Introduction

A common requirement of today’s networks is to allow remote users to connect to and access resources available on the network at any time of the day and night. SonicWALL’s SonicOS has the functionality to allow users to establish secure IPSEC-based VPN tunnels over the Internet to handle this requirement.

Because most modern networks have a segmented (secure) architecture that uses both LAN and DMZ segments, it’s often a requirement to allow remote users access to both of these sections of the network.

One of the features of SonicWALL’s SonicOS Enhanced firmware is the administrator is able to control the locations on the network a VPN client is able to access based on the username that the user enters to authenticate to the SonicWALL security appliance. This provides a great degree of control to SonicWALL administrators. For example, one end user may be able to access only an e-commerce server on the DMZ while another user is able to access all of the subnets that are being protected by the SonicWALL. By enabling the SonicWALL to allow users access to network resources that are sitting behind it using a remote connection with the data encrypted and sent across a VPN tunnel, remote users will be able to utilize additional services such as NetBIOS or MAPI access without opening these services directly to the Internet.

This TechNote focuses on the configuration required to allow Global VPN Clients (GVC) to access different segments of the network (for example the LAN or DMZ) behind a SonicWALL security appliance.

Network Topology

In this example, the environment consists of a corporate network, and a remote user connecting using the WAN GroupVPN and the GVC. The corporate network is protected and segmented by a SonicWALL security appliance running SonicOS Enhanced.

On the corporate network, there are two servers located on the DMZ. The first server is an email server that has been assigned a private address 10.10.10.10/24 and has port 25 forwarded from the WAN IP address of the SonicWALL. The second server is a Web server that has been assigned the private address 10.10.10.11 and has ports 80, 443 and 21 forwarded from the WAN IP address of the SonicWALL.

The LAN segment has been assigned a private IP subnet as well, 192.168.168.0 with a 24-bit subnet mask. User desktops as well as file, print, and authentication services are located on the private LAN, which do not require direct inbound Internet traffic.
The remote client has acquired a public IP address from its local ISP and now requires access to both the LAN and DMZ segments of the corporate network. To achieve this, a VPN tunnel will be established between the remote user’s computer and the SonicWALL security appliance at the corporate office.

Below is a diagram of the network.

**Configuration**

**Network Configuration**

At the corporate location, both LAN and DMZ networks are configured with internal IP addresses corresponding to the diagram above. The WAN IP of the SonicWALL security appliance is given as 1.1.1.1/24 (for the purposes of this example). To enable the ability to have the SonicWALL security appliance support a DMZ the OPT port (or x2 interface on the PRO series) was assigned to the DMZ zone (it is assumed that this has already been setup for the purpose of this example).
This configuration is illustrated in the diagram below:
## Network > Interfaces

### Interface Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Zone</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>IP Assignment</th>
<th>Status</th>
<th>Comment</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>LAN</td>
<td>192.168.180.160</td>
<td>255.255.255.0</td>
<td>Static</td>
<td>100 Mbps full-duplex, Default LAN</td>
<td><img src="image1" alt="image" /></td>
<td></td>
</tr>
<tr>
<td>WAN</td>
<td>WAN</td>
<td>1.1.1.1</td>
<td>255.255.255.0</td>
<td>Static</td>
<td>100 Mbps full-duplex, Default WAN</td>
<td><img src="image2" alt="image" /></td>
<td></td>
</tr>
<tr>
<td>OPT</td>
<td>DMZ</td>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
<td>Static</td>
<td>100 Mbps full-duplex</td>
<td><img src="image3" alt="image" /></td>
<td></td>
</tr>
</tbody>
</table>

### Interface Traffic Statistics

<table>
<thead>
<tr>
<th>Traffic Statistics</th>
<th>LAN</th>
<th>WAN</th>
<th>OPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Unicast Packets</td>
<td>969</td>
<td>0</td>
<td>63</td>
</tr>
<tr>
<td>Rx Broadcast Packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bytes</td>
<td>142426</td>
<td>0</td>
<td>7930</td>
</tr>
<tr>
<td>Tx Unicast Packets</td>
<td>1198</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tx Broadcast Packets</td>
<td>9</td>
<td>248</td>
<td>3</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>945298</td>
<td>10577</td>
<td>192</td>
</tr>
</tbody>
</table>

Status: Ready
VPN Configuration

Since the remote clients will be connecting to the corporate network using GVC, the WAN GroupVPN must be configured and enabled on the SonicWALL security appliance. To configure the WAN GroupVPN, perform the following tasks:

1. Navigate to **VPN > VPN Policy Wizard** in the management interface.
2. The welcome screen displays. Click **Next**.

![VPN Wizard Welcome Screen](image-url)
3. Choose **WAN GroupVPN** as the VPN policy type.

4. Enter a pre-shared key that you will use for all your remote clients in the **Use this preshared key** field or select **Use default key** to use a default key. In this example, the preshared key is s0n1cw@ll.
5. Configure the details of the authentication and encryption for the VPN policy from the **DH Group** (default Group 2), **Encryption** (default 3DES), and **Authentication** (default SHA-1) drop-down menus and specify the lifetime in the **Life Time (seconds)** field.
6. In the User Authentication screen, check the **Enable User Authentication** box and select the group of users you would like to authenticate against the SonicWALL security appliance using the GVC. The default group is **Trusted Users**; this means that any user that tries to authenticate to the SonicWALL security appliance must be a member of the Trusted Users group, or a sub-group of it.
7. The Configure Virtual IP Adapter screen allows you to configure the remote client to receive an internal LAN IP address when they connect to the SonicWALL security appliance. This enables the remote client to be “seen” as being on the internal corporate network despite the fact that they are indeed not physically sitting on the local LAN segment. Check the Use Virtual IP Adapter box to enable this feature, or leave it unchecked to disable the feature, then click Next.
8. The WAN GroupVPN Configuration Summary provides the configuration changes that will be made on the SonicWALL security appliance. Click **Apply** to apply these changes.
Configuring a SonicWALL User

You need to create a user account that can be used to authenticate against the SonicWALL security appliance by a remote user.

1. Navigate to Users > Local Users in the SonicWALL security appliance administration screen.
2. Click Add User to create the local user.

3. Click the Groups tab and verify that the user is in the local group named Trusted Users, or the group you specified in the wizard that would be allowed to authenticate against the SonicWALL security appliance for remote users.

4. Click OK.

We now need to decide where this local user shall have access to on the corporate network by configuring the VPN Access tab for either the user or the group (to which the user belongs). If the administrator wanted to have highly granular control over what the remote user was able to access on the network (for example, only allowing the user to access port 80 on the web server on the DMZ) then they would need to use access rules to further limit what the remote user was able to access. In this example we will use the VPN Access tab to allow the Trusted Users group to access both the LAN subnet and the DMZ subnet of the corporate network.
5. Click Local Groups and then click the Configure icon for the Trusted Users group.
6. Click the **VPN Access** tab of the **Trusted Users** group and highlight the network components that you would like the remote users to have access to. In this case, we are electing that the remote users will have access to the “LAN subnets” and the “DMZ Subnets”. This could just as easily consist of the LAN segment and a single web server in the DMZ, if required.

![VPN Access Tab](image)

7. Once this is complete, click **OK** and exit the SonicWALL security appliance administration screen.

**GVC Configuration**

The remote computer must now be setup to remotely connect to the SonicWALL security appliance. In this example, we will setup a remote access connection back to the corporate headquarters.

1. Open SonicWALL GVC and select **File > New connection** from the menu bar. Click **Next**.
2. Check the **Remote access** radio button and click **Next**

![New Connection Wizard](image)

3. On the Remote Access page, you will be prompted for the IP address or domain name of the SonicWALL security appliance to which you would like to connect. Type your IP address or domain name in the **IP Address or Domain Name** field and optionally give the connection a name in the **Connection Name** field. Click **Next**.

![New Connection Wizard](image)
4. Optionally create a desktop shortcut by checking the **Create a desktop shortcut for this connection** box and optionally enable this connection automatically when the program is launched by checking the **Enable this connection when the program is launched** box. Click **Finish**.

5. Double click the connection you just created. You will be prompted for the pre-shared key that was specified during the setup of the WAN GroupVPN (in this example we used s0n1cw@ll). Enter your pre-shared key and click **OK**.
6. Enter your user name in the **Username** field and your password in the **Password** field. Due to the configuration we entered earlier this user must be a member of the **Trusted Users** group on the SonicWALL security appliance. The user created during this example was called “SonicWALL”.

7. Click **OK**. SonicWALL GVC will try and connect to the SonicWALL security appliance to establish the secure tunnel. If the connection is successful, the user will see a popup balloon in their taskbar showing that the connection was successful.

---

**Verifying Your Connection**

You need to verify that you can contact the servers on both the LAN segment and the DMZ segment of the network by trying to ping a server on each segment. Navigate to **Start > Run** on your Windows taskbar. Type `cmd` in the **Open** field and click **OK**. At the prompt, type Ping 10.10.10.10, where 10.10.10.10 will be replaced with an actual IP address on your LAN or DMZ segment.
Troubleshooting Common Problems

If there are problems connecting to the SonicWALL security appliance using the remote client, determine if the remote client requests are reaching the SonicWALL security appliance. To determine this you should look at the logs on the SonicWALL security appliance (click Logs on the left hand side of the SonicWALL administration interface) and also on the remote computer in the GVC by selecting View > Log Viewer within the main screen of the GVC interface.
Here is an example of a correctly completed phase 1 and 2 tunnel negotiation between the remote user’s GVC and the SonicWALL security appliance. If correctly configured, your remote clients should have similar output.

If the log does not look the same, verify the configuration by again performing the setup processes in this tech note.

If the connection to the SonicWALL security appliance is timing out, you should check to ensure that the GVC does not have a router or firewall that could be blocking access to the SonicWALL security appliance.

Refer to the SonicWALL knowledge portal (http://www.SonicWALL.com/knowledgeportal) for further help in troubleshooting GVC connectivity issues.

If a connection is being made to the SonicWALL security appliance but the user is unable to authenticate, verify that the user is typing in the correct credentials and also ensure they have the correct rights to access the SonicWALL security appliance remotely (refer to step 3 of the section Configuring a SonicWALL User in this tech note).
If the user is able to authenticate correctly and the tunnel is brought up but they are still unable to access network resources, verify the access rules on the SonicWALL security appliance, which may be restricting remote users from getting to particular network resources. Check the pre-existing access rules on the SonicWALL security appliance (in the user interface under **Firewall > Access Rules > VPN > LAN** or **VPN > DMZ**). Access rules can be used to limit the remote user’s access to network resources on the internal network behind the SonicWALL security appliance, and configured incorrectly, access rules may be restricting the remote users from getting to particular network resources. The screenshots below shows the default rules regarding remote users connecting to the LAN and DMZ, respectively.

*Access Rules (VPN > LAN)*

![Access Rules (VPN > LAN)](image-url)
If the access rules are correct, verify that the servers that the remote clients are trying to reach are online and able to be routed to, and they themselves are not blocking inbound traffic through the use of a software firewall.
Related Documentation

For more information, refer to the following SonicWALL TechNotes on www.sonicwall.com/support/documentation:

- Using a Secondary Public IP Range for NAT in SonicOS Enhanced
- Configuring the SonicWALL security appliance DHCP for GVC in SonicOS Enhanced
- Configuring the SonicWALL security appliance DHCP for GVC in SonicOS Standard
- Configuring Port Forwarding on a SonicWALL Security Appliance
- Terminating the WAN GroupVPN and Using VPN Access in SonicOS Enhanced
- Terminating the WAN GroupVPN to the LAN/DMZ using SonicOS Standard
- Typical DMZ Configuration with FTP, SMTP, and DNS Servers
- Common Issues with GVC
- Network Browsing with IP Helper NetBIOS Relay
- Creating One-to-One NAT Policies in SonicOS Enhanced
- Three Types of Network Modes in SonicOS Enhanced
- Using the SonicOS Enhanced Wizard to Configure a Public Server
- SonicOS Enhanced: Configuring Group VPN for Global Clients
- Group VPN Configuration

Document Created: 9/27/06
Document Last Updated: 10/10/06