



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at [wvOASIS.gov](http://wvOASIS.gov). As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at [WVPurchasing.gov](http://WVPurchasing.gov) with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 7

List View

- General Information
- Contact
- Default Values
- Discount
- Document Information
- Clarification Request

Procurement Folder: 1918839

Procurement Type: Central Master Agreement

Vendor ID: 000000199010

Legal Name: EPLUS TECHNOLOGY INC

Alias/DBA:

Total Bid: \$313,298.97

Response Date: 03/23/2026

Response Time: 14:16

Responded By User ID: markcarretta

First Name: Mark

Last Name: Carretta

Email: mcarretta@eplus.com

Phone: 412-258-1697

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT2600000023

Published Date: 3/10/26

Close Date: 3/24/26

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No. 1 - Network Load Balancer Appliances

Total of Header Attachments: 7

Total of All Attachments: 7



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

**State of West Virginia  
 Solicitation Response**

**Proc Folder:** 1918839  
**Solicitation Description:** Addendum No. 1 - Network Load Balancer Appliances  
**Proc Type:** Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2026-03-24 13:30	SR 0231 ESR03092600000005786	1

**VENDOR**  
 000000199010  
 EPLUS TECHNOLOGY INC

**Solicitation Number:** CRFQ 0231 OOT2600000023  
**Total Bid:** 313298.9699999999720603227615 **Response Date:** 2026-03-23 **Response Time:** 14:16:47  
**Comments:**

**FOR INFORMATION CONTACT THE BUYER**  
 Toby L Welch  
 (304) 558-8802  
 toby.l.welch@wv.gov

**Vendor Signature X** **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	A10 Thunder 3350S Network Load Balancers, Pt#: TH335	3.00000	EA	35680.890000	107042.67

Comm Code	Manufacturer	Specification	Model #
43222634			

**Commodity Line Comments:** Thunder 3350S CFW, 1U, 1CPU, 6x1GC, 2x1GF, 8x10/1GF, 4x10GF, 64GB, 1SSD, No LOM, No FTA, no S+R ASIC, SSL Builtin + SSL Card, screwless railkit, 2 AC PSU, FIPS Compliant

**Extended Description:**

A10 Thunder 3350S Network Load Balancers, Part Number: TH3350S-020-CFW-FIPS "or Equal".

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appl	9.00000	EA	668.600000	6017.40

Comm Code	Manufacturer	Specification	Model #
43222634			

**Commodity Line Comments:** 10 GIG SFP+ FIBER TRANSCEIVER - SHORT RANGE

**Extended Description:**

10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appliance, Part Number: AXSK-SFP+ SR "or Equal"

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	(1) seat for training on Application Delivery Controller (AD	1.00000	EA	4178.800000	4178.80

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** Training Credits are redeemable for A10 Networks training items for up to 12 months by any employee of the organization. For a full list of training policies and class schedule, refer to A10's training website.

**Extended Description:**

(1) seat for training on Application Delivery Controller (ADC) Administration Course, SKU: AX-TR "or Equal".

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	1 each Gold SupportService Program for wo (2) appliances 3yr	2.00000	EA	35329.610000	70659.22

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** 24X7 TECHNICAL SUPPORT ACCESS/ADVANCED HARDWARE REPLACEMENT - 3 YEARS

**Extended Description:**

1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 3 Year period

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	1 Basic Support Service Program for one (1) appliance 3Yr	1.00000	EA	37465.920000	37465.92

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** 9 AM - 6 PM M-F TECHNICAL SUPPORT ACCESS/HARDWARE REPAIR - 3 YEARS

**Extended Description:**

1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 3 year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	Yr4 renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	14653.010000	29306.02

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** GOLD SUPPORT 1 YEAR

**Extended Description:**

1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" Year 4 Renewal

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	Yr 4 Renewal 1 Basic Support Service Program for one (1) app	1.00000	EA	13267.600000	13267.60

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** HW, FIRMWARE 8X5 M-F TECH SUPPORT FOR AX1000 - BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 4 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 3 year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	Yr 5 Renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	15656.650000	31313.30

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** GOLD SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" Year 4 Renewal

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	Yr 5 Renewal 1 Basic Support Service Program for one (1) app	1.00000	EA	14048.040000	14048.04

Comm Code	Manufacturer	Specification	Model #
81112201			

**Commodity Line Comments:** HW, FIRMWARE 8X5 M-F TECH SUPPORT FOR AX1000 - BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 3 year period.



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

State of West Virginia  
 Centralized Request for Quote  
 Info Technology

<b>Proc Folder:</b> 1918839			<b>Reason for Modification:</b>
<b>Doc Description:</b> Network Load Balancer Appliances			
<b>Proc Type:</b> Central Master Agreement			
<b>Date Issued</b>	<b>Solicitation Closes</b>	<b>Solicitation No</b>	<b>Version</b>
2026-03-09	2026-03-24 13:30	CRFQ 0231 OOT2600000023	1

**BID RECEIVING LOCATION**

BID CLERK  
 DEPARTMENT OF ADMINISTRATION  
 PURCHASING DIVISION  
 2019 WASHINGTON ST E  
 CHARLESTON WV 25305  
 US

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :** ePlus Technology, inc.

**Address :**

**Street :** 13595 Dulles Technology Dr.

**City :** Herndon

**State :** VA **Country :** USA **Zip :** 20171

**Principal Contact :** Don McLaughlin

**Vendor Contact Phone:** 703-984-8400 **Extension:**

**FOR INFORMATION CONTACT THE BUYER**  
 Toby L Welch  
 (304) 558-8802  
 toby.l.welch@wv.gov

**Vendor Signature X**  **FEIN#** 54-1904151 **DATE** 3/24/26

**ADDITIONAL INFORMATION**

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish an open-end contract to purchase three (3) new network load balancer appliances with maintenance and support per the attached documents

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	A10 Thunder 3350S Network Load Balancers, Pt#: TH335	3.00000	EA	\$ 35,680.89	\$107,042.67

Comm Code	Manufacturer	Specification	Model #
43222634	A10 Networks		TH3350S-020-CFW-FIPS

**Extended Description:**

A10 Thunder 3350S Network Load Balancers, Part Number: TH3350S-020-CFW-FIPS "or Equal".

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appl	9.00000	EA	\$ 668.60	\$6,017.40

Comm Code	Manufacturer	Specification	Model #
43222634	A10 Networks		AXSK-SFP+ SR

**Extended Description:**

10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appliance, Part Number: AXSK-SFP+ SR "or Equal"

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	(1) seat for training on Application Delivery Controller (ADC)	1.00000	EA	\$4,178.80.	\$4,178.80

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		TRAINING-CREDIT

**Extended Description:**

(1) seat for training on Application Delivery Controller (ADC) Administration Course, SKU: AX-TR "or Equal".

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	1 each Gold Support Service Program for two (2) appliances 3yr	2.00000	EA	\$35,329.61	\$70,659.22

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		GOLD SUPPORT 3 YEAR

**Extended Description:**

1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 3 Year period.

INVOICE TO			SHIP TO		
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US			WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	1 Basic Support Service Program for one (1) appliance 3Yr	1.00000	EA	\$37,465.92.	\$37,465.92

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks.		BASIC SUPPORT 3 YEAR

**Extended Description:**

1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 3 year period.

INVOICE TO			SHIP TO		
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US			WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Yr4 renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	\$ 14,653.01	\$ 29,306.02

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		GOLD SUPPORT 1 YEAR

**Extended Description:**

1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 1 year period.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
7	Yr 4 Renewal 1 Basic Support Service Program for one (1) app	1.00000	EA	\$ 13,267.60	\$ 13,267.60

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 4 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 1 year period.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
8	Yr 5 Renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	\$ 15,656.65.	\$ 31,313.30

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		GOLD SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 1 year period.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
9	Yr 5 Renewal 1 Basic Support Service Program for one (1) app	1.00000	EA	\$ 14,048.04	\$ 14,048.04

Comm Code	Manufacturer	Specification	Model #
81112201	A10 Networks		BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 1 year period.

**SCHEDULE OF EVENTS**

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 3:00 p.m.	2026-03-16

	Document Phase	Document Description	Page
OOT2600000023	Final	Network Load Balancer Appliances	7

**ADDITIONAL TERMS AND CONDITIONS**

See attached document(s) for additional Terms and Conditions



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

State of West Virginia  
 Centralized Request for Quote  
 Info Technology

Proc Folder: 1918839			Reason for Modification:
Doc Description: Network Load Balancer Appliances			
Proc Type: Central Master Agreement			
Date Issued	Solicitation Closes	Solicitation No	Version
2026-03-09	2026-03-24 13:30	CRFQ 0231 OOT2600000023	1

**BID RECEIVING LOCATION**

BID CLERK  
 DEPARTMENT OF ADMINISTRATION  
 PURCHASING DIVISION  
 2019 WASHINGTON STE  
 CHARLESTON WV 25305  
 US

**VENDOR**

Vendor Customer Code:  
 Vendor Name : ePlus Technology, inc.  
 Address:  
 Street: 13595 Dulles Technology Dr.  
 City: Herndon  
 State: VA Country: USA Zip: 20171  
 Principal Contact : Don McLaughlin  
 Vendor Contact Phone: 703-984-8400 Extension:

**FOR INFORMATION CONTACT THE BUYER**

Toby I Welch  
 (304) 558-8802  
 toby.i.welch@wv.gov

Vendor  
 Signature X

FEIN# 54-1904151

DATE 3/24/26

All offers subject to all terms and conditions contained in this solicitation

**ADDITIONAL INFORMATION**

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish an open-end contract to purchase three (3) new network load balancer appliances with maintenance and support per the attached documents

**INVOICE TO****SHIP TO**

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	A10 Thunder 3350S Network Load Balancers, Pt#: TH335	3.00000	EA	\$ 35,680.89	\$107,042.67

Comm Code	Manufacturer	Specification	Model#
43222634	A10 Networks		TH3350S-020-CFW-FIPS

**Extended Description:**

A10 Thunder 3350S Network Load Balancers, Part Number: TH3350S-020-CFW-FIPS "or Equal".

**INVOICE TO****SHIP TO**

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appl	9.00000	EA	\$ 668.60	\$6,017.40

Comm Code	Manufacturer	Specification	Model#
43222634	A10 Networks		AXSK-SFP+ SR

**Extended Description:**

10Gb SR-Optical Transceiver for the A10 Thunder AX 3350 Appliance, Part Number: AXSK-SFP+ SR "or Equal"

**INVOICE TO.****1 HIPTO:**

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	(1) seat for training on Application Delivery Controller (AD	1.00000	EA	\$ 4,178.80.	\$ 4,178.80

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		TRAINING-CREDIT

**Extended Description:**

(1) seat for training on Application Delivery Controller (ADC) Administration Course, SKU: AX-TR "or Equal".

**INVOICE TO ..****SHIP TO**

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	1 each Gold Support Service Program for two (2) appliances 3yr	2.00000	EA	\$ 35,329.61	\$ 70,659.22

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		GOLD SUPPORT 3 YEAR

**Extended Description:**

1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 3 Year period

INVOICE TO: .ISHIPTO

DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US
---	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	1 Basic Support Service Program for one (1) appliance 3Yr	1.00000	EA	\$37,465.92	\$ 37,465.92

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		BASIC SUPPORT 3 YEAR

**Extended Description:**  
1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 3 year period.

INVOICE TO: SHIP TO

DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 <b>KANAWHA</b> BLVD E CHARLESTON WV US
---	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Yr4 renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	\$ 14,653.01	\$ 29,306.02

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		GOLD SUPPORT 1 YEAR

**Extended Description:**  
1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 1 year period.

INVOICE TO

SHIP TO

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
7	Yr 4 Renewal 1 Basic Support Service Program for one (1) app	1.00000	EA	\$ 13,267.60	\$ 13,267.60

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 4 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 1 year period..

INVOICE TO

SHIP TO

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLDG 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
8	Yr 5 Renewal 1 each Gold Support Service Program for two (2)	2.00000	EA	\$ 15,656.65.	\$ 31,313.30

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		GOLD SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 each Gold Support Service Program for two (2) appliances listed in section 3.1.1 for a total quantity of 2 Gold Support Service Program "or Equal" for 1 year period.

**INVOICE TO****SHIP TO**

DEPARTMENT OF  
ADMINISTRATION  
OFFICE OF TECHNOLOGY  
1900 KANAWHA BLVD E,  
BLDG 5 10TH FLOOR  
CHARLESTON WV  
US

WV OFFICE OF  
TECHNOLOGY  
BLD G 5, 10TH FLOOR  
1900 KANAWHA BLVD E  
CHARLESTON WV  
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
9	Yr 5 Renewal 1 Basic Support Service Program for one (1) app	2.00000	EA	\$ 14,048.04	\$ 14,048.04

Comm Code	Manufacturer	Specification	Model#
81112201	A10 Networks		BASIC SUPPORT 1 YEAR

**Extended Description:**

Yr 5 Renewal 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" for 1 year period.

**SCHEDULE OF EVENTS**

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-03-16

	Document Phase	Document Description	Page
OOT2600000023	Draft	NetworkLoadBalancer Appliances	7

**ADDITIONAL TERMS AND CONDITIONS**

See attached document(s) for additional Terms and Conditions

## INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. **REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. **MANDATORY TERMS:** The Solicitation may contain **mandatory** provisions identified by the use of the words "**must**," "**will**," and "**shall**." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. **PRE-BID MEETING:** The item identified below shall apply to this Solicitation.

A pre-bid meeting will not be held prior to bid opening

A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the **mandatory** pre-bid meeting. Failure to attend the **mandatory** pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

**4. VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions **must be submitted on or before the date listed below and to the address listed below to be considered.** A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are non-binding.

Submitted emails should have the solicitation number in the subject line. Question

Submission Deadline: Monday March 16, 2026 @ 3:00 p.m.

Submit Questions to: Toby L Welch  
2019 Washington Street, East Charleston, WV 25305  
Fax: (304) 558-3970  
Email: [Toby.L.Welch@wv.gov](mailto:Toby.L.Welch@wv.gov)

**5. VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

**6. BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through wvOASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. The Purchasing Division will not accept bids or modification of bids via email.

**Bids submitted in paper, facsimile, or via wvOASIS must contain a signature. Failure to submit a bid in any form without a signature will result in rejection of your bid.**

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:

BUYER: Toby L Welch

SOLICITATION NO.: CRFQ OOT2600000023

BID OPENING DATE: TUESDAY MARCH 24, 2026

BID OPENING TIME: 1:30 P.M.

FAX NUMBER: 304-558-3970

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

**Bid Delivery Address and Fax Number:**

Department of Administration, Purchasing Division 2019 Washington Street East

Charleston, WV 25305-0130

Fax: 304-558-3970

**7. BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when continuation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery or via delivery by mail).

Bid Opening Date and Time: 3/24/26 @ 1:30 P.M.

Bid Opening Location:

Department of Administration, Purchasing Division

2019 Washington Street East

Charleston, WV 25305-0130

**8. ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgement Form. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

**9. BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

**10. ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand **shall** clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

**D** This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

**11. COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6.2, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

**12. REGISTRATION:** Prior to Contract award, the apparent successful Vendor **must** be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

**13. UNIT PRICE:** Unit prices **shall** prevail in cases of a discrepancy in the Vendor's bid.

**14. PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § SA-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: [www.state.wv.us/admin/purchase/vrcNenpref.pdf](http://www.state.wv.us/admin/purchase/vrcNenpref.pdf).

**15A. RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: [www.state.wv.us/admin/purchase/vrcNenpref.pdf](http://www.state.wv.us/admin/purchase/vrcNenpref.pdf).

**15. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:**

For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR§ 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR§ 148-22-9 prior to contract award to receive the preferences made available to resident vendors.

**16. WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules§ 148-1-4.7.

**17. ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

**18. NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules§ 148-1- 5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

**19. ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules§ 148-1-4.6. and§ 148-1-6.3."

20. **WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.7. This authority does not apply to instances where state law mandates receipt with the bid.

21. **EMAIL NOTIFICATION OF AWARD:** The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor wvOASIS or the Purchasing Division's website to determine when a contract has been awarded.

22. **EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that **shall** form the basis of a contractual agreement. **Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid.** Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

## **GENERAL TERMS AND CONDITIONS:**

**1. CONTRACTUAL AGREEMENT:** Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

**2.1. "Agency" or "Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

**2.2. "Bid" or "Proposal"** means the vendors submitted response to this solicitation.

**2.3. "Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

**2.4. "Director"** means the Director of the West Virginia Department of Administration, Purchasing Division.

**2.5. "Purchasing Division"** means the West Virginia Department of Administration, Purchasing Division.

**2.6. "Award Document"** means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

**2.7. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

**2.8. "State"** means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

**2.9. "Vendor" or "Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**3. CONTRACT TERM; RENEWAL; EXTENSION:** The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

**Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of THREE (3) YEARS. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_) and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to TWO (2) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**D Alternate Renewal Term** - This contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

**D Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within \_\_\_\_\_ days.

**D Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within \_\_\_\_\_ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

**D** the contract will continue for \_\_\_\_\_ years;

**D** the contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

**D One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

**D Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_ and continues until the project for which the vendor is providing oversight is complete.

**D Other:** Contract Term specified in \_\_\_\_\_

**4. AUTHORITY TO PROCEED:** Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

**5. QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

**D Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

**D Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

**Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

**D One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

**D Construction:** This Contract is for construction activity more fully defined in the specifications.

**6. EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

**7. REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

**LICENSE(S) /CERTIFICATIONS/ PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a foml acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

**8. INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

**Commercial General Liability Insurance** in at least an amount of: \$, 1,000,000.00 per occurrence.

**Automobile Liability Insurance** in at least an amount of: \$1,000,000.00 per occurrence.

**Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: \_\_\_\_\_ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

**Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Cyber Liability Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

**Pollution Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Aircraft Liability** in an amount of: \_\_\_\_\_ per occurrence.

**9. WORKERS' COMPENSATION INSURANCE:** Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**10. VENUE:** All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

**11. LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

\_\_\_\_\_ for \_\_\_\_\_

Liquidated Damages Contained in the Specifications.

Liquidated Damages Are Not Included in this Contract.

**12. ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

**14. PAYMENT IN ARREARS:** Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. {The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.}

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**17. ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**18. FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

**19. CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.

**20. TIME:** Time is of the essence regarding all matters of time and performance in this Contract.

**21. APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

**22. COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**23. ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

**24. MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

**25. WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

**26. SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**28. WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in [www.state.wv.us/admin/purchase/privacy](http://www.state.wv.us/admin/purchase/privacy).

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 50-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**32. LICENSING:** In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, penning, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, penning, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**34. VENDOR NON-CONFLICT:** Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**37. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

**38. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

**39. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

**D** Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at [purchasing.division@wv.gov](mailto:purchasing.division@wv.gov).

**40. BACKGROUND CHECK:** In accordance with W. Va. Code§ 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

**41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS:** Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code§ SA-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code§ SA-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.
- c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
  1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
  2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In Accordance with W. Va. Code§ 5-19-1 et seq., and W. Va. CSR§ 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code§ 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**44. PROHIBITION AGAINST USED OR REFURBISHED:** Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § SA-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title)\_\_\_\_\_

(Address)\_\_\_\_\_

(Phone Number)/(Fax Number)\_\_\_\_\_

(email address)\_\_\_\_\_

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

*By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.*

\_\_\_\_\_  
(Company)

\_\_\_\_\_  
(Signature of Authorized Representative)

\_\_\_\_\_  
(Printed Name and Title of Authorized Representative) (Date)

\_\_\_\_\_  
(Phone Number) (Fax Number)

\_\_\_\_\_  
(Email Address)

REQUEST FOR QUOTATION  
**Network Load Balancer Appliances**

---

**SPECIFICATIONS**

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for the purchase of new network load balancer appliances. The network load balancer appliances will reroute network traffic to a secondary set of servers in the event the primary servers become unresponsive. In addition, they provide flexibility to take a host or primary site down for maintenance while the load is redirected. Network traffic load is balanced across a number of hosts, which enhances the scalability and availability of mission critical IP-based services such as virtual private networks, streaming media, terminal services, and proxies. Multiple lines of business applications are hosted behind these devices to ensure business continuity of the state government in the event of a disaster or failure. The high availability that is provided detects host failures and automatically redistributes traffic to operational hosts.
  
2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in Section 2 of the General Terms and Conditions.
  - 2.1 **"Appliance"** means a device or piece of equipment designed to perform a specific task.
  
  - 2.2 **"Business Hours"** means Monday 9:00 AM to Friday 6:00 PM EST excluding weekends and Federal and State holidays. State Holidays are as follows:
    - New Year's Day (January 1)
    - Martin Luther King Day (Third Monday in January)
    - President's Day (Third Monday in February)
    - Memorial Day (Last Monday in May)
    - West Virginia Day (June 20)
    - Independence Day (July 4)
    - Labor Day (First Monday in September)
    - Columbus Day (Second Monday in October)
    - Veterans Day (November 11)
    - Thanksgiving (Fourth Thursday in November)
    - Day After Thanksgiving (Fourth Friday in November)
    - Christmas Day (December 25)
  
  - 2.3 **"Contract Item"** means network load balancer appliances, optical transceivers, and training as more fully described by these specifications.

REQUEST FOR QUOTATION  
**Network Load Balancer Appliances**

---

- 2.4 **"ECC"** means Error Correction Code. ECC is used on Random Access Memory (RAM) or memory. ECC is used for validating data being sent to and from the RAM.
- 2.5 **"FIPS"** means Federal Information Processing Standards.
- 2.6 **"Gb"** means Gigabit. A gigabit is used to measure the data transfer rates. This is not to be confused with gigabyte, which is abbreviated GB.
- 2.7 **"GB"** means Gigabyte. A gigabyte is a measure of computer data storage capacity.
- 2.8 **"Pricing Page"** means the pages, contained in wvOASIS or attached as Exhibit A, upon which Vendor should list its proposed price for the Contract Items.
- 2.9 **"RAM"** means Random Access Memory. This is where current data is kept and can be accessed quickly by an appliances processor.
- 2.10 **"SSD"** means Solid State Drive. SSD is a mass storage device that is similar to a hard disk drive in that it can read and write data to the drive. However, it maintains the stored data in a permanent state.
- 2.11 **"SSL"** means Secure Socket Layer. A secure protocol that provides encryption for sending information securely over the internet.
- 2.12 **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
- 2.13 **"VRRP"** means Virtual Router Redundancy Protocol. VRRP is a networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

**3. GENERAL REQUIREMENTS:**

- 3.1 **Mandatory Contract Item Requirements:** Contract Item must meet or exceed the mandatory requirements listed below.

**Network Load Balancer Appliances:**

REQUEST FOR QUOTATION  
**Network Load Balancer Appliances**

---

**3.1.1 Commodity Line 1:** Vendor must provide a quantity of three (3) A10 Thunder 3350S Network Load Balancers, Part Number: TH3350S-020-CFW-FIPS "or Equal".

Thunder 3 OS\_Network Load Balancer or Equal must contain the following hardware specifications:

- 3.1.1.1 Must fit in 1 U of rack space
- 3.1.1.2 Must have a minimum of 1 Central Processing Unit
- 3.1.1.3 Must have a minimum of 6 1 Gb over Copper ports
- 3.1.1.4 Must have a minimum of 2 1 Gb (SFP) Fiberports
- 3.1.1.5 Must have a minimum of 4 10Gb (SFP+) Fiber ports
- 3.1.1.6 Must have a minimum of 32GB of RAM (ECC)
- 3.1.1.7 Must be equipped with a Solid State Drive (SSD)
- 3.1.1.8 Must feature Hardware acceleration/ SSL Offload
- 3.1.1.9 Must support Virtual Router Redundancy Protocol supplement - A (VRRP-A) Failover
- 3.1.1.10 Must have FIPS 140-2 certification or better
- 3.1.1.11 Must support Layer 4-7 load balancing
- 3.1.1.12 Any appliance listed as refurbished or "like new" condition will be disqualified.

**Optical Transceivers:**

**3.1.2 Commodity Line 2:** Vendor must provide a quantity of three (3) each per appliance for a total quantity of nine , 10Gb SR-Optical Transceiver for the AIO Thunder AX3350 Appliance, Part Number: **AXSK-SFP+SR** "or Equal"

- 3.1.2.1 Transceivers must be compatible with the Thunder 3350 Network Load Balancer or Equal product bid on Commodity Line 1
- 3.1.2.2 Vendor must submit documentation that the Transceivers are certified by the manufacturer upon delivery
- 3.1.2.3 Any networking components listed as refurbished or "like new" condition will be disqualified.

**Training:**

REQUEST FOR QUOTATION  
Network Load Balancer Appliances

---

**3.1.3 Commodity Line 3:** Vendor must provide a quantity of one (1) seat for training on Application Delivery Controller (ADC) Administration Course, SKU: AX-TR "or Equal".

3.1.3.1 Vendor must provide instructor-led training course at the vendor's facility. The course must cover the following topics.

**3.1.3.1.1** Advanced Core Operating System Management

3.1.3.1.2 Load balancing

3.1.3.1.3 HTTP protocol

3.1.3.1.4 HTTPS protocol

3.1.3.1.5 Acceleration

3.1.3.1.6 Security

3.1.3.1.7 High Availability

3.1.3.1.8 Troubleshooting

3.1.3.1.9 aFlex

**Hardware Maintenance and Support:**

**3.1.4 Commodity Line 4:** Vendor must provide a quantity of 1 each Gold Support Service Program for Three appliances listed in section 3.1. I for a total quantity of 2 Gold Support Service Program "or Equal" For 3 year period, with 2, I year renewals.

3.1.4.1 Vendor will provide technical phone support 24 hours a day, 7 days a week.

3.1.4.2 Vendor will provide software updates, patches, and releases.

3.1.4.3 Vendor will provide advanced hardware replacement in the event of failure for the length of the contract.

**3.1.4.3.1** System failure will be confirmed by phone support or email support.

**3.1.4.3.2** Tech support personnel must issue a Return Material Authorization (**RMA**) number.

**3.1.4.3.3** Replacement hardware must be new. Hardware listed as refurbished, reconditioned, or "like new" condition will not be accepted.

**3.1.4.3.4** The advance replacement should be received the next business day.

REQUEST FOR QUOTATION  
**Network Load Balancer Appliances**

---

**3.1.5 Commodity Line 5:** Vendor must provide a quantity of 1 Basic Support Service Program for one (1) appliance listed in section 3.1.1 for a total quantity of 1 Basic Support Service Program "or Equal" For 3 Yr Period with 2, 1 year renewals.

3.1.5.1 Vendor will provide technical phone support during Business Hours as defined in Section 2. from 9:00AM to 6:00PM EST

3.1.5.2 Vendor will provide software updates, patches, and releases.

3.1.5.3 Vendor will provide advanced hardware replacement in the event of failure as confirmed by the vendor's technical support personnel during the first 30 calendar days from date of installation.

**3.1.5.3.1** System failure will be confirmed by phone support or email support.

**3.1.5.3.2** Tech support personnel must issue a Return Material Authorization (RMA) number.

**3.1.5.3.3** Replacement hardware must be new. Hardware listed as refurbished, reconditioned, or "like new" condition will not be accepted.

3.1.5.4 Vendor will provide hardware repair in the event of failure after 30 calendar days from installation during the Basic Support Service Program "or Equal" from date of installation. After system failure is confirmed technical support personnel via phone or email support a Return Material Authorization number will be issued.

**3.1.5.4.1** The appliance will be repaired, or, at the vendor's discretion, will be replaced with new hardware at equal or better value. Hardware listed as refurbished, reconditioned, or "like new" condition will not be accepted.

**3.1.6 Commodity Line 5-7:** Vendor must include in their bid the cost of optional Annual renewals the Gold Support Services Program quantity of one (1) each for two (2) appliances for initial 3 year period with 2, 1 year renewals and the Basic Support Services Program quantity of one (1) for 3 years with 2, 1 year renewals. These optional Annual renewals will be initiated by the Agency, agreed to by the Vendor and processed as a Change Order authorized by the West Virginia Purchasing Division.

REQUEST FOR QUOTATION  
Network Load Balancer Appliances

---

**4. CONTRACT AWARD:**

**4.1 Contract Award:** The Contract is intended to provide Agency with a purchase price for the Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

**Evaluation and Awarded Contract will be based upon the Total Price for all items requested.**

Renewal options for years 4 and 5 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

**4.2 Pricing Page:** Vendor should complete the Pricing Page and submit it as part of the bid response. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

**4.2.1** If the Vendor is submitting an Equivalent Brand, this information including Model Number must be submitted with their bid submission.

**4.2.2** Vendor will include the renewal cost should the agency opt to renew for years 4 and 5. Vendor should complete the Pricing Page in its' entirety as failure to do so may result in Vendor's bid being disqualified.

**4.2.3** Vendor should electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document. In most cases, the Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to the following address: [Laura.B.Hooper@WV.gov](mailto:Laura.B.Hooper@WV.gov).

***VENDOR'S WHO WISH TO RESPOND TO A CENTRALIZED REQUEST FOR QUOTATION (CRFQ) ONLINE MAY SUBMIT INFORMATION THROUGH THE STATE'S WVOASIS VENDOR SELF SERVICE (VSS). VENDORS SHOULD DOWNLOAD THE EXHIBIT "A": PRICING PAGE THAT IS ATTACHED SEPARATELY TO THE CRFQ AND PUBLISHED TO THE VSS. VENDORS MUST COMPLETE THIS FORM WITH THEIR PRICE INFORMATION AND INCLUDE IT AS AN ATTACHMENT TO THEIR ONLINE RESPONSE WITH AN ATTACHMENT TYPE OF "PRICING". THE PRICING***

REQUEST FOR QUOTATION  
Network Load Balancer Appliances

---

***PAGE ATTACHMENTS (PRICING) ARE THEN  
DOWNLOADED BY THE BUYER DURING THE  
SCHEDULED BID OPENING FOR BID EVALUATION.***

***IF UNABLE TO RESPOND ONLINE VENDOR MUST SUBMIT  
THE EXHIBIT "A" PROPOSAL FORM/PRICING PAGES  
WITH YOUR BID PRIOR TO THE SCHEDULED BID  
OPENING DATE.***

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

**5. PAYMENT:**

5.1 **Payment:** Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

**6. DELIVERY AND RETURN:**

6.1 **Shipment and Delivery:** Vendor shall ship the Contract Items immediately after being awarded this Contract and receiving a purchase order. Vendor shall deliver the Contract Items within 30 calendar days after receiving a purchase order. Contract Items must be delivered to Agency at:

West Virginia Office of Technology  
ATTENTION: Carmen Young  
908 Bullitt St.  
Charleston, WV 25301-1002

6.2 **Late Delivery:** The Agency placing the order under this Contract must be notified in writing if the shipment of the Contract Items will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the Contract, and/or obtaining the Contract Items from a third party.

Any Agency seeking to obtain the Contract Items from a third party under this provision must first obtain approval of the Purchasing Division.

6.3 **Delivery Payment/Risk of Loss:** Vendor shall deliver the Contract Items F.O.B. destination to the Agency's location.

6.4 **Return of Unacceptable Items:** If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return

REQUEST FOR QUOTATION  
**Network Load Balancer Appliances**

---

within five (5) days of being notified that items are unacceptable, or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. AH returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

- 6.5 **Return Due to Agency Error:** Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

**7. VENDOR DEFAULT:**

7.1 The following shall be considered a vendor default under this Contract.

7.1.1 Failure to provide Contract Items in accordance with the requirements contained herein.

7.1.2 Failure to comply with other specifications and requirements contained herein.

7.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

7.1.4 Failure to remedy deficient performance upon request.

7.2 The following remedies shall be available to Agency upon default.

7.2.1 Immediate cancellation of the Contract.

7.2.2 Immediate cancellation of one or more release orders issued under this Contract.

7.2.3 Any other remedies available in law or equity.



Where Technology  
Means More®

## State of West VA

Network Load Balancer Appliances RFQ

CRFQ 0231 OOT2600000023

March 24, 2026

**Thomas Sartori**

Senior Account Executive

4601 Creekstone Dr, Suite 110

Durham, NC 27706

Phone: 919-389-8622

Email: [thomas.sartori@eplus.com](mailto:thomas.sartori@eplus.com)



March 24, 2026

State of West VA

Thank you for offering ePlus Technology, inc. (“ePlus”) the opportunity to respond to your RFQ for **Network Load Balancer Appliances**. We have reviewed the State of West VA’s stated goals and requirements contained in your RFP. We are confident that our solution provides a proven approach – combining appropriate practices, technology, and intellectual capital to meet and exceed your process improvement and cost savings objectives.

The following response and attachments will clearly demonstrate how ePlus will assist you in achieving your goals. Our proposal contains all the supporting information you should need.

ePlus is submitting its proposal on the understanding and with the expectation that the State of West VA and ePlus Technology, inc. will have the opportunity to work together to enter into a mutually acceptable contract for the products and services described in an agreed upon statement of work.

The experience that ePlus will demonstrate throughout the process will highlight how our strengths and expertise can be applied to your organization to generate positive business results. We look forward to the opportunity in the very near future to personally present our solution.

Thank you for your consideration.

Sincerely,

A handwritten signature in blue ink that reads "Don McLaughlin".

Don McLaughlin  
Senior Vice President



## Table of Contents

---

Executive Summary .....	2
ePlus Company Information .....	3

**Attachments:**

Attachment 1 - ePlus Quote V5-State WV-A10-23468774-20260313

Attachment 2 – A10-DS-Control[28]

Attachment 3 – A10-DS-Thunder-ADC[17]

Attachment 4 – FIPS Spec Sheet

---

### COPYRIGHT AND TRADEMARKS

OneSource, OneSource Procurement, Content+, and Manage+ are the trademarks of ePlus. OneSource, Procurement, Content+, and Manage+ software products are copyrighted and all rights reserved by ePlus. The style and format of this proposal is copyrighted and all rights reserved by ePlus. All other company and product names are the trademarks or registered trademarks of their respective companies.

© 2000 – 2025 ePlus  
13595 Dulles Technology Drive  
Herndon, VA 20171  
703.984.8400  
All rights reserved.

### ePlus as a Reseller

ePlus is fully committed to holding the discount structure contained in our bid response for the life of the contract but is subject to future potential manufacturer changes in overall pricing models to its resellers. ePlus would require the opportunity to amend its committed discount in order to maintain an equivalent level of margin to be able to continue the supply. ePlus will provide the documentation to support manufacturer modification that supports a change any pricing structure. It is possible that changes can also occur in other manufacturer terms such as changes in warranty terms that are outside of ePlus’ control and we reserve the right to modify this schedule from time to time to accommodate these potential changes by providing written notice. If changes of this nature are not something for which you would consider an exception, ePlus would merely require the opportunity to vacate the particular award(s) effected by the manufacturer's changes which are outside of our control.

### PROPOSAL VALIDITY PERIOD

This proposal is valid for sixty (60) days from the date of submission (March 24, 2026).

## Executive Summary

The ePlus Technology team would like to thank the State of West Virginia for the opportunity to propose the A10 Thunder 3350S Network Load Balancer platform.

Purchasing the A10 Networks Load Balancer platform from ePlus will provide the State of West Virginia with high-performance application delivery, robust security, and a predictable cost model.

The proposed solution is designed to provide the State of West Virginia:

- **Superior Performance & Scalability:** Built on the Advanced Core Operating System (ACOS), these devices use a symmetric multi-core processing architecture to deliver massive throughput with ultra-low latency.
- **All-Inclusive Licensing:** A10 includes all software features in the base price, providing a lower Total Cost of Ownership (TCO).
- **Integrated Security:** The solution proposed functions as more than just load balancers by consolidating security features such as a Web Application Firewall (WAF), DDoS protection, and SSL/TLS inspection into a single platform. The A10 Thunder 3350S CFW (Convergent Firewall) with FIPS compliance proposed is a high-performance network security appliance to deliver multiple security functions through that single platform. It is typically purchased by government agencies like the State of West Virginia that require high-speed traffic processing alongside stringent FIPS 140-2 Level 3 data encryption standards.

### Security and Compliance

The primary reason customers like the State of West Virginia select the "FIPS" variant of this model is to satisfy rigorous legal and regulatory requirements for cryptographic security.

- **FIPS 140-2 Level 3 Compliance:** This model includes a Hardware Security Module (HSM) that provides tamper-resistant storage for SSL private keys.
- **Secure SSL/TLS Offload:** It offloads intensive encryption tasks from backend servers while keeping keys within logical and physical cryptographic boundaries.
- **Advanced Firewall Capabilities:** It consolidates a stateful firewall, IPsec VPN, and Secure Web Gateway (SWG) into a single appliance.
- **Ease of Management:** A10 provides a familiar Cisco-like Command Line Interface (CLI) and elegant Web GUI, making it easier for network teams to deploy and manage without extensive retraining.
- **Future-Proofing:** The ACOS (Advanced Core Operating System) architecture is designed for scalability, making it ready for high-demand environments well into the future.

## ePlus Company Information

ePlus is a customer first, services led, results driven and trusted industry leader that helps organizations secure, modernize, optimize, and scale their IT. For more than 30 years, we have stood side by side with over 5,000 customers across the U.S., Europe, and Asia, helping navigate an increasingly complex and dynamic IT, regulatory and workforce environment. Backed by an unparalleled bench of technical experts, more than 7,000 certifications and accreditations, top industry recognition, and a relentless commitment to innovation on behalf of everyone we serve, ePlus drives truly transformational results. We achieve these outcomes via expertise across Artificial Intelligence, Data Center, Cloud, Security, Enterprise and Carrier-Grade Networking and Collaboration, as well as a robust set of professional, managed, consultative and other services. It's equal parts strategy, execution, and results, always with our customers at the core. Each day. Every day. The Company is headquartered at 13595 Dulles Technology Drive, Herndon, VA, 20171, USA. For more information, visit [www.eplus.com](http://www.eplus.com), call 888-482-1122, or email [info@eplus.com](mailto:info@eplus.com).

## Financial Overview

Founded in 1990, ePlus inc. (NASDAQ NQGS: PLUS) is a public company with annual adjusted gross billings of \$3.28B and shareholders equity of \$977.6M as of its most recent fiscal year ending March 31, 2025. Our full financial statements of quarterly and annual audited financials can be viewed at <http://www.eplus.com/investors/financial-reporting/annual-reports> or [www.sec.gov](http://www.sec.gov).

**PLUS**  
Nasdaq Listed

## Locations

### National Headquarters

ePlus Technology, inc.  
13595 Dulles Technology Drive  
Herndon, VA 20171  
Phone: 703-984-8400  
Fax: 703-984-8600  
[www.eplus.com](http://www.eplus.com)  
[List of all ePlus Locations/Offices](#)



## Partnerships and Expertise

Our customers benefit from our deep collaborative partnerships with leading technology providers, enabling us to create solutions that connect the dots between IT investments and business outcomes so technology means more, and does more, for them. ePlus maintains deep partnerships with top manufacturers, including Arista, AWS, Check Point, Cisco, CrowdStrike, Dell Technologies, Digital Realty, Extreme, F5, Fortinet, Gigamon, HP, HPE, Intel, Juniper Networks, Lenovo, Microsoft Azure, NetApp, Nutanix, Nvidia, Palo Alto Networks, Proofpoint, Pure Storage, Rubrik, Schneider Electric, Varonis, Vertiv and Zoom—many who look to us for their own technology needs.



## Commitment to Diversity, Inclusion & Belonging

ePlus is dedicated to fostering, cultivating, and preserving a culture that embraces diversity, enables inclusion, and makes our employees feel comfortable bringing their authentic selves to work. We celebrate the many diverse qualities that make our employees unique—gender, ethnicity, race, sexual orientation, age, ability, veteran status, religion, culture, background, experience, strengths, perspectives and more. We are dedicated to customer and community service, acting with integrity in all things, and putting our ethics into practice.

### ePlus Values:

**Respectful communication and cooperation.** We treat each other with dignity and respect. Always.

**Teamwork and employee participation.** We encourage the representation of all groups and perspectives in our daily interactions, both internally and externally.

**Work/life balance that supports our employees' varying needs.** The health and well-being of our employees is at the core of our success. Our Well and Good wellness program encourages and enables our employees to improve nutrition, fitness, stress, sleep, connection, and fun, and rewards them for their participation and engagement.

**Embracing the communities** in which our employees, our business partners and our customers live and work. Good corporate citizenship is fundamental to who we are as a company, and our global team is committed to making a positive difference in the communities in which we live and work. Our collective efforts include employee giving, corporate matching, and volunteerism to combat homelessness, hunger, and cancer and to increase access to education. Our employees' dedication to making a positive impact in the world is a source of great pride for our company.

At ePlus, we know that our employees are our most valuable asset. The collective sum of our individual differences, life experiences, knowledge, innovation, self-expression, unique capabilities, and talents drives not only our culture, but also our reputation and shared achievements. That is why we apply our diversity, inclusion, and belonging philosophy to all aspects of our business to help us partner with, recruit, retain, and develop the best talent.

**ePlus. Where Technology Means More.®**

## ePlus Awards and Accreditations

### Awards

#### 2025

Broadcom Growth Partner of the Year for VMware  
CRN® 2025 Managed Service Provider 500 Elite 150  
CRN® 2025 Tech Elite 250  
CRN® 2025 Solutions Provider 500  
Digital Realty Rising Star Partner of the Year  
F5 BeF5 Partner of the Year  
Lenovo North American Infrastructure Partner of the Year  
Nutanix Portfolio Partner of the Year  
Pure Storage Innovator Partner of the Year  
Ragan Workplace Wellness Award for Physical Wellness

#### 2024

Cisco Global Mass Scale Infrastructure Partner of the Year  
Cisco Americas Mass Scale Infrastructure Partner of the Year  
Cisco U.S. East Collaboration Partner of the Year  
Cisco U.S. East Software Partner of the Year  
Cisco U.S. Northeast Partner of the Year.  
CRN® 2024 Managed Service Provider 500 Elite 150  
CRN® 2024 Tech Elite 250  
CRN® 2024 Solutions Provider 500  
Cybersecurity Excellence Awards: Cyber Portfolio Management  
F5 North America 2023 Strategic Solutions Partner of the Year  
Juniper Partner of the Year for Cloud-Ready Data Center  
Lenovo U.S. Infrastructure Solutions Partner of the Year z  
Northrup Grumman Supplier Excellence Award  
Varonis Growth Partner of the Year

#### 2023

Cisco Global Customer Experience Partner of the Year  
Cisco WebexOne Reimagine Work Partner of the Year, Americas  
BizLibrary: Best Overall Learning & Development Experience  
CRN® 2023 Managed Service Provider (MSP) 500 Elite 150  
CRN® 2023 Tech Elite 250  
CRN Solutions Provider 500  
NetApp North American Flexpod Partner of the Year  
Pure Storage Fastest Growth Partner of the Year  
Rubrik 2023 Public Sector Partner of the Year  
Rubrik North American Partner Sales Champion of the Year  
Top Workplaces USA 2023  
Veeam Growth Partner of the Year



## Accreditations

- |                         |                                       |
|-------------------------|---------------------------------------|
| AICPA SSAE Type 2 SOC 1 | OneSource Family of Software Products |
| AICPA SSAE Type 2 SOC 1 | Managed Services Center               |
| AICPA SSAE Type 2 SOC 1 | Service Desk                          |
| AICPA SSAE Type 2 SOC 2 | Cloud Hosted Services                 |
| HIPAA and HITECH        | Cloud Hosted Services                 |
| ISO9001 QMS             | Warehouse Operations                  |



## Advanced Authorizations and Staff Certifications

Strategic alliances with the industry’s leading manufacturers keep ePlus engineers and sales professionals at the forefront of technology, enabling them to deliver industry-leading solutions to our clients. With an extensive roster of staff certifications, we also hold the following partnership designations:

### A10 Networks

- + Elite Partner



### Amazon Web Services

- + Advanced Consulting Partner
- + Public Sector Partner
- + Solution Provider Partner
- + Immersion Day Partner
- + AWS Marketplace CPPO Partner
- + Storage Competency
- + Windows on EC2 Delivery Partner



### Cisco: Gold Level Partner (continued)

- + Cisco Webex Calling with Calling Plan
- + Cisco Hyperflex Specialization
- + Cisco IoT Specialization
- + Cisco Webex Contact Center Specialization

### Dell Technologies: Titanium Solution Provider



#### Portfolio and Solution Competencies:

- + Core Client
- + Server
- + Storage
- + Networking
- + Data Protection

### Calix

- + Elite Partner



### Check Point

- + 4 Star Partner
- + ASCP(EMS) Certified
- + Harmony Specialization



### Fortinet



#### Expert Partner Level

- + SD-WAN Specialization
- + Cloud Business Model Certified
- + Integration Business Model Certified

### Ciena

- + Elite Partner



### Harmonic



- + Platinum Partner

### Cisco: Gold Level Partner

#### Master Specializations

- + Master Data Center and Hybrid Cloud Specialization
- + Master Collaboration Specialization
- + Master Networking Specialization
- + Master Security Specialization
- + Master Service Provider Technology Specialization
- + Master Service Provider



### HP Inc. Amplify Partner Program



#### Power Partner

### Hewlett Packard Enterprise Platinum Level Partner



#### Hybrid IT (Server/Storage)

- + HPE Partner Ready: Solution Provider – Platinum Partner
- + HPE Partner Ready: Services Partner – Gold

#### Edge (Aruba/Networking)

- + HPE Partner Ready for Networking: Solution Provider – Platinum Partner
- + Silver Peak Partner Edge Program: Platinum Partner

### Intel

- + Intel Partner Alliance Program: Titanium Partner

#### Advanced Specializations

- + Advanced Collaboration Architecture Specialization
- + Advanced Customer Experience Specialization
- + Advanced Data Center Architecture Specialization
- + Advanced Unified Contact Center Enterprise Specialization
- + Advanced SP Architecture Specialization
- + Advanced Security Architecture Specialization

**Juniper Networks**

Elite Partner



**Microsoft**

Gold Level Partner



- + Cloud Solutions Provider
- + Gold Application Integration
- + Gold Data Center
- + Gold Cloud Platform
- + Gold Cloud Productivity
- + Gold Windows and Devices

**NetApp**

Solution Specializations

- + FlexPod Specialized



Implementation Services Certified

- + E-Series
- + HCI
- + ONTAP

Integration Services Certified

- + E-Series
- + ONTAP
- + ONTAP SAN

NetApp Keystone Sell-with

Professional Services Certified

- + ONTAP SAN

Support Services Certified

**Nokia**

- + Broadband Access Networks Expert
- + Fixed Wireless Access Expert
- + IP Routing
- + Optics



**NUTANIX**

Pioneer Level Partner



**NVIDIA**

Elite Partner

- + Generative Sales AI Advisor
- + Generative Technical AI Advisor
- + DGX Ready Offerings
- + NVIDIA DGX SuperPOD Specialization
- + NVIDIA DGX-Ready Managed Services certification



**Palo Alto**

Diamond Innovator Partner Level  
SASE Specialization Partner



**Pure Storage**

Elite Partner

Service Delivery Partner (Managed Service Provider)



**Rubrik**

Elite Plus Partner Level



**VMware**

Principal Partner

- + Data Center Master Services Competency
- + Networking Master Services Competency
- + VMware Cloud on AWS Master Services Competency
- + Data Center Virtualization
- Transform Networking and Security
- + Empower Digital Workspace
- Cloud Management and Automation
- + Cloud Provider
  - + Cloud Native



**Additional Key Vendors**





## The ePlus Difference: Look Beyond What's Practical to Achieve What's Possible

At ePlus, we believe that the future belongs to those who look beyond what's practical to achieve what's possible. We specialize in helping our customer organizations explore the “what ifs” — and to experience more than they could have envisioned on their own. With ePlus, they can experience more than they expect.

Our top priority is always to make sure that the services and solutions we offer are aligned with what our customers need to succeed. And, as our customers' technology needs, resource constraints and talent needs grow fast and furious, so too does the level of expertise ePlus brings to the table, along with a customized set of services and solutions developed just for them.

ePlus moves beyond merely implementing IT solutions to harnessing technology and driving transformation. We help accelerate and reignite growth, enabling organizations to stay ahead of change, unlock new opportunities, accelerate progress, and achieve more than they ever imagined. Our offerings are comprised of a large portfolio of possibilities — spanning the technology lifecycle — developed to help position customer organizations to tap into unimagined opportunity and potential.

Our customers are at the core of every decision, every investment and every one of our offerings. Our solutions portfolio is designed, and continues to grow, with our customers' desired business outcomes in mind. The ePlus portfolio of solutions and services spans the following:

- **ARTIFICIAL INTELLIGENCE** – Unlock the full potential of AI with guidance at any stage of the journey, from assessing readiness, defining use cases, deciding to build or consume, and ensuing a successful proof of concept to design, implementation, and management.
- **CLOUD & DATA CENTER** – Leverage cloud in transformative ways by modernizing data center infrastructure, extending those capabilities to cloud, accelerating cloud migrations and optimizing cloud platforms (and spend) to meet dynamic and evolving business needs.
- **SECURITY** – Ensure security and reliability by design from end to end with cutting-edge solutions, tools, intelligence and managed services that help diagnose, predict, map, secure and protect every facet of an environment.
- **NETWORKING** – Build a resilient, efficient, agile, defensive and intelligent network capable of supporting modern initiatives. Design and deploy next-generation enterprise and service provider networks to ensure that all domains are supported with high-performing, fault-tolerant, secure, intelligent and application-aware solutions.
- **COLLABORATION** – Empower hybrid work and unleash productivity from anywhere, simply and securely. With full integration into existing business tools and processes, modern collaboration solutions accelerate workplace/workspace transformation, enhance employee and customer experiences and ensure secure interactions with predictable cost models.
- **SERVICES** – Maximize return on IT investments, facilitate implementations and enhance technology performance through our broad portfolio of consultative and managed services. Driven by technical expertise, our award-winning team brings a modular approach to designing, developing, protecting, optimizing and managing the technology that fuels our customers' business at every stage of their lifecycle.
- **FINANCING AND CONSUMPTION MODELS** – Boost investment power by aligning technology and payment solutions to provide cost predictability and easy access to hardware, software and services.



Customer Name: STATE OF WEST VIRGINIA  
 Quote No: 23468774  
 Quote Name: A10  
 Quotation Date: 02/11/2026

Sales Support Contact: Stephanie Sunderman  
 Sales Support Phone: 7039848198  
 Sales Support Email: Stephanie.Sunderman@eplus.com  
 Account Executive: Mark Carretta  
 Account Executive Phone: 4122581697  
 Account Executive Email: mcarretta@eplus.com

Customer PO No:  
 Order No:  
 Expiration Date: 03/31/2026

ePlus Technology inc, 13595 Dulles Technology Drive, Herndon, VA, 20171

Line No.	Part Number	MFG	Description/Line Notes	QTY	Unit Price	Ext Price
001	TH3350S-020-CFW-FIPS	A10 NETWORKS	THUNDER 3350S <b>Line Note:</b> Thunder 3350S CFW, 1U, 1CPU, 6x1GC, 2x1GF, 8x10/1GF, 4x10GF, 64GB, 1SSD, No LOM, No FTA, no S+R ASIC, SSL Built-in + SSL Card, screwless railkit, 2 AC PSU, FIPS Compliant	2	35,680.89	71,361.78
002	GOLD SUPPORT 3 YEAR	A10 NETWORKS	24X7 TECHNICAL SUPPORT ACCESS/ADVANCED HARDWARE REPLACEMENT - 3 YEARS	2	35,329.61	70,659.22
003	AXSK-SFP+ SR	A10 NETWORKS	10 GIG SFP+ FIBER TRANSCEIVER - SHORT RANGE	9	668.60	6,017.40
004	TRAINING-CREDIT	A10 NETWORKS	TRAINING CREDITS ARE REDEEMABLE FOR A10 NETWORKS <b>Line Note:</b> Training Credits are redeemable for A10 Networks training items for up to 12 months by any employee of the organization. For a full list of training policies and class schedule, refer to A10's training website.	40	104.47	4,178.80
005	TH3350S-020-CFW-FIPS	A10 NETWORKS	THUNDER 3350S CFW, 1U, 1CPU, 6X1GC, 2X1GF, 8X10/1G F, 4X10GF, 64GB, 1SSD, NO LOM, NO FTA, NO S+R ASIC, SSL BUILT-IN + SSL	1	35,680.89	35,680.89
006	BASIC SUPPORT 3 YEAR	A10 NETWORKS	9 AM - 6 PM M-F TECHNICAL SUPPORT ACCESS/HARDWARE REPAIR - 3 YEARS	1	37,465.92	37,465.92
<b>Sub-Total (USD)</b>						<b>225,364.01</b>
<b>4YR</b>						
007	BASIC SUPPORT 1 YEAR	A10 NETWORKS	HW, FIRMWARE 8X5 M-F TECH SUPPORT FOR AX1000 - BASIC SUPPORT	1	13,267.60	13,267.60
008	GOLD SUPPORT 1 YEAR	A10 NETWORKS	GOLD SUPPORT 1 YEAR	2	14,653.01	29,306.02
<b>Sub-Total (USD)</b>						<b>42,573.62</b>
<b>5YR</b>						
009	BASIC SUPPORT 1 YEAR	A10 NETWORKS	HW, FIRMWARE 8X5 M-F TECH SUPPORT FOR AX1000 - BASIC SUPPORT	1	14,048.04	14,048.04
010	GOLD SUPPORT 1 YEAR	A10 NETWORKS	GOLD SUPPORT 1 YEAR	2	15,656.65	31,313.30
<b>Sub-Total (USD)</b>						<b>45,361.34</b>
<b>Totals</b>						<b>313,298.97</b>

<b>Shipping:</b>	<b>Sub Total (USD): 313,298.97</b>	
<b>Packing:</b>		<b>Est. Tax (USD): TBD if Applicable</b>
		<b>Shp&amp;Hnd (USD): 0.00</b>
		<b>Total (USD): 313,298.97</b>

All orders are governed by your organization's signed agreement with ePlus or applicable public sector contract; if there is no such agreement the Customer Terms and Conditions for Products and/or Services located at [www.ePlus.com](http://www.ePlus.com) govern. No additional or contrary terms in a purchase order shall apply, and ePlus' performance shall not be deemed acceptance of any preprinted PO terms. Use of software, subscription services or other products resold by ePlus is subject to manufacturer/publisher end user agreements or subscription terms. Any periodic payment obligations for specific offerings, along with customer-incurred overages, consumption fees, add-ons, quantity adjustments and automatic renewals are non-cancelable for any reason except by public sector customers required by law to terminate due to non-appropriation of funds.

PLEASE NOTE: Recent supply chain disruption and tariffs on certain imports are causing price increases for many IT products, with little or no notice, and beyond ePlus' control. As a result, this quote is subject to change without notice, even before the expiration date reflected above. Related manufacturer policy changes may result in orders being non-cancelable and products non-returnable except in accordance with the manufacturer warranty. Please confirm pricing and other restrictions prior to order placement. Unless freight amount is indicated, or is zero, freight will be added to the invoice. Unless Bill-To company is exempt from Sales Tax, it will be added to the invoice. Recognizing that the global pandemic has disrupted operations for many organizations, ePlus will ship products for delivery in accordance with customer's written ship-to instructions and products will be deemed delivered notwithstanding any failure of customer personnel to sign for receipt due to facility closing or otherwise. Supply chain disruption and tariffs on certain imports in accordance with applicable law may cause price increases for many IT products, with little or no notice, and beyond [SELLER'S] control. When such increases occur, this quote is subject to change without notice, even before the expiration date reflected above.

ePlus offers flexible and easy leasing options for your IT equipment. Use leasing to increase your IT acquisition capability, overcome limited budgets, and manage the lifecycle of your assets. Contact an ePlus Leasing Coordinator at 1-703-984-8021 or [leasing@eplus.com](mailto:leasing@eplus.com) to receive a lease quote today.

<b>Customer Acceptance</b> Signature: _____ Name: _____ Title: _____ Date: _____ Customer PO #: _____	<b>Bill To</b> STATE OF WEST VIRGINIA 1900 KANAWHA BLVD E BLDG 1  CHARLESTON WV 25305 UNITED STATES GALE GIVEN	<b>Ship To</b> STATE OF WEST VIRGINIA   UNITED STATES
--	--	---

## A10 Control

Unified Management, Control and Analytics Platform for Agile Operations and Automation

A centralized management and analytics platform providing full control of your A10 solutions, regardless of whether the solution is deployed on-premises, in the cloud, or in a hybrid environment.

### Agile Management and Intelligent Analytics

The increasing complexity of modern network and security infrastructure, coupled with the rapid adoption of AI and cloud technologies, presents significant challenges for organizations to manage and support their mission-critical services and businesses.

It's a complex and a time-consuming task to understand network infrastructure resources and track service status when its deployment is spread across various geographical locations and multiple clouds. Precise capacity planning and prompt response to scaling demand are critical for AI-powered apps and application services infrastructure as they require higher traffic and transaction volume and are very sensitive to latency. Therefore, administrators should leverage agile management and intelligent analytics to establish efficient operation and management workflow.

A10 Control is the next generation of the management and analytics platform for A10 solutions, consolidating existing A10 Harmony Controller and aGalaxy capabilities. A10 Control provides centralized management for A10 security and infrastructure solutions including application delivery, DNS, CGNAT, SSL Insight, Gi-firewall and DDoS protection deployed in any network or cloud environment. A centralized platform helps collect, analyze and report on application and service traffic flowing through A10 appliances and visualize the service and security posture with intelligent analytics.

#### Platforms



Software/VM

#### Related Products & Services



ADC



A10 Defend  
DDoS Protection



CFW



CGN



SSLi

# Benefits



## Gain

Real-time Intelligent Analytics and Observability

Organizations must guarantee their services are up and running constantly. Thus, understanding the services' condition and gaining observability are critical tasks for their operation teams. A10 Control collects metrics data and transaction logs of the service traffic flowing through A10 devices running A10's Advanced Core Operating System (ACOS) and provides deep visibility into what's happening in the service and network infrastructure. Intelligent analytics and customizable alerts help identify potential issues before they impact end-users and enable proactive troubleshooting via access to contextualized traffic data and logs.



## Increase

Operational Efficiency

Organizations can improve their operation team's agility and efficiency by streamlining the workflow and automating processes. Device lifecycle management including backups, health checks, software upgrade, inventory and license management can be troublesome and time-consuming tasks. A10 Control's intelligent automation and tools enable efficient operation for managing a large number of appliances and services deployed over various underlying infrastructures – from data centers to any clouds.

Comprehensive APIs enable easy integration with popular DevOps, infrastructure-as-code and observability tool chains, and major public and private clouds infrastructure.



## Simplify

Management for Services and Security

One management platform for any A10 solutions; One of A10's unique technical advantages is that all A10 solutions are running on a common OS (ACOS) regardless of platform or form factor. Now, A10 Control is the only management platform administrator needs as consolidating capabilities of A10 Harmony Controller and aGalaxy.

With A10 Control, streamline your IT operations and improve uptime of your services using rich intelligent analytics and embedded automation workflow tools.

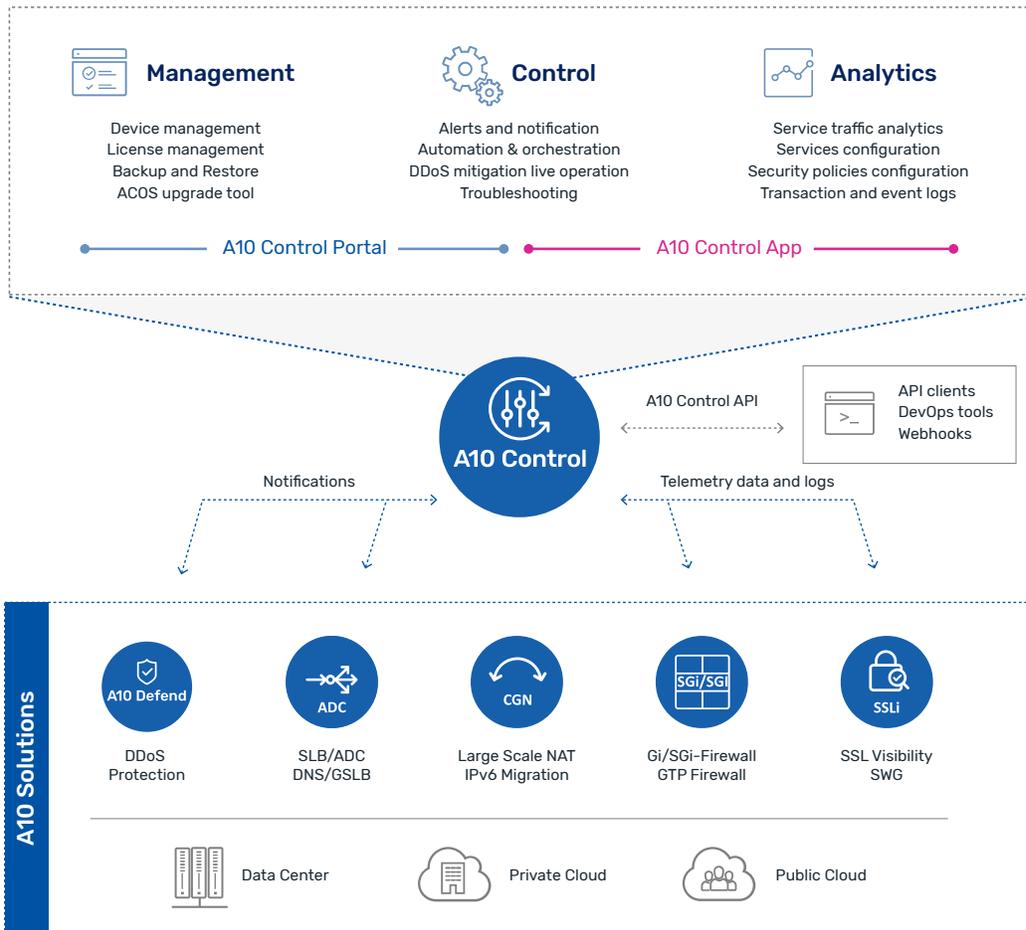


Figure 1. A10 Control is a centralized management and operations platform for A10 infrastructure services and security solutions.

# Features

## Centralized Management



### Device Lifecycle Management

Centralized device lifecycle management for A10 hardware or virtual appliances including public, private cloud, and bare metal. Intuitive inventory and license management for multiple A10 Thunder and A10 Defend DDoS appliances. Automate routine tasks such as backup, inventory reports and schedule automated software upgrades.



### Device Analytics

Detailed device-level analytics are available for A10 devices deployed across various network and cloud environments in different geographic locations. A device health monitor and dashboard provide system resource utilization, device location, traffic and connection metrics, transaction logs and event information.



### Alert and Reporting

Metrics and logs collected from A10 devices are correlated and evaluated against user-defined rules for raising alerts against abnormal events. These alerts are delivered as email notifications and/or via webhook for automated action using collaboration tools such as Slack and Microsoft Teams.

## Service Operations



### Service and Policy Management

Make configuration changes and enforce security policy updates using shared resources such as class-list or IP list for A10 devices deployed across different geographical locations from a central console.



### Multi-tenancy

With a flexible multi-tenancy architecture and role-based access control, each application team and service owner can have their own tenant workspace called organization-unit to manage their services and operations. Tenant allocation is as flexible as having multiple A10 device clusters in a tenant or as granular as assigning a tenant for each L3V/ADP partition of an A10 device.



### API-driven Automation and Integration

Comprehensive A10 Control APIs allow easy integration using DevOps tool chains like Ansible, Chef, Jenkins to automate A10 device configuration management via A10 Control, and to streamline monitoring and operation workflow for the A10 solutions being managed.

## Architecture and System



### Reliable Controller Platform

A10 Control is built upon a solid RHEL foundation with a microservices architecture using Kubernetes, which maximizes the availability of the controller and ensures full regulatory compliance, meeting the latest industry standard. The controller collects and processes various kinds of telemetry data from A10 devices in a secure manner, and never handles service traffic running through data plane of A10 devices. The architecture ensures that service traffic disruption never happens even if the connection between the controller and A10 devices is down.



### Improved Security and Maintainability

A10 has years of expertise in using a microservices architecture in A10 product lines including Harmony Controller. A10 Control has been designed to use with the latest and greatest RHEL software and a next-generation architecture. This has enhanced security and maintainability of the system especially for security and CVE patches.



### Deployment Options

The controller can be installed as a self-managed software solution in single node or multi-node high availability (HA) deployment within a customer's environment. In HA, microservices as well as the data-store of the controller are distributed across nodes.

For details of system requirements and prerequisites for the A10 Control installation, refer to the latest product documentation or contact A10 sales representative.



### Re-architected for Stability and Performance

A10 Control has upgraded versions of all components, frameworks and technologies used in building of the product to boost stability and performance. A10 Control uses a different database system than Harmony Controller for simplified and low-latency data operations and a new and standards-based technology for user authentication management.

# A10 Control Apps

Solution-based comprehensive analytics, configuration and service operation tools are all built into A10 Control as an app.

## Application Deliver Controller (ADC) App

Provides centralized configuration tool and visibility for single or multi-site ADC and DNS deployment. Rich analytics and contextualized logs help gain great insights into app and traffic, and simplify troubleshooting workflow when needed.

## A10 Defend Orchestrator (ADO) App

Previously known as aGalaxy is now available as the ADO app. Provides centralized protection configuration and real-time monitor for DDoS Detector and Mitigator. In case of DDoS incidents, orchestrates actions help streamline workflow with a live mitigation console.

## Carrier Grade NAT (CGN) App

Provides CGNAT technologies configuration tool, management and deep insight into subscribers traffic and NAT pool utilization. Rich service analytics including user session logs increase operational efficiency and help future planning.

## SSL Insight (SSLi) App

Provides wizard-based configuration, guided troubleshooting tool and comprehensive observability into TLS/SSL encrypted traffic for SSL insight or secure web gateway deployment.

## Gi/SGi Firewall (Gi-FW) App

Provides detailed insights into user traffic going through the CFW-CGN device, including firewall rule-based analytics, CGNAT analytics and app category based classification.

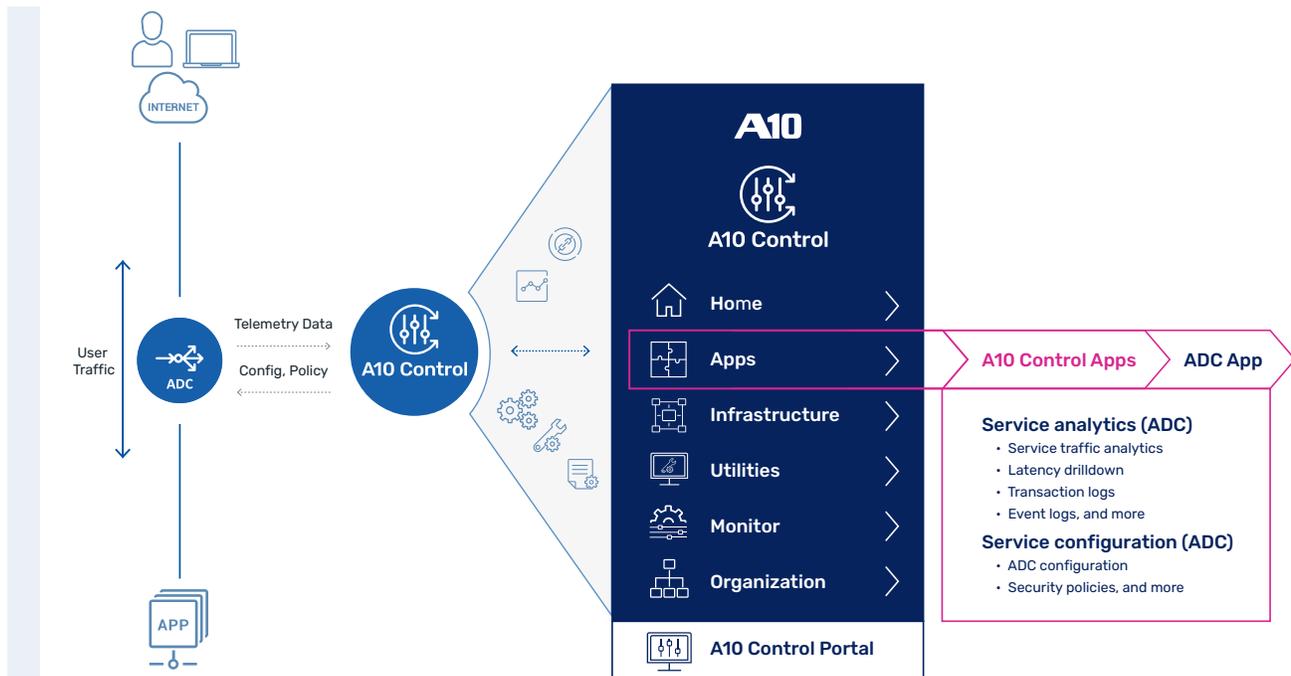


Figure 2. A10 Control collects telemetry from A10 device via control plane and provides analytics and control using a service specific A10 Control App.

# Use Cases

## Supported A10 Solutions

### Application Delivery

High-performance advanced load balancing solution that enables applications to be highly available, accelerated and secure. Deploy with A10 Thunder ADCs or Thunder CFW-ADCs in any form factor including hardware, hypervisor-based software, bare metal, container or in hybrid and multi-cloud environments.

### CGNAT and Gi/SGi-Firewall

Deploy A10 Thunder CGNs for highly scalable and efficient NAT solution that allows service providers and enterprises to extend IPv4 connectivity while enabling smooth transition to IPv6 infrastructure. With A10 Thunder CFW-CGN, it enables consolidation of network function such as CGNAT, Gi/SGi firewall and app visibility, supporting efficient Gi-LAN and mobile core security.

### DNS

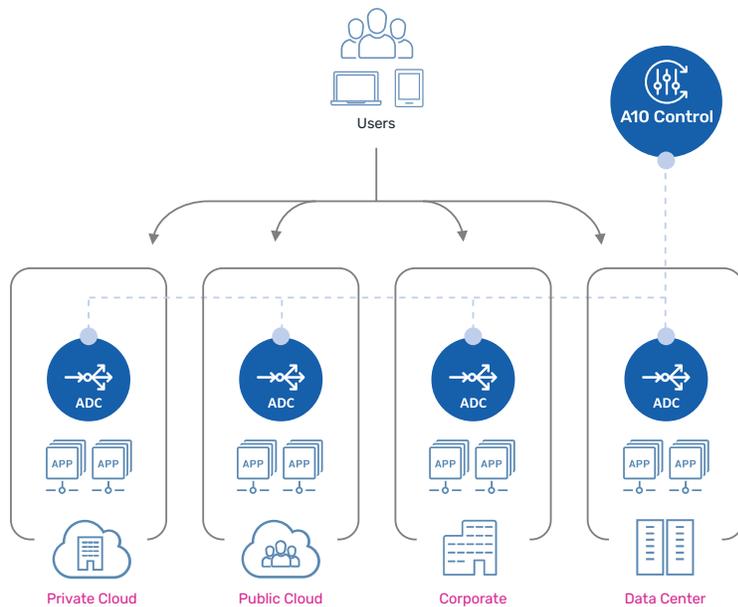
Scalable and secure DNS load balancing and cache solution that makes DNS infrastructure more resilient and efficient. Deploy with A10 Thunder ADCs or Thunder CFW-ADCs in any form factor and environment.

### DDoS Protection

Holistic DDoS defense solution that is scalable, economical, precise, and intelligent to help organizations ensure extended service uptime. Deploy with A10 Defend DDoS Detector and Mitigator.

### SSL Insight

Comprehensive TLS/SSL decryption solution enabling security devices to analyze encrypted enterprise traffic, that can further augment security posture with integrated secure web gateway features. Deploy with A10 Thunder CFW-ADC in any form factor.



### Multi-cloud application delivery deployment

A10 Control can centralize the management and control for application delivery services deployed in hybrid or multi-cloud environment, providing

- ADC analytics
- ADC and security policy enforcement
- ADC device & configuration management, and more.

Figure 3: Multi-cloud ADC use case.

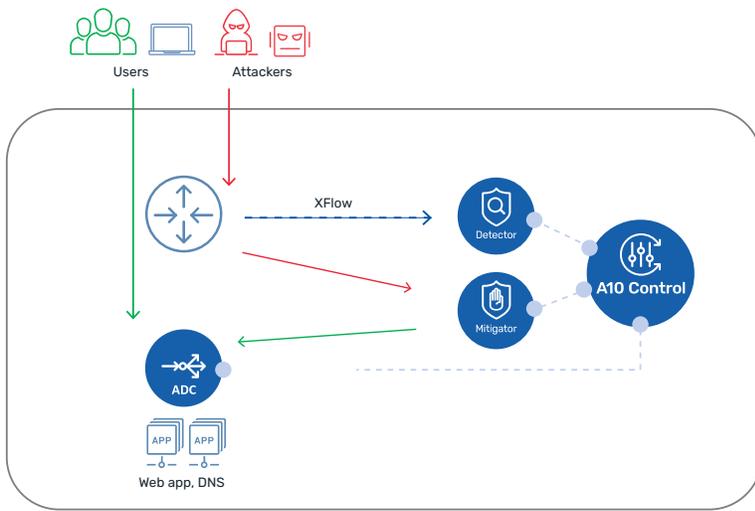


Figure 4: DDoS protection use case.

## DDoS protection for web apps and DNS

A10 Defend DDoS Orchestrator (ADO) running on A10 Control, working together with Mitigator and Detector, enables intelligent automated protection against modern DDoS attack targeting application services and/or network infrastructure.

ADO app provides:

- DDoS defense orchestration and automation
- DDoS mitigation console
- DDoS defense policy configuration
- Incident reports, and more

If A10 ADC is used for application services, it can also be managed and control by the same A10 Control.

# Detailed Features List

## A10 Control Portal

Device Management	
Inventory list	Complete device inventory is available in multiple forms like individual device view and cluster view (single node, VRRP-a pair etc.), providing general system information.
Device management and analytics	Detailed cluster and device-level analytics are available for A10 devices, including system and network information, and analytics for system resource usage and traffic statistics.
Device backup and restore	A10 device's configuration can be backed up periodically and stored in A10 Control. The backup can be used to restore the device as needed.
ACOS image upgrade	Image upgrade utility provides an intuitive and reliable ACOS image upgrade process for registered A10 devices with both manual and scheduled methods. All the upgrade operation logs and records are available in the history view.
Monitoring and Alerts	
Service-level health monitor and alerts	Service traffic and conditions can be monitored with custom trigger rules using a broad range of service-level metrics and thresholds. Alerts can be sent via email and webhook for easier integration with existing monitoring systems.
Device-level health monitor and alerts	Granular device-level trigger rules can be set based on infrastructure/device resource usage, device-level traffic-based thresholds, and system logs. Alerts can be sent via email and webhook for easier integration with existing monitoring systems.
Reporting	Tenant-level inventory report and per-service operation reports are available and can be scheduled for a specific duration. Reports can be downloaded in PDF or sent via email and webhook/ HTTP POST.
Event and audit logs	Event viewer provides consolidated system and service event logs from all registered A10 devices. Audit viewer provides access to audit logs from the A10 Controller, and all registered Thunder and license management activity logs. Granular log filters are available, and logs can be downloaded in CVS format.
Administration and Utilities	
Multi-tenancy management	Multi-tenancy is available with granular role-based access for application teams and service owners. Each tenant (organization-unit) can be mapped with A10 device's partition (ADP/L3V) level.
CLI command utilities	Single or a batch of CLI commands can be remotely executed on multiple device partitions simultaneously.
Shared configuration resource tool	Common configuration resources/templates such as class-list, black/white-list, SLB templates, security templates, TLS/SSL certificates can be created as a shared resource and used across any registered A10 devices regardless of service types.
License management	A10 Control works as an enterprise license manager and can manage and control FlexPool capacity licenses for registered A10 devices.
User management	Flexible user management is available with role-based access control. For example, access areas can be set with organization, tenant, device or specific service/partition, and the permission level can be administrator, operator or custom rule with specific operations.
Authentication management	Besides local authentication, identity provider (IdP) such as Azure or Okta or LDAP can be selected for external authentication and single-sign-on (SSO).

# A10 Control Apps

## Application Delivery

ADC analytics (per virtual service)

- Real-time ADC service-level KPIs including traffic info, error rate and latency
- User traffic-based analytics, including user insights (location, browser), top-k, request insights, time-series latency and more.
- Geolocation-based traffic analysis for latency and volume
- ADC service analytics for common protocols (HTTP/S, SSL and HTTP2)
- ADC cluster analytics for resource usage insight
- Application service analytics for detailed app service conditions and trends
- App server analytics for server health and status
- Latency drilldown and analytics for end-to-end latency and a full request-response cycle

ADC transaction log viewer, providing client, request and response data and latency information

Event and alert log viewer

Centralized ADC configuration tool

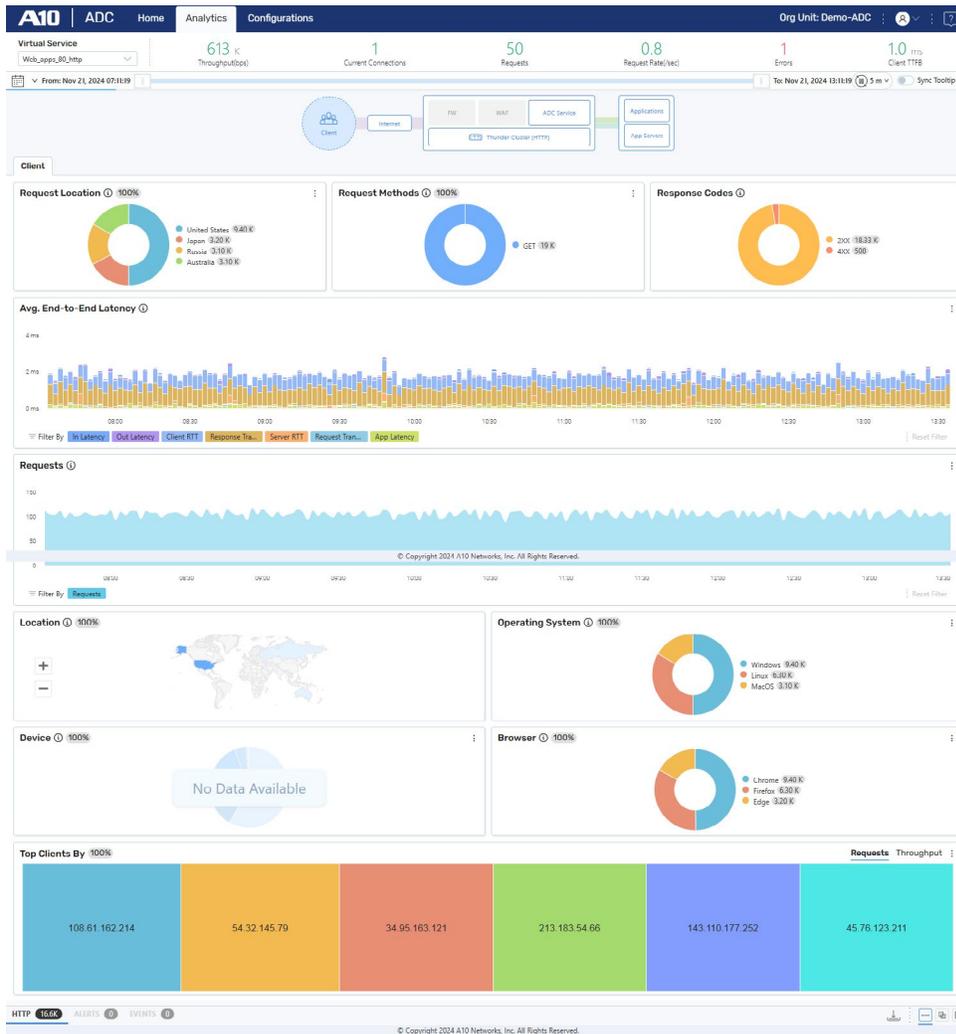


Figure 5. ADC App: ADC analytics for client-based insights.

**Defend Orchestrator**

ADC transaction log viewer, providing client, request and response data and latency information

- DDoS protection workflow orchestration
- Enable seamless communication between Detectors and Mitigators
  - Control and relay DDoS signaling for automated defense operation
  - Send traffic diversion notifications for scrubbing in reactive deployments
  - Manual or automated mitigation actions
  - Automatic DDoS incident reporting after the attack is over

Overview dashboard for DDoS incident and activities

Real-time traffic charts and stats under monitored zone

DDoS mitigation console for live defense operation and monitoring

On-demand and scheduled reports for DDoS incidents, protected zones, device inventory, etc.

On-demand or automated packet capture tool

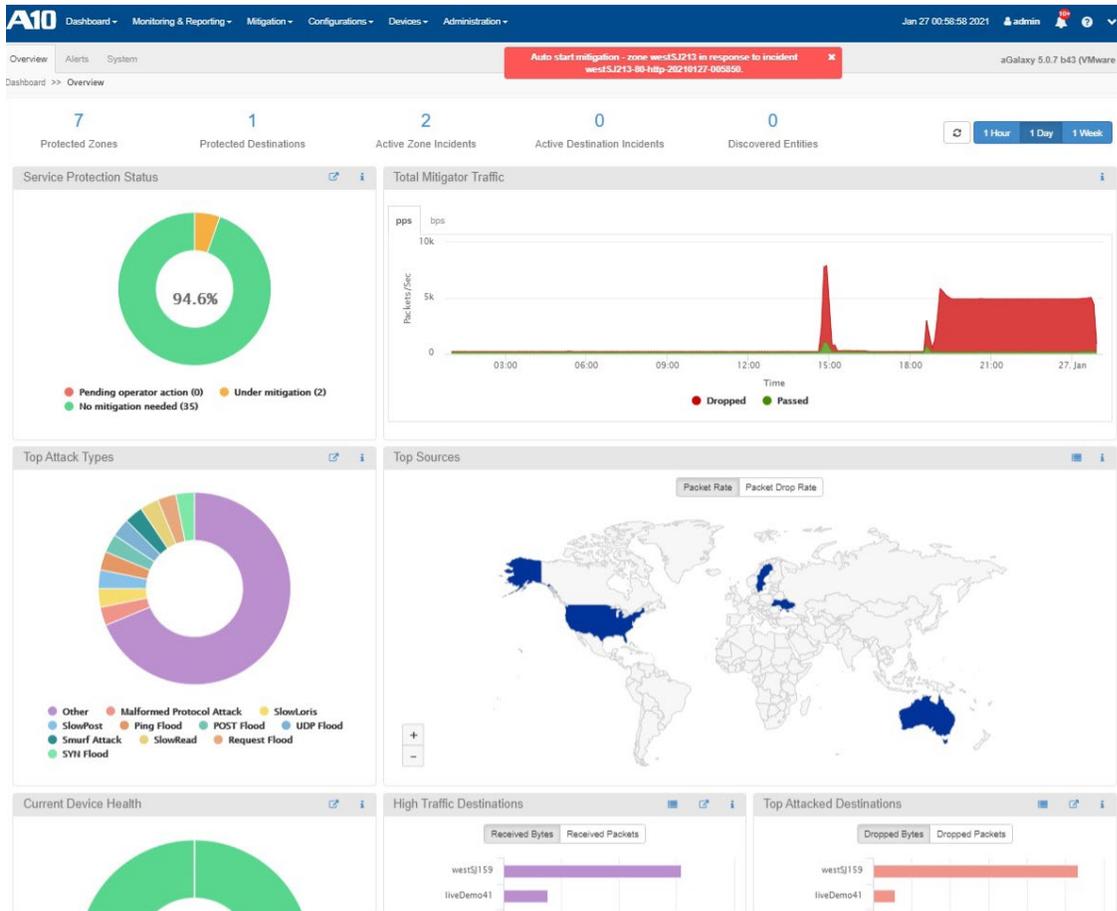


Figure 6. A10 Defend Orchestrator dashboard provides real-time attack statistics and summaries of DDoS incidents.

# Thunder ADC

## Application Delivery Controller and Advanced Load Balancer

Offering a complete application solution, A10 Thunder® Application Delivery Controller (ADC) protects critical applications, ensures server availability and accelerates content delivery. It masters multi-cloud and hybrid cloud deployments with a holistic approach that reduces complexity and cost for IT operations, providing better business outcomes.

### Secure and Agile Application Delivery

From SMBs and large enterprises to service providers and cloud operators, organizations are managing a large and rapidly growing set of mission-critical applications.

A purpose-built solution, A10 Thunder ADC ensures these applications are secure, highly available, and accelerated. It helps ensure business continuity, reduce downtime and build highly available applications across global data centers and/or multiple clouds.

Thunder ADC delivers the capacity, scalability, multi-tenancy and programmability to adjust to an ever-changing environment. Consolidate point products, reduce network complexity and achieve a substantial reduction in TCO.

Thunder ADC is an advanced L4-7 load balancer that delivers multiple layers of security via web and DNS app firewalls, single sign-on (SSO) authentication and in-depth support for advanced encryption including high-performance PFS/ECC. Built upon A10's Advanced Core Operating System (ACOS®) platform, Thunder ADC delivers application security and performance for any environment.

### Platforms



Cloud



Container



Virtual Appliance



Bare Metal



Physical and SPE Appliances

### Related Products



A10 Control  
Centralized Analytics  
and Management



FlexPool  
Capacity Pooling License

# Benefits



## Enhance Application Availability

Organizations must guarantee their applications are constantly accessible. Thunder ADC utilizes multiple load balancing techniques to efficiently distribute workloads across all servers while constantly evaluating application health. Client requests are forwarded to servers that host the proper content and can best respond to ensure secure application and content delivery.



## Ensure Business Continuity

With data centers proliferating worldwide, administrators must maintain around-the-clock global operational integrity. To guarantee cohesion and optimize app delivery among diverse sites or clouds, Thunder ADC includes advanced global server load balancing (GSLB) working with other application delivery features. GSLB expands functionality across global data centers for high availability, fault tolerance, and the best user experience.



## Accelerate Content Delivery

Applications must be responsive – no matter the location – to ensure a superior end-user experience, enhance remote employee productivity and exceed SLA mandates. Thunder ADC overcomes the inherent WAN latencies, inefficient software programs and chatty protocols to provide fast and responsive service. End users receive a superior user experience while organizations gain a competitive advantage.



## Protect Critical Applications

Software development and testing can catch most, but typically not all, coding flaws. The resulting applications are susceptible to attacks that cannot be blocked by intrusion prevention systems (IPS), next-generation firewalls or sandboxing. Businesses lose revenue, suffer damaged brand reputation and loss of confidential data. Thunder ADC provides protection against 'zero day' and other emerging application layer threats with DNS and next-generation web application firewalls.



## Secure Communications

Internet sessions are rapidly adopting encryption to secure online data transport. Clients and servers, meanwhile, negotiate the most secure and complex methods mutually supported. Thunder ADC front-ends servers and offloads cumbersome, processing-intensive tasks associated with the latest cryptographic standards. This maximizes content protection, speeds delivery and lowers infrastructure expenses.



## Consolidate Access Control

Organizations must allow external clients access to web portals, internal resources and mobile/BYOD apps. At the same time, security must be maintained with authentication and be transparent to the user.

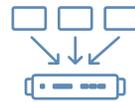
Thunder ADC centrally manages multiple facets of authentication, authorization and accounting (AAA) with a system-wide perspective, while eliminating separate authentication points, for a true single sign-on (SSO) experience.

# Benefits (cont.)



## Hybrid-cloud Operational Efficiency

In a multi-cloud, or hybrid cloud environment, it's essential for IT operations to have a standardized ADC and service visibility from a business and OPEX planning perspective. Thunder ADC can be deployed in a virtual and container environment with flexible and portable licensing, yet deliver feature parity regardless of the form factor. A10 Control, a centralized analytics and management platform, enables effective operation by providing deeper secure application service analytics, easy troubleshooting tools and centralized policy enforcement control.



## Optimize Applications via Multi-Tenancy

To optimize the delivery and security for potentially hundreds of apps in a given data center, IT administrators need a multi-tenant methodology.

Thunder ADC provides the ability to granularly program over 250 individual partitions on a single appliance for tailor-made policies by application, service, or user, while consolidating appliances.

## Thunder 7655S ADC by the Numbers

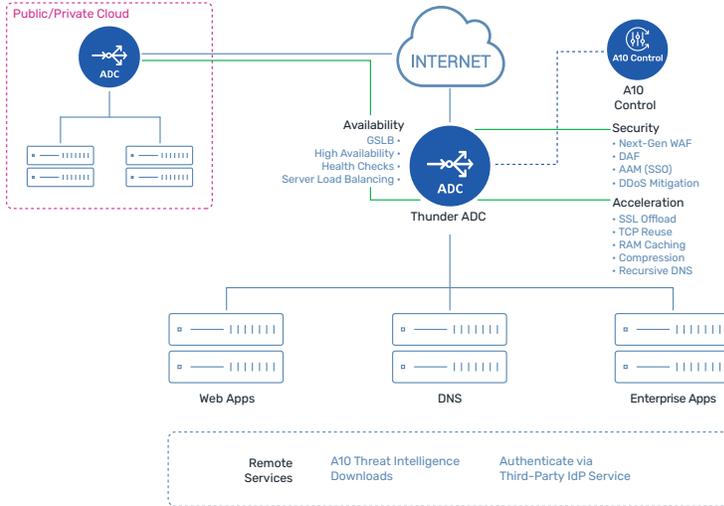


<b>370/340 Gbps</b> L4/L7 Application Throughput	<b>100</b> GE Interfaces	<b>12M</b> L4 Connections Per Second
<b>768M</b> Concurrent Sessions	<b>145 Gbps</b> SSL Bulk Throughput	

### Industry-leading Performance

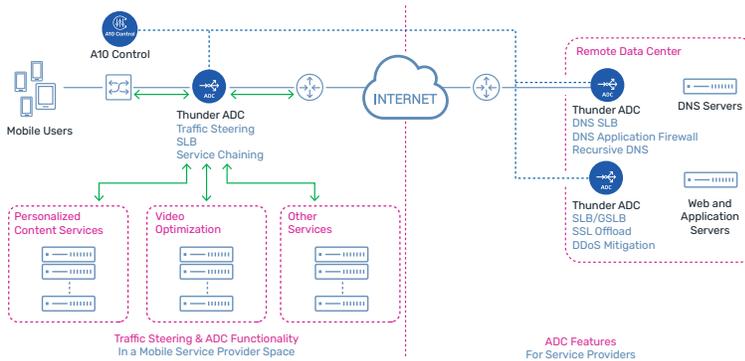
Thunder ADC delivers industry-leading performance – 370 Gbps of application throughput and 145 Gbps of TLS/SSL bulk throughput – in a single 1.5U appliance, rich ADC features (all-inclusive) in the broadest range of form factors, including physical, virtual, bare metal, containers for multi-tenancy and cloud.

# Reference Architectures



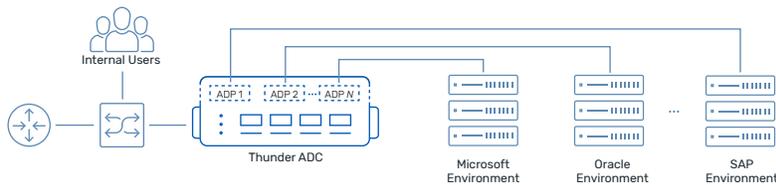
## Enterprise Deployment

Offering industry-leading performance – up to 370 Gbps in a single hardware and 100 Gbps in a virtual appliance, Thunder ADC may be deployed at the core of an environment to deliver high-performance application delivery, load balancing and security. In multi-cloud environments, Thunder ADC can be deployed in any private or public cloud in a virtual or container form factor, with consistent features across clouds.



## Service Provider Deployment

Proven in large-scale service provider environments, Thunder ADC may be deployed to optimize network efficiency and services via traffic steering and service chaining to multiple value-added services, such as video optimization. The solution includes carrier-grade networking (CGN) support for IPv4 address expansion and IPv6 migration.

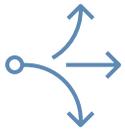


## Application Delivery Partitions

A10 Thunder ADC supports multi-tenant environments with application delivery partitions (ADP). Configure good number of ADC tenant partitions on a single appliance that also enables Layer 3 virtualization. Each partition may be configured for a unique set of policies and offers sufficient resource isolation for most application-oriented use cases.

# Features

## Application Delivery and Performance



### Advanced Server Load Balancing

Thunder ADC is a full-proxy, load-balancing and content-switching solution. With aFlex<sup>®</sup> scripting, deep packet inspection, comprehensive load-balancing algorithms and persistence support, Thunder ADC enables application layer visibility to optimally route inbound requests.

Customizable server health checks ensure only fully functional servers are used to service client needs. The server best able to respond is selected and total servers required can be substantially reduced for lower TCO.



### Broad Acceleration Methodologies

Leverage numerous techniques to overcome inherent distance-related latency, inefficient internet protocols and application design limitations. Acceleration methods, including TCP connection multiplexing, RAM caching, GZIP compression and SSL-offload, expedite content transfer. The solution supports TCP optimization standards such as selective acknowledgment, client keep-alive and window scaling, to further speed delivery.



### Ultra-low Latency For Financial Applications

The Thunder ADC family also offers solutions for low latency applications, featuring specialized Thunder appliances with custom software, to meet the low latency and jitter requirements of financial applications. Featuring ultra-low latency hardware, these appliances offer near instantaneous execution times and provide granular program policies for efficient packet forwarding, while also consolidating multiple network functions, thus reducing hops.



### Global Server Load Balancing (GSLB)

Extend load balancing on a global basis. Thunder ADCs, distributed worldwide, continuously update each other on their respective individual nodes for optimal site selection and status to ensure disaster recovery.

Geographic and network proximity policy metrics optimize multi-site deployments. DNS proxy or DNS server methods further improve implementation flexibility and deployment simplicity.



### High Density Application Delivery Partitions

Provide support for multi-tenant environments with application delivery partitions (ADP). They allow the configuration of 250 or more partitions on a single Thunder ADC appliance, which enables Layer 3 virtualization. Each partition may be configured for a unique set of policies and offers resource isolation for most application-oriented use cases.



### Recursive DNS For Consolidation

Thunder ADC provides powerful recursive DNS capability enabling a one-stop DNS solution that leverages the high performance of ACOS DNS cache service, the scalability of DNS load balancing and the security of DNS application firewall (DAF). This makes the ADC recursive DNS feature a perfect solution for any enterprise or service provider seeking to consolidate DNS services and drive higher customer satisfaction.

## Application Security



### Zero-day Application Protection

A10 Next-Gen WAF, powered by Fastly, leverages advanced technology to protect web applications from complex modern threats while minimizing false positives and ensuring availability. It offers exceptional baseline protection requiring minimal or no tuning and comprehensive attack coverage beyond OWASP Top 10, ATO, and CVEs. By using a threshold-based approach, complemented by intelligent smart parse technology, A10 Next-Gen WAF accomplishes highly effective automated detection and blocking.

The solution offers superior protection and performance compared to any other integrated web application firewall/application delivery controller solution while reducing TCO.



### Powerful DNS LB and Firewall

Thunder ADC enables scalable DNS services by load-balancing multiple DNS servers and with cache DNS capabilities, while supporting recursive DNS lookup. To secure DNS services, the ADC incorporates a sophisticated DNS application firewall (DAF), DNS RPZ and integrated DDoS protection to filter unwanted and malformed requests, stop buffer overflows and head off DNS amplification-based DDoS attacks. It delivers validated DNSSEC pass-through support to prevent threats such as DNS cache-poisoning and spoofing.



### Extensive Cipher Suite Support

Hardware-based SSL offload engines support advanced cryptographic methods at ultra-high capacity. Thunder ADC can manage session security, such as perfect forward secrecy (PFS), with an advanced cipher suite, including elliptic curve cryptography (ECC).

Appliances can process TLS/SSL encryption and decryption at rates 145 Gbps—and up to 140,000 connections per second—when using ECC with 256-bit keys.



### SSO and Application Authentication

The integrated application access management (AAM) module optimizes and enforces authentication and authorization to applications.

The module integrates with authentication servers, identity data stores, identity providers (IdPs) and applications to authenticate users and enforce access privileges. Common AAA and single sign-on (SSO) methods include LDAP, RADIUS, RSA SecurID, TDS SQL, SAML and Kerberos.

AAM interfaces to OCSP responders to validate client certificate status, as well as to Microsoft Active Directory for SharePoint and Outlook Web Access users.

## Application Security (cont.)



### DDoS Protection for App Services

DDoS protection is standard in all Thunder ADC appliances. With FTA-based hardware models, using field-programmable gate arrays (FPGA), protection may be enabled for high-volume attacks against application servers. FPGAs mitigate common volumetric attacks, while general-purpose CPUs mitigate more sophisticated low-and-slow and application attacks, such as Slowloris and HTTP floods. Additional methods to limit unwarranted data floods include connection rate limiting and bandwidth rate limiting per source IP.



### Threat Intelligence Service

An optional subscription, the A10 Threat Intelligence Service provides data from more than three-dozen security sources, including DShield and Shadowserver. The service enables Thunder ADC to instantly recognize and block traffic to and from known malicious IP address sources. The service protects networks from future threats, blocks threats such as spam and phishing, and greatly increases Thunder ADC efficiency.



Next-Gen WAF, Powered by Fastly is PCI DSS compliant as a Level 1 service provider and fulfills PCI requirement 6.6

## Application Visibility and Management



### Analytics

#### Visibility and Logging

When deployed in conjunction with the A10 Control, Thunder ADC provides access to dozens of aggregate and per-request metrics in real time. These include end-to-end response times, latency, popular URLs, and error and health indicators. The data is analyzed to provide per-app reporting and alerts on availability, security and performance.

Detailed Layer 4 based analytics information is separately provided by individual clients, ADC (single appliance or as a cluster) and per server.



### DevOps

#### Automation

Recognizing the need for effective operation for multi-cloud deployment, Thunder ADC has tight integration with many automation, cloud orchestration and DevOps tools.

- Supports various cloud platform and technologies including OpenStack, OpenShift, Kubernetes and more.
- Provides native integration with Infrastructure as Code (IaC) for provisioning and configuration automation, such as Terraform and Ansible.
- Automates network operation with dynamic ADC configuration update using Thunder Kubernetes Connector (TKC), HashiCorp Consul and network infrastructure automation (NIA).
- Monitors application network with common open-source tools such as Prometheus, Grafana and Fluentd.
- Provides quick and easy deployment using resource manager template in public cloud, including Azure Resource Manager (ARM) and AWS CloudFormation templates.
- Seamlessly integrates with well-known tools for improved performance monitoring and log management, such as AWS CloudWatch, Azure Application Insights, vRealize Operations Manager (vROps), Azure Log Analytics Workspace, and vRealize Log Insight (vRLI).



### API

#### Full Programmability

The Thunder ADC platform leverages A10's REST-based aXAPIs to configure all features with 100 percent API coverage. This interface is used to integrate with third-party or custom management consoles, such as SDN platforms (e.g., VMware) and cloud orchestration systems (e.g., OpenStack and Microsoft SCVMM). A software plug-in is available for private clouds leveraging vRealize Orchestrator from VMware.



### Comprehensive

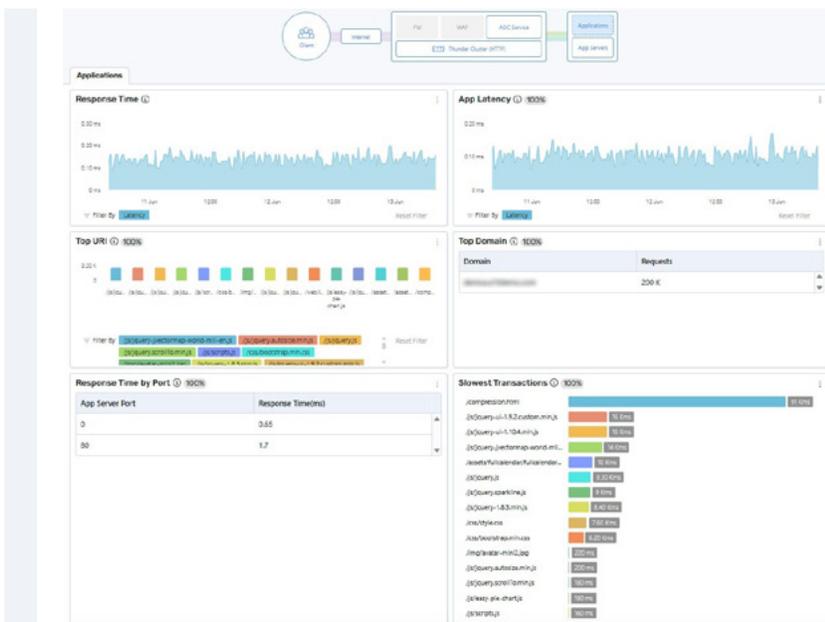
#### Management Tools

A10 Control is a centralized management platform that coordinates and distributes application-centric service policies and configuration files to hundreds of Thunder appliances and device cluster infrastructures across multi-cloud environments. Administrators can automatically discover, track and monitor each appliance including key operational metrics such as CPU and disk usage as well as device partitions and users. The controller performs configuration backup and restore operations and schedules software upgrades.



### ADC Service View

Thunder ADC with A10 Control provides granular real-time analytics of the ADC services. Information available for each application service port includes user traffic throughput and connection rate, load distribution, ADC service latency, RAM cache utilization, compression statistics, SSL connection rates and error traffic rate.



### Applications View

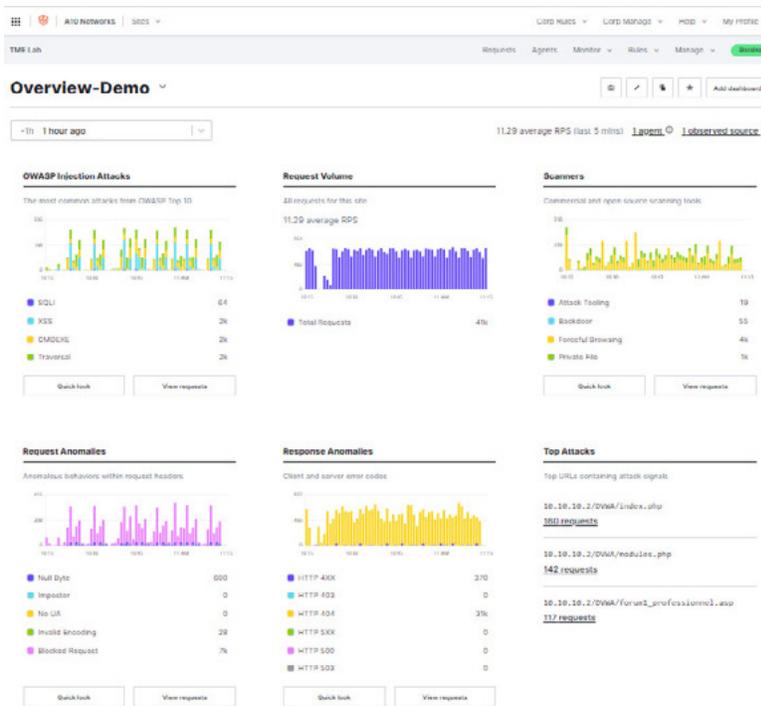
Get a real-time status report of the application services, including application response time and latency, top URL analytics, top domains analytics for global usage visualization, response type analytics by port number and slow transaction analytics per page under the application.



### Response Time Details

This information is useful for troubleshooting delayed application response times. The screen details the time taken in various portions of a HTTP transaction. These graphs also help distinguish application vs. infrastructure related issues.

## A10 Next-Gen WAF Visibility & Analytics



### Next-Gen WAF Dashboard

Gain a holistic perspective on the activity across all applications with a comprehensive understanding of the overall picture. It also includes predefined and customizable dashboards that highlight attack and anomaly trends, allowing for easy monitoring and analysis. Additionally, the system provides real-time visibility and collection of metrics, enabling users to stay updated on the latest information. The events and requests view further enhances the understanding by presenting a detailed timeline that illustrates the sequence of actions leading to blocking.

# Thunder ADC Physical Appliance Specifications

	Thunder 1060S <sub>ADC</sub>		Thunder 3350-E <sub>ADC</sub>	Thunder 3350 <sub>ADC</sub>
Modular License	10 Gbps	25 Gbps	-	-
<b>Performance</b>				
Application Throughput (L4/L7)	10 Gbps / 10 Gbps	25 Gbps / 25 Gbps	30 Gbps / 30 Gbps	40 Gbps / 40 Gbps
Layer 4 CPS	550K	800K	800K	1 Million
Layer 4 Concurrent Sessions	32 Million	96 Million	64 Million	96 Million
Layer 7 CPS (1:1) <sup>1</sup>	200K	480K	330K	500K
SSL Bulk Throughput <sup>2</sup>	10 Gbps	15 Gbps	13 Gbps	18 Gbps
SSL CPS <sup>2</sup>	RSA: 15K ECDSA: 5K	RSA: 28K ECDSA: 9K	RSA: 28K ECDSA: 15K	RSA: 28K ECDSA: 15K
DDoS Protection (SYN flood) SYN/sec	4 Million	8 Million	8 Million	8 Million
<b>Network Interfaces</b>				
1GE (BASE-T)	7	7	6	6
1GE Fiber (SFP)	0	0	2	2
10/1GE Fiber (SFP+/SFP)	4	4	8 + 4 <sup>6</sup>	4 <sup>6</sup>
25/10GE Fiber (SFP28/SFP+)	2	2	0	4
40GE Fiber (QSFP+)	0	0	0	4
100/40GE Fiber (QSFP28/QSFP+)	0	0	0	0
Management Ports	Ethernet mgmt. port, RJ-45 console port			
<b>Hardware Specifications</b>				
Processor	Intel communications processor 20-core [9-core active]	Intel communications processor 20-core	Intel Xeon 8-core	Intel Xeon 8-core
Memory (ECC RAM)	32 GB [24 GB active]	32 GB	16 GB	32 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	Software	Software	Software
TLS/SSL Security Acceleration	Hardware	Hardware	Hardware	Hardware
Dimensions (inches)	1.75 (H) x 17.5 (W) x 17 (D)	1.75 (H) x 17.5 (W) x 17 (D)	1.75 (H) x 17.5 (W) x 18(D)	1.75 (H) x 17.5 (W) x 18(D)
Rack Units (mountable)	1U	1U	1U	1U
Unit Weight <sup>3</sup>	12 lbs	12 lbs	18 lbs	18 lbs
Power Supply (DC option available)	Dual 300W RPS 80 Plus Gold efficiency, 100 - 240 VAC, 50 - 60 Hz	Dual 300W RPS	Dual 750W RPS 80 Plus Platinum efficiency, 100 - 240 VAC, 50 - 60 Hz	Dual 750W RPS
Power Consumption (typical/max) <sup>3</sup>	112W / 127W	112W / 127W	151W / 205W	165W / 238W
Heat in BTU/hour (typical/max) <sup>3</sup>	383 / 434	383 / 434	516 / 700	564 / 831
Cooling Fan (front-to-back airflow)	Removable fans		Hot swap smart fans	
<b>Operating Ranges</b>				
Regulatory Certifications	FCC Class A, UL <sup>+</sup> , ICES, CE, UKCA, CB <sup>+</sup> , VCCI, BSMI <sup>+</sup> , RCM   RoHS	FCC Class A, UL <sup>+</sup> , ICES, CE, UKCA, CB <sup>+</sup> , VCCI, BSMI <sup>+</sup> , RCM   RoHS	FCC Class A, UL <sup>+</sup> , CE, UKCA, VCCI, BSMI, RCM   RoHS	FCC Class A, UL <sup>+</sup> , CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS
Standard Warranty	90-day hardware and software			

## Thunder ADC Physical Appliance (cont.)

	Thunder 3350S <sup>ADC7</sup>	Thunder 4440 <sup>ADC</sup>	Thunder 5440 <sup>ADC</sup>	Thunder 5840 <sup>ADC</sup>
Modular License	50 Gbps	-	-	-
<b>Performance</b>				
Application Throughput (L4/L7)	50 Gbps / 50 Gbps	78 Gbps / 70 Gbps	100 Gbps / 100 Gbps	115 Gbps / 113 Gbps
Layer 4 CPS	2 Million	2 Million	3 Million	4 Million
Layer 4 Concurrent Sessions	128 Million	128 Million	256 Million	256 Million
Layer 7 CPS (1:1) <sup>1</sup>	750K	750K	950K	1.5 Million
SSL Bulk Throughput <sup>2</sup>	30 Gbps	25 Gbps	45 Gbps	55 Gbps
SSL CPS <sup>2</sup>	RSA: 60K ECDSA: 35K	RSA: 70K ECDSA: 42K	RSA: 100K ECDSA: 60K	RSA: 150K ECDSA: 90K
DDoS Protection (SYN flood) SYN/sec	16 Million	110 Million	166 Million	166 Million
<b>Network Interfaces</b>				
1GE (BASE-T)	6	0	0	0
1GE Fiber (SFP)	2	0	0	0
10/1GE Fiber (SFP+/SFP)	8 + 4 <sup>6</sup>	24	24	24
25/10GE Fiber (SFP28/SFP+)	0	0	0	0
40GE Fiber (QSFP+)	0	4	4	4
100/40GE Fiber (QSFP28/QSFP+)	0	0	0	0
Management Ports	Ethernet mgmt. port, RJ-45 console port	Ethernet mgmt. port, RJ-45 console port, Lights out management		
<b>Hardware Specifications</b>				
Processor	Intel Xeon 14-core	Intel Xeon 6-core	Intel Xeon 12-core	Intel Xeon 18-core
Memory (ECC RAM)	64 GB	32 GB	64 GB	64 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	2 x FTA-4	2 x FTA-4	2 x FTA-4
TLS/SSL Security Acceleration	Hardware	Hardware on S model	Hardware on S model	Hardware on S models
Dimensions (inches)	1.75 (H) x 17.5 (W) x 18(D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U	1U	1U	1U
Unit Weight <sup>3</sup>	18 lbs	32.5 lbs	32.5 lbs	32.5 lbs
Power Supply (DC option available)	Dual 750W RPS	Dual 1100W RPS	Dual 1100W RPS	Dual 1100W RPS
		80 Plus Gold efficiency, 100 - 240 VAC, 50 - 60 Hz		
Power Consumption (typical/max) <sup>3</sup>	175W / 222W	360W / 445W	360W / 445W	375W / 470W
Heat in BTU/hour (typical/max) <sup>3</sup>	598 / 758	1,229 / 1,519	1,229 / 1,519	1,280 / 1,604
Cooling Fan (front-to-back airflow)	Hot swap smart fans			
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS, FIPS 140-2 <sup>5</sup>	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS, FIPS 140-2 <sup>5</sup>	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS, FIPS 140-2 <sup>5</sup>
Standard Warranty	90-day hardware and software			

# Thunder ADC Physical Appliance (cont.)

	Thunder 5840-11 ADC	Thunder 6440 ADC	Thunder 7440 ADC	Thunder 7440-11 ADC
Modular License	-	-	-	-
<b>Performance</b>				
Application Throughput (L4/L7)	115 Gbps / 113 Gbps	150 Gbps / 140 Gbps	220 Gbps / 200 Gbps	220 Gbps / 200 Gbps
Layer 4 CPS	4 Million	4 Million	7.5 Million	7.5 Million
Layer 4 Concurrent Sessions	256 Million	256 Million	256 Million	256 Million
Layer 7 CPS (1:1) <sup>1</sup>	1.5 Million	1.4 Million	2.4 Million	2.4 Million
SSL Bulk Throughput <sup>2</sup>	55 Gbps	60 Gbps	75 Gbps	75 Gbps
SSL CPS <sup>2</sup>	RSA: 150K ECDSA: 90K	RSA: 150K ECDSA: 70K	RSA: 200K ECDSA: 70K	RSA: 200K ECDSA: 70K
DDoS Protection (SYN flood) SYN/sec	166 Million	238 Million	332 Million	332 Million
<b>Network Interfaces</b>				
1GE (BASE-T)	0	0	0	0
1GE Fiber (SFP)	0	0	0	0
10/1GE Fiber (SFP+/SFP)	48	48	48	48
25/10GE Fiber (SFP28/SFP+)	0	0	0	0
40GE Fiber (QSFP+)	0	4	4	0
100/40GE Fiber (QSFP28/QSFP+)	4	0	0	4
Management Ports	Ethernet mgmt. port, RJ-45 console port, Lights out management			
<b>Hardware Specifications</b>				
Processor	Intel Xeon 18-core	2 x Intel Xeon 10-core	2 x Intel Xeon 18-core	2 x Intel Xeon 18-core
Memory (ECC RAM)	64 GB / 128 GB <sup>4</sup>	128 GB	128 GB	128 GB
Storage	SSD	SSD	SSD	SSD
Hardware Acceleration	2 x FTA-4	3 x FTA-4	3 x FTA-4	3 x FTA-4
TLS/SSL Security Acceleration	Hardware on S models	Hardware on S model	Hardware on S model	Hardware on S model
Dimensions (inches)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1U	1U	1U	1U
Unit Weight <sup>3</sup>	34.3 lbs	36 lbs	35.7 lbs	35.7 lbs
Power Supply (DC option available)	Dual 1500W RPS	Dual 1100W RPS	Dual 1100W RPS	Dual 1500W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 - 60 Hz			
Power Consumption (typical/max) <sup>3</sup>	550W / 760W	480W / 550W	690W / 820W	820W / 950W
Heat in BTU/hour (typical/max) <sup>3</sup>	1,877 / 2,594	1,638 / 1,877	2,355 / 2,798	2,798 / 3,242
Cooling Fan (front-to-back airflow)	Hot swap smart fans			
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM   RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM   RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM   RoHS, FIPS 140-2 <sup>5</sup>
Standard Warranty	90-day hardware and software			

## Thunder ADC Physical Appliance (cont.)

	Thunder 7460S <sub>ADC</sub>			Thunder 7460S-MAX <sub>ADC</sub>
Modular License	150 Gbps	200 Gbps	250 Gbps	-
<b>Performance</b>				
Application Throughput (L4/L7)	150 Gbps / 130 Gbps	200 Gbps / 175 Gbps	250 Gbps / 220 Gbps	270 Gbps / 235 Gbps
Layer 4 CPS	5 Million	7 Million	9 Million	11 Million
Layer 4 Concurrent Sessions	256 Million	256 Million	256 Million	256 Million
Layer 7 CPS (1:1) <sup>*1</sup>	2 Million	2.5 Million	3.3 Million	3.5 Million
SSL Bulk Throughput <sup>*2</sup>	75 Gbps	85 Gbps	90 Gbps	95 Gbps
SSL CPS <sup>*2</sup>	RSA: 140K ECDSA: 85K	RSA: 180K ECDSA: 100K	RSA: 210K ECDSA: 120K	RSA: 290K ECDSA: 130K
DDoS Protection (SYN flood) SYN/sec	275 Million	275 Million	275 Million	275 Million
<b>Network Interfaces</b>				
1GE (BASE-T)	0			0
1GE Fiber (SFP)	0			0
10/1GE Fiber (SFP+/SFP)	0			0
25/10GE Fiber (SFP28/SFP+)	24			24
40GE Fiber (QSFP+)	0			0
100/40GE Fiber (QSFP28/QSFP+)	4			8
Management Ports	Ethernet mgmt. port, RJ-45 console port			
<b>Hardware Specifications</b>				
Processor	Intel Xeon 36-core [20-core active]	Intel Xeon 36-core [28-core active]	Intel Xeon 36-core	Intel Xeon 52-core
Memory (ECC RAM)	256 GB [192 GB active]	256 GB [192 GB active]	256 GB [192 GB active]	256 GB
Storage	SSD			
Hardware Acceleration	1 x FTA-6			
TLS/SSL Security Acceleration	Hardware			
Dimensions (inches)	1.75 (H) x 17.5 (W) x 30 (D)			
Rack Units (mountable)	1U			
Unit Weight <sup>*3</sup>	39.75 lbs			
Power Supply (DC option available)	Dual 1500W RPS 80 Plus Platinum efficiency, 100 - 240 VAC, 50 - 60 Hz			
Power Consumption (typical/max) <sup>*3</sup>	710W / 790W			
Heat in BTU/hour (typical/max) <sup>*3</sup>	2,423 / 2,696			
Cooling Fan (front-to-back airflow)	Hot swap smart fans			
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%			
Regulatory Certifications	FCC Class A <sup>^</sup> , UL <sup>^</sup> , CE <sup>^</sup> , UKCA <sup>^</sup> , VCCI <sup>^</sup> , KCC <sup>^</sup> , BSMI <sup>^</sup> , RCM <sup>^</sup> , MTCTE <sup>^</sup> , ANATEL <sup>^</sup>   RoHS <sup>^</sup>			
Standard Warranty	90-day hardware and software			

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions. As for network interfaces, it's highly recommended to use A10 Networks' qualified optics/transceivers to ensure network reliability and stability.

<sup>\*1</sup> Layer 7 connections per second - measures number of new HTTP connections (1 HTTP request per TCP connection, without TCP connection reuse) within 1 second | <sup>\*2</sup> Tested with maximum SSL option. Cipher "TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256" with RSA 2K keys, unless noted, are used for RSA cases. "TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256" with EC P-256 are used for PFS cases. | <sup>\*3</sup> With base model. Number varies by hardware options (e.g. SSL cards) | <sup>\*4</sup> With maximum SSL option | <sup>\*5</sup> For FIPS 140-2 Level 2 validated, FIPS models must be purchased | <sup>\*6</sup> 10Gbps speed only | <sup>\*7</sup> Performance numbers are measured with ACOS 5.2.1 release code | <sup>^</sup> Certification in process

# Thunder ADC SPE Physical Appliance Specifications

	Thunder 6655S ADC	Thunder 7655S ADC
Modular License	-	-
<b>Performance</b>		
Application Throughput (L4/L7)	185 Gbps / 170 Gbps	370 Gbps / 340 Gbps
Layer 4 CPS	6 Million	12 Million
Layer 4 Concurrent Sessions	384 Million	768 Million <sup>*3</sup>
Layer 7 CPS (1:1) <sup>*1</sup>	2.25 Million	4.5 Million
SSL Bulk Throughput <sup>*2</sup>	72.5 Gbps	145 Gbps
SSL CPS <sup>*2</sup>	RSA: 100K ECDSA: 70K	RSA: 200K ECDSA: 140K
DDoS Protection (SYN flood) SYN/sec	250 Million	500 Million
<b>Network Interfaces</b>		
100/40GE Fiber (QSFP28/QSFP+)	16	16
Management Ports	Ethernet mgmt. port, RJ-45 console port, Lights out management	
<b>Hardware Specifications</b>		
Processor (Intel Xeon)	28-core	2 x 28-core
Memory (ECC RAM)	192 GB	384 GB
Storage	SSD	SSD
Hardware Acceleration	FTA-5, SPE	2 x FTA-5, SPE
TLS/SSL Security Acceleration	Hardware	Hardware
Dimensions (Inches)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1.5U	1.5U
Unit Weight	39 lbs	44.2 lbs
Power Supply (DC option available)	Dual 1500W RPS	Dual 1500W RPS
	80 Plus Platinum Efficiency, 100 - 240 VAC, 50 - 60 Hz	
Power Consumption (typical/max)	667W / 856W	1,121W / 1,300W
Heat in BTU/hour (typical/max)	2,276 / 2,921	3,826 / 4,436
Cooling Fan (front-to-back airflow)	Hot swap smart fans	
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%	
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM   RoHS, FIPS 140-2 <sup>*4</sup>	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM   RoHS, FIPS 140-2 <sup>*4</sup>
Standard Warranty	90-day hardware and software	

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions. As for network interfaces, it's highly recommended to use A10 Networks' qualified optics/transceivers to ensure network reliability and stability.

\*1 Layer 7 connections per second - measures number of new HTTP connections (1 HTTP request per TCP connection, without TCP connection reuse) within 1 second | \*2 Tested with Cipher "TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256" with 2K keys for RSA cases, "TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256" with EC P-256 for ECC cases | \*3 Capacity has been increased (doubled) from ACOS 5.2.1-P7/6.0.1 onward | \*4 For FIPS 140-2 Level 2 validated, FIPS models must be purchased | ^ Certification in process

## Thunder ADC for Low-latency Appliance Specifications

Thunder 3745	
<b>Performance</b>	
Mean Latency L7 <sup>*1</sup>	1.901 $\mu$ s
Max Latency L7	1.945 $\mu$ s
Concurrent NAT Sessions	32,000
<b>Network Interfaces</b>	
10/1GE Fiber (SFP+/SFP)	4 <sup>*3</sup>
Management Ports	Ethernet mgmt. port, RJ-45 console port
<b>Hardware Specifications</b>	
Processor (Intel Xeon)	2 x 8-core
Memory (ECC RAM)	96 GB
Storage	SSD
Hardware Acceleration	FPM <sup>*2</sup>
Dimensions (Inches)	3.5 (H) x 19 (W) x 27.5 (D)
Rack Units (mountable)	2U
Unit Weight	43.8 lbs
Power Supply (DC option available)	Dual 850 W RPS 80 Plus Platinum efficiency, 100 - 240 VAC, 50 - 60 Hz
Power Consumption (typical/max)	450W / 463W
Heat in BTU/hour (typical/max)	1,536 / 1,580
Cooling Fan (front-to-back airflow)	Hot swap smart fans
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%
Regulatory Certifications	FCC Class A, CE, VCCI, RCM, UKCA, UL/CB
Standard Warranty	90-day hardware and software

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

<sup>\*1</sup> 99th percentile. All the performance numbers are measured using FIX protocol with 670B packet size. | <sup>\*2</sup> Flow processing module (FPM) consists of FTA-3 (Flexible Traffic Accelerator) and SPE (Security and Policy Engine). | <sup>\*3</sup> 10Gbps speed only | <sup>\*</sup> Certification in process

# A10 Thunder on Dell Technologies OEM Solution Bundle Specifications

## Multi-tenant Virtual Platform (MVP) Specifications

A10 Thunder Multi-tenant Virtual Platform (MVP) is an advanced platform enabling multiple virtual instances or services on a single platform, that has the capabilities of delivering Application Delivery Controller (ADC) and Carrier Grade Networking (CGN) solutions along with an expanded feature set of A10 capabilities.

Performance with ADC	A10 Thunder MVP*
Application Throughput (L4 / L7)	200 Gbps / 200 Gbps
Connections Per Second (L4 / L7) <sup>*1</sup>	4.7 million / 2.7 million
SSL Bulk Throughput <sup>*2</sup>	60 Gbps
SSL CPS (RSA / ECDSA) <sup>*2</sup>	166K / 83K
Network Interfaces	
25/10GE Fiber (SFP28/SFP+)	4
100/40GE Fiber (QSFP28/QSFP+)	4
Hardware Specifications	
Processor	2 x Intel Xeon 24-core
Memory	256 GB
Storage	2 x SSD
TLS/SSL Security Processor	Integrated QAT
Power Supply	Dual 1400W redundant power supply

Specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

\*1 Layer 7 connections per second - measures number of new HTTP connections (1 HTTP request per TCP connection, without TCP connection reuse ) within 1 second

\*2 Tested with TLS 1.3 and RSA (2K keys) cipher: "TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256" and ECDSA (EC P-256) cipher: "TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256"

+ Available bandwidth license: 50, 100, 150, 200 Gbps. Maximum throughput performance depends on the license.

Thunder MVP performance specifications are aggregate number that use the following VM profiles:

- A10 Thunder MVP is tested on Dell R760 with 14-VM profile (6 vCPUs, 16 GB memory, 60GB storage, 4 SSL virtual functions (VFs) assigned on each vThunder)

# Thunder ADC Software Appliance Specifications

vThunder ADC										
Supported Hypervisors	VMware ESXi (VMXNET3, SR-IOV, PCI Passthrough), KVM (VirtIO, 0vS with DPDK, SR-IOV, PCI Passthrough)									
Hardware Requirements	See installation guide									
Standard Warranty	90-day software									
Bandwidth Licenses	Lab	200 Mbps	1 Gbps	4 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps	100 Gbps	FlexPool
VMware ESXi	•	•	•	•	•	•	• <sup>*1</sup>	• <sup>*1</sup>	• <sup>*1 *2</sup>	•
KVM	•	•	•	•	•	•	• <sup>*1</sup>	• <sup>*1</sup>	• <sup>*1 *2</sup>	•
Thunder ADC for Public Cloud	AWS	Microsoft Azure	Google Cloud	Oracle Cloud						
Product on Marketplace	Thunder ADC for AWS	Thunder ADC for Azure	Thunder ADC for GCP	vThunder Application Delivery Controller (ADC)						
Throughput <sup>*3</sup>	Up to 10 Gbps	Up to 10 Gbps	Up to 10 Gbps	Up to 24 Gbps						
Licenses <sup>*3</sup>	30-day trial license Pre-installed bandwidth license: • 20 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 5 Gbps, 10 Gbps BYOL bandwidth license FlexPool license	30-day trial license Pre-installed bandwidth license: • 20 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 5 Gbps, 10 Gbps BYOL bandwidth license FlexPool license	30-day trial license Pre-installed bandwidth license: • 20 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 5 Gbps, 10 Gbps BYOL bandwidth license FlexPool license	30-day trial license Pre-installed bandwidth license: • 1 OCPU to 24 OCPU BYOL bandwidth license FlexPool license						
Thunder ADC Container										
Image Format	Open Container Initiative (OCI) compliant									
Operating System	RedHat OpenShift Container Platform (OCP) (Version 4.16)									
System Requirements	<ul style="list-style-type: none"> <li>• Minimum 4 vCPU and 16GB memory</li> <li>• One or more data interfaces</li> <li>• SR-IOV support using NVIDIA or Intel NICs</li> </ul>									
Licenses	BYOL bandwidth license FlexPool license									
Trial Details	Contact A10 Sales									
Thunder ADC for Bare Metal										
System Requirements	See installation guide									
Reference Platforms	Dell Power Edge R760, Super Micro X13									
Bandwidth Licenses <sup>*</sup>	10 Gbps (4 cores), 20 Gbps (8 cores), 40 Gbps (14 cores) and 60 Gbps (24 cores), FlexPool (Up to 60 Gbps per Thunder ADC)									
Standard Warranty	90-day software									

\* 1 SR-IOV | \*2 PCI Passthrough | \*3 Per-instance maximum throughput varies depending on instance type and configurations  
 \* Licenses are tied to the maximum number of CPU cores that can be allocated to ACOS

# Detailed Feature List

Features may vary by appliance.

## Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
  - Fast HTTP, Full HTTP proxy, HTTP/2, HTTP/3
  - High-performance, template-based Layer 7 switching with header/URL/domain manipulation
  - Comprehensive Layer 7 application persistence support
  - SIP, MQTT, RTSP, SMTP, POP3, FTP, FIX and more
- DNS load balancing
  - Layer 4 (UDP/TDP) and Layer 7 (DNS-UDP/DNS-TCP)
  - Recursive DNS lookup
  - DNS firewall/RPZ
  - DNS cache
- Comprehensive load balancing methods
  - Round robin, least connections, weighted RR, weighted LC, fastest response, and more
- aFlex – Deep packet inspection and transformation for customizable, application-aware switching
- Advanced health monitoring
  - Comprehensive protocol support – ICMP, TCP, UDP, HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP and more
  - Scriptable health check support using TCL, Python, Perl, Bash
  - Compound health monitor support
- High availability – active-active, active-standby configurations
- SIP load balancing for VoIP
- STARTTLS support for secure email and LDAP
- Network traffic filtering – high-speed processing of large black/white lists
- Firewall load balancing (FWLB)
- Global server load balancing (GSLB)
- Traffic steering/service chaining
- Transparent cache switching (TCS)
- Next hop load distribution (NHLD) for load balancing multiple links
- Diameter AAA load balancing
- RADIUS load balancing
- Database load balancing
- Internet content adaptation protocol (ICAP) support
- Low latency FIX support

## Application Acceleration

- HTTP acceleration and optimization
  - HTTP connection multiplexing (also called TCP connection reuse)
  - RAM caching
  - HTTP compression
- SSL offload
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- TCP optimization support including selective acknowledgment, client keep-alive and window scaling
- HTTP pipelining
- HTTP/2, SPDY protocol
- HTTP/3, QUIC protocol

## Application Security

- Next-Generation Web Application Firewall (Next-Gen WAF)
- DNS application firewall (DAF)
- Integrated DDoS protection for application services
- Hardware-based DDoS protection
- Application Access Management (AAM) – SAML, WIA, Kerberos, NTLM, TDS SQL Logon, LDAP, RADIUS, Basic, OSCP stapling, HTML Form-based
- AAM RADIUS-based audit support
- Single sign-on (SSO) authentication relay
- Authentication for Microsoft SharePoint, Outlook Web Access, and other packaged and custom applications
- Comprehensive SSL/TLS support
  - TLS 1.2 and TLS 1.3
  - Perfect Forward Secrecy (PFS) with Elliptic Curve Diffie-Hellman Exchange (ECDHE) and other Elliptic Curve Cryptography (ECC) ciphers
  - AES-NI and GCM ciphers
- IP anomaly detection
- DDoS attack detection and prevention using zero-day source behavior attack detection and recognition (ZBAR)

- Defend against HTTP request smuggling
- Connection rate limiting/connection limiting
- Bandwidth rate limiting per source IP
- Dynamically add IPs to black-white lists
- Support for Simple Certificate Enrollment Protocol (SCEP)
- ACME client support for automatic certificate renewal

## A10 Next-Gen WAF, powered by Fastly\*\*

- Comprehensive OWASP top attacks protection
- Account takeover (ATO) protection
- Advanced rate limiting
- Network learning exchange (NLX)
- Virtual patching for CVEs
- Streamlined management and extensive visibility on application attacks and anomalies
- Compliance
- Explicit proxy deployment support

## A10 Threat Intelligence Service\*\*

- Dynamically updated threat intelligence feed

## Scalable, High-performance Platform

- Advanced Core Operating System (ACOS)
  - Multi-core, multi-CPU support
  - Linear application scaling
  - ACOS on data plane
- Linux on control plane
- IPv6 feature parity

## Networking

- Integrated Layer 2/Layer 3
- Transparent mode/gateway mode
- Virtual wire interface support
- Routing – static routes, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+
- L2 protocols (STP, RSTP, MSTP)
- VLAN (802.1Q)
- Link aggregation (802.1AX), LACP
- Access control lists (ACLs)
- Traditional IPv4 NAT/NAPT
- IPv6 NAPT
- Jumbo frame support\*
- Hardware-accelerated VXLAN\*
- NVGRE

## IPv6 Migration/IPv4 Preservation

- Full native IPv6 management and feature support
- SLB-PT (Protocol Translation), SLB-64 (IPv4<->IPv6, IPv6<->IPv4)
- Carrier grade NAT (CGN/CGNAT), Large scale NAT (LSN), NAT444, NAT44, NAT46
  - Integrated DDoS protection for NAT pools
- NAT64/DNS64, DS-Lite, 6rd, LW4o6
- ALG protocol support for protocols with dynamic ports like SIP and FTP

## Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- Web-based AppCentric templates (ACT) intuitive guided configuration tool
- SNMP, syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
- RESTful API (aXAPI)
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs
- Interoperable with A10 Control and Harmony Controller for centralized management, configuration and analytics
- Plug-in available for VMware vRealize Orchestrator deployments

## Virtualization

## Detailed Feature List (Cont.)

- Thunder virtual appliance for VMware vSphere ESXi, and KVM
- Thunder ADC for Amazon Web Services (AWS), Microsoft Azure, Google Cloud and Oracle Cloud
- Thunder ADC for Bare Metal
- Thunder ADC for containers
- Networking acceleration (SR-IOV, DPDK) and management integration
- A10 Thunder on Dell Technologies OEM solution bundle

### Extensibility

- aVCS (Virtual Chassis System)
- Multi-tenancy with application delivery partition (ADP) based management
- Layer 3 - 7 virtualization

### Centralized Management and Analytics with A10 Control

- Multi-tenant service platform architecture
- Device, configuration and certificate management
- Metrics for monitoring device health and performance
- Application traffic insights showing traffic trends based on requests, throughput, and connection rates, along with detailed metrics for top clients, source location, request methods and response codes.
- Performance insights such as average end-to-end latency, server response time, cache utilization and so on
- Application insights visualizing charts of response time and app latency charts, and detailed metrics for top domains, URLs
- Session logs, error logs, and alert notifications for efficient troubleshooting
- On-demand/scheduled per-app service level reports
- Easy integration with popular collaboration platforms like Microsoft Teams and Slack

### DevOps Tools and Integration

- Ansible modules and playbooks
- Terraform Thunder provider
- HashiCorp's Consul and Network Infrastructure Automation (NIA) integration
- Thunder Kubernetes Connector (TKC)
- Microsoft Azure ARM templates
- AWS CloudFormation templates
- OpenStack Octavia driver
- Cloud-init support for auto-configuration on
  - OpenStack
  - OCI
  - AWS
  - Azure
- Prometheus integration for visibility and analytics monitoring
- Automatic certificate renewal with Sectigo, Let's Encrypt, Venafi and more
- Thunder Observability Agent (TOA) for publishing Thunder metrics and logs to
  - AWS CloudWatch
  - Azure Application Insights / Log Analytics
  - VMware vRealize Operations (vROps) / Log Insights (vRLI)

### Carrier-grade Hardware\*

- Advanced hardware architecture
- Hardware-based SYN cookies
- Hot swap redundant power supplies (AC or DC)
- Smart fans (hot swap)
- Solid-state drive (SSD)
- Tamper detection
- Lights out management (LOM/IPMI)
- 25 GbE ports, 40 GbE ports, 100 GbE ports
- High-performance security processor option

### Flexible Licensing

- Modular licensing for Thunder hardware\* allowing "pay-as-you-grow" model and capacity upgrade
- Fixed bandwidth licensing for Thunder running in any software form factor
- FlexPool: portable and flexible capacity pooled licensing for software Thunder running across any private and public clouds

### Security and Capability Assurance Certifications\*

- Next-Gen WAF is PCI DSS compliant as a Level 1 Service Provider
- Common Criteria EAL 2+
- FIPS 140-2 Level 2
- Joint Interoperability Test Command (JITC)
- Network Equipment Building System (NEBS) compliance

\* Features and certifications may vary by appliance.

\*\* Additional subscription or service is required.

## Learn More

About A10 Networks

Contact Us

[A10networks.com/contact](https://a10networks.com/contact)

©2025 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, Thunder, Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: [A10networks.com/a10trademarks](https://a10networks.com/a10trademarks).

Part Number: A10-DS-15100-EN-58 June 2025

# **FIPS 140-2 Level 2 Security Policy**

**For**



**Thunder by A10 Networks, Inc.**

**Versions TH1040, TH3350S, TH6655S, and  
TH7655S**

**Document Version 1.4**

## Table of Contents

1 Module Description .....	3
2 Cryptographic Boundary.....	4
3 Security Functions .....	6
4 Ports and Interfaces.....	12
5 Roles, Services and Authentication .....	13
6 Key Management .....	16
7 Self Tests.....	22
8 Physical Security.....	25
9 Secure Operation.....	26
9.1 Approved Mode of Operation.....	26
10 References.....	27

## 1 Module Description

A10 Networks, Inc.'s Thunders are an outgrowth or evolution of Traffic Manager and Application Delivery Controller (ADC) systems and technologies. These Thunder systems are advanced load balancers for ADC needs and sophisticated address translators for IPv6 migration, while being able to secure and control the traffic directed through the system for enterprise, ISP, and mobile networks. These systems include full proxies able to encrypt, decrypt, and inspect traffic for these networks.

The foundation of the Thunder systems is the A10 Networks, Inc.'s proprietary A10 Core Operating System (ACOS). ACOS is a software framework for maximized networks traffic processing performance that supports a common management and control plane architecture across a range of infrastructures; from data centers to cloud to multi-cloud.

These systems (subsequently referred to as "the module") support SSH, HTTPS, and console management interfaces. For the purposes of FIPS 140-2 the Thunder is classified as multi-chip standalone module.

FIPS 140-2 conformance testing of the module was performed at Security Level 2. The following configurations were tested:

**Table 1: Configurations tested by the lab**

Module Name	Hardware versions	Processor	Firmware versions
Thunder by A10 Networks, Inc.	TH1040	Intel Atom C3958 with AES-NI	5.2.1-P5
	TH3350S	Intel Xeon D-2177NT with AES-NI	5.2.1-P5
	TH6655S	Intel Xeon Gold 6258R with AES-NI	5.2.1-P5
	TH7655S	Intel Xeon Gold 6258R with AES-NI	5.2.1-P5

**Table 2: Module Security Level Statement**

FIPS Security Area	Security Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

## 2 Cryptographic Boundary

The hardware and firmware components of the module are enclosed in a metal enclosure which is the cryptographic boundary of the module. The removable panels of the enclosure are protected by tamper-evident labels. The enclosure is opaque within the visible spectrum.

Images of the module is provided below:

**Figure 1. Thunder TH1040**



**Figure 2. Thunder TH3350S**



**Figure 3. Thunder TH665S**



**Figure 4. Thunder TH765S**



### 3 Security Functions

The table below lists approved cryptographic algorithms employed by the module.

**Table 3: Approved Cryptographic Functions**

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use	
C1940	A10 Networks SSL FIPS Library	AES	FIPS 197, SP 800-38D	ECB, CBC, CTR, GCM <sup>1</sup>	128, 192, 256	Data Encryption/ Decryption KTS <sup>4</sup>	
A1305							
A2499							A10 Networks Data Plane FIPS Library-1
A2500				A10 Networks Data Plane FIPS Library-2			
A1181				A10 Networks IPsec FIPS Library			CBC
A2493				A10 Networks Data Plane FIPS Software Library			
C1940	A10 Networks SSL FIPS Library	DRBG	SP 800-90A	CTR_DRBG		Deterministic Random Bit Generation <sup>2</sup>	
A1305							
A2493							A10 Networks Data Plane FIPS Software Library
A2499	A10 Networks Data Plane FIPS Library-1	KAS-ECC-SSC	SP 800-56Ar3	ECC Ephemeral Unified Scheme	P-256, P-384 (corresponding to 128 or 192 bits of security)	TLS Shared Secret Computation	
A2500							A10 Networks Data Plane FIPS Library-2

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2499	A10 Networks Data Plane FIPS Library-1	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC- SHA-512	160, 256, 384, 512	Message Authentication KTS <sup>4</sup>
A2500	A10 Networks Data Plane FIPS Library-2					
C1940	A10 Networks SSL FIPS Library					
A1305						
A1181	A10 Networks IPsec FIPS Library					
A2493	A10 Networks Data Plane FIPS Software Library			HMAC-SHA-256, HMAC-SHA-384, HMAC- SHA-512	256, 384, 512	
A2493	A10 Networks Data Plane FIPS Software Library	SHS	FIPS 180-4	SHA-256, SHA-384, SHA-512		Message Digest
A1181	A10 Networks IPsec FIPS Library			SHA-1, SHA-256, SHA-384, SHA-512		
A2499	A10 Networks Data Plane FIPS Library-1					
A2500	A10 Networks Data Plane FIPS Library-2					
C1940	A10 Networks SSL FIPS Library					
A1305						

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use			
A1305	A10 Networks SSL FIPS Library	RSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 3072	Digital Signature Generation and Verification; Key Generation			
C1940									
A2499	A10 Networks Data Plane FIPS Library-1		FIPS 186-4	SHA-256, SHA-384, SHA-512, PKCS1 v1.5	2048	Digital Signature Generation and Verification			
A2500	A10 Networks Data Plane FIPS Library-2								
C1940	A10 Networks SSL FIPS Library		ECDSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512	P-256, P-384, P-521	Digital Signature Generation and Verification; Key Generation and Verification		
A1305									
A2499		A10 Networks Data Plane FIPS Library-1						SHA-256, SHA-384, SHA-512	P-256, P-384
A2500		A10 Networks Data Plane FIPS Library-2							
A1305	A10 Networks SSL FIPS Library	DSA		FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512	1024 (verification only), 2048, 3072		Digital Signature Generation and Verification; Key Generation and Key Verification	

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A1305	A10 Networks SSL FIPS Library	KAS-FFC-SSC and Safe Primes	SP 800-56Ar3	Ephemeral Scheme	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)	Shared Secret Computation
A1305		KAS-ECC-SSC		ECC Ephemeral Unified Scheme	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)	
A2499 A2500 A2493	A10 Networks Data Plane FIPS Library-1  A10 Networks Data Plane FIPS Library-2  A10 Networks Data Plane FIPS Software Library	KAS	SP 800-56Ar3 and SP 800-135	ECC Ephemeral Unified Scheme	P-256, P-384 (corresponding to 128 or 192 bits of security)	TLS Shared Secret Computation and TLS Key Derivation
A1305 C1940	A10 Networks SSL FIPS Library	KAS	SP 800-56Ar3 and SP 800-135	Ephemeral Scheme	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)	TLS, IKE v2, SSH Shared Secret Computation and TLS, IKE v2, SSH Key Derivation
				ECC Ephemeral Unified Scheme	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)	

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2493	A10 Networks Data Plane FIPS Software Library	CVL TLS 1.2	SP 800-135			Key Derivation <sup>3</sup>
C1940	A10 Networks SSL FIPS Library	CVL SNMP, TLS 1.2, SSH				
A1305		CVL SNMP, IKE v.2, TLS 1.2, SSH				
CKG (vendor affirmed)	A10 Networks SSL FIPS Library A10 Networks Data Plane FIPS Software Library	Cryptographic Key Generation	SP 800-133			Key generation <sup>2</sup>

Note 1: Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Note 2: not all CAVS tested modes of the algorithms are used in this module.

<sup>1</sup> The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from SP 800-52, Section 3.3.1. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.

<sup>2</sup> CKG is only used to generate asymmetric keys. The module directly uses the output of the DRBG. The generated seed used in the asymmetric key generation is an unmodified output from DRBG. Section 4, example 1, of SP800-133r2 "Using the Output of a Random Bit Generator" is applicable.

<sup>3</sup> No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

<sup>4</sup> KTS (AES-GCM Certs. #C1940 and #A1305; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (AES-CBC and CTR Certs. #C1940 and #A1305 and HMAC Certs. #C1940 and #A1305; key establishment methodology provides 128 or 256 bits of encryption strength).

The module also implements other cryptographic algorithms:

**Table 4.1: Non-Approved, Not Allowed Cryptographic Algorithms \***

<b>Algorithm</b>	<b>Usage</b>
MD5	Used by RADIUS
TLS 1.3	Used by TLS
GCM	Used by IPsec

\* Note: These algorithms must not be used in the Approved Mode of Operation.

**Table 4.2: Non-Approved, Not Allowed Cryptographic Algorithms (disabled by 'system fips enable' command)**

<b>Algorithm</b>	<b>Usage</b>
RSA Encryption/Decryption	Used by TLS
TLS 1.0/1.1 KDF	Used by TLS
GMSSL	Used by TLS
Chacha20-Poly1305	Used by TLS
3DES	Used by TLS and IPsec
DES	Used by IPsec
MD5	Used by IPsec
Not Approved Diffe-Hellman	Used by TLS and IPsec

## 4 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

**Table 5: Ports and Interfaces**

Port Name	Count	Interface(s)
Ethernet Port	TH1040:10 1 GE Copper: 6 1/10 GE Fiber (SFP+): 4	Data Input, Data Output, Control Input, Status Output
	TH3350S: 21 1 GE Copper: 7 1 GE Fiber (SFP): 2 1/10 GE Fiber (SFP+): 8 10 GE Fiber (SFP+): 4	
	TH6655S/TH7655S: 18 1 GE Copper: 2 100 GE Fiber (QSFP28): 16	
Serial Console Port	TH1040/TH3350S: 1	Control Input, Status output, Data Output
	TH6655S: 1	
	TH7655S: 2	
USB Ports	2	Disabled
Power Switch	1	Control Input
Power Port	TH1040/TH3350S: 2	Power Input
	TH6655S: 2	
	TH7655S: 2	
LEDs <sup>1</sup>	3	Status Output

<sup>1</sup> Also each Ethernet port uses 2 LEDs

## 5 Roles, Services and Authentication

The module provides the following roles: a User role and Crypto Officer role. The Crypto Officers initialize and manage the module. Users employ the cryptographic services provided by the module.

The table below provides information on authentication mechanisms employed by each role.

**Table 6.1: Authentication Mechanisms**

Role	Authentication Mechanism
User	<p>User authentication is certificate based with an RSA key of at least 2048 bits, which corresponds to 112-bit security or a probability of one successful attempt equal to <math>2^{-112}</math> or ca. <math>2 \cdot 10^{-34}</math> probability of success.</p> <p>The modules support the maximum of 200,000 user connections per second, even assuming that authentication occurs instantly, this translates to 12,000,000 authentication attempts per minute, and the maximum probability of success is <math>2.4 \cdot 10^{-27}</math>.</p>
Crypto Officer	<p>The minimum requirement for the password strength is eight characters. Any of the 89 characters can be used in any place. Thus, the probability of successfully guessing the password is <math>89^{-8}</math> or ca. <math>3 \cdot 10^{-16}</math> per attempt.</p> <p>The modules support three interfaces for password authentication: console and remote (SSH and GUI/HTTPS). In the worst-case scenario console attack can be combined with the most efficient of the two remote interfaces.</p> <p>The probability of succeeding after 1 minute of attempts is computed as the number of guesses within one minute divided by the total number of possible password combinations (still using the minimum password requirements as the reference).</p> <p><i>Console access:</i> console bandwidth is 9600bps (1200Bps). Given an 8-bite password length, this translates to, 150 (=1200/8) guesses per second or 9,000 (=150*60) guesses per minute.</p> <p><i>GUI/HTTPS:</i> the port supports 1Gbps (1,073,741,824bps). One password GUI transaction consumes at least 8,322 bytes (66,576 bits). Thus, the bandwidth supports 967,684 password guesses per minute (1,073,741,824*60/66,576). However, if we</p>

Role	Authentication Mechanism
	<p>take the time of transactions into consideration, we find that each password transaction in testing took at least .29 seconds. Even assuming a 1000 times faster processing rate, the number of transactions per minute is limited to 206,896 attempts (60/.00029). Thus, GUI/HTTPS can handle at most 206,896 attempts per minute.</p> <p><i>SSH</i>: one SSH session takes at least 6,614 bytes. SSH forces termination after three bad attempts at most in a single session. SSH protocol goes over 1Gbps connection. The maximum number of password attempts per minute is 3,652,735 (=1,073,741,824*60*3/(6,614*8)).</p> <p><i>The overall number of attempts per minute</i> is at most 3,661,735 (3,652,735+9,000) using simultaneously console and SSH authentication. The overall 1-minute probability is at most <math>3,661,735 * 89^{-8}</math> or ca. <math>9.3 * 10^{-10}</math>.</p> <p><i>IPSec PSK</i>: The module uses IPSec PSK of at least 8 printable characters. The total number of IPSec PSK character combinations is at least <math>62^8 = 218,340,105,584,896</math>.</p> <p>IPSec can also use RSA key of at least 2048 bits, which corresponds to 112-bit security or a probability of one successful attempt equal to <math>2^{-112}</math> or ca. <math>2 * 10^{-34}</math> probability of success.</p> <p>IPSec can also use ECDSA key of at least a P-256, which corresponds to 128-bit security or a probability of one successful attempt equal to <math>2^{-128}</math> or ca. <math>3 * 10^{-39}</math> probability of success.</p> <p>Therefore, the probability is less than one in 1,000,000 that a random attempt will succeed, or a false acceptance will occur.</p> <p>The time necessary for one IKE handshake limits the number of IKE handshakes in 1 minute to about 60000. Thus, for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed, or a false acceptance will occur.</p>

The module provides the following services to the operators:

**Table 6.2: Roles and Services**

Service	Role	Access to Cryptographic Keys and CSPs R- read; W – write or generate; E-execute
Installation of the Module	Crypto Officer	Password: W TLS server certificate: W SSH keys: E DRBG seed: E
Login	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E
Device Management	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E
SSH <sup>1</sup>	Crypto Officer	Password: E SSH Keys: E DRBG seed: E
HTTPS <sup>1</sup>	Crypto Officer	Password: E TLS Keys: E DRBG seed: E
Run self-test <sup>2</sup>	Crypto Officer	N/A
Show status <sup>3</sup>	Crypto Officer	N/A
Reboot <sup>4</sup>	Crypto Officer	N/A
Update firmware	Crypto Officer	Firmware load verification ECDSA SHA-256 firmware load verification key: E
Zeroize	Crypto Officer	All keys: W
Establishment of secure TLS network connection	User	TLS keys: E TLS Certificate: E DRBG seed: E
Establishment of secure IPsec network connection	User	IPsec keys: E DRBG seed: E

<sup>1</sup> KTS is supported in the module via HTTPS and SSH services.

<sup>2</sup> Run self-test by physically power cycling the module or by rebooting the module using its user interface.

<sup>3</sup> Show status by observation of LEDs or by observation of status in the user interface.

<sup>4</sup> Reboot by physically power cycling the module or by rebooting the module using its user interface.

## 6 Key Management

The following cryptographic keys and CSPs are supported by the module.

**Table 7: Cryptographic Keys and CSPs**

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
TLS pre-master secret  Established using KAS-ECC-SSC	Used to derive TLS master secret	Plaintext in RAM	Never input or output.	
TLS master secret  Established using KDF TLS	Used to derive TLS AES encryption key and TLS HMAC key	Plaintext in RAM	Never input or output.	
TLS AES encryption key  Established using KDF TLS <sup>3</sup>	Used to encrypt data in TLS protocol	Plaintext in RAM	Never input or output.	128, 256 bits of security
TLS HMAC key  Established using KDF TLS <sup>3</sup>	Used to protect integrity of data in TLS protocol	Plaintext in RAM	Never input or output.	160, 256, 384, 512 bits of security
TLS server RSA private key  Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
TLS server RSA public key  Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
TLS server ECDSA private key  Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS server ECDSA public key  Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS EC Diffie-Hellman private key  Established using DRBG	Used for key establishment during the TLS handshake	Plaintext in RAM	Never input or output.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS EC Diffie-Hellman public key  Established using DRBG	Used for key establishment during the TLS handshake	Plaintext in RAM	Never input. Can be output from the module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
SSH AES encryption key  Established using KDF SSH <sup>3</sup>	Used to encrypt SSH data	Plaintext in RAM	Never input or output.	128, 256 bits of security
SSH HMAC key  Established using KDF SSH <sup>3</sup>	Used to protect integrity of SSH data	Plaintext in RAM	Never input or output.	160, 256, 512 bits of security

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
SSH RSA private key  Established using DRBG or set by operators	Used in SSH handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048 (corresponding to 112 bits of security)
SSH RSA public key  Established using DRBG or set by operators	Used in SSH handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048 (corresponding to 112 bits of security)
SSH Diffie-Hellman Private key  Established using DRBG	Used for key establishment during the SSH handshake	Plaintext in RAM	Never input or output.	2048 (corresponding to 112 bits of security)
SSH Diffie-Hellman Public key  Established using DRBG	Used for key establishment during the SSH handshake	Plaintext in RAM	Never input. Can be output from the module.	2048 (corresponding to 112 bits of security)
IPSec AES encryption key  Established using KDF IKE	Used during encryption and decryption of data within the IPSec protocol	Plaintext in RAM	Never input or output.	128, 192, 256 bits of security
IPSec HMAC key  Established using KDF IKE	Used to protect integrity of data within the IPSec protocol	Plaintext in RAM	Never input or output.	160, 256, 384, 512 bits of security
IPSec PSK  Set by operators	Used for operator authentication	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	>= 8 characters

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
IPsec RSA private key  Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of Security)
IPsec RSA public key  Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
IPsec ECDSA private key  Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
IPsec ECDSA public key  Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
IPSec Diffie-Hellman private key  Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input or output.	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)
IPSec Diffie-Hellman public key  Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input. Can be output from the module.	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
IPSec EC Diffie-Hellman private key  Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input or output.	P-256, P-384 (corresponding to 128 or 192 bits of security)
IPSec EC Diffie-Hellman public key  Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input. Can be output from the module.	P-256, P-384 (corresponding to 128 or 192 bits of security)
Certification Authority RSA Certificate  Set by operators	Used to verify user certificate during the TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
CTR_DRBG CSPs: entropy input, V and Key	Used for generation of random numbers	Plaintext in RAM	Entropy is loaded externally and never output.	Minimum length of the entropy field is 256 bits
Firmware load verification ECDSA public key	Used for firmware load test	Plaintext in RAM Plaintext in flash	Set at the factory. Never output.	P-256 (corresponding to 128 bits of security)
Passwords  Set by operators	Used to authenticate operators	Plaintext in RAM Plaintext in flash	Can be input into the module. Never output.	>= 8 characters
SNMP Secret  Set by operators	Used to authenticate Crypto Officers accessing SNMP management interface	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	

<sup>1</sup> Entropy is loaded externally. The minimum length of the entropy field is 256 bits. Assuming that the entropy source provides full entropy, the module receives 256 bits of entropy.

<sup>2</sup> Public keys are not considered to be CSPs.

<sup>3</sup> SSH and TLS HMAC and AES keys can be used in key-wrapping.

<sup>4</sup> Input or output for all CSPs is electronic.

<sup>5</sup> Zeroization is performed using “security-reset” command.

## 7 Self Tests

The module runs a set of self-tests on power-up. If one of the self-tests fails, the module transitions into an error state where all data output and cryptographic operations are disabled.

The module runs power-up self-tests for the following algorithms:

**Table 8.1: Power-up Self-Tests**

Library/Area	Test
Firmware Integrity Power-up Self Test	Firmware integrity test is performed using MD5 (128-bit) verification.
Power-up Self Test for A10 Networks SSL FIPS Library	<p>For the SSL FIPS Library, tests performed are:</p> <ol style="list-style-type: none"> <li>1. AES (with separate encryption and decryption and indicated key sizes)               <ol style="list-style-type: none"> <li>a. CBC, ECB (128-bit)</li> <li>b. GCM (256-bit)</li> </ol> </li> <li>2. SHA               <ol style="list-style-type: none"> <li>a. SHA-1</li> </ol> </li> <li>3. HMAC               <ol style="list-style-type: none"> <li>a. HMAC-SHA-1</li> <li>b. HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512</li> </ol> </li> <li>4. SP800-90A DRBG KAT               <ol style="list-style-type: none"> <li>a. CTR_DRBG: AES</li> </ol> </li> <li>5. RSA KAT (2048-bit key, using SHA-256)</li> <li>6. ECDSA Pairwise Consistency Test (sign/verify) using P-224, P-256, K-233 and SHA-512</li> <li>7. KAS-FFC-SSC Primitive “Z” Computation KAT per implementation guidance using 2048-bit key</li> <li>8. KAS-ECC-SSC Primitive “Z” Computation KAT per implementation guidance using P-256</li> <li>9. DSA Pairwise Consistency Test (sign/verify) with 2048-bit key and using SHA-384</li> <li>10. KDF KAT               <ol style="list-style-type: none"> <li>a. KDF-135-SNMP</li> <li>b. KDF-135-TLS</li> <li>c. KDF-135-SSH</li> <li>d. KDF-135-IPsec</li> </ol> </li> </ol>

Library/Area	Test
Power-up Self Test for A10 Networks Data Plane FIPS Library 1 and 2	<p>For the Data Plane FIPS Libraries, tests performed are:</p> <ol style="list-style-type: none"> <li>1. AES (with separate encryption and decryption and indicated key sizes) <ol style="list-style-type: none"> <li>a. CBC (128-bit)</li> <li>b. GCM (256-bit)</li> </ol> </li> <li>2. SHA <ol style="list-style-type: none"> <li>a. SHA-1,</li> <li>b. SHA-256, SHA-512</li> </ol> </li> <li>3. HMAC <ol style="list-style-type: none"> <li>a. HMAC-SHA-1</li> <li>b. HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512</li> </ol> </li> <li>4. RSA KAT (2048-bit key, using SHA-256)</li> <li>5. ECDSA Pairwise Consistency Test (sign/verify) using P-256 and SHA-512</li> <li>6. KAS-ECC-SSC Primitive “Z” Computation KAT per implementation guidance using P-256 and P-384</li> </ol>
Power-up Self Test for A10 Networks Data Plane FIPS Software Library	<p>For the Data Plane FIPS Software Library, tests performed are:</p> <ol style="list-style-type: none"> <li>1. SP800-90A DRBG KAT <ol style="list-style-type: none"> <li>a. CTR_DRBG: AES</li> </ol> </li> <li>2. KDF KAT <ol style="list-style-type: none"> <li>a. KDF-135-TLS</li> </ol> </li> </ol>
Power-up Self Test for A10 Networks IPsec FIPS Library	<p>For the IPsec FIPS Library, tests performed are:</p> <ol style="list-style-type: none"> <li>1. AES (with encryption and decryption and indicated key sizes) <ol style="list-style-type: none"> <li>a. CBC (128, 192, 256-bit)</li> </ol> </li> <li>2. SHA <ol style="list-style-type: none"> <li>a. SHA-1</li> <li>b. SHA-256</li> <li>c. SHA-384</li> <li>d. SHA-512</li> </ol> </li> <li>3. HMAC <ol style="list-style-type: none"> <li>a. HMAC-SHA-1</li> <li>b. HMAC-SHA-256</li> <li>c. HMAC-SHA-384</li> <li>d. HMAC-SHA-512</li> </ol> </li> </ol>

During the module operation the following conditional self-tests are performed:

**Table 8.2: Conditional Self-Tests**

<b>Library/Area</b>	<b>Condition</b>	<b>Test</b>
Firmware Update	Firmware Load	Firmware Load Test using ECDSA with P-256 and SHA-256
Conditional Self Test for A10 Networks SSL FIPS Library	Random Number Generation /DRBG	Continuous RNG Test
	RSA	Pairwise Consistency Test
	ECDSA	Pairwise Consistency Test
	DSA	Pairwise Consistency Test
	DH Private/Public Key Validation	DH Private/Public Key Validation tests as per SP800-56Ar3 including FFC Full Public-Key Validation Routine
	ECDH Private/Public Key Validation	ECDH Private/Public Key Validation tests as per SP800-56Ar3 including ECC Full Public-Key Validation Routine
	DRBG Health Test	Performed per SP 800-90A Section 11.3
Conditional Self Test for A10 Networks Data Plane FIPS Library 1 and 2	ECDH Private/Public Key Validation	ECDH Private/Public Key Validation tests as per SP800-56Ar3 including ECC Full Public-Key Validation Routine
Conditional Self Test for A10 Networks Data Plane FIPS Software Library	Random Number Generation /DRBG	Continuous RNG Test
	DRBG Health Test	Performed per SP 800-90A Section 11.3

## 8 Physical Security

The module consists of production-grade components enclosed in a metal enclosure. The enclosure is opaque within the visible spectrum. Sealed containers are used during the shipping of the module. The integrity of the firmware is protected.

The module is protected by tamper evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements. The tamper evident labels are applied at the factory to provide evidence of tampering if a panel is removed.

The Crypto Officer must note the locations of the tamper evidence labels upon receipt of the module. The Crypto Officer must check the integrity of the tamper evident labels periodically thereafter. Upon discovery of tampering the Crypto Officer must immediately disable the module and return the module to the manufacturer.

## 9 Secure Operation

### *9.1 Approved Mode of Operation*

The module is intended to always operate in the Approved Mode of Operation. Module documentation provides detailed setup procedures and guidance for the users and administrators.

Crypto Officer must execute the following command to enable the approved mode of operation

- system fips enable

Crypto Officer must change its password during the installation.

Configuring any of the following features causes the module to operate in the Non-Approved Mode of Operation.

- RADIUS for administrator authentication
- TLS 1.3
- GCM for IPsec
- “system fips disable” configuration command

Module users and administrators shall keep all authentication data confidential and shall not allow unauthorized access to the module.

## 10 References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications

<b>Reference</b>	<b>Specification</b>
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions