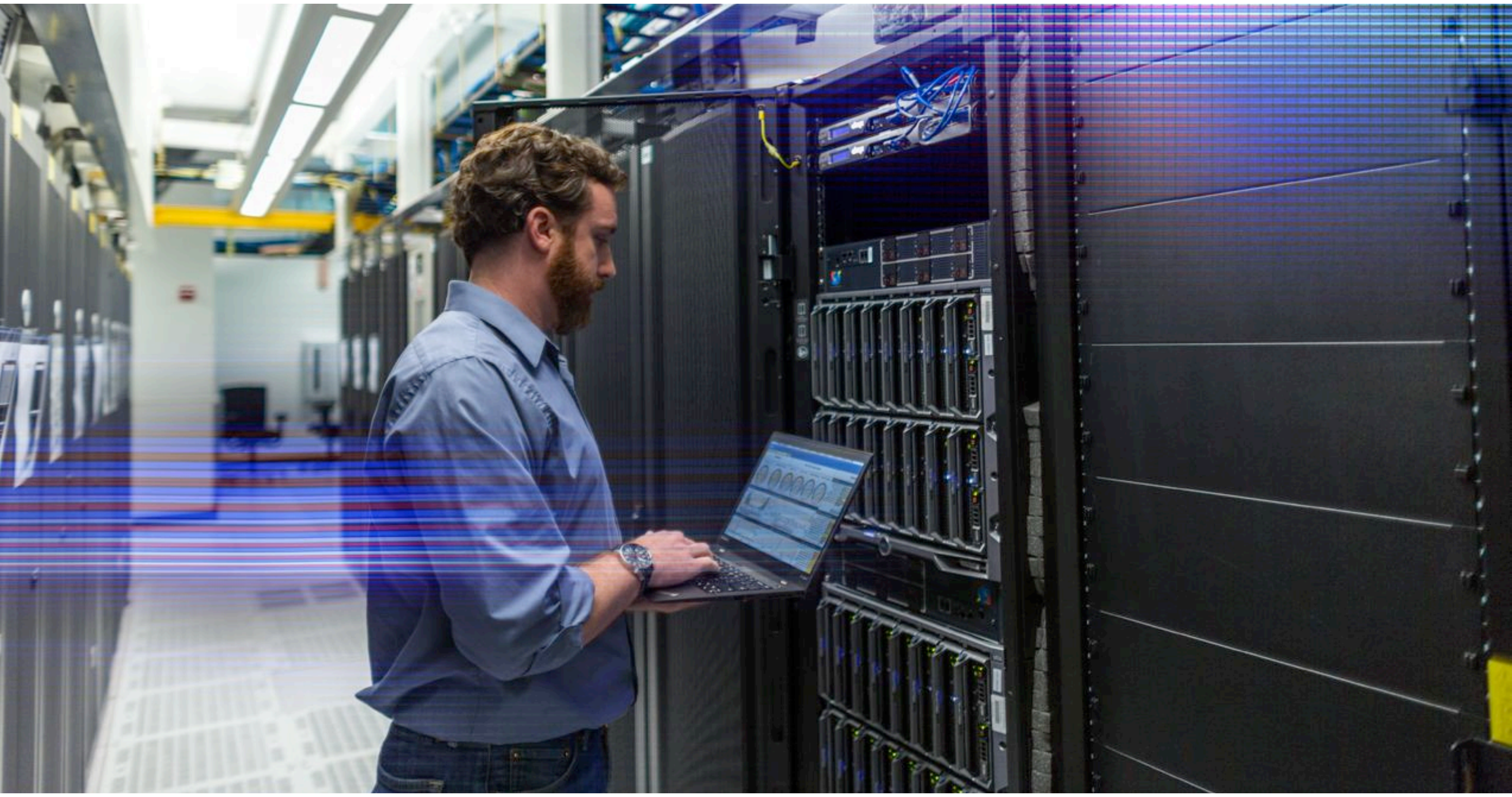
White Paper



Consolidate your Secure Remote Access Delivery Infrastructure with One URL

Learn how NetScaler with Unified Gateway provides One URL for secure remote access and helps reduce TCO, simplifies IT, strengthens security and ensures a high-definition experience for both mobile and traditional application users.

For more than a decade, SSL VPNs have been the “tool of choice” for providing employees and other users with secure remote access to centrally hosted applications, data and systems. Over the past few years, however, many IT departments have supplemented their core remote access infrastructure with a series of point solutions to better address the unique characteristics, conditions and security requirements of several increasingly important use cases. By itself, the need to support user mobility and the use of highly capable, personally owned devices has led to an entire class of mobile VPN technologies. Combined with a smattering of specialized gateways for accessing cloud services, server-hosted virtual desktops and other resources, the result for many enterprises has been an increasingly fragmented secure remote access infrastructure characterized by multiple URLs, spiraling complexity, high cost of ownership and increased vulnerabilities – not to mention an inconsistent and often poor access experience for employees and other users.

This white paper explores the evolution of secure remote access requirements, focusing in particular on the impact of user mobility and growing adoption of bring your own device (BYOD) practices. It then reveals how Citrix® NetScaler® with Unified Gateway resolves the challenges of delivering a modern secure remote access infrastructure by offering enterprises a next-generation solution that unifies the capabilities of classic SSL VPNs, more recent mobile VPNs and many other types of commonly deployed access gateways. With NetScaler with Unified Gateway, users obtain One URL, always-available, high-definition access to the resources they need wherever, whenever and on whatever device they choose to work. IT, in turn, gains a single, unified solution for meeting security

Benefits of using NetScaler with Unified Gateway as the basis for your secure remote access infrastructure include:

- One URL, for accessing any application from any user device.
- Reduced TCO, as a result of having a single unified solution capable of meeting all of the organization’s secure remote access needs.
- Improved security, based on IT having centralized, granular and dynamic control of access to essential systems, applications and data.
- Better user experience and improved productivity, as a result of users having the flexibility to get work done on their terms – from anywhere, using any device.
- Faster response times both for fulfilling new requests for remote access services and for resolving network and application issues.

With the unified approach to secure remote access enabled by NetScaler with Unified Gateway, users get exactly want they want, while IT gets exactly what it needs.

Secure remote access in the pre-mobile era

Before the rise of mobility and, in particular, the emergence of smartphones and BYOD practices, enabling secure remote access to centralized resources was relatively straightforward. Deployments were often limited to a subset of an organization's employees, such as members of the IT department, sales and other field personnel, and the "road warrior" segment of the management team. For each category of user, access was only provided to a handful of applications or network file shares and only enabled from specific, IT owned and managed devices (usually a few select brands and configurations of laptops).

A major benefit of these constrained conditions was that the users and devices remained "known quantities." The relatively high degree of trust this condition afforded meant that it was perfectly acceptable from a risk management perspective for IT to leverage traditional IPSec and SSL VPN technologies that provide full-tunnel access – where a secure channel is established at the device-to-network level and the default access available is from any application on the remote device to any resource on the central network.

For IT security teams with lingering concerns about the potential for a compromised user, application or device to infect the corporate network or retrieve sensitive data, there was always the option to take advantage of advanced policy enforcement capabilities (where available) to dynamically narrow the scope of access based on the user, device, network and other attributes associated with each access session.

Secure remote access today – mobile changes everything

Fast-forward to today and the situation is much different. With mobility and BYOD in the picture, secure access solutions need to account for a whole new set of devices, ownership models, networks, applications and, of course, user expectations. Specific challenges apply for each of these areas.

Mobile devices. Accounting for the diversity of available device types, makes and models can be a real chore. In this regard, the value of a solution will depend on the extent to which client software required for securely accessing resources other than those accessible via common browsers is supported on the mobile platforms of most interest to the organization. It is also important for solutions to account for the feature, display and performance constraints of these smaller form factors.

Mobile ownership models. With BYOD on the rise, it is imperative that solutions incorporate features to compensate for the fact that devices are: (a) no longer a "known quantity" in terms of their security and management state, and (b) routinely being used for non-business purposes that inherently increase their exposure to cyber attacks and likelihood of being compromised. Endpoint scanning and analysis coupled with dynamic policy enforcement is one such feature, while support for per-application tunnels is another.

Mobile networks/connections. No matter what "generation" of technology is used, cellular networks invariably have diminished connection and performance characteristics compared to traditional terrestrial connectivity.

Mobile applications. Accessibility must be extended beyond the usual portfolio of resource types – such as file shares, enterprise web and client-server applications – to also include both commercially available and homegrown mobile apps (many of which have server-side components or dependencies).

Mobile user expectations. With devices in hand and data plans at their disposal, practically all users, employees and otherwise, are now "remote access ready" by default. Built in, too, is the expectation to take full advantage of these capabilities. The result is increased pressure on IT to expand the scope of the remote access program in terms not only of the users and devices that are supported but also the breadth of resources that can be accessed.

Secure access for any application – mobile is not alone

Increasing user mobility and adoption of BYOD practices may be the largest factors currently influencing enterprise solutions for secure remote access, but they certainly aren't the only ones. For organizations taking advantage of virtualization technologies and cloud offerings – for example, for server-hosted desktop and application delivery and software-as-a-service (SaaS), respectively – there is the need, once again, to ensure users can securely and efficiently access these resources (from any device and location at any time). The same requirements apply too, of course, for ordinary web and legacy client/server applications. With the solutions for most enterprises being built up progressively over time, the result for many is an even larger collection of resource-specific gateways and technologies that have come to be a part of the organization's increasingly complex and fragmented access infrastructure.

The impact on secure access infrastructure

To better meet these challenges, many IT departments have chosen to supplement their core remote access infrastructure, typically an SSL VPN solution, with one or more mobile-specific access, security or management technologies. Examples include:

- **ActiveSync proxies** – a bare bones option for securely connecting and authorizing access to email and calendar resources.
- **App-centric VPNs** – a technology where individual applications establish their own dedicated VPN tunnels (note: the benefit of this approach is that it prevents any non-business or potentially compromised personal applications from gaining access to or infecting the corporate network). Better user experience and improved productivity, as a result of users having the flexibility to get work done on their terms – from anywhere, using any device.
- **Container-centric VPNs** – these are similar to app-centric VPNs, but in this case the secure tunnel is available to all applications and resources that are provisioned to a designated, secure workspace (or container) on a client device.
- **Mobile device management (MDM)** – a comprehensive solution for managing mobile devices, including onboarding newly discovered ones and enforcing configuration policies.
- **Mobile application management (MAM)** – conceptually similar to MDM, these solutions extend lifecycle management capabilities beyond the device and operating system levels to account for the corporate applications and data that reside on mobile devices.

A key point to recognize here is that in most cases these supplemental solutions operate completely independently, both of one another and the original SSL VPN. In addition, even when integration is available, this does not alter the likelihood of each solution requiring its own gateway component deployed at each corporate site where remotely accessible resources are located. Added to the other gateways enterprises have already implemented or are considering to secure and optimize access for other classes of resources (see text box below), the net result is a fragmented collection of access methods and infrastructure that negatively impacts:

- User satisfaction and productivity;
- Related capital and operating expenditures; and,
- IT security risk – which is ironic seeing how a primary goal for many of these tools is to strengthen the related security posture.

A better way forward: consolidated secure access infrastructure

Citrix NetScaler with Unified Gateway puts the brakes on the proliferation of access methods and infrastructure in today's enterprises. By incorporating the capabilities needed to support all types of access scenarios, including mobile, in a single unified platform, NetScaler with Unified Gateway not only eliminates the need to purchase and implement additional gateways but also provides One URL to consolidate a wide range of existing solutions. The result is a far better situation for both users and IT.

Advantages for users

NetScaler with Unified Gateway ensures an unparalleled, high-definition user experience by providing a consistent, always available approach for remotely accessing resources of all types.

Always available. NetScaler with Unified Gateway empowers users with choice of device and the ability to work from where they want. Users achieve remote access the same convenient way irrespective of where they are (at home, on the office LAN, in a hotel or mobile), the type of device they have (a smartphone, tablet, laptop or desktop) or the type of resource being accessed (web, SaaS, mobile, client-server or virtualized server-hosted applications) with One URL. Any required technical differences are handled transparently, without the need for user involvement.

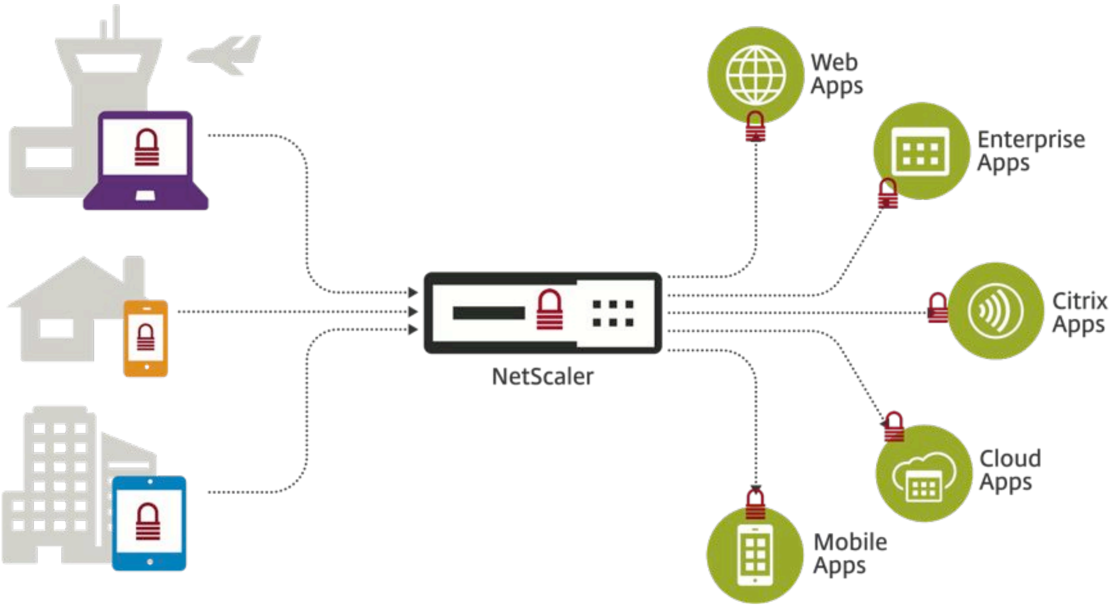


Figure 1 - Unified Secure Remote Access

Always easy. NetScaler with Unified Gateway delivers numerous features that streamline and enhance the remote access process for users including:

- One URL for remote access to all web, SaaS, and Citrix applications from any device.
- SAML 2.0 based federated identity to enable single sign-on across XenApp/XenDesktop, web, enterprise and SaaS applications.
- A customizable landing page identifying accessible resources for each individual user.
- A localized user interface, with choice of English, Spanish, French, German and Japanese.
- Transparent download of required client software or newly established configuration settings upon initial connection.
- Seamless restoration of active sessions when connectivity is "patchy" or users change devices.
- Support for Advanced TCP tuning methods more suitable for mobile and wireless networks (SACK, Nagles, Windows Scaling, TCP Westwood, Cubic, Bicubic, etc.)

Always fast. NetScaler with Unified Gateway accelerates remote access sessions by taking advantage of embedded capabilities for TCP compression and content caching along with extensive protocol-level optimizations for TCP and ICA (the communications protocol used by Citrix XenDesktop® and Citrix XenApp®). To address the unique performance challenges of mobile operations and obviate the need for "yet another gateway," NetScaler with Unified Gateway also incorporates:

- A suite of multi-layer optimizations purpose-built to streamline download and rendering of content on mobile devices.
- Mobile protocol acceleration for enhanced performance over lossy, high latency links.
- Intelligent multipath-network mode to seamlessly leverage both wireless and cellular connectivity options.

For more information on these and other mobile-specific capabilities included with NetScaler with Unified Gateway, see Taking Mobile Delivery to the Next Level with NetScaler MobileStream.

Advantages for IT

NetScaler with Unified Gateway provides the IT department with everything needed to consolidate and unify its infrastructure for delivering secure remote access to essential enterprise resources. To begin with, there is integral support for both broad-based and resource-specific access technologies, including:

- **A full-featured SSL VPN**, for enabling full-tunnel access to practically any resource.
- **An ActiveSync proxy**, for basic mobile use cases.
- **Robust mobile device and mobile application management (MDM/MAM)**, for advanced mobile and BYOD use cases.
- **Application and container–based VPNs**, for the highest levels of BYOD security.
- **Extensive multi-factor AAA (authentication, authorization and auditing) and identity federation capabilities**, for streamlining and securing access to web and SaaS applications.
- **An optimized ICA® proxy**, for secure high-speed access to XenDesktop and XenApp server-hosted virtual desktops and applications.
- **RDP Gateway and Proxy functionality** for support of Remote Desktop, Remote Applications, and Management use cases.

IT also obtains a full suite of management, scalability and other enterprise-class features required for a smooth initial deployment, efficient ongoing operations and the ability to meet the needs of the organization well into the future.

Unified policy management. As a consolidated front-end for practically all of an organization's internal and web resources, NetScaler with Unified Gateway provides a convenient, centralized approach that simplifies the creation and administration of otherwise disparate access policies. Users benefit from a more consistent set of access rules, while less potential for things to "slip through the cracks" reduces IT security risk.

Highly granular, adaptive access control. Embedded SmartAccess and SmartControl technologies allow the degree of access a user obtains in any given scenario to be dynamically adjusted based on a variety of significant attributes, including the user's role, user's location, strength of authentication, device type and configuration status, and relative sensitivity of the resources being accessed. Because NetScaler with Unified Gateway includes in-depth knowledge of the ICA protocol, administrators can even control actions of XenApp and XenDesktop users that might be considered risky in certain situations, such as local print, copy, paste and save-to-disk operations.

Unparalleled visibility. With NetScaler Insight Center™, administrators obtain complete end-to-end visibility into all TCP, HTTP and ICA-based access sessions. Powerful reports provide exhaustive usage and response time details, allowing rapid triage of any connectivity or performance issues that arise. For more information on visibility, please see "Solve the application visibility challenge with NetScaler Insight Center"

Mobile-ready scalability. Mobile and BYOD bring with them more remote users, devices per user and sessions per device. The result is greater connection rates, total connections and required throughput than ever before. NetScaler with Unified Gateway meets these demands and provides plenty of room for growth by delivering one of the most scalable remote access platforms available in the market. In addition, the solution aids the performance and scalability of resource host systems by optionally offloading a bunch of compute-intensive functions, such as authentication, key management and encryption processing.

Cost-saving Compatibility. Choice of form factor (hardware or cloud-ready virtual appliance) and the flexibility to work in conjunction with any of organization's existing access infrastructure (e.g., identity management systems) allows NetScaler with Unified Gateway to fit right in while preserving the value of past investments.

The net result is an unmatched solution for consolidating an organization’s secure access infrastructure and realizing the derivative benefits of reduced TCO, stronger security and happier, more productive users.

Making the move to NetScaler with Unified Gateway

Migrating from other, narrowly focused remote access products and technologies to NetScaler with Unified Gateway’s unified solution to consolidate associated infrastructure, simplify operations and streamline the remote access experience for users is a well understood exercise. Whether the migration effort is conducted using internal IT resources, an external service provider – such as Citrix Consulting Services – or a combination of the two, the high-level process steps, best practices and key considerations that are applicable remain the same. These include:

- Identifying and finalizing the specific business objectives that are applicable and any concurrent initiatives that need to be supported or otherwise accommodated in some manner (Is enabling user mobility a top priority for the organization this year? What are the new business-critical apps being rolled out in the next six months and which users, if any, will need to access them remotely?).
- Engaging all potential stakeholders early and often, both to ensure their requirements are thoroughly understood and being met, as well as to help prioritize the order of migration (What issues, concerns and unmet needs does line management have relative to the organization’s existing secure remote access methods and solutions? Which legacy solutions require attention first?).
- Identifying specific users/groups/roles that require secure remote access and, for each of these entities, establishing the set of apps and systems that need to be accessed and the types of devices – laptops, desktops, smartphones and/or tablets – that need to be supported (Which user groups, applications and devices require attention first – for example, based on importance of the business function being supported or breadth of applicability for a given app?).
- Weeding out remote access use cases that no longer need to be supported (With entrenched products, access rules/policies tend to accumulate over time and often remain “in force” even when the underlying need goes away. Simply carrying forward support for all rules/policies without validating there’s an actual need to do so introduces complexity and risk that can easily be avoided.).
- Ensuring alignment is maintained with the organization’s current security policies and practices (Under which circumstances, if any, should split tunneling be allowed? To what extent should client devices be scanned to determine their security and management state, and how should the results impact accessibility of different types of resources?).
- Evaluating whether authentication policies and practices can be strengthened or standardized as a result of NetScaler with Unified Gateway extensive capabilities in this area (For which remote access scenarios is there the opportunity to better align authentication and authorization practices with industry standards and compliance requirements?).
- Identifying operational and other requirements for monitoring and reporting (What data is needed/available for routine troubleshooting, detailed forensics and internal and external compliance reporting?).
- Ensuring critical service levels will be met (What are the organization’s needs in terms of high availability and scalability of the related services and how should those be met – for example, with HA pairs of appliance or a multi-appliance cluster?).

- Evaluating and prioritizing implementation plans for "new" functionality supported by NetScaler with Unified Gateway that was not provided by the organization's incumbent solutions (When and how does it make the most sense to take advantage of NetScaler Insight Center? Or per-application VPNs?).

Conclusion

To better meet the needs of mobile users, especially those operating with highly capable personally owned devices, many enterprises have supplemented their core remote access infrastructure with a series of mobile-specific access gateways and technologies. Combined with a similar set of solutions for supporting a variety of other resources – such as web, client/server and cloud/SaaS applications – the result for many IT departments is a fragmented collection of access methods and infrastructure that is confusing to users, costly to the organization and introduces greater security risk.

A next-generation secure remote access solution, Citrix NetScaler with Unified Gateway addresses the challenges today's enterprise has with proliferating remote access infrastructure. Because it incorporates the capabilities to support all types of remote access scenarios – including mobile – in a single unified platform, NetScaler with Unified Gateway not only eliminates the need to implement additional gateways, but also provides the opportunity to consolidate a wide range of existing solutions. For organizations that migrate to NetScaler with Unified Gateway and take full advantage of its unparalleled suite of capabilities, the net result is the ability to substantially reduce associated costs, complexity and security risks while increasing user satisfaction and productivity.