

NetXGATE IPSec VPN Installation Guide

Release 1.1 Issue 1 June 2020

Disclaimer

Precautions have been taken to ensure accuracy of the information provided in this manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues. NetXGATE reserves the right to revise this documentation and to make changes in content from time to time without obligation to provide notification of such changes. NetXGATE provides this documentation without warranty expressed, implied, statutory, or otherwise and specifically disclaims any warranty of merchantability or fitness for a particular purpose. NetXGATE may make improvements or changes in the IPSec Solution described in this documentation at any time. Product specifications in this manual are provided for the convenience of our customers. They are all correct at the time of publication. NetXGATE reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or functions described here.



NetXGATE IPSec VPN Overview -

NetXGATE IPSec VPN is based on the industry-standard IPsec VPN implementation. It provides a easy-to-setup, secure solution for connecting remote offices and partners through the Internet. Remote office networks can securely connect to your network using site to site VPN connections that enable network-to-network VPN connections.

The maximum number of policies you can add depends on which NetXGATE model you have. The larger models allow more connections.

Planning Site to Site Configurations

You have many options when configuring site to site VPN and can include the following options:

Branch Office (Gateway to Gateway)	A NG firewall is configured to connect to another NG firewall through a VPN tunnel. Or, a NG firewall is configured to connect through IPsec to another manufacturer's firewall.
Hub and Spoke Design	All NG VPN gateways are configured to connect to a central hub, such as a corporate firewall. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a NG Firewall. Note -For Hub and Spoke scenario we suggest NG SSL VPN in place of IPSec where both end having NG Firewall.
Mesh Design	All sites connect to all other sites. All sites must have static IP addresses.

A few other things to note:

• The firewall must have a routable WAN IP address whether it is dynamic or static.

General VPN Configuration

This article describes the steps to configure a Site-to-Site IPsec VPN connection using Pre-shared key as an authentication method for VPN peers. Specific scenarios might be



different . Note that configuring IPsec VPNs for IPv4 and IPv6 are very similar; however, certain VPN features are currently not supported in IPv6

The following settings will be assumed:

IPsec Endpoint Settings

Site	A	Site B				
Name	HQ-BGL Office	Name	Branch Office- London			
Local WAN IP	111.1.100.3	Remote WAN IP	222.1.200.2			
Local LAN Subnet	192.168.100.0/24	Remote LAN Subnet	172.16.100.0/24			



Step 1 : Configuring the IPsec VPN

1-Navigate **Configuration** > **VPN** > Click to **IPSec**.

2-New Template will Open , Click to **Add** – (On Left top Corner), will open one more template.



Now follow the following step .

Note- Many of these settings may be left at their default values.

- I. Enable to service so that the tunnel will be operational.
- II. Name the VPN. The tunnel name cannot include any spaces or upper case .
- III. Description : Enter a description related to the server being configured for your reference.
- IV. IPSec Mode : Default Value Tunnel.
- V. Mention the Local LAN IP want to make a route to branch as same in the Remote side
- VI. Nat Traversal : Default value- Disable
- VII. Local WAN Connection : Select as the 'Static' and mention the WAN-IP | Gateway (Site-A). - Local ID is the optional.
- VIII. Remote WAN IP / FQDN : Mention Remote / Other End WAN IP (Site-B).
- IX. Remote WAN Gateway / FQDN Model : Default Value- Auto detect (You may also Specify the Remote WAN Gateway if confirm).
- X. Local ID : Default value- Optional
- XI. **Pre share key** : Generate and provide to the Remote | Other-Side . Key should be same on both Site.
- XII. IKE mode : Make it as the main and Key Exchange mode as Auto and create the Phase 1 and Phase 2 configure as same for both branch and head office and Enable the Dead Per detection to enable anyone side is sufficient.

The following image shows an example of how to configure the settings:

Network Settings	Tunnel ID Service	Name	Desc	IPSec Mode Local LAN	Subnet Remote LAN Subn	net Local WAN Co
Firewall / NAT	IPSec - VPN: New Tunnel					
IPv6	- Network			Encryption		
Web Security	Service:	Enable	*	IKE Mode:	Main	~
VPN	Name:	vpn_ipsec_bgl_london		Key Exchange Protocol:	Auto	*
SSL-VPN Server	Description:	IPSec_Tunnel-Bangalore	2London	Phase 1 Multi Proposals:	Disable	*
IPSec VPN	IPSec Mode:	Tunnel	~	Phase 1 Encryption:	AES-128-CBC	~
Cisco VPN	Local LAN Subnet:	192.168.100.0/24		Phase 1 Authentication:	SHA1	~
WireGuard Server WireGuard Client				DH Group:	DH2 (DH-1024)	~
PPTP Server				Phase 1 Key Timeout	2600	
GRE Tunnel	Remote LAN Subnet:	172.16.100.0/24		(Seconds):	3000	
High Availability				Phase 2 Multi Proposals:	Disable	*
QoS			1021	Phase 2 Encryption:	AES-128-CBC	~
Alerts / Loos / Reports	NAT Traversat:	Disable	Ť	Phase 2 Authentication:	SHA1	*
-	Local WAN Connection:	Static IP		PFS DH Groupt	Same as Phase 1	~
	Local WAN IP:	111.1.100.3		Phase 2 Key Timeout	18000	
	Local WAN Gateway:	111.1.100.1		(Seconds):	- Calle	
	Local ID:	Optional		Deau Peer Detection (DPD):	Enable	
	Remote WAN IP/FQDN:	222.1.200.2		(Seconds):	30	
	Remote WAN	Auto Detect	*	DPD Timeout (Seconds):	120	
	Gateway/FQDN Mode:	low-		DPD Action:	Hold	~
	Kenole ID;	Optional				



Step 2 : Creating a security policy

The IPsec wizard automatically created a security policy allowing IPsec VPN users to access the internal network under Firewall / NAT > Zone Policy . However, policy must be created if you want to allow users to access the particular Local resource through the VPN Tunnel from Other Site.

Note-Disable the Rule, if any Such VPN 2 LAN rule already created under Firewall Zone Policy.

Now follow the following step.

- 1. To create a New policy, go to Configuration > Firewall /NAT > Filter rules .
- 2. New Template of Filter Rules will Open . Create new by Clicking to 3 Add (On Left top Corner).

Set a policy name that will identify what this policy is used for (in the example, *IPsec-VPN-Internet*).

- 3. Set the **Source Zone** to the **VPN**, Set **Source Address** to the 'IPsec client address range' or **Any**. Similarly **Destination zone** to **LAN**. **Destination Address** to Particular Local LAN resource or **Any** if you want to allow complete LAN.
- 4. Configure any remaining firewall and security options as desired.

The following image shows an example of how to configure the settings:

Configuration	🔾 Add 🔾 Add After 🔾	💿 Add 💿 Add Before 🕜 Modify 🛄 View Details 🕞 Copy 🕥 Details 📰 Actions •							
Network Settings Routing / Load Balance	Filter Rule: New Rule	Filter Rule: New Rule							
Firewall / NAT	- Control Enable:	Enable	~	Action:	Accept	v			
GeolP Filter	Rule Name:	IPSec VPN 2 LAN	Not 1	Protocol:	All				
MAC-IP Binding	Time Restriction [Manage]:	Disable	~	Logi	Enable	*			
Zone Policy Port Forward	Connections per Second:	No Limit							
Source NAT	- Source Zone			Destination Zone					
One-to-One NAT NetMap NAT	Zone:	VPN	*	Zone:	LAN	*			
NAT Helpers	- Source Qualifier			Destination Qualifier					
Show Config IPv6 Web Security	Source Address:	Specify IP	~	Destination Address:	Specify IP	*			
	Source IP:	172.16.100,0/24		Destination IP:	192.168.100.0/24				
/PN Igh Availability	Exclude Source Address:	None	~	Exclude Destination	None				
QoS Management	Source Interface:	Any	~	Address: Destination Interface:	Any	~			
Alerts / Logs / Reports	Save 📀 🗶 C	ancel							



Step 3 : Verifying IPSec-VPN connection state

Once the connection is established, the NetXGATE displays the status of the connection, including the IP address, connection duration, etc.

On the NetXGATE, go to Status > VPN > IPsec and verify that the tunnel State is UP.

Dashboard C	Configuration	S	tatus	Repor	rts Administrat	tion			NG50
Open All Close All	19	Sec Tunn	el Status						
Status		🔀 Restart Selected Tunnel							start Selected Tunnel
System Info	E	State	Tunnel ID	Service	Name	Phase	Desc	Local LAN Subnet	Remote LAN Subnet
IPv6 Network		UP	1	Enable	vpn ipsec bol london	IPSec SA Established	IPSec_Tunnel-Bangalore2London	192.168.100.0/24	172.18.100.0/24
VPN SSL-VPN Servers SSL-VPN Clients SSL-VPN Clients SSL-VPN Clients SSL-VPN Clients SSL-VPN Clients System System User HolSpot Services Updates Traffic Analyzers Troubleshoot		ipsec ipsec	etails: vpn_ip ipsec[26024 ipsec[14646 ipsec[14646	isec_bgl_ (): ESTABI (): INSTAI (): 192.11 (): 19	Iondon LISHED 39 minutes ago LLED, TUNNEL, regid 74 68.100.0/24 === 172.16.	L , 111.1.100.3[111.1.100.3 8, ESP SPIs: c4a1a605_i 100.0/24	9222.1.200.2[222.1.200.2] 9b09048b_o Q Sea	rch Displa	sying records 1 -1 of 1

For Detail IPSec VPN Live Log, Navigate to **Status** >**Troubleshoot**>**System Log** >**VPN** >**IPSec VPN**.