

Virtual Desktop Infrastructure and the Network

The Data Center becomes the New Edge

Introduction

Virtualization has been revolutionizing the IT world, enabling businesses to gain tremendous advantages, such as cost reductions in infrastructure and utilities. Increased redundancy, business recovery improvements, and greater business scalability are also being realized. These benefits are driving virtualization technology into nearly every IT organization. Cloud computing is also on the rise, taking virtualization to the next level. The next logical step for today's corporate IT infrastructure is desktop virtualization, also known as Virtual Desktop Infrastructure (VDI).

The idea is simply to provide standard desktops as virtual machines that are accessible by users through other devices, such as desktops, laptops, thin clients, mobile devices, tablets and smartphones. While there are obvious total cost of ownership (TCO) advantages to virtualization for the server and storage areas, the main drivers for VDI are improved service to the user, reduced operational cost for the support organization, and increased security (data is kept within the data center and not stored on the device itself). As stated earlier, VDI also improves the client support model. Centralizing patch management and recovery enables thousands of user machines to be easily supported. Any device accessing the desktop can easily be replaced without reconfiguration.

VDI completely revamps the traditional access control model. From client side to server/VM side enforcement, keeping the same controls in place at the data center and traditional desktop client environments is critical.

This paper focuses on how customers can leverage an intelligent network infrastructure to take full advantage of VDI infrastructure in the data center and access network environments, while providing optimal security.

Challenges with VDI

Depending on an organization's size, increasing the number of virtualized servers from hundreds to tens of thousands virtual desktops presents significant challenges for the network infrastructure. About 15 to 25 times more VDI instances can be expected in the data center when compared to the number of servers and VMs typically operating within an organization. Compared to virtualized servers, whereby an administrator controls what software is installed and how the server operates, VDI deployment administrators control all aspects of how these virtual machines are configured. With virtual desktop, the traditional "edge" has moved into the data center.

This creates security concerns and mandates that compliance requirements be reviewed. There is an increased need for similar visibility and better controls than what is offered on the access network with a traditional device. Some questions that should be asked include:

- How do you secure access from these virtual desktops into your data center?
- How do you automatically provision the proper access roles for each user in the data center?
- How can you visualize and track who is using your VDI machines and how are they being accessed at a particular point in time?

The Enterasys solution for data center VDI deployments provides answers to all these questions.

Benefits

Automation

- Automate the provisioning of access for VDI users in the access and data center to lower operational costs for IT

Visibility & Control

- Granular control of access per VDI user in the access data center to increase security
- Visualize active and track historical VDI users to address regulatory requirements

Reduced Cost

- Leverage VDI to decrease IT helpdesk costs
- Increase employee productivity with VDI on new devices like tablets and smartphones
- Reduce OPEX with automated service provisioning of the VDI infrastructure in the data center as well as for the users and devices in the access network

VDI – A Quick Introduction

Different architectures are available for virtualizing desktops. In this paper, we will focus on the most popular configuration – a client connecting to a server running the virtual desktop. The virtual desktop is a virtual machine running in a hypervisor environment with video and sound streamed to the user's machine of choice. All processing logic runs on the server, and all files are stored within the data center (typically an external SAN/NAS within the data center). To achieve this, the following components are necessary:

- Hypervisor server
 - A physical server capable of hosting multiple virtual machines, e.g. VMware ESX, Citrix XenServer
- Virtual machines/desktops
 - Standard desktop operating systems like Windows (XP, Vista, 7) or Linux (Suse Desktop, Ubuntu Desktop, etc.) on a VM
- Virtual desktop agent
 - Used to manage the desktop and for connection to the user's client machine via a remote session protocol
- Virtual desktop pool
 - A group of virtual desktops with common criteria, such as the same operating system, pre-installed software, etc., and used by a group of employees with similar business needs
 - Fixed user-desktop assignment
 - Dynamic assignment
 - Dynamic desktop creation
- Desktop controller
 - Server that is aware of all desktops, including the configuration, pools, user assignments, etc., of each
 - Handles the user login (usually via a login website) and the desktop assignment
- Thin client
 - Physical device used to see and control the user's virtual desktop
 - A thin client with very limited resources including CPU, RAM, hard disk, etc. – or a standard laptop, smartphone, tablet, or other mobile device. For this particular category, the security requirements might lead to a VDI solution.

Enterasys Solution Overview – Access and Data Center Network

The following section describes the architectural components that form the complete Enterasys solution to addressing the needs of a VDI deployment, covering both the data center network and the access network.

Since a variety of devices are used today to access VDI infrastructures, device type detection is the first and most important step to ensure that appropriate security measures, such as device assessment and access control, are appropriately applied. The detection of new devices, along with the ability to detect device type and initiate the registration or authentication process for each device is a primary feature provided by Enterasys [NAC^{NG}](#) (Network Access Control - Next Generation). Various sources are used, including network and agent-based assessment, DHCP OS fingerprinting, captive portal (used for remediation and registration, guest services) and external profilers.

Employees should be able to access the network anytime/anywhere, and the network should dynamically assign the right access policy in accordance with the rules/guidelines for the connecting device and/or user. Authentication is required to properly identify the employee and device before dynamically granting access to the IT infrastructure.

The function of assessment goes beyond identity to assess the end system. In doing so, the compliance of the end system configuration with corporate or governmental regulations is verified, while also enabling the detection of potential vulnerabilities on the device. Subsequent remediation can then be applied.

Upon successful authentication and assessment, dynamic authorization is the final step for connecting a device to the network. Enterasys recommends using policies that are enforced at the entry point (access layer) to the infrastructure. This allows very granular control while mitigating the risk associated with attacks to the infrastructure. The dynamic authorization at the entry point also enables mobility – applying the same rules to the device as it moves through the network infrastructure.

Depending on the organization, this might include restricting services only to VDI protocols. Individual organizations can determine what services are applied to devices using VDI. If an end user is accessing VDI from a smartphone or tablet, adding Internet services will allow users to enjoy the applications installed on the device. This might not apply or be desirable for a traditional thin client.

Within the data center, Enterasys [Data Center Manager \(DCM\)](#), in conjunction with Enterasys [data center switching](#) products, enables IT administrators to track users and virtual desktops throughout the data center (or in access layer networks leveraging Enterasys Network Management Suite, [NMS](#)). DCM not only visualizes the user-to-VM mapping, but also applies a user-based policy to traffic originated by each VM in the data center. This allows IT departments not only to comply with regulatory requirements but also provides an increased level of security when different user groups are served by the same VDI farm.

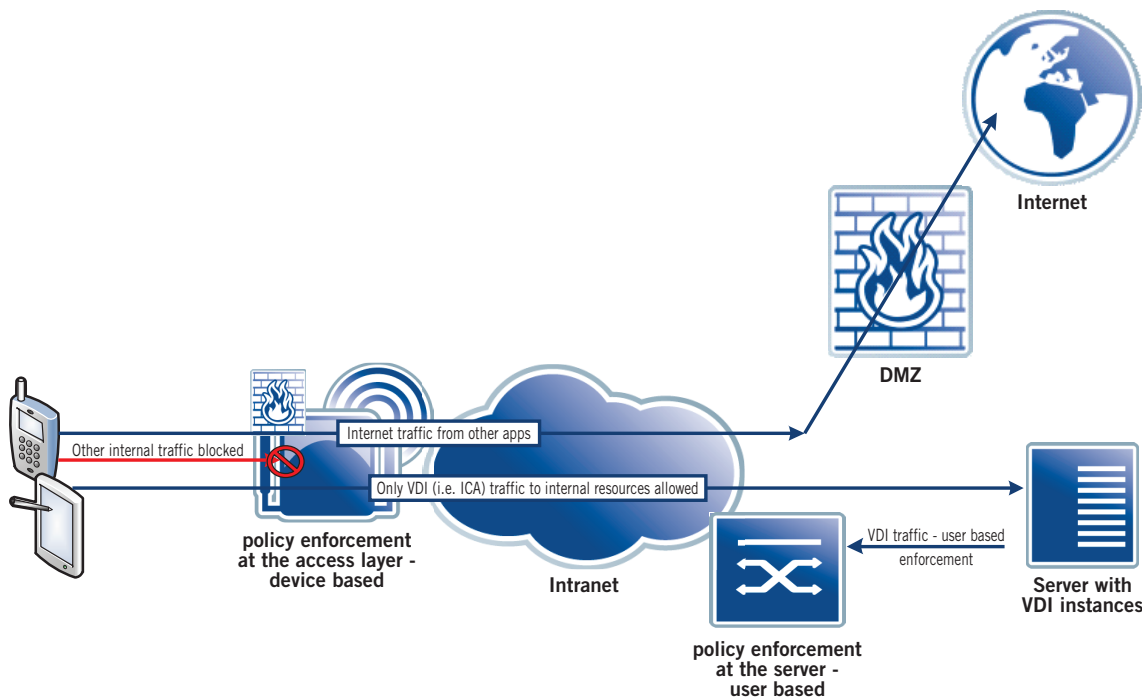


Figure 1: Secure access for any user and device using VDI

Enterasys Data Center Switching

The latest, high-performance data center switch, the Enterasys [S-Series](#), is specifically designed to support large virtualized data centers. Using large buffers, low latency, flow prioritization and many other techniques, it operates effectively in high-density, high-load virtual data centers. A key feature is the ability to dynamically apply up to 9,000 different roles and 64,000 classification rules per switch system, more than any other data center switch in the market. These roles and rules can be applied on a per virtual machine or user basis with no limitations to the number of unique identities per physical switch port. Network access for each virtual machine is automatically and dynamically provisioned with its corresponding access profile. This ensures that granular access control and quality-of-service rules can be applied to every VM in the data center to identify, authenticate, provision, and secure thousands of virtual desktops without any performance impact.

Enterasys Data Center Manager (DCM)

Delivering network services in real-time in a virtualized environment, Enterasys Data Center Manager (DCM) integrates Enterasys Network Management Suite (NMS) with hypervisors and their management systems – bridging the divide between virtual and physical network provisioning applications. Enterasys DCM is a powerful, unified management solution that delivers visibility, control and automation over the whole data center fabric, including network infrastructure, servers, storage systems and applications across both physical and virtual environments.

Enterasys DCM requires no special software or applications loaded onto hypervisors or virtual machines. The solution interfaces directly with the native operating systems. Server and VM visibility and control are provided with no bias to the server or operating system vendor. Enterprises have the freedom to choose the server vendor that best fits their requirements, eliminating vendor lock-in. DCM is unique in the industry by providing support for all major virtualization platforms: Citrix XenServer and XenDesktop, Microsoft Hyper-V and VMware vSphere, ESX, vCenter and VMware View.

Using DCM, an IT operator can automatically identify, locate, authenticate and provision access for virtual machines and desktops within the data center. This is done for VDI using various protocols:

- Citrix XenDesktop:
 - An agent can be installed on the XenDesktop Delivery Controller to retrieve all user sessions and update the information within Enterasys NMS. Thus, the switches can dynamically assign the corresponding user-specific role to each virtual desktop.
 - Users and virtual desktops are tracked through the lifetime on the data center infrastructure.
- VMware View:
 - Introducing the PC-over-IP protocol (PCoIP), VMware offers the ability to enable user-based 802.1x authentication in addition to the traditional machine-based authentication of the remote desktop protocol (RDP).
 - This option allows for the use of all access control features as is common in non-virtual desktops, including real-time location and dynamic role assignment across the whole network using the native capabilities of the operating system running within the virtual machine.

Data Center Manager (DCM) Integration Workflows

This section provides a brief overview on how DCM integrates with industry-leading VDI solutions from Citrix and VMware. The focus is on the workflow and how the systems interact with each other.

Workflow: Citrix XenDesktop

This section describes the steps when DCM is integrated with Citrix XenDesktop (built on top of XenServer).

1. Users sign into the XenDesktop Delivery Controller from various device types using the web interface.
2. Each user is assigned his/her corresponding virtual desktops.
3. The session data (which user is assigned to which virtual desktop) is pushed to the Enterasys DCM solution.

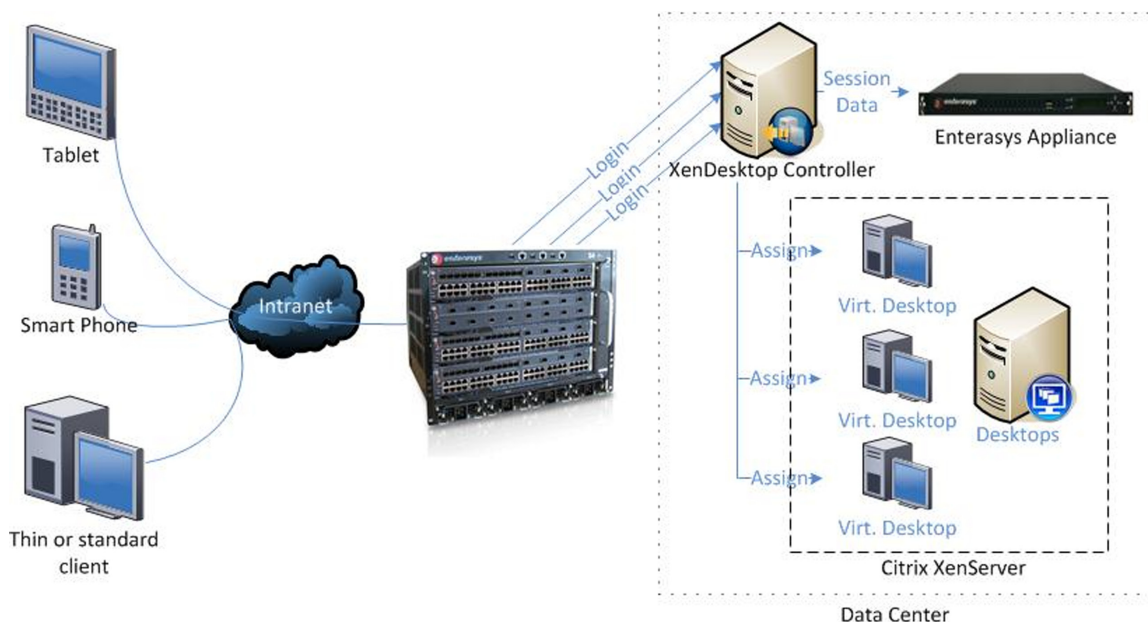


Figure 2: Login process for XenDesktop users

4. The Enterasys DCM solution is provisioning the corresponding profile and policies for each virtual desktop on the S-Series switch and the vSwitch (if necessary) based on the user's role. Role information can be stored locally or is typically retrieved by leveraging LDAP or MS Active Directory data.
 - In the access network, Enterasys NAC^{NG} is used to control access.
5. The users access resources in the infrastructure through their virtual desktops. Access control and Quality-of-Service rules are applied to the traffic originated by the virtual desktops.

6. The network administrator can track and identify all virtual desktops, the logged-in users, and the assigned profile.

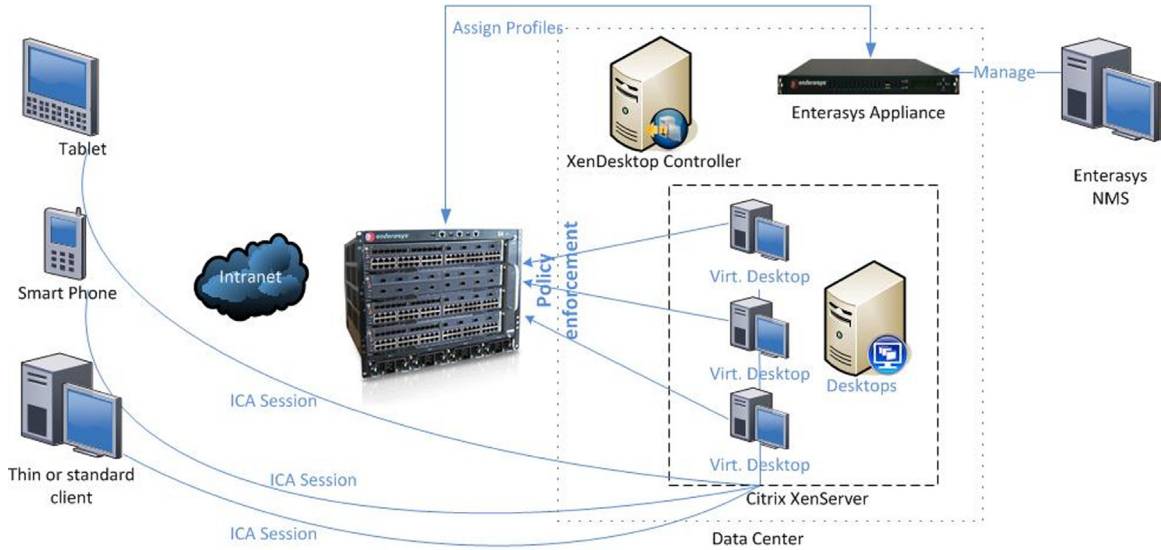


Figure 3: Policy enforcement in the data center for XenDesktop

Workflow: VMware View

This section describes the solution that integrates DCM with VMware View (built on top of vSphere).

1. Users sign into the VMware View Manager using thin or thick clients.
2. Each user is assigned his/her corresponding virtual desktops.
3. Upon selecting and logging in to the desired virtual desktop, the virtual machine authenticates its data center network connection using 802.1x EAPOL messages.

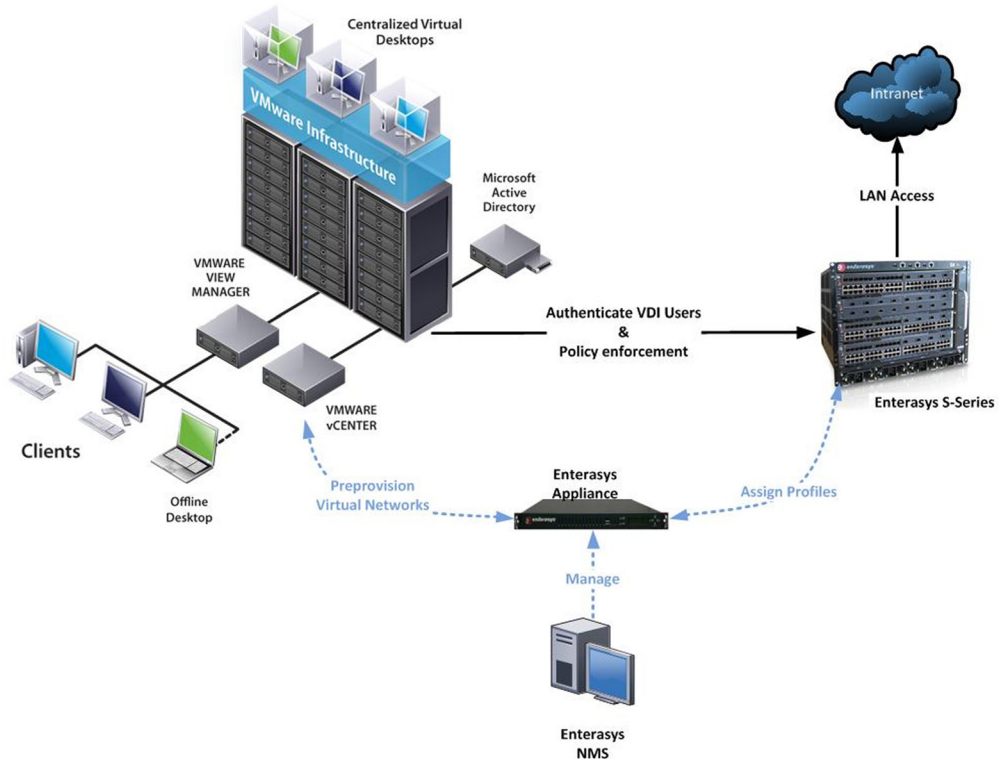


Figure 4: Message flow and policy enforcement using VMware View

4. The Enterasys DCM solution provisions the corresponding profiles and policies for each virtual desktop on the S-Series switch and the vSwitches (if necessary) based on the user's role. Role information can be stored locally or is typically retrieved by leveraging LDAP or MS Active Directory data.
 - In the access network, Enterasys NAC^{NG} is used to control access.
5. The users access resources in the infrastructure through their virtual desktops. Access control and Quality-of-Service rules are applied to the traffic originated by the virtual desktops.
6. The network administrator can track and identify all virtual desktops, the logged-in users, and the assigned profile.

Conclusion

Managing hundreds or even thousands of virtual desktops that are moving dynamically between different switch ports, switches, and even data centers is quite complex. It increases the management burden and poses threats to the corporate IT infrastructure. Enterasys offers a complete solution to tackle these challenges. One can dynamically assign profiles to virtual desktops based on user information and their roles. This secures the VDI usage in the data center, manages network connectivity and performance, and provides visibility and compliance/audit data in the virtual data center. Access provisioning for any device type entering the corporate network is fully automated as well. Granular control of access provides increased security for unmanaged, unmanageable and private devices – as part of a “Bring Your Own” (BYO) device to work – on the corporate network. Businesses can leverage the efficiency gained through new and innovative devices, along with a reduced OPEX, through automated service provisioning at the access layer.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

