



Deployment Guide for Citrix XenDesktop

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





CİTRİX'

Table of Contents

1. Overview	3
1.1 Best-In-Class Solution for Citrix XenDesktop	3
1.2 Prerequisites for Implementation	4
2. Local Availability	5
2.1 Desktop Delivery	6
2.1.1 Load Balancing	
2.1.2 XenDesktop Site Configuration	
2.2 Remote Access	
2.3 Section Summary	
3. Global Availability	11
3.1 Global Server Load Balancing	
3.2 Site Roaming	15
4. Disaster Recovery	17
5. Palo Alto Networks Next-Generation Firewall Deployment	18
5.1 Overview of User-ID Integration	
5.2 User-ID with Citrix XenDesktop	
5.2.1 User-ID Agent	
5.2.2 Users and groups	21
5.3 Security Policy	23
5.3.1 Safe Application Enablement	
5.3.2 Threat Prevention	
5.4 Logging	25
6. References	



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-inclass 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-inclass 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 <u>XenServer Pooled Desktops (Local and Remote)</u> Implementation Guide in the <u>XenDesktop Design Handbook</u>.

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[™], Global-Protect[™] 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:





	Screensh	ot	Description
	Load Balancing Wizard for Citrix)	(enDesktop	In the Load Balance WI servers section
	Load Balance DDC servers Configure virtual server for load ba	alancing Desktop Delivery Controller servers.	
		СПКІХ	• Enter in the virtual IP address: 172.18.1.28
	Introduction	Virtual Server	Verify the Port is correct: 80
	Load Balance WI servers	P Address* 172 . 18 . 1 . 29 Port* 80	Verify the Protocol is correct: HTTP
	Summary	Projecon ni P	Add the Web Interface servers IP address
		P Address* Port	o 172.18.1.20
		172.18.1.16.80 Remove	o 172.18.1.21
			 Ensure the Validate Credentials box is unchecked
		Health Montoring	Adjust the Site Path to: /Citrix/DesktopWeb/ for XopDosition 5 x
		Password	Select Next
			Note: Changing the Cite Dath verichle is a new
	Sep	Sip> <back bert=""> Cpos</back>	requirement with NetScaler VPX 9.x. Please check documentation specific to your version of NetScaler details.
Ł	Load Balancing Wizard for Citrix	KenDesktop	In Load Balance DDC servers section
	Configure virtual server for load b	alancing Desktop Delivery Controller servers.	• Enter in the virtual IP address: 172.18.1.29
			Verify the Port is correct: 80
	Load Balance WI servers	Virtual Server	Verify the Protocol is correct: HTTP
	Load Balance DDC servers	Protocol HTTP	
		DDC Servers	Add the DDC servers IP address
		P AUDICES POL	○ 172.18.1.16
		172.18.1.17.80	o 172.18.1.17
			• Ensure the Validate Credentials box is
		Heath Monitoring	unchecked
		Validate Credentials	Select Next
		Password	
		Domain Name	
	Э Нер	Skip > < Back Next > Close	
	Load Balancing Wizard for Citrix	KenDesktop	At Summary screen, verify settings and click Finish
	Summary Configuration summary.	сітвіх	
	 Introduction Load Balance WI servers 	Configuration settings for load balancing Web Interface servers :	
	Load Balance DDC servers	Protocol : HTTP	
	Summary	Menido Leas connection Persistence: COOKENSERT Web Interface servers : 172.18.1.20.80, 172.18.1.21.80	
		Configuration settings for load balancing Desktop Delivery Controller servers : Virtual Server IP : 172:18:1.29	
		Port: 80 Protocol: HTTP Method : Least Connection	
		Persistence : NONE Desktop Delivery Controller servers : 172.18.1.18.80, 172.18.1.17.80	
		To make any changes, click Back. To complete the configuration, click Finish.	



XenDesktop Load Balancing				
	Screensho	ot		Description
6	Load Balancing Wisard for Citric Jammary Configuration summary. B Introduction B Load Balance W servers B Load Balance DOC servers B Summary	Type Bane P Address State Type DD, VIL, DT, 172.16.1.28, 08, 8×69 172.16.1.28.20 IP Bernice Group Member 702, VIL, DT, 172.16.1.28, 08, 8×69 172.16.1.28.20 IP Bernice Group Member 702, VIL, DT, 172.16.1.28, 08, 8×69 172.16.1.28.20 IP Bernice Group Member 702, VIL, 172.16.1.28, 08, 9×69 172.16.1.280 IP Bernice Group Member 702, VIL, 172.16.1.28, 08, 9×69 172.16.1.280 IP Bernice Group Member 702, VIL, 12.1.28, 08, 9×69 172.16.1.280 IP Bernice Group Member 702, VIL, 12.1.28, 08, 9×69 172.16.1.178.00 IP Cock Los do up Member 702, DDC, 172.16.1.28, 08, 9×69 172.16.1.178.00 IP Service Group Member 702, DDC, 172.16.1.28, 08, 9×69 172.16.1.178.00 IP Cock Los do up Member 702, DDC, 172.16.1.28, 08, 9×69 172.16.1.178.00 IP	CITRIX.	Verify configurations are in "Up" state and click Exit If configuration errors occur, refer to Citrix support article <u>CTX121092</u> for guidance on troubleshooting
	Э Нер		Ext	



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.

Со	Configure XenDesktop Web Interface			
	Screenshot	Description		
1	Image: State State Image: State State Image: State State Image: State State <th> Within the Citrix Desktop Studio management console Select Citrix Web Interface Select XenApp Web Sites Select Internal Site Select Server Farms from Edit Settings </th>	 Within the Citrix Desktop Studio management console Select Citrix Web Interface Select XenApp Web Sites Select Internal Site Select Server Farms from Edit Settings 		
2	Manage Server Farms - Internal Site X Add and edit fam names and specify the order in which fams are contacted. You can also specify XML and SSL server ports, transport types, and enable ticketing for all servers. Earns (in change password order): Name XML port XML transport SSL Relay port Servers XerDes B0 HTTP Move Lip Move Down Add Edit Bemove Move Down Advanced Settings Configure socket pooling and XML Service communication for all farms. Advanced OK Cancel D	Highlight the appropriate server farm and select Edit		
3	Edit Farm Earn name: KenDesktop Server Settings Servers (in failover order): 172.18.1.29 Move Up Move Down Add Edit Bemove Uge the server list for load balancing Bypass any failed server for: 1 Move Down XML Service port: 80 Iransport type: HTTP SSL Relay port: 443 Ticketing Settings Configure the lifetime of client authentication tickets. DK Cancel	 Remove the physical server address and replace with the virtual IP address for the DDC created on NetScaler: 172.18.1.29 Select OK 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:

Co	onfigure Access Gateway for Loa <u>d Balancec</u>	I Web Interface
	Screenshot	Description
1	<complex-block></complex-block>	 Within the NetScaler console Select Access Gateway – Global Settings Select Change Global Settings
2	Global Access Gateway Settings Network Configuration \ Client Experience \ Security' Published Applications \ ICA Proxy ON Web Interface Address http://172.18.1.28/ctris/xendesktop Web Interface Address http://172.18.1.28/ctris/xendesktop Web Interface Portal Mode NORMAL Single Sign-on Domain gsb.local Citrix Receiver Home Page	 Select the Published Applications tab Update the Web Interface Address with the load balanced IP address for the XenDesktop Web Interface servers 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:





CİTRİX[.]

Screenshot Description 2 In the Create IP dialog In the Create IP dialog Address and Netmask 172.18.1.85 255.255.255.0 Select GSLB Site IP radio button Click Create Click Close 3 Immediate State S	
 In the Create IP dialog Add the IP Address and Netmask 172.18.1.85 255.255.255.0 Select GSLB Site IP radio button Click Create Click Close 3 Image: Ima	
 Add the IP Address and Netmask 172.18.1.85 255.255.255.0 Select GSLB Site IP radio button Click Create Click Close 	
 172.18.1.85 255.255.255.0 Select GSLB Site IP radio button Click Create Click Close 	
 vvvtual Router D 255.255.255.0 Select GSLB Site IP radio button Click Create Click Close 3 Within the Network-IP panel	
 Select GSLB Site IP radio button Click Create Click Close 	
 Click Create Click Close Click Close 	
 Click Close Click Close Click Close 	
Click close Click click click Click click click click Click click click click click Click click click click click click click click click click	
3 Within the Network-IP panel	
3 Within the Network-IP panel	
3 Image: Market Mar	
3 Image: Second access only 3 Image: Second access only	
3 Implementations 3 Implementations	
3 Image: Contractions Within the Network-IP panel	
3 Contractions Within the Network-IP panel	
3 Contractor Within the Network-IP panel	
3 Constant of the management applications Within the Network-IP panel	
3 Contraction of Contractions	
3 Control and the second secon	
Select the GSI B Site IP address just creat	ed
Comment C	
LLm. 0 01/L11 M 0 04/L01 Margin Frame 04/L01 04/L01 <th></th>	
0.4974a (12111) ¥ ¥16425 (1417) Advi 19425 (14425 (1442) Advi 19425 (1442) (14	
Lier Liens # Gasteg # Jan	
Planew Tay III // III Benak 2022/2021 Type (52.8 MP 1944)20 Met 194420 Met 194420 Met 194420 Met 194420	
Danne Bann Bann Bann Bann Bann Bann Bann	
4 In the Configure IP	
Check Enable Management Access cont	trol to
P Address* 172.18.1.85 Mode Active support the below listed applications	
Netmas <u>k</u> * 255.255.255.255 Type GSLB site IP • Click OK	
Virtual Router D	
Options	
ARP Virtual Server Dynamic Routing	
Application Access Controls	
Enable Management Access control to support the below listed applications.	
Applications	
□ Tel <u>h</u> et _ ETP _ SNM P	
Allow access only to management applications	
W Help OK Close	



	Screenshot	Description
5	Control and Microsofter Control and Microsofter Contro and Microsofter Control and Microsofter <th> Within the NetScaler console Select GSLB – GSLB Wizard for Citrix XenDesktop Select Next on the opening screen </th>	 Within the NetScaler console Select GSLB – GSLB Wizard for Citrix XenDesktop Select Next on the opening screen
6		 Within the Specify GSLB domain screen Enter in a valid fully qualified domain name. This is the address users will enter within their browser. agee.extsite.local Select Next
7	GSLB Wizard for Citrix XenDesktop Configure GSLB sites Cick on Intits to create sites. Cintropaction Introduction Specify GSLB domain Configure GSLB domain Configure GSLB domain Configure GSLB domain Sconfigure GSLB domain Configure GSLB domain Sconfigure GSLB domain Sconfigure GSLB domain Configure GSLB domain Sconfigure GSLB domain Type Site P Address Access Outeway Ser State Wheth Clock Reth	 Within the Configure GSLB Sites screen Select Add Local Site
8	Local Site Configuration Site P Agdress* 172.18.1.85 (GSLB site P) Site Name 172.18.1.85_site Access Gateway Server* USAG Advanced Web Interface Server XD_WLEXT_172.18.1.28_80_bvip Site Path	 Select the Site IP Address (GSLB site IP) from the pull-down menu Verify the information automatically populated Site Name: 172.18.1.85_site Access Gateway virtual server: USAG Web Interface virtual IP address and port: 172.18.1.28:80



Со	nfigure Global Server Load Balancing for X	KenDesktop
	Screenshot	Description
9	Remote Site Configuration Site P Agdress* 172.17.1236_site Site Name 172.17.1236_site Access Gateway Server* 172.17.1 200 Desigtop Delivery Controller Server 172.17.1 217.1 <tr< th=""><th> Select Add Remote Site Enter in the Site IP Address: 172.17.1.236 Verify the Site Name: 172.17.1.236_site Enter the Access Gateway Server and Port: 172.17.1.232 port 443 Enter the Web Interface Server and Port: 172.17.1.230 port 80 Enter the Desktop Delivery Controller Server and Port: 172.17.1.231 port 80 Select Create </th></tr<>	 Select Add Remote Site Enter in the Site IP Address: 172.17.1.236 Verify the Site Name: 172.17.1.236_site Enter the Access Gateway Server and Port: 172.17.1.232 port 443 Enter the Web Interface Server and Port: 172.17.1.230 port 80 Enter the Desktop Delivery Controller Server and Port: 172.17.1.231 port 80 Select Create
1 0	OSB Wizard for Clinix XenDezidop Configure GSB alies Citku niska to create alea. Introduction Specify GSB Sommin Configure GSB alies Configure GSB alies Configure GSB alies Security GSB Sommin Virginities Configure GSB alies Summary Beb	 Verify local and remote sites are up Select Next to complete the wizard
1	GSLB Wisard for Citrix XenDesistop Image: Configuration summary. Configuration summary. Citrix X Introduction GSLE configuration settings : Daman Name: age gab local Protoci: SSL Citrix X Configure GSLB steer Summary GSLE configuration settings : Daman Name: age gab local Protoci: SSL Protoci: SSL Protoci: SSL Protoci: SSL To make any changes, cick Back. To complete the configuration, cick Finab. Image: Step Steer Stee	Select Finish on summary screen
1 2	Still Waard for Citrix XenDesktop Citrix Summary Configuration summary. Citrix XenDesktop Introduction Introduction Citrix Specify GSLB domain Following configuration is created success luby. Citcl Exit to close the wicard. Introduction Configure GSLB state State Visual VD_age gab. bical_gabova AUA. UP AUA. State State State State State State State GSLB State Visual VD_age gab. bical_gabova AUA. UP AUA. UP (UCCAL). GSLB Service XD_172.161.31_443_gabeve 172.161.31.443_gabeve UCCAL. UCCAL. UCCAL. UCCAL. GSLB Service XD_172.171.1232_443_gabeve 172.171.1232_443_gbbeve UP T/T Tr. 1705.state (REMOTE) UP GSLB Visualizer Uve wha configuration in GSLB Visualizer. UNIS Server Configuration in GSLB Visualizer. UNIS Server Configuration Ext	 On the GSLB Wizard for Citrix XenDesktop Configuration Summary screen Verify all settings are correct Click Exit 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:

Со	Configure Site Roaming			
	Screenshot	Description		
1	Screensnot New Object - Group X See Create in: gsb.local/GSLB MCS Group name Image: Create in: gsb.local/GSLB MCS Group name (pre-Windows 2000): Image: Create in: gsb.local/GSLB MCS Group name (pre-Windows 2000): Image: Create in: gsb.local/GSLB MCS Group name (pre-Windows 2000): Image: Create in: gsb.local/GSLB MCS Group name (pre-Windows 2000): Image: Create in: gsb.local/GSLB MCS Group scope Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Group name (pre-Windows 2000): Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image: Create in: gsb.local/GSLB MCS Image:	Description On a domain controller, access the Active Directory Users and Computers utility • Create a Group for each data center site • Provide a valid and descriptive name • Populate the group with the appropriate users 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	Control of the second sec	 On each Web Interface server in the configuration: Navigate to: C:\InetPub\wwwroot\Citrix\siteName\conf Open the file: WebInterface.conf Find the line that starts with Farm1 		
3	Image: Contraction of States Image: Contraction of States <td< th=""><th>Add a new line to define the XenDesktop farm in the second site: Farm2=172.17.1.231, Name=EUXenDesktop, etc., etc. Ensure that the Farm2 parameter points to the XenDesktop VIP address in the second site. Note: the Farm1 line can be copied and pasted to simplify configuration. Simply change the prefix Farm(n), address and name.</th></td<>	Add a new line to define the XenDesktop farm in the second site: Farm2=172.17.1.231, Name=EUXenDesktop, etc., etc. Ensure that the Farm2 parameter points to the XenDesktop VIP address in the second site. Note : the Farm1 line can be copied and pasted to simplify configuration. Simply change the prefix Farm(n), address and name.		
4	Webstweetweetweetweetweetweetweetweetweetwe	Add the following new lines with appropriate domain\group combination: Farm1Groups=gsIb\NAUsers Farm2Groups=gsIb\EUUsers 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:

Co	Configure Site Failover		
	Screenshot	Description	
1	International Margin International Margin The approximation of the second	Within the WebInterface.conf file on each webserver in the configuration add the following new line:	
	<pre>/ #lighthitheouting transmission terms (port) // *lighthicked and terms (port) // *lighthic</pre>	RecoveryFarm1=172.17.1.231, Name; XenDesktop Recovery, etc., etc.	
	benergenammentes (foot tegeri-) e standbest toor tegeri-) to and tegeri- thomat store tegeri- thomat store tegeri- thomat store tegeri- thomat store tegeri- standbest tegeri- e Standbest teg	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.	
	Improve the second seco	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	
On-demand applications	Enables Terminal Services integration, and identification of users based on port-ranges via a Terminal Services agent	
Hosted Virtual Desktop	Enables transparent user or group identification based on	
Streamed VHD Desktops	authentication against Windows authentication domain. This is achieved via a User-ID agent that monitors authentication	
Local virtual machine (VM) desktops	event logs	

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

🚰 Palo Alto Networks User-ID Ag	gent		
		Commit	Exit
User Identification			
Discovery	Setup		
Monitoring	Service Logon Account Username for Active Directory	Administrator@CITRIXDEMO.LOCAL	
Logs	Enable Security Log Monitor	Yes	
	Security Log Monitor Frequency (sec.)	1	
	Enable Server Session Read	No	
	Server Session Read Frequency (sec.)	10	
	Novell eDirectory Query Interval (sec.)	30	
	Enable WMI Probing	Yes	
	Enable NetBIOS Probing	Yes	
	WMI/NetBIOS Probing Interval (min.)	20	
	Enable User Identification Timeout	Yes	
	User Identification Timeout (min.)	45	
	Liser-TD Service TCP Port	5007	_
	Access Contro Name Authentication Server Monitor Client F User name for Active Directory Adm Password	Probing Cache Agent Service eDirectory	
Connected		OK Cancel	

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



Setup	Agent Status							
Monitoring	Agent is runningStartStop							
	Connected Devices							
	Device Address	Status						
	10.5.124.103 : 51882	Connected		-				
				-				
	Connected Servers							
	Connected Servers	Туре	Status	Т				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected	I				
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected					
	Connected Servers Server win-dmc.citrixdemo.local(10.5.124.104)	Type Microsoft Active Directory	Status Connected					

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.

Alto Networks User-II) Agent		_
lp			
			Commit Exit
er Identification			
P Setup			
) Discovery	Discovered Users		
onitoring			
Logs	I		Search
	IP Address	User	
	10.5.124.104	citrixdemo\administrator	
	10.5.124.105	citrixdemo\administrator	
	10.5.124.116	citrixdemo\ioe	
	10.5.124.117	win7-destop1\ctx_streamingsvc	
	10.5.124.118	citrixdemo\citrix01	
	Total Count: 5		Delete
			Delete



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

NETWORKS	Dachboard A(CC Monitor	Policios Objects	Notwork	Dovico		🐣 Commit 🤞
	Dashboard	Monitor	Policies Objects	Network	Device		
							S 0
Setup	User-ID Agents Termi	inal Services Agents	Group Mapping Settings	Captive Portal Set	tings		
User Identification	٩,						→
Response Pages	Name Lo	cation Disable	d Host	Port	Proxy	NTLM Auth	Connected
III Local User Database Que Authentication Profile Authentication Sequence III Client Certificate Profile Occess Domain	+ Add - Delete + Mov	ve Up 💿 Move Down 🗧	C Refresh Connected				

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.

6.	admin@PA-5050 v	sys2> show us	ser ip-user-mapping		
7.					
8.	IP	Ident.	User	Idle Timeout	Max. Timeout
9.					
10.	x.x.x.104	AD	citrixdemo\administrator	3321	3321
11.	x.x.x.116	AD	citrixdemo\citrix01	3027	3027
12.	x.x.x.117	AD	citrixdemo\citrix02	3027	3027
13.	Total: 3 users				
14.					

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.



Name	CitrixDemo					
Location	citrix					-
Servers	Server	Address	Port	Domain	citrixdemo	
	win-dmc	10.5.124.104	389	Туре	active-directory	-
				Base	dc=citrixdemo,dc=local	-
				Bind DN	administrator@citrixdemo.local	
		h		Bind Password		
	Add Dele			Confirm Bind	•••••	
				Passworu	SSL SSL	
				Time Limit	30	
				Bind Time Limit	30	
				Retry Interval	[1 - 3600]	

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.

Name Cit	rixDemo	Location	citrix	~
Server Profile	ïtrixDemo	✓ Update Interval	[60 - 86400]	
roup Objects				
Search Filter				
Object Class	group			
Group Name	name			
Group Member	member			
ser Objects				
Search Filter				
Object Class	person			
User Name	sAMAccountName			
	Disabled			

palo

the network security compare

X

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.



NETWORKS	Dashboard	ACC	Monitor	Policies Obj	ects Netw	vork Device		<u>å</u>	Commit 💣
	Virtual System citrix		~						😋 🔞 Help
Security	Q								→ 🗙
-∰≫ NAT									
- 💑 QoS	Name	Zone	Address	User	Zone	Address	Application	Action	Profile
Decryption Application Override	Basic Network Services	M datacenter	any	any	Page corporate	any	💷 dns 🎹 ping	0	none
- Captive Portal - Jos Protection	RDP	M corporate	any	S cn=administrators	Matacenter	Solution domain controller solution domain controller	III ms-rdp III t.120	0	none
	Safe Web Browsing	🚧 datacenter	any	S cn=finance,cn=us	(22) corporate	any	web-browsing	0	
_	+ Add - Delete C	Clone 🖌 Enabl	le 💿 Disable	S Move Top Mov	e Up 💽 Move Do	own 💿 Move Bottom	Highlight Unused Rules	_	3 rule(s)
	coxadmin Logout								: 🧑 Lasks

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.

		Vir	tual System <mark>c</mark>	itrix	~				Manua	al 🔽 🤇	Э 🕢 н
🔍 (ad	ldr.dst im	==)								→ × + (R 🛱
	Receive Time	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Byte
p	09/24 17:44:31	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	25
Þ	09/24 17:44:31	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	6
p	09/24 17:44:31	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	14
Þ	09/24 17:44:31	trust	untrust	1000	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	9
Þ	09/24 17:43:29	trust	untrust	-	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	20
Þ	09/24 17:43:28	trust	untrust	-	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	27
Þ	09/24 17:43:26	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	10
Þ	09/24 17:42:53	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust	7	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust	-	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust	-	citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	
Þ	09/24 17:42:53	trust	untrust		citrixdemo\citrix02	208-80-56-11.clickability.com	80	web-browsing	allow	anyanyallow	



Source User ctrixdemoljoe 🗵

3.9

ML Filtering								
	Category	Sessions	Bytes					
1	search-engines	17	294.8 K					
2	internet-portals	11	542.8 K					
3	computer and internet security	9 💴	540.4 K					
-4	business and economy	6 🖬	17.4 K					
5	online-gambling	5 💷	4.3 K					
6	unknown	4 🖬	115.9 K 🔤					
7	streaming-media	1	3.3 K					

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.

Palo Alto Networks, "The Network Security Company," the Palo Alto Networks Logo, App-ID, GlobalProtect, and WildFire are trademarks of Palo Alto Networks, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

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. ©2012 Citrix Systems, Inc. All rights reserved. Citrix® and NetScaler® are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.