CISCO SECURE

SSL Inspection Bundles

SSL and TLS establish an encrypted link that allows sensitive data to be securely transmitted over the internet. Unfortunately, encryption also creates blind spots for IT teams who are unable to inspect traffic for malicious content. In addition, attackers can use encrypted threats to gain unauthorized access to networks and deliver malware to unsuspecting users. To manage security risks, organizations must have real-time visibility into encrypted traffic.

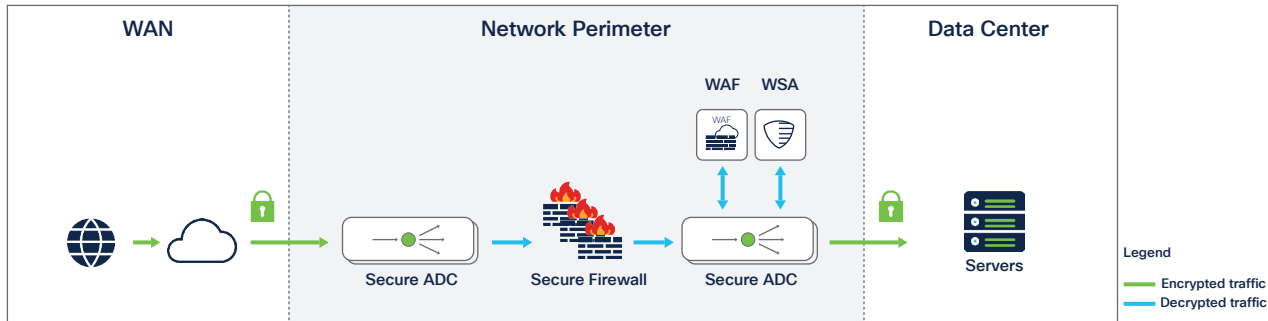Inbound SSL Offloading or Known Key

Figure 1. Cisco Secure Firewall with SSL Offload for Inbound Encrypted Traffic

Key benefits

Visibility into encrypted traffic
Real-time visibility into encrypted traffic

High-volume SSL traffic inspection
Highest capacity ECC processing of SSL traffic; over 200 Gbps

**Increases availability and performance with minimal latency**
Optimizes network performance and availability with SSLi load balancing and offloading

Selective inspection bypass
- Ability to bypass data that should not be decrypted for privacy and compliance reasons
- Helps meet confidentiality and compliance mandates (i.e., HIPAA, SOX, PCI-DSS, ISO 27000)

The bridge to possible

The solution

Cisco® SSLi Bundles combine Secure ADC® SSL acceleration with Secure Firewall and/or Secure Web Appliance to offer a highly scalable solution for SSL traffic inspection. The solution provides visibility into encrypted traffic with minimal latency and reduces overall security costs by offloading SSLi functions to purpose-built devices. Each bundle uses a front- and backend Secure ADC in a "sandwich" configuration for high availability (HA) and scaling of SSL inspection beyond current limits.
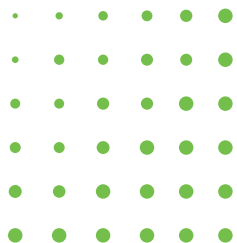
Mitigating today's encrypted threats

Full visibility to SSL and TLS traffic
High-capacity SSL/TLS processing with support for latest SSL/TLS standards.

Scale SSL inspection beyond current limits
Enhanced SSL inspection capabilities for existing Secure Firewall and Secure Web Appliance customers. Offloads CPU-intensive processes to purpose-built SSL acceleration hardware.

Lower TCO
Improves the performance and extends the useful life of existing security devices. Standardize, automate, and secure applications across multiple clouds.

Complete end-user privacy
Quickly determines which traffic to send for inspection and which traffic should be kept private and bypass the security inspection. Protects confidential data.

Superior performance and reduced latency
Only decrypt and reencrypt traffic once. Transparent traffic steering and service chaining ensure that only relevant traffic is passed to each security service.

More information

SSL Inspection Bundles Solution Brief

www.cisco.com/c/en/us/products/collateral/
security/ssli-bundles-wp.html

Learn more

Secure ADC Data Sheet

www.cisco.com/c/en/us/products/collateral/
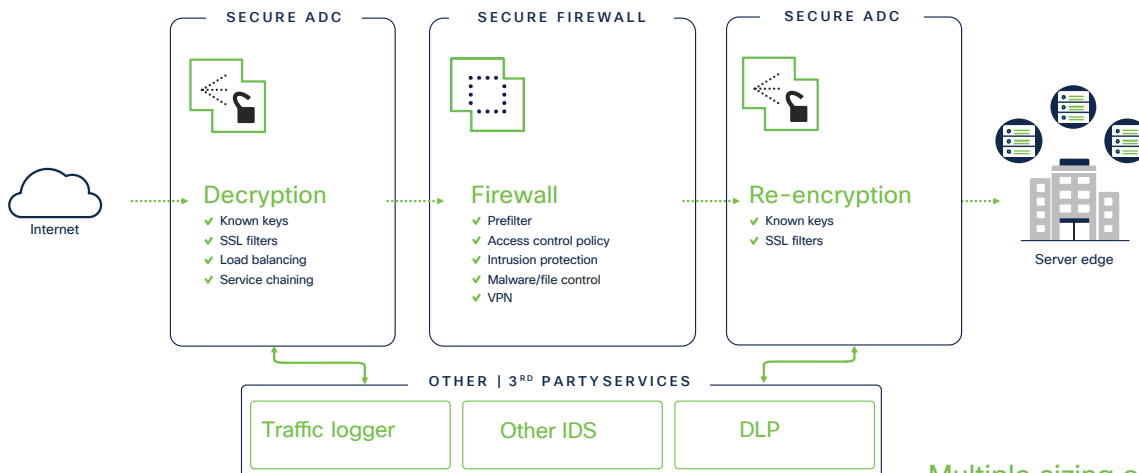security/secure-adc-alteon-ds.html

Secure ADC Technical Specifications

www.cisco.com/c/en/us/products/collateral/
security/alteon-technical-specs-ds.html

Next steps

For more information about our SSL inspection solutions, contact your Cisco sales representative today.

Inbound SSL offload use case

SECURE ADC

Decryption
- ✔ Known keys
- ✔ SSL filters
- ✔ Load balancing
- ✔ Service chaining

SECURE FIREWALL

Firewall
- ✔ Prefilter
- ✔ Access control policy
- ✔ Intrusion protection
- ✔ Malware/file control
- ✔ VPN

SECURE ADC

Re-encryption
- ✔ Known keys
- ✔ SSL filters

Internet

Server edge

OTHER | 3RD PARTY SERVICES

| Traffic logger | Other IDS | DLP |

Learn more: cisco.com/go/secure

Multiple sizing options:

Configuration	SSLi capacity
Large	72 Gbps
Medium	38 Gbps
Small	20 Gbps
Entry	6 Gbps