

## IPSec Site to Site: EPG5000 to EPG600

On EPG600:

1.

General SA Network Advanced

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
Peer ID type	IP Address
Peer ID	36.225.39.65

Local WAN IP  
Remote WAN IP

Apply Cancel

2. Use default settings.

General SA Network Advanced

IKE(Phase 1)Proposal

Exchange	Main Mode
DH Group	Group 2
Encryption	3DES
Authentication	SHA1
Life Time	28800 (1080-86400 secs)

IPSec(Phase 2)Proposal

Protocol	ESP
Encryption	3DES
Authentication	SHA1
Perfect Forward Secrecy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DH Group	Group 2
Life Time	28800 (1080-86400 secs)

Apply Cancel

3.

General SA **Network** Advanced

Security Gateway Type

Security Gateway

Local Network

Local Address

Local Netmask

Remote Network

Remote Address

Remote Netmask

Apply Cancel

The screenshot shows the 'Network' tab of a configuration interface. It contains several input fields for network parameters. Three blue callout boxes with white text point to specific fields: 'Remote WAN IP' points to the 'Security Gateway' field containing '36.225.39.65'; 'Local Gateway IP' points to the 'Local Address' field containing '192.168.100.1'; and 'Remote Network address' points to the 'Remote Address' field containing '192.168.200.0'. The 'Security Gateway Type' is set to 'IP Address'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

4. Use default settings

General SA Network **Advanced**

NAT Traversal  Enable  Disable

Dead Peer Detection  Enable  Disable

Apply Cancel

The screenshot shows the 'Advanced' tab of the configuration interface. It contains two settings: 'NAT Traversal' with 'Enable' selected (radio button), and 'Dead Peer Detection' with 'Disable' selected (radio button). At the bottom right, there are 'Apply' and 'Cancel' buttons.

5. Click "Apply", a profile has been created.

No.	Enable	Name	Type	Local Address	Remote Address	Crypto-suite	Gateway	Select
1	<input checked="" type="checkbox"/>	HQ	IPSec	192.168.100.0/24	192.168.200.0/24	ESP-3DES-SHA1	36.225.39.65	<input type="checkbox"/>

On EPG5000:

1.

General SA Network Advanced

Name	to_HQ
Connection Type	IPSec
Authentication Type	pre-shared key
Shared Key	1234567890
Confirm	1234567890
Local ID Type	IP Address
Local ID	36.225.39.65
Peer ID type	IP Address
Peer ID	118.167.32.184

Local WAN IP

Remote WAN IP

Apply Cancel

2. Use default settings.

General SA Network Advanced

IKE(Phase 1)Proposal

Exchange	Main Mode
DH Group	Group 2
Encryption	3DES
Authentication	SHA1
Life Time	28800 (1080-86400 secs)

IPSec(Phase 2)Proposal

Protocol	ESP
Encryption	3DES
Authentication	SHA1
Perfect Forward Secrecy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DH Group	Group 2
Life Time	28800 (1080-86400 secs)

Apply Cancel

3. Use default settings.

General SA **Network** Advanced

---

Security Gateway Type: IP Address

Security Gateway: 118.167.32.184 Remote WAN IP

Local Network

Local Address: 192.168.200.1 Local Gateway IP

Local Netmask: 255.255.255.0

Remote Network

Remote Address: 192.168.100.0 Remote Network address

Remote Netmask: 255.255.255.0

Apply Cancel

4.

General SA Network **Advanced**

---

NAT Traversal:  Enable  Disable

Dead Peer Detection:  Enable  Disable

Apply Cancel

5. Click "Apply", a profile has been created.

No.	Enable	Name	Type	Local Address	Remote Address	Crypto-suite	Gateway	Select
1	<input checked="" type="checkbox"/>	to_HQ	IPSec	192.168.200.0/24	192.168.100.0/24	ESP-3DES-SHA1	118.167.32.184	<input type="checkbox"/>

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	<input type="checkbox"/>

No.	Name	Type	Gateway/Peer IP address	Transmit Packets	Received Packets	Uptime	Select
1	to_HQ	IPSec	118.167.32.184	23026182	548137	00:00:47	<input type="checkbox"/>

