Solution Brief

Ultra-high-performance Data Center Security

Unleashing the power of Thunder Convergent Firewall (CFW)

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 a comprehensive security feature set. CFW includes a data center firewall (DCFW), secure web gateway, IPsec VPN, carrier-class firewalls for mobile networks, and secure application delivery.

Thunder CFW includes all Thunder ADC, CGN and SSLi features.

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.

Challenge

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

Solution

A data center firewall is included with A10 Thunder CFW and provides unprecedented performance and scalability to protect against advanced threats and 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

- Comprehensive 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

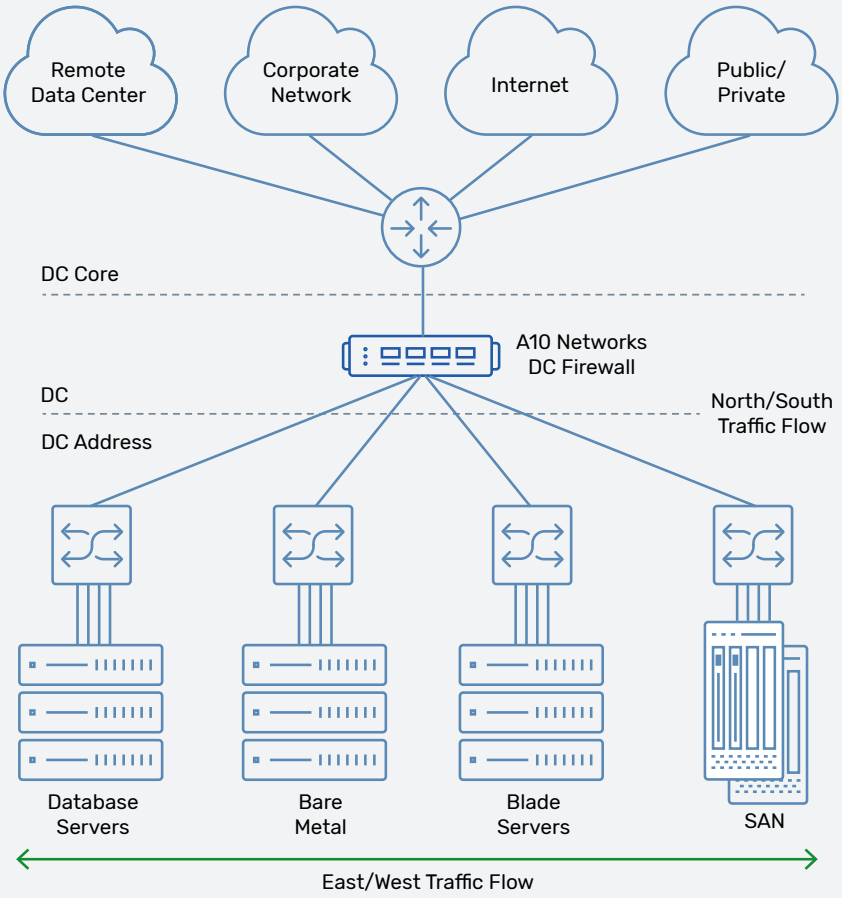

Figure 1: Traffic flows within the data center

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 used. This type of functionality can also be used to isolate departmental traffic without the requirement to implement separate firewalls.

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

The A10 Networks Data Center Security Solution

A10 Networks data center firewall is an extremely high-performance stateful firewall that provides up to 370 Gbps throughput, support for 8 million layer 4 connections per second (CPS), and a connection table that can provide enough capacity to support up to 384 million concurrent sessions. 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 secure web gateway, IPsec VPN, and carrier-class firewall. Thunder CFW also helps eliminate single-purpose devices from data centers by consolidating security and application delivery controller (ADC) features on one platform to reduce hardware and operating costs.

Protect Multi-tenant Environments

Organizations around the world have embraced cloud computing, virtualizing their data centers to improve operational efficiency, agility and scale. 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 Controller provides visibility and analytics and offers unprecedented telemetry as well as 100 percent RESTful API coverage. The product supports multi-tenancy features like application delivery partitions (ADP) for segmentation.

Management of each ADP can be administered separately, allowing different groups within an organization to manage its own resources.

Application Awareness and Control

The A10 DCFW supports application awareness and control to identify malicious, harmful, or unwanted applications and suspicious behavior patterns, mapping them to the appropriate security threat/risk level and enforcing policy according to the business logic. The DCFW also monitors usage per application and category and collects and exposes monitored data via logging and statistics.

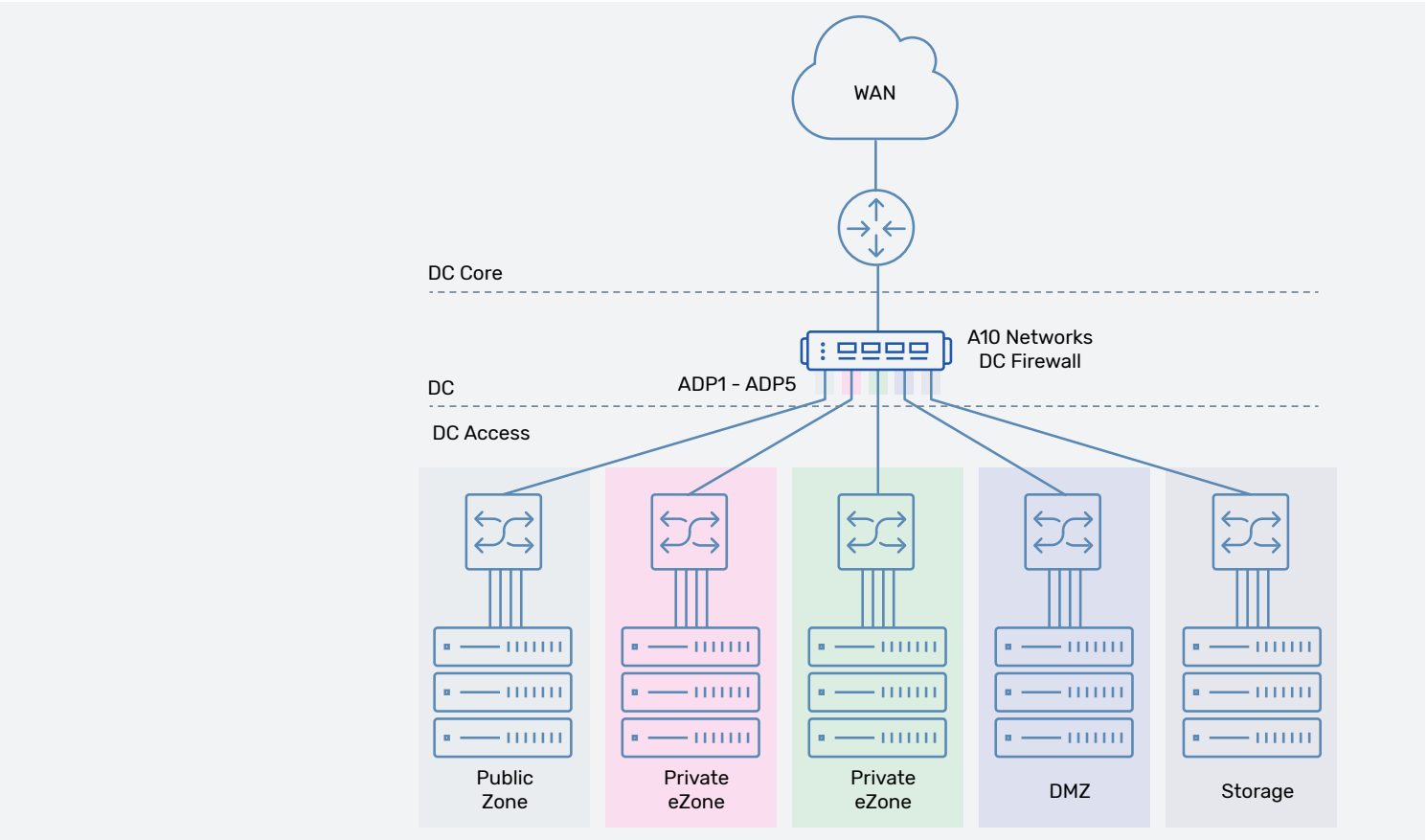

Figure 2: Data center traffic classification zones

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 Harmony Controller 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 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 A10's Advanced Core Operating System (ACOS®), customers can use load balancing and security features simultaneously without impacting performance. Operational costs because multiple security and application delivery features can be managed using a single management interface.

Solution Components

- Thunder Convergent Firewall
- Data center firewall
- A10 Harmony Controller
- aXAPI® REST-based API

Ultra-high-performance Data Center Security 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 the 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. 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.

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally. For more information, visit a10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us
a10networks.com/contact

Part Number: A10-SB-19157-EN-02 NOV 2021