Secure XenApp and XenDesktop, Embrace the Flexibility

Discover 10 reasons NetScaler is the best way to future-proof your infrastructure
As you refresh your network, it’s important to understand that not every solution is equal when it comes to supporting complementary initiatives around virtualization and mobility. With employees working in more places than ever, you need to make sure that you can deliver a great user experience for apps, desktops and mobile workspaces in every scenario—while maintaining complete control and security. If the application delivery controller (ADC) you choose can’t support the broader requirements of your business and IT strategy, you risk getting locked into limitations, inefficiencies and add-on costs that you’ll regret for years to come. If your plans include virtual delivery with Citrix XenApp or XenDesktop, the right choice to make is Citrix NetScaler.

NetScaler is designed explicitly to meet the needs of today’s geographically distributed organizations and highly mobile workforce. Complete integration with Citrix XenApp, XenDesktop and XenMobile streamlines administration and helps IT optimize the scalability, availability and performance of these deployments. NetScaler Gateway provides unified, comprehensive access for users in any location. As part of an integrated, single-vendor solution for virtualization, enterprise mobility and application delivery, NetScaler allows simplified management, visibility and support to speed problem resolution. Today, companies of all sizes use NetScaler to secure and optimize their complex application environments, from virtual applications and desktops like Citrix XenApp and XenDesktop, web applications, SaaS and IaaS to Microsoft Exchange, SharePoint and databases.

This paper highlights 10 reasons to choose NetScaler to support your XenApp and XenDesktop deployments:
1. ICA proxy for secure access to Citrix XenApp and XenDesktop
2. End-to-end user and application launch-related data visibility
3. Centrally-managed, scenario-based access control
4. Per-application Micro-VPN support and encryption for mobile apps
5. Built-in monitors for StoreFront and XML brokers
6. Easy configuration for XenApp, XenDesktop and XenMobile
7. Single-URL remote access
8. Integrated global server load balancing
9. Flexible multi-factor authentication
10. Framehawk support for the best mobile user experience

1. ICA proxy for secure access to Citrix XenApp and XenDesktop

The modern workforce relies on convenient access to applications and desktops wherever people work. This mobile reality poses new challenges for IT in terms of security and quality of service. NetScaler meets both sets of requirements with ICA proxy service for XenApp and XenDesktop users, acting as the secure gateway for all ICA connections over SSL. Employees can use a Citrix Receiver client on any type of device—laptop, thin client, tablet or smartphone—to establish an SSL tunnel to NetScaler. Single sign-on pass-through to StoreFront gives users fast, convenient access to all the business apps they need to be fully productive.

For IT, NetScaler eliminates the need for additional software components or licenses to enable SSL communication. Secure Ticket Authority (STA) validation helps ensure end-to-end security for XenApp and XenDesktop connections by verifying that each request is from a valid user and provide exact information about which XenApp or VDA server will provide the requested app or desktop.
2. End-to-end user and application launch-related data visibility

To maintain high productivity and meet aggressive SLA targets for apps and services, you need to be able to proactively monitor the health of your environment and resolve problems quickly. NetScaler enables complete visibility and analytics for XenApp and XenDesktop users, channels and apps with HDX Insight functionality, an integral component of the NetScaler Management and Analytics System (MAS). HDX Insight allows IT administrators to quickly and easily obtain answers to countless operational and strategic questions leveraging the rich underlying data combined with extremely flexible data presentation capabilities for web and XenApp/XenDesktop applications. Real-time and historical reports support end-to-end monitoring for HDX traffic and instant triage of application and network issues.

NetScaler Management and Analytics System is a next-generation application visibility solution from Citrix that overcomes the limitations of traditional methods and technologies to fully address the application visibility challenges facing today’s enterprises. NetScaler appliances at strategic locations in the network gather and calculate AppFlow™ data across the entire end-to-end XenApp and XenDesktop chain—from the client device, client network and NetScaler appliance itself, to the server-side network and individual application servers. NetScaler can parse, decrypt, decompress and decompose ICA packets and traffic down to the level of individual virtual channels to provide in-depth visibility into the ICA protocol, including packet loss, jitter, consumed licenses and browser rendering time for web traffic.

NetScaler Management and Analytics System, makes it easy for IT to schedule reports that can be generated and sent on demand. Also, you can collect data from XenApp and XenDesktop farms and correlate with Windows session information to allow 100 percent transparency for troubleshooting scenarios. NetScaler integrates with Citrix Director for ease of management and monitoring of your XenApp and XenDesktop infrastructure.

Gateway Insight provides visibility into any failures encountered by users, regardless of the access mode, at the time of logging on to NetScaler Gateway. You can view a list of all available users, number of active users, number of active sessions, and bytes and licenses used by all users at any given time. You can view the end-point analysis (EPA), authentication, single sign-on (SSO), and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

Gateway Insight also provides visibility into the reasons for virtual application launch failure. This enhances your ability to troubleshoot any kind of logon or application launch failure issues. You can view the number of applications launched, number of total and active sessions, and the number of total bytes and bandwidth consumed by the applications. You can view details of users, sessions, bandwidth, and launch errors for an application.

Gateway Insight allows you to view the number of gateways, number of active sessions, and the total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, SSO, and application-launch failures for a gateway. You can also view the details of all users associated with a gateway, and their logon activity.
3. Centrally-managed, scenario-based access control

A complete security policy goes beyond location and network. NetScaler enables complete, granular contextual security for XenApp and XenDesktop users across a broad range of usage situations and device configurations. Security policies may require different levels of access depending on a given XenApp or XenDesktop user’s profile, device, location and network. NetScaler leverages SmartAccess and SmartControl to provide centrally-managed, policy-based access control. With SmartControl, IT gets a centralized point of management to create sophisticated inbound and outbound access control policies for XenApp and XenDesktop across every NetScaler appliance in the environment. These policies are enforced in the DMZ as opposed to the Intranet, improving security at the edge. Before allowing access to resources, SmartControl performs endpoint analysis (EPA) of new devices to ensure that proper OS, patch levels anti-virus, security suites and DAT files are in place.

IT has the flexibility to define access policies according to the specific security requirements of each scenario, and dynamically adapt policies to ensure that each user’s devices and data remain protected under all conditions. With SmartAccess, admins can restrict the ability of users in insecure environments to copy, email or print data, or to save confidential files to removable media. They can limit users on public kiosks to only viewing of data. SmartAccess policies include OPSWAT-based EPA software that scans remote devices and determines the presence and freshness of anti-virus software, client firewalls and can also detect other attributes such as hard-drive encryption. These policies can be applied dynamically as users move between different devices, applications and locations. Admins can leverage this functionality to enforce compliance with rules that govern privacy and the secure storage of data. This is critical for enterprises that are affected by regulations such as those in some European countries that require data about its residents be stored within the country’s borders.

4. Per-application Micro-VPN support and encryption for mobile apps

NetScaler provides Micro-VPN support for Citrix Worx Apps, enterprise (in-house developed) apps wrapped with MDX, and mobile apps wrapped and contributed by partners in Citrix’s Worx Gallery. Other EMM solutions only support “per app VPN”, which is an iOS-only feature that allows designated apps to access a single tunnel, and it requires MDM enrollment to be enabled (which is becoming less and less viable in BYOD scenarios).

Micro-VPN requires NetScaler for protecting mobile application data and supports iOS, Android, and Windows Phone/Mobile while providing an individual tunnel — with potentially different endpoints — for each managed app. This provides vastly stronger and more flexible security options.

NetScaler provides three different tunneling mechanisms that are used by XenMobile to improve throughput and security for the enterprise.

a. User authenticated reverse web proxy with network level SSO via Kerberos, Microsoft NTLM, and other hypertext transport protocol (HTTP) challenge/response protocols
b. User authenticated full VPN tunnel for non-HTTP(S) traffic, and end-to-end Secure Sockets Layer (SSL) and client certificates
c. Ticketed application tunnel for email and other long-lived connections

5. Built-in monitors for StoreFront and XML brokers

NetScaler monitors for StoreFront and XML brokers are fully integrated—not deployed separately as an app on an external server—making it possible to monitor XenApp and XenDesktop apps themselves, not just the reachability of their servers. To ensure security and efficiency, for monitoring the apps, NetScaler Gateway sends specific application level requests to ensure security and efficiency and, only when a proper response is received from the app, the app is considered UP.
6. Easy configuration for XenApp, XenDesktop and XenMobile

Correct configuration of XenApp, XenDesktop and XenMobile helps IT ensure optimal accessibility and performance while avoiding security gaps and potential problems. NetScaler simplifies setup for Citrix solutions with step-by-step wizards that help IT configure all components the right way, quickly and easily.

7. Single-URL remote access with Unified Gateway

The proliferation of separate URLs for remote access to different services leads to a fragmented, frustrating and unproductive user experience. NetScaler speeds authenticated user access to XenApp, XenDesktop and XenMobile apps with Single URL, a unified platform to address all mobile and remote access requirements. By integrating providing integrated access via NetScaler Gateway, IT can cut down on sprawl from function-specific devices and let employees get to work more quickly and conveniently. Behind this single URL, administrators have a single point for configuration, security, and control of remote access to applications.

To accomplish this, NetScaler with Unified Gateway, along with NetScaler’s Content Switching capacities and extensive authentication infrastructure, provides access to organizational sites and apps through this single URL. Additionally, remote users can use iOS or Android mobile devices and Linux, PC or Mac systems with the NetScaler Gateway client plug-ins for uniform access to the Unified Gateway URL, wherever they may be.

Make any type of application including published Citrix XenApp and XenDesktop applications available through a Unified Gateway URL.

8. Integrated global server load balancing (GSLB)

Global server load balancing (GSLB) helps organizations with multiple sites and geographically distributed services ensure availability for XenApp and XenDesktop while providing an additional layer of protection, fault tolerance, failover and optimization. NetScaler Gateway GSLB routes secure client connection traffic across datacenters based on availability, health, proximity and responsiveness.

In a distributed XenApp/XenDesktop deployment, StoreFront might not select an optimal datacenter when multiple equivalent resources are available from multiple datacenters. In these cases, StoreFront randomly selects a datacenter. It can send the request to any of the XenApp/XenDesktop servers in any datacenter, regardless of proximity to the client making the request.

GSLB Powered Zone Preference functionality examines the client IP address when an HTTP request arrives at the NetScaler Gateway appliance and uses the real client IP address to create the datacenter preference list that is forwarded to StoreFront. This allows the user to connect to the optimal delivery controller in the zone via Storefront. StoreFront selects the optimal gateway VPN VServer for the selected datacenter zone, adds this information to the ICA file, with appropriate IP addresses, and sends it to the client.

9. Flexible multi-factor authentication

Given the vulnerability of only using passwords, multi-factor authentication to applications and desktops is essential for effective security. NetScaler’s multi-factor (nFactor) authentication gives administrators an easy, flexible way to authenticate users, based on different kinds of user access, credentials provided or application demands. nFactor
simply stands for “next factor”, which allows you to edit an XML file that contains the page information for the NetScaler to ask for whatever credentials you would like, in whichever order you would like. This is all accomplished using policies and policy labels. NetScaler allows you the flexibility to:

- Configure pass-through for an authentication factor. This means that no explicit login interaction is required for that factor.
- Configure the order in which different types of authentication are applied. Choose from any of the authentication mechanisms that are supported on the NetScaler appliance for your nFactor authentication setup. These factors are executed in the order in which you configure them.
- Configure the NetScaler to proceed to an authentication factor that must be executed when authentication fails.

NetScaler Gateway’s AAA module offers extensive features to support flexible, policy-driven authentication for XenApp and XenDesktop users, including cascading, nFactor authentication. Broad protocol support includes LDAP, Radius, Cert, SAML, Kerberos, 401 and NTLM.

10. Framehawk support for the best mobile user experience

Employees need to be able to work productively in remote and mobile scenarios without sacrificing user experience. Support for Framehawk technology enables NetScaler to improve delivery of XenApp and XenDesktop traffic in low or challenging bandwidth situations. By grooming ICA transport over less than desirable network paths, the solution ensures the best experience for every user.

Figure 2: Delivering HDX Framehawk with NetScaler
Conclusion

Your virtualization and mobility initiatives are central to your ability to support a modern workforce. By choosing NetScaler, an ADC designed specifically to complement and enhance current and future investments in Citrix XenApp, XenDesktop and XenMobile, you can ensure the best experience for users, the best security for your organization and the best results for your business.

When pairing an ADC with your XenApp or XenDesktop deployment, remember NetScaler:

1. Eliminates the need for additional software components or licenses to enable SSL communication with ICA proxy for secure access to Citrix XenApp and XenDesktop.
2. Is the only ADC to enable complete visibility and analytics for XenApp and XenDesktop users, channels and apps for user and application launch-related data visibility.
3. Leverages SmartAccess and SmartControl to provide centrally-managed, policy-based access control.
4. Provides Micro-VPN support for Citrix Worx Apps, enterprise (in-house developed) apps wrapped with MDX, and mobile apps wrapped and contributed by partners in Citrix's Worx Gallery.
5. Offers built-in monitors for StoreFront and XML brokers.
6. Simplifies setup for Citrix solutions with step-by-step wizards that help IT configure all components the right way, quickly and easily.
7. Speeds authenticated user access to XenApp, XenDesktop and XenMobile apps with Single URL, a unified platform to address all mobile and remote access requirements.
8. Connects users to the optimal delivery controller in the zone via Storefront.
9. Gives administrators multi-factor (nFactor) authentication for easy, flexible user authentication based on different kinds of user access, credentials provided or application demands.
10. Supports Framehawk which improves delivery of XenApp and XenDesktop traffic in low or challenging bandwidth situations.

For more information, please visit: