Table of Contents

1. Introduction
   1.1. Audience and Purpose of this Document
   1.2. Available Guides
   1.3. What is the aXsGUARD Gatekeeper?
   1.4. About VASCO

2. General Concepts
   2.1. Overview
   2.2. What is a Virtual Private Network?
   2.3. What is PPTP?
      2.3.1. Protocol Description
      2.3.2. Key Elements of PPTP Security
   2.4. Standard PPTP Deployment
   2.5. Routing Scenarios
      2.5.1. Overview
      2.5.2. Source and Destination Address in Different IP Ranges
      2.5.3. Source and Destination address in the Same IP Range
   2.6. Firewalls and PPTP

3. PPTP Server Configuration
   3.1. Overview
   3.2. Activating the PPTP Server
   3.3. General Configuration Settings
   3.4. Authentication Settings
      3.4.1. Recommended Method
      3.4.2. Supported Authentication Methods
      3.4.3. Configuring the Authentication Method
   3.5. User Settings
   3.6. PPTP Firewall Settings
      3.6.1. Overview
      3.6.2. Allowing PPTP Traffic
      3.6.3. Firewall Rights
      3.6.4. Example of Firewall Settings for PPTP
   3.7. Logging
4. **PPTP Client Configuration**

4.1. Overview  
4.2. Client-Side Firewall  
4.3. Windows XP Configuration  
4.4. Windows Vista Configuration  
4.5. Windows 7 Configuration

5. **Troubleshooting**

5.1. Client-Side Troubleshooting  
5.2. Server-Side Troubleshooting

6. **Support**

6.1. Overview  
6.2. If you encounter a problem  
6.3. Return procedure if you have a hardware failure

**Alphabetical Index**
List of Figures

2.1. VPN Concept
2.2. PPTP Packet
2.3. PPTP Control and Data Channel
2.4. Listing the PPP Device with ipconfig
2.5. PPTP Client and PPTP Server with different IP ranges
2.6. PPTP Client and PPTP Server in same IP Range
2.7. Consequences of Compromised Client
3.1. PPTP Feature Activation
3.2. PPTP General Configuration Settings
3.3. PPTP Authentication Settings
3.4. User Settings
3.5. Firewall Configuration
3.6. Automatic Activation of Firewall Rules
3.7. User Level Firewall Settings
3.8. PPTP Log entries
4.1. Windows XP Network Connections
4.2. Connecting to the Network at my Workplace
4.3. Virtual Private Connection
4.4. Connection Name
4.5. VPN Server Selection
4.6. PPTP VPN Properties
4.7. Require Data Encryption
4.8. Windows Vista PPTP Setup
4.9. Set up a Connection or Network
4.10. Connect to a Workplace
4.11. Use My Internet Connection
4.12. Connection IP and Description
4.13. User Name and Password Screen
4.14. Final Configuration Step
4.15. Connecting to the PPTP Server
4.16. Connection Successful
4.17. PPTP Connection Status
4.18. Windows 7 Control Panel
4.19. Windows 7 Control Panel
4.20. Windows 7 Network and Sharing Center
4.21. Set up a New Connection or Network
4.22. Connect to a Workplace
4.23. Creating a New Connection
4.24. Creating a New Connection
4.25. PPTP Connection Settings
4.26. PPTP Connection Settings
4.27. PPTP Status
5.1. Include Windows Logon Domain
5.2. PPTP Error 619
List of Tables

3.1. PPTP General Settings
3.2. PPTP User Settings
3.3. User Level Firewall Settings
List of Examples

3.1. Restricting access to two LAN servers
Document Version. This is version 1.7 of the aXsGUARD Gatekeeper PPTP How To.

VASCO Products. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH are referred to in this document as ‘VASCO’. VASCO Products comprise Hardware, Software, Services and Documentation. This document addresses potential and existing VASCO customers and has been provided to you and your organization for the sole purpose of helping you to use and evaluate VASCO Products. As such, it does not constitute a license to use VASCO Software or a contractual agreement to use VASCO Products.

Disclaimer of Warranties and Limitations of Liabilities. VASCO Products are provided ‘as is’ without warranty or conditions of any kind, whether implied, statutory, or related to trade use or dealership, including but not limited to implied warranties of satisfactory quality, merchantability, title, non-infringement or fitness for a particular purpose. VASCO, VASCO DISTRIBUTORS, RESELLERS AND SUPPLIERS HAVE NO LIABILITY UNDER ANY CIRCUMSTANCES FOR ANY LOSS, DAMAGE OR EXPENSE INCURRED BY YOU, YOUR ORGANIZATION OR ANY THIRD PARTY (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF DATA) ARISING DIRECTLY OR INDIRECTLY FROM THE USE, OR INABILITY TO USE VASCO SOFTWARE, HARDWARE, SERVICES OR DOCUMENTATION, REGARDLESS OF THE CAUSE OF THE LOSS, INCLUDING NEGLIGENCE, EVEN IF VASCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR IF THEY WERE FORESEEABLE. OUR MAXIMUM AGGREGATE LIABILITY TO YOU, AND THAT OF OUR DISTRIBUTORS, RESELLERS AND SUPPLIERS SHALL NOT EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. THE LIMITATIONS IN THIS SECTION SHALL APPLY WHETHER OR NOT THE ALLEGED BREACH OR DEFAULT IS A BREACH OF A FUNDAMENTAL CONDITION OR TERM, OR A FUNDAMENTAL BREACH. THIS SECTION WILL NOT APPLY ONLY WHEN AND TO THE EXTENT THAT APPLICABLE LAW SPECIFICALLY REQUIRES LIABILITY DESPITE THE FOREGOING EXCLUSIONS AND LIMITATIONS.

Intellectual Property and Copyright. VASCO Products contain proprietary and confidential information. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights. No part of these Products may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted by VASCO or its authorized licensee in writing. This document is protected under US and international copyright law as an unpublished work of authorship. No part of it may be transferred, disclosed, reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, for any purpose, except as expressly permitted in writing by VASCO or its authorized licensee.

Trademarks. VASCO®, VACMAN®, IDENTIKEY®, aXsGUARD™, DIGIPASS®, DIGIPASS as a Service™ and the ® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. Other company brand or product names or other designations, denominations, labels and/or other tags, titles, as well as all URLs (Internet addresses) linked to such designations or communications (irrespective of whether protected by intellectual property law or not), mentioned in VASCO Products may be the trademarks or registered trademarks or be part of any other entitlement of their respective owners.

RADIUS Disclaimer. Information on the RADIUS server provided in this document relates to its operation in the DIGIPASS as a Service environment. We recommend that you contact your NAS/RAS vendor for further information.

Copyright © 2011 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved.
Chapter 1. Introduction

1.1. Audience and Purpose of this Document

In this How To, we explain the basic principles of PPTP and how to deploy the aXsGUARD Gatekeeper PPTP server in your network. This document is intended for technical personnel and network administrators.

In Chapter 2, General Concepts, we briefly explain the concept of Virtual Private Networking (VPN) and PPTP.

In Chapter 3, PPTP Server Configuration, we explain the different configuration settings of the PPTP server, such as acceptable IP ranges, DNS settings and recommended user settings. We also explain how to implement DIGIPASS authentication for PPTP, as this is the most secure authentication method.

In Chapter 4, PPTP Client Configuration, we explain how to configure your Windows XP, Windows Vista and Windows 7 client to successfully establish a PPTP connection with the aXsGUARD Gatekeeper PPTP server.

In Chapter 5, Troubleshooting, some solutions are offered to solve difficulties.

In Chapter 6, Support, we explain how to request support and return hardware for replacement.

As software development is an ongoing process, the screens included in this guide may slightly differ from the software version installed on your aXsGUARD Gatekeeper appliance.

1.2. Available Guides

Other documents in the set of aXsGUARD Gatekeeper documentation include:

- aXsGUARD Gatekeeper Installation Guide, which explains how to set up the aXsGUARD Gatekeeper, and is intended for technical personnel or system administrators.
- How to guides, which provide detailed information on the configuration of each of the features available as add-on modules (explained in Section 1.3, “What is the aXsGUARD Gatekeeper?”). These guides cover specific features such as:
  - aXsGUARD Gatekeeper Authentication
  - aXsGUARD Gatekeeper Firewall
  - aXsGUARD Gatekeeper Single Sign-On
  - aXsGUARD Gatekeeper VPN
  - aXsGUARD Gatekeeper Reverse Proxy
  - aXsGUARD Gatekeeper Directory Services
Access to aXsGUARD Gatekeeper guides is provided through the permanently on-screen **Documentation** button in the aXsGUARD Gatekeeper Administrator Tool.

Further resources available include:

- Context-sensitive help, which is accessible in the aXsGUARD Gatekeeper Administrator Tool through the **Help** button. This button is permanently available and displays information related to the current screen.
- Training courses covering features in detail can be organized on demand. These courses address all levels of expertise. Please see [http://www.vasco.com](http://www.vasco.com) for further information.

Welcome to aXsGUARD Gatekeeper security.

### 1.3. What is the aXsGUARD Gatekeeper?

The aXsGUARD Gatekeeper is an authentication appliance, intended for small and medium sized enterprises. In addition to strong authentication, the aXsGUARD Gatekeeper has the potential to manage all of your Internet security needs. Its modular design means that optional features can be purchased at any time to support, for example, e-mail and Web access control. The aXsGUARD Gatekeeper can easily be integrated into existing IT infrastructures as a stand-alone authentication appliance or as a gateway providing both authentication services and Internet Security.

Authentication and other features such as firewall, e-mail and Web access, are managed by security policies, which implement a combination of rules, for example, whether a user must use a DIGIPASS One-Time Password in combination with a static password for authentication. Security Policies are applied to specific users or groups of users and can also be applied to specific computers and the entire system.

### 1.4. About VASCO

VASCO is a world leader in strong authentication and e-signature solutions, specializing in online accounts, identities and transactions. As a global software company, VASCO serves a customer base of approximately 10,000 companies in over 100 countries, including approximately 1,500 international financial institutions. In addition to the financial sector, VASCO’s technologies secure sensitive information and transactions for the enterprise security, e-commerce and e-government industries.

For further information, please visit [http://www.vasco.com](http://www.vasco.com).
Chapter 2. General Concepts

2.1. Overview

In this section, we explain the general concepts of Virtual Private Networking (VPN), in particular the Point to Point Tunneling Protocol (PPTP). Topics covered in the section include:

- The key elements underpinning PPTP: authentication, tunneling and encryption.
- The standard PPTP deployment: how a PPTP client interacts with a PPTP server.

2.2. What is a Virtual Private Network?

A Virtual Private Network (VPN) is a network which uses a public (inherently insecure) network infrastructure, such as the Internet, to provide a private (secured) connection between hosts and network applications. A VPN also ensures the integrity of data as it traverses the Internet, through authentication, tunneling and encryption. In other words, a VPN allows roaming or remote users to securely connect to corporate LAN resources, such as shared folders, applications, databases or e-mail. Several VPN protocols are available, such as the PPTP protocol explained in this manual.

Figure 2.1. VPN Concept
2.3. What is PPTP?

2.3.1. Protocol Description

PPTP stands for Point to Point Tunneling Protocol and is an extension of the PPP protocol, defined per RFC 1171. PPTP allows organizations to use the Internet to securely transmit data across a VPN. It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet, which is referred to as tunneling or encapsulation. PPTP in its barest form works by encapsulating packets inside PPP packets, which are in turn encapsulated in Generic Routing Encapsulation (GRE) packets. The GRE packets are sent over IP to the destination PPTP server and back again. The image below shows the structure of a PPTP network packet.

![PPTP Packet Diagram]

Figure 2.2. PPTP Packet

2.3.2. Key Elements of PPTP Security

The PPTP protocol provides the following key security elements:
• Authentication: The VPN server verifies the VPN client’s identity and restricts VPN access to authorized users only (MS-CHAP and MS-CHAP v2). The VPN server may also provide audit and accounting capabilities to monitor who accessed which information and when.

• Tunneling: A technology that enables one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by another network. Tunneling is also referred to as encapsulation (see Section 2.3.1, “Protocol Description”) and is achieved by the GRE and PPP protocol.

• Encryption: To insure privacy, data transmission via the VPN over the Internet is rendered unreadable to unauthorized clients through encryption (MPPE).

• Compression: The process of reducing the amount of information necessary to transmit data.

**Authentication.** PPTP VPN servers use two authentication protocols:

• PAP: The Password Authentication Protocol is a simple authentication protocol to authenticate a user with a Network Access Server. PAP sends user names and passwords over the network in cleartext and is therefore insecure.

• CHAP: Stands for Challenge Handshake Authentication Protocol and functions as follows:

1. The PPTP VPN server sends a challenge to the requesting client.
2. The client uses this challenge and the password to calculate a response, which is sent to the server.
3. The PPTP VPN server checks the provided response against its own calculation of the expected response. If the received response matches, the server acknowledges the authentication; if not, the connection is terminated.

- PAP is not supported by the aXsGUARD Gatekeeper because it is insecure. Only MS-CHAP is supported.
- VASCO recommends DIGIPASS authentication, as this is the most secure option.

**Tunneling.** A VPN uses an IP tunneling mechanism where the packet formats and the addressing used by the VPN might be unrelated to the packet formats and addressing which is used to route the tunneled packet across the Internet (see Section 2.5, “Routing Scenarios” for more information about PPTP and Routing). For this reason, PPTP uses the Generic Routing Encapsulation (GRE) protocol. The GRE protocol is defined per RFC-1701, 1702 and 2784 and is identified as IP Protocol 47. GRE is used to implement several categories of encryption and network security. In its most basic form, GRE allows any network-layer protocol (or in some cases, protocols from other layers, e.g. Ethernet frames) to be encapsulated in any other network-layer protocol. In its current form, GRE has been implemented in most UNIX network stacks, routers and other network equipment and is widely supported.

**Encryption.** PPTP supports PPP-based data encryption mechanisms. The Microsoft implementation of PPTP supports optional use of Microsoft Point-to-Point Encryption (MPPE), based on the RSA/RC4 algorithm. 40 bit encryption is supported, but highly insecure (see Section 3.3, “General Configuration”)

© VASCO Data Security 2011
The aXsGUARD Gatekeeper enforces 128 bit encryption by default, as this is the most secure option.

**Compression.** Compression reduces the amount of information necessary to transmit data, hereby saving bandwidth and increasing the data transfer speed. PPTP uses the Compression Control Protocol (CCP) used by the PPP protocol. PPP negotiates MPPE (see above) with the aXsGUARD Gatekeeper PPTP server using CCP.

### 2.4. Standard PPTP Deployment

Two hosts are involved in the deployment of PPTP:

- A PPTP Client with access to the Internet.
- A PPTP Server, such as the aXsGUARD Gatekeeper PPTP server.

A PPTP connection between the client and the server consists of two channels, a control channel and a data channel. These are explained below.

**PPTP Control Channel.** The PPTP control channel is the initial channel which is negotiated between a PPTP client on the Internet and the aXsGUARD Gatekeeper PPTP server. A TCP connection is therefore made to the PPTP server on TCP port 1723, as shown in the illustration below. This control channel is used to negotiate tunnel parameters, such as the encryption method and the compression algorithm (see Section 2.3.2, “Key Elements of PPTP Security”). The PPTP control channel also establishes, manages, and releases the PPTP data channel.

**PPTP Data Channel.** Once the PPTP control channel is up, a second channel is negotiated to secure the data transfer within the tunnel. This is the PPTP data channel. On this data channel, PPTP uses the GRE protocol (see Section 2.3.2, “Key Elements of PPTP Security”) to encapsulate the PPP packets for secure delivery to the aXsGUARD Gatekeeper PPTP server. In turn, the aXsGUARD Gatekeeper PPTP server verifies and decapsulates these packets before delivery to the destination host in the LAN.

![Figure 2.3. PPTP Control and Data Channel](image)
2.5. Routing Scenarios

2.5.1. Overview

Once the PPTP VPN is up, a PPP interface with its own IP address is assigned to both the client and the PPTP server. The client’s interface settings can be viewed by running the `ipconfig` command from a Windows command prompt as shown below.

![Image of ipconfig output]

**Figure 2.4. Listing the PPP Device with ipconfig**

On the client side, all network traffic not destined for the local network is routed through the PPP interface, until the PPTP connection is terminated. This means that a strict Firewall Policy should be enforced on the PPTP client and server (see Section 2.6, “Firewalls and PPTP” and Section 3.6, “PPTP Firewall Settings”). On the server side, only PPTP traffic is routed through this interface. Different routing scenarios apply, depending on the network address which is assigned to the client’s PPP interface. These are explained in the following sections.

2.5.2. Source and Destination Address in Different IP Ranges

The client’s PPP interface has an IP address in a different IP range than the LAN of the PPTP server, as shown in the image below. Standard routing applies.
The PPTP client with IP 10.0.0.1 sends a request to a server in the aXsGUARD Gatekeeper LAN. This server has IP 192.168.250.200. The server receives the request and replies using the client’s IP address 10.0.0.1 as its destination. Since this IP address (10.0.0.1) is in a different range than the aXsGUARD Gatekeeper LAN, the packet is automatically routed through the PPP interface (gateway) of the aXsGUARD Gatekeeper.

Figure 2.5. PPTP Client and PPTP Server with different IP ranges

The PPTP client with IP 10.0.0.1 sends a request to a server in the aXsGUARD Gatekeeper LAN. This server has IP 192.168.250.200. The server receives the request and replies using the client’s IP address 10.0.0.1 as its destination. Since this IP address (10.0.0.1) is in a different range than the aXsGUARD Gatekeeper LAN, the packet is automatically routed through the PPP interface (gateway) of the aXsGUARD Gatekeeper.

2.5.3. Source and Destination address in the Same IP Range

The client’s PPP interface has an IP address in the same IP range as the LAN IP of the PPTP server, as shown in the image below. Traffic can only be routed correctly using Proxy ARP, which is explained below.
The PPTP client with IP 192.168.250.100 sends a request to a server in the aXsGUARD Gatekeeper LAN. This server has IP 192.168.250.200. The server replies using the client’s IP address 192.168.250.100 as its destination. Since this address is within the same IP range as the aXsGUARD Gatekeeper LAN, the contacted server “thinks” it can reply directly via the LAN using ARP. This is not the case, since the reply needs be routed back to the originating client and not the LAN. The aXsGUARD Gatekeeper solves this problem by using Proxy ARP, as explained below.

**PROXY ARP.** Proxy ARP is a technique in which a host, usually a router, answers ARP requests intended for another host by supplying its own physical address. By "pretending" to be another host, the aXsGUARD Gatekeeper correctly routes the traffic back to the requesting host. Proxy ARP is defined per RFC 1027. For more information about ARP, see the appropriate online resources.

2.6. **Firewalls and PPTP**

It is highly recommended to configure the aXsGUARD Gatekeeper Firewall so that only required network resources can be accessed by the client. This also improves security in case a client’s computer is hijacked (illustrated below).

The default system-wide Firewall Policies on the aXsGUARD Gatekeeper provide the appropriate security for PPTP VPN access. However, system administrators can and should implement the strictest PPTP Firewall Security at the group or user level, as explained in Section 3.6, “PPTP Firewall Settings”.

Avoid the use of the no-restrictions and int-no-restrictions Firewall Policies at all times, except for testing or troubleshooting purposes in non-live environments (see Section 3.6, “PPTP Firewall Settings”).
Risk as illustrated above

1. A hacker on the Internet scans public IP addresses for open services and vulnerabilities.
2. The hacker hijacks the client which has a public IP address.
3. The hacker can execute any attack posing as the hijacked computer and can access the resources of the corporate LAN through the hijacked computer's PPTP connection.

Recommendations

• Create strict, separate aXsGUARD Gatekeeper Firewall Policies for PPTP VPN access on a user / group basis in agreement with your company policies, as explained above. The aXsGUARD Gatekeeper PPTP Firewall configuration is explained in Section 3.6, “PPTP Firewall Settings”.
• Use a strong hardware or software Firewall on the client side. Ensure that outgoing traffic to TCP port 1723 and the GRE protocol are allowed, otherwise the client will not be able to connect to the PPTP server (see Section 4.2, “Client-Side Firewall”).

Figure 2.7. Consequences of Compromised Client
Chapter 3. PPTP Server Configuration

3.1. Overview

In this section, we explain the required aXsGUARD Gatekeeper PPTP server configuration settings, such as:

- Activating the PPTP Server
- Encryption Settings.
- Accepted IP ranges.
- DNS settings.
- VPN user settings.
- Important PPTP authentication settings, such as DIGIPASS authentication and Directory Services authentication.
- Recommended Firewall Policies.

3.2. Activating the PPTP Server

Before you can access the PPTP configuration settings, you must activate the PPTP feature on the aXsGUARD Gatekeeper.

1. Log on to the aXsGUARD Gatekeeper as explained in the System Administration How To.
2. Navigate to System ⇒ Feature Activation.
3. Expand the VPN & RAS tree.
4. Check the Do you use the aXsGUARD Gatekeeper PPTP Server? option.
5. Click on Update.

Figure 3.1. PPTP Feature Activation
3.3. General Configuration Settings

1. Log on to the aXsGUARD Gatekeeper as explained in the System Administration How To.
2. Navigate to VPN & RAS ⇒ PPTP ⇒ General. A screen as shown below is displayed.
3. Configure the settings as explained in the table below.
4. Click on Update when finished.

![Figure 3.2. PPTP General Configuration Settings](image)

© VASCO Data Security 2011
The aXsGUARD Gatekeeper itself is not a WINS server. The WINS server is usually the primary domain controller in your Windows domain.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept proposed remote client IP</td>
<td>Check to accept the IP address proposed by the remote client. IP address restrictions may apply to certain applications in the corporate network. For these applications to be available, the connecting client needs to be configured to propose the required IP address for the application as opposed to the ones which are made available (Start and End IP addresses explained below). Accepting remote client IP addresses is a useful option which allows PPTP clients to locally print documents via a terminal server (RDP Session). The necessary drivers for printer sharing can be installed on the client, so that the printer can be accessed by the terminal server.</td>
</tr>
<tr>
<td>Accept 40 bit encryption (insecure)</td>
<td>40-bit encryption produces less encryption overhead, but is highly insecure. This setting is not recommended.</td>
</tr>
<tr>
<td>Start IP address</td>
<td>The first IP address of the address pool available for PPTP clients. The client acquires this address via DHCP.</td>
</tr>
<tr>
<td>End IP address</td>
<td>The last IP address of the address pool available for PPTP (DHCP).</td>
</tr>
<tr>
<td>Domain Name Server (DNS)</td>
<td>Specify the DNS server(s) to be used by the remote PPTP client. This is usually the LAN IP address of the aXsGUARD Gatekeeper or the IP address of the primary Domain Controller (Active Directory) in your Windows network.</td>
</tr>
<tr>
<td>Windows Internet Naming Server (WINS)</td>
<td>Specify the WINS server(s) to be used by the remote PPTP client. This is required when using Directory Services password authentication (see note below).</td>
</tr>
</tbody>
</table>
3.4. Authentication Settings

3.4.1. Recommended Method

VASCO highly recommends the use of DIGIPASS authentication for PPTP access. This is the most secure option. You can also combine Local Passwords with DIGIPASS Authentication.

3.4.2. Supported Authentication Methods

The following authentication methods can be enforced for PPTP:

- Static Password
- DIGIPASS
- DIGIPASS or Static Password
- Directory Service Password (Active Directory, see note below)
- DIGIPASS or Directory Service Password
- Static Password and DIGIPASS
- RADIUS Back-end Password
- RADIUS Back-end or Static Password
- DIGIPASS or RADIUS Back-end Password

- AD Authentication needs a WINS server to work, because the aXsGUARD Gatekeeper needs to resolve the domain/workgroup name to the IP address of the AD Server.
- AD Authentication is only possible if the Directory Services module is activated and configured. For more information, consult the aXsGUARD Gatekeeper Directory Services How To, which is available via the Documentation button in the Administrator Tool.

3.4.3. Configuring the Authentication Method

To set or adjust the authentication settings for the PPTP service:

1. Log on to the aXsGUARD Gatekeeper with an administrator account.
2. Navigate to Authentication ⇒ Services.
3. Select the PPTP VPN service.
4. Select the desired Authentication Policy, e.g. DIGIPASS.
5. Update your settings.
Unsupported Authentication Policies generate a validation warning when selected. More information about Authentication Methods, Rules and Policies and how to assign them to aXsGUARD Gatekeeper services, computers, groups and users, is provided in the Authentication How To, which is accessible via the on-screen Documentation button in the Administrator Tool.

The following VPN settings can be edited at the user level:

- Authorization or denial to use the VPN service.
- The password used to authenticate with the VPN server.
- The user’s VPN Firewall settings (explained separately in Section 3.6, “PPTP Firewall Settings”).

To adjust a user’s VPN settings:

1. Navigate to Users & Groups ⇒ Users.
2. Select the appropriate user name.
3. Select the Remote Access tab and adjust the settings as explained in the table below.
### Figure 3.4. User Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Enabled</td>
<td>Check / uncheck to enable / disable the user account.</td>
</tr>
<tr>
<td>Use different password for RAS</td>
<td>Check this option if you want the user to authenticate with a different Local Password than the one specified for aXsGUARD Gatekeeper authentication. You can specify a different Local Password in combination with DIGIPASS Authentication. The user then must enter the specified password, followed by the DIGIPASS OTP. You cannot overrule the Active Directory Password with a Local Password.</td>
</tr>
<tr>
<td>Password</td>
<td>This field only appears when the option above is checked. Enter the VPN password twice for verification.</td>
</tr>
<tr>
<td>PPTP (VPN) RAS</td>
<td>Check to enable PPTP access for the user. Uncheck to disable PPTP access.</td>
</tr>
</tbody>
</table>

### Table 3.2. PPTP User Settings
3.6. PPTP Firewall Settings

3.6.1. Overview

Always use the strictest Firewall settings for PPTP (also see Section 2.6, “Firewalls and PPTP”). Do not use the aXsGUARD Gatekeeper no-restrictions and the int-no-restrictions Firewall Policies as these seriously jeopardize your network security. These policies should be used for testing or troubleshooting only and in a network that is shielded from the Internet.

Firewall Rights determine which services, ports and hosts a user can or cannot access. It is therefore critical to implement the strictest Firewall Policies on the aXsGUARD Gatekeeper, to prevent damage in case the client’s computer is compromised. Network traffic should be restricted to the resources that are needed by the PPTP client, as illustrated below. The Firewall settings for the aXsGUARD Gatekeeper PPTP service are configured in two stages:

- Allow PPTP traffic (and enforce Strong Authentication, e.g. DIGIPASS).
- Implement strict PPTP VPN Firewall Rules and restrict access to the needed resources.

Both stages of the PPTP Firewall configuration are explained in Section 3.6.2, “Allowing PPTP Traffic” and Section 3.6.3, “Firewall Rights”. An example is provided in Section 3.6.4, “Example of Firewall Settings for PPTP”.

3.6.2. Allowing PPTP Traffic

PPTP traffic must be allowed by the aXsGUARD Gatekeeper for clients to successfully connect to the PPTP service. The int-pptp-1 and int-pptp-2 rules are automatically added to the stat-int (system-wide) Firewall Policy when the PPTP service is activated via System ⇒ Feature Activation ⇒ VPN & RAS. A validation message as shown below is displayed. The Firewall rules int-pptp-1 and int-pptp-2 open TCP port 1723 and allow GRE traffic (IP protocol ID 47). Both are required for PPTP access.
System-Wide Firewall Rights: System-Wide Firewall Rights apply to all users in the aXsGUARD Gatekeeper network. Since connected PPTP VPN users are considered a part of the secure network zone, it is of utmost importance to restrict the System-Wide Firewall Rights as much as possible. The default aXsGUARD Gatekeeper System-Wide Firewall Policies (\texttt{stat-sec} and \texttt{stat-z-fix}) provide appropriate security for PPTP VPN access. However, you can overrule these default Policies simply by creating custom Firewall Policies which deny the default traffic. The created Firewall Policies should then be added to the Group’s or User’s VPN & RAS Firewall settings (explained further). This solution allows you to:

- Maintain any changes you have made to System-Wide Firewall Policies.
- To implement even stricter Firewall Policies than the system default policies.

A list of aXsGUARD Gatekeeper Firewall Rules that are active by default is available in the Firewall How To. This document can be accessed via the on-screen Documentation button in the Administrator Tool. You can also click on a Firewall Rule / Policy to view its contents.

User / Group Firewall Rights. As mentioned in Section 2.6, “Firewalls and PPTP”, VASCO highly recommends the use of a strong client-side firewall and the creation of dedicated Firewall Policies for PPTP VPN access on the aXsGUARD Gatekeeper. A predefined Firewall Policy, \texttt{fwd-access-lan}, is available in case administrators choose not to create their own Firewall Policies. This Policy allows all outbound network traffic from the aXsGUARD Gatekeeper’s secure LAN interface. This being said, VASCO strongly recommends to create your own PPTP Firewall Policies.

To adjust a user’s VPN Firewall settings:

1. Navigate to Users & Groups ⇒ Users.
2. Click on the appropriate user name.
3. Select the Firewall tab and adjust the VPN & RAS Policy Mode as explained in the table below.
4. Update your settings.
Example

3.1. Restricting access to two LAN servers

Assume you only wish to grant access to 2 specific servers in the LAN for a PPTP VPN user. Access to any other servers in the LAN is not allowed.

This requires you to create two new through Firewall Rules on the aXsGUARD Gatekeeper, allowing traffic to the specific servers. An additional Firewall Rule dropping all traffic must be created afterwards.

The new Firewall Rules must then be added to a Firewall Policy, which in turn must be assigned to the VPN & RAS Firewall settings of the PPTP user (see Section 3.6.3, “Firewall Rights”).

Create the Firewall Rules for allowed traffic

1. Navigate to Firewall ⇒ Rules ⇒ Through.
2. Search for the fwd-access-lan Rule and click to view its contents.
3. Click on the Edit as New button.
4. Provide a name and description for the new Rule.
5. Check the enabled option.
6. Do not specify a Source IP.
7. Specify the Destination IP of the server which can be accessed, e.g. 10.0.0.1/32.
8. Select Allow as the target.
9. Decide whether you want to log traffic by checking / unchecking the Log this rule target? option.
10. Save the Rule.
11. Repeat the same steps for the second server, e.g. 10.0.0.2/32.

Create the Firewall Rules for traffic that must be dropped

1. Repeat steps 1 to 6 as explained above.
2. Do not specify a Destination IP.
3. Select Drop as the target.
4. Repeat steps 9 and 10 as explained above.

Add the Firewall Rules to a Firewall Policy

1. Navigate to Firewall ⇒ Policies ⇒ Dynamic.
2. Click on the Add New button.
3. Enter a name and a description for the Firewall Policy.
4. Check the enabled option.
5. Add the Firewall Rules created above (Add the "allow" Rules first, followed by the "drop" Rule).
6. Save the Firewall Policy.

Add the Firewall Policy to the VPN & RAS Group Settings of the user

1. Add the new Firewall Policy to the user's VPN Group Policy, add it separately or overrule the user's VPN Firewall policy (see above). Ensure that this Firewall Policy is the only one in the list.
2. Update your settings.

As a result, only network traffic towards the specific servers (e.g. 10.0.0.1 and 10.0.0.2) is allowed, since this Firewall Policy is listed first in the Firewall chain. Any other traffic is dropped.

The options as described in Section 3.6.3, “Firewall Rights” are fully explained in the aXsGUARD Gatekeeper Firewall How To guide, which can be accessed via the Documentation button in the Administrator Tool.

3.7. Logging

To access the PPTP logs

1. Log on to the aXsGUARD Gatekeeper as explained in the System Administration How To.
2. Navigate to VPN & RAS ⇒ Logs ⇒ PPTP.
3. Click on the appropriate log file.
Important information recorded in the logs:

- When a connection was initiated / terminated
- The public IP address of the remote client
- The PPP IP address used by the remote client
- The authentication information
- Information about encryption
- The type of compression
- Useful error messages for troubleshooting
Chapter 4. PPTP Client Configuration

4.1. Overview

In this chapter, we explain how to configure your PPTP client in:

- Windows XP 32-bit
- Windows Vista 32-bit
- Windows 7 32-bit

4.2. Client-Side Firewall

As mentioned in Section 2.6, “Firewalls and PPTP”, VASCO recommends the use of a strong client-side Firewall. Ensure that PPTP VPN pass-through is allowed on the client Firewall, otherwise you will not be able to connect to the aXsGUARD Gatekeeper PPTP server. Refer to your Firewall’s documentation if necessary.

4.3. Windows XP Configuration

1. Click on Start ⇒ Control Panel ⇒ Network and Internet Connections ⇒ Network Connections. A screen as shown below should appear.
2. Click on Create a new connection in the left pane.
3. Select *Connect to the network at my workplace* and click on *Next*.

4. Select *Virtual Private Network Connection* and click on *Next*.
5. Enter a Connection Name and click on Next.

**Figure 4.3. Virtual Private Connection**

**Figure 4.4. Connection Name**
6. Enter the public IP address or the public FQDN of the aXsGUARD Gatekeeper PPTP server and click on Next. Afterwards click on Finish.

![New Connection Wizard with VPN Server Selection](image)

**Figure 4.5. VPN Server Selection**

7. In the connection screen, click on Properties.
8. Select the Security Tab and check the Require data encryption option. Click on OK to continue.
9. Enter the user name and password provided by your system administrator and click on the Connect button. The connection should be up after a few seconds.

You can verify the status of the VPN connection by navigating to the Network Connections screen (see step 1).

4.4. Windows Vista Configuration

1. From the Start button, select Connect To.
2. Select *Set up a connection or network*.
3. Select Connect to a workplace.
4. Click on Next.
5. Select *Use my Internet Connection (VPN)*.

6. In the *Internet Address* field, type the external IP address or the FQDN of the aXsGUARD Gatekeeper PPTP server.

7. In the *Destination Name* field, type a description for your PPTP VPN Connection.

8. Select the *Don’t connect now* option and click on *Next*.

Figure 4.11. Use My Internet Connection

*Note:* If prompted for *Do you want to use a connection that you already have?*, select *No, create a new connection* and click on *Next*.  

© VASCO Data Security 2011
9. Enter the username and password provided by your system administrator.

![Warning: Do not enter a password if you are using DIGIPASS authentication.]

**Figure 4.12. Connection IP and Description**
10. Click on the Create button and then the Close button.

**Figure 4.13. User Name and Password Screen**

**Figure 4.14. Final Configuration Step**
11. To connect to the PPTP VPN server after creating the VPN Connection, click on Start, then on Connect to.
12. Select the VPN connection in the window and click on Connect.

![Connecting to the PPTP Server](image)

Figure 4.15. Connecting to the PPTP Server

13. Enter the user name and password provided by your system administrator and click on the Connect button. The connection should be up after a few seconds.
You can verify the status of the VPN connection by clicking on the Network Icon in the lower right corner of your Windows desktop (see the image below).

Figure 4.16. Connection Successful

You can verify the status of the VPN connection by clicking on the Network Icon in the lower right corner of your Windows desktop (see the image below).

Figure 4.17. PPTP Connection Status

4.5. Windows 7 Configuration

1. Click on the Start button and navigate to the Control Panel.
2. In the Control Panel, select *Network and Internet*. 

![Windows 7 Control Panel](image)

**Figure 4.18. Windows 7 Control Panel**
3. Select **Network and Sharing Center**.

4. Click on **Set up a new connection or network**.
5. Select *Connect to a Workplace* and click on *Next*.

6. Select the first option (*create a new connection*) as shown below and click on *Next*.
7. Click on *Use my Internet connection*.
8. Enter the external IP address or FQDN of the aXsGUARD Gatekeeper PPTP server you are connecting to (e.g. 62.58.227.146 or vpn.mydomain.com) and enter a name for the connection (e.g. office).

9. Leave the other options open and click on Next.

![Figure 4.25. PPTP Connection Settings](image)

10. Enter the user name and password provided by your system administrator to connect to the remote aXsGUARD Gatekeeper PPTP server.

11. Enter the domain you are connecting to (optional).
12. Click on Connect. You should be connected after a few seconds, depending on the speed of your Internet connection.

You can verify the status of the VPN connection by clicking on the Network Icon in the lower right corner of your Windows desktop (see the image below).
Figure 4.27. PPTP Status
Chapter 5. Troubleshooting

5.1. Client-Side Troubleshooting

The client is connected to the PPTP VPN, but cannot access any resources.

1. Check the VPN & RAS Firewall rights of the user and adjust them if necessary (see Section 3.6, “PPTP Firewall Settings”).
2. Check the IP address of the client’s PPP device. If the client’s PPP device’s IP address is within the same range as its Ethernet IP address, the problem is ARP-related (see Section 2.5.3, “Source and Destination address in the Same IP Range”).

Modify the IP address range of the client accordingly. Refer to the documentation of the Operating System if necessary.

PPTP error: "Your credentials have failed remote network authentication".

1. Your username or password may be incorrect. Contact your system administrator.
2. Check if the connecting PC is in a Windows domain. If this is the case, check the properties of your VPN connection and ensure that the Include Windows logon domain option is unchecked (see image below).
PPTP Error 734: The PPP link control protocol was terminated. You probably are using incompatible encryption or authentication settings for PPTP:

1. Create a new VPN connection with standard settings (see Section 4.3, “Windows XP Configuration”).
2. Test the new VPN connection.

PPTP Error 741: The local computer does not support the required data encryption type. See error 734 above.

PPTP Error 769: The specified destination is not reachable. The hostname or IP address of the machine you are connecting to is incorrect. Check your settings and/or contact your system administrator if necessary.

PPTP Error 678: There was no answer. See error 769 above.

PPTP Error 619: the specified port is not connected. If you see the following message:
1. The client sits behind a firewall which is blocking PPTP / GRE traffic. The firewall should be configured to allow this traffic (see Section 2.6, “Firewalls and PPTP” and Section 4.2, “Client-Side Firewall”). Refer to your router / firewall documentation if necessary.

2. Verify the user’s PPTP settings on the aXsGUARD Gatekeeper (see Section 3.5, “User Settings”).

3. Another error occurred while setting up the connection, restart Windows and try again.

4. Your Internet Service provider or in-between networks are blocking GRE packets.

I cannot log on with my Active Directory Password (Directory Services Password).

- On the aXsGUARD Gatekeeper, verify if the correct Authentication Policy has been assigned under Authentication ⇒ Services.
- Verify if the user exists on your Active Directory Server. If the user exists, make sure the AD user account isn’t locked. If the user is not present or locked, authentication fails.
- A WINS server is required. The aXsGUARD Gatekeeper needs to be able to resolve the domain/workgroup to the AD IP (see Section 3.4.2, “Supported Authentication Methods”). The GlobalNames zones (WINS successor) should work as well. WINS is slowly getting phased out by Microsoft being and being replaced by "GlobalNames zones". On MS server 2008, WINS is no longer a role but has become a "feature". The WINS configuration itself is exactly the same as on MS server 2003. For more information about setting up a WINS server, consult your Microsoft documentation. Information can also be found on this MS Technet link: http://technet.microsoft.com/en-us/library/cc787831%28WS.10%29.aspx
- Verify if the DS username with DS tree search permissions has the appropriate privileges on the AD server. See the section "Specifying a Directory Base“ in the aXsGUARD Gatekeeper Directory Services How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool. Only search (read) permissions are required, but you may try to escalate the privileges as a last resort. Consult your Microsoft documentation if necessary.

5.2. Server-Side Troubleshooting

PPTP log Error read(fd=5,buffer=804d580,len=8196) from PTY failed:
status = -1 error = Input/output error. The client is most probably getting PPTP error 619 as mentioned above. GRE packets are being prevented from reaching the aXsGUARD Gatekeeper.
1. Log on to the aXsGUARD Gatekeeper Administrator Tool as explained in the Command Line Interface How To.
2. Use the `tcpdump` command on the Internet device.

**PPTP log Error**

```
GRE: read(fd=7,buffer=8056b60,len=8260) from network
failed: status = -1 error = Protocol not available
```

1. Client firewall: Make sure your client Firewall is not blocking outbound network traffic for port 1723 and IP protocol 47 (see Section 2.6, “Firewalls and PPTP” and Section 4.2, “Client-Side Firewall”). Many consumer grade routers have PPTP pass-through disabled by default. Make sure this option is enabled.

2. Server firewall: Make sure the aXsGUARD Gatekeeper PPTP server can receive a connection on port 1723 and that protocol 47 is being allowed (see Section 2.6, “Firewalls and PPTP” and Section 3.6, “PPTP Firewall Settings”).

Protocol 47 is not the same as port 47. This is a simple but common problem. Do not get port 47 confused with protocol 47. Opening port 47 on your firewall is not the same as allowing protocol 47 or GRE.

**The PPTP service cannot be started.** If `pppd` (the PPTP service) does not have any users configured, it will not start. The result is a session that ends prematurely with an error on the user side which indicates that the server has closed the connection.
Chapter 6. Support

6.1. Overview

In this section we provide instructions on what to do if you have a problem, or experience a hardware failure.

6.2. If you encounter a problem

If you encounter a problem with a VASCO product, follow the steps below:

1. Check whether your problem has already been solved and reported in the Knowledge Base at the following URL: http://www.vasco.com/support
2. If there is no solution in the Knowledge Base, please contact the company which supplied you with the VASCO product.
3. If your supplier is unable to solve your problem, they will automatically contact the appropriate VASCO expert.

For details about support capabilities by user, visit: http://www.vasco.com/support/support_services/types_of_customes.aspx

6.3. Return procedure if you have a hardware failure

If you experience a hardware failure, contact your VASCO supplier.
A

Authentication, Supported Authentication Methods
aXsGUARD Gatekeeper, What is the aXsGUARD Gatekeeper?

C

CHAP, Key Elements of PPTP Security
Control channel, Standard PPTP Deployment

D

Data channel, Standard PPTP Deployment
Documentation, Available Guides

E

Encapsulation, Protocol Description

F

Firewall rights, Firewall Rights

G

GRE, Key Elements of PPTP Security

I

ipconfig, Overview

M

MPPE, Key Elements of PPTP Security

P

PAP, Key Elements of PPTP Security
Point to Point Tunneling Protocol, Protocol Description
Port 1723, Standard PPTP Deployment
PPTP, Protocol Description
Proxy ARP, Source and Destination address in the Same IP Range