

# Configuration Guide



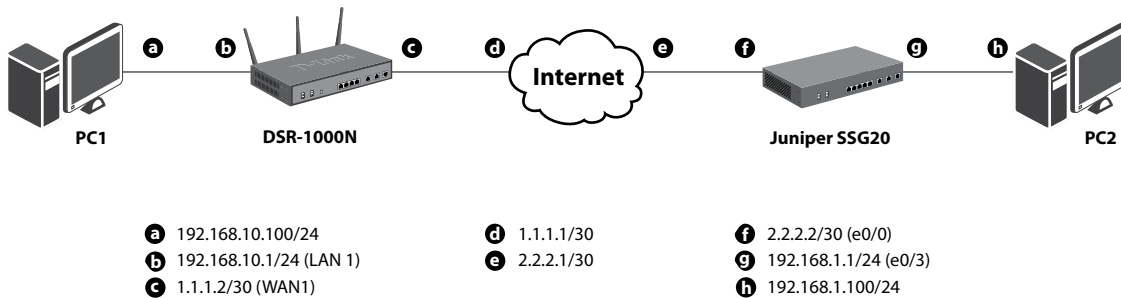
How to set up the IPSec site-to-site Tunnel between the D-Link DSR Router and the Juniper Firewall

## 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 Juniper SSG20. The screenshots in this document is from firmware version 1.03B12 of DSR-1000N and firmware version 6.2.0r 2.0 of Juniper SSG20. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

## 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**

Juniper\_SSG20 Untrust\_Zone(e0/0): **2.2.2.2/30**

Juniper\_SSG20 Trust\_Zone(e0/3): **192.168.1.1/24**

### 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

1. 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.

The screenshot displays the WAN1 Setup configuration page. On the left is a navigation menu with options: Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled 'WAN1 SETUP' and includes a 'LOGOUT' link. A descriptive paragraph states: 'This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, Account Information etc. This information is usually provided by your ISP or network administrator.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'. The configuration is organized into three sections: 'ISP Connection Type' with a dropdown set to 'Static IP' and input fields for IP Address (1.1.1.2), IP Subnet Mask (255.255.255.252), and Gateway IP Address (1.1.1.1); 'Domain Name System (DNS) Servers' with input fields for Primary DNS Server (168.95.1.1) and Secondary DNS Server (8.8.8.8); and 'MAC Address' with a dropdown set to 'Use Default Address' and a text field for MAC Address (00:00:00:00:00:00).

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 Juniper SSG20 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 Juniper SSG20 through VPN tunnel.

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS
Wizard	IPSEC CONFIGURATION <span>LOGOUT</span>			
Internet Settings	This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.			
Wireless Settings	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Network Settings	<b>General</b>			
DMZ Setup	Policy Name: <input type="text" value="IPSec1"/>			
VPN Settings	Policy Type: <input type="button" value="Auto Policy"/> ▼			
USB Settings	IPsec Mode: <input type="button" value="Tunnel Mode"/> ▼			
VLAN Settings	Select Local Gateway: <input type="button" value="Dedicated WAN"/> ▼			
	Remote Endpoint: <input type="button" value="IP Address"/> ▼			
	<input type="text" value="2.2.2.2"/>			
	Enable Mode Config: <input type="checkbox"/>			
	Enable NetBIOS: <input type="checkbox"/>			
	Enable RollOver: <input type="checkbox"/>			
	Protocol: <input type="button" value="ESP"/> ▼			
	Enable DHCP: <input type="checkbox"/>			
	Local IP: <input type="button" value="Subnet"/> ▼			
	Local Start IP Address: <input type="text" value="192.168.10.0"/>			
	Local End IP Address: <input type="text"/>			
	Local Subnet Mask: <input type="text" value="255.255.255.0"/>			
	Remote IP: <input type="button" value="Subnet"/> ▼			
	Remote Start IP Address: <input type="text" value="192.168.1.0"/>			
	Remote End IP Address: <input type="text"/>			
	Remote Subnet Mask: <input type="text" value="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 Juniper SSG20 on the later step.

Phase1(IKE SA Parameters)	
Exchange Mode:	Main ▼
Direction / Type:	Both ▼
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP ▼
Local Identifier:	
Remote Identifier Type:	Remote Wan IP ▼
Remote Identifier:	
Encryption Algorithm:	3DES ▼
Key Length:	
Authentication Algorithm:	SHA-1 ▼
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:	<input type="checkbox"/>
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.

**Phase2-(Manual Policy Parameters)**

**SPI-Incoming:**

**SPI-Outgoing:**

**Encryption Algorithm:**

**Key Length:**

**Key-In:**

**Key-Out:**

**Integrity Algorithm:**

**Key-In:**

**Key-Out:**

---

**Phase2-(Auto Policy Parameters)**

**SA Lifetime:**

**Encryption Algorithm:**

**Key Length:**

**Integrity Algorithm:**

**PFS Key Group:**

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	ADVANCED	TOOLS	STATUS												
<ul style="list-style-type: none"> <li>Device Info ▶</li> <li>Logs ▶</li> <li>Traffic Monitor ▶</li> <li>Active Sessions</li> <li>Active RunTime Sessions</li> <li>Wireless Clients</li> <li>LAN Clients</li> <li>Active VPNs</li> </ul>	<p style="color: red; font-weight: bold;">Operation succeeded</p> <p style="color: red; font-size: small;">The page will auto-refresh in 10 seconds</p>															
<b>ACTIVE VPN</b>				<b>LOGOUT</b>												
This page displays the active VPN connections, IPSEC as well as SSL.																
<b>Active IPsec SAs</b>																
<table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr style="background-color: #f2f2f2;"> <th>Policy Name</th> <th>Endpoint</th> <th>tx ( KB )</th> <th>tx ( Packets )</th> <th>State</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>IPsec</td> <td>2.2.2.2</td> <td>0.00</td> <td>0</td> <td>IPsec SA Not Established</td> <td style="text-align: center;"><input type="button" value="Connect"/></td> </tr> </tbody> </table>					Policy Name	Endpoint	tx ( KB )	tx ( Packets )	State	Action	IPsec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>
Policy Name	Endpoint	tx ( KB )	tx ( Packets )	State	Action											
IPsec	2.2.2.2	0.00	0	IPsec SA Not Established	<input type="button" value="Connect"/>											
<b>Active SSL VPN Connections</b>																
<table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr style="background-color: #f2f2f2;"> <th>User Name</th> <th>IP Address</th> <th>Local PPP Interface</th> <th>Peer PPP Interface IP</th> <th>Connect Status</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="height: 20px;"> </td> </tr> </tbody> </table>					User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status							
User Name	IP Address	Local PPP Interface	Peer PPP Interface IP	Connect Status												
<p style="text-align: center;"><b>Poll Interval:</b> <input type="text" value="10"/> (Seconds) <input type="button" value="Start"/> <input type="button" value="Stop"/></p>																

## Juniper\_SSG20 Settings

1. Set up the Untrust\_Zone and Trust\_Zone IP addresses. Navigate to the **Network > Interfaces > List**. Click **"Edit"**.

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/2				Down	-	<a href="#">Edit</a>
ethernet0/3				Up	-	<a href="#">Edit</a>
ethernet0/4				Down	-	<a href="#">Edit</a>
bgroup1	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup2	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
ethernet0/0	2.2.2.2/30	Untrust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/1	172.16.1.1/24	DMZ	Layer3	Down	-	<a href="#">Edit</a>
serial0/0	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
tunnel.1	unnumbered	Trust	Tunnel	Ready	-	<a href="#">Edit</a>
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	<a href="#">Edit</a>

Configure **Untrust\_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of external network connecting point which is shown as the point "f" on the topology. Click the button **"OK"** to complete this setting.

Interface: ethernet0/0 (IP/Netmask: 2.2.2.2/30)

Properties: Basic | Policy | DHCP | VPN | IDMP | Monitor | 802.1X | IRDP

Interface Name: ethernet0/0 0014.6e6.70d0

Zone Name: **Untrust**

Obtain IP using DHCP  
 Obtain IP using PPPoE  
 **Static IP**

Automatic updates DHCP server parameters  
 Create new pppoe setting

IP Address / Netmask: **2.2.2.2 / 30**  Manageable  
 Manage IP #: **2.2.2.2 0014.6e6.70d0**

Interface Mode:  NAT  Route

Block Intra-Subnet Traffic:

Service Options

Management Services:  Web UI  Telnet  SSH

SNMP  SSL

Other Services:  Ping  Path MTU (PMTU)  Ident-radius

Maximum Transfer Unit (MTU) Admin MTU:  bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

NTP Server:

WebAuth:  IP Address:   SSL Only

G-ARP:

Traffic Bandwidth: Egress:  kbps  
Ingress:  kbps

VRRP:

OK Apply Cancel

Configure **Trust\_Zone** with relative information as below. The **IP Address/ Netmask** of Basic tab is the IP address of internal network connecting point which is shown as the point “g” on the topology. Click the button “OK” to complete this setting.

Network > Interfaces > Edit

Interface: bgroup9 (IP/Netmask: 192.168.1.1/24)

Properties: Basic | Bind Port | MID | DIP | VIP | Secondary IP | ICMP | Monitor | ERDP

Interface Name: bgroup9 0014.f6e6.70c9

Zone Name: Trust

Obtain IP using DHCP  Automatic update DHCP server parameters

Obtain IP using PPPoE  None

**Static IP**  IP Address / Netmask: 192.168.1.1 / 24  Manageable

Manage IP: 192.168.1.1 0014.f6e6.70c9

Interface Mode:  NAT  Route

Block Intra-Subnet Traffic:

Service Options

Management Services:  Web UI  Telnet  SSH

SSL  SshRP

Other Services:  Ping  Path MTU (IPv4)  Ident-reset

Maximum Transfer Unit (MTU): Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

NTP Server:

WebAuth:  IP Address: 0.0.0.0  SSL Only

G-ARP:

Traffic Bandwidth: Egress: Maximum Bandwidth: 0 Kbps

Ingress: Maximum Bandwidth: 0 Kbps

2. Add a Tunnel Interface. Navigate to the **Network > Interfaces > List**. Select “**Tunnel IF**” from scroll down menu. Press the button “**New**” to increase a new tunnel interface.

Network > Interfaces (List)

List: 20 per page

List: ALL(9) Interfaces

Tunnel IF

Name	IP / Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.1.1/24	Trust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/2				Down	-	<a href="#">Edit</a>
ethernet0/3				Down	-	<a href="#">Edit</a>
ethernet0/4				Up	-	<a href="#">Edit</a>
bgroup1	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup2	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
ethernet0/0	2.2.2.2/30	Untrust	Layer3	Down	-	<a href="#">Edit</a>
ethernet0/1	172.16.1.1/24	DMZ	Layer3	Down	-	<a href="#">Edit</a>
serial0/0	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
tunnel.1	unnumbered	Trust	Tunnel	Down	-	<a href="#">Edit</a>
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	<a href="#">Edit</a>



Configure relative settings as below.

Network > Interfaces > Edit ssg20 ?

Interface: tunnel.1 (IP/Netmask: 0.0.0.0/0)

Properties: [Basic](#) [MP](#) [DP](#) [VP](#) [KOMP](#) [NMTB](#) [Tunnel](#)

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Fixed IP

IP Address / Netmask:  /

Unnumbered

Interface: ethernet0/0 (trust-vr)

Maximum Transfer Unit(MTU) Admin MTU:  Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy:

Traffic Bandwidth

Egress	Maximum Bandwidth	<input type="text" value="0"/> Kbps
Ingress	Guaranteed Bandwidth	<input type="text" value="0"/> Kbps
	Maximum Bandwidth	<input type="text" value="0"/> Kbps

NHRP Enable:

3. Add an IPsec Remote Gateway. Navigate to the [VPNs > AutoKey Advanced > Gateway](#). Press the button **"New"** and fill in relative information as below.

VPNs > AutoKey Advanced > Gateway > Edit ssg20 ?

Gateway Name: DSR

Version:  IKEv1  IKEv2

Remote Gateway

Static IP Address IP Address/Hostname: 1.1.1.2

Dynamic IP Address Peer ID:

Dialup User User:

Dialup User Group Group:

ACVPN - Dynamic Local ID:

ACVPN - Profile

Press the button **“Advanced”** for preshared key setting. Fill in relative information as below. Insert the Pre-shared Key which is as same as the one put in DSR-1000N in the previous step.

VPN > AutoKey Advanced > Gateway > Edit

SSG20

Juniper NETWORKS

Home

Configuration

Network

Security

Policy

VPNs

AutoKey IKE

AutoKey Advanced

Gateway

P1 Proposal

P2 Proposal

XAuth Setting

VPN Groups

Manual Key

L2TP

Monitor Status

Objects

Reports

Wizards

Help

Logout

IKEv2 Auth Method

Self: None

Peer: None

Preshared Key: [Redacted]

Local ID: [optional]

Outgoing Interface: ethernet0/0

Security Level

Predefined: Standard, Compatible, Basic

User Defined: Custom

Phase 1 Proposal

pre-g2-3des-sha, pre-g2-aes128-sha

Mode (Initiator): Main (ID Protection), Aggressive

Enable NAT-Traversal

UDP Checksum

Keepalive Frequency: 0 Seconds (0-300)

Peer Status Detection

Heartbeat: Hello 0 Seconds (1-3600, 0: disable)

4. Create a new VPN tunnel. Navigate to **VPNs > AutoKey IKE**. Press the button **“New”**.

VPN > AutoKey Advanced > Gateway

SSG20

Juniper NETWORKS

Date/Time

Update

Admin

Auth

Intranet Auth

Report Settings

Network

Binding

DNS

Zones

Interfaces

List

Backup

DHCP

802.1X

Routing

PPP

Security

Policy

VPNs

AutoKey IKE

AutoKey Advanced

Gateway

P1 Proposal

P2 Proposal

XAuth Settings

VPN Groups

Manual Key

L2TP

List 20 peer page

New

Name	Peer Type	Address / ID / User Group	Local ID	Security Level	Configure
DSR	Static	1.1.1.2	-	Custom	Edit Auth +

Fill in relative information as below.

VPN Name: ipsec\_1

Remote Gateway: Predefined DSR

Gateway Name: [Empty]

Version: IKEv1

Type: Static IP

Outgoing Interface: ethernet0/0

Security Level: Standard

Advanced

Press the button "**Advanced**" and configure settings as below. The internal network group, which is indicates the IP information on **Local IP/ Netmask**, under Juniper SSG20 allows access to the remote network group, which indicates the IP information on Remote **IP/ Netmask**, under DSR-1000N through VPN tunnel.

Predefined: Standard  Compatible Basic

User Defined: Custom

Phase 2 Proposal

Local IP / Netmask: 192.168.1.0 / 24

Remote IP / Netmask: 192.168.10.0 / 24

Service: ANY

Bind to: Tunnel Interface tunnel.1

5. Create the Routings. Navigate to **Network > Routing > Routing Entries**.

Select **"trust-vr"** from the drop down menu on the top and left corner. Press the button **"New"**.

The screenshot shows the Juniper NCU interface for configuring routing entries. The left sidebar shows the navigation tree with 'Routing' selected. The main area displays a table of routing entries for the 'trust-vr' virtual router. The table has columns for IP/Netmask, Gateway, Interface, Protocol, Preference, Metric, Vsys, Description, and Configure. Below the table is a legend for route types and protocols.

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	2.2.2.0/30		ethernet0/0	C			Root		-
*	2.2.2.2/32		ethernet0/0	H			Root		-
*	0.0.0.0/0	2.2.2.1	ethernet0/0	C		1	Root		-
	172.16.1.0/24		ethernet0/1	C			Root		-
	172.16.1.1/32		ethernet0/1	H			Root		-
*	192.168.1.0/24		bgrou0	C			Root		-
*	192.168.1.1/32		bgrou0	H			Root		-
*	192.168.10.0/24		tunnel.1	S	20	1	Root		<a href="#">Remove</a>

Legend:  
 \* Active route    C Connected    I Imported    eB EBGP    O OSPF    E1 OSPF external type 1    H Host Route  
 P Permanent    S Static    A Auto-Exported    iB IBGP    R RIP    E2 OSPF external type 2  
 D Dynamic    N NHRP

Fill in relative information as below.

The screenshot shows the 'Configuration' page for a new routing entry. The 'Virtual Router Name' is 'trust-vr'. The 'IP Address/Netmask' is '192.168.10.0 / 24'. The 'Next Hop' is set to 'Virtual Router' with 'untrust-vr' selected. The 'Gateway' radio button is selected, and the 'Interface' is 'tunnel.1'. The 'Gateway IP Address' is '0.0.0.0'. The 'Permanent' checkbox is unchecked, and the 'Tag' is '0'. The 'Metric' is '1' and the 'Preference' is '20'. There is a 'Description' field which is currently empty. 'OK' and 'Cancel' buttons are at the bottom.

6. Set up the Policies. Navigate to **Policy > Policies**. Create the first rule. Select **“Trust”** and **“Untrust”** in the **“From”** and **“To”** drop down menus respectively. Press the button **“New”**.

Policy > Policies (From All zones To All zones) ssg20

List 20 per page

From Trust To Untrust Go New

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	Permit		Edit Clone Remove	<input checked="" type="checkbox"/>	Move

Fill in relative information as below.

Name (optional) To\_DSR

Source Address  New Address 192.168.1.0 / 24  Address Book Entry Any Multiple

Destination Address  New Address 192.168.10.0 / 24  Address Book Entry Any Multiple

Service ANY Multiple

Application None

---

WEB Filtering

Action Permit Deep Inspection

Antivirus Profile None

Antispam enable

Tunnel VPN None

Modify matching bidirectional VPN policy

L2TP None

Create the second rule. Select **"Untrust"** and **"Trust"** in the **"From"** and **"To"** drop down menus respectively. Press the button **"New"**.

List **20** per page

From **Untrust** To **Trust** Go **New**

From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	✔		<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a>	<input checked="" type="checkbox"/>	↕ ⋮
2	192.168.1.0/24	192.168.10.0/24	ANY	✔		<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a>	<input checked="" type="checkbox"/>	↕ ⋮

Fill in relative information as below.

**Name (optional)** from\_DSR

**Source Address**  
 New Address 192.168.10.0 / 24  
 Address Book Entry 192.168.10.0/24 Multiple

**Destination Address**  
 New Address 192.168.1.0 / 24  
 Address Book Entry 192.168.1.0/24 Multiple

**Service** ANY Multiple

**Application** None

---

WEB Filtering

**Action** Permit Deep Inspection

**Antivirus Profile** None

**Antispam enable**

**Tunnel** VPN None

Modify matching bidirectional VPN policy

**L2TP** None

7. Check VPN status. Navigate to **VPNs > Monitor Status**.

The screenshot displays the Juniper Networks SSG20 VPN Monitor Status page. The page title is "VPNs > Monitor Status" and the user is logged in as "sbg20". The left sidebar shows the navigation menu with "VPNs" and "Monitor Status" highlighted. The main content area shows a table with one entry for "ipsec\_1".

VPN Name	SA ID	Policy ID	Peer Gateway IP	Type	SA Status	Link
ipsec_1	00000001	-1/-1	1.1.1.2	AutoIKE	Active	Off

**D-Link<sup>®</sup>**

Visit our website for more information  
[www.dlink.com](http://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.**