

Stoneware webNetwork Powered by ThinkServer

Solution Guide

Lenovo Enterprise Product Group

Version 1.21

May 2013

©2013 Lenovo. All rights reserved.



LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. This information could include technical inaccuracies or typographical errors. Changes may be made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The following terms are trademarks of Lenovo in the United States, other countries, or both: Lenovo, and ThinkServer.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft, Microsoft Windows Server, and the Windows Logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Contents

Introduction.....	5
webNetwork Unified Cloud Solutions Overview	5
Benefits of the webNetwork Unified Cloud	6
webNetwork Solution Architecture.....	7
Introduction.....	7
Architectural Overview.....	7
webNetwork Solution Hardware Components	11
ThinkServer RD330 Hosts	11
Summit X440 Switch.....	12
Network Architecture.....	12
webNetwork Solution Software Components.....	14
webRelay and webNetwork Servers.....	14
Directory Services.....	15
Solution Security.....	15
Performance Considerations.....	18
Exposing Private and Public Cloud Resources	21
webNetwork Integration with LanSchool Distance Learning	24

List of Figures

Figure 1 – Multi-tenancy	6
Figure 2 – Example of simple architecture with one combined internal webNetwork Server / webRelay Server	8
Figure 3 – Example of “true” dual firewall DMZ architecture with one combined internal webNetwork Server / webRelay Server, and one dedicated public webRelay Server	9
Figure 4 – Example of load balanced external webRelay Servers	9
Figure 5 – Example of load balanced internal and external webRelay Servers and clustered webNetwork Servers	10
Figure 6 – Example of fully clustered and independent redundant webRelay Servers	10
Figure 7 – webNetwork Network Architecture	13
Figure 8 – webRelay and webNetwork Server Two-Tier Architecture	14
Figure 9 – Directory Services authentication of end user requests for service	15
Figure 10 – Security Architecture	16
Figure 11 – webNetwork Authentication Methods	17
Figure 12 – webNetwork Clustering	18
Figure 13 – webNetwork Load Balancing	19
Figure 14 – webNetwork Failover	20
Figure 15 – webNetwork Quality of Service	21
Figure 16 – LanSchool Connection Server in webNetwork	25

List of Tables

Table 1 – webNetwork Host Configurations	11
Table 2 – webNetwork Supported Application Types	22
Table 3 – webNetwork Unified Cloud Services	22

Introduction

This document describes the webNetwork Unified Cloud solution by Stoneware, a Lenovo company, and provides guidance for deploying and configuring this solution in an enterprise. The audience for this document is IT administrators and managers, as well as channel partners planning to evaluate or deploy the webNetwork solution using Lenovo servers and networking equipment from Lenovo partners.

This document covers the solution architecture, and factors that should be considered when implementing the solution. It describes several reference configurations that, depending on specific customer needs, can be used as a base for deployment in a customer environment.

We provide an overview of the recommended servers, networking, and software required to implement the solution, and this information can be used to plan, and procure the required components to set up the solution. Based on specific customer requirements, further customization of the solution may be required. Services available from Lenovo can help customers in this regard.

webNetwork Unified Cloud Solutions Overview

Information Technology has evolved into three separate islands of automation and isolation: 1) the *private cloud* comprised of files, applications, and services in your data center, 2) the *public cloud* comprised of files, applications and services outside your organization, and 3) the many applications and files that remain on *end user's devices*. While cloud computing is changing nearly every aspect of how computer applications and data are delivered, end users still want simplicity while accessing their IT services from multiple devices, and IT administrators still need to manage and control the delivery of services while maintaining appropriate security policies.

Stoneware's webNetwork platform meets these requirements, by enabling organizations to create a Unified Cloud where files, applications and services from public and private clouds, and even individual devices, can be accessed through a single web-based interface with a single password.

webNetwork provides secure web access to applications and data, from anywhere, using any device, without requiring VPN's. The solution allows organizations to create their own "private" cloud that is hosted on site using their own servers and storage, and secures the data center by isolating devices from it.

Applications are intelligently delivered through a context aware browser-based desktop that understands and utilizes device capabilities appropriately. It provides the user with seamless access from any device with browser capability to Web based applications, published (e.g. Windows Terminal Services, Citrix, or VMware), virtualized or local Windows applications, and local and remote files. It allows delivery of applications and services to end users without having to recode or change existing infrastructure or application stacks.

webNetwork enables management of applications and services delivery based on predetermined parameters set by the administrator. Service delivery can be defined based on specific user groups, device type, location, device and network capabilities, and context. Service delivery can also be managed based on application requirements. If a user is attempting to access a given application, but has a poor quality connection, webNetwork can default to a lower bandwidth application or services option.

Benefits of the webNetwork Unified Cloud

Organizations of all sizes that are looking to provide a cloud based remote access solution that provides strong security without significant complexity or expense will benefit from webNetwork. Customers in all business segments, including education, government, and healthcare, have decreased IT costs by delivering services in a scalable, web-based cloud platform that easily scales to thousands of concurrent users. webNetwork has also proven itself as a viable, cost effective alternative to "Virtual Desktop" environments (VDI), and because webNetwork delivers IT services through a web interface, webNetwork can easily support the growing number of "Bring Your Own Device" (BYOD) environments.

webNetwork's security architecture also reduces the need for gateway appliances and firewall modifications, and can easily enable employees', partners', and vendors' access to internal resources without granting access to the internal network. Access to resources is easily granted or removed by controlling user's directory rights.

A unique multi-tenancy capability is also ideally suited for Hosted and Managed Services Providers (MSP's) who want to offer solutions to their customers. Multi-tenancy enables MSPs to manage multiple customers through a single instance of webNetwork (see Figure 1). Tenants receive a unique login page with their own custom profiles.

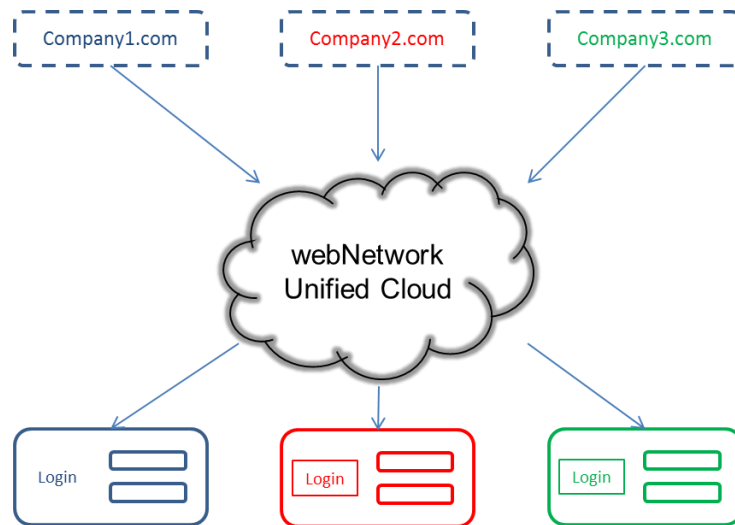


Figure 1 – Multi-tenancy

Stoneware's LanSchool has also been integrated into webNetwork's Unified Cloud to deliver classroom management from the cloud. Organizations can provide classroom management for distance learning students who are connecting to the cloud in either a Bring Your Own Device, or a traditional classroom setting.

webNetwork Solution Architecture

Introduction

The webNetwork Unified Cloud solution consists of webNetwork server software running on Lenovo ThinkServer Servers, interconnected with Extreme Networks switching equipment. While the webNetwork system necessarily interfaces with other application and infrastructure servers in the data center to create the overall solution, the data center servers are beyond the scope of this paper and are not addressed here.

This section describes the solution elements required to connect users with the IT resources available in the data center to include the webNetwork Servers, and LanSchool Distance Learning Connection Servers.

Several reference configurations are shown to demonstrate various capabilities of the solution, and how it can scale as an organization's needs evolve. The reference configurations offer specific choices for hardware and networking, but the hardware is general purpose, and a wide range of configuration options are possible.

The webNetwork solution can begin with support for small numbers of users with a single server, and grow into a full enterprise system supporting thousands of users in a predictable and modular fashion. The solution scales easily without forfeiture of previous investment in software or hardware.

Architectural Overview

webNetwork is architected as a two-tier server-based solution that is written in Java, and is capable of running on any operating system platform including Windows 2003, Windows 2008, Linux (SuSE, Redhat, Ubuntu), and Mac OS X, installed on either physical or virtual servers. The system is divided into two components, the "webRelay Server" and "webNetwork Server," and these integrate with other servers in the data center.

While webNetwork can be installed on one server for small or trial implementations, it is usually installed on a minimum of two servers in the private data center.

The decision to implement a single or multi-server configuration will be based on several factors including number of concurrent users, solution performance, security concerns, as well as cost.

For smaller organizations, where it is impractical to deploy a multi-server configuration due to the additional hardware expense, a basic single server installation running both the

webNetwork Server and webRelay (on the same host server) can be utilized as shown in Figure 2.

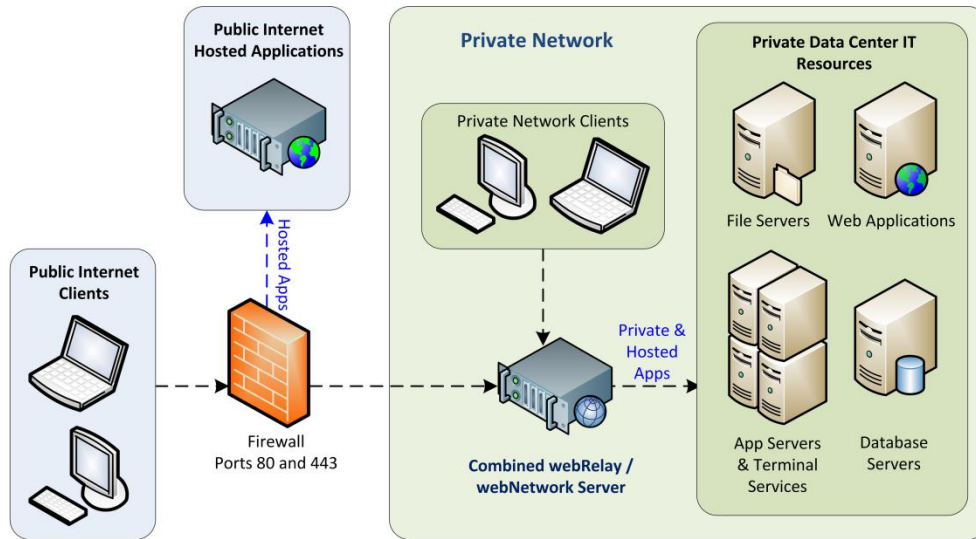


Figure 2 – Example of simple architecture with one combined internal webNetwork Server / webRelay Server

As the webNetwork System grows, it can be reconfigured into a two-tiered configuration without additional licensing expense.

For larger organizations, and when increased performance and security are important, a two-tier configuration (with at least a dedicated webRelay Server and a combined webNetwork Server / webRelay) is highly recommended as shown in Figure 3. The two-tiered nature of webNetwork allows it to easily be deployed within a “true” dual firewall DMZ architecture providing additional security and flexibility. The two-tiered implementation is always recommended when maximum security is a priority.

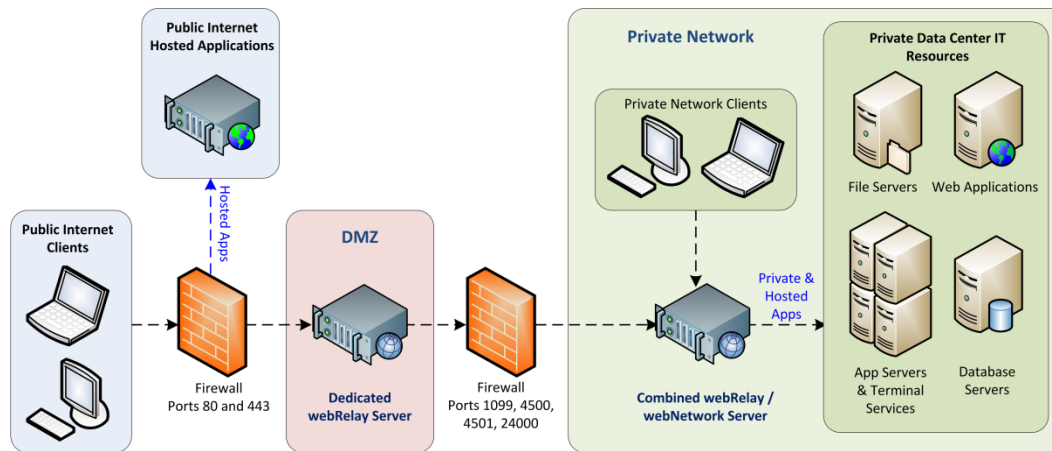


Figure 3 – Example of “true” dual firewall DMZ architecture with one combined internal webNetwork Server / webRelay Server, and one dedicated public webRelay Server

Additional webRelays and webNetwork Servers can be added to scale support for more users. There is a one to many relationship between the webNetwork Server and the webRelay Server. Multiple webRelays can be configured to access a single webNetwork Server. This configuration allows the webNetwork system to scale, to build redundancy in the relay process, and to create flexibility allowing the system to adapt to the customer's network environment.

To handle even greater numbers of concurrent users, one combined internal webNetwork Server / webRelay Server can be used with two dedicated public webRelays (see Figure 4). This configuration is useful for load balancing between DMZ webRelay Servers. A hardware load balancer to balance the load between the webRelays is recommended for maximum flexibility and performance.

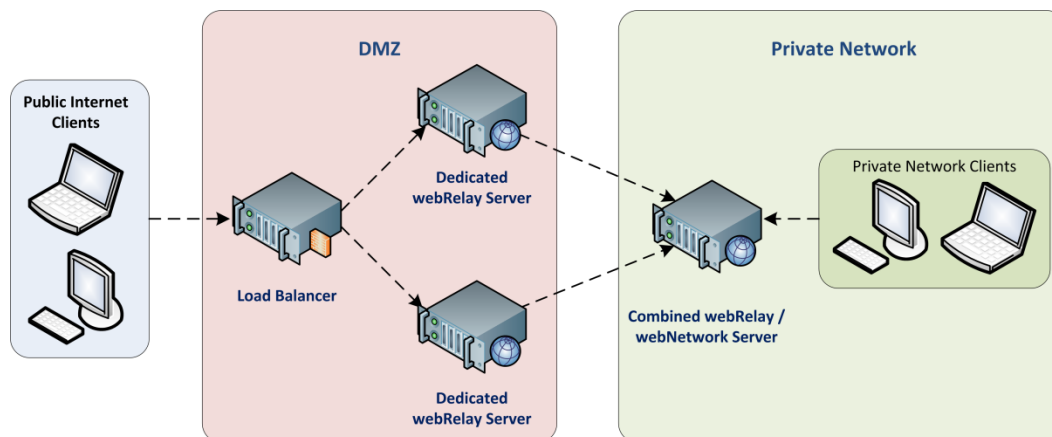


Figure 4 – Example of load balanced external webRelay Servers

The addition of another combined internal webRelay / webNetwork Server is useful for load balancing both Internal and DMZ webRelays (see Figure 5). This configuration also allows clustering the webNetwork Servers to provide failover capability, increasing reliability of the solution.

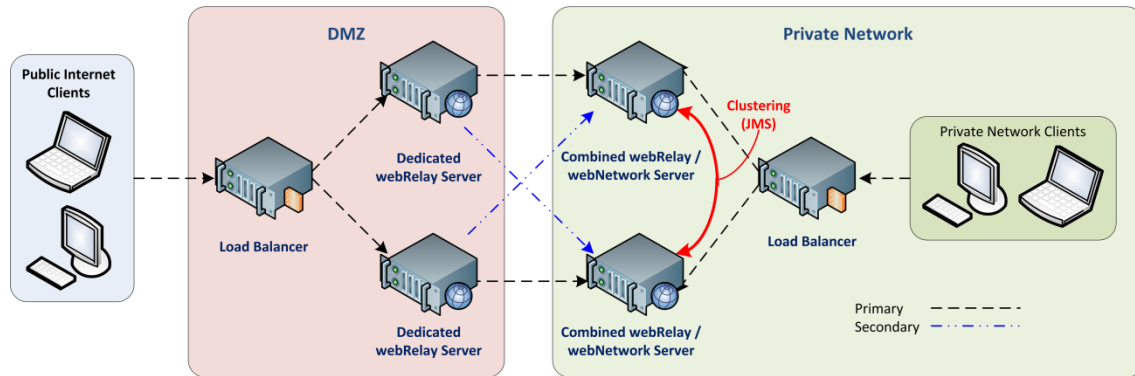


Figure 5 – Example of load balanced internal and external webRelay Servers and clustered webNetwork Servers

Finally, a configuration with two dedicated internal webNetwork Servers, two dedicated internal webRelay Servers, and two dedicated public webRelay Servers (six physical/virtual servers) can provide for fully-meshed clustered servers, and independent redundant internal and DMZ webRelays to provide the ultimate in reliability and performance (see Figure 6).

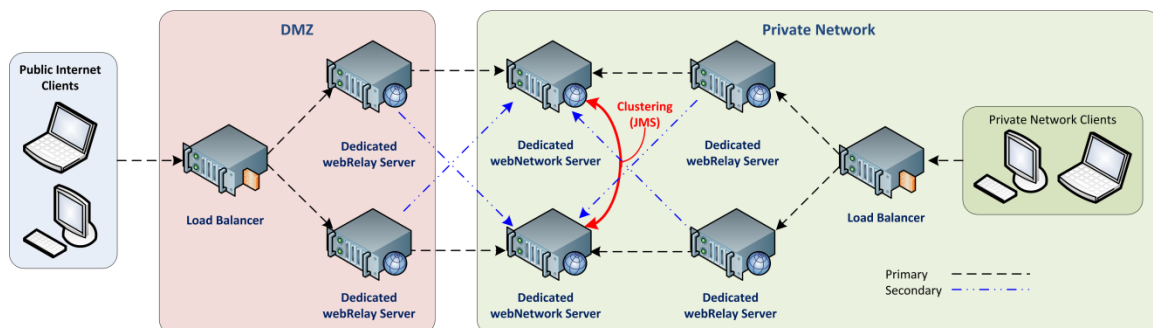


Figure 6 – Example of fully clustered and independent redundant webRelay Servers

webNetwork Solution Hardware Components

ThinkServer RD330 Hosts

The Lenovo ThinkServer RD330 rack server is selected for use with webNetwork to provide optimal solution performance at the lowest cost per user. The RD330 provides powerful choices to meet



demanding enterprise needs while offering outstanding value in a 1U chassis. Supporting two of the latest Intel Xeon E5-2400 processors, the ThinkServer RD330 can provide outstanding enterprise-grade performance, built-in redundancy, and excellent reliability for large or small deployments. Nicely configured, these servers come standard with Web-based remote management, integrated power management, rail kits, hardware RAID, and EasyManage tool-suite for unbeatable value.

The Server hardware configurations for the webNetwork solution are based on the assumption that the servers are dedicated to the webNetwork workloads.

In the webNetwork solution, the webRelay, and webNetwork roles execute from local storage on each server. While local disk requirements are constant, memory is sized to provide approximately 1 MB of RAM per user session above that required by the Operating System and the webNetwork applications. Additional RAM can be added to the system and dedicated to webNetwork further increasing system performance and user experience.

Table 1 provides hardware recommendations based on the number of simultaneous users of the system. Additional users can be supported by adding more servers as needed.

Table 1 – webNetwork Host Configurations

Node	webRelay / webNetwork Servers (for up to 1500 Users)	webRelay / webNetwork Servers (for up to 4500 Users)
Platform	ThinkServer RD330	ThinkServer RD330
Operating System	Microsoft 2012 Server Essentials	Microsoft 2012 Server Essentials
CPU	1x Intel Xeon E5-2407 Quad Core Processor (2.2 GHz)	2x Intel Xeon E5-2407 Quad Core Processor (2.2 GHz)
RAM	4GB Memory (1x 4GB DIMM)	8GB Memory (2x 4GB DIMM)
RAID Controller	1x Lenovo RAID 500 adapter	1x Lenovo RAID 500 adapter
HDD	2x 500GB Enterprise SATA Drives (RAID 1)	2x 500GB Enterprise SATA Drives (RAID 1)
Network Controller	2x Integrated Intel 1Gb Ethernet NICs	2x Integrated Intel 1Gb Ethernet NICs
Platform Management	TMM Premium	TMM Premium
Power Supplies	2x 800W PSUs	2x 800W PSUs

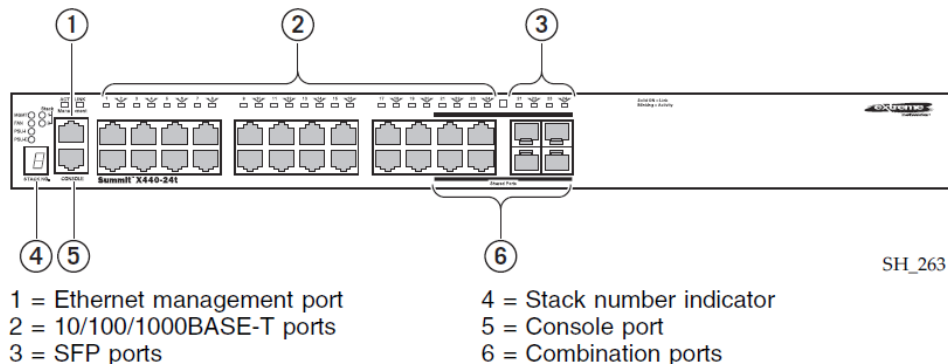
Summit X440 Switch

The Extreme Networks Summit X440 series switches provide Layer 2 and Layer 3 switching on 8, 24, or 48 Ethernet ports delivering high-density Gigabit Ethernet connectivity using fixed 10/100/1000BASE-T ports. X440 switches include enterprise grade features, such as support for Ethernet Automatic Protection Switching (EAPS) resiliency protocol, and Quality of Service (QoS) advanced traffic management for converged applications. A robust, modular operating system helps ensure uptime with process isolation, monitoring and automatic restart. The switches can be stacked reducing management overhead by combining multiple switches into a single logical unit.

Additional port types are supported on various models include the following:

- Four 1000BASE-X SFP ports on all eight-port models
- Four combo (copper/fiber) ports on all 24 port models
- On 48 port models, four combo ports on the x440-48p, x440-48t, and x440-L2-48t, and two combo ports on the x440-48p-10G and x440-48t-10G
- Two 10G BASE-X SFP+ ports on two of the 24 port models, the x440-24p-10G and x440-24t-10G, and two of the 48 port models, the x440-48p-10G and x440-48t-10G

For all models, a serial console port on the front panel allows you to connect a terminal and perform local management. An Ethernet management port can be used to connect the system to a parallel management network for administration. Alternatively, you can use an Ethernet cable to connect this port directly to a laptop to view and locally manage the switch configurations.



Network Architecture

In nearly all cases, the webNetwork solution will be integrated into an organization's existing network infrastructure. To highlight the key considerations when integrating with the network, consider the reference configuration of load balanced internal and external webRelay servers and clustered webNetwork servers as shown in Figure 5. The network architecture for this configuration in a single location is shown in Figure 7.

Because of the nature of the network traffic between the webNetwork servers, application servers, and clients themselves, the network is setup to use a minimum number of VLANs that span across multiple switches, keeping the network as flat as possible. This example assumes all Top of Rack (ToR) network traffic is designed to be layer 2 and is switched locally without using VLANs. All layer 3 traffic routed through a core or distribution switch. External users connect to the network through the Internet facing firewall to the DMZ, and their traffic is directed to a load balancer (not shown in the diagram) and sent to the proper webRelay Server. Similarly, internal users are directed to an internal load balancer and then to the internal webRelay servers.

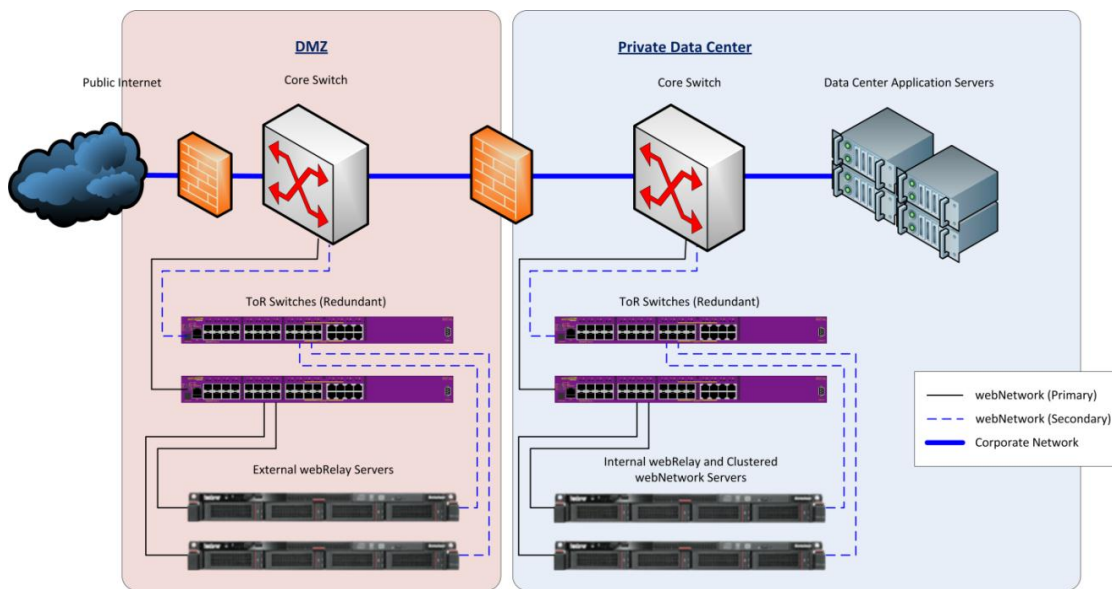


Figure 7 – webNetwork Network Architecture

Each webRelay server and webNetwork server is connected to a Summit X440. A second switch can be added for redundancy (as shown) using active failover links. An optional method of increasing resiliency to the core network is to use Extreme Networks' SummitStack technology to create separate virtual switches. Each of the webRelay servers are configured to communicate with the LAN firewall in order to reach the data center application servers, and are connected to a core switch of their respective network segment (either the DMZ or Private Network).

Each webRelay and webNetwork server has two integrated 1Gbps Ethernet NICs that provide the primary and secondary network paths. Optional 1Gbps or 10Gbps Ethernet NICs can be added and NIC ports can be teamed to provide additional bandwidth and resiliency. Server management traffic is connected via a dedicated management port on the servers, and can be segregated onto a separate VLAN if desired.

webNetwork Solution Software Components

This section describes the software components of the webNetwork solution, and describes the key attributes available for optimizing the solution performance and security.

webRelay and webNetwork Servers

The relay / server two-tier architecture provides secure access to applications and resources published within the webNetwork Unified Cloud. The webRelay and webNetwork Servers are architected to run separately allowing the internal applications and services to be isolated from the external users requesting the resources (see Figure 8).

The webRelay can be strategically positioned within any existing network infrastructure (e.g. inside the DMZ, outside the firewall, or internal to the datacenter), but it is designed to run inside the DMZ.

The webRelay, located in the DMZ, creates a secure entry point into the webNetwork system and requests applications and services on the behalf of the end user, ultimately rendering the Virtual Web Desktop. By isolating users to the webRelay, you are ensuring that they do not have physical access to the private network.

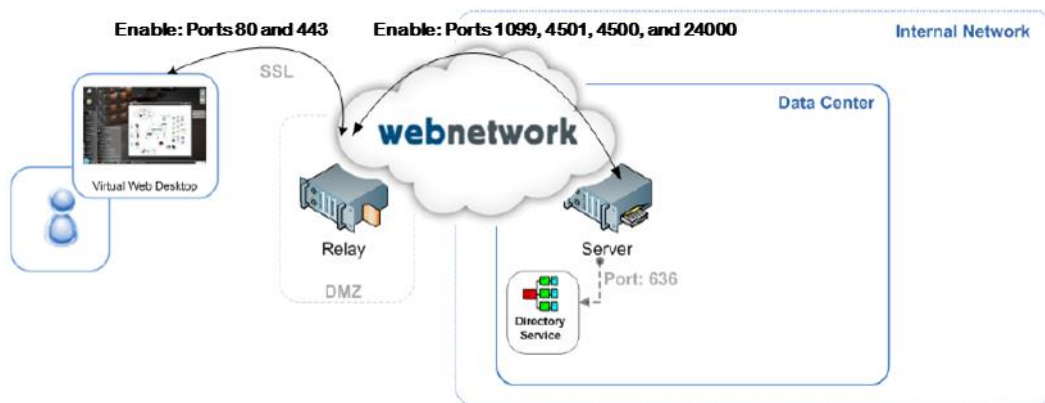


Figure 8 – webRelay and webNetwork Server Two-Tier Architecture

The webNetwork servers, designed to run inside the data center, receive the user requests from the webRelay. From their trusted position, the webNetwork servers communicate with the network directory service to evaluate the requests based on the user ACL (Access Control List), then forward the user requests to the appropriate internal application server and provide the response to send back to the browser via the webRelay.

Directory Services

The webNetwork solution utilizes an organization's existing directory services and user management processes to control access to cloud applications and services without requiring another account management approach to be used.

All requests for service are forwarded to the webNetwork Server, which validates the user's credentials (username and password) against the directory service. The user's credentials must be validated by the directory service prior to accessing any webNetwork application or resource (see Figure 9). Only those applications, services, and content that have been assigned to a user's account will be presented in the web desktop.

webNetwork also utilizes the Directory Service as the primary system "database." It must therefore modify the directory service tree extending existing class objects (i.e. users, groups, containers) and adding new objects classes that represent configuration items (i.e. menus, links, and web applications).

webNetwork integrates with popular directory service products including Microsoft Active Directory, Novell eDirectory, OpenLDAP, and Open Directory.

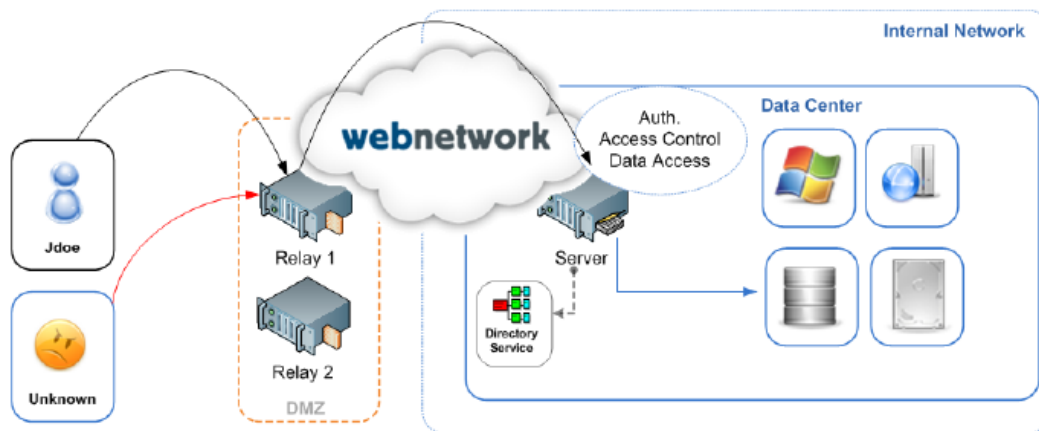


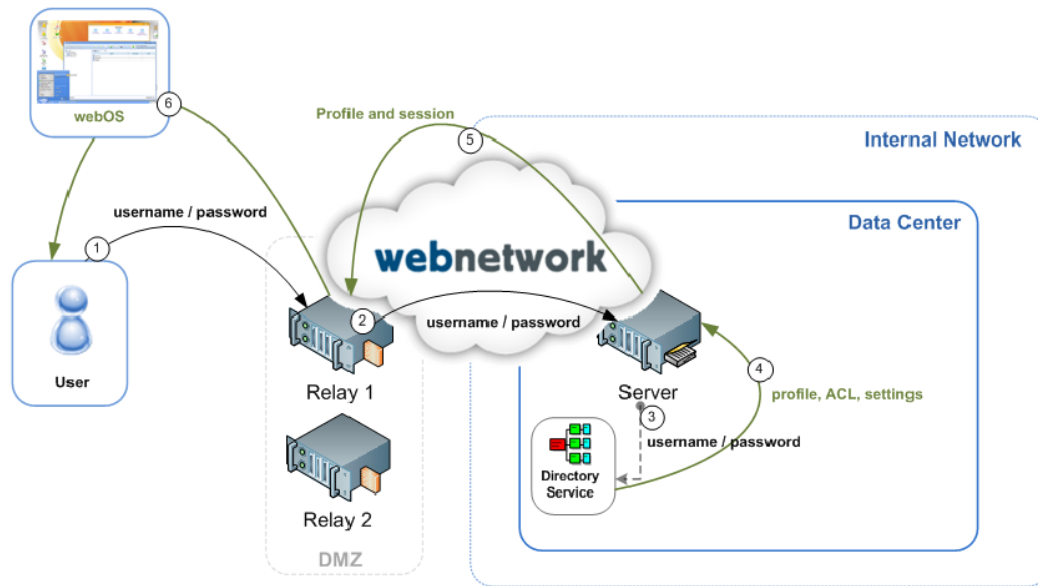
Figure 9 – Directory Services authentication of end user requests for service

Solution Security

A core aspect of the webNetwork solution is that cloud applications and services are properly secured and controlled. Security within the system is comprised of several key elements:

- Two-tier Server/Relay architecture
- Authentication
- Access Control
- Encryption

This section discusses the aspects of security within the architecture and the role each plays in the webNetwork system. Figure 10 depicts the data flow for a user accessing the webNetwork system and shows how these security features are used.



The user submits their credentials to the webNetwork Relay (1). The relay forwards the authentication request to the webNetwork Server (2) which will submit the credentials for validation from the directory service (3). If the credentials are valid, the webNetwork server will build the user's session (4) which will include their profile information, assigned links, and components (ACL), and other specific account settings. The profile and session are sent to the webNetwork Relay where the interface is rendered based on the user's profile settings (5). The relay will build the interface that is dynamically delivered into the user's web browser (6).

Figure 10 – Security Architecture

Two-tier architecture

As described earlier, the system design forces all users' requests for access to internal applications to be redirected by the webNetwork Relay to the webNetwork Server inside the data center. Only the webNetwork Server communicates directly with application servers to fulfill the request. This design requires only a single port to be opened through the internal firewalls. This simplifies deployment by eliminating the large number of firewall rule exceptions that might otherwise need to be created.

Authentication

Each user must authenticate to the system before they are allowed to consume webNetwork services or applications. Multiple authentication methods are supported in the webNetwork security architecture. Users can authenticate with their network username and password,

utilizing the organization's existing directory service to act as the authority for all authentication requests (a first factor). Security can be enhanced by utilizing various two-factor authentication methods including fingerprint scanners using one-time passwords. Through a login policy, the webNetwork system can require a “second” factor of authentication, including:

- Secure Tokens (e.g. - SecurID, ActiveCard, etc.)
- USB Keys (e.g. - USB storage devices, thumb drives, etc.)
- Directory Attributes (e.g. - workforce ID, employee number, etc.)

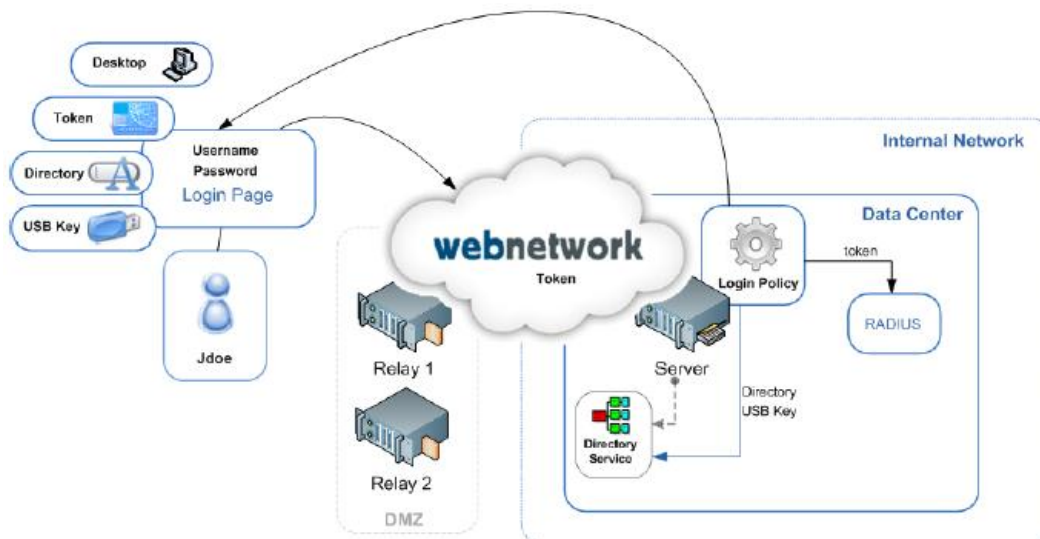


Figure 11 – webNetwork Authentication Methods

Access Control

Simply authenticating to the system does not provide the user with the necessary rights to consume resources. Each application or service exposed through webNetwork must also be managed with regards to access. When a user is added to the system, the user is associated with only cloud resources and applications they are allowed to access. The directory service is leveraged to assign rights directly to the user, group, or any organizational container, enabling access to be controlled by a user's role within the organization.

When a user authenticates to the system, the webNetwork Server creates an Access Control List (ACL) for the user. The Access Control List is maintained as part of the user's session, and contains a list of all accessible applications and resources. Only those authorized resources are displayed in the web desktop.

Encryption

All communications between the end user and the webNetwork cloud, regardless of what the end user is accessing, are encrypted by the webNetwork Relay using Secure Socket Layer (SSL) encryption.

Performance Considerations

webNetwork is also designed to enhance performance and reliability of the solution. This section describes features to support this including clustering, application server load balancing and failover, and quality of service (QoS).

webNetwork Server Clustering

Two or more webNetwork Servers can be joined in a cluster to share session and configuration information to provide additional fault tolerance within the system. Clustering operates in “Active” / “Active” mode, meaning that all servers are fully functional and respond to requests in the cluster configuration.

The webNetwork cluster uses Java Messaging Service (JMS) to communicate user session information, and the cluster configuration between servers (see Figure 12). If a webNetwork Server fails, the webRelays communicating with the webNetwork server will automatically connect with another server in the cluster. When the webNetwork Server rejoins the cluster, all current session information, and the cluster configuration information will be sent to the server.

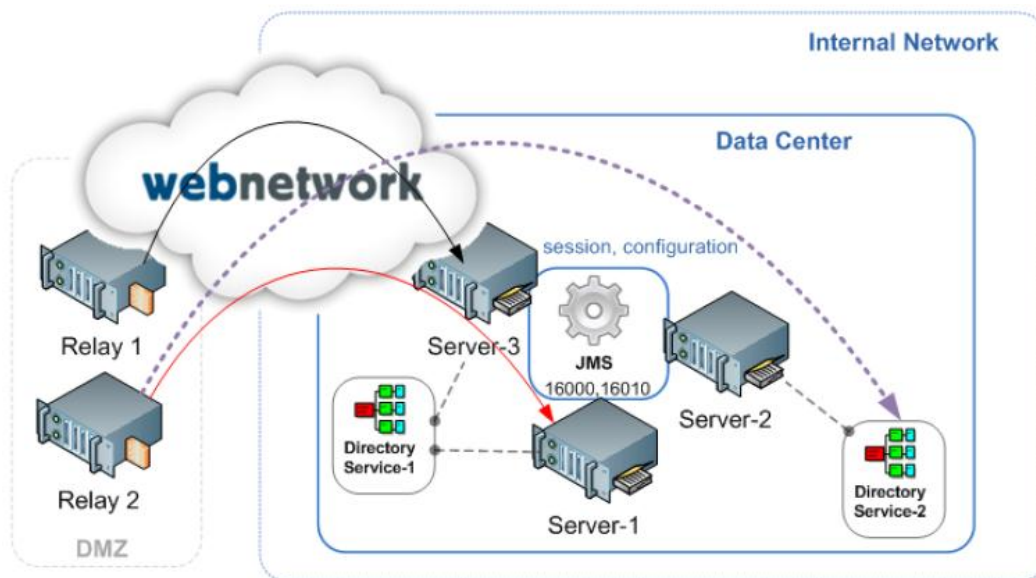


Figure 12 – webNetwork Clustering

Application Server Load Balancing

Application Server Load balancing is a feature of webNetwork designed to provide both scalability and fault tolerance within the webNetwork system. This feature allows access to backend application servers to scale more efficiently, and provides end users with better performance by not overloading a single application server.

Load balancing balances the number of users connecting to two or more backend application servers (e.g. mail-1 and mail-2 in Figure 13) running within the webNetwork system. The

webNetwork Server tracks the number of users accessing each backend application server and balances the number of user sessions between servers. If one application server loses a number of sessions, webNetwork will attempt re-balance the session between the backend servers.

Load balancing is not performed “round robin” based on user requests. Instead, application servers are loaded by the number of user sessions. Balancing requests would break in most deployments because backend servers are typically not clustered at a session-level. No agent is installed on the backend application server. webNetwork will always attempt to balance the same number of sessions across servers.

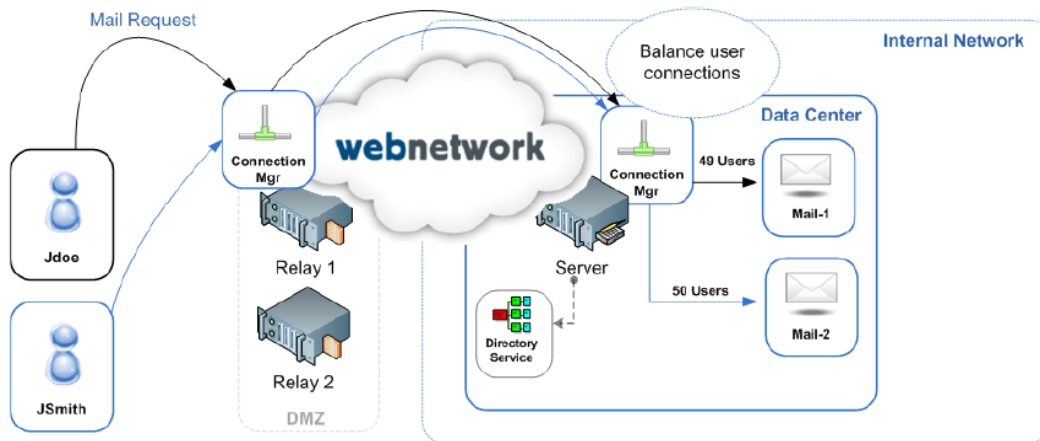


Figure 13 – webNetwork Load Balancing

Application Server Failover

In the event that a backend application server stops responding to requests from the webNetwork system, failover automatically determines where users will be redirected. This provides greater uptime to an application that has been configured on two or more servers.

When two or more servers are assigned to an application, the webNetwork server will validate the application server is responding before sending a user to the application. If the application server fails to respond, the webNetwork server will send the user's connection request to one of the remaining application servers (see Figure 14). Once the failed server returns to service, the webNetwork server will return to the process of load balancing user sessions.

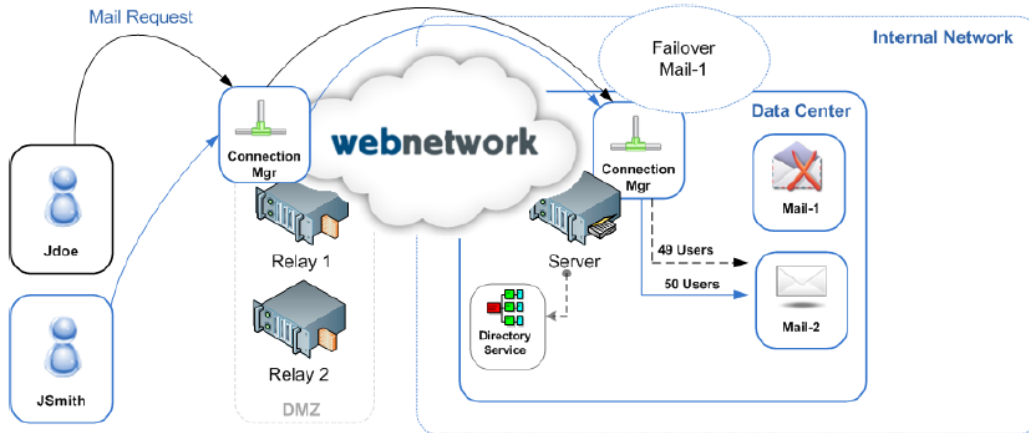


Figure 14 – webNetwork Failover

Quality of Service

webNetwork provides a method to enable the system to communicate with the underlying network infrastructure to direct Quality of Service (QoS) for application delivery. The quality of service setting allows administrators to determine network performance and reliability settings for a specific application, user, group, or container configuration by:

- assigning minimum bandwidth thresholds to specific applications or users
- throttling user bandwidth based on application
- guaranteeing the reliability of the connection between the user and the system
- prioritizing applications performance within the network

When the quality of service is set, the webRelays will read the setting on the configuration object and apply the setting to the outbound TCP packets. The Extreme switches will read the settings and implement the desired flow control by assigning a higher or lower priority to the data traffic. Bandwidth reservations for special traffic groups are also possible, to restrict or accelerate data rates for the specific data type.

As shown in Figure 15, the administrator can set a different quality of service on each application therefore prioritizing the importance of various services.

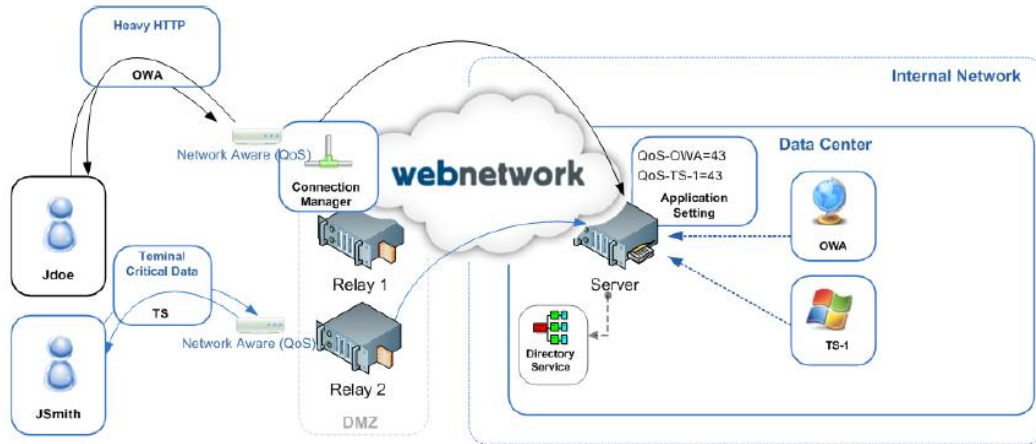


Figure 15 – webNetwork Quality of Service

Exposing Private and Public Cloud Resources

WebNetwork allows organizations to deliver thousands of in-house and third party applications from their Unified Cloud framework. The supported application types are described below in Table 2. Intelligent Application Delivery can dynamically select which delivery method (local to the device, from the public or the private cloud) is most appropriate based on restrictions set by the administrator. This feature allows webNetwork to deliver applications based on the context of both the user and device.

Table 2 – webNetwork Supported Application Types

Application Type	Description
Private Web	HTTP/HTTPS web applications including: .NET, Apache, WebSphere, portals, SharePoint, PHP, Flash, etc.
Public Web	HTTP/HTTPS web applications hosted over the Internet
Hosted Web (SaaS)	specific integration to a growing number of Software as a Service applications including Zoho, Google Docs, Zimbra, Salesforce.com, Apple iTunes U, etc.
Local Applications	Ability to launch applications located on the local device from the web desktop. Supports Windows, Linux, Mac OS X, Android (Cloud Agent), and some iOS applications.
Windows (Terminal Server)	Windows applications published via Terminal Server
Windows (Citrix Server)	Windows applications published via Citrix Presentation Server
Windows (Virtualized Applications)	Windows applications virtualized via Thinstall, Xenocode, InstallFree, App-V, XenApp, etc.
Client-Server (VPN & Proxy)	Applications that communicate over non-HTTP protocols (e.g. database applications, emulators, etc.)
Telnet (VPN & Proxy)	Applications and sessions that communicate to backend telnet servers
VNC (VPN & Proxy)	Servers and clients that implement any variation of VNC (Virtual Network Computing) for remote control
Remote Desktop (Windows)	Applications made available on remote Windows desktops via RDP

webNetwork also provides a rich set of cloud services that integrate an organization's entire IT infrastructure, not just the applications. Table 3 provides a list of services available and a brief description of each. Cloud Services are designated as running on either the webNetwork Server or the webRelay Server. This information is important when designing the deployment of services and planning for the associated network traffic.

Table 3 – webNetwork Unified Cloud Services

Cloud Service	Description	webNetwork Server	webRelay Server
File Services	Provides users access to internal network file systems through the webOS, portal, or mobile interface. With File Services, users can access shared, home, and public directories from anywhere they have an Internet connection. File Services supports features such as drag/drop, local edit, copy/paste, etc.	x	
Report Services	Designed to allow administrators to build, secure, and distribute dynamic database reports throughout the organization. webNetwork's Report Services is unique in that it leverages an organization's investment in Identity Management to build, secure, and distribute critical business information to the people who need it. Supports most ODBC/JDBC databases.	x	

Cloud Service	Description	webNetwork Server	webRelay Server
Form Services	Allows organizations to create their own web-based forms for the collection and presentation of information to both internal and external users. Form Services are designed for the non-developer, enabling webNetwork administrators to build and distribute web forms throughout the webNetwork cloud. Organizations will find the ability to create ad-hoc web forms for collecting information from customers, employees, and the public.	x	
Personal Desktop	A feature designed to connect a user with his office desktop when working from home or on the road. Personal desktop provides users with access to files, documents, reports, and applications sitting on their personal desktops that may not be practical to publish in the webNetwork cloud.		x
Registration	A self-service feature allowing users to register their own system account. Supports CAPTCHA, directory integration, and can be customized to validate against 3rd party databases.		x
Self Service	Set of applications that enable users to manage their own system account.		x
Password Self Service	Allows users to reset their forgotten passwords. Challenge/Response system requires users to answer a set of challenge questions before password reset. Supports immediate reset or emailed activation link.	x	
Document Publishing	Feature that enables users to publish and share documents with other system users. Ideal for departmental sharing of documents. Features include PDF conversion, check-in/check-out, etc.		x
News and Alerts	Provides users with news and alert messages based on their role within the organization. Administrators are able to easily notify all or specific users of corporate events, departmental notices, or system maintenance.		x
Login Scripts	Login Scripts allow the administrator to change the login process for any user by adding simple script commands. Login Scripts dynamically change the user's login based on conditional logic created by the organization.		x
Forums	Application designed for the discussion of ideas. The forums provide the end user with a means of presenting an idea and then monitoring the feedback from other users with regards to the idea.		x
Blogs	A blog is an application designed to support regular entries of commentary. Blogs are widely used both personally and in group settings to journal and comment on specific issues, ideas, thoughts, or events.		x
Polling	A community service application that allows an organization to query end users for information and opinions. Polls can be created for the purpose of taking surveys, requesting feedback, voting on issues, or collecting user opinions		x
teamPages	Provides organizations with a collaborative web interface by which end users can share information in an Intranet or Extranet setting. With teamPages, organizations can turn group of network users into a "team" with just a click of a button. teamPages is perfect for organizations who needs to share information or collaborate with people as part of their job.	x	

Cloud Service	Description	webNetwork Server	webRelay Server
webPages	A vertical specific application designed to provide schoolteachers with a simple means of publishing content and information to parents and students. webPages provides a “template” system by which teachers can provide valuable information to their class without becoming an HTML editor or web page designer. webPages simplifies the process of moving content online by providing a common “look and feel” across an entire school district and allowing teachers to rapidly publish educational information.	x	
Push Console	Advanced web technology that allows administrators to “push” events out to the user's web desktop. With no client or plug-in code required, the push console can automatically start applications, send messages, lock the web desktop, open web sites, log user off the system, etc.		x
Calendaring	Enables the sharing of personal and group calendars with other users accessing the webNetwork system. Supports features such as email notification, event approval, and integrates with the Groupware Agent.		x
Mail, Tasks, and Contacts	Integrates a user's mail messages, tasks, and contacts into the webOS and portal web desktops. Leverages the Groupware Agent to integrate a user's organizational messaging system.		x
Groupware Agent	An enhancement pack to the community service applications that provides enterprises with the ability to integrate their collaborative systems into their webNetwork environment. Groupware agent supports both Microsoft Exchange and Novell GroupWise		x
External Users	Allows organizations to provide external users and groups with access to webNetwork resources without creating these accounts in their production network environment. The External User feature federates a secondary directory to store non-organizational accounts (e.g. vendors, customers, public, etc.) which reduces licensing costs and improves account security.		x
Folder Monitor	Integrated File Services feature designed to automatically scan a file system directory on a local workstation and move its contents to a backend network file system.		x
Network Aware Cloud Services	Integration with network vendors to control the quality of service based on the user or the IT service. webNetwork administrators can control the bandwidth allocated or priority of network service based on the applications being accessed through the webNetwork private cloud. Feature enables the creation of very scalable and efficient private cloud platforms.		x

webNetwork Integration with LanSchool Distance Learning

LanSchool is classroom management software for demonstrating concepts, monitoring students' progress, and removing distractions in the classroom.

LanSchool has been integrated with webNetwork cloud technology, enabling organizations to provide classroom management and distance teaching delivery from the Cloud. Students can bring their own devices (BYOD) into the classroom environment. During class, the instructor can

manage the students' devices, but when the student leaves the class, the device returns to its original state under the student's full control.

Students can be located anywhere in the world as long as Internet connectivity is possible with the webRelay server.

An optional LanSchool Connection Server simplifies deployment, reducing the need for configuration changes to routers and wireless access points to support wired or wireless environments and VLANs inside an organization, facilitating the connection between student devices and the LanSchool Teacher Console (see Figure 16). LanSchool Distance Teaching leverages webNetwork's unique two-tier security architecture to provide secure, end-to-end access to the LanSchool Connection Server for students over the Internet.

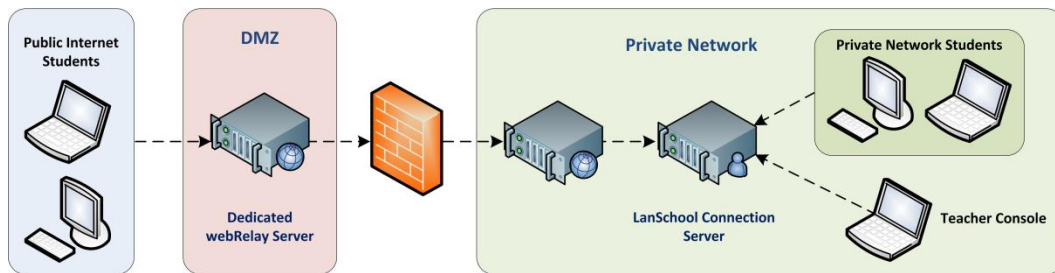


Figure 16 – LanSchool Connection Server in webNetwork

The LanSchool Connection Server also supports a hybrid environment that allows local clients in a peer-to-peer mode along with distance students accessing the classroom through the cloud.

The LanSchool Teacher Consoles are required to be inside the internal network to communicate directly with the LanSchool Connection Server.

The Server hardware configurations for the LanSchool solution are based on the assumption that the server is dedicated to providing the LanSchool Connection Server workload, or are combined with a webNetwork Server workload. Server configuration requirements are particular to the network environment and classroom requirements. Lenovo provides services that can help determine actual server requirements to meet any customer's needs.