



VPN Tunnel Digi vs Linksys

Configuration of a VPN tunnel between the Digi Connect Port WAN and a Linksys VPN Router

Tunnel initiated by the Linksys Router RV42

1. Configuring the Digi Connect Port WAN VPN

To establish a link to the Digi from the Linksys you need to have a public IP address from the carrier network:

System Summary

Model:	ConnectPort WAN VPN
Ethernet MAC Address:	00:40:9D:32:09:40
Ethernet IP Address:	10.49.2.117
Mobile IP Address:	88.128.13.97

Setup of the Digi ConnectPort WAN VPN tunnel

▼ 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

Apply



Configuration of a VPN tunnel between the Digi Connect Port WAN and a Linksys VPN Router

Tunnel initiated by the Linksys Router RV42

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:32:09:40@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: 10.49.2.0

Subnet Mask: 255.255.255.0

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address: 192.168.101.0

Subnet Mask: 255.255.255.0



Configuration of a VPN tunnel between the Digi Connect Port WAN and a Linksys VPN Router

Tunnel initiated by the Linksys Router RV42

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:

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	AES (256-bit)	MD5	7000 secs	Group 2	Remove
<input type="text" value="Pre-Shared Key"/>	<input type="text" value="DES (64-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="86400"/> secs	<input type="text" value="Group 2"/>	<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	
AES (256-bit)	MD5	3600 secs	Remove
<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>

Connections Management

Virtual Private Network (VPN) Connections

Action	Description	Remote Address	Local Address	Status
<input type="checkbox"/>	Tunnel 1	217.91.93.51	88.128.13.97	Connected



Configuration of a VPN tunnel between the Digi Connect Port WAN and a Linksys VPN Router

Tunnel initiated by the Linksys Router RV42

2. Configuring the Linksys Router

LINKSYS
A Division of Cisco Systems, Inc.

VPN | System Summary | Setup | DHCP | System Management | Port Management | Firewall | VPN

Summary | Gateway to Gateway | Client to Gateway | VPN Client Access | VPN

Edit the Tunnel

Tunnel No. 8
Tunnel Name testdn
Interface WAN1
Enable

Local Group Setup

Local Security Gateway Type IP Only
IP address 217 . 91 . 93 . 51
Local Security Group Type Subnet
IP address 192 . 168 . 101 . 0
Subnet Mask 255 . 255 . 255 . 0

Remote Group Setup

Remote Security Gateway Type IP Only
IP address 88 . 128 . 13 . 97
Remote Security Group Type Subnet
IP address 10 . 49 . 2 . 0
Subnet Mask 255 . 255 . 255 . 0

IPsec Setup

Keying Mode IKE with Preshared key
Phase1 DH Group Group2
Phase1 Encryption AES-256
Phase1 Authentication MD5
Phase1 SA Life Time 7000 seconds
Perfect Forward Secrecy
Phase2 Encryption AES-256
Phase2 Authentication MD5
Phase2 SA Life Time 3600 seconds
Preshared Key secretkey

Advanced +



Configuration of a VPN tunnel between the Digi Connect Port WAN and a Linksys VPN Router

Tunnel initiated by the Linksys Router RV42

Advanced

Advanced -

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm MD5

NetBIOS broadcast

NAT Traversal

Dead Peer Detection (DPD) Interval 10 seconds

Save Settings
Cancel Changes

Press the connect button

8	testdn	Waiting for Connection	AES/MD5	192.168.101.0 255.255.255.0	10.49.2.0 255.255.255.0	88.128.13.97	Connect	Edit
---	--------	------------------------	---------	--------------------------------	----------------------------	--------------	-------------------------	----------------------

Now it's connected

8	testdn	Connected	AES/MD5	192.168.101.0 255.255.255.0	10.49.2.0 255.255.255.0	88.128.13.97	Disconnect	Edit
---	--------	-----------	---------	--------------------------------	----------------------------	--------------	----------------------------	----------------------

System Log

VPN Log
[Refresh](#)
[Clear](#)
[Close](#)

Current Time: Fri Feb 29 16:29:07 2008

Time ▲	Event-Type	Message
Feb 29 16:28:56 2008	VPN Log	[Tunnel Negotiation Info] >>> Initiator Send Aggressive Mode 1st packet
Feb 29 16:28:56 2008	VPN Log	initiating Aggressive Mode #708, connection "ips7"
Feb 29 16:28:56 2008	VPN Log	STATE_AGGR_1: initiate
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] <<< Initiator Received Aggressive Mode 2nd packet
Feb 29 16:28:58 2008	VPN Log	Aggressive mode peer ID is ID_IPV4_ADDR: '88.128.13.97'
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] >>> Initiator send Aggressive Mode 3rd packet
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Aggressive Mode Phase 1 SA Established
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Initiator Cookies = f214 f3fc 4548 80c5
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Responder Cookies = 51b8 6945 a3d 34e0
Feb 29 16:28:58 2008	VPN Log	initiating Quick Mode PSK+TUNNEL+AGGRESSIVE
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] >>> Initiator send Quick Mode 1st packet
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] <<< Initiator Received Quick Mode 2nd packet
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Inbound SPI value = f758a175
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Outbound SPI value = 44c417f9
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] >>> Initiator Send Quick Mode 3rd packet
Feb 29 16:28:58 2008	VPN Log	[Tunnel Negotiation Info] Quick Mode Phase 2 SA Established, IPSec Tunnel Connected