



DIGIPASS Authentication for Juniper SSL-VPN



DIGIPASS BY VASCO



The world's leading software company specializing in **Internet Security**



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 © 2010 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

Disclaimer	1
Table of Contents	2
Reference guide	4
1 Overview.....	5
2 Technical Concepts	6
2.1 Microsoft	6
2.1.1 Windows 2008 Server.....	6
2.2 Juniper	6
2.2.1 SA2500.....	6
2.3 VASCO.....	6
2.3.1 IDENTIKEY server or aXsGUARD Identifier.....	6
3 Setup – without IDENTIKEY.....	7
3.1 Architecture.....	7
3.2 Juniper	7
3.2.1 Authentication Servers.....	7
3.2.2 User Realms	8
3.2.3 User Roles.....	8
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 Authentication Servers.....	11
4.2.2 User Realms	11
4.2.3 Sign-in page.....	12
4.3 IDENTIKEY Server	12



4.3.1	<i>Policies</i>	13
4.3.2	<i>Client</i>	14
4.3.3	<i>User</i>	15
4.3.4	<i>DIGIPASS</i>	15
4.4	Test the Solution	17
5	Solution - Virtual DIGIPAS	18
5.1	Architecture	18
5.2	Juniper	19
5.2.1	<i>Authentication Servers</i>	19
5.3	VASCO	20
5.3.1	<i>SMS gateway</i>	20
5.3.2	<i>IDENTIKEY Server</i>	21
5.4	Test the Solution	23
6	FAQ	25
7	Appendix	25



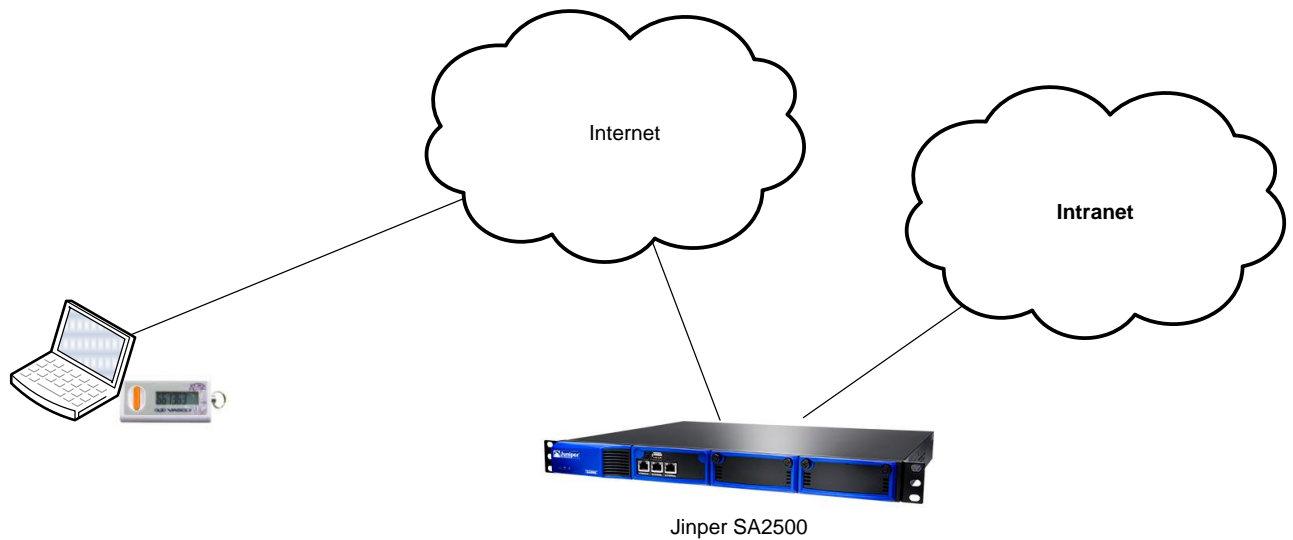
Reference guide

ID	Title	Author	Publisher	Date	ISBN



1 Overview

This whitepaper describes how to configure a Juniper SA2500 SSL VPN Appliance in combination with the VASCO IDENTIKEY 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.





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 server or aXsGUARD Identifier

IDENTIKEY 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 Server is supported on 32bit systems as well as on 64bit systems.

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



The use and configuration of an IDENTIKEY Server and an aXsGUARD Identifier 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.

The screenshot shows the configuration page for an authentication server. The fields are filled with the following values:

- Name: Active Directory
- Primary Domain Controller or Active Directory: 192.168.0.x
- Backup Domain Controller or Active Directory: 192.168.0.x
- Domain: DOMAIN
- Authentication protocol: Kerberos (most secure) is selected.
- Kerberos Realm Name: Use LDAP to get Kerberos realm name is selected.
- Admin Username: administrator
- Admin Password: [Redacted]

- 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
 - http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
- **Select** Use LDAP to get Kerberos realm name
- **Save**

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: Active Directory Only Label to reference this realm

Description: For users that do not have a Digipass. (low)

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Active Directory Specify the server to use for authenticating users.

Directory/Attribute: Same as above Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

Additional authentication server

Dynamic policy evaluation

- Name: fill in a **meaningful name**
- Description: fill in a **meaningful description**
- Authentication: Select the **Authentication Server** that is specified in [3.1.1 Auth. Servers](#)
- Directory/Attribute: **Same as above**
- Accounting: **None**
- **Save**

3.2.3 User Roles

According to specified criteria users can have different roles. For example

- 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



3.2.4 Sign-in

Now we have to select which realm we want to use to Sign in on our VPN website.

The screenshot shows a configuration page for authentication realms. At the top, there are radio buttons for 'Users', 'Administrators', and 'Authorization Only Access'. Below this are fields for 'Sign-in URL' (with a format hint: <host>/<path>/; Use * as wildcard), 'Description', 'Sign-in page' (set to 'Default'), and 'Meeting URL' (set to */meeting/). The main section is titled 'Authentication realm' and contains instructions: 'Specify how to select an authentication realm when signing in.' There are two radio options: 'User types the realm name' and 'User picks from a list of authentication realms'. The second option is selected. Below this, there are two lists: 'Available realms' (empty) and 'Selected realms' (containing 'Active Directory C'). Buttons for 'Add ->', 'Remove', 'Move Up', and 'Move Down' are present.

3.3 Test the Setup

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

The screenshot shows the Juniper - VASCO authentication portal. At the top, there is a browser tab labeled 'Juniper - VASCO'. Below the browser window is the VASCO logo and the text 'THE AUTHENTICATION COMPANY'. The main heading is 'Welcome to the Juniper - VASCO'. Below this, there are two input fields: 'Username' and 'Password'. To the right of the 'Username' field, there is a message: 'Please sign in to begin your secure session.' Below the input fields is a 'Sign In' button.

Username: a **user** known in the Active Directory specified in [3.2.1 Authentication Servers](#)

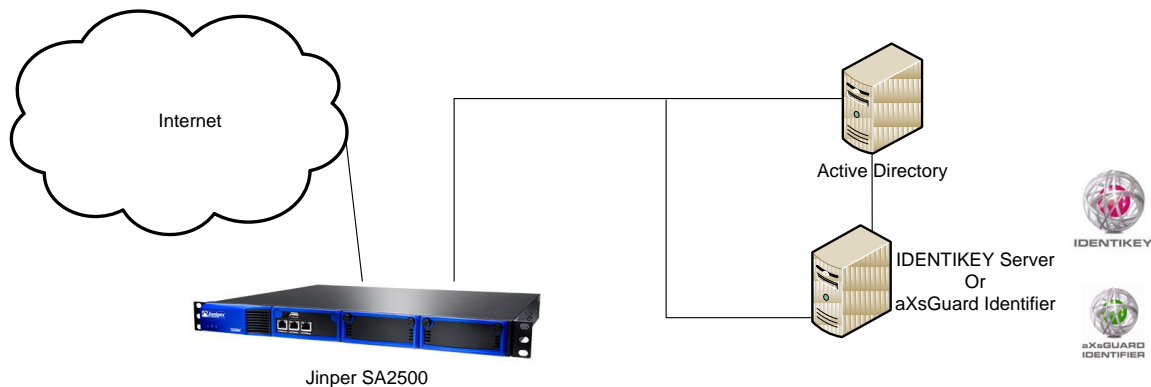
Password: the **password** of the Active Directory user





4 Solution

4.1 Architecture



4.2 Juniper

4.2.1 Authentication Servers

In order to authenticate using IDENTIKEY server we need a new RADIUS authentication server

The screenshot shows the configuration page for a RADIUS authentication server. The 'Settings' tab is selected, and the 'Users' section is visible. The configuration fields are as follows:

Name:	IDENTIKEY	Label to reference this server.
NAS-Identifier:		Name of the device as known to Radius server
Primary Server		
Radius Server:	10.132.224.202	Name or IP address
Authentication Port:	1812	
Shared Secret:	••••••	
Accounting Port:	1813	Port used for Radius accounting, if applicable
NAS-IP-Address:		IP address
Timeout:	30	seconds
Retries:	0	

Users authenticate using tokens or one-time passwords
Note: If you select this, the device will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.

- Name : fill in a **meaningful name**
- NAS-Identifier : The **name** of the **Juniper box known to the network**
- Radius Server : The **IP adres** of the **IDENTIKEY Server**
- Authentication Port : **Standard 1812**
- Shared Secret : Enter a **secret word**
- Accounting Port : **Standard 1813**
- NAS-IP-Address : The **IP adres** of the **Juniper box** (Intern)
- **Enable** Users authenticate using tokens or one-time passwords
- **Save**

4.2.2 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 [4.1.1 Auth. Servers](#)
- Directory/Attribute: **Same as above**
- Accounting: **None**
- **Save**

4.2.3 Sign-in page

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



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 Server

There are lots of possibilities when using IDENTIKEY Server. We can Authenticate with:

- Local users (Defined in IDENITKEY)
- Active Directory (Windows)
- ...

In this whitepaper we will use Local users to authenticate.



4.3.1 Policies

In the Policy the behavior of the authentication is defined. It gives all the answers on: I have got a user and a password, what now?

- **Create** a new Policy



Create new Policy

Create a policy by completing the details below. * indicates mandatory fields.

Policy ID *

Description

Inherits From

- **Policy ID** : Fill in a meaningful name
- **Inherits From**: Base Policy



Inherits means: The new policy will have the same behavior as the policy from which he inherits, except when otherwise specified in the new policy.

Example:

	Base Policy	New Policy	Behaviour
1	a		New policy will do a
2	b		New policy will do b
3	c	f	New policy will do f
4	d		New policy will do d
5	e	g	New policy will do g

The new policy is created now we are going to edit it.

[Click here to manage Juniper Test](#)

- **Click** edit



Edit Policy Settings

Description: Demo Juniper

Local/Back-End Authentication

Local Authentication: Digipass/Password

Back-End Authentication: Default

Back-End Protocol: Default

SAVE CANCEL

- Local Authentication : **Digipass/Password**
- **Save**

4.3.2 Client

In the clients we specify the location from which IDENTIKEY Server will accept requests and which protocol they use.

We are going to add a new RADIUS client.

Create a client by completing the details below. * indicates mandatory fields.

Client Type *: RADIUS Client

Location *: 10.132.224.201

Policy ID *: Juniper Test

Protocol ID: RADIUS

Shared Secret:

Confirm Shared Secret:

CREATE CANCEL

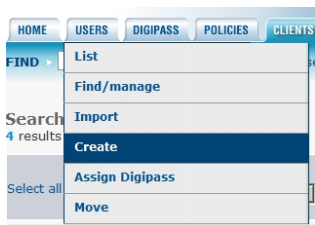
- Client Type : select **Radius Client** from "**select from list**"
- Location : Fill in the IP Address of the Juniper box
- Policy ID : Select the Policy that was created in [4.2.1 Policies](#)
- Protocol ID: **RADIUS**
- Shared Secret: same **word** as entered in [4.1.1 Auth. Servers](#)
- Confirm Shared Secret: reenter the **shared secret**
- **Save**



4.3.3 User

In order to login to the VPN/SSL we need a user.

We are going to create a user.



Create a user by completing the details below. * indicates mandatory fields.

User ID *	<input type="text" value="JuniperUser"/>
Domain *	<input type="text" value="master"/>
Organizational Unit	<input type="text" value="No Organizational unit"/>
Enter static password	<input type="password" value="....."/>
Confirm static password	<input type="password" value="....."/>
Local Authentication	<input type="text" value="Default"/>
Back-End Authentication	<input type="text" value="Default"/>
Disabled	<input type="checkbox"/>
Locked	<input type="checkbox"/>

- User ID: Fill in the **username**
- Enter static password: Fill in a **password**



Password is used when there is no Digipass assigned.

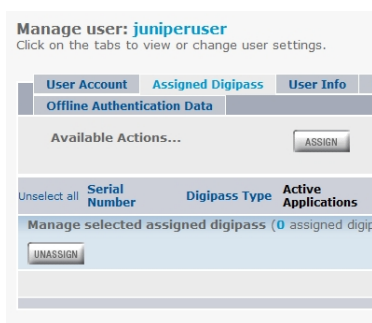
- Confirm static password: **Confirm the password**

4.3.4 DIGIPASS

The purpose of using IDENTIKEY Servers, is to be able to log in using One Time Passwords (OTP). To make it possible to use OTP we need to assign a Digipass to the user. The Digipass is a device that generates the OTP's.

There are several ways to link a Digipass to a User. Here we are assigning a Digipass we start selecting a User. (assuming the Digipasses are already loaded into IDENTIKEY Server)

- Open the user by clicking on its name
- Select **Assigned Digipass**



- Click **ASSIGN**



Application Name: [text field]

Application Type: [Any] [v]

Search upwards in the organizational hierarchy

On clicking NEXT:

Search and auto-select during assignment

Description: [text field]

Results per page (10~100): [10]

[NEXT] [CANCEL]

- Click **Next**

Assign Digipass

Follow the steps below to select users and assign them Digipass.

1. Search Digipass 2. Select Digipass 3. Options 4. Finish

Assign Digipass Summary

No. of Users selected: 1

No. of Digipass found matching the selection criteria: auto-select next available

Assignment Options

Grace period: [0] Days [v]

Verify the selected options and click Assign to proceed assigning the Digipass. Click Cancel to abort the assign Digipass operation.

[ASSIGN] [CANCEL]

- Grace period: **0 Days**



Grace period is the period that a user can log in with his static password. The first time the user uses his DIGIPASS the grace period will expire.

- Click **ASSIGN**



Assign Digipass

Follow the steps below to select users and assign them Digipass.

1. Search Digipass 2. Select Digipass 3. Options 4. Finish

Task completed! You have assigned 1 Digipass, as summarized below.

Select all	Serial Number	Digipass Type	Active Applications	UserID
<input type="checkbox"/>	0091234568	DPG03	APPL1 1	juniperuser

0 digipass selected

MORE actions...
[For these Users...]

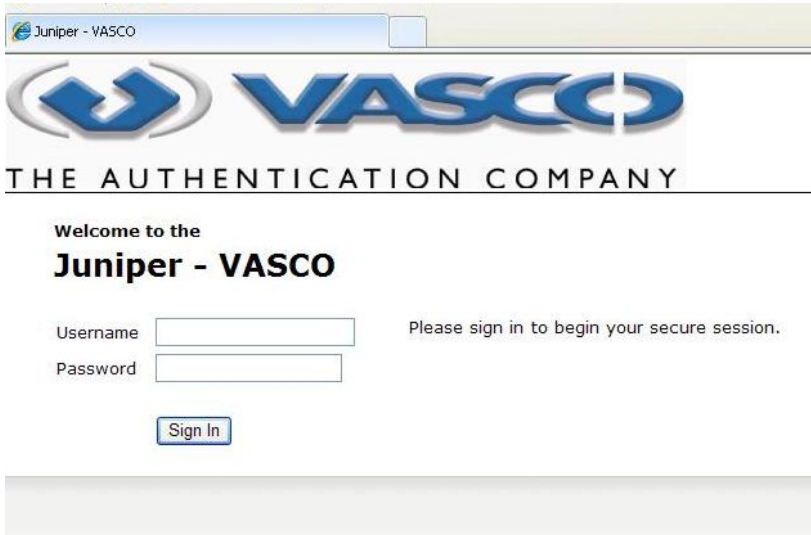
[FINISH]

- Click **Finish**



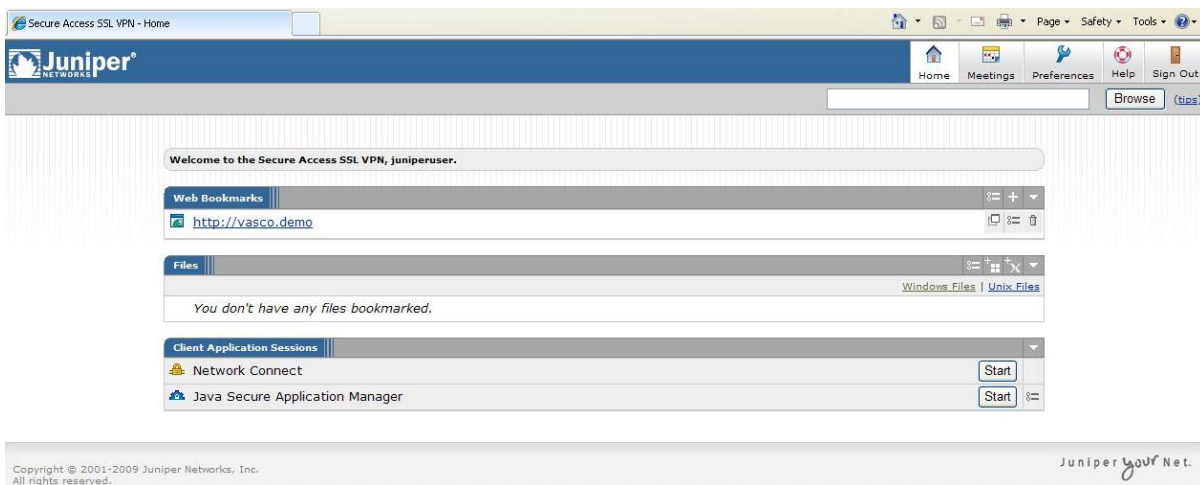
4.4 Test the Solution

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



Username: **JuniperUser** created in [4.2.3 User](#)

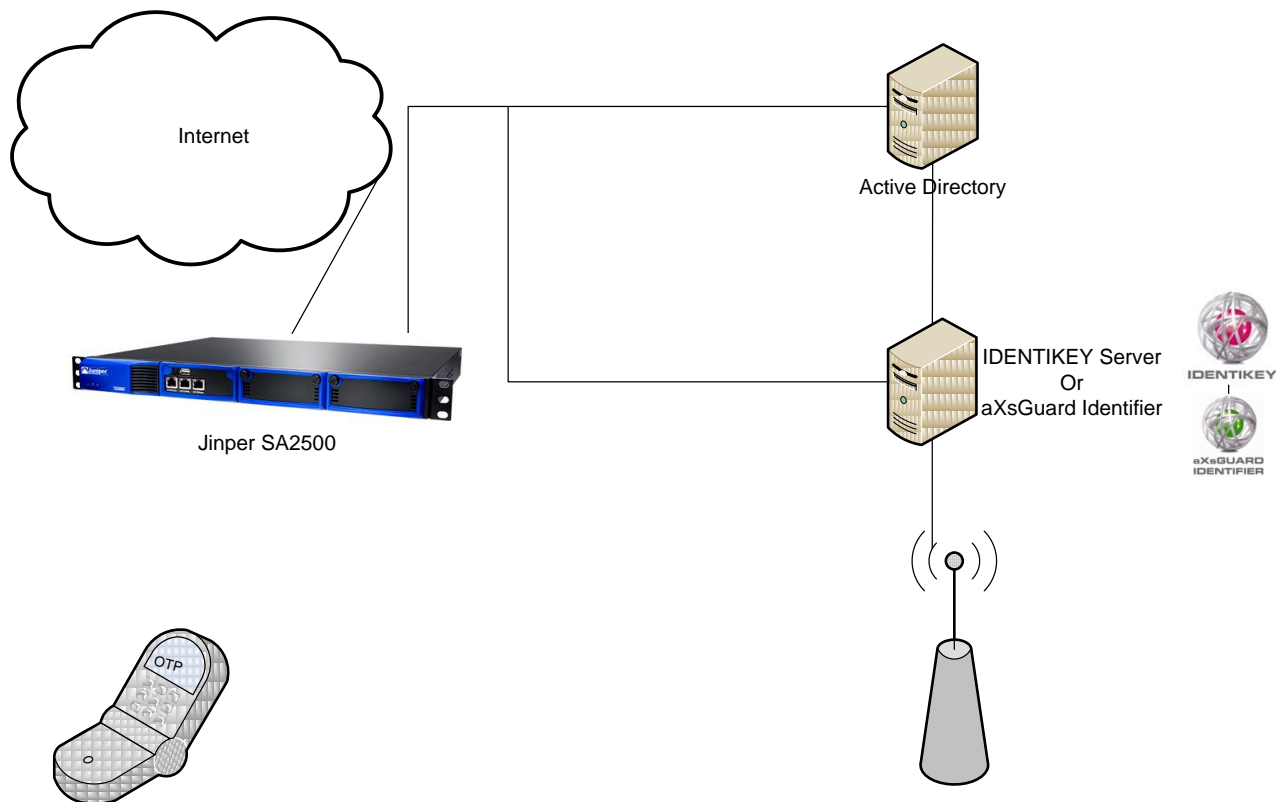
Password: **OTP** generated by the Digipass linked to that user





5 Solution - Virtual DIGIPAS

5.1 Architecture



Juniper can also be configured to use Virtual Digipass. Virtual Digipass is a solution where the OTP is sent via mail or SMS. The user only needs his mobile phone, no other device or installation is needed.

The following prerequisites have to be confirmed on the IDENTIKEY Server:

- Digipasses in IDENTIKEY Server are Virtual Digipasses OR have Virtual Back Up Digipas enabled
- SMS gateway has to be enabled and configured
 - If you want to use SMS as delivery method
- Mail server has to be enabled and configured
 - If you want to use E-mail as delivery method
- The users mobile phone number has to be filled in to IDENTIKEY Server

In this document we will use an **SMS gateway**.



5.2 Juniper

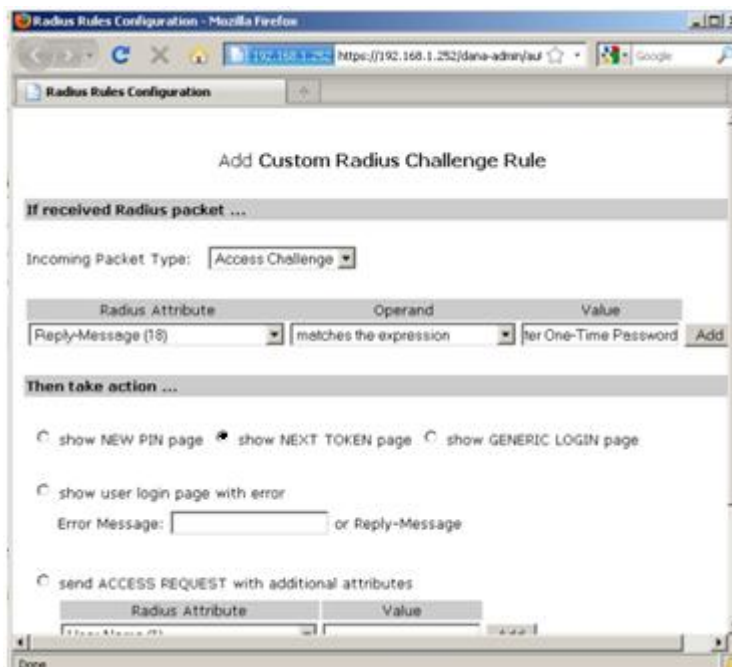
5.2.1 Authentication Servers

In order to authenticate using virtual Digipass we have to modify the settings of the radius authentication sever (IDENTIKEY).

- Open the authentication server called **IDENTIKEY**
- Scroll down to Custom **Radius Authentication Rules**



- Click **New Radius Rule**
- A **Pop-up** will appear



Fill in following settings:

- Incoming Packet Type: **Access Challenge**
- Radius Attribute: **Reply-Message (18)**
- Operand: **matches the expression**
- Value: **enter One-Time Password**
- Then take action ... : **show NEXT TOKEN page**
- Click **Save Changes**
- Also **save changes** for the **authentication server**



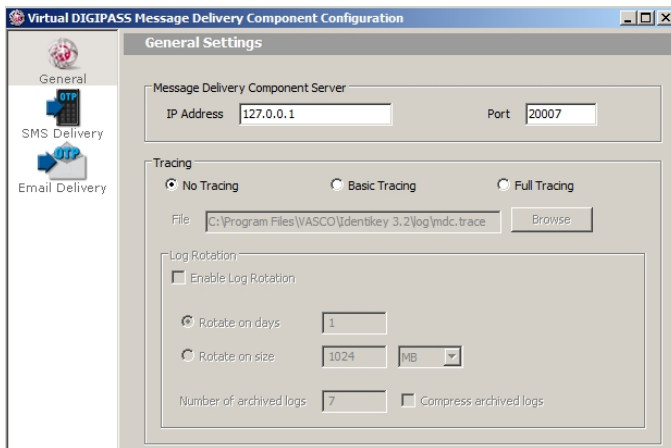
Juniper will show an extra webpage (login-page) when this rule is triggered. The Trigger is a standard radius attribute that is returned by the radius server (IDENTIKEY).



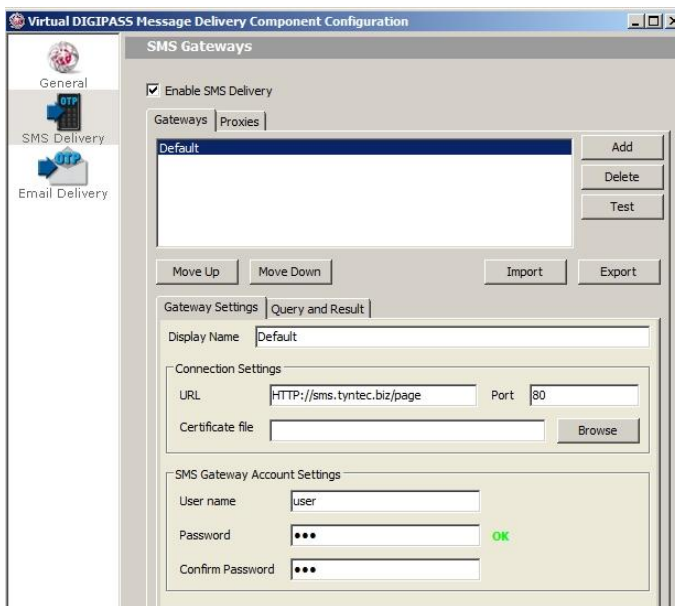
5.3 VASCO

5.3.1 SMS gateway

Start > all programs > VASCO > IDENTIKEY Server > Virtual DIGIPASS MDC Configuration



- **Select SMS Delivery**



- Fill in the **gateway information**



There are several SMS gateway providers. Settings are different depending on the provider.

Providers can be:

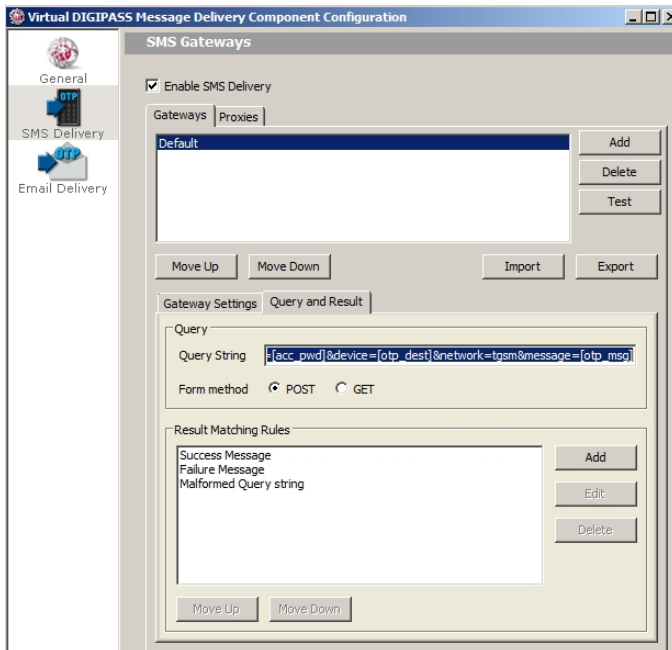
<http://www.clickatell.com>

<http://www.tyntec.com/>

...



- Select **Query and Result**



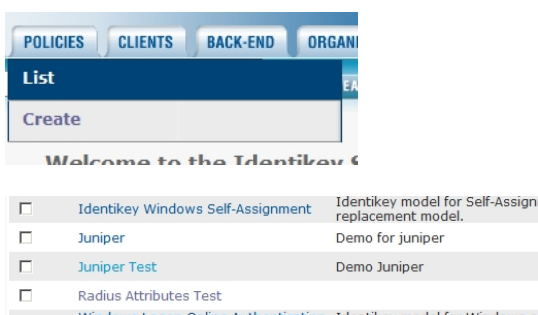
- Fill in the **Query string** (Depends on provider)
- Select **POST** or **GET** (Depends on provider)

5.3.2 IDENTIKEY Server

Now that we have configured the SMS gateway, we have to edit the policy. We have to enable the function Virtual Digipass and define a trigger.

Go to Start > all programs > VASCO > IDENTIKEY Server > IDENTIKEY Web admin

- **Login**
- Select **Policies > List**



- Select the **policy** that is used in combination with Juniper
- Go to **Virtual Digipass**





- Select **Edit**

Policy User Digipass Challenge **Virtual Digipass** DP Contr

Password Randomization DCR RADIUS

Edit Virtual Digipass Settings

Delivery Method

Primary Virtual Digipass

Request Method

Request Keyword

Backup Virtual Digipass

BVPD Mode

Time Limit(days)

Max. Uses/User

Request Method

Request Keyword



There are two kinds of Virtual Digipasses:

1. **Primary Virtual Digipass:** A Primary Virtual Digipass is handled similarly to a standard physical Digipass. It is imported into the IDENTIKEY server, assigned to a User, and treated by the IDENTIKEY server as any other kind of Digipass. Also a Primary Virtual Digipass has its own serial number.
2. **Backup Virtual Digipass:** The Backup Virtual Digipass is meant as a back-up system for a forgotten/stolen/broken standard Digipass. The Backup Virtual Digipass has not its own serial number, but is a feature that can be enabled on a standard Digipass.

- Delivery Method: **Select SMS**
- Primary Virtual Digipass: **Only possible when Virtual Digipass was ordered**
- Request Method: **Password**



This is the trigger: When the user enters his static password in the password field, an SMS will be sent to his mobile phone.

- Backup Virtual Digipass: **Only possible when Backup Virtual Digipass is enabled**
- BVPD Mode: **Yes - Permitted**
- Request Method: **Keyword**
- Request Keyword: **sendotp**

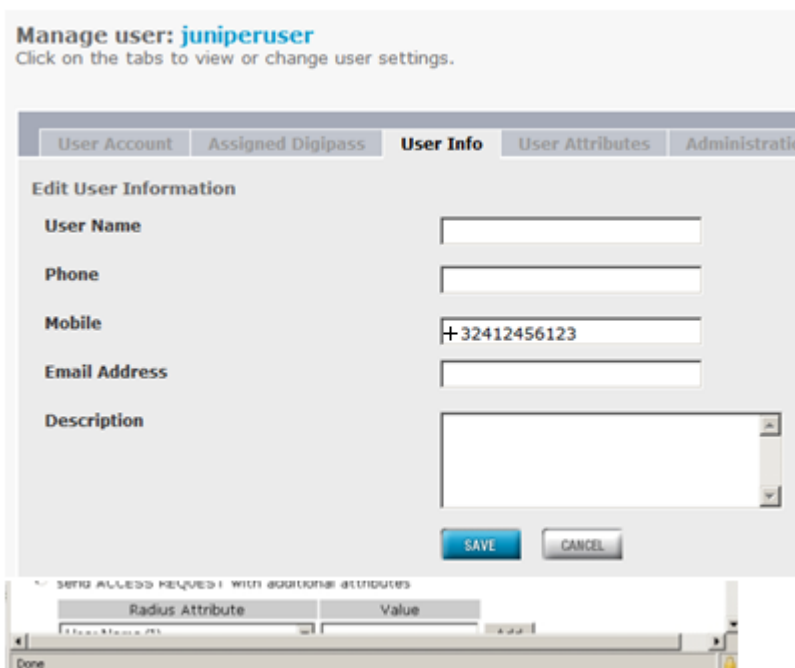
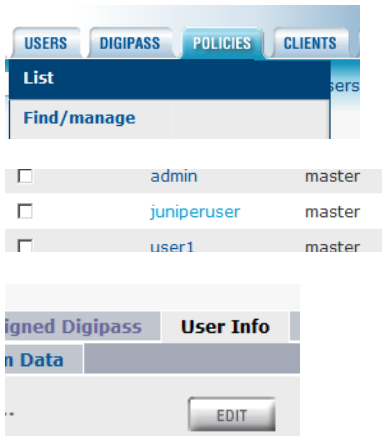


This is the trigger: When the user enters sendotp in the password field, an SMS will be sent to his mobile phone.

- **Save**



In both cases IDENTIKEY server will return a standard RADIUS attribute (Reply-Message (18)) with the value: "**enter One-Time Password**", to the requesting client. The client can trigger special behavior when this attribute is returned (Like we do in [5.2.1 Authentication servers](#)).



- **Mobile:** Fill in the mobile number of the user



Must contain a phone number that consists of only numbers, spaces and brackets () { } []. There may also be a + at the beginning of the number. A maximum of 20 characters can be entered here.

- **Save**

5.4 Test the Solution

Browse to the application, this would be the IP address of the juniper appliance



Juniper - VASCO

VASCO
THE AUTHENTICATION COMPANY

Welcome to the
Juniper - VASCO

Username Please sign in to begin your secure session.
Password

- Username: **JuniperUser** created in [4.2.3 User](#)
- Password: **Static password** (when Virtual Digipass is linked to the user)

Or

- Password: **sendotp** (when Backup Virtual Digipass is enabled)
- An **SMS** will be send to the **mobile phone**, containing an **OTP**
- An new webpage is asking for the **OTP**

Next: Token

PLEASE PROVIDE THE NEW OTP PROVIDED BY THE TOKEN

OTP

- Fill in **OTP**

Secure Access SSL VPN - Home

Juniper NETWORKS

Home Meetings Preferences Help Sign Out

Welcome to the Secure Access SSL VPN, juniperuser.

Web Bookmarks

- http://vasco.demo

Files

You don't have any files bookmarked.

Client Application Sessions

- Network Connect
- Java Secure Application Manager

Copyright © 2001-2009 Juniper Networks, Inc. All rights reserved. Juniper your Net.



6 FAQ

7 Appendix