SSL Visibility and Inspection with FortiADC

FortiADC's ASIC-powered SSL processing can offload cryptographic functions from firewalls and intrusion prevention systems for high-performance encrypted threat detection and mitigation

SSL Offloading has been a foundational feature of modern application delivery controllers (ADCs) going back for the past 10 years. Most applications now employ SSL/TLS to protect traffic as it traverses the internet, however the encryption and decryption of secure traffic to "clear text" is highly processor intensive.

In the early days of secure applications, the cryptographic functions of encryption and decryption were handled by servers, however they were limited in what they could process. Even today the best data center servers can only manage transaction loads in the hundreds of transactions per second. The latest 2,048 and 4,096 encryption keys strain servers, effectively rendering them unable to process SSL transactions on their own.

Every modern ADC offers SSL offloading to alleviate the encryption and decryption functions from servers. Entry model ADCs offer primarily software-based SSL/TLS cryptographic engines that are adequate for smaller application environments. Mid-range and enterprise data center models feature hardware-accelerated SSL ASICs that dramatically increase the transactional processing capability. A typical ADC with software-based SSL can offload a few thousand secure transactions a second, where hardware-accelerated models increase this by a factor of 10 or more.

CHALLENGE

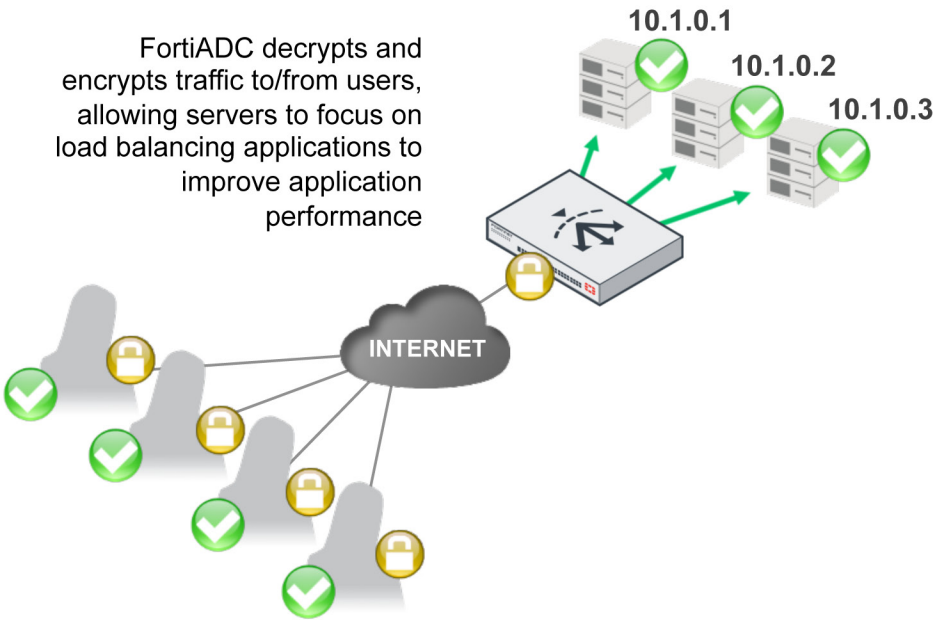
- Identify and mitigate threats in encrypted traffic
- Provide seamless and secure user experience
- Minimize firewall and IPS performance degradation

SOLUTION

- FortiADC to offload SSL traffic from servers and firewalls
- FortiADC and FortiGate for encrypted threat mitigation
- FortiADC SSL Visibility for secure traffic threat analysis

BENEFITS

- Seamless inspection and mitigation for threats in encrypted traffic
- Offloads encryption/decryption from FortiGate for improved performance
- Flexible deployment options for passive and active threat detection



The Rise of Encrypted Threats

By the end of 2016, it is predicted that over two-thirds of all internet traffic will be encrypted. While this is great for the protection and security of data in motion across the internet, it presents a challenge for traditional inspection devices like next generation firewalls and intrusion prevention systems (IPSs) to keep up.

Many organizations assume that SSL/TLS traffic is secure and protected from threats. This is partially true as the risk of tampering with the traffic is highly unlikely, especially with the larger encryption keys in use today. However, this does not mean that the contents of the secure traffic are secure. For example, if an infected file is downloaded securely from a well-known file sharing service, it's still infected when it's received by the end user.

As more and more enterprise applications are moved to the cloud, the amount of encrypted traffic through the data center to users is increasing dramatically. Traditional firewalls and IPS devices can decrypt, inspect and re-encrypt this traffic, however it usually comes at a significant cost to overall performance.

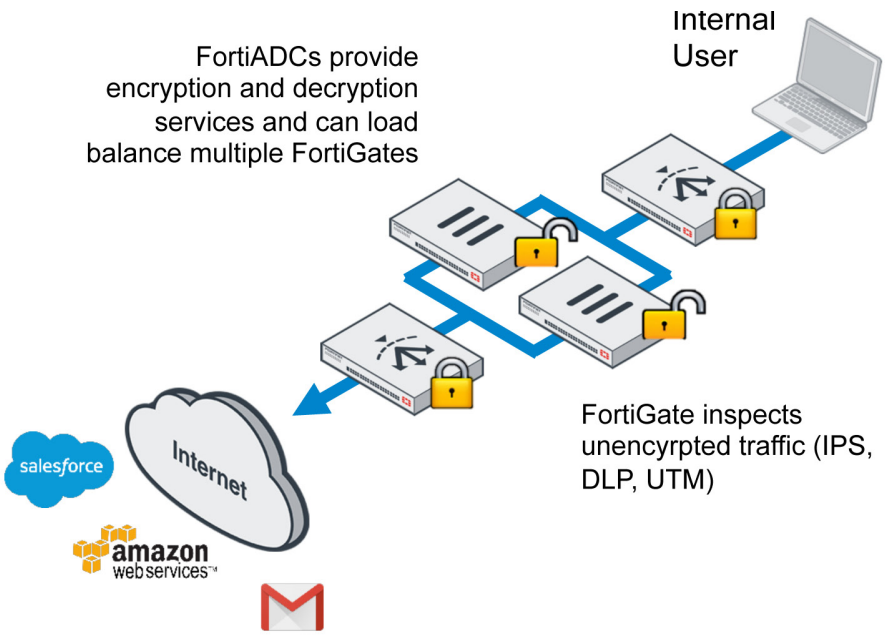
Detecting and Mitigating Encrypted Threats with FortiADC

In addition to being a high-performance application delivery controller with advanced SSL offloading features, FortiADC can be deployed to provide decryption and re-encryption services to other data center security platforms for threat inspection of secure traffic content.

FortiADC offers two primary deployment configurations; SSL Inspection (Forward-Proxy) for active threat detection and mitigation, and SSL Visibility for passive threat detection and analysis.

SSL Inspection with Active Threat Mitigation

In this configuration, an inspection device such as a FortiGate firewall or IPS is "sandwiched" between a pair of FortiADC appliances in an inline configuration. The FortiADCs at the front and rear of the configuration decrypt all secure traffic to "clear text" that is then passed to the inspection device to detect and mitigate threats. If the traffic passes inspection, the firewall or IPS passes the traffic back to the FortiADC for re-encryption and on to its destination.

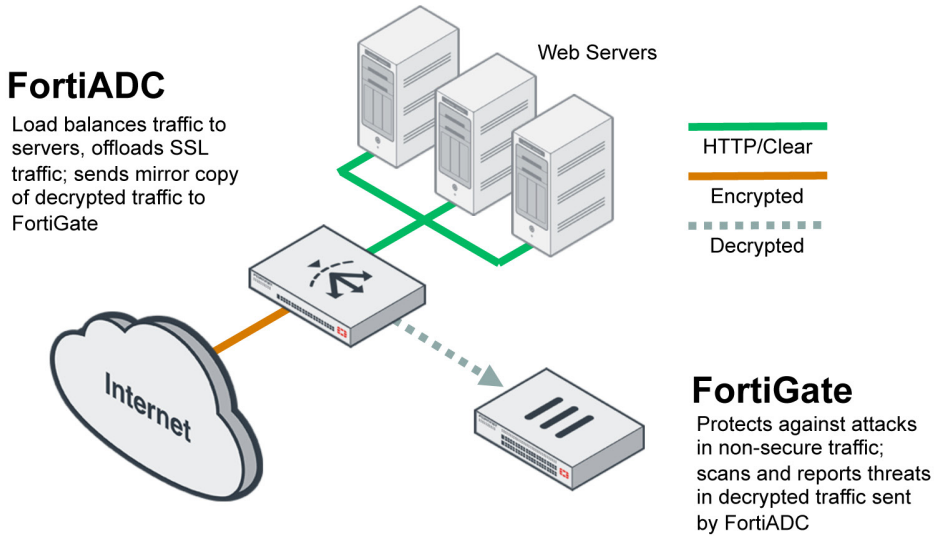


This configuration supports all inbound and outbound traffic from a data center and to the internet. FortiADC supports FortiGuard' Web Filtering Service where trusted groups of websites such as financial services or healthcare-related sites can be exempt from this inspection for privacy or compliance reasons.

Additionally, FortiADC can support load balancing of traffic to multiple firewalls that are deployed between the pair of FortiADCs. This can be used to add additional capacity for inspection while maintaining encryption for traffic entering and leaving the cluster.

SSL Visibility for Inspection Only

Using FortiADC's HTTP/S and TCP/S Mirroring feature lets users configure a duplicate un-encrypted data stream to be sent to another device for inspection and analysis. In this deployment typically a single FortiADC is used to provide SSL offloading for secure application traffic, however a copy of the decrypted traffic is sent off to a firewall or IPS/Antivirus for threat detection.



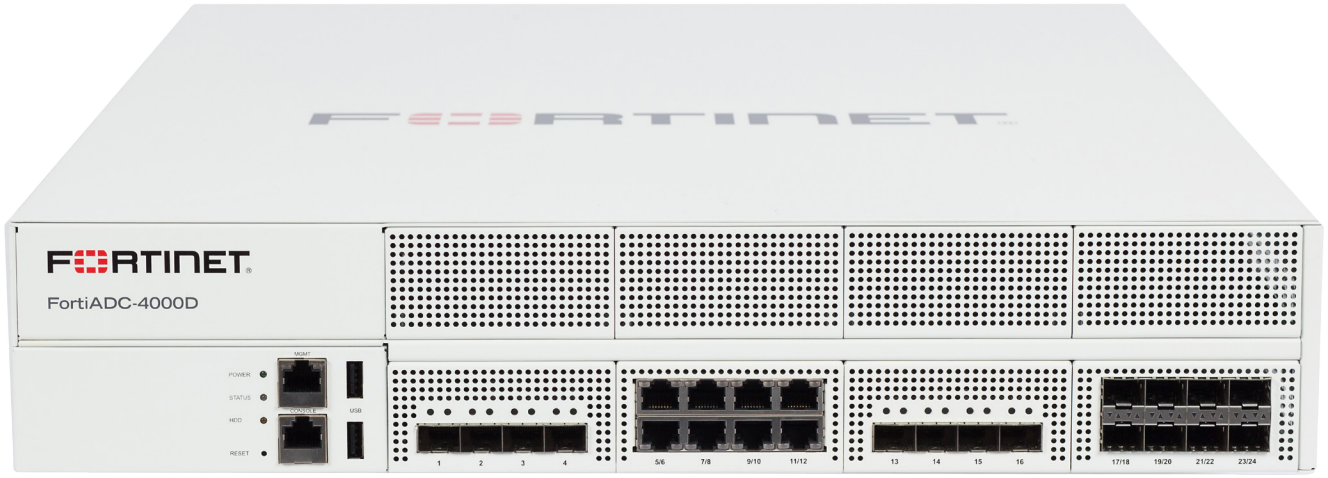
Unlike SSL Inspection and Mitigation, this setup only allows for the detection of encrypted threats in a passive manner. If a threat is detected, it is logged by the detection device for alerting or analysis purposes.

Benefits of FortiADC for SSL Visibility and Inspection

- Up to 34,000 transactions per second for enterprise-grade SSL encryption/decryption with a 2048 key size
- Dual-purpose solution for secure application delivery and encrypted threat detection
- Minimizes performance impacts on FortiGate by offloading SSL decryption/encryption
- Seamless inspection and mitigation of secure traffic with security certificate integrity
- Flexible deployment options for active or passive inspection of encrypted traffic
- Increase Overall Performance and improve user QoE

FortiADC Application Delivery Controllers

FortiADC hardware and virtual Application Delivery Controllers provide unmatched Server Load Balancing performance whether to scale an application across a few servers in a single data center or serve multiple applications to millions of users around the globe. With included SSL Offloading, HTTP Compression, Global Server Load Balancing, Firewall and Link Load Balancing, they offer the performance, features and security needed at a single all-inclusive price.



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

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

September 30, 2016