Ultra-High-Performance Data Center Protection in a Compact Appliance

Unleashing the power of Thunder Convergent Firewall

Challenge:

Protect data center services and assets from increasingly sophisticated threats, while providing a high-performance solution that can scale with growing traffic demands.

Solution:

Data Center Firewall (DCFW) is included with A10 Thunder CFW and provides unprecedented performance and scalability to protect against advanced threats, web application and DDoS attacks. Thunder CFW is a flexible security solution that consolidates a suite of advanced features in a single physical or virtual appliance.

Benefits:

- All-inclusive security feature set
- Multi-tenant support providing secure traffic path isolation
- Compact and efficient design with multiple port configuration options
- Single interface to manage multiple security feature sets
- Full IPv4 and IPv6 feature parity on both data and management interfaces
- Complete data and control plane separation

The data center firewall is a critical element in protecting valuable data center assets and one of the most important components in an organization's overall security policy. The performance and stability of the data center firewall is crucial in ensuring that the availability of services is not disrupted and that response times are not degraded by latency, which could impact application performance. Poor performance factors, such as application delay and packet loss, can also result in a significant financial impact.

A10 Networks® Thunder® Convergent Firewall (CFW) enables the ultra-high-performance data center with an all-inclusive security feature set. This includes stateful Data Center Firewall (DCFW), Web Application Firewall (WAF), DNS Application Firewall (DAF), Application Access Management (AAM), Application Layer Gateway (ALG) support, Distributed Denial of Service (DDoS) mitigation, and advanced Layer 4 through Layer 7 server load balancing.

The Challenge

There are certain metrics that should be considered when implementing a firewall for the data center as compared to implementing a firewall to protect a corporate network perimeter. Performance characteristics of the data center firewall are extremely important due to the high volume of traffic, which is much greater than protecting Internet access at the edge of the corporate network. Traffic patterns and policy enforcement will be different, and this affects the data center firewall's packet inspection process during heavy loads. Traditional north/south traffic patterns between clients and the data center have evolved to include east/west traffic between application and database servers, as well as inter-data center traffic between data centers and the public/private cloud.

The firewall needs to inspect the various flows of traffic within the data center to apply appropriate policies, and organizations are challenged with the task of optimizing traffic paths. This is especially true in hybrid data center environments, where there is a continuing migration to inter-VM traffic. To address multiple flow directions within the data center, the implementation of distinct classification zones to enforce specific security policies and provide data confidentiality may be desired. This requires the data center firewall to provide the flexibility to partition and separate flows, where each zone can contain unique security polices and interfaces. By isolating data center traffic, methods such as redirecting and hair-pinning east/west traffic to existing north/south firewall interfaces can be avoided, and optimal traffic paths can be utilized. This type of functionality can also be used to isolate departmental traffic without the requirement to implement separate firewalls.

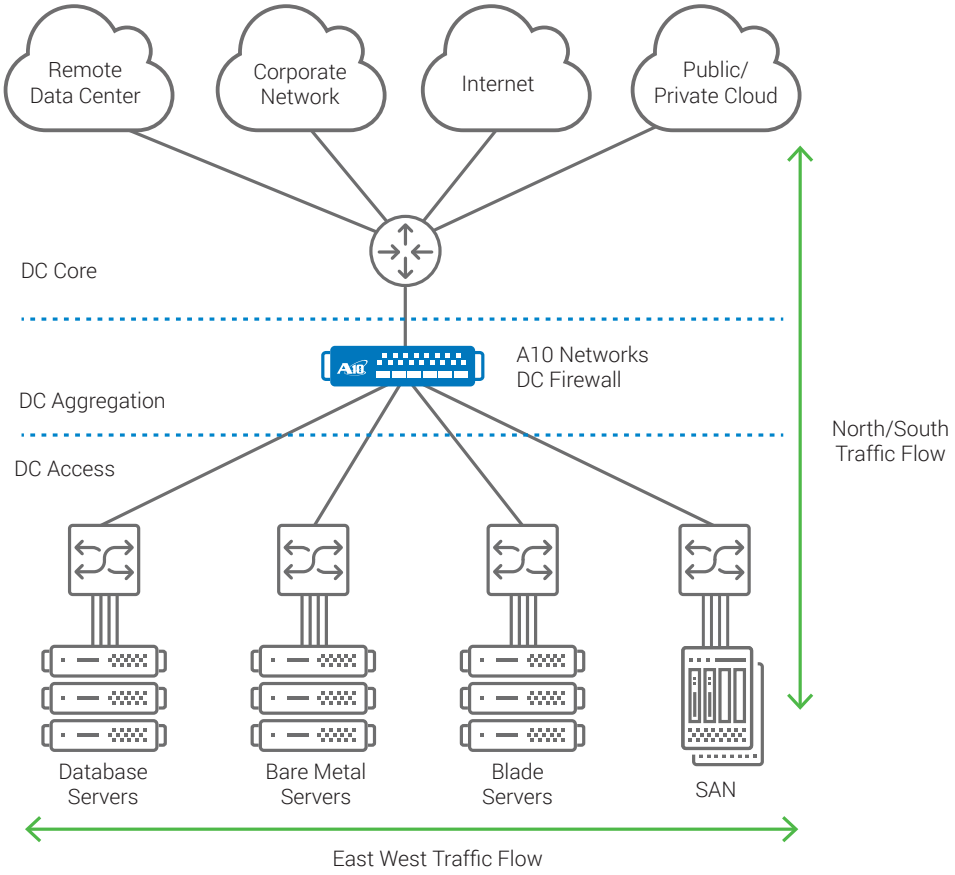

Figure 1: Traffic flows within the data center

The data center firewall must be able sustain high throughput, support hundreds of thousands of sessions accessing server farms, and also process high TCP connection rates because of the constant setup and tear down of connections to the application servers.

The A10 Networks Data Center Firewall Solution

A10 Networks Data Center Firewall (DCFW) is an extremely high-performance stateful firewall that provides up to 220 Gbps throughput, support for 6.5 million connections per second (CPS), and a connection table which can address up to 256 million concurrent sessions for large data center applications. The A10 DCFW also supports up to 128K firewall rules to accommodate large multi-tenant environments.

The A10 DCFW is included as a standard feature in the A10 Thunder CFW product line, which also incorporates several other security elements, such as a Web Application Firewall (WAF) and DNS Application Firewall (DAF). A10 Thunder CFW supports Application Delivery Partitions (ADPs) that allow Thunder CFW to be logically partitioned into independent Layer 3 domains to isolate traffic flows and apply individual sets of security features to various traffic types.

Protect Multi-Tenant Environments

Organizations around the world have embraced cloud computing, virtualizing their data centers to improve operational efficiency, agility and scale. Trends such as continuous application deployment, Network Functions Virtualization (NFV) and Software Defined Networking (SDN) all require automation, which requires complete programmability. Data center firewalls must adapt to this new paradigm, supporting virtual deployment, on-demand scaling and cloud orchestration. Thunder CFW with an integrated data center firewall leverages the A10 Harmony™ architecture to deliver completely programmable security for the data center. A10 Harmony unifies policy control, offers unprecedented telemetry and provides 100% RESTful API coverage.

The A10 Thunder CFW provides support for Layer 3 virtualization (L3V), which allows independent Application Delivery Partitions (ADPs) to be created that have direct access to their own networking and application resources. Each L3V ADP is an independent L3 domain that allows for complete traffic path separation in multi-tenant environments. Dictated by different security or traffic policies, unique security profiles can be created. One ADP can support stateful firewall with DDoS mitigation, while another ADP might include WAF support for HTTP traffic inspection and enforcement. With the Thunder CFW load-balancing support, an ADP can be dedicated to a specific application, such as DNS server load balancing with the DNS Application Firewall (DAF) enabled.

Management of each ADP can be administered separately, allowing different groups within an organization to manage their own resources. The L3V ADP support is available on both A10

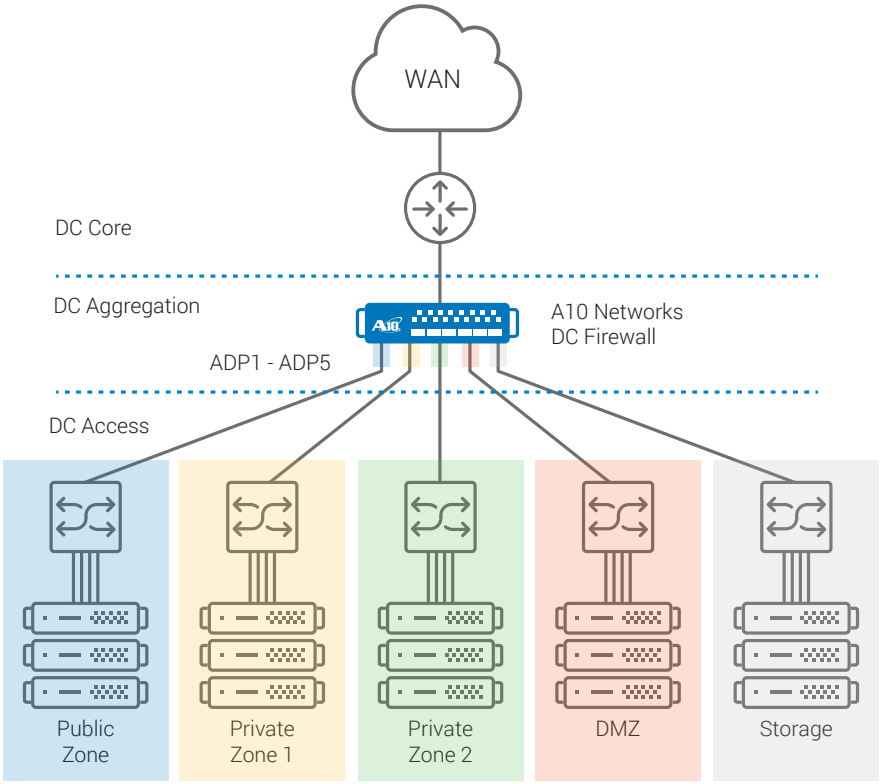

Figure 2: Data center traffic classification zones

Thunder CFW physical and virtual appliances. The Thunder CFW L3V ADP support provides the flexibility to address various security requirements in a multi-tenant data center environment using a single security platform.

Web Application Firewall (WAF)

A10's Web Application Firewall (WAF) guards web servers against the critical Open Web Application Security Project (OWASP) top ten threats facing web-based application servers. The WAF inspects both the traffic towards the web application and the response traffic from the application. By securing both the web application infrastructure and the application user, the WAF complements the A10 DCFW to add protection at a more granular level.

A10's WAF feature is designed to recognize many of today's threats, with flexibility to customize checks for emerging threats. Instead of integrating third-party WAF code, as many other vendors do, A10 has developed the WAF specifically for A10 Networks Advanced Core Operating System (ACOS®). This approach results in a highly scalable and high performing security solution.

The WAF also enables a full defense stack with other A10 security mechanisms in order to protect web applications, ensure against code vulnerabilities and prevent data leakage; this aids in regulatory security compliance, such as Payment Card Industry Data Security Standard (PCI DSS) requirements.

DNS Application Firewall (DAF)

A10 DNS Application Firewall (DAF) is included with the A10 Thunder CFW and is designed to ensure that the DNS infrastructure is protected and DNS server resources are optimized. A10 DAF inspects all DNS traffic to verify that it is legitimate, and it blocks or redirects malicious traffic for additional inspection.

DNS attacks, such as sending malformed DNS packets from spoofed source IP addresses, can be easily stopped by dropping traffic that does not conform to standard DNS packet types. By providing high-performance traffic surge protection using IP rate limiting, DNS servers are protected against flood attacks, so valuable resources are available to process DNS traffic or address increased periods of load.

Attackers can also exploit DNS servers by sending requests using unusual query types or Opcodes. Thunder CFW can be configured to allow or deny certain DNS query types and specific DNS Opcodes. The A10 DAF provides advanced protection against DNS infrastructure exploitation with granular application rules for query behavior and mitigation methods, such as IP rate limiting.

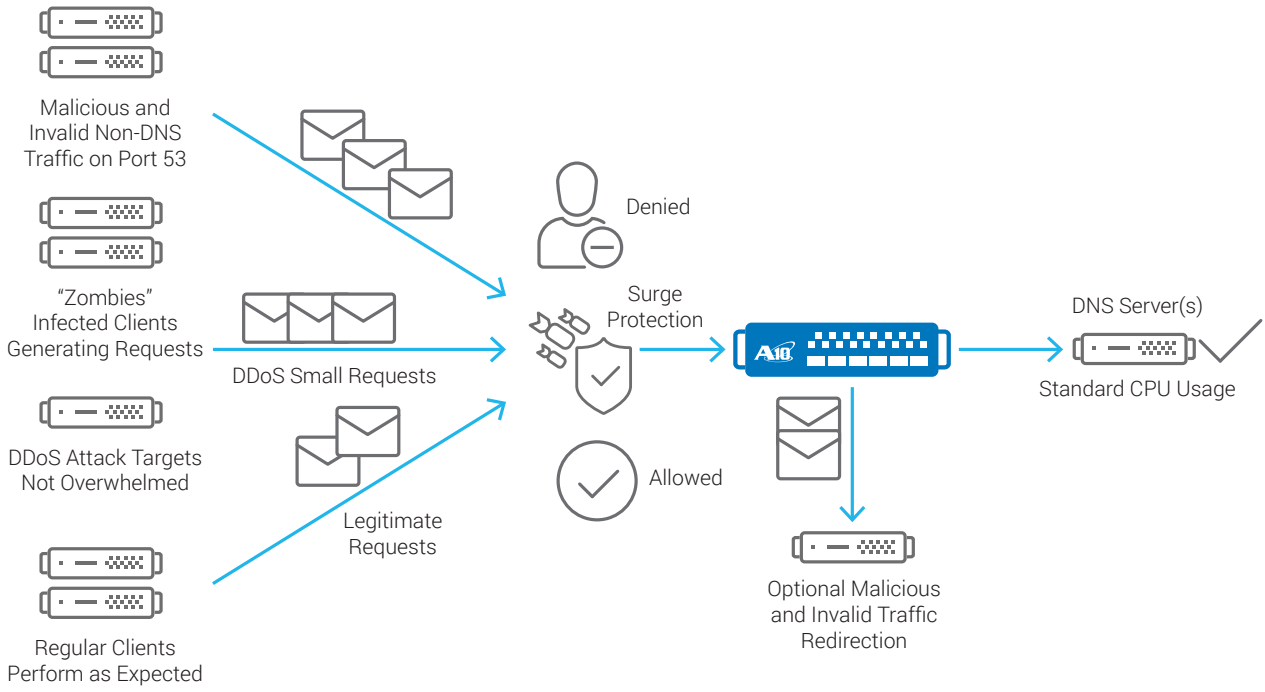

Figure 3: The DNS Application Firewall can detect attacks, non-DNS traffic and DNS queries from known malicious clients.

Features and Benefits

Comprehensive and Scalable Management

To streamline and automate management, Thunder CFW includes an industry standard CLI, a web user interface, and A10 Networks aXAPI® REST-based API, which can integrate with third-party management systems. For larger deployments, the A10 Networks aGalaxy® Centralized Management System ensures that routine tasks can be performed at scale across multiple Thunder CFW appliances, regardless of physical location.

Logging and Reporting

Thunder CFW supports high-speed syslog logging as well as email alerts and NetFlow and sFlow statistics for traffic analysis. A real-time dashboard displays system information, memory and CPU usage, as well as network status.

Lower OPEX and CAPEX

A10 Thunder CFW reduces data center costs by consolidating multiple security services on a single, powerful platform. This reduces the number of network devices required, lowers power consumption and cooling costs, and saves valuable rack space.

The A10 Data Center Firewall takes unification a step further by converging not just security but also networking and application delivery features where it makes sense, empowering organizations to eliminate single-purpose devices from their data centers and reduce hardware and operating costs. Because firewall policies are fully integrated into the ACOS operating system, customers can use load balancing and security features simultaneously without impacting performance. Operational costs are further reduced because multiple security and application delivery features can be managed using a single management interface.

Solution Components

- Thunder Convergent Firewall (Thunder CFW)
- Data Center Firewall (DCFW)
- aGalaxy® Centralized Management System
- aXAPI® REST-based API

Summary – Ultra-High-Performance Data Center in a Compact Appliance

The Data Center Firewall feature set is included in the A10 Thunder CFW along with several other key components to provide a powerful and flexible security solution. Thunder CFW is built on A10's Advanced Core Operating System (ACOS) platform, with a Symmetric Scalable Multi-Core Processing (SSMP) software architecture, which delivers the ultra-high performance needed to meet current and future data center traffic loads.

Thunder CFW is a very high performing security solution in a compact appliance, allowing organizations to stop emerging threats at scale. Combining a Shared Memory Architecture and Flexible Traffic Accelerator (FTA) technology, the Data Center Firewall offers ultra-high throughput and unmatched connection rates, eliminating traditional performance bottlenecks while protecting data center assets.

Next Steps

For more information, please contact your A10 representative and visit: www.a10networks.com/firewall.

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: A10-SB-19157-EN-01
Apr 2016

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@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.