

# Implementation Guidelines



Wireless Secure Access

## **DynaPass Implementation Guidelines**

### **Abstract**

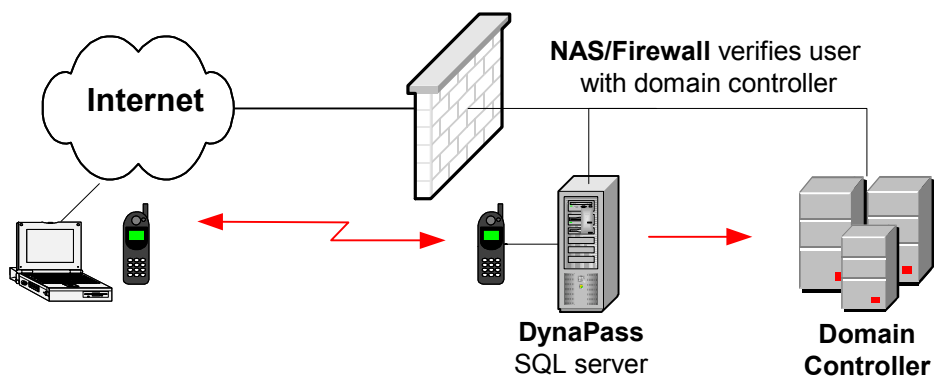
This document describes DynaPass implementations. Examples are based on different technologies used for Remote Access to private networks. It doesn't cover all issues or details; it is only intended to give basic fundamentals for how DynaPass can be implemented.

### **Overview**

DynaPass can be installed and configured in many different ways in your network. The purpose of this document is to give some general guidelines about how to implement DynaPass in different environments. Basically DynaPass assigns passwords and control User Accounts in a Domain. The Domain can be implemented as a Windows NT Domain, a W2000 Active Directory or a NOVELL NDS/eDirectory. Selected users in the Domain can be controlled by DynaPass. These users can request a password by sending an SMS from his mobile phone to the DynaPass server. DynaPass responds to the request with a number of actions.

- Checks if the request originates from a registered mobile phone
- The account is enabled (it will be disabled when the configured time limit expires)
- A random password is assigned to the account.
- The password is returned to the user as an SMS to the users mobile phone.

The user can now log on to the domain using the received password. When the time limit expires he will no longer be able to logon to the domain, the account is disabled and the password does not exist anymore. This does not necessarily mean that he cannot continue working when the time limit has expired. He can still use the resources he did set up during the initial login but he will not be able to allocate new resources.



When you configure DynaPass to control users in your main logon domain the result is that the user must always get a password from DynaPass to be able to access resources on the network. Selected users, for

## *DynaPass – Implementation Guidelines*

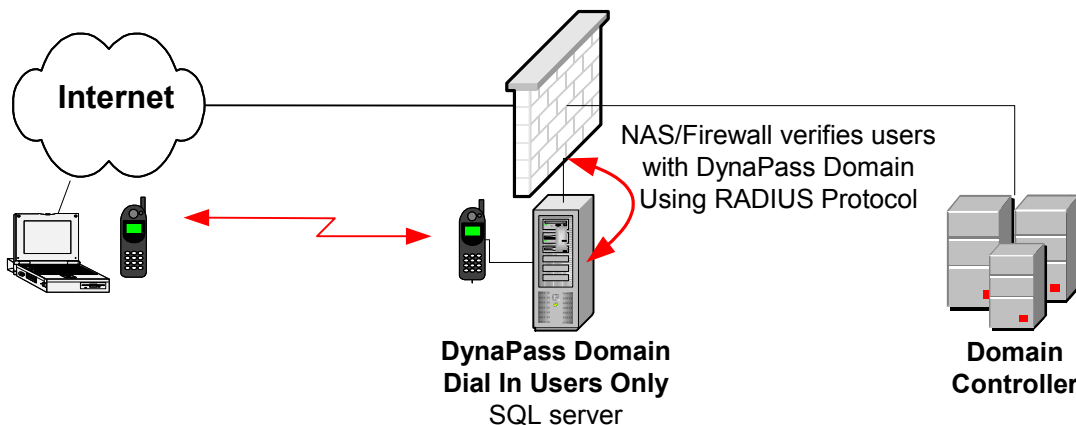
example critical accounts and users with dial in access can be controlled by DynaPass. The procedure is always the same regardless of where the user is located when he tries to log on. If you want maximum security and protection for your network you should select this configuration and use DynaPass for **all** users. Obviously this means a change of the log on procedures to the domain for all users. It also affects the way you log on when you want to use your machine for local tasks only.

Cached log on **to the domain** (using last successful domain log on name and password) when you power up your computer “off line” is still possible but since the password is valid only for a short time and frequently changed you will sooner or later loose it (probably by deleting the corresponding DynaPass message from your phone). In this situation you must physically connect to the domain or use a local account to be able to log on and access your computer.

If you consider your current "in the office" log on procedures safe and don't want to change these, you can install DynaPass to control **only remote access users**. This can be implemented in many different ways and this document will show some examples.

### **Let DynaPass Create the Door and Provide the Key**

The general idea in all examples is to let DynaPass control **the Entrance** to your network. Once you are inside your normal domain security policies and procedures are used. To achieve this we set up a separate domain and configure DynaPass to control the users in this domain. This domain contains **only** the users that are allowed access from the outside world. The Network Access Server (NAS) always ask this domain controller to verify the user before he is connected to your network. User names in the DynaPass domain can be the same as in the main domain. Note however that there are no trusts between the DynaPass domain and the main domain.



The NAS can be of different nature, for example Microsoft RRAS or CISCO VPN concentrator as long as it can verify a user against the DynaPass domain. This can be done using the RADIUS protocol or the Microsoft

## *DynaPass – Implementation Guidelines*

standard protocol. You must install Microsoft IAS (included in W2000 server) to enable the RADIUS support on the DynaPass domain controller.

### **Logon Procedures**

The total login procedure will take place in two steps. Step one is a DynaPass controlled logon with the NAS to open the door and step two is a "normal" logon to the "normal" logon domain with the username and password used "in the office". Depending of the type of logon client used and the way Dial Up Networking in the client computer is configured this procedure is transparent to the user. For example, if you use MS Dial Up Networking and mark the checkbox "Logon to Domain" active, the second step will be performed automatically with the credentials used when the user originally logged on to his computer. If these credentials are not valid the user will be prompted to enter user name and password again as a part of the second step in the logon procedure

### **Recommendations**

The most frequent way of using DynaPass together with remote access is to let the user request for a password from his mobile phone. This opens up the possibilities to introduce the time limits for passwords and the automatic disabling of user accounts. Suitable timeframe is normally set to 10 – 15 minutes, which leaves the user this time for logon.

With this setting **ALL** accounts will be disabled when not in use. There will be no accounts open for logon or brute force attacks.

Maximum security in DynaPass can be achieved by a combination of an individual prefix. The user has to combine the prefix with the password received by the mobile phone. The prefix is **never** sent to the GSM phone, it is only known by the user and DynaPass.

User names in the DynaPass domain can be the same as in the main domain. The reason for this is that it will be transparent for the users and they don't have to remember different usernames (most likely they won't even notice that they are using different accounts) Note however that there are no trusts between the DynaPass domain and the main domain.

### **Miscellaneous**

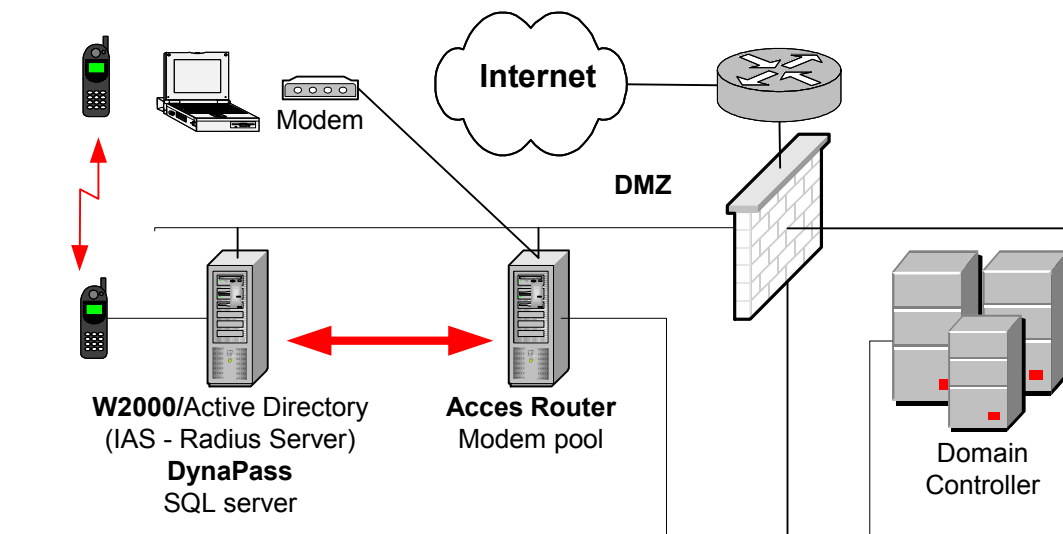
No changes are required in the Domain and the logon procedures used when connected directly to the LAN.

Administration of the Remote Access users is minimal, merely that the user has an account in the DynaPass Server. No particular user rights other than allow dial in access should be set.

DynaPass requires no special software or add-ins in the client computers.

## **DynaPass and Secure Access Using Modems.**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access the network. After successful authentication he can proceed to logon to the “corporate domain” using the credentials supplied at power on of the client computer. If this is not successful, or automatic logon to domain is disabled, the user will be prompted to enter user name and password.



### **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights. DynaPass is installed as a service and is using MS SQL Server as its system database.

Internet Authentication Service (IAS) is installed if the Access Router is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

It's recommended that there are no trusts between the Domain Controller and DynaPass server.

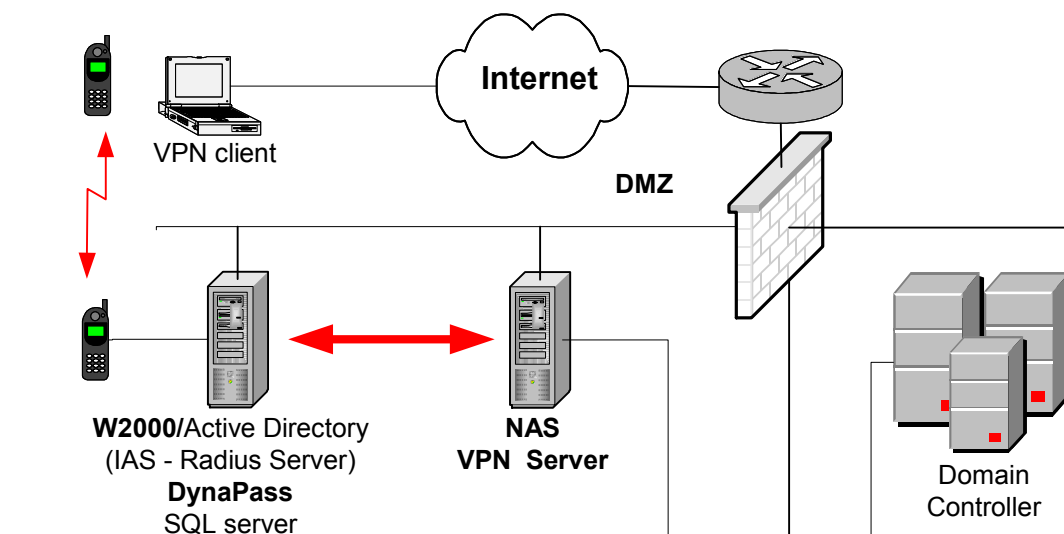
### **Access Router/Modem pool**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the corporate network. This Access Router or Modem Pool is either using Radius or Microsoft standard protocol to A.D. for enquiries.

## *DynaPass – Implementation Guidelines*

### **DynaPass and VPN Tunnel Server**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access the network. After successful authentication he can proceed to logon to the “corporate domain” using the credentials supplied at power on of the client computer. If this is not successful, or automatic logon to domain is disabled, the user will be prompted to enter user name and password.



### **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights. MS SQL Server hosts the DynaPass system database.

Internet Authentication Service (IAS) is installed if the Access Router/VPN Tunnel Server is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

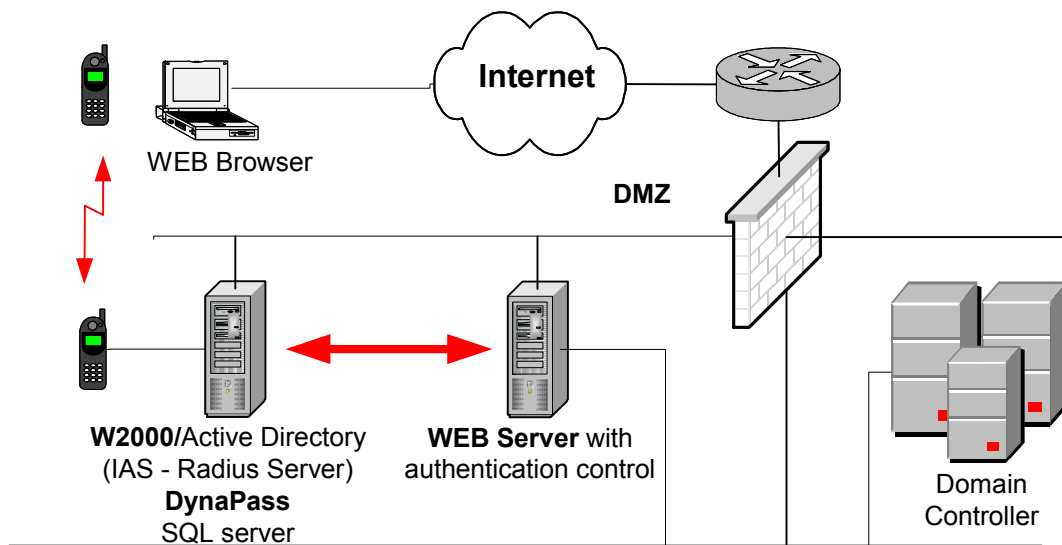
It's recommended that there are no trusts between the Domain Controller and DynaPass server.

### **VPN Tunnel Server**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the tunnel will be established and the user will be granted access to the corporate network. The VPN Tunnel Server is using Radius or Microsoft standard protocol to A.D. for enquiries. Note that the VPN server is published through the firewall with a public IP address.

## **DynaPass and Secure Web Access**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access the WEB server or part of the WEB server. After successful authentication he can access protected pages and directories in the WEB server. Depending on which resources and services that are available to the user he can now logon to those services such as WEB mail etc.



## **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights. MS SQL Server hosts the DynaPass system database.

Internet Authentication Service (IAS) is installed if the WEB server is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

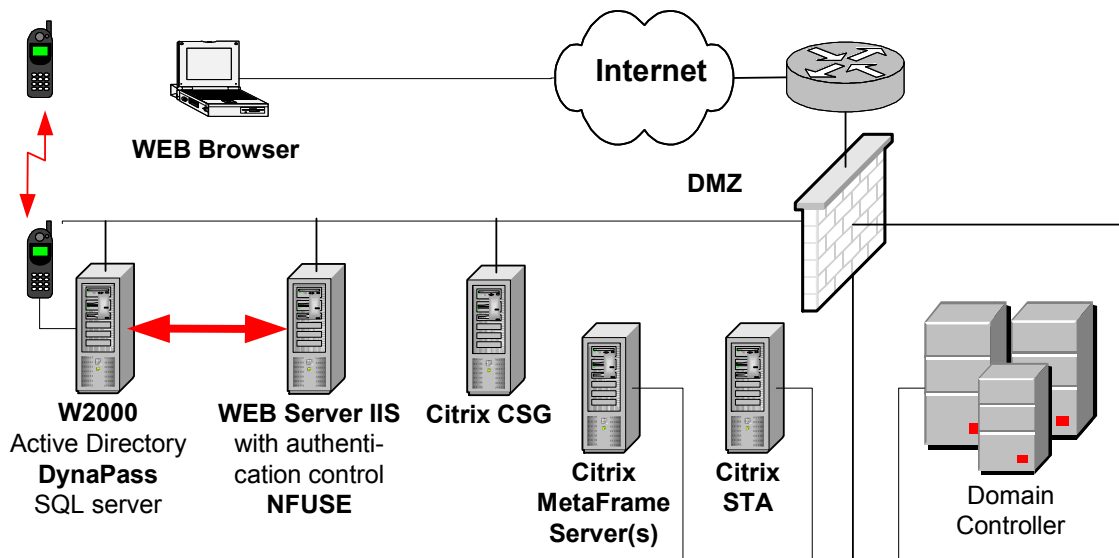
It's recommended that there are no trusts between the Domain Controller and DynaPass server.

## **WEB server**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password then the user will be granted access to the WEB server or part of the WEB server. The WEB server is using Radius or Microsoft standard protocol to A.D. for enquiries. The WEB server is published through the firewall with a public IP address.

## **DynaPass and CITRIX Secure Gateway NFUSE**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access the WEB server with Citrix NFUSE. After authentication he can access protected pages where he can make the NFUSE logon to the Citrix Metaframe Server(s). After a successful logon to NFUSE the Citrix STA will issue a ticket to the user through the Citrix CSG and the session is now handled by the Citrix CSG.



### **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights. MS SQL Server hosts the DynaPass system database.

Internet Authentication Service (IAS) is installed if the WEB server is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

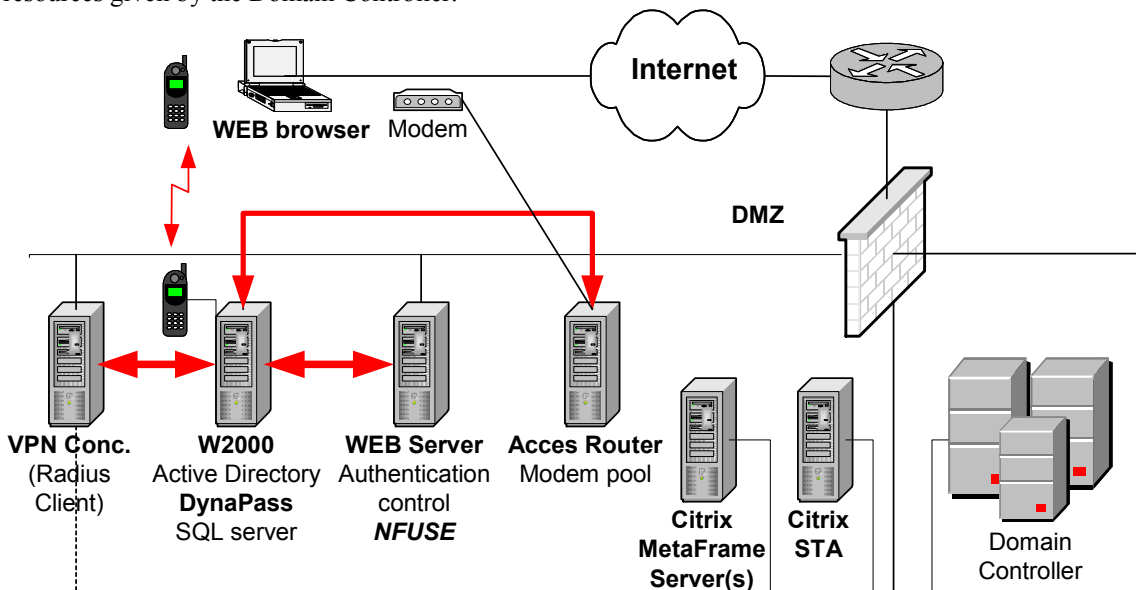
It's recommended that there are no trusts between the Domain Controller and DynaPass server.

### **WEB server/NFUSE**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the WEB server with Citrix NFUSE. The WEB server is using Radius or Microsoft standard protocol to A.D. for enquiries. The WEB server is published through the firewall with a public IP address.

## **DynaPass in a Mixed Environment**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access the different services such as Modem/Access Router, VPN Tunnel and WEB Access (including NFUSE). After successful authentication he can access different resources depending on access medium and resources given by the Domain Controller.



### **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights independently of which service that is used. MS SQL Server hosts the DynaPass system database.

Internet Authentication Service (IAS) is installed if the any service is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

It's recommended that there are no trusts between the Domain Controller and DynaPass server.

## *DynaPass – Implementation Guidelines*

### **Access Router/Modem Pool**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the corporate network. This Access Router or Modem Pool is either using Radius or Microsoft standard protocol to A.D. for enquiries.

### **VPN Tunnel Server**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the tunnel will be established and the user will be granted access to the corporate network. The VPN Tunnel Server is using Radius or Microsoft standard protocol to A.D. for enquiries. Note that the VPN server is published through the firewall with a public IP address.

### **WEB Server**

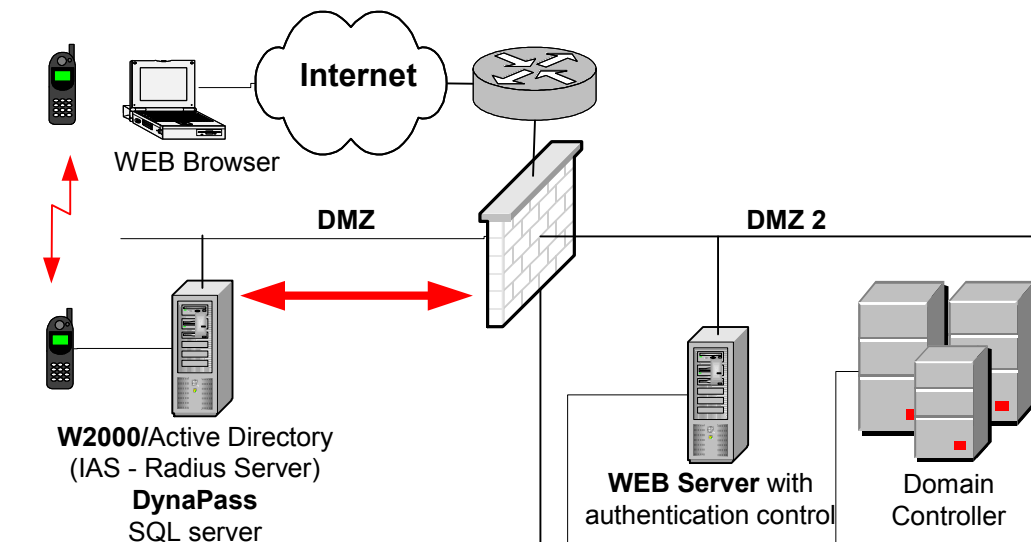
All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the WEB server. The WEB server is using Radius or Microsoft standard protocol to A.D. for enquiries. The WEB server is published through the firewall with a public IP address.

### **WEB Server/NFUSE**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the WEB server with Citrix NFUSE. The WEB server is using Radius or Microsoft standard protocol to A.D. for enquiries. The WEB server is published through the firewall with a public IP address.

## **DynaPass and Firewall authentication**

The user has to be authenticated by DynaPass using the name and password for the DynaPass domain before he can access services on DMZ 2. After successful authentication through the Firewall the user can access protected services such as WEB mail, Terminal servers etc. Depending on which resources and services that are available to the user he can now logon to those services.



### **DynaPass**

The DynaPass server is a MS Windows 2000 Server with Active Directory, containing all users that have been granted Remote Access rights. MS SQL Server hosts the DynaPass system database.

Internet Authentication Service (IAS) is installed if the Firewall is using a Radius Client for authentication. With IAS installed the DynaPass server will act as a Radius Server.

It's recommended that there are no trusts between the Domain Controller and DynaPass server.

### **Firewall**

All authentications are passed through to the DynaPass server, which checks the username and password. If the user has a valid and enabled account and is entering a valid password the user will be granted access to the DMZ 2. The requirement on the Firewall is that it supports external directory for authentication e.g. Radius or native Microsoft API.