CISCO
SECURE

White paper
Cisco public

SSL Inspection (SSLi) Bundles for Scalable Inspection of SSL/TLS Encrypted Traffic

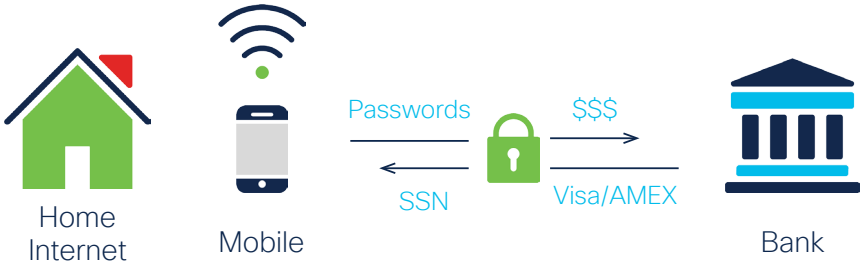
March 2022

Contents

Executive summary

The majority of internet traffic is encrypted to protect sensitive data from eavesdropping, theft, and manipulation. In recent years, the volume of internet traffic that is encrypted has risen from 50% in 2016 to over 90% in 2020. While data encryption is a critical technology for ensuring privacy and protecting confidential information, encryption increases security risks for organizations as they lose visibility into network traffic and attackers use encrypted traffic to launch cyberattacks.

Cisco and Radware partner to offer SSL inspection (SSLi) Bundles. SSLi Bundles offer Cisco® Secure Firewall (formerly Cisco Firepower NGFW) customers and Web Security Appliance (WSA) customers scalable and effective options for inspection of encrypted traffic, dramatically reducing security risks.



Encryption protects privacy and secures sensitive data in transit

SSL/TLS background

Secure Sockets Layer (SSL) is a widely used security technology that establishes an encrypted communications link, enabling sensitive information such as online banking transactions, credit card numbers, and login credentials to be securely transmitted over the internet. Even if the communication is intercepted, the data cannot be read because the information is encrypted.

Transport Layer Security (TLS) is the next generation of SSL secure transport. TLS helps protect web applications from data breaches and other attacks. It is mainly used to encrypt web communications, such as web browsers loading a website. HTTPS is an implementation of TLS on top of the HTTP protocol that ensures the privacy and security of web services.

Escalating attacks using encrypted data

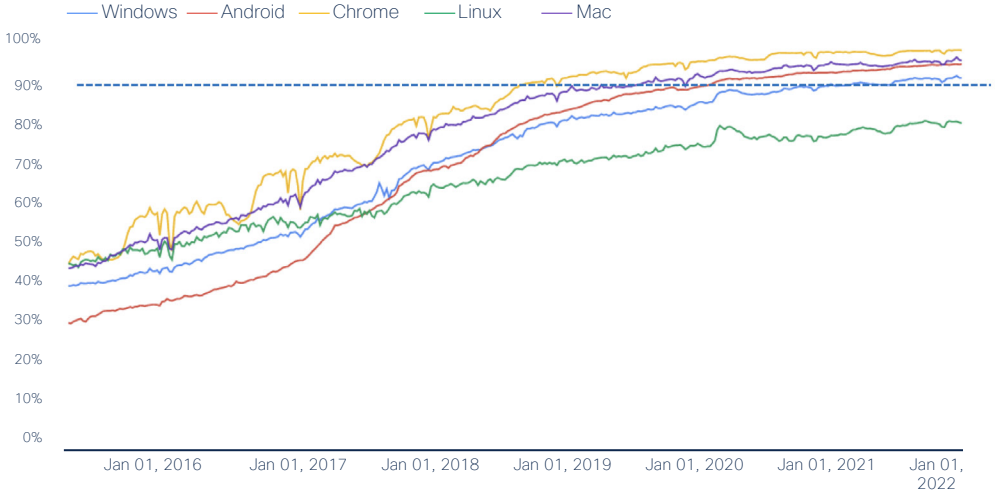
The use of SSL/TLS has exploded in recent years as encryption is increasingly used to protect data and comply with security and data protection regulations. The Google Transparency Report noted that more than 90% of the pages loaded in Chrome were encrypted.[1]

[1] Google 1Q2022 Transparency Report, https://transparencyreport.google.com/https/overview?hl=en

90%
and Growing

Percentage of encrypted traffic on Chrome

Percentage of pages loaded over HTTPS in Chrome by platform



Fragment navigations, history push state navigations, and all schemes besides HTTP/HTTPS (including new tab page navigations) are not included.

Source: Google transparency report

The challenge

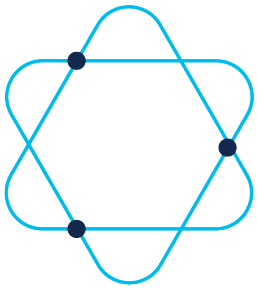
While data encryption is highly effective for protecting sensitive information, encryption creates serious blind spots and dramatically increases security risks because IT teams are unable to inspect traffic for malware and other malicious content that can be embedded in encrypted data.

Additionally, although modern security devices such as Cisco Secure Firewall and WSA have built-in SSL/TLS inspection capabilities, the performance of these devices can be severely impacted by SSL/TLS inspection, which places heavy demands on the processing power of security devices and can leave them vulnerable to exploit.

The solution: Cisco SSL inspection bundles

To address the growing need for the inspection of encrypted data, Cisco offers SSLi bundles, a scalable and cost-effective solution that provides visibility into encrypted traffic, reduces the attack surface, and allows customers to optimize their Cisco Secure Firewall and WSA security deployments.

Cisco SSL inspection bundles provide Secure Firewall and WSA customers with scalable and efficient options for offload and inspection of encrypted traffic. The SSL inspection bundles provide high availability, increased scalability, and granular privacy control of encrypted traffic protection while offloading SSL/TLS traffic processing from security devices.

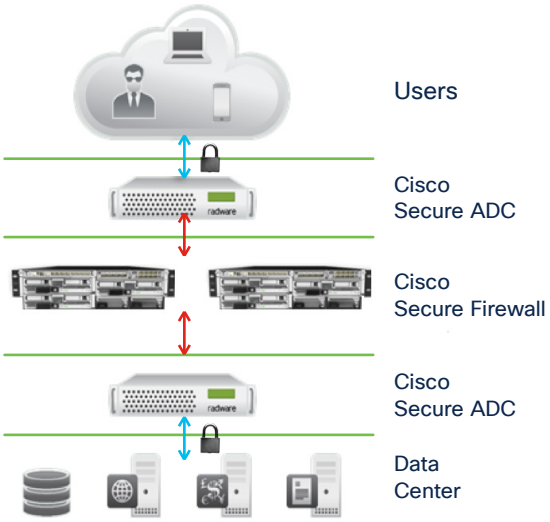


Each bundle includes a front-and back-end Cisco Secure Application Delivery Controller (ADC)[2] for SSL inspection with user-privacy categorization subscription and support.

Cisco offers four (4) predefined SSLi bundles to simplify sizing/dimensioning and provide an optimized SSLi solution to meet every customer need.

Bundles are deployed in pairs for high availability and/or individually to scale gateway designs incrementally. These bundles simplify dimensioning because they are defined according to real-life encrypted IMIX bandwidth performance for this use case.

As a result, the bundles can be applied to any of the Cisco encrypted traffic inspection requirements without the need for special consideration of real-life traffic patterns and the SSL/TLS inspection capacity. Additional Cisco Secure ADC SKUs are available via the Cisco GPL.



SSL inspection bundle with front-and back-end Secure ADCs

Bundle size	SSLi perf.	SKU type	Cisco SKU
Large	72 Gbps	Hardware	RD-9800S-SLI
		Secure URL subscription	L-RD-SURL-9K-1Y
Medium	38 Gbps	Hardware	RD-7612S-HSLI
		Secure URL subscription	L-RD-SURL-7K-1Y
Small	20 Gbps	Hardware	RD-6024S-HSLI
		Secure URL subscription	L-RD-SURL-6K-1Y
Entry	6 Gbps	Hardware	RD-5424-SLI
		Secure URL subscription	L-RD-SURL-5K-1Y

Note: A Secure URL subscription is only needed for outbound SSL/TLS inspection.

Features

Flexible and simplified security service management

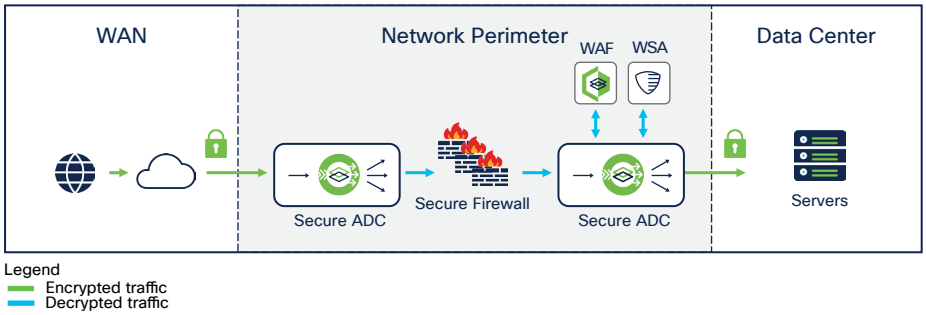
Cisco SSL inspection uses traffic profiles and policies to transparently steer traffic through the various security inspection servers in the chain. SSLi service chaining enables simplified security service provisioning and reduces the administrative tasks involved in service management and maintenance.

A single location for encryption policy enforcement with robust algorithm and protocol support

Cisco SSL inspection provides a central location where encryption policies can be enforced while ensuring that traffic is decrypted/re-encrypted only once. Organizations can comply with best practices and compliance requirements in one place, while providing support for modern standards and algorithms like TLS 1.3 and Elliptical Curve Encryption regardless of the lack of support

[2] Cisco Secure ADC solutions are powered by Radware.

Inbound SSL Offloading or Known Key



in underlying all-in-one or standalone security services that will inspect the clear-text/decrypted traffic in the service chain. Not only does this provide predictable engineering and lower latency, it also provides consistency in execution for security organizations. Because SSL/TLS encryption is the focus for Cisco SSL inspection, you can rely on future-proof support for new protocols and algorithms as they emerge, instead of managing exceptions while differing underlying security services provide their implementations of these at different release cycles.

In addition to HTTPS, Cisco SSL inspection provides SSL visibility for mail protocols (IMAPS, SMTPS, POP3S), FTPS, and generic TLS traffic.

It can also discover outbound SSL/TLS traffic on any TCP port addressing dynamic use cases.

Flexible deployment options

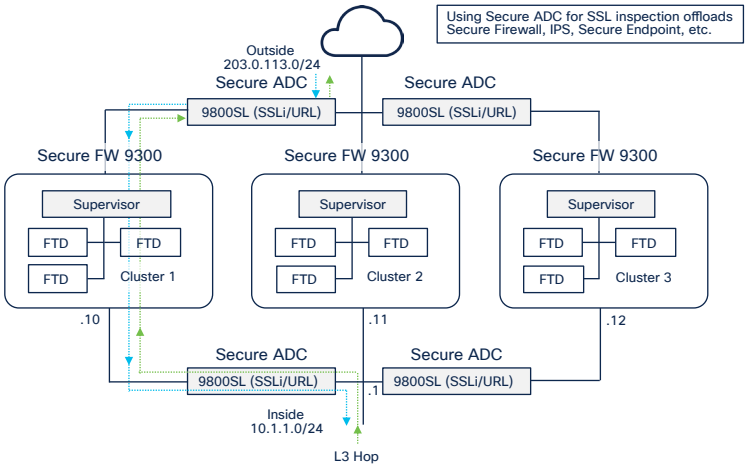
Cisco SSLi inspect can be implemented as a bump in the wire device, overseeing all of the organization's traffic to and from the internet with virtual/physical separation between the DMZ and the enterprise's internal network. Based on its advanced application classification capabilities, Cisco SSL inspection seamlessly intercepts and steers traffic to the various security solutions for in-depth inspection before allowing it to continue to its destination. The solution allows traffic steering to active inline devices as well as forwarding a copy of the traffic to out-of-path passive devices.

In addition to providing high-performance, hardware-based SSL/TLS decryption options, SSL inspect is available for deployment in distributed, virtual environments as a virtual appliance or NFV, or within IaaS environments (Microsoft Azure, Amazon Web Services, Google Cloud Platform, Alibaba Cloud, etc.) with industry-leading price/performance.

Furthermore, Cisco SSL inspection has a unique ability to connect to any type of value-add security service (VAS), including 1- or 2-leg solutions, L2 and L3 solutions, or out-of-path solutions that read network traffic in TAP mode.

SSL Inspection Deeper Dive

High-performance SSL decryption use case



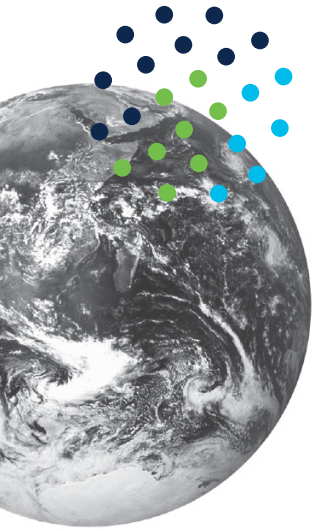
Improved security solutions capacity

Cisco SSL inspection provides several capabilities, which improve the utilization of the enterprise's security devices:

- By steering only the relevant traffic to the security service for inspection, the load on that service can be controlled and reduced, enabling cost-effective sizing or elasticity.
- SSL inspect enables redundant security inspection solution servers to operate in an active-active mode through persistent load balancing to increase the traffic inspection capacity of the entire deployed solution. This means that, to scale up, Cisco can apply additional bundles as needed to increase SSL/TLS capacity either for the first time or over time.

Advanced high availability

The unique deployment architecture of SSL inspect and its inherent load balancing capabilities enables it to scale each of the security service farms separately and thus ensure traffic will always flow through the most available element. Even in cases where service elements are down, Cisco SSL inspection provides a simple way to define a policy that decides whether to bypass to an unresponsive security service, ensuring continuous internet connectivity, or to block the traffic and avoid bypassing critical inspection services.



Outbound traffic management for complete privacy, increased security, and higher productivity

Cisco SSL inspection provides complete outbound traffic management based on an embedded URL classification engine. In cases where the employee is browsing sites with private personal information, such as consumer banking or healthcare, the privacy module automatically designates that session as private, avoids decryption, and bypasses all inspection servers and sends the traffic directly to its destination, ensuring user privacy.

In cases where decryption is not possible for technical reasons, such as applications with embedded or pinned public certificates, decryption can be administratively bypassed.

Additional benefits

As a smart centralized traffic steering solution, the SSL inspect, with its high-capacity SSL hardware engine, decrypts all relevant SSL encrypted traffic before forwarding it to the various security solutions and re-encrypts the traffic before forwarding it to the final destination. Offloading traffic decryption and re-encryption delivers the following key benefits:

- Lower latency for all transactions, as traffic is only decrypted/re-encrypted once for all solutions and not by each security solution separately.
- Reduced overall cost/performance by offloading CPU-intensive SSLi functions from security devices and leveraging purpose-built, industry-leading Secure ADC for scalable SSL inspection.

Challenges of inspecting SSL traffic with "all-in-one" security devices

- SSL/TLS standards are constantly evolving and support for TLS 1.3, ECC, etc. is not always available in "all-in-one" solutions.
- Configuration of traffic flows through multiple security devices is complex. It becomes even more challenging as each security device has its own requirements, certificate repository, and policies.
- High availability is costly (often requires 1+1 redundancy), complex to configure, and often prone to human error.
- Certificate management across a security gateway architecture is also difficult to maintain.
- Performance and scalability are costly; users suffer from increased latency; security tools run out of capacity, often leading to forklifts to scale up.

Cisco Secure ADC technical specifications[3]

Specifications	Alteon D-9800SL	Alteon D-7612SL	Alteon D-6024SL	Alteon D-5424SL
Performance				
Maximum L4 / L7 throughput	320 Gbps / 150 Gbps	200 Gbps / 125 Gbps	80 Gbps / 74 Gbps	40 Gbps / 32 Gbps
Layer 4 connections per second	4.7M	2.5M	1.4M	525K
Maximum Layer 4 concurrent connections	280M	184M	82M	44M
Layer 7 requests per second	8M	4M	2.55M	930K
SSL performance				
RSA CPS (2K keys)	RSA CPS (2K keys): 195K	RSA CPS (2K keys): 101K	RSA CPS (2K keys): 53K	20K
ECC CPS (P256)	ECC CPS (P256): 115K	ECC CPS (EC-P256): 47K	ECC CPS (EC-P256): 27.3K	12K
SSL bulk encryption throughput (Gbps)	85	45	22	9
FIPS RSA CPS (2K keys)[4]			N/A	
FIPS bulk encryption (Gbps)[4]			N/A	
Licenses				
Available throughput licenses	240 and 320 Gbps	160 and 200 Gbps	30, 60, and 80 Gbps	12, 22, and 40 Gbps
Max number of virtual ADC instances	72	64	32	10
HW specifications				
Processor	2 x Intel 18-core CPU	2 x Intel 18-core CPU	Intel 6-core CPU	Intel 12-core CPU
Memory	192GB	192GB	32GB / up to 256GB	32GB
Traffic ports	8 x 100 GbE / 40 GbE / 10 GbE	6 x 40 GbE QSFP+ 12 x 10 GbE SFP+	24 x 10 GbE SFP+	4 x 10 GE SFP+ 16 x 1 GE SFP 8 x 1 GE RJ45
HPP (high-performance package)	N/A	Includes 500GB SSD, dual power supply 6 x 10 Gbps pluggable optics multimode SR 2 x 40 Gbps pluggable optics multimode SR	Includes 64GB RAM, 500GB SSD, dual power supply, 6 x 10 Gbps pluggable optics multimode SR	N/A
USB port	Yes	Yes	Yes	Yes
RS-232C console	Serial connection	Serial connection	RJ-45 serial connection	RJ-45 serial connection

[3] Alteon and AppWall are registered trademarks of Radware, Inc. Alteon ADC is sold by Cisco as Cisco Secure ADC.

Specifications	Alteon D-9800SL	Alteon D-7612SL	Alteon D-6024SL	Alteon D-5424SL
Environmental specifications				
Power	Auto-range dual power supply	Auto-range power supply	Auto-range power supply	Auto-range power supply
	80 plus platinum certified (AC PSU)	80 plus certified (AC PSU)	80 plus certified	80 plus certified
	AC: 100-240 V, 47-63 Hz	AC: 100-240 V, 47-63 Hz	AC: 100-240 V, 47-63 Hz	AC: 100-240 V, 50-60 Hz
	Power consumption: 800W	Power consumption: 400W	Power consumption: 250W	Power consumption: 125W
	DC power supply is optional	Dual power supply is optional	Dual power supply is optional	Dual power supply is optional
		DC power supply is optional	DC power supply is optional	
Heat dissipation	1800 BTU/h	1364 BTU/h	850 BTU/h	427 BTU/h
Dimensions	445 mm (17.54") W x 730 mm (28.75") D x 87 mm (3.44" / 2U) H	438 mm (17.24") W x 438 mm (17.24") D x 88 mm (3.4" / 2U) H	436 mm (17.1") W x 480 mm (18.9") D x 88 mm (3.4" / 2U) H	EIA rack or standalone: 481 mm (18.9")
		EIA rack or standalone: 482 mm (19")	EIA rack or standalone: 482 mm (19")	
Weight	15.2 kg (33.5 lb)	Single power supply: 11 kg (24.2 lb)	Single power supply: 11 kg (24.2 lb)	Single power supply: 6.8 kg (15 lb)
		Dual power supply: 12 kg (26.4 lb)	Dual power supply: 11.7 kg (25.8 lb)	Dual power supply: 7.5 kg (16.5 lb)
Operating environmental	Temperature: 10-40°C (50-104°F)	Temperature: 0-40°C (32-104°F)	Temperature: 0-40°C (32-104°F)	Temperature: 0-40°C (32-104°F)
	Humidity: 8% to 90% noncondensing	Humidity: 5% to 95% noncondensing	Humidity: 10% to 95% noncondensing	Humidity: 5% to 95% noncondensing
Airflow direction	Front-to-back	Front-to-back	Front-to-back	Front-to-back
Minimum CFM		200	200	21.9

Specifications	Alteon D-9800SL	Alteon D-7612SL	Alteon D-6024SL	Alteon D-5424SL
	ENVIRONMENTAL SPECIFICATIONS	COMPLIANCE & CERTIFICATIONS	COMPLIANCE & CERTIFICATIONS	COMPLIANCE & CERTIFICATIONS
Compliance				
RoHS2	Compliant (EU directive 2011 / 65 / EU)	Compliant (EU directive 2011 / 65 / EU)	Compliant (EU directive 2011 / 65 / EU)	Compliant (EU directive 2011 / 65 / EU)
Safety/EMC/EMI	FCC Part 15B (Class A); ICES-003:2016 Issue 6, Class A; ANSI C63.4:2014; EN 60950-1:2006 + A11:2009 +A1:2010 +A12:2011 +A2:2013; EN 62479:2010; EN 50581:2012; EN 55024:2010; EN 55032:2012 Class A; EN 61000-3-2:2014; EN 61000-3-3:2013; AS / NZS CISPR 32:2013; AS / NZS 60950.1: 2011	FCC Part 15, Subpart B; ANSI C63.4:2014; ICES-003 Issue 6:2016 (updated Apr. 2017); CISPR 22:2008; CAN / CSA-CISPR 22-10; IEC 60950 1:2005 / AMD 1:2009; IEC 60950 1:2005 / AMD2:2013; IEC 60950-1:2005; EN 60950-1:2006 / A11:2009 / A1:2010 / A12:2011 / A2:2013; IEC 62368-1:2014; EN 62368-1:2014 / A11:2017; EN 55032:2015+AC: 2016 Class A; AS / NZS CISPR 32:2015, Class A; CISPR 32:2015+C1: 2016, Class A; EN 55024:2010+A1:2015; EN 55035:2017; EN 61000-3-2:2014, Class A; EN 61000-3-3:2013; EN 61000-4-2:2009, EN 61000-4-3:2006 +A1:2008 +A2:2010; EN 61000-4-4:2012; EN 61000-4-5:2014; EN 61000-4-6:2014+AC:2015; EN 61000-4 11:2004+A1:2017; EN 300 386 V2.1.1 (2016-07)	FCC Part 15, Class A; IC ICES-003; UL 60950-1:2007 R10.14; CAN / CSA-C22.2 No. 60950-1-07+ A1:2011+A2:2014; EN 55022:2010 / AC:2011 Class A; EN 61000-3-2:2014; EN 61000-3-3:2013; EN 55024:2010; IEC 61000-4-2:2008; IEC 61000-4-3:2006+A1:2007; IEC 61000-4-4:2012; IEC 61000-4-5:2014; IEC 61000-4-6:2013; IEC 61000-4-8:2009; IEC 61000-4-11:2004; IEC 61000-4-12:2006; IEC 60950-1:2005 (Second Edition)+Am 1:2009+Am 2: 2013; EN 60950-1: 2006+A11:2009+A1: 2010+ A12:2011+A2: 2013; NEBS	FCC Part 15, Subpart B, Class A; IC ICES-003:2016 Issue 6, Class A; ANSI C63.4:2014; UL 60950-1:2007 R10.14; CAN / CSA-C22.2 No. 60950-1-07+A1: 2011+A2:2014; UL 62368-1:2007 R10.14; CAN / CSA-C22.2 No. 62368-1-14; EN 55024:2010; EN 55032:2015 +AC:2016 / CISPR 32:2015 +COR1: 2016 / AS/NZS CISPR 32:2015, Class A; EN 300 386 V2.1.1 (2016-07); EN 61000-3-2:2014; EN 61000-3-3: 2013; EN 61000-4-2:2009; EN 61000-4-3: 2006 +A1:2008 +A2:2010; EN 61000-4-4:2012; EN 61000-4-5:2014; EN 61000-4-6:2014; EN 61000-4-8:2010; EN 61000-4-11:2004
Certifications	CCC (China), UL (US, Canada), CE (Europe), FCC (US), KCC (Korea), BSMI (Taiwan), EAC (Russia), VCCI (Japan), NRCS (South Africa), TCVN (Vietnam), BIS (India)	CCC (China), UL (US, Canada), CE (Europe), FCC (US), KCC (Korea), BSMI (Taiwan), EAC (Russia), VCCI (Japan), Anatel (Brazil)	CCC (China), TUV (US, Canada), CE (Europe), FCC (US), KCC (Korea), BSMI (Taiwan), EAC (Russia), VCCI (Japan), Anatel (Brazil), SDPPI (Indonesia)	CCC (China), TUV (US, Canada), CE (Europe), FCC (US), KCC (Korea), BSMI (Taiwan), EAC (Russia), VCCI (Japan), Anatel (Brazil)

[4] FIPS 140-2 Level 3

Summary

To address the growing need for the inspection of encrypted data, Cisco offers SSLi bundles, a scalable and cost-effective SSL/TLS offload and inspection solution that provides visibility into encrypted traffic and reduces the risk of cyberattacks delivered over encrypted data.

Cisco SSL inspection bundles provide Cisco Secure Firewall and WSA customers with scalable and effective options for offload and inspection of encrypted traffic. The SSL inspection bundles provide high availability, increased scalability, and granular privacy control of encrypted traffic protection while offloading SSL/TLS traffic processing from legacy security devices.

Learn more

Cisco partners with Radware to provide best-of-breed DDoS, WAF, SSL, ADC, and bot management solutions that enhance network resilience, ensure application availability, and protect digital enterprises worldwide.

To learn more, please visit: Cisco.com cisco.com/go/secure

Cisco SSLi Bundles at-a-glance (AAG):

www.cisco.com/c/en/us/products/collateral/security/ssli-bundles-aag.pdf

Cisco Secure ADC data sheet:

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

Secure ADC technical specifications:

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

For questions about our solutions or for sales support, please contact Cisco at www.cisco/com/c/en/us/buy.