



Securing access to Citrix[®] applications using Citrix Secure Gateway and SafeWord[™] PremierAccess[™]

App Note

December 2001

DISCLAIMER:

This White Paper contains Secure Computing Corporation product performance information that is meant as a guide to customers. Performance is greatly influenced by traffic profiles and how the hardware and software are set up and configured. Therefore, the performance data within implies no guarantee by Secure Computing that the customer will realize the same performance levels.

© 12/07/01, v.SCC120600. Secure Computing Corporation. All Rights Reserved. SafeWord, PremierAccess, Sidewinder, Type Enforcement, SecureOS, SoftToken, Strikeback, SmartFilter, and safe, secure extranets for e-business are either registered trademarks or trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names and images mentioned and / or used herein belong to their respective owners.

Table of Contents

Objective	3
Introduction	3
Before you begin	3
Setting up Citrix Secure Gateway and SafeWord PremierAccess ..	4
Integrating Citrix Secure Gateway with SafeWord PremierAccess	5
Modifying NFuse to support single sign-on	10
Modifying NFuse to support reduced sign-on	12
Firewall considerations	13
Summary	15

Objective

This paper discusses the implementation of Citrix® Secure Gateway in conjunction with SafeWord™ PremierAccess™ and its Universal Web Agent and Web Login Server to provide secure, authorized access to published Citrix applications.

Introduction

SafeWord PremierAccess is policy-based access control software that allows system administrators to personalize user access privileges and protect Web applications, VPNs, remote access points, and other networked resources. PremierAccess offers directory-enabled authentication and authorization to positively identify users before they are allowed to access protected resources. Within the PremierAccess architecture, users are assigned one or more roles that are used to specify what resources they can access and under what conditions. These user roles, when combined with access control lists, can be used to easily define granular, comprehensive, and flexible security policy for an entire enterprise.

Citrix Secure Gateway is designed to secure all Citrix Independent Computing Architecture (ICA®) traffic traveling across unsecured networks between MetaFrame® servers and Secure Socket Layer (SSL)-enabled ICA client workstations. Since the ICA traffic is secured with SSL encryption, this makes firewall traversal easier, provides heightened security, simplifies deployment, and enables tight integration with Citrix® Nfuse™ application portal software.

PremierAccess can protect published Citrix applications at both session initiation and at the initial user login with various forms of strong user authentication. The first method, protecting the session initiation, can be accomplished with the SafeWord Agent for Citrix. Please refer to <http://www.securecomputing.com/index.cfm?sKey=690> for more details on the SafeWord Agent for Citrix.

This document will focus on the latter method, protecting the user login and providing simple, secure access to published Citrix applications. Citrix MetaFrame, NFuse, and Secure Gateway, when combined with the advanced Web access control capabilities of PremierAccess and its Universal Web Agent and Web Login Server, allow organizations to offer sophisticated yet secure access to personalized Web-based application portals for their user population. Furthermore, by enforcing user authentication and access control at the application portal level (NFuse), PremierAccess can allow organizations to authenticate Citrix MetaFrame users with the industry's widest range of authentication options including memorized passwords, one-time (dynamic) passwords, challenge-response tokens, digital certificates, smart cards, USB tokens, and biometric devices. Finally, with a minimal amount of configuration, PremierAccess can also support single or reduced sign-on to Citrix applications, as well as the ability to provide secure group logins to shared Citrix accounts.

Before you begin

This paper has been written with the assumption that the reader is familiar with both the software and concepts behind PremierAccess; the Universal Web Agent and Web Login Server; and Citrix software including MetaFrame, NFuse, and Citrix Secure Gateway. The

documentation for both PremierAccess and the various components that comprise Citrix Secure Gateway is strongly recommended as prerequisite reading.

Setting up Citrix Secure Gateway and SafeWord PremierAccess

Citrix Secure Gateway requires four server components: the Citrix server farm (MetaFrame XP™), Citrix Secure Gateway, the Secure Ticket Authority, and Citrix NFuse. Although these components can be consolidated onto only a few servers, it is recommended for most environments to distribute the services across several servers for load balancing and redundancy. The documentation provided with Citrix Secure Gateway discusses how to distribute these services in an effective manner and Citrix administrators are advised to refer to those documents. The minimum number of servers recommended for securing Citrix Secure Gateway with PremierAccess is five. The components running on their respective servers are:

1. Citrix MetaFrame XP server running the Citrix XML Service
2. PremierAccess
3. The Secure Ticket Authority
4. Citrix Secure Gateway
5. Citrix NFuse protected by Universal Web Agent and Web Login Server¹

Before an administrator begins to install the Citrix components, the following data should be readily available.

Item	Notes	Example
MetaFrame XP server running the Citrix XML Service	Should know both the fully qualifiable domain name and IP address of the server	mfxp.citrixland.com 192.168.27.27
Listener port for the Citrix XML Service	By default, this is shared with the default port for IIS, but it can be changed to a different value	TCP/88
Citrix Secure Gateway server	Must know both the fully-qualifiable domain name and IP address of the server	csg.citrixland.com 192.168.27.28
Listener port number for SSL connections to the Citrix Secure Gateway	By default, this should be port 443	TCP/443
Secure Ticket Authority (STA)	Must know both the fully qualifiable domain name and IP address of the server	sta.citrixland.com 192.168.27.29
NFuse Web server and UWA/WLS	Must know both the fully qualifiable domain name and IP address of the server	nfuse.citrixland.com 192.168.27.30
Listener port for the NFuse Web server	The port that the Universal Web Agent uses to talk to the NFuse Web server	TCP/5081

¹ Although NFuse runs as a servlet under a variety of Web servers, this document assumes that NFuse will be running under Microsoft IIS.

Listener ports (HTTP/HTTPS) for the UWA	The ports that the Universal Web Agent listens for requests	TCP/80 & TCP/443
Listener ports (HTTP/HTTPS) for the WLS	The ports that the Web Login Server uses to authenticate users	TCP/5080 & TCP/5443
Session management port for the UWA	The port that the Universal Web Agent uses when it receives session management data from the PremierAccess AAA server	TCP/9998
PremierAccess AAA server	Should know both the fully qualifiable domain name and IP address of the server	swpa.citrixland.com 192.168.27.31
Listener port for EASSP 201 on the AAA server	By default, this should be port 5031	TCP/5031
Name of the Web ACL protecting the UWA	This value is used to tell the UWA to return personalization attributes to the Web application (NFuse)	NFuse_Web_ACL

Furthermore, administrators are advised to install all the Citrix components first, verify that Citrix Secure Gateway is operating properly, and then proceed with the installation of PremierAccess, the Universal Web Agent, and the Web Login Server.

Integrating Citrix Secure Gateway with SafeWord PremierAccess

Once Citrix Secure Gateway has been successfully installed, only a few simple modifications need to be made to the Citrix components before integrating Secure Gateway with PremierAccess.

NFuse is used as the user authentication point for Citrix Secure Gateway. The login pages on the NFuse server are used to proxy a user's credentials (Windows username, passwords and domain) to the MetaFrame server farm for authentication as well as to set session cookies in the user's browser once the user has authenticated successfully to the domain.² In order to secure Citrix Secure Gateway with PremierAccess, the NFuse service is augmented with the PremierAccess Universal Web Agent and Web Login Server. The Universal Web Agent and Web Login Server provide an additional level of user authentication to NFuse or, with a few simple customizations, can be configured as the sole authentication mechanism to Citrix applications.

The IIS server hosting NFuse requires a few configuration changes in order to interoperate with the Universal Web Agent and Web Login Server and ensure the security of the Web server content. These changes are:

² Although Citrix MetaFrame XP supports user authentication to standalone Windows servers, this document refers to all types of Windows user credentials as Windows domain credentials.

1. Disabling SSL on IIS
2. Changing the default port number of the Web server from port 80 to port 5081
3. Modifying the security settings for IIS so that only localhost (127.0.0.1) and the IP address of the local machine can connect to the Web server
4. Verifying that IIS is running on a server with a fully qualifiable domain name (the domain name should be resolvable in DNS)

Once IIS has been properly configured, the Universal Web Agent and Web Login Server can be installed with their respective default settings.

Each instance of the Universal Web Agent is associated with a single Web access control list (Web ACL). Web ACLs are created by system administrators on the PremierAccess Admin Console and are used to specify which individual URLs on a particular Web server will be protected. The level of protection for URLs may vary within the Web ACL. Stringent access controls, such as time and date restrictions or authenticator strength requirements³ may be placed on some URLs, while more permissive access controls may be placed on other URLs. By default, all instances of the Universal Web Agent point to the *DEFAULT_WEB_ACL* that protects all URLs on the Web server.

Although the Universal Web Agent will attempt to protect NFuse with the *DEFAULT_WEB_ACL*, it is recommended to create a separate Web ACL in the PremierAccess Admin Console so that any configuration changes will not affect the *DEFAULT_WEB_ACL*. If a new Web ACL is created for the Universal Web Agent, it should be configured to pass personalization attributes back to the Web application (NFuse) if administrators are interested in implementing reduced or single sign-on to NFuse for their users. As displayed in Figure 1, this can be accomplished from the Personalization tab when configuring the Web ACL.

³ Authenticator strength is a unique feature in PremierAccess that allows enterprises to define the strength of various types of authenticators. Authenticators can range from basic memorized passwords to dynamic passwords to digital certificates. Depending on the security requirements of an individual enterprise, certain types of authenticators can be designated stronger than other types using the authenticator strength feature.

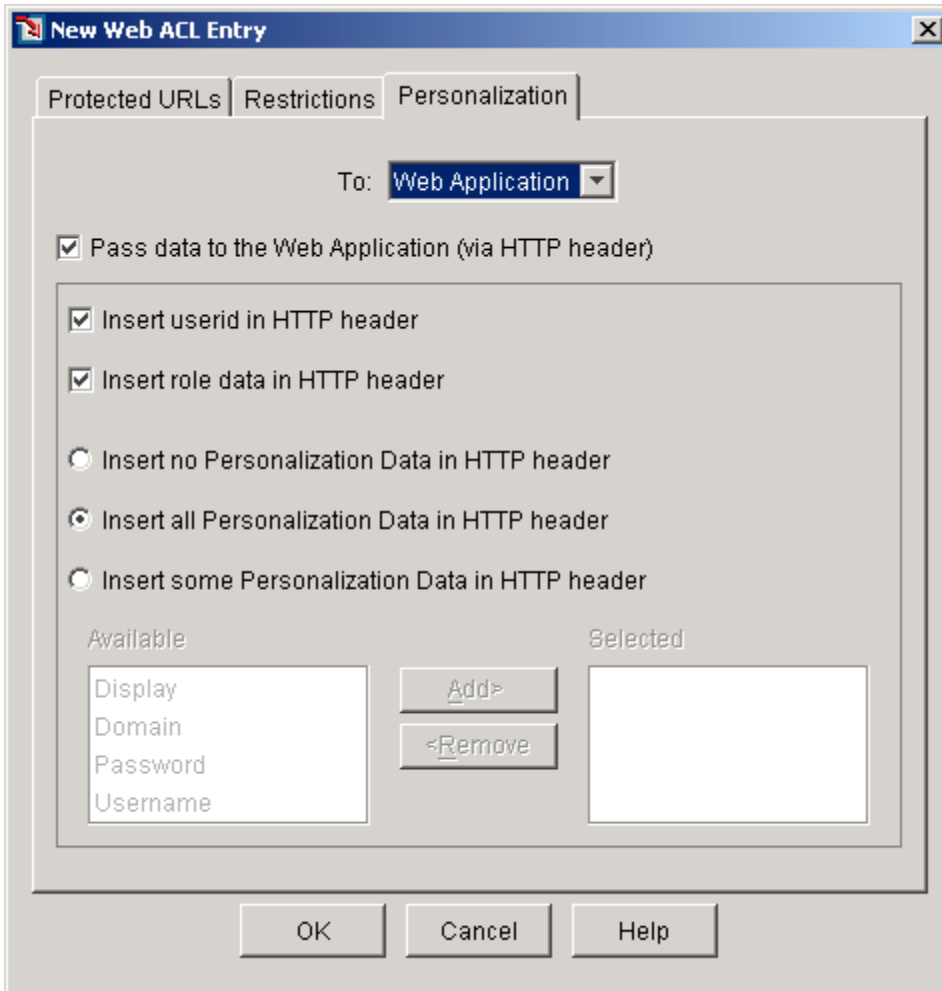


Figure 1: Configuring the Web ACL to return all personalization attributes.

Citrix NFuse communicates directly to the MetaFrame server farm using the Citrix XML Service. By default, when installing MetaFrame on a server running IIS, the Citrix installer will attempt to configure the Citrix XML Service to listen on a shared port with IIS. Although this configuration does work, it is recommended to install this service on a dedicated port such as TCP/88 and securing the XML traffic with SSL. If MetaFrame and NFuse are installed on separate servers, there are no issues with IIS and the Citrix XML Service sharing a port. *However, it is absolutely critical to change the port number of the XML Service if both MetaFrame and NFuse are running from a single server and the Universal Web Agent protects NFuse.* In the example provided in this document, MetaFrame and NFuse are running on separate servers, but the Citrix XML Service has been configured to run on port 88. Please refer to the Citrix MetaFrame documentation for more details on changing the port number for the XML Service and securing the data with SSL.

Please note that if the port number for the Citrix XML Service is changed, then the configuration file for the NFuse Extensions needs to be modified in order to reflect this change. This file is called *csf_conf.inc* located in the CSG directory under *%systemroot%\inetpub\wwwroot* on the NFuse server. If the Citrix XML Service is running

© 12/07/01, v.SCC120600. Secure Computing Corporation. All Rights Reserved. SafeWord, PremierAccess, Sidewinder, Type Enforcement, SecureOS, SoftToken, Strikeback, SmartFilter, and safe, secure extranets for e-business are either registered trademarks or trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names and images mentioned and / or used herein belong to their respective owners.

on port 88, then the numCitrixServerPort line should be changed to *numCitrixServerPort=88*

No special steps are required when installing the Citrix Secure Gateway and Secure Ticket Authority components. As discussed in the Citrix documentation, these components must be installed on servers with fully qualifiable domain names and have the proper server and root certificates installed. Please refer to the Citrix Secure Gateway documentation for more details.

After the Universal Web Agent and Web Login Server have been installed, PremierAccess will be protecting the NFuse login page. At this point, it is important to note that for many enterprises this level of protection is completely acceptable. The user experience will be:

1. User attempts to access the NFuse Web server
2. Access attempt intercept by the Universal Web Agent
3. User's browser redirected to Web Login Server
4. User authenticates successfully against PremierAccess at the Web Login Server
5. User redirected to protected resource (NFuse login page)
6. User provides Windows domain credentials at the NFuse login page
7. User passes Windows authentication and is presented with a list of published applications

In the scenario described above, the user must provide credentials for two authentications; the first set consisting of the credentials for PremierAccess and the second set consisting of a Windows domain username and password.

The remainder of this document describes various methods to either streamline this dual authentication process or consolidate the authentication processes to the point where the user essentially needs to provide a single credential (*single sign-on*) to gain access to his published Citrix applications.

Modeling personalization attributes – user vs. role-based personalization fields

Once PremierAccess has been installed, administrators have the ability to create specific personalization attributes for either specific users or user roles. These personalization attributes can include Citrix display mode preferences as well as a Windows username, password, and domain. These personalization attributes are displayed in Figure 2.

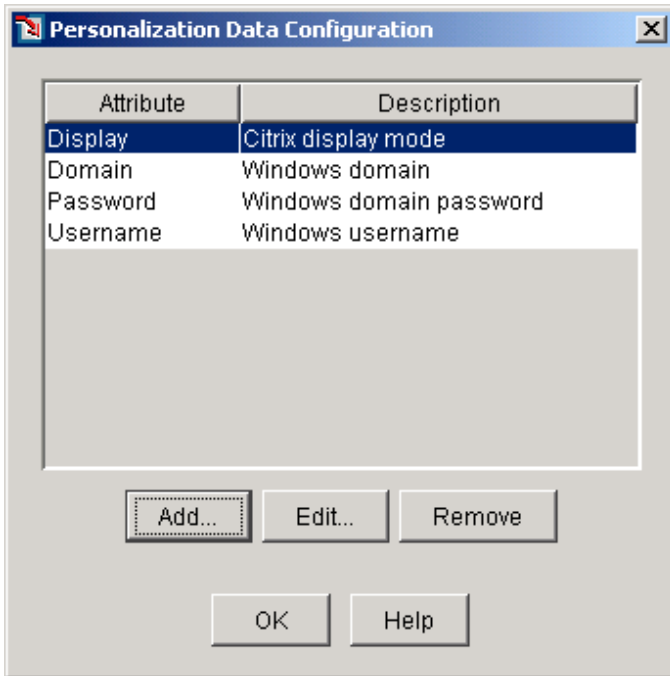


Figure 2: Configuring personalization data in the PremierAccess admin console.

The Domain, Password, and Username personalization fields can be defined to allow any value or specific set of values. The Display personalization field, as shown in Figure 3, refers to the Citrix display mode and should only allow contain the following values: 640x480, 800x600, 1024x768, 1280x1024, seamless, and fullscreen. The Display personalization field, when passed back to NFuse, defines the video mode that the ICA client will use to display published applications.

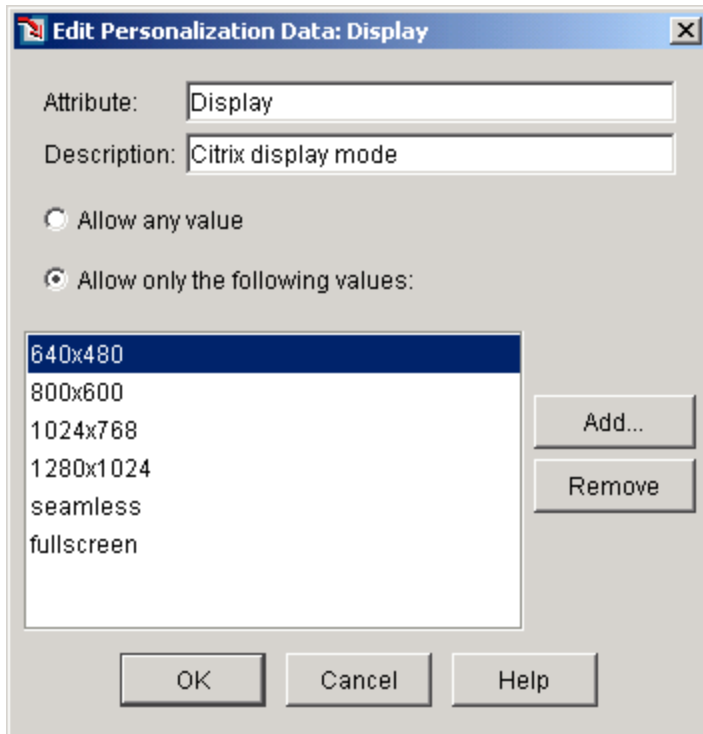


Figure 3: Setting the appropriate values for the Citrix display mode personalization attribute.

After personalization fields have been defined, the PremierAccess administrator has the option of assigning specific attributes to either individual users or roles. Assigning the personalization attributes to user records is desirable in environments where individual users have access to a different set of published applications. In such a case, the PremierAccess user's personalization attributes Username, Password, and Domain should match exactly to the same user's Windows domain credentials. However, in an environment where most users will have access to the same applications or certain groups of users have access to a similar set of applications, then it makes more sense to set the personalization attributes at the role level. In this case, the PremierAccess role's personalization attributes Username, Password, and Domain should match exactly the credentials for a shared user account in the Windows domain.

It is also important to mention that users can be assigned the same personalization attributes in both their user record or in a role assigned to them. *In a case where a user is assigned a personalization attribute that corresponds to a value assigned to one of his roles, the personalization field stored in the user record will take priority.*

Modifying NFuse to support single sign-on

After the Secure Gateway NFuse extensions are installed, it is simple to modify the pages for single sign-on functionality. In order to enable single sign-on, the following steps need to be taken on the NFuse server:

1. In the %systemroot%\inetpub\wwwroot\CSG folder, rename *default.htm* to *default.old* (this page contains the Web forms used to collect Windows domain credentials for NFuse users)
2. Duplicate *applist.asp* and rename the new copy of the file *default.asp*
3. Replace the following lines of *default.asp*:

```
user = Request.Cookies("NFuseData")("NFuse_User")
domain = Request.Cookies("NFuseData")("NFuse_Domain")
password = Request.Cookies("NFuseData")("NFuse_Password")
displayMode = Request.Cookies("NFuseMode")("NFuse_DisplayMode")
```

with

```
If ((Request.ServerVariables("HTTP_USERNAME") = "") AND
(Request.ServerVariables("HTTP_DOMAIN") = "") AND
(Request.ServerVariables("HTTP_PASSWORD") = "")) Then
Response.Redirect("blank.htm")
```

```
Response.Cookies("NFuseData")("NFuse_User") =
Request.ServerVariables("HTTP_USERNAME")
Response.Cookies("NFuseData")("NFuse_Domain") =
Request.ServerVariables("HTTP_DOMAIN")
Response.Cookies("NFuseData")("NFuse_Password") =
Request.ServerVariables("HTTP_PASSWORD")
Response.Cookies("NFuseMode")("NFuse_DisplayMode") =
Request.ServerVariables("HTTP_DISPLAY")
```

```
user = Request.Cookies("NFuseData")("NFuse_User")
domain = Request.Cookies("NFuseData")("NFuse_Domain")
password = Request.Cookies("NFuseData")("NFuse_Password")
displayMode = Request.Cookies("NFuseMode")("NFuse_DisplayMode")
```

Once these changes have been made, single sign-on to Citrix NFuse has been enabled. When a user passes PremierAccess authentication, the user's cached Windows domain credentials (stored as personalization attributes) are automatically passed to the NfuseData and NfuseMode cookies. NFuse, once reading the contents of the user's cookies, is then able to generate the application list for the user. The user experience will be:

1. User attempts to access the NFuse Web server
2. Access attempt intercept by the Universal Web Agent
3. User's browser redirected to Web Login Server
4. User authenticates successfully against PremierAccess at the Web Login Server
5. User redirected to protected resource (NFuse)
6. Universal Web Agent automatically passes cached Windows domain credentials (stored as personalization attributes) to NFuse
7. Windows domain credentials are authenticated by NFuse with no user interaction and the user is presented with a list of published applications

In the event a user passes PremierAccess authentication and lacks the personalization fields containing cached Windows domain credentials, the user will automatically be redirected to

a blank HTML page. This blank page can be easily replaced with an error page by removing the reference to *blank.htm* and replacing it with another page.

Modifying NFuse to support reduced sign-on

For some enterprises, reduced sign-on to Citrix NFuse balances user convenience with an organization's need for security. In this method, some simple modifications need to be made to the default NFuse login page, *default.htm*.

1. In the `%systemroot%\inetpub\wwwroot\CSG` folder, rename *default.htm* to *default.asp*
2. Replace the following line:

```
<input type="text" name="user" class="loginEntries">
```

with

```
<font face="Verdana, Arial, Helvetica, sans-serif" size="2"
color="#FF0000"><b><%=
Request.ServerVariables("HTTP_USERNAME")%></b></font><input
type="hidden" value="<%=
Request.ServerVariables("HTTP_USERNAME")%>" name="user"
class="loginEntries">
```

3. Replace the following line:

```
<input type="text" name="domain" class="loginEntries">
```

with

```
<font face="Verdana, Arial, Helvetica, sans-serif" size="2"
color="#FF0000"><b><%=
Request.ServerVariables("HTTP_DOMAIN")%></b></font><input
type="hidden" value="<%=
Request.ServerVariables("HTTP_DOMAIN")%>" name="domain"
class="loginEntries">
```

4. Replace all instances of *default.htm* with *default.asp* in *frameset.asp*

Once these modifications have been made, reduced sign-on to NFuse will be enabled. The user experience will be:

1. User attempts to access the NFuse Web server
2. Access attempt intercept by the Universal Web Agent
3. User's browser redirected to Web Login Server
4. User authenticates successfully against PremierAccess at the Web Login Server
5. User redirected to protected resource (NFuse)
6. Universal Web Agent automatically passes cached Windows domain username and domain name (stored as personalization attributes) to NFuse which automatically populates the login form

© 12/07/01, v.SCC120600. Secure Computing Corporation. All Rights Reserved. SafeWord, PremierAccess, Sidewinder, Type Enforcement, SecureOS, SoftToken, Strikeback, SmartFilter, and safe, secure extranets for e-business are either registered trademarks or trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names and images mentioned and / or used herein belong to their respective owners.

7. User types his Windows domain password and clicks “Log In” where he presented with his list of published applications.

When a user passes PremierAccess authentication, the cached Windows domain credentials are automatically passed as personalization elements that are used to populate hidden form files and are also displayed as non-modifiable text. This prevents users from circumventing the PremierAccess authentication and providing a different set of Windows domain credentials to NFuse. In the example above, the personalization elements representing the Windows username and domain are passed to NFuse. The user must still enter his password in order to see his list of published applications.

Firewall considerations

As discussed earlier, using Citrix Secure Gateway in conjunction with PremierAccess requires a minimum of five servers. Due to the specific and secure nature of certain servers, it is important to clarify the position of each server in relation to any firewalls in use by the enterprise.

Citrix recommends a zonal architecture when implementing firewalls around a Secure Gateway deployment. In this architecture, there are three zones: the untrusted network, the demilitarized zone (DMZ), and the secure network. Figure 4 displays each of these three zones and the components that reside in each zone.

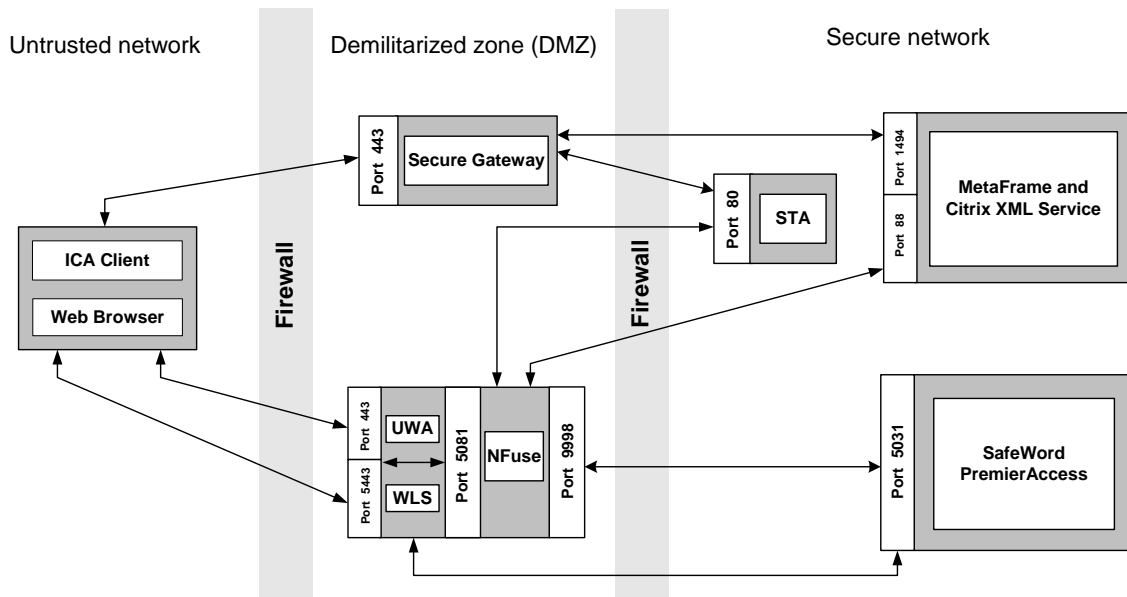


Figure 4: Placement of PremierAccess and Citrix Secure Gateway servers in relation to firewalls.

The untrusted network, for many organizations, may represent the Internet or some other insecure network. It is from this untrusted network that client devices will authenticate and gain access to published Citrix applications. The DMZ will consist of the servers required for users to pass their authentication credentials and establish an application session with the Secure Gateway server. The servers in the DMZ include the Secure Gateway server, the Universal Web Agent, the Web Login Server, and the NFuse server. The final zone is the

© 12/07/01, v.SCC120600. Secure Computing Corporation. All Rights Reserved. SafeWord, PremierAccess, Sidewinder, Type Enforcement, SecureOS, SoftToken, Strikeback, SmartFilter, and safe, secure extranets for e-business are either registered trademarks or trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names and images mentioned and / or used herein belong to their respective owners.

trusted, secure network. This is the most sensitive portion of the network since it houses the Citrix server farm, the PremierAccess server components, and the Secure Ticket Authority.

The table in Figure 5 portrays the port numbers that need to be open on the firewall in order to allow the appropriate traffic to travel across the various networks.

Source zone	Destination zone	Source server	Destination server	Port number	Description
Internet	DMZ	Web browser	UWA	TCP/443	User access to NFuse server (HTTP or HTTPS)
Internet	DMZ	Web browser	WLS	TCP/5443	User authentication point for PremierAccess (HTTPS)
Internet	DMZ	ICA client	Secure Gateway	TCP/443	SSL-secured ICA traffic
DMZ	Trusted network	UWA	PremierAccess AAA server	TCP/5031	Web access policy (EASSP 201)
DMZ	Trusted network	WLS	PremierAccess AAA server	TCP/5031	User authentication credentials (EASSP 201)
DMZ	Trusted network	NFuse	STA	TCP/80	Ticketing data
DMZ	Trusted network	NFuse	MetaFrame server	TCP/88	Citrix XML traffic
DMZ	Trusted network	Secure Gateway	MetaFrame server	TCP/1494	ICA traffic
DMZ	Trusted network	Secure Gateway	STA	TCP/80	Ticketing data
Trusted network	DMZ	PremierAccess AAA server	UWA	TCP/9998	User session management data

Figure 5: List of ports that need to be open on the firewalls.

Summary

Using PremierAccess with Citrix Secure Gateway provides an organization with four principal advantages.

- PremierAccess gives organizations the flexibility to use the widest range of authentication options to ensure the protection of their Citrix infrastructure.
- PremierAccess adds personalized, single or reduced sign-on to published Citrix applications ensuring a positive and convenient user experience.
- PremierAccess adds role-based access control to Citrix applications. This allows administrators to model extremely granular and easy-to-manage access policy.
- PremierAccess can provide strong authentication for wide range of products, from VPNs to Web portals to remote access solutions, allowing organizations to use one product to provide access control to meet all their needs.