Putting the "Secure" in Secure Remote Access

Learn how Citrix NetScaler with Unified Gateway delivers a single, consolidated remote access infrastructure featuring comprehensive access, threat and data protection.

CITRIX®

Citrix NetScaler with Unified Gateway is a secure remote access solution that addresses the challenges today's enterprises have with proliferating remote access infrastructure. Because it incorporates the capabilities to support all types of remote access scenarios – including mobile users and devices – in a single unified platform, NetScaler with Unified Gateway not only eliminates the need to implement additional gateways, but also provides an opportunity to consolidate a wide range of existing solutions. Leveraging NetScaler with Unified Gateway in this capacity enables CIOs to substantially reduce TCO and complexity of their remote access infrastructure and associated operations while simultaneously increasing user satisfaction and productivity.[1]

This white paper explores one of the core strengths that make Citrix® NetScaler® with Unified Gateway an ideal choice for remote access consolidation. In particular, it provides an in-depth treatment of the extensive set of security capabilities that NetScaler with Unified Gateway incorporates to deliver thorough, end-to-end protection for all aspects of an organization's remote access environment – from accessible networks, apps and data to the remote access infrastructure itself.

The security challenge with "secure" remote access

User authentication and encrypted tunnels are well-recognized, long-standing staples for ensuring the confidentiality and integrity of remote access sessions (and data) traversing untrusted networks. When remote access deployments were limited to a well-defined subset of an organization's employees using corporate-managed devices to reach a handful of applications, these basic VPN technologies were even deemed sufficient. Little else, if anything, was considered necessary from a security perspective.

These days, however, the remote access landscape is much different. More often than not, IT departments are now under pressure to enable remote access for any user, operating in any location with any type of device, to any type of resource – including enterprise web, mobile, cloud/SaaS and client-server applications, hosted desktops and data.

Establishing comprehensive protection for this greater (and still growing) set of remote access use cases requires thinking about security in a more holistic manner. One helpful approach is to consider the need for security across three distinct dimensions:

- **The physical dimension.** In addition to the access network, other components of the end-to-end path requiring attention include the client device, enterprise network and accessible systems, apps and data. Not to be overlooked, too, is the security of the access gateway itself, as well as any "downstream" resources that become accessible as a result of having obtained access to the enterprise network – such as cloud/SaaS apps.
- **The logical dimension.** Providing protection for network-level protocols and services is really only a starting point. Many threats today are capable of completely bypassing controls that operate solely at this level. Establishing comprehensive protection, therefore, also requires paying attention to higher layers of the computing stack – most notably those pertaining to individual applications, associated business logic and the data itself.
- **The functional dimension.** Having defenses that combine multiple security technologies, methods and mechanisms is essential to thwarting today's multi-vector threats. Beyond user authentication and network/transport encryption, other types of security countermeasures that require attention include: dynamic access control, DDoS protection, data security, and malware/advanced threat detection.

NetScaler with Unified Gateway: The ultimate remote access security blanket

NetScaler with Unified Gateway is a secure unified front-end for all applications that provides administrators granular application and device-level control, while enabling users to work from anywhere, using any device. Built on top of the market-leading NetScaler® application delivery platform, NetScaler with Unified Gateway combines an extensive portfolio of remote access security features with a powerful set of broader, datacenter security capabilities to deliver the complete multi-layer, multi-function, end-to-end protection that today's complex remote access deployments require.

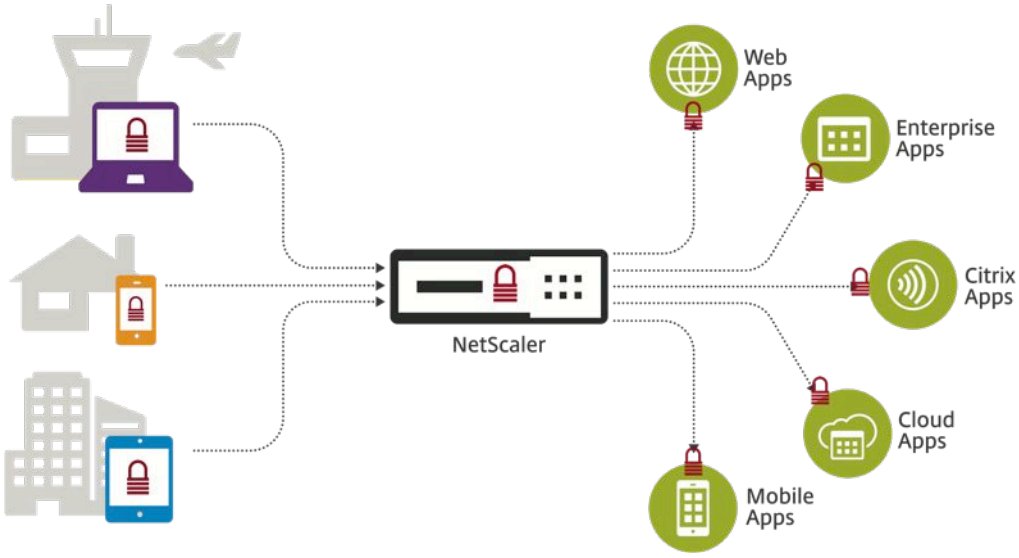

Figure 1: NetScaler with Unified Gateway provides end-to-end remote access protection

The remainder of this paper details the extensive security capabilities NetScaler with Unified Gateway provides.

Comprehensive User and App–Centric Access Management

For NetScaler with Unified Gateway, providing end-to-end protection begins with enabling granular control over which users and devices are able to access which specific resources under different operating conditions. With a combination of powerful proxies, discrete tunneling options and adaptive user and app –centric controls at their disposal, IT administrators can render risky, loose-fitting, one size fits all security policies and access mechanisms – and the legacy solutions that require them – a thing of the past.

Identity based access control

NetScaler with Unified Gateway serves as an authentication and authorization proxy that not only delivers a first, powerful layer of protection but also helps standardize this part of the access experience for users who, historically, have had to navigate an inconsistent morass of mechanisms and policies when trying to obtain access to different types of resources.

With NetScaler with Unified Gateway, all inbound application requests are blocked until the identity of the corresponding user and their device is validated. Access is then strictly confined to those parts of the enterprise network and the specific applications for which each individual user is authorized. To maximize compatibility with existing identity and access management tools and protect investments, NetScaler with Unified Gateway provides SAML 2.0 federated identity and supports extensive set of authentication mechanisms including local authentication, RADIUS, LDAP, TACACS, Digital Certificates, NTLM and Kerberos constrained delegation. Enabling single sign-on (SSO) to all web, cloud, Citrix XenDesktop® and Citrix XenApp® resources further simplifies and enhances the user experience.

Dynamic access control and centralized policy management

A combination of endpoint analysis capabilities and the innovative SmartControl feature set enables administrators to avoid the limitations of fixed access control policies and instead provision remote access services that automatically adapt to changing conditions.

Endpoint analysis. Integrated endpoint scanning establishes whether client devices are in compliance with enterprise security and management policies, such as having the latest versions of their respective operating systems and all software patches installed. For devices that fail these checks, access can be restricted to pre-defined remediation zones where users can obtain the tools needed to bring them into compliance.

SmartControl With SmartControl, administrators can now manage user policies from NetScaler console. The policies are enforced in the DMZ as opposed to in the Intranet and improves security at the edge. The administrators can configure one rule that allows a strongly authenticated mobile salesperson using a corporate device access to the full suite of hosted sales tools, while a second rule limits members of the sales team using password-only authentication from unknown devices

to a XenApp-hosted app for generating and managing proposals. Because NetScaler with Unified Gateway includes in-depth knowledge of the ICA® protocol, administrators can even control actions of XenDesktop and XenApp users that might be considered risky in certain situations, such as local print, copy, paste and save-to-disk operations.

Secure tunneling options and controls

All access sessions are protected from eavesdropping by standards-based SSL/TLS encryption. With the classic SSL VPN capability, the resulting tunnel can be used to provide access to a broad set of resources, including entire networks. Alternately, administrators can use the solution's innovative MicroVPN feature to define a secure tunnel for a single, designated application. This approach inherently restricts the reach of client devices, thereby limiting the impact of any that might be compromised.

Closely related split tunneling and browser cache controls provide yet another important layer of data protection. With the basic split tunneling feature, users are blocked from accessing any other network (or networked resource such as a printer) for the duration of their remote access session. Available as a pre-defined configuration option, an enhanced alternative instead blocks access to the Internet and other networks while still allowing access to services on a client's local subnet (e.g., print and file shares). The browser cache cleanup feature, on the other hand, ensures that all objects and data are flushed from local browser cache immediately upon completion of each and every access session.

Powerful proxies

Embedded proxies deliver unparalleled application-specific control and protection.

ICA proxy. An integral proxy for ICA – the communication protocol for XenDesktop and XenApp – enables NetScaler with Unified Gateway to secure and optimize associated remote access sessions like no other solution available in the market. While alternatives suffer from incomplete and outdated efforts to reverse-engineer ICA functionality, NetScaler with Unified Gateway benefits from intimate knowledge of the protocol and the ways XenDesktop and XenApp are designed to use it. One result, for example, is the ability for administrators to set and enforce policies for individual app-level functions such as local printing and copy/paste.

ActiveSync proxy. NetScaler with Unified Gateway can also serve as a termination and policy enforcement point for inbound ActiveSync traffic (used to enable native email services for mobile clients). The embedded ActiveSync proxy provides an important layer of protection for back-end Exchange servers and allows administrators to control email access based on a wide variety of parameters, such as whether the associated device is jail broken, in an undesirable geographic location, or out of compliance in some other way. The ability to leverage client-side certificates further enhances security by eliminating the need to cache Active Directory credentials on each mobile device requiring native email access.

Similar proxy coverage and security capabilities are also available for RDP-based services and applications.

Powerful Security Management

Equally important to its extensive access management capabilities are the powerful security management features of NetScaler with Unified Gateway.

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.

With NetScaler Insight Center™, administrators also obtain complete end-to-end visibility into all TCP, HTTP and ICA-based access sessions. HDX Insight™, in particular, provides unparalleled capabilities for monitoring and auditing the ICA traffic associated with Citrix XenDesktop and Citrix XenApp virtual desktops and applications, respectively. Coupled with extensive event logging, full RADIUS accounting, a complete audit trail of administrative actions and robust reporting capabilities, the result is the ability not only to investigate known security incidents, but also to proactively uncover misuse and other telltale signs of compromised clients or attacks against an organization's internal resources.

As powerful as they are, however, providing granular control over access to networked resources and robust security management capabilities are only two parts of the equation for end-to-end protection. With NetScaler, enterprises also benefit from an extensive set of security capabilities focused on the direct prevention and mitigation of numerous types of threats targeting organizations today.

Comprehensive Threat Protection

Protection is provided not only from threats that work by exploiting allowed access sessions, but also those designed to "take down" the remote access infrastructure itself.

Network ACLs and a default-deny posture

Independent of its many app and user level access controls, NetScaler with Unified Gateway also incorporates core network firewall functionality. In particular, support for access control lists (ACLs) provides the means to preemptively filter inbound traffic based on attributes such as source port/IP, destination port/IP, protocol, VLAN tags, ICMP type and many others. In addition, the default configuration setting to automatically drop packets that are not explicitly allowed by policy enables NetScaler with Unified Gateway to inherently stop all sorts of unwanted, unauthorized and potentially malicious traffic from gaining access – and subsequently doing harm – to the enterprise network.

Multi-layer protocol validation

Many types of cyber threats operate by perverting protocols that are commonly allowed by policy, such as TCP and HTTP. NetScaler with Unified Gateway thwarts all attacks relying on such techniques by validating and enforcing rules for acceptable usage of these protocols.

TCP validation. NetScaler with Unified Gateway features a high performance, standards-compliant TCP/IP stack that has been enhanced to (a) automatically drop malformed packets that could pose a threat to back-end resources, and (b) prevent disclosure of connection and host information (e.g., server addresses and ports) that could prove useful to hackers intent on perpetrating an attack.

HTTP validation. Enforcing RFC compliance and best practices for HTTP usage is a highly effective way that NetScaler with Unified Gateway eliminates an entire swathe of attacks based on malformed requests and illegal HTTP protocol behavior. Custom checks and enforcement rules can also be added to the security policy by taking advantage of integrated content filtering, custom response actions, and bi-directional HTTP re-write capabilities. Potential use cases include (a) preventing users from accessing specified parts of a web site unless they are connecting from authorized locations, and (b) defending against HTTP-based malware (e.g., Nimda, Code Red).

Similar validation and security capabilities are also available for UDP, DNS, RADIUS, Diameter, SSL, TFTP and SIP.

Multi-layer DDoS protection

Distributed denial of service (DDoS) attacks designed to take down an enterprise's external-facing services – and thereby impede remote and mobile users – are a constant and growing threat. NetScaler with Unified Gateway defenses in this area include:

- An integral API call-out mechanism that can be used to automatically trigger external DDoS protection services based on real-time traffic conditions;
- A high-performance architecture and extensive set of mechanisms for mitigating flood-oriented attacks targeting common network and connection layer services; and,
- Numerous features for countering more insidious low-bandwidth, application-layer variants, without impacting legitimate transactions.

To learn more about these capabilities, please refer to: "Citrix NetScaler: A powerful defense against denial of service attacks."

No-compromise SSL

By incorporating dedicated SSL acceleration hardware with support for both 2048 and 4096 bit keys, NetScaler with Unified Gateway delivers essential encryption capabilities that avoid the need to make tradeoffs between having stronger security and maintaining a high-performance user experience.

Another related feature is policy-based encryption. With this capability, administrators can configure NetScaler with Unified Gateway to automatically encrypt portions of legacy apps that were originally designed to not use encryption, but now warrant it.

For those organizations requiring a high-level of cryptographic assurance, NetScaler with Unified Gateway is also available in FIPS 140-2 Level 2 compliant models.

DNS security

In the absence of a robust, secure DNS implementation, the availability and accessibility of datacenter-hosted services and applications are put in jeopardy. Configured in DNS proxy mode, NetScaler with Unified Gateway provides high-scale load balancing of an organization's DNS servers while insulating them from attacks with a combination of DNSSEC, rate limiting and protocol validation capabilities. Organizations that deploy NetScaler with Unified Gateway as an authoritative DNS server also benefit from a hardened implementation of the associated BIND software.

Data loss protection

Safe object data checks provide administrator-configurable protection for sensitive business information, such as customer numbers, order sizes and financial details. Regular expressions can be used to define the format of such information, while accompanying policies dictate how to respond when matching strings are detected – for example, by blocking all return traffic or only masking (or removing) the offending fields. Different actions can be configured for each individual Safe Object rule.

A pre-defined implementation of the safe object capability, the credit card check feature prevents inadvertent leakage of credit card numbers. Inspection of header information and payload data provides the thoroughness needed to avoid false negatives, while algorithmic string matching delivers the high-accuracy detection needed to avoid false positives. If a credit card number is discovered, and the administrator has not allowed credit cards numbers to be sent for the app in question, then the response can either be blocked in its entirety or forwarded with all but the last four digits of the number masked (e.g., xxxx-xxxx-xxxx-5678).

Extensible threat and malware protection

The NetScaler SDX™ service delivery platform provides another substantial layer of threat protection. Featuring an advanced virtualized architecture, NetScaler SDX is a multi-services platform that enables consolidated operation of multiple independent instances of key services, including NetScaler with Unified Gateway and third-party applications. Its open and extensible design results in a future-proof approach for delivering a wide range of traditional and advanced threat protection technologies, both now and in the future. One compelling example is the ability to run the Palo Alto Networks VM-Series on NetScaler SDX and thereby supplement the extensive security capabilities of NetScaler with Unified Gateway with the power of a next-generation enterprise security platform capable of stopping both known and unknown threats, including advanced malware and targeted attacks.

Conclusion

Citrix NetScaler with Unified Gateway is a secure access solution that puts the brakes on the proliferation of access methods and infrastructure that is commonplace among enterprises today. A major strength of NetScaler with Unified Gateway that makes it an ideal choice for consolidating disparate remote access solutions and infrastructure is its unparalleled security functionality. Built on top of the market-leading NetScaler application delivery platform, NetScaler with Unified Gateway combines an extensive portfolio of access management features with a powerful set of broader, datacenter security capabilities to deliver the complete multi-layer, multi-function, end-to-end protection today's complex remote access deployments require.

For further information on Consolidation, please read Consolidate Your Secure Remote Access Delivery Infrastructure with One URL on www.citrix.com/gateway

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®