aXsGUARD Gatekeeper
Reverse Proxy How To 1.5
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®, and 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 aXsGUARD Gatekeeper environment. We recommend that you contact your NAS/RAS vendor for further information.

Copyright © 2009 VASCO data Security, Inc, VASCO data Security International GmbH All rights reserved.
Table of Contents

1. Introduction .................................................................................................................................................8
   1.1 Audience and Purpose of this Document ...............................................................................................8
   1.1 What is the aXsGUARD Gatekeeper? ........................................................................................................9
   1.2 About VASCO .........................................................................................................................................9

2. Reverse Proxy Concept .................................................................10
   2.1 Overview .............................................................................................................................................10
   2.2 What is the Reverse Proxy? ..................................................................................................................10
   2.3 Reverse Proxy versus Port Forwarding ....................................................................................................11
   2.4 Reverse Proxy versus DMZ ......................................................................................................................11
   2.5 Reverse Proxy: Separate Connections ....................................................................................................12
   2.6 Supported Protocols ...............................................................................................................................13

3. Reverse Proxy HTTP and HTTPS Features ........................................................................14
   3.1 Overview .............................................................................................................................................14
   3.2 RFC Compliance ..................................................................................................................................14
   3.3 URL Sanitizing ......................................................................................................................................14
   3.4 Request Filtering ....................................................................................................................................15
       3.4.1 Deny Requests .................................................................................................................................15
       3.4.2 Allow Requests .................................................................................................................................16
   3.5 Base URL Protection ...............................................................................................................................16
   3.6 Single Point of Access ............................................................................................................................17
       3.6.1 Concept .........................................................................................................................................17
       3.6.2 Examples .......................................................................................................................................18
   3.7 HTTPS Encryption: Self-Signed and Trusted Certificates .................................................................19
       3.7.1 Self Signed Certificates ..................................................................................................................19
       3.7.2 Trusted CA Certificates ..................................................................................................................19
       3.7.3 Domain Name Mismatch ................................................................................................................20
   3.8 HTTPS and SSL Encryption ....................................................................................................................21
       3.8.1 HTTPS Gateway for External Connections ....................................................................................22
       3.8.2 HTTPS for Internal Connections ....................................................................................................22
   3.9 Authentication Methods ...........................................................................................................................23
       3.9.1 aXsGUARD Gatekeeper Authentication ..........................................................................................24
       3.9.2 Single Sign-On (SSO) .......................................................................................................................26
   3.10 Predefined Back-End Servers .............................................................................................................30
   3.11 Advanced Settings .................................................................................................................................32
## Illustration Index

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reverse Proxy Concept</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>DMZ Concept</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Reverse Proxy Security</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>Request Filtering: Deny Requests</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>Base URL Protection</td>
<td>16</td>
</tr>
<tr>
<td>6</td>
<td>Single Point of Access</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>Digital Certificates</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>Self Signed Certificate</td>
<td>20</td>
</tr>
<tr>
<td>9</td>
<td>Untrusted Certificate Warning</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>SSL Connection Setup</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>HTTPS and SSL Encryption</td>
<td>22</td>
</tr>
<tr>
<td>12</td>
<td>Back-End Server Authentication</td>
<td>23</td>
</tr>
<tr>
<td>13</td>
<td>aXsGUARD Gatekeeper Authentication</td>
<td>24</td>
</tr>
<tr>
<td>14</td>
<td>Form Based Authentication</td>
<td>24</td>
</tr>
<tr>
<td>15</td>
<td>Authentication Method Selection</td>
<td>25</td>
</tr>
<tr>
<td>16</td>
<td>OWA Form-Based Authentication</td>
<td>26</td>
</tr>
<tr>
<td>17</td>
<td>Single Sign-On Overview</td>
<td>27</td>
</tr>
<tr>
<td>18</td>
<td>Single Sign-On Authentication Flow</td>
<td>27</td>
</tr>
<tr>
<td>19</td>
<td>Back-end Credentials</td>
<td>28</td>
</tr>
<tr>
<td>20</td>
<td>Password Auto-Learn Feature</td>
<td>29</td>
</tr>
<tr>
<td>21</td>
<td>External Tab</td>
<td>35</td>
</tr>
<tr>
<td>22</td>
<td>Internal Tab</td>
<td>36</td>
</tr>
<tr>
<td>23</td>
<td>Backend Tab</td>
<td>37</td>
</tr>
<tr>
<td>24</td>
<td>Advanced Settings Tab</td>
<td>38</td>
</tr>
<tr>
<td>25</td>
<td>Self-signed Certificate</td>
<td>39</td>
</tr>
<tr>
<td>26</td>
<td>Importing a PKCS12 Certificate</td>
<td>40</td>
</tr>
<tr>
<td>27</td>
<td>Importing a PEM Certificate with Password</td>
<td>41</td>
</tr>
<tr>
<td>28</td>
<td>Importing a PEM Certificate with separate Key</td>
<td>41</td>
</tr>
<tr>
<td>29</td>
<td>External Tab</td>
<td>42</td>
</tr>
<tr>
<td>30</td>
<td>Internal Tab</td>
<td>43</td>
</tr>
<tr>
<td>31</td>
<td>Backend Tab</td>
<td>44</td>
</tr>
<tr>
<td>32</td>
<td>Example of Port Forwarding</td>
<td>45</td>
</tr>
<tr>
<td>33</td>
<td>External Tab</td>
<td>47</td>
</tr>
<tr>
<td>34</td>
<td>Internal Tab</td>
<td>47</td>
</tr>
<tr>
<td>35</td>
<td>Backend Tab</td>
<td>48</td>
</tr>
<tr>
<td>36</td>
<td>External Tab</td>
<td>49</td>
</tr>
<tr>
<td>Image Number</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Image 37</td>
<td>Backend Tab</td>
<td>51</td>
</tr>
<tr>
<td>Image 38</td>
<td>Backend Tab</td>
<td>51</td>
</tr>
<tr>
<td>Image 39</td>
<td>FTP Reverse Proxy</td>
<td>52</td>
</tr>
<tr>
<td>Image 40</td>
<td>Reverse Proxy behind NAT Router</td>
<td>54</td>
</tr>
</tbody>
</table>
Index of Tables

Table 1: Overview of Predefined Back-end Servers..........................................................................................................................31
Table 2: Overview of Advanced Options..................................................................................................................................................32
1. **Introduction**

1.1 **Audience and Purpose of this Document**

This document is intended for technical experts and system administrators. It describes the concept and configuration of the aXsGUARD Gatekeeper Reverse Proxy with HTTP(S) and FTP back-end servers. In this guide, we explain the different security features of the aXsGUARD Gatekeeper Reverse Proxy module and we provide several configuration examples.

In sections 1.1 and 1.2, we introduce the aXsGUARD Gatekeeper and VASCO.

In section 2, we explain the aXsGUARD Gatekeeper Reverse Proxy concept and its advantages.

In section 3, we explain the features of the aXsGUARD Gatekeeper HTTP and HTTPS Reverse Proxy, such as URL sanitizing, SSL encryption and DIGIPASS Authentication.

In section 4 we explain the aXsGUARD Gatekeeper FTP Reverse Proxy features.

In section 5, we provide some practical configuration examples of Reverse Proxy entries.

In section 6, we provide a configuration example of an FTP reverse proxy entry.

In section 7, we provide some solutions to solve difficulties.

In section 8, we explain how to request support, and return hardware for replacement.

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 and / or system administrators.
- 'How to guides', which provide detailed information on configuration of each of the features available as 'add-on' modules (explained in the next section). 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 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 www.vasco.com for further information.

Welcome to aXsGUARD Gatekeeper security.
1.1 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, Web access and VPN management. 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.

1.2 About VASCO

VASCO is a leading supplier of strong authentication and Electronic Signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as a global software company for Internet Security serving customers in more than 100 countries, including many international financial institutions. VASCO’s prime markets are the financial sector, enterprise security, e-commerce and e-government.

Over 50 of VASCO’s client authentication technologies, products and services are based on the VASCO’s one and unique core authentication platform: VACMAN *. VASCO solutions comprise combinations of the VACMAN core authentication platform, IDENTIKEY * authentication server, aXsGUARD authentication appliances, DIGIPASS * client Password and Electronic Signature software and DIGIPASS PLUS authentication services. For further information on these security solutions, please see www.vasco.com.
2. Reverse Proxy Concept

2.1 Overview

In this section, we introduce the aXsGUARD Gatekeeper Reverse Proxy. Topics covered in this section include:

- A definition of Reverse Proxy
- The advantages of using a Reverse Proxy
- Supported protocols

2.2 What is the Reverse Proxy?

The aXsGUARD Gatekeeper Reverse Proxy services Internet client requests by forwarding these requests to the correct server in the LAN, while providing access control, auditing and content monitoring (see the image below).

An Internet client connects to the aXsGUARD Gatekeeper Reverse Proxy Server requesting some service, such as a file or a web page, available on a server in the LAN. If authorized, the resource is provided by the aXsGUARD Gatekeeper Reverse Proxy server, which connects and requests the service on behalf of the Internet client. This means that a direct connection from the Internet to the LAN server is prevented and the server is shielded from possible attacks and exploits.

From now on, we will use the term back-end server when referring to a server in the secure LAN or DMZ.
2.3 Reverse Proxy versus Port Fowarding

With port forwarding, the back-end server is directly accessible from the Internet and vulnerabilities in the back-end server can be more easily exploited.

If a back-end server is compromised, your private data in the secure LAN is fully exposed.

**Caution**

VASCO strongly advises against the use of port forwarding, due to its inherent security risks. More information about port forwarding is available in the aXsGUARD Gatekeeper *Advanced Networking Concepts* guide, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.

2.4 Reverse Proxy versus DMZ

Another method to allow access to a web server is the use of a DMZ (see the example below). The DMZ concept is explained in the aXsGUARD Gatekeeper *Firewall How To*, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool. The DMZ solves the problem of possible access to private data in the secure LAN. However, the DMZ server itself can still be compromised, as it is directly accessible from the Internet. Furthermore, a connection from your DMZ web server to a database server in the secure LAN is impossible due to the aXsGUARD Gatekeeper Firewall concept (see the aXsGUARD Gatekeeper *Firewall How To*).

**Note**

Traffic from the DMZ to the secure LAN can be implemented with advanced Firewall Rules. However, VASCO does not recommend their use. The slightest misconfiguration may have a serious impact on your network security.
2.5 Reverse Proxy: Separate Connections

The aXsGUARD Gatekeeper Reverse Proxy server offers an alternative solution to port forwarding and the DMZ method described in sections 2.3 and 2.4. The aXsGUARD Gatekeeper Reverse Proxy prevents direct access to a server(s) in the secure LAN, hereby protecting it from hacking attempts and OS vulnerability exploits. Instead, the aXsGUARD Gatekeeper Reverse Proxy uses two separate connections; one to accept the request from the Internet client and another one to forward the connection to the server in the secure LAN (from which data is retrieved). Hence, your private data in the secure LAN remains private and is shielded from potential intruders.

The aXsGUARD Gatekeeper Reverse Proxy server also allows you to securely connect a Web server with a database server in the LAN (see below). This is not the case with a DMZ setup (see section 2.4).
2.6 Supported Protocols

The aXsGUARD Gatekeeper Reverse Proxy works at the URL level and inspects HTTP traffic. It also allows to modify contents in a URL (URL Replacement).

It supports the following TCP/IP protocols:

- HTTP
- HTTPS
- FTP

VASCO strongly recommends the use of the aXsGUARD Gatekeeper Reverse Proxy for all back-end servers which are using these protocols.
For back-end servers using other protocols, preference should be given to a DMZ or a VPN solution.

**Note**

RPC is a protocol directly above TCP/IP and is not supported. However, some back-end servers do support RPC over HTTP(S), which is supported if the implementation on the back-end server is RFC compliant.
3. **Reverse Proxy HTTP and HTTPS Features**

3.1 **Overview**

This chapter explains the main concept and features of the aXsGUARD Gatekeeper Reverse Proxy server for HTTP and HTTPS back-end servers: Topics covered in this section include:

- RFC compliance
- URL sanitizing
- HTTP encryption
- User authentication

3.2 **RFC Compliance**

By international agreements, referred to as RFC (Requests For Comments), a URL needs to comply with certain standards. These standards are enforced by default by the aXsGUARD Gatekeeper Reverse Proxy server, providing a secure environment for back-end servers.

Extensive information about URL standards is available in RFC 2396: http://www.ietf.org

---

**Example**

An example of an RFC standard is the length of a URL. Not all web applications can handle extensively long URLs. Such URLs may cause buffer overflows, resulting in unwanted program behavior (hacking attempt) or a crash. The aXsGUARD Gatekeeper Reverse Proxy server automatically rejects requests containing oversized URLs.

---

3.3 **URL Sanitizing**

Per RFC, only certain ASCII characters are allowed in a URL. Characters which deviate from RFC standards are converted. The conversion of URL characters is referred to as escaping (see the example below).

---

**Example**

A space in a URL is converted to `%25`.

---

Since not all back-end servers comply with the international standards (RFCs), they are vulnerable to attacks. To protect these servers, the aXsGUARD Gatekeeper Reverse Proxy is equipped with a URL sanitizer. The URL sanitizer filters out all non RFC compliant URL characters **before a query string**.

---

**Note**

The bold characters in the following URL constitute a query string and are **NOT** escaped by the URL sanitizer: `http://www.imdb.com/find?s=all&q=the+great+escape&x=0&y=0`
3.4 Request Filtering

The aXsGUARD Gatekeeper Reverse Proxy server allows to add URL restrictions on top of the enforced RFC standards. The Reverse Proxy can be configured to reject URLs or parts thereof. The URLs have to be manually entered in the Reverse Proxy configuration screen. Via the Reverse Proxy, administrators can block URLs with specific content and allow exceptions.

The default configuration of the aXsGUARD Gatekeeper Reverse Proxy server is optimised for a Microsoft IIS back-end server.

Filters either:
- Deny requests
- Allow requests (exceptions)

Example
All URLs containing the word scripts, such as http://www.mydomain.com/scripts/adduser.php are blocked, while the URL http://www.mydomain.com/scripts/subscribe-infosession.php is defined as an exception. The aXsGUARD Gatekeeper Reverse Proxy server accepts requests for URL(s) which defined as an exception.

3.4.1 Deny Requests

URLs matching the configured patterns, or parts thereof, are denied. You can use wildcards to define patterns:
- An asterisk or star wildcard has the broadest meaning of all wildcards, as it either represents zero characters, all characters or any string e.g., www.*com matches with http://www.google.com, http://www.microsoft.com, etc., but also http://www.3com.co.uk/.
- A question mark is used to designate any character, e.g. the string www.?unet.com matches with http://www.aunet.com, http://www.bunet.com, http://www.cunet.com, etc.
- A '/' designates the beginning of the server portion in a URL, e.g. slashdot.org matches with http://slashdot.org/, http://slashdot.org/login.pl, but not http://mail.slashdot.org/.
3.4.2 Allow Requests

URL restrictions can be overruled by adding a full URL entry or a part thereof, using the same wildcards as explained in section 3.4.1.

3.5 Base URL Protection

Another method of implementing URL restrictions, is the Base URL Protection. This protection restricts access to the defined URL path(s), e.g. a web server can have several paths www.vasco.com/public, private and support. By adding the word public to the Base URL field, only www.vasco.com/public will be accessible. All other requests, for instance www.vasco.com/private are blocked.

Multiple Base URLs can be added. For instance: with a Microsoft OWA 2003 server, the paths /exchange/, /exchweb/ and /public/ can be used (see below).

Note

Make sure to use a forward slash '/' before and after each entry, for instance /public/.
3.6 Single Point of Access

3.6.1 Concept

The aXsGUARD Gatekeeper Reverse Proxy server is the single point of Internet access towards your back-end server(s) in the Secure LAN. The Reverse Proxy will select one of the configured back-end servers based on the URL which is entered by users on the Internet (see Image 6).

Hence, multiple back-end servers with different hostnames can be made available to Internet users, while only a single public IP address is needed on port 443 or 80. It is advised to use multiple hostnames rather than multiple ports, as ports which deviate from the RFC standards (80 and 443) may not be allowed by some Internet firewall or routers. Hostnames are also more easy to remember than port numbers. The use of non-standard ports requires users to specify a port number after the URL, i.e. http://www.companyname.com:8080.

Each reverse proxy entry should have unique IP address, port and hostname. Multiple hostnames (FQDNs) can be specified for a single back-end. The hostname is not mandatory, but highly recommended, as for each IP address/port combination there can only be one reverse proxy entry without a hostname. The aXsGUARD Gatekeeper Proxy Server automatically reverts to this entry when no matching Reverse Proxy entry is found for a DNS name used for an incoming request. Some examples are provided in section 3.6.2.

Note

Adding a period to the external hostname in the Reverse Proxy entry prevents the aXsGUARD Gatekeeper from automatically adding its system domain to the common name of the certificate.
### 3.6.2 Examples

#### Example1 - One reverse proxy entry using port 443
In this scenario, it is recommended to leave the hostname field empty. This way, all DNS names resolving to the specified IP address will be allowed by the Reverse Proxy. When a hostname is entered, only requests matching the entered FQDN will be allowed by the aXsGUARD Gatekeeper Reverse Proxy Server.

**Tip**
If a hostname is specified, you cannot enter the public IP address in the browser’s URL field. Both the hostname and IP address should be added when needed.

#### Example2 - One public IP address with multiple reverse proxy entries using port 443
The IP address and port number are predefined. This means only the hostname parameter can be used to point to the correct server in the secure LAN. A server with the hostname `intranet.yourdomain.com` and aXsGUARD Gatekeeper authentication can be used to connect to the intranet webserver. Another host, for instance `owa.yourdomain.com`, can be added to connect to your corporate MS Outlook Web Access server.

A third Reverse Proxy entry can be added for your company website. In this case you can choose to add `www.yourdomain.com` as a hostname in the Reverse Proxy entry or you can choose not to specify a hostname at all. In the first case, all non-matching FQDNs resolving to the Reverse Proxy’s IP will be blocked as a security precaution. In the second case, any FQDN which resolves to this IP address will provide a connection to the company website.
3.7 HTTPS Encryption: Self-Signed and Trusted Certificates

A certificate is a computer file containing information which uniquely identifies its owner. The information consists of the owner’s public key, the expiration date of the certificate, the name of the Certificate Authority (CA), a unique name (host name), the signature of the CA (signed with the CA’s private key), and other descriptive data. Certificates are encoded by the CA’s private key and can be verified with the CA’s public key. Any unauthorised changes to the certificate file will generate a warning message.

3.7.1 Self Signed Certificates

A company may choose to create and sign its own certificate. This means the company acts as a CA and signs its own certificate. When you connect to a website with a self-signed certificate, a warning message similar to Image 8 appears.

3.7.2 Trusted CA Certificates

Rather than signing their own certificate, companies may choose to purchase a certificate from a trusted known CA. A trusted CA is an independent network entity, responsible for the issuance and management of digital certificates, e.g. VeriSign and GlobalSign. Websites with a certificate signed by a trusted CA do not generate a warning message (see Image 8).
3.7.3 Domain Name Mismatch

The warning message *Domain Name Mismatch* occurs when the domain name entered in the URL field does not match the host name used in the server’s certificate. This is to inform users that the site may not be the site as originally intended by the user (man-in-the-middle attack).

The same message appears when a site changes its domain name (FQDN) without purchasing a new certificate for the changed domain name or when entering the server’s public IP address (e.g. `https://62.58.227.146`) rather than the domain name (i.e. `https://www.vasco.com`) to contact the server (see Image 9).
3.8 HTTPS and SSL Encryption

An HTTPS connection is a secured HTTP connection. All data in the connection is encrypted using the Secure Sockets Layer (SSL) protocol. (See the image below).

SSL is based on the public/private key (PKI) encryption model. The public key is published by means of a certificate stored on the secure webserver.

Image 10: SSL Connection Setup
3.8.1 HTTPS Gateway for External Connections

Enabling HTTPS for external connections is strongly advised, as all data is sent towards the user(s) on the insecure Internet (see below). The HTTPS protocol can be activated for each reverse proxy entry.

The aXsGUARD Gatekeeper SSL Gateway keeps the maintenance and monitoring of the SSL infrastructure centralized, eliminating the need for SSL maintenance on the back-end server(s).

Besides self-signing, the aXsGUARD Gatekeeper supports the integration of trusted party (CA) SSL certificates. These certificates can be imported via the aXsGUARD Gatekeeper Administrator tool. Currently, PKCS#12 and PEM certificates are supported.

You can either import a single PEM certificate file or a PEM certificate with a separate key file, which in its turn can be encrypted and password protected.

![Image 11: HTTPS and SSL Encryption]

3.8.2 HTTPS for Internal Connections

Using HTTPS for the communication between the aXsGUARD Gatekeeper Reverse Proxy and the back-end server in the secure LAN is not recommended, as this produces encryption overhead.

Some back-end servers only support HTTPS. For these servers it is more convenient to allow HTTPS, rather than modifying the back-end server configuration.

Note

You can only use HTTPS for internal connections if it has been configured for the external connection.
3.9 Authentication Methods

The aXsGUARD Gatekeeper protects your back-end server with authentication. Before access is granted to the back-end server, authentication on the aXsGUARD Gatekeeper needs to be successful.

Three types of authentication are available on the aXsGUARD Gatekeeper Reverse Proxy server:

- **Back-end server authentication:**
  
  The back-end server handles the entire authentication process; the aXsGUARD Gatekeeper only conveys authentication requests and replies between the client and the back-end server.

- **aXsGUARD Gatekeeper authentication:**
  
  The aXsGUARD Gatekeeper requests and verifies the user credentials before contacting the back-end server; the authentication process in handled entirely by the aXsGUARD Gatekeeper. This method allows you to enforce DIGIPASS Autentication. More information about Autentication is available in the aXsGUARD Gatekeeper Authentication How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.

- **Single Sign-On (SSO) authentication:**
  
  SSO requires the back-end server to use form-based authentication; the aXsGUARD Gatekeeper forwards the back-end server’s authentication request, e.g. the Outlook Web Access logon page, to the client on the Internet. The client’s credentials are intercepted and examined by the aXsGUARD Gatekeeper. After successful authentication with the aXsGUARD Gatekeeper, the aXsGUARD Gatekeeper credentials are replaced by the preconfigured back-end credentials to authenticate with the back-end server.

In the following sections, we explain aXsGUARD Gatekeeper authentication and SSO authentication in greater detail.
3.9.1 aXsGUARD Gatekeeper Authentication

The aXsGUARD Gatekeeper prompts for user credentials when a webpage is requested. No requests are forwarded to the back-end server as long as the requesting user is not successfully authenticated with the aXsGUARD Gatekeeper (see the image below).

The aXsGUARD Gatekeeper uses basic authentication. Basic authentication is a method which enables users to provide their credentials through a pop-up window (see below).

**Note**

It is advised to use SSL (HTTPS) with basic authentication, otherwise all password transmissions occur in clear text.
Because of its concept and design, basic authentication cannot be implemented simultaneously on the back-end server and on the aXsGUARD Gatekeeper. For example, if you enable basic authentication on a Microsoft Outlook Web Access 2003 server and the aXsGUARD Gatekeeper is technically impossible.

**Note**

VASCO advises the use of Single Sign-On (SSO) if authentication is required on the aXsGUARD Gatekeeper and the back-end server.

**User credentials**

The aXsGUARD Gatekeeper offers a variety of authentication methods. Once an method has been selected, it applies to all reverse proxy entries. Detailed information about aXsGUARD Gatekeeper authentication methods is available in the aXsGUARD Gatekeeper Authentication How To, which is accessible by clicking on the permanently available Documentation button.

The following authentication methods are available for the aXsGUARD Gatekeeper Reverse Proxy:

- **Deny Always:** e.g. when you are maintaining your back-end server
- **VASCO DIGIPASS**
- **DIGIPASS and Directory Service:** Directory Service password followed by DIGIPASS OTP.
- **DIGIPASS and Static Password:** aXsGUARD Gatekeeper password, followed by VASCO DIGIPASS OTP.
- **DIGIPASS or Directory Service:** Directory Service password or DIGIPASS OTP.
- **DIGIPASS or Static Password:** VASCO DIGIPASS OTP or aXsGUARD Gatekeeper password.
- **Directory Service password,** e.g. your Active Directory password.
- **Static Password:** aXsGUARD Gatekeeper local password.

To select the authentication method for the aXsGUARD Gatekeeper Reverse Proxy:

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which is accessible by clicking on the permanently available Documentation button in the Administrator Tool.

2. Navigate to Authentication > Services.

3. **Select** the desired authentication method (see below).

4. **Click on Update.**

![Image 15: Authentication Method Selection](image-url)
3.9.2 Single Sign-On (SSO)

Requirements

SSO is only possible if the back-end server uses form-based authentication, i.e. the user credentials are entered in a form which is incorporated in the webpage, rather than a separate pop-up window (see section 3.9.1) and the image below.

How does it work?

The user enters his aXsGUARD Gatekeeper credentials which are verified by the Reverse Proxy (see Image 17).

Note

Users only see the back-end authentication form (e.g. the Outlook Web Access authentication screen), never the authentication page of the aXsGUARD Gatekeeper.
If the user successfully authenticates with the aXsGUARD Gatekeeper, a set of predefined user credentials is forwarded to the back-end server; the user is automatically and transparently authenticated with the back-end server. Hence, the name Single Sign-On.

The authentication page of the back-end server is resent to the user if he or she fails to authenticate with the aXsGUARD Gatekeeper (see the image below).
Predefined user credentials

Single Sign-On only works if the back-end credentials for each user are entered on the aXsGUARD Gatekeeper. The credentials need to be entered/updated in the aXsGUARD Gatekeeper Administrator Tool each time they are added/modified on the back-end server.

The back-end server credentials can only be entered / modified by an Administrator. To enter / modify the back-end server credentials:

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which is accessible by clicking on the permanently available Documentation button in the Administrator Tool.

2. Navigate to Users&Groups > Users.

3. Click on the user name of which the back-end server credentials need to be entered / modified.

4. Click on the Reverse Proxy tab.

5. Enter the back-end server credentials.

6. Click on Update.

Note

If no password is entered, the user’s aXsGUARD Gatekeeper password is used to authenticate with the back-end server.
Password Auto-Learning

The aXsGUARD Gatekeeper Reverse Proxy is equipped with a back-end password auto-learning feature, so that users only have to provide the back-end server’s password during the first authentication (until it expires, according to the set password policy on the back-end server). If enabled, the aXsGUARD Gatekeeper safely stores the provided back-end server password for future use (see Image 20), so that users only have to provide one set of credentials and don’t have to remember.

The password auto-learning feature allows you to implement DIGIPASS authentication; the user authenticates with the aXsGUARD Gatekeeper using his / her back-end password in combination with a One-Time Password (DIGIPASS OTP). The back-end password and OTP are entered as a single string. After successful authentication, the DIGIPASS OTP password is truncated; the remaining part of the entered authentication string (the back-end password) is saved by the aXsGUARD Gatekeeper and forwarded to the back end server.

Tips

Although you can also use other aXsGUARD Gatekeeper password types (static password) in combination with the back-end server password, it is strongly advised to use DIGIPASS Authentication, which is the most secure option. Possible authentication scenarios are explained further in this section.

A Reverse Proxy entry has to be created by full administrator. Only advanced administrators can configure the Password Auto-Learn feature and the password separator string.

1. A user on the Internet provides his back-end password and DIGIPASS OTP.
2. The aXsGUARD Gatekeeper verifies the DIGIPASS OTP.
3. If the DIGIPASS OTP is valid, the back-end password is saved by the aXsGUARD Gatekeeper for future use.
4. The saved back-end password is forwarded to the back-end server for authentication.
Possible authentication scenarios:

1. Users authenticate using only their aXsGUARD Gatekeeper password while their back-end server password is stored on the aXsGUARD Gatekeeper (Single Sign-On).

2. Users authenticate using only their aXsGUARD Gatekeeper password while their back-end server password is not stored on the aXsGUARD Gatekeeper. Authentication fails and the back-end server authentication form is presented to the user. As authentication is transparent for the users, the administrator should verify whether the authentication problem is related to the back-end server or the aXsGUARD Gatekeeper.

3. Users authenticate using only their aXsGUARD Gatekeeper password, but the stored back-end server password is invalid (e.g., changed by Active Directory password policy). Authentication fails and the back-end server authentication form is returned to the user. As authentication is transparent for the users, the administrator should verify whether the authentication problem is related to the back-end server or the aXsGUARD Gatekeeper.

4. Users authenticate with the back-end server and the aXsGUARD Gatekeeper password using a password separator string. The back-end password, which precedes the separator string, is stored on the aXsGUARD Gatekeeper for future back-end server authentication (Single Sign-On).

5. Users authenticate with the back-end server and the aXsGUARD Gatekeeper password without a password separator string. This is only possible with a DIGIPASS. The back-end server password, which precedes the DIGIPASS OTP, is stored on the aXsGUARD Gatekeeper for future back-end server authentication.

Tip
The password separator string is specified in the aXsGUARD Gatekeeper Administrator Tool and is only needed when not using DIGIPASS authentication. Only advanced administrators can configure the Password Auto-Learn feature and the password separator string.

3.10 Predefined Back-End Servers

The aXsGUARD Gatekeeper Reverse Proxy server allows you to choose from a list of preconfigured back-end servers (see Table 1). When you choose a preconfigured back-end server, the correct settings are automatically applied, e.g., the base path settings, URL Sanitizing, form-based authentication settings, NTLM settings, etc.

Additionally, some automatic redirects are activated depending on the selected back-end type, e.g., if you select MS OWA 2003, a redirect from https://owa.mydomain.com to https://owa/mydomain.com/exchange is configured automatically.

Caution
Do not use the No specific back-end option for a Microsoft Outlook Web Access (OWA) back-end server. Instead, select one of the predefined back-end servers. Not selecting one of the preconfigured back-end servers may cause back-end authentication (NTLM) failure.
## Table 1: Overview of Predefined Back-end Servers

<table>
<thead>
<tr>
<th>Predefined Back-end</th>
<th>Description</th>
</tr>
</thead>
</table>
| **OWA 2007**        | With Office Outlook Web Access 2007, you can use a Web browser to access your Microsoft Exchange Server mailbox from any computer with an Internet connection. You can use Outlook Web Access with Microsoft Internet Explorer or many other browsers for UNIX, Apple Macintosh, or computers running Microsoft Windows. Outlook Web Access is an effective solution for people who require roaming, remote access, or cross-platform functionality.  
  Two authentication types are available:  
  - Form-based authentication (see section 3.9.2)  
  - Basic authentication (see section 3.9.1) |
| **OWA 2003**        | Same as above, but version 2003.  
  Two authentication types are available:  
  - Form-based authentication (see section 3.9.2)  
  - Basic authentication (see section 3.9.1) |
| **OWA 2000**        | Same as above, but version 2000.  
  - Form-based authentication (see section 3.9.2)  
  - Basic authentication (see section 3.9.1) |
| **Citrix 3**        | Citrix Metaframe 3 allows you to run applications you have at work from anywhere in the world. For detailed information about Citrix products, visit: [www.citrix.com](http://www.citrix.com) |
| **Citrix 4**        | Citrix Metaframe 4 allows you to run applications you have at work from anywhere in the world. For detailed information about Citrix products, visit: [www.citrix.com](http://www.citrix.com) |
  For detailed information about Citrix products, visit: [www.citrix.com](http://www.citrix.com) |
| **XenApp 5**        | Citrix XenApp is a Windows application delivery system that manages applications in a datacenter and delivers them as an on-demand service to users anywhere using any device.  
  For detailed information about Citrix products, visit: [www.citrix.com](http://www.citrix.com) |
| **Citrix ICA Converter** | ICA files which are downloaded from a Citrix Web Interface server, are transformed by the aXsGUARD Gatekeeper, allowing seamless authentication with the Citrix back-end server. |
### 3.11 Advanced Settings

**Note**

These settings can and should be modified by advanced administrators only.

When you are logged on to the aXsGUARD Gatekeeper, a number of advanced configuration options become available for the Reverse Proxy:

Table 2: Overview of Advanced Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Timeout</td>
<td>Specifies the time in seconds during which the TCP connection between the connecting Internet client, the aXsGUARD Gatekeeper Reverse Proxy and the back-end server remains alive (Keep-Alive parameter in HTTP 1.1). 300 seconds is the system default.</td>
</tr>
<tr>
<td>Base URL</td>
<td>Enter the URL(s) which are allowed, e.g. /public/. Enter / to allow all paths on the server. Only the specified URL(s) are allowed.</td>
</tr>
<tr>
<td>Allow tcp optimization to Server</td>
<td>Enables the recycling of the existing TCP connection between the aXsGUARD Gatekeeper Reverse Proxy and the back-end server.</td>
</tr>
<tr>
<td>Allow tcp optimization to Client</td>
<td>Enables the recycling of the existing TCP connection between the Internet client and the aXsGUARD Gatekeeper Reverse Proxy.</td>
</tr>
<tr>
<td>Disable NTLM</td>
<td>Disables NTLM authentication if checked. NTLM authentication is optional for an Outlook Web Access back-end server.</td>
</tr>
<tr>
<td>Public IP outside multilayer NAT</td>
<td>The public IP address (Internet address) of the router connected to the aXsGUARD Gatekeeper Internet interface.</td>
</tr>
<tr>
<td>Public TCP port outside multilayer NAT</td>
<td>The port number of the public IP address (Internet address) of the router connected to the aXsGUARD Gatekeeper Internet interface.</td>
</tr>
<tr>
<td>Activate debug logging</td>
<td>If enabled, extra entries are added to the log files for debugging purposes.</td>
</tr>
</tbody>
</table>

**Caution**

It is highly insecure to enable NTLM authentication while TCP optimization is enabled.
4. Reverse Proxy FTP Features

4.1 Overview

This chapter explains the settings and features of the aXsGUARD Gatekeeper Reverse Proxy server for FTP back-ends. The following topics are covered:
- Authentication
- The Source Host List
- FTP Connection Tracking

4.2 Authentication

Only local aXsGUARD Gatekeeper authentication is available for FTP back-end servers. It is not possible to authenticate with a DIGIPASS or Single Sign-On. The aim is to enable authentication for and protect FTP servers which allow anonymous authentication by default.

4.3 Source Host List

You can limit FTP back-end access to a single or set of source IP addresses, i.e. users on the Internet with static IP addresses. The IP addresses should be entered as comma-separated values without spaces. Entering an asterisk (*) means that requests from all source hosts are accepted.

4.4 FTP and Connection Tracking (SPICT)

SPICT stands for Stateful Packet Inspection with Connection Tracking and refers to the ability to maintain state information about a connection in memory tables, such as source and destination IP address and port number pairs (known as socket pairs), protocol types, connection state and timeouts. Firewalls of this type are known as stateful. Stateful firewalls are inherently more secure than its "stateless" counterpart, simple packet filtering.

FTP uses a control (port 21) and a data connection (port 20). The aXsGUARD Gatekeeper Firewall uses SPICT to allow both connections through the Firewall (see the aXsGUARD Gatekeeper Advanced Firewall Concepts guide, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool).

Note

The aXsGUARD Gatekeeper has to be rebooted when a destination different from TCP port 21 is configured for the FTP back-end server.
5. **HTTP(S) Configuration Examples**

### 5.1 Overview

This section provides some examples of HTTP(s) Reverse Proxy configurations, such as:

- The Microsoft OWA 2003 back-end server with basic authentication.
- The Microsoft OWA 2003 back-end server with basic authentication and SSL certificates.
- The Citrix back-end server with Single Sign-On.
- Setting up a corporate web site.
- Setting up an Intranet web server with aXsGUARD Gatekeeper authentication.

### 5.2 Microsoft OWA 2003 with Basic Authentication

#### 5.2.1 Overview

This example requires that the MS OWA 2003 back-end server is configured for basic authentication or integrated authentication. Integrated authentication is a special form of basic authentication using the same HTTP properties. The simultaneous use of basic authentication on the aXsGUARD Gatekeeper and the back-end server is not possible. Since SSO (see section 3.9.2) is only possible with form-based authentication on the back-end server, aXsGUARD Gatekeeper cannot be implemented.

- HTTP or HTTPS

You can choose between HTTP or HTTPS for the internal and/or external connection. As explained in section 3.8.1, it is highly recommended to use HTTPS for the external connection (as this is the most secure option).

Depending on the configuration settings of the MS OWA 2003 back-end server, HTTP or HTTPS can be selected for the internal connection. In this configuration example, we use HTTP for the internal connection.

#### 5.2.2 Configuration

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.
2. Navigate to Reverse Proxy > HTTP(S).
3. Click on Add New.
4. Follow the configuration steps as explained further (starting on page 35).
5. Click on Save.
Step 1: External Tab

1. Enter a name for the Reverse Proxy entry, e.g. owa2003.
2. Enter a description for the Reverse Proxy entry (optional).
3. Check the Enabled option.
4. Enter the public IP address. This is the Internet IP address of your aXsGUARD Gatekeeper.
5. Enter the port number. 443 is the default port for HTTPS.
6. Enable the Use secure HTTP (HTTPS) option.
7. Enter the Certificate connection name (see note below and in section 3.6.1).
8. Enter the Incoming hostname.

Notes

If you do not put a period behind the Certificate Connection Name, the name is automatically expanded with the system domain name, e.g. owa is extended to owa.mydomain.com.

If you put a period behind the Certificate Connection Name, the name is not expanded with the system domain name.
Step 2: Internal Tab

1. Click on the Internal Tab.
2. Enter the IP address or hostname of the OWA 2003 server.
3. Enter the destination port of the OWA 2003 server.

Notes

Only activate the Use HTTPS to Destination option if the OWA server is listening for HTTPS traffic. The configuration settings should be identical to the settings on the clients in the secure LAN.

If you select Use HTTPS to destination, change the destination port to 443.

Using HTTPS for the communication between the aXsGUARD Gatekeeper Reverse Proxy and the back-end server produces encryption overhead. You should only use HTTPS if it is also used for the external connection.
Step 3: Backend Tab

1. Click on the Backend Tab.
2. Select None as the Authentication type.
3. Select the Outlook Web Access 2003 (basic authentication) option.
4. Click on Save.

Cautions
Selecting the no specific back-end option for an OWA back-end is insecure (see section 3.10).

Advanced Tab: Please refer to section 3.11. The advanced settings can only be modified by advanced administrators. Caution is advised.
Step 4: Advanced Tab

1. Click on the Advanced Tab.

2. Enter the settings as shown below. (Details are available in section 3.11).

3. Click on Save.

Caution
It is highly insecure to enable NTLM authentication while TCP optimization is enabled.

Firewall Rules granting Internet access to the newly configured Reverse Proxy entry are automatically added to the stat-revproxy static Firewall Policy. Please refer to the aXsGUARD Gatekeeper Firewall How To for detailed information about static Firewall Policies.
5.3 Microsoft OWA 2003 with Basic Authentication and SSL Certificate

5.3.1 Overview

You can use a self-signed certificate or an SSL certificate issued by a trusted CA, e.g. GlobalSign or VeriSign on the aXsGUARD Gatekeeper Reverse Proxy. Two types of SSL certificates are currently supported by the aXsGUARD Gatekeeper; PKCS#12 and PEM certificates.

5.3.2 Self-Signed Certificate

To set up a Reverse Proxy entry for the Microsoft OWA 2003 back-end with a self-signed certificate, follow the same procedure as described in section 5.2.

To select / create a self-signed certificate:

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.
2. Navigate to Reverse Proxy > HTTP(S).
3. Click on the name of the Reverse Proxy entry for which you want to create or select a self-signed certificate.
4. Expand the External Certificate menu.
5. Select aXsGUARD Gatekeeper self-signed certificate from the drop-down menu (see below).
6. Click on Update.

Image 25: Self-signed Certificate
5.3.3 Trusted CA Certificates

To set up a Reverse Proxy entry for the Microsoft OWA 2003 back-end with a trusted CA certificate, follow the same procedure as described in section 5.2.

- Importing a PKCS#12 certificate

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.
2. Follow the same steps as explained in section 5.3.2.
3. Select PKCS#12 Certificate from the drop-down menu.
4. Click on the browse button to select the certificate file.
5. Check the Private Key is encrypted option, if the key is encrypted
6. Enter the password to decrypt the provided certificate file (only applies if the certificate file is encrypted).
7. Click on Update.

Image 26: Importing a PKCS12 Certificate
Importing a PEM certificate

Follow the same steps as explained on page 40. You can import a single PEM certificate file or a PEM certificate with a separate key file, which in turn could be encrypted and password protected.

**PEM Certificate:**

1. Select **PEM Certificate File** from the drop-down menu.
2. Click on the **browse** button to select the provided certificate file.
3. Check the **Private Key is Encrypted** box (if applicable).
4. Enter the password to decrypt the certificate file (if applicable).
5. Click on **Update**.

![Image 27: Importing a PEM Certificate with Password](image)

**PEM Certificate with separate Key file:**

1. Select **PEM certificate file and separate key file** from the drop-down menu.
2. Click on the **browse** button to select the provided certificate file.
3. Click on the **browse** button to select the provided private key file.
4. Check the **Private Key is Encrypted** box (if applicable).
5. Enter the password to decrypt the certificate file (if applicable).
6. Click on **Update**.

![Image 28: Importing a PEM Certificate with separate Key](image)
5.4 Microsoft OWA 2003 with Form-Based Authentication and SSO

5.4.1 Overview

This example requires that the MS OWA 2003 back-end server is configured with use form-based authentication. Please refer to the appropriate Microsoft documentation for information about enabling form-based authentication on the OWA 2003 server.

In this example, we will configure the Reverse Proxy entry with Single Sign-On.

- HTTP or HTTPS

You can choose between HTTP or HTTPS for the internal and/or external connection. As explained in section 3.8.1, it is highly recommended to use HTTPS for the external connection (as this is the most secure option).

Depending on the configuration settings of the MS OWA 2003 back-end server, HTTP or HTTPS can be selected for the internal connection. In this configuration example, we use HTTP for the internal connection.

5.4.2 Configuration

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.
2. Navigate to Reverse Proxy > HTTP(S).
3. Click on Add New.
4. Follow the configuration steps as explained further.
5. Click on Save.

- Step 1: External Tab

1. Use the same settings as explained in section 5.2.
2. Check the Use Secure HTTP (HTTPS).

Tip

When selecting Use Secure HTTP (HTTPS), the destination port should be changed to 443.
Step 2: Internal Tab

1. Click on the Internal Tab.

2. Enter the IP address or hostname of the OWA 2003 server.

3. Enter the destination port of the OWA 2003 server.

4. Check the Use HTTPS to Destination option as it is required to use form-based authentication on an OWA 2003 server. The settings should be identical to those for clients in the secure LAN.

Note

You can select the Use HTTPS to Destination option only if it is used for the external connection. When selected, the destination port should be modified to 443.
Step 3: Backend Tab

1. Click on the backend tab.
2. Set the Authentication type to Single Sign-on.
4. Configure the password auto-learn settings, if desired. See section 3.9.2 for more information about password autolearning and using the separator string.
5. Click on Save.

Image 31: Backend Tab

Cautions
Selecting the no specific back-end option for an OWA back-end server is insecure (see section 3.10).

As explained in section 3.9.2, Single Sign-On only functions if the back-end credentials for each user exist on the aXsGUARD Gatekeeper. The predefined credentials used for an OWA 2003 back-end server are labeled: OWA User name and OWA Password.

Step 4: Advanced Tab

Use the same settings as used in section 5.2.

Note

Advanced Tab: Please refer to section 3.11. The settings can only be modified by advanced administrators. Detailed information about the aXsGUARD Gatekeeper administrator levels is available in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool. Caution is advised.

Firewall Rules granting Internet access to the newly configured Reverse Proxy entry are automatically added to the stat-revproxy static Firewall Policy. Please refer to the aXsGUARD Gatekeeper Firewall How To for detailed information about static Firewall Policies.
5.5  Citrix Server with Single Sign-On

5.5.1  Overview

A Citrix setup uses two separate connections. A connection using the HTTP or HTTPS protocol is initiated to contact the Citrix Metaframe server, i.e. a portal requiring authentication. After authentication, a list of available applications is displayed. Selecting an application provides an ICA file containing the description of the connection settings for the selected application.

The ICA file is then used by an ICA client (installed on the client PC) to run the application using a second connection. The client will connect to the Citrix server on TCP port 1494 (ICA protocol).

The second connection cannot be sent through the aXsGUARD Gatekeeper Reverse Proxy, as only the HTTP, HTTPS and FTP protocols are supported. A port forwarding entry is required to allow this connection to work.

Inbound traffic towards the aXsGUARD Gatekeeper’s public IP address on TCP port 1494 has to be forwarded to the internal IP address of the Citrix server using the same TCP port. An example of port forwarding is shown below. Make sure to select the correct Internet device and IP addresses.

Another alternative is to use the Citrix Access Gateway. The gateway creates an ICA connection through an HTTPS connection, eliminating the necessity for port forwarding. As it uses HTTPS, a Reverse Proxy entry towards the Citrix Access Gateway server can easily be created.

The advantage of both setups is that DIGIPASS and Single Sign-On authentication are made possible.

For more information about Citrix and the Citrix Access Gateway, visit: http://www.citrix.com
5.5.2 Configuration

In this example, Single Sign-On authentication is used as the authentication method.

✦ HTTP or HTTPS

You can choose between HTTP or HTTPS for the internal and/or external connection. As explained in section 3.8.1, it is highly recommended to use HTTPS for the external connection (as this is the most secure option).

Depending on the configuration settings of the MS OWA 2003 back-end server, HTTP or HTTPS can be selected for the internal connection. In this configuration example, we use HTTP for the internal connection.

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.

2. Navigate to Reverse Proxy > HTTP(S).

3. Click on Add New.

4. Follow the configuration steps as explained further.

5. Click on Save.

✦ Step 1: External Tab

1. Enter a name for the Reverse Proxy entry, e.g. citrix.

2. Enter a description for the Reverse Proxy entry (optional).

3. Check the Enabled option.

4. Enter the public IP address. This is the Internet IP address of your aXsGUARD Gatekeeper.

5. Enter the port number. 443 is the default port for HTTPS.

6. Enable the Use secure HTTP (HTTPS) option.

7. Enter the Certificate connection name, e.g. citrix (see note below and in section 3.6.1).

8. Enter the incoming hostname, e.g. citrix.mydomain.com.


Note

If you do not put a period behind the Certificate Connection Name, the name is automatically expanded with the system domain name, e.g. owa is extended to owa.mydomain.com, citrix is extended to citrix.mydomain.com.

If you put a period behind the Certificate Connection Name, the name is not expanded with the system domain name.
Step 2: Internal Tab

1. Click on the Internal Tab.
2. Enter the IP address or hostname of the Citrix back-end server.
3. Enter the Destination Port of the Citrix back-end server.
4. Do not check the Use HTTPS to Destination option.

Tip

When selecting Use Secure HTTP (HTTPS), the destination port should be changed to 443.
Note
You can select the Use HTTPS to Destination option only if it is used for the external connection. When selected, the destination port should be modified to 443.

Step 3: backend Tab

1. Click on the backend Tab.
2. Set the Authentication type to Single Sign-On.
3. Set the back-end server to Citrix 4.x.
4. Enable the Allow AutoLearn option (see section 3.9.2).
5. Specify the split symbol for password auto-learning (see section 3.9.2).
6. Click on Save.

![Image 35: Backend Tab]

Note
Advanced Tab: Please refer to section 3.11. The settings can only be modified by advanced administrators. Caution is advised.

Firewall Rules granting Internet access to the newly configured Reverse Proxy entry are automatically added to the stat-revproxy static Firewall Policy. Please refer to the aXsGUARD Gatekeeper Firewall How To for detailed information about static Firewall Policies.
5.6 Running a Company Website

5.6.1 Overview

In this example we do not configure any authentication with the aXsGUARD Gatekeeper, as the company website should be available for anyone connected to the Internet.

- HTTP or HTTPS

You can choose between HTTP or HTTPS for the internal and/or external connection. As explained in section 3.8.1, it is highly recommended to use HTTPS for the external connection (as this is the most secure option).

5.6.2 Configuration

1. Log on to the aXsGUARD Gatekeeper as explained in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.
2. Navigate to Reverse Proxy > HTTP(S).
3. Click on Add New.
4. Follow the configuration steps as explained further.
5. Click on Save.

Step 1: External Tab

1. Enter a name for the Reverse Proxy entry, e.g. webserver.
2. Enter a description for the Reverse Proxy entry (optional).
3. Check the Enabled option.
4. Enter the public IP address. This is the Internet IP address of your aXsGUARD Gatekeeper.
5. Enter the port number. Since this is a web server, we use port 80.
6. Disable the Use secure HTTP (HTTPS) option.
7. Enter the incoming hostname, e.g. www.mydomain.com. (include the last period in the hostname as noted in section 3.6.1).
**Step 2: Internal Tab**

1. Click on the **Internal Tab**.
2. Enter the IP address or hostname of the web server back-end.
3. Enter the **Destination Port** of the back-end server.
4. Do not check the **Use HTTPS to Destination** option.

**Notes**

You can select the Use HTTPS to Destination option only if it is used for the external connection. When selected, the destination port should be modified to 443. Using HTTPS between the aXsGUARD Gatekeeper Reverse Proxy and the back-end server produces encryption overhead. You can only select HTTPS if it is selected for the external connection.

**Step 3: Backend Tab**

1. Click on the **backend Tab**.
2. Set the Authentication type to **None**.
3. Set the back-end server to **No specific back-end**.
4. Click on **Save**
Step 4: Advanced Tab

Note

Advanced Tab: Please refer to section 3.11. The settings can only be modified by advanced administrators. Caution is advised.

Firewall Rules granting Internet access to the newly configured Reverse Proxy entry are automatically added to the \textit{stat-revproxy} static Firewall Policy. Please refer to the aXsGUARD Gatekeeper \textit{Firewall How To} for detailed information about static Firewall Policies.

5.7 Running an Intranet Web Server

This setup is almost identical to the setup of the company website explained in section 5.6. Only the back-end settings are different, since authentication is required before Internet access is allowed to the intranet website.

Backend Tab

1. Click on the backend Tab.
2. Set the Authentication type to aXsGUARD.
3. Set the back-end server to No specific back-end.
4. Click on Save.
6. FTP Reverse Proxy Configuration Example

6.1 Overview

The section explains how to create a new FTP Reverse Proxy entry in the aXsGUARD Gatekeeper Administrator Tool.

6.2 Configuration

Step 1: External Tab

1. Navigate to Reverse Proxy > FTP.
2. Enter a name for the FTP server, e.g. ftp.
3. Check the Enabled option.
4. Enter the aXsGUARD Gatekeeper external IP (Internet address).
5. Enter the port number on which the external IP address is listening (21 is the default for FTP).
6. Enter the IP address or DNS name of the FTP server in your LAN / DMZ.
7. Enter the IP address(es) of the host(s) which are allowed to connect to the FTP server. To allow all hosts, use an asterisk (*).
8. Click on Save to finish.

Firewall Rules granting Internet access to the newly configured Reverse Proxy entry are automatically added to the stat-revproxy static Firewall Policy. Please refer to the aXsGUARD Gatekeeper Firewall How To for detailed information about static Firewall Policies.
7. Troubleshooting

I don't have access to the Reverse Proxy meny in the Administrator Tool

Any newly purchased software needs to be activated (System > Feature Activation > Reverse Proxy)

I cannot authenticate with the Reverse Proxy

Try to authenticate directly with the internal server using the internal IP address and port number to rule out configuration problems on the back-end server.

One user can not authenticate with the Reverse Proxy

- If Single Sign-On authentication is used, verify the user's preconfigured credentials (see section 3.9.2).
- Please try authenticating directly with the internal server using the internal IP address and port number to rule out password problems on the internal server.
- Make sure the user account is not locked on the aXsGUARD Gatekeeper or the back-end server.

Single Sign-On is not working

- Make sure the back-end user credentials exist on the aXsGUARD Gatekeeper. Access the Administrator Tool and navigate to Users & Groups > Users to verify / reset the credentials. Create the credentials if necessary.
- If the user credentials are already present, verify if they are in accordance with the user credentials on the back-end server.

I can't connect to the FTP back-end server on a custom port (not 21)

When using a port different than the standard TCP port 21 for the FTP back-send server, the aXsGUARD Gatekeeper needs to be restarted.

I am getting an error message 'Bad Gateway'

Verify the settings for the internal connection. Make sure port 443 is used when SSL is activated.

I cannot see the Use HTTPS to Destination check box in the internal tab

Make sure the Use secure HTTP (HTTPS) option is checked in the external tab

I am getting an error message 'The page must be viewed over a secure channel'

Verify the settings for the internal connection. Make sure port 443 is used when SSL is activated.

I am getting an error message for a specific page

- Enable Activate debug logging in the Reverse Proxy entry settings. This option is only available for users with Advanced Administration access rights in the aXsGUARD Gatekeeper.
- Retry the page which causes the error and consult the rewrite logfile of the Reverse Proxy entry (Under Reverse Proxy > Logs) in the Administrator tool.

Tip

Enter the name of the specific reverse proxy entry to so that only the relevant log files are displayed.

- Check for log entries mentioning forcing response code 403 as shown in the example below. The reverse proxy blocks requests containing this pattern. Activating the URL Sanitizer may correct the problem.
The aXsGUARD Gatekeeper is sitting behind an ISP or Corporate Router

In some instances, the aXsGUARD Gatekeeper sits behind a corporate or ISP router which is managed externally (see below).

**Issue**

- An HTTP redirect is initiated by the aXsGUARD Gatekeeper Reverse Proxy (e.g., the predefined back-end server is Outlook Web Access).
- The aXsGUARD Gatekeeper sits behind a NAT segment, i.e. 10.0.0.1 while the public IP address of the router is 195.12.7.33 (for example). This address resolves to owa.mycompany.com
- If both conditions are met, then Internet users receive a redirect towards https://10.0.0.1/exchange
- 10.0.0.1 is a private IP address and cannot be resolved on the Internet.

**Solution**

- Make sure to enter the correct parameters in the Reverse Proxy entry, i.e. the public IP address or the FQDN (owa.mycompany.com). See section 3.11.
- It is also possible to modify the port number in the redirect.
I don’t have access to the password auto-learning option.

Only advanced aXsGUARD Gatekeeper administrators may configure this option. Log on to the Administrator Tool with an advanced administrator account.

More information about aXsGUARD Gatekeeper administrator levels is available in the aXsGUARD Gatekeeper System Administration How To, which can be accessed by clicking on the permanently available Documentation button in the Administrator Tool.

“Use secure HTTP (HTTPS)” in the external tab doesn’t work.

If you select the option "Use secure HTTP (HTTPS)" for a Reverse Proxy entry, you need to set the port to 443. When the Secure Extranet web server and Webmail features are activated this is not possible, because these services also use port 443 by default. System administrators are therefore advised to modify the port numbers of these services.

When a Certificate Connection Name is entered, the system domain is automatically appended.

domain.com becomes domain.com.axsguarddomain.com. This can be avoided by adding a period to the certificate connection name (see the notes in sections 3.6.1 and 5.2).
8. Support procedure

8.1 Overview

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

8.2 If you encounter a problem

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

1. Check whether your problem has already been solved and reported in section 7 or 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. If necessary, VASCO experts can access your remotely to solve any problems.

8.3 Return procedure if you have a hardware failure

If you experience a hardware failure, please contact your VASCO supplier.
## Alphabetical Index

<table>
<thead>
<tr>
<th>Accessing Documents</th>
<th>Password auto-learning</th>
<th>8</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>PEM</td>
<td>8, 23</td>
<td></td>
</tr>
<tr>
<td>aXsGUARD Gatekeeper</td>
<td>PKCS#12</td>
<td>22, 39</td>
<td></td>
</tr>
<tr>
<td>Back-end</td>
<td>PKI</td>
<td>8, 10, 12, 14p.</td>
<td></td>
</tr>
<tr>
<td>Basic authentication</td>
<td>Private key</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>Public key</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td>Return Procedure</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Reverse Proxy</td>
<td>8, 10, 12, 14p.</td>
<td></td>
</tr>
<tr>
<td>Citrix</td>
<td>Reverse Proxy versus Port Fowarding</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>DIGIPASS</td>
<td>RFC</td>
<td>14, 17</td>
<td></td>
</tr>
<tr>
<td>Directory Services</td>
<td>Sanitizer</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>DMZ</td>
<td>Self-signed certificate</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td>Single Sign-On</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Domain Name Mismatch</td>
<td>Signature</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>Static password</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>FQDN</td>
<td>Support</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>Training Courses</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>URL</td>
<td>13pp., 20</td>
<td></td>
</tr>
<tr>
<td>ICA client</td>
<td>VPN</td>
<td>8, 13</td>
<td></td>
</tr>
<tr>
<td>NTLM</td>
<td>Wildcards</td>
<td>15p.</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>OTP</td>
<td></td>
<td>29</td>
<td></td>
</tr>
</tbody>
</table>