Configuration Guide



Overview

This document describes how to implement IPSec with pre-shared secrets establishing site-to-site VPN tunnel between the D-Link DSR-1000N and the Fortigate100. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 3.00-b0750 of Fortigate100. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.



2

Situation note

Site-to-site VPN could be implemented in an enterprise allows to access and exchange data among more than two geographical sites or offices. Once the site-to-site VPN set up, the clients in the groups of the different located sites are as in the internal networks. As companies may have other gateway appliances which are not D-Link products, this document will be useful when you intend to create IPSec VPN tunnel between DSR and other existing gateway appliance.



IP addresses

DSR WAN: **1.1.1.2/30** DSR LAN: **192.168.10.1/24**

FortiGate100 WAN: **2.2.2.2/30** ForiGate100 LAN: **192.168.1.99/24**

IPSec Parameters

IPSec Mode: Tunnel Mode IPSec Protocol: ESP Phase1 Exchange Mode: Main Phase1 Encryption: 3DES Phase1 Authentication: SHA1 Phase1 Authentication Method: Pre-Shared Key Diffie-Hellman Group: **G2** Phase1 Lifetime: **28800 sec** Phase2 Encryption: **3DES** Phase2 Authentication: **SHA1** Phase2 Lifetime: **3600 sec**

Configuration Step

DSR Settings

 Set up the WAN IP address. Navigate to the Internet Settings > WAN1 Settings > WAN1 Setup.
 Fill in relative information based on the settings of topology. The IP Address of the field of ISP Connection Type is the IP address of external network connecting point which is shown as the point "c" on the topology. Click the button "save settings" to complete WAN IP address settings.



2. Set up the IPSec policy. Navigate to the VPN Settings > IPSec > IPSec Policies.

Press the button "Add" to increase a new policy. In General Section, fill in relative information. The IP address of **Remote Endpoint** refers to the external network connecting point of Fortigate 100 which is shown as the point "f" on the topology. The internal network group, which indicates the IP information on Local Start IP Address, under DSR-1000N allows access to the remote network group, which indicates the IP information on **Remote Start IP Address**, under Fortigate 100 through VPN tunnel.

ชีรส-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard 🕨				2
Internet Settings	IPSEC CONFIGURATION			LOGOUT
Wireless Settings	This name allows user to ad	d/edit VPN (IPsec) policie	s which includes Auto and Mar	nual nolicies
Network Settings	Save Settings	Don't Save Setting		indi ponoso.
DMZ Setup				
VPN Settings	General			
USB Settings	Policy Name:	IPSe	ecl	
VLAN Seturigs	Policy Type:	Aut	o Policy V	
	IPsec Mode:	Tun	nnel Mode 🛛 🔻	
	Select Local Gateway:	Dec	dicated WAN V	
	Remote Endpoint:	IP A	Address V	
		2.2.2	2.2	
	Enable Mode Config:			
	Enable NetBIOS:			
	Enable RollOver:			
	Protocol:	ESP		
	Enable DHCP:			
	Local IP:	Sub	onet 🔻	
	Local Start IP Address:	192.	168.10.0	
	Local End IP Address:			
	Local Subnet Mask:	255.	255.255.0	
	Remote IP:	Sub	met 🔻	
	Remote Start IP Addres	ss: [192.	168.1.0	
	Remote End IP Addres	s:		
	Remote Subnet Mask:	255.	255.255.0	_

In Phase 1 Section, fill in relative information. Please notice that the **Pre-shared Key** must be as same as the pre-shared key which will be inserted on Fortigate 100 on the later step.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both V
Nat Traversal:	
On:	۲
Off:	0
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP V
Local Identifier:	
Remote Identifier Type:	Remote Wan IP 🔻
Remote Identifier:	
Encryption Algorithm:	3DES V
Key Length:	
Authentication Algorithm:	SHA-1 V
Authentication Method:	Pre-shared key
Pre-shared key:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None 🔻
Authentication Type:	User Database
Username:	
Password:	

In Phase 2 Section, fill in relative information.

hase2-(Manual Policy Parameters	3)
SPI-Incoming:	
SPI-Outgoing:	
Encryption Algorithm:	DES
Key Length:	
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1
Key-In:	
Key-Out:	
hase2-(Auto Policy Parameters)	
SA Lifetime:	Seconds V
Encryption Algorithm:	3DES V
Key Length:	
Integrity Algorithm:	SHA-1 V
PFS Key Group:	DH Group 1 (768 bit)

Click the button "**save settings**" to complete IPSec Policy settings.

3. Check the VPN status. Navigate to the Status > Active VPNs.

The activity will be shown on the list while the tunnel is established with the other side.

DSR-1000N	SETUP		ADVA	NCED	TOOLS	STATUS		
Device Info		Operation succeeded The page will auto-refresh in 10 seconds						
Traffic Monitor	ACTIVE VPN					LOGOUT		
Active Sessions Active RunTime	This page disp	This page displays the active VPN connections, IPSEC as well as SSL.						
Wireless Clients	Active IPsec S	As	18	()		-111 - V		
LAN Clients	Policy Name	Endpoint	tx (KB)	tx (Packets)	State	Action		
Active VPNs	IPSec	2.2.2.2	0.00	0	IPsec SA Not Established	Connect		
	Active SSL VF	N Connect	tions					
	User Name	IP Address	s Local	PPP Interface	Peer PPP Interface IP	Connect Status		
		Poll Inte	rval: 10	(Seconds)	Start Stop			

FortiGate Settings

1. Set up the WAN IP address, Navigate to the System > Network. Click button "edit".

FortiGr	are. 100				C	H () &
WEB CONFIG	Interface	Zone Options				
Status	Create New				[<u>Column Se</u>	ttings]
Network	Name	IP/Netmask	Access	Administrative Status	Link Status	1000
DHCP	dmz	10.10.10.1 / 255.255.255.0	HTTPS,PING	0	0	2
Config	external	2.2.2.2 / 255.255.255.252	PING	0	0	2
Admin	internal	192.168.1.99 / 255.255.255.0	HTTP,HTTPS,PING	0	0	2
Maintenance Router Firewall VPN User AntiVirus Intrusion Protectio Web Filter AntiSpam						

Edit IP Address with following information. The **IP/Netmask** of Interface tab is the IP address and Netmask of external network connecting point which is shown as the point "f" on the topology.

📰 Гоятібате	≡. 100	P 🖬 🛛 🗎
WEB CONFIG	nterface Zone Options	
- System		
Status	Edit Interface	
Network	Name external (00:09:0F:02:02:26)	
Config	Alias	
Admin	Link Status Down	
Certificates	Addressing mode	
Maintenance	Manual DHCP PPPoE	
Router	IP/Netmask: 2.2.2.2/255.255.255.252	
Firewall	DDNS Enable	
VPN	Ping Server Enable	
Lieor	Administrative Access HTTPS GPING HTTP	
	SSH SNMP TELNET	
AntiVirus	MTU Override default MTU value (1500). (bytes)	
Intrusion Protectio	Secondary ID Address	- I I I I
Web Filter		÷.
AntiSpam	Description (63 characters)	v

2. Set up the default gateway. Navigate to Router > Static. Press the button "Create New". Fill in relative information as below.

	are. 100			- 6 6 6
System	Static Route	Policy Route		
- Router			Edit Static Route	
Static		Destination IP/Mask	0.0.0/0.0.0	
Dynamic Monitor		Device	external 🔻	
Firewall		Gateway	2.2.2.1	
VPN		Distance	10 (1-255)	
User		(OK Cancel	
AntiVirus	<u></u>			

3. Set up the IPSec Tunnel, go to the VPN > IPSec > Auto Key (IKE).

Press the button "**Create Phase1**". Fill in Name, IP Address and Pre-share key. The **IP Address** under Remote Gateway is the IP address of external network connecting point of DSR-1000N which is shown as the point "**c**" on the topology. Insert the **Pre-shared Key** which is as same as the one put in DSR-1000N in the previous step.

8	р овті6	ATE. 100			- 20 1
s Sy	ystem	Auto Key (IKE)	Manual Key Concentr	ator Monitor	
R	outer			Edit Phase 1	
FI	irewall		Name	IPSec1	
~ VI	PN		Remote Gateway	Static IP Address 🔻	
PF SS	SEC PTP SL		IP Address Local Interface	external V	
U	ser		Mode Authentication Method	Aggressive Main (ID protection) Preshared Key	
A	ntiVirus		Pre-shared Key	••••••	
w	/eb Filter		Peer Options	Accept any peer ID	
A	ntiSpam		Advanced	(XAUTH, NAT Traversal, DPD)	
IN	I, P2P & VolP			OK Cancel	
Lo	og&Report				

🎇 Роктіби	are. 100	- 20 1
WEB CONFIG	Auto Key (IKE) Manual Key Concentrator Monitor	
System	Advanced XAUTH, NAT Traversal, DPD)	A
Router	Enable IPSec Interface Mode	
Firewall	Local Gateway IP 💿 Main Interface IP	
- VPN	Specify 0.0.0.0	
IPSEC	P1 Proposal	
PPTP	1 - Encryption 3DES V Authentication SHA1 V	
User		h
Aptil/inue	Keylife 28800 (120-172800 seconds)	
	Local ID (optional)	
	XAUTH O Disable Enable as Client Enable as Server	
Web Filter	NAT Traversal 🥥 Enable	
AntiSpam	Keepalive Frequency 10 (10-900 seconds)	
IM, P2P & VoIP	Dead Peer Detection 🥥 Enable	
Log&Report	OK Cancel	

Press the button "**Advanced**". Configure the setting as below.

Navigate to VPN > IPSec > Auto Key (IKE). Press the button "**Create Phase2**" and configure below relative information.

П Ровті Б	ere. 100	■ 2 8
System	5 Auto Key (IKE) Manual Key Concentrator Monitor	
Router	Edit Phase 2	
- VPN	Phase 1 [IPSec] 7	
PPTP SSL	P2 Proposal 1- Encryption: 3DES V Authentication: SHA1 V	
User	2-Encryption: 3DES V Authentication: MD5 V E	
Antivirus Intrusion Protection	Enable perfect forward secrecy(PFS).	
Web Filter	Keyffe: Seconds v 3600 (Seconds) 5120 (KBytes)	
IM, P2P & VoIP	Quick Mode Selector Source address 192.168.1.0/24	
Log&Report	Source port Destination address 192.168.10.0/24	
	Destination port 0	
	OK Cancel	•

4. Set up Firewall Policy. Navigate to Firewall > Policy. Press button "**Create New**" and configure the settings as below.

📰 FoeriGeri	≡. 100			- 20 2
WEB CONFIG	Policy			
System				1
Router		Edit Policy		
- Firewall	Source Interface/Zone	[internal]	1	
Policy	Source Andrees	IDSec Local Net	Multiple	
Address	Destination Interface/Zone		mouple	
Service	Destination Interface/2 one	UDDer Denste Met	All Martin	
Virtual IP	Destination Address	IPSec_Remote_Net V	Multiple	
Protection Profile	Schedule	always V		
VPN	Service	ANY	Multiple	
User	Action	IPSEC V		
AntiVirus	VON Turnel	Incest		
Intrusion		Indexed NAT	<u> </u>	
Protection	Allow outbound			
Web Filter		Cobband fert		
AntiSpam	Protection Profile	unfittered 🗸		
IM, P2P & VolP	😡 Log Allowed Traffic			
Log&Report	Traffic Shaping			
	Comments (maximum 63)	characters)		

5. Set up the Firewall Policy. Navigate to the Firewall > Policy. Press the button "**Create New**" and configure settings as below.

	ATE. 100	and the second				- 4 0 8
	Policy					
System						
Router			Edit Policy			
+ Firewall		Source Interface/Zone	Internal			
Policy		Source Address	all	7	Multiple	
Service		Destination Interface/Zone	external			
Schedule		Destination Address	all	Ŧ	Multiple	
Virtual IP Protection Profile		Schedule	always	٧		
VPN		Service	ANY	V	Multiple	
		Action	ACCEPT	V		
User						
AntiVirus		MAT NAT	Dynamic IP Pool			
Intrusion Protection			Poed Port			
Web Filter		Protection Profile				
AntiSpam		Solution Contraction Contraction				
IM, P2P & VolP		Authentication				
LoosBeport		Traffic Shaping				
		User Authentication Dis	sclaimer			
		Redirect URL				
		Comments (maximum 63 c	haracters)	-		
		E				
		_	OK Cancel			

6. Check the IPSec status. Navigate to the VPN > IPSec > Monitor.

	EGATIGATE. 100								PHOR
	WEB CONFIC	;							
	Svetem	Auto Key	(IKE) Manual Key	Concentrator	Monitor				
1	System	Type All V [Clear All Filters]						M 4 1	/1 > >
	Router	V Name	🝸 Туре	Remote Gateway	Remote Port	Timeout	Proxy ID Source	Proxy ID Destination	T Status
	Firewall	IPSec1	Static IP or Dynamic DNS	1.1.1.2	0	0	192.168.1.0/24	192.168.10.0/24	O Bring Up
	VDN								
4	IDEEC								
1	PPTP								
	SSL								
N.	User								
1	AntiVirus								
	Intrusion Protection								
J.	Web Filter								
	AntiConn								
1	Antispam								
	IM, P2P & VoIP								
	Log&Report								



Visit our website for more information www.dlink.com

D-Link, D-Link logo, D-Link sub brand logos and D-Link product trademarks are trademarks or registered trademarks of D-Link Corporation and its subsidiaries. All other third party marks mentioned herein are trademarks of the respective owners.

Copyright © 2011 D-Link Corporation. All Rights Reserved.