citrix

White Paper

Secure Citrix Virtual Apps and Desktops

Embrace the Flexibility

Discover 10 reasons Citrix ADC is the best way to future-proof your infrastructure

As you refresh your network, it's important to understand that not every solution is equal when it comes to supporting complementary initiatives around virtualization and mobility. With employees working in more places than ever, you need to make sure that you can deliver a great user experience for apps, desktops and mobile workspaces in every scenario—while maintaining complete control and security. If the application delivery controller (ADC) you choose can't support the broader requirements of your business and IT strategy, you risk getting locked into limitations, inefficiencies and add-on costs that you'll regret for years to come. If your plans include virtual delivery with Citrix Virtual Apps and Desktops, the right choice to make is Citrix ADC.

ADC is designed explicitly to meet the needs of today's geographically distributed organizations and highly mobile workforce. Complete integration with Citrix Virtual Apps, Desktops and Citrix Endpoint Management streamlines administration and helps IT optimize the scalability, availability and performance of these deployments. Citrix ADC Gateway provides unified, comprehensive access for users in any location. As part of an integrated, single-vendor solution for virtualization, enterprise mobility and application delivery, ADC allows simplified management, visibility and support to speed problem resolution. Today, companies of all sizes use ADC to secure and optimize their complex application environments, from virtual applications and desktops like Citrix Virtual Apps and Desktops, web applications, SaaS and IaaS to Microsoft Exchange, SharePoint and databases.

This paper highlights 10 reasons to choose ADC to support your Virtual Apps and Desktops deployments:

1. ICA proxy for secure access to Citrix Virtual Apps and Desktops

2. End-to-end user and application launch-related data visibility

3.Centrally-managed, scenario-based access control

4. Per-application Micro-VPN support and encryption for mobile apps

5. Built-in monitors for StoreFront and XML brokers

6. Easy configuration for Virtual Apps and Desktops and Citrix Endpoint Management

7. Single-URL remote access

8. Integrated global server load balancing

9. Flexible multi-factor authentication

10. Adaptive Transport support for the best user experience.

1. ICA Proxy for secure access to Citrix Virtual Apps and Desktops

The modern workforce relies on convenient access to applications and desktops wherever people work. This mobile reality poses new challenges for IT in terms of security and quality of service. ADC meets both sets of requirements with ICA proxy service for Citrix Virtual Apps and Desktop users, acting as the secure gateway for all ICA connections over SSL. Employees can use a Citrix Workspace client on any type of device—laptop, thin client, tablet or smartphone—to establish an SSL tunnel to ADC. Single sign-on pass-through to StoreFront gives users fast, convenient access to all the business apps they need to be fully productive.

For IT, ADC eliminates the need for additional software components or licenses to enable SSL communication. Secure Ticket Authority (STA) validation helps ensure end-to-end security for Citrix Virtual Apps and Desktops connections by verifying that each request is from a valid user and provide exact information about which Virtual Apps or VDA server will provide the requested app or desktop

2. End-to-end user and application launch-related data visibility

To maintain high productivity and meet aggressive SLA targets for apps and services, you need to be able to proactively monitor the health of your environment and resolve problems quickly. ADC enables complete visibility and analytics for Citrix Virtual Apps and Desktops users, channels and apps with HDX Insight functionality, an integral component of the Citrix Application Delivery Management (ADM). HDX Insight allows IT administrators to quickly and easily obtain answers to countless operational and strategic questions leveraging the rich underlying data combined with extremely flexible data presentation capabilities for web and Citrix Virtual Apps and Desktops applications. Real-time and historical reports support end-to-end monitoring for HDX traffic and instant triage of application and network issues.

Citrix Application Delivery Mangement is a next-generation application visibility solution from Citrix that overcomes the limitations of traditional methods and technologies to fully address the application visibilitßy challenges facing today's enterprises. ADC appliances at strategic locations in the network gather and calculate AppFlow™ data across the entire end-to-end Citrix Virtual Apps and Desktops chain—from the client device, client network and ADC appliance itself, to the server-side network and individual application servers.

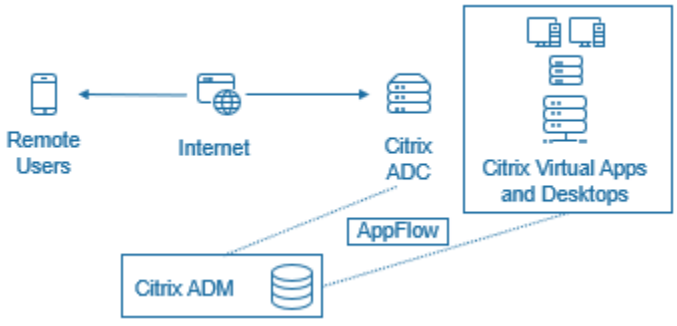

Figure 1: HDX Insight with ADC provides application visibility

ADC can parse, decrypt, decompress and decompose ICA packets and traffic down to the level of individual virtual channels to provide in-depth visibility into the ICA protocol, including packet loss, jitter, consumed licenses and browser rending time for web traffic.

Citrix Application Delivery Management, makes it easy for IT to schedule reports that can be generated and sent on demand. Also, you can collect data from Virtual Apps and XenDesktop farms and correlate with Windows session information to allow 100 percent transparency for troubleshooting scenarios. ADC integrates with Citrix Director for ease of management and monitoring of your Virtual Apps and Desktops infrastructure

3. Centrally-managed, scenario-based access control

A complete security policy goes beyond location and network. ADC enables complete, granular contextual security for Citrix Virtual Apps and Desktops users across a broad range of usage situations and device configurations. Security policies may require different levels of access depending on a given Citrix Virtual Apps or Desktops user's profile, device, location and network. ADC leverages SmartAccess and SmartControl to provide centrally-managed, policy-based access control. With SmartControl, IT gets a centralized point of management to create sophisticated inbound and outbound access control policies for Citrix Virtual Apps and Desktops across every ADC appliance in the environment. These policies are enforced in the DMZ as opposed to the Intranet, improving security at the edge. Before allowing access to resources, SmartControl performs endpoint analysis (EPA) of new devices to ensure that proper OS, patch levels anti-virus, security suites and DAT files are in place.

IT has the flexibility to define access policies according to the specific security requirements of each scenario, and dynamically adapt policies to ensure that each user's devices and data remain protected under all conditions. With SmartAccess, admins can restrict the ability of users in insecure environments to copy, email or print data, or to save confidential files to removable media. They can limit users on public kiosks to only viewing of data. SmartAccess policies include OPSWAT-based EPA software that scans remote devices and determines the presence and freshness of anti-virus software, client firewalls and can also detect other attributes such as hard-drive encryption. These policies can be applied dynamically as users move between different devices, applications and locations. Admins can leverage this functionality to enforce compliance with rules that govern privacy and the secure storage of data. This is critical for enterprises that are affected by regulations such as those in some European countries that require data about its residents be stored within the country's borders.

4. Per-application Micro-VPN support and encryption for mobile apps

ADC provides Micro-VPN support for Citrix Endpoint Management Enterprise (in-house developed) apps wrapped with MDX. Other EMM solutions only support "per app VPN", which is an iOS-only feature that allows designated apps to access a single tunnel, and it requires MDM enrollment to be enabled (which is becoming less and less viable in BYOD scenarios). Micro-VPN requires ADC for protecting mobile application data and supports iOS, Android, and Windows Phone/ Mobile while providing an individual tunnel — with potentially different endpoints — for each managed app. This provides vastly stronger and more flexible security options.ADC provides three different tunneling mechanisms that are used by Endpoint Management to improve throughput and security for the enterprise. a. User authenticated reverse web proxy with network level SSO via Kerberos, Microsoft NTLM, and other hypertext transport protocol (HTTP) challenge/response protocols b. User authenticated full VPN tunnel for non-HTTP(S) traffic, and end-to-end Secure Sockets Layer (SSL) and client certificates c. Ticketed application tunnel for email and other long-lived connections

5. Built-in monitors for StoreFront and XML brokers

ADC monitors for StoreFront and XML brokers are fully integrated—not deployed separately as an app on an external server—making it possible to monitor Citrix Virtual Apps and Desktops themselves, not just the reachability of their servers. To ensure security and efficiency, for monitoring the apps, Citrix Gateway sends specific application level requests to ensure security and efficiency and, only when a proper response is received from the app, the app is considered UP.

6. Easy configuration for Citrix Virtual Apps and Desktops and Citrix Endpoint Management

Correct configuration of Citrix Virtual Apps and Desktops and Citrix Endpoint Management helps IT ensure optimal accessibility and performance while avoiding security gaps and potential problems. Citrix ADC simplifies setup for Citrix solutions with step-by-step wizards that help IT configure all components the right way, quickly and easily.

7. Single URL remote access with Citrix ADC

The proliferation of separate URLs for remote access to different services leads to a fragmented, frustrating and unproductive user experience. ADC speeds authenticated user access to Citrix Virtual Apps and Desktops and Citrix Endpoint Management apps with Single URL, a unified platform to address all mobile and remote access requirements. By integrating providing integrated access via Citrix ADC, IT can cut down on sprawl from function-specific devices and let employees get to work more quickly and conveniently. Behind this single URL, administrators have a single point for configuration, security, and control of remote access to applications. To accomplish this, Citrix ADC with Unified Gateway, along with CItrix ADC's Content Switching capacities and extensive authentication infrastructure, provides access to organizational sites and apps through this single URL. Additionally, remote users can use iOS or Android mobile devices and Linux, PC or Mac systems with the Citrix ADC client plug-ins for uniform access to the Citrix ADC URL, wherever they may be.Make any type of application including published Citrix Virtual Apps and Desktops applications available through a Unified Gateway URL.

8. Integrated Global server load balancing (GSLB)

Global server load balancing (GSLB) helps organizations with multiple sites and geographically distributed services ensure availability for Citrix Virtual Apps and Desktops while providing an additional layer of protection, fault tolerance, failover and optimization. Citrix ADC GSLB routes secure client connection traffic across datacenters based on availability, health, proximity and responsiveness. In a distributed Citrix Virtual Apps and Desktops deployment, StoreFront might not select an optimal datacenter when multiple equivalent resources are available from multiple datacenters. In these cases, StoreFront randomly selects a datacenter. It can send the request to any of the Citrix Virtual Apps and Desktops servers in any datacenter, regardless of proximity to the client making the request. GSLB Powered Zone Preference functionality examines the client IP address when an HTTP request arrives at the Citrix ADC appliance and uses the real client IP address to create the datacenter preference list that is forwarded to StoreFront. This allows the user to connect to the optimal delivery controller in the zone via Storefront. StoreFront selects the optimal gateway VPN VServer for the selected datacenter zone, adds this information to the ICA file, with appropriate IP addresses, and sends it to the client.

9. Flexible multi-factor authentication

Given the vulnerability of only using passwords, multi-factor authentication to applications and desktops is essential for effective security. Citrix ADC's multi-factor (nFactor) authentication gives administrators an easy, flexible way to authenticate users, based on different kinds of user access, credentials provided or application demands.

nFactor simply stands for "next factor", which allows you to edit an XML file that contains the page information for the Citrix ADC to ask for whatever credentials you would like, in whichever order you would like. This is all accomplished using policies and policy labels.

Citrix ADC allows you the flexibility to:

- Configure pass-through for an authentication factor. This means that no explicit login interaction is required for that factor.
- Configure the order in which different types of authentication are applied. Choose from any of the authentication mechanisms that are supported on the Citrix ADC appliance for your nFactor authentication setup. These factors are executed in the order in which you configure them.
- Configure the NetScaler to proceed to an authentication factor that must be executed when authentication fails.

Citrix ADC's AAA module offers extensive features to support flexible, policy-driven authentication for Citrix Virtual Apps and Desktops users, including cascading, nFactor authentication. Broad protocol support includes LDAP, Radius, Cert, SAML, Kerberos, 401 and NTLM.

10. Adaptive Transport support for the best experience

Employees need to be able to work productively in remote and mobile scenarios without sacrificing user experience. Support for Adapative Transport technology enables Citrix ADC to improve delivery of Citrix Virtual Apps and Desktops traffic in low or challenging bandwidth situations. By grooming ICA transport over less than desirable network paths, the solution ensures the best experience for every user.

Conclusion

Your virtualization and mobility initiatives are central to your ability to support a modern workforce. By choosing Citrix ADC, an ADC designed specifically to complement and enhance current and future investments in Citrix Virtual Apps and Desktops and Citrix Endpoint Management, you can ensure the best experience for users, the best security for your organization and the best results for your business.

When pairing an ADC with your Citrix Virtual Apps and Desktops deployment, remember Citrix ADCr:

1. Eliminates the need for additional software components or licenses to enable SSL communication with ICA proxy for secure access to Citrix Virtual Apps and Desktops.

2. Is the only ADC to enables complete visibility and analytics for Citrix Virtual Apps an Desktops users, channels and apps for user and application launch-related data visibility.

3. Leverages SmartAccess and SmartControl to provide centrally-managed, policy-based access control.

4. Provides Micro-VPN support for Citrix Endpoint Management enterprise (in-house developed) apps wrapped with MDX,

5. Offers built-in monitors for StoreFront and XML brokers.

6. Simplifies setup for Citrix solutions with step-by-step wizards that help IT configure all components the right way, quickly and easily.

7. Speeds authenticated user access to Citrix Virtual Apps and Desktops and Citrix Endpoint Management apps with Single URL, a unified platform to address all mobile and remote access requirements.

8. Connects users to the optimal delivery controller in the zone via Storefront.

9. Gives administrators multi-factor (nFactor) authentication for easy, flexible user authentication based on different kinds of user access, credentials provided or application demands.

10. Supports Adaptive Transport which improves delivery of Citrix Virtual Apps and Desktops traffic in low or challenging bandwidth situations

citrix

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

©2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).