How to establish a VPN tunnel between WMU9000 VPN and NetGear Prosafe VPN Client?



VPN setting Information:

Phase 1 Lifetime: 3600. Phase 2 Lifetime: 3600. Data Encryption/ Authentication: esp-3des-md5. IKE Diffie-Hellman Group: Group 2 (1024-bits). Perfect Forward Secrecy (PFS): Enable. Pre-Shared Key: matrixtonetgear.

Procedure:

WMU 9000 VPN IPSec Setting :

1. Configure the IPSec settings of the WMU 9000 VPN.

DHCP DDNS	Firewall Virtual Server	Static Routes	VPN SIP	Bandwidth Management
IPSec VPN Setting				
*Tunnel Name	toNetGear (1)		
Tunnel Status	Enable 🛩 (2)			
Local Secure Group				
IP Address/Mask	192.168.100.0/24 (3)	A.B.C.D/M>		
Remote Secure Group				
IP Address/Mask		<a.b.c.d m=""></a.b.c.d>		
Remote Secure Gatew	ay (Road Warriors Please	Specify 0.0.0.0)		
*⊙IP Address ○FQDN	0.0.0.0	(4)		
Local ID				
Peer ID				
Encryption	3DES 💉 (5)			
Authentication	MD5 🖌 (6)			
Encapsulation	Tunnel 💉 (7)			
$\operatorname{Key} \operatorname{Management}$				
Key Exchange Method	Auto(IKE)			
PFS	Enable 🖌 (8)	24		
*Pre-Shared Key	matrixtonetgear (<u>n</u>		
Key Litetime	3600 (10) <1200-28	3800>		
	(11)	Change Reset		

Step (1): Type the Tunnel name for *Tunnel name*: [toNetGear]. Step (2): Choose the Tunnel Status: [Enable]. Step (3): Type the Local Secure Subnet IP address and maskbit for *Local Secure Group*: [192.168.1.0/24].

- Step (4): Type the Peer VPN Gateway IP Address for *Remote Secure Gateway*: [0.0.0.0].
- Step (5): Choose the Data Encryption Algorithm: [3DES].
- Step (6): Choose the Data Authentication Algorithm: [MD5].
- Step (7): Choose the mode of the Encapsulation: [Tunnel].
- Step (8): Choose the Perfect Forward Secrecy (PFS): [Enable]
- Step (9): Type the Pre-Shared Key for *Pre-Shared Key*: [matrixtonetgear].
- Step (10): Type the IKE (Phase 1) lifetime for *Key Lifetime*: [3600].
- Step (11): Click "Change" button to setup this IPSec VPN setting.

Now, in the following, we describe the procedure to set up the IPSec VPN in the NetGear Prosafe VPN Client.

1. Add an VPN connection and configure the settings of the VPN connection.

N Security Policy Editor - NETGEAR ProSafe VPI	f Client 📃 🗖 🗙
Ele Edit Options Help	Netreeare Connection Security Secure Non-secure Block Remote Party Identity and Addressing ID Type IP Subnet Subnet: 192.168.100.0 (1) Mask: 255.255.255.0 Protocol All Port All ID Type IP Address (2) 192.168.2.100

Step (1): First, choose the ID Type of the Remote Secure Subnet: [IP Subnet].

Second, type the Remote Secure Subnet IP address for *Subnet*: [192.168.100.0]. Finally, type the Remote Secure Subnet Mask for *Mask*: [255.255.255.0]

- Step (2): First, enable the check box and choose the connect type: [Secure Gateway Tunnel]. Second, choose the ID Type of the Remote VPN Gateway: [IP Address]. Finally, type the ip address of the Remote VPN Gateway: [192.168.2.100].
- 2. Configure the settings of my identity.

N Security Policy Editor - NETGEAR ProSaf	e VPN Client
<u>F</u> ile <u>E</u> dit <u>Options H</u> elp	
Network Security Policy	NETGEAR 💦
My Connections My Identity Security Policy Authentication (Phase 1) Proposal 1 Key Exchange (Phase 2) Proposal 1 Other Connections	My Identity Select Cgrifficate (1) Pre-Shared Key None (2) ID Type Port IP Address (3) All (192.168.2.200) Virtual Adapter Disabled (192.168.2.200) Internet Interface Name [1] 3Com EtherLink XL 10/100 PCI For Completing IP 192.168.2.200

Step (1): Click "Pre-Shared Key" button to enter the Pre-Shared Key. Please refer to the following figure.

Pre-Shared Key
Enter Key (1) Enter Pre-Shared Key (at least 8 characters) This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key". ********** OK Cancel

1.1: Click the "Enter Key" button to enter the Pre-Shared Key: [matrixtonetgear].

Step (2): Choose the Certificate: [None].Step (3): Choose the ID Type of the Local VPN Gateway: [IP Address].And, type the ip address of the Local VPN Gateway: [192.168.2.200].

3. Configure the settings of the Security Policy.

File Edit Options Help	
Network Security Policy	NETGEAR 💦
My Connections toMatrix My Identity Security Policy Authentication (Phase 1) Proposal 1 Proposal 1 Other Connections PFS K En	Policy t Phase 1 Negotiation Mode Main Mode (1) Aggressive Mode Use Manual Keys nable Perfect Forward Secrecy (PFS) (2) ey Group Diffie-Hellman Group 2 v nable Replay Detection

Step (1): Select the Phase 1 Negotiation Mode: [Main Mode].

- Step (2): Enable the *Enable Perfect Forward Secrecy (PFS)* check box. And, choose the PFS Key Group: [Diffie-Hellman Group 2].
- 4. Configure the settings of the Phase 1 (Authentication).

N Security Policy Editor - NETGEAR ProSafe	: VPN Client
<u>File Edit Options H</u> elp	
Network Security Policy	NETGEAR 🔀
My Connections toMatrix My Identity Security Policy Authentication (Phase 1) Proposal 1 Connections Other Connections	Authentication Method and Algorithms Authentication Method Pre-Shared Key (1) Encryption and Data Integrity Algorithms Encrypt Alg Triple DES (2) Hash Alg MD5 (2) Hash Alg MD5 (2) Key Group Diffie-Hellman Group 2 (3)

Step (1): Choose the Authentication Method: [Pre-Shared Key].

Step (2): Configure the Encryption and Data Integrity Algorithms. First, choose the Encrypt Algorithm: [Triple DES]. Second, choose the Hash Algorithm: [MD5]. Next, choose the SA life type: [Seconds]. Finally, type the lifetime of the Phase 1: [3600].
Step (3): Choose the Key Group: [Diffie-Hellman Group 2].

Step (5). Choose the Key Group. [Diffie-fremman Group 2].

5. Configure the settings of the Phase 2 (Key Exchange).

N Security Policy Editor - NETGEAR ProSa	e VPN Client 📃 🗖 🗙				
<u>File E</u> dit <u>Options</u> <u>H</u> elp					
B B B K ■ ★ ↓ Network Security Policy	NETGEAR S				
My Connections toMatrix My Identity Security Policy Authentication (Phase 1) Proposal 1 Key Exchange (Phase 2) Proposal 1 Other Connections	IPSec Protocols SA Life Seconds Seconds (1) Compression None Encapsulation Protocol (ESP) Encrypt Alg Triple DES Hash Alg MD5 Encapsulation Tunnel Authentication Protocol (AH)				
	Hash Alg SHA-1				

Step (1): Choose the SA life type: [Seconds]. And, type the lifetime of the Phase 1: [3600].

Step (2): First, enable the *Encapsulation Protocol (ESP)* check box. Second, choose the Encrypt Algorithm: [Triple DES]. Next, choose the Hash Algorithm: [MD5]. Finally, choose the mode of the encapsulation: [Tunnel].

6. Connect the VPN connection (toMatrix).

		24
	<u>Security Policy Editor</u> Certificate <u>M</u> anager	
	Deactivate Security Policy	
the second second	R <u>e</u> load Security Policy <u>R</u> emove Icon	
	<u>L</u> og Viewer <u>C</u> onnection Monitor	-
	Disconnect	-
My Connections\toMatrix	Connect 🕨	1 Distant
HAS MELTING AND AND AND	<u>H</u> elp	1
📑 未命名1 👩 Hand	About NETGEAR ProSafe VPN Client	下午 06

7. Establish the IPSec VPN Tunnel. Please refer the following figure.

8. The statuses of the IPSec VPN connection.

N Connection Monitor - N	IETGEAR P	ProSafe VPN Clie	nt					
Global Statistics Non-Secured Packets Dropped Packets	10931	Secured Packets Secured Data (KE	5667 Sytes) 971	<u>R</u> eset	<u>C</u> lose Details			
Connection Name Loca	al Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
😋 My Connection 192.1	168.2.200	255.255.255.255	192.168.100.0	255.255.255.0	192.168.2.100	ALL	ALL	ALL