



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***. 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*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



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: 2050712
Solicitation Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules
Proc Type: Central Purchase Order

Solicitation Closes	Solicitation Response	Version
2026-09-22 13:30	SR 0708 ESR09212600000002668	1

VENDOR
000000224557
SAITECH INC

Solicitation Number: CRFQ 0708 ABC2700000001
Total Bid: 25860
Response Date: 2026-09-21
Response Time: 19:13:33
Comments:

FOR INFORMATION CONTACT THE BUYER
James W Atkins
(304) 558-0094
james.w.atkins@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	Firewalls	2.00000	EA	12800.000000	25600.00

Comm Code	Manufacturer	Specification	Model #
43222501			

Commodity Line Comments:

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	1U Rack Mount Shelf	2.00000	EA	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43211600			

Commodity Line Comments:

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	SFP+ Transceiver Module	4.00000	EA	65.000000	260.00

Comm Code	Manufacturer	Specification	Model #
43211600			

Commodity Line Comments:

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

Header 10

List View

General Information [Contact](#) [Default Values](#) [Discount](#) [Document Information](#) [Clarification Request](#)

Procurement Folder: 2050712

Procurement Type: Central Purchase Order

Vendor ID: 000000224557

Legal Name: SAITECH INC

Alias/DBA:

Total Bid: \$25,860.00

Response Date: 09/21/2026

Response Time: 19:13

Responded By User ID: Aarti

First Name: Aarti

Last Name: K

Email: service@shopsaitech.com

Phone: 5104400256

SO Doc Code: CRFQ

SO Dept: 0708

SO Doc ID: ABC2700000001

Published Date: 9/14/26

Close Date: 9/22/26

Close Time: 13:30

Status: Closed

Solicitation Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

Total of Header Attachments: 10

Total of All Attachments: 10



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: 2050712			Reason for Modification:
Doc Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules			
Proc Type: Central Purchase Order			
Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-31	2026-09-22 13:30	CRFQ 0708 ABC2700000001	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 : Saitech Inc
Address : 42640 Christy Street, Fremont, CA 94538
Street : 42640 Christy Street
City : Fremont
State : CA **Country :** US **Zip :** 94538
Principal Contact : Ernesto Juarez
Vendor Contact Phone: 510-440-0256 **Extension:** 315

FOR INFORMATION CONTACT THE BUYER

James W Atkins
(304) 558-0094
james.w.atkins@wv.gov

Vendor Signature X *Ernesto Juarez* **FEIN#** 75-300-4589 **DATE** 9/21/2026

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 Alcohol Beverage and Control Administration to establish a contract for the one time purchase of Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules per the attached specifications and terms and conditions

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Firewalls	2.00000	EA	\$ 12,800.00	\$ 25,600.00

Comm Code	Manufacturer	Specification	Model #
43222501	Fortinet	FortiGate-120G Hardware plus 5 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) FG-120G-BDL-950-60	

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	1U Rack Mount Shelf	2.00000	EA	FG-120G-BDL-950-60 - Firewall comes with rack mount	

Comm Code	Manufacturer	Specification	Model #
43211600		FG-120G-BDL-950-60 - Firewall comes with rack mount	

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	SFP+ Transceiver Module	4.00000	EA	\$ 65.00	\$ 260.00

Comm Code	Manufacturer	Specification	Model #
43211600	Fortinet	10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0C to 70C, for systems with SFP+ slots	FN-TRAN-SFP+SR

Extended Description:
 Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

SCHEDULE OF EVENTS		
Line	Event	Event Date
1	Questions Due by 2pm EST	2026-09-08

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:

Submit Questions to:

2019 Washington Street, East Charleston, WV 25305

Fax: (304) 558-3970

Email:

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:

SOLICITATION NO.:

BID OPENING DATE:

BID OPENING TIME:

FAX NUMBER:

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 confirmation 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:

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.

[] 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 § 5A-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/vrc/Venpref.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/vrc/Venpref.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 _____. 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 _____ 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)

☐ **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.

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

☐ **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:

☐ the contract will continue for _____ years;

☐ 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).

☐ **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.

☐ **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.

☐ **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.

☐ **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.

☐ **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.

☐ **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.

☐ **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 a 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 form 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: _____ per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ 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.

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 5G-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, permitting, 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, permitting, 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.

☐ 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.

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 § 5A-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 § 5A-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 hearth, 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 § 5A-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) _____

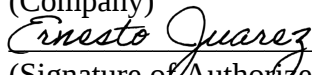
(Address) _____

(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)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.:

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | |
|---|--|
| ☐ Addendum No. 1 | ☐ Addendum No. 6 |
| ☐ Addendum No. 2 | ☐ Addendum No. 7 |
| ☐ Addendum No. 3 | ☐ Addendum No. 8 |
| ☐ Addendum No. 4 | ☐ Addendum No. 9 |
| ☐ Addendum No. 5 | ☐ Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Company



Authorized Signature

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

REQUEST FOR QUOTATION
Switches, Transceiver Modules, Power Cords, Twinaxial Cables, SaaS Support and Subscription

SPECIFICATIONS

1. PURPOSE AND SCOPE: The West Virginia Purchasing Division is soliciting bids on behalf of Alcohol Beverage and Control Administration to establish a contract for the one time purchase of 6 Extreme Networks Ethernet Switches or equal, 4 Extreme Networks Transceiver modules or equal, 6 Power Cords, 4 Twinaxial cables, and 6 ExtremeCloud IQ Pilot SaaS Subscription and EW SaaS support - 3 years or equal.

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 “Contract Item” means switches, transceiver modules and technical support and maintenance as more fully described by these specifications.

2.2 “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.

2.3 “Solicitation” means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.4 “PoE” means Power over Ethernet.

2.5 “GbE” means Gigabit Ethernet.

2.6 “SFP” means Small Form-Factor Pluggable.

2.7 “GBIC” means Gigabit Interface Converter

2.8 “GBps” means Gigabit per second.

2.9 “Gigabit” means 1,000 megabits per second.

2.10 “GHz” means Gigahertz.

3. GENERAL REQUIREMENTS:

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

3.1.1 Extreme Networks 48x10/100/1000Base-T Ethernet Switch POE+(PN 5320-48P-8XE) or Equal (Qty 6)

REQUEST FOR QUOTATION

Switches, Transceiver Modules, Power Cords, Twinaxial Cables, SaaS Support and Subscription

- [illegible]

REQUEST FOR QUOTATION

Switches, Transceiver Modules, Power Cords, Twinaxial Cables, SaaS Support and Subscription

4. CONTRACT AWARD:

4.1 Contract Award: The Contract is intended to provide Agencies 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.

4.2 Pricing Page: Vendor should complete the Pricing Page by filling in the unit price and total prices for each line item. 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.

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 or notice to proceed. Vendor shall deliver the Contract Items within 60 working days after receiving a purchase order or notice to proceed. Contract Items must be delivered to Agency at 900 Pennsylvania Ave. 4th floor, Charleston, WV 25302.

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 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.

REQUEST FOR QUOTATION

Switches, Transceiver Modules, Power Cords, Twinaxial Cables, SaaS Support and Subscription

If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All 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.

REQUEST FOR QUOTATION
Switches, Transceiver Modules, Power Cords, Twinaxial Cables, SaaS Support and Subscription

Exhibit A

<u>Item</u>	<u>Specification</u>	<u>Description</u>	<u>Brand Bid</u>	<u>Model Bid</u>	<u>UM</u>	<u>Unit Cost</u>	<u>Qty</u>	<u>Extended Cost</u>
1.	3.1.1	Extreme Networks 48x10/100/1000Base-T Ethernet Switch POE+ or Equal (PN 5320-48P-8XE)			Each	\$	X6	\$
2.	3.1.2	Extreme Networks - SFP+ transceiver module - 10GigE - 10G-SR or Equal (PN 10301)			Each	\$	X4	\$
3.	3.1.3	Power Cord, 15A, USA, NEMA 5-15, IEC320-C15 or Equal (PN 10099)			Each	\$	X6	\$
4.	3.1.4	Extreme Networks 1M SFP+ Twinaxial Cable (PN 10304)			Each	\$	X4	\$
5.	3.1.5	ExtremeCloud IQ Pilot SaaS Subscription and EW SaaS Support - 3 years or Equal (PN XIQ-PIL-S-C-EW-3YR)			Each	\$	X6	\$
Total Bid Amount								\$

Kindly check the filled addendum

(PRICING PAGE MUST BE COMPLETED AND SUBMITTED WITH BID)

**Vendor Name
(PRINT)**

Saitech Inc

Vendor Signature



Email Address

ernesto@esaitech.com



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: 2050712			Reason for Modification:
Doc Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules			
Proc Type: Central Purchase Order			
Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-31	2026-09-22 13:30	CRFQ 0708 ABC2700000001	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 : Saitech Inc.
Address : 42640 Christy Street, Fremont, CA 94538
Street : 42640 Christy Street
City : Fremont
State : California **Country :** US **Zip :** 94538
Principal Contact : Ernesto Juarez
Vendor Contact Phone: 510-440-0256 **Extension:** 307

FOR INFORMATION CONTACT THE BUYER

James W Atkins
(304) 558-0094
james.w.atkins@wv.gov

Vendor Signature X *Ernesto Juarez* **FEIN#** 753004589 **DATE** 9/21/2026

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 Alcohol Beverage and Control Administration to establish a contract for the one time purchase of Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules per the attached specifications and terms and conditions

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Firewalls	2.00000	EA	\$ 12,800.00	\$ 25,600.00

Comm Code	Manufacturer	Specification	Model #
43222501		FortiGate-120G Hardware plus 5 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) FG-120G-BDL-950-60	

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	1U Rack Mount Shelf	2.00000	EA	FG-120G-BDL-950-60 - Firewall comes with rack mount	

Comm Code	Manufacturer	Specification	Model #
43211600	Fortinet	FG-120G-BDL-950-60 - Firewall comes with rack mount	

Extended Description:

Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO		SHIP TO	
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US		ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	SFP+ Transceiver Module	4.00000	EA	\$ 65.00	\$ 260.00

Comm Code	Manufacturer	Specification	Model #
43211600	Fortinet	10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0C to 70C, for systems with SFP+ slots	FN-TRAN-SFP+SR

Extended Description:
 Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

SCHEDULE OF EVENTS		
<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions Due by 2pm EST	2026-09-08

	Document Phase	Document Description	Page 4
ABC2700000001	Final	Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SOLICITATION NUMBER: CRFQ ABS27*01

Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as (“Solicitation”) to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☐ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☒ Correction of error
- ☐ Other

Description of Modification to Solicitation:

1. Correct Specifications

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of Alcohol Beverage and Control Administration to establish a contract for the one-time purchase of 2 Palo Alto Networks Enterprise Firewall (PAN-PA-550), 2 Palo Alto Networks network device rack mount shelf - 1U and 4 Palo Alto Networks - SFP+ transceiver module - 10GbE.
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 **"Contract Item"** means firewalls, rack mounting shelves and transceiver modules as more fully described by these specifications.
 - 2.2 **"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.
 - 2.3 **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
 - 2.4 **"GB"** means gigabyte which is a multiple of the unit byte for digital information.
 - 2.5 **"Gbps"** means gigabits per second, a data transfer speed measurement for high-speed networks such as gigabit ethernet.
 - 2.6 **"Mbps"** means megabits per second which is a unit of measurement for bandwidth and throughput on a network.
 - 2.7 **"OEM"** means original equipment manufacturer.
 - 2.8 **"RMA"** means Return Merchandise Authorization, which is a process that allows customers to return a product to a seller for a refund, replacement, or repair, typically within a warranty period
 - 2.9 **"VLAN"** means Virtual Local Area Network.
 - 2.10 **"DNS"** means Domain Name Servers which is the Internet's system for converting alphabetic domain names into numerical IP addresses.
 - 2.11 **"DMZ"** means a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually the internet.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

2.12 "SQL" means Structured Query Language which is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).

2.13 "SFP+" means Enhanced Small Form-Factor Pluggable which is a compact, hot-pluggable network interface module that is used for data communications.

2.14 "ML" means Machine Learning which is subset of artificial intelligence (AI) that focuses on algorithms that enable computers to learn from and make predictions based on data without being explicitly programmed for each task.

3. GENERAL REQUIREMENTS:

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

3.1.1 Palo Alto Networks Next-Generation Firewall (PAN-PA-550) or Equal (Qty 2)

3.1.1.1 System must have embedded machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention.

3.1.1.2 System must identify applications and users across all ports, regardless of evasion tactics or encryption, allowing for granular policy control.

3.1.1.3 System must receive software updates from designated servers located in the US.

3.1.1.4 System must support high availability with active/active and active/passive modes.

3.1.1.5 System must support centralized administration with Panorama® network security management or equal.

3.1.1.6 System must have audit logs that document security-related events.

3.1.1.7 System must have a minimum Firewall Throughput of 6.5 Gbps.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

3.1.1.8 System must be capable of locking administrator accounts after no more than three (3) unsuccessful attempts to logon with an invalid password.

3.1.1.9 System must be configurable to require multi-factor authentication for remote device management.

3.1.1.10 Vendor must be an authorized reseller of all equipment bid. All equipment must be new and genuine; refurbished or gray market equipment will not be accepted.

3.1.2 Palo Alto Networks network device rack mount shelf - 1U (PAN-1RU-4POST-RACK-11) or Equal (Qty 2)

3.1.2.1 Shelf must be four post rack-mountable design with a height of one rack unit.

3.1.2.2 Shelf must be compatible with PAN-PA-550 firewall or equal.

3.1.3 Palo Alto Networks - SFP+ transceiver module - 10GbE (PAN-SFP-PLUS-SR) or Equal (Qty 4)

3.1.3.1 Transceiver modules must work with 10 Gigabit Ethernet data link protocol, enabling a data transfer rate of 10 Gb/s.

3.1.3.2 Modules must have an Ethernet 10GBase-SR interface.

3.1.3.3 SFP+ modules must be compatible with PAN-PA-550 firewall or equal.

3.2 Alternate 'or Equal' Submission

3.2.1 Vendor submitting an alternate brand must include manufacturer part/model numbers with bid pricing. Vendors submitting an alternate brand of firewall must provide technical documentation demonstrating that the proposed equipment meets or exceeds all mandatory functional specifications in Section 3.1.1. For alternate firewall submissions, the vendor is solely responsible for including all necessary security software subscriptions (including, but not limited to, WildFire, Advanced Threat Prevention, and

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

management capabilities equivalent to those provided by the state's enterprise agreement) for the duration of the hardware life. For any alternate accessory items bid (e.g., non-Palo Alto SFP+ transceiver modules), the vendor must provide documentation confirming hardware compatibility and full interoperability with the firewall appliances being provided. Vendor must include alternate brand information with alternative part numbers on the Pricing Sheet.

3.2.2 If Vendor is submitting an "or Equal" product, this information must be provided at the time of submitting bid response. Any documentation supporting such should be submitted with bid response. This information may be required before award of contract.

3.2.3 Vendor will assume any costs related to any required installation of new software, hardware and/or training of the alternate submission provide as part of this agreement.

4. CONTRACT AWARD:

4.1 Contract Award: The Contract is intended to provide Agencies 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.

4.2 Pricing Page: Vendor should complete the Pricing Page by filling in the unit price and total prices for each line item. 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.

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.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

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 or notice to proceed. Vendor shall deliver the Contract Items within 60 working days after receiving a purchase order or notice to proceed. Contract Items must be delivered to Agency at 900 Pennsylvania Ave. 4th floor, Charleston, WV 25302.

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 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. All 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.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

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.

REQUEST FOR QUOTATION
Next-Gen Firewalls, Rack Mounting Shelves and SFP+ Transceiver Modules

Exhibit A

<u>Item</u>	<u>Specifi cation</u>	<u>Description</u>	<u>Brand Bid</u>	<u>Model Bid</u>	<u>UM</u>	<u>Unit Cost</u>	<u>Qty</u>	<u>Extended Cost</u>
1.	3.1.1	Palo Alto PAN-PA-550 Next-Gen Firewall or Equal	<u>Fortinet</u>	<u>FG-120G-BDL-950-60</u>	Each	<u>\$ 12,800.00</u>	2	<u>\$ 25,600.00</u>
2.	3.1.2	1U Rack Mount Shelf (PAN-1RU-4POST-RACK-11) or Equal	<u>Fortinet</u>		Each	<u>\$</u>	2	<u>\$</u> Pricing included in Firewall
3.	3.1.3	SFP+ Transceiver Module 10GbE (PAN-SFP-PLUS-SR) or Equal	<u>Forinet</u>	<u>FN-TRAN-SFP+SR</u>	Each	<u>\$ 65.00</u>	4	<u>\$ 260.00</u>
TOTAL BID AMOUNT								<u>\$ 25,860.00</u>

Vendor Name (PRINT)	<u>Saitech Inc.</u>
Vendor Signature	<u><i>Ernesto Suarez</i></u>
Contact Phone #	<u>510-440-0256</u>
Email Address	<u>ernesto@esaitech.com</u>

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ ABC27*01

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

☒ Addendum No. 1	☐ Addendum No. 6
☒ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Saitech Inc.

Company

Ernesto Juarez

Authorized Signature

9/21/2026

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.



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: 2050712			Reason for Modification: Addendum No. 1 Correct the Specifications
Doc Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules			
Proc Type: Central Purchase Order			
Date Issued	Solicitation Closes	Solicitation No	
2026-08-31	2026-09-22 13:30	CRFQ 0708 ABC2700000001	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:
Vendor Name : Saitech Inc.
Address : 42640 Christy Street, Fremont, CA 94538
Street : 42640 Christy Street
City : Fremont
State : California **Country :** USA **Zip :** 94538
Principal Contact : Ernesto Juarez
Vendor Contact Phone: 510-440-0256 **Extension:** 307

FOR INFORMATION CONTACT THE BUYER

James W Atkins
(304) 558-0094
james.w.atkins@wv.gov

Vendor Signature X *Ernesto Juarez* **FEIN#** 753004589 **DATE** 9/21/2026

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

ADDITIONAL INFORMATION
ADDENDUM NO. 1
Addendum No. 1 issued to publish and distribute the attached information to the Vendor Community
The West Virginia Purchasing Division is soliciting bids on behalf of Alcohol Beverage and Control Administration to establish a contract for the one time purchase of Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules per the attached specifications and terms and conditions

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Firewalls	2.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222501		Find filled addendum 2	

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	1U Rack Mount Shelf	2.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43211600		Find filled addendum 2	

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO		SHIP TO	
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US		ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	SFP+ Transceiver Module	4.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43211600	Find filled addendum 2		

Extended Description:
 Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

SCHEDULE OF EVENTS		
<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions Due by 2pm EST	2026-09-08

	Document Phase	Document Description	Page 4
ABC2700000001	Final	Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules	

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: 2050712

Doc Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

Reason for Modification:

Addendum No. 2

Vendor questions and Responses

Proc Type: Central Purchase Order

Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-31	2026-09-22 13:30	CRFQ 0708 ABC2700000001	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : Saitech Inc.

Address : 42640 Christy Street, Fremont, CA 94538

Street : 42640 Christy Street

City : Fremont

State : California

Country : USA

Zip : 94538

Principal Contact : Ernesto Juarez

Vendor Contact Phone: 510-440-0256

Extension: 307

FOR INFORMATION CONTACT THE BUYER

James W Atkins
(304) 558-0094
james.w.atkins@wv.gov

**Vendor
Signature X**

Ernesto Juarez

FEIN# 753004589

DATE 9/21/2026

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

ADDITIONAL INFORMATION
ADDENDUM NO. 2
Addendum No. 2 issued to publish and distribute the attached information to the Vendor Community
ADDENDUM NO. 1
Addendum No. 1 issued to publish and distribute the attached information to the Vendor Community
The West Virginia Purchasing Division is soliciting bids on behalf of Alcohol Beverage and Control Administration to establish a contract for the one time purchase of Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules per the attached specifications and terms and conditions

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Firewalls	2.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43222501	Find filled Addendum 2		

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	1U Rack Mount Shelf	2.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43211600	Find filled Addendum 2		

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	SFP+ Transceiver Module	4.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43211600	Find filled Addendum 2		

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

SCHEDULE OF EVENTS		
<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions Due by 2pm EST	2026-09-08

SOLICITATION NUMBER: CRFQ ABS27*01

Addendum Number: 2

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☐ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☒ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☐ Other

Description of Modification to Solicitation:

1. Vendor Questions and responses

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

Q1. Is this a new design or a rip-and-replace? What products do you currently have in place? Do you have specs for the firewall and SFPs? This will help us to determine what products to offer.

A: This is a hardware refresh. The state will not be disclosing details regarding existing internal network models or active configurations. Technical requirements for the firewalls and transceiver modules are fully detailed in Section 3.1 of the RFQ specifications.

Q2. The spec asks for central management like Panorama, but Panorama only manages Palo Alto firewalls - with any other brand you would be getting a different management system either way. With Check Point, a pair of firewalls can be managed from the appliances themselves at no added cost, or from a separate management system we would price into the bid. Which do you need?

A: If submitting an alternate brand, the vendor must include centralized management software/capabilities equivalent to Panorama (capable of unified logging, template-based policy distribution, and multi-device administration) priced into the bid, in accordance with Section 3.1.1.5 and Section 3.2.1. Managing appliances individually without a centralized management platform is not acceptable.

Q3. The spec asks for both active/active and active/passive. Active/active is a highly unusual setup for a pair of firewalls - is that something you are intending to run, or will you be using active/standby?

A: The requirement specifies that the hardware/operating system platform must support both Active/Active and Active/Passive High Availability modes to meet state standards. The primary intended operational deployment is Active/Passive (active/standby).

Q4. It says to include the security software "for the duration of the hardware life," but does not say how many years, and there is no line on the pricing page to put it on.

A: For any alternate "or Equal" firewall submission, software subscription pricing must cover a 5-year lifecycle. All subscription costs must be included in the unit/extended pricing provided on Exhibit A (Pricing Page) under Item 1 for the firewall hardware, as outlined in Section 3.2.1. Separate line-item software fees will not be accepted.

Q5. Which address should this ship to? The spec says 900 Pennsylvania Avenue in Charleston, wvOASIS says the ABCA warehouse in Nitro.

A: Please deliver to the official RFQ delivery address specified in Section 6.1: West Virginia Alcohol Beverage Control Administration, 900 Pennsylvania Ave., 4th Floor, Charleston, WV 25302.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ ABC27*01

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

☒ Addendum No. 1	☐ Addendum No. 6
☒ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Saitech Inc.

Company

Ernesto Juarez

Authorized Signature

9/21/2026

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.



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: 2050712			Reason for Modification: Addendum No. 2 Vendor questions and Responses
Doc Description: Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules			
Proc Type: Central Purchase Order			
Date Issued	Solicitation Closes	Solicitation No	Version
2026-09-14	2026-09-22 13:30	CRFQ 0708 ABC2700000001	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:
Vendor Name : Saitech Inc.
Address : 42640 Christy Street, Fremont, CA 94538
Street : 42640 Christy Street
City : Fremont
State : California **Country :** USA **Zip :** 94538
Principal Contact : Ernesto Juarez
Vendor Contact Phone: 510-440-0256 **Extension:** 307

FOR INFORMATION CONTACT THE BUYER

James W Atkins
(304) 558-0094
james.w.atkins@wv.gov

Vendor Signature X *Ernesto Juarez* **FEIN#** 753004589 **DATE** 9/21/2026

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

ADDITIONAL INFORMATION
ADDENDUM NO. 2
Addendum No. 2 issued to publish and distribute the attached information to the Vendor Community
ADDENDUM NO. 1
Addendum No. 1 issued to publish and distribute the attached information to the Vendor Community
The West Virginia Purchasing Division is soliciting bids on behalf of Alcohol Beverage and Control Administration to establish a contract for the one time purchase of Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules per the attached specifications and terms and conditions

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Firewalls	2.00000	EA	\$ 12,800.00	\$ 25,600.00

Comm Code	Manufacturer	Specification	Model #
43222501	Fortinet	FortiGate-120G Hardware plus 5 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) FG-120G-BDL-950-60	

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO	SHIP TO
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US	ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	1U Rack Mount Shelf	2.00000	EA	FG-120G-BDL-950-60 - Firewall comes with rack mount	

Comm Code	Manufacturer	Specification	Model #
43211600	Fortinet	FG-120G-BDL-950-60 - Firewall comes with rack mount	

Extended Description:
Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

INVOICE TO			SHIP TO		
ALCOHOL BEVERAGE CONTROL COMMISSION 4TH FLOOR 900 PENNSYLVANIA AVE CHARLESTON WV US			ABCA WAREHOUSE HUB INDUSTRIAL PARK 97 INDEPENDENT AVE NITRO WV US		

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	SFP+ Transceiver Module	4.00000	EA	\$ 65.00	\$ 260.00

Comm Code	Manufacturer	Specification	Model #
43211600	Fortinet	FN-TRAN-SFP+SR 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0C to 70C, for systems with SFP+ slots	

Extended Description:
 Next-Gen Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions Due by 2pm EST	2026-09-08

	Document Phase	Document Description	Page 4
ABC2700000001	Final	Firewalls, Rack Mounting Shelves & SFP+ Transceiver Modules	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SOLUTION BRIEF

Enable Deep Visibility for Applications, Users, and Devices with FortiGate Next-Generation Firewalls

Executive Summary

Traditional firewalls are typically only able to allow or block connections based on port and protocol. However, network access is now dynamic and contextual, operating under zero-trust principles. In addition, the modern enterprise is hybrid, spanning on-premises data centers, public clouds, corporate branches and campuses, as well as remote sites. Today's IT teams require deep visibility into applications, users, and devices to defend enterprise networks against cyberthreats across the entire environment, but this is often a challenge.

Compounding the visibility problem is that almost all internet traffic is now encrypted. Enterprises are finding large swathes of network blind spots as they shift from expensive hub-and-spoke architectures to distributed models with direct internet access at sites. Malicious actors can exploit these network gaps, hiding threats in encrypted traffic.

FortiGate Next-Generation Firewalls (NGFWs) deliver the visibility into encrypted traffic and user, application, and device activity necessary to build contextual, evolving network and security policies that secure digital transformation. FortiGate NGFWs can identify and control all users, applications, and devices on the network with advanced data collection and analysis techniques. As the key component of the Fortinet Security Fabric, FortiGate NGFWs integrate this visibility and protection across IT domains, covering the entire network infrastructure.

Application Control

The FortiGuard Application Control Service attaches to FortiGate NGFWs and quickly identifies known and unknown applications traversing the network. It enables easy creation of policies to allow, deny, and restrict access to applications, certain functions within applications, and application categories.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38



Over 95% of internet traffic is now encrypted.¹

FortiGate NGFWs can identify applications not only by matching their port and protocol but also by the application signature, heuristic behaviors, and other identifying indicators. With a combined look at application signatures and internet service database (ISDB) applications, FortiGate can set over 4,200 application control rules. Below are some ways FortiGate identifies applications beyond Layers 3 and 4.

Application signatures: Allowed network traffic is assigned a signature based on transaction characteristics and whether the application port is default or nonstandard. Traffic is scanned for threats and deep analysis.

Encryption: If FortiGate detects encryption such as secure sockets layer (SSL)/transport layer security (TLS), Hypertext Transfer Protocol Secure (HTTPS), or secure shell (SSH), and a decryption policy rule is in place, the session is decrypted, and application signatures are applied again on the decrypted flow.

Decoders: If the application protocol is known, it is then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol. Decoders validate that the traffic conforms to the protocol specification and provide support for network address translation (NAT) traversal and opening dynamic pinholes for applications such as session initiation protocol (SIP) and file transfer protocol (FTP).

Heuristics: FortiGate heuristic analysis uses behavioral analytics to determine the identity of evasive applications. This includes applications that use port 80, port 443, or engage in port hopping—for example, Voice over Internet Protocol (VoIP), collaboration, and peer-to-peer (P2P) applications that cannot be identified through advanced signature and protocol analysis.

If the FortiGate is unable to identify an application based on its signature, then it will rely on behavioral characteristics through heuristics, classifying the previously unknown application into an existing application group and applying dynamic filters or policy-based forwarding to achieve the desired result.

Identifying applications can provide meaningful context about the network. FortiGate can reveal information about the inherent function, application ports, protocol, technology, and behavioral characteristics of the application, which enables IT teams to make confident and informed access policies. Once the team understands how an application is being used on the network, a variety of policies and responses beyond allow and block can be applied.

FortiGuard Application Control also allows organizations to build policies and control functions within each application. Examples include:

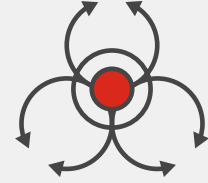
- Allowing access to Facebook but blocking Facebook Messenger file transfers
- Letting users access Gmail but disabling Google Chat
- Blocking file uploads to Dropbox, Box, or Google Drive
- Filtering unwanted video categories from being viewed on YouTube

FortiOS, the FortiGate operating system, provides extensive visibility into application usage in real time, as well as trends over time through views, visualizations, and reports. Application control keeps malicious, risky, and unwanted applications out of the network through control points at the perimeter, in the data center, and internally between network segments.

User Identification

Identifying users beyond their IP addresses is another critical part of enterprise security. FortiOS can identify users based on a variety of sources and methods, such as Microsoft Active Directory (AD), LDAP servers, syslog, port mapping, and XFF headers.

FortiGate user identification provides better visibility into network activity and detection against malicious or damaging behavior. FortiGate user identification identifies users across operating systems in any location, providing improved visibility into application usage based on users. This gives IT teams a more relevant picture of network activity.



A Gartner survey shows rising concern of AI-enhanced malicious attacks.

The power of user identification becomes evident when an unfamiliar application is found on the network. Whether using FortiView or application control logs, security teams can discern:

- The application
- The user
- Bandwidth and session consumption
- Source and destination of the application traffic
- Any associated threats

User mapping

FortiGate can create profiles of users on the network and match usernames to the IP addresses in received packets. User information can be mapped to security policies for safer network usage, reserving application access only for those who have a business need. User mapping can enable one set of rules or policies for less risky applications like Salesforce or PowerPoint while at the same time setting more stringent policies for sensitive applications like pen-testing tools or remote desktop controllers.

Group mapping

Defining policy rules based on user groups can simplify IT management, as policies and rules are already in place and do not need to be reconfigured when adding new users to groups. FortiGate can apply these rules and group updates, supporting a variety of directory servers, including Microsoft AD, Novell eDirectory, and Sun ONE Directory Server. After enabling user identification and leveraging group mapping, security policies can be configured for specific users and groups. These include application categories and subcategories, underlying technologies, and application characteristics. Policy rules can be defined to safely enable applications based on users and groups of users, in either outbound or inbound directions.

Examples of user-based and group-based policies include:

- Tools like: SSH, Telnet, and FTP on standard ports are restricted to corporate IT
- Policies like:
 - Allow sales to access Salesforce and Microsoft 365
 - Allow all users to watch YouTube but block specific video categories

User identification helps shape policies that support and protect employees, guests, and other stakeholders. FortiGate can provide deep user insight and automate policy controls.

Device identification

While user identification provides user-based policy, and application identification provides app-based policy, device identification provides policy rules that are based on a device, regardless of changes to its IP address or location. By providing traceability for devices and associating network events with specific devices, device ID delivers context for how events relate to devices. It writes policies that are associated with devices instead of users, locations, or IP addresses, which can change over time. Device ID is important for security, decryption, quality of service (QoS), and authentication policies.

With FortiGate, advanced device policies and prioritization can be categorized by:

- Class, such as secure networked devices
- Critical devices, such as servers and medical devices
- Environmental devices, like badge readers, cameras, and fire alarms
- Internet-of-Things (IoT) devices, like smartwatches and other connected “smart” devices



SSL/TLS 1.3 decryption

Given that malware is regularly hidden in encrypted traffic, it's critical that encrypted traffic is examined. FortiGate NGFWs deliver SSL/TLS 1.3 decryption with no network slowdowns. Further, FortiGates can decrypt specific kinds of traffic and make exclusions based on sites or categories. With Fortinet's high-performance proprietary security processing units, there is no need to choose between security and performance.

Central and unified management

Centralized and unified management is the most critical capability of an HMF. If separate domains, such as corporate sites, public and private clouds, and remote workers, require protection via separate dashboards, then IT complexity increases while visibility is greatly reduced.

Centralized management coordinates and unifies disparate security domains into a single enterprise IT security solution—simple, unified, and automated protection that extends from corporate sites to the cloud and remote workers. And because different organizations have different requirements for managing their dispersed network firewalls, all form factors of the centralized management must be supported, including appliances, VMs, SaaS, and managed firewall services.

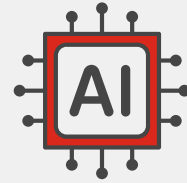
Centralized management also delivers enormous value in bringing network operations center (NOC) and security operations center (SOC) teams together using a single pane of glass to manage, monitor, and secure the entire attack surface.

FortiGuard AI-Powered Security Services

With over 8 million sensors deployed around the world, FortiGate NGFWs are able to leverage the latest global threat intelligence through FortiGuard AI-Powered Security Services. With real-time, comprehensive security updates, FortiGate can protect the entire network with multilayered security defenses such as URL and DNS filtering, anti-malware and inline sandboxing, as well as hardware-accelerated IPS for high-performance virtual patching. These cybersecurity services protect the enterprise from both known and previously unknown attacks. Independent testing from NetSecOpen² shows that FortiGate NGFWs are 99.98% effective against malicious exploits and evasions.

Conclusion

Identifying applications, users, and devices on the network is an important capability in managing and securing enterprise networks. FortiGate NGFWs are known for their advanced visibility and control over network traffic, as well as unparalleled performance. FortiGate defines and automates policies that ensure appropriate use, stop threats, and reduce the enterprise attack surface. Centralized and unified management integrates the FortiGate appliance with other security form factors, such as virtual firewalls, cloud-native firewalls, and Firewall-as-a-Service, to build a seamless security solution across the entire IT environment. The latest FortiGuard AI-Powered Security Services ensure up-to-date defenses from even the newest and most advanced attacks.



Gartner predicts 17% of total cyberattacks will involve generative AI by 2027.³

¹ ["HTTPS encryption on the web,"](#) Google Transparency Report, Google, accessed January 2, 2025.

² [Network Security Product Performance Testing: Fortinet FortiGate 601F NGFW,](#) NetSecOpen Certification, published February 1, 2024.

³ [Forecast: Information Security, Worldwide, 2022-2028, 2Q24 Update,](#) Gartner, August 24, 2024.

3.1.1.1 System must have embedded machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention.

Artificial Intelligence, Machine Learning Security with Deep Visibility FortiGate series next-generation firewalls (NGFW) combine artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats. Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, FortiGate NGFWs deliver secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

3.1.1.2 System must identify applications and users across all ports, regardless of evasion tactics or encryption, allowing for granular policy control.

1. **Application awareness with deep packet inspection (DPI):** FortiGates offer complete visibility into application-layer traffic. They identify specific apps and user activities regardless of port or protocol. This approach enables granular, zero-trust access control that aligns security enforcement with business intent.
2. **Intrusion prevention with stateful inspection:** An integrated intrusion prevention system (IPS) extends beyond basic firewall capabilities to identify and block network-based exploits targeting vulnerable systems. It helps detect malicious behavior in real-time and prevents attacks before they reach critical assets.
3. **AI-driven threat intelligence and malware protection:** FortiGates leverage AI-driven threat intelligence feeds to stay ahead of evolving cyberattack campaigns. They detect, classify, and block emerging threats faster and more accurately by correlating global indicators of compromise (IoCs) with live traffic.
4. **SSL/TLS inspection and packet filtering for encrypted traffic:** FortiGates can decrypt and inspect HTTPS tunnels to identify hidden threats that use encryption to bypass detection. This ensures complete visibility across encrypted sessions without compromising privacy or performance.
5. **Advanced malware and anomaly detection with AI analytics:** FortiGates use sandboxing and AI-based behavioral analytics to examine suspicious files and anomalies and counter malware. This proactive detection model identifies zero-day attacks before they can execute or spread laterally.

6. **User and device-based policy enforcement:** FortiGates integrate identity and device awareness into policy decisions, implementing controls based on user role, device type, and risk level. This enables dynamic, context-aware enforcement that supports zero-trust access across hybrid and remote environments.
7. **Scalable, high-performance architecture for future-proof networks:** FortiGates deliver high throughput and low latency even under heavy encrypted traffic. The scalable architecture supports secure operations across data centers, campuses, branches, and cloud environments without trade-offs in performance or protection.

3.1.1.3 System must receive software updates from designated servers located in the US.

This is easily set in the config.

config system fortiguard

set update-server-location usa

end

3.1.1.4 System must support high availability with active/active and active/passive modes.

High Availability Configurations Active-Active, Active-Passive, Clustering are all supported.

Here are reference links to the config for each

<https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/357558/ha-active-active-cluster-setup>

<https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/900885/ha-active-passive-cluster-setup>

<https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/599385/ha-virtual-cluster-setup>

3.1.1.5 System must support centralized administration with Panorama® network security management or equal.

System supports FortiManager Cloud which delivers all the functionality of Panorama security management. FortiManager Data sheet is attached

3.1.1.6 System must have audit logs that document security-related events.

FortiGate firewalls natively generate and deliver comprehensive audit logs that document security-related events. In the FortiOS ecosystem, these are categorized as **Security Logs** (which operate alongside the system management logs).

Whenever traffic hits your **FortiGate 120G cluster**, the hardware acceleration chips and software engines evaluate the packets against your security rules. If an event matches a security profile, an unalterable log entry is natively generated.

1. The Security-Related Event Categories

FortiGate breaks down security events into specific, granular sub-logs that you can monitor natively via the Web GUI under **Log & Report**:

- **Application Control Logs:** Identifies when an application bypasses standard port rules or attempts evasion tactics, logging the exact application signature matched (e.g., detecting BitTorrent over Port 80).
- **Intrusion Prevention (IPS) Logs:** Documents network exploits, brute-force patterns, and vulnerability scanning attempts blocked by the IPS engine.
- **AntiVirus / Sandbox Logs:** Records instances where a known malware string, trojan, or zero-day variant was detected and quarantined at the gateway.
- **Web Filtering & DNS Logs:** Logs blocked attempts to access malicious domains, command-and-control servers, or categories that violate your corporate security posture.
- **SSL/TLS Inspection Logs:** Documents details on certificate issues, untrusted connection rejections, or decryption events during Deep Packet Inspection.

2. Granular Policy Control Tracking

Security logs are explicitly bound to your **Firewall Policies**. When building a policy on the FortiGate, you have native, granular control over how security events are documented:

- **Log All Sessions vs. Security Events:** You can configure a policy to *only* generate a log entry when a security threat is actively triggered (reducing log volume), or log every single successful session connection for full visibility.
- **Packet Capture (PCAP):** For deep forensic auditing, you can natively toggle the firewall to automatically capture and attach the actual raw data packets of an IPS or malware attack directly to the log entry.

3.1.1.7 System must have a minimum Firewall Throughput of 6.5 Gbps.

FortiGate 120G far exceeds this.

System Performance and Capacity Firewall Throughput

(1518 / 512 / 64 byte UDP packets) 39 / 39 / 28 Gbps

Please see included data sheet

3.1.1.8 System must be capable of locking administrator accounts after no more than three (3) unsuccessful attempts to logon with an invalid password.

Yes FortiGates support this, here is the detail.

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be configured using the CLI.

A maximum of ten retry attempts can be configured, and the lockout period can be 1 to 2147483647 seconds (over 68 years). The higher the retry attempts, the higher the risk that someone might be able to guess the password.

To configure the lockout options:

```
config system global
```

```
    set admin-lockout-threshold <failed_attempts>
```

```
    set admin-lockout-duration <seconds>
```

```
end
```

Example:

To set the number of retry attempts to 1, and the lockout time to 5 minutes, enter the following commands:

```
config system global
```

```
    set admin-lockout-threshold 1
```

```
    set admin-lockout-duration 300
```

```
end
```

3.1.1.9 System must be configurable to require multi-factor authentication for remote device management.

Yes, FortiGate firewalls can absolutely be configured to require Multi-Factor Authentication (MFA/2FA) for remote device management.

1. Native FortiToken Authentication

Every FortiGate firewall ships with **two free FortiToken Mobile licenses** baked into the hardware. This allows administrators to use the FortiToken app on their smartphone as a time-based one-time password (TOTP) generator.

GUI Configuration: Navigate to **System > Administrators**, edit the targeted admin profile, toggle the **Two-factor Authentication** slider, select **FortiToken**, choose an available token serial number, and send the activation QR code to the admin's email.

CLI Configuration:

text

config system admin

edit "admin_username"

set two-factor fortitoken

set fortitoken <SERIAL_NUMBER>

set email-to "admin@company.com"

next

2. SAML Single Sign-On (SSO) Integration

For large enterprise networks using a central Identity Provider (IdP)—such as **Microsoft Entra ID (Azure AD), Okta, or Ping Identity**—FortiGate natively supports SAML authentication for administrative access. [[1](#), [2](#)]

3. Remote Server MFA via RADIUS / TACACS+

If your infrastructure uses central network access controllers like **FortiAuthenticator** or Cisco ISE, you can configure FortiGate to delegate authentication to these systems. The remote RADIUS server can be configured to prompt the administrator for their standard Active Directory password followed immediately by an OTP challenge string.

4. Natively Enforced Global Mandates

If you want to ensure that *no one* can log in locally without multi-factor verification, newer versions of FortiOS allow you to enforce a blanket requirement across the box via the CLI:

text

```
config system global
```

```
    set multifactor-authentication mandatory
```

```
end
```

5. Native Email and SMS Options

For lighter deployments, FortiGate can natively stream login verification codes via **Email or SMS**. While functional, these options are generally considered less secure than standard app-based tokens or SAML identity validation due to risks like SIM-swapping or email interception

3.1.1.10 Vendor must be an authorized reseller of all equipment bid. All equipment must be new and genuine; refurbished or gray market equipment will not be accepted.

3.1.2 Palo Alto Networks network device rack mount shelf - 1U (PAN-1RU 4POST-RACK-11) or Equal (Qty 2) 3.1.2.1 Shelf must be four post rack-mountable design with a height of one rack unit. 3.1.2.2 Shelf must be compatible with PAN-PA-550 firewall or equal.

FortiGate 120G natively supports 19 inch standard rack with the front ears so shelf is not needed for it.

3.1.3 Palo Alto Networks - SFP+ transceiver module - 10GbE (PAN-SFP PLUS-SR) or Equal (Qty 4)

3.1.3.1 Transceiver modules must work with 10 Gigabit Ethernet data link protocol, enabling a data transfer rate of 10 Gb/s.

3.1.3.2 Modules must have an Ethernet 10GBase-SR interface.

3.1.3.3 SFP+ modules must be compatible with PAN-PA-550 firewall or equal.

FN-TRAN-SFP+SR is the Fortinet equivalent

The **Fortinet FN-TRAN-SFP+SR** is an industry-standard 10 Gigabit Ethernet (10GBASE-SR) SFP+ optical transceiver module. It is primarily designed for high-speed, short-range fiber connectivity such as core firewall uplinks, switch stacking, or storage network connections.

Core Optical & Performance Specs

- **Data Rate: 10 Gbps** (supports speeds ranging from 1.25 Gbps to 11.3 Gbps for multi-rate applications).
- **Wavelength: 850 nm** (Short Range / SR).
- **Fiber Type: Multi-Mode Fiber (MMF).**
- **Connector Type: Duplex LC** (Two female LC ports).
- **Maximum Distance Capacity:**
 - Up to **300 meters** over standard **OM3** MMF.
 - Up to **400 meters** over **OM4** MMF.
 - Up to **550 meters** depending on specialized legacy or premium OM5 signaling contexts.

Electrical & Operational Specs

- **Power Dissipation / Consumption:** Natively low draw, typical operational usage is between **600 mW and 1W**.
- **Operating Temperature:** Standard commercial grade, **0°C to 70°C** (32°F to 158°F).
- **Digital Diagnostics Monitoring (DDM / DOM): Fully Supported.** This allows FortiOS to natively read live telemetry from the optic, including transceiver temperature, laser bias current, TX optical power, and RX optical power.

Standards Compliance

- Compliant with **IEEE 802.3ae** (10GBASE-SR).
- Built to **SFF-8431** and **SFF-8432** physical and mechanical Small Form-factor Pluggable (SFP+) MSA standards.

For alternate firewall submissions, the vendor is solely responsible for including all necessary security software subscriptions (including, but not limited to, WildFire, Advanced Threat Prevention, and management capabilities equivalent to those provided by the state's enterprise agreement) for the duration of the hardware life.

Fortinet Transceivers

Transceiver Modules for Fortinet Products

Highlights

Copper and optical options

Supports

- SFP
- SFP+
- SFP28
- SFP56
- QSFP+
- DAC
- CFP2
- QSFP28
- QSFP56
- QSFP-DD

Performance from 1 Gbps
to 400 Gbps

Tested for compatibility
with Fortinet appliances

Take the Guesswork Out of Selecting Transceivers

Common connectivity problems in enterprise and data center networks are often traced back to low-quality and incompatible transceiver modules, rather than a fault in the network appliances themselves. Fortinet's transceivers have been purpose-built and tested to work with Fortinet equipment, ensuring that your network is as stable and robust as possible, and taking the guesswork out of selecting compatible transceivers.

Wide Range for Maximum Flexibility

Supporting various form factors, media types, and throughput, Fortinet transceivers provide connectivity options to meet many different network architectures and deployment scenarios. Whether your network demands high-speed 400 GE inside the data center, or long-range 1 GE to connect data centers in different cities, Fortinet has a transceiver to meet your needs.



Available in



Appliance

Key Features and Benefits

Various Interface Options

Fortinet transceivers support various interfaces including: SFP, SFP+, DAC, and newer high-speed standards including SFP28, SFP56, QSFP+, CFP2, QSFP28, QSFP56, and QSFP-DD.

Tested for Compatibility

You can rest assured that your Fortinet transceivers have been tested for compatibility on Fortinet products, taking the guesswork out of selecting transceivers for your environment.

Maximize Network Uptime

Eliminate connectivity problems to maximize network uptime by using quality transceivers, designed to work with Fortinet products.

Cost Effective

Transceiver modules can be expensive, especially those with sensitive high-speed optics. Fortinet delivers high-quality transceivers, while keeping cost to a minimum.

Quick Reference Matrix

Maximum Transmission Distance	SFP (100MBPS)	SFP (GE)	SFP (2.5 GE)	SFP+ (10 GE)	SFP28 (25 GE)	SFP56 (50 GE)
10 Meter				SP-CABLE-ADASFP+		
30 Meter				FN-TRAN-SFP+GC		
80 Meter				FN-TRAN-SFP+GC-T80		
100 Meter		FN-TRAN-GC			FN-TRAN-SFP28-SR	FN-TRAN-SFP56-SR
150 Meter						
220 Meter		FN-TRAN-SX (62.5/125 μm) FR-TRAN-SX (62.5/125 μm)		FN-TRAN-SFP+LRM on MMF		
300 Meter			FN-TRAN-SFP2-SX	FN-TRAN-SFP+SR FN-TRAN-SFP+LRM on SMF FN-TRAN-SFP+SRI		
400 Meter				FN-TRAN-SFP+SRI (on OM4 MMF)		
500 Meter		FN-TRAN-SX (50/125 μm) FR-TRAN-SX (50/125 μm) FN-TRAN-SXI (50/125 μm)				
550 Meter				FN-TRAN-SFP+SR (on OM4 MMF)		
2 Kilometer	FN-TRAN-FX FN-TRAN-SFX					
10 Kilometer		FN-TRAN-LX FN-TRAN-SFP-1BD10 FN-TRAN-SFP-1BU10		FN-TRAN-SFP+LR FN-TRAN-SFP+LRI	FN-TRAN-SFP28-LR	
25 Kilometer			FN-TRAN-SFP2-LX			
30 Kilometer				FN-TRAN-SFP+BD27 FN-TRAN-SFP+BD33		
40 Kilometer		FN-TRAN-SFP-1BD40 FN-TRAN-SFP-1BU40 FN-TRAN-EX		FN-TRAN-SFP+ER FN-TRAN-SFP+ERI		
80 Kilometer				FN-TRAN-SFP+ZR		
90 Kilometer		FR-TRAN-ZX				
Maximum Transmission Distance	QSFP+ (40 GE)	CFP2 (100 GE)	QSFP28 (100 GE)	QSFP56 (200 GE)	QSFPDD (400 GE)	
10 Meter						
30 Meter						
100 Meter	FN-TRAN-QSFP+SR FG-TRAN-QSFP+SR-BIDI (on OM3 MMF) FN-TRAN-QSFP+BIDI (on OM3 MMF)	FG-TRAN-CFP2-SR10	FN-TRAN-QSFP28-SR FN-TRAN-QSFP28-BIDI (on OM4 MMF) FN-TRAN-QSFP28-BIDI-I	FN-TRAN-QSFP56-SR4	FN-TRAN-QSFPDD-SR8	
150 Meter	FN-TRAN-QSFP+SR FG-TRAN-QSFP+SR-BIDI (on OM4 MMF) FN-TRAN-QSFP+BIDI (on OM4 MMF)		FN-TRAN-QSFP28-BIDI (on OM5 MMF)			
220 Meter						
300 Meter						
400 Meter						
500 Meter			FN-TRAN-QSFP28-DR		FN-TRAN-QSFPDD-DR4	
2 Kilometer			FN-TRAN-QSFP28-CWDM4 FN-TRAN-QSFP28-FR	FN-TRAN-QSFP56-FR4	FN-TRAN-QSFPDD-DR4+ FN-TRAN-QSFPDD-FR4	
10 Kilometer	FN-TRAN-QSFP+LR FN-TRAN-QSFP+LRI	FG-TRAN-CFP2-LR4	FN-TRAN-QSFP28-LR		FN-TRAN-QSFPDD-LR4	
20 Kilometer			FN-TRAN-QSFP28-ER			
30 Kilometer						
40 Kilometer	FN-TRAN-QSFP+ER					
80 Kilometer						
90 Kilometer						



Specifications

TRANSCEIVER MODULES										
HARDWARE	FN-TRAN-FX	FN-TRAN-SFX	FN-TRAN-FE	FN-TRAN-GC	FN-TRAN-SX	FN-TRAN-SXI	FR-TRAN-SX	FN-TRAN-LX	FN-TRAN-EX	FR-TRAN-ZX
Protocol Standard	100Base-FX	100Base-FX (SGMII)	100Base-T	1000Base-T	1000Base-SX	1000Base-SX	1000Base-SX	1000Base-LX	1000Base-EX	1000Base-LX
IEEE Standard	802.3u	802.3u	802.3u	802.3ab	802.3z	802.3z	802.3z	802.3z	802.3z	802.3z
Module Type	SFP	SFP	SFP	SFP	SFP	SFP	SFP	SFP	SFP	SFP
Data Link Rate for Ethernet	100 Mbps	100 Mbps	100 Mbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps
Transmission Range	2 km	2 km	100 m	100 m	220 m / 500 m	500 m	500 m	10 km	40 km	90 km
Media	MM	MM	Copper Interface	Copper interface	MM	MM	MM	SM	SM	SM
Wavelength (nm)	1310	1310			850	850	850	1310	1310	1550
Connector Type	Duplex LC	Duplex LC	RJ-45	RJ-45	Duplex LC	Duplex LC	Duplex LC	Duplex LC	Duplex LC	Duplex LC
Power Dissipation	< 1.1 W	< 1.2 W	< 1 W	1.05 W	< 800 mW	< 500 mW	< 500 mW	< 830 mW	1 W	< 700 mW
Operating Temperature	-40°C to 85°C	-40°C to 85°C	-40 to 85°C	-40°C to 85°C	-20°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C
Hot Plug	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TRANSCEIVER MODULES						
HARDWARE	FN-TRAN-SFP-1BD10*	FN-TRAN-SFP-1BU10**	FN-TRAN-SFP-1BD40***	FN-TRAN-SFP-1BU40****	FN-TRAN-SFP2-SX	FN-TRAN-SFP2-LX
Protocol Standard	1000BASE-BX10	1000BASE-BX10	1000BASE-BX10	1000BASE-BX10	2500BASE-X	2500BASE-X
IEEE Standard	802.3ah	802.3ah	802.3ah	802.3ah	802.3z	802.3z
Module Type	SFP	SFP	SFP	SFP	SFP	SFP
Data Link Rate for Ethernet	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	2.5 Gbps	2.5 Gbps
Transmission Range	10 km	10 km	40 km	40 km	300 m	25 km
Media	SM	SM	SM	SM	MM	SM
Wavelength (nm)	TX: 1490 RX: 1310	TX: 1310 RX: 1490	TX: 1490 RX: 1310	TX: 1310 RX: 1490	850	1310
Connector Type	Simplex LC	Simplex LC	Simplex LC	Simplex LC	Duplex LC	Duplex LC
Power Dissipation	< 1 W	< 1 W	< 1 W	< 1 W	< 1 W	< 1 W
Operating Temperature	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C
Hot Plug	Yes	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes	Yes

* connects to FN-TRAN-1BU10, ordered separately

** connects to FN-TRAN-1BD10, ordered separately

*** connects to FN-TRAN-1BU40, ordered separately

**** connects to FN-TRAN-1BD40, ordered separately



Specifications

TRANSCEIVER MODULES						
HARDWARE	FN-TRAN-SFP+GC	FN-TRAN-SFP+GC-T80	FN-TRAN-SFP+SR	FN-TRAN-SFP+SRI	FN-TRAN-SFP+LR	FN-TRAN-SFP+LRI
Protocol Standard	10GBASE-T	10GBase-T	10GBase-SR	10GBase-SR	10GBase-LR	10GBase-LR
IEEE Standard	802.3an	802.3an	802.3ae	802.3ae	802.3ae	802.3ae
Module Type	SFP+	SFP+	SFP+	SFP+	SFP+	SFP+
Data Link Rate for Ethernet	10 Gbps	10 Gbps	10 Gbps	11.1 Gbps	10 Gbps	10.3 Gbps
Transmission Range	30 m (Cat6A or better)	80 m (Cat6a or better)	300 m (OM3) 550 m (OM4)	300 m (OM3) - 400 m (OM4)	10 km	10 km
Media	Copper interface	Copper Interface	MM	MM	SM	SM
Wavelength (nm)	—	—	850	850	1310	1310
Connector Type	RJ-45	RJ-45	Duplex LC	Duplex LC	Duplex LC	Duplex LC
Power Dissipation	2.5 W	1.88 W	600 mW	< 1 W	850 mW	< 1 W
Operating Temperature	-5°C to 85°C	-5°C to 85°C	0°C to 70°C	-40°-85°C	0°C to 85°C	-40°-85°C
Hot Plug	Yes	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	No	No	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes	Yes

TRANSCEIVER MODULES						
HARDWARE	FN-TRAN-SFP+ER	FN-TRAN-SFP+ERI	FN-TRAN-SFP+LRM	FN-TRAN-SFP+ZR	FN-TRAN-SFP+BD27*	FN-TRAN-SFP+BD33**
Protocol Standard	10GBASE-ER	10GBase-ER	10GBase-LRM	10G-Base-ZR	10G-Base-LR/LW	10G-Base-LR/LW
IEEE Standard	802.3ae	802.3ae	802.3aq	802.3ae	802.3ae	802.3ae
Module Type	SFP+	SFP+	SFP+	SFP+	SFP+	SFP+
Data Link Rate for Ethernet	11.3 Gbps	10.3 Gbps	11.3 Gbps	11.3 Gbps	11.3 Gbps	11.3 Gbps
Transmission Range	40 km	40 km	220 m MMF 300 SMF	80 km	30 km	30 km
Media	SM	SM	MM/SM	SM	SM	SM
Wavelength (nm)	1550	1550	1310	1550	TX: 1271 RX: 1331	TX: 1331 RX: 1271
Connector Type	Duplex LC	Duplex LC	Duplex LC	Duplex LC	Single LC	Single LC
Power Dissipation	1.5 W	< 1.8 W	< 1 W	< 1.5 W	< 1 W	< 1 W
Operating Temperature	-5°C to 70°C	-40°-85°C	0°C to 70°C	-5°C to 70°C	-5°C to 85°C	-5°C to 85°C
Hot Plug	Yes	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes	Yes

* Connects to FN-TRAN-SFP+BD33, ordered separately.

** Connects to FN-TRAN-SFP+BD27, ordered separately.



Specifications

TRANSCEIVER MODULES		
HARDWARE	FN-TRAN-SFP28-SR	FN-TRAN-SFP28-LR
Protocol Standard	25GBase-SR, 10GBase-SR	25GBase-LR, 10GBase-LR
IEEE Standard	802.3by, 802.3ae	802.3cc
Module Type	SFP28	SFP28
Data Link Rate for Ethernet	25.78 / 10.3 Gbps	25.78 Gbps
Transmission Range	100 m	10 km
Media	MM	SM
Wavelength (nm)	850	1310
Connector Type	Duplex LC	Duplex LC
Power Dissipation	1.2 W	1.5 W
Operating Temperature	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes
Serial ID PROM	Yes	Yes
Digital Monitoring	Yes	Yes
Auto Negotiation	No	No
Link Status	Yes	Yes

TRANSCEIVER MODULES						
HARDWARE	FN-TRAN-QSFP+SR	FN-TRAN-QSFP+LR	FN-TRAN-QSFP+LRI	FN-TRAN-QSFP+ER	FG-TRAN-QSFP+SR-BIDI	FN-TRAN-QSFP+BIDI
Protocol Standard	40GBase-SR4	40GBase-LR4	40GBase-LR4	40G-Base-ER4	40GBase-SR-BiDi	40GBase-SR-BiDi
IEEE Standard	802.3ba	802.3ba	802.3ba	802.3bm	802.3ba	802.3ba
Module Type	QSFP+	QSFP+	QSFP+	QSFP+	QSFP+	QSFP+
Data Link Rate for Ethernet	1.06 Gbps–41.2 Gbps	41.2 Gbps	41.2 Gbps	41.3 Gbps	41.2 Gbps	41.2Gbps
Transmission Range	100 m (OM3)–150 m (OM4)	10 km	10 km	40 km	100 m (OM3)–150 m (OM4)	100 m (OM3)–150 m (OM4)
Media	MM	SM	SM	SM	MM	MM
Wavelength (nm)	750–980	1264.5 - 1277.5 1284.5 - 1297.5 1304.5 - 1317.5 1324.5 - 1337.5	1264.5 - 1277.5 1284.5 - 1297.5 1304.5 - 1317.5 1324.5 - 1337.5	1264.5 - 1277.5 1284.5 - 1297.5 1304.5 - 1317.5 1324.5 - 1337.5	850–900	850–900
Connector Type	MPO-12	Duplex LC	Duplex LC	Duplex LC	Duplex LC	Duplex LC
Power Dissipation	< 1.5 W	< 3.5 W	< 3.5 W	< 3.5 W	< 3.5 W	< 3.5 W
Operating Temperature	0°C to 70°C	0°C to 70°C	-40°–85°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	No	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes	Yes



Specifications

TRANSCEIVER MODULES					
HARDWARE	FG-TRAN-CFP2-SR10	FG-TRAN-CFP2-LR4	FN-TRAN-QSFP28-SR	FN-TRAN-QSFP28-LR	FN-TRAN-QSFP28-FR
Protocol Standard	100GBase-SR10	100GBase-LR4	100GBase-SR4	100GBase-LR4	100GBase-FR
IEEE Standard	802.3ba	802.3ba	802.3bm	802.3ba	802.3bm/cd/cu
Module Type	CFP2	CFP2	QSFP28	QSFP28	QSFP28
Data Link Rate for Ethernet	103.12 Gbps	103.1 Gbps	103.1 Gbps	103.1 Gbps	103.1 Gbps
Transmission Range	100 m (OM3)–150 m (OM4)	10 km	100 m (OM4)	10 km (SMF)	2 km
Media	MM	SM	MM	SM	SM
Wavelength (nm)	850	1310	850	1294.53 – 1296.59 1299.02 – 1301.09 1303.54 – 1305.63 1308.09 – 1310.19	1310
Connector Type	24 fiber MPO	Duplex LC	MPO12	Duplex LC	Duplex LC
Power Dissipation		< 8 W	< 3.5 W	< 3.5 W	< 4.5 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes

TRANSCEIVER MODULES					
HARDWARE	FN-TRAN-QSFP28-ER	FN-TRAN-QSFP28-DR	FN-TRAN-QSFP28-CWDM4	FN-TRAN-QSFP28-BIDI	FN-TRAN-QSFP28-BIDI-I
Protocol Standard	100G-Base-LR4	100G-Base-DR	100GBase-CWDM4	100GBase-SR-BiDi	100G-Base-SR1.2
IEEE Standard	802.3ba/bm	802.3bm/cd/cu	802.3bm	802.3bm	802.3bm
Module Type	QSFP28	QSFP28	QSFP28	QSFP28	QSFP28
Data Link Rate for Ethernet	103.1 Gbps	103.1 Gbps	103.1 Gbps	103.1 Gbps	106.25 Gbps
Transmission Range	20 km	500 m	2 km	100 m	100 m
Media	SM	SM	SM	MM	MM
Wavelength (nm)	1294.53 – 1296.59 1299.02 – 1301.09 1303.54 – 1305.63 1308.09 – 1310.19	1304.5 – 1317.5	1264.5 – 1277.5 1284.5 – 1297.5 1304.5 – 1317.5 1324.5 – 1337.5	850 900	850 900
Connector Type	Duplex LC	Duplex LC	Duplex LC	Duplex LC	Duplex LC
Power Dissipation	< 3.5 W	< 4.5 W	< 3.5 W	< 3.5 W	< 4 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	10°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes



Specifications

TRANSCEIVER MODULES			
HARDWARE	FN-TRAN-SFP56-SR	FN-TRAN-QSFP56-SR4	FN-TRAN-QSFP56-FR4
Protocol Standard	50G-Base-SR	200G-Base-SR4	200G-Base-FR4
IEEE Standard	802.3cd	802.3cd	802.3bs
Module Type	SFP56	QSFP56	QSFP56
Data Link Rate for Ethernet	53.125 Gbps	212.5 Gbps	212.5 Gbps
Transmission Range	100 m	100 m	2 km
Media	MM	MM	SM
Wavelength (nm)	850	850	1264.5 – 1277.5 1284.5 – 1297.5 1304.5 – 1317.5 1324.5 – 1337.5
Connector Type	Duplex LC	MPO-12	Duplex LC
Power Dissipation	< 1.5 W	< 4.5 W	< 6 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes
Link Status	Yes	Yes	Yes

TRANSCEIVER MODULES					
HARDWARE	FN-TRAN-QSFPDD-SR8	FN-TRAN-QSFPDD-LR4	FN-TRAN-QSFPDD-FR4	FN-TRAN-QSFPDD-DR4	FN-TRAN-QSFPDD-DR4+
Protocol Standard	400G-Base-SR8	400G-Base-LR4	400G-Base-FR4	400G-Base-DR4	400G-Base-DR4
IEEE Standard	802.3bs	802.3bs	802.3cu	802.3bs	802.3bs
Module Type	QSFP-DD	QSFP-DD	QSFP-DD	QSFP-DD	QSFP-DD
Data Link Rate for Ethernet	425 Gbps	425 Gbps	425 Gbps	425 Gbps	425 Gbps
Transmission Range	100 m	10 km	2 km	500 m	2 km
Media	MM	SM	SM	SM	SM
Wavelength (nm)	850	1271 1291 1311 1331	1271 1291 1311 1331	1310	1311
Connector Type	MPO-16 APC	Duplex LC	Duplex LC	MPO-12	MPO-12
Power Dissipation	< 9 W	< 10.5 W	< 12 W	< 12 W	< 14 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes	Yes
Serial ID PROM	Yes	Yes	Yes	Yes	Yes
Digital Monitoring	Yes	Yes	Yes	Yes	Yes
Auto Negotiation	Yes	Yes	Yes	Yes	Yes
Link Status	Yes	Yes	Yes	Yes	Yes



Specifications

DIRECT ATTACH CABLES				
HARDWARE	FN-CABLE-SFP+1	FN-CABLE-SFP+3	FN-CABLE-SFP+5	SP-CABLE-ADASFP+
Protocol Standard	10GBase-CR	10GBase-CR	10GBase-CR	10GBase-CR
Data Link Rate for Ethernet	10 Gbps	10 Gbps	10 Gbps	1 Gbps to 10 Gbps
Module Type	SFP+	SFP+	SFP+	SFP+
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W	< 0.5 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes
Cable Length	1 m	3 m	5 m	10 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Active
Transceiver	Included	Included	Included	Included
Compliance	RoHS	RoHS	RoHS	RoHS
Bend Radius	22 mm (30 AWG)	22 mm (30 AWG)	33 mm (24 AWG)	25 mm (30 AWG)
Cable Diameter	4.5 mm	4.5 mm	5.6 mm	4.5 mm
Digital Monitoring	Yes	Yes	Yes	Yes

DIRECT ATTACH CABLES			
HARDWARE	FN-CABLE-SFP28-1	FN-CABLE-SFP28-3	FN-CABLE-SFP28-5
Protocol Standard	25GBase-CR	25GBase-CR	25GBase-CR
Data Link Rate for Ethernet	25 Gbps	25 Gbps	25 Gbps
Module Type	SFP28	SFP28	SFP28
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W
Operating Temperature	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C
Hot Plug	Yes	Yes	Yes
Cable Length	1 m	3 m	5 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included
Compliance	RoHS	RoHS	RoHS
Bend Radius	35 mm (30 AWG)	35 mm (30 AWG)	35 mm (30 AWG)
Cable Diameter	4.83 mm	4.83 mm	4.83 mm
Digital Monitoring	Yes	Yes	Yes



Specifications

DIRECT ATTACH CABLES				
HARDWARE	FN-CABLE-QSFP+1	FN-CABLE-QSFP+3	FN-CABLE-QSFP+5	FN-CABLE-QSFP+7
Protocol Standard	40GBase-CR4	40GBase-CR4	40GBase-CR4	40GBase-CR4
Data Link Rate for Ethernet	40 Gbps	40 Gbps	40 Gbps	40 Gbps
Module Type	QSFP+	QSFP+	QSFP+	QSFP+
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W	<0.1 W
Operating Temperature	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C
Hot Plug	Yes	Yes	Yes	Yes
Cable Length	1 m	3 m	5 m	7 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included	Included
Compliance	RoHS	RoHS	RoHS	RoHS
Bend Radius	37.5 mm (28 AWG)	37.5 mm (28 AWG)	44 mm (26 AWG)	49 mm (24 AWG)
Cable Diameter	7.5 mm	7.5 mm	8.8 mm	9.8 mm
Digital Monitoring	Yes	Yes	Yes	Yes

DIRECT ATTACH CABLES (DAC)				
HARDWARE	FN-CABLE-SFP56-DAC-L1	FN-CABLE-SFP56-DAC-LB5	FN-CABLE-QSFP56-DAC-L1	FN-CABLE-QSFP56-DAC-LB5
Protocol Standard	50GBase-CR	50GBase-CR	200G-BASE-CR4	200G-BASE-CR4
Data Link Rate for Ethernet	50 Gbps	50 Gbps	200 Gbps	200 Gbps
Module Type	SFP56	SFP56	QSFP56	QSFP56
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W	< 0.1 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes
Cable Length	1 m	2.5 m	1 m	2.5 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included	Included
Compliance	RoHS	RoHS	RoHS	RoHS
Bend Radius	22.5 mm (30 AWG)	27.5 mm (28 AWG)	35.0 mm (30 AWG)	42.5 mm (28 AWG)
Cable Diameter	4.5 mm	5.5 mm	7.0 mm	8.5 mm
Digital Monitoring	No	No	No	No

DIRECT ATTACH CABLES (DAC)				
HARDWARE	FN-CABLE-QSFP28-1	FN-CABLE-QSFP28-2	FN-CABLE-QSFP28-3	FN-CABLE-QSFP28-5
Protocol Standard	100GBase-CR4	100GBase-CR4	100GBase-CR4	100GBase-CR4
Data Link Rate for Ethernet	100 Gbps	100 Gbps	100 Gbps	100 Gbps
Module Type	QSFP28	QSFP28	QSFP28	QSFP28
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W	< 0.1 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes
Cable Length	1 m	2 m	3 m	5 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included	Included
Compliance	RoHS	RoHS	RoHS	RoHS
Bend Radius	25 mm (30 AWG)	25 mm (30 AWG)	25 mm (30 AWG)	25 mm (30 AWG)
Cable Diameter	6.4 mm	6.4 mm	6.4 mm	6.4 mm
Digital Monitoring	N/A	N/A	N/A	N/A



Specifications

	DIRECT ATTACH CABLE (DAC)	DIRECT ATTACH CABLE (DAC)	ACTIVE OPTICAL CABLE (AOC)
HARDWARE	FN-CABLE-QSFPDD-DAC-01	FN-CABLE-QSFPDD-DAC-B5	FN-CABLE-QSFPDD-AOC-03
Protocol Standard	400GBase-CR8	400GBase-CR8	400G Ethernet
IEEE Standard	IEEE802.3bs	IEEE802.3bs	IEEE802.3bs
Data Link Rate for Ethernet	425 Gbps	425 Gbps	425 Gbps
Module Type	QSFP-DD	QSFP-DD	QSFP-DD
Power Dissipation	< 0.1 W	< 0.1 W	8 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes
Cable Length	1 m	2.5 m	3 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	OM3
Transceiver	Included	Included	Included
Compliance	RoHS	RoHS	RoHS
Bend Radius	31.5 mm (30 AWG)	40.6 mm (26 AWG)	—
Cable Diameter	9.0 mm	11.6 mm	—
Digital Monitoring	No	No	Yes

	BREAKOUT DIRECT ATTACH CABLES (DAC)		
HARDWARE	FN-CABLE-QSFP28-4SFP28-1	FN-CABLE-QSFP28-4SFP28-3	FN-CABLE-QSFP28-4SFP28-5
Protocol Standard	25GBase-CR	25GBase-CR	25GBase-CR
IEEE Standard			
Data Link Rate for Ethernet	1× 100 Gbps 4× 25 Gbps	1× 100 Gbps 4× 25 Gbps	1× 100 Gbps 4× 25 Gbps
Module Type	1x QSFP28 4x SFP28	1x QSFP28 4x SFP28	1x QSFP28 4x SFP28
Power Dissipation	< 0.1 W	< 0.1 W	< 0.1 W
Operating Temperature	-40°C to 85°C	-40°C to 85°C	-40°C to 85°C
Hot Plug	Yes	Yes	Yes
Cable Length	1 m	3 m	5 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included
Compliance	RoHS	RoHS	RoHS
Bend Radius	30 mm (30 AWG)	30 mm (30 AWG)	30 mm (30 AWG)
Cable Diameter	4.83 mm	4.83 mm	4.83 mm
Digital Monitoring	Yes	Yes	Yes



Specifications

BREAKOUT DIRECT ATTACH CABLES (DAC)				
HARDWARE	FN-CABLE-QSFPDD-2QSFP56-L1	FN-CABLE-QSFPDD-2QSFP56-LB5	FN-CABLE-QSFPDD-8SFP56-L1	FN-CABLE-QSFPDD-8SFP56-LB5
Protocol Standard	400G/200G Ethernet	400G/200G Ethernet	400G/50G Ethernet	400G/50G Ethernet
IEEE Standard	802.3cd	802.3cd	802.3cd	802.3cd
Data Link Rate for Ethernet	1× 400 Gbps 2× 200 Gbps	1× 400 Gbps 2× 200 Gbps	1× 400 Gbps 8× 50 Gbps	1× 400 Gbps 8× 50 Gbps
Module Type	1x QSFP-DD 2x QSFP56	1x QSFP-DD 2x QSFP56	1x QSFP-DD 8x SFP56	1x QSFP-DD 8x SFP56
Power Dissipation	0.1 W	0.1 W	0.1 W	0.1 W
Operating Temperature	0°C to 70°C	0°C to 70°C	0°C to 70°C	0°C to 70°C
Hot Plug	Yes	Yes	Yes	Yes
Cable Length	1 m	2.5 m	1 m	2.5 m
Cable Type	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive	Twinax Copper Passive
Transceiver	Included	Included	Included	Included
Compliance	RoHS	RoHS	RoHS	RoHS
Bend Radius	70 mm (30 AWG)	85 mm (28 AWG)	45 mm (30 AWG)	50 mm (28 AWG)
Cable Diameter	7.0 mm	8.5 mm	4.5 mm	5.0 mm
Digital Monitoring	No	No	No	No

BREAKOUT CABLES				
HARDWARE	FG-TRAN-QSFP-4xSFP	FG-TRAN-QSFP-4SFP-5	FG-CABLE-SR10-SFP+	FG-CABLE-SR10-SFP+5
Connector A	1× 40 GE QSFP+	1× 40 GE QSFP+	1× 100 GE SR10 CFP2	1× 100 GE SR10 CFP2
Connector A Type	MPO	MPO	MPO	MPO
Connector B	4× 10 GE SFP+	4× 10 GE SFP+	10× 10 GE SFP+	10× 10 GE SFP+
Connector B Type	LC duplex	LC duplex	LC duplex	LC duplex
Cable Length	1 m	5 m	1 m	5 m
Cable Type	OM3 MMF	OM3 MMF	OM3 MMF	OM3 MMF
Transceiver	Not included	Not included	Not included	Not included

Fortinet Breakout Cables — Qualified on Fortinet Products (on applicable interfaces)



Ordering Information

Product	SKU	Description
Transceivers		
1 GE SFP Transceiver module, 10km, BiDi	FN-TRAN-SFP-1BD10	1 GE SFP BiDi transceiver module, long range 10km, single LC connector, SMF, TX:1490nm/ RX:1310nm, -40°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-1BU10, ordered separately).
1 GE SFP Transceiver module, 10km, BiDi	FN-TRAN-SFP-1BU10	1 GE SFP BiDi transceiver module, long range 10km, single LC connector, SMF, TX:1310nm/ RX:1490nm, -40°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-1BD10, ordered separately).
1 GE SFP Transceiver module, 40km, BiDi	FN-TRAN-SFP-1BD40	1 GE SFP BiDi transceiver module, long range 40km, single LC connector, SMF, TX:1490nm/ RX:1310nm, -40°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-1BU40, ordered separately).
1 GE SFP Transceiver module, 40km, BiDi	FN-TRAN-SFP-1BU40	1 GE SFP BiDi transceiver module, long range 40km, single LC connector, SMF, TX:1310nm/ RX:1490nm, -40°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-1BD40, ordered separately).
1 GE SFP LX Transceiver module, long range	FN-TRAN-LX	1 GE SFP transceiver module, long range 10km, LC connector, SMF, 1310nm, -40°C to 85°C, for systems with SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver module, 100m range	FN-TRAN-GC	1 GE SFP transceiver module, range 100m, RJ45 connector, -40°C to 85°C, for systems with SFP/ SFP+ slots.
1 GE SFP SX Transceiver module, short range	FN-TRAN-SX	1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -20°C to 85°C, for systems with SFP slots.
1 GE SFP transceiver module, short range 500m	FN-TRAN-SXI-4PACK	Pack of four 1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP slots.
1 GE SFP SX Transceiver module, MMF, -40°C~85°C operation	FR-TRAN-SX	1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP slots.
1 GE SFP transceiver module, long range 40km	FN-TRAN-EX-4PACK	Pack of four 1 GE SFP transceiver module, long range 40km, LC connector, SMF, 1310nm, -40°C to 85°C, for systems with SFP/SFP+ slots.
1 GE SFP Transceiver module, 90 km range, -40°C~85°C operation	FR-TRAN-ZX	1 GE SFP transceiver module, long range 90km, LC connector, SMF, 1550nm, -40°C to 85°C, for systems with SFP slots.
Pack of four 1 GE SFP transceiver module, short range 500m	FN-TRAN-SXI-4PACK	Pack of four 1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP slots.
2.5 GE SFP Transceiver module, 20km range	FN-TRAN-SFP2-LX	2.5 GE SFP+ transceiver module, long range 25km, LC connector, SMF, 1310nm, -40°C to 70°C, for systems with SFP/SFP+ slots.
2.5 GE SFP Transceiver module, short range	FN-TRAN-SFP2-SX	2.5 GE SFP+ transceiver module, long range 300m, LC connector, MMF, 850nm, -40°C to 70°C, for systems with SFP/SFP+ slots.
10 GE SFP+ Transceiver module, short range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range 550m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP+ slots.
10 GE SFP+ transceiver module, short range	FN-TRAN-SFP+SRI	10 GE SFP+ transceiver module, short range 400m, LC connector, MMF, 850nm, -40°C to 85°C, for systems with SFP+ slots.
10 GE SFP+ Transceiver module, long range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range 10km, LC connector, SMF, 1310nm, 0°C to 70°C, for systems with SFP+ slots. TAA Compliant.
10 GE SFP+ transceiver module, 10km range	FN-TRAN-SFP+LRI	10 GE SFP+ transceiver module, long range 10km, LC connector, SMF, 1310nm, -40°C to 85°C, for systems with SFP+ slots.
10 GE SFP Transceiver module, long range MMF	FN-TRAN-SFP+LRM	10 GE SFP+ transceiver module, long range 220m/300m, LC connector, OM1 MMF/SMF, 1310nm, 0°C to 70°C, for systems with SFP+ slots.
10 GE SFP+ Transceiver module, short range, BiDi	FN-TRAN-SFP+BD27	10 GE SFP+ BiDi transceiver module, long range 30km, single LC connector, SMF, TX:1271nm/ RX:1331nm, -5°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver module, short range, BiDi	FN-TRAN-SFP+BD33	10 GE SFP+ BiDi transceiver module, long range 30km, single LC connector, SMF, TX:1331nm/ RX:1271nm, -5°C to 85°C, for systems with SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
10 GE SFP+ Transceiver module, extended range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, long range 40km, LC connector, SMF, 1550nm, -40°C to 85°C, for systems with SFP+ slots.
10 GE SFP+ transceiver module, 40km range	FN-TRAN-SFP+ERI	10 GE SFP+ transceiver module, long range 40km, LC connector, SMF, 1550nm, -40°C to 85°C, for systems with SFP+ slots.
10 GE SFP+ Transceiver module, extended range	FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, long range 80km, LC connector, SMF, 1550nm, -5°C to 70°C, for systems with SFP+ slots.
10 GE copper SFP+ RJ45 Transceiver module, 30m range	FN-TRAN-SFP+GC	10 GE SFP+ transceiver module, range 30m, RJ45 connector, CAT6A, -5°C to 85°C, for systems with SFP+ slots.
10 GE copper SFP+ RJ45 Transceiver module, 80m range	FN-TRAN-SFP+GC-T80	10 GE SFP+ transceiver module, range 80m, RJ45 connector, CAT6A, -5°C to 85°C, for systems with SFP+ slots.



Ordering Information

Product	SKU	Description
25 GE SFP28 transceiver module, long range	FN-TRAN-SFP28-LR	25 GE / 10 GE SFP28 transceiver module, long range 10km, LC connector, SMF, 1310nm, 0°C to 70°C, for systems with SFP28 slots.
25 GE SFP28 Transceiver module, short range	FN-TRAN-SFP28-SR	25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots.
40 GE QSFP+ Transceiver module, short range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range 150m, MPO-12 connector, four channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ Transceiver module, extended range	FN-TRAN-QSFP+ER	40 GE QSFP+ transceiver module, long range 40km, LC connector, SMF, 40GBase-ER4, 0°C to 70°C, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ Transceiver module, short range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ BiDi transceiver module, short range 150m, LC connector, MMF, 850nm/900nm, 0°C to 70°C, for systems with QSFP28 slots.
40 GE QSFP+ BiDi Transceiver module, short range 150m	FN-TRAN-QSFP+BiDi	40 GE QSFP+ BiDi transceiver module, short range 150m, LC connector, MMF, 850nm/900nm, 0°C to 70°C, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ Transceiver module, long range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range 10km, LC connector, SMF, 40GBase-LR4, 0°C to 70°C, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ transceiver module, 10km range	FN-TRAN-QSFP+LRI	40 GE QSFP+ transceiver module, long range 10km, LC connector, SMF, 40GBase-LR4, -40°C to 85°C, for systems with QSFP+/QSFP28 slots.
50 GE SFP56 Transceiver module, short range	FN-TRAN-SFP56-SR	50 GE SFP56 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots.
100 Mb SFP Transceiver module, 2km range over MMF	FN-TRAN-FX	100 M SFP transceiver module, long range 2km, LC connector, MMF, 1310nm, -40°C to 85°C, for systems with SFP slots and capable of 10/100Mb mode selection.
100 M SFP transceiver module, long range 2km over MMF, SGMII interface	FN-TRAN-SFX	100 M SFP transceiver module with SGMII interface, long range 2km, LC connector, MMF, 1310nm, -40°C to 85°C, for systems with SFP slots and SGMII interface.
100M Fast Ethernet transceiver module, range 100M	FN-TRAN-FE-4PACK	Pack of four 100M Fast Ethernet transceiver module, range 100m, RJ45 connector, -40°C to 85°C, for systems with SFP slots.
100 GE CFP2 Transceiver module, long range	FG-TRAN-CFP2-LR4	100 GE CFP2 transceiver module, long range 10km, LC connector, SMF, 1310nm, 0°C to 70°C, for systems with CFP2 slots.
100 GE CFP2 Transceiver module, short range	FG-TRAN-CFP2-SR10	100 GE CFP2 transceiver module, short range 100m, MPO-24 connector, ten-channel parallel MMF, 850nm, 0°C to 70°C, for systems with CFP2 slots.
100 GE QSFP28 Transceiver module, short range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceiver module, short range 100m, MPO-12 connector, four-channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP28 slots. TAA compliant.
100 GE QSFP28 Transceiver module, long range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceiver module, long range 10km, LC connector, SMF, 100GBase-LR4, 0°C to 70°C, for systems with QSFP28 slots.
100 GE QSFP28 transceiver module, long range	FN-TRAN-QSFP28-FR	100 GE QSFP28 transceiver module, long range 2km, LC connector, SMF, 1310nm, 100GBase-FR, 0°C to 70°C, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver module, extended range	FN-TRAN-QSFP28-ER	100 GE QSFP28 transceiver module, long range 20km, LC connector, SMF, 100GBase-LR4, 0°C to 70°C, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver module, short range	FN-TRAN-QSFP28-DR	100 GE QSFP28 transceiver module, short range 500m, LC connector, SMF, 1310nm, 0°C to 70°C, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver module, CWDM	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceiver module, long range 2km, LC connector, SMF, 100GBase-CWDM4, 0°C to 70°C, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver module, short range, BiDi	FN-TRAN-QSFP28-BIDI	100 GE QSFP28 BiDi transceiver module, short range 100m, LC connector, MMF, 850nm/900nm, 0°C to 70°C, 100GBase-SR-BiDi, for systems with QSFP28 slots.
100 GE QSFP28 Transceiver module, short range, BiDi	FN-TRAN-QSFP28-BIDI-I	100 GE QSFP28 BiDi transceiver module, short range 100m, LC connector, MMF, 850nm/900nm, 0°C to 70°C, 100G-Base-SR1.2, for systems with QSFP28 slots.
200 GE QSFP56 Transceiver module, short range	FN-TRAN-QSFP56-SR4	200 GE QSFP56 transceiver module, short range 100m, MPO-12 connector, four-channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP56 slots.
200 GE QSFP56 transceiver module, 2km range	FN-TRAN-QSFP56-FR4	200 GE QSFP56 transceiver module, long range 2km, LC connector, SMF, 200G-Base-FR4, 0°C to 70°C, for systems with QSFP56 slots.
400 GE QSFPDD Transceiver module, short range	FN-TRAN-QSFPDD-SR8	400 GE QSFPDD transceiver module, short range 100m, MPO-16 connector, eight-channel parallel MMF, 850nm, 0°C to 70°C, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver module, short range	FN-TRAN-QSFPDD-DR4	400 GE QSFPDD transceiver module, short range 500m, MPO-12 connector, four-channel parallel SMF, 1310nm, 0°C to 70°C, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver module, long range	FN-TRAN-QSFPDD-LR4	400 GE QSFPDD transceiver module, long range 10km, LC connector, SMF, 400G-Base-LR4, 0°C to 70°C, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver module, mid range	FN-TRAN-QSFPDD-FR4	400 GE QSFPDD transceiver module, long range 2km, LC connector, SMF, 400G-Base-FR4, 0°C to 70°C, for systems with QSFP-DD slots.
400 GE QSFPDD Transceiver module, mid range	FN-TRAN-QSFPDD-DR4+	400 GE QSFPDD transceiver module, long range 2km, MPO-12 connector, four-channel parallel SMF, 1311nm, 0°C to 70°C, for systems with QSFP-DD slots.



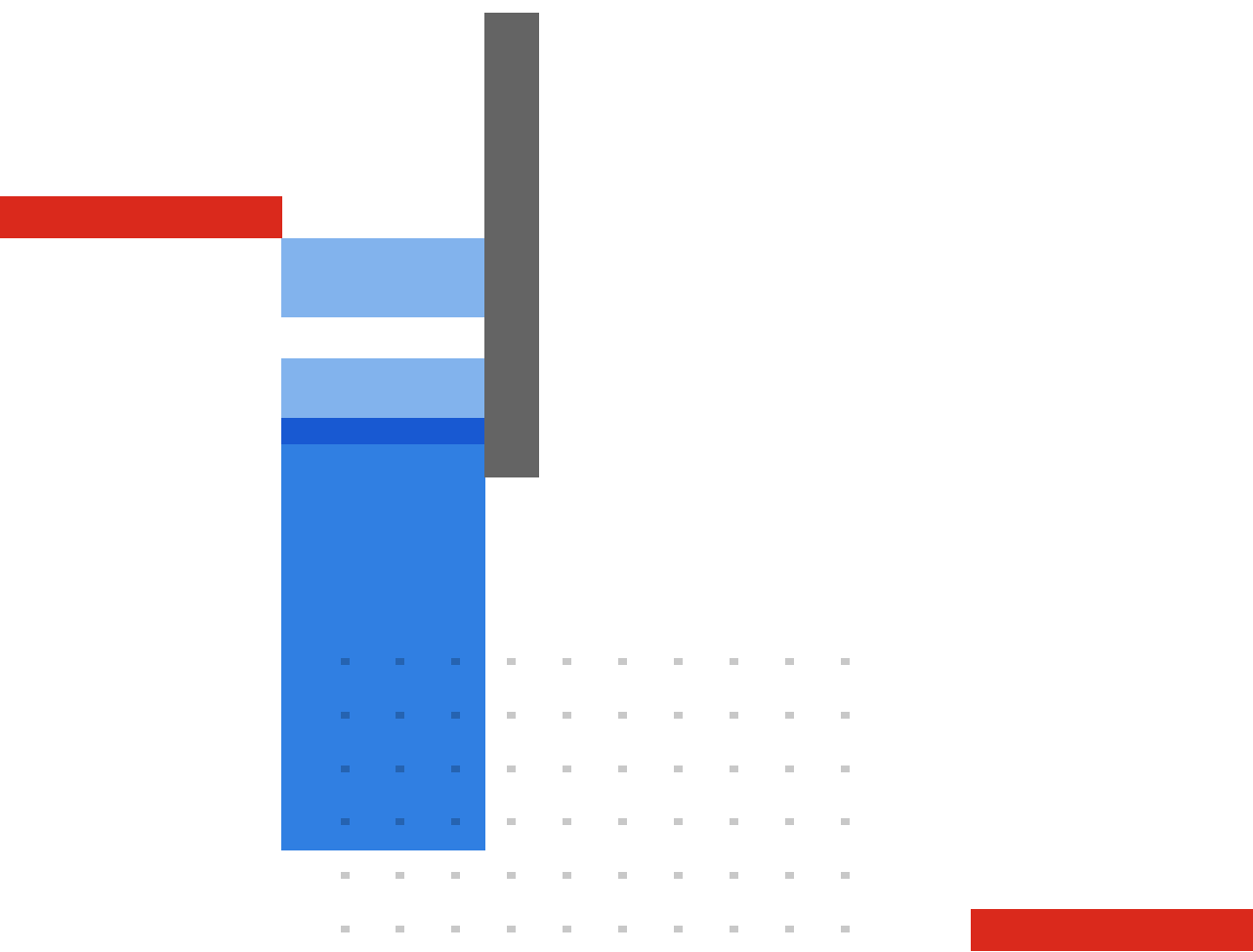
Ordering Information

Product	SKU	Description
Cables		
10 GE SFP+ active direct attach cable, 10m/32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m, 0°C to 70°C, transceivers included, for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ passive direct attach cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with SFP/SFP+ slots.
10 GE SFP+ passive direct attach cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m, 0°C to 70°C, transceivers included, for systems with SFP/SFP+ slots.
10 GE SFP+ passive direct attach cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m, 0°C to 70°C, transceivers included, for systems with SFP/SFP+ slots.
25 GE passive direct attach cable 1m	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable, 1m, -40°C to 85°C, transceivers included, for systems with SFP28 slots.
25 GE passive direct attach cable 3m	FN-CABLE-SFP28-3	25 GE SFP28 passive direct attach cable, 3m, -40°C to 85°C, transceivers included, for systems with SFP28 slots.
25 GE passive direct attach cable 5m	FN-CABLE-SFP28-5	25 GE SFP28 passive direct attach cable, 5m, -40°C to 85°C, transceivers included, for systems with SFP28 slots.
40 GE QSFP+ passive direct attach cable 1m	FN-CABLE-QSFP+1	40 GE QSFP+ passive direct attach cable, 1m, -40°C to 85°C, transceivers included, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ passive direct attach cable 3m	FN-CABLE-QSFP+3	40 GE QSFP+ passive direct attach cable, 3m, -40°C to 85°C, transceivers included, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ passive direct attach cable 5m	FN-CABLE-QSFP+5	40 GE QSFP+ passive direct attach cable, 5m, -40°C to 85°C, transceivers included, for systems with QSFP+/QSFP28 slots.
40 GE QSFP+ passive direct attach cable, 7m	FN-CABLE-QSFP+7-4PACK	Pack of four 40 GE QSFP+ passive direct attach cable, 7m, -40°C to 85°C, transceivers included, for systems with QSFP+/QSFP28 slots.
40 G/100G QSFP+ to 4x SFP+/SFP28 optical breakout 1m	FG-TRAN-QSFP-4XSFP	40G/100G QSFP+/QSFP28 to SFP+/SFP28 parallel breakout MPO to 4xLC connectors, OM3 MMF, 1m, transceivers not included.
40 G/100G QSFP+ to 4x SFP+/SFP28 optical breakout 5m	FG-TRAN-QSFP-4SFP-5	40G/100G QSFP+/QSFP28 to SFP+/SFP28 parallel breakout MPO to 4xLC connectors, OM3 MMF, 5m, transceivers not included.
50 GE SFP56 passive direct attach cable, 1m	FN-CABLE-SFP56-DAC-L1	50 GE SFP56 passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with SFP56 slots.
50 GE SFP56 passive direct attach cable, 2.5m	FN-CABLE-SFP56-DAC-LB5	50 GE SFP56 passive direct attach cable, 2.5m, 0°C to 70°C, transceivers included, for systems with SFP56 slots.
100 GE SR10 to 10x 10 GE fan out cable, 1m	FG-CABLE-SR10-SFP+	100 GE CFP2 parallel breakout MPO to 10xLC connectors, OM3 MMF, 1m reach, transceivers not included.
100 GE SR10 to 10x 10 GE fan out cable, 5m	FG-CABLE-SR10-SFP+5	100 GE CFP2 parallel breakout MPO to 10xLC connectors, OM3 MMF, 5m reach, transceivers not included.
100 GE passive direct attach cable 1m	FN-CABLE-QSFP28-1	100 GE QSFP28 passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with QSFP28 slots.
100 GE passive direct attach cable 2m	FN-CABLE-QSFP28-2	100 GE QSFP28 passive direct attach cable, 2m, 0°C to 70°C, transceivers included, for systems with QSFP28 slots.
100 GE passive direct attach cable 3m	FN-CABLE-QSFP28-3	100 GE QSFP28 passive direct attach cable, 3m, 0°C to 70°C, transceivers included, for systems with QSFP28 slots.
100 GE passive direct attach cable 5m	FN-CABLE-QSFP28-5	100 GE QSFP28 passive direct attach cable, 5m, 0°C to 70°C, transceivers included, for systems with QSFP28 slots.
100 GE QSFP28 to 4x 25 GE SFP28 direct attach cable breakout, 1m	FN-CABLE-QSFP28-4SFP28-1	100 GE QSFP28 breakout to 4x 25 GE SFP28 passive direct attach cable, 1m, -40°C to 85°C, transceivers included, for systems with QSFP28/QSFP+, SFP28/SFP+ slots.
100 GE QSFP28 to 4x 25 GE SFP28 direct attach cable breakout, 3m	FN-CABLE-QSFP28-4SFP28-3	100 GE QSFP28 breakout to 4x 25 GE SFP28 passive direct attach cable, 3m, -40°C to 85°C, transceivers included, for systems with QSFP28/QSFP+, SFP28/SFP+ slots.
100 GE QSFP28 to 4x 25 GE SFP28 direct attach cable breakout, 5m	FN-CABLE-QSFP28-4SFP28-5	100 GE QSFP28 breakout to 4x 25 GE SFP28 passive direct attach cable, 5m, -40°C to 85°C, transceivers included, for systems with QSFP28/QSFP+, SFP28/SFP+ slots.
200 GE QSFP56 passive direct attach cable, 1m	FN-CABLE-QSFP56-DAC-L1	200 GE QSFP56 passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with QSFP56 slots.
200 GE QSFP56 passive direct attach cable, 2.5m	FN-CABLE-QSFP56-DAC-LB5	200 GE QSFP56 passive direct attach cable, 2.5m, 0°C to 70°C, transceivers included, for systems with QSFP56 slots.
400 GE passive direct attach cable 1m	FN-CABLE-QSFPDD-DAC-01	400 GE QSFPDD passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with QSFP-DD slots.
400 GE passive direct attach cable 2.5m	FN-CABLE-QSFPDD-DAC-B5	400 GE QSFPDD passive direct attach cable, 2.5m, 0°C to 70°C, transceivers included, for systems with QSFP-DD slots.
400 GE QSFPDD Active Optical Cable, 3m	FN-CABLE-QSFPDD-AOC-03	400 GE QSFPDD active optical cable, 3m, 0°C to 70°C, transceivers included, for systems with QSFP-DD slots.
400 GE QSFPDD breakout to 2x 200 GE QSFP56 passive direct attach cable, 1m	FN-CABLE-QSFPDD-2QSFP56-L1	400 GE QSFPDD breakout to 2x 200 GE QSFP56 passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with QSFPDD, QSFP56 slots.
400 GE QSFPDD breakout to 2x 200 GE QSFP56 passive direct attach cable, 2.5m	FN-CABLE-QSFPDD-2QSFP56-LB5	400 GE QSFPDD breakout to 2x 200 GE QSFP56 passive direct attach cable, 2.5m, 0°C to 70°C, transceivers included, for systems with QSFPDD, QSFP56 slots.
400 GE QSFPDD breakout to 8x 50 GE SFP56 passive direct attach cable, 1m	FN-CABLE-QSFPDD-8SFP56-L1	400 GE QSFPDD breakout to 8x 50 GE SFP56 passive direct attach cable, 1m, 0°C to 70°C, transceivers included, for systems with QSFPDD, SFP56 slots.
400 GE QSFPDD breakout to 8x 50 GE SFP56 passive direct attach cable, 2.5m	FN-CABLE-QSFPDD-8SFP56-LB5	400 GE QSFPDD breakout to 8x 50 GE SFP56 passive direct attach cable, 2.5m, 0°C to 70°C, transceivers included, for systems with QSFPDD, SFP56 slots.



Fortinet Corporate Social Responsibility Policy

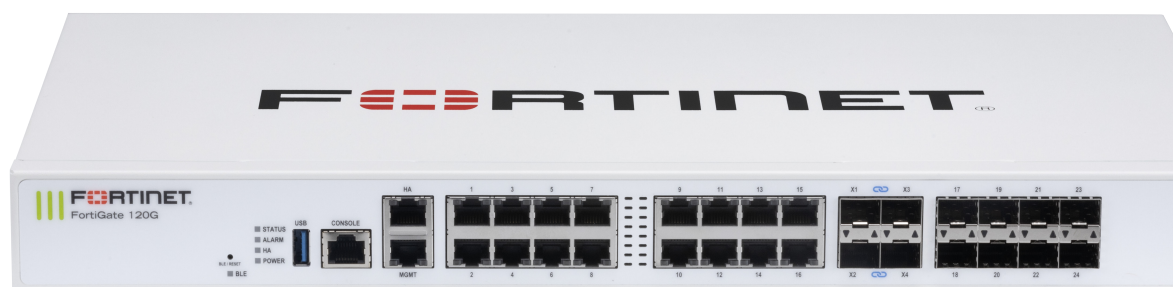
Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FortiGate 120G Series



Highlights

Leader in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

Secure Networking with FortiOS for converged networking and security

State-of-the-art unparalleled performance with Fortinet's patented SPU and vSPU processors

Enterprise security with consolidated AI/ML-powered FortiGuard services

Deep visibility into applications, users, and devices beyond traditional firewall techniques

Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 120G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 120G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (ZTNA) automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast threat protection and SSL inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
5.3 Gbps	3.1 Gbps	2.8 Gbps	Multiple GE RJ45, SFP, and 10GE SFP+ Slots Variants with internal storage

Use Cases



Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-Powered Security Services, natively integrated with your NGFW, secures web, content, and devices and protects networks from ransomware, malware, zero days, and sophisticated AI-powered cyberattacks
 - Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
 - Fortinet's patented SPU technology provides industry-leading high-performance protection
-



Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
 - Delivers superior quality of experience and effective security posture for hybrid working models, SD-Branch, and cloud-first WAN use cases
 - Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing
-



Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

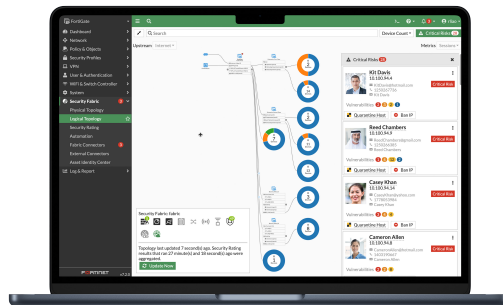
FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

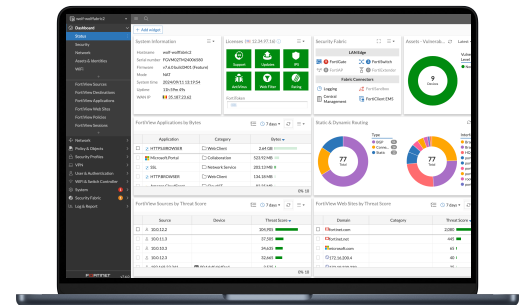
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

Learn more about what's new in FortiOS. <https://www.fortinet.com/products/fortigate/fortios>



Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status





FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR(optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.



FortiManager

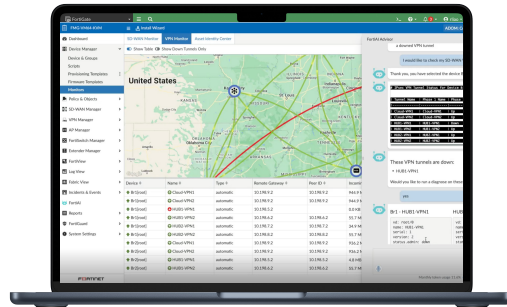


AI-Powered, Automation-Driven, Enterprise-Class Centralized Management at Scale

FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

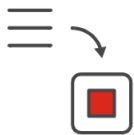
FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.



GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.

FortiConverter Service



Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiCare Services

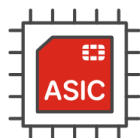


Expertise at your service

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.



Fortinet ASICs: Unrivalled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

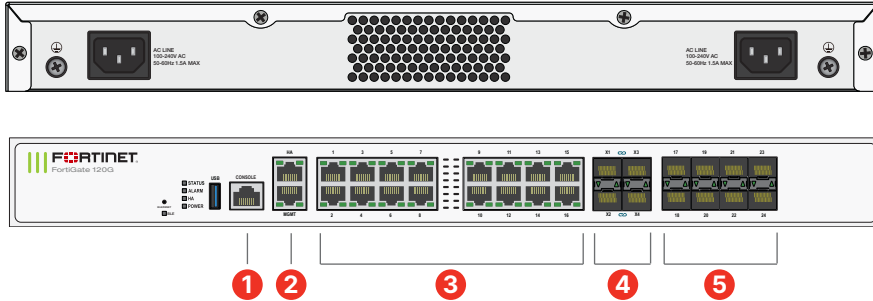
Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Secure SD-WAN ASIC SP5

- Combines a RISC-based CPU with Fortinet's proprietary security processing unit (SPU) content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

Hardware

FortiGate 120G/121G Series



Interfaces

1. 1x RJ45 Console Port
2. 2x RJ45 HA and Management Ports
3. 16x GE RJ45 Ports
4. 4x 10GE SFP+ FortiLink Slots
5. 8x SFP Ports

Hardware Features



Trusted Platform Module (TPM)

The FortiGate 120G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.



Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 120G series offers dual built-in non-hot swappable power supplies.



Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.

Specifications

	FORTIGATE 120G	FORTIGATE 121G
Hardware Specifications		
Hardware Accelerated GE RJ45 Ports		16
GE RJ45 Management / HA		1 / 1
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)		4
USB Ports		1
Console (RJ45) Port		1
Internal Storage	—	1 × 480 GB SSD
Trusted Platform Module (TPM)		✓
Bluetooth Low Energy (BLE)		✓
Signed Firmware Hardware Switch		—
System Performance* — Enterprise Traffic Mix		
IPS Throughput ²		5.3 Gbps
NGFW Throughput ^{2,4}		3.1 Gbps
Threat Protection Throughput ^{2,5}		2.8 Gbps
System Performance and Capacity		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		39 / 39 / 28 Gbps
Firewall Latency (64 byte UDP packets)		3.17 μs
Firewall Throughput (Packets Per Second)		42 Mpps
Concurrent Sessions (TCP)		3 M
New Sessions/Second (TCP)		140 000
Firewall Policies		10 000
IPsec VPN Throughput (512 byte) ¹		35 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2000
Client-to-Gateway IPsec VPN Tunnels		16 000
SSL-VPN Throughput		1.5 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		500
SSL Inspection Throughput (IPS, avg. HTTPS) ³		3 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³		2100
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		315 000
Application Control Throughput (HTTP 64K) ²		6.7 Gbps
CAPWAP Throughput (HTTP 64K)		35 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		48*
Maximum Number of FortiAPs (Total / Tunnel Mode)		128 / 64
Maximum Number of FortiTokens		5000
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 120G	FORTIGATE 121G
Dimensions		
Height x Width x Length (inches)	1.73 × 17 × 10	
Height x Width x Length (mm)	44 × 432 × 254	
Weight	12.17 lbs (5.52 kg)	
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1RU	
Operating Environment and Certifications		
Input Rating	100-240VAC, 60-50Hz	
Power Supply Efficiency Rating	N/A	
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Maximum Current	1.0A @100V, 0.5A @240V	
Power Consumption (Average / Maximum)	38 W / 40 W	43 W / 47 W
Heat Dissipation	138 BTU/hr	159 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	20% to 90% non-condensing	10% to 90% non-condensing
Noise Level	49 dBA	
Air Flow	Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	USGv6/IPv6	

* FortiOS 7.6.1+ is required for supporting up to 48 FSW. All prior releases support up to 32.

Note: All performance values are "up to" and vary depending on system configuration.

¹ IPsec VPN performance test uses AES256-SHA256.

² IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

³ SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

⁴ NGFW performance is measured with Firewall, IPS and Application Control enabled.

⁵ Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct ¹ , AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video ¹ Filtering, Malicious Certificate	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP) ²	•	•			
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS ²	•				
	Application Control		-----included with FortiCare Subscription-----			
	Inline CASB ¹		-----included with FortiCare Subscription-----			
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users ³					•
	FortiGate Cloud One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaas—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeolPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		-----included with FortiCare Subscription-----			

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

2. Full features available when running FortiOS 7.4.1.

3. Only supported on FortiGate models from the 100F onwards (F-series and all later series).
See the [FortiSASE Ordering Guide](#) for supported models and corresponding user license allocations.



FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.



Ordering Information

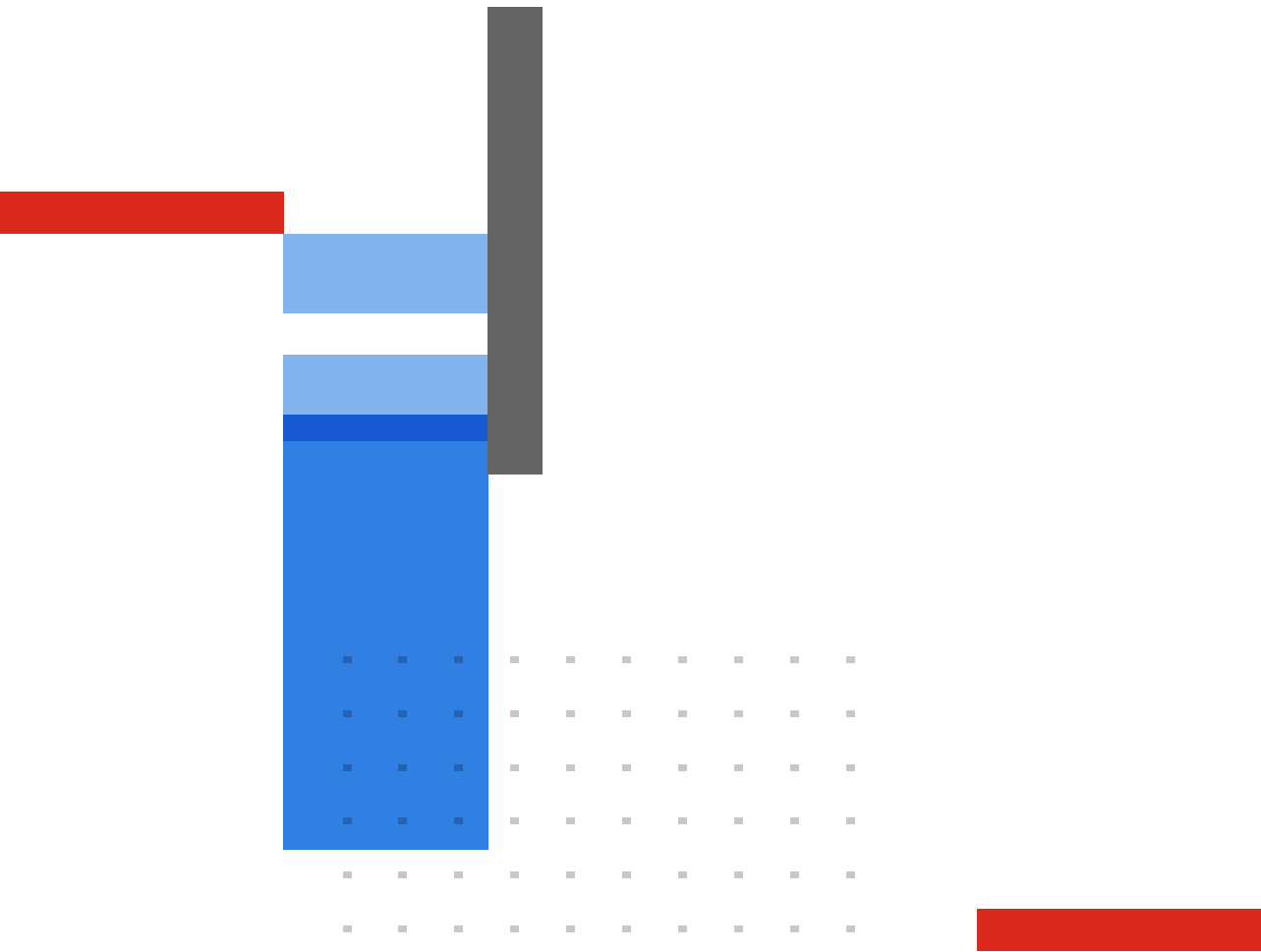
Product	SKU	Description
FortiGate 120G	FG-120G	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 4x 10GE SFP+ slots, SP5 hardware accelerated, dual AC power supplies.
FortiGate 121G	FG-121G	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, 4x 10GE SFP+ slots, SP5 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies.
Transceivers		
1 GE SFP EX Transceiver Module	FN-TRAN-EX	1 GE SFP EX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP Transceiver Module, 10km	FN-TRAN-SFP-1BD10	1 GE SFP transceiver module, 10km range single BiDi for systems with SFP slots (connects to FN-TRAN-1BU10, ordered separately).
1 GE SFP Transceiver Module, 40km	FN-TRAN-SFP-1BD40	1 GE SFP transceiver module, 40km long range single BiDi for systems with SFP slots (connects to FN-TRAN-1BU40, ordered separately).
1 GE SFP Transceiver Module, 10km	FN-TRAN-SFP-1BU10	1 GE SFP transceiver module, 10km range single BiDi for systems with SFP slots (connects to FN-TRAN-1BD10, ordered separately).
1 GE SFP Transceiver Module, 40km	FN-TRAN-SFP-1BU40	1 GE SFP transceiver module, 40km long range single BiDi for systems with SFP slots (connects to FN-TRAN-1BD40, ordered separately).
100M SFP transceiver module, long range 2km	FN-TRAN-SFX	100M SFP transceiver module with SGMII interface, long range 2km, LC connector, MMF, 1310nm, -40°C to 85°C, for systems with SFP slots and capable of 100M mode selection.
1 GE SFP SGC Transceiver Module	FN-TRAN-SGC	SGMII host interface, copper 10M/100M/1000M
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP ZX Transceiver Module	FN-TRAN-ZX	1 GE SFP ZX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER-BD27	10GE SFP+ transceiver module, Extended range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+ER-BD33, ordered separately).
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER-BD33	10GE SFP+ transceiver module, Extended range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+ER-BD27, ordered separately).
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE copper SFP+ RJ45 Transceiver Module (80m Range)	FN-TRAN-SFP+GC-T80	10 GE copper SFP+ RJ45 transceiver module (80m range) for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10 GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
Cables		
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.