



**GreenBorder™ Professional**  
version **2.7.3**

# **VPN Configuration Guide**



331 Fairchild Dr.  
Mountain View, CA 94043

<http://www.greenborder.com/>

Document Version: **2.7.3 Final**

Revision Date: **July 2005**

©2002-2005 Green Border Technologies, Inc. All rights reserved.

GreenBorder is a trademark or registered trademark of Green Border Technologies, Inc. in the United States and/or other countries.

Microsoft, Outlook, Windows, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Check Point, SecuRemote, SecureClient, VPN-1, Firewall-1, SmartCenter, and VPN-1 Pro are trademarks or registered trademarks of Check Point Software Technologies Ltd.

# VPN Configuration Guide

---

## Introduction

GreenBorder protection depends only on the configuration of your trusted networks. This configuration does not change dynamically and doesn't need to be updated to respond to new threats. Remote VPN users that are not connected to your network remain up-to-date and protected without needing constant updates. However, there are a few configuration options to consider when planning your support for VPN users:

- Does your trusted corporate network use private IP addresses?

Private addresses inside the firewall are a common choice for organizations with limited public addresses. IP addresses used for private networks are listed in the following table.

<b>Network Address</b>	<b>Subnet Mask</b>
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

These addresses might be used on a remote network that a VPN user connects at home, in a hotel, or at a wireless hotspot. In that case, GreenBorder must determine that the remote network is not part of the trusted network; therefore, you must configure your network rules with the “require server authentication to trust” flag. For details about how to configure network rules, see “Configuring Trust in Private IP Ranges” on page 2.

- Do remote users access web-based resources on the public Internet?

For example, remote users might use the public Internet for Outlook Web Access or for web-based access to corporate applications. Internal users might just use Exchange or servers inside the firewall. In this case, you would need to create rules to trust the web-based sites that remote users access. (See “Configuring Web-based Resources for Remote Users” for more information.)

- Do you use Check Point® SecuRemote® or Check Point® SecureClient™ VPN clients?

Check Point SecuRemote and SecureClient VPN clients can create “transparent” VPN connections that might cause problems with GreenBorder agents. The primary issue is that GreenBorder does not recognize the transparent connection, and so does not properly trust the VPN connection. Check Point SecureClient operating in Office Mode can work around these issues. See the sections “Issues with Transparent VPN Connections” and “Working with Check Point VPN Clients” for more information.

In most cases, the configuration you need for VPN users does not affect non-VPN users inside the firewall. Therefore, for all GreenBorder users, you can use a single configuration with additions for VPN users. If you want to keep the configuration for VPN users separate from the configuration for internal users, it is a simple matter to create a new configuration, or derive a configuration for VPN users from an existing configuration. Refer to Chapter 4, “Creating and Configuring Agent Configurations in the GreenBorder *Administrator’s Guide* for information on deriving or creating new configurations.

## Configuring Trust in Private IP Ranges

If you use private IP addresses on your corporate network, you need to set the “Trust only on interfaces that authenticate a server” option in your Trusted Network rules for VPN users. Figure 1-1 shows how you would set this option.

**Figure 1-1** Setting Trust Only on Interfaces that Authenticate a Server

**Add Trusted Network**

Enter the IP prefix, domain, or host name of the trusted network. Use x to indicate wildcards in the network address (192.168.1.x). Hostnames are resolved to a range of IP addresses when the Agent receives them. The Netmask is computed automatically, but you can specify your own if you need to make more specific.

Hostname or IP Address	*	192.168.x.x
Description	*	Internal 192 Networks
Port		<input checked="" type="radio"/> All <input type="radio"/> Port <input type="text" value="0"/>
Netmask	*	255 . 255 . 255 . 0
Trust		<input checked="" type="checkbox"/> Trust only on interfaces that authenticate a server <input type="button" value="?"/>

\* Required Field(s)

**NOTE** – You cannot modify the inherited network rules in an inherited configuration, you can only add new rules. To create special rules for VPN users, you can modify the network rules in the parent configuration or start with a clean configuration that does not have a parent.

By setting this option, the network range will only be trusted when the GreenBorder Management Server can be contacted over the network interface. This prevents the GreenBorder agent from trusting remote networks at a home or hotel, for example, because the GreenBorder Management Server will not be reachable on those networks.

However, when a GreenBorder user initiates a VPN connection, the new VPN interface will trigger the GreenBorder agent to try again to authenticate its GreenBorder Management Server. If the GreenBorder Management Server is authenticated, all of the network addresses that are routed over the VPN interface and that match Trusted Network rules will be trusted.

## Security Risks of Not Requiring Authentication

In some cases, it might not be possible to have a GreenBorder Management Server available for VPN users to authenticate, or your VPN client might create transparent connections that do not trigger an authentication request (see the section “Issues with Transparent VPN Connections” below.) Therefore, your only option for VPN users might be to not require server authentication. You still have some protection if your VPN client prevents access to other networks while the VPN is connected. In this case, the remote computer is effectively cut off from the remote network while the VPN is active, so the

only risks are damage and theft of data on the computer (versus potential use of the computer to attack servers inside the corporate network).

If the option to require server authentication is not checked, a network will always be trusted. This creates a security risk because the GreenBorder agent will allow connections to Protected Ports from other hosts on a trusted network. The default Protected Ports include ports used for file and printer sharing, for example. These ports might be vulnerable to attack. On the corporate network, the benefit of using network file and printer sharing usually outweighs the security risks, but on a remote network there is no reason to have these ports open.

A less serious issue with not requiring trust is that any web site on a remote network that matches your Trusted Network rules will be trusted. This creates a scenario where an attacker on the remote network could get a user to visit a web page hosted on that network (by using a DNS poisoning or injection attack). The hostile web page would be on a network considered trusted, and so would not be protected by GreenBorder. Any code running from that web site would have access not only to the user's computer but could also use a VPN connection to access your corporate network.

These risks are presented so that you understand the implications of not using the option to require server authentication to trust a network. In some rare cases, you might decide to accept these risks if you have other security countermeasures.

## Issues with Transparent VPN Connections

A transparent VPN connection creates an IPSec tunnel into the corporate network without creating a new network interface. The VPN clients that GreenBorder has tested that create transparent connections are Check Point SecuRemote and SecureClient.

If no new network interface is created for the VPN connection, there is no event to trigger the GreenBorder agent to authenticate the GreenBorder Management Server. If you use the option to require server authentication to trust a network, the network accessible through the VPN will not be trusted. When the computer connects to the remote network, there is no GreenBorder Management Server available, so all networks are considered untrusted. Because there is no event to cause the GreenBorder agent to authenticate the server, all networks remain untrusted even after the VPN tunnel is created.

The security risks under these conditions are from content and code inside the GreenBorder environment. If the remote user has been browsing the Internet, there might still be malware inside the GreenBorder environment from that browsing. Because the VPN connection is untrusted, anything running inside the GreenBorder environment has access to servers accessible through the VPN. Moreover, if the user browses the corporate intranet, that browsing will be done inside GreenBorder. Browsing inside GreenBorder

could be intercepted or traced by malware introduced to the GreenBorder environment from another Internet site.

To mitigate these security risks, you should not use transparent VPN connections with GreenBorder. Check Point SecureClient has a configuration option called Office Mode that is not transparent. It creates a new interface whenever the VPN connection is established. (See the section “Installing GreenBorder over a VPN Connection” for more information.)

If you must use a VPN client in transparent mode, consider not requiring server authentication to trust a network. The risks associated with this configuration are discussed in “Security Risks of Not Requiring Authentication.” The risks of not requiring authentication are often more tolerable than the risks of forcing your corporate intranet to be browsed within GreenBorder.

# Configuring Web-based Resources for Remote Users

Remote users might need access to web-based corporate applications, such as Outlook Web Access. Some of these applications might be on servers available over the Internet to make it easy for users to access them without using a VPN tunnel into the corporate network. Because these resources are not part of your internal network (and might not even be accessible from within the corporate firewall), you might not have added them as Trusted Network rules in your configurations.

Add Trusted Network rules for any web-based corporate applications that remote users need to access. If an application is hosted at a fixed external IP address, use the IP address for the rule; otherwise, you can use the name of the application host.

## Installing GreenBorder over a VPN Connection

If the GreenBorder agent is installed over a VPN connection, the user will have to manually update the configuration before the GreenBorder agent will start.

When the GreenBorder agent is installed, it has a default, unusable configuration. When the computer restarts after installation, the agent downloads the latest configuration from its GreenBorder Management Server. If the agent was installed over a VPN connection, the GreenBorder Management Server will not be available until the VPN connection is reestablished (which is not normally during boot up). Therefore, after a user installs GreenBorder over a VPN connection, the GreenBorder Security Agent will be disabled (there will be a red X on the tray icon), and the user will be notified that no configuration has been downloaded.

To start the GreenBorder agent after installing over a VPN connection, do the following:

- 1** Establish the VPN connection so that the GreenBorder Management Server can be reached.
- 2** Right-click the GreenBorder tray icon and click Update. A dialog box will show the progress as the agent contacts its server and downloads the latest configuration.
- 3** Troubleshoot any VPN Installation issues. (See the next section “Troubleshooting VPN Installation Issues.”)

## Troubleshooting VPN Installation Issues

If the GreenBorder Security Agent is still not enabled, the most likely reason that the GreenBorder Management Server is not reachable. You can take the following steps to troubleshoot the problem:

- 1** Verify that the VPN is actively connected.
- 2** Verify that the GreenBorder Management Server is running. Contact your administrator, or if you are the administrator, visit the GreenBorder Management Server web interface at <http://YOUR-SERVER-NAME/GreenBorder>.
- 3** Check the Application event log to verify that the problem is that the server was not reached by doing the following:
  - a** Right-click My Computer (on the Start Menu or Desktop) and select Manage. This opens the Computer Management console.
  - b** Under System Tools, open Event Viewer and double-click Application.
  - c** Look in recent errors for an Error from GB Network Authenticator. Double-click the event to see the contents.
  - d** If the event is "Failed to authenticate server: 'YOUR-SERVER-NAME'", the problem is that the server could not be reached.
  - e** If there is no error from the GB Network Authenticator or the error is not an authentication failure, contact GreenBorder support for more help.
- 4** Check whether the server can be reached by doing the following:
  - a** Use a web browser to try the name found in the Application event log. For example, if the server name given is YOUR-SERVER-NAME, open Internet Explorer and try to go to <http://YOUR-SERVER-NAME>
  - b** If you get an error page, look at the bottom of the page to see what the error is. If the error is "Cannot find server or DNS Error," the server is not reachable.
  - c** If you get a different error, such as an "HTTP 404 - File not found" or a permission error, the GreenBorder Management Server is reachable, but there may be another problem. Contact GreenBorder support for more help.
- 5** If the server cannot be reached, try to disconnect the VPN connection, connect again, then try to Update the GreenBorder configuration.

- 6** If the server is still unreachable, try using its fully qualified name. For example, if the server is YOUR-SERVER-NAME and your domain is Example.com, try using Internet Explorer to visit `http://YOUR-SERVER-NAME.Example.com/`.
- 7** If you do not get a DNS error (that is, you get a permissions error or a page not found), the server is reachable using the fully qualified name, and you can do the following:
  - a** You can resolve this by editing the registry value that holds the server name. If you are familiar with modifying the registry, use an editor such as `regedit.exe` to update the value in `HKEY_LOCAL_MACHINE\Software\GreenBorder\ServerUrl` with the fully qualified name of the GreenBorder Management Server.
  - b** If you are not familiar with editing the registry, contact GreenBorder support for assistance.
- 8** If the server is still not reachable, it may be on a network segment that is not accessible by VPN users. Contact GreenBorder support for assistance with resolving the issue.
- 9** Right-click the GreenBorder tray icon and click Enable.

## Working with Check Point VPN Clients

This section lists the clients tested with GreenBorder and briefly discuss installation and security issues with Check Point VPN clients.

### Clients Tested with GreenBorder

GreenBorder has tested the following Check Point VPN clients to ensure that they are compatible with the GreenBorder Security Agent:

- Check Point SecuRemote (R55) (If you do not use private IP addresses; see “Security Issues with GreenBorder when Check Point VPN Clients use Transparent Mode” on page 9)
- Check Point SecureClient (R55)

If your Check Point VPN client does not appear on this list, contact GreenBorder support. GreenBorder is continuously updating the list of tested applications, and we are always willing to verify applications that our customers use.

## Installing Check Point VPN Clients with GreenBorder

There is no special installation procedure required for installing GreenBorder and Check Point VPN clients on the same machine. The software may be installed in any order.

If you install GreenBorder remotely on a computer connected to the corporate network using the VPN, be sure to read “Installing GreenBorder over a VPN Connection” on page 6.

## Security Issues with GreenBorder when Check Point VPN Clients use Transparent Mode

If you use private IP addresses inside your corporate network, and you use a Check Point VPN client in transparent mode, there may be security issues for remote GreenBorder users. If you use Check Point SecureClient, you can address the security issues by using Office Mode instead of operating the VPN client in transparent mode.

The sections “Configuring Trust in Private IP Ranges” and “Issues with Transparent VPN Connections” describes security issues in detail

To configure Office Mode for your VPN users, you should consult your Check Point® Firewall-1® or Check Point® VPN-1® server documentation. To help you get started with basic testing or a pilot project, the procedure from the Check Point documentation provided in the following sections can help you create a basic Office Mode configuration.

## Configuring Office Mode on the Check Point Firewall-1 or VPN-1 Server

This section describes how to configure your Check Point VPN for Office Mode. The instruction in this chapter are provided as a “Quick Start.” However, you should consult your Check Point documentation, from which these procedures were derived, for detailed information.

Before configuring Office Mode, the assumption is that standard VPN Remote Access has already been configured. For more details on how to configure VPN Remote Access, refer to your Check Point VPN documentation.

You must select an internal address space designated for remote users Using Office Mode before you start the Office Mode configuration. This internal address space can be any IP address space as long as the addresses in this space do not conflict with addresses used

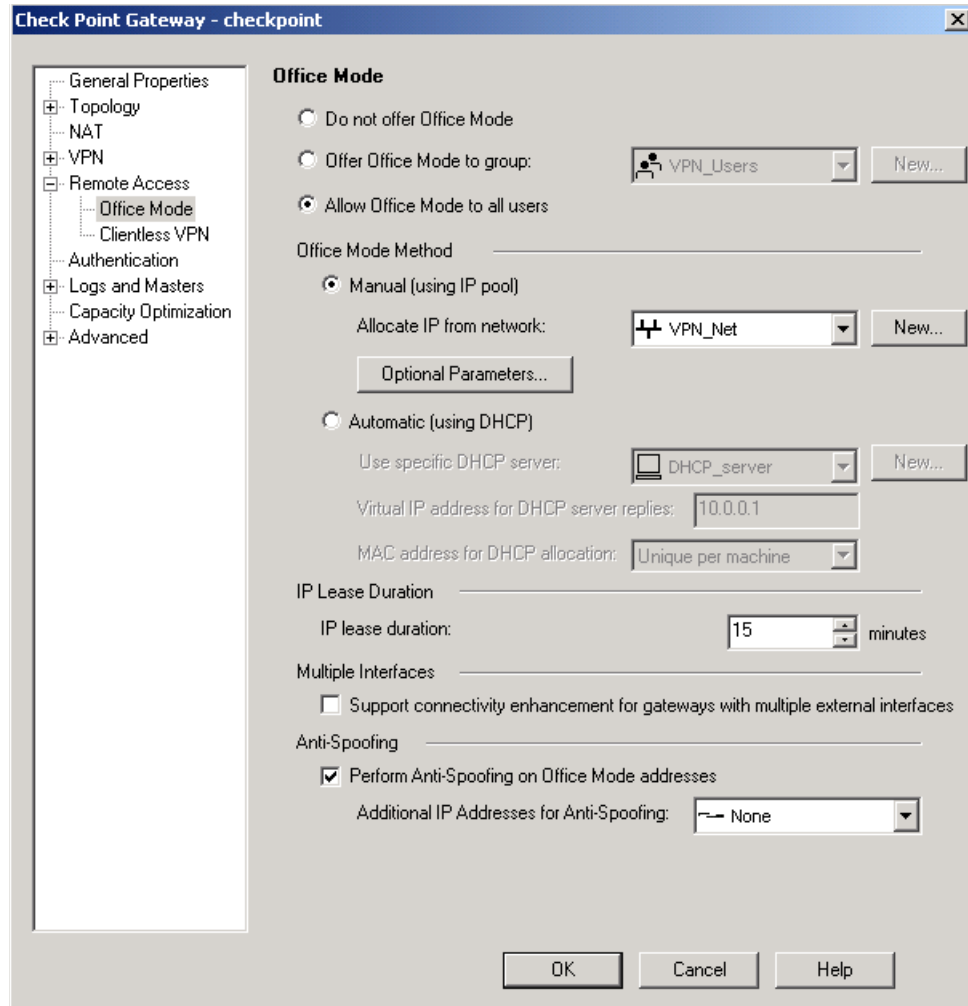
within the enterprise domain. It is possible to chose address spaces that are not routable on the Internet, such as 10.x.x.x.

The basic configuration of Office Mode using DHCP for address allocation can be found in your Check Point VPN-1 documentation.

To deploy the basic Office Mode (using IP pools), perform the following steps:

- 1** Create a network object to represent the IP Pool by selecting **Manage>Network Objects>New>Network**.
- 2** In the **Network Properties - General** tab, set the IP pool range of addresses as follows:
  - In Network Address specify the first address to be used (for example, 10.130.56.0)
  - In **Net Mask** enter the subnet mask according to the amount of addresses you wish to use (entering 255.255.255.0, for example. This will designate all 256 IP address from 10.130.56.1 till 10.130.56.254)
  - Changes to the **Broadcast Addresses** section and the **Network Properties - NAT** tab are not necessary.
- 3** Open the Gateway object through which the remote user will connect to the internal network and select the **Remote Access > Office Mode** page. Enable **Office Mode** for either all users or for a certain group. Figure 1-2 shows the Office Mode page with Office Mode enable for all users.

**Figure 1-2**



Now do the following:

- In the **Allocate IP from network** select the IP Pool network object you have previously created.
- **IP lease duration**— specify the duration in which the IP is used by the SecureClient machine.
- Under Multiple Interfaces, specify whether you want routing to be done after the encapsulation of Office Mode packets, allowing traffic to be routed correctly when you gateway has multiple external interfaces.

- Select **Anti-Spoofing** if you want the firewall to check that Office Mode packets are not spoofed.

It is possible to specify which WINS and DNS servers Office Mode user should use.

To specify WINDS and/or DNS servers, continue to step 4. Otherwise go to step 7.

**i NOTE** – WINS and DNS servers should be set on the Check Point® SmartCenter™ machine only when IP pool is the selected method.

- 4** Create a DNS server object by selecting **Manage>Network objects>New>Node>Host** and specify the DNS machine's name, IP address, and subnet mask. Repeat this step if you have additional DNS servers.
- 5** Create a WINS server object by selecting **Manage>Networks objects >New>Node>Host** and specify the WINS machine's name, IP address, and subnet mask. Repeat this step if you have additional WINS servers.
- 6** In the **IP Pool section** of the **Check Point Gateway - Remote Access >Office Mode** page, click the **"optional parameters"** button.
  - In the **IP Pool Optional Parameters** window, select the appropriate objects for the primary and backup DNS and WINS servers.
  - In the **Domain name** fields, specify the suffix of the domain where the internal names are defined. This instructs the Client as per what suffix to add when it addresses the DNS server (for example, exmaple.com).
- 7** Install the Policy.
- 8** Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode user through the Check Point® VPN-1 Pro™ Gateway. For instance, in the example above, it is required to add routes to the class C subnetwork of 10.130.56.0 through the gateway's IP address.

In addition to the steps mentioned for the gateway side configuration, a few configuration steps have to be performed on the client side to connect the gateway in Office mode. (See **"Configuring Check Point SecureClient to Use Office Mode"** .

# Configuring Check Point SecureClient to Use Office Mode

On the client's machine the following steps should be performed to connect to the gateway in Office Mode.

- 1** Right click the SecureClient icon in the system tray. From the pop-up menu, select **Configure**.
- 2** Select **Tools>Configure Connection Profile>Advanced** and select **Support Office Mode**.
- 3** Click **OK, Save and Close**, then select **Exit** from your **File** menu.
- 4** Double click your SecureClient icon on the bottom right side of your screen. If you are using a dial-up connection to connect to the gateway select **Use Dial-Up** and chose the name of your dial-up connection profile from the drop down menu. (It is assumed that such a profile already exists.) If dial-up is not used (that is, connection to the gateway is done through a network interface card), proceed to step 5.
- 5** Select **Connect** to connect to the organization using Office Mode.

The administrator can simplify configuration by configuring a profile in advance and providing it to the user.

