Transition to hybrid cloud and SaaS with NetScaler Unified Gateway

Overview

Implementing a traditional SSL VPN solution or an IDaaS solution will not provide single sign-on (SSO) to all applications and data. While an SSL VPN will provide network access and SSO to applications in a datacenter, an IDaaS solution will just provide SSO to applications in the cloud or delivered as SaaS.

Due to lack in functionality of SSL VPN solutions to provide SSO, traffic monitoring, and access security to SaaS applications, customers deployed IDaaS as a separate solution from an existing SSL VPN–based solution.

In addition to SaaS applications, many enterprise customers have deployed an MDM solution, and a VDI solution from one or multiple vendors. These solutions each require an additional gateway since most vendors do not provide a single access point supporting both VDI and MDM solutions.

As a result, many enterprise customers have up to 5 gateways deployed in their datacenter—all from different vendors. This redundancy, over the years, has caused datacenters to be complex and has inhibited customers from moving to cloud or highly-agile datacenter networks.

Citrix Unified Gateway provides users with one access point and SSO to business applications and data deployed in a datacenter, the cloud, or delivered as SaaS across a range of devices—laptops, desktops, thin clients, tablets, and smart phones. It provides consolidation; helps reduce the footprint of remote access infrastructure; reduces cost; and provides ease of management and a better end-user experience. NetScaler Unified Gateway helps transition IT to hybrid cloud and SaaS environments.

Citrix Unified Gateway has 3 primary use cases

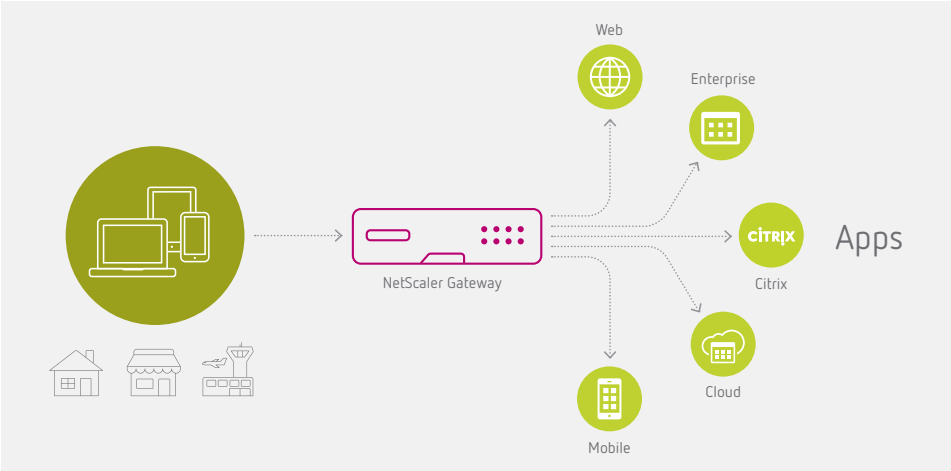
1. Single sign-on to all applications

Federation and single sign-on

NetScaler Unified Gateway provides federated identity and supports SAML 2.0, OAuth, and OpenID to achieve single sign-on across all applications whether they are web, VDI, enterprise, or SaaS applications.

User directory on-premises

NetScaler Unified Gateway provides SSO to SaaS applications such as Office 365 and



All SaaS applications are supported, including:

amazon web services | box | workday | Office 365 | ADP | zendesk | servicenow | salesforce | Google Apps for Work

Authentication mechanisms:

- SAML
- Microsoft Active Directory
- Kerberos
- Radius
- Diameter
- Oauth

Salesforce, and keeps the user directory on-premises. It can be implemented as an IdP or proxy for ADFS and provides SSO to SaaS applications.

Multi-factor (nFactor) authentication

NetScaler Unified Gateway provides nFactor authentication mechanisms and allows granular control over who is accessing the network; what is being accessed; and how and when it is accessed. It supports all the authentication mechanisms such as RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0, and OpenID 2.0.

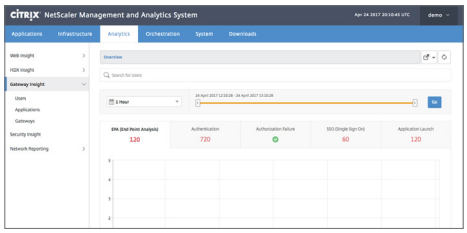
Contextual access control policies

NetScaler Unified Gateway allows granular access control to business applications based on the state of the end-user device, user, user location, and other data. An IT administrator can create, manage, and enforce these policies to access data securely in an application environment. These policies can be implemented for VDI, web, mobile, enterprise, and SaaS applications.

Visibility and Monitoring

NetScaler Management and Analytics System (MAS) includes Gateway Insight, which provides visibility of the end-to-end user experience for all applications accessed through NetScaler Unified Gateway. It provides information for application support teams to troubleshoot issues regarding authentication failures, including EPA check failures and single sign-on failures.

Gateway Insight



2. Consolidate SSL VPN infrastructure

One URL helps consolidate remote access infrastructure

NetScaler Unified Gateway provides one URL and consolidates remote access infrastructure. It provides remote access from any device to any application. For IT, this helps improve efficiency and reduce cost of ownership. For end users, it provides one URL for accessing any application from any location and improves the user experience. Users can now access any application, using any device type, from any location.

Content Switching

Given the spread of enterprise datacenters or customers across multiple geographies, you may want to present different content to different users. For example, you may want to allow users from an IP range of a customer or partner to have access to a special web portal or to content relevant to users from a specific geographical area and in a specific language. You may also want to present content tailored to specific devices, such as smartphones. Content switching enables the NetScaler appliance to distribute client requests across multiple servers based on specific content that you wish to present to users.

This also allows users to experience clientless access to certain applications such as Microsoft Sharepoint, Microsoft OWA, and Microsoft Lync.

Contextual Access Control

NetScaler Unified Gateway allows IT administrators to define and enforce access control policies based on certain parameters like state of the end-user device, location of the user, and applications being accessed. IT administrators can prioritize policies to be enforced if a user is part of multiple groups and sub-domains.

Custom Portal

NetScaler Unified Gateway provides a highly customizable portal that allows customers to brand it with their organization's look and feel. Customers can select logos, background colors, and EULA agreements as part of this customization.

Always-On

NetScaler Unified Gateway allows auto-reconnect of a session if a user is moving between networks. This mostly happens if a user goes from a home network to work or vice versa. NetScaler Unified Gateway provides an "always connected" experience for end users.

Platforms supported for NetScaler SSL VPN plugin

NetScaler Unified Gateway provides an SSL VPN client for Windows, Mac, Linux, Android, and iOS platforms. It also provides access to applications without installing a client on an end-user device (such as clientless mode through a browser).

Support for MDM/MAM solutions

NetScaler Unified Gateway supports Citrix XenMobile and provides a full device level VPN and a per app VPN (MicroVPN) for MDM/MAM deployments.

NetScaler Unified Gateway also supports Microsoft Intune and provides conditional access, nFactor Authentication, and full device-level VPN for accessing on-premises applications. For more information, please read our solution brief.

IPv6 support

NetScaler Unified Gateway offers IPv6 support for common industry platforms.

3. Secure access to VDI applications

HDX proxy to Citrix XenApp and Citrix XenDesktop

NetScaler Unified Gateway provides HDX proxy to Citrix XenApp and Citrix XenDesktop applications. It provides proxy in two modes: Basic and Advanced.

Basic HDX proxy: Basic HDX proxy includes passing the HDX protocol through the gateway appliance. It also provides basic load balancing and two-factor authentication for end users.

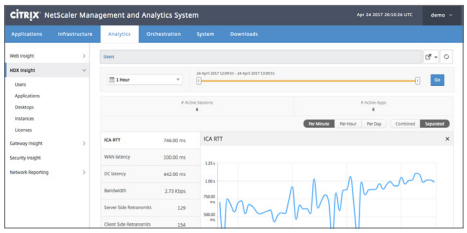
Advanced HDX proxy: Advanced HDX proxy includes contextual access control with SmartAccess and SmartControl policies; GSLB across any datacenter and the cloud; multi-factor authentication; and high availability for Citrix XenApp and Citrix XenDesktop workloads.

Visibility and Monitoring

NetScaler MAS provides HDX Insight, that allows IT organizations to achieve end to end visibility of Citrix XenApp and Citrix XenDesktop applications. No other vendor, apart from Citrix, provides this visibility and therefore it is a valuable tool for IT administrators and support teams to proactively resolve issues and have better support SLAs.

The striped HDX Insight feature allows administrators to configure and deploy HDX Insight in a cluster environment and view aggregated reports in the NetScaler Management and Analytics System (MAS) across the cluster.

HDX Insight



Clustering

Clustering allows administrators to deploy NetScaler Unified Gateway in a cluster where all nodes in the cluster are serving traffic. Administrators can use an existing Gateway™ configuration and scale seamlessly in a cluster deployment without having to restrict the VPN configuration to a single node.

Support for Multi-VDI environment

Stateless Microsoft RDP Proxy
IT administrators can use NetScaler Unified Gateway to provide single sign-on and secure access to Microsoft RDP/RDS. An IT administrator can provide access to Microsoft RDP in either a clientless or a full tunnel SSL VPN mode, and without the need for any custom clients.

Support for VMware Horizon or View (PCoIP)
NetScaler Unified Gateway provides support to proxy and single sign-on to VMware Horizon applications using PCoIP protocol. It provides load balancing, high availability (HA), and a secure way to deliver VMware Horizon applications.

Platforms supported for NetScaler SSL VPN plugin

NetScaler Unified Gateway provides an SSL VPN client for Windows, Mac, Linux, Android, and iOS platforms. It also provides access to applications without installing a client on end-user devices (such as in a clientless mode through a browser).

For more information

Learn more about NetScaler Unified Gateway at citrix.com/gateway.

For information on NetScaler hardware appliances, please refer to our hardware appliance datasheet.

For information about NetScaler virtual appliances, please refer to our Netscaler VPX datasheet.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States