VPN Connections via DSL VPN Routers

ID Number: 26662448

Warranty, liability and support

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). However, claims arising from a breach of a condition which goes to the root of the contract shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions do not imply a change in the burden of proof to your detriment.

Copyright© 2007 Siemens A&D. It is not permissible to transfer or copy this Application or excerpts of it without first having prior authorization from Siemens A&D in writing.

For questions about this document please use the following e-mail address:
mailto:csweb@ad.siemens.de
Foreword

Applications are functional and tested automation configurations based on A&D standard products and non-Siemens products for easy, fast and inexpensive implementation of automation tasks. Each of these Applications covers a frequently occurring subtask of a typical customer problem.

The Application helps you obtain answers to the following questions: Which products are required for these subtasks? How do they function when combined? To answer these questions, a tested example application is provided.

However, depending on the plant requirements, a variety of other components (e.g., other CPUs, power supplies, etc.) can be used to implement the functionality on which this Application is based. For these components, please refer to the corresponding SIEMENS A&D catalogs.

Series of documentations on “WAN access methods”

This application is part of a series of documentations on “WAN access methods”. This series consists of:

- An application on WAN access using VPN connections (this document).
- An application on WAN access using port forwarding.
- An application describing WAN access using analog Ethernet dial in / out routers.
- An overview document providing ordering help, which are successively developed.

Reference to Automation and Drives Service & Support

This entry is from the internet application portal of Automation and Drives Service & Support. Clicking the link below directly displays the download page of this document.

Table of Contents

Table of Contents ......................................................................................................... 4
1 Fields of Application and Benefits ................................................................ 6
2 Fundamental technical Principles .................................................................. 10
  2.1 VPN ................................................................................................................ 10
  2.2 IPsec .............................................................................................................. 12
  2.3 IPsec protocol security mechanisms .............................................................. 14
      2.3.1 The key ..................................................................................................... 14
      2.3.2 The connection establishment .................................................................. 14
      2.3.3 Data exchange via IPsec .......................................................................... 16
      2.3.4 Criticism of IPsec ..................................................................................... 17
  2.4 DynDNS ......................................................................................................... 18
3 Configuration ..................................................................................................... 20
  3.1 Hardware configuration ............................................................................... 20
      3.1.1 Gateway-gateway VPN ........................................................................... 21
      3.1.2 Client-gateway VPN ............................................................................... 23
  3.2 Software requirements .................................................................................. 25
4 Required Hardware and Software Components ........................................ 26
  4.1 Gateway-gateway VPN ................................................................................ 26
  4.2 Client-gateway VPN ..................................................................................... 27
5 DynDNS Setup ................................................................................................. 29
  5.1 Setting up a DynDNS account ...................................................................... 30
  5.2 Creating a DynDNS host .............................................................................. 33
6 Gateway-Gateway VPN Router 1 ............................................................ 37
  6.1 Login to the router ....................................................................................... 38
  6.2 Basic internet access settings ...................................................................... 39
  6.3 Checking internet connection ...................................................................... 41
  6.4 Checking WAN mode .................................................................................... 42
  6.5 DynDNS parameterization ........................................................................... 43
  6.6 Settings in the local plant network ............................................................... 45
  6.7 VPN parameterization using wizard ............................................................ 46
  6.8 VPN parameterization via direct input ......................................................... 48
7 Gateway-Gateway VPN Router 2 ............................................................ 54
  7.1 VPN connections using wizard .................................................................. 55
  7.2 VPN connections via direct input ............................................................... 56
  7.3 Status information for VPN connections .................................................... 58
  7.4 Diagnostics for VPN connections ............................................................... 60
8 Client-Gateway VPN Router ....................................................................... 61
8.1 VPN connection using wizard ................................................................. 62
8.2 VPN connection via direct input ........................................................... 64

9  Client-Gateway VPN PC Client ............................................................. 68
  9.1 Opening Security Policy Editor ............................................................. 69
  9.2 Inserting a new connection ................................................................. 70
  9.3 “My Identity” ..................................................................................... 72
  9.4 Setting the security policy ................................................................. 74
  9.5 Authentication Proposal ................................................................. 75
  9.6 Key Exchange Proposal ................................................................. 76
  9.7 Activating and deactivating the VPN connection ............................. 78
  9.8 Testing the VPN connection on the client ....................................... 79

10 Necessary Hardware Preparation ....................................................... 82

11 Performance Data ........................................................................... 83
  11.1 Constraints ..................................................................................... 83
  11.2 Experiences from the application ................................................... 83
  11.3 Security features ........................................................................... 85
  11.4 Tested applications ..................................................................... 86

12 History ........................................................................................... 86
1 Fields of Application and Benefits

Automation problem

Remote access to an automation system (SIMATIC S7 or SIMOTION) is to be realized via Ethernet. The following functions are to be possible:

- PG functions (with SIMATIC S7, HMI systems, SIMOTION, etc.) with
  - diagnostic functions,
  - remote programming and
  - remote maintenance.
- Standard Ethernet communication services such as SEND / RECEIVE, FTP and HTTP accesses.

The data is to be accessed via a secure data link via the internet.

Standard hardware and software components are to be used as end points of the secure data transmission. These end points are to be used as protection and as a transition to the secure plant networks.
Automation solution

The diagrammatic approach shown in the figure below is applied:

Figure 1-1

The approach described in this application deals with two variants that ensure secure data transmission using VPN connections.

These variants are

- a gateway-to-gateway connection and
- a client-to-gateway connection respectively.

Both solutions use the IPsec protocol. This protocol ensures the highest possible transmission security between the two tunnel endpoints. Both network components (such as routers) and terminal units (with VPN client software) can be used as tunnel endpoints. Both cases will be considered in greater detail in the following sections.
Routers and VPN client products of the FVS 338 or VPN01L type by NETGEAR are used as examples. If the functionality is comparable, any other device can be used. The minimum requirements for operation are summarized in chapter 6 Gateway-Gateway VPN Router 1.

The minimum requirement for the communication interface is a digital ISDN B channel. An analog telephone line is sufficient to establish the connection, but this connection is not stable (see application describing WAN access using analog Ethernet dial in / out routers).

Fields of application

This application is particularly suitable for use with extended plant structures requiring real-time and secure transmission of a considerable data volume. An important requirement for using this application is a sufficient bandwidth of the data link to the internet provider.

The field of application of these connection types comprises the entire IP communication spectrum.

This includes

- PG functions for STEP 7 and SIMOTION SCOUT,
- process visualization (HMI),
- process data communication,
- FTP communication,
- HTML accesses and
- internet access.
Benefits

The use of this application enables customers to establish a secure data communication between plants and systems protected against data corruption and against access by third parties worldwide with reasonable technical extra work in a way that is simple and cost-effective.

The bandwidths of this communication that are possible today also allow continuous operation with considerable data volumes. Aside from the mere programming and maintenance functions, this also enables real-time monitoring from longer distances using SCADA systems.

Constraints

The usable data volume that is restricted by the uplink and downlink bandwidth is the main constraint.

The fact that the used transport medium is the internet is another constraint. Compared to local networks, the data transmission time is considerably increased. Transmission times of 50 to 100 ms are possible even if the physical distances are small. For this reason, this method is not suitable for real-time mode.
2 Fundamental technical Principles

Introduction

This chapter deals with the definition and the description of the VPN functionality. A particular focus is on the IPsec protocol on which the VPN are based.

Furthermore, the DynDNS is described that is necessary for the localization in dynamic IP networks such as the internet.

2.1 VPN

Definition

A Virtual Private Network (VPN) is a data network that is used for transporting private data through a public network (for example, the internet). It thus enables secure transmission via a non-secure network.

Nodes of a VPN can exchange data as in an internal LAN and it is not required that the individual nodes be directly connected to one another. This connection is usually encrypted and thus secure; however, this is not always the case. A VPN, also referred to as a tunnel, can also be an unsecured clear text tunnel.

VPN structure

VPN are a subgroup of the virtual networks. They are not an individual protocol but a whole collection of protocols. The figure below helps you obtain a rough overview.

Figure 2-1

As shown in the representation, VPN are divided into two categories. In addition, the overlay VPN used in the application are divided into the applicable layers of the ISO/OSI reference model.
Layer 2 VPN support the tunneling of most diverse protocols by the VPN. This method is advisable for the application with different protocols, but it is controversial. The security mechanisms used in layer 2 VPN are considered to be only partially secure.

Layer 3 VPN support the tunneling based on the Internet Protocol. The IPsec protocol used here is the basis of this application.

**Different connection types**

VPN are differentiated into three different connection types, which are partly also used in this application.

<table>
<thead>
<tr>
<th>VPN connection types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site to Site / Point to Point</td>
<td>This connection type describes the connection of two networks. VPN gateways establishing the VPN tunnel are used on both sides. These tunnels are normally permanent. This enables to connect, for example, two remote office locations.</td>
</tr>
<tr>
<td>Site to End</td>
<td>VPN are frequently used to grant mobile employees outside an office location access to the internal network and thus to the data stored in this network. In this process the computer of the employee establishes a VPN connection to the VPN gateway known to it. This enables the employee to work as if he/she was directly connected to the local network (Remote Access VPN). This method can also be used for radio links (End-to-Site-VPN).</td>
</tr>
<tr>
<td>End to End</td>
<td>This connection type enables individual computers to establish VPN connections among each other. This connection type is very rarely used and is used only when the security requirements in a local network are extremely high. This connection type is also referred to as a Host to Host VPN.</td>
</tr>
</tbody>
</table>
2.2 IPsec

Introduction
IPsec (short for Internet Protocol Security) was developed in 1998 to correct the weaknesses of the Internet Protocol (IP) in the area of security architecture. To ensure protection, IPsec offers

- confidentiality,
- authenticity and
- integrity.

These factors are to prevent, in particular, replay attacks that are a security risk to other security-oriented protocols.

Specification
Like all specifications concerning TCP/IP, IPsec is defined as RFC. RFC 2401 describes the IPsec protocol architecture. Based on this RFC, the RFC relevant to the IPsec protocol that are referenced include the ones listed in the following table:

<table>
<thead>
<tr>
<th>RFC</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3519</td>
<td>Mobile IP Transversal of Network Address Translation (NAT) Devices</td>
</tr>
<tr>
<td>RFC 3706</td>
<td>A Traffic-Based Method of Detecting Dead Internet Key Exchange Peers (IKE)</td>
</tr>
<tr>
<td>RFC 3830</td>
<td>Multimedia Internet Keying (MIKEY)</td>
</tr>
<tr>
<td>RFC 4301</td>
<td>Security Architecture for the Internet Protocol</td>
</tr>
<tr>
<td>RFC 4302</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>RFC 4303</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>RFC 4306</td>
<td>Internet Key Exchange (IKEv2) Protocol</td>
</tr>
</tbody>
</table>

Different connection types
IPsec uses several designations for the connection types, which are described in the following.

IPsec has two different modes; these modes are

- transport mode and
- tunnel mode.

The difference between the two modes is the handling of the IP headers. In transport mode, the transmission of the IP header with the source and destination information of the data packet is unencrypted. In tunnel mode, the transmission of the entire message frame is encrypted and thus encapsulated. Tunnel mode prevents a third party from reading out the
source and destination information of a data packet. Tunnel mode is the mode used for VPN tunnels on the internet.

This differentiation helps you better understand the following connection types.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Type of connection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport mode</td>
<td>Host to Host</td>
<td>The connection type known for VPN as an End to End connection between two terminal units, e.g. PCs.</td>
</tr>
<tr>
<td></td>
<td>Host to Router</td>
<td>This version of the End to End connection is normally used for diagnostic or network management purposes for network components.</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>Gateway to Gateway</td>
<td>This connection type is specified by VPN as a Site to Site connection. A secure VPN tunnel is established between two gateways. This connects two locally separated networks. In this document, this application is described with the gateway-to-gateway connection.</td>
</tr>
<tr>
<td></td>
<td>Peer to Gateway</td>
<td>The Site to End connection type known from VPN describes the connection of a terminal unit to a VPN gateway. This method is used for using VPN software clients as described in this application in the client-gateway connection section.</td>
</tr>
<tr>
<td></td>
<td>Peer to Peer</td>
<td>This version of the End to End connection between two terminal units is more common than the variant in transport mode. This variant will not be considered in detail in the following sections.</td>
</tr>
</tbody>
</table>
2.3 IPsec protocol security mechanisms

Introduction by means of a connection establishment

To represent the different security mechanisms of the IPsec protocol, a connection establishment will be used to schematically show the security features that can be selected.

2.3.1 The key

Key exchange

The decision on the exchange of the keys is made already when configuring the VPN connection. A selection between two ways is possible:

- Manual Keying
- IKE

We advise against using manual keying since this type of key can be guessed very easily; this makes the VPN connection corruptible.

IKE (Internet Key Exchange), defined in RFC 2409, forms a secure two-stage connection establishment variant. This secure connection establishment is the type used for this application.

2.3.2 The connection establishment

IKE phase model

Internet Key Exchange (IKE according to RFC 2409) is a simplified method for establishing secure, authenticated connections.

IKE differentiates between modes in which keys are exchanged. The entire IKE procedure is performed in two phases.

In the first phase, a secure authenticated connection is established.

In the second phase, the keys required for the protocols are exchanged. These different keys (encryption, hashes) are derived from a master key.

The representation below describes the two phases of the IKE phase model:
Phase 1

A secure connection between the two tunnel endpoints is established in the course of the first phase. Within RFC 2409 this is referred to as ISAKMP Security Association (SA). Two modes are possible to set up this SA.

- **Main mode**
  Three pairs of messages are transmitted, each with one request message and one response message. The first two messages negotiate the security method. The next two messages exchange the public keys of the Diffie-Hellman method and further information for the encryption. The last two messages, which have already been encrypted, authenticate the encryption data using shared secrets.

- **Aggressive mode**
  In this mode, only three messages are exchanged. The first message contains the public key of the Diffie-Hellman method, further information
for the encryption and information to identify the nodes. The response message contains the same data of the responder. In the third message, which has already been encrypted, the initiator is authenticated and the authorizations are transferred.

Considered from the transmission security level, Main mode has to be preferred to Aggressive mode. However, there is no difference in the security of the data that is transmitted later since phase 1 is the first encryption step.

Phase 2

In phase 2, the established ISAKMP SA is used to negotiate a security association based on a secure service. This is done in the form of Informational Exchanges and provides that the data is encrypted and protected against corruption by means of suitable hash algorithms.

2.3.3 Data exchange via IPsec

Data transmission and connection monitoring

In operation, the secure data exchange between two tunnel endpoints is secured in the following different ways.

Authentication Header (AH)

Authentication Header ensures the authenticity of the transmitted packets and authenticates the sender. In particular, there is a protection against replay attacks.

Encapsulating Security Payload (ESP)

Encapsulating Security Payload is to ensure the authentication, the integrity of the transmitted data and the confidentiality of IP packets.

ISAKMP Keepalive (DPD)

ISAKMP Keepalive is a continuous connection check and supports the system in maintaining the connection. If the connection was aborted, it is automatically reestablished. ISAKMP Keepalive is specified in RFC 3706.

UDP Keepalive

In the event of a longer delay in the data input, UDP Keepalive prevents the time-out automatically initiated by NAT. This prevents a port change behind an NAT router. UDP Keepalive is specified in RFC 3519.
2.3.4 Criticism of IPsec

Opinions of cryptography experts

The cryptography experts Bruce Schneider and Niels Ferguson have repeatedly evaluated the IPsec protocol and found several points of criticism. Aside from the way the actual protocol was developed, the experts criticize in particular the high complexity resulting in an increased error-proneness. However, both experts also stress that IPsec currently provides the best security for the original IP.
2.4 DynDNS

Introduction
DynDNS (Dynamic Domain Name System Entry) is an internet service that allows to set up a fixed host name as an alias for a dynamically changing IP address. It thus enables an internet node to remain available under the same domain name despite its changing IP address.

Comparison of DynDNS and fixed IP address
A comparison of the addressing variants is necessary to optimize the selection between the two options. To limit the consideration, the comparison comprises the following areas:

- Availability of the service,
- costs of the service,
- reliability and
- configuration overhead in the gateway.

The following overview ensues from these areas for the two variants:

<table>
<thead>
<tr>
<th>Considered area</th>
<th>Fixed IP address</th>
<th>DynDNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of the service</td>
<td>The service is not available in all regions of the world or via all ISP / internet accesses</td>
<td>The service is possible with every internet access, restrictions exist only for networks with NAT addressing.</td>
</tr>
<tr>
<td>Costs of the service</td>
<td>The costs for each used IP address depend on the provider (ISP).</td>
<td>Normally free, possibly subject to a small fee in the professional sector; in this case, however, additional features are offered.</td>
</tr>
<tr>
<td>Reliability in the access</td>
<td>No interruption of the connection. The reliability only depends on the connection to the internet.</td>
<td>The online connection is usually interrupted by the provider (ISP) at regular intervals (approx. 24 hours). No connection is available for the period between disconnect and reconnect.</td>
</tr>
<tr>
<td>Configuration overhead in the gateway</td>
<td>Little, the configuration is performed when setting up the internet access.</td>
<td>Depending on the used DynDNS provider, the overhead may be considerable. (As an example, see chapter 5)</td>
</tr>
</tbody>
</table>
Providers on the internet

The DynDNS service is offered by most diverse groups and organizations. Normally, the service is free for private users, but the application with extended services may be subject to a fee. The following table provides a small selection of known providers:

Table 2-5

<table>
<thead>
<tr>
<th>Provider</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>DynDNS.org</td>
<td>Provider used in this application</td>
</tr>
<tr>
<td>TZO.com</td>
<td>Provider of paid services with several</td>
</tr>
<tr>
<td></td>
<td>additional features</td>
</tr>
<tr>
<td>lego.net</td>
<td>Asian provider</td>
</tr>
</tbody>
</table>

Use in this application

In this application, the DynDNS service is necessary to locate the used gateway, the NETGEAR FVS 338 router, on the internet. Therefore, the internet accesses used in the application require no fixed IP address, as would be required for the use of the SCALANCE S modules.

The assignment of a fixed IP address is not possible in all cases, the use of DynDNS is an alternative.
3 Configuration

3.1 Hardware configuration

Overview

This application consists of two parts:

- The gateway-gateway VPN part and
- the client-gateway VPN part.

In the following sections, both parts will be considered in this order.
3.1.1 Gateway-gateway VPN

The first part is a VPN connection between two gateways. The figure below shows the hardware configuration of this part of the application.

Figure 3-1

Plant side (IP network B)

On the plant side, the hardware configuration consists of a DSL router (NETGEAR FVS 338) realizing the internet connection via a DSL modem and an ISP; the following components are connected to it:

- A CPU 315-2 DP via a CP 343-1 Advanced
- A field PG via the integrated network card
- A SIMOTION D435 via the integrated network interface
The DSL router (NETGEAR FVS 338) is connected to an ISP and thus to the internet via a DSL modem.

To locate the router on the internet, the router logs on to the DynDNS service. It thus allows a unique assignment between the changing IP address and the fixed domain name. The VPN connection is addressed by means of the domain name.

Via the internet connection, the VPN tunnel is operated from the router. The router represents the first tunnel endpoint and operates as a gateway.

**PC side**

On the PC side, the hardware configuration consists of a PC that is also connected to a NETGEAR DSL router (type: FVS 338) via Ethernet. The DSL router, NETGEAR FVS 338, is connected to an ISP and thus to the internet via a DSL modem.

To locate the router on the internet, also this router logs on to the DynDNS service. It thus allows a unique assignment between the changing IP address and the fixed domain name. The VPN connection is addressed by means of the domain name.

Via the internet connection, the VPN tunnel is operated from the router. The router represents the second tunnel endpoint and also operates as a gateway.

**Note**

The VPN connection establishment can be initiated from both sides.
3.1.2 **Client-gateway VPN**

The second part is a VPN connection between a VPN client and a VPN gateway.

The figure below shows the hardware configuration of the application.

**Figure 3-2**

### Plant side (IP network B)

On the plant side, the hardware configuration consists of a DSL router (NETGEAR FVS 338) realizing the internet connection via a DSL modem and an ISP; the following components are connected to it:

- A CPU 315-2 DP via a CP 343-1 Advanced
- A field PG via the integrated network card
- A SIMOTION D435 via the integrated network interface
The DSL router (NETGEAR FVS 338) is connected to an ISP and thus to the internet via a DSL modem.

To locate the router on the internet, the router logs on to the DynDNS service. It thus allows a unique assignment between the changing IP address and the fixed DynDNS domain name. The VPN connection is addressed by means of the DynDNS domain name.

Via this internet connection, the VPN tunnel is operated from the router. The router represents the passive tunnel endpoint and operates as a gateway.

**PC side**

On the PC side, the hardware configuration consists of any PC / laptop computer that is connected to the internet via any IP-capable interface (e.g., WLAN, ISDN or DSL) via any ISP.

The PC side does not require additional hardware.
3.2 Software requirements

Plant side (IP network B)

If the controllers have already been parameterized, only an operating system with a functional internet browser on the PG is required on the plant side.

PC side

Aside from the operating system, the software components of the applications to be used are necessary in both parts of the application on the PC side; these components include:

- Web browser
- FTP client
- STEP 7 (STEP 7 V 5.3 and higher)
- SIMOTION SCOUT (SIMOTION SCOUT V 4.0 and higher)

Additional software for the client-gateway VPN application

Aside from the listed components, the client-gateway application additionally requires the following software components:

- Necessary software for the internet access.
- VPN01L VPN client software.
  (The software client is part of the scope of delivery of the FVS 338)

Note

Theoretically, other standard VPN clients can also be used. When using other standard VPN clients, the problem is the use of the DynDNS name for addressing the gateway.
4 Required Hardware and Software Components

4.1 Gateway-gateway VPN

Products

Table 4-1

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETGEAR FVS338</td>
<td>2</td>
<td>---</td>
<td>As a VPN gateway (tunnel endpoint)</td>
</tr>
<tr>
<td>PS 305</td>
<td>1</td>
<td>6ES7 307-1EA00-0AA0</td>
<td>Standard PS</td>
</tr>
<tr>
<td>CPU 315-2 DP</td>
<td>1</td>
<td>6ES7 315-2AG10-0AB0</td>
<td>Standard CPU</td>
</tr>
<tr>
<td>CP 343-1 Advanced</td>
<td>1</td>
<td>6GK7 343-1GX21-0XE0</td>
<td>IT / Advanced CP</td>
</tr>
<tr>
<td>SIMOTION D435</td>
<td>1</td>
<td>6AU1 435-0AA00-0AA0</td>
<td>SIMOTION CPU**</td>
</tr>
<tr>
<td>Field PG</td>
<td>1</td>
<td>6ES7 712-1BB1.-0…</td>
<td>MLFB depending on configuration</td>
</tr>
<tr>
<td>PC</td>
<td>1</td>
<td>…</td>
<td>Any, with internet connection</td>
</tr>
</tbody>
</table>

* or comparable module
** or comparable SIMOTION CPU with Ethernet interface

Accessories

Table 4-2

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL modem</td>
<td>2</td>
<td>---</td>
<td>Depending on provider / router ***</td>
</tr>
<tr>
<td>Ethernet cable</td>
<td>&gt;4</td>
<td>6XV1 870-3Q…</td>
<td>MLFB depending on length</td>
</tr>
</tbody>
</table>

*** VPN routers with integrated DSL modem are available, the FVS 338 requires a modem.

Configuration software/tools

Table 4-3

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>1</td>
<td>---</td>
<td>Part of the PC operating system.</td>
</tr>
<tr>
<td>STEP 7 (V 5.3 and higher)</td>
<td>1</td>
<td>6ES7 810-4CC08-0YA5</td>
<td>MLFB of STEP 7 V 5.4</td>
</tr>
<tr>
<td>SIMOTION SCOUT</td>
<td>1</td>
<td>6AU1 810-0BA40-0XA0</td>
<td>MLFB of SIMOTION V 4.0</td>
</tr>
</tbody>
</table>
### 4.2 Client-gateway VPN

#### Products

**Table 4-4**

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETGEAR FVS338</td>
<td>1</td>
<td></td>
<td>As a VPN gateway (tunnel endpoint)</td>
</tr>
<tr>
<td>PS 305</td>
<td>1</td>
<td>6ES7 307-1EA00-0AA0</td>
<td>Standard PS</td>
</tr>
<tr>
<td>CPU 315-2 DP</td>
<td>1</td>
<td>6ES7 315-2AG10-0AB0</td>
<td>Standard CPU</td>
</tr>
<tr>
<td>CP 343-1 Advanced</td>
<td>1</td>
<td>6GK7 343-1GX21-0XE0</td>
<td>IT / Advanced CP**</td>
</tr>
<tr>
<td>Field PG</td>
<td>1</td>
<td>6ES7 712-1BB1.-0...</td>
<td>MLFB depending on configuration</td>
</tr>
<tr>
<td>PC</td>
<td>1</td>
<td></td>
<td>Any, with internet connection</td>
</tr>
</tbody>
</table>

#### Accessories

**Table 4-5**

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL modem</td>
<td>1-2</td>
<td></td>
<td>Depending on provider / router ***</td>
</tr>
<tr>
<td>Ethernet cable</td>
<td>&gt; 4</td>
<td>6XV1 870-3Q...</td>
<td>MLFB depending on length</td>
</tr>
</tbody>
</table>

*** Routers with integrated DSL modem are available, the FVS 338 requires a modem.

#### Configuration software/tools

**Table 4-6**

<table>
<thead>
<tr>
<th>Component</th>
<th>No.</th>
<th>MLFB / order number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>1</td>
<td></td>
<td>Part of the PC operating system.</td>
</tr>
<tr>
<td>STEP 7 (V 5.3 and higher)</td>
<td>1</td>
<td>6ES7 810-4CC08-0YA5</td>
<td>MLFB of STEP 7 V 5.4</td>
</tr>
<tr>
<td>SIMOTION SCOUT</td>
<td>1</td>
<td>6AU1 810-0BA40-0XA0</td>
<td>MLFB of SIMOTION V 4.0</td>
</tr>
<tr>
<td>VPN01L VPN client software</td>
<td>1</td>
<td>VPN01L (single license) / VPN05L (5 licenses)</td>
<td>VPN01L is part of the delivery scope of the FVS 338</td>
</tr>
</tbody>
</table>
Configuration and Startup of the Example

Overview

The following chapters describe the steps required to establish a VPN connection. The description starts with the setup of a DynDNS account and ends with the setup of the two parts of the application with the VPN connections between two gateways or between a client and a gateway.
5 DynDNS Setup

Preliminary remark

As already described in chapter 2.4 DynDNS, different providers exist which offer the DynDNS service. Since the routers offered by NETGEAR cooperate, among other providers, with DynDNS.org, this service was selected.

This chapter describes the process of setting up such a DynDNS entry. Depending on the used router, another DynDNS service provider can also be chosen; accordingly, the settings differ depending on the provider.

Task of the DynDNS service

The task of the DynDNS service is to grant access to the IP address of this destination station to any node on the internet. The service only knows the DynDNS domain name.

To achieve this, the DynDNS domain name must be known to the DynDNS service. The router updates the IP address as soon as it is connected to the internet via the ISP.

In the first step, the DynDNS domain name is created in the following.
5.1 Setting up a DynDNS account

Preparation
Since the DynDNS account can only be parameterized online, open the internet connection and go to the web page of the service.

Calling DynDNS home page
To visit the DynDNS home page, enter this address in the address bar of your internet browser:
http://www.dyndns.org

Creating an account
The first step is to create an account. The information in the account is necessary to store the access data for the DynDNS service in the router at a later time. In this way, the router can update the IP information.

On the DynDNS home page, select the “Account” menu option.

On the following page, you can enter your account. It is assumed that such an account does not yet exist; for this reason, “Create Account” has to be selected on the left side of the website.
DynDNS Setup

VPN Connections via DSL VPN Routers

ID Number: 26662448

Entering account data

On the next page, the information necessary for the account has to be entered.

Screen shots 5-1 and 5-2 show the settings.

Figure 5-1

The following entries have to be made:

- Specify a username you selected.
  If this name has already been used, you have to select a new one that has not yet been used.

- Enter an e-mail address.
  This address is required to check your authenticity. You will later receive an e-mail message at this address. (For security reasons, the e-mail account has to be entered again.)

- Specify a password.
  In the subsequent process the password confirms your authenticity to the service, particularly when it is used in the router. (The password also has to be entered again.)

Further use requires account name and password.
The second part of the logon refers to the terms of use.

Figure 5-2

Confirm the AUP. When you create more than one account, the DynDNS.org service is subject to a fee. If you create only one account, the second check mark has to be set.

Finally, select “Create Account” to confirm the account.

Note

One account is sufficient to create several hosts.

Confirmation e-mail message

After selecting the “Create Account” button, the DynDNS.org service sends a confirmation e-mail message. This is indicated by the following message.

Figure 5-3
5.2 Creating a DynDNS host

Account activation

After receiving the confirmation e-mail message and after using the internet link for activating the account, DynDNS.org indicates the activation with a confirmation.

Figure 5-4

Account Confirmed

The account has been confirmed. You can now log in and start using your account.

Necessary hosts

This application requires up to 2 hosts with DynDNS entries. These hosts have to be defined with the following entries:

- Teststation10.homedns.org
- Teststation20.homedns.org

Login at DynDNS.org

After using the "login" link of the shown confirmation e-mail message, the Login screen opens. Alternatively, the DynDNS.org link can be loaded again.
Adding host service

After the login the possible services for the account are displayed.

Figure 5-5

Creating a DynDNS entry requires a host that is created via “Add Host Service”.

Figure 5-6

The free Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains we offer, allowing your computer to be more easily accessed from various locations on the Internet. We provide this service, for up to five ($5) hostnames, free to the Internet community.

The Dynamic DNS service is ideal for a home website, file server, or just to keep a pointer back to your home PC so you can access those important documents while you’re at work. Using one of the available third-party update clients you can keep your hostname always pointing to your IP address, no matter how often your ISP changes it. No more fumbling to find that piece of paper where you wrote down your IP address, or emailing all your friends every time it changes. Just tell them to visit yourname.dyndns.org instead!

To enter a new host, an input window for the necessary data is opened via “Create Hosts”.
Host data

Figure 5-7 shows the input screen with the data necessary for the host.

Figure 5-7

The following fields must be filled out:

Table 5-1

<table>
<thead>
<tr>
<th>Input field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The host name assigned here is the name used for the IP address on the internet. The first part of the address can be freely assigned, the second part has to be selected from the list. Double assignment of host names is not possible.</td>
</tr>
<tr>
<td>TTL</td>
<td>TTL defines the update of the data on the internet. The default value, 60 seconds, is sufficient.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address indicates the first address that is used for the DynDNS host. Any address can be selected for the address specified here. The address is adjusted during dial-up to the ISP by the router. A value must be entered here; otherwise, the entry will not be applied.</td>
</tr>
</tbody>
</table>
The default values of all other entries do not have to be changed.

After using the “Create New Host” button, the host entry has been completed, provided that there is no overlap with other entries.

Confirming the entry

The entry is confirmed as follows:

Figure 5-8

The entry has been completed.

It is also possible to make additional entries.

ATTENTION  The DynDNS entries made here and the access data will be used in the course of this application. They have been created only for demonstration purposes and are no longer used.
6 Gateway-Gateway VPN Router 1

Preliminary remark

The NETGEAR FVS 338 routers used in these applications are examples of the routers available on the market. If the functional scope is identical, the settings made here can also be made by other devices of other manufacturers.

Content of the chapter

This chapter describes the necessary parameterization steps for the router settings. The parameters for the internet connection, for the local network and for the VPN connection are shown.

Since most modules of this type can be parameterized by HTML settings via a web browser, the NETGEAR also uses this option. This is explained by the following step-by-step instructions.

Important properties of the used routers

To use this application, the following properties and functions of the router are necessary:

- PPPoE functionality for connecting to the internet via an ISP
- DynDNS functionality for locating the router on the internet
- VPN gateway functionality
- DHCP functionality for the internal network
- SPI firewall (as a useful supplement)

Note

A decisive function in the NETGEAR router is the capability of establishing VPN tunnels also with endpoints that can be located via DynDNS. This function must be supported by other router combinations for this situation.
6.1 Login to the router

The parameterization requires a web browser. Open it on your PG in the plant network.

Note

Normally, the module can also be parameterized via the internet. Please ensure that password and connection (e.g., via VPN) are secure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Note / explanation</th>
</tr>
</thead>
</table>
| 1.   | In the address bar, enter the IP address of the router. For the first startup this IP address is specified by the manufacturer, often with the following address: | 192.168.0.1  
For details, please refer to the technical documentation included in the delivery. |
| 2.   | Enter user name and password from the module documentation. Select the “Login” button to open the module parameterization. |
6.2 Basic internet access settings

After a successful login of the router the first page of the router configuration opens. This is normally the parameterization of the ISP (internet service provider).

Since the settings of the ISP can be very diverse and since various modules use wizards, the procedure is not described in detail.

Frequently used basic parameters are listed in the following sections.

**ISP parameters**

Figure 6-1
Table 6-2

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISP Login</td>
<td>ISP Login contains the ISP access data. The data can include a <strong>login</strong>, a <strong>password</strong> and possibly a mac address. Some ISP authenticate the users only by the mac address; for this reason, select &quot;No&quot; for &quot;Require a Login&quot;. If a special mac address is necessary, this has to be configured separately.</td>
</tr>
<tr>
<td>ISP Type</td>
<td>ISP type is divided into two sections:</td>
</tr>
<tr>
<td></td>
<td>• Connection type</td>
</tr>
<tr>
<td></td>
<td>the method used for the data transmission is defined in this section. Normally, DSL uses <strong>PPPoE</strong> (Point-to-Point Protocol over Ethernet)</td>
</tr>
<tr>
<td></td>
<td>• ISP parameters</td>
</tr>
<tr>
<td></td>
<td>if required, additional parameters can be stored here.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Idle Time</strong> parameter is of interest to this application. It defines how long the internet connection remains established without data traffic from or to the private network.</td>
</tr>
<tr>
<td>Internet IP Address</td>
<td>The public IP address of the module is parameterized here. The variant with “Get Dynamically from ISP” shown above is the default setting. The ISP dynamically assigns the IP address to the module. If the connection has a fixed IP address, this address has to be stored here.</td>
</tr>
<tr>
<td>Domain Name Server</td>
<td>In this group, it is defined via which DNS servers domain names are resolved to IP addresses. A direct setting may be required if, for example, a fixed IP address is assigned. The default setting is the setting with direct assignment by the ISP shown above.</td>
</tr>
</tbody>
</table>

**Characteristic feature of this router**

Since, aside from the DSL functionality, this router supports a dial-up interface for use with an analog modem as a fall back strategy, a second, comparable tab exists for the parameterization of the dial-up interface.
6.3 Checking internet connection

The router supports the user in checking the internet connection. For this reason, the connection status is displayed on a separate page.

In the case of the NETGEAR router, this is done directly from the start page by selecting the “Broadband Status” option.

Figure 6-2

“Connection State” indicates that the internet connection has been successfully established. The current public IP address and the gateway and DNS data are also listed here.
6.4 Checking WAN mode

Setting routing method and used WAN port

In the configuration user interface of the NETGEAR router, select the WAN Mode tab to define the settings for

- the used routing mode between WAN and LAN. Either NAT (Network Address Translation) or Classical Routing can be selected. NAT is used in this application.

- the WAN ports to be used. You can select whether DSL or dial-up interface is to be used, or whether DSL with dial-up as backup is to be used. In this application, only the Broadband setting for DSL is used.

Figure 6-3
6.5 **DynDNS parameterization**

**Introduction**

DynDNS as a service has already been set up in chapter 5 of this application. The following sections focus on the application with the NETGEAR router.

**Assigning the DynDNS parameters**

After selecting the DynDNS provider to be used, you have to log on to the provider. When logging on to the DynDNS provider, you will have to specify 3 important parameters:

- The used user name. This name identifies you as a user and the devices using the DynDNS service.
- The password assigned to the user name. To secure the authentication of the user.
- Host / Domain Name. The DNS names with which the IP addresses are resolved on the internet.
  - VPN router 1: Teststation10.homedns.org
  - VPN router 2: Teststation20.homedns.org

These parameters have to be specified during the DynDNS parameterization of the respective router.
6.6 Settings in the local plant network

IP address / IP band of the router

The “LAN Setup” tab enables you to adjust the LAN settings of the
- router or of the
- DHCP server of the router in the

local network.

If the IP address of the router is changed, the router can only be accessed via the new IP address (after storing the data). The DHCP server settings allow the modules to be automatically set up during startup. They react to changes of the network settings by reassigning an IP address or the gateway / DNS parameters to the router.

Figure 6-5
6.7 VPN parameterization using wizard

VPN parameterization using the VPN Wizard

The NETGEAR routers offer two options to create a VPN tunnel.

- The first option is the use of the VPN Wizard.
- The second option is the direct input of the policies.

To start the VPN Wizard, select the “VPN” option and “VPN Wizard” below in the menu.

The page of the VPN Wizard has the structure shown in the following figure:

Figure 6-6

To run the wizard for a gateway-gateway VPN connection, you have to fill out the following fields.
### Table 6-3

<table>
<thead>
<tr>
<th>Field</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Type</td>
<td>Specifies whether the peer endpoint of the VPN tunnel is an additional gateway or a VPN client.</td>
</tr>
<tr>
<td>Connection Name</td>
<td>The meaningful assignment of a connection name selected by you facilitates the later assignment of the VPN connections.</td>
</tr>
<tr>
<td>Pre-Shared-Key</td>
<td>“Pre-Shared-Key” is the basic key for creating the IPsec encryption. The key can be between eight and 49 characters long.</td>
</tr>
<tr>
<td>Remote WAN IP / Address</td>
<td>The “Remote WAN IP / Address” address parameter is used to define the IP address of the remote station. Either the internet IP address of the remote gateway (tunnel endpoint) or its (DynDNS) domain name can be specified.</td>
</tr>
<tr>
<td>Local WAN IP / Address</td>
<td>The “Local WAN IP / Address” address parameter is used to specify the IP address of your own station. This is necessary for the VPN connection establishment since the authenticity of the connection partners is checked here. Either the internet IP address of the local gateway (tunnel endpoint) or its (DynDNS) domain name can be specified. The router specifies the DynDNS entry if it has already been configured.</td>
</tr>
<tr>
<td>Remote LAN IP Address</td>
<td>The base address of the remote network’s IP band has to be entered here, this entry is necessary to create a suitable routing entry in the local router. The IP bands of both networks <strong>must</strong> differ.</td>
</tr>
<tr>
<td>Remote LAN Subnet Mask</td>
<td>The final necessary information to be provided is the remote subnet mask of the network.</td>
</tr>
</tbody>
</table>

It is only advisable to enter the IP address for the WAN IP address if this address is static. If an address is dynamically assigned, the use of DynDNS is necessary.

**Note**

The first option to configure a gateway-gateway VPN connection is now completed.

**ATTENTION**

In the case of the NETGEAR routers used here, a domain name (frequently as FQDN (Fully Qualified Domain Name)) can be both a static and a DynDNS entry. When using other router types or routers of other manufacturers, this property has to be checked.
6.8 VPN parameterization via direct input

Overview of the IKE policies

Alternatively to configuring the VPN connection using the VPN Wizard, a configuration via the policies is also possible.

For the NETGEAR FVS 338 the first step is to configure the IKE Policies.

Figure 6-7

Input of the IKE policies

The IKE policies contain information on the connection establishment. They include the two destination addresses, the used password and information on the used encryption. To create a new policy, use “add…” to insert it. Select “edit” to edit an existing policy.
The IKE policies use the following information:

**Table 6-4**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Aside from the policy name, the connection type (a connection that can be established on both sides for gateway-gateway VPN) and the IKE negotiation mode (Main mode) are defined in the General field.</td>
</tr>
<tr>
<td>Local Address</td>
<td>As a local address, either the IP address, only recommended for a static IP address of the internet connection, or an FQDN can be entered. If the router uses DynDNS, the default address set here is the set DynDNS address.</td>
</tr>
</tbody>
</table>
### Field | Input
--- | ---
Remote Address | As a remote address, either the IP address, only recommended for a static IP address of the internet connection, or an FQDN can be entered.
IKE SA Parameters | This set of parameters contains information on the selected encryption algorithms. The entry of the pre-shared key is important to the user. Aside from the local and remote internet IP addresses, this key authenticates the connection partners among one another.
Extended Authentication | XAUTH is a protocol extension by CISCO to prevent “man-in-the-middle” attacks.

Except for the pre-shared key, the default values of the IKE SA parameters were not changed.
Overview of the VPN policies

The second and final step is to configure the “VPN Policies”.

Figure 6-9

Input of the VPN policies

The VPN policies contain information that goes beyond the IKE policies such as the structure of the two networks to be networked and information on handling the encryption in the time characteristic of the connection.

To create a new policy, use “add…” to insert it. Select “edit” to edit an existing policy.
The VPN policies use the following information:
### General
Aside from the policy name, the policy type – which is Auto Policy and should not be changed – is defined in the General field. The IP address or the FQDN again has to be specified for the remote endpoint of the VPN tunnel. If NetBIOS is to be possible, this has to be selected here.

### Traffic Selection
The two networks to be connected are described in this section. The IP basebands and the subnet masks of the networks to be connected have to be specified here. This is required for the routing lists of the routers.

### Manual Policy Parameters
When Manual Policy is selected instead of Auto Policy in the General field, additional settings have to be made here.

### Auto Policy Parameters
The Auto Policy Parameters define how and how often the used key is renewed in the course of the VPN connection. A new key is negotiated every 3600 seconds, the algorithms used for the negotiation are described. The IKE policy described in the last chapter was selected as an IKE policy.

The Traffic Selection parameters have to be provided with subnet information for the gateway-gateway VPN connection. Assigning ANY or individual addresses to the parameter is not advisable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Aside from the policy name, the policy type – which is Auto Policy and should not be changed – is defined in the General field. The IP address or the FQDN again has to be specified for the remote endpoint of the VPN tunnel. If NetBIOS is to be possible, this has to be selected here.</td>
</tr>
<tr>
<td>Traffic Selection</td>
<td>The two networks to be connected are described in this section. The IP basebands and the subnet masks of the networks to be connected have to be specified here. This is required for the routing lists of the routers.</td>
</tr>
<tr>
<td>Manual Policy Parameters</td>
<td>When Manual Policy is selected instead of Auto Policy in the General field, additional settings have to be made here.</td>
</tr>
<tr>
<td>Auto Policy Parameters</td>
<td>The Auto Policy Parameters define how and how often the used key is renewed in the course of the VPN connection. A new key is negotiated every 3600 seconds, the algorithms used for the negotiation are described. The IKE policy described in the last chapter was selected as an IKE policy.</td>
</tr>
</tbody>
</table>

**Note**
The second option to configure VPN connections is now completed.
7 Gateway-Gateway VPN Router 2

Content of the chapter

This chapter describes the necessary parameterization steps for setting the 2nd router for the gateway-gateway VPN connection. It additionally describes how to obtain status information on the VPN connection, how to activate / deactivate the VPN connection and how to diagnose the VPN connection respectively.

Changes compared to router 1

Since the configuration of the two routers is almost identical, a complete step-by-step description of the configuration is not necessary.

The following sections describe the points that differ from the description in chapter 6 “Gateway-Gateway VPN Router 1”.

Parameter comparison

To compare the parameters of router 1 and router 2, a comparison of the two routers is listed in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Router 1</th>
<th>Router 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP band</td>
<td>192.168.2.1</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DynDNS identifier</td>
<td>Teststation10.homedns.org</td>
<td>Teststation20.homedns.org</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>Password</td>
<td>Password</td>
</tr>
<tr>
<td>VPN parameters</td>
<td>IKE SA Parameters</td>
<td>IKE SA Parameters</td>
</tr>
<tr>
<td></td>
<td>Auto Policy Parameters</td>
<td>Auto Policy Parameters</td>
</tr>
</tbody>
</table>

As shown in the table, the configuration differs only in the network parameters of the local Ethernet network and in the parameters of the DynDNS identifier for the internet IP address. The encryption parameters remain identical.

Necessary adjustments

Thus, the following adjustments are required:

- The DynDNS address, see chapter 6.5 DynDNS address.
- The network address, see chapter 6.6 Settings in the local plant network.
- The VPN connections, see chapter 6.7 and the following chapters.

The changes in the VPN parameterization will be considered in greater detail in the following sections.
7.1 VPN connections using wizard

VPN Wizard

The changes compared to the settings described in chapter 6.7 are shown in the following screen shot.

Figure 7-1

As can be seen in the figure, the WAN IP addresses have been swapped. In addition, the LAN IP address has been adjusted to the remote network. Like the pre-shared key or the VPN parameters, the shared secrets remain unchanged.
7.2 VPN connections via direct input

IKE policies

The alternative configuration via IKE policies for router 2 has to be adjusted as follows:

Figure 7-2

Compared to router 1, the only change in the IKE parameters is the fact that the WAN IP addresses have been swapped.
VPN policies

The parameters of the VPN policies for router 2 change as follows:

As for the IKE parameters, the only changes compared to router 1 are the swapped IP address bands. All other parameters remain unchanged according to the parameters of router 1.
7.3 Status information for VPN connections

Checking connection status

The NETGEAR FVS 338 router offers the function to check the connection status of a VPN connection. This function is integrated in comparable routers in a similar way.

Aside from the “Policies”, the “VPN” tab also includes the “Connection Status”.

Figure 7-4
Activating VPN connection

The status in the last figure shows that the VPN connection is not established. By activating the connection establishment using "Connect", an attempt to establish the connection is made – no matter from which of the two routers.

When the connection has been successfully established, the status information changes as follows:

Figure 7-5

<table>
<thead>
<tr>
<th>State</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec SA Established</td>
<td>![drop]</td>
</tr>
</tbody>
</table>

Using the "Drop" button, the connection can be disconnected if required.

Note

If a router was reset or switched on, the connection has to be established using this menu option. Communication is only possible after the connection has been established.
7.4 Diagnostics for VPN connections

VPN logs

The NETGEAR FVS 338 router provides a logbook for the VPN functions. This logbook contains entries on the different phases and modes of the connection establishment, the continuous operation of the connection (with ACK exchange) and entries on occurring errors.

The logbook is a helpful tool when diagnosing difficulties concerning the connection or connection establishment.

The logbook is located in the "Monitoring" tab in "VPN Logs".

A typical display of a successful connection establishment may look as follows:

Figure 7-6

Note

Error entries are stored as text. For further information with regard to the error messages, please use the manuals or hotlines of the manufacturers.
8 Client-Gateway VPN Router

Preliminary remarks

The application described in the following sections is possible in a comparable way also with other routers.

The decisive factor for the planned application is that the used VPN gateways and client products accept DynDNS addresses as address parameters for the VPN tunnel endpoint (gateway).

Content of the chapter

This chapter describes the necessary parameterization steps for the router settings for the application with a VPN client.

Changes in the VPN parameterization

Since the parameterizations for the internet access described in chapter 6 are identical for the used routers, it is not necessary to describe them. This chapter contains only the parameterization of the VPN connection using the VPN Wizard or via the policies.
8.1 VPN connection using wizard

VPN Wizard

To parameterize a VPN client connection, the settings have to be adjusted as follows:

Figure 8-1

Compared to the parameters from the chapters describing the gateway-gateway VPN connection, the peer type is set to VPN client. Thus, the following two parameters change:

1. The local / remote WAN IP address was replaced by identifier information.
2. The remote LAN information is grayed out and thus no longer user-accessible.

Since only one terminal unit is connected, network information concerning the LAN information is no longer required.
The identifier information can be handled flexibly. The FQDN (the DynDNS address) or the IP address is advisable for the local endpoint.

Since the remote endpoint can have changing IP addresses or since it can be located behind an NAT gateway, it is not advisable to specify the IP address of the client PC. An e-mail account is entered instead of the IP address. This is not mandatory (other entry is possible), but the VPN PC client supports e-mail addresses and thus makes it advisable to enter an e-mail account.

**Note**
The specified e-mail address stands symbolically for a shared secret. This information is not checked, therefore addresses that do not exist can also be used. (See used e-mail address in the screen shot)
8.2 VPN connection via direct input

Input of the IKE policies

The parameters of the IKE policies for the VPN gateway have to be specified as follows:

The differences in the parameters of the IKE policies are limited to the “General” section and the “remote address”.

As already described for the wizard, an e-mail address was entered as a shared secret in “remote address”. This address is still considered as an FQDN; this cannot be changed in the router and thus has to be considered
as a circumstance of the parameterization. An e-mail address is parameterized in the client.

The “General” field includes a larger difference. The following has to be considered.

Table 8-1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction / Type</td>
<td>The router is parameterized as a “responder”. The parameterization defines that it only reacts to attempts to establish a connection. Connections are not established independently. This will be performed exclusively by the client.</td>
</tr>
<tr>
<td>Exchange Mode</td>
<td>The shortened connection establishment of the VPN connection is selected with the “Aggressive” exchange mode. This is the default setting of the router, but an adjustment to the more extensive “Main” mode is permissible and recommended.</td>
</tr>
</tbody>
</table>

**Note**

The exchange of the VPN keys via Aggressive mode is permissible but not recommended. If possible, the use of the Main mode has to be strived for, see the IPsec protocol description in this document.
VPN policies

The parameters of the VPN policies for the VPN gateway are shown in the screen shot below.

Figure 8-3

The differences in the parameters of the VPN policies are limited to the “Traffic Selection” section and the “Remote Endpoint”.

In contrast to the gateway-gateway connection, no remote network parameters are specified here. This is not required since no remote network but an individual node is connected.
The “Any” remote IP has to be assigned.

The e-mail address already mentioned in the IKE parameters has to be entered as an FQDN for the “Remote Endpoint” parameter. This replaces the DynDNS address.
Preliminary remarks

The router network configured as a VPN gateway in the previous chapter can now be accessed on a tunneled basis from a VPN client application via a secure VPN connection.

Content of the chapter

This chapter deals with the necessary parameterization steps to set the VPN connection on the VPN PC client. It additionally describes how to obtain status information on the VPN client connection, how to activate / deactivate the VPN client connection and how to diagnose the VPN client connection on the client and on the router respectively.

Software installation

To operate a PC as a VPN client, VPN client software is required. NETGEAR delivers a VPN01L VPN software client with the FVS 338 router (see chapter 4.2 Configuration software / tools).

The software is installed as described in the documentation provided by NETGEAR; this makes it unnecessary to describe the installation.
9.1 Opening Security Policy Editor

Ways to open the editor

After installing the VPN client, there are two options to open the Security Policy Editor.

These options are:

- By selecting \textit{Start} > \textit{NETGEAR ProSafe VPN Client} > \textit{Security Policy Editor}

- By double-clicking the \textbf{\textit{icon}} in the task bar.
9.2 Inserting a new connection

New Connection

Select Edit > Add > Connection to insert a new VPN connection, “New Connection”.

Figure 9-1

The parameters to be specified here are divided into two groups:

Table 9-1

<table>
<thead>
<tr>
<th>Group</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Security</td>
<td>Secure / Non-secure / Block</td>
<td>It can be selected whether the data transmitted via this connection are to be secure, non-secure or blocked.</td>
</tr>
</tbody>
</table>
| Only Connect Manually |                            | For the connection mode, you can select between  
|                     |                            |   • automatically, i.e. the connection is established as  
|                     |                            |     soon as the VPN client is ready (not checked),  
|                     |                            |     • manually, i.e. the connection is only established by  
|                     |                            |     activation of the user on the client (checked).  |
### Group: Remote Party Identity and Addressing

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Type Network</td>
<td>By selecting the ID type for the network, it can be defined whether the connection is configured to:</td>
</tr>
<tr>
<td></td>
<td>• an entire network (IP Subnet),</td>
</tr>
<tr>
<td></td>
<td>• an address range (IP Address Range) or</td>
</tr>
<tr>
<td></td>
<td>• an individual address (IP Address)</td>
</tr>
<tr>
<td>Subnet</td>
<td>When an entire network has been selected, the IP base address of the network is specified. (When specifying the ID type address range or an individual address, the address or the address range has to be entered here.)</td>
</tr>
<tr>
<td>Mask</td>
<td>The subnet mask associated with the IP base address has to be specified for unique assignment of the subnet. (A Class C network in the example.)</td>
</tr>
<tr>
<td>Protocol / Port</td>
<td>The selection of the protocol or the protocol / port combination enables the user to allow specific protocols and further limiting services via a connection. This function is not used in this example.</td>
</tr>
</tbody>
</table>

#### Secure Gateway Tunnel

The "Connect using Secure Gateway Tunnel" option always has to be selected.

#### ID Type Remote Address

To connect a gateway to the client, two setting variants have proven to be successful:

1. ID Type Any / Gateway Hostname, with DynDNS name of the gateway
2. Domain Name / Gateway Hostname, with DynDNS name of the gateway for both parameters

Enter the data of your connection partner as described.

**Note**

For a better assignment of the client connection, you can select a meaningful name for the connection.
9.3  “My Identity”

Opening the “My Identity” dialog box

Click the plus sign to the left of the connection name to open the next parameter level. Select the “My Identity” item to open the parameters window for the input of the VPN client identity parameters.

Since no certificate is being used, the Select Certificate parameter has to be set to “None”.

The following scenario appears:

Figure 9-2

The following parameters have to be adjusted.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Type</td>
<td>Either&lt;br&gt;• an IP address,&lt;br&gt;• a domain name or&lt;br&gt;• an e-mail address can be specified as ID type. In this example, an e-mail address is used that does not exist and that is not checked (see router configuration).</td>
</tr>
<tr>
<td>Virtual Adapter</td>
<td>The virtual adapter is necessary and has to be configured with “Required”.</td>
</tr>
<tr>
<td>Internet Interface</td>
<td>Windows can use only one interface as an internet interface. When using several NICs, a setting may be necessary. Normally, a parameterization with “Any” is sufficient.</td>
</tr>
</tbody>
</table>

The confirmation of the configuration requires the pre-shared key, which can be entered after using the “Pre-Shared Key” button.

**Entering the pre-shared key**

To enter the key, this window opens:

Figure 9-3

![Pre-Shared Key](image)

Enter the pre-shared key stored in the router. Confirm the input with OK.
9.4 Setting the security policy

Setting the tunnel establishment mode

To set the mode to establish the connection, Security Policy has to be selected.

As specified in the router configuration, the “Aggressive Mode” option has to be selected in “Select Phase 1 Negotiation Mode”.

The other default settings remain unchanged.

“Main Mode” may also be used or necessary for other configurations / routers.
9.5 Authentication Proposal

Creating the Authentication Proposal

Two items are located below Security Policy in the menu tree:

- Authentication (Phase 1) and
- Key Exchange (Phase 2).

The first phase of the connection establishment is described by the authentication. The necessary data has already been stored in My Identity. Thus, only the used mechanisms are described here.

If a proposal has already been created, in Authentication (Phase 1), it is only required to check whether the settings correspond to the gateway settings.

Figure 9-5

In some cases, the life of the secure association (SA Life) has to be set; it must correspond to the value of the configuration in the gateway. Normally, this value is between 3600 and 28800 seconds (one or eight hours).
9.6 Key Exchange Proposal

Creating the Key Exchange Proposal

As a second item, Key Exchange (Phase 2) is located below Security Policy in the menu tree.

In the second phase of the tunnel establishment, the encryption generated in phase 1 is exchanged and a new encryption is initiated. The data necessary for this process is automatically generated by the client and the gateway and is still based on the shared secrets.

The parameters assigned here describe only the used mechanisms and have to correspond to the gateway values.

Figure 9-6

In some cases, the life of the secure association (SA Life) has to be set; it must correspond to the value of the configuration in the gateway. Normally, this value is between 3600 and 28800 seconds (one or eight hours).
Completing the configuration

When using the button with the disk icon, the configuration is saved and activated.

By selecting Menu > File, a configuration can also be exported or imported.
9.7 Activating and deactivating the VPN connection

Activating the VPN tunnel from the client side

To activate the VPN tunnel on the client side, the VPN client icon on the task bar, must be right-clicked. The context menu opens.

By selecting Connect… > VPN_Client, the VPN tunnel is established.

Deactivating the VPN tunnel from the client side

To deactivate the VPN tunnel on the client side, the Disconnect … > VPN_Client1 option has to be selected in the context menu.
9.8 Testing the VPN connection on the client

To test the connection, the client offers two options:

- Log Viewer
- Connection Monitor

Like the activation / deactivation of the VPN tunnel, both diagnostic capabilities can be found via the context menu.

Log Viewer

VPN Log displays the management data transmitted during the communication.

The Log Viewer can be started via

Log Viewer...

In the Log Viewer, errors in the configuration or in the connection establishment can be diagnosed.

Figure 9-8
Connection Monitor

The Connection Monitor displays the currently used or parameterized VPN connections.

To open the Connection Monitor, **Connection Monitor**…

has to be selected in the context menu.

The network addresses and the transmitted encrypted or lost data packets are displayed as additional information.

Figure 9-9

![Connection Monitor](image)
Connection diagnostics on the gateway side

Aside from the already described Monitoring function, the gateway also offers the option to check a connection status that can be found in the gateway in **VPN > Connection Status**.
10 Necessary Hardware Preparation

PC side

On the PC side, it has to be observed that the IP address is automatically obtained via DHCP in both cases, gateway-gateway or client-gateway connection. The remaining settings are automatically made by the router or the internet provider.

Plant side (IP network A and B)

On the controller side, the IP address has to be permanently assigned according to the IP band. The local router has to be entered as a default gateway. No additional settings are required.
11 Performance Data

11.1 Constraints

Technical restrictions

From a technical perspective two decisive restrictions have to be named:

- The applicable data bandwidth:
  The data bandwidth ensues from the used communication connection. When using, for example, a TDSL 1000 connection, the resulting bandwidth is 1000 kb downstream and 128 kb upstream. It is thus only possible to send up to 128 kb of data from the plant side to the communication partner. This corresponds to two ISDN B channels. The use of a symmetric connection variant with 1000 / 1000 kb is recommended.
  Some gateways also have a bandwidth limitation for VPN, which, depending on device and manufacturer, is listed in the technical specifications.

- The response time:
  the response time is the period the communication requires to reach the partner and to be answered. In a local network, this period is very short, mostly < 1 ms. On the internet this response time can quickly increase to > 100 ms. Fast online functions (in the real-time range), as are necessary with SIMOTION, are thus not possible via the internet.

11.2 Experiences from the application

For use via remote access, the following information was gathered for the different products.

SIMATIC S7

Aside from the fixed IP address located in the subnet, the SIMATIC S7 Ethernet interface must include the IP address of the local router in the Ethernet as a parameter (as a default gateway / router). Here the IP address would be the address of the respective NETGEAR FVS 338 router in the local network.

STEP 7

The functions
- read out diagnostic data,
- download the program to the controller and
- monitor variables / blocks

could be successfully executed. The speed corresponded to the interfaces in the local network.
Functions based on MAC, for example Edit Ethernet Node, could not be used.

If the PG is in the configuration as a SIMATIC PC station, the complete IP parameters of the physical Ethernet interface have to be entered in the parameters of the SIMATIC PC station’s logical Ethernet interface.

**SIMOTION**

The functions

- read out diagnostic data,
- download the program to the controller,
- monitor variables / blocks and
- go online to SIMOTION and SINAMICS

could be successfully executed. The speed corresponded to the interfaces in the local network.

Moving the drives via the machine control panel integrated in SCOUT was not possible. The connection collapsed due to the high data load and the required response times. A visualization via PROTOOL PRO using the SIMOTION profile was also not possible.

**WinCC flexible**

The functions

- read out diagnostic data and
- download the configuration to the panel

could be successfully executed. The speed corresponded to the interfaces in the local network.

The visualization with WinCC flexible in the standard profile with refresh times > 200 ms was successfully possible on a small scale.

**Note**

Use in the settings of the PG/PC panel of your PC the configuration of the fixed IP address.

The function TCP/IP (Auto) -> [NIC] does not work as soon as different IP subnets are being used. This is because this feature tries to set up an IP address of the destination IP subnet on the PC. With the revised IP address the PC loses the assignment to the local router and the connection can not be established.
11.3 Security features

IPsec

As already described in chapter 2.3.4 Criticism of IPsec, IPsec is the most secure method for data transmission via IP-capable networks in the present state of the art.

IPsec as a basis of the VPN connection thus ensures the highest possible security for the data transmission using VPN via the internet or within a network.

IPsec-based VPN connections are not perfect, but they are secure compared to port forwarding.
11.4 Tested applications

Tested software

The following software versions have been successfully tested with this application:

Table 11-1

<table>
<thead>
<tr>
<th>Application</th>
<th>Successfully tested software</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML access</td>
<td>Internet Explorer 6 and 7, Firefox, Opera</td>
</tr>
<tr>
<td>FTP accesses</td>
<td>FTP client of Windows XP SP 2, WS FTP, Filezilla</td>
</tr>
<tr>
<td>PG functions</td>
<td>STEP7 V 5.4 SP 1, SIMOTION SCOUT V 4.0 HF2</td>
</tr>
</tbody>
</table>

12 History

Table 12-1

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>10/11/07</td>
<td>First edition</td>
</tr>
</tbody>
</table>