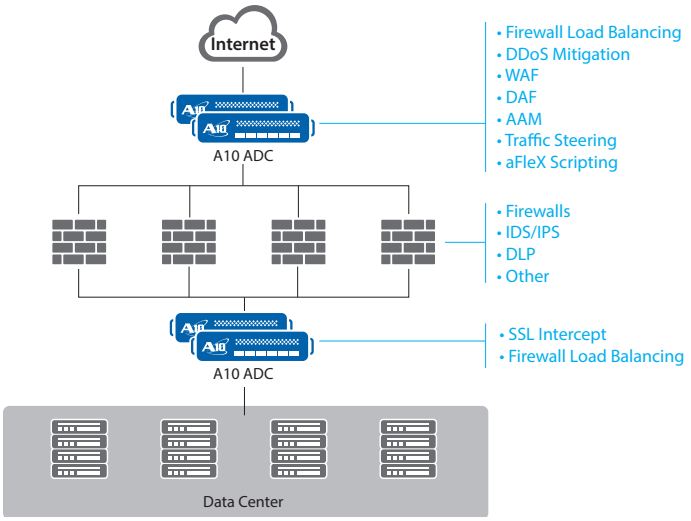
SCALING AND OPTIMIZING DMZ SECURITY

Optimizing Security Functions in the DMZ

Protecting Critical Applications

Every security professional has to tread the line between enforcing application security against increasingly sophisticated cyber attacks while also providing sufficient access for legitimate end users. If security is too tight, the application may become unusable for the end user; if security is too light, then an organization can be compromised, bringing revenue loss and brand damage. Almost every organization has applications that must be publically accessible, and as technology rapidly evolves, organizations are challenged to maintain this delicate balance between provisioning sufficient security and ensuring access for legitimate users.

- **Scaling security devices and encrypted communications** – As networks grow, existing security infrastructure needs to scale with it. As organizations increase their network capacity, they must consider transitioning to higher performance security devices (for example, firewalls), which can be both costly and complex. Securing content with encrypted communications (HTTPS, SSH, and so on) creates an inordinate load on these DMZ security devices, since they implement resource-intensive encryption and decryption functions in order to implement deep-packet inspection (DPI) and analyze application traffic. Organizations who do not decrypt and inspect traffic to unknown public sites create a blind spot that is left open for exploitation by data extrusion and malware, including advanced persistent threats (APTs).
- **Emerging volumetric DDoS attacks** – New types of security threats create new challenges for security staff, and one of the most prominent is the rise in distributed denial of service (DDoS) attacks that hit websites and key network infrastructure. Unlike targeted Web attacks, DDoS attacks flood publically available infrastructure with high volume network attacks and harder to detect application attacks, making the network and application servers unavailable for legitimate use. This problem is compounded when DDoS attacks cripple network infrastructure and applications that serve both external and internal users. Unavailable resources primarily threaten customer satisfaction, impact brand image and create revenue loss, but DDoS attacks are also being used to distract IT staff while other malicious activity occurs, for example theft from bank accounts[1].
- **Static application of security services** – Conventional network security services must be applied inline on a particular VLAN or subnet dedicated to the particular service or user group. Unfortunately, this means that expensive network security equipment must be overprovisioned to handle all loads at all times, regardless of what type of service each individual flow actually requires. As budget and resources are not infinite, an optimized and more flexible approach to applying service chaining dynamically, only when needed, would be optimal.



DMZ security device scaling, offload and acceleration

Scaling and Optimizing Your DMZ Security Infrastructure

A10 Networks offers a range of security products with the new premium A10 Thunder™ and the original AX Series application delivery controllers (ADCs), and the A10 Thunder Threat Protection System (TPS). Each is built on A10's Advanced Core Operating System (ACOS®) with rich security feature sets. These A10 products can help you significantly scale the efficiency and improve the security posture of your DMZ security infrastructure.

[1] http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/

Scaling security devices and encrypted communications is a critical requirement as your network grows in complexity and size.

- Firewall load balancing (FWLB) in the A10 Thunder ADC line enables simplified high availability (HA) and also maximizes the performance of your existing network firewalls. Firewalls support HA typically in an active/passive configuration, which can be costly to upgrade if additional performance is needed. FWLB scales your DMZ security equipment by adding additional firewalls as needed, avoiding the need to rip-and-replace existing devices, while also offloading resource-intensive functions from performance constrained security devices (such as SSL offload, DDoS mitigation, white and blacklists). FWLB enables easy firewall maintenance, minimizing network interruption by load-balancing the traffic among the available firewalls, ensuring resilient, adaptable firewall operations.
- TLS/SSL encryption, used for HTTPS, is the most common secure network communication method for sensitive Internet data from your internal servers to users outside your organization's firewalls. The SSL handshake and bulk encryption operations are CPU-intensive tasks, affecting the performance of firewalls, intrusion prevention systems (IPS) and other DMZ security devices that must process application content in clear text. Acting as a reverse proxy, the SSL offload feature enables Thunder ADCs to offload SSL transactions from these security appliances, freeing compute resources to focus on their more value-added analytics and security functions. SSL offload optimizes your DMZ security infrastructure and ensures that it can scale with increased encrypted traffic loads.
- **The SSL intercept feature** is a forward proxy that eliminates blind spots in corporate defenses by decrypting internally generated user traffic headed to the Internet through the DMZ. Similar to SSL offload, SSL intercept decrypts and inspects traffic before forwarding it to DMZ security devices to enforce security policies on outbound traffic (for example, firewalls, IDS/IDP and DLP). The data is then encrypted again and sent to its final external destination. The A10 ADC platform's dedicated SSL security processors offload CPU-intensive SSL encryption functions to allow security devices to be utilized for core inspection and mitigation functionality.

Emerging DDoS attacks are becoming increasingly problematic due to escalation in size, frequency and bandwidth volume. These attacks leverage large distributed networks of botnets that use legitimate protocols to overwhelm network and server resources, circumventing conventional signature-based security devices. And, since DDoS attacks often leverage large-scale volumes measured at many gigabits per second, they can overwhelm the relative low performance of most security devices. As a result, newer and higher performing DDoS detection and mitigation solutions are needed in the DMZ.

- DDoS detection and mitigation solutions are available in our ADC product lines to further protect and offload DMZ security appliances from the load of these volumetric attacks. The ADC and TPS products provide DDoS security features that protect against multi-vector attacks, including both network-layer and application-layer attacks such as slow HTTP attacks (like Slowloris), high volume TCP SYN floods and anomalous protocol usage.

Selectively apply dynamic security service chains to ensure that each application or user group selectively receives appropriate security policies, while offloading DMZ security infrastructure from processing all packets inline.

- **Traffic steering and service chaining** technology enables redirection of flows based on specific attributes, which may be protocol or content-based. A10 ADC appliances can redirect traffic types based on their "fingerprints" to the appropriate service for optimization or security processing. This improves network efficiency as service chaining policies ensure that only traffic that requires processing by each specific security device is sent to that device, which scales and optimizes your investment in those resource constrained security devices. With our open API (aXAPI®) and ICAP support, interaction with the traffic management controllers and the redirect policy can be updated dynamically.

Summary

A10 products offer a variety of solutions to solve challenges and problems for your security and DMZ environment, while ensuring that your applications remain highly available, accelerated and secure.

A10 Thunder products are selected by many organizations today for multiple factors, including having all basic and advanced features provided with an all-inclusive ADC or TPS license, and a flexible choice of form factors to support your specific network needs.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: 19101-EN-03 Feb 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
brazil@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.