SOLUTION BRIEF

Achieve High-performance SSL Visibility and Inspection With FortiADC

Executive Summary

As more and more enterprise applications move to the cloud, the amount of encrypted traffic through the data center to users increases dramatically. As of January 2, 2021, 95% of traffic on Chrome for Windows was encrypted.[1] While this is good news overall, encryption does not remove all risk. For years, cyber criminals have been hiding malware in encrypted traffic, which is then welcomed into the network by security controls that do not inspect that traffic.

To solve the danger of hidden malware, SSL inspection must be used to ferret out malicious code. But most inspection technologies available today put an untenable drag on network performance. The Fortinet FortiADC application delivery controller can be deployed to provide decryption and reencryption services to other data center security platforms for threat inspection of secure traffic content.

Encrypted Traffic Is Not Safe Traffic

Many organizations assume that secure sockets layer/transport layer security (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.

About FortiADC

FortiADC hardware and virtual ADCs deliver:

- Unmatched server load balancing
- SSL offloading
- HTTP compression
- Global server load balancing
- Web application firewall
- Link load balancing
- Sandboxing, IPS, and other security

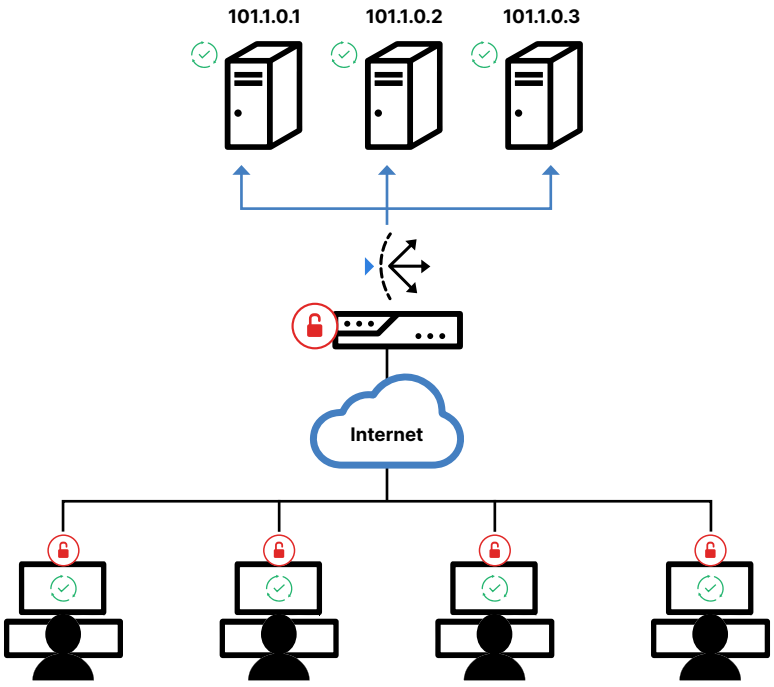

Figure 1: FortiADCs decrypt and encrypt traffic to/from users, allowing servers to focus on load-balancing applications to improve application performance.

Addressing Performance Challenges

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. FortiADC is a high-performance ADC with advanced SSL-offloading features. The appliance's application-specific integrated circuit (ASIC)-powered SSL processing can offload cryptographic functions from firewalls and intrusion prevention systems for high-performance encrypted threat detection and mitigation.

FortiADC offers three primary deployment configurations:

- SSL inspection (Forward-Proxy) for active threat detection and mitigation
- SSL visibility for passive threat detection and analysis
- SSL proxy for improved visibility and performance

SSL Inspection With Active Threat Mitigation

In this configuration, an inspection device such as a FortiGate firewall or intrusion prevention system (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 reencryption and on to its destination.

This configuration supports all inbound and outbound traffic from a data center and to the internet. FortiADC supports the 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.

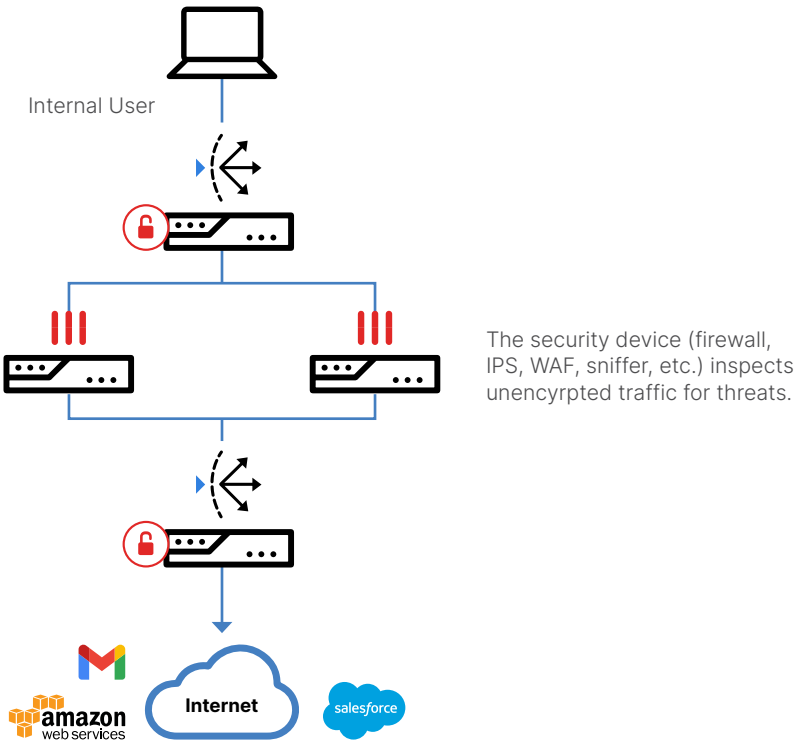

Figure 2: FortiADCs provide encryption and decryption services and can load balance multiple firewalls or other security devices.

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 or to ensure the availability of firewalls, virtual private networks (VPNs), and other security services—while maintaining encryption for traffic entering and leaving the cluster.

SSL Visibility for Inspection Only

Using FortiADC's Hypertext Transmission Protocol Secure (HTTPS) and Transmission Control Protocol Secure (TCPS) mirroring feature lets users configure a duplicate unencrypted 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 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.

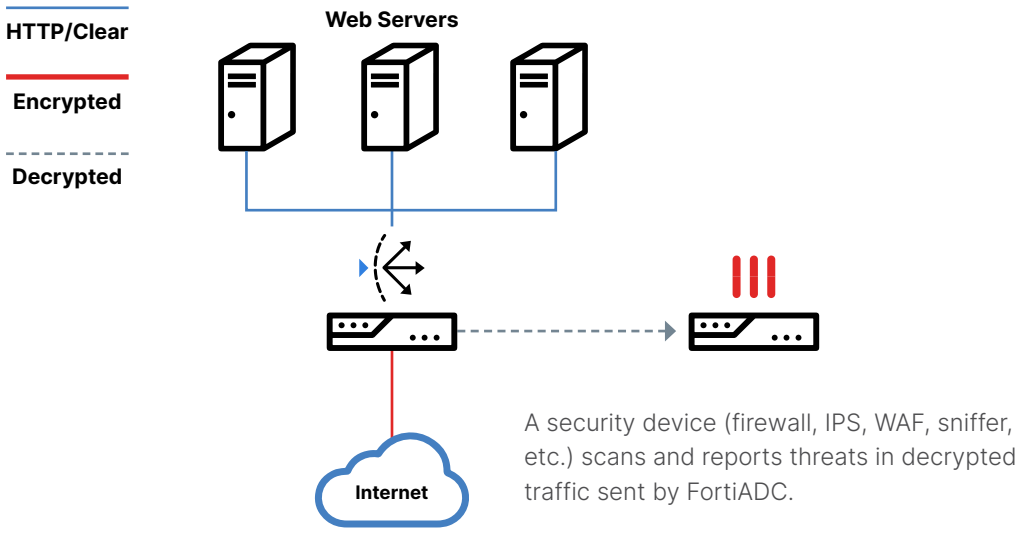

Figure 3: FortiADCs load balance traffic to servers, offload SSL traffic, and send mirror copy of decrypted traffic to the security device.

SSL Proxy for Improved Visibility and Performance

FortiADC can be switched to a new SSL proxy mode, which can act as a dedicated SSL proxy device to offer a full SSL encryption/decryption solution. It provides the following functions:

- Full SSL proxy (decrypt and reencrypt traffic)—supports TLS 1.3
- Firewall load balancing
- Full visibility for SSL traffic on HTTPS or TCPS, especially to other security devices for deep inspection (inline or mirror)
- High-performance SSL offloading by dedicated SSL ASIC
- Easy deployment using configuration wizard

Benefits of Using FortiADC for Visibility and Performance

FortiADC offers a variety of benefits including:

- 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
- Minimized performance impacts 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
- Increased overall performance and improved user quality of experience (QoE)

An Inspection Strategy Is Necessary

Encryption is at a critical crossroads for protection and hacking. With the average cost of a data breach hitting $3.86 million in 2020,2 organizations cannot afford to ignore the very real threat of malware entering their networks in encrypted traffic. With FortiADC, enterprises get the inspection they require with no impact to performance.

[1] "HTTPS encryption on the web," Google Transparency Report, accessed January 15, 2021.

[2] "Cost of a Data Breach Report," Ponemon Institute and IBM Security, 2020.

October 1, 2021 2:49 AM
887610-A-0-EN