

Setup VPN from Digi ConectPort device using dynamic IP address to Juniper Netscreen 5GT with a static IP address

Environment:

Juniper has a static IP address

DIGI acquires a Dynamic address from mobile provider

Juniper settings

192.168.2.0/24 – Local_Subnet in Trust Address list

192.168.10.0/24 – remote_subnet in Untrust Address list

Peer id: remote@digicom.com

Untrust IP: 66.77.174.69 in route mode

VPN Settings

Gateway: Dynamic IP Address using peer ID of remote@digicom.com

Preshared key of 1234567890

P1 proposal: PRE-G2-3DES-SHA

Aggressive Mode

IKE: Custom security level

Remote gateway: Digi defined in phase 1

P2 proposal: G2-ESP-3DES-SHA

Proxy ID:

Local IP/ Netmask: 192.168.2.0/24

Remote IP/ Netmask: 192.168.10.0/24

Policy: From untrust to trust VPN

Digi ConnectPort settings:

Device address: 192.168.10.1/ 24

VPN IKE Settings:

General Settings

Connection Mode: Aggressive

Diffie-Hellman: Group 2

IKE Settings

Authentication: PreShared Key

Encryption: 3DES (192bit)

Integrity: SHA1

SA Lifetime: 28800 secs

VPN Policy Settings

Description: Digi Remote VPN

Remote VPN Tunnel: 66.77.174.69

VPN Tunnel: ISAKMP

Local Endpoint: Local endpoint is a subnet

Identity

Mobile0

Negotiate tunnel as soon as interface is up

Use the following as the identity: remote@digicom.com

Local Endpoint

IP Address: 192.168.10.0

Subnet Mask: 255.255.255.0

Remote Endpoint

IP Address: 192.168.2.0

Subnet Mask: 255.255.255.0

Preshared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID: 66.77.174.69

Use the following pre-shared key to negotiate IKE security settings: 66.77.174.69

ISAKMP Phase 2 settings

Encryption: 3-DES

Authentication: SHA-1

SA Lifetime: 3600 secs

DIGI Settings

General Security Settings

Connection Mode:

Diffie-Hellman:

Enable Perfect Forward Secrecy (PFS)

Enable Antireplay

Miscellaneous Settings

Suppress SA lifetime during IKE phase 1

Internet Key Exchange (IKE) Security Settings

Use the default policies to negotiate Internet Key Exchange (IKE) security settings

Use the following policies to negotiate Internet Key Exchange (IKE) security settings

Authentication	Encryption	Integrity	SA Lifetime	
Pre-Shared Key	3-DES (192-bit)	SHA1	28800 secs	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="button" value="Add"/>

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:

ISAKMP Phase 2 Policy Settings

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

Encryption	Authentication	SA Lifetime	
3-DES	SHA1	3600 secs	Remove
<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>

Juniper Settings

Untrust

Filter: ALL 0-9 A B C D E F G-I J-L M N O P Q R S T U V W X-Z

Name	IP/Domain Name
Any	0.0.0.0/0
Dial-Up VPN	255.255.255.255/32
Remote_Subnet	192.168.10.0/24

Trust

Filter: ALL 0-9 A B C D E F G-I J-L M N O P Q R S T U V W X-Z

Name	IP/Domain Name
Any	0.0.0.0/0
Dial-Up VPN	255.255.255.255/32
Local_Subnet	192.168.2.0/24

VPNs > AutoKey Advanced > Gateway > Edit

Gateway Name

Security Level Standard Compatible Basic Custom

Remote Gateway Type

- Static IP Address
- Dynamic IP Address
- Dialup User
- Dialup User Group

IP Address/Hostname

Peer ID

User

Group

NOTE: PreShared Key is case sensitive

PreShared Key Use As Seed

Local ID (optional)

Outgoing Interface untrust

OK Cancel Advanced

Security Level

Predefined Standard Compatible Basic
User Defined Custom

Phase 1 Proposal

pre-g2-3des-sha	None
None	None

Mode (Initiator) Main (ID Protection) Aggressive

VPN Name Remote_IKE
Security Level Standard Compatible Basic Custom

Remote Gateway Predefined Digi_Gateway
 Create a Simple Gateway

Gateway Name

Type Static IP
 Dynamic IP

Security Level

Predefined Standard Compatible Basic
User Defined Custom

Phase 2 Proposal

g2-esp-3des-sha / None
 None / None

Replay Protection
Transport Mode (For L2TP-over-IPSec only)

Bind to None
 Tunnel Interface
 Tunnel Zone

Proxy-ID
Local IP / Netmask 192.168.2.0 / 24
Remote IP / Netmask 192.168.10.0 / 24
Service ANY

VPN Group None

VPN Monitor
Source Interface default
Destination IP 0.0.0.0
Optimized
Rekey

Return Cancel



Policies (From All zones To All zones)

List 20 per page

From All zones

To

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action
2	Remote_subnet	Local_subnet	ANY	 

From Trust To Untrust, total policy: 1

CLI Info (note wrappage)

```
set interface trust ip 192.168.2.1/24
set interface untrust ip 66.77.174.69/29
set address "Trust" "Local" 192.168.2.0 255.255.255.0
set address "Untrust" "Remote_Subnet" 192.168.10.0 255.255.255.0
set ike gateway "Digi_Gateway" address 0.0.0.0 id "Remote@digicom" Aggr outgoing-interface "untrust" preshare "XXX" proposal "pre-
g2-3des-sha"
set ike gateway "Digi_Gateway" cert peer-ca all
unset ike gateway "Digi_Gateway" nat-traversal
set vpn "Remote_IKE" gateway "Digi_Gateway" no-replay tunnel idletime 0 proposal "g2-esp-3des-sha"
set policy id 2 name "DIGI_VPN" from "Untrust" to "Trust" "Remote_Subnet" "Local" "ANY" tunnel vpn "Remote_IKE" id 1 log
set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" permit
set vpn "Remote_IKE" proxy-id local-ip 192.168.2.0/24 remote-ip 192.168.10.0/24 "ANY"
```