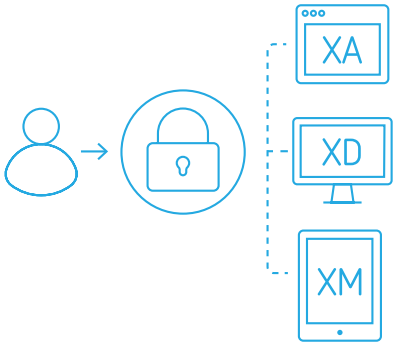
Secure, Remote Access for XA/XD/XM with NetScaler



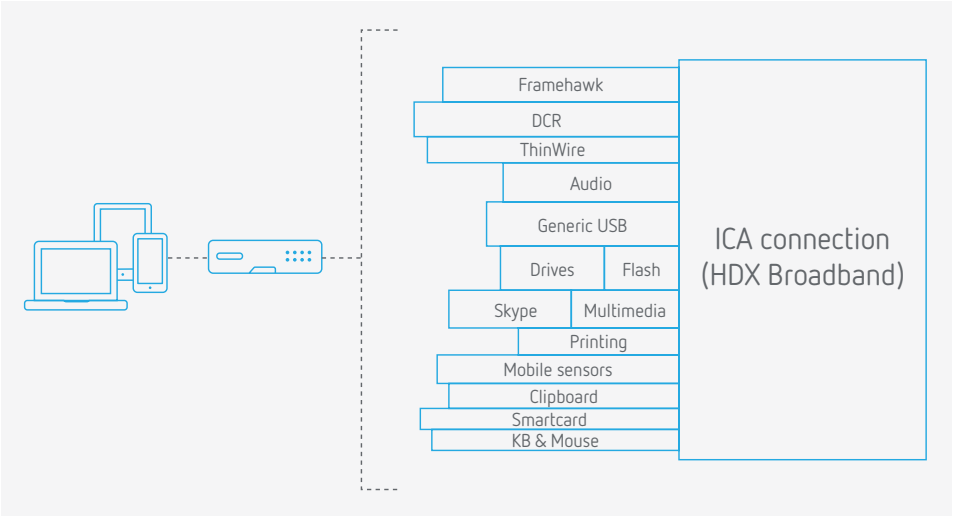
The Challenges of Application Delivery

Employees today are working from anywhere, using several devices and this is forcing IT to have to deliver every type of application; whether it's from the on-prem datacenter or the public cloud. This is causing organizations to struggle just to keep up and find a way to ensure a seamless end-user experience from anywhere. Citrix NetScaler is the best secure, remote access solution for XenApp/XenDesktop deployments.

ICA Proxy for XenApp and XenDesktop – NetScaler provides secure remote access to Citrix apps and desktops without the need to create a full SSL-VPN tunnel into your network (using ICA proxy). Users can access all their apps from one URL via single-sign on.

SmartAccess – This feature provides policies when users to access their virtual apps or desktops from personal devices. IT can use the SmartAccess policy engine to run Endpoint Analysis (EPA) scans on client devices to determine whether the proper antivirus software is installed on the device. Pre-authentication checks and post-authentication checks on inbound user sessions ensure that the client device meets all pre-established policies and can apply these security policies based on whether users pass a NetScaler Gateway Endpoint Analysis check, granting or denying them access to their virtual desktops or applications.

SmartControl with NetScaler Unified Gateway – Whereas SmartAccess is controlled in the XA/XD policy engine, SmartControl policies are centralized on the NetScaler so that restrictions can be enforced at the network layer, before the user even gets a chance to connect to a backend resource. NetScaler becomes a single point of configuration and enforcement and makes the decision to block access to any features.



Application Availability for XenApp/XenDesktop

While XenApp is built to be inherently fault-tolerant, NetScaler provides intelligent health monitoring of critical XenApp services and can redirect users away from issues before they can become disruptive to their session. NetScaler intelligently knows which backend server is best able to handle that request and will direct the request to that server.

By combining the monitoring capabilities with server load balancing, this enables an even higher level of resiliency for your customer's

XenApp infrastructure. Even in low or challenging bandwidth situations, NetScaler ensures the best mobile user experience by providing the best ICA transport over less than desirable network paths with support for Framehawk technology.

Application Visibility

Many times, IT support lacks the visibility to pinpoint user issues. This results in frustrated users being less productive. As a part of NetScaler's Management and Analytics System (MAS), **HDX Insight** provides critical, end-to-end visibility for XenApp/XenDesktop traffic passing through the NetScaler ADC on both LAN and WAN links. HDX Insight enables IT admins to view real-time client historical reports, end-to-end performance data for troubleshooting. Because the NetScaler sits between the clients and servers, it has the ability to collect flow and user-session level information which is valuable for application performance monitoring and analytics. HDX Insight is integrated into Citrix Director for single console management and works with other 3rd party collectors such as Splunk and Solar Winds.

NetScaler for XenMobile

Load Balancing for XenMobile Server

By placing a NetScaler appliance in-front of your XenMobile Server, NetScaler can handle all decryption, encryption and authentication, freeing your MDM server(s) from those tasks and enhancing performance. Because NetScaler is responsible for offloading all SSL traffic in the DMZ, IT admins can securely place their MDM server on the internal network without having to worry about potential insecure connections.

ActiveSync Filtering Support

ActiveSync Filtering provides a device level authorization service to the NetScaler, so authorization to access the applications on the backend servers is controlled by a combination of defined policies and the NetScaler is required for filtering any unauthorized connections. NetScaler device policies permit mobile access only for connections originating from authenticated applications or from Windows mobile phones.

Micro VPN Tunneling

These are VPN tunnels, which are application specific, rather than device-wide and require a NetScaler to access these applications. The logic is directly embedded into applications that the IT Administrator trusts and wants to provide access to. Once the NetScaler discovers the correct device platform, users are allowed to connect to their mobile apps and resources in the internal network when they connect using Worx Home. When Android and iOS devices connect by using Worx Home, a VPN tunnel opens to the NetScaler and then is passed to the App Controller in the internal network.

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