



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

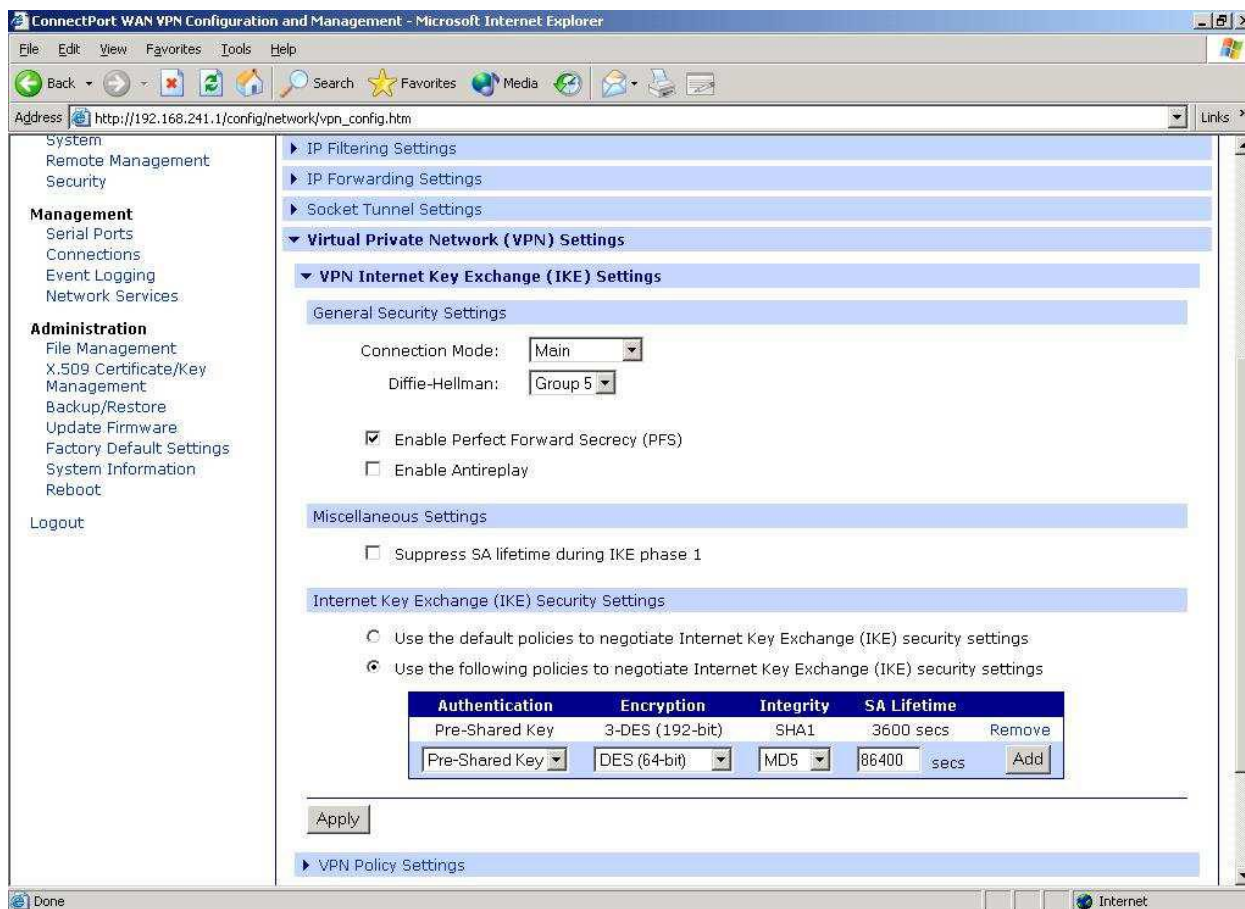
1. Strongswan Installation

Get installation package from www.strongswan.org and install (tested with Strongswan version 2.8.4 and direct PPPOE DSL connection with fixed public IP on the linux (Debian 4.0) machine)

2. Digi Connect WAN 3G / VPN configuration with firmware 2.14 and earlier

IP: 192.168.241.1, Netmask 255.255.255.0

VPN Settings – Phase 1:



Main Mode, Grp. 5, PFS activated
PSK / 3DES / SHA1 / 3600s key lifetime



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

VPN Settings - Phase 2:

The screenshot shows a web browser window titled "ConnectPort WAN VPN Configuration and Management - Microsoft Internet Explorer". The address bar shows "http://192.168.241.1/config/network/vpn_tunnel_config.htm?1". The page content is divided into a left sidebar and a main configuration area.

Connectware™

Home

Configuration

- Network
- Mobile
- Serial Ports
- Camera
- Alarms
- System
- Remote Management
- Security

Management

- Serial Ports
- Connections
- Event Logging
- Network Services

Administration

- File Management
- X.509 Certificate/Key Management
- Backup/Restore
- Update Firmware
- Factory Default Settings
- System Information
- Reboot

Logout

VPN - Tunnel #1 - Configuration

Description: Tunnel 1

Remote VPN Address: 217.91.93.51

VPN Tunnel: ISAKMP

Local Endpoint Type: Local endpoint is a subnet

Identity

Network Interface: mobile0

Negotiate tunnel as soon as interface comes up

Use the following as the identity: 00:40:9D:2E:54:83@digi.com

Use the interface IP address

Use the identity certificate X.509 distinguished name (DN)

Local Endpoint

Tunnel Network Traffic from the following Local Network:

IP Address: 192.168.241.0

Subnet Mask: 255.255.255.0

Remote Endpoint



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

ConnectPort WAN VPN Configuration and Management - Microsoft Internet Explorer

Address: http://192.168.241.1/config/network/vpn_tunnel_config.htm?1

Reboot
Logout

IP Address: 192.168.241.0
Subnet Mask: 255.255.255.0

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address: 192.168.240.0
Subnet Mask: 255.255.240.0

Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:
217.91.93.51

Use the following pre-shared key to negotiate IKE security settings:
nBnP524

ISAKMP Phase 2 Policy Settings

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
3-DES	MD5	5400 secs	Remove
None	None	28200 secs	Add

Apply Cancel

Copyright © 1996-2007 Digi International Inc. All rights reserved.
www.digi.com

Endpoint: fixed public DSL IP
Identity: 00:40:9D:2E:54:83@digi.com
Local network: 192.168.241.0/24 , Netmask 255.255.255.0
Remote network: 192.168.240.0/20 , Netmask 255.255.240.0
ID: fixed public DSL IP
PSK: nBnP524
3DES / MD5 / 5400s key lifetime



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

3. Connect WAN VPN configuration with firmware 2.7 and later

Virtual Private Network (VPN) Settings

VPN Global Settings

General Security Settings

Enable Antireplay

Miscellaneous Settings

Suppress SA lifetime during IKE phase 1

Suppress Delete Phase 1 SA Message For PFS

VPN - Tunnel #1 - Configuration

Description:

Remote VPN Address:

VPN Tunnel:

Local Endpoint Type:

Identity

Network Interface:

Negotiate tunnel as soon as interface comes up

Use the following as the identity:

Use the interface IP address

Use the identity certificate X.509 distinguished name (DN)

Local Endpoint

Tunnel Network Traffic from the following Local Network:

IP Address:

Subnet Mask:

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address:

Subnet Mask:

Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:

Use the following pre-shared key to negotiate IKE security settings:



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode:

Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

Enable NAT Traversal (NAT-T)

Keep Alive Interval:

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	3-DES (192-bit)	MD5	86400 secs	Group 5	Remove
<input type="text" value="Pre-Shared Key"/>	<input type="text" value="3-DES (192-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="86400"/> secs	<input type="text" value="Group 5"/>	<input type="button" value="Add"/>

ISAKMP Phase 2 Settings

General Security Settings for Phase 2

Diffie-Hellman:

ISAKMP Phase 2 Policies

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
3-DES	MD5	5400 secs	Remove
<input type="text" value="3-DES"/>	<input type="text" value="MD5"/>	<input type="text" value="5400"/> secs	<input type="button" value="Add"/>



4. Strongswan 2.8.4 Software Configuration

eth0 static IP 192.168.255.1
firestarter installed (apt-get install firestarter)
firestarter started and set to "firewall off" (Pause icon)

/etc/ipsec.conf:

```
# /etc/ipsec.conf - strongSwan IPsec configuration file
# RCSID $Id: ipsec.conf.in,v 1.7 2006/01/31 13:09:10 as Exp $
# Manual: ipsec.conf.5
# Help: http://www.strongswan.org/docs/readme.htm
version 2.0 # conforms to second version of ipsec.conf
specification
# basic configuration
config setup
# THIS SETTING MUST BE CORRECT or almost nothing will work;
# %defaultroute is okay for most simple cases.
interfaces=%defaultroute
# Debug-logging controls: "none" for (almost) none, "all" for
lots.
klipsdebug=none
plutodebug=none
#crlcheckinterval=600
#strictcrlpolicy=yes
#cachecrls=yes
# Use auto= parameters in conn descriptions to control startup
actions.
#plutoload=%search
#plutostart=%search
# Close down old connection when new one using same ID shows
up.
uniqueids=yes
nat_traversal=no
# defaults for subsequent connection descriptions
# (mostly to fix internal defaults which, in retrospect, were badly
chosen)
conn %default
authby=rsasig
leftrsasigkey=%cert
rightrsasigkey=%cert
left=217.91.93.51
#leftnexthop=217.91.93.51
leftid="C=DE, ST=Dortmund, O=Customer Inc., OU=Test, CN=head"
leftsubnet=192.168.240.0/20
leftcert=/etc/ipsec.d/certs/head-cert-2007.pem
leftsourceip=192.168.255.1
right=%any
keyingtries=0
#disablearrivalcheck=yes
auto=add
compress=no
ike=aes128-sha-modp1536,aes256-sha-modp1536,3des-shamodp1536,3des-
md5-modp1536,3des-md5-modp1024,3des-sha-modp1024
esp=aes128-sha1,aes256-sha1,3des-sha1,3des-md5
```



Digi Application Guide

VPN Tunnel Connection to Strongswan Linux Software VPN Appliance

```
dpdaction=hold
dpddelay=120
dpdtimeout=1200
keylife = 3h
ikelifetime = 2h
### test connections for Customer and Digi
conn "head-user1"
#rightid="00:40:9D:2E:A2:FF@digi.com"
#leftsubnet=192.168.255.0/24
rightid="C=DE, ST=Dortmund, O=Customer Inc., OU=Test, CN=digi1"
rightsubnet=192.168.240.0/24
conn "head-user2"
authby=secret
rightid="00:40:9D:2E:54:83@digi.com"
rightsubnet=192.168.241.0/24
```

/etc/ipsec.secrets:

```
# RCSID $Id: ipsec.secrets.proto,v 1.3.6.1 2005/09/28 13:59:14 paul Exp
$
# This file holds shared secrets or RSA private keys for inter-Pluto
# authentication. See ipsec_pluto(8) manpage, and HTML documentation.
# RSA private key for this host, authenticating it to any other host
# which knows the public part. Suitable public keys, for ipsec.conf,
# DNS,
# or configuration of other implementations, can be extracted
# conveniently
# with "ipsec showhostkey".
: PSK "nBnP524"
```

3. VPN Operation / Debugging

Make sure the firewall is turned off (firestarter or iptables)

- If verbose debug output is needed, go to console 1 and do a

```
tcpdump -i eth0 not port ssh and not port domain and not arp
```

- To monitor VPN exchange messages, go to console 2 and do a

```
tail -f /var/log/auth.log
```

- To start IPsec on the linux side, go to console 3 and do a

```
ipsec start
and
ipsec status
```

(other commands are `ipsec stop` and `ipsec restart`)

- Make sure the Digi device has established mobile connection. From the Digi's local network, do a ping 192.168.255.1

Console 1 & 2 on the linux machine should generate positive output – SA established.