paloalto NETWORKS
the network security company™

CITRIX®

# Deployment Guide for Citrix XenDesktop

*Securing and Accelerating Citrix XenDesktop with Palo Alto Networks Next-Generation Firewall and Citrix NetScaler Joint Solution*

## Table of Contents

# 1. Overview

Business productivity hinges on providing users of IT resources secure access to the right applications and the right content – on demand. Enterprise IT strategies are rapidly evolving to support a world in which any user can safely access any application or data, using any device, from any location.

One of the biggest impediments in achieving this degree of flexibility is the enterprise network. Legacy networks were built to provide highly reliable connectivity between users, hosts, and networks, but with no awareness or context of application-layer traffic. This inherently limits the ability of the network to deliver to users the secure and transparent access to apps, data and virtual desktops they need to be productive, and to protect the organization from attack.

While virtualization addresses one attribute of this problem by providing highly flexible solutions that allow customer with the tools to dynamically address the needs of a growing and changing business, it also introduces flexibility requirements on today's security technologies to efficiently secure business processes. Security solutions need to be at least as flexible and dynamic as the environment they secure in order to be effective and not become a hindrance to the business.

What is required is a new approach – a cloud network that safely enables applications with the best-in-class performance and availability.

Palo Alto Networks and Citrix have come together to deliver best-in-class functionality upon which enterprises can build next-generation cloud networks. In addition to sharing a common vision of which networks must evolve, each company is delivering best-in-class solutions that already meet these requirements.

## 1.1 Best-In-Class Solution for Citrix XenDesktop

Citrix XenDesktop is the leading solution for virtualized desktops and applications providing the necessary tools for achieving a truly flexible workplace where work can truly happen from anywhere. Citrix NetScaler is the preferred choice of providing secure remote access to the XenDesktop environment. The solution leverages the NetScaler's remote access features, multi-site datacenter support, network consolidation, and load balancing feature set. Palo Alto Networks next-generation firewalls ensure that virtual desktop users comply to security policies, can safely access applications allowed by policies and are protected from modern threats.

The combination of Citrix NetScaler and Palo Alto Networks next-generation firewall delivers on a best-in-class solution that effectively protects the underlying datacenter and keeps end-users highly productive from anywhere they happen to be using the virtualized desktop.

This document explains how a Citrix XenDesktop environment is configured to provide the best and most secure connectivity to remote users using NetScaler and Palo Alto Networks next-generation firewall.

## 1.2 Prerequisites for Implementation

The steps in this guide assume that a base XenDesktop infrastructure has been created and a NetScaler environment has been configured with basic setup, licensing and an Access Gateway configuration. For guidance on setting up this infrastructure, please refer to the XenServer Pooled Desktops (Local and Remote) Implementation Guide in the XenDesktop Design Handbook.

When setting up the NetScaler and Web Interface components for high availability, a number of virtual IP addresses and domain names are required to complete the configuration. The following components are required to complete the steps required in this guide:

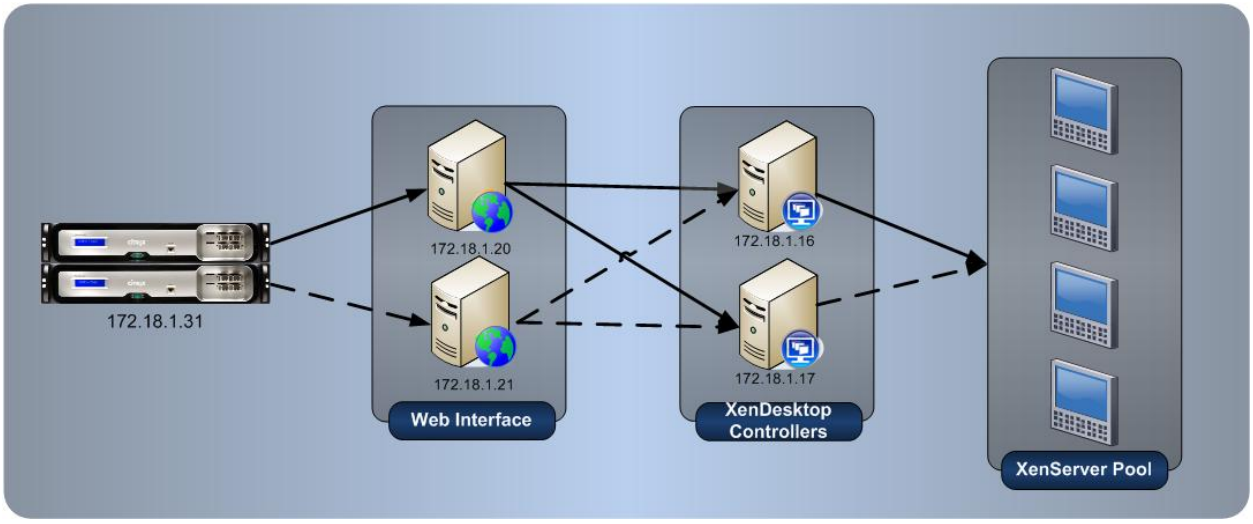
- NetScaler IP (NSIP)
- NetScaler Management IP (MIP)
- Web Interface Virtual IP (VIP) for each site configured with load balancing
- XML Broker VIP for each site configured with load balancing
- Global Server Load Balancing (GSLB) Site IP for each GSLB site
- GSLB fully qualified domain name (FQDN) for external access
- NetScaler ADNS IP address
- Access Gateway FQDN for each site with an Access Gateway configured
- Access Gateway VIP for each site with an Access Gateway configured

Within this document, sample values have been provided for virtual and physical IP addresses and domain names. Specific IP address ranges and FQDN entries will vary depending upon the configuration of the target environment. Naming conventions and IP address ranges should be discussed with appropriate IT organizations and substituted for the sample values in individual implementations.

Palo Alto Networks Next-Generation Firewalls PAN-OS 4.1, a security-specific operating system that allows organizations to safely enable applications using App-ID™, User-ID™, Content-ID™, GlobalProtect™ and WildFire™ was used.

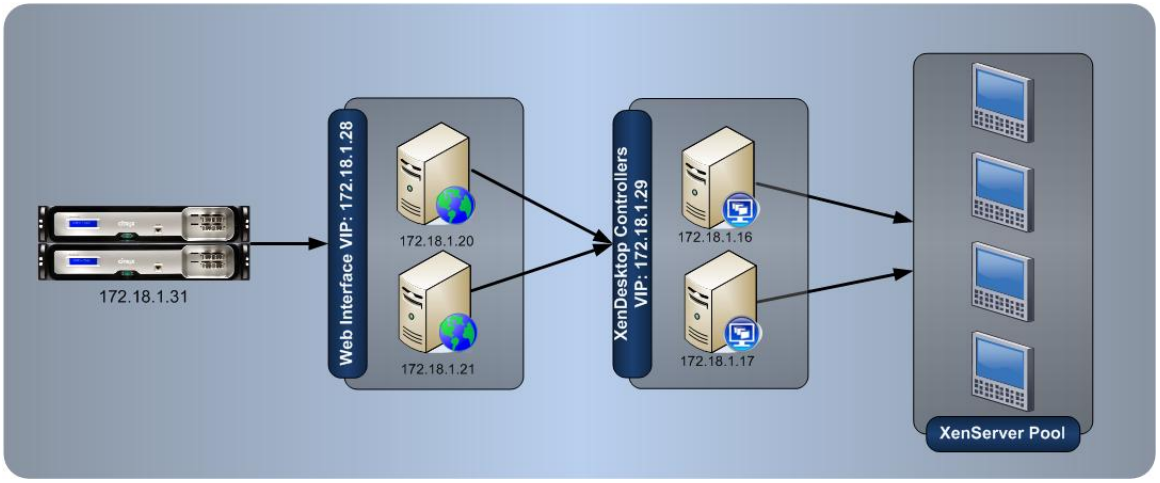
## 2. Local Availability

In many enterprise-level XenDesktop implementations, the architecture typically incorporates redundancy, as shown in the following diagram:




Although the core XenDesktop infrastructure contains redundancy, there are portions where components are only used in the event of a failure of the primary (dotted lines). For example, redundant Web Interface servers are recommended, but there must be a way for connections to be routed to the secondary in the event of a failure of the primary.

The Local Availability section of this document focuses on how to enable the high-availability features of XenDesktop as well as utilize NetScaler to provide greater levels of availability through the use of smart monitors and intelligent load balancing. Once configured, manually managed redundant configurations to and from the Web Interface can be removed as NetScaler directs requests appropriately, as shown in the following diagram:



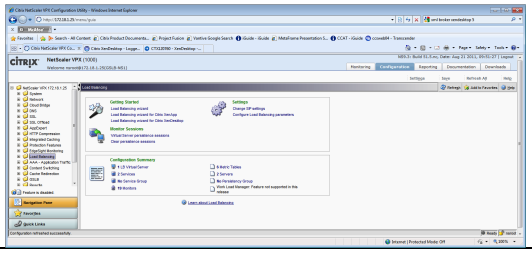
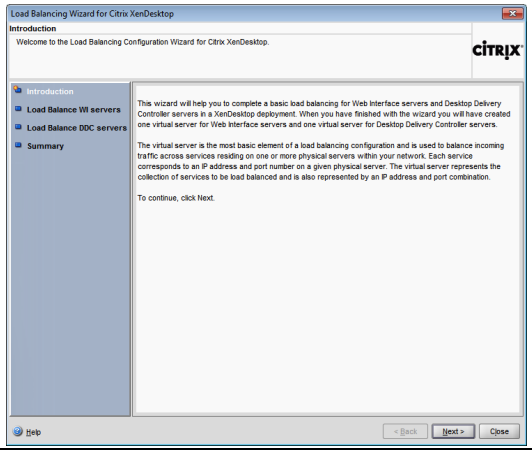

The configuration steps that follow focus on Desktop Delivery.

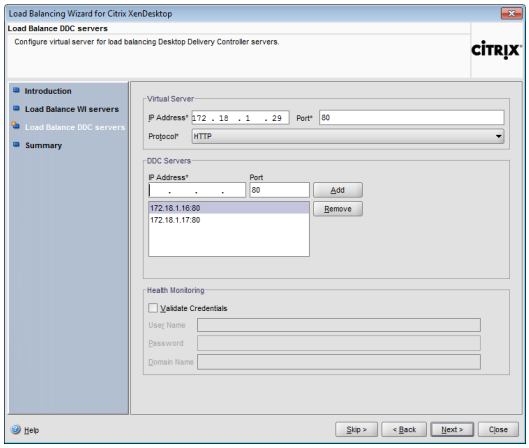
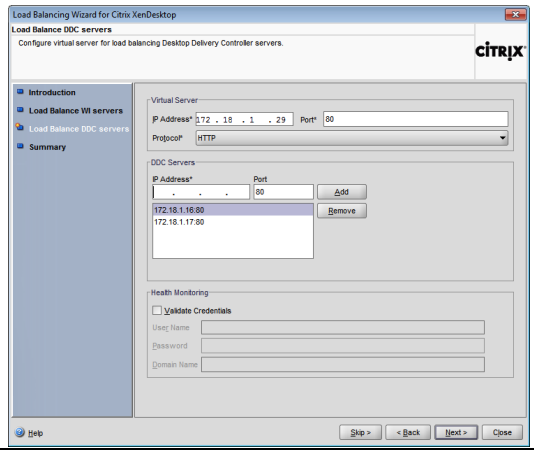
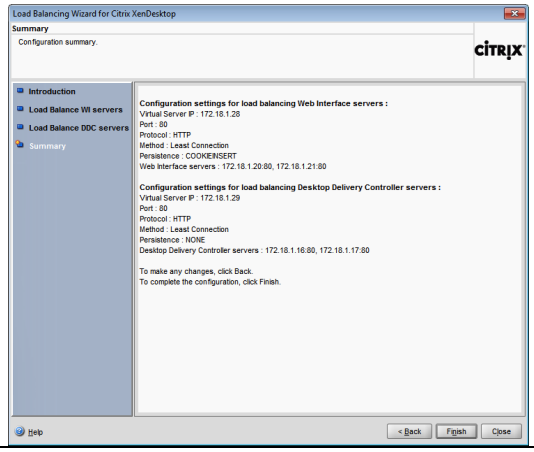
## 2.1 Desktop Delivery

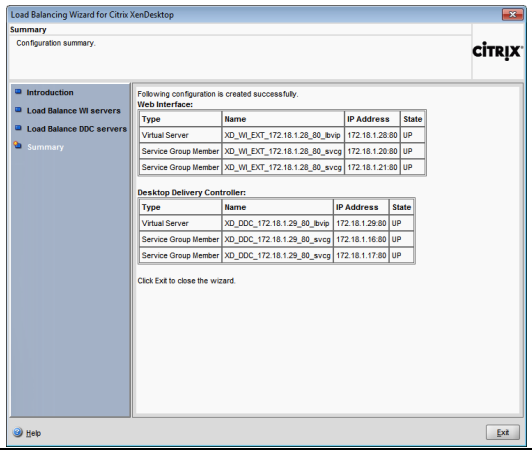
Utilizing redundant Web Interface servers requires users to remember multiple addresses or dictates the need for a load balancing solution. Intelligent load balancing with NetScaler prevents users from being directed to servers with inactive services. Before NetScaler directs a user request to a Web Interface server, NetScaler uses the built-in monitors to validate the services are functioning properly. The configuration is as follows:

### *2.1.1 Load Balancing*

NetScaler is used to improve detection of potential problems with the initial access components of XenDesktop. By utilizing NetScaler's XenDesktop load balancing wizards, the XenDesktop Web Interface and desktop controllers are monitored. The results of the monitors are subsequently used to make load balancing decisions for new user requests. The configuration of the NetScaler is as follows:

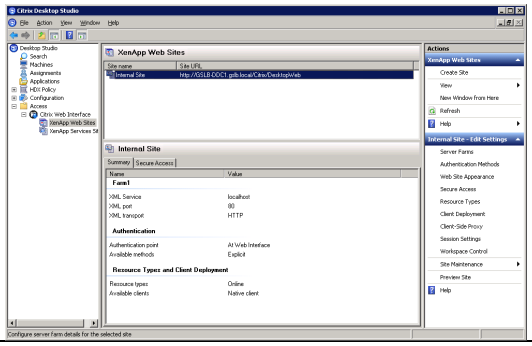
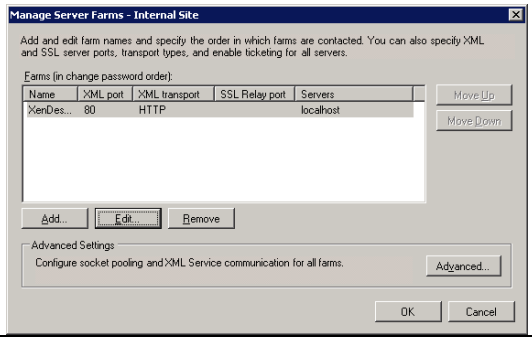
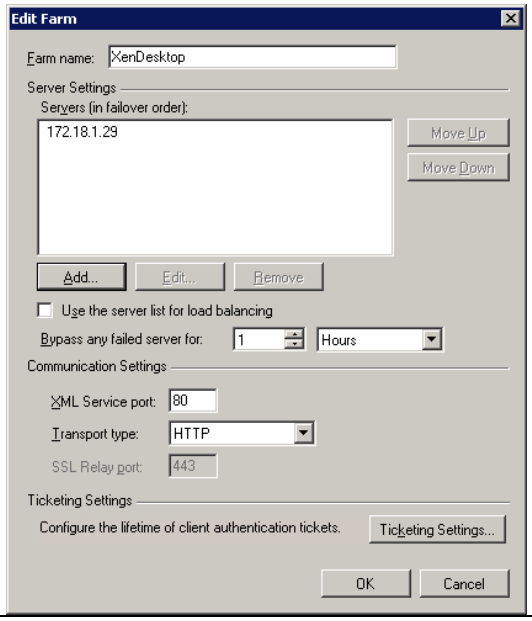
| XenDesktop Load Balancing | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | Within the NetScaler console<br>• Select **Load Balancing – Load Balancing wizard for Citrix XenDesktop** |
| 2 |  | At the Introduction screen, click **Next** |

| XenDesktop Load Balancing | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 3 |  | In the **Load Balance WI servers** section<br>• Enter in the virtual IP address: **172.18.1.28**<br>• Verify the Port is correct: **80**<br>• Verify the Protocol is correct: **HTTP**<br>• Add the Web Interface servers IP address<br>○ **172.18.1.20**<br>○ **172.18.1.21**<br>○ Ensure the **Validate Credentials** box is unchecked<br>• Adjust the Site Path to: **/Citrix/DesktopWeb/** for XenDesktop 5.x<br>• Select **Next**<br>• **Note:** Changing the Site Path variable is a new requirement with NetScaler VPX 9.x. Please check documentation specific to your version of NetScaler for details. |
| 4 |  | In **Load Balance DDC servers** section<br>• Enter in the virtual IP address: **172.18.1.29**<br>• Verify the Port is correct: **80**<br>• Verify the Protocol is correct: **HTTP**<br>• Add the DDC servers IP address<br>○ **172.18.1.16**<br>○ **172.18.1.17**<br>○ Ensure the **Validate Credentials** box is unchecked<br>• Select **Next** |
| 5 |  | At Summary screen, verify settings and click **Finish** |

| XenDesktop Load Balancing | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 6 |  | Verify configurations are in “Up” state and click **Exit**<br><br>If configuration errors occur, refer to Citrix support article CTX121092 for guidance on troubleshooting |

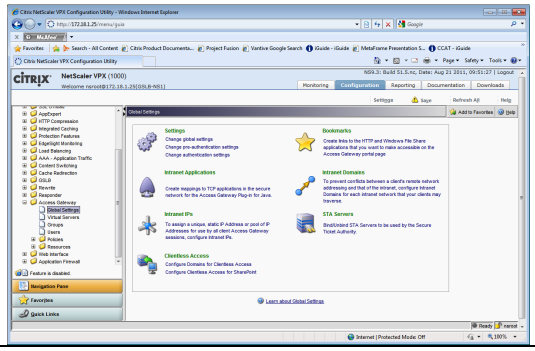
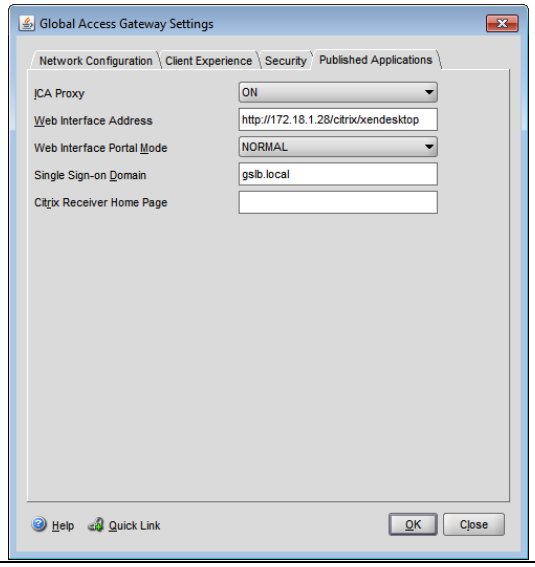
### *2.1.2 XenDesktop Site Configuration*

Now that there are virtual IP addresses created corresponding to the load balanced pool, those virtual addresses are used within the Web Interface configuration for the XenDesktop site. The Web Interface configuration steps must be performed for each WI server in the environment.

| Configure XenDesktop Web Interface | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | Within the **Citrix Desktop Studio** management console<br>• Select **Citrix Web Interface**<br>• Select **XenApp Web Sites**<br>• Select **Internal Site**<br>• Select **Server Farms** from Edit Settings |
| 2 |  | • Highlight the appropriate server farm and select **Edit** |
| 3 |  | • Remove the physical server address and replace with the virtual IP address for the DDC created on NetScaler: **172.18.1.29**<br>• Select **OK**<br>• Select **OK** |

## 2.2 Remote Access

In many situations, users originate from an external location, thus requiring them to have secure remote access to the internal network. Using Access Gateway, integrated on the NetScaler, provides a highly available single site. If you have a single Access Gateway virtual server on your NetScaler, you can configure the global settings to point to the virtual IP of the load balanced web interface as follows:

| Configure Access Gateway for Load Balanced Web Interface | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | Within the **NetScaler** console<br>• Select **Access Gateway – Global Settings**<br>• Select **Change Global Settings** |
| 2 |  | • Select the **Published Applications** tab<br>• Update the **Web Interface Address** with the load balanced IP address for the XenDesktop Web Interface servers<br>• Click **Ok** |

## 2.3 Section Summary

At this point, all components within the site are configured for high availability. The same processes should be conducted at the remaining sites. Once this is complete, each site should be tested for availability and fault tolerance before continuing onto the global availability.

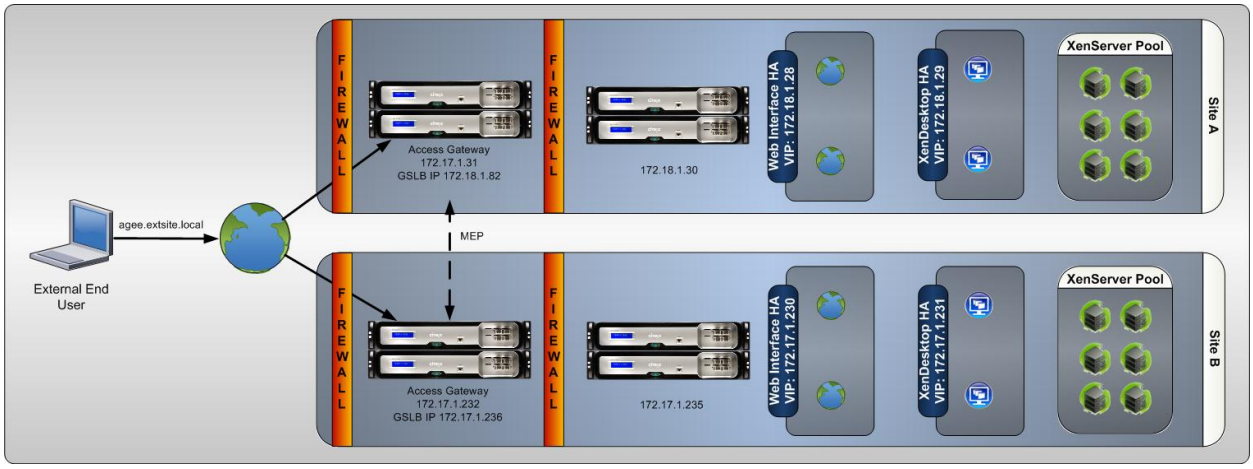
# 3. Global Availability

With the potential of a user accessing the environment from any location and across multiple data centers, there is a need to provide the user with the correct access point. The first part of this process is to get the user to an entry point without requiring multiple addresses or workflows. Secondly, users must be directed to the data center that contains their resources in order to provide the best user experience. The configuration of global availability is discussed in the following sections:

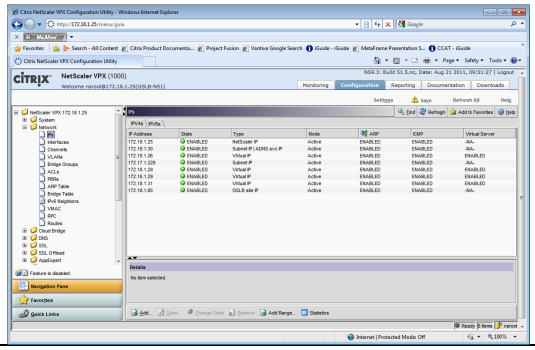
- Global Server Load Balancing
- Site Roaming

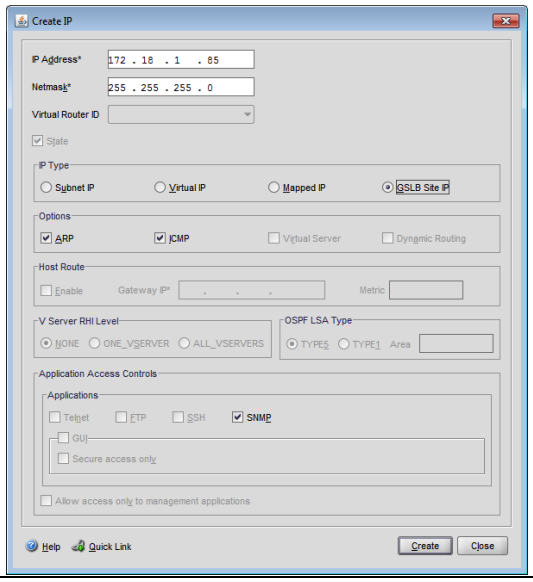
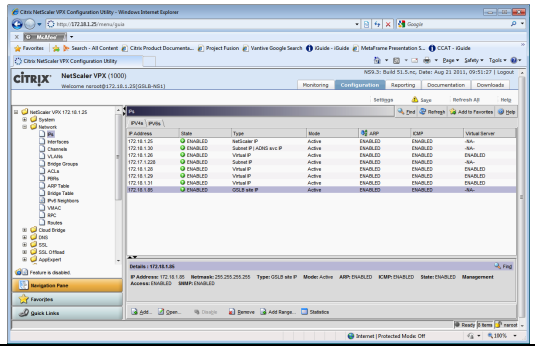
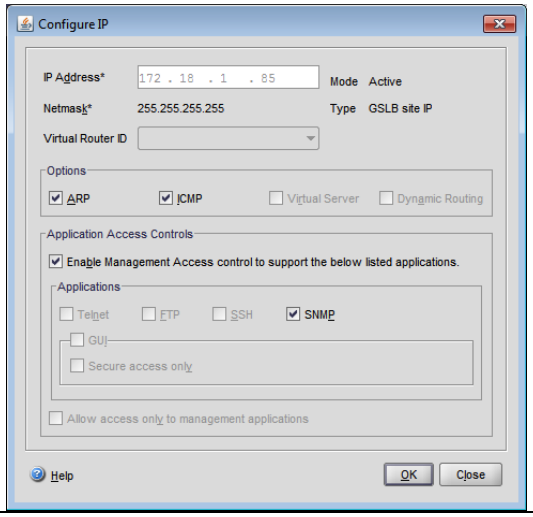
## 3.1 Global Server Load Balancing

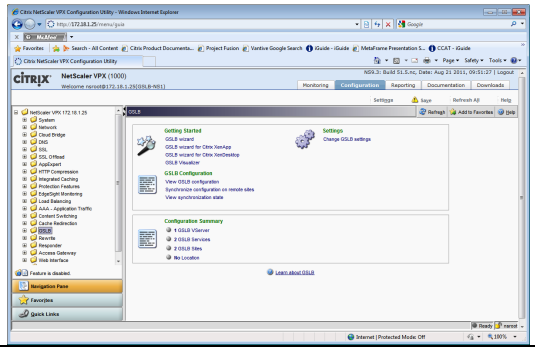
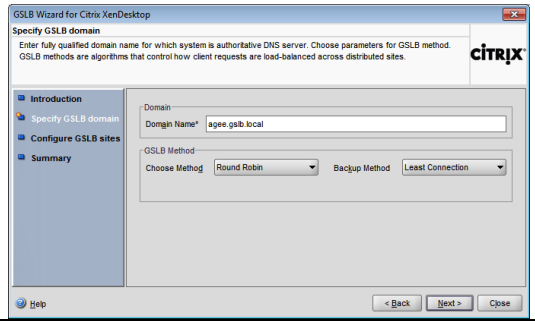
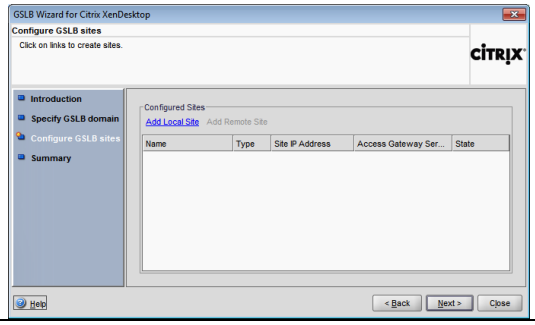
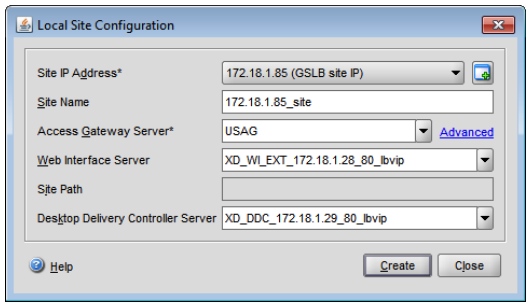
The global server load balancing configuration allows a user to enter in a single fully-qualified domain name and have that address direct them to an available site. This configuration is done with NetScaler deployed within each data center as the following figure shows.

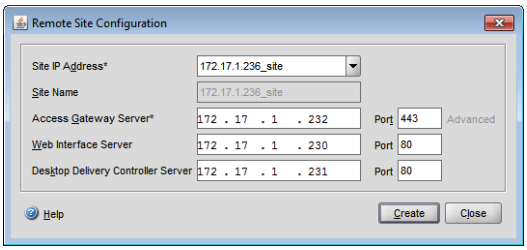
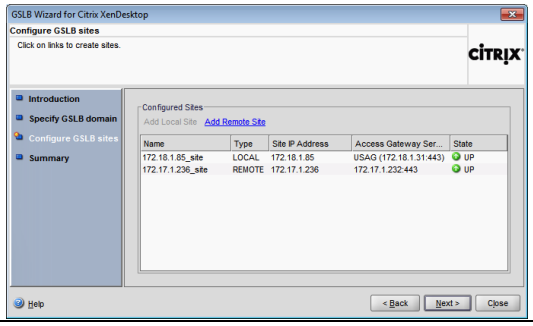
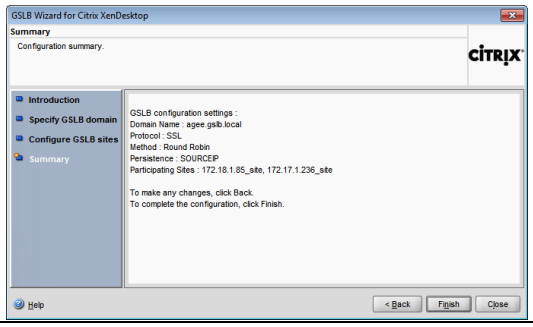
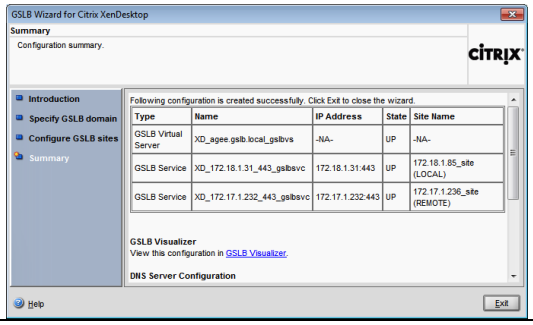



The configuration is as follows:

| Configure Global Server Load Balancing for XenDesktop | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | Within the **NetScaler** console<br>• Select **Network-IP**<br>• Click **Add** in the IP pane |

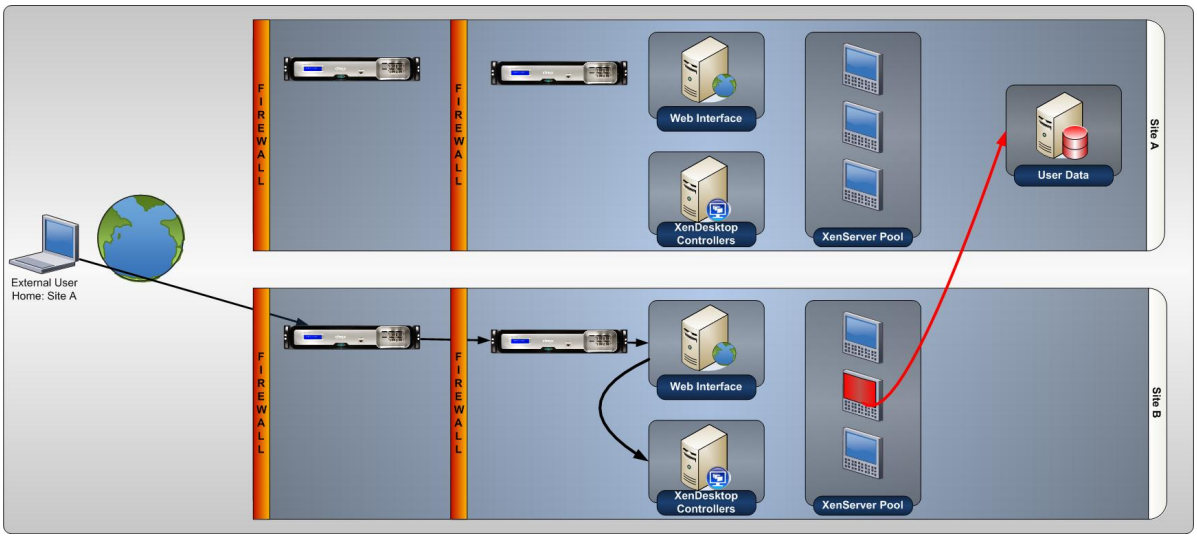
| Configure Global Server Load Balancing for XenDesktop | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 2 |  | In the Create IP dialog<br>• Add the **IP Address** and **Netmask**<br>  ○ **172.18.1.85**<br>  ○ **255.255.255.0**<br>• Select **GSLB Site IP** radio button<br>• Click **Create**<br>• Click **Close** |
| 3 |  | Within the **Network-IP** panel<br>• Select the GSLB Site IP address just created<br>• Click **Open** |
| 4 |  | In the **Configure IP** dialog<br>• Check **Enable Management Access control to support the below listed applications**<br>• Click **OK** |

| Configure Global Server Load Balancing for XenDesktop | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 5 |  | Within the **NetScaler** console<br>• Select **GSLB – GSLB Wizard for Citrix XenDesktop**<br>• Select **Next** on the opening screen |
| 6 |  | Within the **Specify GSLB domain** screen<br>• Enter in a valid fully qualified domain name. This is the address users will enter within their browser.<br>o **agee.extsite.local**<br>• Select **Next** |
| 7 |  | Within the **Configure GSLB Sites** screen<br>• Select **Add Local Site** |
| 8 |  | • Select the **Site IP Address** (GSLB site IP) from the pull-down menu<br>• Verify the information automatically populated<br>o Site Name: **172.18.1.85_site**<br>o Access Gateway virtual server: **USAG**<br>o Web Interface virtual IP address and port: **172.18.1.28:80**<br>o Desktop Delivery Controller Server virtual address and port: **172.18.1.29:80**<br>• Select **Create** |

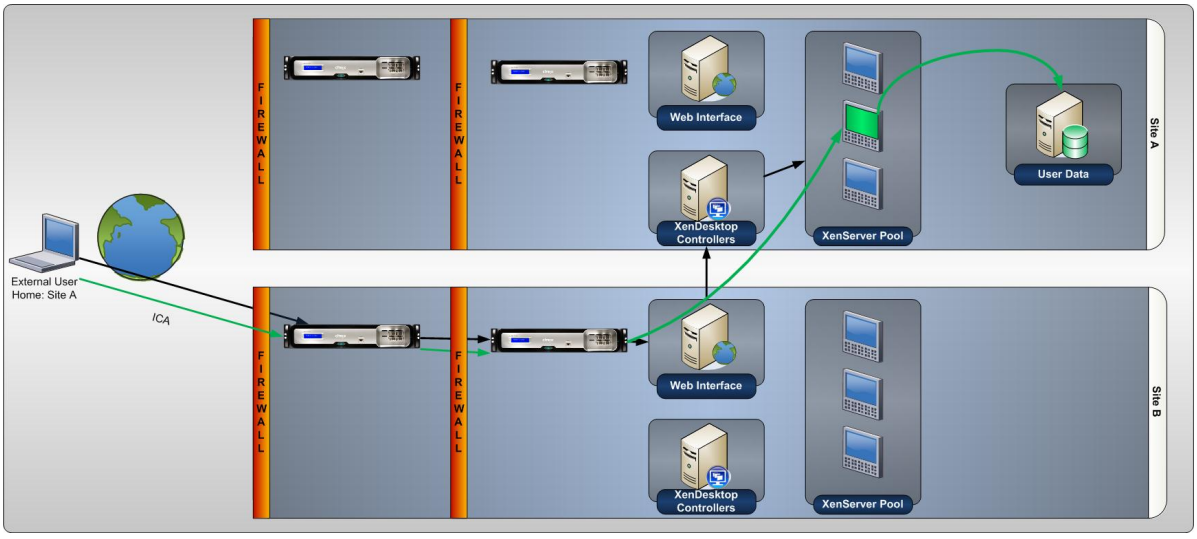
| Configure Global Server Load Balancing for XenDesktop | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 9 |  | • Select **Add Remote Site**<br>• Enter in the Site IP Address: **172.17.1.236**<br>• Verify the Site Name: **172.17.1.236_site**<br>• Enter the Access Gateway Server and Port: **172.17.1.232** port **443**<br>• Enter the Web Interface Server and Port: **172.17.1.230** port **80**<br>• Enter the Desktop Delivery Controller Server and Port: **172.17.1.231** port **80**<br>• Select **Create** |
| 10 |  | • Verify local and remote sites are up<br>• Select **Next** to complete the wizard |
| 11 |  | • Select **Finish** on summary screen |
| 12 |  | On the **GSLB Wizard for Citrix XenDesktop** Configuration Summary screen<br>• Verify all settings are correct<br>• Click **Exit**<br>Repeat This process on the NetScaler devices for each site in the GSLB configuration. |

## 3.2 Site Roaming

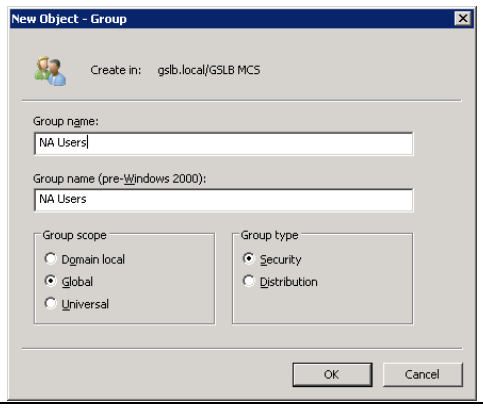
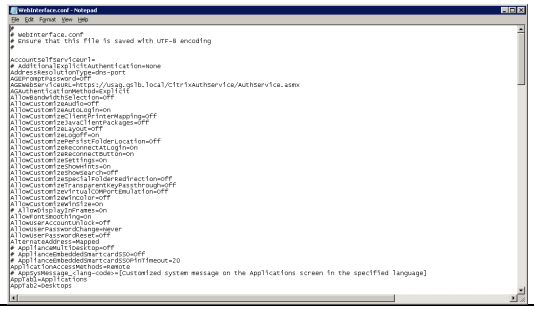
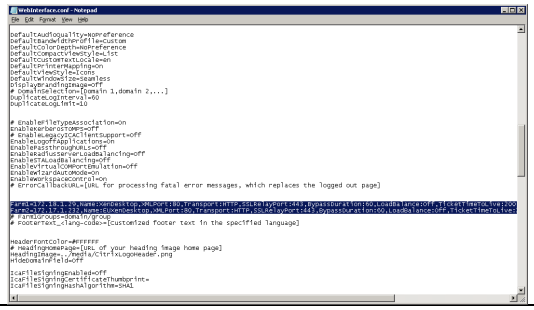
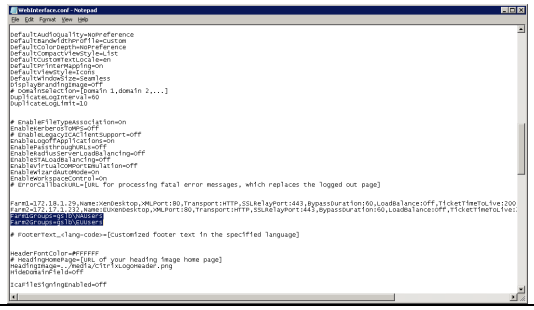
The global server load balancing configuration allows users to use a single address and gain access to the environment. There are situations where NetScaler directs a user to one data center but the user's virtual desktop is running in another data center, along with their profile and data. The following diagram shows what could happen if site roaming is not utilized.




As can be seen, the user accesses a virtual desktop in one data center. The virtual desktop must then traverse the WAN link to access the user data, resulting in a poor user experience. In these situations, it is advisable to utilize the site roaming feature of Web Interface, which redirects a user's virtual desktop request to an appropriate site as shown in the following diagram.

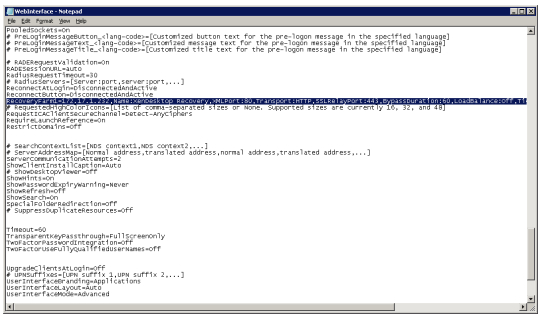


As can be seen, virtual desktop to user data communication stays local, thus improving the user experience. The site roaming feature is configured as follows:

| Configure Site Roaming | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | On a domain controller, access the **Active Directory Users and Computers** utility<br>• Create a **Group** for each data center site<br>• Provide a valid and descriptive name<br>• Populate the group with the appropriate users<br>The Active Directory group links a set of users with a particular data center, thus defining the user's preferred, or "Home", data center. |
| 2 |  | On each Web Interface server in the configuration:<br>• Navigate to: **C:\InetPub\wwwroot\Citrix*siteName*\conf**<br>• Open the file: **WebInterface.conf**<br>• Find the line that starts with **Farm1** |
| 3 |  | Add a new line to define the XenDesktop farm in the second site:<br>**Farm2=172.17.1.231, Name=EUXenDesktop, etc., etc.**<br>Ensure that the Farm2 parameter points to the XenDesktop VIP address in the second site.<br>***Note**: the Farm1 line can be copied and pasted to simplify configuration. Simply change the prefix Farm(n), address and name.* |
| 4 |  | Add the following new lines with appropriate domain\group combination:<br>**Farm1Groups=gslb\NAUsers**<br>**Farm2Groups=gslb\EUUsers**<br>***Note**: Each farm should have a corresponding group entry and each FarmNGroup can contain multiple Active Directory groups.* |

# 4. Disaster Recovery

The final step to provide a high-availability solution is to incorporate disaster recovery. The global server load balancing configuration with NetScaler directs users to sites with availability of components, but if that site is not able to support a disaster recovery scenario or the user is not allowed virtual desktops from the site, a failover farm can be configured and used. The configuration is as follows:

| Configure Site Failover | | |
|---|---|---|
| | **Screenshot** | **Description** |
| 1 |  | Within the WebInterface.conf file on each webserver in the configuration add the following new line:<br><br>**RecoveryFarm1=172.17.1.231, Name; XenDesktop Recovery, etc., etc.**<br><br>If the Web Interface is unable to identify a resource for the user based on the Site Roaming configuration, the user will be directed to resources within the Recovery Farm configuration.<br><br>The RecoveryFarm parameter should point to the XenDesktop VIP address in the second site. |

# 5. Palo Alto Networks Next-Generation Firewall Deployment

Palo Alto Networks next-generation firewalls can be deployed at the backend of Citrix XenDesktop virtual desktop infrastructure to safely enable applications for virtual desktop users. One of the key benefits of the Palo Alto Networks integration with Citrix XenDesktop applications is the User-ID technology which allows organizations to set up firewall policies based on users and groups rather than static IP addresses on the network.

## 5.1 Overview of User-ID Integration

In a virtual environment, where a user connects to a XenDesktop environment from any type of device, Palo Alto Networks provides a variety of solutions to allow customers to leverage User-ID in a completely virtualized environment.

| Citrix XenDesktop Options | Palo Alto Networks User Identification |
|---|---|
| Hosted share desktops | Enables identification of multiple users using the same network address<br>Enables Terminal Services integration, and identification of users based on port-ranges via a Terminal Services agent |
| On-demand applications | |
| Hosted Virtual Desktop | Enables transparent user or group identification based on authentication against Windows authentication domain.<br>This is achieved via a User-ID agent that monitors authentication event logs |
| Streamed VHD Desktops | |
| Local virtual machine (VM) desktops | |

The main difference between the different VDI solutions offered from the perspective of the firewall is if a relation between the relation between an IP address and user is one to one, or one to many.

- In standard XenDesktop setup, each user is assigned a virtual desktop with exactly one IP address. This scenario is addressed by the standard functionality of the User-ID agent. The agent creates a relation between the user and the IP address of the host by detecting the authentication of the user.
- In the case of XenApp for example, in which many users share one IP address, the User-ID Terminal Services Agent can assign TCP and UDP port ranges to users sharing the IP address of the Terminal Server. The firewall can then distinguish between users based on the source port of the session they establish.

## 5.2 User-ID with Citrix XenDesktop

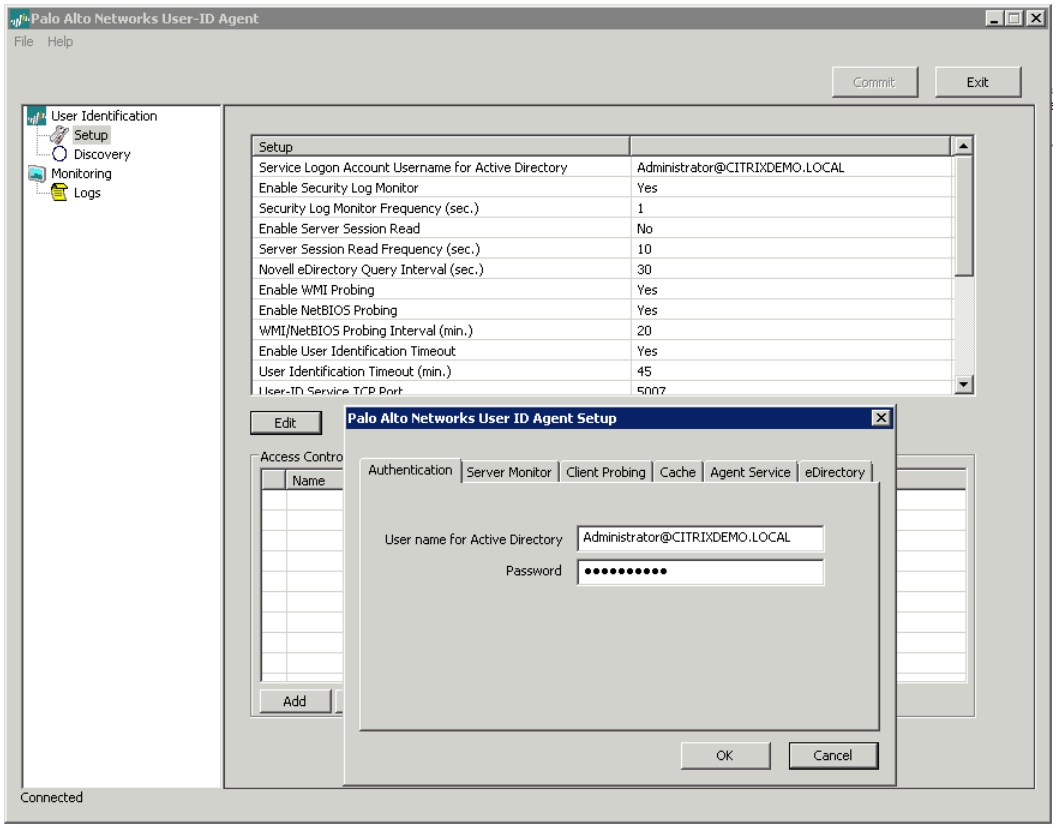
When a user connects to XenDesktop, a new virtual desktop is created and a unique IP address is assigned. As soon as the login process is initiated, an authentication event is logged on the domain controllers, which is monitored by a Palo Alto Networks User-ID agent. The username and IP address is communicated to the firewall via a secure network connection. This information can then be combined with user group information gathered from Active Directory, allowing the administrator to configure security policies based on user groups.

Safe application enablement rules and content inspection rules can then be applied on an individual user or user group basis on the firewall. The interaction between the virtual desktop infrastructure and the Palo Alto Networks next generation firewall simplifies policy creation and management, allowing the firewall to dynamically identify users and appropriate security rules.

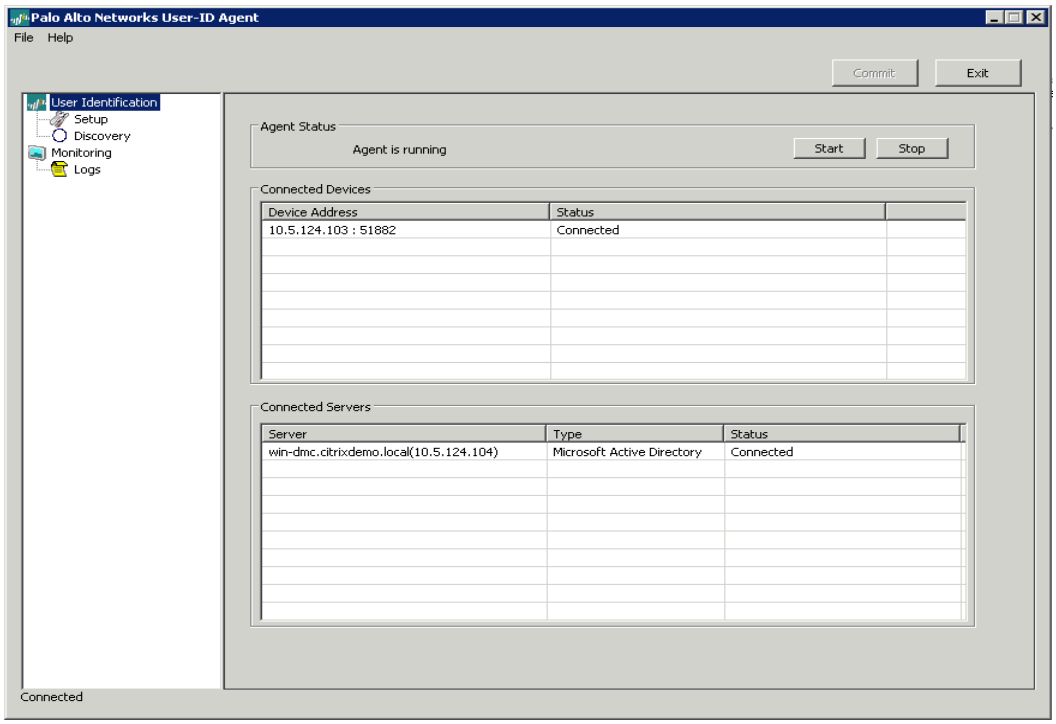
### *5.2.1 User-ID Agent*

The User-ID Agents can be installed on any Windows Server in the environment, provided it is a domain member. The Agent would then use configured credentials to remotely monitor the authentication events happening on Microsoft Active Directory Domain Controllers and/or Microsoft Exchange Servers to establish a relation between the username and the device being used on the network.

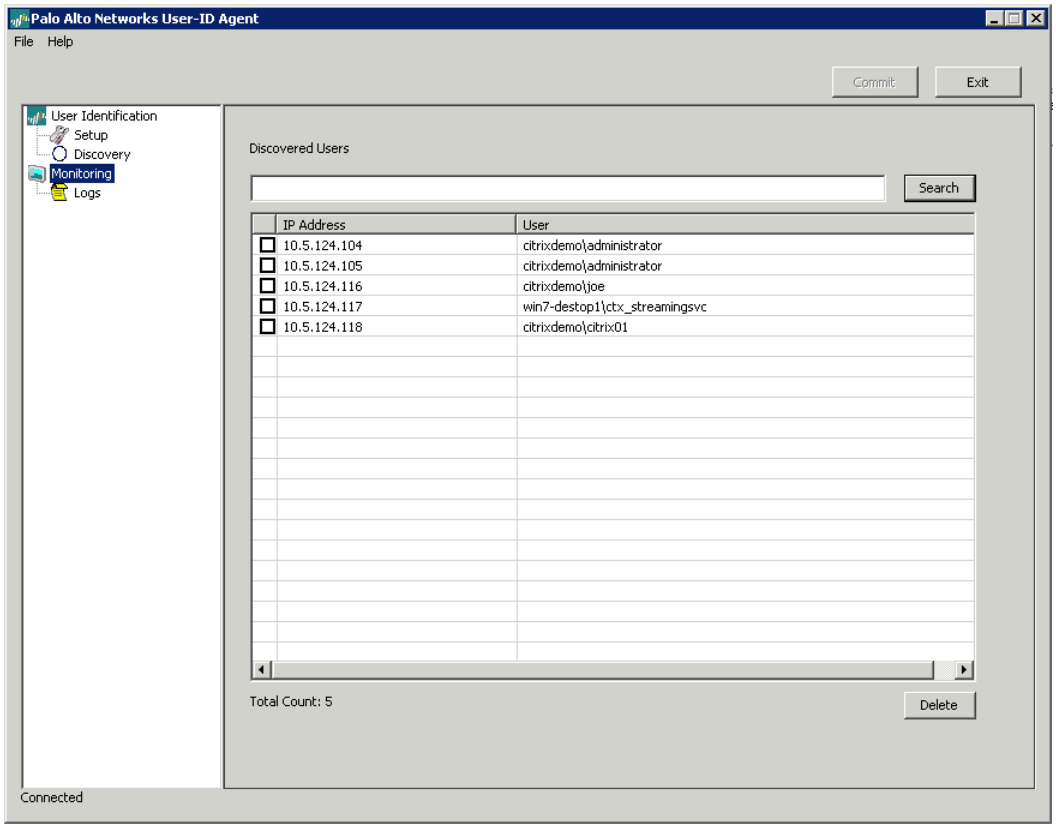
The User-ID Agent can be deployed in its standard configuration. The only required setting is the appropriate credentials needed to access and read the security logs on a Microsoft Windows Domain



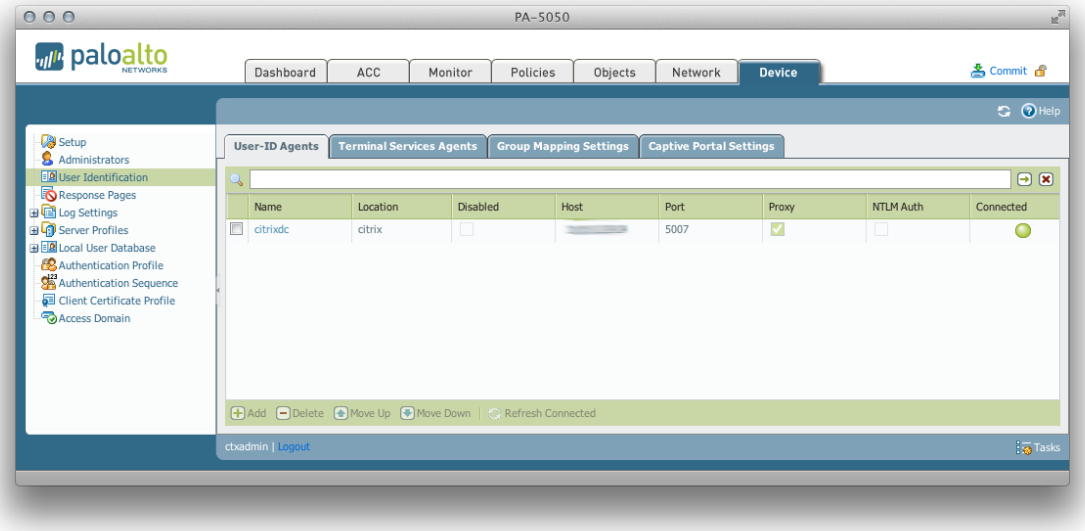

Controller or Microsoft Exchange Server. Usually, when deployed on a domain controller, “Event Log Reader” permissions are sufficient.




To verify the agent functionality an administrator can monitor which user logon events and IP addresses are identified by the agent via the integrated “Monitoring “ tab.



Palo Alto Networks next generation firewalls then connect to the Agents over a secure connection and




read the information gathered by the agent in order to enforce security policy based on users and groups.

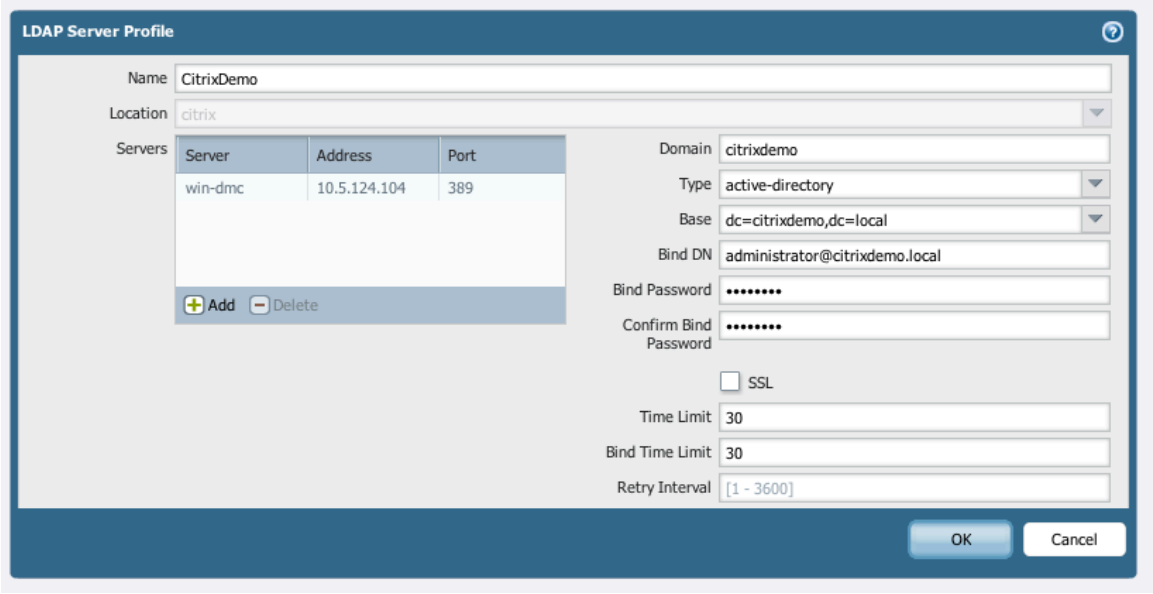
In a virtualized environment using XenDesktop, any virtual desktop running on a hypervisor supported by XenDesktop has an IP address on the network. Once the user connects and authenticates to Desktop Delivery Controller and launches his virtual desktop, an authentication event is created on an Active Directory Domain Controller. This authentication event allows the User-ID Agent to identify the user, who just launches his or her virtual desktop session.

```
admin@PA-5050 vsys2> show user ip-user-mapping

IP              Ident.  User                    Idle Timeout  Max. Timeout
--------------------------------------------------------------------------
x.x.x.104       AD      citrixdemo\administrator  3321          3321
x.x.x.116       AD      citrixdemo\citrix01       3027          3027
x.x.x.117       AD      citrixdemo\citrix02       3027          3027
Total: 3 users
```

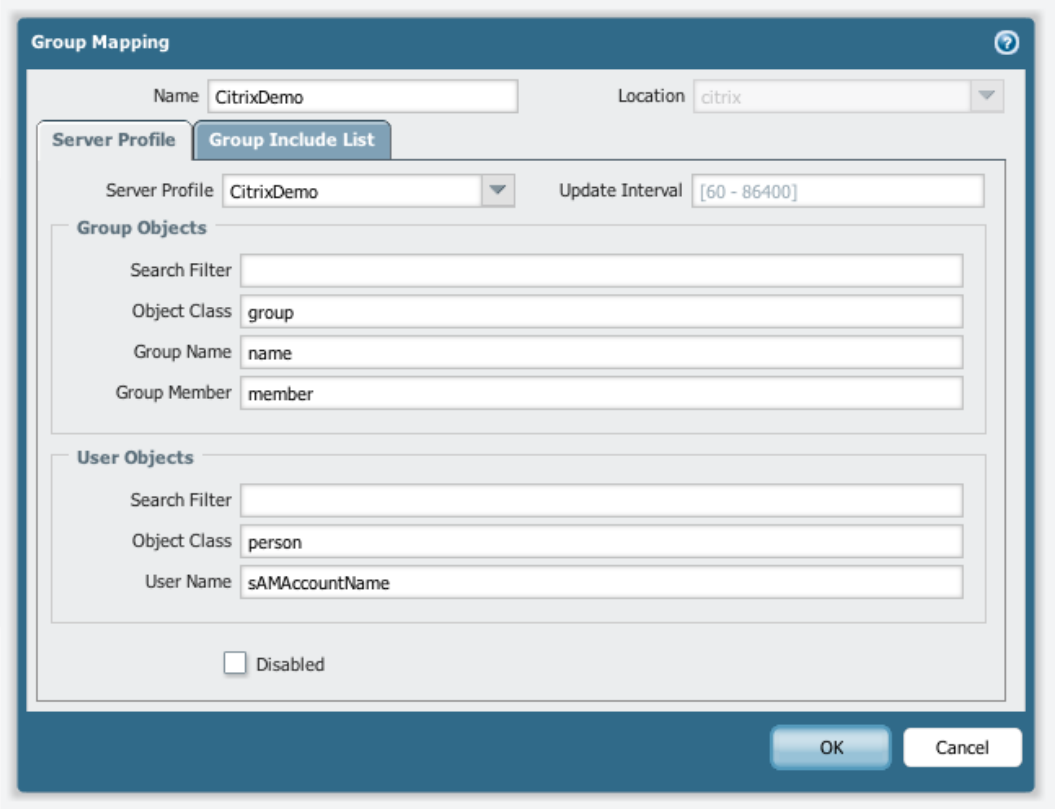
### *5.2.2 Users and groups*

Palo Alto Networks next generation firewalls can retrieve user and group information from most directory systems via LDAP. In an Active Directory environment, a LDAP server profile needs to be configured pointing either to the regular directory via TCP 389 or the Global Catalog via port 3268.




The authentication credentials used to connect to Active Directory need sufficient permissions to read the user and group details from the directory.

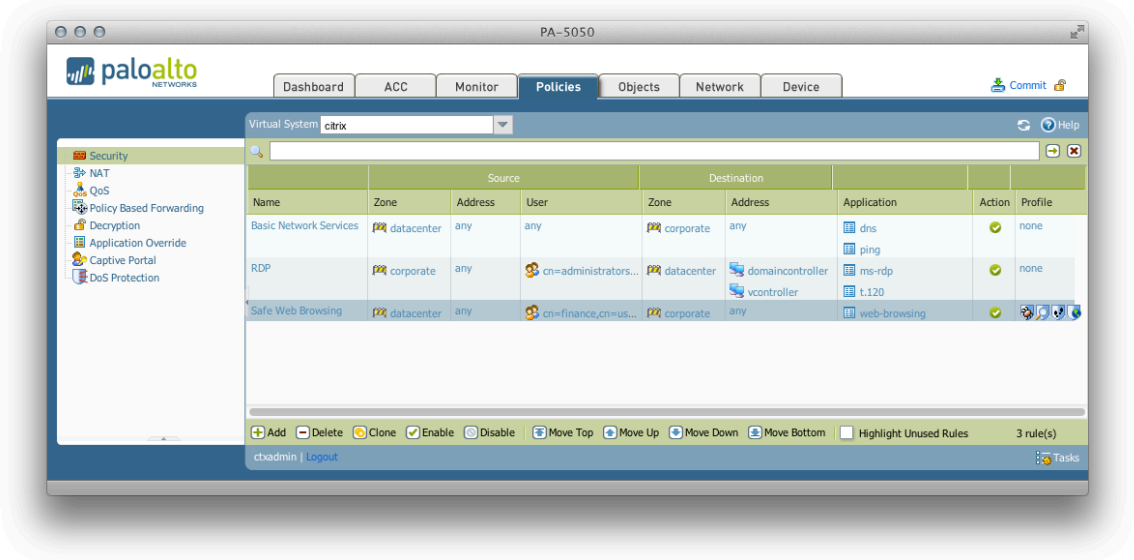
As a next step, User-ID requires to configure a group mapping filter. This includes the standard attributes and objectclasses used to retrieve user and group information. If a directory type is chosen in the “LDAP Server Profile”, the “User Group Mapping” settings will be pre-populated with the appropriate default values and no changes should be necessary.




If only a specific set of user groups are required in policy, the list of user groups retrieved by the firewall can be narrowed down by selecting the corresponding groups in the “Group Include List”.

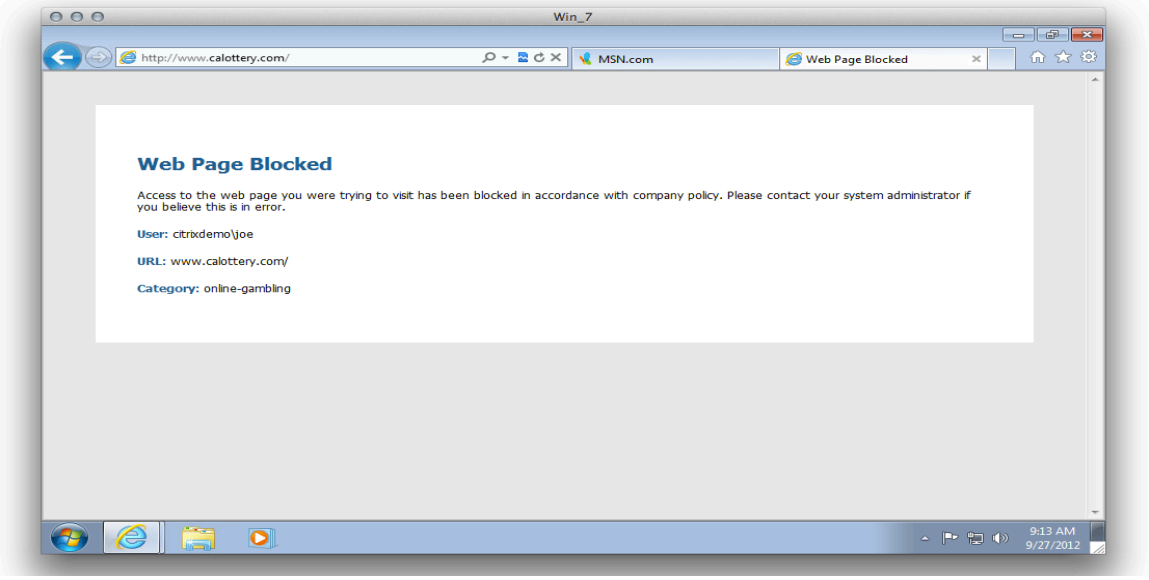
## 5.3 Security Policy

Once all User-ID components are configured, the administrator can start creating firewall rules including users in the source column.




### *5.3.1 Safe Application Enablement*

Applications to be enabled can be selected by clicking on the Application tab and “Add”. Applications can be safely enabled for users in virtual desktop infrastructures like for every other client machine. For example, a standard firewall security policy could allow selected user groups to browse the internet, but only allow access to work related websites. Access to any other not work related website can be safely




blocked informing the user about the policy violation.

### *5.3.2 Threat Prevention*

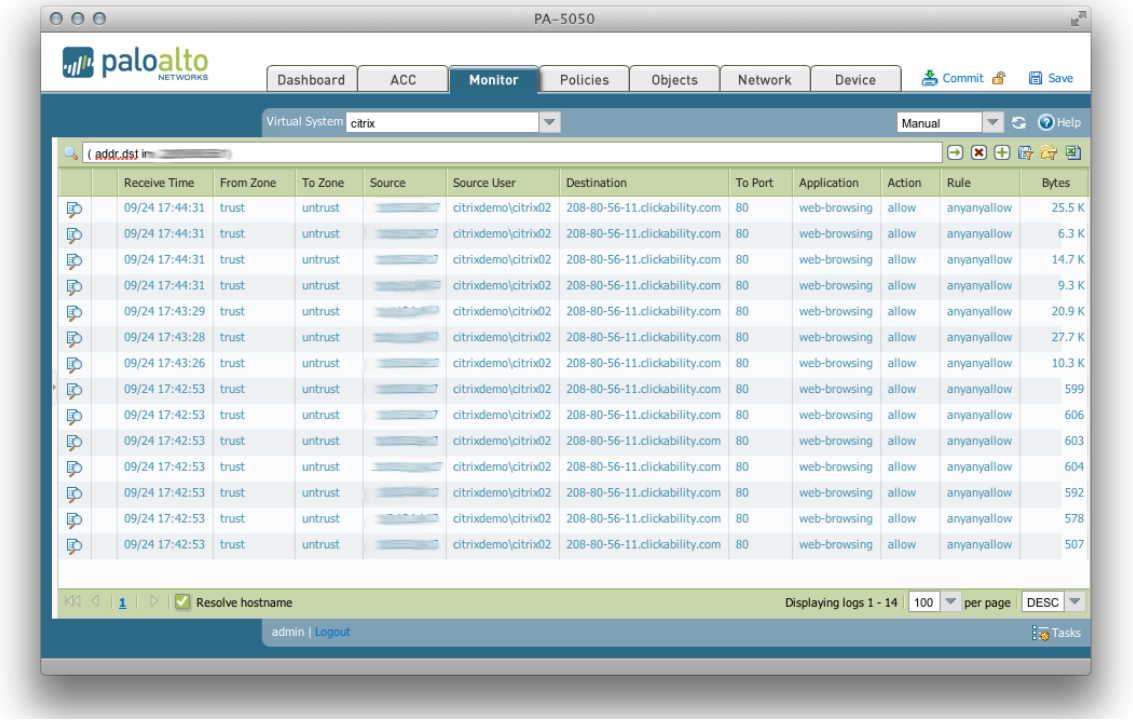
In addition to safely enabling the application used by the virtual desktop users, the next-generation firewall can scan the applications for threats. These include viruses, malware, spyware, or files with confidential data. By creating a security profile, the firewall can prevent a user from unknowingly infecting virtual desktop environment. Each rule in the security policy can have its own security profile applied, allowing for the greatest flexibility in setting policy.

To begin creating the security profile, locate the Profile column in the security policy page. If nothing has been configured there yet, it will indicate “none”. Click the “none” and a dialog window will open. Choose “Profiles” from this window to configure the security profile.

In the security profile window, select the specific profile settings for each of the different areas, Antivirus, Vulnerability Protection, etc. Some of these will have pre-configured profiles, such as “default” or “strict”. These pre-configured options can be chosen, or a customized profile can be created. Please see Palo Alto Networks Administration Guide for details on creating custom profiles.

## 5.4 Logging

User-ID in a virtualized network provides more than just policy enforcement on users and user groups, but also visibility into user activity by application, for example web browsing.In addition, more detailed logs and reports can be created. For example, every website a user is browsing to from a virtual desktop can be logged and used for reporting purposes.




# 6. References

**About Palo Alto Networks**

Palo Alto Networks™ is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks' platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks' products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks' products are used by more than 9,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.



**About Citrix**

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.