Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

Copyright

Copyright © 2013 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXsGUARD™, DIGIPASS® and ® 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. 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 in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.
Table of Contents

1 Overview .................................................................................................................. 4

2 Technical Concepts ................................................................................................... 5
   2.1 Microsoft .............................................................................................................. 5
      2.1.1 Windows 2008 Server ................................................................................ 5
   2.2 Juniper ................................................................................................................ 5
      2.2.1 SA2500 ................................................................................................. 5
   2.3 VASCO ................................................................................................................. 5
      2.3.1 IDENTITY Federation Server ...................................................................... 5
      2.3.2 IDENTITY Authentication Server .................................................................. 5

3 Setup – without IDENTITY ...................................................................................... 6
   3.1 Architecture .......................................................................................................... 6
   3.2 Juniper ................................................................................................................ 6
      3.2.1 Authentication Servers ............................................................................... 6
      3.2.2 User Realms ........................................................................................... 7
      3.2.3 User Roles ............................................................................................ 7
      3.2.4 Sign-in............................................................................................... 9
   3.3 Test the Setup ...................................................................................................... 9

4 Solution .................................................................................................................. 11
   4.1 Architecture .......................................................................................................... 11
   4.2 Juniper ................................................................................................................ 11
      4.2.1 System Configuration ................................................................................. 11
      4.2.2 Authentication Servers ................................................................................ 13
      4.2.3 User Realms ................................................................................................. 14
      4.2.4 Sign-in page .............................................................................................. 14
   4.3 IDENTITY Federation Server ............................................................................... 15
      4.3.1 Applications ............................................................................................. 15
4.4 Test the Solution ........................................................................................................ 16
5  FAQ .......................................................................................................................... 17
6  Appendix .................................................................................................................. 17
1 Overview

This document describes how to configure a Juniper SA2500 SSL VPN Appliance in combination with the VASCO IDENTIKEY Federation Server. The combination of those two products makes it possible to set up a secure remote connection between the outside world and the company’s internal network.

This solution makes use of the Security Assertion Markup Language (SAML), an open standard for exchanging authentication and authorization data between parties. SAML is commonly used for web Single Sign On (SSO).

More information about SAML:
2 Technical Concepts

2.1 Microsoft

2.1.1 Windows 2008 Server
Windows 2008 Server is one of the latest server releases of the Microsoft Family. This server can play different roles, like there are:

- Domain Controller
- Web Server
- Mail Server
- ...

To use windows server in order to authenticate users, using Juniper, we need a Domain Controller.

2.2 Juniper

2.2.1 SA2500
Juniper Networks SA2500 SSL VPN Appliance enables small to medium-sized companies to deploy cost-effective, secure remote and extranet VPN access, as well as intranet security.

2.3 VASCO

2.3.1 IDENTIKEY Federation Server
IDENTIKEY Federation Server is a virtual appliance providing you with the most powerful identity & access management platform. It is used to validate user credentials across multiple applications and disparate networks.

The solution validates users and creates an identity ticket enabling web single sign-on for different applications across organizational boundaries. As validated credentials can be reused, once a user's identity is confirmed, access to authorized services and applications is granted. Users can securely switch between the different applications and collaborate with colleagues, business partners, suppliers, customers and partners using one single identity.

IDENTIKEY Federation Server works as an Identity Provider within the local organization, but can also delegate authentication requests (for unknown users) to other Identity Providers. In a Federated Model, IDENTIKEY Federation Server does not only delegate but also receives authentication requests from other Identity Providers, when local users want to access applications from other organizations within the same federated infrastructure.

2.3.2 IDENTIKEY Authentication Server
IDENTIKEY Authentication Server is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

IDENTIKEY Appliance is a standalone authentication appliance that secures remote access to corporate networks and web-based applications.

⚠️ The use and configuration of an IDENTIKEY Authentication Server and an IDENTIKEY Appliance is similar.
3 Setup – without IDENTIKEY

Before adding 2 factor authentication it is important to validate a standard configuration without One Time Password (OTP).

3.1 Architecture

3.2 Juniper
3.2.1 Authentication Servers

In order to authenticate using Active Directory, we need to add an authentication server with the specifications of Active Directory.

- Name: fill in a meaningful name
- Primary Domain Controller: The IP address of the Domain Controller
- Backup Domain Controller: The IP address of the Backup Domain Controller (Optional)
- Domain: The domain to which the Domain Controller belongs.
- **Enable** Allow domain to be specified as part of username
  - Ex: domain\user1
- **Enable** Allow trusted domains
- Admin Username: Enter a username of a user that has admin privileges in Active Directory
- Admin Password: Enter the users password
- **Enable** Kerberos
- **Select** Use LDAP to get Kerberos realm name
3.2.2 User Realms

The User Realm is used to specify which authentication server has to be used in order to authenticate a user.

- Name: fill in a meaningful name
- Description: fill in a meaningful description
- Authentication: Select the Authentication Server that is specified in 3.2.1 Auth. Servers
- Directory/Attribute: Same as above
- Accounting: None
- Save

3.2.3 User Roles

User roles are used for both access rights and user privileges (bookmarks, remote desktop, telnet, ...) 

- Click on the Role Mapping tab
- New Rule

- Select Rule based on Group membership and click Update
- Click on Groups to get the Group selection popup
- Click on Search
- You will see a list of all your Active Directory groups
- Check the box for the groups that you want to use in Juniper SSL VPN and click Add Selected on top.
• Click OK
• In Rule... If users is a member of any of these selected groups >> Select one or more groups and click the “Add” button.
• ... then assign these roles >> select the Juniper role you want to assign to these groups (you will need to create roles before you start!)
• Save Changes

For more information about user roles, consult Juniper documentation
3.2.4 Sign-in

Now we have to select which realm (created in 3.2.2 User Realms) we want to use to Sign in on our VPN website.

- Sign-in URL: */ (this will result in http://10.4.0.168/)
- Select User Picks from a list of authentications realms
- Add Actica Directory Only
- Save

3.3 Test the Setup

Browse to the SSL VPN Web portal, this would be the IP address of the Juniper appliance.
Username: a **user** known in the Active Directory specified in 3.2.1 Authentication Servers

Password: the **password** of the Active Directory user


## 4 Solution

The Juniper supports the Security Assertion Markup Language (SAML) protocol, this is used as an authentication protocol. This protocol, together with the IDENTIKEY Federation Server (IFS), will result in a secure and user-friendly Single Sign On (SSO) Solution.


### 4.1 Architecture

![Architecture Diagram](image)

### 4.2 Juniper

#### 4.2.1 System Configuration

To use SAML, the Juniper needs to be configured

- **Click** Configuration
- **Click** SAML
- **Click** Settings
- Timeout value for metadata fetch request: **300**
- Validity of uploaded/downloaded metadata file: **365**
- Host FQDN for SAML: **juniper.labs.vasco.com**
- **Save Changes**

- **Click** New Metadata Provider

- **Name:** IFS Meta Provider
- **Location:** Remote
- **Download URL:** [https://ifs.labs.vasco.com/ifs/profiles/saml2](https://ifs.labs.vasco.com/ifs/profiles/saml2)

ifs.labs.vasco.com has to be changed with the FQDN of your own IFS

- **Import** Certificate
- **Check** Identity Provider
- **Check** Service Provider
- **Save Changes**

The Entity Ids name is needed in a later stage.
4.2.2 Authentication Servers

In order to authenticate using IDENTIKEY Federation Server we need a new SAML authentication server:

- **Server Name**: fill in a meaningful name
- **SAML Version**: 2.0
- **Configuration Mode**: Metadata
- **Identity Provider Entity Id**: Select the Ids created in System Configuration
- **Allowed Clock Skew (minutes)**: 10
- **Check Support Single Logout**
- **Select Post**
- **Select Certificate**: select a valid certificate
- **Select Device Certificate for Signing**: select a valid certificate
- **Select Device Certificate for Encryption**: select a valid certificate
- **Metadata Validity**: 10
- **Save Changes**

When the authentication server is saved, click the download Metadata. This file is needed in a later stage.
4.2.3 User Realms

Now we have to specify a new user realm where we will link the new Authentication Server.

- Name: fill in a meaningful name
- Description: fill in a meaningful description
- Authentication: Select the Authentication Server that is specified in 4.2.2 Auth. Servers
- Directory/Attribute: None
- Accounting: None
- Save

4.2.4 Sign-in page

Now we have to link our new user realm to the Sign-in page

- Selected realms: Select the realm created in User realms

⚠️ It is possible to select multiple realms. This will give a select list on the Sign-in page with the multiple possibilities.
4.3 IDENTIKEY Federation Server

In order to perform an authentication, the Juniper box needs to be added to the IDENTIKEY Federation Server, as an application.

4.3.1 Applications

- Application type: **Generic SAML v2.0 application**
- Selected profiles: **select an authentication profile**
- Select distribution method: **Upload metadata file**
- Metadata file: **The file downloaded in Authentication Servers**
- **Save**

- Select import method: **Upload certificate file**
- Certificate: **upload a valid certificate**
4.4 Test the Solution

Browse to the SSL VPN Web portal, this would be the IP address of the Juniper appliance.

Username: **User known to the IFS**

Password: **OTP** generated by the Digipass linked to that user.