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@digi.com

Untrust IP: 66.77.174.69 in route mode

VPN Settings

Gateway: Dynamic IP Address using peer ID of remote@digi.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 Checked

Use the following as the identity: remote@digi.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

Pre-Shared Key 🔻

General Security Settings Aggressive 🔻 Connection Mode: Group 2 ▼ Diffie-Hellman: ☑ Enable Perfect Forward Secrecy (PFS) ☐ Enable Antireplay Miscellaneous Settings Suppress SA lifetime during IKE phase 1 Internet Key Exchange (IKE) Security Settings O 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

MD5 ▼

86400

secs

Add

DES (64-bit)

VPN -	Tunnel #1	- Configura						
	Description:	Beltsville						
Remote	VPN Address:	66.77.174.69						
	VPN Tunnel:	ISAKMP						
Local E	Endpoint Type:	Local endp						
Identity	/							
Networ	k Interface: n	nobile0 🔻						
		as soon as inte						
E 110	goddee tariirei	as soon as mice						
Use the following as the identity: remote@digi.com								
C Use the interface IP address								
O Use	the identity o	ertificate X.509						
Local E	ndpoint							
		c from the follow						
	IP Address:	192.168.10.0						
9	Subnet Mask:	255.255.255.0						
	abrice ridoki	200.200.200.0						
Remote	Endpoint							
Tunnel	Network Traffi	to the followin						
	IP Address:	192.168.2.0						
9	Subnet Mask:	255.255.255.0						
	ared Key Settir							
_		ddress, FQDN, o						
Į(66.77.174.69							
Use the	e following pre	-shared key to r						
_	66.77.174.69							
ISAKMP	Phase 2 Polic	y Settings						
Use the		cies to negotial						
	Encryptio							
	3-DES	SHA						
	None	None						

Apply Cancel

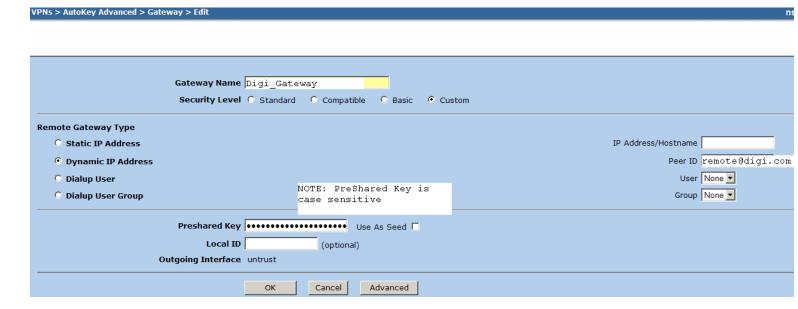
Juniper Settings

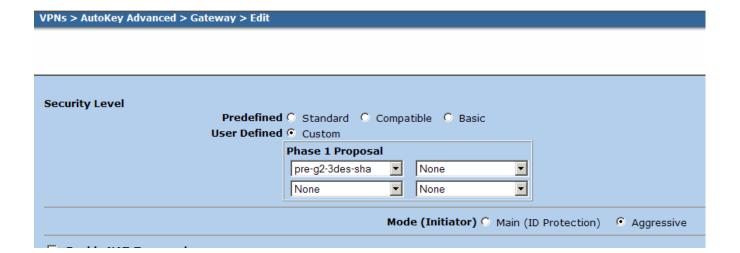


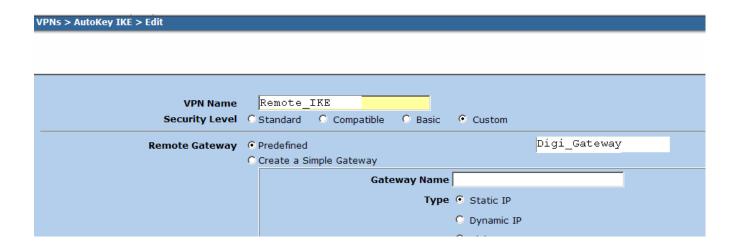
Name	IP/Domain Name		
Any	€ 0.0.0.0/0		
Dial-Up VPN	<u>255.255.255.255/32</u>		
Remote_Subnet	<u>a</u> 192.168.10.0/24		

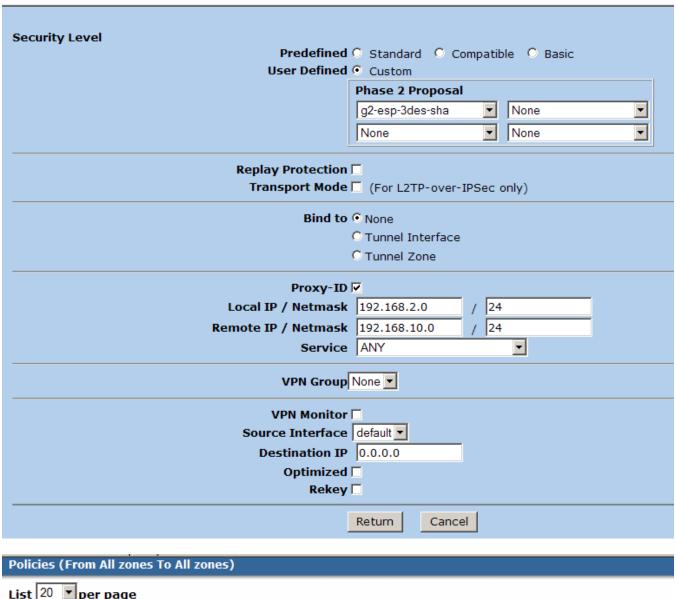
Trust Filter: ALL 0-9 A B C D E F G-I J-L M N O P Q R S T U V W X-Z

Name	IP/Domain Name		
Any	€ 0.0.0.0/0		
Dial-Up VPN	<u>\$\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</u>		
Local_Subnet	<u></u> 192.168.2.0/24		









Policies (From All zones To All zones)					
List 20 per page					
From All zones	То [

From Untrust To Trust, total policy: 1										
ID	Source	Destination	Service	Action						
2	Remote_Subnet	Local_Subnet	ANY	a -						

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@digi.com" Aggr outgoing-interface "untrust" preshare "XXX" proposal "preg2-3des-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" permit
set vpn "Remote_IKE" proxy-id local-ip 192.168.2.0/24 remote-ip 192.168.10.0/24 "ANY"
```