FORTINET

Solution Brief

Application Delivery Network Solutions from Fortinet

Building a high-performance, secure application delivery infrastructure for your mission-critical applications

Introduction

As applications become more complex and security threats increase everyday, delivering applications to end-users only continues to get more challenging. You need to ensure your application delivery infrastructure can meet the performance needs of your business and keep it is safe from the latest threats today and in the future.

The Fortinet application delivery network (ADN) is a framework that unites your datacenter elements so that applications are available, responsive, and secure. There are many considerations and options available that can meet your basic needs. In order to optimize application delivery, you need an integrated single-vendor solution that won't cause bottlenecks or create unwanted security loopholes.

Fortinet's application delivery controllers (ADCs), network security platforms, link load balancers, Web Application Firewalls (WAF) and global server load balancing (GSLB) products provide everything you need to build a high-performance and secure application delivery infrastructure that is flexible and ready to grow with your business.

Start with Your Application Needs

It's a good idea to first start with building a traffic profile for your applications. By defining your needs up front, you'll be sure to buy the right ADN solution that fits your criteria and your budget. Below are some of the elements you should consider in this step:

- Application technologies/platforms
- Number of users
- Bandwidth/transaction sizes
- Application symmetry

Application Challenges

- Availability
- Scalability
- Performance
- Security
- Continuity
- Cost reduction

Deployment

- FortiADC™
- FortiGate®
- FortiWeb™
- AscenLink™
- FortiDirector™

Segments

- Small/Medium Business
- Enterprise
- Datacenter
- MSP

- Response SLAs
- Demand profiles (peak/off-peak)
- SSL and security
- Application growth trends

After you have a good idea of the application traffic profile, then you should look at the needs of your environment:

- Capacity of your current infrastructure
- Existing infrastructure integration
- Hardware, virtual and hybrid needs
- Infrastructure topology
- Redundancy and Disaster recovery
- Evolution, growth and future technologies

Once you've completed your assessment of your application and environment you'll have the criteria to evaluate an ADN solution based on performance and features.

The Core Elements of an ADN

An ADN is an end-to-end model for all the elements that deliver applications to users. The ADN typically consists of an application delivery controller, firewall and a link load balancer. In Figure 1 you can see all the typical elements of an ADN–the Server Side, Security and the Outer Perimeter.

Server Side

Once your applications outgrow a single server you need to add scalability, which means adding additional server resources. In most cases, these servers are added alongside the other servers in your data center. With this comes a series of new challenges such as traffic management and server resource leveling. An application delivery controller manages multiple servers in a cluster or clusters to allow applications to scale beyond a single server, in effect creating a single virtual server. ADCs manage resources to route users to the best available servers and can route traffic to specific destinations using configurable rules. They also can provide additional features like the offloading of secure traffic to alleviate server encryption/decryption processing, and HTTP compression to reduce bandwidth needs for content-rich applications.

Security Core

The Security Core provides the tools and services to defend your application from basic and advanced threats. Here's where you need a strong firewall, VPN, antivirus/antimalware scanning, and other security features. Next Generation Firewalls (NGFW) include intrusion prevention systems (IPS) with deep packet scanning, application control and user access policies to provide comprehensive protection.

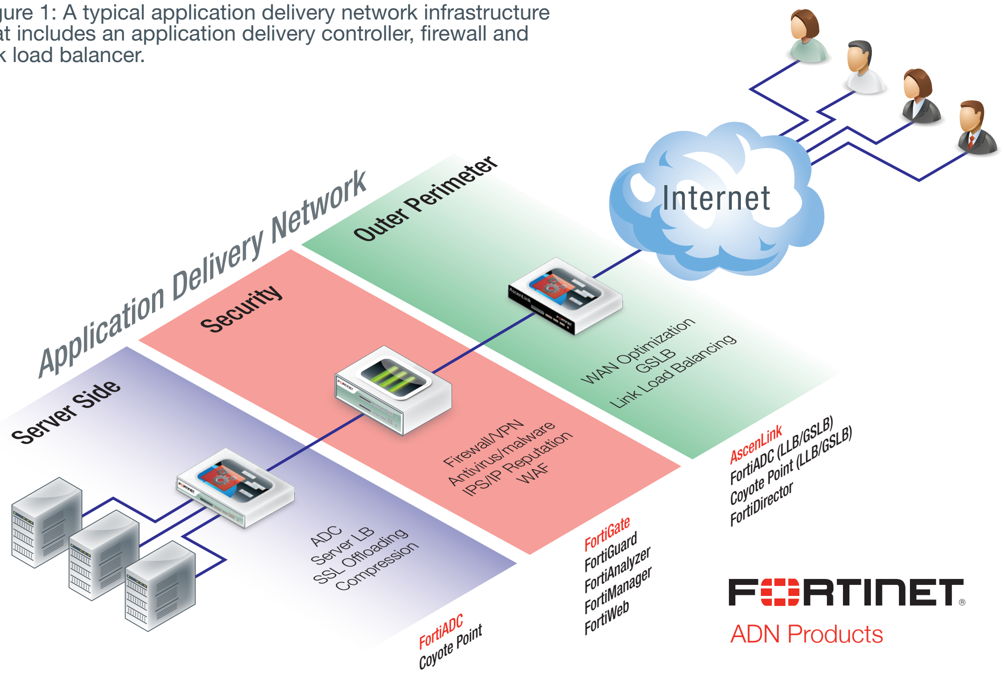
Web Application Firewalls (WAF) are another next-generation technology targeted at protecting web-based application traffic using advanced techniques to provide protection against malicious sources, application layer DoS attacks and threats like SQL injection and Cross-site scripting,

Outer Perimeter

In simple cases a single link to an ISP opens your application to the outside world. With larger applications that require more bandwidth, redundant connectivity, span multiple datacenters or that serve geographically diverse locations you're going to need more than one WAN link.

Basic Link Load Balancing (LLB) addresses bandwidth and redundancy through the use of multiple WAN links. A link load balancer connects many WAN links to the network and routes inbound and outbound traffic based on things like availability, performance, or business rules to use lowest-cost links. If a link should fail, traffic is routed to others to ensure your application remains available to users.

Figure 1: A typical application delivery network infrastructure that includes an application delivery controller, firewall and link load balancer.



Things get more complicated when applications expand across multiple data centers for disaster recovery or to better serve remote locations. Global Server Load Balancing (GSLB) simplifies this by using a DNS-based resolution platform that routes traffic between two or more datacenters. If a datacenter should go down, traffic is automatically routed to another, or you may opt to map your users to the closest datacenter to improve application performance.

Single or Multiple Components

The Server, Security and Perimeter elements can be separated out or can be combined to 2 or even one appliance. You should select an option based on performance, redundancy, interoperability, and management.

Performance: Devices that combine one or more of the ADN components (e.g. an ADC with a firewall and link load balancing) eliminate many of the bottlenecks of passing data between devices. However, there's a trade-off as a single appliance only has so much processing power to handle all these tasks generally limiting this type of solution to smaller to mid-sized application environments. By separating the elements out using different appliances you can scale the ADN to support significantly larger applications.

Redundancy: Single points of failure are the greatest risk to application downtime. Regardless of single or multiple device combinations, any component that fails will affect your application with varying degrees of impact. A single device or an ADC failure will take the application down for everyone. A firewall or link load balancer failure will affect users on the external network. High Availability and fault-tolerant device failover helps to mitigate appliance failures. Even a single device can be configured to provide 100% uptime if it is used in a fault-tolerant configuration or in combination with GSLB to route traffic to another datacenter.

The FortiADC-300E Application Delivery Controller delivers a complete end-to-end ADN in a single appliance with server load balancing, firewall and link load balancing.

Interoperability: Best of breed, single manufacturer, or legacy hardware? A single device simplifies this, however in many cases the ADN exists in a broader IT infrastructure. It is important that you understand the needs of your environment as it relates to interoperability and choose a solution that supports basic things like SNMP and open APIs. A single manufacturer like Fortinet will offer additional integration between elements to simplify inter-box connectivity and traffic management.

Single vs. Multiple Components

	Single Appliance	Multiple Components
Pros	Minimized bottlenecks Reduced interoperability complexity Simplified management	Higher throughputs Lower risk of single point of failure Flexibility in upgrades/expansion
Cons	Lower Capacity limits Higher risk of single point of failure Limited upgrades/expansion	Inter-device bottlenecks More complex interoperability Complex management

Management: A single combined device simplifies management, reporting and visibility. For multiple appliance solutions you have three options to manage a multi-device environment–custom scripting, an integrated platform or manage everything manually. In a custom-scripted environment you have to configure each device to operate with your management tools. Optimally you should be looking for devices that interoperate seamlessly and are integrated into a centralized management console.

Building a Fortinet ADN

When you review the options on the market today, most manufacturers focus on one of the three main parts of the ADN with other elements treated as an afterthought. We start with security first, however we make sure our products deliver on speed, reliability and have the features you need to build an entire ADN solution.

For smaller application environments we offer single device options like full-featured FortiADCs that include server load balancing, firewall, link load balancing and GSLB. Fortinet also offers all the components you'll need to build a high-performance, secure ADN for enterprise and datacenter environments using FortiADC application delivery controllers, FortiGate network security platforms, FortiWeb Web Application Firewalls, AscenLink link load balancers, FortiDirector cloud-based GSLB and other products you'll need to protect, control and manage your infrastructure.

FortiADC – Application Delivery Controllers

FortiADCs deliver class-leading server load balancing and application traffic management solutions to optimize the availability, user experience, and performance of mobile, cloud-based and enterprise applications. All our FortiADCs include the latest firewall, link load balancing and GSLB technologies for a complete ADN in a single hardware or virtual appliance.

FortiGate – Network Security Platforms

The award-winning FortiGate Network Security Platform delivers unmatched performance and protection while simplifying your network. Fortinet offers models to satisfy any deployment requirement, from the desktop FortiGate-20 series for small offices and retail networks to the chassis-based FortiGate-5000 series for large enterprises, service providers, data centers and carriers. FortiGate platforms integrate the purpose-built FortiOS™ operating system with custom FortiASIC™ processors and the latest-generation CPUs to provide comprehensive, high-performance security.

FortiWeb – Web Application Firewalls

FortiWeb web application firewall protects your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS attacks and sophisticated threats like SQL injection and Cross-site scripting. FortiWeb platforms help you prevent identity theft, financial fraud and denial of service. It delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

AscenLink – Link Load Balancers

Fortinet AscenLink integrates multiple low cost WAN links to perform on par with expensive leased lines. It reduces ISP subscriber charges to a fraction of a leased line rental, while load balancing and bandwidth management reduces overhead. Tunnel Routing technology delivers link aggregation and fault tolerance over multiple links to ensure optimum delivery of delay sensitive applications.

FortiDirector – Cloud-based GSLB

The FortiDirector Global Server Load Balancing (GSLB) Service is a cloud-based approach to solving the complexities of expanding applications across multiple data centers for disaster recovery, improved performance and reduced delivery costs.

The Benefits of a Fortinet ADN

Whether you opt for a single component option like a FortiADC or a multi-appliance Fortinet infrastructure for your ADN, you'll be guaranteed you'll get the security, performance, and interoperability to meet the demands of almost any application environment.

Security: Fortinet is a leader in network security and unified threat management. All our products build on that expertise to ensure your ADN is protected today and in the future.

Performance: All of Fortinet's appliances and virtual products are built to perform. From FortiGate's latest FortiASIC NP6 processor that delivers unmatched price and performance to new FortiADCs that can deliver up to 30 Gbps of throughput, Fortinet delivers security and cutting-edge performance.

Interoperability: When you buy a Fortinet solution, you get an integrated ADN. Our products are designed to leverage and seamlessly interoperate with other Fortinet products and services like FortiManager and FortiAnalyzer. We optimize and test our products to minimize bottlenecks to increase overall performance between platforms when used together in an ADN.

Other Fortinet Products

There are many other components that can comprise a comprehensive ADN infrastructure. Fortinet offers a wide array of products that can add advanced threat protections like FortiGuard Threat Protection Services and FortiWeb Web Application Firewall.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480