

Application Note

# Configuring a Lan-to-Lan VPN with SSG5 and Check Point Appliance Safe@Office 500

---

Version 1.0

January 2008



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

## Contents

Introduction .....	3
Configuration Steps .....	4
Corporate Site Configuration(SSG5) Example .....	5
Remote Site Configuration (Checkpoint Appliance)Example.....	8
Verifying Functionality.....	16

## Introduction

It becomes occasionally necessary to create an IPSec VPN tunnel to a non-Juniper firewall. This article provides a general out line of the necessary configurations that should be performed in order to successfully establish an IPSec VPN tunnel between a Juniper firewall device and a Checkpoint firewall appliance.

## Included Platforms and Software Versions

This document applies to the following Juniper devices running ScreenOS 5.4.0 or later -

- All NetScreen platforms including 5GT,25, 50, 204, 208, 500, 5200 and 5400
- All ISG platforms including 1000 and 2000
- All SSG platforms including 5, 20, 140, 320M, 350M, 520/520M and 550/550M

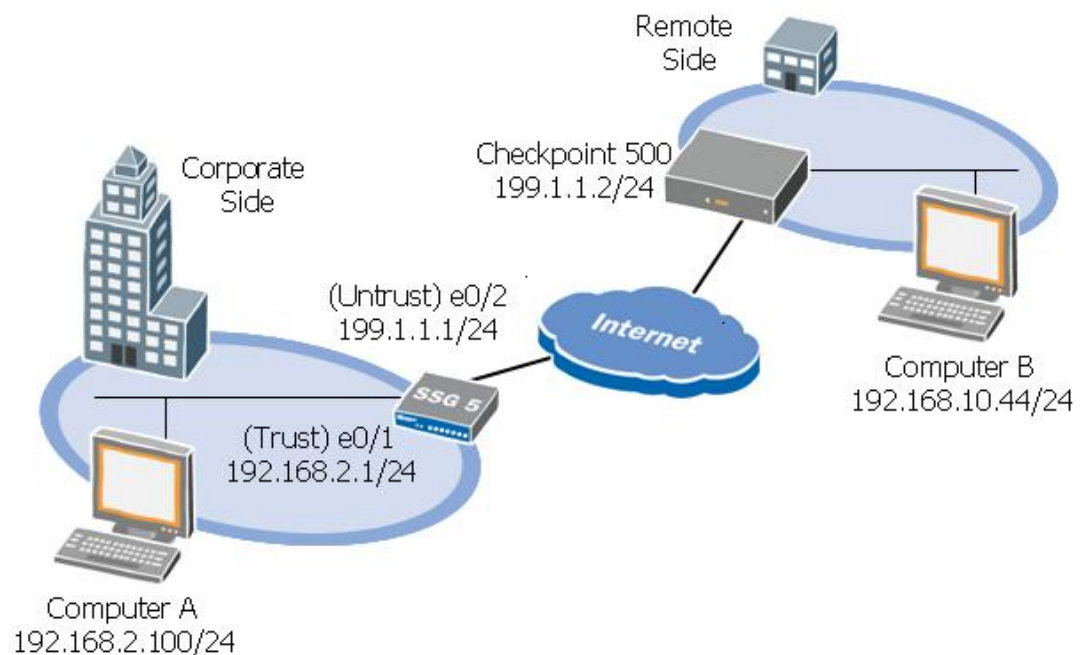
This document applies to the following Checkpoint Appliance running 6.0.76x

- Check Point Safe@Office 500 Appliance

## Network Diagram

Refer to Figure 1 below for Network Topology used for this configuration example.

**Figure 1.**



## Configuration Steps

This example assumes the following (refer to Figure 1):

- Internal LAN interface for the Corporate side will be ethernet0/1 in zone “Trust” and will have private IP 192.168.2.1/24.
- Internet interface for both sites will be using an IP address from network segment IP 199.1.1.0/24 ; SSG5 is configured with IP 199.1.1.1/24 on ethernet0/2 in zone “Untrust” and the Checkpoint Appliance is configured with IP 199.1.1.2/24 on the Internet Setup (Primary).
- Internal LAN for the Remote site will be using the network segment of IP 192.168.10.0/24, with the host computer having an address of 192.168.10.44/24.
- Policies for clear (non-encrypted) traffic on the SSG5.
- The address range to reach Remote site hosts from Corporate site is 192.168.10.0/24.
- The address range to reach Corporate site hosts from Remote site is 192.168.2.0/24
- All traffic between the Corporate and Remote LANs are to be permitted, and traffic may be initiated from either side.
- Basic non-VPN settings such as system settings, user login, and default security settings are already pre-configured on both devices.

### Basic Steps to Configure

Note that both Corporate and Remote sites have similar configuration. A policy based VPN would be used on the SSG5 to direct remote site traffic through the VPN.

1. Configure IP addresses for interfaces ethernet0/1 and ethernet0/2. Bind the interfaces to the “Trust” and “Untrust” zones respectively. (We use the defined zones “Trust” and “Untrust” for the VPN setup.)
2. Configure address book entries for “Trust” and “Untrust” zones. This will be used in the security policy.
3. Configure IKE gateway profile.
4. Configure VPN profile referencing IKE gateway from step 3.
5. Configure bidirectional security policy to permit Corporate site LAN to Remote site LAN using the address book entries created in step 2.
6. Configure Site-to-Site VPN on Checkpoint with the VPN wizard.

## Corporate Site Configuration (SSG5)

### Example

#### 1. Configure IP addresses and bind interfaces to zones.

##### WebUI

Network > Interfaces > Edit (for **ethernet0/1**): Enter the following, then click **OK**.

Zone Name: **Trust**  
Static IP, Address/Netmask: **192.168.2.1/24**  
Interface Mode: **Nat**

Network > Interfaces > Edit (for **ethernet0/2**): Enter the following, then click **OK**.

Zone Name: **Untrust**  
Static IP, Address/Netmask: **199.1.1.1/24**  
Interface Mode: **Route**

##### CLI

```
set interface ethernet0/1 zone "Trust"  
set interface ethernet0/1 ip 192.168.2.1/24  
set interface ethernet0/1 nat  
set interface ethernet0/2 zone "Untrust"  
set interface ethernet0/2 ip 199.1.1.1/24  
set interface ethernet0/2 route
```

#### 2. Configure address book entries.

##### WebUI

Objects > Addresses > List > New: Enter the following, and then click **OK**.

Address Name: **local-net**  
IP Address/Netmask: **192.168.2.0/24**  
Zone: **Trust**

Objects > Addresses > List > New: Enter the following, and then click **OK**.

Address Name: **remote-net**  
IP Address/Netmask: **192.168.10.0/24**  
Zone: **Untrust**

##### CLI

```
set address "Trust" "local-net" 192.168.2.0 255.255.255.0  
set address "Untrust" "remote-net" 192.168.10.0 255.255.255.0
```

### 3. Configure IKE gateway.

#### WebUI

VPNs > Auto Key Advanced > Gateway > New: Enter the following, but do NOT click **OK** yet.

Gateway Name: **CGW**  
Remote Gateway Type  
Static IP Address/Hostname: **199.1.1.2**  
Preshared Key: **juniper**  
Outgoing Interface: **ethernet0/2**

Then click **Advanced**. Enter the following, and then click **Return**.

Security Level User Defined: **Standard**  
Mode (Initiator): **Main (ID Protection)**  
Local Cert: None

Then click **OK**.

#### CLI

```
set ike gateway "CGW" address 199.1.1.2 Main outgoing-interface ethernet0/2 preshare  
juniper sec-level standard
```

### 4. Configure VPN profile.

#### WebUI

VPNs > Auto Key IKE > New: Enter the following, but do NOT click **OK** yet.

VPN Name: **CVPN**  
Remote Gateway Predefined: **CGW**

Then click **Advanced**. Enter the following, and then click **Return**.

Security Level Predefined: **Standard**  
Bind to: **None**

Then click **OK**.

#### CLI

```
set vpn "CVPN" gateway "CGW" no-replay tunnel idletime 0 sec-level standard
```

## 5. Configure security policy from Corporate LAN to Remote LAN.

### WebUI

Policy>Policies > (From: **Trust**, To: **Untrust**) New: Enter the following, and then click **OK**.

Source Address

Address Book Entry: **local-net (192.168.2.0/24)**

Destination Address

Address Book Entry: : **remote-net (192.168.10.0/24)**

Service: **ANY**

Action: **Tunnel**

Tunnel: **CVPN**

**Check** Modify matching bidirectional VPN policy

### CLI

```
set policy id 2 from "Trust" to "Untrust" " local-net " " remote-net " "ANY"  
tunnel vpn "CVPN" id 2 pair-policy 3 log  
set policy id 2  
exit  
set policy id 3 from "Untrust" to "Trust" " remote-net " " local-net " "ANY"  
tunnel vpn "CVPN" id 2 pair-policy 2 log  
set policy id 3  
exit
```

## Remote Site Configuration (Checkpoint Appliance)

### Example

#### WebUI

We will be using the VPN wizard to create a Site-to-Site VPN to the Corporate Site.

#### 1. Configure a Site-to-Site VPN.

VPN> VPN Sites > New Site (button below)



Select Site-to-Site VPN and click Next>

## 2. Configure IP addresses of the Corporate VPN Gateway.

Enter the IP address of the corporate VPN gateway (199.1.1.1)



The screenshot shows the 'Safe@Office VPN Site Wizard' interface. The title bar is dark blue with the text 'Safe@Office VPN Site Wizard' in white. Below the title bar, the main content area has a light gray background. At the top of this area, the heading 'VPN Gateway Address' is displayed in bold. Below the heading, there is a line of text: 'Enter the IP address of the VPN gateway to which you want to connect.' Underneath this text, there is a label 'VPN Gateway' followed by a text input field containing the IP address '199.1.1.1'. Below the input field, there are two checked options, each with a small square icon containing a checkmark. The first option is 'Bypass NAT:' followed by the text 'Don't perform Network Address Translation (NAT) between this site and the internal network'. The second option is 'Bypass the firewall:' followed by the text 'Bypass the firewall between this site and the internal network'. At the bottom of the form, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Check the **Bypass NAT** and **Bypass the firewall** options and click on Next>

### 3. Configure the VPN parameters.

Select the **Specify Configuration** option and select Next>



**Safe@Office VPN Site Wizard**

**VPN Network Configuration**

How do you want to obtain the VPN network configuration?  
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

- Download Configuration:**  
Obtain the network configuration by downloading it from the site.
- Specify Configuration:**  
Enter the network configuration manually.
- Route All Traffic:**  
All network traffic will be routed via this site (Including Internet traffic)
- Route Based VPN:**  
Create a virtual tunnel interface for this VPN site, allowing it to participate in dynamic or static routing schemes.

### 4. Configure the Corporate LAN as the destination network.

Enter **192.168.2.0/255.255.255.0** as the **destination network**; leave the backup gateway field blank.



**Safe@Office VPN Site Wizard**

**VPN Network Configuration**

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.	192.168.2.0	255.255.255.0 [/24]
2.		255.255.255.0 [/24]
3.		255.255.255.0 [/24]

Backup Gateway

Select Next>

### 5a. Configure the Preshared Key.

Select the `Shared Secret` and select Next>



The screenshot shows the 'Safe@Office VPN Site Wizard' window. The title bar is dark blue with the text 'Safe@Office VPN Site Wizard'. Below the title bar, the main area has a light gray background. At the top of this area, the text 'Authentication Method' is displayed. Below that, the instruction 'Select the authentication method used by this VPN site.' is shown. There are two radio button options: 'Shared Secret' (which is selected) and 'Certificate'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

### 5b. Configure the Preshared Key.

Enter `juniper` as the preshared key in **Use Shared Secret** and select Next>



The screenshot shows the 'Safe@Office VPN Site Wizard' window. The title bar is dark blue with the text 'Safe@Office VPN Site Wizard'. Below the title bar, the main area has a light gray background. At the top of this area, the text 'Authentication' is displayed. Below that, the instruction 'Please enter your credentials :' is shown. Underneath, the text 'Use Shared Secret.' is followed by a text input field containing a series of black dots, representing the preshared key. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

## 6. Configure the IKE Phase 1 and Phase 2 negotiation parameters.

Leave the Phase 1 settings to the default of **Security Methods**-Automatic, **Diffie-Hellman group**-Automatic, **Renegotiate every** 1440 minutes, Phase 2 will be customized to match the configurations on the Corporate Site as the following; **Security Methods** AES-128/SHA1, **Perfect Forward Secrecy** Enabled, **Diffie-Hellman group** Group 2(1024 bit) and **Renegotiate every** 3600 (seconds)



The screenshot shows the 'Safe@Office VPN Site Wizard' interface. The title bar is dark blue with the text 'Safe@Office VPN Site Wizard'. Below the title bar, the section is titled 'Security Methods'. A sub-header reads: 'Select the security and integrity methods for this site, or select "Automatic" to automatically select the best security methods supported by the site.' Below this is a link: '▲ Hide Advanced Settings'. The configuration is divided into two sections: 'Phase 1' and 'Phase 2'. Each section has four rows of settings, each with a label, a value field, and a help icon (a question mark in a square). At the bottom of the form are three buttons: '< Back', 'Next >', and 'Cancel'.

Phase	Setting	Value	Unit
Phase 1	Security Methods	Automatic	
	Diffie-Hellman group	Automatic	
	Renegotiate every	1440	minutes
Phase 2	Security Methods	AES-128/SHA1	
	Perfect Forward Secrecy	Enabled	
	Diffie-Hellman group	Group 2 (1024 bit)	
	Renegotiate every	3600	seconds

Select Next>

### 7a. Test Connectivity to the Corporate Site

This part of the setup will try and establish a connection with the Corporate site, select Next> to start the process.



### 7b. Test Connectivity to the Corporate Site

This will successfully establish the IKE Phase1



### 7c. Test Connectivity to the Corporate Site

The following message confirms to have established IKE Phase1 successfully with the Corporate Site.



### 8a. Save the profile

Provide a Site Name (SSG5) to the configured profile and select Next>



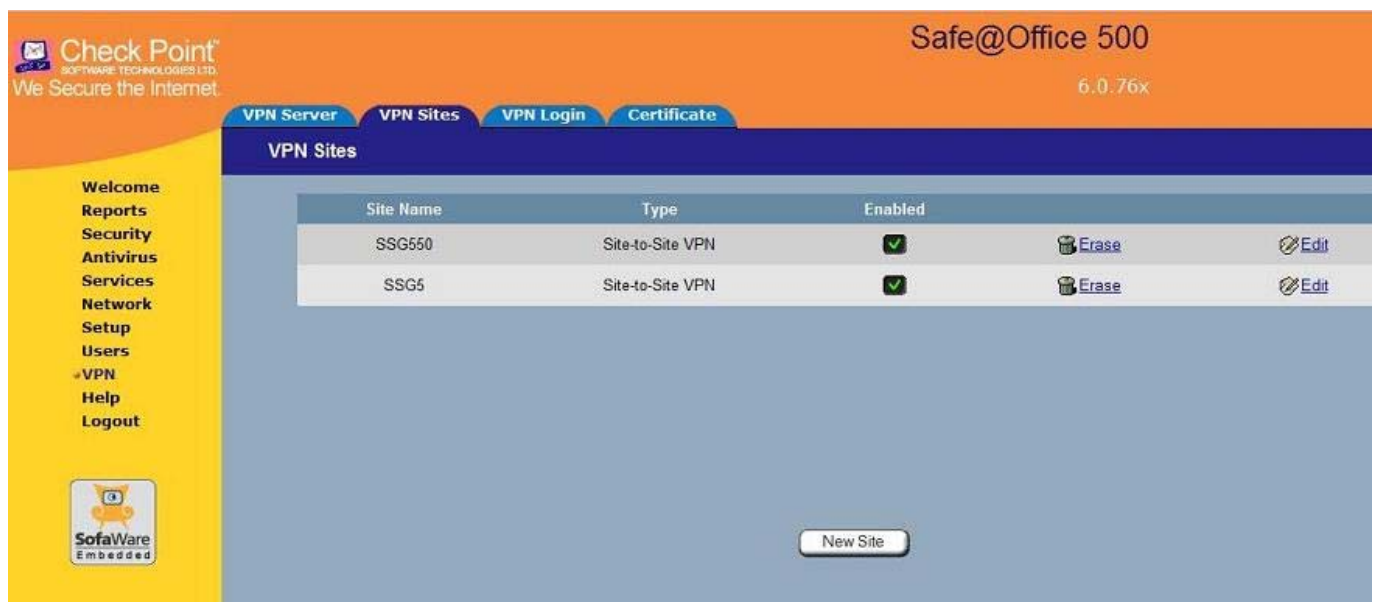
### 8b. Save the profile

Click on Finish and this will save the VPN profile to the VPN Sites.



### 9. Verify the VPN profile

Navigate through VPN>VPN Sites to verify whether the profile has been added to the list.



## Verifying Functionality

### Confirming VPN Security Association Status

The first step would be to confirm VPN status. Assuming that traffic is already flowing through the VPN and the tunnel should be in UP state, confirm the security association status with command: `get sa` (see example output below).

```
SSG5-> get sa
total configured sa: 1
HEX ID      Gateway      Port Algorithm      SPI      Life:sec kb Sta PID vsys
00000001< 199.1.1.2    500 esp:a128/sha1 3ebaffd6 2463 unlim A/- -1 0
00000001> 199.1.1.2    500 esp:a128/sha1 8b8a3e9e 2463 unlim A/- -1 0
```

We can see that the remote peer is **199.1.1.2**. The State shows **A/-**. The possible states are below:

I/I	SA Inactive, VPN is currently not connected.
A/-	SA is Active, VPN monitoring is not enabled
A/D	SA is Active, VPN monitoring is enabled but failing thus DOWN
A/U	SA is Active, VPN monitoring is enabled and UP

For additional troubleshooting assistance for IKE and IPSec, refer to the [Juniper Firewall VPN Configuration and Resolution Guide](#).

### Testing Traffic Flow Across the VPN

Once you have confirmed status of the security association, then the next step is to test traffic flow across the VPN. One way to test traffic flow is using ping. We can ping from the local host PC to the remote host PC. We can also initiate ping from the Juniper Firewall/VPN device itself. Below is an example of testing ping from the Corporate site Firewall/VPN device to the Remote side PC host.

```
SSG5-> ping 192.168.10.44 from ethernet0/1

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 192.168.10.44, timeout is 1 seconds from
ethernet0/1
!!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=20/23/30 ms
```

Recall that to reach the Remote site network; the destination address must be from the segment specified in the address book entry. Note also that when initiating ping from the Firewall/VPN device the source interface needs to be specified in order to be sure that the correct source can be referenced in the policy lookup. In this case ethernet0/1 resides in the same security zone as the Corporate host PC. Therefore interface ethernet0/1 will need to be specified in ping so that the policy lookup can be from zone "Trust" to zone "Untrust".

Likewise, to confirm bi-directional operation, we can initiate a ping from the Remote site peer to the Corporate network host PC.

To verify the status of the connection on the Checkpoint Appliance, navigate through Reports>VPN Tunnel

Alternatively the event log can be checked to find details of the VPN initiated to the Corporate Site, by navigating through Reports>Event Log.



If successful, then that confirms that the policies are correct to allow the traffic in both directions.

If either side is not successful, then refer to the [Juniper Firewall VPN Configuration and Resolution Guide](#). Contact Checkpoint Software Technologies for configuration issues and troubleshooting on the Checkpoint Firewall.

Copyright © 2007, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.