IPSec Site to Site: EPG5000 to EPG600 On EPG600:

Name	HQ	
Connection Type	IPSec •	
Authentication Type	pre-shared key 🔻	
Shared Key	1234567890	
Confirm	1234567890	
Local ID Type	IP Address 🔻	
Local ID	118.167.32.184	Domoto W/
Peer ID type	IP Address V	Remote w
Peer ID	36.225.39.65	
default settings. General SA Net	work Advanced	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal	work Advanced	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange	work Advanced	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group	work Advanced Main Mode T Group 2 T	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption	work Advanced Main Mode T Group 2 T 3DES T	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication	Main Mode Group 2 V 3DES V SHA1 V	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time	Main Mode Group 2 3DES SHA1 (1080-86400 secs)	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time IPSec(Phase 2)Proposa	Main Mode Group 2 3DES SHA1 28800 (1080-86400 secs)	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time IPSec(Phase 2)Proposa Protocol	Main Mode Group 2 SHA1 28800 (1080-86400 secs) ESP	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time IPSec(Phase 2)Proposa Protocol Encryption	Main Mode Group 2 3DES SHA1 28800 (1080-86400 secs)	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time IPSec(Phase 2)Proposa Protocol Encryption Authentication	Main Mode Group 2 3DES SHA1 28800 (1080-86400 secs) ESP 3DES SHA1	Apply Cancel
default settings. General SA Net IKE(Phase 1)Proposal Exchange DH Group Encryption Authentication Life Time IPSec(Phase 2)Proposa Protocol Encryption Authentication Perfect Forward Secrecy	Main Mode Group 2 Group 2 SHA1 Z8800 (1080-86400 secs) I ESP SHA1 SHA1 DES SHA1 C BESP Disable Disable	Apply Cancel

rippiy Guilder

Genera		SA	Network /	Advanced		
Secu	rity Gate	eway Ty	pe IP Ac	Idress 🔻	R	emote WAN IP
Secu	rity Gate	eway	36.22	5.39.65		
Loca	Netwo	ork				
Local	Address	s	192.1	68. 100.1	Local Gat	eway IP
Local	Netmas	sk	255.2	55.255.0		
Rem	ote Net	twork	402.4		Remote Net	work address
Remo	ote Addr	ess	192.10	68.200.0		
Remo	ote Netr	nask	255.2	55.255.0		
4. Use defa	ult set	tings	Notwork	Advanced	Apply	Cancel
Genera	1	SA	Network	Auvanceu		
NAT Deac	Travers I Peer D	al etection	● Ena ● Ena	ble © Disable ble ® Disable	Apply	Cancel
NAT Dead 5. Click "App	Travers I Peer D Dly", a j	al etection profile	• Ena • Ena has been crea	ble © Disable ble ® Disable ated.	Apply	Cancel
NAT Dead 5. Click "App No. Enable	Travers Peer D Dly", a p Name	al etection profile Type	• Ena • Ena has been crea Local Address	ble O Disable ble O Disable ated. Remote Address	Apply s Crypto-suite	Cancel Gateway Select

3.

EPG5000:		
General SA N	letwork Advanced	
Name	to_HQ	
Connection Type	IPSec •	
Authentication Type	pre-shared key 🔻	
Shared Key	1234567890	
Confirm	1234567890	
Local ID Type	IP Address 🔻	Local WAN IP
Local ID	36.225.39.65	
Peer ID type	IP Address V	Remote WAN IP
	440 407 00 404	

2. Use default settings.

IKE(Phase 1)Proposal	
Exchange	Main Mode 🔹
DH Group	Group 2 🔻
Encryption	3DES 🔻
Authentication	SHA1 T
Life Time	28800 (1080-86400 secs)
IPSec(Phase 2)Proposa	al
Protocol	ESP V
Encryption	3DES 🔻
Authentication	SHA1 T
Perfect Forward Secrecy	Enable Isable
DH Group	Group 2 🔻
Life Time	28800 (1080-86400 secs)

3. Use default settings.

Ge	eneral	SA		Network	Adva	anced				
	Security (Gateway	Туре	IP.	Addres	ss 🔻		Rei	mote WAN IF	
	Security (Gateway		118	.167.3	2.184				
L	ocal Ne	twork		di s						
	Local Add	ress		192	.168.2	00.1	-	Local Gatev	vay IP	
1	Local Net	mask		255	.255.2	55.0	1			_
F	Remote	Networ	k					Remote Netwo	ork address	
1	Remote A	ddress		192	.168.1	00.0	1-			
1	Remote N	letmask		255	.255.2	55.0]			
								Apply	Cancel	
4. Gi	eneral	SA		Network	Adv	anced				
0		vorsal				Disable				
	Dead Per	or Detect	ion	© E	nable	Disable Disable				
	Deaure				naple	Isable		Apply	Cancel	
5. Cl	ick "App	oly", a j	orofile	e has bee	n cre	eated.				
No.	Enable	Name	Type	Local Ad	dress	Remote Ad	dress	Crypto-suite	Gateway	Select
1		to_HQ	IPSec	192.168.20	0.0/24	192.168.10	0.0/24	ESP-3DES-SHA1	118.167.32.184	

Now I can see the VPN is on, and can ping the Gateway or Device on the other site.

No.	Name	Type	Gateway/Peer IP address	Transmit Packets	Received Packets	Uptime	Select
1	HQ	IPSec	36.225.39.65	6324747	111622379	00:10:00	
No.	Name	Туре	Gateway/Peer IP ad <mark>d</mark> ress	Transmit Packets	Received Packets	Uptime	Select
1	to_HQ	IPSec	118.167.32.184	23026182	548137	00:00:47	
Pingir Reply Reply Reply Ping s Appro: M	inistrator: CAwin ng 192.168 from 192. from 192. from 192. from 192. statistics ackets: Sen ximate rouu inimum = 6	dows\system3 .100.1 wi 168.100.1 168.100.1 168.100.1 168.100.1 for 192. nt = 4, F nd trip t ms, Maxim	th 32 bytes of data th 32 bytes of data : bytes=32 time=8ms : bytes=32 time=7ms : bytes=32 time=8ms : bytes=32 time=6ms 168.100.1: Received = 4, Lost = :imes in milli-secon um = 8ms, Average =	- • × • • • • • • • • • • • • • • • • •	ministrator: C\windows\system32(cm ing 192.168.200.1 with 3 y from 192.168.200.1: by y from 192.168.200.1: by y from 192.168.200.1: by y from 192.168.200.1: by statistics for 192.168 Packets: Sent = 4, Rece oximate round trip times Minimum = Oms, Maximum =	dexe 32 bytes of ytes=32 time ytes=32 time ytes=32 time vtes=32 time .200.1: ived = 4, Lo s in milli-s = 1ms, Avera	data: =1ms TTL=64 =1ms TTL=64 <1ms TTL=64 <1ms TTL=64 <1ms TTL=64 st = 0 (0% loss econds: ge = 0ms