sie können sich diese Regeln mit dem Linux®-Befehl „iptables-save“ anzeigen lassen:

```
…
-A in_generic -i br0 -p udp -m udp --dport 500 -j ACCEPT
-A in_generic -i br0 -p udp -m udp --dport 4500 -j ACCEPT
-A in_generic -i br0 -p esp -j ACCEPT
…
```

Beschreibung des XML-Tags „<interface name="VPN" rname="br0" ethernet="no" ipsec="yes"/>“

Das zusätzliche XML-Tag „<interface name="VPN" rname="br0" ethernet="no" ipsec="yes"/>“ fügt nach dem Neustart der Firewall Ausnahmeregeln für die Dienste hinzu, die über den IPsec-Tunnel erreicht werden können. Das bezieht sich ausschließlich auf die erreichbaren Dienste über das X1-Interface (br0) innerhalb des IPsec-Tunnels und nicht auf die erreichbaren Dienste außerhalb des Tunnels. Diese Dienste sind z.B.:

- FTP/FTPS
- SSH
- HTTPS

Sie können sich diese Ausnahmeregeln mit dem Linux®-Befehl „iptables-save“ anzeigen lassen: Am Beispiel des HTTPS-Dienstes haben sie die folgende Form:

```
-A in_https -i br0 -p tcp -m policy --dir in --pol ipsec --proto esp --mode tunnel
-m tcp --dport 443 -j ACCEPT
```

Bitte beachten Sie zusätzlich die Hinweise bezüglich der Firewall-Konfiguration für den Controller, siehe Kapitel „Hardening“ > „Firewall konfigurieren“.

Hinweis

Beachten Sie die Firewall-Einstellungen bei dem VPN-Szenario „Site-to-Site“!
Bei dem VPN-Szenario „Site-to-Site“ und aktivierter Firewall, können alle aktiven Dienste der nachgelagerten Client-Systeme über die freigeschalteten Ports 500 bzw. 4500 erreicht werden, sofern der Tunnel erfolgreich aufgebaut werden konnte.

Implementieren Sie zusätzliche Maßnahmen, um die Zugriffe auf sensible Client-Systeme zu unterbinden. Dies kann z. B. durch zusätzliche Firewall-Konfigurationen erfolgen (siehe Kapitel „Hardening“ > … > „White List für Netzwerke anlegen“) oder durch eine Separierung des Netzwerks. Hierzu finden Sie weitere Informationen im White Paper „IT Sicherheit in Produktionsanlagen“, welches Sie im Download-Bereich unter https://www.wago.com anfordern können.

7.1.5.7 Konfiguration auf den Controller übertragen

Der Controller wird konfiguriert, wenn Sie die folgenden Tätigkeiten durchgeführt haben:

- IPsec-Dienst auf dem Controller eingerichtet
- Zertifikate erzeugt
- IPsec-Konfigurationsdateien (ipsec.conf und ipsec.secret) erstellt

1. Öffnen Sie das WBM und melden Sie sich als Administrator („admin“) an.
2. Navigieren Sie zum Menü **OpenVPN/IPsec.**
3. Wählen Sie im Bereich „IPsec“ die Konfigurationsdateien aus, die Sie auf das Gerät übertragen wollen.

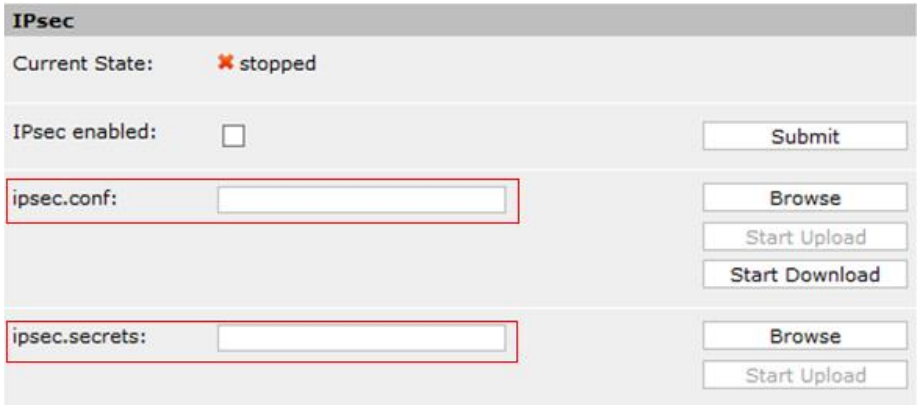

Abbildung 70: WBM, Konfigurationsdateien für IPsec auswählen

4. Wählen Sie im Bereich „Certificate Upload“ im Eingabefeld **New Certificate** die entsprechenden Zertifikate. (Root-CA-Zertifikat und Zertifikat für Client oder Server).
5. Wählen Sie im Eingabefeld **New Private Key** Ihren privaten Schlüssel.

Abbildung 71: WBM, Zertifikate auswählen

Hinweis

Ablageorte der Zertifikate und Schlüssel!
Die Zertifikate werden nach Erstellung in dem Ordner /etc/certificates/ abgelegt. Der private Schlüssel wird in dem Ordner /etc/certificates/keys/ abgelegt.

6. Aktivieren Sie im Bereich „IPsec“ das Kontrollfeld **IPsec enabled**, damit der IPsec-Dienst nach einem Neustart zur Verfügung steht.

Abbildung 72: IPsec-Dienst aktivieren

7. Bestätigen Sie Ihre Eingabe über die Schaltfläche [**Submit**].
8. Navigieren Sie zum Menü **Administrator** > **Reboot**.
9. Betätigen Sie die Schaltfläche [**Reboot**].

Anschließend startet der Controller neu und die IPsec-Applikation wird gestartet.

7.2 Port-Authentisierung gemäß IEEE 802.1X

Die Controller PFCX00 unterstützen unter anderem einen Mechanismus, der es erlaubt, die Controller als Supplikanten für die Port-Authentisierung gemäß IEEE 802.1X zu betreiben.

Diese Funktionalität wird durch die Linux®-Applikation „wpa_supplicant“ bereitgestellt. Es werden zwei Verfahren für eine Authentisierung des Supplikanten verwendet:

- **Port-Authentisierung mittels Benutzername und Kennwort**
  Die Authentisierung erfolgt über die Angabe von Anmeldedaten in Form von Benutzername und Kennwort, die innerhalb der Konfigurationsdatei (siehe nachfolgendes Kapitel) angegeben werden müssen. Dieses Verfahren wird mit dem Authentifizierungsprotokoll EAP-MD5 realisiert.
- **Port-Authentisierung mittels Zertifikat**
  Alternativ ist es möglich, dem Supplikanten ein „Client-Zertifikat“ zu hinterlegen, welches zur Authentisierung verwendet wird. Dieses Verfahren wird mit dem erweiterbaren Authentifizierungsprotokoll EAP-TLS realisiert.

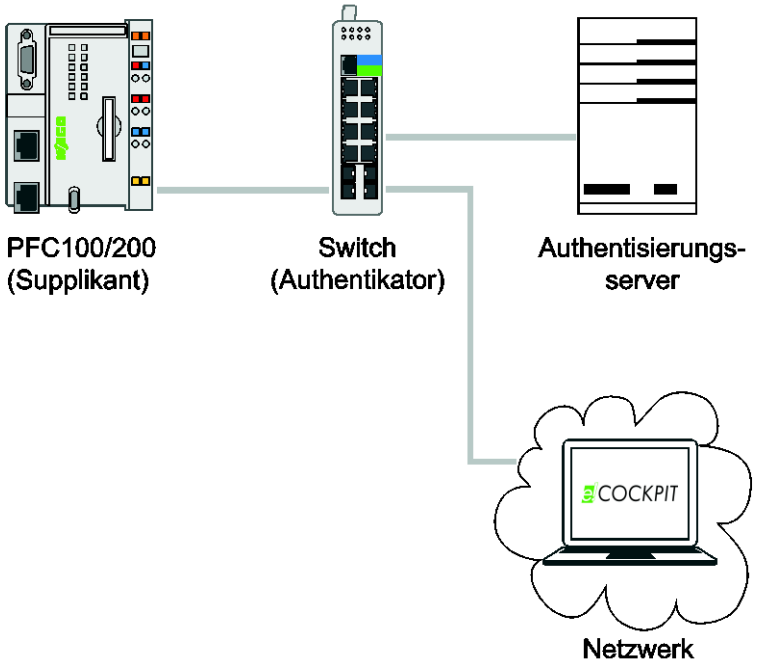

Abbildung 73: Grundprinzip der Port-Authentisierung

Die in der Abbildung „Grundprinzip der Port-Authentisierung“ dargestellte Netzwerkarchitektur veranschaulicht die grundsätzliche Port-Authentisierung gemäß IEEE 802.1X:

Der Controller (Supplikant) ist mit dem Switch (Authentikator) verbunden; dabei muss beim Switch die Port-Authentisierung aktiv geschaltet sein.

Über den Switch sind sowohl Authentisierungsserver (z. B. RADIUS-Server) als auch das Netzwerk verbunden, aus dem der Controller über die Applikation ***e!****Cockpit* konfiguriert werden soll.

Hinweis

Ohne Authentisierung ist keine Kommunikation mit dem Netzwerk möglich!
Wenn der Controller sich nicht bei dem Authentisierungsserver authentisiert hat, ist es nicht möglich, den Controller über das Netzwerk zu erreichen. Ebenso hat der Controller keine Möglichkeit die Teilnehmer des Netzwerks zu erreichen!

Die Authentisierung erfolgt durch den Switch, der die Anfrage des nicht-authentisierten Controllers an den Authentisierungsserver weiterleitet. Sofern die Authentisierung beim Authentisierungsserver erfolgreich war, schaltet der Switch den Zugang zum Netzwerk für den Controller frei; andernfalls wird der Zugriff verweigert.

Der Switch tauscht die Authentisierungsdaten mit dem Controller über das Extensible Authentication Protocol over LANs (EAPOL) aus. Die Authentisierungsdaten zwischen Switch und Authentisierungsserver werden, im Falle eines RADIUS-Servers, in RADIUS-Paketen gekapselten EAP-Paketen ausgetauscht.

Hinweis

Das RADIUS-Protokoll muss vom Switch unterstützt werden!
Die Kommunikation zwischen Switch und Authentisierungsserver erfolgt über ein spezifisches Authentisierungsprotokoll, wie z. B. RADIUS. Der Switch transformiert die EAP-Pakete des Supplikanten in das RADIUS-Protokoll, bzw. die RADIUS-Pakete vom Authentisierungsserver in das EAP-Protokoll. Voraussetzung dafür ist, dass der Switch dieses Protokoll unterstützt.

7.2.1 Port-Authentisierung mittels Benutzername und Kennwort gemäß EAP-MD5

Der Kern dieses Verfahrens ist das Challenge Handshake Authentication Protocol (CHAP) in Kombination mit dem MD5-Hash-Algorithmus.

Der Supplikant baut zunächst eine EAPOL-Verbindung mit dem Switch auf. Sobald die Verbindung aufgebaut ist, sendet der Authentisierungsserver ein „Challenge Request“ (Zufallswert) an den Supplikanten. Daraufhin bildet der Supplikant einen MD5-Hash-Wert über die Eingabeparameter „Challenge“ (Zufallswert des Authentisierungsservers) und „Passwort“ des Supplikanten. Den berechneten Hash-Wert sendet der Supplikant als „Challenge Response“ an den Authentisierungsserver zurück.

Da der Authentisierungsserver sowohl das Passwort des Supplikanten als auch die gesendete Challenge kennt, erzeugt der Server ebenfalls einen MD5-Hash-Wert aus den beiden Eingabeparametern und vergleicht seinen erzeugten Hash-Wert mit dem Wert des Supplikanten. Sofern beide Werte identisch sind, hat sich der Supplikant erfolgreich authentisiert.

Die folgende Abbildung veranschaulicht das Prinzip der Port-Authentisierung:

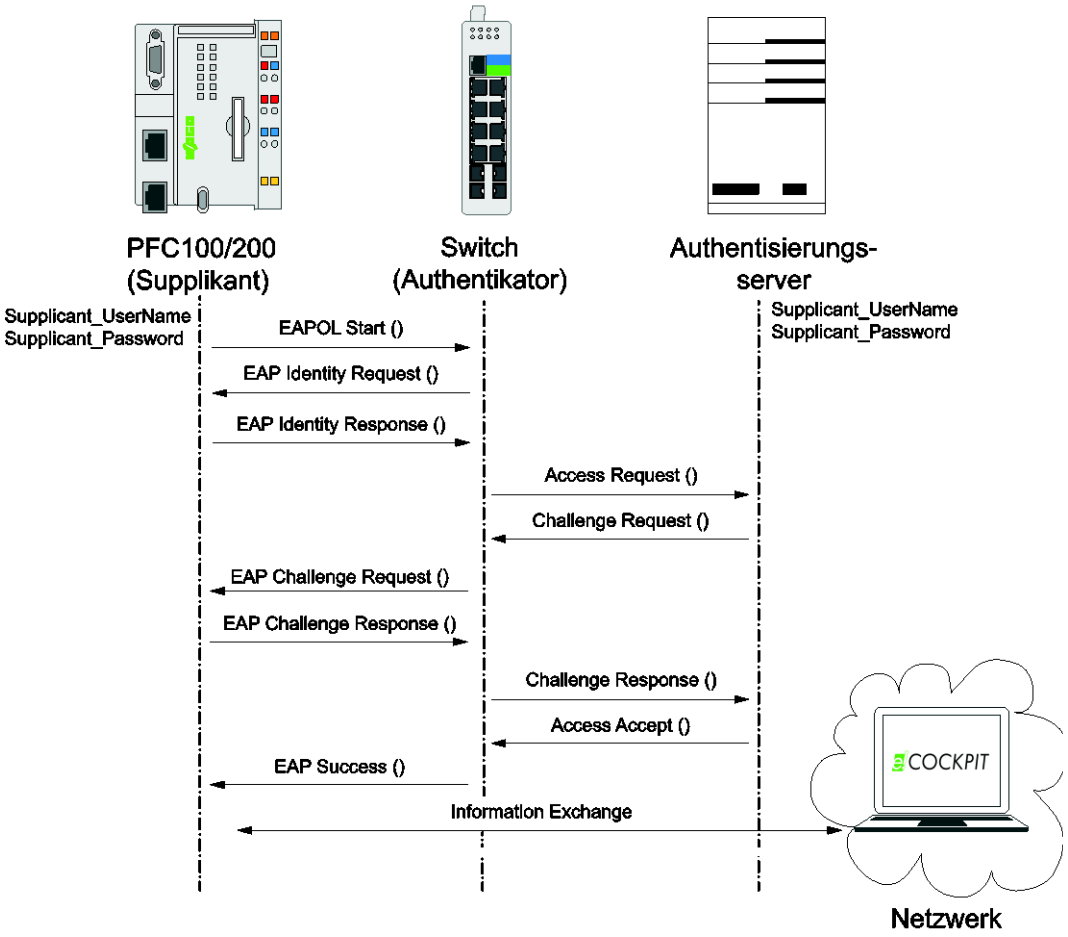

Abbildung 74: Ablauf der Port-Authentisierung gemäß EAP-MD5

1. Sobald die Applikation „wpa_supplikant“ auf dem Controller ausgeführt wird, sendet der Controller die initiale Nachricht „EAPOL Start“ an den Switch.
2. Der Switch sendet anschließend die Anforderung „EAP Identity Request“ an den Controller, wodurch dieser aufgefordert wird, sich zu identifizieren.
3. Anschließend sendet der Controller seine Identität („Supplicant_UserName“) an den Authentikator, die an den Authentisierungsserver weitergeleitet wird.
4. Der Authentisierungsserver prüft die Identität, indem er einen Abgleich mit seiner Benutzerdatenbank macht.
5. Sofern die Identität bekannt ist, sendet der Authentisierungsserver eine Zufallszahl „Challenge-Request“ an den Controller, die für die Authentisierung benötigt wird.
6. Nach Erhalt der Nachricht „Challenge-Request“, sendet der Controller seine Authentisierungsdaten als „Challenge Response“ zurück an den Authentisierungsserver (MD5 Hash-Wert über Zufallszahl des Servers und des Supplikantenpassworts).
7. Daraufhin wird die Nachricht „Challenge Response“ vom Authentisierungsserver geprüft.
8. Wenn der Challenge-Response-Mechanismus erfolgreich war, sendet der Authentisierungsserver die Nachricht „Access Accept“ an den Controller.
9. Der Switch gewährt so Zugang zu dem Netzwerk und dem Teilnehmer wird die erfolgreiche Authentisierung bestätigt.
10. Der Controller kann somit auf das Netzwerk zugreifen bzw. von den Teilnehmern des Netzwerks erreicht werden.

7.2.1.1 EAP-MD5-Port-Authentisierung einrichten

1. Editieren Sie die Konfigurationsdatei /etc/wpa_supplicant.conf des Controllers wie folgt:

```
network={
          key_mgmt=IEEE8021X
          eap=MD5
          identity="Supplicant_Name"
          password="Supplicant_Password"
          eapol_flags=0
}
```

2. Konfigurieren Sie Switch und Authentisierungsserver (z. B. RADIUS-Server).
3. Starten, bzw. testen Sie die EAP-TLS-Authentisierung auf dem Controller mit dem folgenden Befehl:

```
wpa_supplicant -dd -Dwired -ibr0 -c/etc/wpa_supplicant.conf
```

Tabelle 10: Beschreibung der Parameter

Parameter	Bedeutung
-dd	Debug-Modus
-D	Treiber, der verwendet werden soll (wired: kabelgebunden)
-i	Interface der Geräte (br0: ETHERNET-Interface X1; br1: ETHERNET-Interface X2)
-c	Pfad zur WPA-Supplicant-Konfigurationsdatei (wpa_supplicant.conf)

Für weitere Informationen bezüglich der Parameter/Konfiguration siehe:
https://linux.die.net/man/8/wpa_supplicant

Information

Port-Authentisierung mittels Zertifikat ist sicherer!
Nutzen Sie, wenn möglich, die zertifikatbasierte Authentisierung (EAP-TLS), da hiermit sowohl die Authentizität des Clients und des Servers als auch die Integrität der Kommunikation durch zeitgemäße kryptografische Verfahren gesichert werden kann:

- Beidseitige Authentisierung,
- integritätsgesicherte Aushandlung von Verschlüsselungsverfahren,
- sicherer Schlüsselaustausch zwischen zwei Endpunkten.

7.2.2 Port-Authentisierung mittels Zertifikaten (EAP-TLS)

Bei der zertifikatsbasierten Port-Authentisierung mittels EAP-TLS benötigen sowohl Authentisierungsserver als auch Supplikant ein gültiges und vertrauenswürdiges digitales Zertifikat (X.509) von einer Zertifizierungsstelle (CA). Dafür wird eine „Public Key Infrastructure“ (PKI) vorausgesetzt. Das CA-Zertifikat bildet den „Vertrauensanker“ bei der Authentisierung, sodass die Vertrauenswürdigkeit (Authentizität) der Kommunikationsteilnehmer sichergestellt werden kann. Die ausgestellten digitalen Zertifikate der Zertifizierungsstelle (CA) für den Supplikanten und den Authentisierungsserver werden für die gegenseitige Authentisierung verwendet. Die Sicherung der Kommunikation erfolgt über das etablierte TLS-Protokoll. Der Zugang zum Netzwerk wird gewährt, wenn sowohl der Server als auch der Supplikant sich gegenseitig authentisiert haben. Die Angabe eines Passworts, wie beim EAP-MD5-Verfahren, ist in diesem Fall nicht mehr erforderlich (siehe Kapitel „Port-Authentisierung mittels Benutzername und Kennwort gemäß EAP-MD5“)

Hinweis

Es müssen zunächst Zertifikate und Schlüssel erstellt werden!
Es müssen zunächst Zertifikate und Schlüssel für den PFC und den Authentisierungsserver erstellt werden. Hinweise zur Erstellung und Einrichtung von Zertifikaten finden Sie im Kapitel „Zertifikate erstellen und austauschen“.

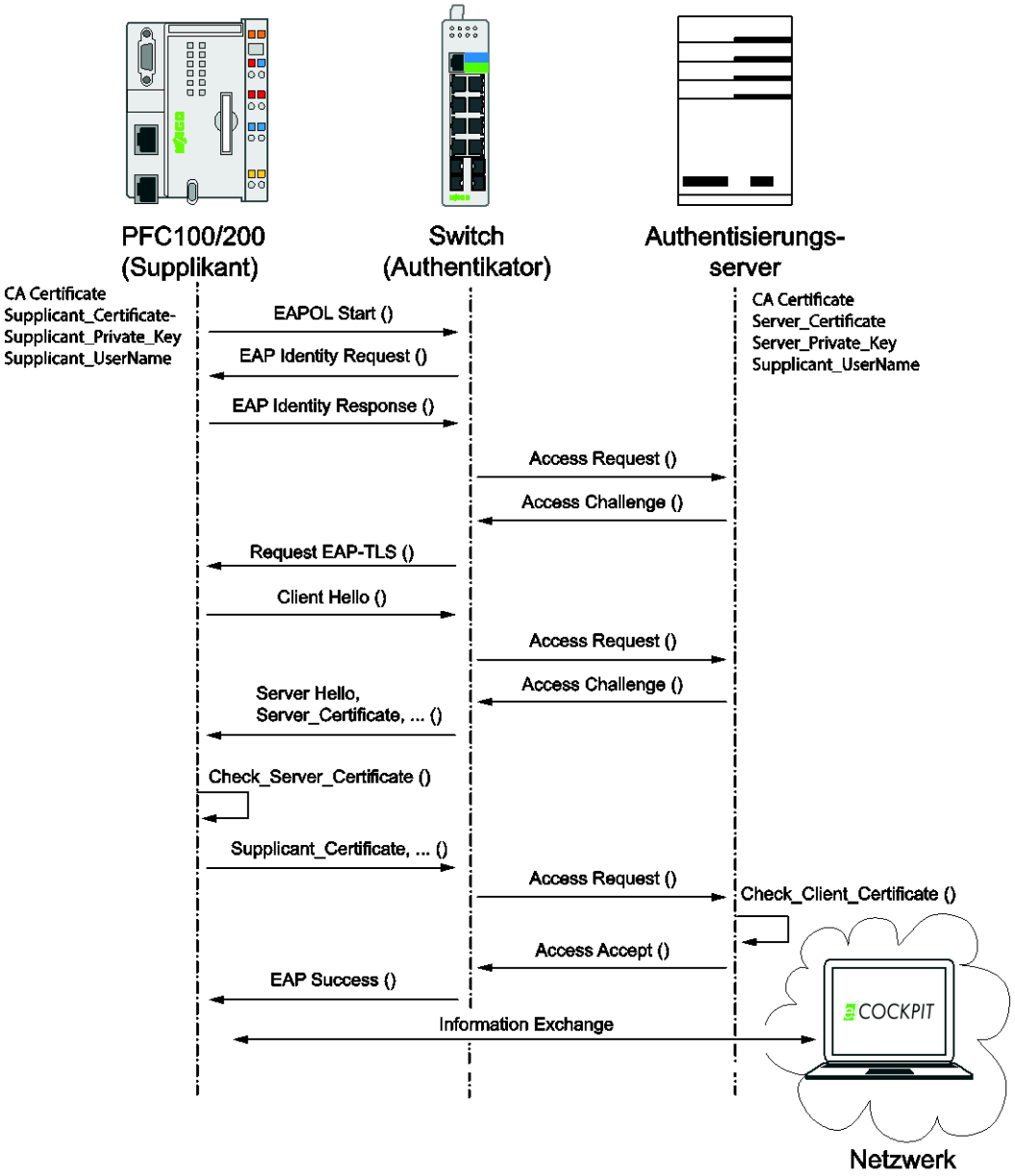

Abbildung 75: Port-Authentisierung gemäß IEEE 802.1X, Zertifikat

1. Sobald die Applikation „wpa_supplikant“ auf dem Controller ausgeführt wird, wird der Controller aufgefordert sich zu identifizieren und sendet seine Identität (Supplicant_UserName) an den Authentisierungsserver.
2. Der Authentisierungsserver prüft, ob die Identität innerhalb seiner Identitätsdatenbank vorhanden ist.
3. Sofern die Identität vorhanden ist, wird an den Controller die Nachricht „Request EAP-TLS“ gesendet, die den Controller auffordert, einen TLS-Handshake durchzuführen.
4. Der Controller beginnt den TLS Handshake mit der Nachricht „Client Hello“, in der unter anderem die unterstützten Cipher Suites aufgelistet werden.
5. Daraufhin antwortet der Authentisierungsserver mit einer Nachricht „Server Hello“ und sendet sein Serverzertifikat an den Controller.
6. Nach Erhalt des Serverzertifikats, wird mithilfe des CA-Zertifikats geprüft, ob das Zertifikat vertrauenswürdig und gültig ist.

7. Falls der Controller dem Serverzertifikat vertraut und die Gültigkeit verifiziert wurde, sendet der Controller sein Zertifikat an den Authentisierungsserver.
8. Mit dem Controllerzertifikat wird analog zum Schritt 6 verfahren.
9. Wenn der Authentisierungsserver dem Controllerzertifikat vertraut und das Zertifikat gültig ist, wird dem Controller über die Nachricht „Access Accept“ bzw. „EAP-Success“ der Zugang zum Netzwerk gewährt.

Hinweis

Kein Zugriff auf das Netzwerk bei nicht erfolgreicher Authentisierung!
Wenn die Authentisierung misslingt, besitzen Server und Controller entweder kein Zertifikat oder ein vorhandenes Zertifikat wurde von der Gegenstelle abgelehnt. Somit kann kein Zugriff auf das Netzwerk erfolgen!

7.2.2.1 EAP-TLS-Port-Authentisierung einrichten

1. Erstellen Sie Zertifikate und Schlüssel für die Port-Authentisierung, siehe Kapitel „Hardening“ > … > Zertifikate erstellen und austauschen“.
2. Editieren Sie die Konfigurationsdatei /etc/wpa_supplicant.conf des Controllers wie folgt:

```
network={
          key_mgmt=IEEE8021X
          eap=TLS
          identity="Supplicant_Name"
          ca_cert="/etc/certificates/CA.crt"
          client_cert="/etc/certificates/Supplicant.pem"
          private_key="/etc/certificates/keys/Supplicant_Key.pem"
          eapol_flags=0
}
```

3. Konfigurieren Sie Switch und Authentisierungsserver (z. B. RADIUS-Server).
4. Starten, bzw. testen Sie die EAP-TLS-Authentisierung auf dem Controller mit dem folgenden Befehl:

```
wpa_supplicant -dd -Dwired -ibr0 -c/etc/wpa_supplicant.conf
```

Tabelle 11: Beschreibung der Parameter

Parameter	Bedeutung
-dd	Debug-Modus
-D	Treiber der verwendet werden soll (wired: kabelgebunden)
-i	Interface der Geräte (br0: ETHERNET-Interface X1; br1: ETHERNET-Interface X2)
-c	Pfad zur WPA-Supplicant-Konfigurationsdatei (wpa_supplicant.conf)

Für weitere Informationen bezüglich der Parameter/Konfiguration siehe:
https://linux.die.net/man/8/wpa_supplicant

7.2.3 Automatische Port-Authentisierung während des Boot-Vorgangs

Um die Applikation „wpa_supplicant“ nicht manuell ausführen zu müssen (siehe Kapitel „Port-Authentisierung mittels Benutzername und Kennwort gemäß EAP-MD5“), können Sie ein Startskript erstellen. Das beispielhafte Startskript in der nachfolgenden Abbildung ermöglicht es Ihnen, die Port-Authentisierung automatisch durchzuführen, während der Controller startet. Voraussetzung ist, dass Sie eine entsprechende Konfiguration innerhalb der Konfigurationsdatei „/etc/wpa_supplicant.conf“ angelegt haben (siehe z. B. Kapitel „EAP-MD5-Port-Authentisierung einrichten“). Nach dem Start des Skripts läuft die Applikation „wpa_supplicant“ als Hintergrundprozess.

Für das Einrichten des Start-Skripts sind die folgenden Schritte notwendig:

1. Erstellen Sie eine Datei „wpa_supplicant“ mit dem nachfolgenden Inhalt:

```
#!/bin/sh

#
# wpa_supplicant
#
PATH=/usr/bin:/usr/sbin:/bin:/sbin

PREFIX="wpa_supplicant: "
WPA="/sbin/wpa_supplicant"
WPA_CONF="/etc/wpa_supplicant.conf"
WPA_IF="br0"
WPA_DRIVER="wired"
WPA_DAEMON_OPT="-B"
WPA_OPTIONS="-D$WPA_DRIVER -i$WPA_IF -c$WPA_CONF $WPA_DAEMON_OPT"

case $1 in

        start)
                echo "${PREFIX}starting"
                if start-stop-daemon --start --quiet --oknodo --exec ${WPA} --
      ${WPA_OPTIONS}; then
                        echo "${PREFIX}done"
                else
                        echo "${PREFIX}error, could not start wpa_supplicant"
                fi
                ;;
        stop)
                echo "${PREFIX}stoppping"
                if start-stop-daemon --stop --quiet --oknodo --exec ${WPA}; then
                        echo "${PREFIX}done"
                else
                        echo "${PREFIX}error, could not stop wpa_supplicant "
                fi
                ;;
        *)
                echo "${PREFIX}usage: ${0} [start|stop]"
                exit 1
                ;;
esac
```

2. Übertragen Sie die Datei „wpa_supplicant“ in den Ordner /etc/init.d/ des Controllers.

3. Verbinden Sie sich mit der Linux®-Konsole (z.B. über SSH oder die serielle Konsole).

4. Erstellen Sie einen symbolischen Link für die Ausführung des Skripts während des Boot-Vorgangs. Linux®-Befehl:

```
ln -s /etc/init.d/wpa_supplicant /etc/rc.d/S97_wpa_supplicant
```

Nach dem Neustart wird die Applikation „wpa_supplicant“ als Hintergrundprozess gestartet und versucht, sich mit einer Gegenstelle (z.B. Authentisierungsserver) zu authentisieren.

Hinweis

Beachten Sie die Angabe der Schnittstelle!
In der Beispieldatei „wpa_supplicant“ erfolgt die Authentisierung über die Schnittstelle X1 (br0). Bitte passen Sie die Interface-Variable „WPA_IF“ innerhalb ihres Startskripts entsprechend ihrer Konfiguration an!

7.3 Simple Certificate Enrollement Protocol (SCEP)

Mit dem HTTP-basierten „Simple Certificate Enrollment Protokoll“ (SCEP) ist die zentrale Verteilung und das Management von Gerätezertifikaten auf beliebig vielen Controllern in einem Netzwerk möglich. Die Bereitstellung und Verwaltung der Zertifikate wird von einem SCEP-Server übernommen. Das jeweilige Gerät (Controller) generiert sich selbstständig ein RSA-Schlüsselpaar und fordert ein Zertifikat an. Der SCEP-Server überprüft die Anforderung und generiert ein signiertes X.509-Zertifikat, das anschließend via SCEP-Protokoll abgeholt und lokal installiert werden kann, siehe Abbildung „Simple Certificate Enrollement Protocol“ (SCEP). Es wird zwischen einem manuellen und automatischen Modus unterschieden. Beide Modi werden in den folgenden Kapiteln beschrieben.

Zur Sicherstellung von Integrität und Vertraulichkeit sind die übertragenen Daten in PKCS#7-Formaten verpackt.

Hinweis

Konfigurieren Sie zunächst die nötige Infrastruktur!
Zum Erstellen und Bereitstellen von Zertifikaten über das SCEP-Protokoll benötigen Sie eine entsprechende Infrastruktur. Der Server kann z. B. als Windows-2003-ServerCA mit einem speziellen Plug-in (mscep.dll) realisiert werden.

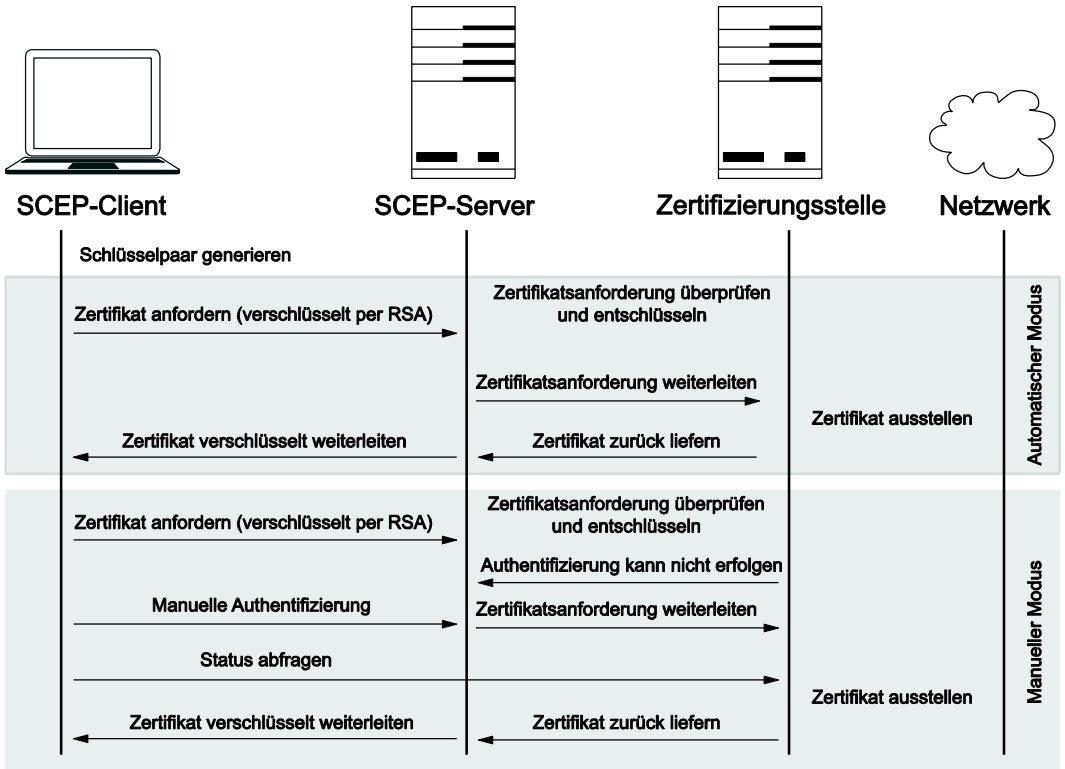

Abbildung 76: Simple Certificate Enrollement Protocol (SCEP)

7.3.1 Automatische Bearbeitung der Anfrage

Bei der automatischen Bearbeitung muss die Authentizität des Antragsstellers über eine Sicherheitsabfrage gewährleistet sein. Wenn die Sicherheitsabfrage in der Zertifikatsanfrage mit dem aktuell gültigen Wert auf dem Server übereinstimmt, kann ein Gerätezertifikat automatisch ausgestellt werden.

1. Der Client generiert ein RSA-Schlüsselpaar.
   Der öffentliche Teil dieses Schlüsselpaars wird später zusammen mit der Anfrage an den Server übermittelt. Der private Teil des Schlüsselpaars verbleibt im Client.
2. Der Client sendet den öffentlichen Teil des generierten Schlüsselpaars (Public key) zusammen mit Angaben zu seiner Identität (Namen, E-Mail-Adresse etc.) als Zertifikatsanforderung an den Server. Diese Anfrage wird mit dem privaten Teil des Schlüsselpaars signiert.
3. Der Server prüft die Zertifikatsanfrage und stellt das Gerätezertifikat ohne weitere Interaktion aus, wenn die Daten für die Authentifizierung genügen.
4. Das Gerätezertifikat wird an den Client weitergeleitet und z. B. für einen VPN-Betrieb bereitgestellt.

7.3.2 Manuelle Bearbeitung

Der Server schaltet in den „Manuellen Modus“, wenn er weitere Informationen für die Authentifizierung des Antragsstellers benötigt. D. h., dass der Server die Zertifikatsanfrage so lange in einen Wartezustand stellt, bis die Bewilligung oder Ablehnung der Zertifizierungsstelle vorliegt. Im „Manuellen Modus“ wird das Zertifikat nicht direkt ausgeliefert. Stattdessen kann der Client kontinuierlich abfragen, ob die Authentifizierung stattgefunden hat. Sobald dies geschehen ist, erhält der Client das Zertifikat auf seine Anfrage.

1. Der Client generiert ein RSA-Schlüsselpaar.
2. Der Client sendet den öffentlichen Teil des generierten Schlüsselpaars (Public key) zusammen mit Angaben zu seiner Identität (Namen, E-Mail-Adresse etc.) als Zertifikatsanforderung an den Server. Diese Anfrage wird mit dem privaten Teil des Schlüsselpaares signiert.
3. Der Server prüft die Zertifikatsanfrage und stellt diese in einen Wartezustand, wenn die Authentifizierung nicht durchgeführt werden kann.
4. Der Client wird informiert, dass die Authentifizierung nicht erfolgen kann.
5. Es erfolgt eine manuelle Authentifizierung, z. B. über das Telefon.
6. Der Client stellt durch zyklisches Abfragen fest, ob er das Zertifikat abrufen kann.
7. Der Server prüft die Zertifikatsanfrage und stellt das Gerätezertifikat ohne weitere Interaktion aus, wenn die Daten für die Authentifizierung genügen.
8. Das Gerätezertifikat wird vom Client abgerufen und z. B. für einen VPN-Betrieb bereitgestellt.

7.3.2.1 SCEP-Prozess einrichten

ACHTUNG

Synchronisation der Uhrzeit auf dem Controller!
Für die Zertifikatsprüfung per SCEP-Protokoll müssen Datum und Uhrzeit aller Controller synchronisiert sein. Das erfolgt am einfachsten per Network Time Protocol (NTP).

Sie können sich mit dem folgenden Befehl zunächst eine Auflistung der verfügbaren Parameter des SCEP-Clients anzeigen lassen:

```
ipsec scepclient --help
```

1. Erzeugen Sie ein 2048-RSA-Schlüsselpaar gemäß dem PKCS1-Standard, siehe Kapitel „Hardening“ > … > „Private Schlüssel erzeugen“.

Hinweis

Exportieren Sie das Schlüsselpaar und laden Sie es in Ihr Gerät!
Erstellen und exportieren Sie Ihr RSA-Schlüsselpaar aus der Schlüsselverwaltungssoftware XCA. Wählen Sie dafür das Exportformat „.der“ aus. Das Schlüsselpaar kann anschließend über das WBM in den Controller geladen werden: **OpenVPN/IPsec** > **Certificate Upload** > **New Private Key**. Der private Schlüssel wird in dem Ordner /etc/certificates/keys/ abgelegt.

2. Laden Sie die CA-Zertifikate für die PKCS7-Verschlüsselung (Anforderung) und die PKCS7-Signaturprüfung (Antwort):

```
ipsec scepclient --out cacert --url
http://10.1.101.53/certsrv/mscep/
```

Anschließend werden, je nach Konfiguration der Infrastruktur, CA-Zertifkate geladen, die für die Sicherung der SCEP-Kommunikation verwendet werden. In diesem Beispiel sind es die Zertifikate „caCert-ra-1.der“ für die Verschlüsselung der SCEP-Anfrage und „caCert-ra-2.der“ für die Signaturüberprüfung der SCEP-Antwort des Servers.

3. Laden Sie ein Zertifikat von der Zertifizierungsstelle auf Basis des erzeugten RSA-Schlüsselpaars (initial) und der geladenen CA-Zertifikate aus Schritt 2:

```
ipsec scepclient --out cert=pfc200Cert.der --in
pkcs1=pfc200private.der --in cacert-enc=caCert-ra-1.der --in cacert-
sig=caCert-ra-2.der --url http://10.1.101.53/certsrv/mscep/ -p
90261AC82C586743
```

Hinweis

Beachten Sie, dass die Namen lediglich Platzhalter sind!
Die Namen des oben genannten Schlüsselpaars (pfc200Cert.der“/„pfc200private.der) sowie der Server-, und Passphrase-Parameter (--url, -p) sind Platzhalter und können nach Bedarf anders vergeben werden!

Nach Eingabe des Befehls wird ein selbst signiertes Zertifikat für die PKCS7-Signatur erstellt. Anschließend wird eine Zertifikatsanfrage (PKCS10) mit dem

PKCS1-Schlüssel (Signatur) erstellt. Danach wird eine PKCS7-Anfrage mithilfe der CA-Zertifikate verarbeitet. Da die PKCS7-Signatur auf Basis von selbst signierten Zertifikaten erfolgt, muss zusätzlich ein Passwort (-p) angegeben werden, welches über den URL-Aufruf der Zertifizierungsstelle bereitgestellt wird. Je nach Konfiguration der Zertifizierungsstelle kann das Passwort auch entfallen. Das vertrauenswürdige Zertifikat „pfc200Cert.der" wird anschließend im Verzeichnis „/etc/certificates" gespeichert.

Wenn nach Ablauf des aktuellen Zertifikats eine erneute Zertifikatsanfrage gestellt wird, kann das aktuell verwendete vertrauenswürdige Zertifikat verwendet werden. Es muss kein neues selbst signiertes Zertifikat erstellt werden. Da es sich bei dem Zertifikat um ein vertrauenswürdiges Zertifikat handelt, entfällt die Passworteingabe (-p). Durch Angabe des Parameters „–in cert-self=pfc200Cert.der", wird kein selbstsigniertes Zertifikat verwendet, sondern das aktuelle Zertifikat „pfc200Cert.der":

```
ipsec scepclient --out cert=pfc200Cert.der --in cert-self=pfc200Cert.der
--in pkcs1=pfc200private.der --in cacert-enc=caCert-ra-1.der --in cacert-
sig=caCert-ra-2.der --url http://10.1.101.53/certsrv/mscep/
```

Hinweis

Weiterführende Informationen zu SCEP!
Weitere Informationen bezüglich der Applikation „scepclient" finden Sie unter:
http://manpages.ubuntu.com/manpages/artful/man8/scepclient.8.html!

8 Anhang

8.1 FAQ zu IPsec

Ein fehlerhafter Aufbau einer IPsec-Verbindung kann verschiedene Ursachen haben. In diesem Kapitel bekommen Sie Hinweise auf mögliche Schwierigkeiten, die bei einer IPsec-Konfiguration auftreten können. Gleichzeitig werden Maßnahmen zur Fehleranalyse auf den Controllern PFC200/PFC100 dargestellt.

Tabelle 12: Hinweise und Maßnahmen

Hinweise	Maßnahmen
Da die Verschlüsselungs- und Authentisierungsverfahren konfigurierbar sind, können unter Umständen Probleme beim Aufbau einer „Security Association“ (SA) mit unterschiedlichen VPN-Produkten auftreten. Im Falle unterschiedlicher Konfigurationen der IPsec-Gegenstellen kann es zu einem Fehlerfall kommen. Dabei kann die Verbindung nicht aufgebaut werden.	Achten Sie darauf, dass die IPsec-Gegenstellen die gleichen Authentisierungs- und Verschlüsselungsverfahren verwenden. Diese Konfiguration wird beim Controller innerhalb der Konfigurationsdatei „ipsec.conf“ vorgenommen ,siehe Kapitel „IPsec“ > „Konfigurationsdateien erstellen“.
Beim Routing zwischen den Netzen bei einem Site-To-Site-Szenario müssen die Adressbereiche der zu verbindenden Teilnetze unterschiedlich sein.	• Definieren Sie einen eigenen Adressbereich (unterschiedliche Subnetze) für die zu verbindenden Teilnetze. • Vergeben Sie IP-Adressen nach dem „Zusammenschalten“ der Netze nicht mehrfach, da es sonst zu einer fehlerhaften IPsec-Verbindung kommt. • Beachten Sie, dass die IPsec-Applikation „strongSwan“ bei einem erfolgreichen Aufbau automatisch eine Route in der Routing-Tabelle 220 hinzufügt. Linux®-Befehl: `root@PFC200-405679:~ ip route list table 220`
Das Schlüsselaustauschprotokoll IKEv2 ist stabiler und anwenderfreundlicher als das Schlüsselaustauschprotokoll IKEv1.	Verwenden Sie das Schlüsselaustauschprotokoll IKEv2 anstatt IKEv1, um größere Probleme bei der NAT-Technologie, dynamischen IP-Adressen und mobilen Endgeräten vorzubeugen.
Eine hohe Verschlüsselung bzw. kryptografische Sicherung führt zu einem hohen Ressourcenverbrauch. Dadurch kann es zu Verzögerungen und Anomalien im Programmablauf kommen, sodass die Steuerung nicht mehr ihren eigentlichen Aufgaben nachgehen kann.	Verwenden Sie eine nicht zu hohe Verschlüsselung bzw. achten Sie auf die Wahl der Schlüssellängen für die kryptografischen Verfahren, entsprechend den technischen Richtlinien des BSI TR-02102-4 (Version 2017-01)!
Wenn Sie Zertifikate verwenden, muss die Uhrzeit auf den IPsec-Gegenstellen identisch sein. Es kann sonst zu Problemen bei der Verifikation der Zertifikate führen, infolgedessen keine IPsec-Verbindung aufgebaut werden kann.	• Achten Sie darauf, dass die Uhrzeit auf allen Systemen gleich ist! • Wenn Sie keinen Zeitserver verwenden, können Sie die Uhrzeit bzw. das Datum manuell über die Konsole (date --set "YYYY-MM-DD HH:MM") oder das WBM ändern.

Hinweis

Weitere Informationen finden Sie direkt unter strongSwan!
Ein FAQ von strongSwan finden Sie unter:
https://wiki.strongswan.org/projects/strongswan/wiki/FAQ!

8.1.1 Zusätzliche IPsec-Fehler- bzw. Statusanalyse

- Bewerten Sie für die IPsec-Fehleranalyse die IPsec-Logeinträge, welche unter dem Linux®-Pfad „`/var/log/messages`“ aufgeführt sind.
- Es ist möglich, den Log-Level der Logging-Ausgaben in der Konfigurationsdatei „ipsec.conf“ zu erhöhen, um detailliertere Informationen im Fehlerfall zu erhalten.
  https://wiki.strongswan.org/projects/strongswan/wiki/LoggerConfiguration
- Lassen Sie sich die eingehenden und ausgehenden Netzwerkpakete mit dem folgenden Befehl anzeigen (z. B. über den SSH-Dienst):
  `tcpdump port not 22 -n -i eth0.`
- Detailliertere Informationen bezüglich Konfiguration und Test einer IPsec-Verbindung erhalten Sie unter:
  http://wiki.strongswan.org/projects/strongswan/wiki/UserDocumentation.

Abbildungsverzeichnis

Abbildung 1: Zwiebelschalenmodell 21
Abbildung 2: Referenzarchitektur 23
Abbildung 3: Physikalische Schnittstellen am WAGO-Controller 25
Abbildung 4: Physikalische Schnittstellen am WAGO-Controller mit GSM/3G-Modem-Schnittstelle....25
Abbildung 5: Service-Schnittstelle deaktivieren 32
Abbildung 6: Linux®-Konsole deaktivieren 33
Abbildung 7: TLS Configuration....35
Abbildung 8: Diffie-Hellmann-Parameter erstellen 35
Abbildung 9: Schlüssellänge, DH Parameter....36
Abbildung 10: PuTTYgen starten 37
Abbildung 11: PuTTYgen Schlüsselerzeugung....38
Abbildung 12: PuTTY-Konfiguration 39
Abbildung 13: PuTTY Konfiguration speichern 40
Abbildung 14: Anmeldung über Passworteingabe deaktivieren 40
Abbildung 15: Anmeldung per root login verweigern 41
Abbildung 16: Neustart Putty....43
Abbildung 17: Datenbank XCA....44
Abbildung 18: Vorlage anlegen, Register „Inhaber“ 45
Abbildung 19: Vorlage erstellt....46
Abbildung 20: Zertifikat erstellen 47
Abbildung 21: Neuen Schlüssel anlegen 48
Abbildung 22: Neues Zertifikat angelegt....48
Abbildung 23: Neues Gerätezertifikat erstellen....49
Abbildung 24: Neuen Schlüssel anlegen 50
Abbildung 25: Registerkarte Erweiterungen 51
Abbildung 26: X509v3 Subject Alternative Name, IP-Adresse eingeben 52
Abbildung 27: Neuer Zertifikatsantrag, Schlüsselverwendung Client 52
Abbildung 28: Gerätezertifikat erstellt....53
Abbildung 29: Root-CA-Zertifikat exportieren 54
Abbildung 30: Controller-Zertifikat exportieren 54
Abbildung 31: Ablageort „/etc/lighttpd/root-ca.pem“....55
Abbildung 32: Grünes Schloss im Browser (Firefox)....55
Abbildung 33: Zertifikatsperrliste anlegen....56
Abbildung 34: Zertifikatsrückzug 57
Abbildung 35: CRL erstellen....57
Abbildung 36: Rücknahmeliste exportieren 58
Abbildung 37: WAGO-Service-Kommunikation deaktivieren....59
Abbildung 38: Standard-Netzwerkports ändern 60
Abbildung 39: Unverschlüsselten Zugang auf das WBM sperren 61
Abbildung 40: Zugang zur CODESYS Laufzeitumgebung deaktivieren 61
Abbildung 41: Direktzugriff auf die CODESYS Webvisualisierung sperren 62
Abbildung 42: Zugriff auf die Laufzeitumgebung ***e!****RUNTIME* sperren 63
Abbildung 43: Passwörter im Web-Based-Management ändern....64
Abbildung 44: Passwort für den Benutzer „admin“ ändern....65
Abbildung 45: Firewall-Konfiguration im WBM....67
Abbildung 46: User-Filter: White List anlegen....69

Abbildung 47: Anlegen einer Black List für alle Zugriffe 70
Abbildung 48: Reihenfolge der Filterregeln 70
Abbildung 49: User Filter: White List für Netzwerke anlegen 72
Abbildung 50: Freigabe von definierten Netzwerken 73
Abbildung 51: MAC-Adressen eintragen 75
Abbildung 52: MAC-Adressenfilter aktivieren 75
Abbildung 53: Site-to-Site-VPN 77
Abbildung 54: Host-to-Site-VPN 77
Abbildung 55: Host-to-Host-VPN bzw. Remote-Desktop-VPN 77
Abbildung 56: „IP Forwarding“ aktivieren 78
Abbildung 57: Firewall Konfiguration – OpenVPN 80
Abbildung 58: Netzwerktopologie, Routing 81
Abbildung 59: Routing enabled 82
Abbildung 60: Static Routes 82
Abbildung 61: Host-to-Host-Verbindung 83
Abbildung 62: Site-to-Site-VPN 87
Abbildung 63: WBM, Konfigurationsdatei auswählen 90
Abbildung 64: WBM, Zertifikate auswählen 91
Abbildung 65: OpenVPN-Dienst aktivieren 91
Abbildung 66: Host-to-Host-Verbindung, IPsec 95
Abbildung 67: Site-to-Site-VPN, IPsec 97
Abbildung 68: Static Routes, Zugriff der Clients auf ein Netzwerk hinter dem IPsec-Client 99
Abbildung 69: Static Routes , Zugriff der Clients auf ein Netzwerk hinter dem IPsec-Server 100
Abbildung 70: WBM, Konfigurationsdateien für IPsec auswählen 103
Abbildung 71: WBM, Zertifikate auswählen 103
Abbildung 72: IPsec-Dienst aktivieren 104
Abbildung 73: Grundprinzip der Port-Authentisierung 105
Abbildung 74: Ablauf der Port-Authentisierung gemäß EAP-MD5 107
Abbildung 75: Port-Authentisierung gemäß IEEE 802.1X, Zertifikat 110
Abbildung 76: Simple Certificate Enrollement Protocol (SCEP) 114

Tabellenverzeichnis

Tabelle 1: Darstellungen der Zahlensysteme 8
Tabelle 2: Schriftkonventionen 8
Tabelle 3: Abkürzungen 13
Tabelle 4: Basiskonfiguration Server 16
Tabelle 5: Basiskonfiguration Client 17
Tabelle 6: Anwendungen für PFC100/PFC200 18
Tabelle 7: WBM-Benutzer 18
Tabelle 8: Registerkarte „Inhaber“ 45
Tabelle 9: Aktionen für Filterregeln 66
Tabelle 10: Beschreibung der Parameter 108
Tabelle 11: Beschreibung der Parameter 111
Tabelle 12: Hinweise und Maßnahmen 118

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Telefon: 0571/887 – 0
Telefax: 0571/887 – 844169
E-Mail: info@wago.com
Internet: www.wago.com