

Build a cloud network leveraging best-in-class security and application delivery



With the proliferation of enterprise applications, consumer applications and cloud-based services, IT managers are challenged to maintain control over their networks, ensure compliance, and guarantee service levels. To restore control and enable businesses to fully embrace mobility and consumerization, IT requires technologies that allow any user to safely access any application from any device in any location. Moreover, the solution must deliver against stringent SLAs by ensuring the highest levels of security, performance, and availability, while providing the flexibility required to quickly adapt to changing conditions. To accomplish all of these objectives, today's enterprises need a next-generation network that natively understands application traffic so it can intelligently apply the right protection and optimization capabilities, with cloud scale.

This paper explains why combining two best-in-class solutions—the Citrix NetScaler application delivery controller (ADC) and the Palo Alto Networks Next-Generation Firewall (NGFW)—is the best approach for today's enterprises to build a network capable of fully addressing cloud requirements for secure application delivery.

The legacy network challenge

The problem for many of today's organizations is that their existing networks were designed in an era characterized by known users, operating in fixed locations, accessing a well-defined set of IT-managed resources from IT-controlled desktops and laptops.

The limitations of these legacy infrastructures are considerable, and include:

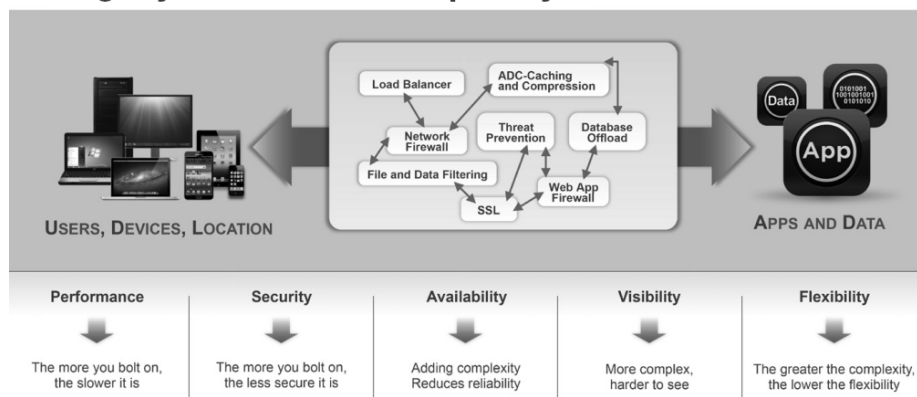
- Insufficient application intelligence to effectively and granularly enforce security policies, illuminate application-specific performance issues, and maximize application availability
- Insufficient security capabilities to keep up with the tactics of modern threats and the ever-increasing focus on theft of valuable information (e.g., credit card numbers)
- The inability to adequately support enterprise mobility by accommodating bring your own device (BYOD) initiatives and providing a high-definition experience for users connecting via a wide range of access networks and technologies

- A lack of inherent network scalability to quickly and affordably add capacity to accommodate new apps, users, devices, and delivery models
- Insufficient flexibility with rigid form factors that do not facilitate the seamless transition from physical to virtual network elements

The challenge in overcoming these deficiencies is to obtain a complete set of best-in-class capabilities designed from the ground-up for cloud architectures. Not only is it necessary to address all aspects of application delivery—security, availability, performance, and visibility—in a comprehensive manner, but each capability should be best-in-class. After all, having robust security is meaningless if unreliable infrastructure and poor performance prevent users from accessing essential resources and keep them from being productive in the first place.

Additionally, the aggregate solution needs to exhibit the qualities and characteristics that define cloud architectures, including affordability, and elastic scalability. In this regard, the traditional approach for obtaining best-in-class capabilities—implementing a series of “pizza boxes” each providing a relatively narrow set of functionality—is anathema. The cost, complexity, and degraded scalability characteristic of this approach is a major step in the wrong direction. Instead, enterprises need a solution that consolidates a complete set of application delivery capabilities into as few devices as possible—without having to compromise in terms of their being best-in-class.

Legacy datacenter complexity



The best-in-class cloud network solution

To successfully deliver any application to any user with any device in any location, IT leaders must look to solution providers with the right technology vision, and a proven track record for delivering on that vision. Citrix and Palo Alto Networks are well-recognized leaders in their respective markets—application delivery and network security—and fulfill these qualifications. Combined, they provide today’s enterprises with an ideal solution for building a cloud network fully capable of addressing cloud era requirements for secure application delivery.

Individually, both solutions are best in class. Both NetScaler and the Palo Alto Networks NGFWs are market-leading products, deployed in thousands of the most demanding enterprise and public cloud networks worldwide. Both provide best-in-class capabilities operating on a platform purpose-built to optimally deliver their respective services. And both emphasize application intelligence and fully exploit it to maximize the effectiveness of their respective capabilities (e.g., app-aware acceleration and load balancing for NetScaler, and safe application enablement for Palo Alto Networks NGFWs). This is in stark contrast to the majority of solutions available today, which exhibit feature-function weak spots typical of all-in-one products, rely on “bolted-on” capabilities that compromise performance, and/or lack the app intelligence necessary to be truly effective in the cloud era.

Together, both solutions deliver a comprehensive set of capabilities. The pairing of NetScaler ADCs with Palo Alto Networks NGFWs leaves IT managers wanting for nothing when it comes to secure application delivery. Each aspect of the discipline—security, availability, performance, and visibility—is fully addressed. Some examples of the capabilities of the combined solution include:

Security

- Next-generation firewall application control (regardless of evasive tactics)
- Multi-facet, bi-directional threat protection (AV, IPS, and targeted/ unknown attacks)
- L4 & L7 DDoS protection
- Web application firewall
- Data/content leak protection
- Line-rate SSL inspection
- Seamless user authentication/authorization
- Flexible secure remote access (SSL VPN)
- Integrated in application delivery infrastructure
- Integrated in security infrastructure
- Built-in compliance enforcement and reporting

Availability

- L4 load balancing
- L7 content switching
- Database load balancing
- Global resource load balancing
- Server and application health monitoring

Performance

- Most advanced application acceleration
- Intelligent data compression & content caching
- Network and protocol optimization
- Traffic prioritization and rate controls
- Server offload (SSL, TCP connections)

Visibility

- Real-time insight of application flows
- User activity monitoring and analytics
- Embedded content and data visibility

The combined solution facilitates the evolution to cloud networking.

Implementing the combined solution requires two components, not ten or twenty. Cost and complexity is significantly less than with single-purpose best-in-class designs, where appliance sprawl is commonplace. Reduced latency from fewer 'moving parts' yields enhanced performance. A simpler overall design translates into better security (based on fewer gaps and opportunities for configuration errors), clearer visibility, and increased reliability and adaptability. Two deployment options are available:

- Easy-to-deploy appliances – Each component solution is also available as affordable, easy-to-deploy appliances that scale to 20+ Gbps. In addition, Citrix TriScale Technology scales network infrastructures, affordably and with no additional complexity. With TriScale, IT managers can: scale up—by leveraging NetScaler Pay-As-You-Grow licensing to increase performance on-demand with no added hardware; scale out—by leveraging TriScale Clustering to expand capacity up to 32x further with zero downtime; and/or scale in—by leveraging NetScaler SDX to consolidate up to 80 isolated ADC instances on a single platform. These unmatched strengths extend to Palo Alto Networks NGFWs, in turn, when NetScaler scaling capabilities are employed to aggregate NGFW capacity.
- Consolidated deployment on a Citrix NetScaler SDX platform – Multiple instances of Palo Alto Networks VM-Series and NetScaler ADC can be consolidated on a NetScaler SDX platform. With the combined solution, organizations can achieve substantial infrastructure consolidation, reducing costs and complexity without compromising on functionality. Mutual support for an open XML API further facilitates the transformation to a cloud delivery model by enabling real-time orchestration of individual technologies and capabilities in response to changing conditions.

Both deployment options provide a best-in-class solution for building a next generation network, one that:

- Incorporates application intelligence at its foundation for superior effectiveness
- Aligns with a cloud-first strategy to ensure affordability and seamless scalability
- Enables delivery of all types of applications to all users under all conditions with the best security, availability, performance, and visibility

Enabling cloud-era business initiatives

The combined solution is well positioned to facilitate several CIO and business-driven initiatives. The examples covered in the following sections provide proof points of the solution's value at the core of today's—and tomorrow's—enterprise cloud networks.

Initiative #1 – Provide secure access to any application regardless of location. Regardless of whether users access the network remotely or locally, a critical consideration is the ability to control their actions once they're on the network. This is where the App-ID, User-ID, Content-ID and WildFire technologies of the Palo Alto Networks NGFW are instrumental. With these technologies, IT not only gains visibility of precisely who is accessing which applications and data from which types of devices, but also the ability to control these activities by enforcing granular policies. For example, using the Palo Alto Networks NGFW, organizations can enforce control over employee-owned devices between security zones, such as from the corporate LAN to the Internet. IT can also implement GlobalProtect to extend corporate policies to employee-owned devices being used externally. The net result is a solution that enables application access while delivering robust network security and enabling BYOD, rather than hindering it.

Enabling mobile users is also essential to the success of today's businesses. The combined solution addresses this need not only with integrated SSL VPN technology, but also with the flexibility to optimize each deployment based on operational and organizational considerations. IT managers can elect to support secure remote access capability in either: (a) the application delivery infrastructure (e.g., if it's being used to support a specific application like Citrix XenDesktop, or if it's "owned" by an application or networking team), or, (b) the network security infrastructure (e.g., if the intent is to support a broader array of apps, or have it be the responsibility of the security team).

Whichever approach is pursued, security is further bolstered by granular access policies that provide dynamic host profiling checks and a powerful head-end "backstop" of antivirus, intrusion prevention, and targeted attack detection capabilities to thwart any threats originating from compromised mobile devices. A streamlined, high definition user experience is also facilitated based on support for single sign on, session persistence, optimal path selection, and the ability to guarantee the availability of datacenter resources.

Initiative #2 – Ensure data security compliance. The need to maintain compliance with pervasive data privacy and security regulations (e.g., PCI DSS, HIPAA/HITECH, NERC CIP, etc.) is critical. However, it is made more complex by the inescapable trend toward increasing use, both authorized and not, of social media, personal file-sharing apps, and other consumer-oriented cloud services. The resulting challenges are twofold: (1) protecting against leakage of sensitive data and (2) maintaining threat defenses that are consistent with the general requirement to do whatever is “reasonable and appropriate” to contain IT security risk. The combined Citrix and Palo Alto Networks solution helps in both of these areas by providing IT with the means to:

- Accurately identify and control the use of more than a thousand applications (including common social networking and cloud-based services), regardless of any evasive techniques that are used to mask their operation
- Detect and respond (e.g., via alerting, blocking, or selective masking) to sensitive data contained in both employee communications and to externally initiated transactions
- Engage a robust set of defensive controls (AV, IPS, and targeted attack detection) to account for the high prevalence of web/cloud services that are malware infected or otherwise compromised
- Establish highly effective yet affordable segmentation with a combination of granular access control (e.g., by application, user and content) and fully isolated multi-tenancy
- Generate logs rich with user, content, and app-layer details to help validate policy conformance and support further analysis and forensic investigation, if necessary

Initiative #3 – Enable mainstream virtual desktop delivery. The substantial benefits that can be realized—reduced cost of operations and desktop ownership, stronger security, and greater business agility—make a compelling case for embracing desktop virtualization. Fully realizing these gains, however, depends on ensuring 100% uptime, delivering a high-definition user experience (so users aren’t motivated to circumvent the solution) and providing adequate protection, particularly for remote users. In this regard, the combination of NetScaler and

Palo Alto Networks NGFWs conveys a number of significant advantages, including:

- Local and global load balancing to ensure availability—which is absolutely critical given the degree of dependency users have on the centralized VDI infrastructure
- Advanced, identity-based application control and threat prevention at the
- back-end to enable granular control, content leak protection, and protection for resources users access from their virtual desktops
- Palo Alto Networks User-ID integration with Citrix XenDesktop environments allow security policies for applications to be enforced on an individual or user-group basis, and provides visibility into user activity via detailed reports and logs.

- DDoS and robust threat prevention to further maximize VDI up-time
- Secure remote access with granular control down to the level of individual virtual channels to support the large percentage of users likely to be operating remotely
- XenDesktop-specific optimizations and infrastructure health monitoring to ensure a high-performance user experience

Initiative #4 – Proactively manage any attack at any scale. There's no way around the fact that business-critical resources are increasingly under attack. Adequately protecting them is a top priority for virtually every organization, regardless of size or vertical industry affiliation. The combined solution serves this objective by providing protection against any attack, at any scale.

The set of powerful protections made available to enterprises with this solution include the following:

- Extensive L4 and L7 defenses against DDoS attacks
- Granular, user and app-focused access control that reduces the scope of attack by controlling applications that may carry threats
- Complete integrated threat framework with high-performance stream-based protection against viruses, spyware, and intrusions
- Advanced protection against modern malware and targeted/zero-day attacks
- Comprehensive web application protection via the industry's highest capacity web app firewall
- Dynamic header/response re-writing to "hide" tell-tale information about internal systems that hackers can use to devise and perpetrate attacks

The result is a comprehensive cocktail of essential network security for preventing both known and unknown threats coupled with robust defenses designed to thwart app-specific threats, including zero-day attacks targeting app-layer vulnerabilities.

Equally important, however, is the ability to provide all of this protection at scale. To begin with, the solution features purpose-built hardware platforms—designed specifically to support high-speed delivery of all services, including security. For example, the high-performance, multi-core architecture of NetScaler MPX defends against SYN flood attacks at volumes of nearly 20 million connections per second, and delivers over 12 Gbps of web app firewall performance—a level that is unmatched by other products in this class.

Similarly, for the Palo Alto Networks NGFW, its innovative Single Pass Parallel Processing (SP3) Architecture reduces latency by performing security functions once. This software architecture coupled with a multi-core hardware processing architecture ensures high performance protection is delivered under the most demanding conditions. And for organizations that need even more firepower, there's Citrix TriScale. By enabling network architects to cluster as many as 32

NetScaler appliances and load balance as many Palo Alto Networks NGFWs as necessary, TriScale takes high-performance network defense beyond the 1 Tbps threshold.

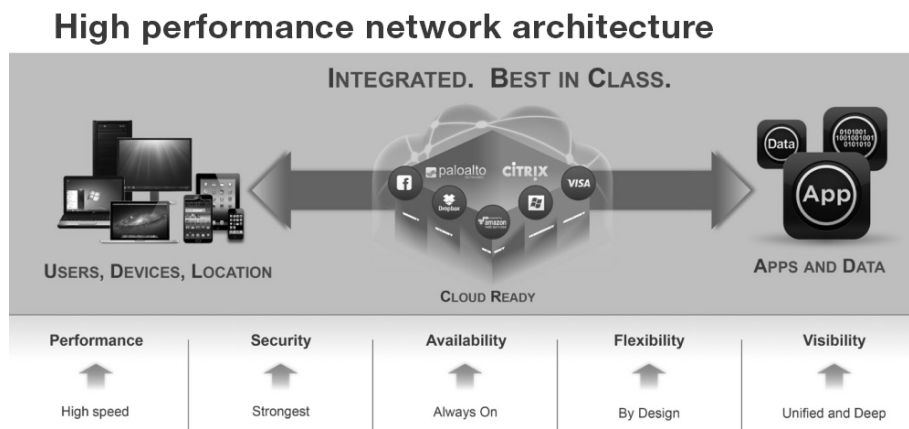
Initiative #5 – Transform to cloud networking. Much like desktop virtualization, but on a greater scale, cloud networking promises a more affordable and agile way for building datacenters and delivering IT services. The combination of Citrix NetScaler and Palo Alto Networks NGFW aligns with this initiative in many ways. With the combined solution, IT managers can achieve substantial infrastructure consolidation, reducing costs and complexity without compromising on functionality. They're also able to realize superior scalability and adaptability as a result of Citrix TriScale technology, and greater flexibility than with the “pizza box” approach.

Mutual support for an open XML API further facilitates the transformation to cloud networking by enabling real-time orchestration of individual technologies and capabilities in response to changing conditions. The ability to deploy full-featured virtual appliances alongside or instead of purpose-built physical appliances also provides greater flexibility in provisioning core services, either on-premise or in third-party cloud infrastructures.

Conclusion

Operating together, Citrix NetScaler Application Delivery Controller and Palo Alto Networks Next-Generation Firewall provide enterprises with a powerful, best-in-class cloud network solution for secure application delivery. Multiple virtual NetScaler ADC and Palo Alto Networks VM-Series instances can be consolidated on a Citrix NetScaler SDX platform or deployed as discrete, appliances.

The combined solution has been validated for key enterprise applications, and not only fulfills the fundamental objective of the modern IT department—the secure delivery all types of apps to all users in all locations—but also enables a wide array of other business- critical initiatives while ensuring the highest levels of performance, security, availability, visibility and flexibility.



Citrix Partner**About Palo Alto Networks**

Palo Alto Networks™ is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks' platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks' products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks' products are used by more than 9,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, "The Network Security Company," the Palo Alto Networks Logo, App-ID, GlobalProtect, and WildFire are trademarks of Palo Alto Networks, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

**Corporate Headquarters**

Fort Lauderdale, FL, USA

India Development Center

Bangalore, India

Latin America Headquarters

Coral Gables, FL, USA

Silicon Valley Headquarters

Santa Clara, CA, USA

Online Division Headquarters

Santa Barbara, CA, USA

UK Development Center

Chalfont, United Kingdom

EMEA Headquarters

Schaffhausen, Switzerland

Pacific Headquarters

Hong Kong, China

About Citrix

Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was \$2.59 billion. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler, TriScale, NetScaler SDX, NetScaler MPX, NetScaler App Deliver Controller and XenDesktop are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.