Securing virtual desktop infrastructure with Citrix NetScaler
Today’s enterprises are rapidly adopting desktop virtualization as a means to reduce operating costs, enable workplace flexibility, increase business agility and bolster their information security and compliance posture. Actually realizing these benefits, however, depends upon ensuring the security and availability of the virtual desktop infrastructure. This paper explains why Citrix® NetScaler® is ideally suited to these tasks. By integrating an extensive set of network and application-layer protection mechanisms, advanced access and action control capabilities and a wealth of additional service delivery features, NetScaler not only preserves the benefits promised by virtual desktops, it maximizes them.

**The security situation with desktop virtualization**

Migrating to virtual desktop technologies and techniques from traditional desktop deployment and management approaches is a top initiative for enterprises of all types and sizes worldwide. Indeed, Gartner expects adoption of hosted virtual desktops alone to reach 70 million users by 2014.¹ Driving this growth is a compelling set of benefits. With a full-featured desktop virtualization solution enterprises can substantially and sustainably reduce desktop ownership and operating costs, enable complete workplace flexibility and increase business agility by providing rapid support for strategic initiatives such as mergers and acquisitions, geographic expansion and dynamic partnership arrangements.

Another major advantage of desktop virtualization is a significantly strengthened information security and compliance posture. This benefit derives primarily from the ability to centralize all data and applications in the corporate datacenter. Because users view and manipulate their desktops remotely, there is no need for potentially sensitive material to be distributed to the local device.

Security is also enhanced because centralization of desktop applications and operating systems increases IT administrators’ control over these crucial resources. Centralized control not only makes it easier to pursue standardization that reduces complexity, cost and an organization’s attack surface, but also boosts the ease, speed and thoroughness with which updates and security patches can be implemented. Another advantage of a centralized model is that granting and revoking access rights and privileges can be accomplished quickly and efficiently. Moreover, there’s no dependence on having users return distributed devices, software or data – because, with desktop virtualization, there aren’t any.
No free lunch

Desktop virtualization clearly has a lot to offer today’s enterprises. However, fully realizing its benefits is not a given. To preserve potential gains, organizations must, among other tasks, ensure the security of their desktop virtualization implementations. This may sound a bit circular – organizations must invest in one set of security measures to effectively gain the benefits of a second set – but that’s exactly the point in this case. Robust security capabilities are required for several reasons:

- **Remote access.** With mobility and telecommuting initiatives on the rise, a substantial percentage of users are likely to require access to their desktops from a remote location, and often over an insecure public network.

- **Device proliferation.** Consumerization has sparked the need to support a rapidly expanding variety of client devices with widely varying security characteristics and profiles. This is further complicated by the fact that most of these devices are no longer owned or controlled by the enterprise. The crucial point, in any case, is that even though desktop virtualization can eliminate local retention of sensitive data, a compromised client device still poses a threat. Sensitive data can still be viewed and the rights attributed to the user/device can be exploited to launch a far more damaging attack.

- **Extent of access.** With desktop virtualization users have access to an entire desktop. In addition to their immediate applications and data they can also get to all of the downstream resources their desktops are entitled to access. This elevates the importance of security in general, and access control in particular.

- **Concentration of resources.** The importance of robust defenses is also elevated because desktop virtualization involves putting many of an organization’s eggs in a single basket. In contrast to the conventional, distributed model of desktop computing, a single successful attack now has the potential to impact a substantial number of users and desktop systems.

There is also the big picture to consider. Today’s hackers are highly organized and motivated to do damage and make off with valuable data. As a result, robust defenses are generally required, if for no other reason than to provide protection from an increasingly sophisticated and hostile threat landscape.
Citrix NetScaler in a nutshell

NetScaler is an enterprise-class solution that makes apps and services run five times better with a powerful combination of network-based acceleration, server offload, high availability and application security. Market proven, NetScaler is used by the world’s largest websites, with an estimated 75 percent of Internet users accessing a site delivered by NetScaler on any given day. In addition, thousands of enterprises rely upon NetScaler for their public-facing web, intranet and virtual desktop delivery needs.

How Citrix NetScaler helps

An advanced solution for delivering apps and cloud and enterprise services, NetScaler provides an extensive set of capabilities that make it an ideal choice for front-ending an organization’s desktop virtualization infrastructure. Particularly relevant in this context are the numerous security mechanisms and features that NetScaler delivers to help protect virtual desktop infrastructure. These are grouped into three distinct categories.

Network-layer protection

NetScaler provides core, network-layer protection for virtual desktop infrastructure (VDI) in several ways. To begin with, administrators can use NetScaler to enforce a basic level of access control using straightforward, layer 3 and 4 access control lists (ACLs) to selectively permit legal traffic while blocking traffic that is deemed unsafe. In addition, a couple of key design features automatically protect any infrastructure NetScaler is used to front-end. For example, NetScaler incorporates a high-performance, standards-compliant TCP/IP stack that has been enhanced to:

- automatically drop traffic that is malformed and could pose a threat to the entire virtual desktop infrastructure
- prevent disclosure of low-level connection information (e.g., IP addresses, server port numbers) that could prove useful to hackers intent on perpetrating an attack
- automatically thwart many types of denial of service (DoS) attacks that exploit gaps in common protocols

Application-layer protection

Moving up the computing stack, another significant NetScaler design feature is its proxy architecture. Coupled with HTTP/URL re-write and L7 content filtering capabilities, this allows NetScaler to:

- shield connection brokers and other downstream VDI components from direct TCP and UDP connections initiated from external users, thereby reducing their exposure to malware and other types of attacks
- provide cloaking and content security for these same components to effectively hide server error codes, real URLs and other pieces of information that could give hackers the details they need to formulate custom attacks automatically thwart many types of denial of service (DoS) attacks that exploit gaps in common protocols

client

Citrix NetScaler

- Secure Access
- Application Security
- High-availability

Virtual Desktop Infrastructure
Many VDI implementations contain web-based components that also need robust protection against attacks. The integrated NetScaler App Firewall™ protects against application-layer attacks, such as SQL injection, cross-site scripting and buffer overflow threats.

NetScaler App Firewall provides:

• a flexible, hybrid-security model that protects against known vulnerabilities using an updated attack-signature database and a positive security model to defeat zero-day attacks for which signatures do not yet exist
• easy-to-configure security policies and templates for simple and fast deployment and management
• full integration with NetScaler so that security and VDI availability can be managed via a common policy and console

Greater application-layer protection is also derived from enhanced support for 2048-bit SSL encryption keys. Consistent with guidance from NIST Special Publication 800-57, key lengths for certificates supporting public key cryptography – an underlying component of SSL – are now routinely 2048 bits (versus the previously accepted 1024-bit standard). This doubling of the standard key size represents an exponential increase in the number of CPU cycles required to process SSL transactions – on average, five times more. To ease the migration to 2048-bit SSL certificates, NetScaler boosts SSL performance with advanced acceleration capabilities to keep organizations from having to sacrifice security in order to maintain performance SLAs.

Advanced access and action control

An integral component of the product, NetScaler Access Gateway™ is a full-featured SSL VPN that gives administrators granular, application-level control while empowering users with remote access to their virtual desktops from anywhere. With Access Gateway, IT administrators can manage access control and limit actions within sessions based on both user identity and the endpoint device. The result is better application security, data protection and compliance management – without the need to deploy another device.

The first two ways that Access Gateway supports remote access to virtual desktops are by providing an encrypted tunnel and supporting a wide range of methods for user authentication. Desktop sessions traversing public networks are protected from eavesdropping while the enterprise remains able to leverage its existing directory and identity management infrastructure.
Next up is granular and adaptive access control. With Access Gateway, administrators can tightly control access to virtual desktops using policies comprised of both fixed and dynamic attributes, including user identity and role, strength of authentication, location, time of day, and identity and security status of the client device. Supporting this capability is another important security feature: endpoint analysis. Integrated endpoint scanning can be used to continually monitor client devices to determine if client security software – such as antivirus, personal firewall or other mandatory programs – are active and up-to-date. Devices that fail these checks can effectively be denied access, granted limited access or quarantined by restricting their access to sites that provide the tools necessary to restore them to a compliant configuration.

Advanced action and data control capabilities provide yet another crucial layer of protection, particularly given the proliferation of client devices and growing tendency toward user ownership and self-management. Related features include:

- enhanced split tunneling control, where users can access their desktop and the client's local subnet but are prevented from directly accessing the Internet
- adaptive action control, where local printing, copy, paste and save-to-disk functionality can be restricted via adaptive policies
- browser cache cleanup, where objects and data stored on the local browser are removed upon completion of the virtual desktop session

Rounding out the portfolio of protection features are the extensive logging, auditing and reporting capabilities provided by the NetScaler central management console, Citrix Command Center. These are invaluable not only for troubleshooting purposes, but also to uncover misuse and other telltale activities that might be indicative of a compromised client or virtual desktop, or a broader-based attack against the organization's virtual desktop environment.

**Additional considerations**

Network security is only one piece of a complete security strategy for VDI – albeit a critically important one. It is also just one aspect of what NetScaler has to offer.

**Beyond NetScaler**

As powerful as NetScaler features for protecting virtual desktops are, they address only one dimension of a comprehensive security strategy for VDI. Besides network security, enterprises should consider the need for:

- **Client security.** Despite desktop virtualization’s centralized operating model, a compromised client device still poses a threat. NetScaler endpoint analysis, action control, and data cleanup features definitely go a long way in this regard. Under certain high-risk access scenarios; however, it may also be necessary to implement a comprehensive suite of endpoint security software.
• **Virtual system security.** This involves maintaining good virtual machine hygiene (e.g., ensuring virtual desktops use the latest, fully patched versions for embedded apps and operating systems, and retiring VMs that are no longer in use). It also entails providing network isolation for all VDI components and potentially implementing encryption for associated storage volumes given the concentration of resources involved.

• **Virtual desktop security.** VDI effectively brings user devices, with their high-risk behavior of connecting to networks and computers with varied trust levels, directly into the heart of the enterprise datacenter. Consequently, it is imperative to consider VM- and/or hypervisor-level implementation of anti-virus/anti-malware agents, activity monitoring and threat prevention software. It might also make sense to provide different classes of users with different virtual desktop configurations and to subsequently segregate virtual desktop VMs according to their relative trust level.

Beyond security

By itself, adequately securing virtual desktop infrastructure is not sufficient to fully preserve the benefits of desktop virtualization. Enterprises also need to ensure the availability, performance and scalability of whatever solution they decide to implement. After all, what good is a highly secured virtual desktop environment if it’s not consistently available? Or if performance is so poor that users perceive it to be unavailable, even when it isn’t?

This is where NetScaler truly excels as a front-end solution for an organization’s desktop virtualization infrastructure. In addition to its compelling set of network security features, NetScaler delivers:

• a combination of enterprise-class server load balancing, global server load balancing and health monitoring, capabilities to ensure virtual desktop availability and business continuity

• an extensive collection of mechanisms that not only enhance virtual desktop performance over the network but also streamline the user experience

• intelligent load distribution and server offload capabilities that enable seamless scalability of virtual desktop infrastructure

Conclusion

Available as a high-performance hardware appliance or a flexible, software-based virtual appliance, NetScaler can be easily and cost-effectively deployed as a front end to today’s virtual desktop solutions. By delivering a robust set of network-layer security, application-layer security and advanced access and data control capabilities, NetScaler not only preserves but extends the benefits organizations have come to expect when embracing desktop virtualization. More than just a security solution, NetScaler also helps IT managers substantially improve the availability, performance and scalability of their virtual desktop implementations.

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the company transforming how people, businesses and IT work and 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 250,000 enterprises. Citrix touches 75 percent of Internet users each day and 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®, NetScaler®, NetScaler App Firewall™ and NetScaler Access Gateway™ 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.