TECHDOCS

Podręcznik

WAGO-I/O-SYSTEM 750

750-8xxx(/xxx-xxx)

PFC100/200

Cyberbezpieczeństwo sterowników PFC100/PFC200

Wersja 1.0.0

© 2019 WAGO Kontakttechnik GmbH & Co. KG
Wszystkie prawa zastrzeżone.

WAGO ELWAG Sp. z o. o.

50-506 Wrocław
ul. Piękna 58a

Tel.: +48 71 360 29 70

Fax: +48 71 360 29 99

E-mail: info@wago.com

Strona www: http://www.wago.com

Wsparcie techniczne

Tel.: +48 71 360 29 33

e-mail: support@wago.com

Podjęto wszelkie możliwe starania zmierzające do zapewnienia prawidłowości i kompletności niniejszej dokumentacji. Ponieważ jednak pomimo zachowania najwyższej staranności wykluczenie błędów nie jest możliwe, autorzy będą wdzięczni za wszelkiego rodzaju wskazówki i sugestie.

E-mail: documentation@wago.com

Należy zwrócić uwagę na fakt, że zastosowane w niniejszym podręczniku nazwy sprzętu i oprogramowania oraz nazwy marek poszczególnych firm podlegają ochronie znaków towarowych, marek lub ochronie patentowej.

Znak WAGO jest zarejestrowanym znakiem towarowym spółki WAGO Verwaltungsgesellschaft mbH.

Spis treści

1 Wskazówki dotyczące dokumentacji

Wskazówka

Należy zachować dokumentację!
Niniejsza dokumentacja jest częścią produktu. Dlatego należy ją przechowywać przez cały czas użytkowania produktu. Dokumentację tę należy przekazać kolejnemu właścicielowi lub użytkownikowi produktu. Należy również zapewnić aktualizację dokumentacji o pojawiające się uzupełnienia.

Niniejsza dokumentacja odnosi się do standardowych wersji produktów, a także do wszystkich wariantów sterownika PFC100/PFC200.

1.1 Prawa autorskie

Niniejsza dokumentacja, wraz ze wszystkimi zawartymi w niej ilustracjami, jest chroniona prawami autorskimi. Wszelkie zastosowanie niniejszej dokumentacji niezgodne z przepisami prawa autorskiego jest zabronione. Powielanie, tłumaczenie na inne języki, jak również archiwizacja elektroniczna i fototechniczna oraz modyfikacja wymagają pisemnej zgody ze strony firmy WAGO Kontakttechnik GmbH & Co. KG, Minden. Nieprzestrzeganie tego zalecenia upoważnia do wnoszenia roszczeń odszkodowawczych.

1.2 Symbole

NIEBEZPIECZEŃSTWO 	**Ostrzeżenie przed obrażeniami ciała!** Oznacza bezpośrednie zagrożenie, wiążące się z dużym ryzykiem śmierci lub poważnych obrażeń ciała.
NIEBEZPIECZEŃSTWO 	**Ostrzeżenie przed obrażeniami ciała spowodowanymi przez prąd elektryczny!** Oznacza bezpośrednie zagrożenie, wiążące się z dużym ryzykiem śmierci lub poważnych obrażeń ciała.
OSTRZEŻENIE 	**Ostrzeżenie przed obrażeniami ciała!** Oznacza możliwe zagrożenie, wiążące się z umiarkowanym ryzykiem śmierci lub poważnych obrażeń ciała.
OSTROŻNIE 	**Ostrzeżenie przed obrażeniami ciała!** Oznacza możliwe zagrożenie, wiążące się z niewielkim ryzykiem lekkich lub średnio lekkich obrażeń ciała.
UWAGA 	**Ostrzeżenie przed szkodami materialnymi!** Oznacza możliwe zagrożenie, którego skutkiem mogą być szkody materialne.
Wyładowania elektrostatyczne 	**Ostrzeżenie przed szkodami materialnymi w następstwie wyładowań elektrostatycznych!** Oznacza możliwe zagrożenie, którego skutkiem mogą być szkody materialne.
Wskazówka 	**Ważna wskazówka!** Oznacza możliwość nieprawidłowego funkcjonowania, która jednak nie pociąga za sobą szkód materialnych.
Informacja 	**Dodatkowe informacje** Odsyła do dalszych informacji, niestanowiących istotnej części dokumentacji (np. do informacji zawartych na stronie www).

1.3 Zastosowane systemy liczbowe

Tabela 1: Zastosowane systemy liczbowe

System liczbowy	Przykład	Komentarz
dziesiętny	100	zwykły zapis
szesnastkowy	0x64	notacja szesnastkowa
binarny	'100' '0110.0100'	zapis w apostrofach, półbajt oddzielony kropką

1.4 Sposoby zapisu

Tabela 2: Sposoby zapisu

Zapis	Znaczenie
kursywa	Nazwy ścieżek i plików są zapisywane kursywą, np.: *C:\Programy\Oprogramowanie WAGO*
bold	Punkty menu są pogrubione, np.: **Zapisz**
>	Znak „większy od“ między dwiema nazwami oznacza wybór określonego punktu menu, np.: **Plik > Nowy**
wprowadzanie danych	Nazwy pól do wprowadzania lub wyboru danych są przedstawiane pogrubioną czcionką, np.: **Początek zakresu pomiarowego**
„Wartość“	Wartości wprowadzane lub wybierane są zapisywane w cudzysłowie, np.: w polu **Początek zakresu pomiarowego** wprowadź wartość „4 mA“.
[Przycisk]	Nazwy przycisków znajdujących się w polach dialogowych są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. **[Wprowadzanie]**
[Klawisz]	Nazwy klawiszy na klawiaturze są przedstawione pogrubioną czcionką i ujęte są w nawias kwadratowy, np. **[F5]**

2 Ważne objaśnienia

Rozdział ten zawiera wyłącznie zestawienie najważniejszych zasad bezpieczeństwa oraz wskazówek. Zostaną one także przedstawione w poszczególnych rozdziałach. W celu ochrony przed obrażeniami ciała oraz zapobiegania uszkodzeniom urządzeń, konieczne jest staranne zapoznanie się ze wskazówkami dotyczącymi bezpieczeństwa oraz ich przestrzeganie.

2.1 Podstawy prawne

2.1.1 Zastrzeżenie prawa do zmian technicznych

Firma WAGO Kontakttechnik GmbH & Co. KG zastrzega sobie prawo do zmian. W przypadku udzielania patentu lub ochrony wzoru użytkowego, wszystkie prawa są zastrzeżone dla WAGO Kontakttechnik GmbH & Co. KG. Produkty obce są wymieniane bez podawania informacji o prawach patentowych. Dlatego nie można wykluczyć istnienia tego rodzaju praw.

2.1.2 Kwalifikacje personelu

Wszystkie prace przy urządzeniach WAGO-I/O-SYSTEM 750 mogą być wykonywane wyłącznie przez wykwalifikowanych elektryków z odpowiednią wiedzą fachową w zakresie techniki automatyzacji. Osoby te muszą znać aktualne normy i wytyczne dotyczące AKPiA.

Wszelkie ingerencje w układ sterowania wolno wykonywać wyłącznie specjalistom, dysponującym odpowiednią wiedzą z zakresu programowania PLC.

2.1.3 Stosowanie WAGO-I/O-SYSTEM 750 zgodne z przeznaczeniem

Interfejsy sieciowe, sterowniki sieciowe oraz moduły I/O modularnego systemu o nazwie WAGO-I/O-SYSTEM 750 służą do odczytu sygnałów dwustanowych i analogowych z czujników, oraz przesyłania ich do elementów wykonawczych lub do nadrzędnych układów sterowania. Przy użyciu sterowników sieciowych możliwe jest ich (wstępne) przetwarzanie.

Urządzenia należy stosować w otoczeniu roboczym, gdzie wystarczający jest stopień ochrony IP20. Charakteryzuje się on ochroną przed dotykiem oraz przed wnikaniem ciał stałych o wielkości ≥ 12,5 mm, lecz brakiem ochrony przed wnikaniem wody. Dlatego też używanie urządzeń w otoczeniu wilgotnym lub zakurzonym jest niedozwolone, o ile nie podano inaczej.

Używanie urządzeń WAGO-I/O-SYSTEM 750 w pomieszczeniach mieszkalnych bez dodatkowych środków jest dozwolone tylko wówczas, gdy spełniają one wymagania dotyczące granic emisji (emisje zakłóceń) zgodnie z EN 61000 6 3. Odpowiednie informacje znajdują się w rozdziale „Opis urządzenia“ > „Normy i dyrektywy“ podręcznika dotyczącego zastosowanego interfejsu/sterownika sieciowego.

Zastosowanie WAGO-I/O-SYSTEM 750 w przestrzeniach zagrożonych wybuchem wymaga specjalnej obudowy ochronnej, zgodnie z dyrektywą 2014/34/WE. Dodatkowo należy pamiętać, że konieczne jest uzyskanie świadectwa badania typu, potwierdzającego prawidłowy montaż systemu w obudowie lub szafie rozdzielczej.

Wdrożenie funkcji bezpieczeństwa, takich jak wyłączniki awaryjne lub monitorowanie drzwi bezpieczeństwa, może być realizowane tylko przez moduły F-I/O modularnego systemu WAGO-I/O-SYSTEM 750. Tylko te bezpieczne moduły F-I/O zapewniają bezpieczeństwo funkcjonalne, zgodnie z najnowszymi standardami międzynarodowymi. Bezreakcyjne moduły wyjściowe WAGO mogą być sterowane za pomocą funkcji bezpieczeństwa.

2.1.4 Stan techniczny urządzeń

Urządzenia są dostarczane na potrzeby danego zastosowania, w sprzętowej i programowej konfiguracji fabrycznej. Nie zawierają żadnych części, które wymagają od użytkownika konserwacji czy napraw. Następujące czynności powodują wyłączenie odpowiedzialności WAGO Kontakttechnik GmbH & Co. KG:

- naprawy
- wprowadzanie zmian w sprzęcie lub oprogramowaniu, które nie są opisane w instrukcji obsługi
- użycie komponentów niezgodne z ich przeznaczeniem

Dalsze szczegóły podano w umowach kontraktowych. Prośby i zapytania dotyczące zmiany konfiguracji lub nowej konfiguracji osprzętu i oprogramowania należy kierować do firmy WAGO Kontakttechnik GmbH & Co. KG.

3 Wstęp

Od kiedy urządzenia przemysłowe zostały włączone do sieci internetowej, systemy sterowania takie jak WAGO-I/O-SYSTEM padają ofiarą cyberataków. Aby zminimalizować zagrożenia bezpieczeństwa i uniknąć szkód gospodarczych, wprowadzono trzy główne kryteria bezpieczeństwa, które powinien spełniać system:

- **Dostępność**:
  Dane i funkcje systemu powinny być dostępne na czas i na żądanie.
- **Integralność**
  Należy zagwarantować poprawność i kompletność danych wrażliwych oraz prawidłowe funkcjonowanie systemu.
- **Poufność**
  Dane i informacje o ochronie powinny być dostępne wyłącznie dla osób do tego upoważnionych.

Niniejsza dokumentacja opisuje potencjalne zagrożenia bezpieczeństwa i ma na celu przeciwdziałanie tym zagrożeniom poprzez odpowiednie i skuteczne działania.

Zasady bezpiecznego projektowania systemu obejmują:

- **Minimalne uprawnienia / zasada "Need-to-know"**:
  Komponenty użytkownika i systemu mają minimalne uprawnienia i prawa dostępu wymagane do wykonania określonej czynności.
- **Warstwowe poziomy bezpieczeństwa / Zasada "Defense-in-Depth"**:
  Zagrożenia dla bezpieczeństwa są minimalizowane nie tylko przez pojedynczy środek zaradczy, ale przez kilka zróżnicowanych i uzupełniających się środków bezpieczeństwa.
- **Zasada redundancji:**
  Systemy są zaprojektowane w taki sposób, aby awaria jednego elementu nie miała wpływu na funkcjonowanie systemów bezpieczeństwa. Prawdopodobieństwo i dotkliwość problemów (np. ataków typu "odmowa usługi") spowodowanych nadmiernym zużyciem zasobów systemowych należy odpowiednio zminimalizować.

Produkty WAGO oparte na ETHERNET zostały zaprojektowane do pracy w zamkniętej przemysłowej sieci komunikacyjnej. Jeśli urządzenia nie będą używane tylko w zamkniętych, przemysłowych sieciach, integrator i operator muszą podjąć dodatkowe środki bezpieczeństwa, aby zapewnić optymalne wykorzystanie produktów.

Jeżeli sieci przemysłowe są dostępne publicznie (np. poprzez publiczne interfejsy sieciowe w ramach zamkniętej sieci przemysłowej), lub możliwe do odnalezienia (np. przez połączenia transmisji danych przez publiczny ruch danych (Internet)), należy podjąć organizacyjne i techniczne środki bezpieczeństwa w celu ochrony sieci wewnętrznej i spełnienia kryteriów bezpieczeństwa. Środki bezpieczeństwa, które należy podjąć, zależą od spodziewanego ryzyka, powstającego przez potencjalny wpływ zewnętrzny.

Sterowniki PFC100 i PFC200 oferują rozbudowane funkcje bezpieczeństwa, takie jak TLS, SSH, VPN i firewall na bazie hosta. Zintegrowane zabezpieczenie hasłem i bezpieczna komunikacja chronią przed dostępem do funkcji i treści programów, oraz przed wprowadzaniem złośliwego oprogramowania.

Te i inne zabezpieczenia zalecane w niniejszej dokumentacji, pomogą zminimalizować ryzyko awarii ze strony niektórych zagrożeń związanych z maszynami i sprzętem, oraz ułatwią spełnienie opisanych powyżej kryteriów bezpieczeństwa. Oprócz zaleceń, WAGO będzie badać, oceniać i korygować zgłoszone potencjalne luki w zabezpieczeniach, chyba że działania korygujące zakłócą ogólne funkcjonowanie produktu. Informacje w niniejszej dokumentacji są stale aktualizowane.

3.1 Skróty

Tabela 3: Skróty

Skrót	Znaczenie	Opis
AH	Nagłówek uwierzytelniający	Protokół AH zapewnia autentyczność danych do przesłania oraz uwierzytelnienie nadawcy w ramach IPsec (VPN). AH zapewnia integralność i autentyczność danych. Jednak dane użytkownika nie są szyfrowane i dlatego są dostępne dla wszystkich.
BSI	Federalny Urząd ds. Bezpieczeństwa w Technologii Informacyjnej	BSI jest niezależnym i neutralnym organem zajmującym się kwestiami bezpieczeństwa informatycznego w społeczeństwie informacyjnym.
ESP	Encapsulating Security Payload	Protokół ESP jest odpowiedzialny za zapewnienie autentyczności, integralności i poufności pakietów IP, które mają być transmitowane. W przeciwieństwie do protokołu AH, protokół ESP dodatkowo szyfruje dane użytkownika.
IKE	Internet key exchange	IKE jest kluczowym protokołem do wymiany kluczy protokołu internetowego (patrz rozdział "IPsec").
IPsec	Internet Protocol Security	IPsec jest rozszerzeniem protokołu internetowego (IP). Dzięki zaawansowanym mechanizmom szyfrowania i uwierzytelniania, pakiety IP można zabezpieczyć kryptograficznie i transportować przez publiczne i niezabezpieczone sieci.
PSK	Pre-Shared Key	Pre-Shared Key, wstępnie udostępniony klucz oznacza, że klucze do uwierzytelniania i szyfrowania są wymieniane wcześniej między uczestnikami.

Tabela 3: Skróty

Skrót	Znaczenie	Opis
ROOT-CA	Jednostka certyfikująca	Główny urząd certyfikacji sygnuje własny certyfikat. Certyfikat główny (root-CA) tworzy zatem wspólną kotwicę zaufania dla wszystkich podrzędnych certyfikatów.
SA	Security Association	Security Association (bezpieczne połączenie) jest główną podstawą każdego połączenia IPsec. Opisuje, w jaki sposób dwie łączące się strony w sieciach komputerowych mogą komunikować się ze sobą bezpiecznie. Te umowy bezpieczeństwa są ustalane indywidualnie dla nagłówka uwierzytelniania (AH) i ładunku bezpieczeństwa (ESP).
SCEP	Simple Certificate Enrollment Process	SCEP upraszcza proces żądania i wydawania certyfikatów w wewnętrznych zaufanych sieciach. Chodzi o to, że każdy standardowy użytkownik sieci może niezależnie uzyskać swój cyfrowy certyfikat drogą elektroniczną.
SPI	Security Parameter Index	SPI to numer, który wraz z adresem docelowym IP i protokołem bezpieczeństwa definiuje konkretne bezpieczne połączenia (SA).
VPN	Virtual Private Network	Wirtualna sieć prywatna to samodzielna sieć logiczna, w której uczestnicy są przestrzennie od siebie oddaleni, i połączeni przez tunel VPN.
WBM	Web-Based-Management	Urządzenia WAGO mogą być konfigurowane i administrowane przez WWW za pośrednictwem przeglądarki internetowej.

4 Konfiguracja standardowa

Poniżej znajduje się standardowa konfiguracja sterowników. Możliwe zagrożenia wynikające z dostępu sieciowego lub fizycznego opisano w rozdziale "Scenariusze zagrożeń". Wynikające z tego niezbędne środki, podejmowane w celu uniknięcia tych zagrożeń, opisano w rozdziale "Uodpornianie".

4.1 Fizyczne interfejsy

Sterowniki mają fizyczne interfejsy, wymienione w poniższej tabeli.

Urządzenie	Znaczenie
gniazdo karty pamięci	gniazdo karty pamięci SD
RS-232/-485	złącze komunikacyjne
RJ-45 (ETHERNET)	złącze sieciowe ETHERNET
złącze serwisowe	połączenie szeregowe dla czynności serwisowych na urządzeniach WAGO
przycisk resetowania	przycisk krótkiego skoku o różnych funkcjach, w zależności od położenia przełącznika trybu pracy
przełącznik trybu pracy	różne funkcje (RUN, STOP, RESET), w zależności od stanu urządzenia
złącza ETHERNET X1/X2	złącza sieciowe
modem 3G	wewnętrzny modem mobilny (tylko w 750-8207)

Obsługiwane są następujące systemy magistrali obiektowych:

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

Wskazówka

Więcej informacji można znaleźć w instrukcjach obsługi!
Więcej informacji na temat fizycznych interfejsów i magistrali obiektowych można znaleźć w podręcznikach danego sterownika!

4.2 Usługi sieci

Standardowo obsługiwane protokoły lub usługi sterowników wymienione są poniżej. Oprócz tych usług, podpunkt "Usługi specyficzne dla urządzenia" zawiera listę usług wykonywanych tylko przez określone urządzenia.

Wskazówka

Można wyświetlać aktywne porty!
Można wyświetlić aktualnie otwarte aktywne porty, uruchamiając polecenie "netstat -tulp" jako użytkownik "root" na konsoli Linux®!

Tabela 4: Podstawowy serwer konfiguracji

Port	Protokół	Opis	Program
20/TCP 21/TCP	FTP (File Transfer Protocol)	Protokół przesyłania plików[2)]	pure-ftpd
20/TCP 21/TCP	FTPS (File Transfer Protocol over SSL)	Szyfrowany protokół przesyłania plików[2)]	pure-ftpd
22/TCP	SSH (Secure Shell)	Szyfrowany protokół sieciowy do zdalnego dostępu[1)]	dropbear
22/TCP	SFTP (Secure File Transfer Protocol)	Szyfrowany protokół przesyłania plików[1)]	sftp-server
23/TCP	Telnet	Protokół sieciowy do zdalnego dostępu[2)]	busybox
53/TCP 53/UDP	DNS (Domain Name System)	Protokół udostępniania nazw [2)]	dnsmasq
67/UDP	DHCP (Dynamic Host Configuration Protocol)	Protokół parametryzacji urządzenia[2)]	dnsmasq
69/UDP	TFTP (Trivial File Transfer Protocol)	Protokół przesyłania plików[2)]	tftpd
80/TCP	HTTP (Hyper Text Transfer Protocol)	Protokół ładowania stron internetowych[1)]	lighttpd
161/UDP 162/UDP (Trap)	SNMP v1 (Simple Network Management Protocol v1)	Protokół kontroli i monitorowania elementów sieci [2)]	net-smnp
161/UDP 162/UDP (Trap)	SNMP v2c (Simple Network Management Protocol v2c)	Protokół kontroli i monitorowania elementów sieci [2)]	net-smnp
161/UDP 162/UDP (Trap)	SNMP v3 (Simple Network Management Protocol v3)	Protokół kontroli i monitorowania elementów sieci [2)]	net-smnp
443/TCP	HTTPS (Hyper Text Transfer Protocol over SSL)	Protokół bezpiecznego przesyłania stron internetowych [1)]	lighttpd
4500/UDP	IPsec (Internet Protocol Security)	Protokół do łączenia dwóch zaufanych urządzeń/sieci w niezaufanej sieci, np. Internet	ipsec
500/UDP	IKEv2 (Internet-Key-Exchange-Protokoll)	Protokół automatycznej wymiany kluczy dla IPsec	charon
502/TCP 502/UDP	MODBUS	Protokół wymiany danych procesowych (***e!****RUNTIME*)[1)]	codesys3
502/TCP 502/UDP	MODBUS	Protokół wymiany danych procesowych (CODESYS V2)[1,5)]	plclinux_rt
514/UDP	Syslog	Protokół przesyłania komunikatów dziennika [1,4)]	syslog-ng

Tabela 4: Podstawowy serwer konfiguracji

Port	Protokół	Opis	Program
1194/UDP	OpenVPN	Protokół do łączenia dwóch urządzeń/sieci za pośrednictwem niezaufanej sieci, np. Internet.	openvpn
1740/UDP	PLC Handler	Środowisko systemowe ***e!****RUNTIME*[1,2)]	codesys3
2159/TCP	GDB remote serial protocol	Protokół do debugowania zdalnych targetów	gdbserver
2455/TCP	PLC Handler	Środowisko systemowe CODESYS [1,3,5)]	plclinux_rt
4048/TCP	OPC UA (OPC Unified Architecture)	Protokół wymiany danych [3)]	codesys3
6626/TCP	I/O-Check	Własny protokół WAGO do parametryzacji urządzeń 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	Środowisko systemowe ***e!****RUNTIME*[3)]	codesys3
UDP		Port bez funkcji otworzony przez ***e!****RUNTIME* [3)]	codesys3

[1)] Usługa jest aktywna w ustawieniach fabrycznych
[2)] Usługa musi zostać aktywowana przez użytkownika, lub aktywuje się automatycznie, gdy tylko aplikacja (CODESYS/***e!****RUNTIME*-) zostanie uruchomiona na urządzeniu
[3)] Usługa/port zależy od używanego środowiska systemowego
[4)] Usługa/port jest powiązany z hostem lokalnym i nie można go uzyskać z zewnątrz
[5)] Dostępne tylko dla PFC200

Tabela 5: Podstawowa konfiguracja klienta

Port	Protokół	Opis	Program
52/TCP 52/UDP	DNS (Domain Name System	Protokół udostępniania nazw	-
68/UDP	DHCP (Dynamic Host Configuration Protocol)	Protokół parametryzacji urządzenia	busybox
69/UDP	TFTP (Trivial File Transfer Protocol)	[2)]	busybox
123/UDP	SNTP/NTP (Network Time Protocol)	Protokół synchronizacji czasu w sieci	ntpclient
1883/TCP 8883/TCP	MQTT (Message Queue Telemetry Transport)	Protokół do komunikacji maszyna-maszyna	dataagent
4500/UDP	IPsec (Internet Protocol Security)	Protokół do łączenia dwóch zaufanych urządzeń/sieci w niezaufanej sieci, np. Internet	Ipsec
514/UDP	Syslog	Protokół przesyłania komunikatów dziennika [1,4)]	syslog-ng
1194/UDP	OpenVPN	Protokół do łączenia dwóch urządzeń/sieci za pośrednictwem niezaufanej sieci, np. Internet.	openvpn

[1)] Klient jest aktywny w ustawieniach fabrycznych
[2)] Klient musi zostać aktywowany przez użytkownika, lub aktywuje się, gdy tylko aplikacja (CODESYS/***e!****RUNTIME*) zostanie uruchomiona na urządzeniu
[3)] Klient zależy od używanego środowiska systemowego
[4)] Klient jest powiązany z hostem lokalnym i nie można go uzyskać z zewnątrz

4.2.1 Usługi specyficzne dla urządzenia

Tabela 6: Zastosowania dla PFC100/PFC200

Urządz.	Port	Protokół	Opis	Program
PFCx00	102/TCP	IEC 61850	Protokół transmisji między systemami sterowania i urządzeniami zdalnymi (telesterowanie)	CODESYS V2.3
PFCx00	2404/TCP 2404/UDP	IEC 60870-5-104		
PFCx00	20000/TCP 20000/UDP	DNP3 (Distributed Network Protocol)		

4.3 Użytkownicy i hasła

Poniższe rozdziały opisują domyślnych użytkowników różnych usług sterownika.

4.3.1 Użytkownicy WBM

WBM ma własną administrację użytkownika. Występujący tu użytkownicy są ze względów bezpieczeństwa odseparowani od pozostałych grup w systemie.
Nie można tworzyć nowych użytkowników; istniejący użytkownicy są trwale zapisani w aplikacji. Informacje na temat zmiany haseł znajdują się w rozdziale "Uodpornianie" > ...> "Zmiana haseł w systemie zarządzania przez WWW".

Tabela 7: Użytkownicy WBM

Użytkownik	Uprawnienia	Standardowe hasło
admin	pełne (administrator)	wago
user	ograniczone	user
guest	tylko wyświetlanie	Logowanie niedozwolone. Stosowane, gdy logowanie nie nastąpiło.

4.3.2 Użytkownicy systemu Linux®

Grupa użytkowników systemu Linux® obejmuje użytkowników systemu operacyjnego. Usługi oferowane przez urządzenie są wykonywane na podstawie własnego użytkownika, który jest zablokowany do logowania. Można dodać dodatkowych użytkowników.

Wskazówka

Hasła dla użytkowników usług
Logowanie takich użytkowników usług jak www, messagebus, rpcuser, nobody lub opc, jest zablokowane. Tych haseł nie należy zmieniać!

Użytkownik	Charakterystyka	Standardowe hasło
root	administrator	wago
admin	użytkownik Runtime CODESYS	wago
user	użytkownik	user

Informacje na temat zmiany haseł znajdują się w rozdziale "Uodpornianie“ > … > „Zmiana hasła Linux® przy użyciu konsoli Linux®".

4.3.3 Użytkownicy SNMP

Usługa SNMP ma własne zarządzanie użytkownikami. W ustawieniach fabrycznych nie ma założonych żadnych użytkowników.

Informacja

Więcej informacji można znaleźć w instrukcji obsługi produktu!
Więcej informacji na temat usług SNMP można znaleźć w instrukcji sterownika na stronie www.wago.com!

4.3.4 CODESYS i wizualizacja internetowa *e!RUNTIME*

W przypadku wizualizacji internetowej CODESYS i ***e!****RUNTIME* można ustawić hasło dla każdego projektu, dla każdej grupy roboczej.

Informacja

Użytkownicy i hasła nie są tworzone automatycznie!
Użytkownicy i hasła do wizualizacji CODESYS i ***e!****RUNTIME* muszą zostać stworzeni przez użytkownika końcowego!

5 Scenariusze zagrożeń - zagrożenia dla przemysłowych systemów sterowania

W tym rozdziale opisano potencjalne scenariusze zagrożeń, które mogą wystąpić podczas łączenia się z siecią publiczną, np. z Internetem. Ponadto, w oparciu o opisane scenariusze, zalecamy rozwiązania (Defense-in-Depth) i konkretne środki zaradcze dla sterowników.

Poniższa lista stworzona przez BSI podaje przykłady krytycznych zagrożeń dla przemysłowych systemów sterowania. W rozdziale tym kładzie się nacisk na bezpośrednie zagrożenia dla sterowników.

- inżynieria społeczna i phishing
- infiltracja złośliwego oprogramowania za pośrednictwem wymiennych nośników i sprzętu zewnętrznego*
- infekowanie złośliwym oprogramowaniem za pośrednictwem Internetu i intranetu*
- włamanie przez zdalny dostęp konserwacyjny
- błąd ludzki i sabotaż
- elementy sterujące podłączone do Internetu*
- błędy techniczne i siła wyższa
- dyskredytacja ekstranetu i komponentów chmury
- ataki (D)DoS*
- dyskredytacja smartfona w środowisku produkcyjnym

* bezpośrednie zagrożenie dla sterownika

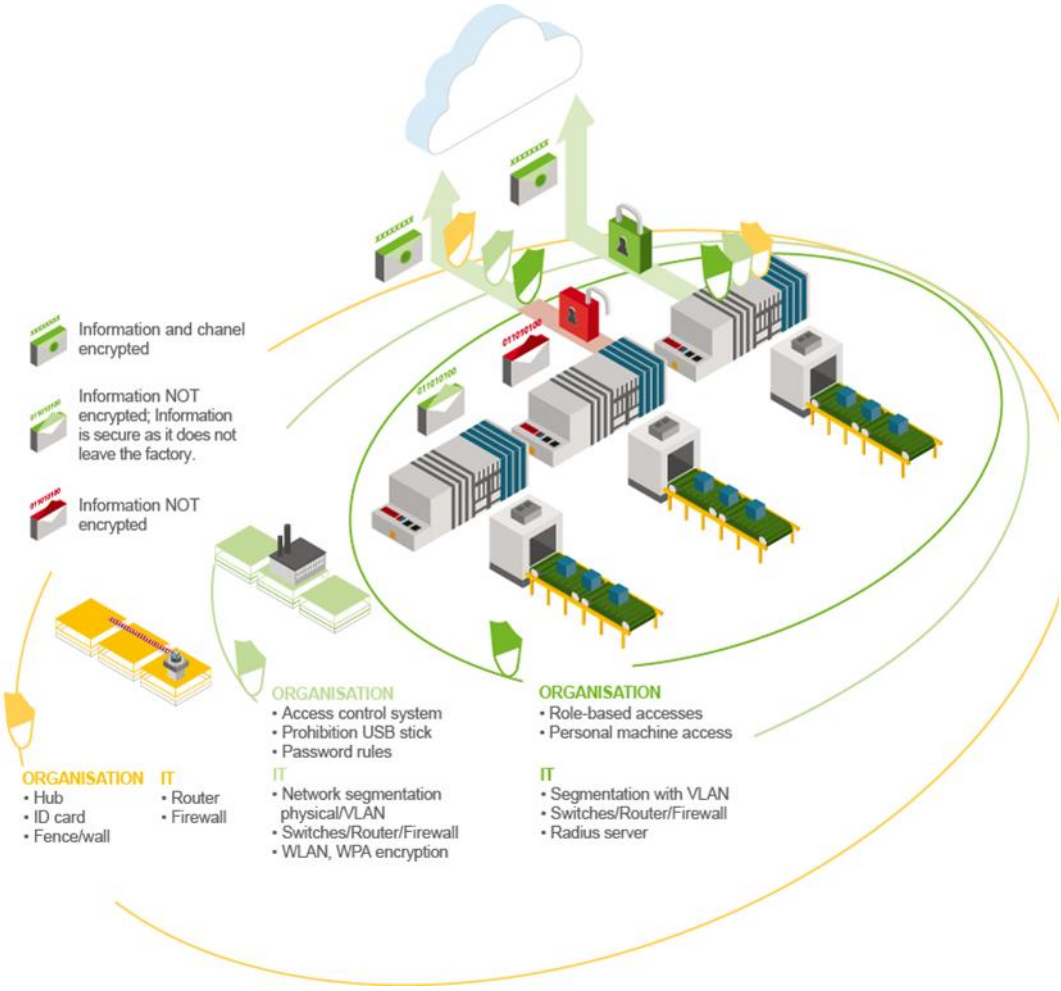
Aby osiągnąć poziom ochrony, który stanowi przeciwwagę dla większości zagrożeń, należy zastosować podejście holistyczne, zgodne z zasadą Defense-in-Depth.

Wskazówka

W celu uzyskania dalszych informacji, należy zwrócić uwagę na zalecenia BSI!
Aby uzyskać więcej informacji, zapoznaj się z zaleceniem "IT w produkcji" wydanym przez Federalny Urząd ds. Bezpieczeństwa Informacji> "Bezpieczeństwo systemu sterowania w przemyśle, 10 najważniejszych zagrożeń i środków zaradczych 2016".

5.1 Zasada Defense-in-Depth

Zarządca infrastruktury musi traktować całościowo wymienione na liście BSI zagrożenia dla przemysłowych systemów sterowania. Infrastruktura jest bezpieczna tylko wtedy, gdy zarówno organizacyjne, jak i techniczne środki bezpieczeństwa wdrażane są w sposób kompleksowy i wzajemnie się uzupełniają. W ten sposób można zapobiec dyskredytacji całego systemu lub urządzenia, wskutek sforsowania jakiegoś środka bezpieczeństwa. Zasada Defense-in-Depth może być zastosowana do całej architektury operatora, a także do pojedynczego sterownika.



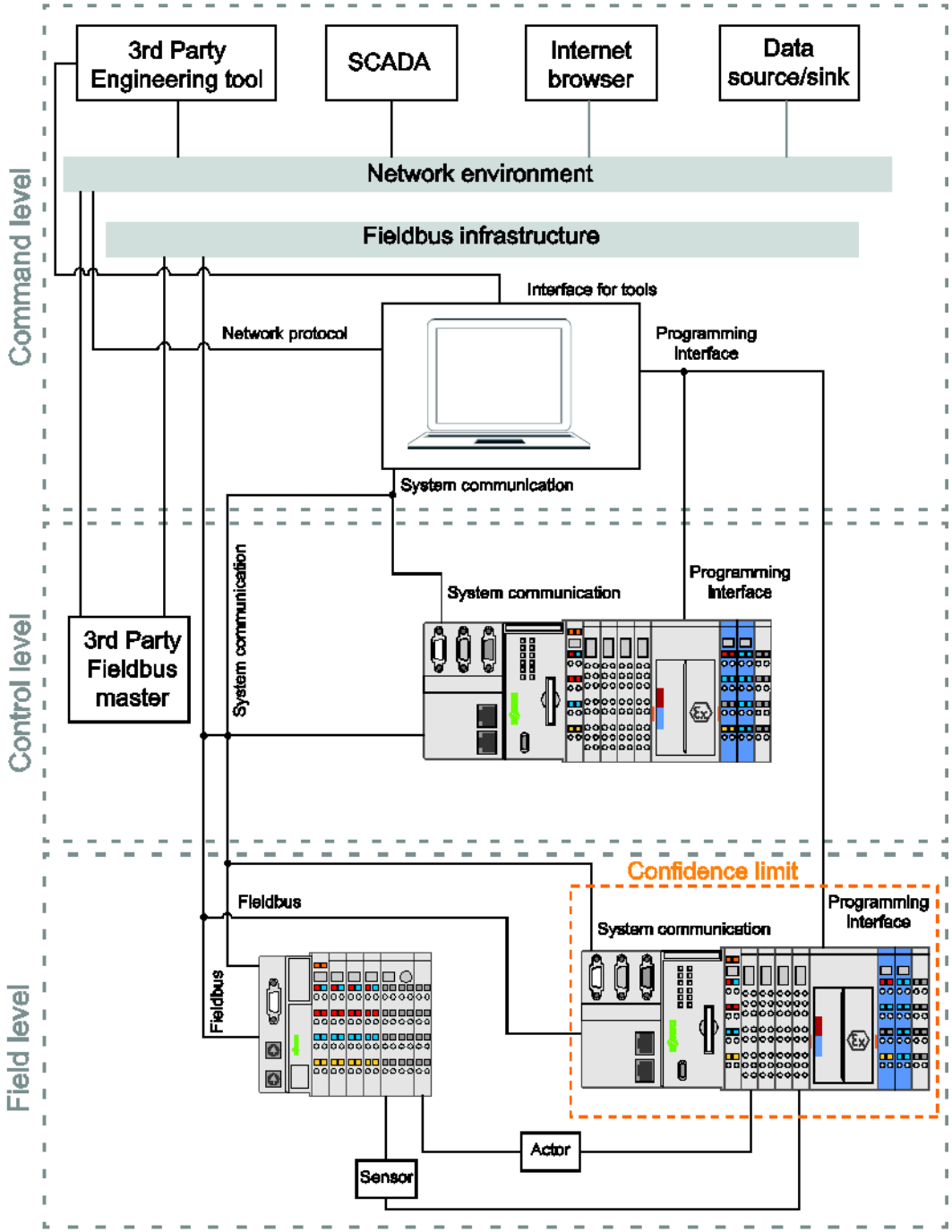
Rys. 1: Model cebuli

Ilustracja "Model cebuli" pokazuje przykład infrastruktury, która jest chroniona kompleksowymi środkami bezpieczeństwa. W najbardziej zewnętrznej warstwie (żółtej), ochrona dostępu fizycznego jest reprezentowana w postaci kontroli dostępu. Fizyczna ochrona dostępu dba o to, aby osoby nieupoważnione nie mogły łatwo dostać się do krytycznych urządzeń. Środkowa warstwa (jasnozielona) przedstawia wytyczne i procesy w połączeniu z technicznymi środkami zabezpieczenia sieci. Środki te stanowią dodatkowe utrudnienie dla potencjalnego agresora. Jednakże, jeśli agresor wniknie aż do sterowników, środki bezpieczeństwa na poziomie sterowników mogą dalej minimalizować ryzyko dyskredytacji (ciemnozielona warstwa). Poniżej rozważane są jedynie zagrożenia i potencjalne mechanizmy bezpieczeństwa na poziomie sterowania.

Wskazówka

Więcej informacji na temat cyberbezpieczeństwa w zakładach produkcyjnych!
Szczegółowe środki wdrażania cyberbezpieczeństwa w produkcji opisano w białej księdze "Bezpieczeństwo IT w zakładach produkcyjnych". Można pobrać ten dokument na stronie https://www.wago.com/downloads.

5.2 Określone zagrożenia odniesione do architektury referencyjnej



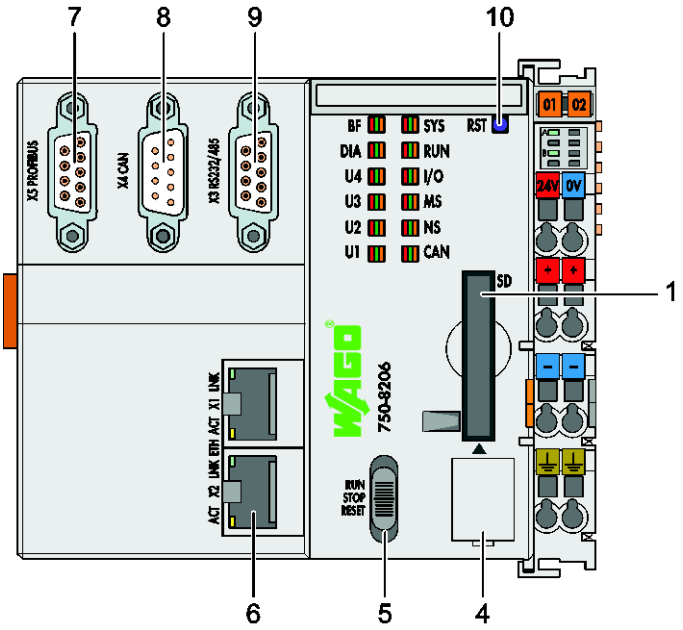
Rys. 2: Architektura referencyjna

Architektura referencyjna przedstawia klasyczne środowisko aplikacji, w którym stosowane są systemy sterowania WAGO.

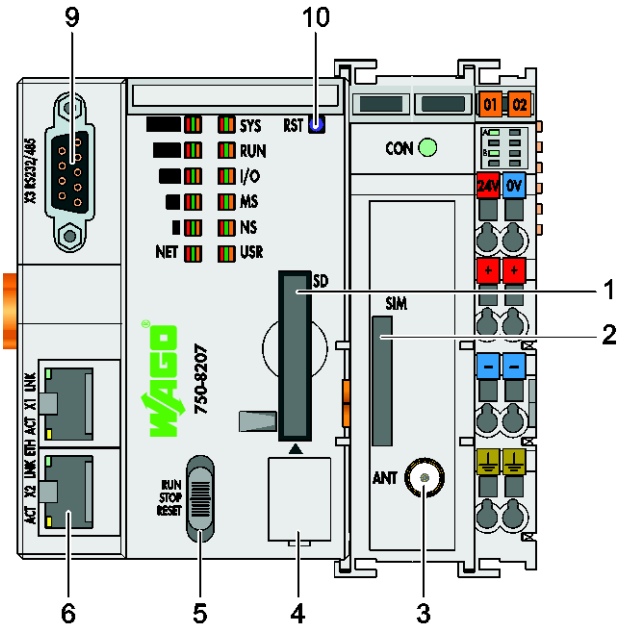
Tak zwana granica zaufania reprezentuje przejście z obszaru zaufanego do niezaufanego, a tym samym oddziela różne poziomy zabezpieczeń. Granica zaufania ma szczególne znaczenie, ponieważ możliwe ataki mogą wystąpić w trakcie przechodzenia z lub do innego obszaru. Różne złącza, których sterownik używa do komunikacji z innymi systemami, stanowią dla niego potencjalne zagrożenie.

Poniżej opisano scenariusze możliwych cyberataków, które mogą wystąpić zarówno poprzez fizyczny, jak i sieciowy dostęp do sterownika. Jeśli agresor ma fizyczny dostęp do sterownika, interakcja może odbywać się za pośrednictwem złączy, przez dodatkowo podłączone urządzenia wejściowe.

5.2.1 Fizyczne interfejsy na sterowniku WAGO



Rys. 3: Fizyczne interfejsy na sterowniku WAGO



Rys. 4: Fizyczne interfejsy na sterowniku WAGO z interfejsem modemu GSM/3G

1 gniazdo na kartę pamięci
2 gniazdo karty SIM
3 antena
4 złącze serwisowe
5 przełącznik trybu pracy
6 złącza ETHERNET
7 złącze sieci obiektowej – PROFIBUS DP
8 złącze sieci obiektowej – CANopen
9 moduł interfejsu szeregowego (RS-232)
10 przycisk resetowania

Wskazówka **Podręczniki dla sterowników WAGO!**
Szczegółowe informacje na temat sterowników można znaleźć w odpowiednich podręcznikach produktów, na stronie www.wago.com.

5.2.1.1 Przycisk resetowania

Za pomocą przycisku resetowania (**10**) można wykonać różne funkcje w zależności od położenia przełącznika trybu. Aby uniemożliwić reset urządzenia do ustawień fabrycznych, co dezaktualizuje hasła, dostęp do przycisku resetowania powinien być ograniczony do osób upoważnionych.

Wskazówka **Ograniczenie dostępu do szafy sterowniczej!**
Zamontuj sterownik w szafie sterowniczej i upewnij się, że tylko ograniczona grupa osób ma do niej dostęp!

Ustawienia sieciowe i następujące hasła mogą być resetowane:
- „admin“ (Linux),
- „admin“ (WBM)
- „user“ (WBM)

Następujące hasła nie mogą być resetowane:
- „root“ (Linux)
- „user“ (Linux)

5.2.1.2 Przełącznik trybu pracy

Za pomocą przełącznika trybu pracy (**5**) można wybierać pomiędzy trybami pracy STOP, RUN i RESET. Aby uniknąć ataku "Denial of Service" (DoS) na działającą aplikację CODESYS lub ***e!****RUNTIME*, dostęp do selektora trybu powinien być ograniczony do autoryzowanej grupy osób.

Wskazówka **Ograniczenie dostępu do szafy sterowniczej!**
Zamontuj sterownik w szafie sterowniczej i upewnij się, że tylko ograniczona grupa osób ma do niej dostęp!

5.2.1.3 Złącza ETHERNET (X1 / X2)

Dwa złącza ETHERNET (**6**) sterownika mogą pracować w trybie switch lub jako oddzielne złącza. W ustawieniach fabrycznych aktywowany jest tryb switch. Przegląd usług sieciowych można znaleźć w rozdziale "Konfiguracja standardowa"> "Usługi sieciowe".

Jeśli porty ETHERNET nie są używane, można ograniczyć ich funkcję poprzez konfigurację, patrz rozdział "Uodpornianie"> ...> "Ograniczanie dostępu przez interfejsy sieciowe".

Wskazówka

Należy przestrzegać wskazówek dotyczących bezpieczeństwa dla urządzeń ETHERNET!
Należy przestrzegać wskazówek bezpieczeństwa WAGO dla urządzeń opartych na ETHERNET zawartych na stronie https://www.wago.com/en/automation-technology/security.

5.2.1.4 Złącze serwisowe

Złącze serwisowe (**4**) jest przeznaczone do używania protokołu serwisowego WAGO. Pozwala ono na skonfigurowanie systemu za pomocą oprogramowania "WAGO Ethernet Settings", "WAGO-I/O-*Check*" lub ***e!****COCKPIT.*

Jeśli złącze serwisowe nie jest używane, powinno zostać ze względów bezpieczeństwa wyłączone, aby zminimalizować ryzyko ataku, zobacz "Uodpornianie"> ... "Wyłącz interfejs serwisowy".

5.2.1.5 Moduł interfejsu szeregowego (RS-232)

Złącze komunikacyjne RS-232 (9) nie jest domyślnie przypisane i jest przeznaczone do użytku w systemie runtime CODESYS lub ***e!****RUNTIME.*

Jeśli port szeregowy nie jest używany, nie powinien być przypisywany (unassigned), patrz rozdział "Uodpornianie"> ...> Wyłączanie konsoli Linux® na porcie szeregowym ".

Wskazówka

Złącze komunikacyjne RS-232 nie zawsze jest dostępne!
Zwróć uwagę, że interfejs RS-232 nie jest dostępny na wszystkich urządzeniach!

5.2.1.6 Gniazdo na kartę pamięci

Sterowniki mają gniazdo kart pamięci (1). Agresor może uruchomić system z karty SD za pomocą spreparowanej karty SD. Po zainstalowaniu karty SD, sterownik zasadniczo uruchamia się z niej. Danymi w wewnętrznej pamięci flash można w ten sposób manipulować albo może dojść do ataku na aplikację sterującą. Taka manipulacja jest trudna lub niemożliwa do wykrycia.

Wskazówka

Ograniczenie dostępu do szafy sterowniczej!
Zamontuj sterownik w szafie sterowniczej i upewnij się, że tylko ograniczona grupa osób ma do niej dostęp!

5.2.1.7 Interfejs modemu GSM / 3G

Niektóre sterowniki mają dodatkowy moduł modemu z gniazdem do karty SIM (2) i gniazdem SMA do anteny (3) w celu korzystania z funkcji telekomunikacji mobilnej. Karta SIM powinna być chroniona przed nieautoryzowanym dostępem za pomocą numeru PIN.

Wskazówka

Ograniczenie dostępu do szafy sterowniczej!
Zamontuj sterownik w szafie sterowniczej i upewnij się, że tylko ograniczona grupa osób ma do niej dostęp!

Wskazówka

Sygnał anteny w szafie sterowniczej może być zbyt słaby!
Upewnij się, że sygnał anteny jest wystarczający, jeśli urządzenie będzie schowane w szafie sterowniczej. Jeśli sygnał anteny jest zbyt słaby, nie ma dostępu do sieci komórkowej!

5.2.2 Dostęp przez sieć

W tym rozdziale opisano potencjalne cyberataki oparte na dostępie sieciowym, takie jak ataki za pośrednictwem sieci lokalnych. Rosnąca złożoność i powszechny dostęp do sieci uczestników komunikacji w obrębie sieci wielowarstwowych (patrz rysunek "Architektura referencyjna") może stanowić wielorakie zagrożenie bezpieczeństwa systemu atakami cyberprzestępców. Ponieważ sterowniki przemysłowe są coraz gęściej połączone siecią korporacyjną, stają się dodatkowym celem ataku.

5.2.2.1 Elementy oprogramowania

Luki w użytkowanym oprogramowaniu stanowią potencjalne zagrożenie, ponieważ mogą ułatwiać wniknięcie złośliwego kodu lub przeprowadzenie ataków typu DoS.

Aby przeciwdziałać tym zagrożeniom, zaleca się aktualizowanie oprogramowania sterownika (na przykład poprzez aktualizację firmware`u). Regularnie aktualizuj system za pomocą łat dostarczonych przez WAGO Kontakttechnik GmbH & Co. KG. Ponadto, wykonuj procedury uodpornienia systemu, które sprawią, że sterownik będzie bezpieczniejszy.

Aby uzyskać aktualną listę pakietów Linux® sterownika, możesz uruchomić następujące polecenie na konsoli Linux®:

„ipkg list".

5.2.2.2 Ataki typu "Man-in-the-middle"

Ataki typu "Man-in-the-middle" są atakami na kanał komunikacyjny między dwoma komunikującymi się partnerami. Agresor udaje, że jest godnym zaufania źródłem, więc dwaj komunikujący się partnerzy nie są w stanie wykryć, że komunikują się z agresorem. W ten sposób agresor może odczytać i manipulować wszystkimi przesyłanymi informacjami.

Aby zapewnić optymalne bezpieczeństwo sterowników, zaleca się zmianę konfiguracji TLS ze "Standard" na "Strong", patrz rozdział "Uodpornianie"> ...> "Szyfrowanie TLS". Ponadto zaleca się wymianę generycznego certyfikatu TLS, patrz rozdział "Uodpornianie"> ...> Tworzenie i wymiana certyfikatów.

5.2.2.3 Interfejsy sieciowe i protokoły

Skanery portowe mogą być wykorzystywane przez cyberprzestępców do sprawdzania obcych komputerów pod kątem dostępności poprzez otwarte interfejsy. Każdy otwarty interfejs stwarza potencjalne zagrożenie, ponieważ przez nie używane usługi sieciowe można uzyskać dostęp do systemu.

Aby zablokować niektóre interfejsy sieciowe/protokoły, które nie są potrzebne w określonym środowisku aplikacji, można użyć firewalla. Więcej informacji na ten temat zamieszczono w rozdziale „Uodpornianie“ < … > „Konfiguracja firewalla“.

Przegląd wszystkich usług sieciowych używanych domyślnie przez WAGO, można znaleźć w rozdziale "Konfiguracja standardowa" ...> "Usługi sieciowe".

Wskazówka

Należy przestrzegać wskazówek bezpieczeństwa dla sterowników WAGO z dostępem sieciowym!
Informacje dotyczące bezpieczeństwa dla sterowników WAGO z dostępem sieciowym można znaleźć na stronie https://www.wago.com/de/automatisierungstechnik/security

5.2.2.4 Firewall

Firewall umożliwia ustawienie zabezpieczenia przed połączeniami niebezpiecznymi i/lub szkodliwymi. Reguła firewalla powinna zawsze być skonfigurowana restrykcyjnie, aby ograniczyć dostęp do określonego złącza sieciowego. Dostęp do złącza sieciowego powinien być ograniczony tylko do pojedynczych komputerów lub podsieci, które potrzebują dostępu do usługi. Więcej informacji na temat reguł firewalla można znaleźć w rozdziale "Uodpornianie"> Konfigurowanie firewalla".

5.2.3 Dostęp za pośrednictwem użytkowników i haseł

Wskazówka

Zmiana haseł
Ustawione fabrycznie standardowe hasła dla wszystkich użytkowników podane są w niniejszej instrukcji i nie stanowią wystarczającego zabezpieczenia! Zmień hasła zgodnie z Twoimi wymaganiami przy pierwszym uruchomieniu!

Zabezpieczenie za pomocą standardowych haseł, lub haseł o niskiej złożoności nie zapewnia odpowiedniej ochrony. Potencjalny agresor może z łatwością ominąć ochronę hasłem i uzyskać dostęp do konta użytkownika z odpowiednimi uprawnieniami.

Wymienione poniżej usługi mają własną administrację użytkownika wraz z kontami użytkowników:

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

Zalecenia dotyczące bezpiecznych haseł:

- Zmieniaj hasło regularnie
- Użyj co najmniej ośmiu znaków
- Nie zapisuj hasła w postaci zwykłego tekstu na dysku twardym
- Użyj jak największej liczby różnych znaków, małych i wielkich liter oraz znaków specjalnych i cyfr
- Hasło nie powinno odnosić się do informacji osobistych - na przykład bez imion i dat urodzin

Informacja

Więcej informacji znajdziesz w Narodowym Instytucie Standardów i Technologii (NIST)!
NIST podaje wskazówki dotyczące bezpiecznych haseł w "NIST Special Publication 800-63B" w sekcji "Authentikator and Verifier Requirements"! (https://pages.nist.gov/800-63-3/sp800-63b.html)

6 Uodpornianie systemu

Uodpornianie systemu (Hardening) oznacza zwiększanie jego bezpieczeństwa, poprzez szereg środków mających na celu lepszą ochronę przed zagrożeniami, patrz rozdział "Zagrożenia dla przemysłowych systemów sterowania".

Sterowniki WAGO oparte są na systemie Linux®. System operacyjny Linux® oferuje wiele usług sieciowych, które nie powinny być dostępne dla każdego systemu i każdego użytkownika. Aktywne powinny być tylko niezbędne procesy z minimalnymi uprawnieniami. Poniżej przedstawione są niektóre działania, które pomogą zredukować do minimum krytyczne aspekty bezpieczeństwa Twojego systemu.

Wskazówka

Ten dokument nie może być uznany za kompletny!
Upewnij się, że kontrola bezpieczeństwa Twojej aplikacji jest przeprowadzana zgodnie z Twoimi wymaganiami!

6.1 Ograniczenie dostępu fizycznego

6.1.1 Wyłączanie złącza serwisowego

Złącze serwisowe służy między innymi do komunikacji z oprogramowaniem WAGO-I / O-CHECK i ustawieniami WAGO-ETHERNET. Jeśli złącze serwisowe nie jest używane na stałe, powinno być wyłączone, patrz także rozdział "Zagrożenia dla przemysłowych systemów sterowania"> "Określone zagrożenia w odniesieniu do architektury odniesienia".

Wskazówka

Złącze serwisowe może być wyłączony tylko przez administratora!
Aby dezaktywować złącze serwisowe, potrzebujesz autoryzacji administratora!

1. W WBM wybierz punkt menu **Administration** > **Service Interface** aby wyłączyć złącze serwisowe.

Rys. 5: Wyłączanie złącza serwisowego

2. W obszarze „Assign Owner of Service Interface“ zaznacz pole wyboru **Unassigned.**To powoduje, że złącze szeregowe nie jest przypisane do żadnej aplikacji i jest możliwe, aby na przykład program CODESYS mógł uzyskać do niego dostęp za pośrednictwem bloków funkcyjnych.

3. Naciśnij przycisk **[Change Owner].**

4. Zrestartuj sterownik, aby zastosować zmianę.

6.1.2 Wyłączanie konsoli Linux® na porcie szeregowym

Sterownik ma złącze szeregowe RS-232, które można skonfigurować dla różnych funkcji. W wersji fabrycznej nie jest przypisane i może być używane przez takie aplikacje, jak np. CODESYS. Alternatywnie port szeregowy można przypisać do systemu Linux®, w wyniku czego udostępniony będzie wiersz poleceń systemu Linux®. To ustawienie umożliwia użycie portu szeregowego do komunikacji z konsolą Linux®.

Jeśli port szeregowy jest skonfigurowany do innych aplikacji, dostęp do konsoli jest zablokowany. Jeśli port szeregowy nie jest używany regularnie w celu uzyskania dostępu do konsoli, zaleca się wyłączenie powiązania portu szeregowego z konsolą.

Wskazówka

Konsola systemu Linux® może być wyłączona tylko przez administratora!
Aby dezaktywować konsolę Linux® potrzebujesz uprawnień administratora !!

1. W WBM wybierz **Administration > Serial Interface**, aby wyłączyć dostęp do konsoli Linux®.

2. Zaznacz pole wyboru **[Unassigned]**.
   Gwarantuje to, że zącze szeregowe nie zostanie przypisane do wiersza poleceń

Rys. 6: Wyłączanie konsoli Linux®

3. Kliknij przycisk **[Change Owner],** aby zastosować zmianę.

6.2 Bezpieczny dostęp do sieci

6.2.1 Komunikacja szyfrowana

6.2.1.1 Uwierzytelnianie serwera WWW

Strony WBM sterownika można otwierać przy pomocy protokołu HTTP lub HTTPS. Preferowany jest HTTPS, gdyż wykorzystuje on protokół TLS. Protokół TLS zabezpiecza komunikację poprzez kodowanie i uwierzytelnienie.

Standardowe ustawienie sterownika umożliwia zaawansowane kodowanie, wykorzystuje jednak tylko zwykłe metody uwierzytelnienia. Ponieważ uwierzytelnianie odgrywa kluczową rolę dla wszystkich bezpiecznych kanałów komunikacyjnych, zdecydowanie zaleca się bezpieczniejszy rodzaj uwierzytelnienia. Bazą uwierzytelnienia jest certyfikat bezpieczeństwa zapisany w sterowniku. Domyślną lokalizacją certyfikatu bezpieczeństwa jest /etc/lighttpd/https-cert.pem.

W ustawieniu fabrycznym, sterownik używa generycznego certyfikatu bezpieczeństwa w formacie x509. Aby umożliwić bezpieczne uwierzytelnienie, generyczny certyfikat bezpieczeństwa należy zastąpić specyficznym dla danego urządzenia.

6.2.1.2 Szyfrowanie TLS

Podczas nawiązywania połączenia HTTPS przeglądarka internetowa i serwer WWW negocjują wersję TLS i metodę kryptograficzną.

Poprzez grupę "TLS Configuration" strony WBM "Security" można przełączać dopuszczone przez HTTPS procedury kryptograficzne i użyteczne wersje TLS.

Możliwe są ustawienia "Strong" i "Standard". Przy ustawieniu "Strong" serwer internetowy zezwala tylko na wersję TLS 1.2 i na silne algorytmy. Starsze oprogramowanie i starsze systemy operacyjne mogą nie obsługiwać protokołu TLS 1.2 i algorytmów szyfrowania. Ustawienie "Standard" zezwala na wersje TLS 1.0, TLS 1.1, TLS 1.2, a także metody kryptograficzne, które obecnie nie są już uważane za bezpieczne. Użycie jest zalecane tylko w przypadku zgodności wstecznej ze starszymi systemami.

Informacja

Wytyczna TR-02102 BSI
Zasady dotyczące ustawienia "Strong" są oparte na wytycznej technicznej TR-02102 Federalnego Urzędu ds. Bezpieczeństwa Informacji. Wytyczne można znaleźć w Internecie pod adresem: https://www.bsi.bund.de> "Publikacje"> "Wytyczne techniczne".

Informacja

Wytyczne BSI dotyczące migracji do TLS 1.2

Wytyczne Federalnego Urzędu ds. Bezpieczeństwa Informacji dotyczące migracji do TLS 1.2 zawierają "matryce zgodności", które określają, które oprogramowanie jest zgodne z TLS 1.2.

Przewodnik można znaleźć w Internecie pod adresem: https://www.bsi.bund.de> "Tematy"> "Standardy i kryteria"> "Minimalne standardy".

Dla optymalnego bezpieczeństwa zaleca się zmianę konfiguracji TLS w systemie zarządzania przez WWW z ustawienia "Standard" na "Strong".

1. Przejdź w WBM do menu **Security** > **TLS Configuration**.

2. Aktywuj pole **Strong**.

Rys. 7: Zmiana konfiguracji TLS

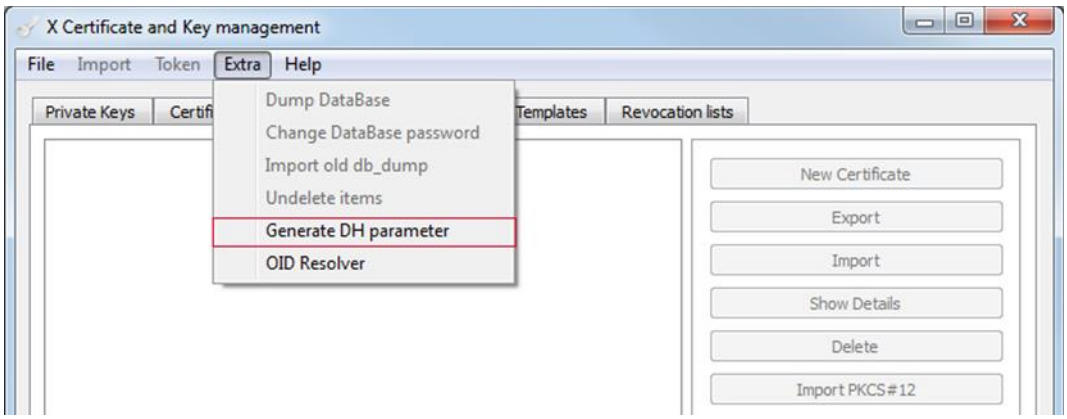
3. Kliknij przycisk **[Submit]**, aby zastosować zmianę.

6.2.1.3 Tworzenie parametrów Diffiego-Hellmana

Protokół Diffiego-Hellmana jest metodą ustalania wspólnego klucza cyfrowego. W takim przypadku nie jest przesyłany tajny klucz sesji, a jedynie wynik operacji arytmetycznej. Dzięki temu dwóch użytkowników komunikacji może bezpiecznie komunikować się za pośrednictwem publicznej sieci. Używają wybranej przez siebie metody szyfrowania, która wykorzystuje klucz wspólny, uzgodniony metodą Diffiego-Hellmana.

Możesz wygenerować parametry Diffiego-Hellmana za pomocą oprogramowania do zarządzania kluczami XCA.

1. Otwórz oprogramowanie XCA i wybierz z menu **Extra** podmenu **Utwórz parametr DH**.

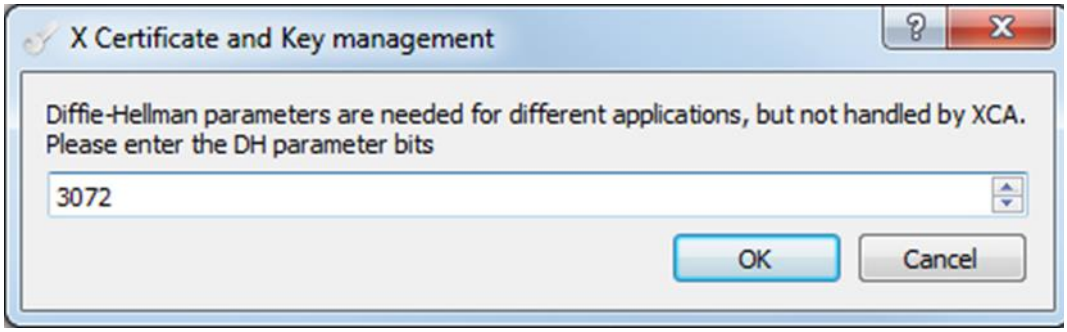


Rys. 8: Tworzenie parametrów Diffiego-Hellmana

2. Wybierz klucz długości co najmniej 2000 bitów.

Wskazówka

Należy przestrzegać wymagań dot. długości klucza!
W przypadku planowanego użycia po roku 2022, długość klucza powinna wynosić co najmniej 3000 bitów, patrz BSI TR 02102-1, strona 56/57, "7.2.1. Diffiego-Hellmana"!



Rys. 9: Długość klucza, parametry DH

Wskazówka

Tworzenie parametrów może potrwać dłużej!
W zależności od wybranego rozmiaru klucza, tworzenie parametrów DH może zająć dużo czasu!

Parametry "p" i "g" są tworzone w tle. Po zakończeniu otwiera się okno dialogowe do zapisywania parametrów. Parametry "p" i "g" nie muszą być utrzymywane w tajemnicy i mogą być przesyłane przez niezabezpieczone połączenie. W wymianie kluczy metodą Diffiego-Hellmana, każdy z partnerów komunikacji wybiera każdy tajny numer oprócz parametrów "p" i "g". Od publicznego i tajnego numeru każdorazowo obliczana jest nowa liczba. Nowe numery są wymieniane ponownie w celu utworzenia wspólnego, tajnego klucza "k", który nie jest dostępny dla stron trzecich.

Wymiana kluczy Diffiego-Hellmana jest używana do połączeń SSL / TLS, patrz rozdział "OpenVPN", a także do serwera WWW, patrz następny rozdział.

6.2.1.3.1 Wymiana parametrów Diffiego-Hellmana dla serwera WWW

Można zamienić wygenerowane parametry Diffiego-Hellmana (patrz rozdział "Generowanie parametrów Diffiego-Hellmana") dla serwera WWW, na własne:

1. Załaduj wygenerowane parametry przez SCP / FTPS / SFTP do kontrolera w następującym folderze:
   / Etc / lighttpd /

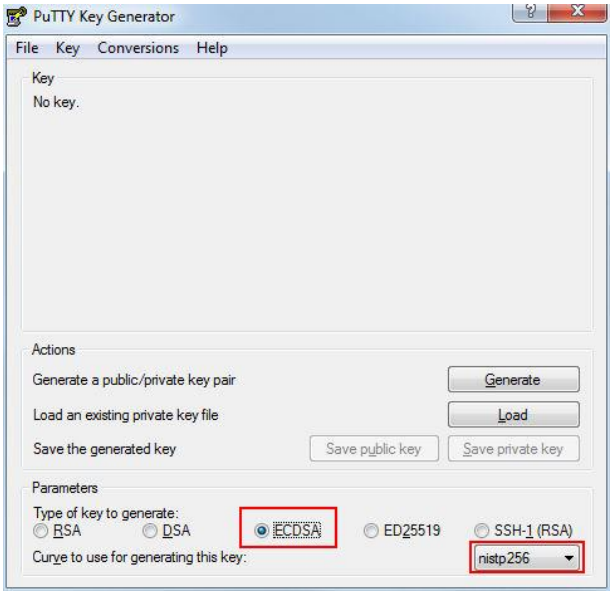
2. Podaj plik parametrów w plikach konfiguracyjnych tls-strong.conf i tls-standard.conf w kluczu ssl.dh:
   ssl.dh-file = "/ etc / lighttpd / <nazwa twojego pliku parametrów dh>"

3. Na koniec zrestartuj serwer WWW:
   /etc/init.d/lighttpd stop
   /etc/init.d/lighttpd start

6.2.1.4 Uodpornianie dostępu do SSH

Oprócz uwierzytelniania nazwy użytkownika i hasła, SSH obsługuje również uwierzytelnianie na podstawie pary kluczy prywatny/publiczny. Można utworzyć klucze np. za pomocą bezpłatnego programu Windows "Putty Key Generator" (Putty v0.68 lub nowszy, krok 1-10). Ponadto należy zablokować login użytkownika root (patrz rozdział "Uodpornianie dostępu do SSH"> "Odmowa logowania przez root logowania") i zmienić port domyślny (patrz rozdział "Zmiana standardowych portów sieciowych").

1. Uruchom narzędzie PuTTY - PuTTYgen:



Rys. 10: Uruchomienie PuTTYgen

2. Wybierz typ generowanego klucza (ECDSA) i krzywą eliptyczną (nistp 256).

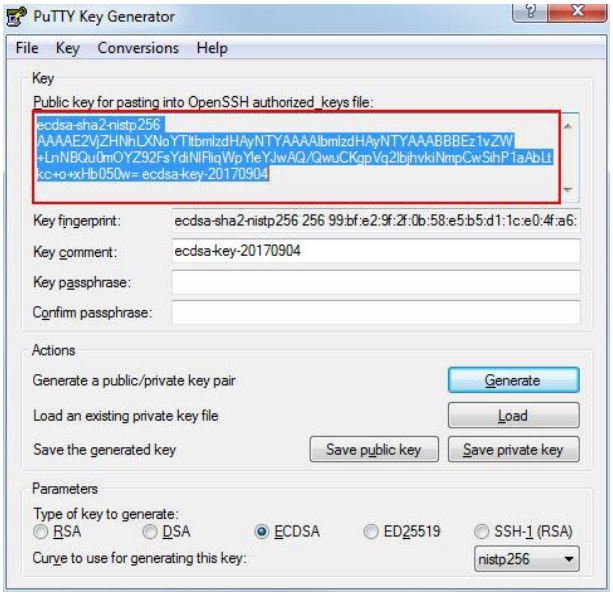
Wskazówka

Zwróć uwagę na zalecenia dotyczące procedur kryptograficznych!
Zgodnie z wytycznymi technicznymi BSI TR-02102-4 (wersja 2017-01), ECDSA określa długość klucza na co najmniej 250 bitów!

3. Następnie kliknij pole **[Generate]**, aby rozpocząć generowanie klucza.

4. Podczas generowania klucza, poruszaj dowolnie myszką w oknie, aż pasek postępu dojdzie do końca. PuTTYgen generuje przypadkowe liczby, niezbędne do generowania kluczy, między innymi dzięki ruchom kursora myszy.

Po zakończeniu generowania, dane kluczy są wyświetlane w oknie:



Rys. 11: Generowanie kluczy za pomocą PuTTYgen

5. Kliknij przycisk **[Save public key]** i przycisk **[Save private key]**, aby zapisać swoją parę kluczy.

6. Wprowadź hasło dla klucza prywatnego w polu **Key passphrase**.

7. Potwierdź hasło w polu **Confirm passphrase**.

8. Przechowuj klucz prywatny w bezpiecznym miejscu, aby żadna nieuprawniona osoba nie mogła się uwierzytelnić za pomocą Twojego klucza w urządzeniu.

Klucz publiczny musi być przechowywany na sterowniku w katalogu domowym użytkownika, który powinien użyć klucza do uwierzytelnienia się (np. /Home/user). Należy tam najpierw utworzyć podfolder ".ssh" i plik "authorized_keys", patrz poniższy opis.

Wskazówka

Zwróć uwagę na uprawnienia do pliku!
Katalog ".ssh" musi mieć uprawnienie Linux® **rwx ------ (700)** a plik "authorized_keys" musi mieć uprawnienie Linux® **rw ------- (600)**; w przeciwnym razie klucz nie zostanie przyjęty!

9. Utwórz katalog „.ssh“ an:
```
user@PFC200-40ED7D:~ pwd
/home/user
user@PFC200-40ED7D:~mkdir .ssh && chmod 700 .ssh
```

10. Skopiuj klucz publiczny z generatora kluczy PuTTY, patrz rysunek "Generowanie kluczy PuTTYgen".

11. Wstaw klucz do pliku „authorized_keys“:
```
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
```

Wskazówka

Podczas wstawiania kluczy zwróć uwagę na składnię!
Każdy klucz musi zostać zapisany w jednym wierszu pliku "authorized_keys"!

12. Przetestuj dostęp za pomocą klucza prywatnego, zanim dezaktywujesz logowanie hasłem.

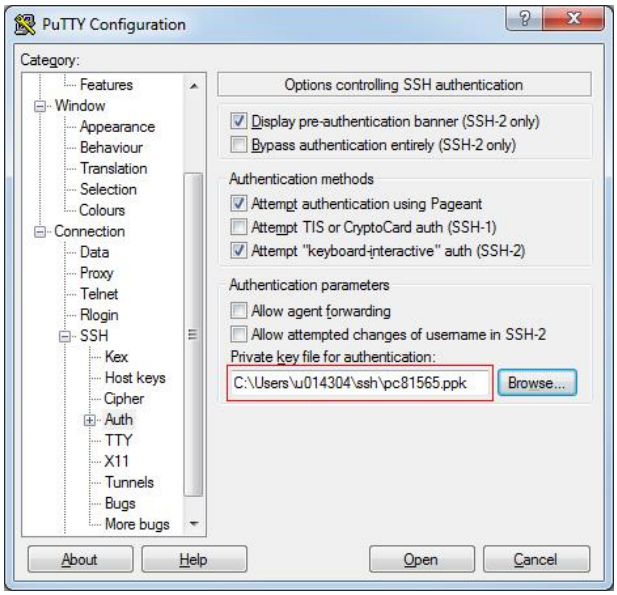
Konfiguracja narzędzia PuTTY

Aby móc użyć klucza do uwierzytelnienia, musisz podać klucz swojemu klientowi SSH. Poniżej znajduje się przykład PuTTY (innych klientów należy konfigurować analogowo):

1. Uruchom narzędzie PuTTY. Otworzy się okno dialogowe "PuTTY Configuration".

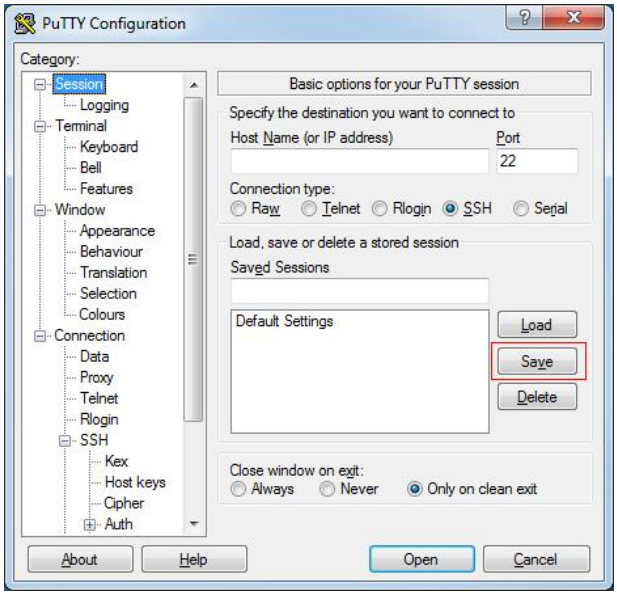
2. W drzewie katalogów przejdź do menu **Connection** > **SSH** > **AUTH.** Otworzy się okno dialogowe opcji uwierzytelniania SSH.

3. W obszarze „Authentication parameters“ wybierz swój klucz prywatny.



Rys. 12: Konfiguracja narzędzia PuTTY

4. Przejdź do menu **Session** w strukturze katalogów.



Rys. 13: Zapisywanie konfiguracji PuTTY

5. Zapisz konfigurację za pomocą przycisku **[Save]**.

6.2.1.4.1 Dezaktywacja logowania poprzez wprowadzenie hasła

Dostępne są dwie opcje:

Plik konfiguracyjny:

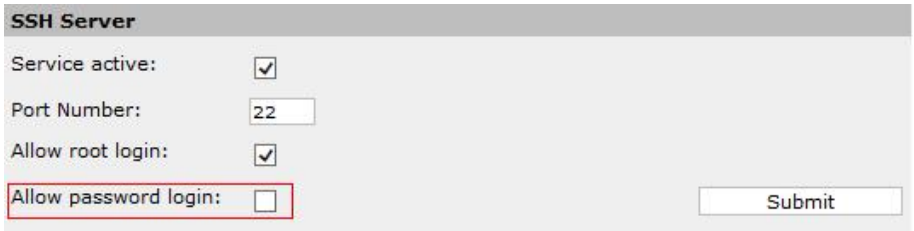
1. Ustaw „`PASSWORD_LOGIN`“ na "false" (default = true). Plik konfiguracyjny można znaleźć tu: /etc/dropbear/dropbear.conf.

2. Zrestartuj usługę.

WBM:

1. Przejdź do menu w WBM **Ports and Services** > **SSH**.

2. Odznacz pole **Allow password login**.



Rys. 14: Dezaktywowanie logowania poprzez wprowadzenie hasła

3. Zapisz ustawienie za pomocą przycisku **[Submit]**.

Zmiany w WBM automatycznie uruchomią ponownie usługę.

6.2.1.4.2 Odmowa logowania przez root logowania

Wskazówka

Upewnij się, że przez pomyłkę nie wyłączysz się z systemu!
Załóż konto użytkownika z tymi samymi uprawnieniami co konto root lub superużytkownik! Użyj poleceń `su` i `sudo` aby nadać indywidualnym użytkownikom uprawnienia administratora.

Dostępne są dwie opcje:

Plik konfiguracyjny:

1. Ustaw „ROOT_LOGIN“ na "false" (default = true). Plik konfiguracyjny można znaleźć tu: /etc/dropbear/dropbear.conf.

2. Zrestartuj usługę.

WBM:

1. Przejdź do menu w WBM **Ports and Services** > **SSH**.

2. Odznacz pole wyboru **Allow root login**.

Rys. 15: Odmowa logowania przez root logowania

3. Zapisz ustawienie za pomocą przycisku **[Submit]**.

Zmiany w WBM automatycznie uruchomią ponownie usługę.

Więcej informacji na ten temat można znaleźć w rozdziale "Uodpornianie> ...> "Tworzenie i wymiana certyfikatów".

6.2.1.5 Tworzenie i wymiana certyfikatów

Certyfikat zapewnia bezpieczne połączenie z komunikacją sieciową i służy do uwierzytelniania zdalnego hosta. Zielona ikona kłódki w przeglądarce wskazuje, że ta witryna ma ważny i zaufany certyfikat, a połączenie jest bezpieczne.

Zaleca się wymianę standardowych certyfikatów WAGO na własne certyfikaty, ponieważ klucz prywatny jest identyczny dla wszystkich urządzeń, klientów i firmware, a zatem nie może zostać sklasyfikowany jako tajny. Własne certyfikaty muszą być sygnowane przez urząd certyfikacji (tzw. Root CA). Certyfikat główny (root) stanowi wspólną kotwicę zaufania wszystkich podrzędnych certyfikatów i musi być przechowywany w lokalnym, zaufanym magazynie przeglądarki (Trust Store) lub klienta.

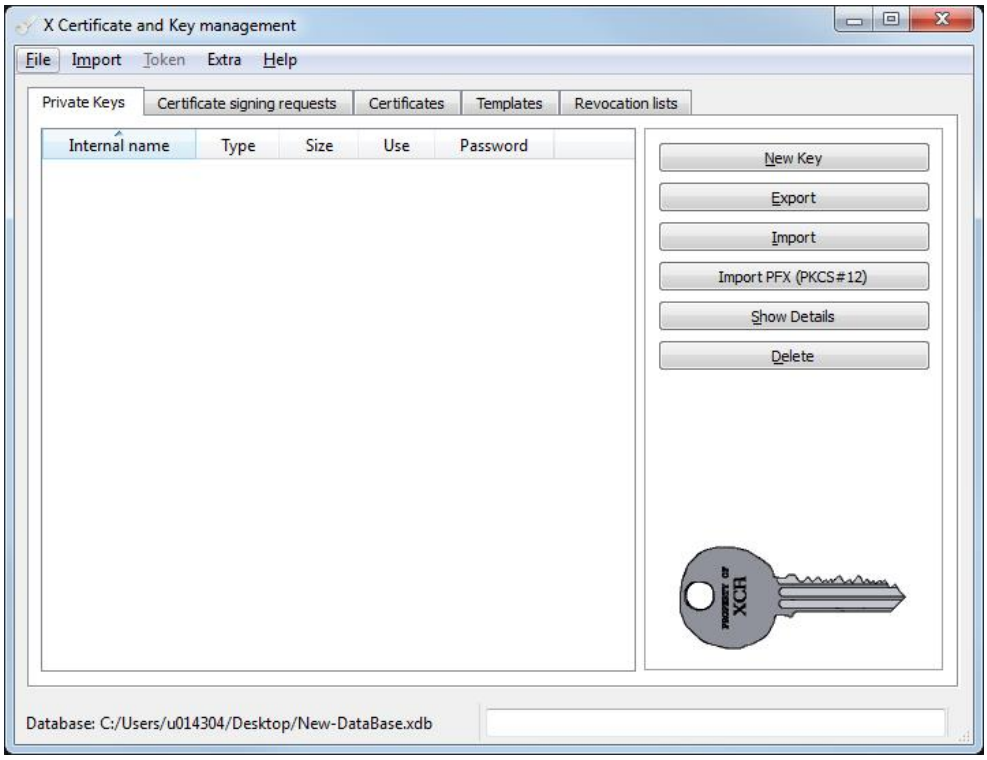
Poniższe rozdziały opisują tworzenie kluczy i certyfikatów za pomocą oprogramowania do zarządzania kluczami XCA. Dzięki darmowemu oprogramowaniu, możliwe jest samodzielne tworzenie certyfikatów Certyfikaty/klucze są przechowywane w lokalnym pliku bazy danych. Baza danych zawierająca klucze prywatne jest chroniona hasłem.

6.2.1.5.1 Generowanie kluczy prywatnych

1. Otwórz oprogramowanie XCA i wybierz w menu **File** podmenu **New Database**.

2. Wybierz lokalizację i odpowiednią nazwę bazy danych.

3. Wprowadź hasło do tworzenia kopii zapasowej bazy danych. Następnie nowo utworzona baza danych zostanie automatycznie otwarta:

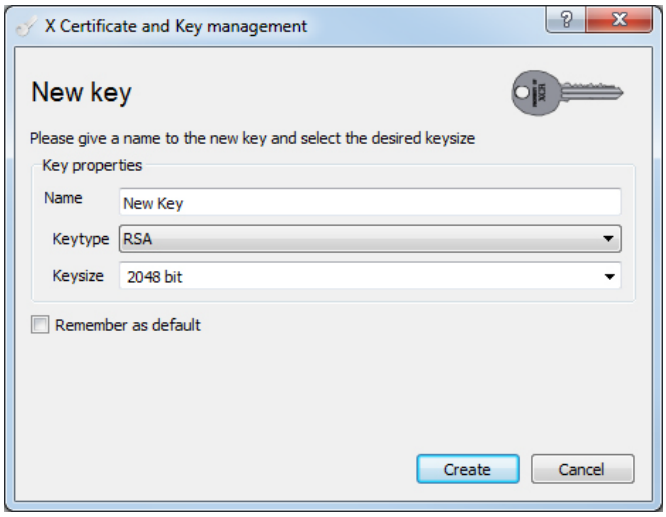


Rys. 16: Baza danych XCA

4. W zakładce "Private Keys" wybierz przycisk **[New Key]**.

Wskazówka

Pamiętaj, że trzeba wygenerować dwa klucze!
Jeden klucz jest wymagany dla głównego urzędu certyfikacji (Root-CA) i certyfikatu urządzenia!

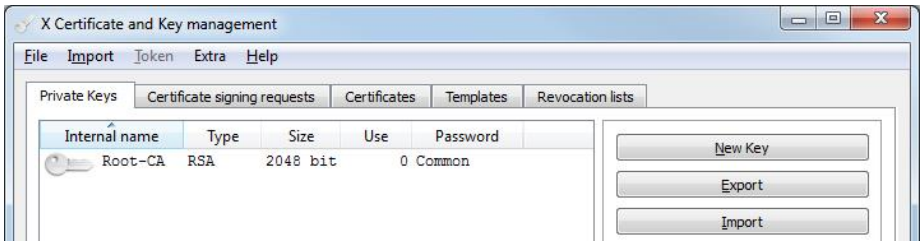


Rys. 17: Zakładanie nowego klucza

5. Przypisz nazwę, typ klucza i długość klucza dla głównego urzędu certyfikacji (Root-CA).
   Przypisanie zależy od tego, czy klucz jest generowany dla głównego urzędu certyfikacji (Root-CA), czy dla sterownika (zalecane długości kluczy - patrz wytyczne techniczne BSI TR-0212-2).

6. Wybierz przycisk **[Create]**, aby utworzyć klucz.

Po utworzeniu klucza pojawi się on w oknie:



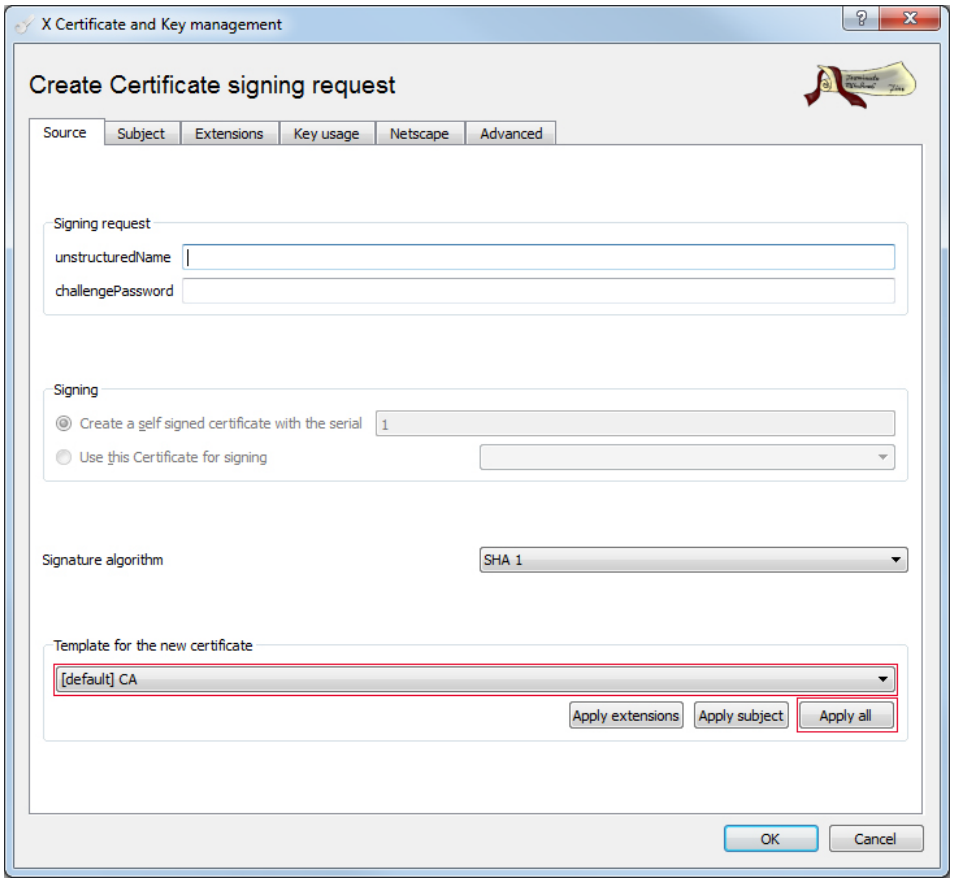
Rys. 18: Utworzenie nowego klucza

7. Powtórz kroki 4 ... 6, aby utworzyć klucz certyfikatu urządzenia.

6.2.1.5.2 Tworzenie żądania głównego certyfikatu CA.

1. Utwórz nowe żądanie certyfikatu dla ROOT-CA, wybierając w zakładce "Certificate signing request" przycisk **[New Request].**

2. W wyświetlonym oknie dialogowym przejdź do zakładki "Source".

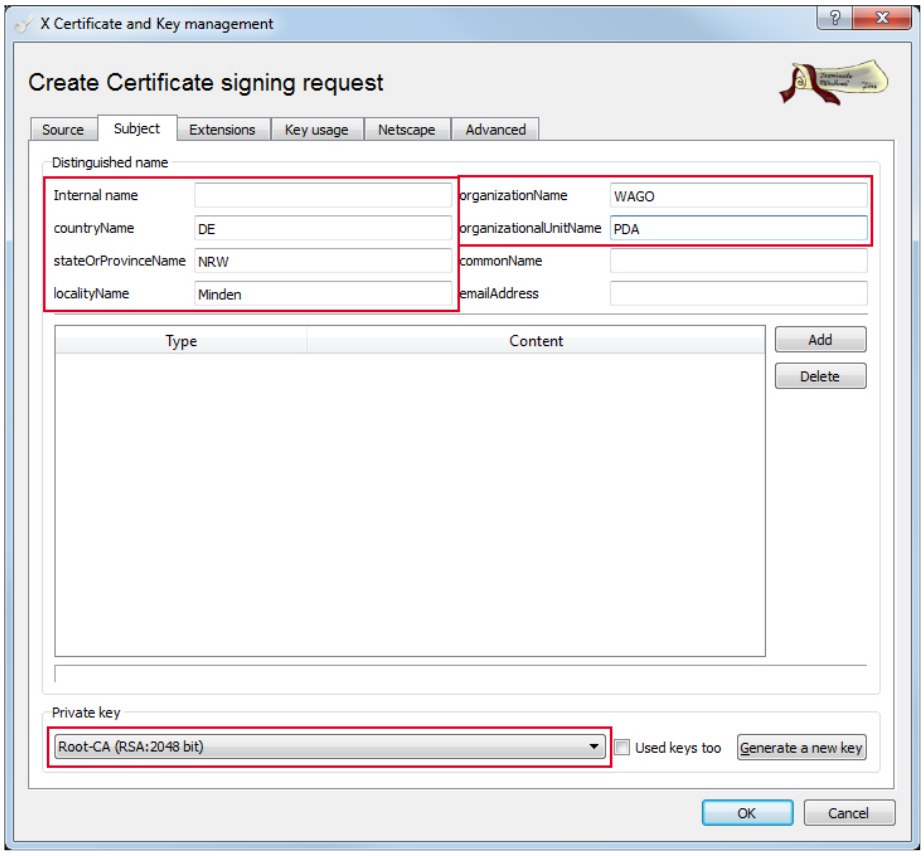


Rys. 19: Tworzenie certyfikatu głównego (root-CA)

3. W obszarze **Template for the new certificate** wybierz pozycję "[default] CA".

4. Wybierz przycisk **[Apply all]**.

5. Przejdź do zakładki „Subject“:



Rys. 20: Tworzenie głównego certyfikatu Root-CA, Subject

Tabela 8: Zakładka "Subject"

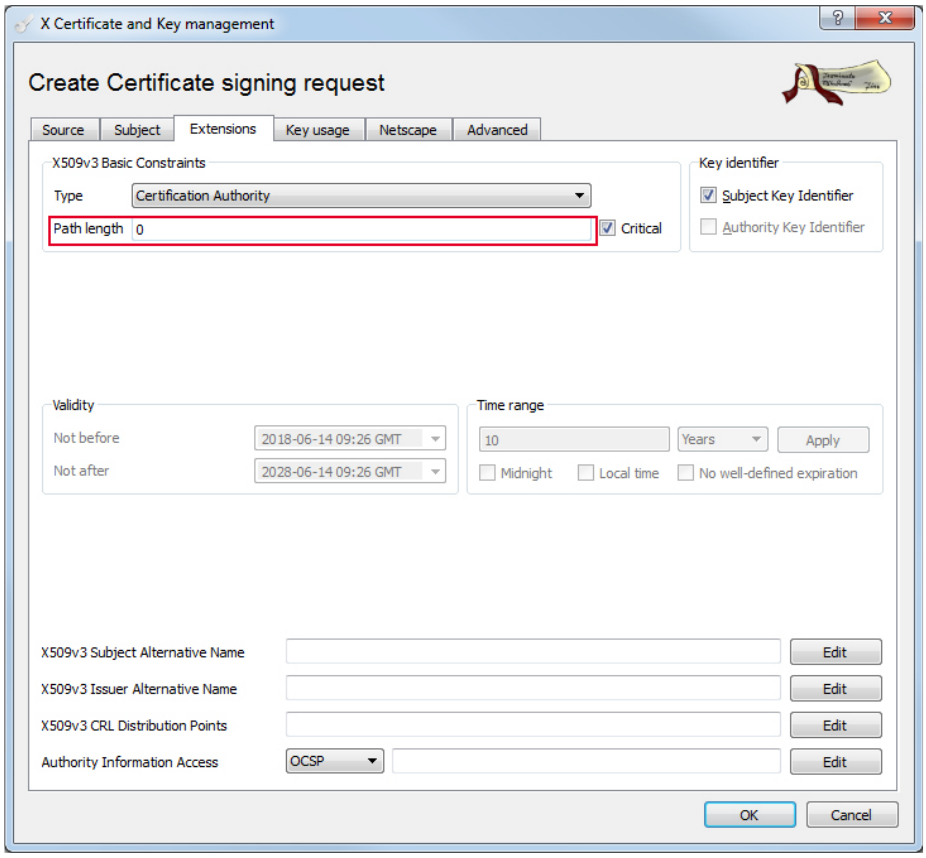
Pole wpisowe	Znaczenie
Internal name	wartość w tym polu służy jako wewnętrzne odniesienie i powinna jednoznacznie identyfikować certyfikat
countryName	kod kraju (np. PL dla Polski)
stateOrProvinceName	województwo (np. DOL)
localityName	miejsce wystawienia certyfikatu
organizationName	nazwa organizacji, która wystawiła certyfikat
organizationUnitName	symbol działu
commonName	w tym miejscu można zdeponować ogólny identyfikator
emailAddress	tutaj można wpisać adres e-mail

6. Wypełnij zaznaczone pola w górnym obszarze.

7. Z listy wyboru **Private Key** wybierz wygenerowany klucz dla głównego urzędu certyfikacji Root-CA (sekcja "Generate Private Keys").

8. Jeśli nie masz jeszcze klucza, wygeneruj nowy klucz za pomocą przycisku **[Generate a new key]**.

9. Przejdź do zakładki „Extensions“:

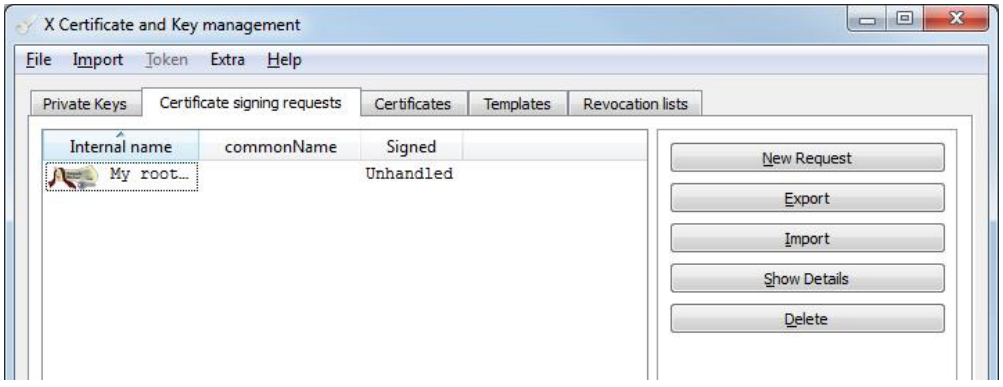


Rys. 21: Tworzenie głównego certyfikatu Root-CA, Extensions

10. Ustaw długość ścieżki w odpowiednim polu na wartość "0".

Jeśli w zakładce "Source" w polu **Template for the new certificate**, wybrałeś domyślny wpis "CA", nie musisz wprowadzać żadnych danych dalszych ustawień. Ustawienia w zakładce "Key usage" powstają automatycznie.

11. Potwierdź wpis, klikając **[OK]**.
Nowe żądanie certyfikatu pojawi się w zakładce "Certificate signing requests":

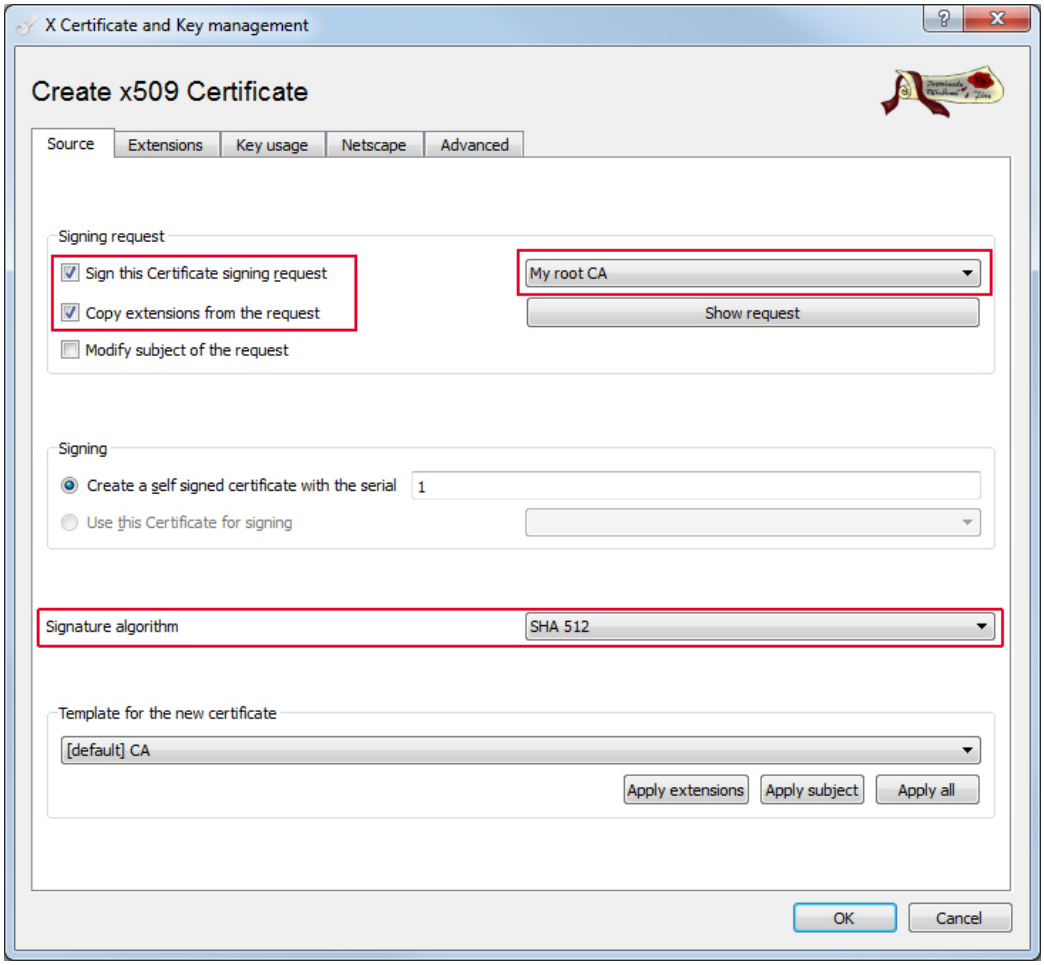


Rys. 22: Nowe żądanie certyfikatu utworzone dla głównego urzędu certyfikacji.

6.2.1.5.3 Tworzenie głównego certyfikatu CA

1. Przejdź do zakładki "Certificates", aby utworzyć certyfikat.

2. Wybierz przycisk **[New Certificate]**. Otwiera się następujące okno dialogowe:



Rys. 23: Zarejestruj żądanie certyfikatu

3. W zakładce "Source" aktywuj pole **Sign this Certificate singing request**.

4. Wybierz wcześniej utworzone żądanie certyfikatu w polu wyboru w prawym górnym rogu.

5. Aktywuj pole **Copy extensions from the request**.

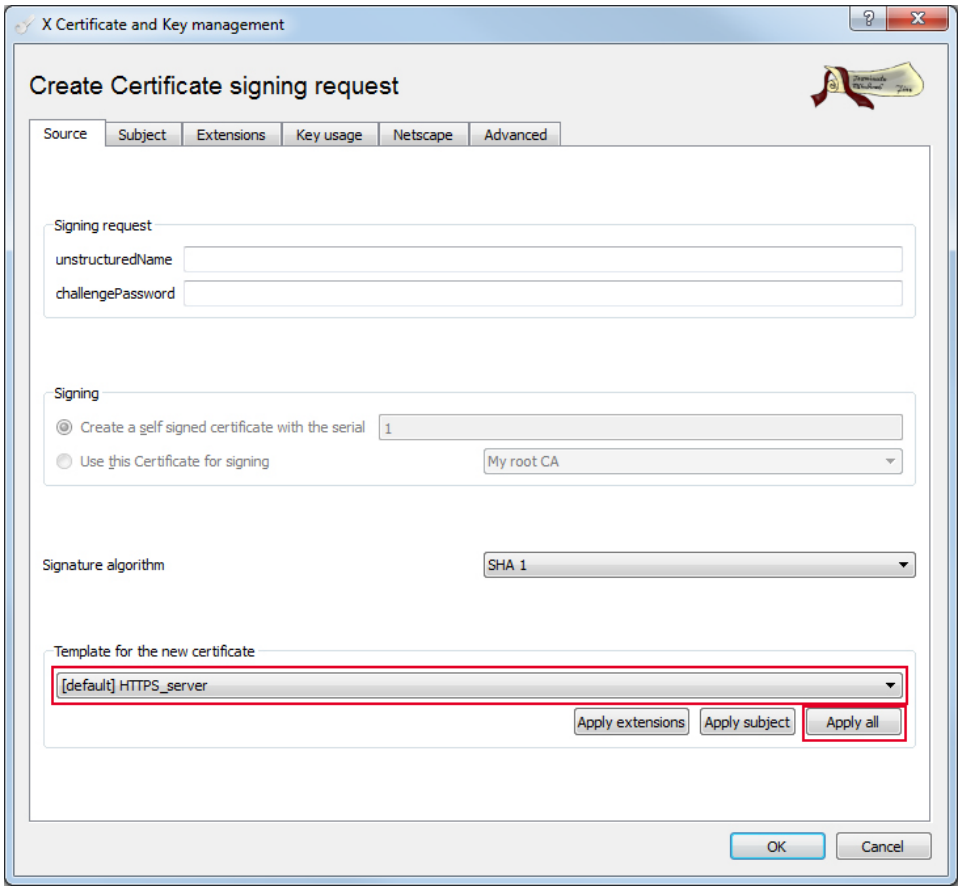
6. Wybierz wartość "SHA 512" w polu wyboru **Signature algorithm** (patrz wytyczne techniczne BSI TR-02102-2).

7. Potwierdź wpis, klikając **[OK]**.
Nowy certyfikat jest wyświetlany w zakładce "Certificates" z zielonym haczykiem.

6.2.1.5.4 Tworzenie żądania certyfikatu urządzenia

1. Utwórz nowe żądanie certyfikatu dla sterownika, wybierając przycisk **[New Request]** w zakładce "Certificate signing request".

2. W wyświetlonym oknie dialogowym przejdź do zakładki "Source".



Rys. 24: Tworzenie głównego certyfikatu Root-CA

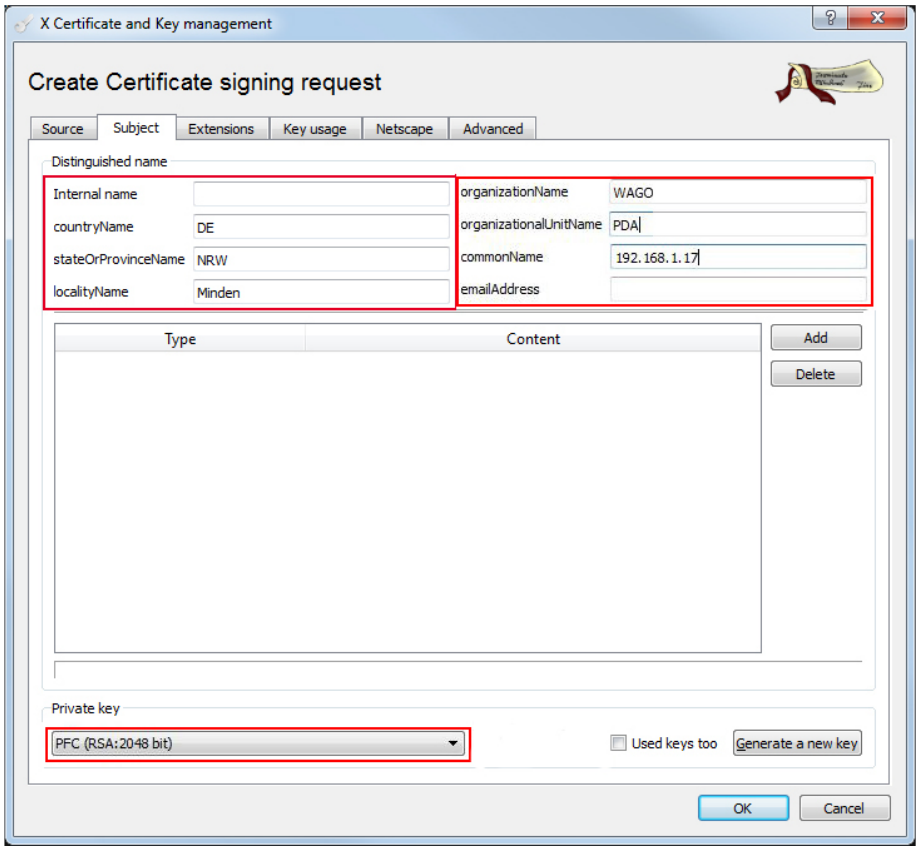
3. W polu **Template for the new certificate** wybierz pozycję "[default] serwer HTTPS".

Wskazówka

OpenVPN wymaga certyfikatów dla klientów!
Podczas konfigurowania OpenVPN, upewnij się, że w polu **Template for the cew certificate** wybrałeś pozycję "[default] HTTPS_client"!

4. Wybierz przycisk **[Apply all]**.

5. Przejdź do zakładki „Subject“:



Rys. 25: Tworzenie głównego certyfikatu Root-CA, Subject

Tabela 9: Zakładka "Subject"

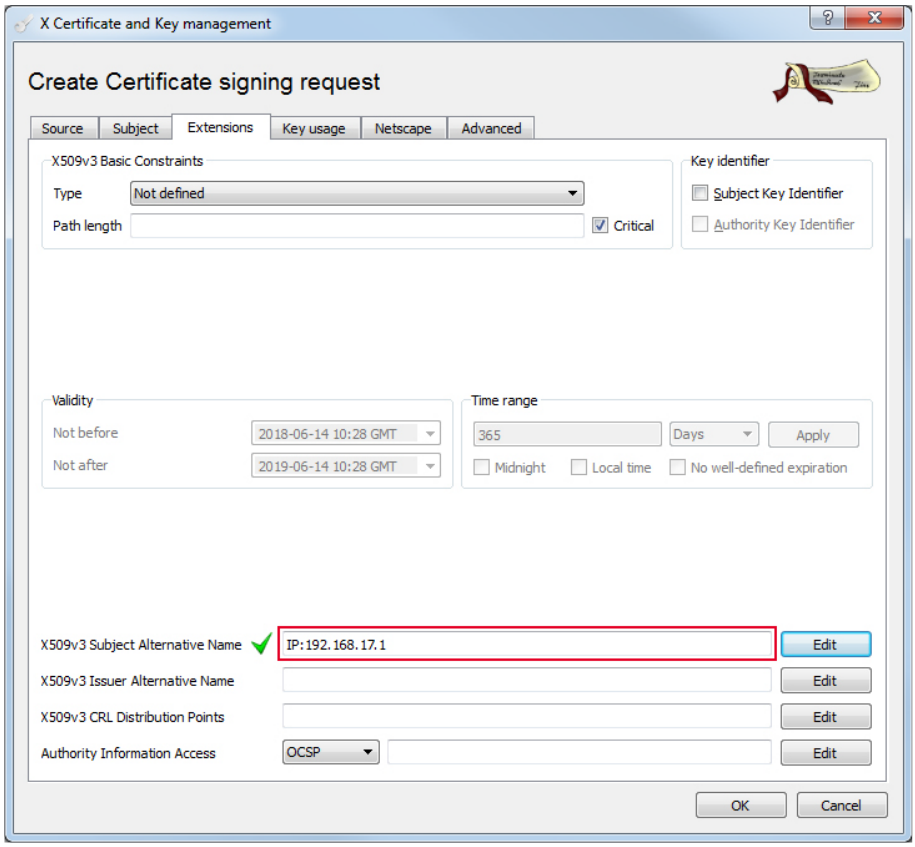
Pole wpisowe	Znaczenie
Internal name	wartość w tym polu służy tylko jako wewnętrzne odniesienie i powinna jednoznacznie identyfikować certyfikat
countryName	kod kraju (np. PL dla Polski)
stateOrProvinceName	województwo (np. DOL)
localityName	miejsce wystawienia certyfikatu
organizationName	nazwa organizacji, która wystawiła certyfikat
organizationUnitName	symbol działu
commonName	jednoznaczny adres IP lub nazwa hosta, w zależności od sposobu uzyskania dostępu do sterownika
emailAddress	tutaj można wpisać adres e-mail

Wskazówka

Wartość w polu "commonName" musi być identyczna z wierszem adresu!
Adres IP lub nazwa hosta są używane przez przeglądarki do określenia tożsamości. Jeśli wartość wprowadzona w "commonName" odbiega od wartości w wierszu adresu, certyfikat nie jest uznawany za ważny!

6. Wypełnij zaznaczone pola w górnym obszarze.

7. Przejdź do zakładki „Extensions“.



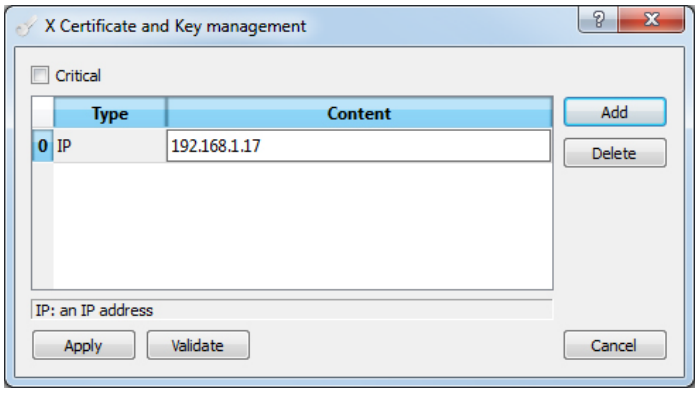
Rys. 26: Zakładka "Extensions", X509v3 Subject Alternative Name

8. W polu **X509v3 Subject Alternative Name** dodaj również adres IP i/lub nazwę hosta. Tą informację należy wprowadzić podczas korzystania z przeglądarek Chrome/Chromium (wersja 58 lub nowsza).

Wskazówka

Wartość w polu "X509v3 Subject Alternative Name" musi być identyczna z wierszem adresu!
Adres IP lub nazwa hosta są używane przez przeglądarki do określenia tożsamości. Jeśli wartość wprowadzona w polu "**X509v3 Subject Alternative Name**" różni się od wartości w wierszu adresu, certyfikat nie jest uznawany za ważny!

9. Wybierz przycisk **[Edit]**. Otwiera się następujące okno:



Rys. 27: X509v3 Subject Alternative Name, wprowadzanie adresu IP

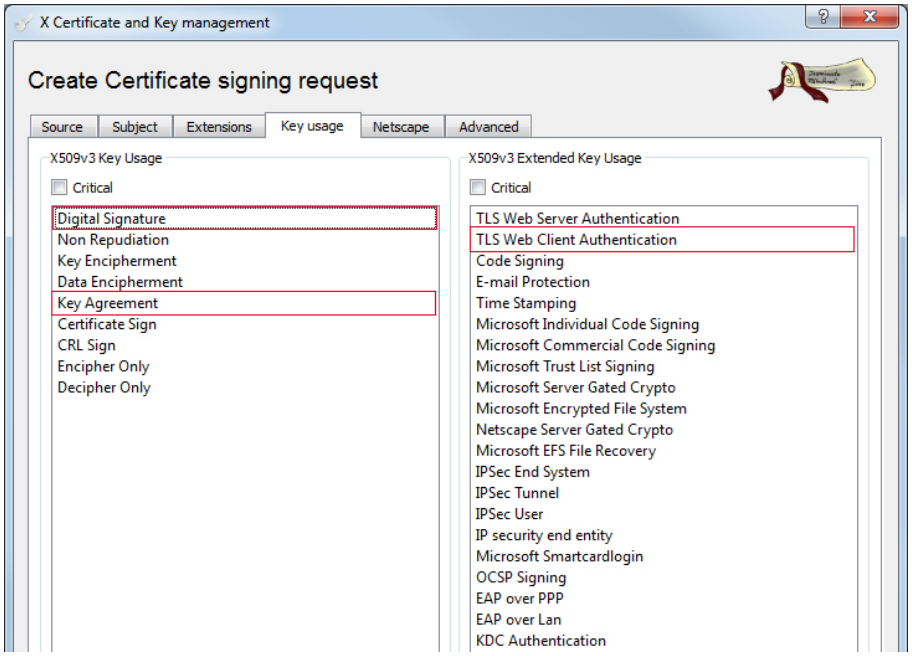
10. Wybierz przycisk **[Add]**.

11. W polu wyboru **Type** wybierz "IP" dla adresu IP lub "DNS" dla nazwy hosta.

12. Wprowadź odpowiednią wartość w polu **Content**.

13. Wróć do zakładki "Key usage", aby ograniczyć korzystanie z certyfikatów.

14. Wprowadź wartości oznaczone na rysunku.



Rys. 28: Nowe żądanie certyfikatu, Key usage, klient

Wskazówka

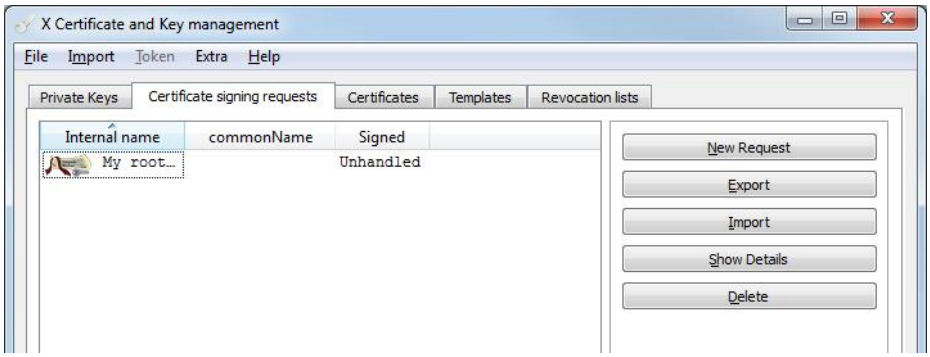
Wprowadź inne wartości podczas uwierzytelniania serwera!
Zwróć uwagę, aby podczas uwierzytelniania serwera wprowadzić w prawym polu informację "TLS Web Server Authentication". W lewym polu wpisywane są wartości "Digital Signature" i "Key Encipherment" lub "Key Agreement". Poza tym proces tworzenia certyfikatu dla Sever/Client jest identyczny!

15. Przejdź do zakładki „Subject“.

16. Z listy **Private Key** wybierz wygenerowany klucz dla sterownika (patrz sekcja "**Generate Private Keys**").

17. Jeśli nie wygenerowałeś jeszcze klucza, zrób to za pomocą przycisku **[Generate a new key]**.

18. Potwierdź wpis, klikając **[OK]**.
Nowe żądanie certyfikatu pojawi się w zakładce "Certificate signing requests":

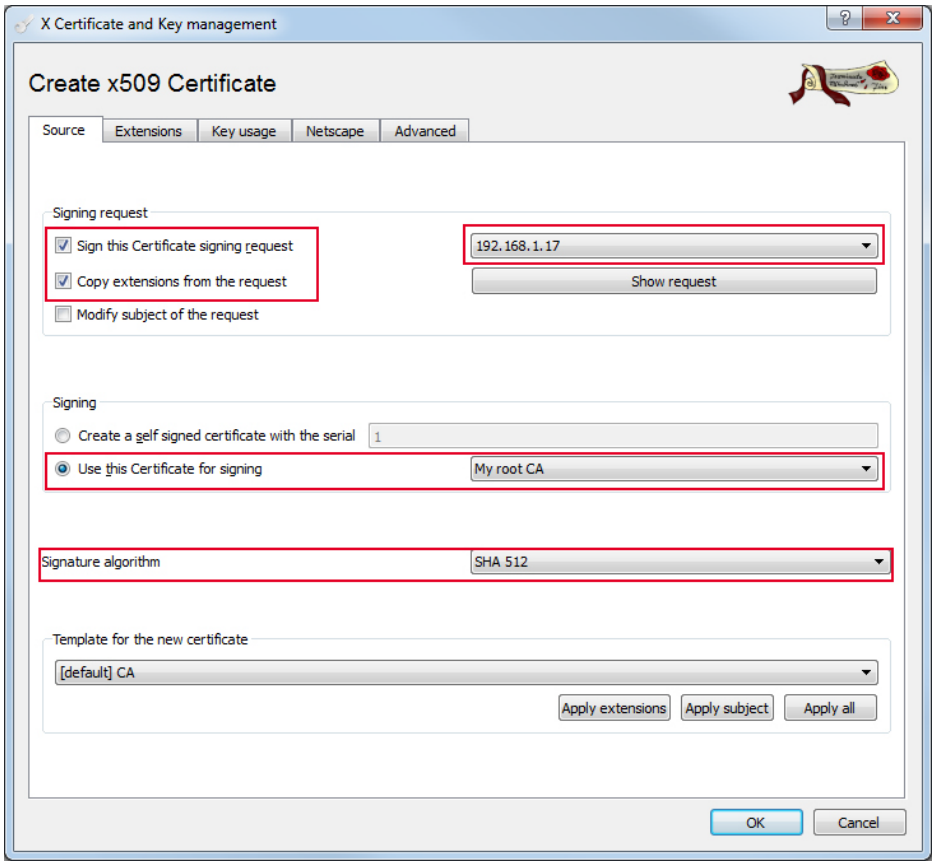


Rys. 29: Tworzenie nowego żądania certyfikatu dla sterownika

6.2.1.5.5 Tworzenie certyfikatu urządzenia

1. Przejdź do zakładki "Certificates", aby utworzyć certyfikat.

2. Wybierz przycisk **[New Certificate]**. Otwiera się następujące okno dialogowe:



Rys. 30: Zarejestruj żądanie certyfikatu

3. W zakładce "Source" aktywuj pole **Sign this Certificate singing request**.

4. Wybierz wcześniej utworzone żądanie certyfikatu w polu wyboru w prawym górnym rogu.

5. Aktywuj pole **Copy extensions from the request**.

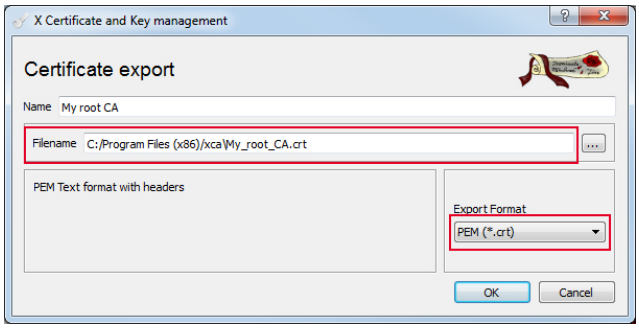
6. Zaznacz pole wyboru **Use This Certificate for signing** i wybierz utworzony certyfikat głównego urzędu certyfikacji.

7. Wybierz wartość "SHA 512" w polu wyboru **Signature algorithm** (patrz wytyczne techniczne BSI TR-02102).

8. Potwierdź wpis, klikając **[OK]**. Nowy certyfikat jest wyświetlany w zakładce "Certificates" pod certyfikatem głównego urzędu certyfikacji, z zielonym ptaszkiem.

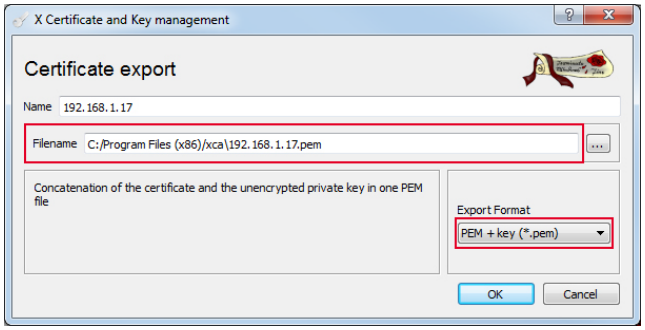
6.2.1.5.6 Eksport certyfikatów

1. W głównym oknie przejdź do zakładki "Certificates" i całkowicie rozwiń strukturę drzewa.
2. Wybierz główny certyfikat CA i kliknij prawym przyciskiem myszy, aby otworzyć menu.
3. Wybierz **Export > File.**



Rys. 31: Eksportowanie głównego certyfikatu Root-CA

4. Wybierz miejsce przechowywania za pomocą przycisku [...].
5. Na liście wyboru **Export Format** wybierz wpis "PEM without Key".
6. Potwierdź przyciskiem **[OK]**.
7. Wybierz certyfikat sterownika i kliknij prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
8. Wybierz **Export > File.**



Rys. 32: Eksportowanie certyfikatu sterownika

9. Wybierz miejsce przechowywania za pomocą przycisku [...].
10. Na liście wyboru **Export Format** wybierz wpis "PEM with Key".
11. Potwierdź przyciskiem **[OK]**.

6.2.1.5.7 Instalacja certyfikatów na kliencie i urządzeniu

Wskazówka

Do zmiany adresu IP/nazwy hosta wymagany jest nowy certyfikat urządzenia!
Jeśli adres IP lub nazwa hosta zostały zmienione, certyfikat dla sterownika musi zostać odtworzony z poprawnym adresem IP lub poprawną nazwą hosta (patrz rozdział "Tworzenie certyfikatu urządzenia"!

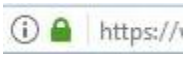
1. Zaimportuj certyfikat głównego certyfikatu CA do przeglądarki.
   Procedura zależy od używanej przeglądarki!

2. Prześlij certyfikaty do sterownika za pomocą FTPS/SCP.

3. Umieść certyfikat PFC w "/ etc / lighttpd /" i zmień jego nazwę na "https-cert.pem".L

4. Zrestartuj serwer sieciowy za pomocą narzędzia: "/etc / config-tools / restart_webserver". Alternatywnie, można ponownie uruchomić urządzenie.

Kiedy, w zależności od przeglądarki, przed adresem internetowym lub za nim pojawi się zielony symbol kłódki, akcja zakończy się sukcesem, a Twoje połączenie będzie od teraz bezpieczne. Przeglądarki często wskazują w wierszu adresu, jak wiarygodne jest połączenie. Firefox np. wskazuje zieloną kłódkę, jeśli certyfikat sygnowany jest przez zaufany główny urząd certyfikacji (Root-CA).



Rys. 33: Zielona kłódka w przeglądarce (Firefox)

6.2.1.6 Tworzenie listy unieważnionych certyfikatów

Wskazówka

Listy unieważnionych certyfikatów (CRL) tylko dla OpenVPN i IPsec!
Listy CRL (Certificate Revocation List) na sterownikach są obecnie używane tylko w połączeniach OpenVPN i IPsec.

Lista CRL zawiera certyfikaty, które podczas swojego okresu ważności zostały unieważnione, okazały się nieprawidłowe, niepoprawne lub unieważnione. Jest to przydatne w przypadku utraty klucza prywatnego lub gdy klient utraci zaufanie. Jeśli na przykład pracownik opuszcza firmę, zwykle należy wcześniej unieważnić jego certyfikat, aby uniemożliwić mu dostęp do sieci firmowej.

Wpis dotyczący unieważnionego certyfikatu może mieć charakter tymczasowy. Lista unieważnionych certyfikatów jest tworzona na serwerze.

Wskazówka

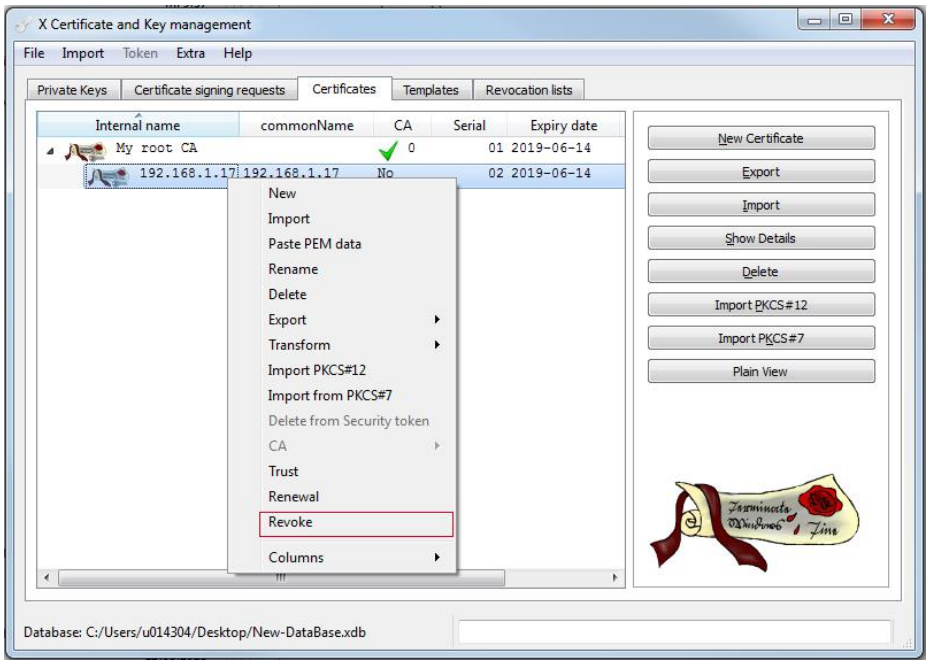
Możesz najpierw utworzyć pustą listę!
Najpierw możesz utworzyć pustą listę CRL, aby uniknąć konieczności restartowania usługi VPN podczas aktualizacji. Pusta lista może również zostać zaktualizowana w trakcie użytkowania!

Można utworzyć listę CRL za pomocą oprogramowania do zarządzania kluczami XCA.

1. Otwórz oprogramowanie XCA i wybierz zakładkę "Certificates“**.**

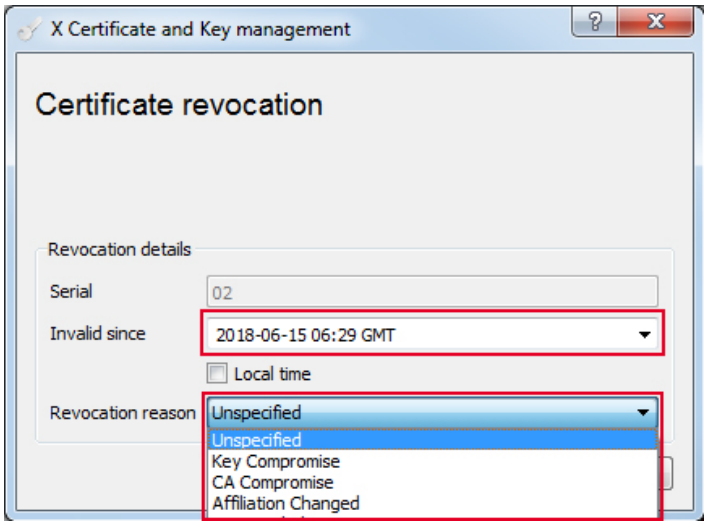
2. Wybierz certyfikat, który chcesz dodać do listy CRL.

3. Wybierz menu **Revoke** prawym przyciskiem myszy.



Rys. 34: Tworzenie listy unieważnionych certyfikatów (CRL)

4. W otwartym oknie możesz podać powód cofnięcia zaufania i datę, od której certyfikat jest nieważny.



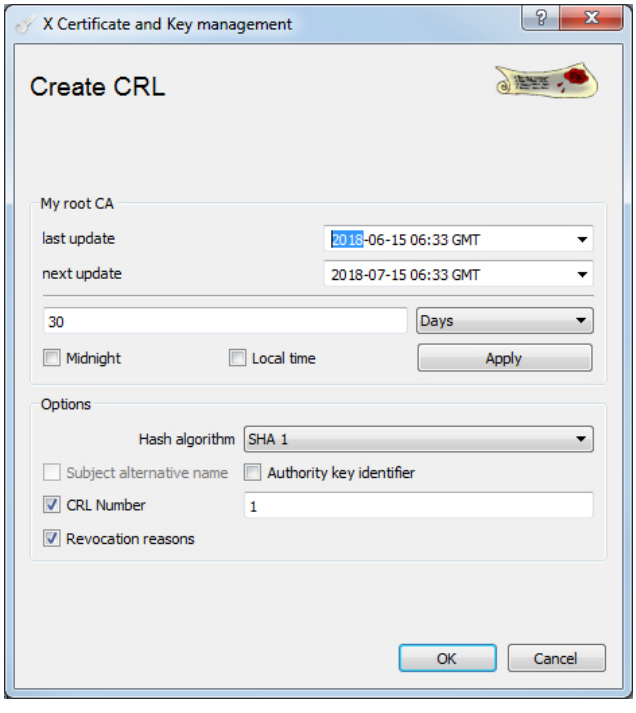
Rys. 35: Cofnięcie certyfikatu

5. W razie potrzeby powtórz kroki 2 ... 4.

6. Przejdź do zakładki "Revocation lists".

7. Prawym przyciskiem myszy przejdź do menu **New**.

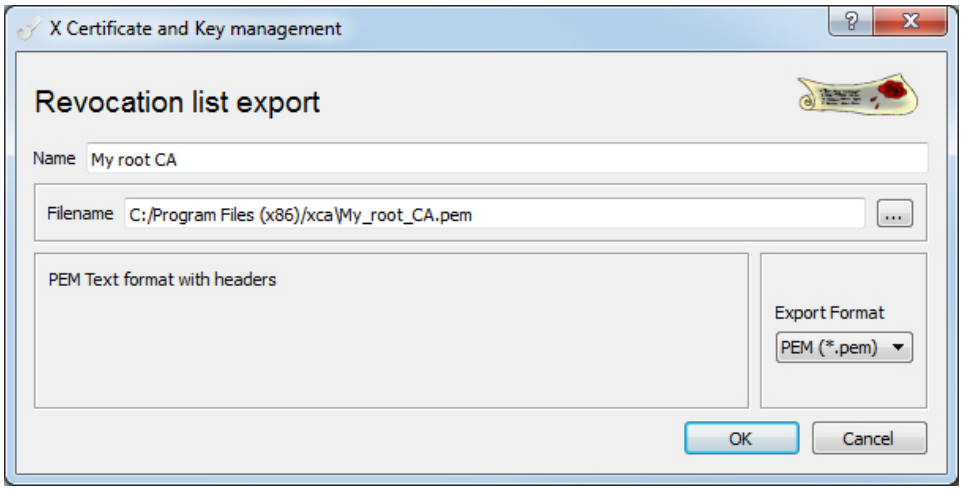
W pojawiającym się oknie nie trzeba wykonywać żadnych dalszych ustawień; XCA automatycznie dodaje do listy unieważnione certyfikaty. Opcjonalnie można ustawić interwał aktualizacji i dostosować algorytm podpisu.



Rys. 36: Tworzenie listy CRL

8. Wybierz przycisk **[OK]**. Lista unieważnionych certyfikatów pojawi się w zakładce "Revocation lists".

9. Wybierz listę unieważnionych certyfikatów i wybierz przycisk **[Export]**.



Rys. 37: Eksport listy cofnięć.

10. Zapisz listę unieważnionych certyfikatów.

11. Wybierz przycisk **[OK]**.

Wskazówka

Zwróć uwagę na strukturę archiwizacji!
Jeśli konfigurujesz sieć OpenVPN, lista unieważnionych certyfikatów musi być przechowywana w katalogu przeznaczonym dla OpenVPN (patrz rozdział "OpenVPN"> "Utwórz pliki konfiguracyjne", Konfiguracja serwera "crl-verify")!

Wskazówka

Zwróć uwagę na miejsca przechowywania list unieważnionych certyfikatów w OpenVPN!
W przypadku OpenVPN plik konfiguracyjny dla OpenVPN musi zostać utworzony wcześniej, ponieważ tam są zdefiniowane lokalizacje archiwum, patrz rozdz. "OpenVPN"> "Utwórz pliki konfiguracyjne"!

Wskazówka

Usługa VPN musi mieć dostęp do listy unieważnionych certyfikatów!
Upewnij się, że usługa VPN może uzyskać dostęp do listy unieważnionych certyfikatów, nawet jeśli nie ma uprawnień roota. Przenieś własność pliku na użytkownika OpenVPN:
`chown openvpn:openvpn <Datei>`
lub utwórz plik tak, aby był "czytelny dla świata"(„world-readable“):
`chmod 644 <Datei>`
(Plik nie zawiera żadnych tajnych informacji).

6.2.2 Ograniczanie dostępu przez otwarte interfejsy sieciowe

Wszelkie usługi lub interfejsy sieciowe, które nie są używane lub nie są konieczne do bieżącej aplikacji, mogą stanowić niepotrzebne ryzyko. Dlatego należy każdorazowo sprawdzać, które usługi i interfejsy sieciowe są potrzebne, a które można dezaktywować. W przypadku systemów produkcyjnych należy jednak wcześniej przetestować, jakie skutki dla systemu spowoduje taka dezaktywacja.

Poniższe rozdziały opisują, jak domyślnie wyłączyć aktywne usługi. Ponadto dostęp do usługi może być ograniczony do konkretnego interfejsu. Ta procedura jest zalecana, gdy usługa jest potrzebna i dlatego nie można jej zamknąć.
To ograniczenie może dodatkowo zmniejszyć obszar narażony na cyberatak. Szczegóły można znaleźć w rozdziale "Uodpornianie"> "Konfigurowanie firewalla".

Wskazówka

Zawsze używaj bezpiecznych protokołów!
Zawsze używaj bezpiecznych protokołów, takich jak np. HTTPS zamiast HTTP i SNMPv3 zamiast SNMPv1 itd.!

6.2.2.1 Dezaktywacja komunikacji serwisowej WAGO

Jeśli komunikacja serwisowa WAGO nie jest używana lub narzędzia programistyczne WAGO-I/O-*Check*, ustawienia ETHERNET lub ***e!****COCKPIT* nie są wymagane, należy je dezaktywować.

1. W WBM wybierz **Ports and Services > Network Services**, aby dezaktywować komunikację usług WAGO.

2. Dezaktywuj pole **Service active** w obszarze "I/O-Check".

Rys. 38: Dezaktywacja komunikacji serwisowej WAGO

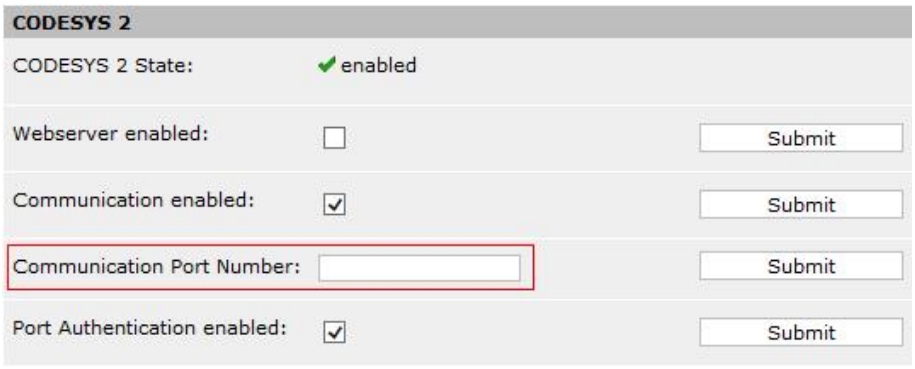
3. Kliknij przycisk **[Submit]**, aby zastosować zmianę.

6.2.2.2 Zmiana standardowych portów sieciowych

Większość zautomatyzowanych ataków w trakcie logowania do usług sieciowych, takich jak SSH, odbywa się na standardowym porcie sieciowym 22. Prostym i skutecznym sposobem, aby się przed tym uchronić, jest zmiana portu SSH. Standardowe porty sieciowe używane w CODESYS i SSH można zmienić za pomocą systemu zarządzania przez WWW.

1. Przejdź do menu **Ports and Services** > **PLC Runtime Services**.

2. W obszarze "CODESYS" w polu **Communication Port Number** należy najlepiej wprowadzić port z obszaru "Dynamic Port Numbers".



Rys. 39: Zmiana standardowych portów sieciowych.

Każdy port sieciowy może być użyty w systemie tylko raz. Dlatego upewnij się, że port nie jest używany przez inną aplikację, ponieważ w przeciwnym razie mogą wystąpić problemy z połączeniem. Podobnie nie należy używać portów zarezerwowanych dla innych usług.

Wskazówka

Dynamic Port Numbers (Dynamiczne numery portów)
Użycie "Dynamic Port Numbers" jest jedynie zaleceniem, aby uniknąć kolizji z już używanymi portami!

"Dynamic Port Numbers" nazywa się również prywatnymi numerami portów. Są to numery portów, z których **każda** aplikacja może się komunikować z **dowolną** inną aplikacją, za pośrednictwem protokołów internetowych TCP lub UDP! Więcej informacji na stronie: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

3. Naciśnij przycisk **[Submit]**, aby zastosować zmianę.

4. Powtórz kroki 2 ... 3 w menu **Ports and Services > SSH** w obszarze "Serwer SSH", aby zmienić tam port.

Wskazówka

Zewnętrzne firewalle muszą być odpowiednio skonfigurowane!
Jeśli używasz zewnętrznego firewalla, być może będziesz musiał zwolnić używane porty!

6.2.2.3 Blokowanie niezaszyfrowanego dostępu do WBM

W wersji fabrycznej sterownika, port TCP/80 jest używany dla WBM i każdej istniejącej wizualizacji sieci. Podczas uzyskiwania dostępu za pośrednictwem protokołu HTTP, przeglądarka jest automatycznie przekierowywana do zaszyfrowanego połączenia. Zaleca się wyłączenie tego portu przez WBM.

1. Otwórz WBM i przejdź do menu **Ports and Services** > **Network Services**.

2. Wyłącz pole **Service active** w obszarze "http".

Rys. 40: Blokowanie niezaszyfrowanego dostępu do WBM

3. Kliknij na przycisk **[Submit]**. Zastosowane będą odpowiednie ustawienia

6.2.2.4 Wyłączanie dostępu do środowiska systemowego CODESYS

Wskazówka

Środowiska systemowego *e!RUNTIME* nie można dezaktywować!
Dezaktywacja dostępu do środowiska systemowego jest możliwa tylko dla CODESYS, ale nie dla ***e!RUNTIME***!

Sterownik dysponuje środowiskiem systemowym CODESYS, za pomocą którego można go programować.

Program CODESYS jest zwykle pobierany za pośrednictwem interfejsów ETHERNET. Dwa interfejsy ETHERNET sterownika można skonfigurować dla różnych funkcji. Po zakończeniu programowania lub pierwszego uruchomienia, dostęp CODESYS do urządzenia można wyłączyć, aby zapobiec możliwości niepożądanego dostępu.

1. W WBM wybierz punkt menu **Ports and Service** > **PLC Runtime Services**, aby dezaktywować dostęp CODESYS.

2. W obszarze "CODESYS" dezaktywuj pole **Communication enabled**.

Rys. 41: Wyłączanie dostępu do środowiska systemowego CODESYS

3. Kliknij przycisk **[Submit]**, aby zastosować zmianę.

6.2.2.5 Blokowanie bezpośredniego dostępu do wizualizacji sieci CODESYS

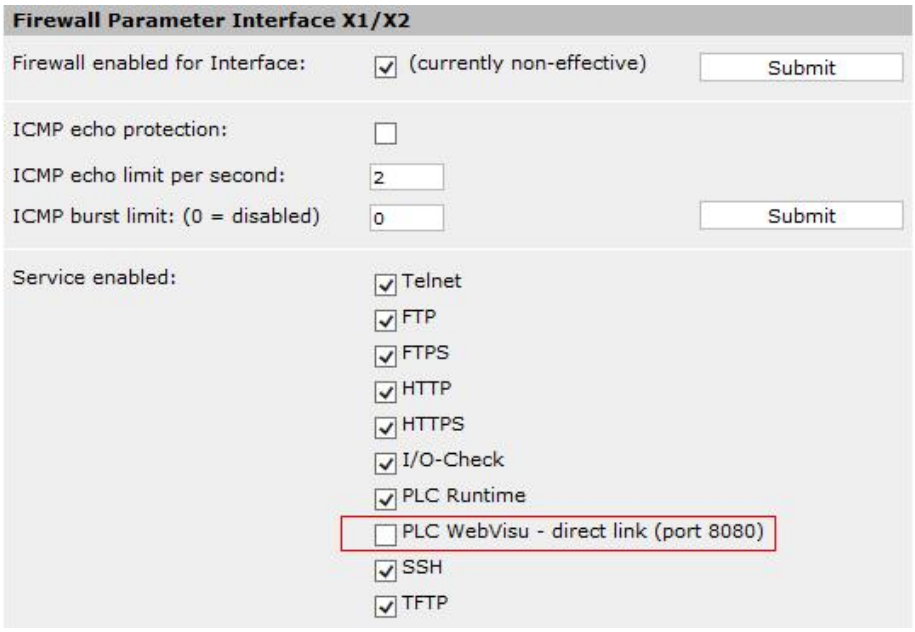
Wizualizację sieci CODESYS można uzyskać za pośrednictwem serwera WWW przez następujące porty:

- Port TCP/80 i/lub TCP/443
- Port TCP/8080

Zaleca się wyłączenie bezpośredniego dostępu przez port TCP/8080 w ustawieniach firewalla, ponieważ możliwe jest tutaj tylko połączenie nieszyfrowane.

1. W WBM wybierz punkt menu **Firewall** > **General Configuration**.

2. W obszarze "Firewall Parameter Interface X1/X2 > Service enabled" dezaktywuj pole **PLC WebVisu – direct link (port 8080)**“.



Rys. 42: Blokowanie bezpośredniego dostępu do wizualizacji sieci CODESYS

3. Kliknij przycisk **[Submit]**, aby zastosować zmianę.

4. Powtórz kroki 2 i 3 w menu **Firewall** > **General Configuration** > **Firewall Parameter Interface VPN**, jeśli używasz „Virtual Private Network“.

Wskazówka

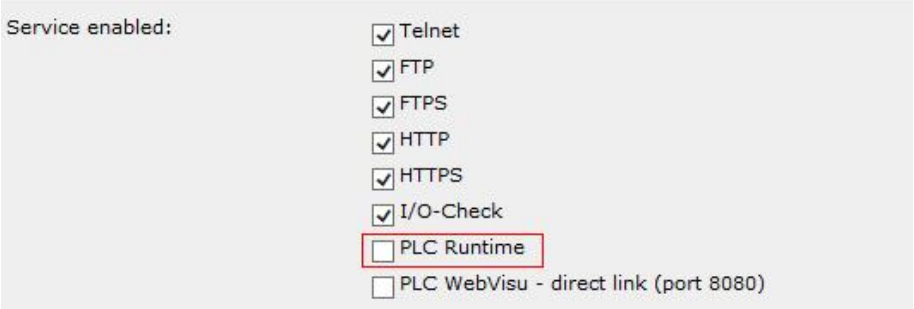
X1 i X2 mogą działać jako osobne interfejsy!
Jeśli używasz dwóch interfejsów ETHERNET X1 i X2 jako oddzielnych interfejsów sieciowych, należy przeprowadzić wymienione wyżej kroki 1 ... 3 dla każdego interfejsu X1 i X2.

6.2.2.6 Blokowanie dostępu do środowiska systemowego *e!RUNTIME*

Najpierw aktywuj firewall, o ile jeszcze nie został aktywowany, patrz rozdział „Konfigurowanie firewalla“ > „Konfigurowanie firewalla systemie zarządzania przez WWW“.

1. W WBM wybierz punkt menu **Firewall** > **General Configuration**.

2. Dezaktywuj pola **PLC Runtime** w obszarach "Interfejs parametrów firewalla X1 / X2" i "Interfejs VPN parametrów firewalla".



Rys. 43: Blokowanie dostępu do środowiska systemowego ***e!****RUNTIME.*

3. Kliknij przycisk **[Submit]**, aby zastosować zmianę.

Blokuje to dostęp do portu 11740/TCP lub portu 2455/TCP, w zależności od używanego środowiska systemowego. Alternatywnie można utworzyć filtr użytkownika dla portu 11740/TCP (***e!****Runtime*) lub dla portu 2455/TCP (CODESYS). Aby uzyskać szczegółowe informacje, patrz rozdział "Konfigurowanie firewalla w systemie zarządzania przez WWW “ >“Tworzenie białej listy dla określonych adresów IP“.

Zamknij port 1740/UDP (*e!**RUNTIME*)**

1. Usuń łącze w systemie plików:
   /usr/lib/cds3-custom-components/libCmpBlkDrvUdp.so
2. Należy ponownie uruchomić ***e!****RUNTIME.*

```
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 Zmiana haseł

Wskazówka

Zmiana haseł standardowych!
Ustawione fabrycznie, standardowe hasła dla wszystkich użytkowników podane w niniejszej instrukcji obsługi nie stanowią wystarczającego zabezpieczenia! Należy zmienić te hasła stosownie do potrzeb. Będą do tego potrzebne uprawnienia administratora!

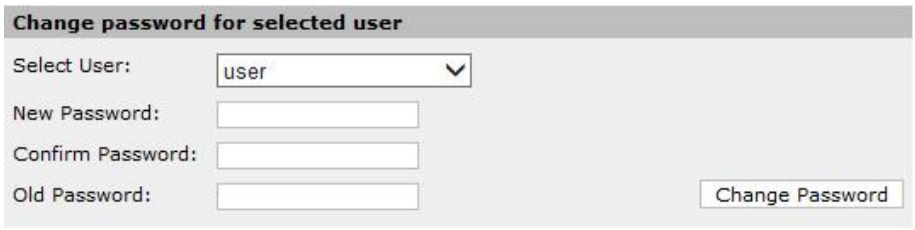
6.3.1 Zmiana haseł w systemie zarządzania przez WWW

Aby otworzyć system zarządzania przez WWW, wprowadź adres IP lub nazwę hosta sterownika w wierszu adresu przeglądarki. Wymagane ustawienia można znaleźć w instrukcji odpowiedniego sterownika.

Wskazówka

Wymagana jest rejestracja!
Aby zmienić domyślne parametry, musisz się najpierw zalogować.
Wprowadź następujące dane dostępowe:
Nazwa użytkownika: admin
Hasło: wago

1. W WBM wybierz pozycję menu **Administration** > **Users**, aby zmienić hasło.



Rys. 44: Zmiana haseł w systemie zarządzania przez WWW

2. Wybierz użytkownika („user“ lub „admin“), dla którego ma być nadane nowe hasło.
3. Wprowadź nowe hasło w polu **New Password**.
4. Potwierdź nowe hasło w polu **Confirm Password**.
5. Kliknij przycisk **[Change Password]** aby zastosować zmianę.

Wskazówka

Zwróć uwagę na dopuszczalne znaki dla haseł!
W haśle dopuszczalne są następujące znaki ASCII: a … z, A … Z, 0 … 9, spacje i znaki specjalne:]!"#$%&'()*+,./:;<=>?@[\^_`{|}~-

Jeśli poza WBM (np. przez CBM) tworzone są hasła zawierające znaki niedopuszczalne w WBM, dostęp do stron WBM nie będzie możliwy!

6.3.2 Zmiana hasła Linux® za pomocą konsoli Linux®

Połączenie z konsolą Linux® można uzyskać za pośrednictwem różnych dostępów:

- przez konsolę, poprzez interfejs RS-232
- przez SSH, poprzez ETHERNET

Sterowniki WAGO są dostarczane z różnymi nazwami użytkowników i standardowymi hasłami:

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

Wprowadzając nowe hasła, należy zapoznać się z zaleceniami dotyczącymi bezpiecznych haseł w rozdziale: "Scenariusze zagrożeń"> ...> "Dostęp przez użytkownika i hasła". Każdy użytkownik może zmienić własne hasło, użytkownik "root" może zmienić hasło dla wszystkich innych użytkowników.

1. Połącz się z konsolą Linux® przez konsolę poprzez interfejs RS-232 lub przez SSH poprzez port ETHERNET.
2. Zmień hasła za pomocą narzędzia Linux® „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
```

Wskazówka

Dla aktualnego użytkownika można pominąć nazwę użytkownika!
Jeśli hasło ma zostać zmienione tylko dla aktualnego użytkownika, nazwa użytkownika może zostać pominięta.

Alternatywnie można zmienić hasło dla użytkownika "admin" poprzez WBM.

1. W WBM wybierz punkt menu **Ports and Services** > **PLC Runtime Services** > **General Configuration**.

Rys. 45: Zmiana hasła dla użytkownika "admin"

2. Wprowadź swoje hasło w polu **Port Authentication Password**.
3. Potwierdź nowe hasło w polu **Confirm Password**.
4. Naciśnij przycisk **[Submit]**, aby zaakceptować hasło.

6.4 Konfiguracja firewalla

Aby zabezpieczyć sieć przed atakami z zewnątrz, należy skonfigurować firewall za pomocą odpowiedniego dla aplikacji zestawu reguł.

UWAGA

Należy zadbać o awaryjny dostęp do systemu!
Zawsze konfiguruj dostęp awaryjny przed skonfigurowaniem firewalla, na przykład dostęp przez połączenie szeregowe. Gwarantuje to, że system nie zostanie omyłkowo wyłączony!

Sterownik ma wbudowaną zaporę hosta opartą na systemie Linux® iptables. Zapora działa jako filtr białej listy; pakiety które nie są wyraźnie dozwolone przez białą listę, są blokowane przez zaporę. Filtry są przetwarzane w tak zwanych łańcuchach (Chains); kolejność w ich obrębie określa kolejność przetwarzania.

Sterownik obsługuje tworzenie własnych reguł filtrowania za pomocą następujących działań:

Tabela 10: Działania dla reguł filtrowania

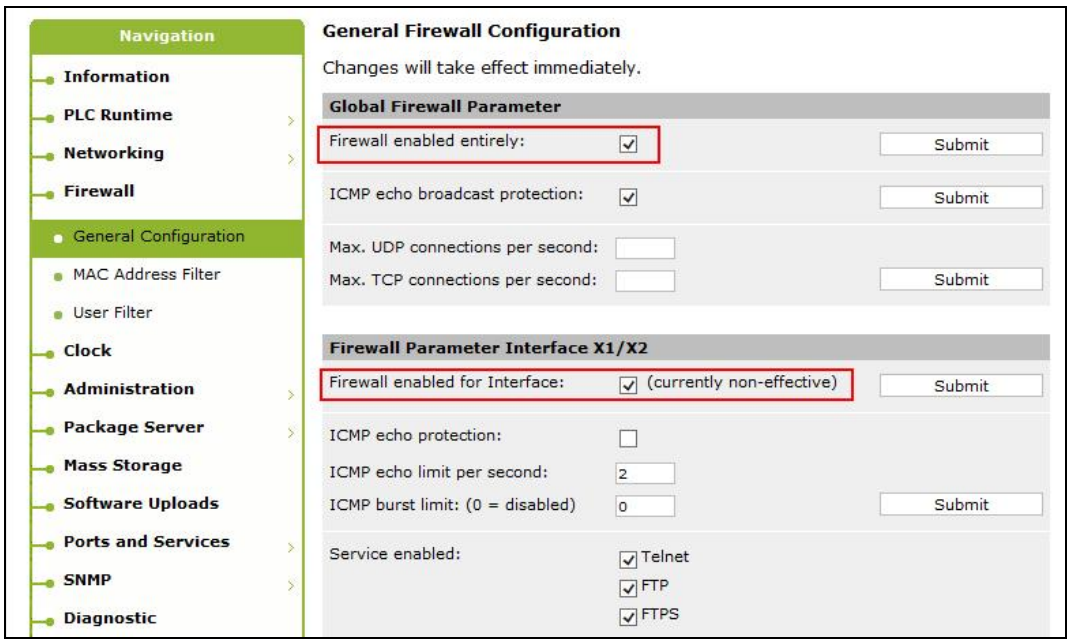
Zdarzenie	Opis
ACCEPT	pakiet jest akceptowany i dopuszczany
DROP	pakiet nie jest dopuszczany; nadawca nie otrzymuje żadnej wiadomości

W WBM można tworzyć własne filtry, patrz rozdział "Konfigurowanie firewalla w systemie zarządzania przez WWW".

Po akcji ACCEPT lub DROP żadne dalsze reguły nie będą przetwarzane.
Jeśli do pakietu nie może być zastosowana żadna reguła, zostanie do niego wykonana reguła predefiniowana. Sterownik jako predefiniowaną regułę stosuje akcję DROP dla przychodzącego ruchu sieciowego, z wyjątkiem już istniejących połączeń.
Filtry tworzone przez użytkowników są natychmiast skuteczne i są przetwarzane przed predefiniowanymi regułami. Informacje na temat wstępnie zdefiniowanych reguł można znaleźć w instrukcji obsługi sterownika na stronie www.wago.com.
Pakiety zaakceptowane przez filtr użytkownika (akcja ACCEPT) są przekazywane bezpośrednio do odpowiedniej usługi, bez przekazywania predefiniowanych reguł.

6.4.1 Konfiguracja firewalla w systemie zarządzania przez WWW (WBM)

Pod pozycją menu **Firewall > General Configuration** można skonfigurować ustawienia firewalla.



Rys. 46: Konfiguracja firewalla w WBM

Aby włączyć firewalla, należy wprowadzić następujące ustawienia:

1. Włącz pole **Firewall enabled entirely** (domyślnie wyłączone).
2. Kliknij na przycisk **[Submit]**. Zastosowane będą odpowiednie ustawienia
3. Włącz pole **Firewall enabled for Interface.**
4. Kliknij na przycisk **[Submit]**. Zastosowane będą odpowiednie ustawienia

Wskazówka

Zezwalaj tylko na dostęp z zaufanych sieci!
Firewall może być aktywowany tylko dla wybranego interfejsu. Zwróć uwagę na strukturę sieci i koncepcję bezpieczeństwa dla twojej aplikacji. Zezwalaj tylko na dostęp do Twojego urządzenia tylko z zaufanych sieci!

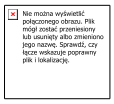
Wskazówka

Reguły firewalla dotyczą zarówno IPsec, jak i OpenVPN!
Konfiguracja reguł zapory VPN za pośrednictwem WBM (**Firewall Parameter Interface VPN**) jest niezależna od zastosowanej technologii VPN (IPsec lub OpenVPN). Fabrycznie zdefiniowane są standardowe reguły IPsec dla interfejsu modemu (wwan) i standardowe reguły dla OpenVPN (tun + i tap +). Wstępnie zdefiniowane reguły można przeglądać przez konsolę Linux® za pomocą komendy "iptables-save".

6.4.1.1 Utwórz białą listę dla określonych adresów IP

Można utworzyć białą listę, która zdefiniowanym adresom IP umożliwia dostęp do usług oferowanych przez system.

UWAGA



Akcję DROP zawsze twórz PO akcji ACCEPT!
Zawsze najpierw stwórz regułę ACCEPT dla własnego adresu IP, w przeciwnym razie istnieje ryzyko zablokowania systemu!

Wskazówka

Reguły filtrowania użytkownika mają pierwszeństwo!
Pamiętaj, że reguły filtrowania użytkownika są wykonywane przed wstępnie zdefiniowanymi regułami w sterowniku. Po akcji ACCEPT wstępnie zdefiniowane reguły nie są już stosowane. Z tego powodu zawsze powinieneś określać port pod "Destination Port", aby przypadkowo nie dać pełnego dostępu do wszystkich portów w Twoim systemie!

W celu utworzenia białej listy, zostaną najpierw do niej dodane wszystkie adresy IP, które mają dostęp do usługi systemu. Następnie tworzony jest filtr z akcją DROP, który blokuje wszystkie inne dostępy.

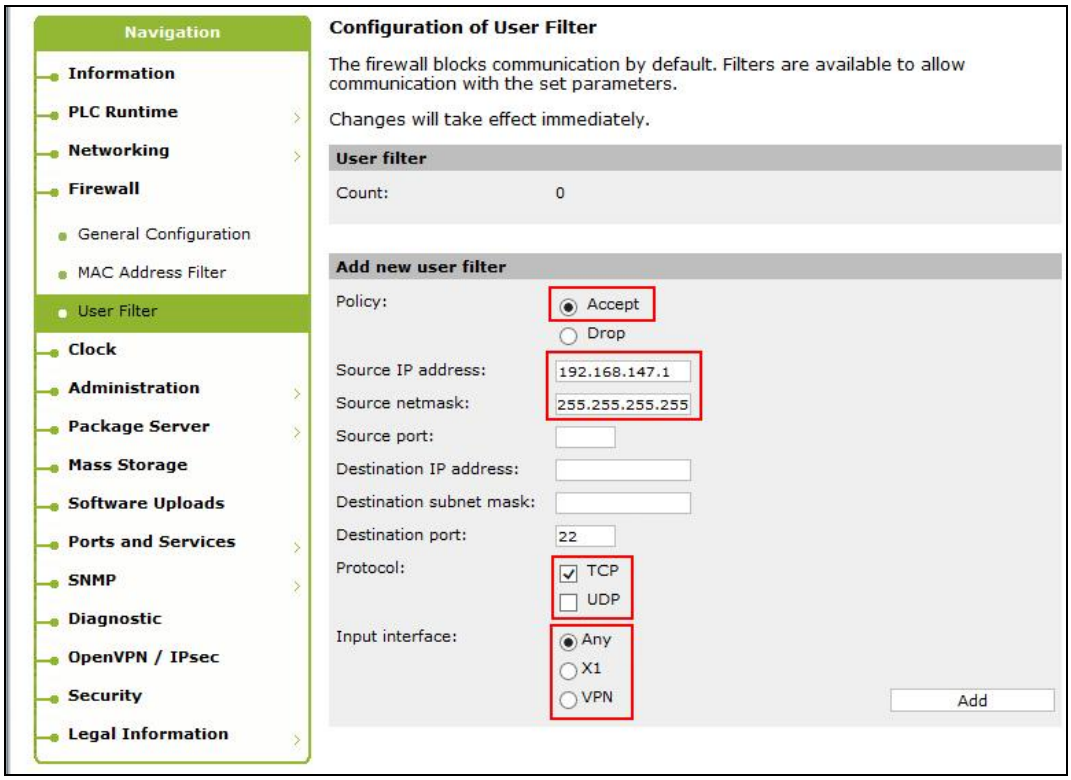
Poniżej znajduje się przykład adresu IP 192.168.147.1 odblokowanego dla dostępu do SSH (patrz kroki 1 ... 8). Wszystkie inne adresy IP są blokowane dla dostępu (patrz kroki 9 ... 16).

Akcja ACCEPT

1. Przejdź do menu **Firewall > User Filter**.
2. W obszarze „Add new user filter > Policy“ aktywuj pole **Accept**.
3. W polu **Source IP address** wpisz adres IP, któremu chcesz zezwolić na dostęp.
4. Wprowadź maskę sieci "255.255.255.255" w polu **Source netmask**, jeśli chcesz zezwolić na dostęp **jedynie** podanemu adresowi IP.
5. Wprowadź w polu **Destination port** port aplikacji, która ma zostać odblokowana.
6. Aktywuj pole **TCP lub UDP**, w zależności od protokołu, który chcesz odblokować.
7. Aktywuj pole **Any, X1** lub **VPN** aby zastosować regułę dla odpowiedniego interfejsu.

Wskazówka

Interfejs X2 nie jest dostępny w trybie switch!
Dwa interfejsy ETHERNET X1 i X2 mogą działać w trybie switch lub jako osobne interfejsy sieciowe. Jeśli używasz obu interfejsów sieciowych, musisz skopiować regułę dla interfejsu X2.



Rys. 47: Filtr użytkownika: Tworzenie białej listy

8. Kliknij przycisk **[Add]**. Zasada jest przyjęta.

Akcja DROP

9. Przejdź do menu **Firewall > User Filter**.

10. W obszarze „Add new user filter > Policy“ aktywuj pole **Drop**.

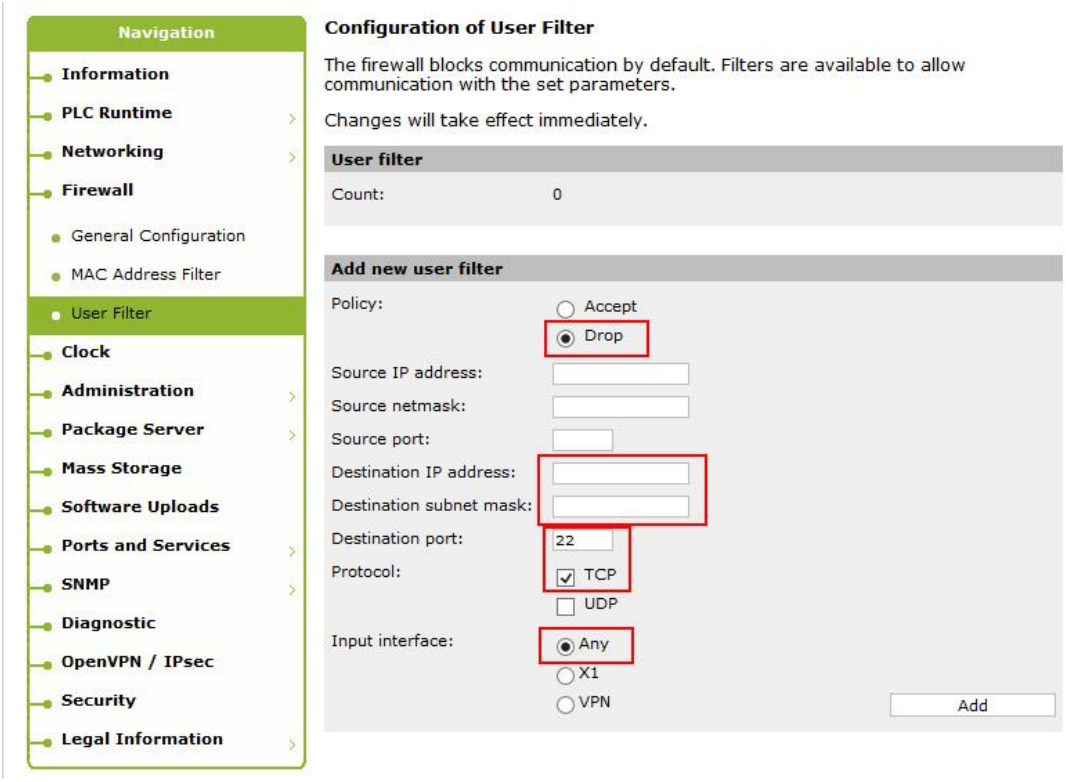
11. Pozostaw puste pole **Source IP adress**.

12. Pozostaw puste pole **Source netmask**.

13. Wprowadź w polu **Destination port** port aplikacji, która ma zostać odblokowana, np. „22“ dla SSH.

14. Aktywuj pole **TCP lub UDP**, w zależności od protokołu, który chcesz odblokować.

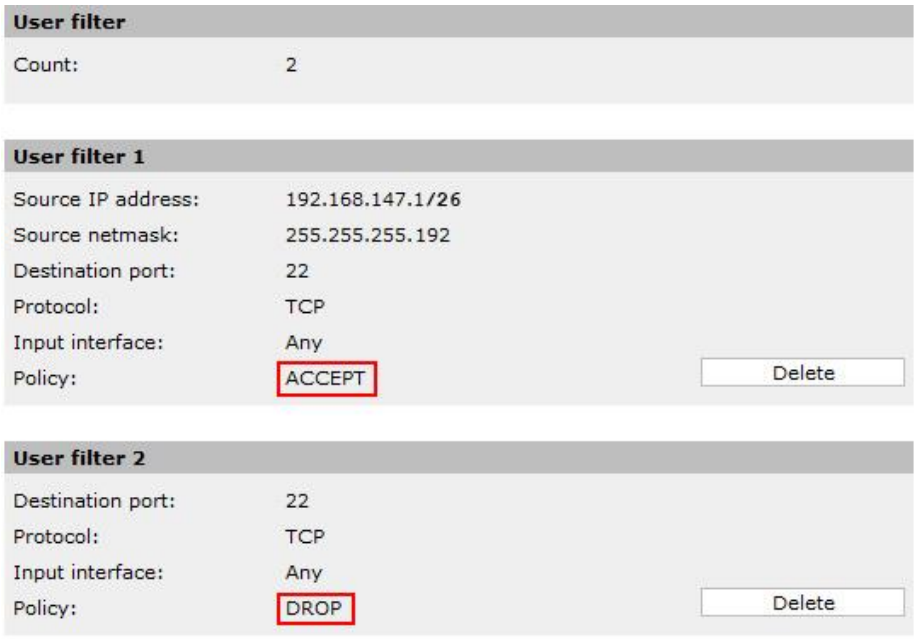
15. Aktywuj pole **Any**, aby zastosować regułę dla każdego interfejsu.



Rys. 48: Tworzenie czarnej listy dla wszystkich dostępów

16. Kliknij przycisk **[Add]**. Zasada jest przyjęta.

W efekcie filtrowanie odbywa się w następującej kolejności:

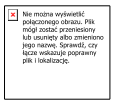


Rys. 49: Kolejność reguł filtrowania

6.4.1.2 Utwórz białą listę dla sieci

Jeśli biała lista ma zostać utworzona dla jednej sieci lub kilku sieci, należy ją najpierw zwolnić za pomocą akcji AKCEPTUJ. Następnie dostęp do wszystkich innych sieci musi zostać zablokowany przez akcję DROP, podobnie jak w przypadku zwolnienia pojedynczego adresu IP. Reguły filtrowania aktywowane w "Firewall" > „General Configuration“ zostaną przez to unieważnione. Dlatego określ port usługi, którą chcesz udostępnić.

UWAGA



Akcję DROP zawsze twórz PO akcji ACCEPT!
Zanim odmówisz dostępu pewnym adresom IP lub sieciom, musisz najpierw utworzyć białą listę, w przeciwnym razie nie będą już mogły być używane. W ten sposób można niechcący zablokować dostęp do sieci!

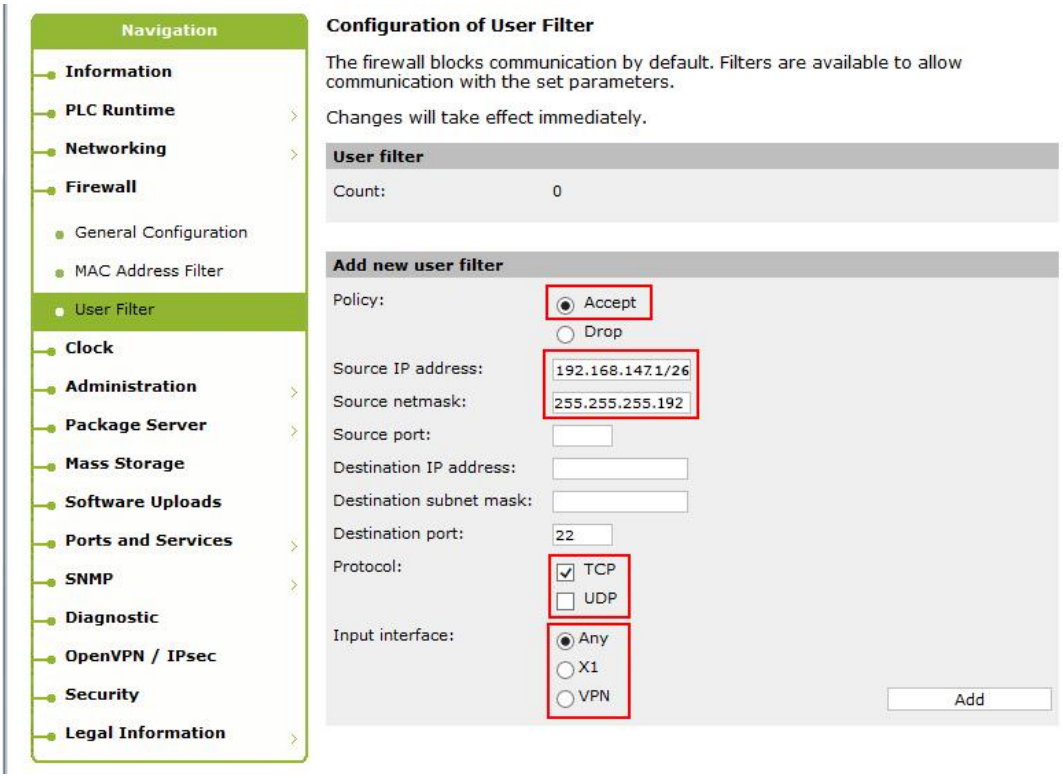
Poniżej znajduje się przykład sieci 192.168.147.1/26 odblokowanej dla dostępu do SSH (patrz kroki 1 ... 8). W przedstawionych przykładach każdy dostęp dla innych abonentów sieci jest wyłączony (patrz kroki 9 ... 16).

Akcja ACCEPT

1. Przejdź do menu **Firewall > User Filter**.
2. W obszarze „Add new user filter > Policy“ aktywuj pole **Accept**.
3. W polu **Source IP address** wpisz adres IP, któremu chcesz zezwolić na dostęp.
4. Wprowadź w polu **Source netmask** maskę sieci „255.255.255.192“.
5. Wprowadź w polu **Destination port** port aplikacji, która ma zostać odblokowana.
6. Aktywuj pole **TCP lub UDP**, w zależności od protokołu, który chcesz odblokować.
7. Aktywuj pole **Any, X1** lub **VPN** aby zastosować regułę dla odpowiedniego interfejsu.

Wskazówka

Interfejs X2 nie jest dostępny w trybie switch!
Dwa interfejsy ETHERNET X1 i X2 mogą działać w trybie switch lub jako osobne interfejsy sieciowe. Jeśli używasz obu interfejsów sieciowych, musisz skopiować regułę dla interfejsu X2.

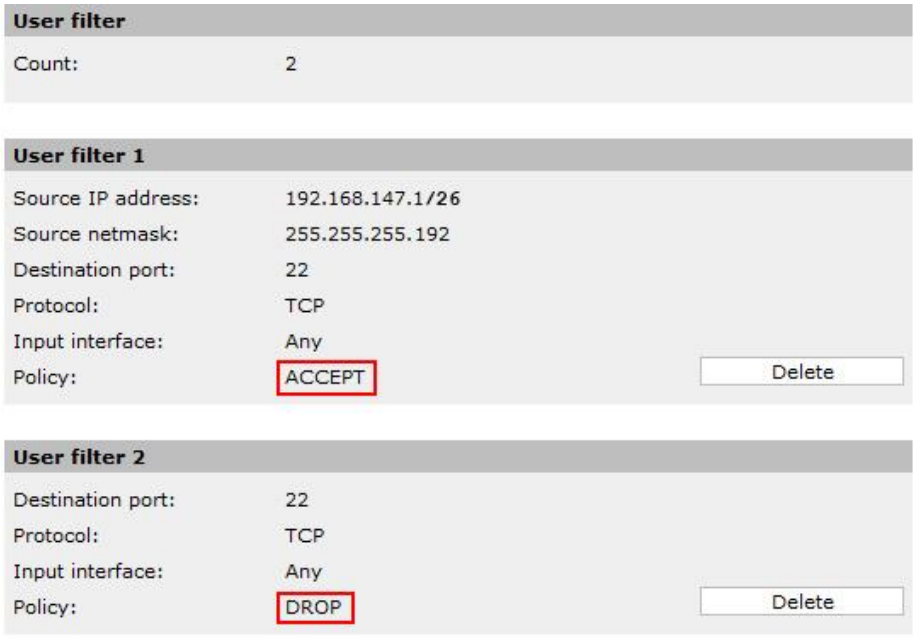


Rys. 50: Filtr użytkownika: Tworzenie białej listy dla sieci

8. Kliknij przycisk **[Add]**. Zasada jest przyjęta.

Akcja DROP

9. Przejdź do menu **Firewall > User Filter**.
10. W obszarze „Add new user filter > Policy“ aktywuj pole **Drop**.
11. Pozostaw puste pole **Source IP adress**.
12. Pozostaw puste pole **Source netmask**.
13. Wprowadź w polu **Destination port** port aplikacji, która ma zostać odblokowana, np. „22“ dla SSH.
14. Aktywuj pole **TCP lub UDP**, w zależności od protokołu, który chcesz odblokować.
14. Aktywuj pole **Any**, aby zastosować regułę dla każdego interfejsu.
15. Kliknij przycisk **[Add]**. Zasada jest przyjęta.



Rys. 51: Odblokowanie zdefiniowanych sieci.

W pokazanym przykładzie sieć 192.168.147.1/26 uzyskała dostęp do SSH. Obejmuje to adresy IP 192.168.147.1 ... 192.168.147.62 i adres rozgłoszeniowy 192.168.147.1.63.

6.4.2 Filtr adresu MAC

Adresy MAC urządzenia można łatwo sfałszować. Filtrowanie adresów MAC, jako jedyny środek bezpieczeństwa, jest zatem niewystarczające. Adresy MAC są używane w warstwie ETHERNET i wymagają fizycznego dostępu do sieci lokalnej (LAN). Nie można więc zapobiec dostępowi z zewnątrz, np. poprzez router. Gdy dostęp do systemu odbywa się przez router, sterownik widzi tylko adres MAC routera. Dlatego zaleca się łączenie filtrowania adresów MAC z innymi mechanizmami ochrony.

Dla sterownika w wersji fabrycznej wprowadzany jest standardowo filtr "White Listing" dla wszystkich adresów MAC WAGO, na podstawie identyfikatora producenta OUI (Organizationally Unique Identifier), ale nie jest on aktywny. Ten filtr powinien zostać usunięty i zastąpiony filtrami pasującymi do warunków w Twojej sieci.

1. Zawsze preferuj adresy MAC innych zaufanych uczestników sieci, zamiast identyfikatora producenta. Identyfikator producenta odblokowuje wszystkie adresy MAC producenta; w wielu przypadkach nie jest to pożądane.

2. Przed aktywacją filtra adresu MAC udostępnij adres MAC swojego PC lub dostępu do urządzenia (np. router, serwer proxy itp.), aby nie zablokować systemu!

6.4.2.1 Konfiguracja adresów MAC w systemie zarządzania przez WWW

Pod pozycją menu **Firewall > MAC Address Filter** można aktywować i skonfigurować filtr adresów MAC:

Przede wszystkim wprowadzane są adresy MAC wszystkich urządzeń, które mogą komunikować się z urządzeniem.

1. W polu **MAC address** w obszarze "MAC address filter whitelist" wprowadź adres MAC, który ma zostać odblokowany.

2. W polu **MAC mask** wprowadź wartość "ff: ff: ff: ff: ff: ff" w obszarze "MAC address filter whitelist".

Wskazówka

Maska MAC dla nowej pozycji na liście
Wpis w polu **MAC mask** określa bity, które są sprawdzane, jeśli ma być odblokowany określony adres MAC.

3. Aktywuj pole wyboru **Filter enabled.**

Rys. 52: Wprowadzanie adresów MAC

4. Naciśnij przycisk **[Add]**. Zarejestrowany adres MAC jest teraz odblokowany.

Wskazówka

Liczba pozycji na liście jest ograniczona!
Można wprowadzić maksymalnie 10 filtrów adresów MAC.

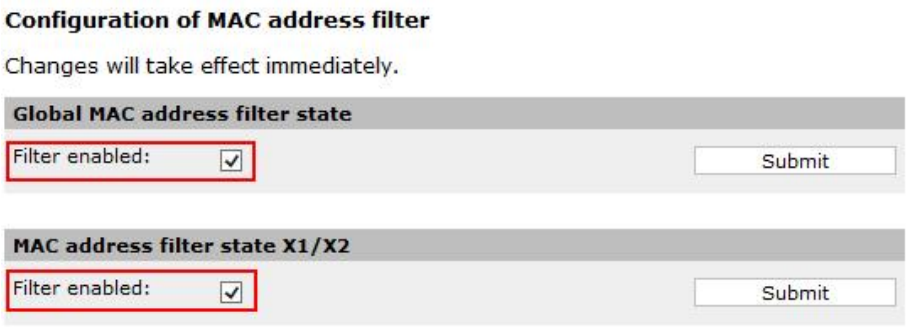
Po wprowadzeniu wszystkich adresów MAC, filtr adresu MAC musi zostać aktywowany.

5. Włącz pole **Filter enabled** w obszarze "Global MAC address filter state", aby włączyć globalny filtr adresów MAC.

6. Naciśnij przycisk **[Submit]**. Zastosowane będą odpowiednie ustawienia.

7. Aktywuj pole **Filter enabled** w obszarze "MAC address filter state X1/X2", aby włączyć filtr adresów MAC dla każdego interfejsu.

8. Naciśnij przycisk **[Submit]**. Zastosowane będą odpowiednie ustawienia.



Rys. 53: Aktywowanie filtra adresu MAC

7 Rozszerzone środki bezpieczeństwa

W niniejszym rozdziale opisano dodatkowe środki bezpieczeństwa, które można wdrożyć w PFC100/200 i w efekcie zwiększyć bezpieczeństwo systemu.

7.1 VPN – Virtual Private Network

7.1.1 Dane ogólne

Termin "Virtual Private Network" oznacza wiele technologii (np. IPsec), które mogą tworzyć wirtualną sieć prywatną w publicznie dostępnej sieci. W ramach takiego zamkniętego połączenia VPN, mogą się ze sobą bezpiecznie komunikować tylko połączeni i autoryzowani uczestnicy.

Zasadniczo istnieją dwie procedury uwierzytelniania: albo na podstawie certyfikatu, albo za pośrednictwem wcześniej zainstalowanego klucza klucza statycznego (Pre-shared Key).

- **Na podstawie certyfikatu**: uwierzytelnianie oparte na certyfikacie weryfikuje lub potwierdza tożsamość punktu końcowego VPN za pomocą certyfikatu cyfrowego. Certyfikat cyfrowy jest oparty na indywidualnej parze kluczy składającej się z klucza prywatnego i publicznego. Jeśli certyfikat cyfrowy punktu końcowego VPN zostanie zdyskredytowany, musi on zostać zablokowany i wymieniony na urządzeniu, którego dotyczy problem, patrz rozdział "Uodpornianie"> ...> "Tworzenie listy unieważnionych certyfikatów".
- **Pre-shared Key**: metoda klucza współdzielonego korzysta ze wspólnego klucza statycznego dla wszystkich punktów końcowych VPN. W przypadku dyskredytacji klucza współdzielonego, musi on zostać ręcznie wymieniony na wszystkich punktach końcowych VPN.

Wskazówka

Zwróć uwagę na zalecenia dotyczące procedur kryptograficznych!
Dodatkowa kopia zapasowa pakietów danych za pomocą szyfrowania prowadzi do opóźnienia, a tym samym do dłuższego czasu tranzytu pakietu. Zwróć uwagę na wybór długości klucza dla procedur kryptograficznych, zgodnie z wytycznymi technicznymi BSI TR-02102-4 (wersja 2017-01)!

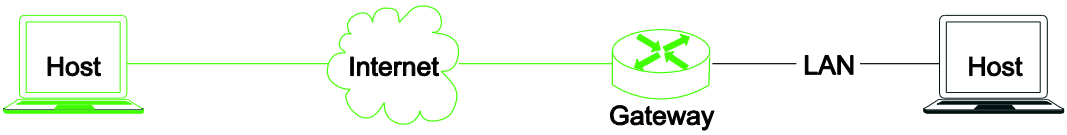
Poniżej przedstawiono typowe podstawowe scenariusze tworzenia sieci VPN:

VPN typu site-to-site

Rys. 54: VPN typu site-to-site

VPN typu site-to-site łączy dwie lub więcej sieci lokalnych w wirtualną sieć logiczną przez Internet, jak pokazano na rysunku "VPN typu site-to-site". Bezpieczna komunikacja odbywa się między dwoma gatewayami (na przykład gateway VPN lub router).

VPN typu host-to-site



Rys. 55: VPN typu host-to-site

VPN typu host-to-site umożliwia określonym użytkownikom (np. Home-Office lub w telefon komórkowy) bezpieczny dostęp do sieci zdalnej, jak pokazano na rysunku "VPN typu host-to-site". Bezpieczna komunikacja odbywa się z systemu końcowego użytkownika (hosta) do gatewaya zdalnej sieci (np. gateway VPN lub router VPN).

VPN typu host-to-host

Rys. 56: VPN typu host-to-host lub pulpit zdalny VPN

Sieć VPN typu host-host umożliwia bezpieczne połączenie VPN między dwoma systemami końcowymi (zabezpieczenie typu end-to-end), jak pokazano na rysunku "VPN typu host-host." Zapewnia to pełną komunikację między uczestniczącymi systemami końcowymi.

Poniższe rozdziały opisują przykładowo oba scenariusze site-to-site i host-to-host dla sterowników.

7.1.2 Tworzenie certyfikatów

W celu uwierzytelniania opartego na wzajemnym certyfikacie, punkty końcowe VPN wymagają certyfikatu podpisanego przez zaufany urząd certyfikacji (CA). Podczas tworzenia certyfikatów postępuj zgodnie z instrukcjami podanymi na końcu tej sekcji.

Instrukcje dotyczące tworzenia certyfikatów i kluczy można znaleźć w rozdziale "Uodpornianie"> ...> "Tworzenie i wymiana certyfikatów".

Wskazówka

W przypadku sieci VPN opartych na protokole TLS (OpenVPN), certyfikat klienta wymaga innego szablonu niż certyfikat serwera!
Należy zwrócić uwagę, aby podczas tworzenia żądania certyfikatu klienta w zakładce "Origin" w polu **Template for the New Certificate** wybrać **[default] HTTPS_client.** Patrz rozdział „Uodpornianie“ > … > „Tworzenie żądania certyfikatu urządzenia“. W opisie wybrano szablon **[default] HTTPS_client**!

Wskazówka

Upewnij się, że ustawiony czas jest taki sam na wszystkich systemach!
Jeśli korzystasz z certyfikatów, czas musi być taki sam we wszystkich systemach. W przeciwnym razie może dojść do problemów, jeśli certyfikaty będą traktowane przez ten sam system jako jeszcze ważne lub jako już wygasłe.

7.1.3 Aktywowanie funkcji „IP Forwarding“

W przypadku VPN typu site-to-site, punkty końcowe VPN muszą być skonfigurowane jako routery. W tym celu w sterowniku należy aktywować funkcję "IP Forwarding". To ustawienie jest domyślnie wyłączone. Aby można było przekazywać przychodzące i wychodzące pakiety do i z sieci, włącz „IP Forwarding“ na sterowniku w następujący sposób:

1. W WBM wybierz **Networking > Routing**, aby aktywować funkcję "IP Forwarding".

2. Zaznacz pole **Routing enabled entirely** w obszarze **„**General Routing Configuration“.

Rys. 57: Aktywowanie funkcji „IP Forwarding“

3. Naciśnij przycisk **[Submit]**, aby zapisać ustawienie.

Alternatywnie można aktywować funkcję "IP Forwarding", wpisując następujący wiersz w pliku "etc / sysctl.conf" lub dostosowując istniejącą pozycję:

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

7.1.4 OpenVPN

Za pomocą bezpłatnego oprogramowania OpenVPN można utworzyć wirtualną sieć prywatną (VPN) za pośrednictwem połączenia TLS. Obsługiwane są dwa tryby pracy:

- **Tryb Routing**: tworzy zaszyfrowany tunel, którym będą przekazywane tylko pakiety IP (warstwa 3 OSI).
- **Tryb Bridging**: umożliwia pełne tunelowanie ramek ETHERNET (warstwa OSI 2), umożliwiając użycie dowolnego protokołu sieciowego.

W następnych rozdziałach krok po kroku opisano konfigurację połączenia OpenVPN.

7.1.4.1 Konfiguracja użytkownika i grupy dla usługi OpenVPN

Najpierw dla usługi OpenVPN należy utworzyć dedykowanego użytkownika i grupę:

1. Zaloguj się do sterownika przez SSH.
2. Utwórz grupę „openvpn“:

```
addgroup -S openvpn
```

3. Utwórz użytkownika "openvpn" i wklej tego użytkownika do wcześniej utworzonej grupy "openvpn":

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

Wskazówka

Wpisz stworzonego użytkownika do pliku konfiguracyjnego OpenVPN!
OpenVPN musi być skonfigurowany w taki sposób, aby użytkownik po inicjalizacji przełączał się do utworzonego powyżej, nieuprzywilejowanego użytkownika, patrz rozdział "VPN typu Host-to-host", punkt "Minimalne uprawnienia"!

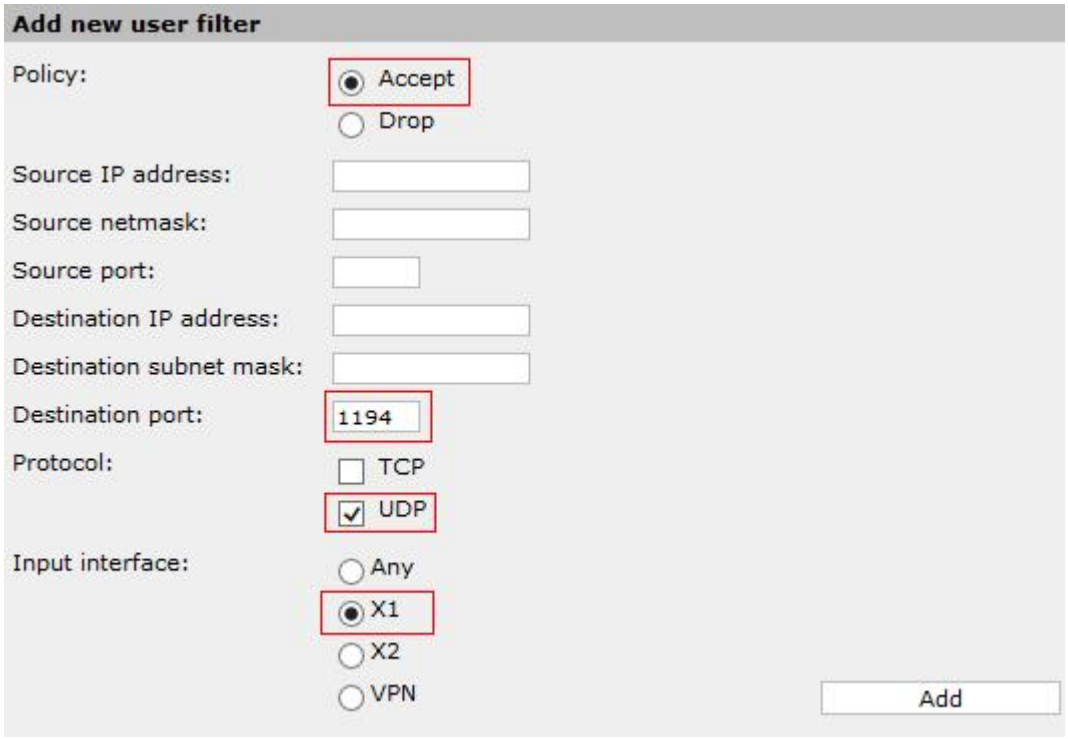
7.1.4.2 Konfiguracja firewalla

Wskazówka

W firewallu OpenVPN musi być udostępniony na serwerze!
Należy utworzyć na serwerze regułę wyjątku dla połączenia OpenVPN, ponieważ firewall nie udostępnia automatycznie połączenia dla sieci VPN!

1. Wybierz w WBM punkt menu **Firewall > User Filter**, aby utworzyć regułę wyjątku dla OpenVPN.

2. Wypełnij pola w obszarze "Add new user filter", jak pokazano na rysunku:



Rys. 58: Konfiguracja firewalla – OpenVPN

Wskazówka

Zwróć uwagę na prawidłowy wpis portu!
Upewnij się, że wpis pod "Destination port" jest identyczny z Twoim skonfigurowanym portem!

3. Naciśnij przycisk **[Add],** aby zastosować filtr.

Alternatywnie możesz skonfigurować firewall za pomocą następującego polecenia z konsoli Linux®:

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

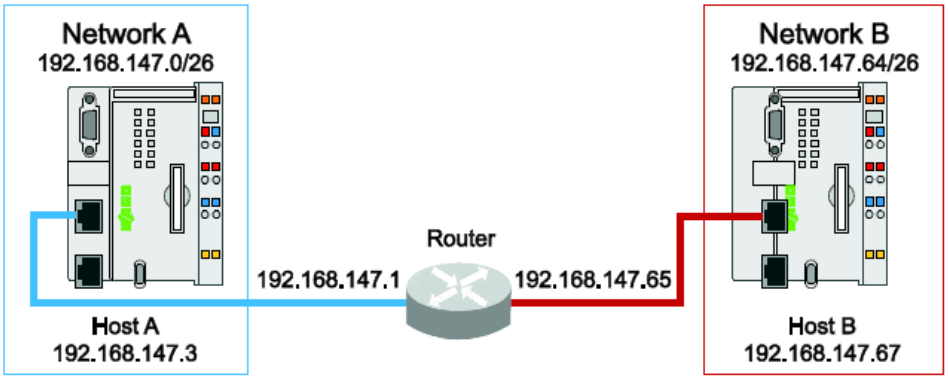
7.1.4.3 Konfiguracja rutowania

Rutowanie umożliwia komunikację poza granicami sieci. Jeśli dwa hosty nie znajdują się w jednej sieci, dane muszą być przesyłane przez router łączący obie sieci. W przypadku dużych sieci jak np. Internet, routerów może być wiele.

Trasy definiują ścieżkę logiczną w sieci do hosta docelowego. Podczas tworzenia tras podawany jest tylko następny host w drodze do hosta docelowego, a nie cała trasa. Jeśli dane są transportowane przez kilka routerów, trasy do następnego routera muszą być również utworzone na pośrednich routerach. W dużych sieciach, takich jak Internet, jest to sterowane automatycznie, dopóki nie zostanie osiągnięty docelowy host (na przykład za pomocą Border Gateway Protocol (BGP)).

Poniżej opisano sposób tworzenia tras na sterowniku. W przypadku innych systemów, zapoznaj się z instrukcją obsługi urządzenia i/lub systemu operacyjnego.

W przypadku opisanej poniżej, przykładowej konfiguracji rutowania, zastosowano następującą topologię sieci:



Rys. 59: Topologia sieci, rutowanie

Host A służy do wymiany danych z hostem B. W tym celu dane z hosta A muszą być przesyłane przez router, który przekazuje dane z sieci A do sieci B. Aby osiągnąć pożądane zachowanie, hostowi A komunikuje się najpierw za pośrednictwem trasy, że sieć B, w której znajduje się host B, jest dostępna za pośrednictwem routera (192.168.147.1).

Dostęp do tej trasy można uzyskać za pomocą narzędzi konfiguracyjnych:

```
/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
```

Alternatywnie możesz dodać trasę do sterownika za pośrednictwem WBM:

1. Wybierz w WBM punkt menu **Networking** > **Routing**.

2. W obszarze "General Routing Configuration" zaznacz pole **Routing enabled entirely**.

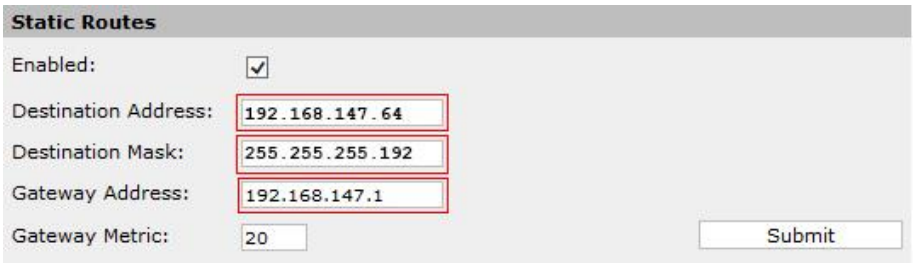
Rys. 60: Routing enabled

3. W obszarze „Static Routes“ zaznacz pole **Enabled**.

4. Wprowadź adres docelowy sieci B w polu **Destination Address.**

5. Wprowadź maskę sieci dla sieci B w polu **Destination Mask**.

6. Wprowadź adres IP routera w polu **Gateway Address.**



Rys. 61: Static Routes

7. Zapisz ustawienie za pomocą przycisku **[Submit]**.

8. Powtórz rutowanie dla hosta B.

Wskazówka

Trasy muszą być tworzone w obu kierunkach!
Należy również utworzyć trasę na hoście B, aby zakomunikować hostowi B, że sieć A jest dostępna przez router (192.168.147.65) Jeśli trasa jest tworzona tylko w jednym kierunku, dane przechodzą np. z hosta A do hosta B; nie może on jednak odesłać z powrotem żadnych danych!

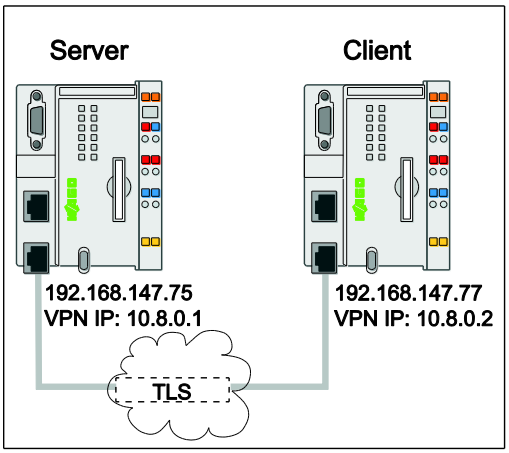
7.1.4.4 Tworzenie plików konfiguracyjnych

Oto dwa pliki konfiguracyjne dla sieci VPN typu host-to-host i site-to-site. Przykładowe konfiguracje można skopiować 1:1 i wykorzystać do swojej konfiguracji VPN. Należy dostosować tylko określone wartości użytkownika.

Wymagania:

- Certyfikaty i klucze zostały wygenerowane, patrz rozdział "Tworzenie i wymiana certyfikatów" oraz "Generowanie parametrów Diffiego-Hellmana".
- Certyfikaty są zlokalizowane w folderze / etc / certificates /. Klucz prywatny jest przechowywany w folderze / etc / certificates / keys /. Należy również określić obie ścieżki w pliku konfiguracyjnym OpenVPN, zobacz w tym celu konfigurację serwera "Specyfikacja lokalizacji pamięci dla certyfikatów i kluczy"!
  Informacje na ten temat znajdują się w rozdziale "Przenoszenie konfiguracji do sterownika".

7.1.4.4.1 VPN typu host-to-host



Rys. 62: Połączenie typu host-to-host

W poniższej przykładowej konfiguracji zakłada się, że serwer jest dostępny pod adresem IP 192.168.147.75, a klient pod adresem IP 192.168.147.77. Zmieniaj te wartości w zależności od okoliczności!

Utwórz następujące konfiguracje klienta i serwera dla VPN typu host-to-host.

Konfiguracja serwera

```
####################
#    Ogólnie     #
####################

# Konfiguracja serwera wieloplatformowego
mode server

##################
#    Sieć     #
##################

# Na jakim interfejsie powinna być oferowana usługa OpenVPN?
# Określ adres IP odpowiedniego interfejsu tutaj lub pomiń
# wpis, jeśli usługa ma być oferowana na wszystkich interfejsach.

local 192.168.147.75

# Na którym porcie ma być dostępna usługa OpenVPN
# Domyślny port to 1194, ale należałoby go unikać, aby nie
# doszło do automatycznego skanowania w Internecie.
port 1194

# Użyj UDP jako protokołu transmisji
proto udp

# Używamy trybu tunelowego, transmitowane są tylko protokoły warstwy 3 OSI.
dev tun

# Z jakiej topologii korzystamy w sieci VPN?
topology subnet

# Klienci dostają przypisany adres IP z następującej puli adresów.
# Nie wolno używać tego zakresu adresów w swojej sieci,
# w przeciwnym razie spowoduje to problemy i nie będzie można skonfigurować sieci
VPN.

server 10.8.0.0 255.255.255.0

# OpenVPN regularnie wysyła pakiety "keep-alive" z kluczem "keepalive"
# Można ustawić częstotliwość i liczbę sekund, po upływie których klient/serwer
# traktowany jest jako nieosiągalny.
keepalive 10 120

######################
#    Kryptografia    #
######################

# Specyfikacja miejsc przechowywania certyfikatów i kluczy
# Należy zachować klucz prywatny w tajemnicy!
ca /etc/certificates/my_root-ca.crt
cert /etc/certificates/my_openvpn_server.crt
key /etc/certificates/keys/my_openvpn_server.key

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

# Parametry Diffiego-Hellmana
dh /etc/certificates/dh2048.pem

# Oprócz certyfikatu klient wymaga klucza statycznego. Jest
# to środek ostrożności przeciwko atakom DoS.
# Możesz wygenerować klucz za pomocą następującego polecenia:
#      openvpn --genkey --secret /etc/openvpn/static.key
tls-auth static.key 0

# Szyfr, który powinien być używany domyślnie. W tym przypadku AES 256
# w trybie CBC (Cipher Block Chaining)
```

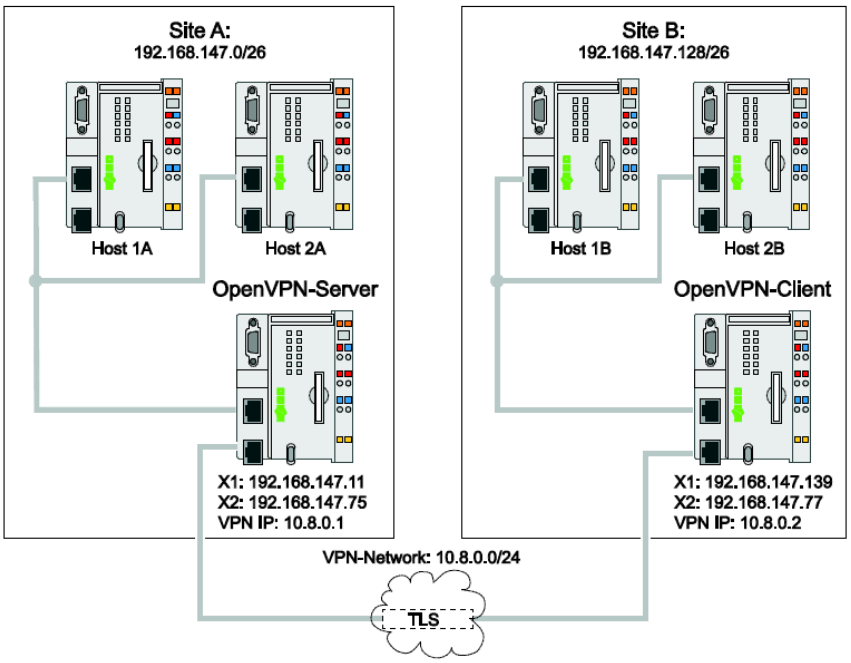
```
szyfr AES-256-CBC

#########################
#    Minimalne uprawnienia    #
#########################

# Usługa powinna działać z minimalnymi uprawnieniami,tutaj jest skonfigurowana
grupa i użytkownik,
# który jest potrzebny do wykonania – tego użytkownika należy ew.
założyć wcześniej. Patrz <Utwórz użytkownika dla OpenVPN>.
user openvpn
group openvpn

# Tryb specjalny, aby po ponownym uruchomieniu połączenie mogło zostać
# nawiązane, bez uprawnień „root"
persist-key
persist-tun

#################
#    Logowanie    #
#################

# Plik, w którym aktualny status jest zapisywany w interwałach minutowych
status /var/log/openvpn-status.log

# Szczegółowość serwera. W przypadku debugowania można tu ustawić wyższą wartość.
# aby przechowywać więcej wiadomości.
verb 4
```

Konfiguracja klienta

```
###################
#    Ogólnie    #
###################

# Konfiguracja klienta
client

#################
#    Sieć    #
#################

# Tutaj musi być taki sam jak serwer. W tym przypadku
# „tun", ponieważ OpenVPN ma działać w trybie tunelowym
dev tun

# Identyfikacja konfiguracji serwera, alternatywnie możliwe jest również TCPI
proto udp

# Tutaj określono serwer OpenVPN i port. Port musi być
# identyczny z portem skonfigurowanym na serwerze
remote 192.168.147.75 1194

# Klient stale próbuje połączyć się z serwerem. Nie ma
# limitu czasu, od którego próby połączenia są przerywane.
resolv-retry infinite

# Nie ma potrzeby łączenia z interfejsem sieciowym
nobind

#########################
#    Minimalne prawa    #
#########################

# Z którym użytkownikiem i którą grupą powinien działać klient OpenVPN.
user openvpn
group openvpn
```

```
# Tryb specjalny, tak aby po ponownym uruchomieniu usługi OpenVPN nawiązać
połączenie z minimalnymi
# uprawnieniami.
persist-key
persist-tun

######################
#    Kryptogrfia     #
######################

# Specyfikacja miejsc przechowywania certyfikatów i kluczy
# Należy zachować klucz prywatny w tajemnicy!
ca /etc/certificates/my_root-ca.crt
cert /etc/certificates/my_openvpn_client.crt
key /etc/certificates/keys/my_openvpn_client.key

# Aby zapobiec atakom typu MitM przy użyciu certyfikatów klienta, klient
# jest proszony o sprawdzenie przeznaczenia certyfikatów. Dlatego podczas
tworzenia
# certyfikatów upewnij się, że wprowadzasz
# poprawne zastosowania.
remote-cert-tls server

# Oprócz certyfikatu klient potrzebuje dodatkowego klucza.
# Jest on identyczny na wszystkich systemach i służy tylko do zapobiegania

# atakom DoS.
tls-auth static.key 1

# Standardowy szyfr. W tym przypadku AES-256 w trybie CBC (Cipher
# Block Chaining. Użyj poniższego polecenia, aby wyświetlić dodatkowe
# obsługiwane szyfry:
#    openvpn --show-ciphers
cipher AES-256-CBC

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

# Plik, w którym aktualny status jest zapisywany w interwałach minutowych.
status /var/log/openvpn-status.log

# Lokalizacja pliku Log, zawsze jest zakładana nowa. Jeśli chcesz
# zachować pamięć ciągłą, zastąp klucz "log"
# kluczem „log-append“.
log /var/log/openvpn.log

# Szczegółowość serwera. W przypadku debugowania można tu ustawić wyższą wartość
# aby móc zachować więcej wiadomości.
verb 4
```

7.1.4.4.2 VPN typu site-to-site



Rys. 63: VPN typu site-to-site

Site-to-site oznacza, że dwie lub więcej sieci są ze sobą połączone i można uzyskać dostęp do hosta za partnerem połączenia (serwer lub klient OpenVPN). W przypadku VPN typu site-to-site rozwiń poprzednio opisaną konfigurację host-to-host, o ustawienia opisane poniżej. W tym miejscu wymienione są tylko różnice; cała konfiguracja nie jest powtarzana.

Konfiguracja serwera OpenVPN

1. Aktywuj "IP Forwarding" na serwerze OpenVPN, aby od klientów OpenVPN uzyskać dostęp do sieci za serwerem OpenVPN , patrz rozdz. "Włącz IP Forwarding".

Serwer OpenVPN działa jako router dla sieci (witryna A) i przekazuje pakiety sieciowe do hostów.

2. Utwórz trasę dla sieci VPN na hostach w sieci za serwerem OpenVPN (witryna A) (patrz rozdział "Konfiguracja rutowania").

Za pomocą trasy, sieć VPN 10.8.0.0/24 jest dostępna za pośrednictwem hosta 192.168.147.11.

3. Wklej następującą część do konfiguracji serwera poniżej ustawień sieci, aby umożliwić dostęp do sieci za serwerem OpenVPN:

```
# Utwórz katalog poniżej katalogu
# konfiguracyjnego OpenVPN do konfiguracji klienta(en)
client-config-dir ccd
```

4. Utwórz plik konfiguracyjny dla każdego klienta pod wcześniej utworzonym katalogiem (patrz konfiguracja serwera "client-config-dir").

Plik musi być nazwany w taki sam sposób jak "commonName" w certyfikacie klienta, patrz rozdział "Tworzenie żądania certyfikatu urządzenia".

Wskazówka

Użytkownik lub grupa OpenVPN musi mieć dostęp do pliku!
Upewnij się, że użytkownik "openvpn" i/lub grupa "openvpn", które utworzyłeś w konfiguracji serwera dla VPN typu host-to-host, mają dostęp do odczytu pliku!

```
# Każdy klient OpenVPN otrzymuje stały adres IP z wcześniej skonfigurowanego
adresu IP
# Pula adresów dla VPN.
ifconfig-push 10.8.0.2 255.255.255.0

# Trasa dla sieci za serwerem musi być udostępniona
# klientowi OpenVPN.
push "route 192.168.147.0 255.255.255.192 10.8.0.1"
```

Dzięki tej konfiguracji klienci OpenVPN mogą uzyskać dostęp do sieci za serwerem OpenVPN.

Wskazówka

To ustawienie jest specyficzne dla klienta!
Zwróć uwagę, że dla każdego klienta OpenVPN należy utworzyć oddzielną konfigurację, jak opisano powyżej. Zastąp w niej adres IP dla danego klienta!

Konfiguracja klienta OpenVPN

1. Aktywuj "IP Forwarding" na kliencie OpenVPN, aby uzyskać dostęp do sieci za klientem OpenVPN, patrz Rozdz. "Włącz IP Forwarding".

Aby hosty znajdujące się za serwerem OpenVPN mogły uzyskać dostęp do hostów znajdujących się za klientem OpenVPN, serwer OpenVPN musi zostać poinformowany o sieci znajdującej się za klientem OpenVPN.

2. Dodaj trasę, rozszerzając konfigurację klienta po stronie serwera, o następujące ustawienia:

```
# udostępnienie sieci za klientem serwerowi OpneVPN.
iroute 192.168.147.128 255.255.255.192
```

Wskazówka

To ustawienie jest specyficzne dla klienta!
Trasa jest specyficzna dla każdego hosta i odpowiedniej sieci za klientem OpenVPN.
Dlatego musisz dostosować trasę dla każdego hosta!

3. Utwórz trasę na hostach w sieci za klientem OpenVPN (Site B) (patrz rozdział "Konfiguracja rutowania").

Ta trasa służy do kierowania pakietów sieciowych z sieci A (192.168.147.0/26) do hostów z sieci B za pośrednictwem klienta OpenVPN (192.168.147.139).

4. Utwórz dodatkowo trasę na hostach w sieci za serwerem OpenVPN (Site A) (patrz rozdział "Konfiguracja rutowania").

Ta trasa ma na celu umożliwienie komunikacji z hostami z sieci B (192.168.147.128/26) za pośrednictwem serwera OpenVPN (192.168.147.11).

Konfiguracja wieloplatformowa

Jeśli wielu klientów lub wiele sieci (Site C, D itp.) jest połączonych z serwerem OpenVPN, klienci muszą mieć możliwość komunikowania się ze sobą. W takim przypadku musisz rozszerzyć konfigurację OpenVPN o ustawienia opisane poniżej.

1. Wklej następujące polecenie konsoli do konfiguracji OpenVPN:

```
# Zezwalaj na komunikację klienta z klientem
client-to-client
```

Dzięki tej konfiguracji klienci mogą się ze sobą komunikować. Aby hosty z podłączonych sieci również mogły komunikować się ze sobą, musisz utworzyć odpowiednie trasy.

2. Dodaj trasę w konfiguracji klienta po stronie serwera:

```
# udostępnienie sieci za klientem serwerowi OpneVPN.
iroute 192.168.147.128 255.255.255.192
```

3. Utwórz trasy dla sieci, do której chcesz uzyskać dostęp (patrz rozdział "Konfiguracja rutowania") na hostach w sieci za klientem i serwerem OpenVPN.

Dzięki tym trasom hosty mogą wysyłać z sieci pakiety danych za pośrednictwem klienta lub serwera OpenVPN.

7.1.4.5 Przeniesienie konfiguracji do sterownika

Możesz skonfigurować sterownik, po wykonaniu następujących czynności:

- skonfigurowanie na sterowniku usługi OpenVPN
- wygenerowanie certyfikatów i kluczy Diffiego-Hellmana
- utworzenie plików konfiguracyjnych OpenVPN

1. Otwórz WBM i zaloguj się jako administrator ("admin").

2. Przejdź do menu **OpenVPN/IPsec**.

3. W obszarze "OpenVPN" wybierz plik konfiguracyjny, który chcesz przesłać do urządzenia.

Rys. 64: WBM, wybór pliku konfiguracyjnego

Wskazówka

Konwencja nazewnictwa i lokalizacja przechowywania pliku konfiguracyjnego!
Plik nie musi się nazywać openvpn.conf, ale po transferze zmienia nazwę na "openvpn.conf" i jest zapisywany w folderze / etc / openvpn /!

4. W obszarze "Certificate upload" w polu **New Certificate** wybierz odpowiednie certyfikaty. (Główny certyfikat CA i certyfikat dla klienta lub serwera). Dla serwera możesz również załadować parametry Diffiego-Hellmana, które są podawane przez serwer.

5. W obszarze "Certificate Upload" w polu **New Private Key** wybierz swój klucz prywatny.

Rys. 65: WBM, wybór aprobat

Wskazówka

Miejsca przechowywania certyfikatów i kluczy!
Certyfikaty są po przesłaniu przechowywane w folderze /etc/certificates/.
Klucz prywatny znajduje się w folderze /etc/certificates/keys/.
Należy także określić obie ścieżki w konfiguracji OpenVPN!

6. W obszarze "OpenVPN" zaznacz pole **OpenVPN enabled**, aby usługa OpenVPN była dostępna po ponownym uruchomieniu.

Rys. 66: Aktywacja usługi OpenVPN

6. Uruchom usługę OpenVPN za pomocą narzędzi konfiguracyjnych:

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

Można też ponownie uruchomić urządzenie.

7.1.5 IPsec

IPsec jest rozszerzeniem protokołu IP, który został uzupełniony o kryteria bezpieczeństwa dotyczące poufności, uwierzytelniania i integralności. Umożliwia to kryptograficzne zabezpieczenie pakietów IP, co zapewnia bezpieczną komunikację w niezabezpieczonych sieciach. Tworzenie kopii zapasowych pakietów odbywa się na warstwie 3 (patrz model OSI, warstwa sieciowa). IPsec rozróżnia następujące tryby transmisji:

- **Tryb tunelowy:** w trybie tunelowym kompletny pakiet IP (w tym nagłówek IP) jest hermetyzowany i wyposażony w nowy, dodatkowy nagłówek IP. Zaletą tego trybu, w porównaniu do trybu transportowego, jest ukrycie adresu źródłowego lub docelowego. Tożsamość faktycznego partnera komunikacji pozostaje ukryta. Tryb tunelowy może być używany w podstawowych scenariuszach host-to-host, host-to-site i site-to-site.
- **Tryb transportowy**: w trybie transportowym nie jest dodawany nowy nagłówek IP, tak więc informacje niezbędne do transmisji pakietów sieciowych są pobierane z oryginalnego nagłówka IP. W tym trybie transmisji nie można łączyć różnych sieci. Ten tryb może być używany tylko w scenariuszu host-host.

7.1.5.1 Protokoły bezpieczeństwa

Protokół IPsec zapewnia dwa protokoły zabezpieczeń: nagłówek uwierzytelniania (AH) i protokół ESP (Encapsulating Security Payload):

- **Nagłówek uwierzytelniania (AH):** "Nagłówek AH" zapewnia integralność i autentyczność przesyłanych danych. AH nie chroni poufności; wszystkie dane są przesyłane w postaci zwykłego tekstu.
- **Encapsulating Security Payload (ESP):** ESP zapewnia integralność i autentyczność w taki sam sposób jak protokół bezpieczeństwa AH. W przeciwieństwie do AH, poufność jest dodatkowo zapewniona przez szyfrowanie przesyłanych danych.

Protokoły bezpieczeństwa ESP i AH mogą być używane osobno lub razem, w zależności od wymagań bezpieczeństwa. Procedury szyfrowania i uwierzytelniania można odpowiednio skonfigurować, patrz rozdział "Rozszerzone środki bezpieczeństwa"> ...> "Tworzenie plików konfiguracyjnych".

7.1.5.2 Internetowy protokół wymiany kluczy (IKE)

Protokół IKE odpowiada za wymianę parametrów połączenia, potrzebnych do utworzenia bezpiecznego kanału komunikacyjnego między punktami końcowymi IPsec. Między innymi wymieniane są następujące parametry:

Rodzaj zabezpieczanej transmisji
- algorytm szyfrowania
- klucze kryptograficzne
- czas trwania ważności kluczy kryptograficznych

Ta dokumentacja uwzględnia jedynie IKEv2 w scenariuszach testowych (patrz rozdział "VPN typu host-to-host" i rozdział "VPN typu site-to-site").

7.1.5.3 Security Policy Database (SPD)

Baza SPD definiuje reguły (zasady bezpieczeństwa), które określają obsługę przychodzących i wychodzących pakietów danych. Istnieją trzy podstawowe funkcje:

- pakiet jest natychmiast odrzucany (DISCARD).
- pakiet jest przesyłany bez zmian (BYPASS).
- pakiet jest przetwarzany przez IPsec (PROTECT).

Obsługa pakietów danych odbywa się za pośrednictwem określonych kryteriów wyboru (selektorów), które są wymienione w pliku konfiguracyjnym "ipsec.conf". Są to na przykład:

- źródłowy lub docelowy adres IP
- protokół Transport-Layer: TCP/UDP
- nazwa tożsamości certyfikatu

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

Aby punkty końcowe IPsec mogły zgodnie z polityką bezpieczeństwa przetwarzać kryptograficznie zabezpieczone pakiety sieciowe, (odszyfrowywanie/sprawdzanie integralności), należy dostarczyć niezbędnych informacji lub parametrów. Te niezbędne informacje są udostępniane w bazie danych odpowiednim punktom końcowym IPsec w celu zminimalizowania dodatkowego obciążenia danych na pakiet sieciowy.

Jednoznaczne przyporządkowanie do parametrów kryptograficznych i algorytmów, które mają być stosowane, odbywa się w bazie danych, z pomocą:

- "Security Parameter Index“ (SPI), wskaźnika, który jest dodatkowo przesyłany dla każdego pakietu IPsec
- docelowego adresu IP transmisji, oraz
- stosowanego protokołu bezpieczeństwa (ESP / AH).

To przyporządkowanie określane jest jako uzgodnienie dotyczące bezpiecznego połączenia („Security Association“, SA). Kontroluje ono komunikację między punktami końcowymi IPsec.

Ponieważ punkty końcowe IPsec mogą być zarówno odbiornikami jak i nadajnikami, dla każdego punktu końcowego IPsec konieczny jest jeden SA na każdy kierunek komunikacji. Zarządzanie wynegocjowanymi SA odbywa się w „Security Association Database“ (SAD), w której wymienione są wszystkie SA. Negocjacje SA odbywają się za pośrednictwem "Internet Key Exchange Protocol" (IKE).

W celu weryfikacji autentyczności punktów końcowych IPsec, podczas ustanawiania SA dostępne są następujące metody uwierzytelniania:

- PSK – Pre Shared Keys
- certyfikat X.509

Podczas identyfikacji partnera komunikacyjnego VPN za pomocą certyfikatu konieczne są dodatkowe informacje w formie "identyfikatora". Identyfikator może mieć postać np. adresu IP, nazwy DNS (FQDN) lub adresu e-mail (FQUN).

Wskazówka

Uruchom Identyfikator na stronie strongSwan w „Subject Alternative Name“ i/lub w Common Name (CN)!
Zaleca się podanie identyfikatora certyfikatu (np. nazwy DNS lub adresu IP) w polu „Subject Alternative Name“. Więcej informacji na temat certyfikatów na stronie strongSwan:
https://wiki.strongswan.org/projects/strongswan/wiki/SimpleCA!

Aby nawiązać udane połączenie za pośrednictwem protokołu IPSec, uczestnicy muszą mieć następujące informacje:

- adres IP partnera komunikacyjnego
- maska podsieci
- nazwa tunelu
- sposób uwierzytelniania
- używana metoda szyfrowania i uwierzytelniania
- klucz procedur kryptograficznych

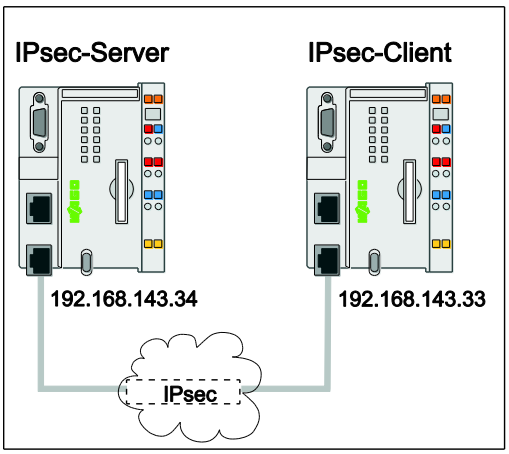
7.1.5.5 Tworzenie plików konfiguracyjnych

Poniżej opisano dwa pliki konfiguracyjne dla połączenia typu host-to-host oraz połączenia site-to-site. Przykładowe konfiguracje można skopiować 1:1 i wykorzystać do swojej konfiguracji VPN. Należy dostosować tylko określone wartości użytkownika. Możliwe jest wyraźne określenie metod ESP lub AH w plikach konfiguracyjnych.

Wskazówka

Obsługiwane pakiety algorytmów szyfrowania (Cipher-Suites) dla aplikacji IPsec strongSwan!
Przegląd obsługiwanych zestawów szyfrów (Cipher-Suites) dla aplikacji IPSsec strongSwan można znaleźć pod następującym linkiem: https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites”.

7.1.5.5.1 VPN typu host-to-host



Rys. 67: Połączenie typu host-to-host, IPsec

W poniższej przykładowej konfiguracji zakłada się, że serwer IPsec jest dostępny pod adresem IP 192.168.143.34, a klient IPsec pod adresem IP 192.168.143.33. Zmieniaj te wartości w zależności od okoliczności!

Oprócz pliku konfiguracyjnego "ipsec.conf" należy utworzyć plik "ipsec.secrets", w którym wymieniony jest klucz tajny uwierzytelniania. Oba pliki można znaleźć w przykładowych konfiguracjach poniżej. W przypadku uwierzytelniania opartego na certyfikatach, na liście znajduje się "Private Key". Procedura PSK zawiera listę wspólnych kluczy "Shared Secret".

Tryb transportowy z certyfikatami X.509

Konfiguracja dla klienta IPsec

```
# /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
```

Konfiguracja dla serwera IPsec

```
# /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
```

Wskazówka

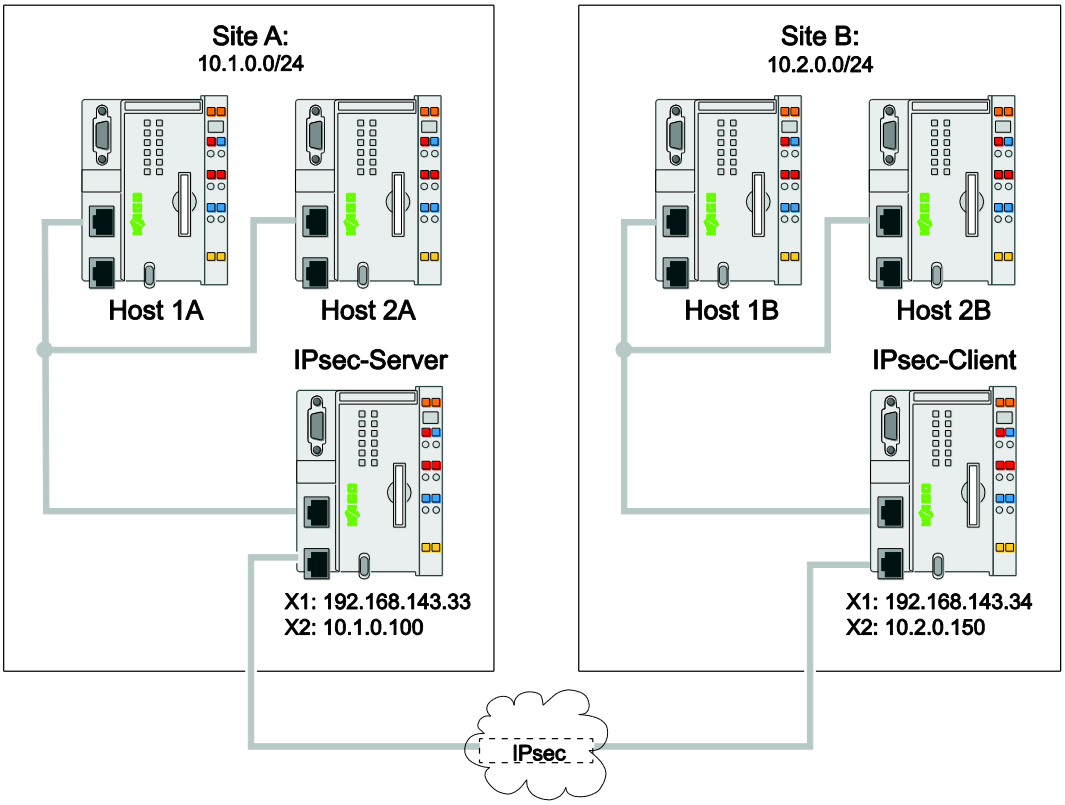
Zwróć uwagę na informacje o parametrach konfiguracyjnych!
Opis poszczególnych parametrów konfiguracyjnych można znaleźć na stronie głównej strongSwan:
https://wiki.strongswan.org/projects/strongswan/wiki/IpsecConf!

Tryb tunelowy z certyfikatami X.509

Wskazówka

W trybie tunelowym wymagane są tylko minimalne zmiany!
W trybie tunelowym należy przypisać wartość "tunnel" do parametru "type" w pliku konfiguracyjnym "ipsec.conf". Alternatywnie można usunąć parametr "typ", ponieważ domyślnym trybem jest wartość "tunnel".

7.1.5.5.2 VPN typu site-to-site



Rys. 68: VPN typu site-to-site, IPsec

VPN typu site-to-site oznacza, że można uzyskać dostęp do systemów znajdujących się za partnerem połączenia (klientem IPsec lub klientem IPsec). W przypadku VPN typu site-to-site można użyć poniższej, przykładowej konfiguracji i dostosować Twoje specyficzne wartości. Plik "ipsec.secret" można pobrać z poprzedniego przykładu.

Konfiguracja dla klienta IPsec

```
# /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
```

Konfiguracja dla serwera IPsec

```
 # /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
```

Wskazówka

Zwróć uwagę na informacje o parametrach konfiguracyjnych!
Opis poszczególnych parametrów konfiguracyjnych można znaleźć na stronie głównej strongSwan:
https://wiki.strongswan.org/projects/strongswan/wiki/IpsecConf!

Dostęp klienta (witryna A) do sieci za klientem IPsec (witryna B)

1. Aktywuj "IP Forwarding" na serwerze IPsec i na kliencie IPsec, aby umożliwić dostęp do sieci za nimi. Patrz rozdział "Dodatkowe środki bezpieczeństwa"> ...> "Aktywuj IP Forwarding".

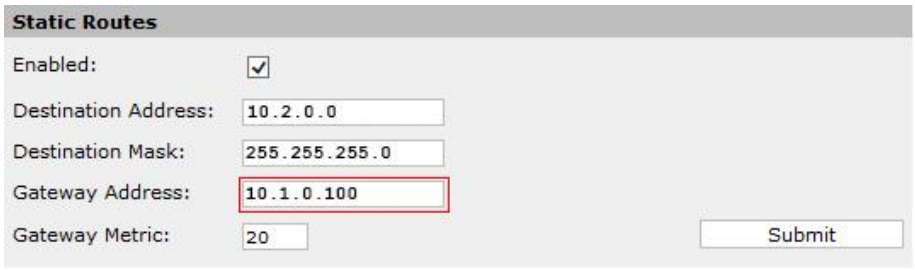
Ponadto trasa musi zostać utworzona w systemach w sieci za serwerem IPsec, aby pakiety dla klientów sieciowych (witryna A) były przekazywane do serwera IPsec. Serwer IPsec przekazuje następnie pakiety do odpowiedniego klienta IPsec.

Można dodać trasę przez WBM:

2. Wybierz w WBM punkt menu **Networking** > **Routing**.

3. Wprowadź adres IP swojego serwera w obszarze „Static Routes“, w polu **Gateway Address.**

4. Zapisz ustawienie za pomocą przycisku **[Submit]**.



Rys. 69: Static Routes, Dostęp klienta do sieci za klientem IPsec

Dostęp klienta (witryna B) do sieci za serwerem IPsec (witryna A)

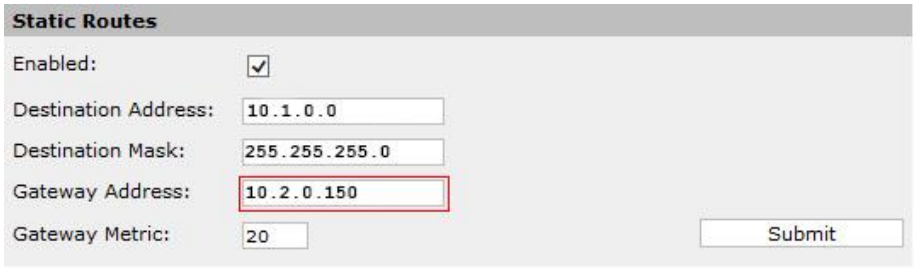
W systemach w sieci za klientem IPsec należy utworzyć trasę, aby pakiety mogły być przekazywane do klienta IPsec wyższego rzędu. Kient IPsec następnie przekazuje pakiety jako routery do serwera IPsec.

Można dodać trasę przez WBM:

5. Wybierz w WBM punkt menu **Networking** > **Routing**.

6. Wprowadź adres IP swojego serwera w obszarze „Static Routes“, w polu **Gateway Address.**

7. Zapisz ustawienie za pomocą przycisku **[Submit]**.



Rys. 70: Static Routes, Klient IPsec przekazuje pakiety jako routery do serwera IPsec.

7.1.5.6 Konfiguracja firewalla

Wskazówka

Protokół IPsec musi być jawnie włączony w firewallu dla X1 i X2!
Należy utworzyć reguły wyjątków dla połączenia IPsec do obu partnerów komunikacyjnych IPsec, ponieważ firewall nie udostępnia automatycznie IPsec VPN przez interfejs X1 lub X2. Istnieją jedynie predefiniowane reguły wyjątków IPsec dla interfejsu modemu (wwan)!

Dodawanie reguł wyjątków IPsec dla interfejsu X1 następuje według następujących kroków (analogicznie dla interfejsu X2):

1. Połącz się z konsolą Linux® sterownika przez SSH lub port szeregowy.

2. Edytuj plik „params.xml“ pod ścieżką /etc/firewall/, np. używając aplikacji Linux® „nano“:

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

Poniższy rysunek przedstawia zmodyfikowany plik "params.xml", który jest wymagany do nawiązania połączenia IPsec za pośrednictwem interfejsu X1:

```
<?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>
```

Opis parametru „ipsec_srv="yes“

Dodatkowy parametr "ipsec_srv =" yes "" przy ponownym uruchomieniu firewalla automatycznie dodaje następującą obsługę trwałych wyjątków dla interfejsu X1 (br0):

- Aktywacja portu 500/UDP (IKE) i 4500/UDP (NAT)
- Aktywacja protokołu bezpieczeństwa IPsec ESP

Możesz wyświetlić te reguły za pomocą polecenia Linux® "iptables-save":

```
…
-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
…
```

Opis znacznika XML „<interface name="VPN" rname="br0" ethernet="no" ipsec="yes"/>“

Dodatkowy znacznik XML "<interface name =" VPN "rname =" br0 "ethernet =" nie "ipsec =" tak "/>" po ponownym uruchomieniu firewalla dodaje reguły wyjątków firewalla dla usług, które można uzyskać poprzez tunel IPsec. Odnosi się to wyłącznie do usług, do których można dotrzeć za pośrednictwem interfejsu X1 (br0) w tunelu IPsec, a nie do usług, do których można uzyskać dostęp poza tunelem. Te usługi to np.:

- FTP/FTPS
- SSH
- HTTPS

Te reguły wykluczeń można wyświetlić za pomocą polecenia Linux® "iptables-save": na przykład dla usługi HTTPS mają następującą formę:

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

Należy również zwrócić uwagę na wskazówki dotyczące konfiguracji firewalla do sterownika, patrz rozdział "Uodpornianie"> "Konfigurowanie firewalla".

Wskazówka

Zapamiętaj ustawienia firewalla w scenariuszu VPN typu site-to-site!
W scenariuszu VPN typu site-to-site i przy aktywowanym firewallu można uzyskać wszystkie aktywne usługi systemów klienta niższego rzędu za pośrednictwem aktywnych portów 500 lub 4500, o ile tunel został pomyślnie utworzony.

Należy wdrożyć dodatkowe środki zapobiegające dostępowi do wrażliwych systemów klienta. To może być np. dodatkowa konfiguracja firewalla (patrz rozdział "Uodpornianie"> ...> "Tworzenie białej listy dla sieci") lub odseparowanie sieci. Więcej informacji można znaleźć w białej księdze "Bezpieczeństwo IT w zakładach produkcyjnych", którą można uzyskać w obszarze pobierania na stronie https://www.wago.com.

7.1.5.7 Przeniesienie konfiguracji do sterownika

Sterownik jest skonfigurowany po wykonaniu następujących czynności:

- usługa IPsec jest skonfigurowana na sterowniku
- wygenerowane zostały certyfikaty
- utworzone są pliki konfiguracyjne IPsec (ipsec.conf und ipsec.secret)

1. Otwórz WBM i zaloguj się jako administrator ("admin").
2. Przejdź do menu **OpenVPN/IPsec.**
3. W obszarze „IPsec“ wybierz pliki konfiguracyjne, które chcesz przesłać do urządzenia.

Rys. 71: WBM, wybór plików konfiguracyjnych dla IPsec

4. W obszarze "Certificate upload" w polu **New Certificate** wybierz odpowiednie certyfikaty. (Główny certyfikat CA i certyfikat dla klienta lub serwera).
5. W polu **New Private Key** wybierz swój klucz prywatny.

Rys. 72: WBM, wybór certyfikatu

Wskazówka

Miejsca przechowywania certyfikatów i kluczy!
Certyfikaty są po utworzeniu przechowywane w folderze /etc/certificates/.
Klucz prywatny znajduje się w folderze /etc/certificates/keys/.

6. W obszarze "IPsec" aktywuj pole **IPsec enabled**, aby usługa IPsec była dostępna po ponownym uruchomieniu.

Rys. 73: Aktywacja usługi IPsec

7. Potwierdź zmiany przyciskiem **[Submit]**.

8. Przejdź do menu **Administrator** > **Reboot**.

9. Naciśnij przycisk **[Reboot]**.

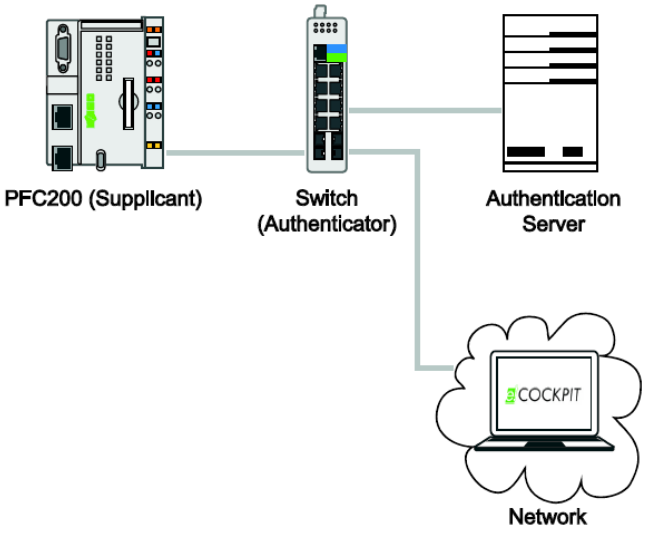
Następnie sterownik uruchomi się ponownie i uruchomi się aplikacja IPsec.

7.2 Uwierzytelnianie portów zgodnie z IEEE 802.1X

Sterowniki PFCX00 obsługują m.in. mechanizm, który pozwala na używanie sterowników jako suplikantów do uwierzytelniania portów zgodnie z IEEE 802.1X.

Ta funkcjonalność jest zapewniona przez aplikację Linux® "wpa_supplicant". Istnieją dwie metody uwierzytelnienia suplikanta:

- **Uwierzytelnianie portów według nazwy użytkownika i hasła**
  Uwierzytelnienie odbywa się poprzez podanie danych logowania w postaci nazwy użytkownika i hasła, które muszą zostać określone w pliku konfiguracyjnym (patrz następny rozdział). Ta procedura jest realizowana za pomocą protokołu uwierzytelniania EAP-MD5.
- **Uwierzytelnianie portów za pomocą certyfikatu**
  Alternatywnie suplikant może zdeponować "certyfikat klienta", który jest używany do uwierzytelniania. Ta procedura jest realizowana za pomocą rozszerzalnego protokołu uwierzytelniania EAP-TLS.



Rys. 74: Podstawowa zasada uwierzytelniania portu

Architektura sieci pokazana na rysunku "Podstawowa zasada uwierzytelniania portu" ilustruje podstawowe uwierzytelnianie portu zgodnie z IEEE 802.1X:

Sterownik (Supplikant) jest podłączony do switcha (Authentikator); W switchu należy aktywować uwierzytelnianie portu.

Zarówno serwer uwierzytelniający (np. Serwer RADIUS), jak i sieć, z której sterownik ma być konfigurowany za pomocą aplikacji ***e!****Cockpit,* są połączone za pomocą switcha.

Wskazówka

Bez uwierzytelnienia nie jest możliwa komunikacja z siecią!
Jeśli sterownik nie uwierzytelnił się na serwerze uwierzytelniania, nie można połączyć się z nim przez sieć. Sterownik nie ma także możliwości dotarcia do uczestników sieci!

Uwierzytelnianie następuje przez switch, który przekazuje żądanie nieuwierzytelnionego sterownika do serwera uwierzytelniania. Jeśli uwierzytelnianie na serwerze uwierzytelniania zakończyło się powodzeniem, switch umożliwia sterownikowi dostęp do sieci; w przeciwnym razie następuje odmowa dostępu.

Switch wymienia dane uwierzytelniające ze sterownikiem poprzez protokół Extensible Authentication Protocol przez LAN (EAPOL). W przypadku serwera RADIUS, dane uwierzytelniające między przełącznikiem a serwerem uwierzytelniającym są wymieniane w pakietach EAP, kapsułowanych w pakietach RADIUS.

Wskazówka

Protokół RADIUS musi być obsługiwany przez switch!
Komunikacja pomiędzy switchem a serwerem uwierzytelniającym odbywa się za pośrednictwem określonego protokołu uwierzytelniania, takiego jak: B. RADIUS. Switch przekształca pakiety EAP suplikanta w protokół RADIUS lub pakiety RADIUS z serwera uwierzytelniania w protokół EAP. Pod warunkiem, że switch obsługuje ten protokół.

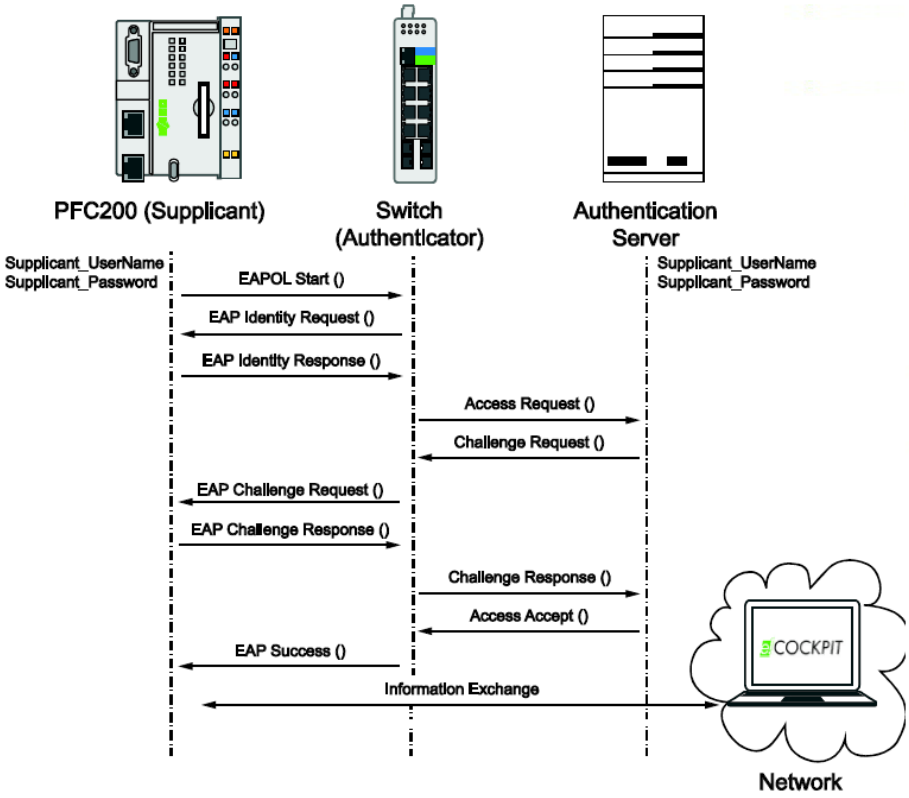
7.2.1 Uwierzytelnianie portów przy pomocy nazwy użytkownika i hasła zgodnie z EAP-MD5

Rdzeniem tej metody jest protokół uwierzytelniania Challenge Handshake (CHAP) w połączeniu z algorytmem mieszającym MD5.

Suplikant najpierw ustanawia połączenie EAPOL ze switchem. Po nawiązaniu połączenia, serwer uwierzytelnienia wysyła do suplikanta „Challenge Request“ (wartość losowa). Suplikant następnie tworzy wartość skrótu MD5 za pomocą parametrów wejściowych "Challenge" (losowa wartość serwera uwierzytelniania) i "Passwort" suplikanta. Obliczona wartość skrótu jest zwracana przez suplikanta do serwera uwierzytelniania jako „Challenge Response“.

Ponieważ serwer uwierzytelniający zna zarówno hasło suplikanta, jak i wysłane zapytanie, serwer generuje również wartość mieszania MD5 (MD5-Hash) z obu parametrów wejściowych i porównuje wygenerowaną wartość skrótu z wartością suplikanta. Jeśli obie wartości są identyczne, to znaczy że suplikant pomyślnie się uwierzytelnił.

Poniższy rysunek ilustruje zasadę uwierzytelniania portów:



Rys. 75: Przebieg uwierzytelnienia portów zgodnie z EAP-MD5

1. Kiedy tylko aplikacja "wpa_supplikant" zostanie wykonana na sterowniku, przesyła on do switcha inicjujący komunikat "EAPOL Start".
2. Switch wysyła następnie do sterownika żądanie „EAP Identity Request“, wzywając go do identyfikacji.

3. Następnie sterownik wysyła swoją tożsamość ("Supplicant_userName") do wystawcy uwierzytelnienia (Authentikator), która jest przekazywana do serwera uwierzytelniania.
4. Serwer uwierzytelniania sprawdza tożsamość, porównując ją z bazą danych użytkowników.
5. Jeśli tożsamość jest znana, serwer uwierzytelniający wysyła do sterownika losową liczbę "Challenge-Request", która jest wymagana do uwierzytelnienia.
6. Po otrzymaniu komunikatu "Challenge-Request", sterownik przesyła swoje dane uwierzytelniające z powrotem do serwera uwierzytelniania jako "Challenge Response" (wartość mieszania MD5 na podstawie losowej liczby serwera i hasła suplikanta).
7. Komunikat „Challenge Response“ jest następnie sprawdzany przez serwer uwierzytelniania.
8. Jeśli mechanizm Challenge-Response powiódł się, serwer uwierzytelniania wysyła do sterownika komunikat "Access Accept".
9. Switch zapewnia w ten sposób dostęp do sieci, a subskrybent potwierdza pomyślne uwierzytelnienie.
10. Sterownik może teraz uzyskać dostęp do sieci lub dotrzeć do uczestników sieci.

7.2.1.1 Konfiguracja uwierzytelnienia portu EAP-MD5

1. Edytuj plik konfiguracyjny /etc/wpa_supplicant.conf sterownika w następujący sposób:

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

2. Skonfiguruj switch i serwer uwierzytelniania (na przykład serwer RADIUS).
3. Uruchom lub przetestuj uwierzytelnianie EAP-TLS na sterowniku za pomocą następującego polecenia:

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

Tabela 11: Opis parametrów

Parametr	Znaczenie
-dd	tryb debugowania
-D	sterownik, którego należy użyć (wired: przewodowy)
-i	interfejs urządzeń (br0: interfejs ETHERNET X1; br1: interfejs ETHERNET X2)
-c	ścieżka do pliku konfiguracyjnego suplikanta WPA (wpa_supplicant.conf)

Dalsze informacje dotyczące parametrów/konfiguracji patrz:
https://linux.die.net/man/8/wpa_supplicant

Informacja

Uwierzytelnianie portów za pomocą certyfikatu jest bezpieczniejsze!
Jeśli to możliwe, użyj uwierzytelniania opartego na certyfikatach (EAP-TLS), ponieważ zapewnia to zarówno uwierzytelnienie klienta i serwera, jak i integralność komunikacji za pomocą najnowocześniejszych procedur kryptograficznych:

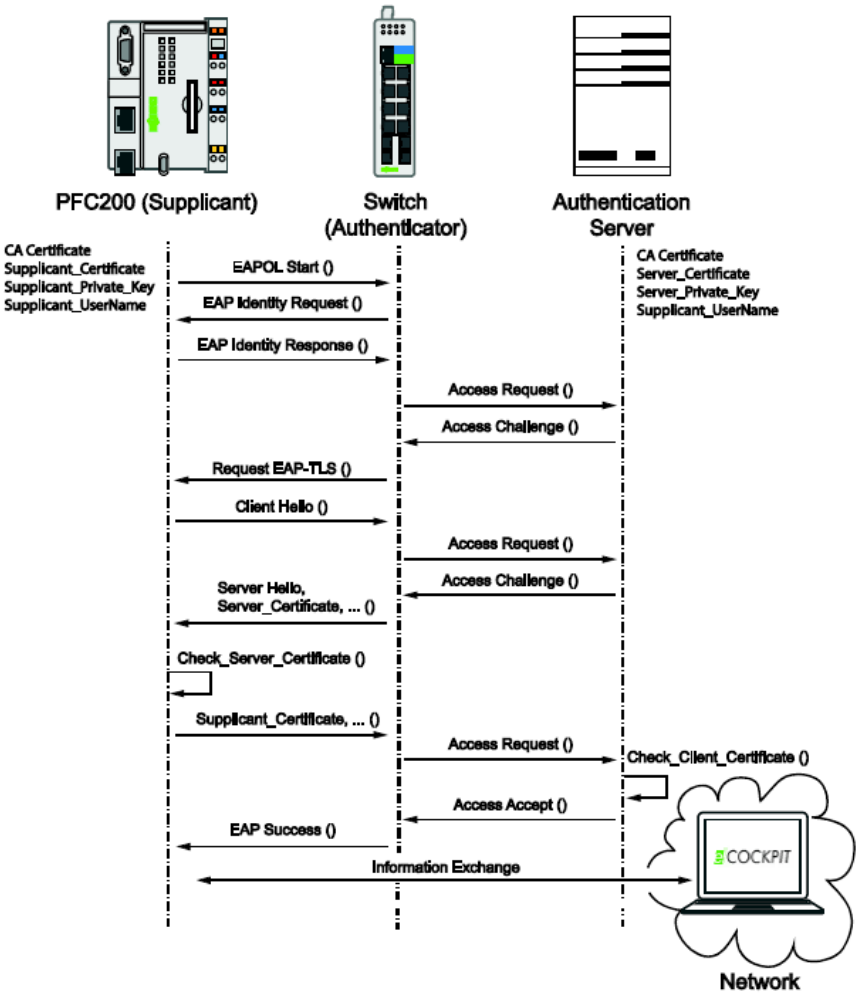
- dwustronne uwierzytelnianie
- negocjacja metod szyfrowania, zabezpieczająca integralność
- bezpieczna wymiana kluczy między dwoma punktami końcowymi

7.2.2 Uwierzytelnianie portów przy użyciu certyfikatów (EAP-TLS)

W przypadku uwierzytelniania portu opartego na certyfikacie przy użyciu protokołu EAP-TLS, zarówno serwer uwierzytelniania, jak i suplikant wymagają ważnego, zaufanego certyfikatu cyfrowego (X.509) od urzędu certyfikacji (CA). Wymaga to "Public Key Infrastructure" (PKI). Certyfikat CA stanowi "kotwicę zaufania" w procesie uwierzytelniania, dzięki czemu można zagwarantować wiarygodność (autentyczność) uczestników komunikacji. Urząd certyfikacji (CA) wydał certyfikaty cyfrowe dla suplikanta, a serwer uwierzytelniania jest używany do wzajemnego uwierzytelniania. Komunikacja jest zabezpieczona przez ustanowiony protokół TLS. Dostęp do sieci jest przyznawany, jeśli zarówno serwer, jak i suplikant wzajemnie się uwierzytelniają. Określenie hasła, podobnie jak w przypadku procedury EAP-MD5, nie jest już konieczne w tym przypadku (patrz rozdział "Uwierzytelnianie portów przy pomocy nazwy użytkownika i hasła zgodnie z EAP-MD5")

Wskazówka

Najpierw należy utworzyć certyfikaty i klucze!
Najpierw należy utworzyć certyfikaty i klucze dla PFC oraz serwer uwierzytelniania. Informacje na temat tworzenia i konfigurowania certyfikatów można znaleźć w rozdziale "Tworzenie i wymiana certyfikatów".



Rys. 76: Uwierzytelnianie portów zgodnie z certyfikatem IEEE 802.1X

1. Kiedy tylko aplikacja "wpa_supplikant" zostanie wykonana na sterowniku, proszony jest on o identyfikację i wysyła swoją tożsamość (supplicant_userName) do serwera uwierzytelniającego.
2. Serwer uwierzytelniania sprawdza, czy tożsamość istnieje w bazie danych tożsamości.
3. Jeśli tożsamość istnieje, do sterownika wysyłany jest komunikat "Request EAP-TLS", żądający od sterownika przeprowadzenia uzgodnienia TLS.
4. Sterownik rozpoczyna uzgadnianie TLS z komunikatem "Client Hello", który zawiera między innymi obsługiwane pakiety szyfrów.
5. Serwer uwierzytelniania odpowiada następnie komunikatem "Server Hello" i wysyła swój certyfikat serwera do sterownika.
6. Po otrzymaniu certyfikatu serwera, certyfikat CA sprawdza czy certyfikat jest zaufany i ważny.
7. Jeśli sterownik ufa certyfikatowi serwera, a ważność została zweryfikowana, sterownik wysyła swój certyfikat do serwera uwierzytelniania.
8. Certyfikat sterownika jest obsługiwany analogicznie do kroku 6.
9. Jeśli serwer uwierzytelniania ufa certyfikatowi sterownika, a certyfikat jest aktualny, sterownik uzyskuje dostęp do sieci za pomocą komunikatu "Access Accept" lub "EAP-Success".

Wskazówka

Brak dostępu do sieci w przypadku nieudanego uwierzytelnienia!
Jeśli uwierzytelnienie nie powiedzie się, to znaczy że serwer i sterownik nie mają certyfikatu, lub istniejący certyfikat został przez partnera komunikacyjnego odrzucony. W takiej sytuacji nie ma dostępu do sieci!

7.2.2.1 Konfiguracja uwierzytelnienia portu EAP-TLS

1. Utwórz certyfikaty i klucze do uwierzytelniania portów, patrz rozdział "Uodpornianie" > ...> Tworzenie i wymiana certyfikatów".
2. Edytuj plik konfiguracyjny /etc/wpa_supplicant.conf sterownika w następujący sposób:

```
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. Skonfiguruj switch i serwer uwierzytelniania (na przykład serwer RADIUS).
4. Uruchom lub przetestuj uwierzytelnianie EAP-TLS na sterowniku za pomocą następującego polecenia:

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

Tabela 12: Opis parametrów

Parametr	Znaczenie
-dd	tryb debugowania
-D	sterownik, którego należy użyć (wired: przewodowy)
-i	interfejs urządzeń (br0: interfejs ETHERNET X1; br1: interfejs ETHERNET X2)
-c	ścieżka do pliku konfiguracyjnego suplikanta WPA (wpa_supplicant.conf)

Dalsze informacje dotyczące parametrów/konfiguracji patrz:
https://linux.die.net/man/8/wpa_supplicant

7.2.3 Automatyczne uwierzytelnienie portu podczas procesu rozruchu

Aby uniknąć konieczności ręcznego uruchamiania aplikacji "wpa_supplicant" (patrz rozdział "Uwierzytelnianie portów przy pomocy nazwy użytkownika i hasła zgodnie z EAP-MD5"), możesz utworzyć skrypt startowy. Przykładowy skrypt startowy na poniższym rysunku pozwala automatycznie wykonać uwierzytelnianie portu podczas uruchamiania sterownika. Warunkiem wstępnym jest utworzenie odpowiedniej konfiguracji w pliku konfiguracyjnym "/etc/wpa_supplicant.conf" (patrz np. rozdział "Konfigurowanie uwierzytelnienia portu EAP-MD5"). Po uruchomieniu skryptu, aplikacja "wpa_supplicant" działa jako proces w tle.

Konfigurowanie skryptu uruchamiania wymaga następujących kroków:

1. Utwórz plik "wpa_supplicant" z następującą treścią:

```
#!/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. Przenieś plik wpa_supplicant do folderu /etc/init.d/ sterownika.

3. Połącz się z konsolą Linux® (na przykład przez SSH lub konsolę szeregową).

4. Utwórz symboliczny link, aby uruchomić skrypt podczas procesu rozruchu. Komenda Linux®:

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

Po ponownym uruchomieniu, aplikacja "wpa_supplicant" jest uruchamiana jako proces w tle i próbuje uwierzytelnić się za pomocą partnera komunikacyjnego (np. serwera uwierzytelniania)

Wskazówka

Zwróć uwagę na specyfikację interfejsu!
W przykładowym pliku "wpa_supplicant" uwierzytelnianie odbywa się poprzez interfejs X1 (br0). Dopasuj zmienną interfejsu "WPA_IF" w skrypcie startowym zgodnie z jej konfiguracją!

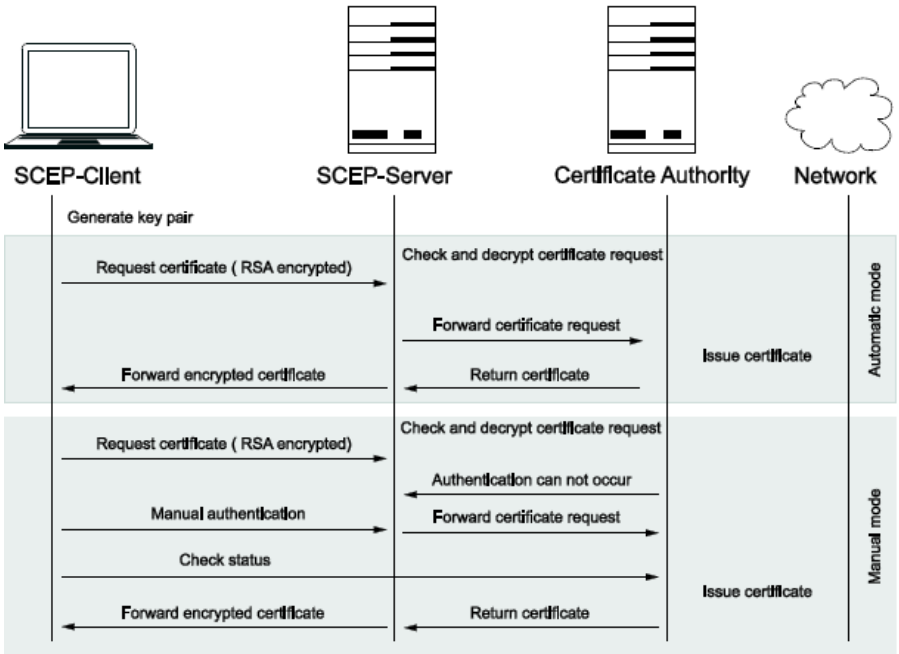
7.3 Simple Certificate Enrollement Protocol (SCEP)

Dzięki opartemu na HTTP "Simple Certificate Enrollment Protokoll" (SCEP) możliwa jest centralna dystrybucja i zarządzanie certyfikatami urządzeń na dowolnej liczbie sterowników w sieci. Dostarczanie certyfikatów i zarządzanie nimi jest obsługiwane przez serwer SCEP. Odpowiednie urządzenie (sterownik) automatycznie generuje parę kluczy RSA i żąda certyfikatu. Serwer SCEP weryfikuje żądanie i generuje sygnowany certyfikat X.509, który można następnie pobrać za pośrednictwem protokołu SCEP i zainstalować lokalnie, jak pokazano na rysunku "Simple Certificate Enrollement Protocol" (SCEP). Rozróżnia się tryb ręczny i automatyczny. Oba tryby opisano w kolejnych rozdziałach.

Aby zapewnić integralność i poufność, przesyłane dane są pakowane w formaty PKCS # 7.

Wskazówka

Najpierw skonfiguruj niezbędną infrastrukturę!
Aby tworzyć i wdrażać certyfikaty przy użyciu protokołu SCEP, potrzebna jest odpowiednia infrastruktura. Serwer można zrealizować np. jako serwerCA Windows 2003 z zainstalowaną specjalną wtyczką (mscep.dll).



Rys. 77: Simple Certificate Enrollement Protocol (SCEP)

7.3.1 Automatyczne przetwarzanie żądania

W przypadku automatycznego przetwarzania, należy zapewnić autentyczność wnioskodawcy za pomocą ankiety bezpieczeństwa. Jeśli parametry bezpieczeństwa w żądaniu certyfikatu są zgodne z bieżącą wartością na serwerze, certyfikat urządzenia może zostać automatycznie wygenerowany.

1. Klient generuje parę kluczy RSA. Publiczna część tej pary kluczy zostanie później wysłana na serwer wraz z żądaniem. Prywatna część pary kluczy pozostaje u klienta.
2. Klient wysyła do serwera publiczną część wygenerowanej pary kluczy (Public key) wraz ze szczegółami jego tożsamości (nazwa, adres e-mail itp.) jako żądanie certyfikatu. To żądanie jest sygnowane prywatną częścią pary kluczy.
3. Serwer sprawdza żądanie certyfikatu i wydaje certyfikat urządzenia bez dalszej interakcji, jeśli dane są wystarczające do uwierzytelnienia
4. Certyfikat urządzenia jest przekazywany do klienta i np. udostępniany do operacji VPN.

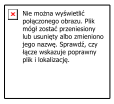
7.3.2 Ręczne przetwarzania żądania

Serwer przechodzi do "trybu ręcznego", jeśli potrzebuje więcej informacji, aby uwierzytelnić wnioskodawcę. Oznacza to, że serwer nadaje żądaniu certyfikatu status oczekiwania, do czasu zatwierdzenia lub odrzucenia urzędu certyfikacji. W trybie ręcznym certyfikat nie jest dostarczany bezpośrednio. Zamiast tego, klient może stale sprawdzać, czy nastąpiło uwierzytelnienie. Po wykonaniu tej czynności klient otrzymuje certyfikat na żądanie.

1. Klient generuje parę kluczy RSA.
2. Klient wysyła do serwera publiczną część wygenerowanej pary kluczy (Public key) wraz ze szczegółami jego tożsamości (nazwa, adres e-mail itp.) jako żądanie certyfikatu. To żądanie jest sygnowane prywatną częścią pary kluczy.
3. Serwer sprawdza żądanie certyfikatu i nadaje mu status oczekiwania, jeśli uwierzytelnienie nie może zostać wykonane.
4. Klient jest informowany, że uwierzytelnienie nie może nastąpić.
5. Istnieje ręczne uwierzytelnianie, np. przez telefon.
6. Klient przez cykliczne zapytania stwierdza, czy może pobrać certyfikat.
7. Serwer sprawdza żądanie certyfikatu i wydaje certyfikat urządzenia bez dalszej interakcji, jeśli dane są wystarczające do uwierzytelnienia
8. Certyfikat urządzenia jest pobierany przez klienta i np. udostępniany do operacji VPN.

7.3.2.1 Konfiguracja procesu SCEP

UWAGA



Synchronizacja czasu na sterowniku!
Aby sprawdzić certyfikat za pomocą protokołu SCEP, należy zsynchronizować datę i godzinę wszystkich sterowników. Najłatwiej to zrobić poprzez Network Time Protocol (NTP).

Możesz najpierw użyć następującego polecenia, aby wyświetlić listę dostępnych parametrów klienta SCEP:

```
ipsec scepclient --help
```

1. Utwórz 2048 parę kluczy RSA zgodnie ze standardem PKCS1, patrz rozdział "Uodpornianie" > ...> "Generowanie kluczy prywatnych".

Wskazówka

Wyeksportuj parę kluczy i prześlij ją na swoje urządzenie!
Utwórz i wyeksportuj parę kluczy RSA z oprogramowania zarządzającego kluczami XCA. Wybierz format eksportu ".der". Para kluczy może być następnie załadowana do sterownika za pośrednictwem WBM: **OpenVPN/IPsec > Certificate Upload > New Private Key.** Klucz prywatny znajduje się w folderze /etc/certificates/keys/.

2. Pobierz certyfikaty CA dla szyfrowania PKCS7 (żądanie) i weryfikacji sygnatury PKCS7 (odpowiedź):

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

Następnie, w zależności od konfiguracji infrastruktury pobierane są certyfikaty CA, które służą do zabezpieczenia komunikacji SCEP. W tym przypadku to certyfikaty "caCert-ra-1.der" dla szyfrowania żądania SCEP i "caCert-ra-2.der" dla weryfikacji sygnatury odpowiedzi serwera SCEP.

3. Pobierz certyfikat z urzędu certyfikacji na podstawie wygenerowanej pary kluczy RSA (początkowej) i certyfikatów CA z kroku 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
```

Wskazówka

Zauważ, że nazwy są tylko symbolami zastępczymi!
Nazwy powyższej pary kluczy (pfc200Cert.der "/" pfc200private.der), jak również parametry serwera i hasła (--url, -p) są symbolami zastępczymi i mogą być w razie potrzeby przypisane inaczej!

Po wprowadzeniu polecenia, tworzony jest samosygnowany certyfikat podpisu PKCS7. Następnie tworzone jest żądanie certyfikatu (PKCS10) za pomocą klucza PKCS1 (sygnatura). W kolejnym kroku żądanie PKCS7 jest przetwarzane przy użyciu certyfikatów CA. Ponieważ sygnatura PKCS7 jest oparta na certyfikatach z sygnaturą własną, należy dodatkowo podać hasło (-p), które jest dostarczane za pośrednictwem wywołania URL urzędu certyfikacji. W zależności

od konfiguracji urzędu certyfikacji, hasło można również pominąć. Zaufany certyfikat pfc200Cert.der jest następnie przechowywany w katalogu / etc / certificates.

Jeśli ponowne żądanie certyfikatu zostanie złożone po wygaśnięciu bieżącego certyfikatu, można użyć obecnie używanego zaufanego certyfikatu. Nie ma potrzeby tworzenia nowego certyfikatu z sygnaturą własną. Ponieważ ten certyfikat jest certyfikatem zaufanym, wpisywanie hasła (-p) jest pomijane. Po określeniu parametru "-in cert-self = pfc200Cert.der" używany jest tylko bieżący certyfikat "pfc200Cert.der":, a nie certyfikat z sygnaturą własną.

```
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/
```

Wskazówka

Dalsze informacje o SCEP!
Więcej informacji na temat aplikacji "scepclient" można znaleźć na stronie: http://manpages.ubuntu.com/manpages/artful/man8/scepclient.8.html!

8 Załączniki

8.1 FAQ na temat IPsec

Błędne nawiązanie połączenia IPsec może mieć różne przyczyny. W tym rozdziale znajdziesz wskazówki na temat możliwych problemów, które mogą wystąpić podczas konfiguracji IPsec. Równocześnie na sterownikach PFC200/ PFC100 wyświetlane są środki do analizy błędów.

Tabela 13: Wskazówki i działania zapobiegawcze

Wskazówki	Działania zapobiegawcze
Ponieważ procedury szyfrowania i uwierzytelniania są konfigurowalne, mogą ewentualnie pojawić się problemy podczas tworzenia "Security Association" (SA) z różnymi produktami VPN. W przypadku różnych konfiguracji partnerów komunikacyjnych IPsec może wystąpić błąd. Nie można nawiązać połączenia.	Upewnij się, że partnerzy komunikacyjni IPsec używają tych samych procedur uwierzytelniania i szyfrowania. Ta konfiguracja jest dokonywana przez sterownik w pliku konfiguracyjnym "ipsec.conf", patrz rozdział "IPsec"> "Tworzenie plików konfiguracyjnych".
Podczas rutowania między sieciami w scenariuszu site-to-site, zakresy adresów podsieci, które mają być połączone, muszą być różne.	• Zdefiniuj oddzielny zakres adresów (różne podsieci) dla podpętli, które mają być połączone. • Nie przypisuj adresów IP kilkakrotnie po połączeniu sieci, w przeciwnym razie wystąpi wadliwe połączenie IPsec. • Zwróć uwagę, że aplikacja IPsec "strongSwan" po udanym założeniu automatycznie dodaje trasę do tabeli rutowania 220. Komenda Linux®: `root@PFC200-405679:~ ip route list table 220`
Protokół wymiany kluczy IKEv2 jest bardziej stabilny i przyjazny dla użytkownika niż protokół wymiany kluczy IKEv1.	Użyj protokołu wymiany klucza IKEv2 zamiast IKEv1, aby zapobiec poważnym problemom z technologią NAT, dynamicznymi adresami IP i urządzeniami mobilnymi.
Silne szyfrowanie lub zabezpieczenia kryptograficzne prowadzi do dużego zużycia zasobów. Może to prowadzić do opóźnień i anomalii w działaniu programu, przez co sterownik nie będzie mógł wykonywać swoich rzeczywistych zadań.	Należy stosować niezbyt silne szyfrowanie lub zwracać uwagę na wybór długości klucza do procedur kryptograficznych, zgodnie z wytycznymi technicznymi BSI TR-02102-4 (wersja 2017-01)!
Jeśli korzystasz z certyfikatów, ustawiony czas dla partnerów komunikacyjnych IPsec musi być taki sam. W przeciwnym razie może to prowadzić do problemów z weryfikacją certyfikatów, w wyniku czego nie będzie można nawiązać połączenia IPsec.	• Upewnij się, że ustawiony czas jest taki sam na wszystkich systemach! • Jeśli nie korzystasz z serwera czasu, możesz ręcznie zmienić godzinę lub datę za pomocą konsoli (data - ustaw "RRRR - MM - DD HH: MM") lub WBM.

Wskazówka

Więcej informacji znajdziesz bezpośrednio na stronie strongSwan!
FAQ z strongSwan można znaleźć na stronie:
https://wiki.strongswan.org/projects/strongswan/wiki/FAQ!

8.1.1 Dodatkowa analiza błędu lub statusu IPsec

- W przypadku analizy błędów IPsec oceń wpisy dziennika IPsec wymienione pod ścieżką Linux® „`/var/log/messages`".
- Możliwe jest zwiększenie poziomu rejestrowania danych logowania w pliku konfiguracyjnym "ipsec.conf" w celu uzyskania bardziej szczegółowych informacji w przypadku błędu.
  https://wiki.strongswan.org/projects/strongswan/wiki/LoggerConfiguration
- Wyświetl przychodzące i wychodzące pakiety sieciowe za pomocą następującego polecenia (np. za pośrednictwem usługi SSH):
  `tcpdump port not 22 -n -i eth0`.
- Więcej szczegółowych informacji na temat konfigurowania i testowania połączenia IPsec, patrz:
  http://wiki.strongswan.org/projects/strongswan/wiki/UserDocumentation.

Spis ilustracji

Indeks tabel

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 • 32385 Minden
Hansastraße 27 • 32423 Minden
Tel: 0571/887 – 0
Telefax: 0571/887 – 169
e-mail: wago.elwag@wago.com
Internet: http://www.wago.com