VASCO THE AUTHENTICATION COMPANY

DIGIPASS Authentication for SonicWALL SSL-VPN

With VACMAN Middleware 3.0

Integration Guideline

Disclaimer

Disclaimer of Warranties and Limitations of Liabilities
This Report is provided on an 'as is' basis, without any other warranties, or conditions.

Trademarks
DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Copyright

Table of Contents

Reference guide

ID	Title	Author	Publisher	Date	ISBN
1	VASCO integration	Olivier Cambier	VASCO Data Security	3 Nov 2006	-
2	SonicWALL integration	Katie De Wilde	SonicWALL, Inc.	3 Nov 2006	-

1 Overview

SonicWALL is a strong leader in secure, easy to configure and affordable SSL-VPN clientless remote access and provides users additional Unified Threat Management security when combined with SonicWALL's firewall/VPN appliances. This addresses all companies going from the SMB (Small & Medium Businesses) to the Enterprise space.

VASCO Data Security has a long history with delivering strong authentication through the DIGIPASS Family that delivers the comfort of using One Time Passwords (OTP's).

VACMAN Middleware combined with SonicWALL SSL-VPN and SonicWALL firewall/VPN appliances is the result of the open market approach delivered through VACMAN Middleware technology.

VACMAN Middleware and SonicWALL gives users the possibility to utilize the strength of the VASCO DIGIPASS Family concept (One Time Password login as Time Based Response Only or Challenge/Response) for easy and secure clientless SSL-VPN remote access (everywhere and every time).

2 Problem Description

Since static passwords are generally known as non-secure and easy to compromise, the challenge was to introduce OTP's (One Time Password) to the remote access market to strongly secure the corporate LAN or central resources. Additionally it would be nice to easily track and manage incoming users via the SonicWALL SSL-VPN and firewall/VPN devices.

Two-factor authentication is an authentication method that requires two independent pieces of information to establish identity and privileges. Two-factor authentication is stronger and more rigorous than traditional password authentication that only requires one factor (the user's password). For this reason SonicWALL Partners with VASCO to provide strong two-factor user authentication.

The following pages present how to solve these issues via a quick and easy configuration on both the SonicWALL SSL-VPN & PRO4060 and the VASCO VACMAN Middleware.

3 Solution & Network Diagram

3.1 Benefits

Two-factor authentication offers the following benefits in combination with SonicWALL SSL-VPN:

- Greatly enhances security by requiring two independent pieces of information for authentication.
- Reduces the risk posed by weak user passwords that are easily cracked.
- Minimizes the time administrators spend training and supporting users by providing a strong authentication process that is simple, intuitive, and automated.

3.2 How does two-factor authentication work?

Two-factor authentication requires the use of a third-party authentication service. The authentication service consists of two components:

- An authentication server on which the administrator configures user names, assigns tokens, and manages authentication-related tasks, like VASCO VACMAN RADIUS Middleware.
- Tokens that the administrator gives to the user which display One Time Passwords (OTP), like VASCO DIGIPASS.

With two-factor authentication, users must enter a valid OTP to gain access. An OTP consists of the following:

- The user's personal identification number (PIN).
- A One Time Password.

Users receive the temporary token codes from their VASCO DIGIPASS. The DIGIPASS displays a new OTP every 32 seconds. (In case of an older DIGIPASS, this time was 36 seconds.) When VACMAN Middleware authenticates the user, it verifies that the OTP timestamp is valid in the current timeframe. If the PIN is correct and the OTP is correct and current, the user is authenticated.

Because user authentication requires these two factors, the VASCO DIGIPASS solution offers much stronger security than traditional passwords (single-factor authentication).

3.3 Supported Platforms

- VACMAN Middleware. This document describes version 3.0.
- SonicWALL SSL-VPN 2000 and 4000 platforms running firmware version 2.0 or higher. This document describes firmware version 2.0.0.0 of SSL-VPN.
- SonicWALL PRO4060 running SonicOS Enhanced 3.x. This document describes SonicOS Enhanced version 3.2.0.3

3.4 Network Diagram

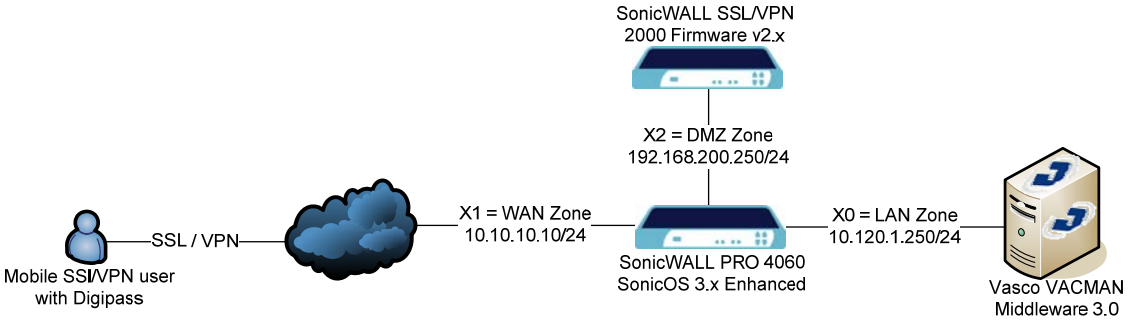

Figure 1: Network Diagram

4 Technical Concept

4.1 General overview

The concept is very easy: the VACMAN Middleware (VM) is installed as a back-end authentication service for the SonicWALL SSL-VPN.

This means that the VM receives all authentication requests from the SonicWALL SSL-VPN. The One Time Password (OTP) within the authentication request will be verified on the VM.

After VM verification, a RADIUS access-accept message is sent to the SonicWALL SSL-VPN for the Authentication part.

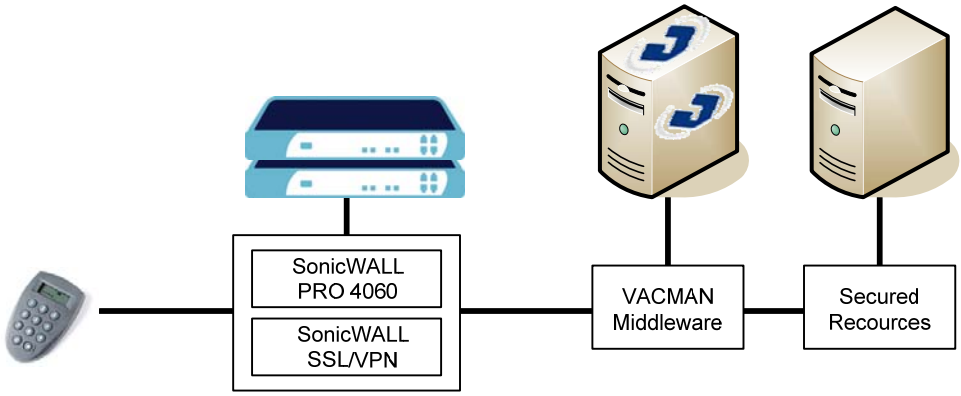

Figure 2: General Overview

4.2 Overview of SonicWALL RADIUS Authentication with VM

The following is a description on the RADIUS authentication sequence WITHOUT DIGIPASS assigned:

- A remote user initiates a connection to the SonicWALL PRO4060.
- The SonicWALL PRO4060 is configured that all https (SSL-VPN) traffic is forwarded to the SonicWALL SSL-VPN.
- The SonicWALL SSL-VPN gathers the remote user's ID and password, and then submits a RADIUS authentication request to the VM.
- VM performs the verification and answers to the SonicWALL SSL-VPN with an access-accept or access-reject message.
- SonicWALL SSL-VPN then provides access to the authenticated user's individual Portal on the SonicWALL SSL-VPN where the protected resources can be accessed via a simple 'bookmark' click or via IPSec-alike NetExtender access.

The following is a description on the RADIUS authentication sequence WITH DIGIPASS Assigned:

- A remote user initiates a connection to the SonicWALL PRO4060.
- The SonicWALL PRO4060 is configured that all https (SSL-VPN) traffic is forwarded to the SonicWALL SSL-VPN.
- The SonicWALL SSL-VPN gathers the remote user's ID and one time password generated by the DIGIPASS, and then submits a RADIUS authentication request to the VM.
- VM performs the OTP verification and answers to the SonicWALL SSL-VPN with an access-accept or access-reject message.
- SonicWALL SSL-VPN then provides access to the authenticated user's individual Portal on the SonicWALL SSL-VPN where the protected resources can be accessed via a simple 'bookmark' click or via IPSec-alike NetExtender access.

4.3 Overview of actions

In the next chapters we will show you how to configure each device and server in the right way to enable the 2-factor authentication with VACMAN Middleware.

• SonicWALL SSL-VPN configuration	SSL-VPN appliance	Chapter 5
• SonicWALL PRO4060 configuration	Firewall appliance	Chapter 6
• VACMAN Middleware configuration	VACMAN Middleware	Chapter 7
• User configuration	Users	Chapter 8
• Sample of a logon	Logon	Chapter 9

5 Configuration of the SonicWALL SSL-VPN

5.1 Login to the SSL-VPN & check version

Browse to the default IP address of the SSL-VPN 2000 or 4000 on its interface labeled 'X0' on https://192.168.200.1 and login with the default values:

User Name: admin Password: password (please change afterwards)

Note: If you enter http://192.168.200.1 it will automatically redirect to https.

Check in the **System > Status** page that the current 'Firmware Version' is minimum version 2.0 :

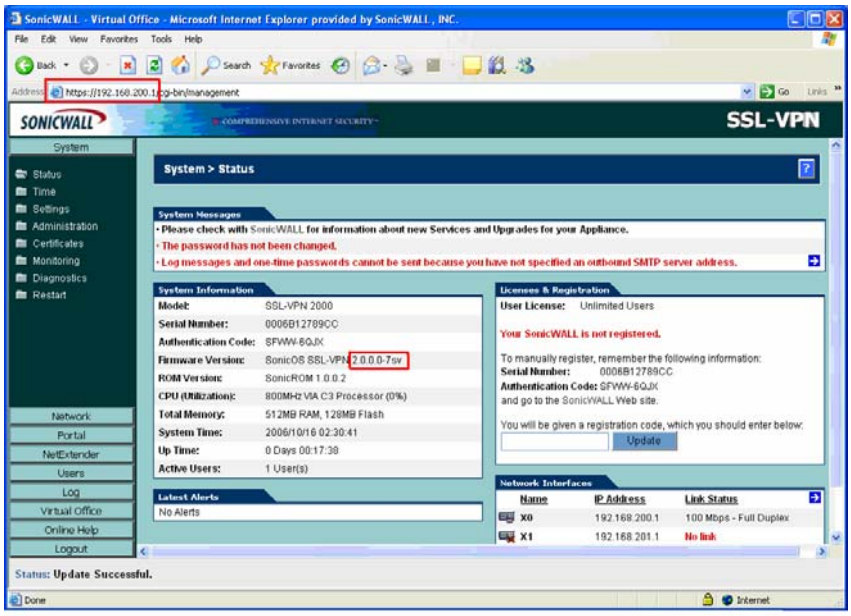

Figure 3: SonicWALL SSL/VPN configuration (1)

If it is not minimum version 2.0, it is advised that you register the SonicWALL SSL-VPN appliance on https://www.mysonicwall.com where you can download the latest firmware version with a valid SonicWALL support entitlement.

Note: Firmware version 2.0 is needed to support two-factor authentication on the SSL-VPN appliance.

Check the **Network > Interfaces** page for the correct IP address of the SSL-VPN's X0 interface. According to the **Network Diagram** in Figure 1 this can be left to the default IP address 192.168.200.1:

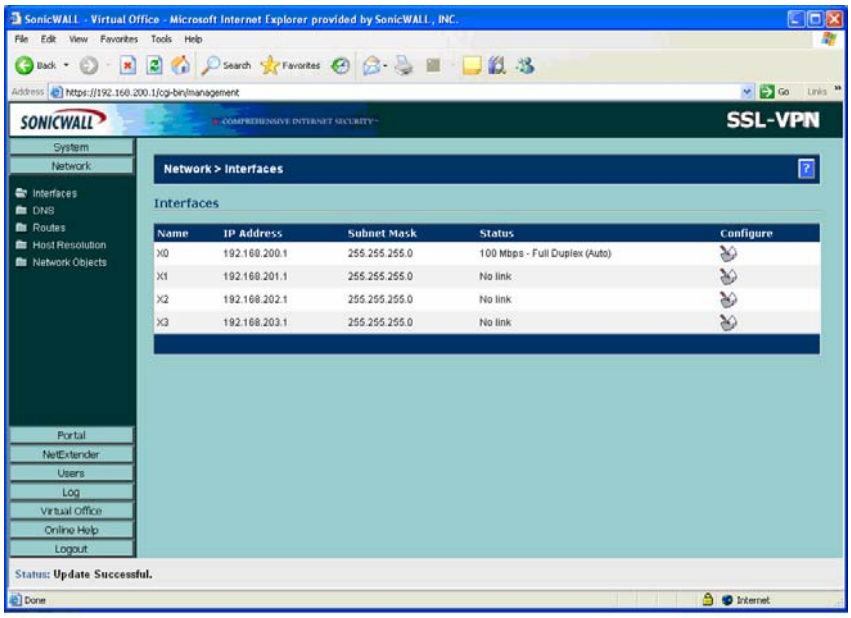

Figure 4: SonicWALL SSL/VPN configuration (2)

5.2 Time setting on the SSL-VPN

Because two-factor authentication depends on time synchronization, it is important that the internal clocks for the SSL-VPN appliance and the VACMAN Middleware are set correctly. On the SSL-VPN appliance, set the time on the **System > Time** page, either via an NTP server or manually, and select the correct Time Zone:

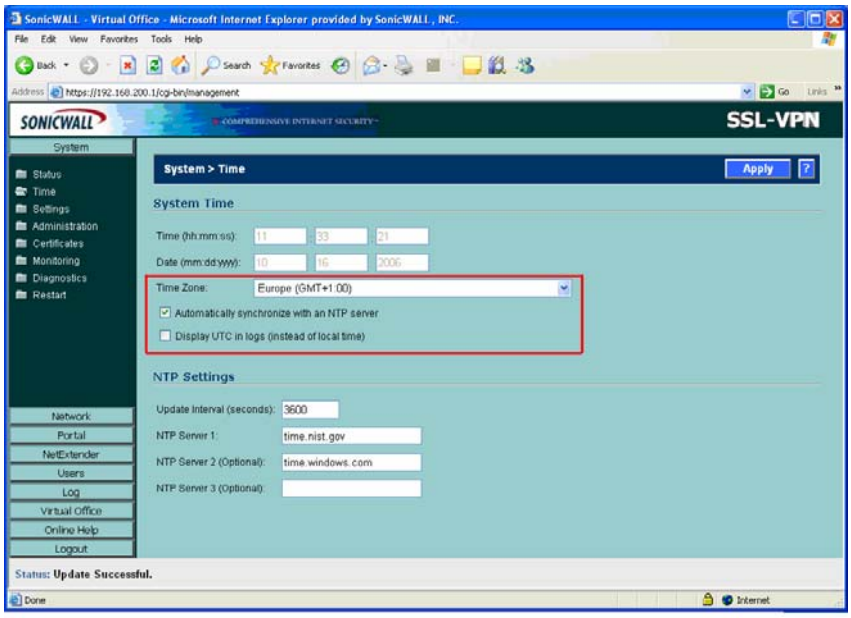

Figure 5: SonicWALL SSL/VPN configuration (3)

5.3 DNS Settings

On the **Network > DNS** page, set the correct DNS Settings and optionally the WINS Settings:

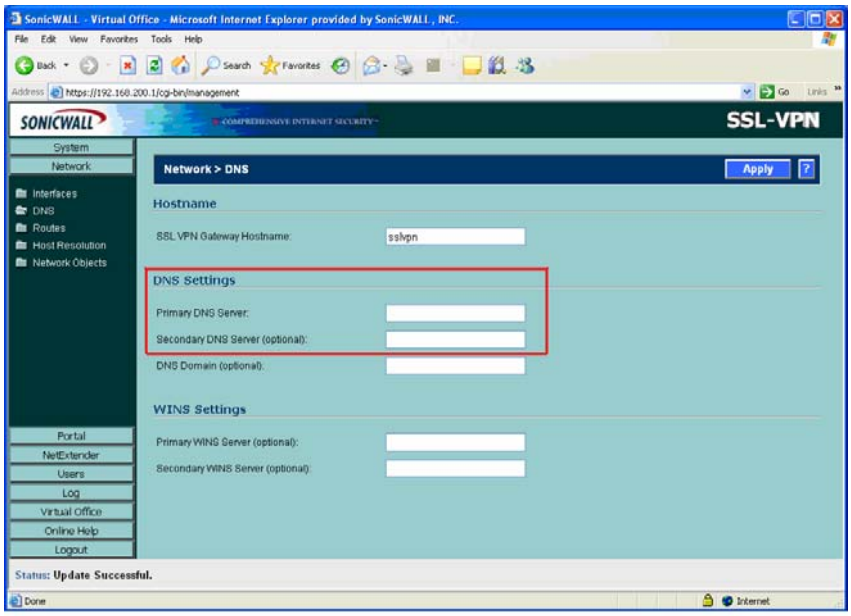

Figure 6: SonicWALL SSL/VPN configuration (4)

5.4 Configure a default route for the SSL-VPN

According to the Network Diagram in **Figure 1**, the default route for the SSL-VPN is the PRO4060's X2 interface that corresponds with the DMZ Zone. This IP address is set to 192.168.200.250 and needs to be configured as the Default Route for the SSL-VPN. Navigate to the **Network > Routes** page and set the correct Default Route on the SSL-VPN X0 interface:

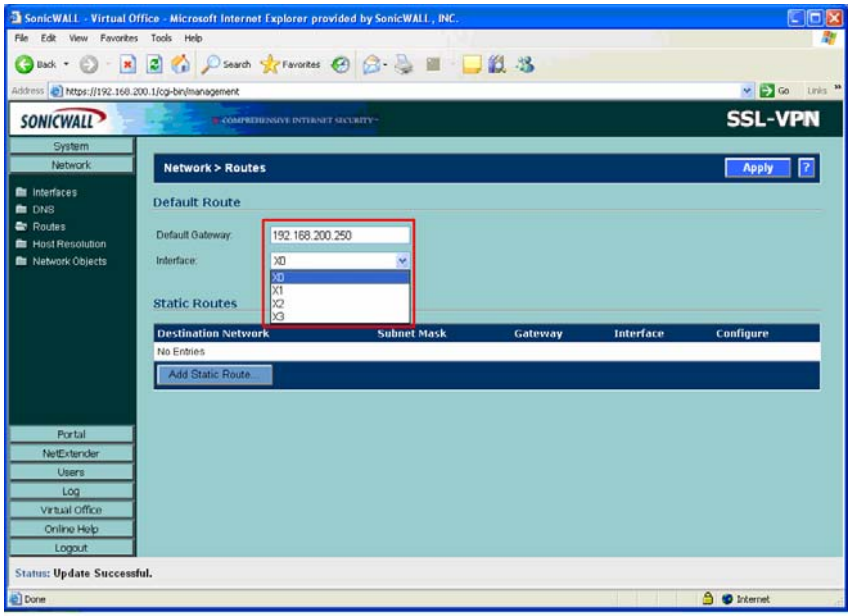

Figure 7: SonicWALL SSL/VPN configuration (5)

5.5 NetExtender Client Address Range

If NetExtender Clients (= IPSec like SSL-VPN tunnels) are used, set the **NetExtender Client Address Range** in the **NetExtender > Client Addresses** page:

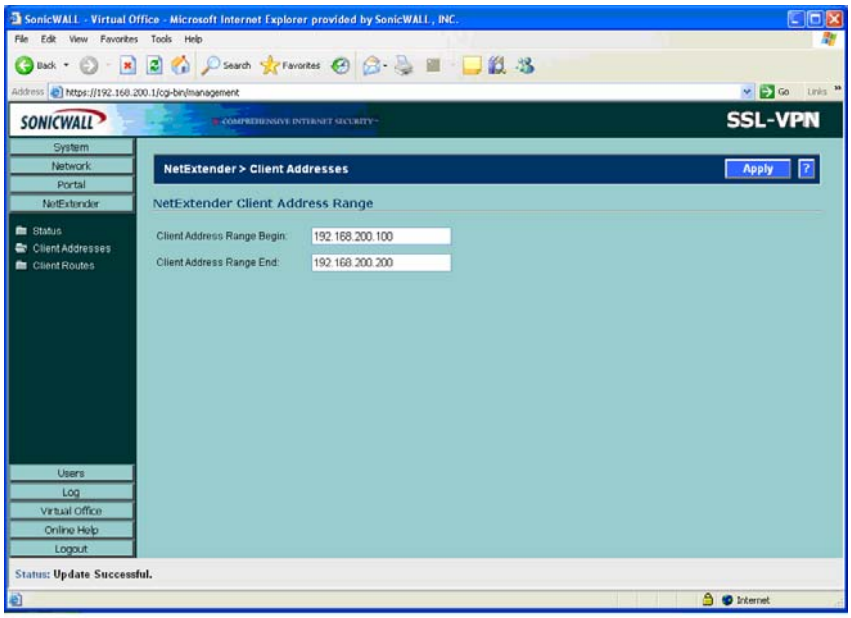

Figure 8: SonicWALL SSL/VPN configuration (6)

In this example, the Client Address Range Begin and End can be left default as Client Addresses will be assigned in the same subnet 192.168.200.0/24 of the SSL-VPN X0 interface.

Note: Make sure you exclude from this range the SonicWALL SSL-VPN X0 interface and the SonicWALL PRO4060's X2 interface IP address, according to the Network Diagram in **Figure 1: Network Diagram**.

5.6 Add NetExtender Client Routes

In the **NetExtender > Client Routes** page, **Add** the correct **Client Routes** for the authenticated remote users accessing the private networks via the SSL-VPN connection:

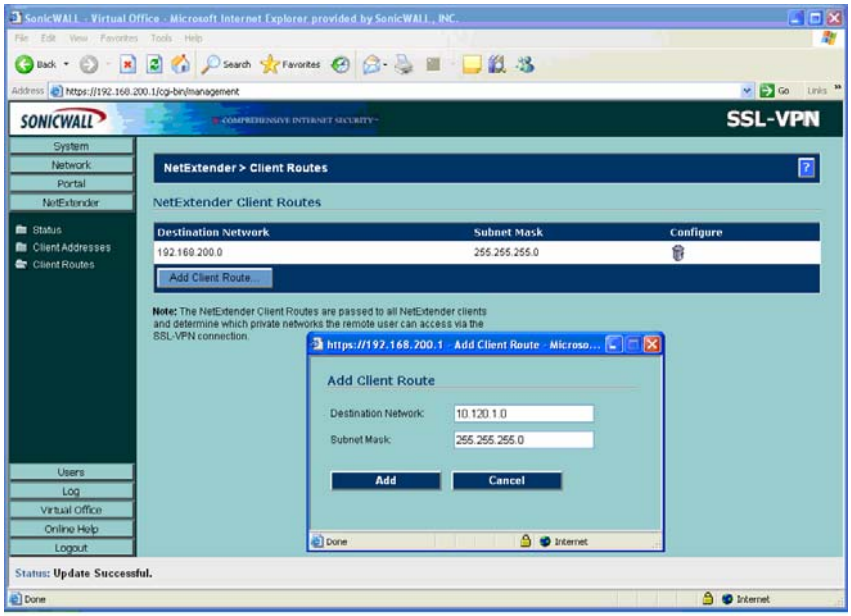

Figure 9: SonicWALL SSL/VPN configuration (7)

According to the Network Diagram in **Figure 1: Network Diagram**, this corresponds with the subnet connected to the X0 (LAN) interface of the SonicWALL PRO4060.

5.7 Create a Portal Domain

'Add Domain' via the **Portal > Domains** page and select 'RADIUS' as the Authentication Type from the Drop-down menu:

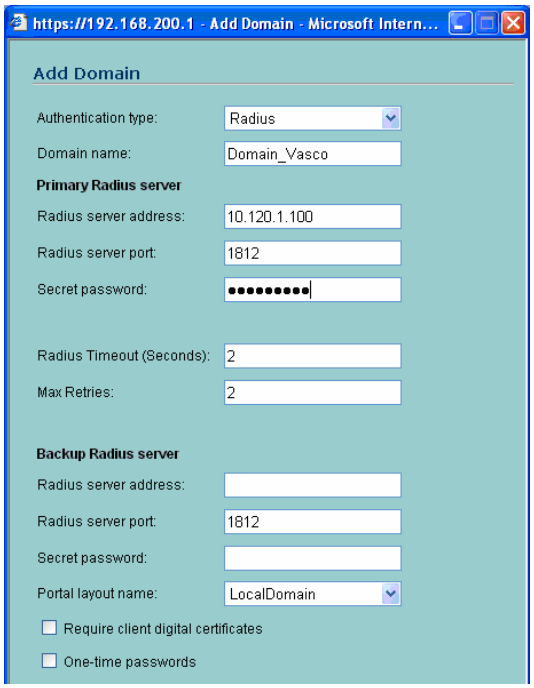

Figure 10: SonicWALL SSL/VPN configuration (8)

Enter a descriptive name for the 'Domain Name'. This is the Domain Name users will select in order to log into the SonicWALL SSL-VPN appliance portal.

The 'RADIUS server address' is the IP address of VACMAN Middleware.

The 'RADIUS server port' needs to match the RADIUS port of VACMAN Middleware, as well as the 'Secret password' that is used for RADIUS authentication between these two elements.

Note: VACMAN Middleware prior to version 3.0 uses a different default port number than 1812 (that is the default value for SonicWALL SSL-VPN). The RADIUS port 1812/1813 is now the default value (that matches the default SSL-VPN values).

In this example only a 'Primary RADIUS server' is used.

5.8 Add a 'local user' for the Domain

Via the **Users > Local Users** page, 'Add a User' to the 'Domain_VASCO' just created.

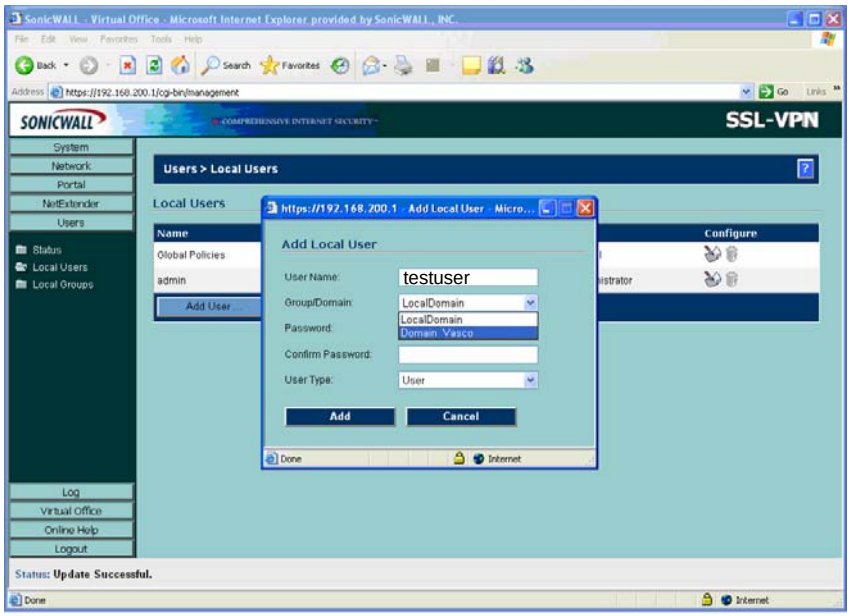

Figure 11: SonicWALL SSL/VPN configuration (9)

Assign this user to the RADIUS Domain, it won't ask for a password (see below), it will just ask for the username. Passwords will be generated through the RADIUS Server. Make sure you duplicate the usernames as on the RADIUS Server (**testuser** in this example).

Figure 12: SonicWALL SSL/VPN configuration (10)

Figure 13: SonicWALL SSL/VPN configuration (11)

5.9 Edit the policy for the user

You can edit the policy for the user by going to the Users > Local Users page and selecting the 'Configure' button:

The default 'Policy' is Allow All Traffic. You can be more restrictive or create optional 'Bookmarks' for the User.

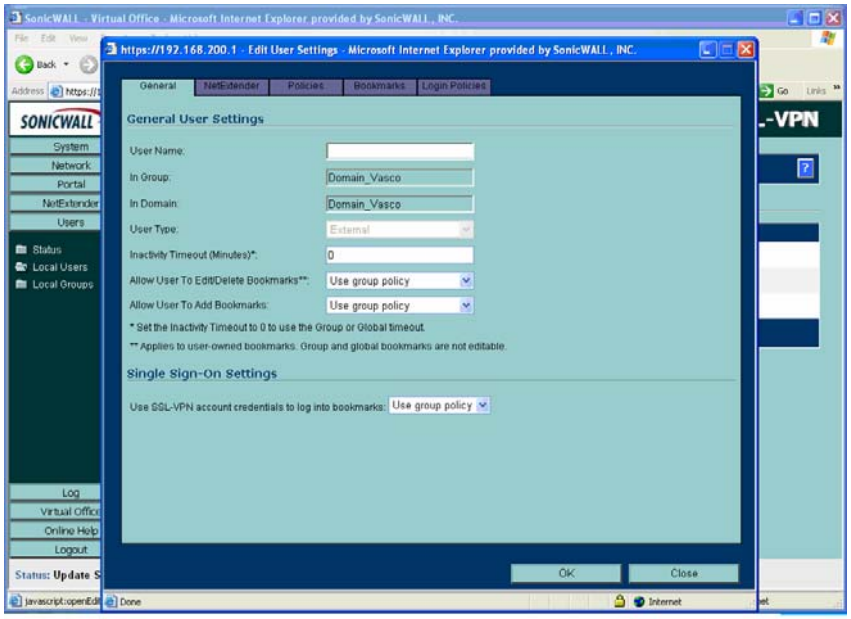

Figure 14: SonicWALL SSL/VPN configuration (12)

6 Configuration of the SonicWALL PRO4060

6.1 Login to the PRO4060

Browse to the default IP address of the SonicWALL PRO4060 on its LAN interface labeled 'X0' on http://192.168.168.168 and login with the default values:

User Name: admin
Password: password (please change afterwards)

The IP address will be changed later on to 10.120.1.250 according the network diagram in **Figure 1: Network Diagram**.

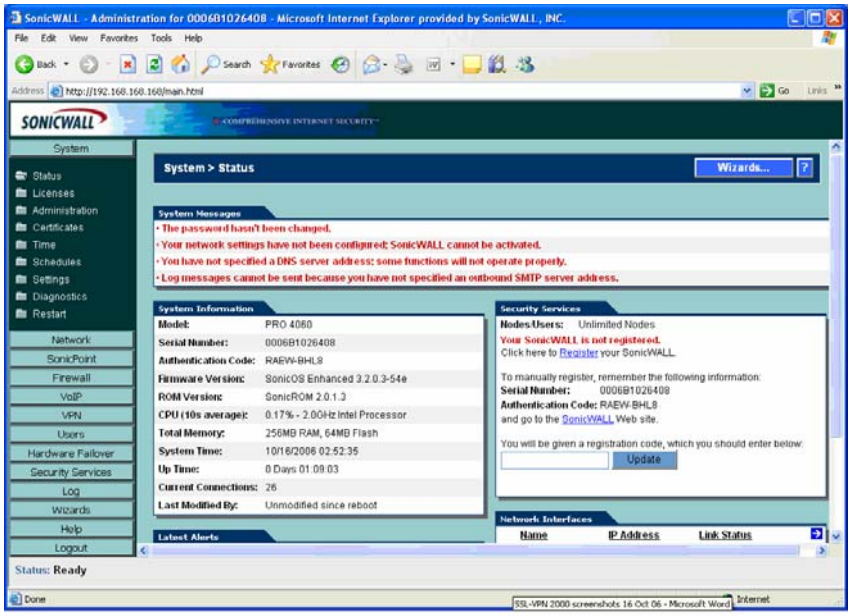

Figure 15: SonicWALL PRO4060 configuration (1)

It is advised that you register the SonicWALL PRO4060 appliance on https://www.mysonicwall.com where you can download the latest firmware version with a valid SonicWALL support entitlement.

6.2 PRO4060 Interface and Zone configuration

You can configure the correct IP addresses and Zones of the interfaces in the **Network > Interfaces** page according to the Network Diagram on page 9:

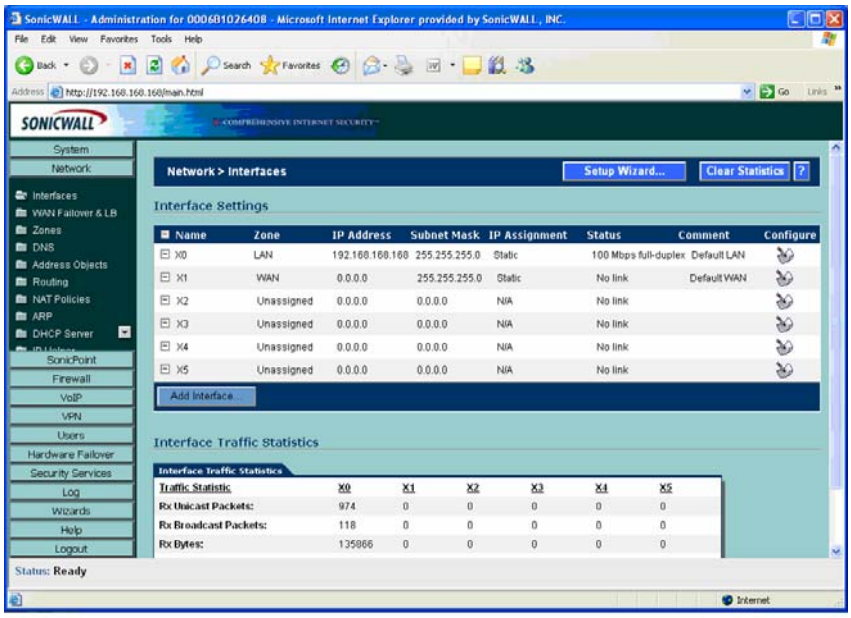

Figure 16: SonicWALL PRO4060 configuration (2)

Click on the 'Configure' button for the X2 interface and match it to the DMZ zone with IP address 192.168.200.250 as follows:

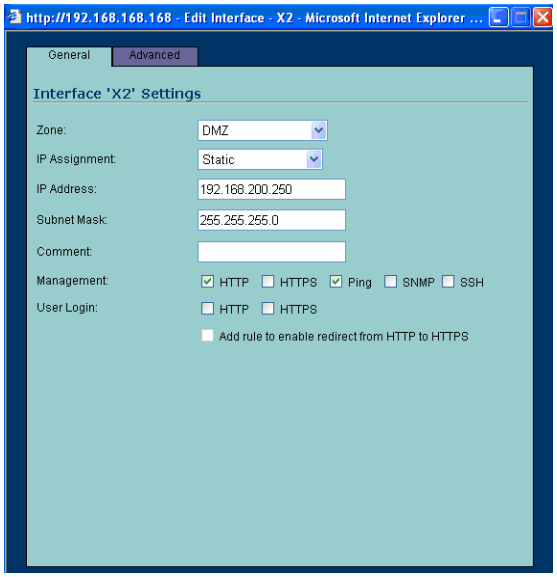

Figure 17: SonicWALL PRO4060 configuration (3)

Click on the 'Configure' button for the X1 interface (fixed tied to the WAN zone) and assign it the IP address 10.10.10.10 as follows:

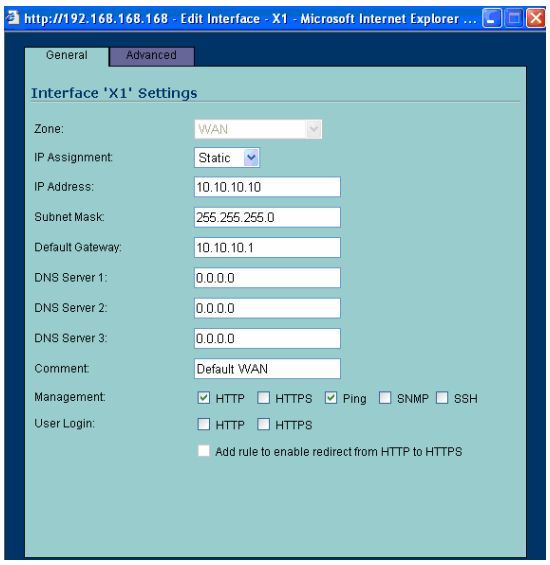

Figure 18: SonicWALL PRO4060 configuration (4)

Finally the X0 interface will be configured (fixed tied to the LAN zone) with IP address 10.120.1.250 as follows:

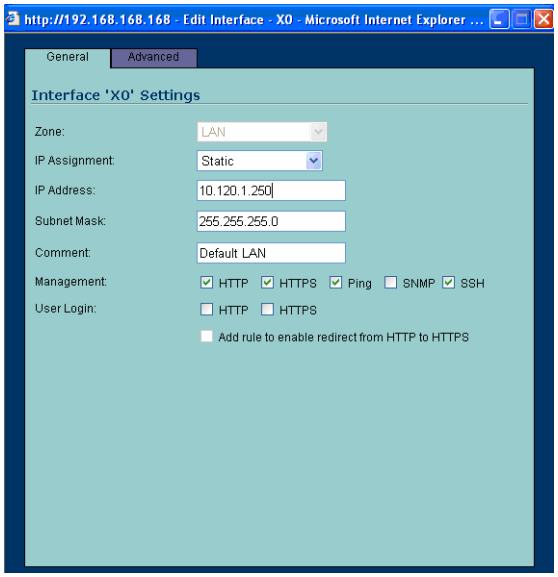

Figure 19: SonicWALL PRO4060 configuration (5)

As the IP address for accessing the GUI of the PRO4060 on its X0 interface is changed, the IP address of the machine (PC) accessing the GUI needs to be reconfigured in the same IP subnet as the X0 interface of the PRO4060.

After these changes, the summary in the **Network > Interfaces** page will look as follows:

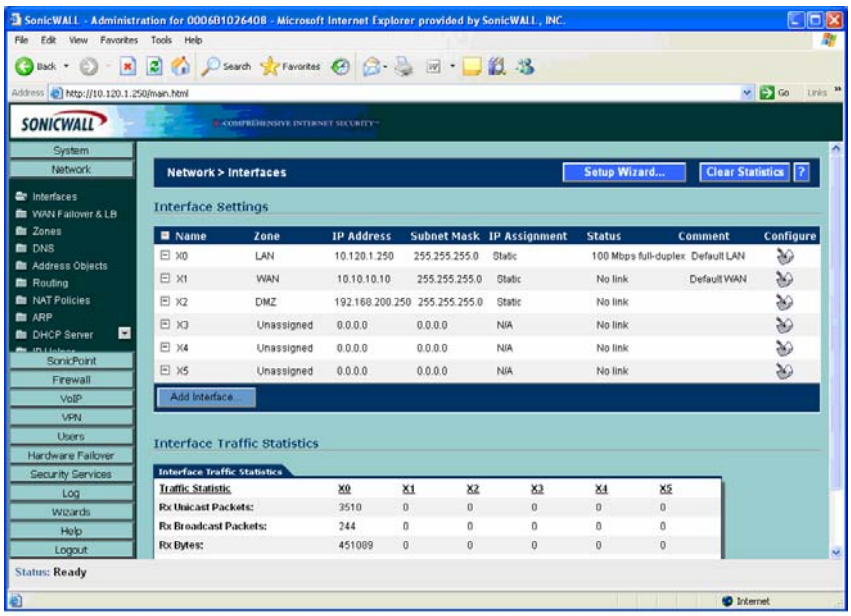

Figure 20: SonicWALL PRO4060 configuration (6)

6.3 Creating the Address Objects

Create a VACMAN Middleware object in the LAN zone with host IP 10.120.1.100 via the **Network > Address Objects** page by clicking the 'Add' button all the way down the screen:

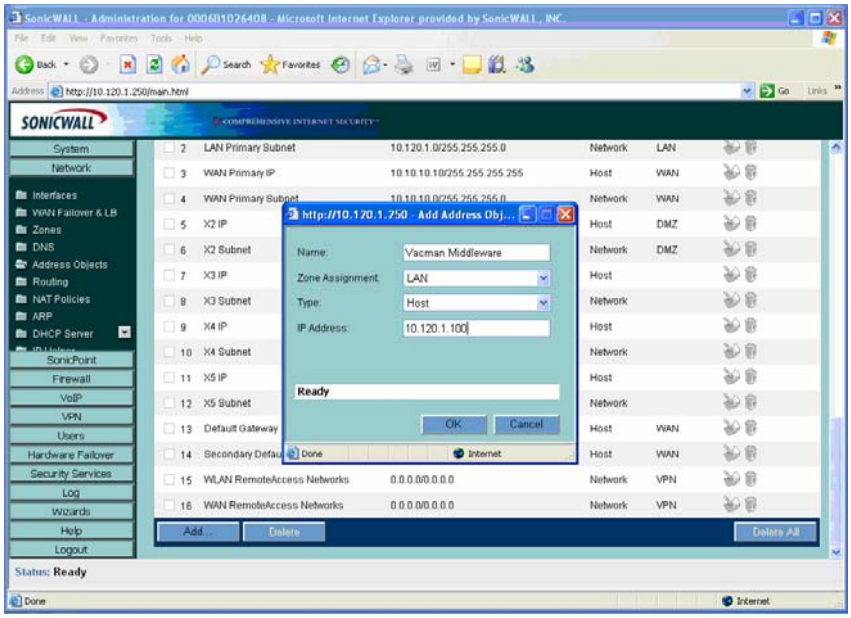

Figure 21: SonicWALL PRO4060 configuration (7)

The IP address matches the Network Diagram on page 9. Do the same for an SSL-VPN 2000 object in the DMZ zone:

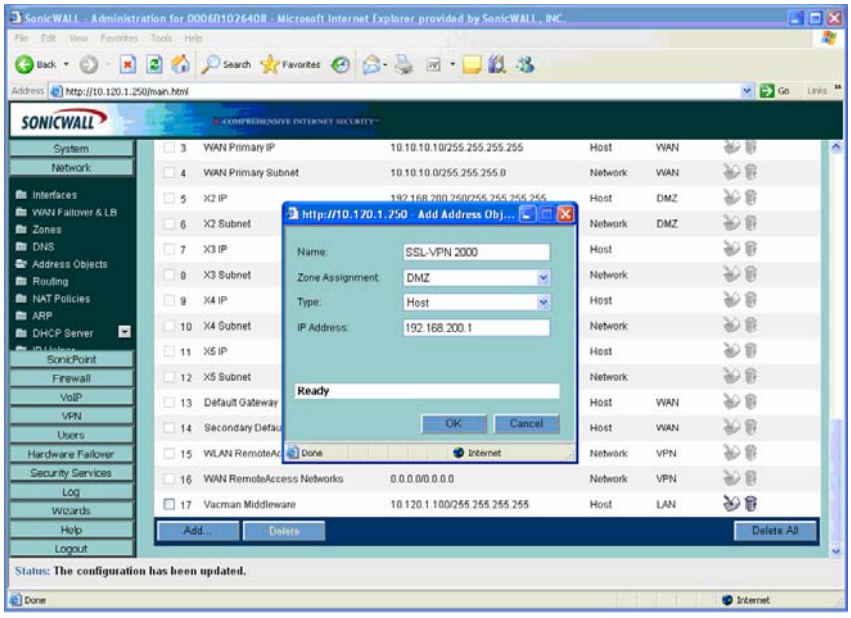

Figure 22: SonicWALL PRO4060 configuration (8)

6.4 Inbound allow rule for https & NAT Policy

In this chapter we will create an inbound 'Allow' rule to permit all https traffic on WAN to the SSL-VPN 2000 object in the DMZ zone. Select **Firewall > Access Rules** in the Matrix from WAN to DMZ:

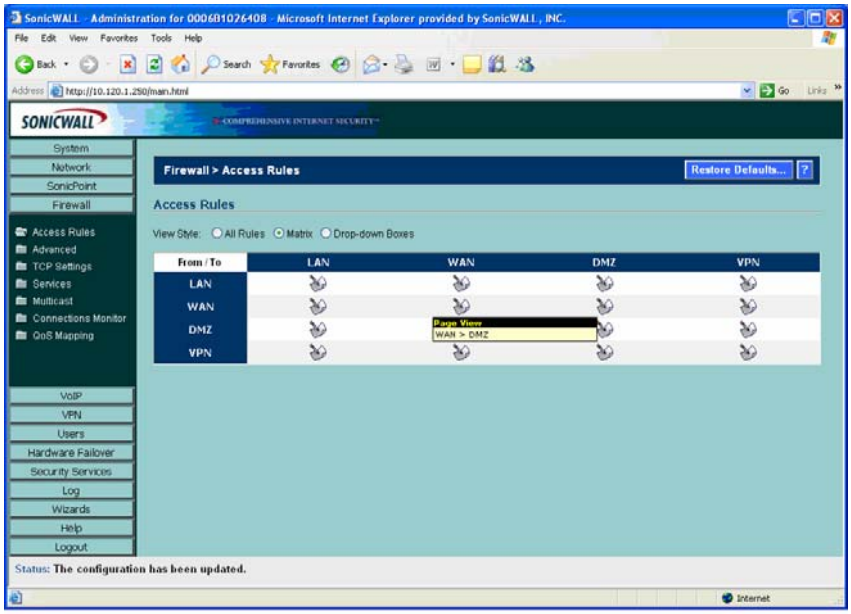

Figure 23: SonicWALL PRO4060 configuration (9)

Step 1: Create an 'Allow' access rule for https on the 'WAN primary IP' address object of the SonicWALL PRO4060 by clicking the 'Add' button:

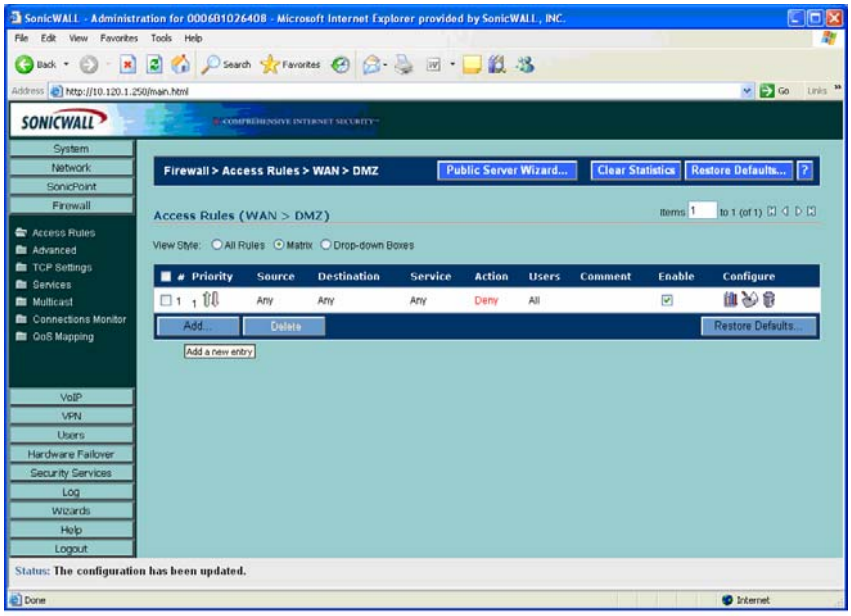

Figure 24: SonicWALL PRO4060 configuration (10)

The ‘Allow’ rule for https should look as follows:

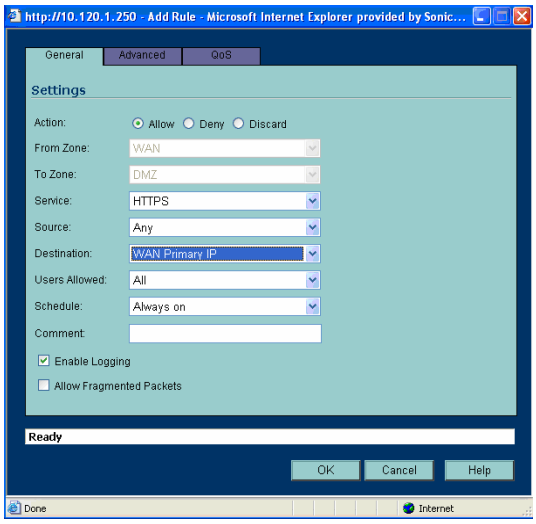

Figure 25: SonicWALL PRO4060 configuration (11)

Click ‘OK’ and the following ‘Access Rules’ will appear in the list from WAN to DMZ:

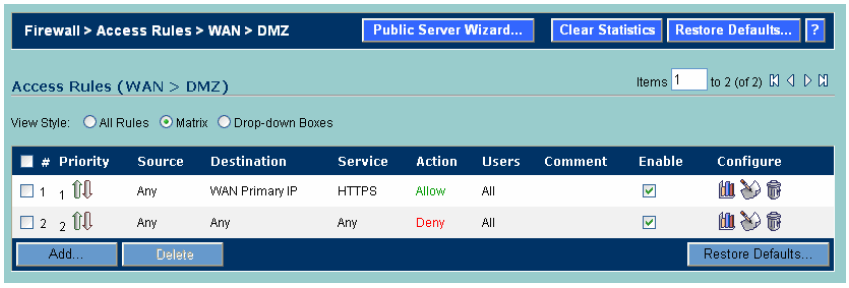

Figure 26: SonicWALL PRO4060 configuration (12)

Step 2: Create a NAT policy to forward the https traffic to the SSL-VPN 2000. Select **Network > NAT Policies** and ‘Add’ the following Policy all the way down the screen:

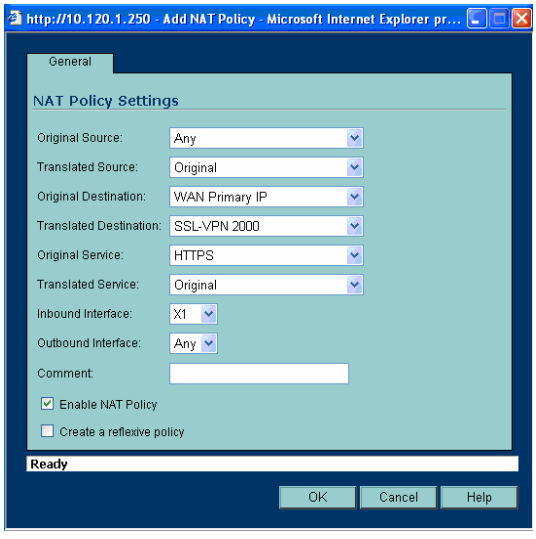

Figure 27: SonicWALL PRO4060 configuration (13)

6.5 Allow rule from DMZ to LAN for VACMAN Middleware

In this chapter we will create an access rule from the DMZ zone to the LAN zone for access to the VACMAN Middleware object. Select the Firewall > Access Rule page and indicate in the Matrix the Access Rules from DMZ to LAN. Add an 'Allow' rule as follows:

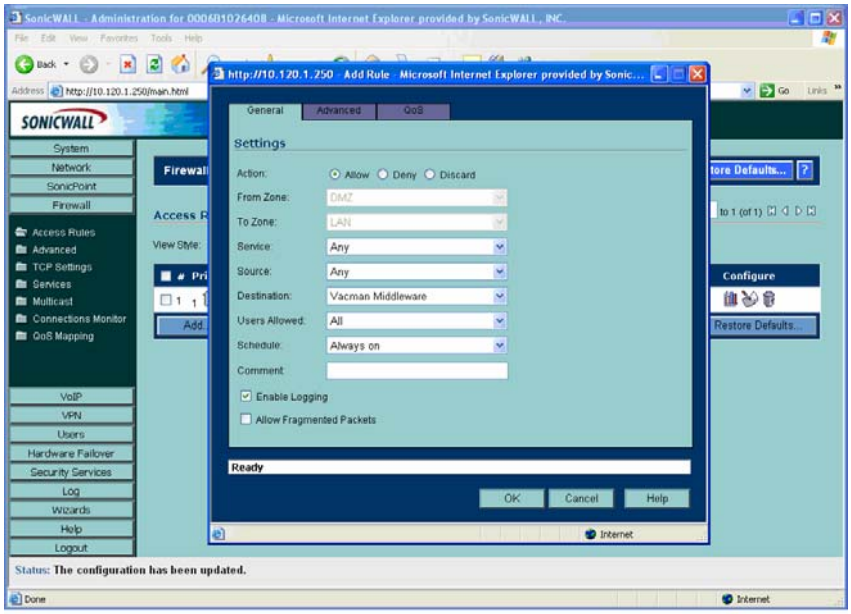

Figure 28: SonicWALL PRO4060 configuration (14)

If access from DMZ to LAN is needed towards more 'Destinations', other than the VACMAN Middleware, you have to add them here accordingly.

7 VACMAN Middleware

7.1 Policy configuration

Setting up the VM only requires you to set up a policy to go to the right back-end (or only local) and to add an extra RADIUS client component pointing to the SonicWALL SSL/VPN Server.

To add a new policy, right-click Policies and choose **New Policy**.

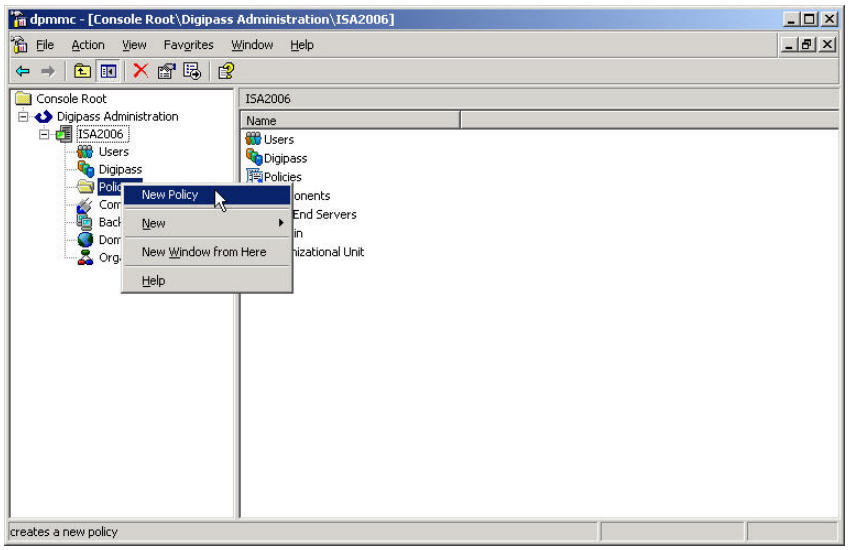

Figure 29: VM Policy Configuration (1)

There are a few policies available by default. You can also create new policies to suit your needs. Those can be independent policies, inherit or copy their settings from default or other policies.

Fill in a **policy name** and choose the **option** most suitable in your situation. If you want the policy to inherit setting from another policy, choose the inherit option. If you want to copy an existing policy, choose the copy option and if you want to make a new one, choose the create option.

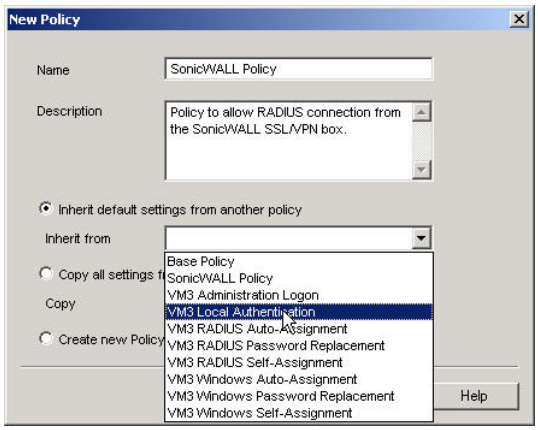

Figure 30: VM Policy Configuration (2)

In the policy properties configure it to use the right back-end server. This could be the local database, but also Windows (Active Directory) or another RADIUS server (RADIUS).

This can be the same authentication service as you were previously using in your SonicWALL VPN/SSL box.

In our example we select our SonicWALL policy:

- *Local Auth.:* Default (DIGIPASS/Password)
- *Back-End Auth.:* Default (None)
- *Dynamic User Registration:* Default (No)
- *Password Autolearn:* Default (No)
- *Stored Password Proxy:* Default (No)
- *Windows Group Check:* Default (No Check)

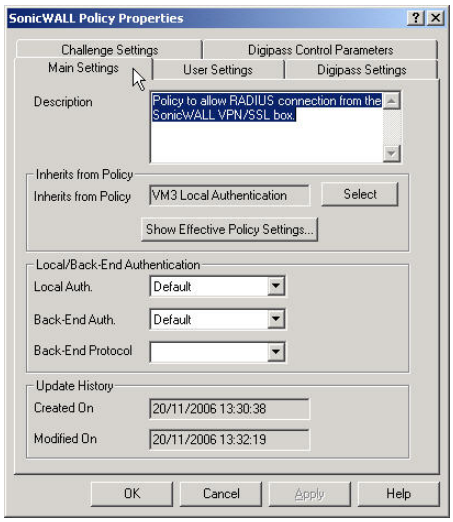

Figure 31: VM Policy Configuration (3)

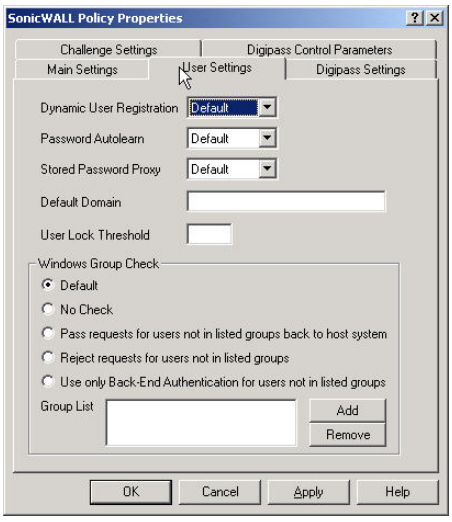

Figure 32: VM Policy Configuration (4)

7.2 Component configuration

Create a new component by right-clicking the Components and choose **New Component**.

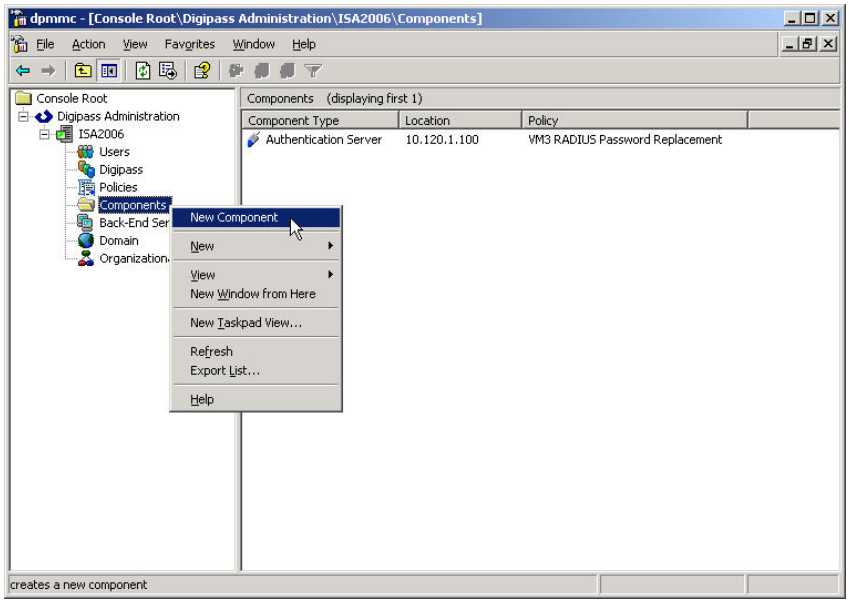

Figure 33: VM Component Configuration (1)

As component type choose **RADIUS Client**. The location is the **IP address of the SonicWALL SSL/VPN box**. In the policy field you should find your **newly created policy**. Fill in the **shared secret** you entered also in the RADIUS server properties on the SonicWALL SSL/VPN box. Click Create.

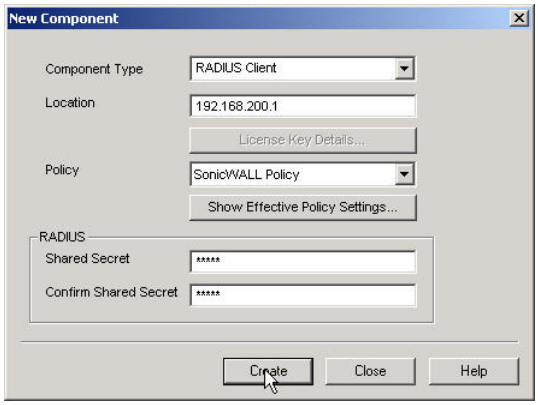

Figure 34: VM Component Configuration (2)

8 User configuration

The **user creation** steps you will find in this chapter are only necessary when you didn't activate the option **Dynamic User Registration (DUR) and/or Password Autolearn** in your policy settings. The assignment of a DIGIPASS can happen manually as explained in the steps below.

8.1 ODBC installation

8.1.1 User creation

User creation, while using an ODBC back-end, will happen in the DIGIPASS Administration MMC. Right-click the Users folder and select **New User ...**.

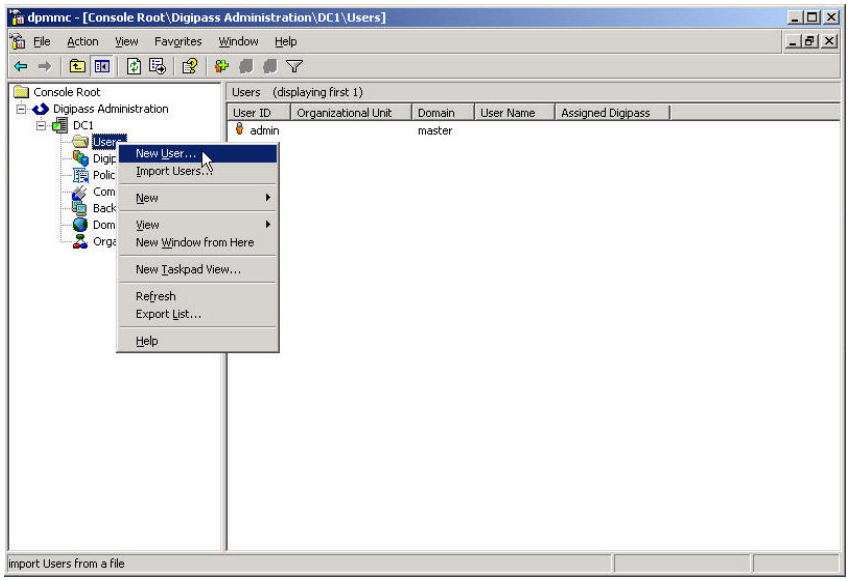

Figure 35: ODBC User Creation (1)

Fill in the username and password fields. Optionally choose the right domain and Organizational Unit and click the **Create** button.

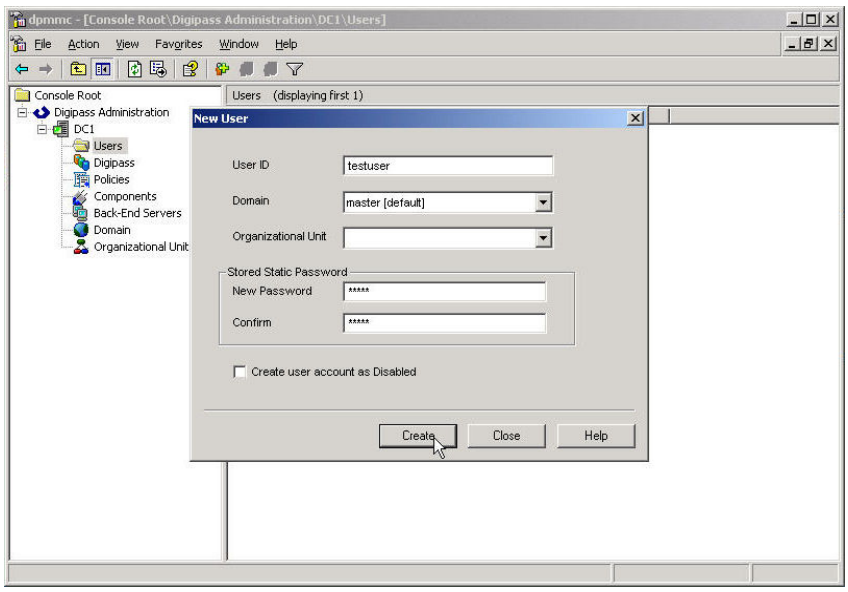

Figure 36: ODBC User Creation (2)

The user will now show up in the Users list of you DIGIPASS Administration MMC. At this point it will be exactly the same as when Dynamic User Recognition (DUR) was enabled.

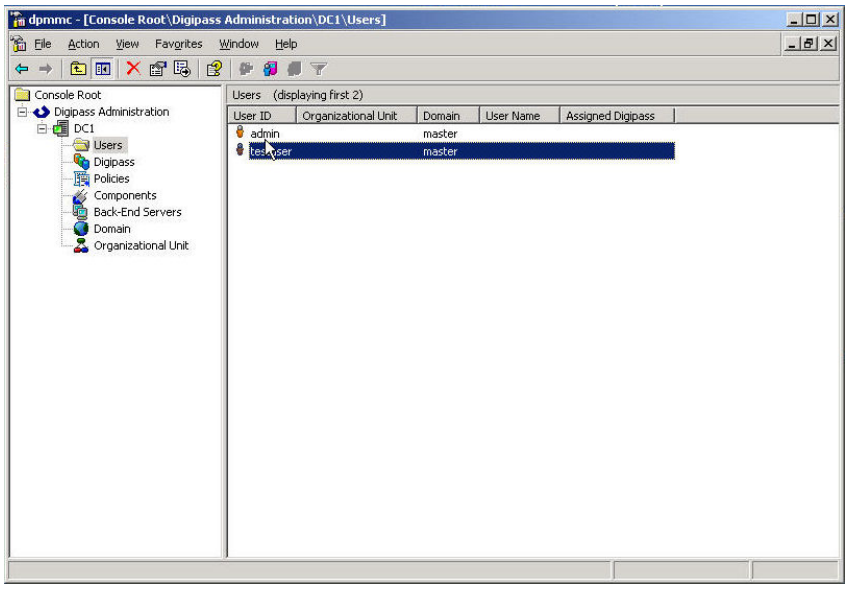

Figure 37: ODBC User Creation (3)

8.1.2 Import DIGIPASS

Right-click the DIGIPASS folder and select **Import DIGIPASS...** .

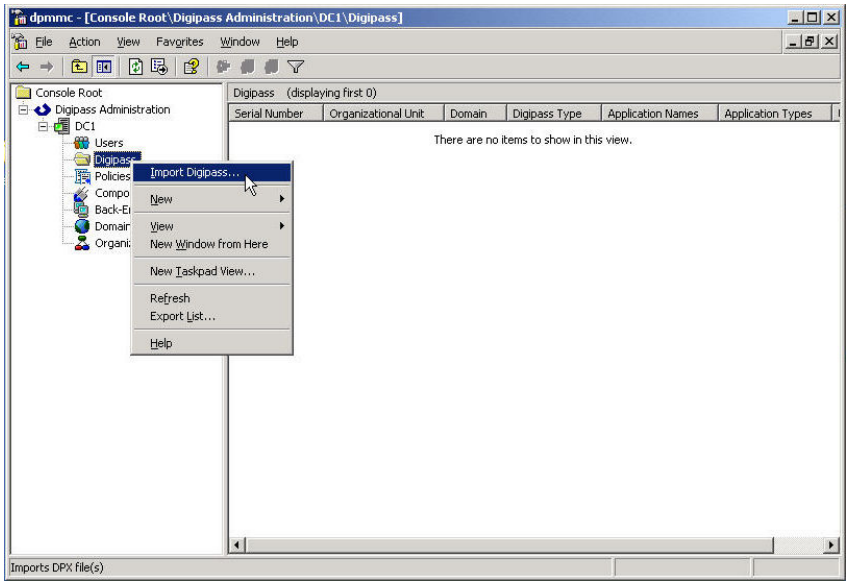

Figure 38: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import ...** buttons above and below the Show Applications button.

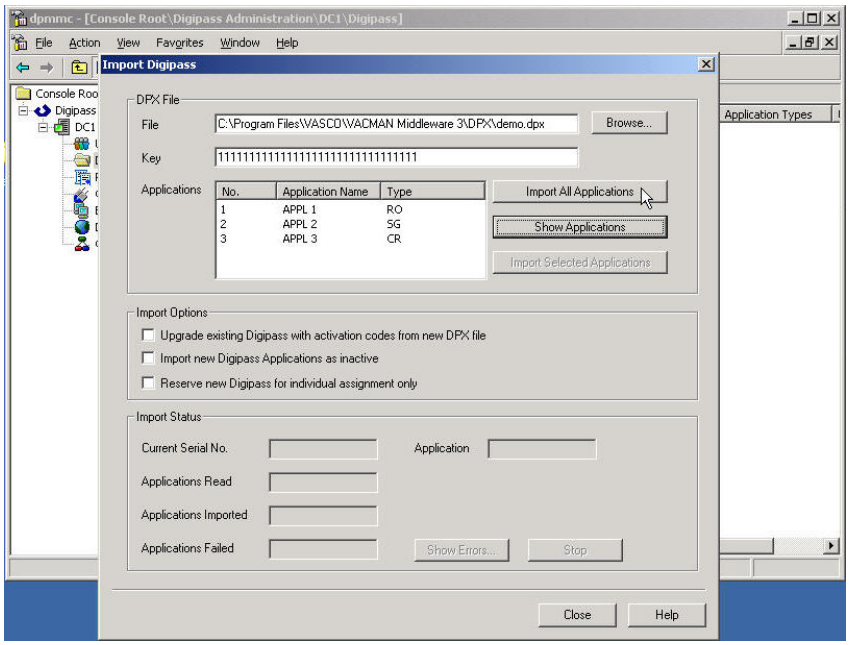

Figure 39: Import DIGIPASS (2)

When the DIGIPASS is imported successfully you will receive a confirmation message.

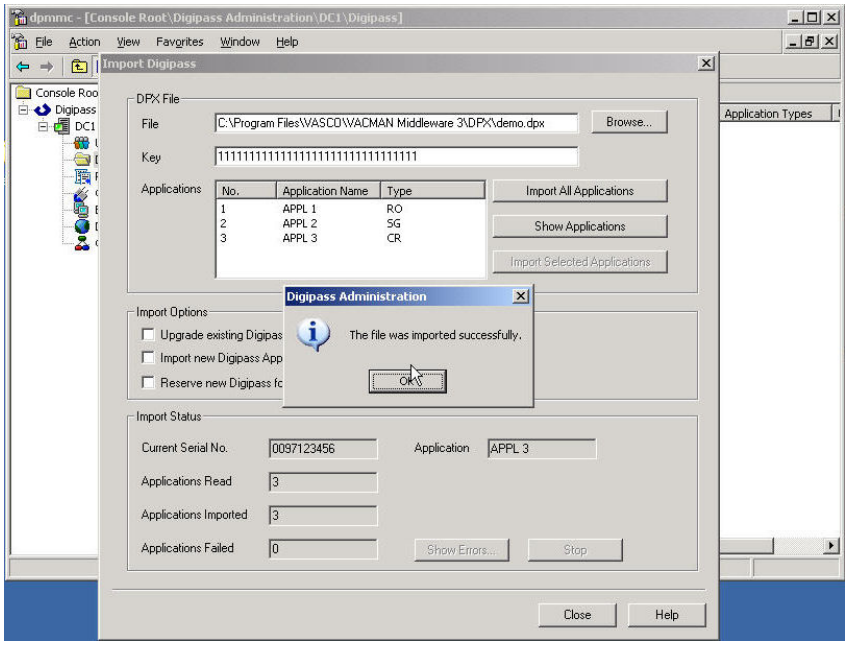

Figure 40: Import DIGIPASS (3)

8.1.3 DIGIPASS Assignment

There are two possible ways to assign a DIGIPASS to a user. You can search for a DIGIPASS and assign it to a user or you can search for a user and assign it to a DIGIPASS. You can see the difference in the following two figures.

Right-click a user and select **Assign DIGIPASS...** or …

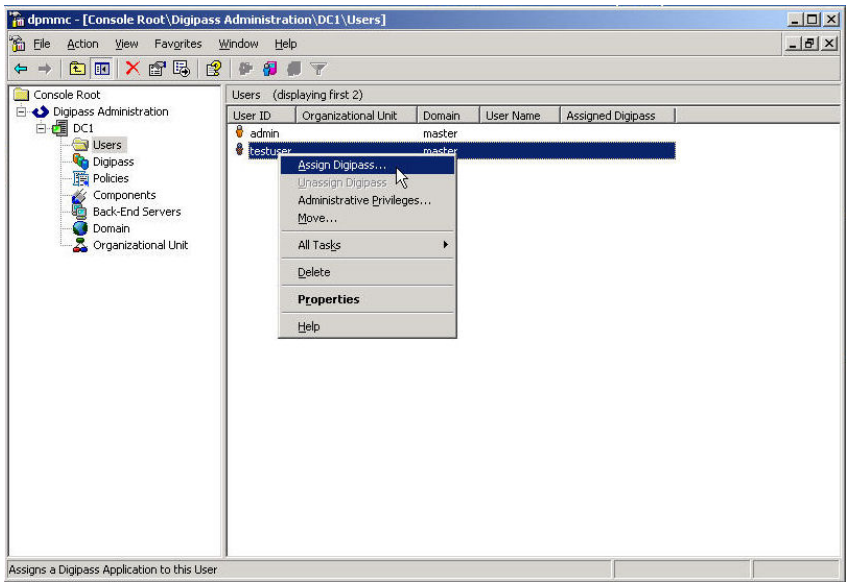

Figure 41: DIGIPASS assignment (1)

… you can right-click a DIGIPASS and select **Assign …** .

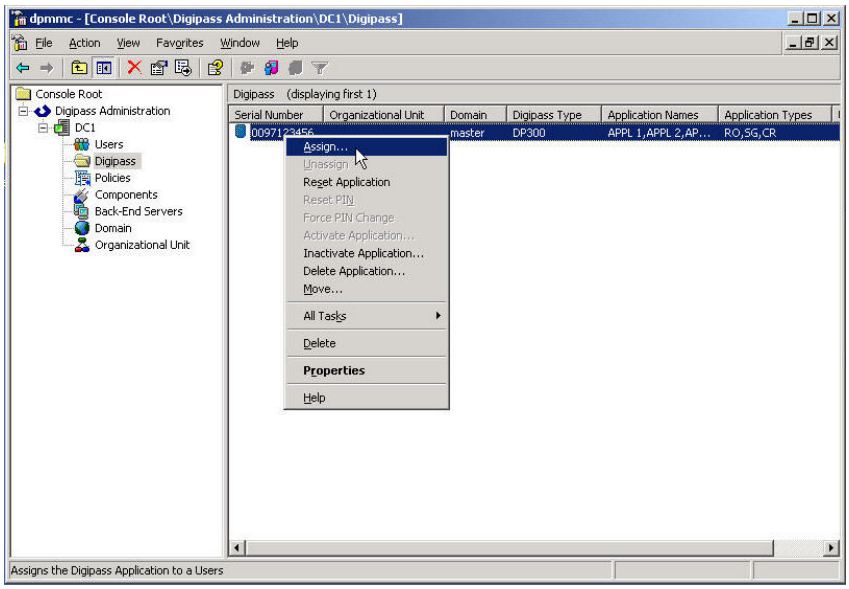

Figure 42: DIGIPASS assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

Notice: If no users show up, make sure the domains of the DIGIPASS and the user match.

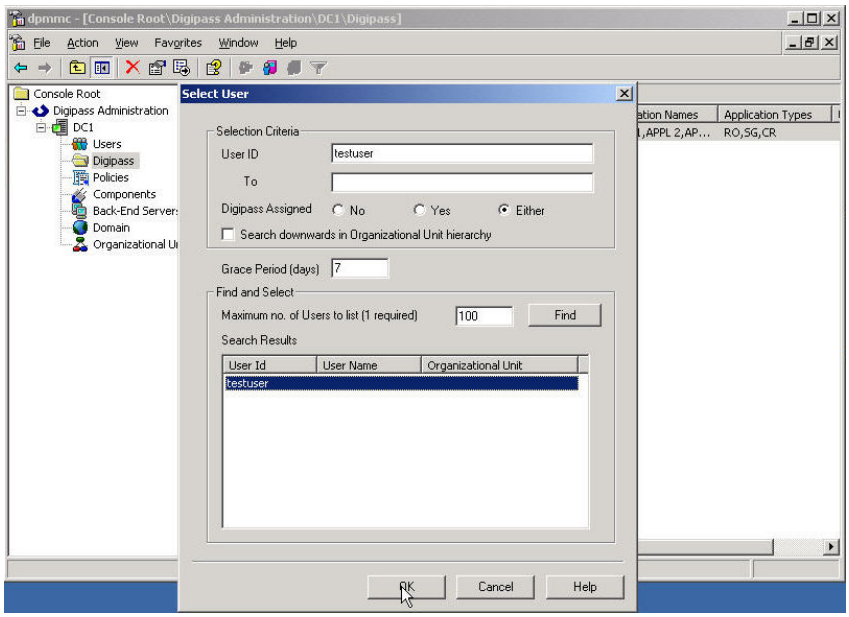

Figure 43: DIGIPASS assignment (3)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or search through serial number. Leaving all options blank will show all possibilities in the same domain.

When the DIGIPASS gets successfully added to your user you will get a confirmation message.

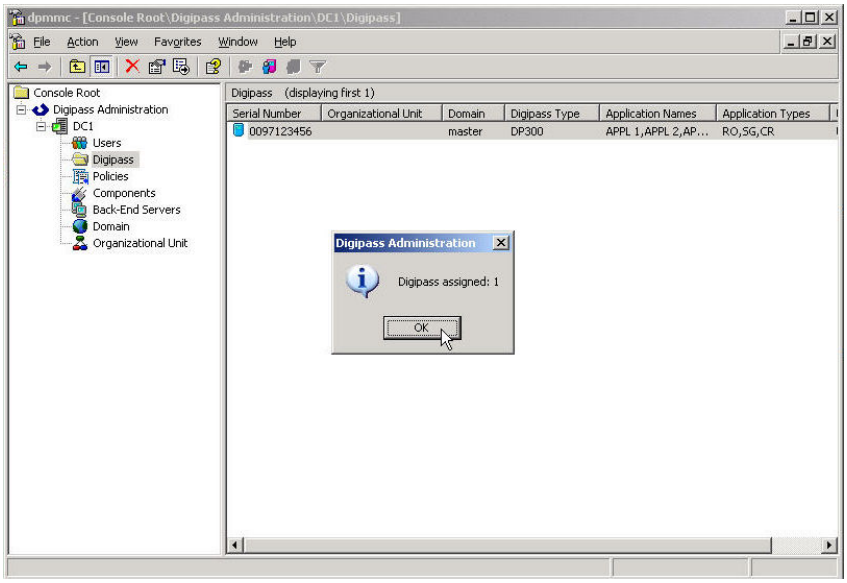

Figure 44: DIGIPASS assignment (4)

8.2 Active Directory installation

8.2.1 User creation

User creation, while using an Active Directory back-end, will happen in the **Active Directory Users and Computers MMC**. Right-click a user and select **Properties**. This can happen automatically when the Dynamic User Registration (DUR) option in the policy settings is active.

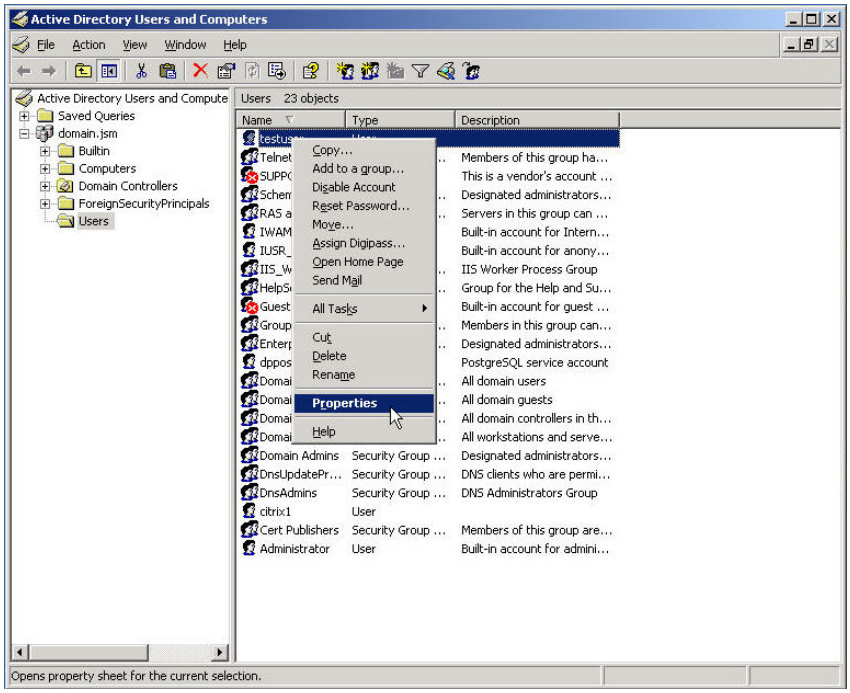

Figure 45: Active Directory User Creation (1)

In the **DIGIPASS User Account** tab you will see a field to manually add a password. This can also be automatically filled by enabling the 'stored password proxy' option in the policy settings.

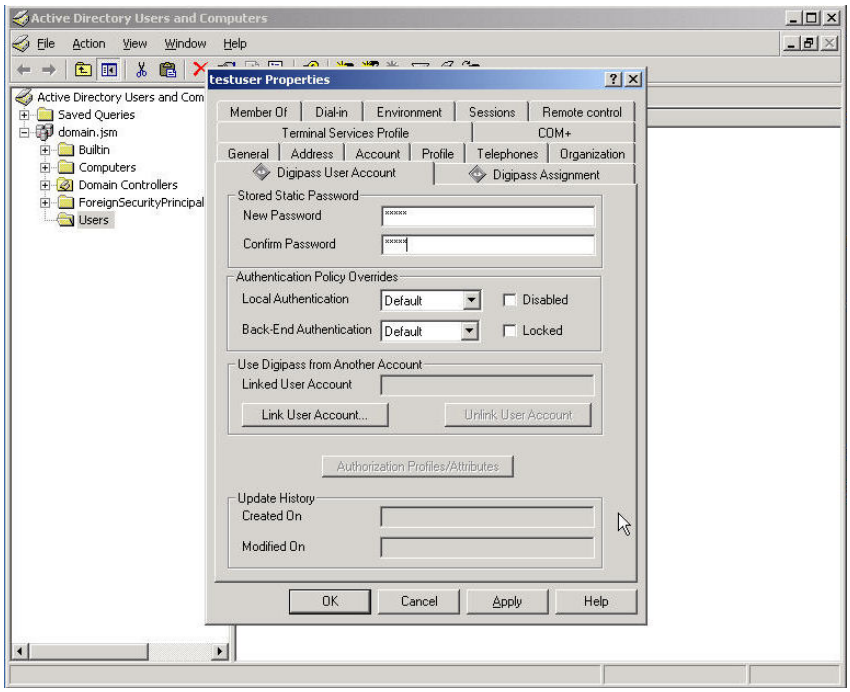

Figure 46: Active Directory User Creation (2)

After clicking the Apply button you will see the Update History fields being filled with the current date and time. When these fields are filled it means the DIGIPASS account exists and can be used.

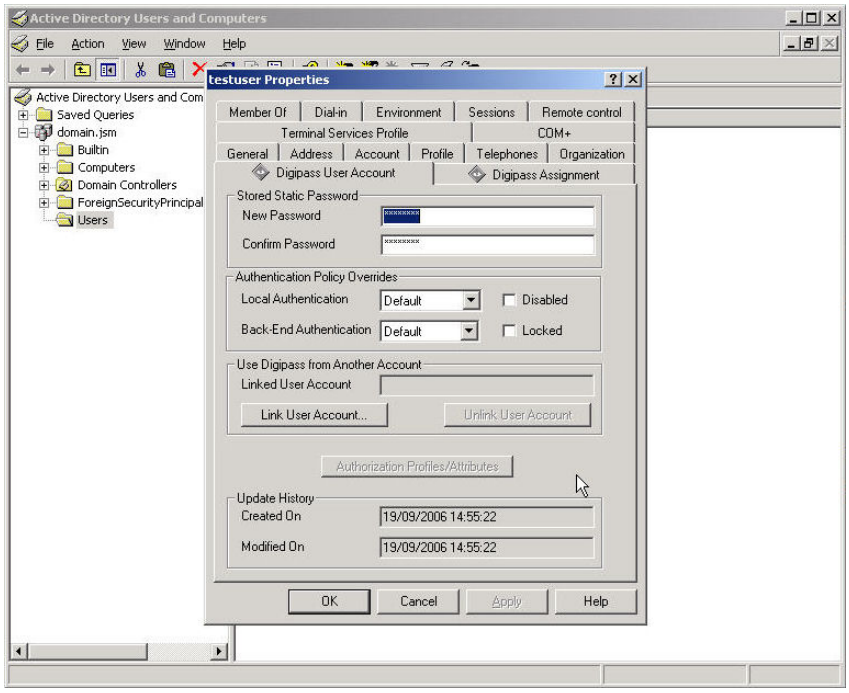

Figure 47: Active Directory User Creation (3)

8.2.2 Import DIGIPASS

To make sure you can see the DIGIPASS folders in the MMC, go to **View** and select the **Advanced Features**. This way you will see the DIGIPASS folders.

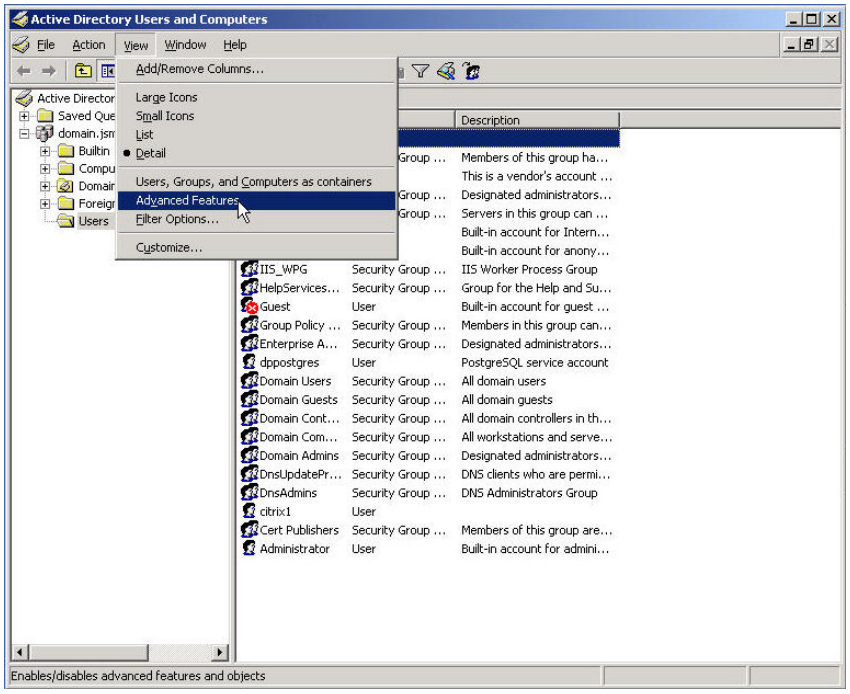

Figure 48: Import DIGIPASS (1)

Right-click the **DIGIPASS-Pool** folder and select **Import DIGIPASS …** .

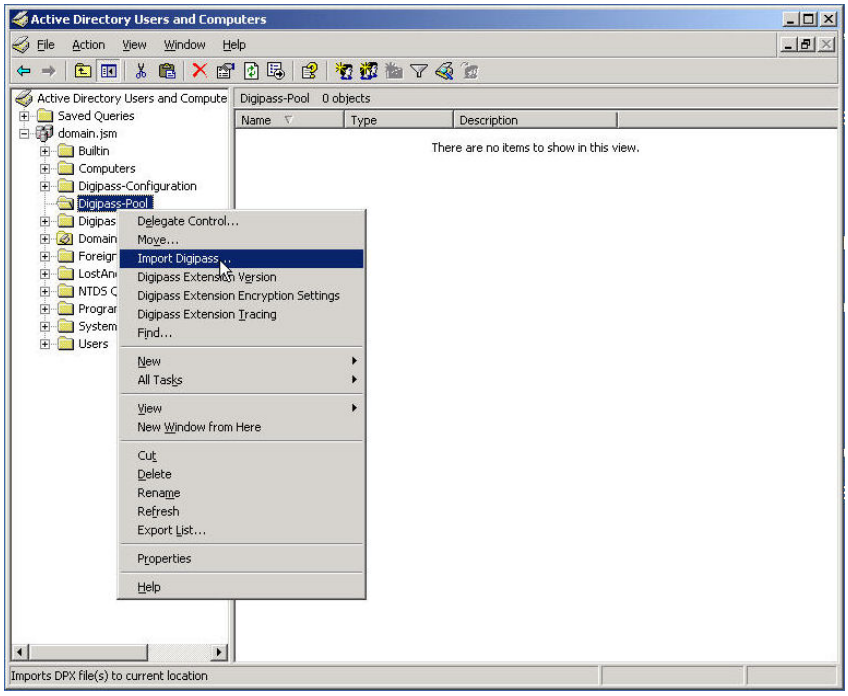

Figure 49: Import DIGIPASS (1)

Browse for your *.DPX file, fill in the Transport Key and look at your available applications by pushing the **Show Applications** button. You can either import all applications or only the ones you selected, by the **Import …** buttons above and below the Show Applications button.

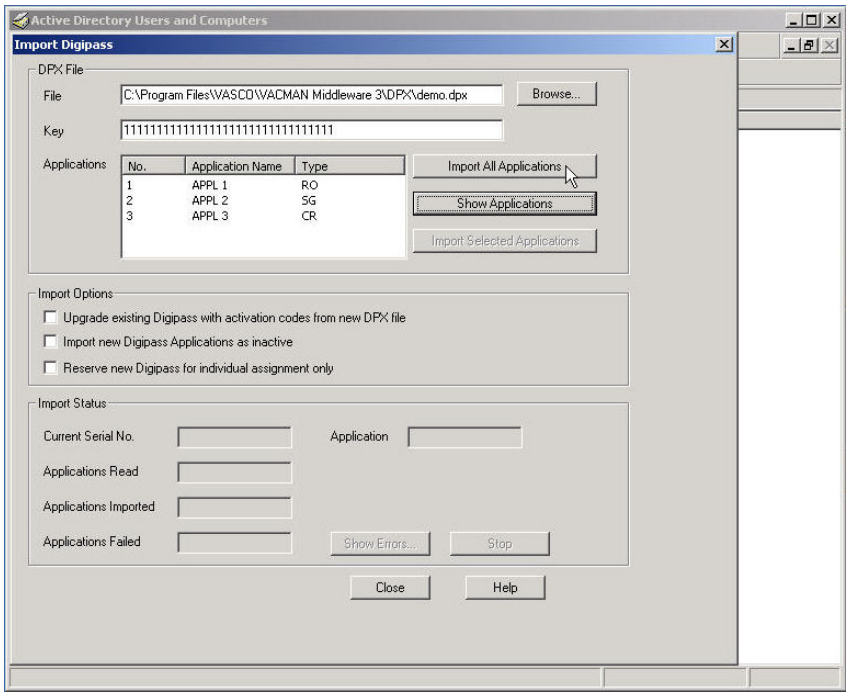

Figure 50: Import DIGIPASS (1)

When the DIGIPASS is imported successfully you will receive a confirmation message.

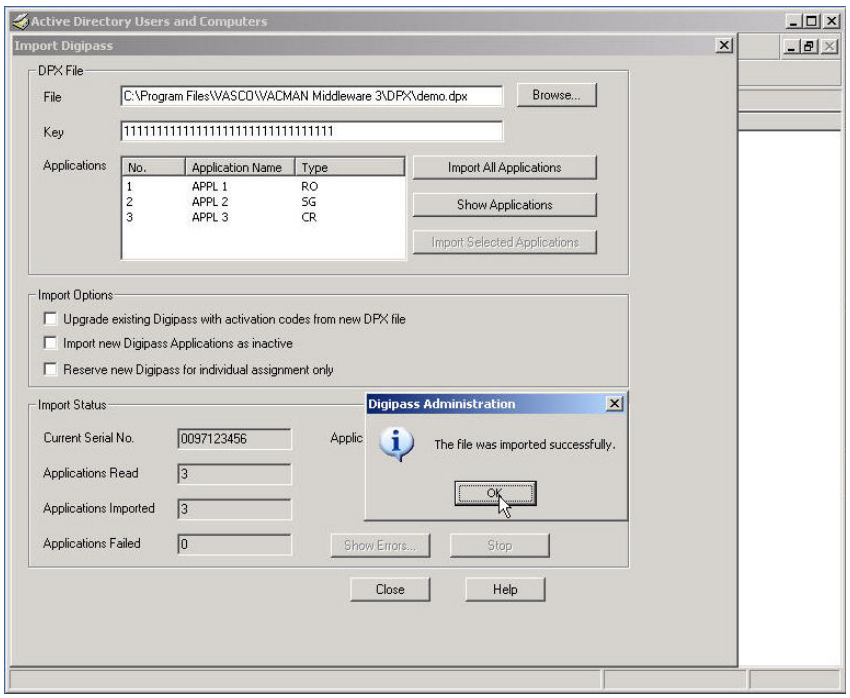

Figure 51: Import DIGIPASS (1)

8.2.3 DIGIPASS assignment

There are two possible ways to assign a user to a DIGIPASS. You can search for a DIGIPASS and assign it to a user or you can search for a user and assign it to a DIGIPASS. You can see the difference in the following two figures.

Right-click a **User** and select **Assign DIGIPASS...** or …

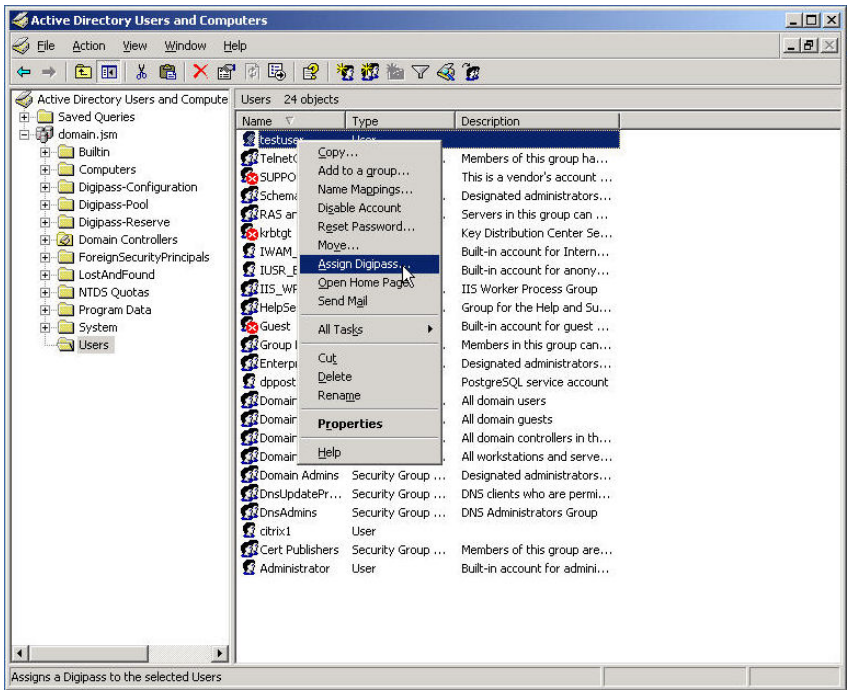

Figure 52: DIGIPASS Assignment (1)

… right-click a **DIGIPASS** and select **Assign DIGIPASS …** .

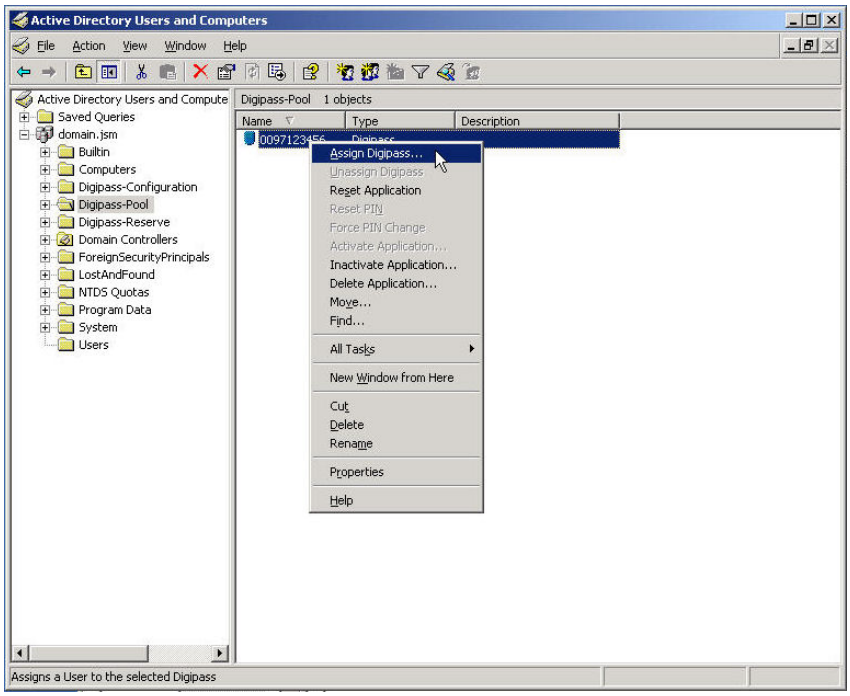

Figure 53: DIGIPASS Assignment (2)

If you leave the User ID **blank** and press the **Find** button, you will get a list of all the available users in the same domain as the DIGIPASS. The usernames are partly searchable too.

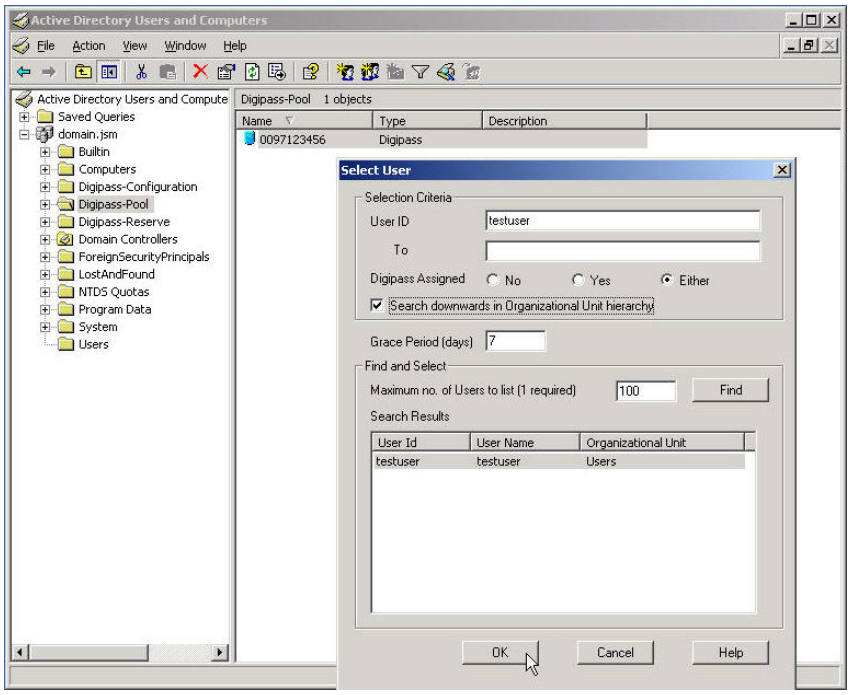

Figure 54: DIGIPASS Assignment (4)

When assigning a DIGIPASS to a user the same procedure will be applicable. You can either select the desired option to search for a DIGIPASS or through serial number. Leaving all options blank will show you all possibilities. Remember to check the "**Search upwards …**" checkbox.

9 Two-factor authentication SSL-VPN test and conclusion

To test the two-factor authentication SSL-VPN connectivity with VACMAN Middleware, connect your PC on the WAN (X1) interface of the PRO4060 according to **Figure 1: Network Diagram**. Point your browser to https://10.10.10.10

First login as an 'Administrator' to the LocalDomain' with:

User Name: 'admin' and Password: 'password' (assuming you left the Administrator access temporarily to the default values for test reasons).

Select **Portal > Domains** and click the 'Configure' button where you can 'Test' the RADIUS connectivity to the VACMAN Middleware by entering a valid RADIUS Username/Password combination:

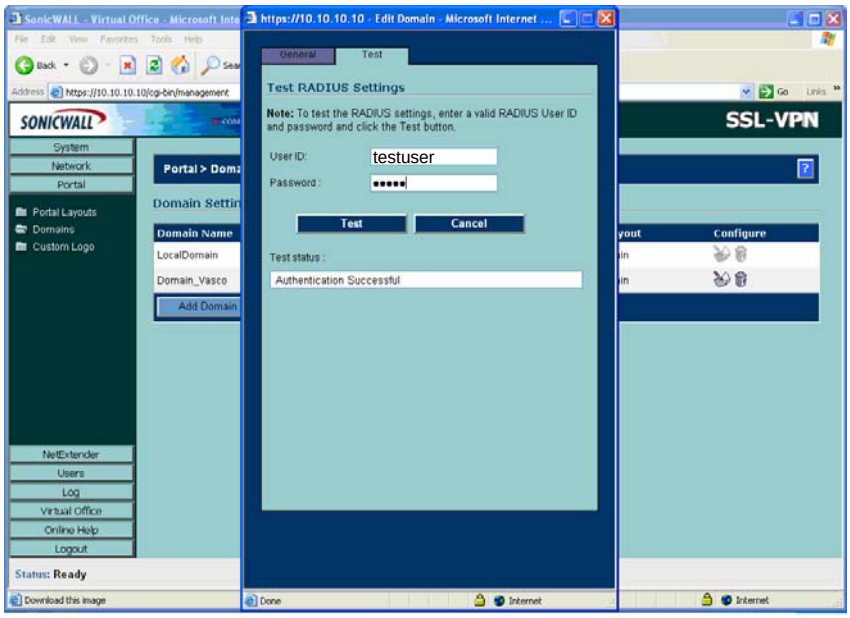

Figure 55: Test and conclusion (1)

If the RADIUS Authentication is successful, logout the Administrator GUI and login https://10.10.10.10 again with the 'testuser' User Name you created:

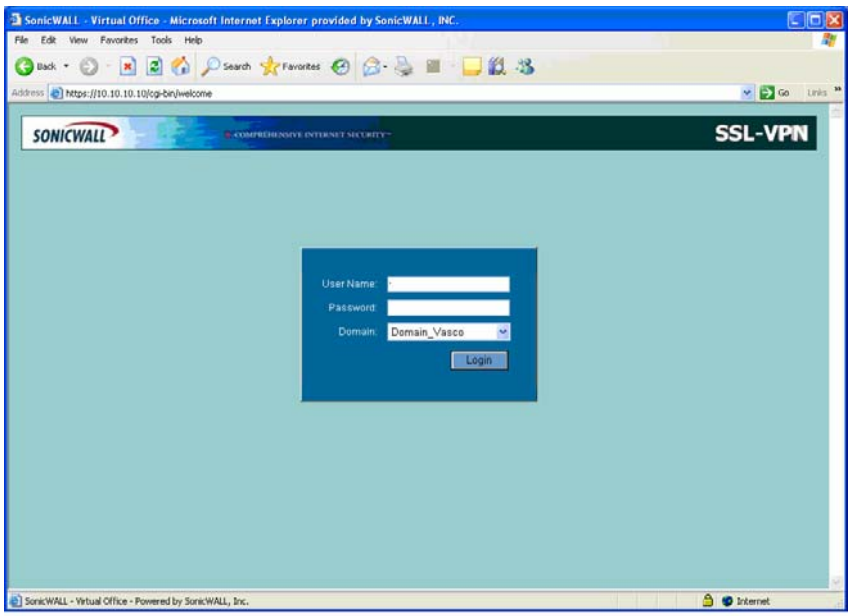

Figure 56: Test and conclusion (2)

Use the FixedPassword+DIGIPASSPIN+DIGIPASSOTP password combination for access to the SSL-VPN Portal where you have access to your Bookmarks or NetExtender (IPSec alike SSL-VPN) connectivity:

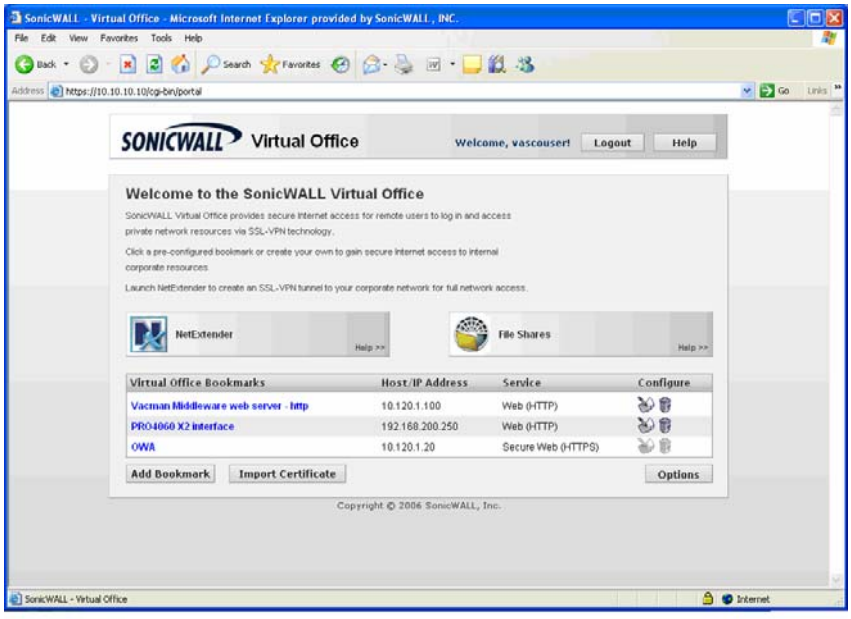

Figure 57: Test and conclusion (3)

Conclusion:

SonicWALL SSL-VPN and firewall/VPN appliances together with DIGIPASS authentication solutions provide easy and secure clientless remote access to the user dependent internal network resources.

10 VACMAN Middleware features

10.1 Installation

The VACMAN Middleware (VM) installation is very easy and straightforward. VM runs on Windows platforms, supports a variety of databases and uses an online registration. Different authentication methods allow a seamless integration into existing environments.

10.1.1 Support for Windows 2000, 2003, IIS5 and IIS6

VM can be installed on Windows 2000 and Windows 2003. Web modules exist for IIS5 and IIS 6 to protect Citrix Web Interface, Citrix Secure Gateway, Citrix Secure Access Manager (Form-based authentication), Citrix Access Gateway and Microsoft Outlook Web Access 2000 and 2003 (Basic Authentication and Form-Based Authentication).

10.1.2 Support for ODBC databases and Active Directory

Any ODBC compliant database can be used instead of the default PostgreSQL database (MS SQL Server, Oracle). Since Version 2.3 of VACMAN Middleware, AD is **not only** intended for storage of DIGIPASS anymore, but configuration and management of your DIGIPASS infrastructure is now also full integrated into the AD management tools. This option requires an AD schema update.

10.2 Deployment

Several VACMAN Middleware features exist to facilitate deployment. Combining these features provides different deployment scenarios from manual to fully automatic.

10.2.1 Dynamic User Registration (DUR)

This feature allows VM to check a username and password not in the database with a back-end RADIUS server or a Windows domain controller and, if username and password are valid, to create the username in the VM database.

10.2.2 Autolearn Passwords

Saves administrators time and effort by allowing them to change a user's password in one location only. If a user tries to log in with a password that does not match the password stored in the VM database, VM can verify it with the back-end RADIUS server or the Windows domain controller and, if correct, store it for future use.

10.2.3 Stored Password Proxy

Allows VM to save a user's RADIUS server password or Windows domain controller password in the database (static password). User's can then log in with only username and dynamic one-time password (OTP). If this feature is disabled, users must log in with username and static password immediately followed by the OTP.

10.2.4 Authentication Methods

Different authentication methods can be set on server level and on user level: local authentication (VM only), Back-End authentication (Windows or RADIUS). On top of that a combination of local and back-end can be configured. The additional parameters 'always', 'if needed' and 'never' offers you additional customization of the back-end authentication process.

The configuration of authentication methods is done within the policy (policies).

10.2.5 Policies

Policies specify various settings that affect the User authentication process. Each authentication request is handled according to a Policy that is identified by the applicable Component record. Components can be radius clients, authentication servers or Citrix web interfaces.

10.2.6 DIGIPASS Self Assign

Allows users to assign DIGIPASS to themselves by providing the serial number of the DIGIPASS, the static password and the OTP.

10.2.7 DIGIPASS Auto Assign

Allows automatic assignment of the first available DIGIPASS to a user on user creation.

10.2.8 Grace Period

Supplies a user with a certain amount of time (7 days by default) between assignment of a DIGIPASS and the user being required to log in using the OTP. The Grace Period will expire automatically on first successful use of the DIGIPASS.

10.2.9 Virtual DIGIPASS

Virtual DIGIPASS uses a text message to deliver a One Time Password to a User's mobile phone. The User then logs in to the system using this One Time Password.

Primary Virtual DIGIPASS

A Primary Virtual DIGIPASS is handled similarly to a standard physical DIGIPASS. It is imported into the VACMAN Middleware database, assigned to a User, and treated by the VACMAN Middleware database as any other kind of DIGIPASS.

Backup Virtual DIGIPASS

The Backup Virtual DIGIPASS feature simply allows a User to request an OTP to be sent to their mobile phone. It is not treated as a discrete object by VACMAN Middleware, and is not assigned to Users, only enabled or disabled. It can be enabled for Users with another type of DIGIPASS already assigned, and used when the User does not have their DIGIPASS available.

10.3 Administration

10.3.1 Active Directory Users and Computers Extensions

Since VACMAN Middleware version 2.3, Managing the users and DIGIPASS can be done within the Active Directory Users and Computers section. Selecting the properties of a user, offers complete User-DIGIPASS management.

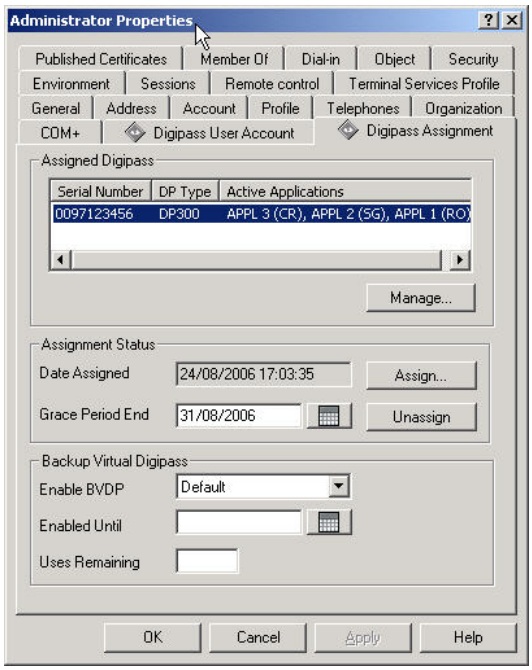

Figure 58: VM Features (1)

10.3.2 Administration MMC Interface

A highly intuitive Microsoft Management Console (MMC) exists to administer the product. An Audit Console is available to give an instant view on all actions being performed on the VM. Both can be installed on the VM server itself or on a separate PC.

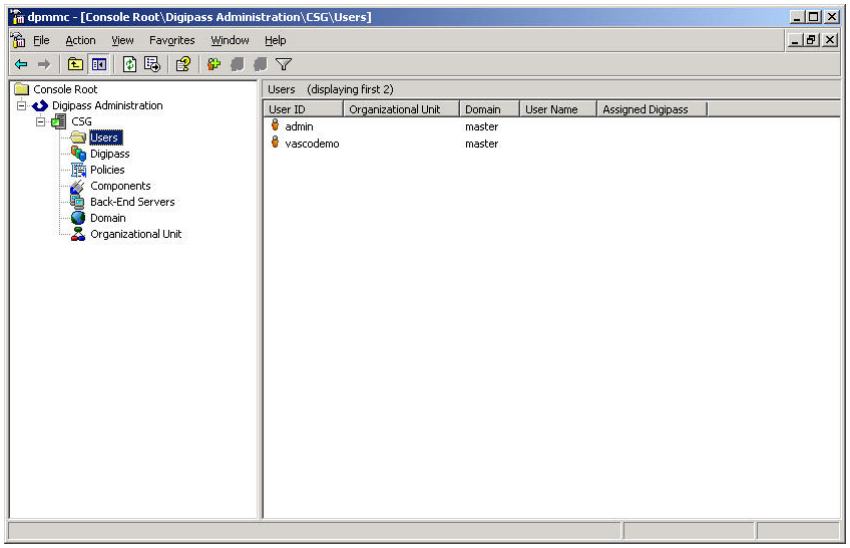

Figure 59: VM Features (2)

10.3.3 User Self Management Web Site

A web site running on IIS has been developed to allow users to register themselves to the VM with their username and back-end (RADIUS or Windows) password, to do a DIGIPASS self assign, to update their back-end password stored in the VM database, to do a change PIN (Go-1/Go-3 DIGIPASS), to do a DIGIPASS test.

Figure 60: VM Features (3)

10.3.4 Delegated administration

Administration can be delegated by appointing different administrators per organizational unit (OU). These administrators can only see the DIGIPASSes and users that were added to his OU.

10.3.5 Granular access rights

It is possible in VACMAN Middleware to setup different permission per user. This can be in function of a domain or an organizational unit. Administrators belonging to the Master Domain may be assigned administration privileges for all domains in the database, or just their own domain. Administrators belonging to any other Domain will have the assigned administration privileges for that Domain only.

It's possible to set different operator access levels.
E.g. A user can be created that only has the rights to unlock a DIGIPASS.

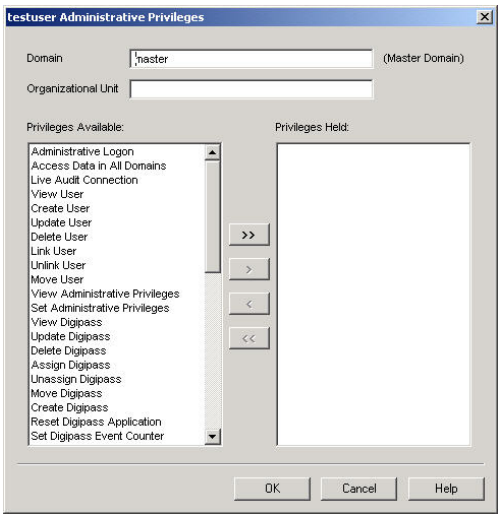

Figure 61: VM Features (4)

11 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO's User Authentication software is carried by the end user on its DIGIPASS products which are small "calculator" hardware devices, or in a software format on mobile phones, other portable devices, and PC's.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO's target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO's time-based system generates a "one-time" password that changes with every use, and is virtually impossible to hack or break.

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO's user authentication software is delivered via its DIGIPASS hardware and software security products. With over 25 million DIGIPASS products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 500 international financial institutions and almost 3000 blue-chip corporations and governments located in more than 100 countries.