A Buying Guide For Next-Gen Remote Access

Get secure remote access to all apps with NetScaler Unified Gateway
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Section 1: What’s happening in the market</td>
</tr>
<tr>
<td>4</td>
<td>What to look for when choosing a next-generation SSL VPN</td>
</tr>
<tr>
<td>5</td>
<td>Section 2: NetScaler Unified Gateway</td>
</tr>
<tr>
<td>7</td>
<td>Improving the end-user experience</td>
</tr>
<tr>
<td>9</td>
<td>Better security</td>
</tr>
<tr>
<td>11</td>
<td>Ease of management</td>
</tr>
<tr>
<td>14</td>
<td>The next generation of remote access</td>
</tr>
<tr>
<td>15</td>
<td>Case study: Large financial institution consolidates remote access infrastructure with Unified Gateway</td>
</tr>
</tbody>
</table>
Enterprises are continuously adopting IT trends such as bring-you-own-device (BYOD) policies, increased mobility, and cloud applications. The number of devices managed by enterprises rose 72% between 2013 and 2014, enabling improved employee productivity outside the office. This uptick in mobility has created demand for different applications and device profiles—including client-server apps, virtual apps, mobile apps, and cloud apps, as well as devices like smartphones, tablets, and more.

Migrating to the cloud? You’re not alone. Moving traditional applications to the cloud has many benefits, including lower CAPEX, the ability for employees to work from anywhere, and easy scalability depending on your business’ needs.

These rapid changes leave businesses facing new challenges and leaning more heavily on their IT departments to ensure employees stay connected virtually anytime, and any place. Traditional Secure Sockets Layer Virtual Private Network (SSL VPN) solutions cannot support the everyday needs of BYOD cultures or provide secure access to traditional, mobile, and cloud applications.

Section 1: What’s happening in the market
In order to give employees the work-from-anywhere-using-any-device flexibility they’ve come to expect, enterprise IT has been left with no alternative but to purchase point products for each of the applications and/or device profiles resulting in complexity in the datacenter. To make matters worse, users are forced to go to different gateways to access each of their applications. This creates a poor user experience and puts the burden on support staff to manage multiple solutions and an increasing number of support issues.

The challenge becomes finding a way to keep remote workers more productive, without compromising security and compliance requirements or increasing management complexity. Since point solutions create massive complexity and burdens IT and users, let’s take a look at the alternative, next-generation SSL VPN solutions.
What to look for when choosing a next-generation SSL VPN

1. Improved end-user experience
A next-generation SSL VPN solution should offer the best end-user experience for all users working from anywhere. To ensure maximum productivity, users should have single sign-on across all their applications. A next-gen SSL VPN solution provides secure access to any application on any device. Users should also be able to roam between the networks without any disruption to their SSL VPN sessions and without having to manually start the VPN.

2. Better security
With the constant threat of internal and external attacks, identity and access management is top of mind. New authentication mechanisms driven by evolution in the application platforms or the devices being used to consume them only increase vulnerability. Look for multi-factor authentication, which asks users to provide additional credentials based on the user, their location, and the state of the device.

3. Ease of management
SAML-based authentication and Active Directory/LDAP services provides transparent authentication and authorization with single sign-on for easy and secure identity and access management to different types of applications across organizational boundaries. A centralized approach for managing all user identities with federation and single sign-on across all the applications removes the need for users to remember multiple passwords.

This e-book discusses the Citrix NetScaler Unified Gateway, Citrix’s next-generation SSL VPN solution, and the ways it helps enterprise IT better address remote access challenges.
Section 2: NetScaler Unified Gateway

Enterprises need a viable solution that provides the best user experience, is easy to manage, and provides complete end-to-end visibility to help support staff troubleshoot issues. NetScaler Unified Gateway consolidates all of an enterprise’s remote access methods into one platform with one URL and one login. This solution provides better security management, lowers the complexity, and creates a better experience for everyone who touches it.

Citrix NetScaler Unified Gateway empowers companies to provide their employees with secure remote access to any business application. By consolidating datacenter infrastructure, it improves efficiency and reduces total cost of ownership for the IT department, while simultaneously improving the user experience and providing better and consistent security. With it, users can virtually access enterprise web and client-server applications, cloud and SaaS applications, and VDI applications from virtually any device, including laptops, desktops, tablets, and smartphones.

Citrix NetScaler Unified Gateway now supports VMware Horizon applications, in addition to Citrix XenApp, Citrix XenDesktop, and Microsoft RDP—providing one front-end for all VDI applications.
Unified secure remote access
Improving the end-user experience

NetScaler Unified Gateway positively impacts business productivity with its ease of use. With a simple access point to all business applications, employees can confidently work on the go with minimal oversight needed from IT. NetScaler Unified Gateway provides the following functionality to simplify and improve the end-user experience.

1. **Easy remote access**: Managing multiple passwords often leads to bad password habits, such as utilizing default passwords across multiple applications, or writing it on a post-it note for others to find. Remote access with NetScaler Unified Gateway becomes simplified with a single URL for all applications. NetScaler Unified Gateway provides federated identity based on **SAML 2.0** and **OAuth** standards for single sign-on across all applications, enabling users to switch between applications without having to login again. They no longer need to bookmark multiple remote access web applications and download their apps, and will only need to login once—helping improve productivity while working remotely.

2. **Interface customization**: Businesses can customize their portals easily with “browse and upload”—no additional coding required. They can add logos, change background colors, customize user license agreements, and more to lead to a better, more customized user experience.

3. **Authentication customization**: Depending on the level of security needs, an IT admin can customize login requirements. Whether a simple username and password or complex authentication mechanisms, including LDAP, digital certificates, secure tokens, RADIUS, TACACS, NTLM, Diameter, Kerberos, OAuth and SAML 2.0, you can choose your level of security.
NetScaler Unified Gateway also supports all operating systems, both mobile and desktop, including Mac, Windows, Linux, iOS, and Android. Workplace productivity increases when users can access data on their favorite device, be it business-allocated or personal—whichever they are most comfortable with and use most often. Use of multiple devices can be especially important for remote workers who may be switching between laptops and phones as they travel or move between home and the office.

4. **Integration:** NetScaler Unified Gateway integrates with every type of app an enterprise has. It not only provides secure delivery for Citrix-owned apps such as XenApp and XenDesktop, but more importantly for any other application, whether they are in the cloud or the datacenter. This mitigates the need for multiple remote-access methods and gives employees everything they need at their fingertips in order to be productive.

5. **Always connected:** More importantly, the connection to the gateway is always on. Even when a user moves between networks, the system will automatically reconnect the session. For example, if a user moves from a LAN to WiFi (or vice versa), the VPN session stays connected. And if a user is remote, the VPN session automatically gets initiated, making end users feel as though they’re always connected. Administrators can also configure a single public IP so that single sign-on capabilities are even more seamless from application to application.
Better security

IT oversight becomes increasingly difficult with multiple applications and devices, and security threats can put your company at risk.

1. Multi-Factor Authentication: NetScaler Unified Gateway provides multi-factor authentication combined with scanning of end-user devices. This allows for granular and contextual security and access control policies. IT teams can discern who is accessing data, what is being accessed, how, and when. This way, access for temporary employees or interns can be separated from access for long-term, full-time employees.

2. End Point Analysis: NetScaler Unified Gateway scans devices before they connect to a network, enabling user access using these devices based on their credentials, as well as the state of the device. If there is a failed result, users are directed to perform steps to meet compliance requirements before they are given access.

This prevents unsafe devices from connecting to the network and possibly opening up weak points for hackers to gain access.
3. **Centralized security and access management:** With single sign-on access through a single URL, the consolidated remote access infrastructure provides fewer access points to company information. Hackers will have limited points of entry into company data, and IT teams will have an easier time managing security efforts without having to manage across multiple gateways. Enterprises get better and more consistent security enforcement.

NetScaler SAML works with Microsoft ADFS 2.0 IDP to provide Active-Directory-based user access to Microsoft cloud services such as Office 365 Exchange. NetScaler SP also works with many other SAML 2.0 compliant IDPs such as SecureAuth, IBM Tivoli, Oracle Access Manager, Shibboleth, SiteMinder, and SimpleSAMLphp.

4. **Easy compliance management:** NetScaler Unified Gateway also meets various security compliance standards. No matter what type of data is being transmitted or displayed remotely, the platform is covered.
Ease of management

Remote access with NetScaler Unified Gateway consolidates all remote access infrastructure, simplifying IT management, and improving monitoring and visibility. IT teams spend less time tracking multiple remote access points and more time focusing on the security and dependability of a simplified datacenter. This means faster response times for both fulfilling new requests for remote access services and for resolving network and application issues. It also becomes easier to monitor network, password, and server errors across applications because all of them—whether cloud-based or datacenter-based—will be on the portal.

1. Better policy control

Two security features within the platform, SmartAccess and SmartControl, allow administrators to set access control based on the user, user role, state of the end-user device, location, and more. XenApp and XenDesktop admins can create, manage, and enforce these policies to access data in XenApp and XenDesktop environments.

SmartControl allows for the managing of XenApp and XenDesktop application policies from a centralized location at the edge of the network. This way, a security or networking admin can manage and enforce XenApp and XenDesktop policies like print, copy, and paste on a NetScaler Unified Gateway device.
The Unified Gateway Policy Visualizer also simplifies configurations by providing a visual representation, which enables easy diagnoses of backend issues. The visualizer shows the following:

- Pre-authentication policies
- Content switching virtual servers
- Load balancing virtual servers
- Web apps
- Authentication policies
- VPN virtual servers
- XenApp/XenDesktop apps
- SaaS apps
2. Improved IT oversight

Unified Gateway also has built-in utilities for visibility and monitoring, namely HDX Insight and Gateway Insight. HDX Insight overcomes the expenses and obstacles associated with achieving better XenApp and XenDesktop virtual application visibility. With it, IT administrators and support teams get both real-time and historical monitoring. It allows IT teams to bypass having to deploy intrusive network taps, install software agents on each server, or instrument applications for specialized monitoring.

Gateway Insight provides information on user-access-related errors that support teams can use to troubleshoot issues such as authentication failures, EPA check failures, single sign-on failures, application launch failures, and more. It covers all applications accessed through the gateway, both providing visibility and capturing end-to-end user behavior.

Administrators can cluster traffic for XenApp and XenDesktop access as well. IT can deploy NetScaler Unified Gateway in a cluster where all nodes are serving traffic. Then IT administrators can use the existing gateway configuration and scale seamlessly in a cluster deployment without having to restrict the VPN configuration to a single node.

The benefits of Unified Gateway go beyond consolidation and visibility. The system can be configured as a proxy to RDP/Terminal servers, providing unified access to end users.
The next generation of remote access

Working remotely benefits both employees and businesses, and Citrix NetScaler Unified Gateway brings IT management into the next generation. It improves the end-user experience, enhances security measures, and makes IT management easier. Enterprise IT no longer needs to spend time keeping track of multiple remote access infrastructures—now everything lives within one portal. Productivity increases since employees no longer waste time switching between access points and can login with single sign-on and a single URL. And they can do it from any device, whether it’s a Windows®, Mac®, Linux®, Android™, or iOS® operating system, saving enterprises both time and money.
Case study:

Large financial institution consolidates remote access infrastructure with Unified Gateway

A large financial institution in Europe has specialized in private banking and asset management for more than 60 years, in addition to working in corporate finance, private equity, and fund administration.

The challenge:

Managing multiple point products for remote access and load balancing, and higher security risks inherent in multiple access points

The financial institution was using Citrix for XenApp and XenDesktop, Juniper/Pulse Secure for SSL VPN and F5 for ADC. Maintaining three different redundant solutions was costly and inefficient.

The institution’s use of Citrix solutions to support its dispersed workforce began with the deployment of Citrix XenApp and Citrix XenDesktop applications, and deployed Citrix NetScaler for secure delivery and load balancing of those applications. They were also using F5 as an application delivery controller (ADC) for load balancing all their internal and external applications. For remote access to all other enterprise applications, the group used Pulse Secure’s, formerly Juniper Junos Pulse, SSL VPN solution. Still, a crucial challenge remained.
The solution:

Consolidation and a single access point for all applications delivered remotely improves TCO and security in datacenter networks.

Citrix offered a solution to consolidate and simplify all the remote access as well as application delivery infrastructure with Unified Gateway.

Citrix NetScaler provided consolidated application delivery network and improved security, visibility, and availability of the networks. With only a single solution, they were able to provide one URL for users to access any type of application.
The benefits:

1. Increasing control and security through centralization and single sign-on

The group is now using its Citrix environment as the foundation for a new business continuity and disaster recovery strategy. Single sign-on enabled better security practices. Previously, users would write their passwords down on sticky notes, and would frequently open support tickets for forgotten passwords. They were also able to implement proper access control and apply their security policies for each application individually, changing the game for the institution.

2. Improving IT efficiency

The institution’s new centralized environment makes it much simpler to provide a fully up-to-date experience for its users. By consolidating their remote access infrastructure with Citrix, they now have a single solution to manage remote access and application delivery, helping them deliver it more efficiently.

3. Maintaining competitive advantage with higher efficiency and lower cost

With XenDesktop, the institution can easily deliver applications and desktops as a service to users in any location. In the past, they struggled to provide adequate support for XenApp and XenDesktop applications. Now with NetScaler HDX Insight, the support staff can resolve application or networking issues within their SLAs. Citrix has enabled them to implement an efficient environment that makes it easier to do their jobs faster.
To learn more about NetScaler Unified Gateway, please visit www.citrix.com/gateway.


Source:

1 “Mobile Analytics Report February 2015,” 2015, Citrix