



# THUNDER CFW

## High-Performance Versatile Firewall

### Supported Platforms



**Thunder CFW**  
physical appliance



**aGalaxy**  
centralized management

### Overview

A10 Networks® Thunder® Convergent Firewall (CFW) is a high-performance, all-inclusive and flexible security solution featuring a Secure Web Gateway, Data Center Firewall, Gi/SGi Firewall and site-to-site IPsec VPN for enterprises and service providers. Thunder CFW uncovers threats in SSL traffic and blocks access to malicious websites at the enterprise perimeter. It also protects high-value assets in the data center from network and Distributed Denial of Service (DDoS) attacks. A10 Thunder CFW offers the performance and the versatility you need to safeguard your applications, your users and your infrastructure.

The A10 Thunder Convergent Firewall (CFW) is a standalone security product, built on A10 Networks Advanced Core Operating System (ACOS®) platform. Thunder CFW is the first converged security solution for service providers, cloud providers and large enterprises that includes:

- A powerful Secure Web Gateway that combines URL filtering, A10's SSL Insight technology, and explicit proxy to increase security efficacy by decrypting SSL traffic at high speed and restricting access to undesirable websites.
- A high-performance Data Center Firewall with an integrated Layer 4 firewall, DDoS protection, and server load balancing. By uniting application delivery control and security on a single platform, Thunder CFW lowers hardware and operating costs.
- A scalable Gi/SGi Firewall with integrated DDoS protection and Carrier Grade Networking (CGN) for mobile carriers. The Gi/SGi Firewall protects mobile infrastructure with advanced policy enforcement.
- High-speed site-to-site IPsec VPN that enables enterprises and service providers to encrypt data at a massive scale and in the cloud.

With its data center efficient design and compact form factor, Thunder CFW provides an integrated security and application networking solution that minimizes rack space, power consumption and cooling costs.

Thunder CFW also leverages the A10 Harmony™ architecture to provide open and standards-based programmability, which offers rapid integration with management and orchestration systems, consistent policy enforcement and telemetry. The A10 Networks aGalaxy® Centralized Management System delivers everything that organizations need to configure, monitor and troubleshoot all A10 Thunder solutions, including Thunder CFW.

### Features and Benefits

Whether you are an enterprise, service provider or mobile carrier, A10 Thunder CFW offers the performance and the versatility you need to safeguard your applications, your users and your infrastructure.

#### Secure Web Gateway

**Decrypt SSL once and inspect multiple times:** Thunder CFW enables security devices to inspect encrypted traffic, eliminating the SSL blind spot in corporate defenses. Leveraging SSL Insight technology, Thunder CFW decrypts SSL traffic and forwards it to third-party security devices for inspection. With the Thunder CFW, organizations can make their security infrastructure effective again.

**Prevent data exfiltration and enforce compliance:** Thunder CFW allows seamless integration with third-party Data Loss Prevention (DLP) solutions via the industry standard ICAP. Thunder CFW can send decrypted traffic to DLP servers for inspection before

forwarding intercepted traffic to a client or a server. According to inspection results from DLP servers, Thunder CFW enforces a policy by either permitting or denying traffic to prevent data leaks and harmful infection.

**Gain superior URL classification coverage:** Thunder CFW provides an optional URL filtering service that maximizes employee productivity and mitigates web-based threats. Thunder CFW can monitor or block access to malicious websites, including malware, spam and phishing sites. The A10 URL Classification Service, powered by Webroot, categorizes over 460 million domains and 13 billion URLs into 83 categories, enabling organizations to block desirable sites and shield their users from online threats.

**Extend the life of security infrastructure:** Thunder CFW, with integrated load balancing, enables organizations to maximize uptime and increase the capacity of their security infrastructure. It also unburdens firewalls and other security devices from computationally intensive tasks like SSL decryption and ICAP support, enabling those devices to do what they do best – detect and stop attacks.

### Data Center Firewall

**Achieve unprecedented firewall performance:** Powered by A10's Advanced Core Operating System (ACOS), Thunder CFW provides high performance in a compact appliance, allowing organizations to stop emerging threats at scale. Combining a Shared Memory Architecture and Flexible Traffic Accelerator (FTA) technology, the Data Center Firewall offers ultra-high throughput and unmatched connection rates, eliminating traditional performance bottlenecks while protecting data center assets.

**Lower OPEX and CAPEX:** Consolidating multiple services on one platform reduces the number of appliances that need to be purchased and cuts power, space and cooling costs. Thunder CFW's Data Center Firewall takes unification further by converging not just security but also networking and application delivery features, empowering organizations to eliminate single-purpose devices from their data centers and reduce hardware and operating costs.

**Protect multi-tenant environments:** Thunder CFW leverages the A10 Harmony architecture to deliver completely programmable security for the data center. A10 Harmony unifies policy control, offers unprecedented telemetry and provides 100% RESTful API coverage. Thunder CFW also supports multi-tenancy features like Application Delivery Partitions (ADPs) for segmentation.

### Gi/SGi Firewall

**Achieve massive scale and multiple functionality in a single compact appliance:** The Thunder CFW, with an integrated Gi/SGi Firewall, delivers the performance that mobile carriers require to scale and protect their networks. With the ability to support large session capacity and high connections-per-second rates, the Thunder CFW will meet both current and future traffic requirements. Thunder CFW enables mobile carriers to efficiently safeguard their infrastructure, including the Gateway GPRS Support Node (GGSN) and P-Gateway in the Evolved Packet Core (EPC).

The Thunder CFW includes integrated Carrier Grade NAT functionality to allow mobile carriers to preserve their investment in IPv4-based infrastructure. Also included are various IPv6 transition technologies, such as NAT64/DNS64, to assist in providing a smooth transition to IPv6 networking and seamless subscriber access to resources regardless of the type of IP version used. Integrated application layer gateways (ALGs) ensure that applications remain addressable and operate transparently through address translation. By including IPv4 preservation and IPv6 migration support in the multi-functional Thunder CFW, operational tasks are greatly simplified.

To protect mobile infrastructure, the Thunder CFW Gi/SGi Firewall provides granular control over network resources, allowing mobile carriers to block network attacks and unauthorized access. It delivers a stateful firewall with a rich set of features to protect subscribers, along with shielding the LTE data and control plane services from multiple types of threats. The Thunder CFW can also secure its own resources, such as Network Address Translation (NAT) pools, to ensure that its operational functions are not compromised.

### Site-to-Site IPsec VPN

**Encrypt data at unparalleled speeds:** Thunder CFW enables enterprises and service providers to build out large-scale VPN deployments. By supporting thousands of VPN tunnels per Thunder CFW platform and a broad array of encryption algorithms and data integrity methods, organizations can deploy Thunder CFW alongside their existing VPN equipment or build out new VPN networks with Thunder CFW appliances.

**Consolidate IPsec VPN, firewall and application delivery:** Thunder CFW combines Data Center Firewall, Gi/SGi Firewall and IPsec VPN on a single platform. Whether used with the Data Center Firewall to support secure interconnectivity between data centers or to support high-speed VPN connections in the cloud, Thunder CFW provides a comprehensive networking and security platform that reduces customers' data center footprint and operating costs.

### Management

**Comprehensive and scalable management:** Thunder CFW devices feature an array of options to simplify and automate management tasks that reduce administrative costs and ensure that complex tasks can be done accurately the first time. To complement our industry-standard CLI and Web GUI, our RESTful API with 100% coverage offers rapid integration with third-party management consoles to efficiently operate one or more Thunder CFW appliances. For larger deployments, our aGalaxy Centralized Management System ensures that routine tasks can be performed at scale, across multiple appliances, regardless of physical location.

Thunder CFW supports granular role-based access control, enabling you to create users and groups and grant read-only or read/write privileges for specific partitions or management interfaces. To scale load-balancing capacity, A10 Networks aVCS® Virtual Chassis System allows multiple appliances to operate as one, with a single management point for all appliances in the virtual chassis.

## Architecture and Key Components

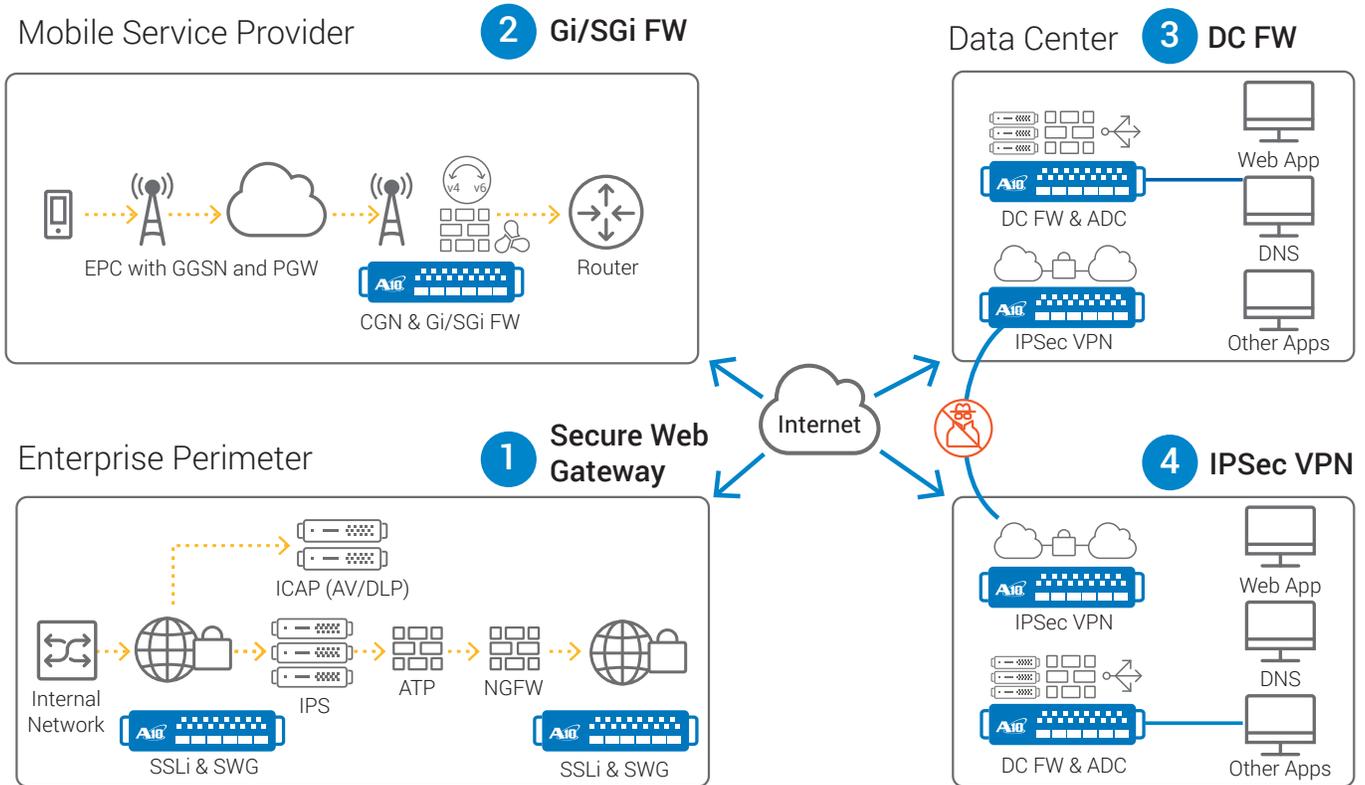


Figure 1: Thunder CFW use cases

## Product Description

### Thunder CFW Product Line

Thunder CFW appliances support any deployment need. Each Thunder CFW appliance is powered by ACOS software, which brings a unique combination of shared memory accuracy and efficiency, 64-bit scalability and advanced flow processing.

Thunder CFW Hardware Appliances:

- The A10 Thunder CFW line of appliances fits all size networks with entry-level models starting at 5 Gbps and scaling to 220 Gbps in a single, rack-mountable appliance to address the most demanding requirements.
- All models are dual power supply-capable, feature solid-state drives (SSDs) and use no inaccessible moving parts for high availability.
- All models benefit from A10's Flexible Traffic Accelerator (FTA) technology, with select models featuring Field Programmable Gate Arrays (FPGAs) for hardware optimized FTA processing; this provides highly scalable flow distribution and DDoS protection capabilities.

- Select models include switching and routing processors for high-speed network processing, dedicated security processors for SSL offload, and lights-out management (LOM) for out-of-band monitoring and management.
- Each appliance offers exceptional performance per rack unit to reduce power consumption costs and ensure a green solution. Coupled with high density 1 GbE, 10 GbE, 40 GbE and 100 GbE port options, Thunder CFW meets the highest networking bandwidth demands.

The aGalaxy® Centralized Management System delivers everything that organizations need to monitor, configure and troubleshoot their Thunder CFW deployment.

## Thunder CFW Specifications Table

	Thunder 840	Thunder 3230(S)	Thunder 3430(S)
<b>Data Center Firewall</b>			
DCFW Throughput	5 Gbps	25 Gbps	38 Gbps
DCFW Layer 4 CPS	200k	1.4 million	2 million
DCFW Concurrent Sessions	8 million	32 million	64 million
DCFW Rules	8k	16k	32k
<b>Secure Web Gateway<sup>*1</sup>*2</b>			
SSLi Throughput (2k key)	0.5 Gbps	3.5 Gbps	5.5 Gbps
SSLi CPS (2k key)	300	12.5k	18k
<b>IPsec VPN<sup>*2</sup></b>			
IPsec Throughput	1.5 Gbps	15 Gbps	30 Gbps
IPsec Tunnels	50	1k	4k
<b>Network Interface</b>			
1 GE Copper	5	0	0
1 GE Fiber (SFP)	0	4	4
1/10 GE Fiber (SFP+)	2	4	4
40 GE Fiber (QSFP+)	0	0	0
Management Interface	Yes	Yes	Yes
Lights Out Management	No	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Communication Processor	Intel Xeon 4-core	Intel Xeon 6-core
Memory (ECC RAM)	8 GB	16 GB	32 GB
<b>Hardware Acceleration</b>			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	Software	1 x FTA-4 FPGA	1 x FTA-4 FPGA
Switching/Routing	Software	Hybrid <sup>*4</sup>	Hybrid <sup>*4</sup>
SSL Security Processor ('S' Models)	N/A	Dual	Dual or Quad
Power Consumption (Typical/Max) <sup>*3</sup>	57W / 75W	190W / 240W	210W / 260W
Heat in BTU/hour (Typical/Max) <sup>*3</sup>	195 / 256	648 / 819	717 / 887
Power Supply (DC option available)	Single 150W (AC only) 100 - 240 VAC, 50-60Hz	Dual 600W RPS 80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz	Dual 600W RPS
Cooling Fan	Single Fixed Fan	Hot Swap Smart Fans	
Dimensions	1.75 in (H), 17.0 (W), 12 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	8.8 lbs	23 lbs	23 lbs
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%		
Regulatory Certifications	FCC Class A <sup>*</sup> , UL, CE <sup>*</sup> , TUV <sup>*</sup> , CB <sup>*</sup> , VCCI <sup>*</sup> , China CCC, BSMI <sup>*</sup> , RCM <sup>*</sup>   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, MSIP, BSMI, RCM, NEBS   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, MSIP, BSMI, RCM, NEBS   RoHS, FIPS 140-2 <sup>*+</sup>
Standard Warranty	90-day Hardware and Software		

\*1 SSLi performance are measured in single appliance SSLi deployment. | \*2 With maximum SSL | \*3 With base model. Number varies by SSL model |

\*4 No dedicated hardware but FTA-4 FPGA handles select switching/routing functions | <sup>\*</sup> Certification in process | <sup>+</sup> FIPS model must be purchased

## Thunder CFW Specifications Table (continued)

	Thunder 4440(S)	Thunder 5330(S)	Thunder 5440(S)
<b>Data Center Firewall</b>			
DCFW Throughput	70 Gbps	70 Gbps	90 Gbps
DCFW Layer 4 CPS	2.8 million	2.8 million	3.5 million
DCFW Concurrent Sessions	64 million	64 million	128 million
DCFW Rules	32k	32k	64k
<b>Secure Web Gateway<sup>*1</sup>   <sup>*2</sup></b>			
SSLi Throughput (2k key)	8 Gbps	8 Gbps	12.5 Gbps
SSLi CPS (2k key)	22k	24k	28k
<b>IPsec VPN<sup>*2</sup></b>			
IPsec Throughput	30 Gbps	35 Gbps	35 Gbps
IPsec Tunnels	4k	4k	8k
<b>Network Interface</b>			
1 GE Copper	0	0	0
1 GE Fiber (SFP)	0	0	0
1/10 GE Fiber (SFP+)	24	8	24
40 GE Fiber (QSFP+)	4	0	4
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon 6-core	Intel Xeon 10-core	Intel Xeon 12-core
Memory (ECC RAM)	32 GB	32 GB	64 GB
<b>Hardware Acceleration</b>			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	2 x FTA-4 FPGA	1 x FTA-4 FPGA	2 x FTA-4 FPGA
Switching/Routing	Hardware	Hybrid <sup>*4</sup>	Hardware
SSL Security Processor ('S' Models)	Dual or Quad	Dual or Quad	Dual or Quad
Power Consumption (Typical/Max) <sup>*3</sup>	360W / 445W	210W / 260W	360W / 445W
Heat in BTU/hour (Typical/Max) <sup>*3</sup>	1,229 / 1,519	717 / 887	1,229 / 1,519
Power Supply (DC option available)	Dual 1100W RPS	Dual 600W RPS	Dual 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz		
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	32.5 lbs	23 lbs	32.5 lbs
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%		
Regulatory Certifications	FCC Class A <sup>^</sup> , UL <sup>^</sup> , CE <sup>^</sup> , TUV <sup>^</sup> , CB <sup>^</sup> , VCCI <sup>^</sup> , China CCC, BSMI <sup>^</sup> , RCM <sup>^</sup>   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, NEBS   RoHS	FCC Class A <sup>^</sup> , UL <sup>^</sup> , CE <sup>^</sup> , TUV <sup>^</sup> , CB <sup>^</sup> , VCCI <sup>^</sup> , China CCC, BSMI <sup>^</sup> , RCM <sup>^</sup>   RoHS, FIPS 140-2 <sup>†</sup>
Standard Warranty	90-day Hardware and Software		

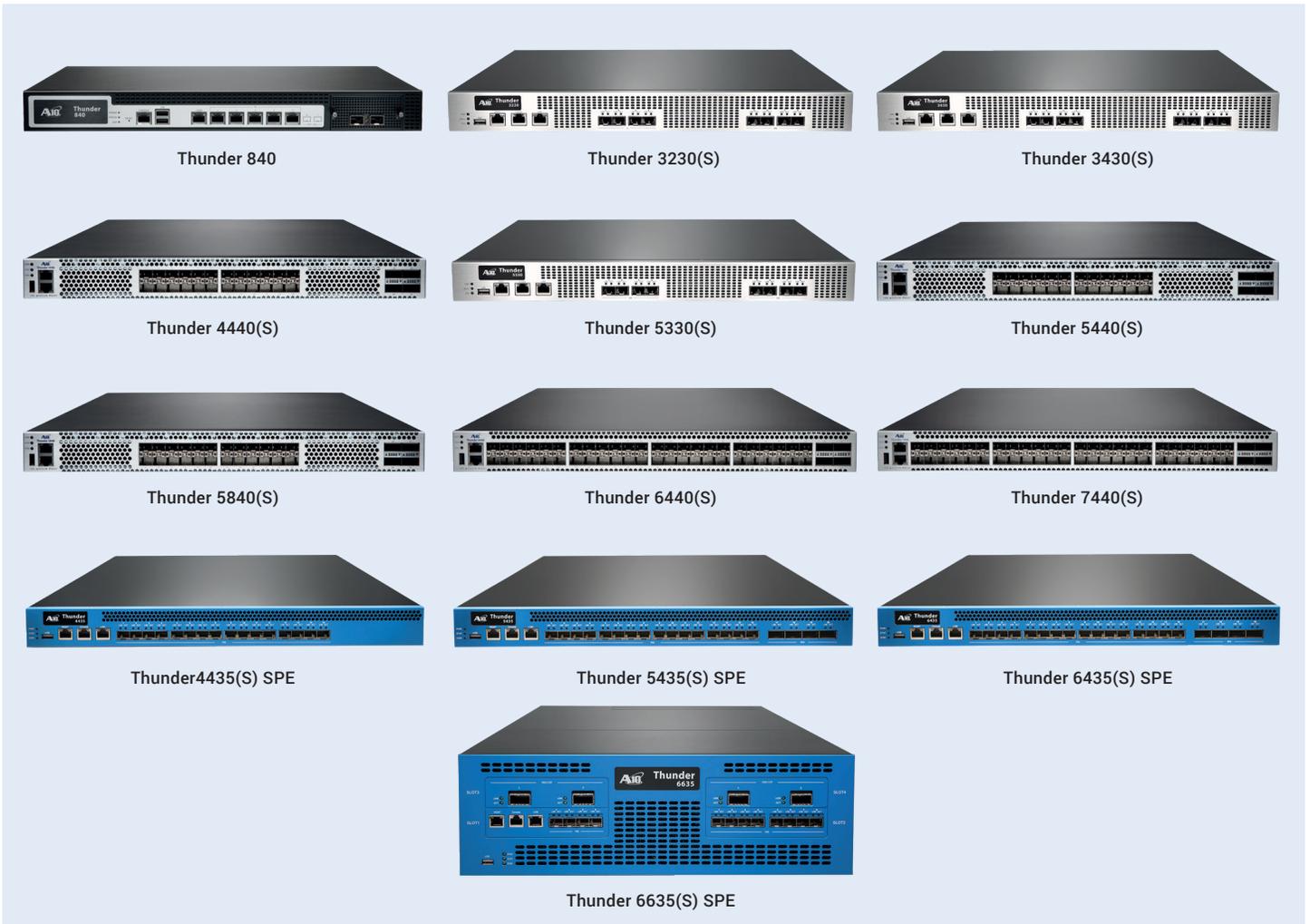
<sup>\*1</sup> SSLi performance are measured in single appliance SSLi deployment. | <sup>\*2</sup> With maximum SSL | <sup>\*3</sup> With base model. Number varies by SSL model |  
<sup>\*4</sup> No dedicated hardware but FTA-4 FPGA handles select switching/routing functions | <sup>^</sup> Certification in process | <sup>†</sup> FIPS model must be purchased

## Thunder CFW Specifications Table (continued)

	Thunder 5840(S)	Thunder 6440(S)	Thunder 7440(S)
<b>Data Center Firewall</b>			
DCFW Throughput	100 Gbps	150 Gbps	220 Gbps
DCFW Layer 4 CPS	4.5 million	4.5 million	6.5 million
DCFW Concurrent Sessions	128 million	256 million	256 million
DCFW Rules	64k	128k	128k
<b>Secure Web Gateway<sup>*1   *2</sup></b>			
SSLi Throughput (2k key)	17.5 Gbps	TBD	TBD
SSLi CPS (2k key)	50k	TBD	TBD
<b>IPsec VPN<sup>*2</sup></b>			
IPsec Throughput	35 Gbps	TBD	TBD
IPsec Tunnels	8k	20k	20k
<b>Network Interface</b>			
1 GE Copper	0	0	0
1 GE Fiber (SFP)	0	0	0
1/10 GE Fiber (SFP+)	24	48	48
40 GE Fiber (QSFP+)	4	4	4
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon 18-core	Intel Xeon Dual 8-core	Intel Xeon Dual 18-core
Memory (ECC RAM)	64 GB	128 GB	128 GB
<b>Hardware Acceleration</b>			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	2x FTA-4 FPGA	3 x FTA-4 FPGA	3 x FTA-4 FPGA
Switching/Routing	Hardware	Hardware	Hardware
SSL Security Processor ('S' Models)	Dual or Quad	2 x Dual	2 x Dual
Power Consumption (Typical/Max) <sup>*3</sup>	375W / 470W	480W / 550W	690W / 820W
Heat in BTU/hour (Typical/Max) <sup>*3</sup>	1,280 / 1,604	1,638 / 1,877	2,355 / 2,798
Power Supply (DC option available)	Dual 1100W RPS	Dual 1100W RPS	Dual 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz		
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	32.5 lbs	36 lbs	36 lbs
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%		
Regulatory Certifications	FCC Class A <sup>*</sup> , UL <sup>*</sup> , CE <sup>*</sup> , TUV <sup>*</sup> , CB <sup>*</sup> , VCCI <sup>*</sup> , China CCC, BSMI <sup>*</sup> , RCM <sup>*</sup>   RoHS	FCC Class A <sup>*</sup> , UL <sup>*</sup> , CE <sup>*</sup> , TUV <sup>*</sup> , CB <sup>*</sup> , VCCI <sup>*</sup> , China CCC <sup>*</sup> , BSMI <sup>*</sup> , RCM <sup>*</sup>   RoHS	FCC Class A <sup>*</sup> , UL <sup>*</sup> , CE <sup>*</sup> , TUV <sup>*</sup> , CB <sup>*</sup> , VCCI <sup>*</sup> , China CCC <sup>*</sup> , BSMI <sup>*</sup> , RCM <sup>*</sup>   RoHS, FIPS 140-2 <sup>*1*</sup>
Standard Warranty	90-day Hardware and Software		
<small>*1 SSLi performance are measured in single appliance SSLi deployment.   *2 With maximum SSL   *3 With base model. Number varies by SSL model   *4 No dedicated hardware but FTA-4 FPGA handles select switching/routing functions   ^ Certification in process   + FIPS model must be purchased</small>			

## Thunder CFW SPE Specifications Table

	Thunder 4435(S) SPE	Thunder 5435(S) SPE	Thunder 6435(S) SPE	Thunder 6635(S) SPE
<b>Data Center Firewall</b>				
DCFW Throughput	38 Gbps	76 Gbps	140 Gbps	150 Gbps
DCFW Layer 4 CPS	2.7 million	2.8 million	5.5 million	5.5 million
DCFW Concurrent Sessions	128 million	128 million	256 million	256 million
DCFW Rules	64k	64k	128k	128k
<b>Secure Web Gateway<sup>*1</sup>   <sup>*2</sup></b>				
SSLi Throughput (2k key)	8 Gbps	8 Gbps	17.5 Gbps	17.5 Gbps
SSLi CPS (2k key)	22k	22k	50k	50k
<b>IPsec VPN<sup>*2</sup></b>				
IPsec Throughput	20 Gbps	20 Gbps	70 Gbps	80 Gbps
IPsec Tunnels	6k	6k	20k	20k
<b>Network Interface</b>				
1 GE Copper	0	0	0	0
1 GE Fiber (SFP)	0	0	0	0
1/10 GE Fiber (SFP+)	16	16	16	12
40 GE Fiber (QSFP+)	0	4	4	0
100 GE Fiber (CXP)	0	0	0	4
Management Interface	Yes	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes	Yes
Console Port	Yes	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes	Yes
Processor	Intel Xeon 10-core	Intel Xeon 10-core	Intel Xeon Dual 12-core	Intel Xeon Dual 12-core
Memory (ECC RAM)	64 GB	64 GB	128 GB	128 GB
<b>Hardware Acceleration</b>				
64-bit Linear Decoupled Architecture	Yes	Yes	Yes	Yes
Flexible Traffic Acceleration	1 x FTA-3+ FPGA	2 x FTA-3+ FPGA	4 x FTA-3+ FPGA	4 x FTA-3+ FPGA
Security & Policy Engine	Hardware	Hardware	Hardware	Hardware
Switching/Routing	Hardware	Hardware	Hardware	Hardware
SSL Security Processor ('S' Models)	Dual	Dual	Quad	2 x Dual, 2 x Quad or 4 x Quad
Power Consumption (Typical/Max) <sup>*3</sup>	350W / 420W	400W / 480W	620W / 710W	995W / 1,150W
Heat in BTU/hour (Typical/Max) <sup>*3</sup>	1,195 / 1,433	1,365 / 1,638	2,116 / 2,423	3,395 / 3,924
Power Supply (DC option available)	Dual 1100W RPS	Dual 1100W RPS	Dual 1100W RPS	2+2 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 – 60 Hz			
Cooling Fan	Hot Swap Smart Fans			
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	5.3 in (H), 16.9 in (W), 28 in (D)
Rack Units (Mountable)	1U	1U	1U	3U
Unit Weight	34.5 lbs	35.5 lbs	39 lbs	74.5 lbs / 78 lbs <sup>*2</sup>
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, MSIP, EAC, NEBS   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, EAC, NEBS   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, EAC, NEBS   RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, EAC, FAC   RoHS
Standard Warranty	90-day Hardware and Software			
*1 SSLi performance are measured in single appliance SSLi deployment.   *2 With maximum SSL   *3 With base model. Number varies by SSL model				



## Detailed Feature List\*

### Data Center Firewall (DCFw)

#### Firewall:

- Stateful L4 network firewall
- Application Layer Gateways (FTP, TFTP, DNS and SIP)
- Web Application Firewall (WAF)
- DNS Application Firewall (DAF)

#### DDoS Protection:

- Flood attack protection: SYN cookies, TCP/UDP/ICMP flood protection, DNS/HTTP flood protection
- Protocol attack protection: Invalid packets, anomalous TCP flag combinations, packet size validation (ping of death)
- Resource attack protection: Slowloris, slow POST, and Sockstress protection, fragmentation
- Rate limiting: IP-based connection, HTTP, DNS request, DNS query, ICMP rate limiting

#### Application Access Management (AAM):

- Authentication methods: HTTP Basic, NTLM over HTTP, form-based, OCSP, TDS SQL Logon and SAML
- Authentication servers: LDAP, Active Directory, RADIUS, OCSP Responder, NTLM, Kerberos, RSA Secure ID, Entrust Identity Guard and SAML Identity Provider (IdP)

- Authentication relay: Kerberos, form-based, LDAP, WS-Federation, and Microsoft SharePoint and Outlook Web Access
- Extensive logging for audit

#### ADC:

- Advanced Layer 4/Layer 7 server load balancing
  - Fast HTTP, full HTTP proxy
  - High-performance, template-based L7 switching with header/URL/domain manipulation
  - Comprehensive L7 application persistence support
- Comprehensive load-balancing methods – round-robin, weighted round-robin (WRR), least connections (LC), fastest response and more
- Comprehensive IPv4/IPv6 support
- A10 Networks aFlex® TCL-based scripting technology – deep packet inspection and transformation for customizable, application-aware switching
- Global Server Load Balancing (GSLB)
- HTTP acceleration: HTTP connection multiplexing (TCP connection reuse), RAM caching, HTTP compression
- SSL acceleration: Hardware SSL offload, TLS 1.2 and 4096-bit SSL key support, Elliptic Curve Diffie-Hellman Exchange (ECDHE) and other ECC ciphers

## Gi/SGi Firewall

### Firewall:

- Stateful Layer 4 network firewall
- ALG protocol support for protocols with dynamic ports (including SIP, FTP)

### DDoS Protection:

- Integrated DDoS protection for NAT pools
- IP anomaly detection

### IPv4 Preservation (CGNAT):

- Carrier Grade NAT (CGN/CGNAT), Large Scale NAT (LSN), NAT444, NAT44

### IPv6 Migration:

- Dual stack support, full native IPv6 management and features
- SLB-PT (Protocol Translation), SLB-64 (IPv4<->IPv6, IPv6<->IPv4)
- NAT64/DNS64, NAT46, DS-Lite, 6rd, LW4o6

## Secure Web Gateway (SWG)

### SSL Insight:

- High-performance SSL decryption and encryption as a forward proxy
- Internet Content Adaptation Protocol (ICAP) support for data loss prevention
- Dynamic port decryption to detect and intercept SSL or TLS traffic regardless of TCP port number
- Forward proxy failsafe to bypass traffic when there is a handshake failure
- SSL Insight bypass based on hostname; bypass list scales up to 1 million Server Name Indication (SNI) values
- Multi-bypass list support
- Decryption of HTTPS, STARTTLS, SMTP, XMPP
- Client certificate detection and optional bypass
- Untrusted certificate handling using the Online Certificate Status Protocol (OCSP)
- TLS alert logging to log flow information from SSL Insight events
- SSL session ID reuse
- Firewall Load Balancing (FWLB)

### URL Filtering:

- URL Classification Service powered by Webroot to selectively bypass trusted websites for SSL decryption\*\*
- Optional monitoring and blocking of malicious or undesirable websites

## Operation modes

- Transparent Forward Proxy
- Explicit Forward Proxy
- Proxy chaining

## IPsec VPN

- Route-based VPN
- Keying methods – IKEv1, IKEv2
- Authentication methods – RSA Signature, Pre-shared Key, Public Key Infrastructure (PKI)
- Key Exchange Diffie-Hellman Groups – 1, 2, 5, 14, 15, 16, 18
- Encryption and data integrity algorithms – DES, 3DES, AES-128, AES-192, AES-256
- OSPF, BGP and Bidirectional Forwarding Detection (BFD) over

IPsec tunnel

- Equal Cost Multipath (ECMP) support
- NAT traversal
- Perfect Forward Secrecy (PFS) support
- Life bytes and time rekey
- PKI support with Simple Certificate Enrollment Protocol (SCEP), Online Certificate Status Protocol (OCSP) and certificate revocation list (CRL) distribution points

## A10 Threat Intelligence Service\*\*

- Dynamic threat intelligence feed updated in near real time
- 30+ public, private and proprietary sources to block “call homes” to command and control servers, identify known attack sources and mitigate zero-day attacks

## High-Performance ACOS Platform

- Scalable platform with multi-core, multi-CPU support
- Linear application performance scaling

## Networking

- Integrated L2/L3
- Transparent mode/gateway mode
- Routing – static routes, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access control lists (ACLs)
- Traditional IPv4 NAT/NAPT, IPv6 NAPT
- Jumbo Frame support
- Hardware-accelerated Virtual Extensible LAN (VXLAN)
- Network Virtualization using Generic Routing Encapsulation (NVGRE)

## Management

- Dedicated management interface (console, SSH, Telnet, HTTPS)
- Web-based GUI with language localization
- Industry-standard CLI support
- Granular role-based access control
- SNMP, syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
- Port mirroring
- REST-style XML API (aXAPI) for all functions
- LDAP, TACACS+, RADIUS support

## Virtualization

- aVCS (virtual chassis system)
- Multi-tenancy with ADPs
  - Partition-based management
  - L2/L3 virtualization

## Carrier-Grade Hardware

- Hot swap redundant power supplies (AC or DC)
- 40 GbE ports, 100 GbE ports
- Tamper detection
- Lights Out Management (LOM/IPMI)
- Hardware Security Module (HSM) option
- High-performance security processor option

\*Features and certifications may vary by appliance

\*\*Additional paid service

## About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: [www.a10networks.com](http://www.a10networks.com).

### Corporate Headquarters

**A10 Networks, Inc**  
3 West Plumeria Ave.  
San Jose, CA 95134 USA  
Tel: +1 408 325-8668  
Fax: +1 408 325-8666  
[www.a10networks.com](http://www.a10networks.com)

Part Number: A10-DS-15112-EN-06  
Aug 2016

### Worldwide Offices

#### North America

[sales@a10networks.com](mailto:sales@a10networks.com)

#### Europe

[emea\\_sales@a10networks.com](mailto:emea_sales@a10networks.com)

#### South America

[latam\\_sales@a10networks.com](mailto:latam_sales@a10networks.com)

#### Japan

[jinfo@a10networks.com](mailto:jinfo@a10networks.com)

#### China

[china\\_sales@a10networks.com](mailto:china_sales@a10networks.com)

#### Hong Kong

[HongKong@a10networks.com](mailto:HongKong@a10networks.com)

#### Taiwan

[taiwan@a10networks.com](mailto:taiwan@a10networks.com)

#### Korea

[korea@a10networks.com](mailto:korea@a10networks.com)

#### South Asia

[SouthAsia@a10networks.com](mailto:SouthAsia@a10networks.com)

#### Australia/New Zealand

[anz\\_sales@a10networks.com](mailto:anz_sales@a10networks.com)

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at [a10networks.com/contact](http://a10networks.com/contact) or call to speak with an A10 sales representative.