

Configuring L2TP/IPSEC VPN Connections from Proventia® M Series Appliance to Windows XP Systems

August 15, 2005

Overview

Introduction

This document describes how to configure an L2TP/IPSEC VPN tunnel from a Proventia M series appliance running a Firmware 3.1 operating system or later to Windows 2000/XP operating systems.

Types of VPN connections

You can use two types of authentication for L2TP/IPSEC VPN connections from a Proventia appliance to a Windows client, as shown in the following table:

| To use this authentication method... | See this topic... |
|--------------------------------------|---|
| Certificate (recommended) | "Task Overview for Establishing L2TP/IPSEC Connections with Certificate Authentication" on page 5 |
| PreShared Key | "Task Overview for Establishing L2TP/IPSEC Connections with CHAP Authentication" on page 18 |

Table 1: VPN tunnel types

Intended use

This document provides an example for configuring VPN from a Proventia M series appliance to any of the following systems:

- Windows 2000
- Windows XP
- Windows XP with Service Pack 1 installed
Note: Patch required. See "NAT-T support patch from Microsoft" on page 21.
- Windows XP with Service Pack 2 installed
Note: See "NAT-T behavior in Windows XP SP 2" on page 21.

The example is not designed for operational use without modification. A knowledgeable IPSEC network administrator or advanced user should design new, custom policies for operational use.

Scope

This document does not provide specific procedures, but rather examples of settings. For specific instructions on how to configure these settings, refer to the documentation listed in the "Related documentation" section of this topic.

Related documentation

Refer to the Proventia Manager Online Help and the *Proventia M Series Appliances User Guide* for more information about the following:

- IKE settings
- IPSEC and IPSEC policies
- security gateways
- access policies
- NAT policies

For related procedures for configuring the Windows XP system, refer to the documentation provided with your system.

In this document

This document contains the following topics:

| Topic | Page |
|--|------|
| Before You Begin | 3 |
| Task Overview for Establishing L2TP/IPSEC Connections with Certificate Authentication | 5 |
| Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using Certificate Authentication | 6 |
| Adding IP Addresses for Remote Windows Clients | 8 |
| Creating Related Access Policies for the Proventia Appliance | 10 |
| Creating Access Policies to Enable Traffic from Subnet A to Subnet B | 12 |
| Creating NAT Rules | 14 |
| Configuring Certificates on the Windows Client | 16 |
| Task Overview for Establishing L2TP/IPSEC Connections with CHAP Authentication | 18 |
| Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using CHAP Authentication | 19 |
| Configuring the Windows XP Client for L2TP/IPSEC VPN Connection Using CHAP Authentication | 21 |
| Troubleshooting | 24 |

Before You Begin

Introduction

This topic includes a topography graphic and a checklist to help you gather the information you need to configure an L2TP/IPSEC VPN for your Proventia M Series appliance and Windows XP system.

Topography

The following graphic illustrates the network topography of a Proventia M Series appliance configured for VPN with a Windows XP system. The example used in this document is based on the topography depicted.

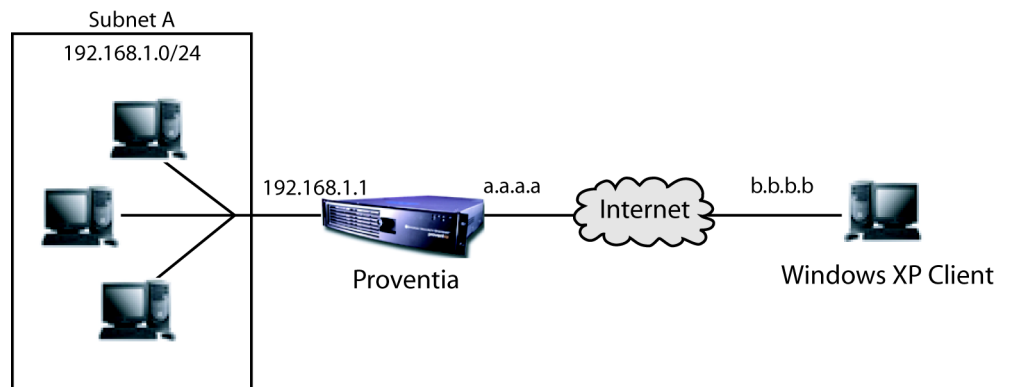


Figure 1: Topography for VPN tunnel from Proventia M Series appliance to Windows XP system

Checklist

The following checklist indicates the information that you need before configuring your VPN tunnel.

| ✓ | Task Description |
|--------------------------|---|
| <input type="checkbox"/> | Proventia M Series Unit A External IP address _____ Note: This is the IP address that you will use where a.a.a.a appears in the examples in this document. |
| <input type="checkbox"/> | Proventia M Series Unit A Internal IP Address _____ |
| <input type="checkbox"/> | Subnet A IP address/mask _____ |
| <input type="checkbox"/> | Windows XP client IP address _____ Note: This is the IP address that you will use where b.b.b.b appears in the examples in this document. |
| <input type="checkbox"/> | Preshared key (minimum of 16 characters) _____ Note: Windows XP stores the presharedkey in cleartext in the registry, accessible by administrators. Active Directory stores IPSEC configuration policies and preshared keys in cleartext. ISS recommends that you use signed certificates identifying the Proventia M Series appliance and Windows XP client for better security. |
| <input type="checkbox"/> | IKE Phase 1 (Main Mode) Authentication <input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 |
| <input type="checkbox"/> | IKE Phase 1 Encryption <input type="checkbox"/> 3DES <input type="checkbox"/> DES <input type="checkbox"/> AES Note: If you select AES, select an AES key length: <input type="checkbox"/> 128 <input type="checkbox"/> 192 <input type="checkbox"/> 256 |
| <input type="checkbox"/> | IKE Phase 1 Key Lifetime Seconds _____ |
| <input type="checkbox"/> | IKE Phase 1 Key Lifetime Kbytes _____ |
| <input type="checkbox"/> | IKE Phase 1 Diffie-Hellman Group <input type="checkbox"/> Group1 <input type="checkbox"/> Group2 <input type="checkbox"/> Group5 |
| <input type="checkbox"/> | IKE Phase 2 (Quick Mode) Authentication <input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 |
| <input type="checkbox"/> | IKE Phase 2 Encryption <input type="checkbox"/> 3DES <input type="checkbox"/> DES <input type="checkbox"/> AES Note: If you select AES, select an AES key length: <input type="checkbox"/> 128 <input type="checkbox"/> 192 <input type="checkbox"/> 256 |
| <input type="checkbox"/> | IKE Phase 2 Key Lifetime Seconds _____ |
| <input type="checkbox"/> | IKE Phase 2 Key Lifetime Kbytes _____ |
| <input type="checkbox"/> | IKE Phase 2 Diffie-Hellman Group <input type="checkbox"/> None <input type="checkbox"/> Group1 <input type="checkbox"/> Group2 <input type="checkbox"/> Group5 |
| <input type="checkbox"/> | Access Policies |

Table 2: Checklist before configuring VPN tunnel

Task Overview for Establishing L2TP/IPSEC Connections with Certificate Authentication

Introduction This topic describes the tasks required to establish an L2TP/IPSEC connection between the Proventia appliance and Windows clients using certificate authentication.

Guideline You are creating a VPN tunnel in which the original IP addresses are preserved in the ESP, so you do not need NAT for the subnets.

Required tasks for certificate authentication To establish the L2TP/IPSEC connection using certificate authentication, you must complete tasks shown in the following table:

| Task | Description |
|------|---|
| 1 | Complete the W2K/XP to M Series VPN wizard. Reference: See “Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using Certificate Authentication” on page 6. |
| 2 | Add IP addresses for remote Windows clients. Reference: See “Adding IP Addresses for Remote Windows Clients” on page 8. |
| 3 | Enable the firewall access policy in Proventia Manager to enable ISAKMP traffic. Reference: See “Enabling an Access Policy to Enable ISAKMP Traffic to the Proventia Appliance” on page 11. |
| 4 | Create firewall access policies in Proventia Manager to enable traffic between subnets. Reference: See “Creating Access Policies to Enable Traffic from Subnet A to Subnet B” on page 12. |
| 5 | Configure the Windows XP client for certificate authentication. Reference: See “Configuring Certificates on the Windows Client” on page 16. |

Table 3: Required tasks for L2TP/IPSEC using certificate authentication

Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using Certificate Authentication

Introduction

This topic describes how to establish an L2TP/IPSEC VPN connection between an M Series appliance and a Windows 2000 or XP VPN client using the VPN Wizard. This VPN connection uses certificate authentication.

Note: This is the first of six tasks to configure an L2TP/IPSEC VPN connection with certificate authentication. To continue, go to the next task: “Adding IP Addresses for Remote Windows Clients” on page 8.

What this wizard generates

After you complete the wizard and click **Save Changes**, the wizard creates access policies for the VPN connection. To remove the connection, you must use Proventia Manager to remove each rule or policy individually. The following table describes the policies that the wizard generates:

| This policy... | Contains this text in the Comment column... |
|---|---|
| Access policy to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to the Proventia appliance external interface | Enable this rule for VPN Connectivity |
| Access policy to allow L2TP traffic on UDP port 1701 | Enable this rule for L2TP/IPSec VPN |
| Access policy to allow L2TP traffic on UDP port 4500 | Enable this rule for L2TP/IPSec VPN |

Order of access policies

The appliance processes access policies in the order that they appear in the Access Policy list.

Accessing the wizard

To access the Firewall/VPN W2K and XP to M Series Wizard:

1. In the navigation pane, click + to expand the **Firewall/VPN** node.
2. Click + to expand the **VPN Wizards** node.
3. Select **W2k/XP to M Series**.

The Firewall/VPN W2K and XP to M Series Wizard page appears.

Configuring wizard settings

Configure the W2K/XP to M Series VPN Wizard with the settings shown in the following table:

| Item | Description |
|------|--|
| Name | Descriptive name Note: You can type up to 32 alphanumeric characters in this field. Example To_WinXP |

Table 4: W2K/XP to M Series Wizard settings for certificate authentication

| Item | Description |
|---------------------|---|
| Comment | <p>Descriptive comment</p> <p>Note: You can type up to 256 characters in this field.</p> <p>Example</p> <p>L2TP tunnel to WinXP</p> |
| L2TP End Point | <p>The IP address you will use for the local endpoint. Select Static Address, and then type the address in the IP Address field in dotted decimal format.</p> <p>Important: Use this option for most Windows L2TP/IPSEC clients. The L2TP End Point IP Address is the IP address for the appliance side of the L2TP VPN tunnel. This IP address is the endpoint of the local VPN connection. The L2TP endpoint IP address for the appliance must be a fixed, globally unique IP address, and should not be in the L2TP IP Address Pool or used for any other interface on the appliance.</p> <p>Examples:</p> <ul style="list-style-type: none"> • L2TP End Point IP Address: 192.168.2.1 • L2TP IP Address Pool: 192.168.2.2-192.168.2.254 |
| Local ID | <p>The external interface IP address of the Proventia appliance. Select Static Address, and then type the address in the IP Address field in dotted decimal format.</p> <p>Example</p> <p>a . a . a . a</p> |
| Remote ID | <p>DER ASN1 DN</p> <p>This is the certificate value that all clients share, and must be in the x.509 certificate given to each client. Options are:</p> <p>/C (country)</p> <p>/S (state or province)</p> <p>/L (locality or city)</p> <p>/O (organization or business)</p> <p>/OU (organizational unit or department)</p> <p>/CN (common name)</p> <p>Example</p> <p>/C=US /S=GA /L=Atlanta /O=ISS /OU=QA /CN=mycomputer</p> <p>Note: Use the * symbol as a wildcard to match any value in that field of the certificate.</p> |
| Authentication Mode | RSA SIGN |

Table 4: W2K/XP to M Series Wizard settings for certificate authentication (Continued)

Adding IP Addresses for Remote Windows Clients

Introduction

You must do the following for remote Windows clients:

- add the IP addresses that the appliance assigns to when they connect
- add username/password pairs

Note: This is the second of six tasks to configure either of the following:

- L2TP/IPSEC VPN connection with certificate authentication
- L2TP/IPSEC VPN connection with CHAP authentication

To continue, go to the next task: “Enabling an Access Policy to Enable ISAKMP Traffic to the Proventia Appliance” on page 11.

Consideration

You can use the Proventia appliance to enter the IP addresses in the IP Pool and add username/password pairs, or you can use RADIUS to authenticate the IP address and login information for the remote clients. For more information, see your RADIUS server documentation.

Adding IP addresses

To add the IP addresses on the appliance:

1. In the navigation pane, click + to expand the **Firewall/VPN** node.
2. Select **Settings**.
3. Select the **VPN Advanced** tab.
4. Select the **L2TP IP Pool** tab.
5. Click **Add**.
6. Specify the IP address range for the L2TP end points in the **IP Range** field.

Note: These are the IP addresses that you want to assign to the remote Windows clients.

L2TP IP address range options are shown in the following table:

| If you want to... | Then do this... |
|---|--|
| Use a static IP address range | Select Static Address Range , and then type the starting and ending IP addresses in the IP Address Range field in dotted decimal format. |
| Use an Address Name network object | Select Address Name , and then select an address entry from the list. Note: Click Configure... to add or edit an Address Name network object. |
| Use a Dynamic Address Name network object | Select Dynamic Address Name , and then select a dynamic address name entry from the list. Note: Click Configure... to add or edit a Dynamic Address Name network object. |

7. Click **OK**.

8. Click **Save Changes**.

Creating a VPN Users List entry with username/password pairs

To create a VPN Users list entry with username/password pairs:

1. In the navigation pane, click + to expand the **Firewall/VPN** node.
2. Select **Settings**.
3. Select the **VPN Advanced** tab.
4. Select the **VPN Users** tab.
5. Click **Add**.
6. Type the VPN user's name in the **User Name** field.
7. To set the user's password, click **Set Password**, and type the user's password in the **Password** field.
8. Type the user's password in the **Confirm Password** field, and then click **OK**.
9. Do one of the following:
 - In the Proventia Manager interface, click **Save Changes**.
 - In the SiteProtector interface, click **OK**

Creating Related Access Policies for the Proventia Appliance

Introduction

You must create additional access policies to do the following:

- enable Internet Security Association and Key Management Protocol (ISAKMP) traffic to the Proventia appliance external interface
Reference: See “Enabling an Access Policy to Enable ISAKMP Traffic to the Proventia Appliance” on page 11.
- enable traffic from subnet A to subnet B without NAT (Network Address Translation)
Reference: See “Creating Access Policies to Enable Traffic from Subnet A to Subnet B” on page 12.

Enabling an Access Policy to Enable ISAKMP Traffic to the Proventia Appliance

Introduction

Although you have created a VPN tunnel from the Windows XP client to the Proventia VPN server, you must configure the firewall to accept or deny traffic from the VPN client. To do this, enable ISAKMP traffic to the Proventia appliance external interface.

This access policy is disabled by default. You must enable it to allow VPN traffic.

To enable ISAKMP traffic to the Proventia appliance, enable the access policy that allows VPN traffic. You can identify this policy by the **Comment** field that includes the following default text:

```
Enable this rule for VPN Connectivity
```

Note: This is the third of six tasks to configure either of the following:

- L2TP/IPSEC VPN connection with certificate authentication
- L2TP/IPSEC VPN connection with CHAP authentication

To continue, go to “Creating Access Policies to Enable Traffic from Subnet A to Subnet B” on page 12.

ISAKMP access policy general settings

Define the access policy general settings as shown in the following table:

| Item | Setting |
|-------------|---------------------------------------|
| Enabled | Selected |
| Action | Allow |
| Log Enabled | Not selected (optional) |
| Comment | Enable this rule for VPN Connectivity |

Table 5: ISAKMP access policy general settings for the Proventia appliance

ISAKMP access policy remaining settings

Define the remaining access policy settings as shown in the following table:

| On this subtab... | Select this item... | With this setting... |
|---------------------|-------------------------|--|
| Protocol | Any | N/A |
| Source Address | Single IP Address | The external interface IP address for the Windows XP client Example b . b . b . b |
| Source Port | Any | N/A |
| Destination Address | Self | N/A |
| Destination Port | Specify Network Objects | ISAKMP_UDP |

Table 6: ISAKMP access policy remaining settings

Creating Access Policies to Enable Traffic from Subnet A to Subnet B

Introduction

You must create two additional access policies on the Proventia appliance to allow all traffic from subnet A to subnet B:

- a policy to allow inbound traffic
- a policy to allow outbound traffic

Note: This is the fourth of six tasks to configure either of the following:

- L2TP/IPSEC VPN connection with certificate authentication
- L2TP/IPSEC VPN connection with CHAP authentication

To continue, go to “Creating NAT Rules” on page 14.

Inbound access policy general settings

Define the inbound access policy general settings as defined in the following table:

| Item | Setting |
|-------------|--|
| Enabled | Selected |
| Action | Allow |
| Log Enabled | Not selected (optional) |
| Comment | Access policy to allow traffic from remote Windows XP client |

Table 7: *Inbound access policy general settings*

Inbound access policy remaining settings

Define the remaining inbound access policy settings as shown in the following table:

| On this subtab... | Select this item... | With this setting... |
|---------------------|--------------------------------------|--|
| Protocol | Any | N/A |
| Source Address | Single IP Address | The IP address of the Windows XP client Example b . b . b . b |
| Source Port | Any | N/A |
| Destination Address | Network Address/#Network Bits (CIDR) | The network IP address and mask for subnet A. Example 192 . 168 . 1 . 0 / 24 |
| Destination Port | Any | N/A |

Table 8: *Inbound access policy remaining settings*

Outbound access policy general settings

Define the outbound access policy general settings as defined in the following table:

| Item | Setting |
|-------------|--|
| Enabled | Selected |
| Action | Allow |
| Log Enabled | Not selected (optional) |
| Comment | Access policy to allow traffic out to remote Windows XP client |

Table 9: *Outbound access policy general settings*

Outbound access policy remaining settings

Define the remaining outbound access policy settings as shown in the following table:

| On this subtab... | Select this item... | With this setting... |
|---------------------|--------------------------------------|--|
| Protocol | Any | N/A |
| Source Address | Network Address/#Network Bits (CIDR) | The network mask for subnet A. Example 192 . 168 . 1 . 0 /24 |
| Source Port | Any | N/A |
| Destination Address | Single IP Address | The IP address of the Windows XP client Example b . b . b . b |
| Destination Port | Any | N/A |

Table 10: *Outbound access policy remaining settings*

Creating NAT Rules

Introduction

In firmware version 2.1 and later, you must add NAT (Network Address Translation) rules to bypass NAT and insure that the appliance does not translate packets that travel between subnets. The additional NAT rules are as follows:

- a Source NAT Rule
- a Destination NAT Rule

Note: This is the fifth of six tasks to configure either of the following:

- L2TP/IPSEC VPN connection with certificate authentication
To continue, go to the last task: “Configuring Certificates on the Windows Client” on page 16.
- L2TP/IPSEC VPN connection with CHAP authentication
To continue, go the last task: “Configuring the Windows XP Client for L2TP/IPSEC VPN Connection Using CHAP Authentication” on page 21

Source NAT Rule general settings

Create a Source NAT Rule with general settings as defined in the following table:

| Item | Setting |
|---------|-------------------------------|
| Name | WinXP_BypassNAT_Src |
| Enabled | Selected |
| Comment | Source NAT Rule to bypass NAT |

Table 11: *Source NAT Rule general settings*

Source NAT Rule remaining settings

Define the remaining Source NAT Rule settings as shown in the following table:

| On this subtab... | Select this item... | With this setting... |
|---------------------|--------------------------------------|---|
| Protocol | Any | N/A |
| Source Address | Network Address/#Network Bits (CIDR) | The IP address and subnet mask for subnet A Example 192.168.1.0/24 |
| Destination Address | Single IP Address | The IP address of the Windows XP client Example b.b.b.b |
| Destination Port | Any | N/A |
| Translated Address | Do Not Translate | N/A |

Table 12: *Source NAT Rule remaining settings*

Note: Make sure that the Source NAT Rule is in the first position in the Source NAT Rules table.

Destination NAT Rule general settings

Create a Destination NAT Rule with general settings as defined in the following table:

| Item | Setting |
|---------|------------------------------------|
| Name | WinXP_BypassNAT_Dst |
| Enabled | Selected |
| Comment | Destination NAT Rule to bypass NAT |

Table 13: *Destination NAT Rule general settings*

Destination NAT Rule remaining settings

Define the remaining Destination NAT Rule settings as shown in the following table:

| On this subtab... | Select this item... | With this setting... |
|---------------------|--------------------------------------|---|
| Protocol | Any | N/A |
| Source Address | Single IP Address | The IP address of the Windows XP client Example b . b . b . b |
| Destination Address | Network Address/#Network Bits (CIDR) | The network mask for subnet A. Example 192 . 168 . 1 . 0/24 |
| Destination Port | Any | N/A |
| Translated Address | Do Not Translate | N/A |

Table 14: *Destination NAT Rule remaining settings*

Note: Make sure that the Destination NAT Rule is in the first position in the Destination NAT Rules table.

Configuring Certificates on the Windows Client

Introduction

This topic describes how to install and verify certificates on the Windows 2000 or XP client.

Installing the certificate

Follow the instructions from your Certificate Authority to configure the client certificate. The following instructions are for the Microsoft Certificate Authority included with Windows 2000 Server.

To install the certificate:

1. On the client computer, login with an account with administrative privileges.
2. Open the Web site for the Microsoft Certificate Authority.

Example

<http://certserver.mycompany.com/certserv>

3. Select **Request a certificate**, and then click **Next**.
4. Select **Advanced Request**, and then click **Next**.
5. Select **Submit a certificate request to this CA using a form**, and then click **Next**.
6. Complete the form with information for your organization.
Important: Do not use the email field. Due to the design differences between Windows 2000 and Windows XP, you must leave this field blank.
7. Select **IPSec Certificate** from the **Intended Purpose** list.
8. Select **Microsoft Base Crypto Provider v1.0**.
9. Select one of the following key sizes:
 - 512
 - 1024
10. Select one of the following for the **Hash Algo** field:
 - SHA-1
 - MD5
11. Select **Store certificate in the local computer certificate store**.
12. Click **Submit**.
13. Click **Install Certificate**.

The certificate installs automatically.

Verifying the certificate

To verify that the certificate was installed correctly on the client:

1. On the client computer, login with an account with administrative privileges.
2. Run MMC .EXE.
3. Select **File** → **Add/Remove Snap In**.
4. Click **Add**.
5. Select **Certificates**, and then click **Add**.

6. Select **Computer Account**, and then click **Next**.
7. Select **Local Computer**, and then click **Finish**.
8. Click **Close**.
9. Click **OK**.
10. Expand the **Certificates** tree.
11. Right-click the Personal folder and the Certificates folder.
The certificate should be listed.
12. Double click on the certificate.
Note: The certificate states “This certificate cannot be verified up to a trusted certificate authority”. This is because the Microsoft Certificate Authority Root Certificate is not installed on this computer.
13. Click on the Certificate Path tab.
14. Highlight the root CA certificate in the tree, and then click **View Certificate**.
The following message displays:

```
This CA Root certificate is not trusted. To enable trust, install
this certificate in the Trusted Root Certification Authorities store.
```
15. Click the Details tab, and then click **Copy to File**.
16. Complete the wizard and export the CA Root Certificate.
Note: ISS suggests that you use the DER format.
17. Browse to the certificate file you exported, and right click it.
18. Click **Install Certificate**.
19. Click **Next**.
20. Select **Place all certificates in the following store**.
21. Click **Browse**, and then select **Trusted Root Certification Authorities**.
22. Click **OK**.
23. Click **Next**, and then click **Finish** on the Certificate Import Wizard.
24. Click **Yes** on the Root Certificate Store dialog to add the certificate.
25. Return to the MMC application, and view the local certificate again in the /Personal/ Certificates folder.
The certificate should now appear as valid.
26. Exit the MMC application.

Task Overview for Establishing L2TP/IPSEC Connections with CHAP Authentication

Introduction

This topic describes the tasks required to establish an L2TP/IPSEC connection between the Proventia appliance and Windows clients using CHAP authentication (preshared keys).

Note: Windows XP stores the presharedkey in cleartext in the registry, accessible by administrators. Active Directory stores IPSEC configuration policies and preshared keys in cleartext. ISS recommends that you use signed certificates identifying the Proventia M Series appliance and Windows XP client for better security.

Required tasks for CHAP authentication

To establish the L2TP/IPSEC connection using CHAP authentication, you must complete tasks shown in the following table:

| Task | Description |
|------|---|
| 1 | Complete the W2K/XP to M Series VPN wizard. Reference: See “Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using CHAP Authentication” on page 19. |
| 2 | Add IP addresses for remote Windows clients. Reference: See “Adding IP Addresses for Remote Windows Clients” on page 8. |
| 3 | Enable the firewall access policy in Proventia Manager to enable ISAKMP traffic. Reference: See “Enabling an Access Policy to Enable ISAKMP Traffic to the Proventia Appliance” on page 11. |
| 4 | Create firewall access policies in Proventia Manager to enable traffic between subnets. Reference: See “Creating Access Policies to Enable Traffic from Subnet A to Subnet B” on page 12. |
| 5 | Create NAT rules. Reference: See “Creating NAT Rules” on page 14. |
| 6 | Configure the Windows XP client for CHAP authentication. Reference: See “Configuring the Windows XP Client for L2TP/IPSEC VPN Connection Using CHAP Authentication” on page 21. |

Table 15: Required tasks for L2TP/IPSEC using CHAP authentication

Configuring the Proventia VPN Wizard for an L2TP/IPSEC VPN Connection Using CHAP Authentication

Introduction

This topic describes how to establish an L2TP/IPSEC VPN connection between an M Series appliance and a Windows 2000 or XP VPN client using the VPN Wizard. This VPN connection uses CHAP authentication (preshared keys).

Note: This is the first of six tasks to configure an L2TP/IPSEC VPN connection with CHAP authentication. To continue, go to the next task: "Adding IP Addresses for Remote Windows Clients" on page 8.

What this wizard generates

After you complete the wizard and click **Save Changes**, the wizard creates Access and IPSEC policies for the VPN connection. To remove the connection, you must use Proventia Manager to remove each rule or policy individually. This wizard creates the following:

- one IPSEC policy
- two Access policies

Using a Pre Shared Key

When the appliance is configured to use a Pre Shared Key to authenticate, only Windows XP clients can connect to the appliance. This is a limitation of the L2TP/IPSEC implementation in Windows 2000. For information about this limitation and ways to alter the default behavior of Windows 2000, see the following Knowledgebase article:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;240262>

Accessing the wizard

To access the Firewall/VPN W2K and XP to M Series Wizard:

1. In the navigation pane, click + to expand the **Firewall/VPN** node.
2. Click + to expand the **VPN Wizards** node.
3. Select **W2k/XP to M Series**.

The Firewall/VPN W2K and XP to M Series Wizard page appears.

Configuring wizard settings

Configure the W2K/XP to M Series VPN Wizard with the settings shown in the following table:

| Item | Description |
|---------|---|
| Name | Descriptive name Note: You can type up to 32 alphanumeric characters in this field. Example <code>To_WinXP</code> |
| Comment | Descriptive comment Note: You can type up to 256 characters in this field. Example <code>L2TP tunnel to WinXP</code> |

Table 16: W2K/XP to M Series Wizard settings for CHAP authentication

| Item | Description |
|---------------------|---|
| L2TP End Point | <p>The IP address you will use for the local endpoint. Select Static Address, and then type the address in the IP Address field in dotted decimal format.</p> <p>Important: Use this option for most Windows L2TP/IPSEC clients. The L2TP End Point IP Address is the IP address for the appliance side of the L2TP VPN tunnel. This IP address is the endpoint of the local VPN connection. The L2TP endpoint IP address for the appliance must be a fixed, globally unique IP address, and should not be in the L2TP IP Address Pool or used for any other interface on the appliance.</p> <p>Examples:</p> <ul style="list-style-type: none"> • L2TP End Point IP Address: 192.168.2.1 • L2TP IP Address Pool: 192.168.2.2-192.168.2.254 |
| Local ID Data | <p>The external interface IP address of the Proventia appliance. Select Static Address, and then type the address in the IP Address field in dotted decimal format.</p> <p>Example a . a . a . a</p> |
| Remote ID | <p>FQDN</p> <p>Note: The Remote ID is the value shared between all clients.</p> <p>Example test.com</p> <p>Important: These instructions assume that each Windows XP client will be behind a NAT device and will use NAT-T during the connection. If the Windows XP clients are not behind a NAT device, select Static IP Address from the Remote ID list, and then type 0 . 0 . 0 . 0 in the Remote ID field. This Remote ID entry allows any IP address as the originating peer of the IPSEC component of the VPN tunnel.</p> |
| Authentication Mode | Pre Shared Key |
| Pre-Shared Key | <p>A text string value of at least 16 alphanumeric characters.</p> <p>Example 1234567890abcdef</p> <p>Note: Use the same text string for the Windows clients.</p> |

Table 16: W2K/XP to M Series Wizard settings for CHAP authentication (Continued)

Configuring the Windows XP Client for L2TP/IPSEC VPN Connection Using CHAP Authentication

Introduction This topic describes how to configure the Windows 2000/XP client for an L2TP/IPSEC connection using CHAP authentication (preshared keys).

NAT-T support patch from Microsoft These instructions assume that the Windows client will be behind a NAT appliance. Microsoft released a patch for Windows 2000 and Windows XP that added support for NAT-T within the IKE negotiations of L2TP/IPSEC. You must install this patch if you are running Service Pack 1 and if the Windows client is behind a NAT device. The patch is located at the following link:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;818043>

NAT-T behavior in Windows XP SP 2 The default behavior for NAT-T within Windows XP Service Pack 2 has changed. Please see the following URL for more information:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;885407>

Procedure To configure the Windows client:

1. In the Windows desktop, click **Start**→**Control Panel**.
2. Do one of the following:
 - If the Control Panel is in Classic view, then double-click **System**.
 - If the Control Panel is in Category View, then click **Performance and Maintenance**, and then double-click **System**.
3. Select the Computer Name tab.
4. Click **Change**.
5. Click **More**.
6. In the **Primary DNS Suffix for this computer** field, type the primary DNS suffix shared by all clients.

Note: This value must be the same value in the corresponding L2TP/IPSEC Remote ID field on the Proventia appliance.

Example

`test.com`

7. Click **OK**, and allow the computer to reboot.
8. After the computer reboots, click **Start**→**Control Panel**.
9. Do one of the following:
 - If the Control Panel is in Classic view, then double-click **Network Connections**.
 - If the Control Panel is in Category View, then click **Network and Internet Connections**.
10. Click **Create a new connection**.

The New Connection Wizard appears.

11. Click **Next**.
12. Select **Connect to the network at my workplace**, and then click **Next**.
13. Select **Virtual Private Network connection**, and then click **Next**.
14. In the **Company Name** field, type a name for the connection, and then click **Next**.
15. In the **Host name or IP address** field, type the external IP address or the resolvable FQDN of the Proventia appliance.
16. Click **Next**.
17. In the **Create this connection for** area, select one of the following:
 - **Anyone's use**
 - **My use only**
18. Click **Next**.
19. Select the **Add a shortcut to this connection to my desktop** box, and then click **Finish**.

Configuring connection properties

To complete the configuration for the new connection:

1. On the Connect window, click **Properties**.
2. Select the Security tab.
3. Select **Advanced (custom settings)**.
4. Click **Settings**.
5. Select **Optional encryption** from the **Data encryption** list.
6. Clear the **Microsoft CHAP (MS-CHAP)** check box.
7. Clear the **Microsoft CHAP Version 2 (MS-CHAP v2)** check box.
8. Select the **Challenge Handshake Authentication Protocol (CHAP)** check box.
Important: Make sure that only the Challenge Handshake Authentication Protocol check box is selected.
9. If a warning dialogue appears, select **Yes**.
10. Select **IPSec Settings**.
11. Select the **Use pre-shared key for authentication** check box.
12. In the **Key** field, type the preshared key you configured for the Proventia appliance, and then click **OK**.
13. Select the Networking tab.
14. Select **L2TP IPSec VPN** from the **Type of VPN** list, and then click **OK**.
15. Type your Windows username in the **User name** field.
16. Type your Windows password in the **Password** field, and then click **Connect**.

Overriding default Windows VPN client behavior

By default, the Windows VPN client routes ALL traffic through the VPN link. If you override this behavior, you must configure routes manually.

Note: Another option to override the default Windows VPN client behavior is to distribute, pre-packaged VPN Setups using the Remote Administration Toolkit from Microsoft. See your Microsoft documentation for more information.

To override the default Windows VPN client behavior:

1. Click **Start** → **Control Panel**.
2. Do one of the following:
 - If the Control Panel is in Classic view, then double-click **Network Connections**.
 - If the Control Panel is in Category View, then click **Network and Internet Connections**.
3. Right click on the VPN connection, and then select **Properties**.
4. Select the Networking tab.
5. Select **TCP/IP**.
6. Click **Properties**.
7. Click **Advanced**.
8. Select the General tab.
9. Clear the **Use default gateway on remote network** check box.
10. Click **OK**.

Troubleshooting

Introduction This topic contains Windows client error messages and steps for troubleshooting.

Error 789 This error displays the following text:

```
Error 789: The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.
```

Possible solutions include the following:

- If the Windows client is configured for certificate authentication, make sure the certificate is installed on the Windows client. Perform the procedure “Verifying the certificate” on page 16.
- The IPSEC service may not be running on the Windows client. To verify, start the IPSEC service, type the following command:

```
net start policyagent
```

If the command fails, uninstall any third party programs that replace the IPSEC stack on Windows, such as SAFEnet Softremote.

Error 781 This error displays the following text:

```
Error 781: no valid certificate
```

If you see this error, then a problem exists with the certificate that the L2TP/IPSEC client is attempting to use. To identify the problem, do the following:

- To verify that the trusted root CA that issued the certificate is installed on the Windows client, perform the procedure “Verifying the certificate” on page 16.
- Verify that the certificate was imported correctly so that it exists for the local computer certificate. Do the following:
 - Run MMC.EXE.
 - Add the certificate snap-in for Local Certificate management, as described in the procedure “Verifying the certificate” on page 16.
 - Double-click the certificate, and verify that the following text appears on the General tab:

```
You have a private key that corresponds to this certificate
```

If this text does not appear, then you may not have imported the certificate from an PKCS#12 container. All certificates imported for use in L2TP/IPSec must be in PKCS#12 format.

Copyright © 2003-2005, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, and Proventia are trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are marks and names of their owners as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.