October 8, 2013

Connie Oswald
Department of Administration
Purchasing Division
2019 Washington Street East Charleston
WV 25305-0130

RE: RFP TAX14006

Ms. Oswald:

AdvizeX Technologies, LLC (AdvizeX) appreciates the opportunity to respond to your RFP related to the one-time purchase of SSL VPN and Authentication hardware and software.

I, Todd May, am the authorized contact person that can speak on behalf of AdvizeX.

My contact information is as follows:

Todd May
Client Relationship Manager
AdvizeX
6480 Rockside Woods Blvd. South, Suite 190
Independence, OH 44131
216-901-1818 x4110
tmay@advizex.com

Based upon our review of RFP TAX14006, it is confirmed that AdvizeX meets all mandatory requirements established in said RFP.

We are looking forward to the next step in this authorization process.

Sincerely,

Todd May
Client Relationship Manager

10/09/13 10:41:18 AM
West Virginia Purchasing Division

# Table of Contents

## 1. SOLICITATION RESPONSE

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

**Solicitation**

| NUMBER | PAGE |
|---|---|
| TAX14006 | 1 |

ADDRESS CORRESPONDENCE TO ATTENTION OF:
CONNIE OSWALD
304-558-2157

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
STATE TAX DIVISION
INFORMATION TECHNOLOGY DIV
1206 QUARRIER STREET
2ND FLOOR
CHARLESTON, WV
25301-1725 304-558-8850

DATE PRINTED: 09/11/2013
BID OPENING DATE: 10/10/2013 BID OPENING TIME 1:30PM

| LINE | QUANTITY | UOP | CAT. NO. | ITEM NUMBER | UNIT PRICE | AMOUNT |
|---|---|---|---|---|---|---|
| | THE STATE OF WEST VIRGINIA AND ITS AGENCY THE WEST VIRGINIA STATE TAX DIVISION REQUEST A QUOTE TO PROVIDE THE ONE TIME PURCHASE OF A SSL VPN SOLUTION AND MULTI-FACTOR AUTHENTICATION SOLUTION USING HARDWARE TOKENS PER THE ATTACHED SPECIFICATIONS, TERMS & CONDITIONS AND INSTRUCTIONS TO BIDDERS. | | | | | |
| 0001 | 2 | EA | | 920-04 SSL VPN HARDWARE APPLIANCE | 15,847 | 31,694 |
| 0002 | 2 | EA | | 920-04 1 YEAR EXTENDED SERVICE AGREEMENT FOR VPN APPLIANCE | INCL. W/ ABOVE | |
| 0003 | 2 | EA | | 920-04 SSL VPN LICENSING FOR 100 CONCURRENT USERS WITH THE PHYSICAL DEVICES IN SEPARATE LOCATIONS. | INCL. W/ ABOVE | |

| SIGNATURE | TELEPHONE | DATE |
|---|---|---|
| Todd May | 216-901-1818 | 10-8-13 |
| TITLE Acct Mgr | FEIN | ADDRESS CHANGES TO BE NOTED ABOVE |

WHEN RESPONDING TO SOLICITATION, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

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

## Solicitation

| NUMBER | PAGE |
|---|---|
| TAX14006 | 2 |

ADDRESS CORRESPONDENCE TO ATTENTION OF:
CONNIE OSWALD
304-558-2157

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
STATE TAX DIVISION
INFORMATION TECHNOLOGY DIV
1206 QUARRIER STREET
2ND FLOOR
CHARLESTON, WV
25301-1725 304-558-8850

DATE PRINTED
09/11/2013

BID OPENING DATE: 10/10/2013 BID OPENING TIME 1:30PM

| LINE | QUANTITY | UOP | CAT. NO. | ITEM NUMBER | UNIT PRICE | AMOUNT |
|---|---|---|---|---|---|---|
| 0004 | 2 | EA | | 920-04 | INCL. W/ ABOVE | |
| | HARDWARE APPLIANCES FOR MULTI-FACTOR AUTHENTIFICATION USING HARDWARE TOKENS. | | | | | |
| 0005 | 90 | EA | | 920-04 | INCL. W/ ABOVE | |
| | APPLICATION BASE SOFTWARE LICENSING | | | | | |
| | | | | | 100 QUOTED | |
| 0006 | 90 | EA | | 920-04 | 2,930 | 2,930 |
| | HARDWARE TOKENS WITH 5 YEAR PROGRAMMABLE LIFESPAN | | | | | |
| 0007 | 90 | EA | | 920-04 | INCL. W/ ABOVE | |
| | HARDWARE TOKEN LICENSING FOR 5 YEARS | | | | | |
| 0008 | 90 | EA | | 920-04 | INCL. W/ ABOVE | |
| | 1 YEAR TECHNICAL SUPPORT/PHONE CONSULTING | | | | | |

SIGNATURE Todd May TELEPHONE 626-901-1810 DATE 10-8-13
TITLE ACCT MGR FEIN ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO SOLICITATION, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

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

**Solicitation**

| NUMBER | PAGE |
|---|---|
| TAX14006 | 3 |

ADDRESS CORRESPONDENCE TO ATTENTION OF:
CONNIE OSWALD
304-558-2157

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE

SHIP TO
STATE TAX DIVISION
INFORMATION TECHNOLOGY DIV
1206 QUARRIER STREET
2ND FLOOR
CHARLESTON, WV
25301-1725 304-558-8850

DATE PRINTED: 09/11/2013
BID OPENING DATE: 10/10/2013 BID OPENING TIME 1:30PM

| LINE | QUANTITY | UOP | CAT NO. | ITEM NUMBER | UNIT PRICE | AMOUNT |
|---|---|---|---|---|---|---|
| 0009 | 1 | EA | | 920-04 | 4 BLOCKS 709.60 | 2,836 |
| | INSTALLATION AND CONFIGURATION OF BOTH SOLUTIONS. | | | | | |
| | ****** THIS IS THE END OF RFQ TAX14006 ****** TOTAL: | | | | | 37,460 |

SIGNATURE: Todd May TELEPHONE: 216-901-1818 DATE: 10-8-13
TITLE: ACCT MGR FEIN: ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO SOLICITATION, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

# 2. UNDERSTANDING OF REQUEST

## *2.1 Purpose and Scope*

AdvizeX Technologies, LLC (AdvizeX) understands RFP# TAX14006 has been created to solicit bids on behalf of the West Virginia State Tax Department, an agency with approximately 90 end-users, for a one-time purchase of a SSL VPN solution and Multi-Factor Authentication solution using hardware tokens.

The proposed solution(s) are needed to pass IRS audits and need to be FIPS 140-2 compliant. The physical locations of the hardware appliances shall be the primary in the Capitol and secondary will be in the Office of Technology's Disaster Recovery building in Flatwoods, WV.

## *2.2 Functional Requirements*

The proposed solution must meet or exceed the requirements listed below:

### 2.2.1 Vendor Requirements

The vendor must provide the following with their solution:

1. Standard manufacturer warranty on all equipment listed on the pricing page
2. Quote 5 years of licensing costs for the MFA tokens
3. Quote any additional items on the Pricing Page that the VPN Solution and MFA Solution need to operate as intended
4. Provide a copy of the FIPS 140-2 Validation Certificate for the solutions bid
5. Bid hardware for the SSL VPN that will be supported for at least six years from the bid's closing date

### 2.2.2 VPN / MFA Authentication Solution Requirements

The VPN / MFA Authentication solution must provide the following:

1. Allow for redundancy; either in an active/passive or active/active state
2. Must be FIPS 140-2 compliant
3. Be compatible with the Multi Factor Solution
4. Be compatible with Windows 7 and 8
5. Produce audit records that contain sufficient information to establish what events occur, the sources of the events, and the outcomes of the events
6. Capable of logging security-relevant events, such as all successful login and logoff attempts, all unsuccessful login attempts, and the audit trail be protected from unauthorized access, use, deletion, or modification. After a set number of failed log in attempts, the user account must be locked out

7. Provide a mechanism to ensure duplicate user account names are not created, e.g., using operating systems functions to manage user accounts
8. Provide the capability of limiting the number of concurrent VPN Sessions that can be opened by a single user
9. Be compatible with Internet Explorer and Google Chrome
10. Be able to tie down a device by either the MAC address or the hard drive's serial number
11. The option of split tunneling to be disabled.
12. All cryptographic functions used by the VPN solution must use FIPS 1402 validated modules
13. The version of SSL to be used is SSL 3.1 (TLS 1.0)
14. Have a GUI/HTML interface
15. Have licensing for 100 concurrent users and be scalable to 250 concurrent users
16. Be capable of encrypting passwords before they are transmitted during authentication with FIPS 140-2 encryption
17. Have configurable session lengths, after which a user session is terminated due to inactivity
18. Be able of denying access to all personal devices; only state issued devices shall be permitted to use VPN
19. The hardware tokens for MFA must be in a key fob or credit card/business card sized form factor

### *2.3 Compliance to Requirements*

Our proposed solution meets the following functional requirements:

| The vendor must provide the following with their solution: | Compliant? |
|---|---|
| 1. Standard manufacturer warranty on all equipment listed on the pricing page | Yes |
| 2. Quote 5 years of licensing costs for the MFA tokens | Yes |
| 3. Quote any additional items on the Pricing Page that the VPN Solution and MFA Solution need to operate as intended | Yes |
| 4. Provide a copy of the FIPS 140-2 Validation Certificate for the solutions bid | Yes |
| 5. Bid hardware for the SSL VPN that will be supported for at least six years from the bid's closing date | Yes |

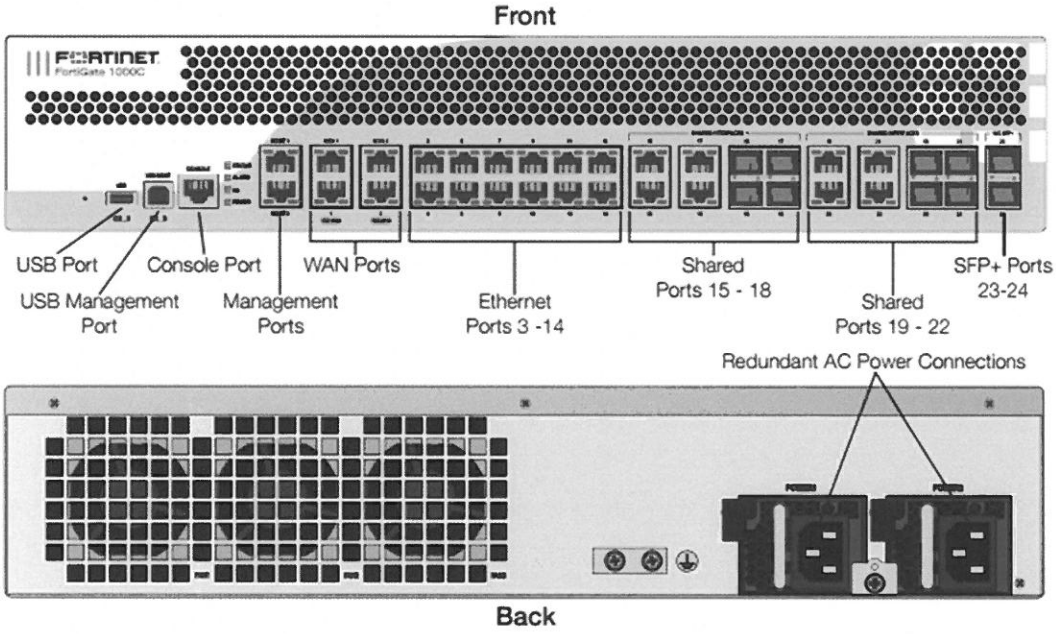
| The VPN / MFA Authentication solution must provide the following: | Compliant? |
|---|---|
| 1. Allow for redundancy; either in an active/passive or active/active state | Yes |
| 2. Must be FIPS 140-2 compliant | Yes |
| 3. Be compatible with the Multi Factor Solution | Yes |
| 4. Be compatible with Windows 7 and 8 | Yes |
| 5. Produce audit records that contain sufficient information to establish what events occur, the sources of the events, and the outcomes of the events | Yes |
| 6. Capable of logging security-relevant events, such as all successful login and logoff attempts, all unsuccessful login attempts, and the audit trail be protected from unauthorized access, use, deletion, or modification. After a set number of failed log in attempts, the user account must be locked out | Yes |
| 7. Provide a mechanism to ensure duplicate user account names are not created, e.g., using operating systems functions to manage user accounts | Yes |
| 8. Provide the capability of limiting the number of concurrent VPN Sessions that can be opened by a single user | Yes |

| | |
|---|---|
| 9. Be compatible with Internet Explorer and Google Chrome | Yes |
| 10. Be able to tie down a device by either the MAC address or the hard drive's serial number | Yes |
| 11. The option of split tunneling to be disabled. | Yes |
| 12. All cryptographic functions used by the VPN solution must use FIPS 1402 validated modules | Yes |
| 13. The version of SSL to be used is SSL 3.1 (TLS 1.0) | Yes |
| 14. Have a GUI/HTML interface | Yes |
| 15. Have licensing for 100 concurrent users and be scalable to 250 concurrent users | Yes, a maximum of 2,500+ is possible |
| 16. Be capable of encrypting passwords before they are transmitted during authentication with FIPS 140-2 encryption | Yes |
| 17. Have configurable session lengths, after which a user session is terminated due to inactivity | Yes |
| 18. Be able of denying access to all personal devices; only state issued devices shall be permitted to use VPN | Yes |
| 19. The hardware tokens for MFA must be in a key fob or credit card/business card sized form factor | Yes |

## *2.4 Recommended Solution Details*

AdvizeX has proposed the Fortinet FortiGate 1000C with one (1) year of 24 x 7 comprehensive support, the Fortiguard UTM Bundle, Advanced Hardware Replacement (Next Business Day), Firmware Upgrades, Antivirus Protection, IPS, Web Content Filtering, and Antispam.

### 2.4.1 Specifications




| FortiGate Model | FortiGate-1000C |
|---|---|
| **Hardware Specifications:** | |
| **10/100/1000 Accelerated Interfaces (RJ-45)** | 12 |
| **SFP and 10/100/1000 Shared Interfaces** | 8 |
| **10/100/1000 Bypass Interfaces** | 2 |
| **10/100/1000 Management Interfaces** | 2 |
| **SFP+ (10 Gb)** | 2 |
| **Maximum Network Interfaces** | 26 |
| **Internal Storage** | 128 GB |
| **USB (Client/Server)** | 1 / 1 |
| **System Performance:** | |
| **Firewall Throughput (1518 byte UDP)** | 16 Gb/s |
| **Firewall Throughput (512 byte UDP)** | 16 Gb/s |
| **Firewall Throughput (66 byte UDP)** | 16 Gb/s |

| | |
|---|---|
| **IPsec VPN Throughput (512 byte packets)** | 8 Gb/s |
| **Antivirus Throughput (Flow Based)** | 1.5 Gb/s |
| **Antivirus Throughput (Proxy Based)** | 500 Mbps |
| **IPS Throughput** | 3.5 Gb/s |
| **Gateway-to-Gateway IPsec VPN Tunnels (System / VDOM)** | 10,000 / 5,000 |
| **Client-to-Gateway IPsec VPN Tunnels** | 20,000 |
| **SSL-VPN Users (recommended max)** | 3,000 |
| **SSL-VPN Throughput** | 350 Mbps |
| **Concurrent Sessions (TCP)** | 2.5 M |
| **New Sessions/Sec (TCP)** | 75,000 |
| **Firewall Policies (Max)** | 100,000 |
| **Unlimited User Licenses** | Yes |
| **Virtual Domains (VDOMs)** | 10 |
| **High Availability Configurations** | Active/Active, Active/Passive, Clustering |
| **Dimensions** | |
| **Height** | 3.5 in ( 88 mm) |
| **Width** | 17 in (432 mm) |
| **Length** | 16.4 in ( 416 mm) |
| **Weight** | 24.6 lb. ( 11.2 kg) |
| **Rack Mountable** | Yes |
| **Environmental** | |
| **AC Power** | 100-240 VAC, 60-50 Hz |
| **Power Consumption (AVG)** | 132.8 W |
| **Heat Dissipation** | 566 BTU/h |
| **Power Consumption (Max)** | 166 W |
| **Redundant Power Supply** | Yes |
| **Operating Temperature** | 32 to 104°F (0 to 40°C) |
| **Storage Temperature** | -13 to 158°F (-25 to 70°C) |

All performance values are "up to" and vary depending on system configuration. Antivirus performance is benchmarked using traffic containing 32 Kbyte HTTP objects. IPS performance measured using 44 Kbyte HTTP files (similar to NSS Labs test methodology)

### 2.4.2 Solution Key Features

The FortiGate-1000C integrates essential security and networking functions into a single device to help identify and thwart multiple threats for mid-sized organizations and large branch offices of large enterprises. With numerous accelerated multi-threat security interfaces, organizations can create multiple security zones for various departments, users, access methods, and even devices to enforce network security at accelerated speeds.

By intercepting and inspecting network traffic at wire speeds, the FortiGate-1000C helps you identify and remove threats hidden within legitimate application traffic. With firewall performance of 20 Gb/s and IPS throughput of 3.5 Gb/s, the FortiGate-1000C is ideal for mid-to-large enterprise deployments. The FortiGate-1000C delivers the performance you need to control your organization's applications, data, and users without becoming a network bottleneck.

The most important features of the proposed solution include the following:

- Up to 20 Gb/s firewall performance and sub-10 microsecond latency ensures optimal performance for latency sensitive environments
- Advanced application control that enables administrators to define and enforce policies for thousands of applications running across networks regardless of port or the protocol used for communication
- DC power option for additional deployment flexibility
- Virtual private network (VPN) technology enforces complete content inspection and multi-threat protection. Traffic optimization prioritizes critical communications traversing VPN tunnels
- Data leakage prevention uses a sophisticated pattern-matching engine to help identify and prevent the transfer of sensitive information outside of network perimeters, even when applications encrypt their communications
- Available FortiManager and FortiAnalyzer appliances simplify security management and reduce operating expenses in multiple deployments
- FortiGuard Subscription Services deliver automated, real-time, up-to-date protection against security threats and exploits.

### 2.4.3 Unified Threat Management (UTM)

The FortiGate-1000C security platform delivers industry-leading performance and flexibility. You can deploy the right blend of essential hardware-accelerated security technologies now and in the future to meet your evolving network requirements. These technologies include firewall, VPN, intrusion prevention, application control, and web content filtering, all managed from a 'single pane of glass' management console. The FortiGate-1000C also includes additional security technologies such as antivirus/ antimalware, Antispam,

vulnerability management, and WAN optimization, allowing you to consolidate stand-alone devices.

The FortiGate-1000C gives you the ability to identify and stop numerous types of threats from a single device. For example, advanced application control enables you to define and enforce policies for thousands of applications running across your network, regardless of port or protocol used. Data leakage prevention technology, using a sophisticated pattern-matching engine, helps identify and prevent the accidental or intentional transfer of sensitive information outside of network perimeters, even when applications encrypt their communications.

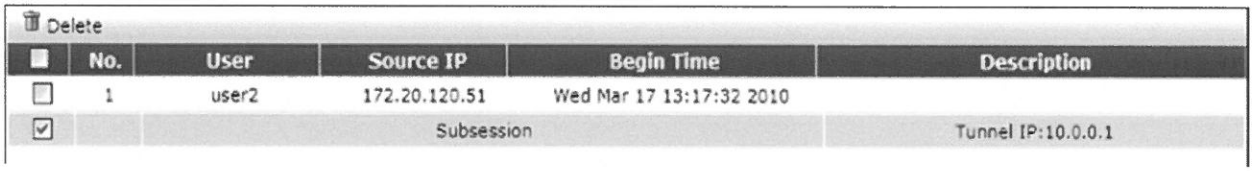
The high port density and types of ports of the FortiGate-1000C gives you the freedom to create multiple security zones for various departments, users, access methods, and even devices. There are eight (8) shared RJ-45/SFP Gigabit Ethernet ports for deployment flexibility, as well as two (2) bypass-protected ports to preserve network availability in the event of a device failure. In addition, 128 GB of onboard flash memory lets you deploy WAN optimization to reduce bandwidth consumption across your WAN connection, enable local reporting, or archive content locally.

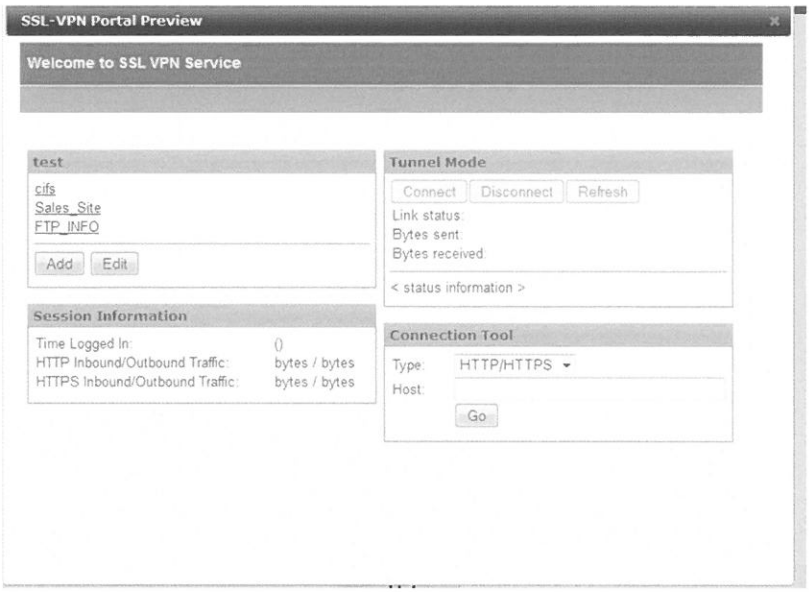
### 2.4.4 Monitoring SSL VPN Users

As requested in the RFP request, a web (GUI) management interface is required for the recommended solution.

With the FortiGate 1000c, you have the ability to manage and monitor VPN end-users with either a web-mode interface or tunnel-mode interface. Management can take place with either username and/or IP address.

For example, to monitor SSL VPN users, go to VPN > Monitor > SSL-VPN Monitor. To disconnect a user, select the user and then select the Delete icon.






## 2.4.5 SSL VPN Portal

SSL VPNs establish connectivity using SSL, which functions at Levels 4 - 5 (Transport and Session). Information is encapsulated at Levels 6 - 7 (Presentation and Application), and SSL VPNs communicate at the highest levels in the OSI model. SSL is not strictly a Virtual Private Network (VPN) technology allows clients to connect to remote networks in a secure way. A VPN is a secure logical network created from physically separate networks. VPNs use encryption and other security methods to ensure that only authorized users can access the network. VPNs also ensure that the data transmitted between computers cannot be intercepted by unauthorized users. When data is encoded and transmitted over the Internet, the data is said to be sent through a "VPN tunnel". A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.

The advantages of a VPN over an actual physical private network are two-fold. Rather than utilizing expensive leased lines or other infrastructure, you use the relatively inexpensive, high-bandwidth Internet. Perhaps more important though is the universal availability of the Internet - in most areas, access to the Internet is readily obtainable without any special arrangements or long wait times.

SSL (Secure Sockets Layer) as HTTPS is supported by most web browsers for exchanging sensitive information securely between a web server and a client. SSL establishes an encrypted link, ensuring that all data passed between the web server and the browser remains private and secure. SSL protection is initiated automatically when a user (client) connects to a web server that is SSL-enabled. Once the successful connection is established, the browser encrypts all the information before it leaves the computer. When the

information reaches its destination, it is decrypted using a secret (private) key. Any data sent back is first encrypted, and is decrypted when it reaches the client.

In addition, the following SSL and TLS are supported by the FortiGate 1000cC

Table 77. SSL and TLS version support table.

| Version | RFC |
|---|---|
| SSL 2.0 | RFC 6176 |
| SSL 3.0 | RFC 6101 |
| TLS 1.0 | RFC 2246 |
| TLS 1.1 | RFC 4346 |

### 2.4.6 FortiToken (Token Authentication Device)

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes every 60 seconds, and when not in use the LCD screen is blanked to extend the battery life.

There is also a mobile phone application, FortiToken Mobile that performs much the same function. FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

Any time information about the FortiToken is transmitted, it is encrypted. When the FortiGate unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPsec VPN, SSL VPN, and even Administrators. See "Associating FortiTokens with accounts".

A FortiToken can be associated with only one account on one FortiGate unit.

If a user loses their FortiToken, it can be locked out using the FortiGate so it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiGate to allow access once again. See "FortiToken maintenance".

## ATTACHMENT A – FIPS 140-2 CONSOLIDATED VALIDATION CERTIFICATE

### FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America


The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0029

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions. Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: 5 June 2013

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 4 June 2013

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Page 1 of 4

6/3/2013

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|---|---|---|---|---|
| **1917** | 05/21/2013 | Brocade® MLXe® and Brocade NetIron® CER Series Ethernet Routers | Brocade Communications Systems, Inc. | Hardware Versions: BR-MLXE-4-MR-M-AC, BR-MLXE-4-MR-M-DC, BR-MLXE-8-MR-M-AC, BR-MLXE-8-MR-M-DC, BR-MLXE-16-MR-M-AC, BR-MLXE-16-MR-M-DC, NI-CER-2024C-ADVPREM-AC, NI-CER-2024C-ADVPREM-DC, NI-CER-2024F-ADVPREM-AC, NI-CER-2024F-ADVPREM-DC, NI-CER-2048FX-ADVPREM-AC, NI-CER-2048FX-ADVPREM-DC, NI-CER-2048F-ADVPREM-AC, NI-CER-2048F-ADVPREM-DC, NI-CER-2048C-ADVPREM-AC, NI-CER-2048C-ADVPREM-DC, NI-CER-2048CX-ADVPREM-AC and NI-CER-2048CX-ADVPREM-DC with FIPS Kit (P/N Brocade XBR-000195) and NI-MLX-MR Management Module; Firmware Version: IronWare Software R05.1.01a |
| **1942** | 05/02/2013 | Cisco Catalyst C4500X-32SFP+ and Catalyst C4500X-F-32SFP+ | Cisco Systems, Inc. | Hardware Versions: Catalyst C4500X-32SFP+ and Catalyst C4500X-F-32SFP+; FIPS kit packaging (CVPN4500FIPS/KIT=); Firmware Version: 3.3.1SG |
| **1943** | 05/02/2013 | Evolution e8350™ - Satellite Router [1], iConnex e800™ - Satellite Router Board [2], iConnex e850MP™ Satellite Router Board [3], iConnex e850MP™ - IND Satellite Router Board [4], iConnex e850MP™ - IND with Heat Sink Satellite Router Board [5], Evolution eM1D1™ Line Card [6] and Evolution eM0DM™ | VT iDirect, Inc. | Hardware Versions: Part #E0000051-0003 [1]; Part #E0001340-0002 [2]; Part #E0000731-0001 [3]; E0000731-0002 [4]; Part #E0000731-0003 [5]; Part #E0000080-0002 [6]; Part #E0000080-0005 [7]; Firmware Version: iDX version 2.3.1 |
| **1944** | 05/03/2013 | Apple iOS CoreCrypto Kernel Module, v3.0 | Apple Inc. | Software Version: 3.0 |

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|---|---|---|---|---|
| **1946** | 05/14/2013 | TW-400 (CUB) | TrellisWare Technologies Inc. | Hardware Version: ASY0540250 rev X1; Firmware Version: 4c-beta2-FIPS |
| **1947** | 05/16/2013 | TW-230 (CheetahNet II) | TrellisWare Technologies Inc. | Hardware Version: ASY0560001 rev X2; Firmware Version: 4c-beta2-FIPS |
| **1948** | 05/16/2013 | Samsung OpenSSL Cryptographic Module | Samsung Electronics Co., Ltd. | Software Version: SFOpenSSL1.0.0e-1.1 |
| **1949** | 05/16/2013 | Harris AES Software Load Module | Harris Corporation | Software Version: R04A01 |
| **1950** | 05/23/2013 | FortiGate-1000C [1], FortiGate-1240B [2] and FortiGate-3140B [3] | Fortinet, Inc. | Hardware Versions: C4HR40 [1], C4CN43 [2] and C4XC55 [3] with Tamper Evident Seal Kits: FIPS-SEAL-RED [1,3] or FIPS-SEAL-BLUE [2]; Firmware Version: FortiOS 4.0, build 8963, 121031 |
| **1951** | 05/23/2013 | FortiGate-80C [1], FortiGate-110C [2], FortiGate-60C [3] and FortiWiFi-60C [4] | Fortinet, Inc. | Hardware Versions: C4BC61 [1], C4HA15 [2], C4DM93 [3] and C4DM95 [4] with Tamper Evident Seal Kits: FIPS-SEAL-BLUE [1,2] or FIPS-SEAL-RED [3,4]; Firmware Version: FortiOS 4.0, build 8963, 121031 |
| **1952** | 05/23/2013 | 3S Group Cryptographic Module (3SGX) | 3S Group Incorporated | Hardware Version: 1.0; Firmware Version: 1.0 |
| **1953** | 05/23/2013 | NXP JCOP 2.4.2 R2 | NXP Semiconductors | Hardware Versions: P5CC081 V1A, P5CD081 V1A, P5CD081 V1D, P5CC145 V0B and P5CD145 V0B; Firmware Versions: JCOP 2.4.2 R2 Mask ID 59 and patchID 3 with Demonstration Applet v1.0 |

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

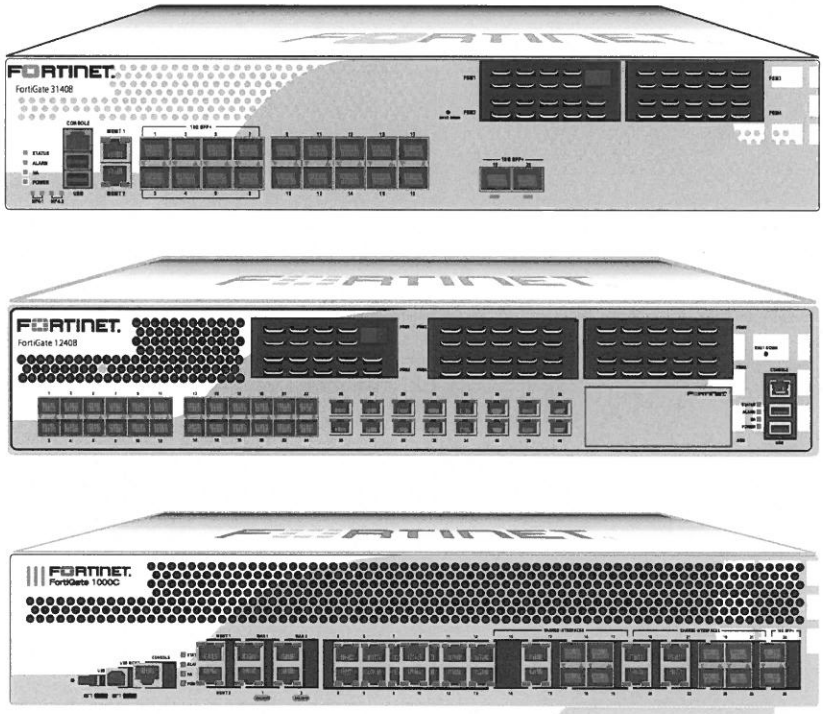
| Certificate Number | Validation / Posting Date | Module Name(s) | Vendor Name | Version Information |
|---|---|---|---|---|
| 1954 | 05/30/2013 | Enhanced Bandwidth Efficient Modem (EBEM) Cryptographic Module | ViaSat, Inc. | Hardware Versions: P/Ns 1010162 Version 1, 1010162 with ESEM Version 1, 1091549 Version 1, 1075559 Version 1, 1075559 with ESEM Version 1, 1091551 Version 1, 1010163 Version 1, 1010163 with ESEM Version 1, 1091550 Version 1, 1075560 Version 1, 1075560 with ESEM Version 1 and 1091552 Version 1; Firmware Version: 02.03.02 |

## ATTACHMENT B – FORTINET FIPS 140-2 SECURITY POLICY

Please refer to the attached document.

# FIPS 140-2 Security Policy

## FortiGate-1000C/1240B/3140B




| *FortiGate-1000C/1240B/3140B FIPS 140-2 Security Policy* | | | |
|---|---|---|---|
| **Document Version:** | 2.0 | | |
| **Publication Date:** | April 16, 2013 | | |
| **Description:** | Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation. | | |
| **Firmware Version:** | FortiOS 4.0, build8963, 121031 | | |
| **Hardware Version:** | FortiGate-1000C(C4HR40) | FortiGate-3140B (C4XC55) | |
| | FortiGate-1240B (C4CN43) | | |

*FortiGate-1000C/1240B/3140B: FIPS 140-2 Security Policy*

01-436-176271-20120718

for FortiOS 4.0 MR3



**Trademarks**

# Contents

# Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiGate-1000C, 1240B and 3140B Multi-Threat Security Systems. This policy describes how the FortiGate-1000C, 1240B and 3140B (hereafter referred to as the 'modules') meet the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. This policy was created as part of the Level 2 FIPS 140-2 validation of the modules.

This document contains the following sections:

- Introduction
- Security Level Summary
- Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation
- Self-Tests
- Non-FIPS Approved Services

The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

## References

This policy deals specifically with operation and implementation of the module in the technical terms of the FIPS 140-2 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at http://docs.forticare.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at http://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at http://www.fortinet.com/support
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at http://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

# Introduction

The FortiGate product family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. FortiGate appliances detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance. In addition to providing application level firewall protection, FortiGate appliances deliver a full range of network-level services — VPN, intrusion prevention, web filtering, antivirus, antispam and traffic shaping — in dedicated, easily managed platforms.

All FortiGate appliances employ Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ firmware achieve breakthrough price/performance. The unique, ASIC-based architecture analyzes content and behavior in real time, enabling key applications to be deployed right at the network edge where they are most effective at protecting enterprise networks. They can be easily configured to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, and related devices, or as complete network protection systems. The modules support High Availability (HA) in both Active-Active (AA) and Active-Passive (AP) configurations.

FortiGate appliances support the IPSec industry standard for VPN, allowing VPNs to be configured between a FortiGate appliance and any client or gateway/firewall that supports IPSec VPN. FortiGate appliances also provide SSL VPN services using TLS 1.0 in the FIPS-CC mode of operation.

# Security Level Summary

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

**Table 1: Summary of FIPS security requirements and compliance levels**

| Security Requirement | Compliance Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | 2 |
| Cryptographic Key Management | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | 2 |

# Module Description

The FortiGate-1000C, 1240B and 3140B are multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements.

The modules have a similar appearance and perform the same functions, but have different numbers and types of network interfaces in order to support different network configurations:

- The FortiGate-1000C has 36 network interfaces with a status LED for each network interface(2x 10GB SP+, 16x shared interfaces (1GB SFP or 10/100/1000 Base-T), 18x 10/100/1000 Base-T)
- The FortiGate-1240B has 40 network interfaces with a status LED for each network interface (24x 1GB SFP, 16x 10/100/1000 Base-T)

- The FortiGate-3140B has 22 network interfaces with a status LED for each network interface (10x 10GB SFP+, 10x 1GB SFP, 2x 10/100/1000 Base-T)

The modules have one, quad core, x86 compatible CPU.

The modules are 2u rackmount devices.

The modules have 3 ventilation fans on the rear panel of the chassis.

The FortiGate-1000C module has 16 shared network interfaces that support a 1GB SFP or 10/100/1000Base-T connection. Only one of the shared interface pair can be used at any given time. The FortiGate-1000C module also has 4 paired Bypass interfaces (WAN1/Port1 and WAN2/Port2). If bypass is enabled, these interfaces provide a physical bypass of the paired port if the module fails, hangs or power is lost. The bypass capability is only available if the module is configure for Transparent operation, not NAT operation. Use of the bypass capability is a non-FIPS approved service.

The FortiGate-1000C has 2 internal, 128GB solid state drives (SSDs).

The FortiGate-1240B module has 6 Fortinet Storage Module (FSM) slots that support removable solid state drives (SSDs). One FSM is installed by default. The module also has one Advanced Mezzanine Card (AMC) slot that can be used to add additional network interfaces. Use of the AMC slot is optional and the AMC slot is excluded from the scope of this FIPS 140-2 validation.

The FortiGate-3140B module has 4 Fortinet Storage Module (FSM) slots that support removable solid state drives (SSDs). One FSM is installed by default.

The FortiGate-1240B and 3140B modules have a pinhole shutdown button that is used to halt the SSDs so they can be hot swapped.

The validated firmware version is FortiOS 4.0, build8963, 121031.

Figure 1, Figure 2 and Figure 3, are representative of the modules tested.

## Cryptographic Module Ports and Interfaces

### FortiGate-1000C

**Figure 1: FortiGate-1000C Front and Rear Panels**

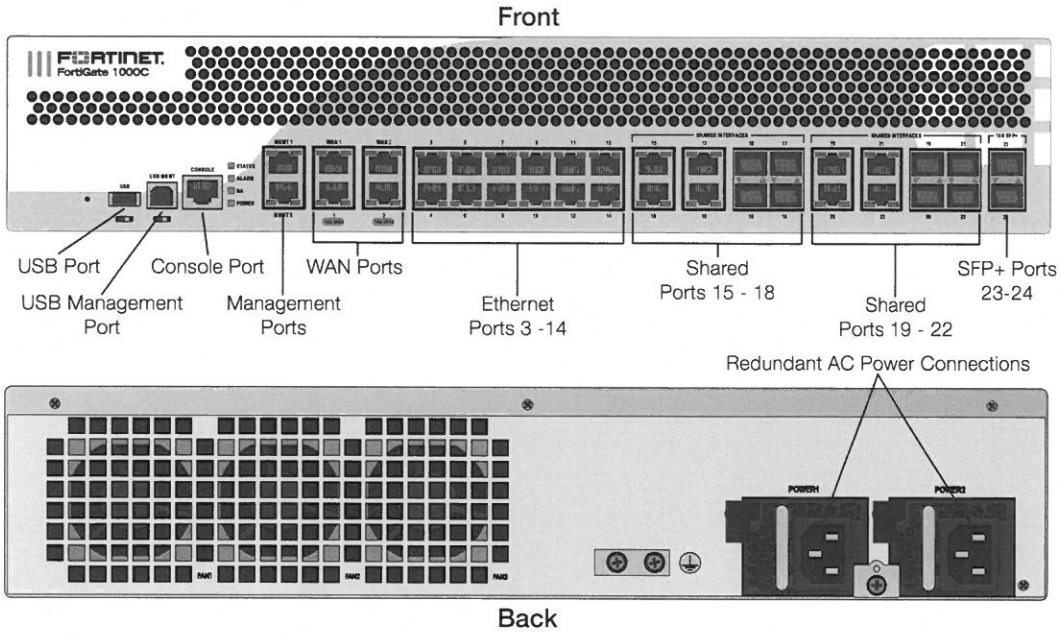



**Table 2: FortiGate-1000C Status LEDs**

| LED | | State | Description |
|---|---|---|---|
| Power | | Green | The module is powered on. |
| | | Off | The module is powered off. |
| Status | | Flashing | The module is starting up. |
| | | Green | The module is running normally. |
| | | Off | The module is powered off. |
| HA | | Green | HA is enabled. |
| | | Red | The module is in failover mode. |
| | | Off | The modules in stand-alone mode. |
| Alarm | | Red | The module is indicating a major fault. |
| | | Amber | The module is indicating a minor fault. |
| | | Off | The module is operating normally. |
| MGMT ports, WAN ports, ports 1-22 (Ethernet) | Link | Green | Port is online. |
| | | Flashing | Port is receiving or sending data. |
| | Activity | Green | Connected at 1000Mbps. |
| | | Amber | Connected at 100Mbps. |
| | | Off | Connected at 10Mbps. |
| Ports 15-24 (SFP) | | Green | Port is online. |
| | | Flashing | Port is receiving or sending data. |

**Table 3: FortiGate-1000C Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| MGMT ports, WAN ports, ports 1-22 | RJ-45 | 10/100/1000 Base-T | Data input, data output, control input and status output | Copper gigabit connection to 10/100/1000 copper networks. |
| Ports 15-22 | SFP | 1 Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Ports 22-24 | SFP+ | 10 Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| CONSOLE | RJ-45 | 9600 bps | Control input, status output | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB Port | USB | N/A | Key loading and archiving, configuration backup and restore | Optional connection for USB token. |
| USB MGMT | USB | N/A | Control input, status output | Optional connection for management/configuration using FortiExplorer. |

**Table 4: FortiGate-1000C Rear Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| POWER | N/A | N/A | Power | 120/240VAC power connection. |

## FortiGate-1240B

**Figure 2: FortiGate-1240B Front and Rear Panels**

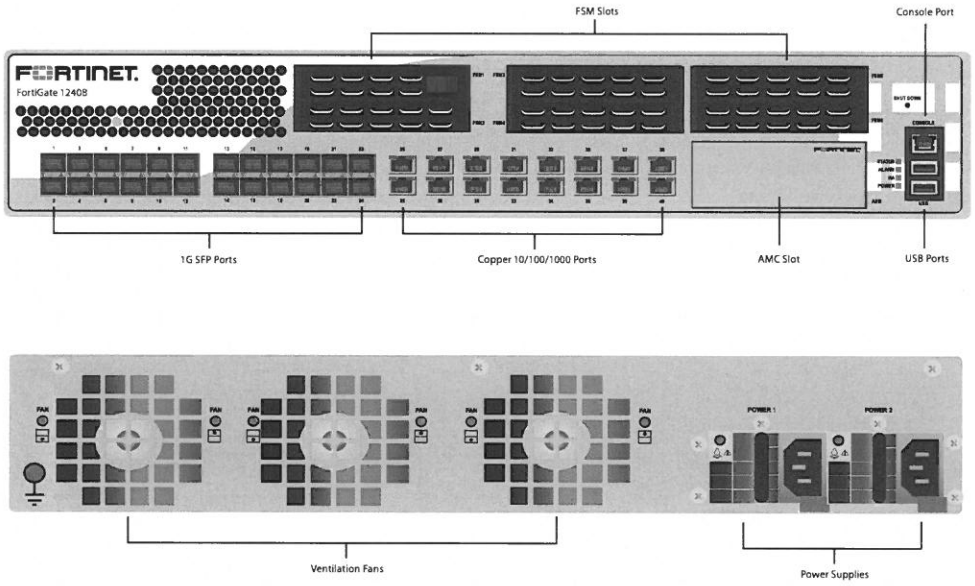



**Table 5: FortiGate-1240B Status LEDs**

| LED | | State | Description |
|---|---|---|---|
| Power | | Green | The module is powered on. |
| | | Off | The module is powered off. |
| Status | | Flashing | The module is starting up. |
| | | Green | The module is running normally. |
| | | Off | The module is powered off. |
| HA | | Yellow | HA is enabled. |
| | | Off | The unit is in stand-alone mode. |
| Alarm | | N/A | Future use. |
| Ports 1 to 24 | Link | Green | Port is online. |
| | | Off | Port is offline. |
| | Activity | Flashing | Port is receiving or sending data. |
| | | Off | Port may be on, but is not receiving or sending data. |

| | | | |
|---|---|---|---|
| Ports 25 to 40 | Link | Green | Port is online. |
| | | Flashing | Port is receiving or sending data. |
| | Activity | Green | Connected at 1000 Mbps. |
| | | Amber | Connected at 100 Mbps. |
| | | Off | Connected at 10Mbps. |
| AC Power | | Green | AC power is connected and has power. |
| | | Amber | AC power is not connected. |
| Fan | | Green | The fan is running and within the speed range. |
| | | Off | The fan is not running or is over the speed range. |

**Table 6: FortiGate-1240B Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| Ports 1 to 24 | SFP | 1 Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Ports 25 to 40 | RJ-45 | 10/100/1000 Base-T | Data input, data output, control input and status output | Copper gigabit connection to 10/100/1000 copper networks. |
| CONSOLE | RJ-45 | 9600 bps | Control input, status output | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB | USB | N/A | Key loading and archiving, configuration backup and restore | Optional connection for USB token. |

**Table 7: FortiGate-1240B Rear Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| POWER | N/A | N/A | Power | 120/240VAC power connection. |

## FortiGate-3140B

**Figure 3: FortiGate-3140B Front and Rear Panels**

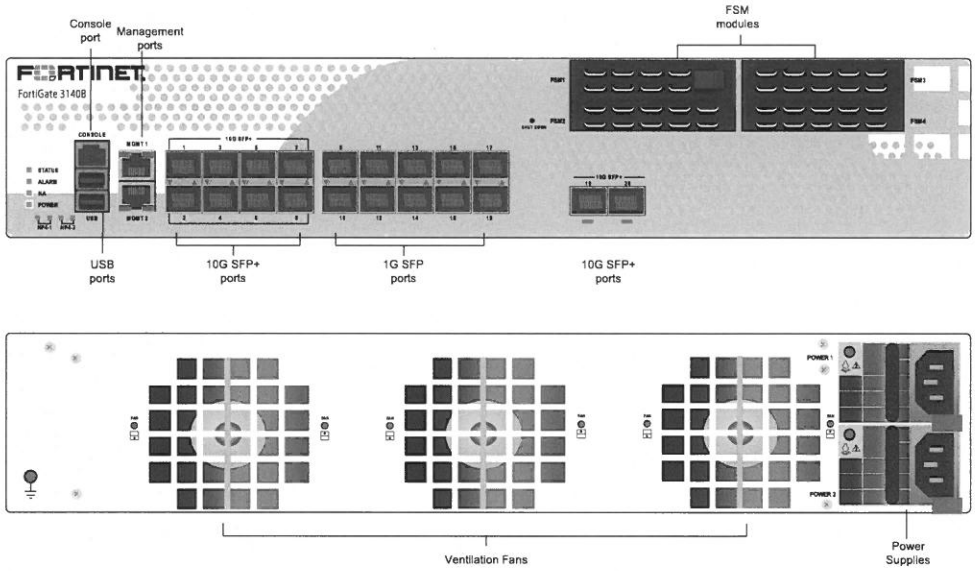



**Table 8: FortiGate-3140B Status LEDs**

| LED | | State | Description |
|---|---|---|---|
| Power | | Green | The module is powered on. |
| | | Off | The module is powered off. |
| Status | | Flashing | The module is starting up. |
| | | Green | The module is running normally. |
| | | Off | The module is powered off. |
| HA | | Green | HA is enabled and in normal mode. |
| | | Red | HA is enabled but in failover mode. |
| | | Off | The unit is in stand-alone mode. |
| Alarm | | N/A | Future use. |
| Ports 1 to 20 | Link | Green | Port is online. |
| | | Off | Port is offline. |
| | Activity | Flashing | Port is receiving or sending data. |
| | | Off | Port may be on, but is not receiving or sending data. |
| Management Ports 1 and 2 | Link | Green | Port is online. |
| | | Flashing | Port is receiving or sending data. |
| | Activity | Green | Connected at 1000 Mbps. |
| | | Amber | Connected at 100 Mbps. |
| | | Off | Connected at 10Mbps. |

| | | |
|---|---|---|
| AC Power | Green | AC power is connected and has power. |
| | Amber | AC power is not connected. |
| Fan | Green | The fan is running and within the speed range. |
| | Off | The fan is not running or is over the speed range. |

**Table 9: FortiGate-3140B Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| Ports 1 to 8, 19 and 20 | SFP+ | 10 Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Ports 9 to 18 | SFP | 1Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Management 1 and 2 | RJ-45 | 10/100/1000 Base-T | Data input, data output, control input and status output | Copper gigabit connection to 10/100/1000 copper networks. |
| CONSOLE | RJ-45 | 9600 bps | Control input, status output | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB | USB | N/A | Key loading and archiving, configuration backup and restore | Optional connection for USB token. |

**Table 10: FortiGate-3140B Rear Panel Connectors and Ports**

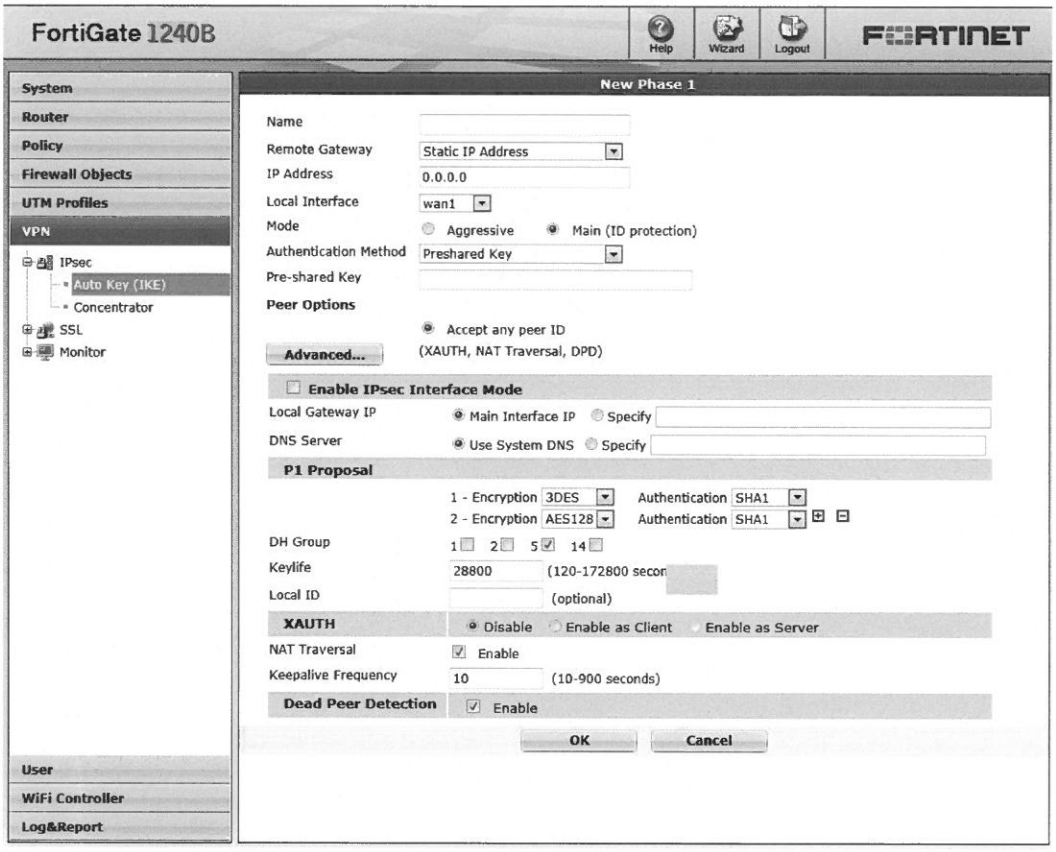
| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| POWER | N/A | N/A | Power | 120/240VAC power connection. |

## Web-Based Manager

The FortiGate web-based manager provides GUI based access to the module and is the primary tool for configuring the module. The manager requires a web browser on the management computer and an Ethernet connection between the FortiGate unit and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.0 is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

**Figure 4: The FortiGate web-based manager**




## Command Line Interface

The FortiGate Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiGate unit and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required (SSH v1.0 is not supported in FIPS-CC mode). Telnet access to the CLI is not allowed in FIPS-CC mode and is disabled.

## Roles, Services and Authentication

### Roles

When configured in FIPS-CC mode, the module provides the following roles:

- Crypto Officer
- Network User

The Crypto Officer role is initially assigned to the default 'admin' operator account. The Crypto Officer role has read-write access to all of the module's administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read/write or read only access permissions including the ability to create operator accounts.

The module provides a **Network User** role for end-users (Users). Network users can make use of the encrypt/decrypt services, but cannot access the module for administrative purposes.

The module does not provide a Maintenance role.

## FIPS Approved Services

The following tables detail the types of FIPS approved services available to each role, the types of access for each role and the Keys or CSPs they affect.

The role names are abbreviated as follows:

| | |
|---|---|
| **Crypto Officer** | CO |
| **User** | U |

The access types are abbreviated as follows:

| | |
|---|---|
| **Read Access** | R |
| **Write Access** | W |
| **Execute Access** | E |

**Table 11: Services available to Crypto Officers**

| Service | Access | Key/CSP |
|---|---|---|
| authenticate to module | WE | Operator Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, RNG Seed, RNG AES Key |
| show system status | WE | N/A |
| show FIPS-CC mode enabled/disabled (console/CLI only) | WE | N/A |
| enable FIPS-CC mode of operation (console only) | WE | Configuration Integrity Key |
| execute factory reset (zeroize keys, disable FIPS mode, console/CLI only) | E | See "Key Zeroization" on page 19 |
| execute FIPS-CC on-demand self-tests (console only) | E | Configuration Integrity Key, Firmware Integrity Key |
| add/delete operators and network users | WE | Operator Password, Network User Password |
| set/reset operator and network user passwords | WE | Operator Password, Network User Password |
| backup configuration file | WE | Configuration Encryption Key, Configuration Backup Key |
| read/set/delete/modify module configuration | WE | N/A |
| enable/disable alternating bypass mode | WE | N/A |

**Table 11: Services available to Crypto Officers**

| Service | Access | Key/CSP |
|---|---|---|
| read/set/delete/modify IPSec/SSL VPN configuration | N/A | IPSec: IPSec Manual Authentication Key, IPSec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key<br>SSL: HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS SSH Session Encryption Key |
| read/set/delete/modify HA configuration | WE | HA Password, HA Encryption Key |
| execute firmware update | E | Firmware Update Key |
| read log data | WE | N/A |
| delete log data (console/CLI only) | N/A | N/A |
| execute system diagnostics (console/CLI only) | WE | N/A |

**Table 12: Services available to Network Users**

| Service/CSP | Access | Key/CSP |
|---|---|---|
| authenticate to module | E | Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Seed, RNG AES Key |
| IPSec VPN controlled by firewall policies | E | Diffie-Hellman Key, IKE and IPSec Keys, RNG Seed, RNG AES Key |
| SSL VPN controlled by firewall policies | E | Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Seed, RNG AES Key |

## Authentication

The modules implement identity based authentication. Operators must authenticate with a user-id and password combination to access the modules remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS) or SSH. Password entry is obfuscated using asterisks and the module does not provide feedback on the authentication process - i.e. the module does not indicate if the password or the user/operator account is incorrect for a failed authentication attempt.

By default, Network User access to the modules is based on firewall policy and authentication by IP address or fully qualified domain names. Network Users can optionally be forced to authenticate to the modules using a username/password combination to enable use of the IPSec VPN encrypt/decrypt or bypass services. For Network Users invoking the SSL-VPN encrypt/decrypt services, the modules support authentication with a user-id/password combination. Network User authentication is done over HTTPS and does not allow access to the modules for administrative purposes.

Note that operator authentication over HTTPS/SSH and Network User authentication over HTTPS are subject to a limit of 3 failed authentication attempts in 1 minute. Operator authentication using the console is not subject to a failed authentication limit, but the number of authentication attempts per minute is limited by the bandwidth available over the serial connection.

The minimum password length is 8 characters when in FIPS-CC mode (maximum password length is 32 characters). The password may contain any combination of upper- and lower-case letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of guessing a password are 1 in 94^8 which is significantly lower than one in a million. Recommended procedures to increase the password strength are explained in "FIPS 140-2 Compliant Operation" on page 24.

For Network Users invoking the IPSec VPN encrypt/decrypt services, the module acts on behalf of the Network User and negotiates a VPN connection with a remote module. The strength of authentication for IPSec services is based on the authentication method defined in the specific firewall policy: IPSec manual authentication key, IKE pre-shared key or IKE RSA key (RSA certificate). The odds of guessing the authentication key for each IPSec method is:

- 1 in $16^{40}$ for the IPSec Manual Authentication key (based on a 40 digit, hexadecimal key)
- 1 in $94^{8}$ for the IKE Pre-shared Key (based on an 8 character, ASCII printable key)
- 1 in $2^{1024}$ for the IKE RSA Key (based on a 1024bit RSA key size)

Therefore the minimum odds of guessing the authentication key for IPSec is 1 in $94^{8}$, based on the IKE Pre-shared key.

## Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of tamper-evident seals to secure the overall enclosure.

The seals are either blue wax/plastic with white lettering that reads "Fortinet Inc. Security Seal" (FortiGate-1240B) or serialized red wax/plastic with black lettering that reads "Fortinet Security Seal" (FortiGate-1000C and FortiGate-3140B).

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto Officer is also responsible for securing and controlling any unused seals.

The surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Ensure the surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and clean the surface with an adhesive remover before following the instructions for applying a new seal.

Additional seals can be requested through your Fortinet sales contact. Reference the following SKUs when ordering: FIPS-SEAL-RED or FIPS-SEAL-BLUE. Specify the type and number of seals required based on the specific module as described below:

The FortiGate-1000C uses 4 red seals to secure:

- the external enclosure (2 seals, see Figure 5 and Figure 6)
- the power supplies (2 seals, see Figure 7)

The FortiGate-1240B uses 5 blue seals to secure:

- the external enclosure (2 seals, see Figure 8 and Figure 9)
- the blank faceplate covering the AMC slot (one seal, see Figure 10)
- the power supplies (2 seals, see Figure 11)

The FortiGate-3140B uses 2 red seals to secure:

- the external enclosure (2 seals, see Figure 12 and Figure 13)

**Figure 5: FortiGate-1000C external enclosure seal, top, right side**

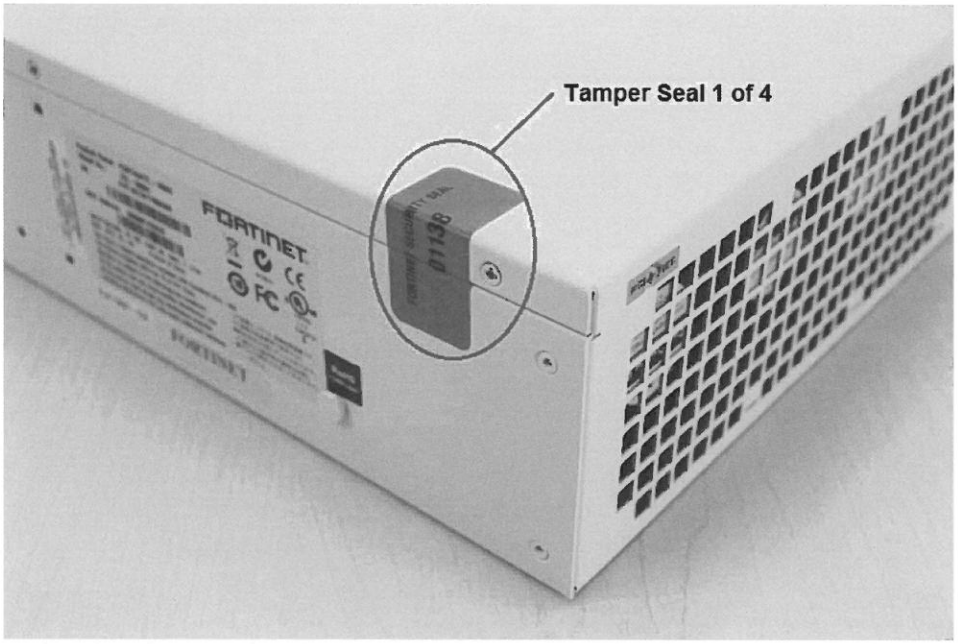



**Figure 6: FortiGate-1000C external enclosure seal, top, left side**

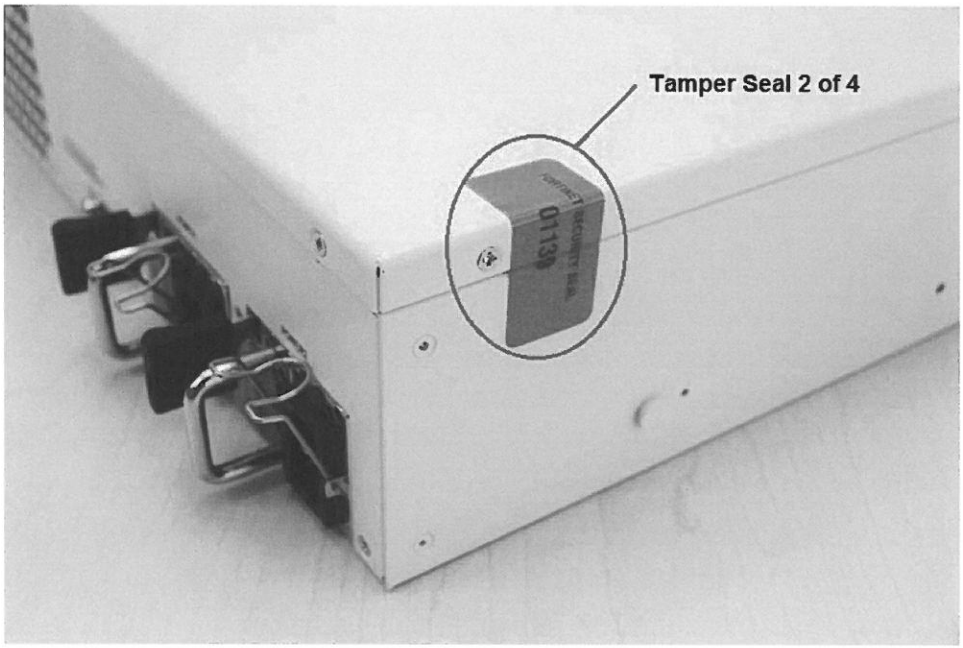


**Figure 7: FortiGate-1000C power supply seals, rear, bottom**

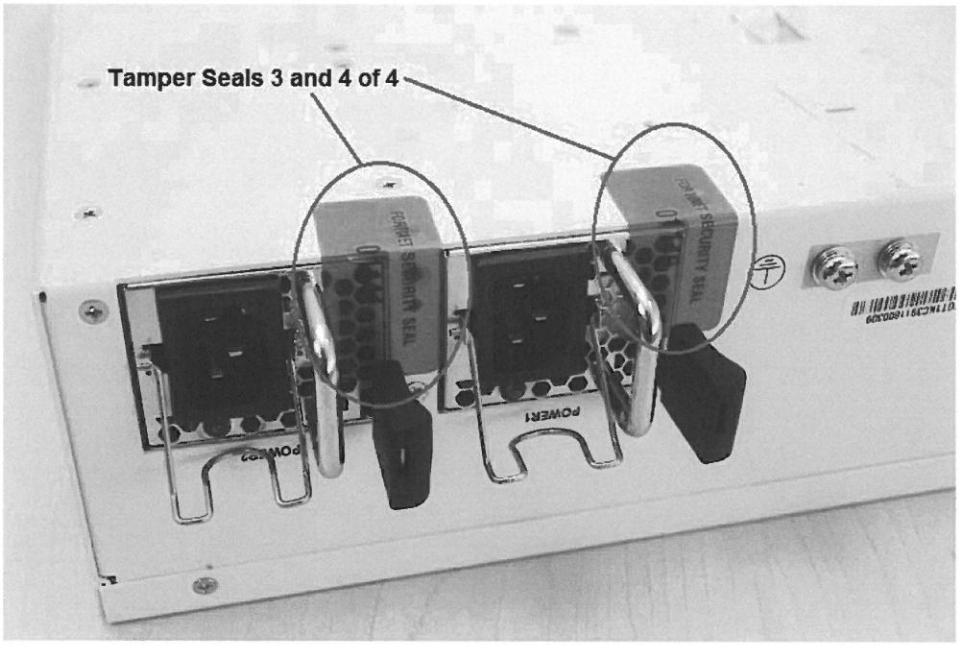



**Figure 8: FortiGate-1240B external enclosure seal, top, left side**

**Figure 9: FortiGate-1240B external enclosure seal, top, right side**

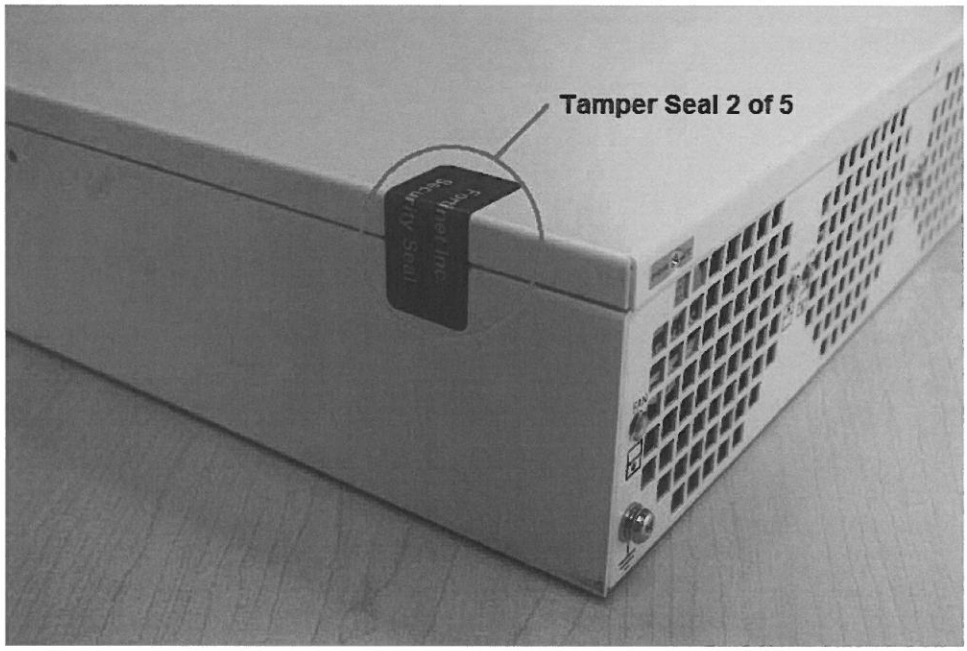



**Figure 10: FortiGate-1240B AMC faceplate seal, front, bottom**

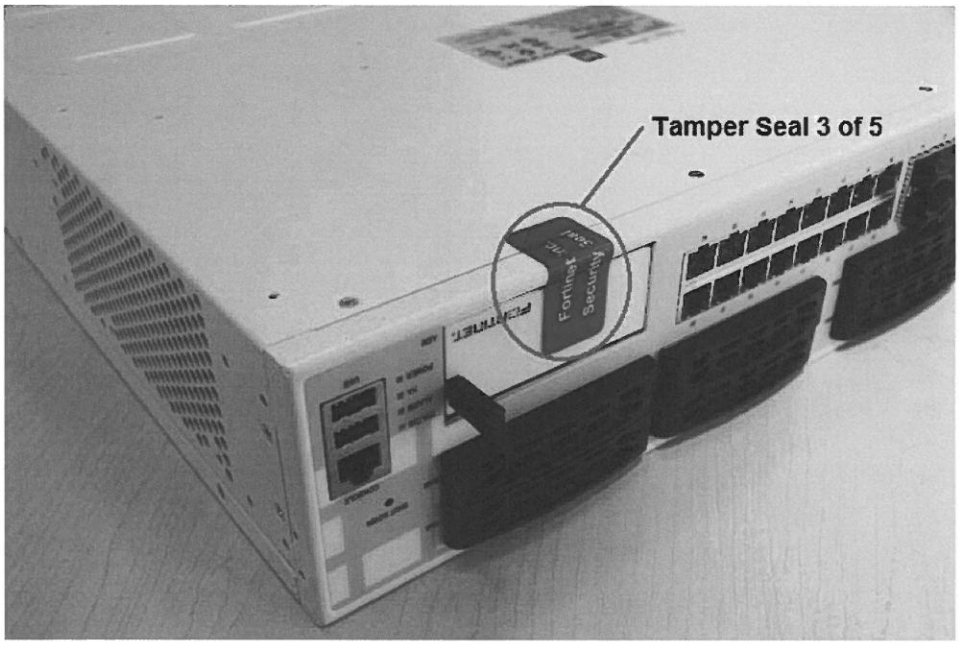


**Figure 11: FortiGate-1240B Power Supply Seals, rear, bottom**

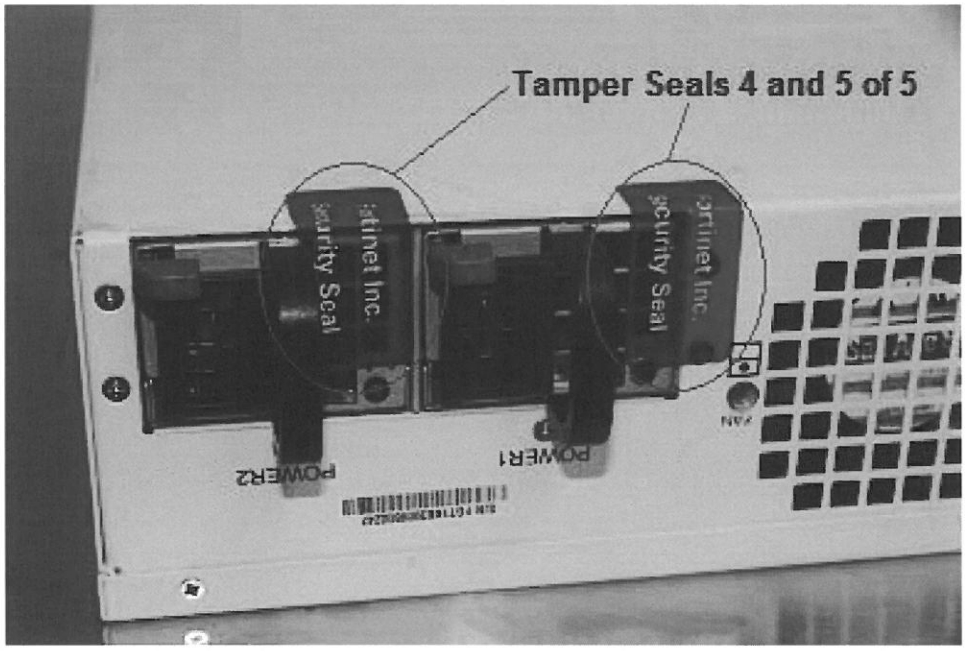



**Figure 12: FortiGate-3140B external enclosure seal, top, left side**

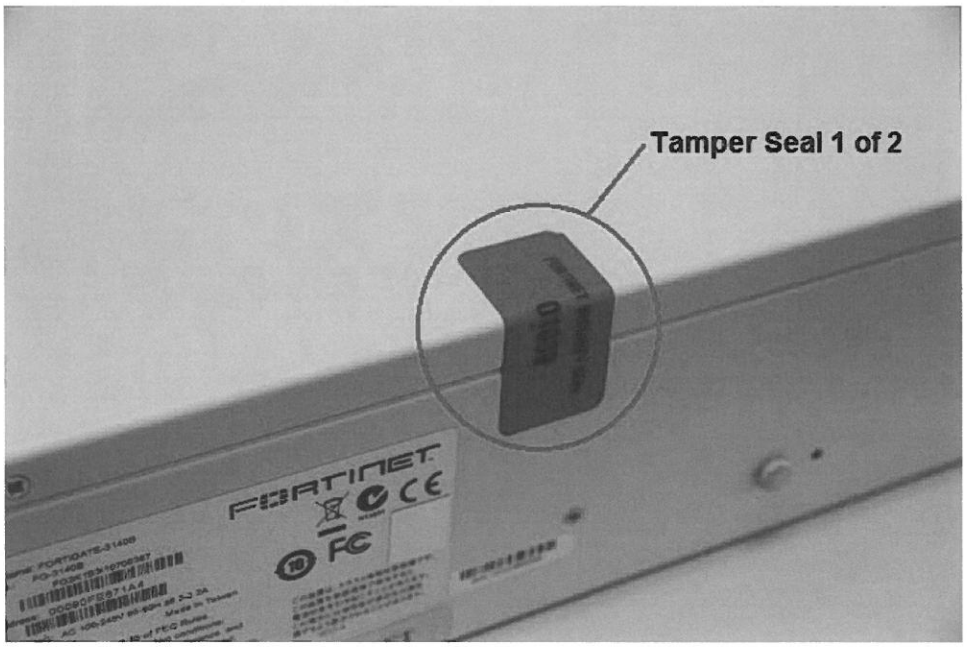
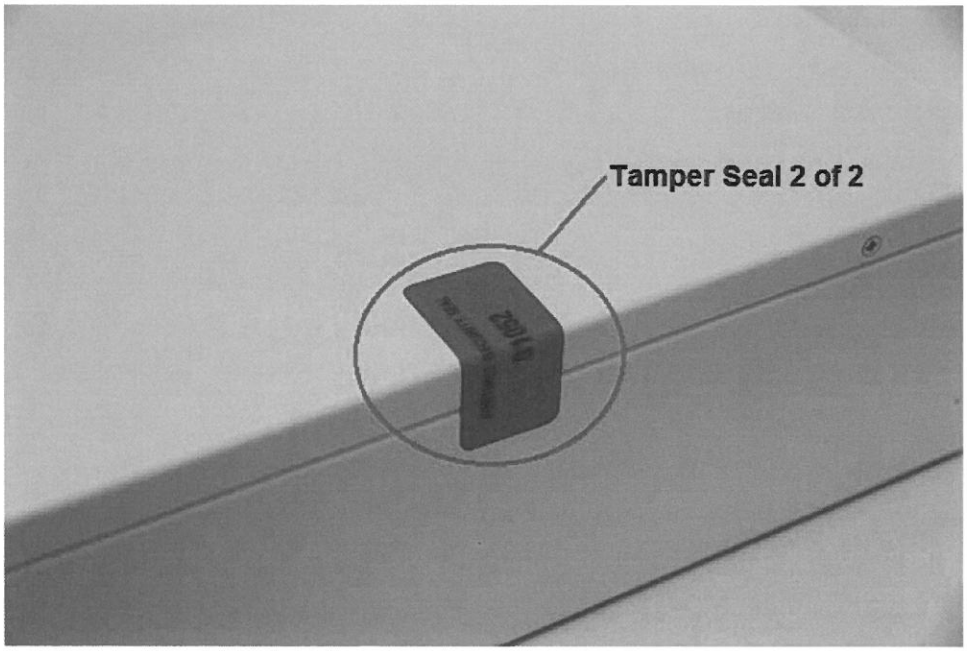


**Figure 13: FortiGate-3140B external enclosure seal, top, right side**




## Operational Environment

The module consists of the combination of the FortiOS operating system and the FortiGate appliances. The FortiOS operating system can only be installed, and run, on a FortiGate appliance. The FortiOS operating system provides a proprietary and non-modifiable operating system.

## Cryptographic Key Management

### Random Number Generation

The modules use a firmware based, deterministic random number generator that conforms to ANSI X9.31 Appendix A.2.4.

The ANSI X9.31 RNG is seeded using a 128-bit AES key (estimated strength 128 bits) and 64 bytes of entropy (estimated strength 60 bits) gathered from a combination of system data and internal resources such as time, memory addresses, kernel ticks, and module identifiers. As the module's ANSI X9.31 RNG implementation only generates random values of size 16 bytes (128 bits), it would take multiple calls to form a 32 byte (256 bit) key. Each call would add another 16 bytes of entropy (estimated strength 12 bits). The total estimated strength for the two calls required to form a 32 byte (256 bit) key is 200 bits.

### Key Zeroization

The zeroization process must performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully.

All keys except the following are zeroized by executing a factory reset:

- ANSI X9.31 RNG AES Key
- Firmware Update Key
- Firmware Integrity Key

- Configuration Integrity Key
- Configuration Backup Key
- SSH Server/Host Key
- HTTPS/TLS Server/Host Key

All keys and CSPs are zeroized by formatting the modules' flash memory storage. To format the flash memory, connect a computer to the modules' console port and reboot the module. Access the configuration menu by pressing any key when prompted (see example below). Select "F" to format the flash memory (boot device).

```
Press any key to display configuration menu...

[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,I,Q,or H:
```

## Algorithms

**Table 13: FIPS Approved Algorithms**

| Algorithm | NIST Certificate Number |
|---|---|
| RNG (ANSI X9.31 Appendix A) | 1131 |
| Triple-DES | 1421, 1422, 1425, 1426 |
| AES | 2274, 2275, 2278, 2279 |
| SHA-1 | 1955, 1956, 1959, 1960 |
| SHA-256 | 1955, 1956, 1959, 1960 |
| HMAC SHA-1 | 1392, 1393, 1396, 1397 |
| HMAC SHA-256 | 1392, 1393, 1396, 1397 |
| RSA PKCS1 (digital signature creation and verification) | 1167, 1169, 1170 |

**Table 14: FIPS Allowed Algorithms**

| Algorithm |
|---|
| RSA (key establishment methodology provides 80 or 112 bits of encryption strength) |
| Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 201bits of encryption strength; non-compliant less than 80-bits of encryption strength) |

**Table 15: Non-FIPS Approved Algorithms**

| Algorithm |
|---|
| DES (disabled in FIPS-CC mode) |
| MD5 (disabled in FIPS-CC mode except for use in the TLS protocol) |
| HMAC MD5 (disabled in FIPS-CC mode) |

Some algorithms may be classified as deprecated, restricted, or legacy-use. Please consult NIST SP 800-131A for details.

The vendor makes no conformance claims to any key derivation function specified in SP 800-135rev1. References to the key derivation functions addressed in SP 800-135rev1 including IKE, SSH, and TLS are only listed to clarify the key types supported by the module. Keys related to IKE, SSH, and TLS are only used in the Approved mode under the general umbrella of a non-Approved Diffie-Hellman scheme, with no assurance claims to the underlying key derivation functions.

## Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the module. The following definitions apply to the table:

| | |
|---|---|
| **Key or CSP** | The key or CSP description. |
| **Storage** | Where and how the keys are stored |
| **Usage** | How the keys are used |

**Table 16: Cryptographic Keys and Critical Parameters used in FIPS-CC Mode**

| Key or CSP | Storage | Usage |
|---|---|---|
| Diffie-Hellman Keys | SDRAM Plaintext | Key agreement and key establishment |
| IPSec Manual Authentication Key | Flash RAM AES encrypted | Used as IPSec Session Authentication Key |
| IPSec Manual Encryption Key | Flash RAM AES encrypted | Used as IPSec Session Encryption Key |
| IPSec Session Authentication Key | SDRAM Plain-text | IPSec peer-to-peer authentication using HMAC SHA-1 |
| IPSec Session Encryption Key | SDRAM Plain-text | VPN traffic encryption/decryption using Triple-DES or AES |
| IKE Pre-Shared Key | Flash RAM AES encrypted | Used to generate IKE protocol keys |
| IKE Authentication Key | SDRAM Plain-text | IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A) |
| IKE Key Generation Key | SDRAM Plain-text | IPSec SA keying material (SKEYID_D) |
| IKE Session Encryption Key | SDRAM Plain-text | Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E) |
| IKE RSA Key | Flash Ram Plain text | Used to generate IKE protocol keys |
| RNG Seed (ANSI X9.31 Appendix A.2.4) | Flash RAM Plain-text | Seed used for initializing the RNG |
| RNG AES Key (ANSI X9.31 Appendix A.2.4) | Flash RAM Plain-text | AES Seed key used with the RNG |
| Firmware Update Key | Flash RAM Plain-text | Verification of firmware integrity when updating to new firmware versions using RSA public key |
| Firmware Integrity Key | Flash RAM Plain-text | Verification of firmware integrity in the firmware integrity test using RSA public key |

**Table 16: Cryptographic Keys and Critical Parameters used in FIPS-CC Mode**

| Key or CSP | Storage | Usage |
|---|---|---|
| HTTPS/TLS Server/Host Key | Flash RAM<br>Plain-text | RSA private key used in the HTTPS/TLS protocols (key establishment) |
| HTTPS/TLS Session Authentication Key | SDRAM<br>Plain-text | HMAC SHA-1 key used for HTTPS/TLS session authentication |
| HTTPS/TLS Session Encryption Key | SDRAM<br>Plain-text | AES or Triple-DES key used for HTTPS/TLS session encryption |
| SSH Server/Host Key | Flash RAM<br>Plain-text | RSA private key used in the SSH protocol (key establishment) |
| SSH Session Authentication Key | SDRAM<br>Plain-text | HMAC SHA-1 key used for SSH session authentication |
| SSH Session Encryption Key | SDRAM<br>Plain-text | AES or Triple-DES key used for SSH session encryption |
| Operator Password | Flash RAM<br>SHA-1 hash | Used to authenticate operator access to the module |
| Configuration Integrity Key | Flash RAM<br>Plain-text | SHA-1 hash used for configuration/VPN bypass test |
| Configuration Encryption Key | Flash RAM<br>Plain-text | AES key used to encrypt CSPs on the flash RAM and in the backup configuration file (except for operator passwords in the backup configuration file) |
| Configuration Backup Key | Flash RAM<br>Plain-text | HMAC SHA-1 key used to encrypt operator passwords in the backup configuration file |
| Network User Password | Flash RAM<br>AES encrypted | Used during network user authentication |
| HA Password | Flash RAM<br>AES encrypted | Used to authenticate FortiGate units in an HA cluster |
| HA Encryption Key | Flash RAM<br>AES encrypted | Encryption of traffic between units in an HA cluster using AES |

## Alternating Bypass Feature

The primary cryptographic function of the module is as a firewall and VPN device. The module implements two forms of alternating bypass for VPN traffic: policy based (for IPSec and SSL VPN) and interface based (for IPSec VPN only).

### Policy Based VPN

Firewall policies with an action of IPSec or SSL-VPN mean that the firewall is functioning as a VPN start/end point for the specified source/destination addresses and will encrypt/decrypt traffic according to the policy. Firewall policies with an action of allow mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

A firewall policy with an action of accept means that the module is operating in a bypass state for that policy. A firewall policy with an action of IPSec or SSL-VPN means that the module is operating in a non-bypass state for that policy.

#### Interface Based VPN

Interface based VPN is supported for IPSec only. A virtual interface is created and any traffic routed to the virtual interface is encrypted and sent to the VPN peer. Traffic received from the peer is decrypted. Traffic through the virtual interface is controlled using firewall policies. However, unlike policy based VPN, the action is restricted to Accept or Deny and all traffic controlled by the policy is encrypted/decrypted.

When traffic is routed over the non-virtual interfaced, the module is operating in a bypass state. When traffic is routed over the virtual interface, the module is operating in a non-bypass state.

In both cases, two independent actions must be taken by a CO to create bypass firewall policies: the CO must create the bypass policy and then specifically enable that policy.

### Key Archiving

The module supports key archiving to a management computer or USB token as part of a module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC-SHA-1 using the Configuration Backup Key.

### Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements for Class A (business use) devices as specified by Part 15, Subpart B, of the FCC rules. The following table lists the specific lab and FCC report information for the modules.

**Table 17: FCC Report Information**

| Module | Lab Information | FCC Report Number |
|---|---|---|
| FG-1000C | The module is declared to conform with EMI/EMC requirements for Class B (business use) devices as specified by Part 15, Subpart B, of the FCC rules. | |
| FG-1240B | Spectrum Research and Testing Laboratory, Inc<br>No. 101-10, Ling 8<br>Shan-Tong Li Chung-Li City<br>Taoyuan, Taiwan<br>03-498-7684<br>03-498-6528 | A10012801 |
| FG-3140B | Compliance Certification Services Inc.<br>Sindian Lab<br>163-1 Jhonsheng Road<br>Sindian City, Taiwan<br>886-2-22170894<br>886-2-22171029 | T111129212-F |

## Mitigation of Other Attacks

The module includes a real-time Intrusion Prevention System (IPS) as well as antivirus protection, antispam and content filtering. Use of these capabilities is optional.

The FortiOS IPS has two components: a signature based component for detecting attacks passing through the FortiGate appliance and a local attack detection component that protects the firewall from direct attacks. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack. The IPS signatures are updated through the FortiGuard IPS service. The IPS engine can also be updated through the FortiGuard IPS service.

FortiOS antivirus protection removes and optionally quarantines files infected by viruses from web (HTTP), file transfer (FTP), and email (POP3, IMAP, and SMTP) content as it passes through the FortiGate modules. FortiOS antivirus protection also controls the blocking of oversized files and supports blocking by file extension. Virus signatures are updated through the FortiGuard antivirus service. The antivirus engine can also be updated through the FortiGuard antivirus service.

FortiOS antispam protection tags (SMTP, IMAP, POP3) or discards (SMTP only) email messages determined to be spam. Multiple spam detection methods are supported including the FortiGuard managed antispam service.

FortiOS web filtering can be configured to provide web (HTTP) content filtering. FortiOS web filtering uses methods such as banned words, address block/exempt lists, and the FortiGuard managed content service.

Whenever a IPS, antivirus, antispam or filtering event occurs, the modules can record the event in the log and/or send an alert email to an operator.

For complete information refer to the FortiGate Installation Guide for the specific module in question, the FortiGate Administration Guide and the FortiGate IPS Guide.

# FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is configured in the FIPS-CC mode of operation.
- The FortiGate unit is installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters should be capitalized
  - One (or more) of the characters should be numeric
  - One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark)
- Administration of the module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - Command line interface (CLI) access via SSH
- Diffie-Hellman groups of less than less than 1024 bits (Group 5) are not used.
- Client side RSA certificates must use 1024 bit or greater key sizes.
- LDAP based authentication must use secure LDAP (LDAPS).
- Only approved and allowed algorithms are used (see "Algorithms" on page 20).

- The tamper evident seals are applied (see "Physical Security" on page 14).

The module can be used in either of its two operation modes: NAT/Route or Transparent. NAT/Route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager Status page and in the output of the `get system status` CLI command.

### Enabling FIPS-CC mode

To enable the FIPS 140-2 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system fips
  set status enable
end
```

The Operator is required to supply a password for the admin account which will be assigned to the Crypto Officer role.

The supplied password must be at least 8 characters long and correctly verified before the system will restart in FIPS-CC mode.

Upon restart, the module will execute self-tests to ensure the correct initialization of the module's cryptographic functions.

After restarting, the Crypto Officer can confirm that the module is running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the module is running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Note that enabling/disabling the FIPS-CC mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS-CC mode is enabled/disabled.

## Self-Tests

The module executes the following self-tests during startup and initialization:

- Firmware integrity test using RSA signatures
- Configuration/VPN bypass test using HMAC SHA-1
- Triple-DES, CBC mode, encrypt known answer test
- Triple-DES, CBC mode, decrypt known answer test
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (test as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (test as part of HMAC SHA-256 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- RNG known answer test

The results of the startup self-tests are displayed on the console during the startup process. The startup self-tests can also be initiated on demand using the CLI command **execute fips kat all** (to initiate all self-tests) or **execute fips kat <test>** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - e.g. when the AES self-test is run, all AES implementations are tested.

The module executes the following conditional tests when the related service is invoked:

- Continuous RNG test
- RSA pairwise consistency test
- Configuration/VPN bypass test using HMAC SHA-1
- Firmware load test using RSA signatures

If any of the self-tests or conditional tests fail, the module enters an error state as shown by the console output below:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

All data output and cryptographic services are inhibited in the error state.

# Non-FIPS Approved Services

The module also provides the following non-FIPS approved services:

- Configuration backups using password protection
- LLTP and PPTP VPN
- Paired Bypass network interfaces (WAN1/Port1 and WAN2/Port2)

If the above services are used, the module is not considered to be operating in the FIPS approved mode of operation.

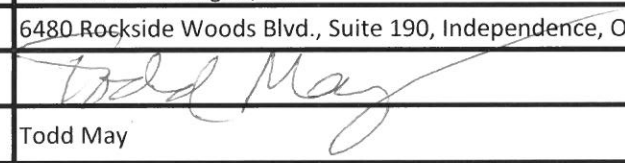
## ATTACHMENT C – TAX14006 COST SHEET

To be submitted in the COST version of the response.

## TAX14006 COST SHEET

| Qty | Product Number | Description | Unit Price | Extended Price |
|---|---|---|---|---|
| 2 | FG-1000C-BDL-950-12 | SSL VPN Hardware Appliance | $15,847 | $31,694 |
| 2 | Included with Above | 1 Year Extended Service Agreement for VPN Appliance | Included with above. | |
| 2 | Included with Above | SSL VPN Licensing for 100 Concurrent Users with the Physical Devices in Separate Locations | Included with above. | |
| | | | | |
| 2 | Included with Above | Hardware Appliances for Multi Factor Authentification using hardware tokens | Included with Above | |
| 90 | NA | Application Base Software Licensing | Included with Above | |
| 1 | FTK-200-100 | Hardware Tokens with 5 year Programmable Lifespan (Qty. 100 per pack) | $2,930 | $2,930 |
| 90 | NA | Hardware Token Licensing for 5 Years | Included with Above | |
| 90 | Included with Above | 1 Year Technical Support/Phone Consulting | Included with Above | |
| | Misc. items | List additional items needed for the solutions to coexist and meet all specs | NA | NA |
| | | | | |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | | | | |
| 4 | FP10-INS02-000-02-00 | Installation and Configuration of both solutions (Remote installation) | $709.00 | $2,836 |
| | | | | |
| | | | Subtotal | $37,460 |
| | | | Shipping | |
| | | | Total | |

********** Please sign and complete ALL of the information below. **********

| | |
|---|---|
| Vendor's Name | AdvizeX Technologies, LLC |
| Vendor's Address | 6480 Rockside Woods Blvd., Suite 190, Independence, OH, 44131 |
| Authorized signature for Vendor |  |
| Authorized printed name for Vendor | Todd May |
| Vendor's Phone/Fax # | 216-901-1818/216-901-1447 |
| Vendor's Email address: | tmay@advizex.com |

***** Lowest cost vendor meeting specifications will be awarded the contract. ******

## ATTACHMENT E – PURCHASING AFFIDAVIT

RFQ No. TAX14006

STATE OF WEST VIRGINIA
Purchasing Division

# PURCHASING AFFIDAVIT

**MANDATE:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

**"Debt"** means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

**"Employer default"** means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

**"Related party"** means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

**AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.**

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: ADVIZEX

Authorized Signature: Todd May Date: 10-8-13

State of Ohio

County of Cuyahoga, to-wit:

Taken, subscribed, and sworn to before me this 7 day of 8 Oct, 2013

My Commission expires _____, 20___.

AFFIX SEAL HERE NOTARY PUBLIC _____

PATRICIA A. TOMMER
Notary Public
State of Ohio
My Commission Expires February 06, 2017

Purchasing Affidavit (Revised 07/01/2012)

| TAX14006 COST SHEET | | | | |
|---|---|---|---|---|
| **Qty** | **Product Number** | **Description** | **Unit Price** | **Extended Price** |
| 2 | FG-1000C-BDL-950-12 | SSL VPN Hardware Appliance | $15,847 | $31,694 |
| 2 | Included with Above | 1 Year Extended Service Agreement for VPN Appliance | Included with above. | |
| 2 | Included with Above | SSL VPN Licensing for 100 Concurrent Users with the Physical Devices in Separate Locations | Included with above. | |
| | | | | |
| 2 | Included with Above | Hardware Appliances for Multi Factor Authentification using hardware tokens | Included with Above | |
| 90 | NA | Application Base Software Licensing | Included with Above | |
| 1 | FTK-200-100 | Hardware Tokens with 5 year Programmable Lifespan (Qty. 100 per pack) | $2,930 | $2,930 |
| 90 | NA | Hardware Token Licensing for 5 Years | Included with Above | |
| 90 | Included with Above | 1 Year Technical Support/Phone Consulting | Included with Above | |
| | Misc. items | List additional items needed for the solutions to coexist and meet all specs | NA | NA |
| | | | | |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | | | | |
| 4 | FP10-INS02-000-02-00 | Installation and Configuration of both solutions (Remote installation) | $709.00 | $2,836 |
| | | | | |
| | | | Subtotal | $37,460 |
| | | | Shipping | |
| | | | Total | |

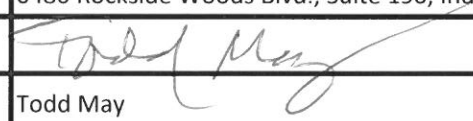
********** Please sign and complete ALL of the information below. **********

| | |
|---|---|
| Vendor's Name | AdvizeX Technologies, LLC |
| Vendor's Address | 6480 Rockside Woods Blvd., Suite 190, Independence, OH, 44131 |
| Authorized signature for Vendor |  |
| Authorized printed name for Vendor | Todd May |
| Vendor's Phone/Fax # | 216-901-1818/216-901-1447 |
| Vendor's Email address: | tmay@advizex.com |

***** Lowest cost vendor meeting specifications will be awarded the contract. ******

| TAX14006 COST SHEET | | | | |
|---|---|---|---|---|
| **Qty** | **Product Number** | **Description** | **Unit Price** | **Extended Price** |
| 2 | FG-1000C-BDL-950-12 | SSL VPN Hardware Appliance | $15,847 | $31,694 |
| 2 | Included with Above | 1 Year Extended Service Agreement for VPN Appliance | Included with above. | |
| 2 | Included with Above | SSL VPN Licensing for 100 Concurrent Users with the Physical Devices in Separate Locations | Included with above. | |
| | | | | |
| 2 | Included with Above | Hardware Appliances for Multi Factor Authentification using hardware tokens | Included with Above | |
| 90 | NA | Application Base Software Licensing | Included with Above | |
| 1 | FTK-200-100 | Hardware Tokens with 5 year Programmable Lifespan (Qty. 100 per pack) | $2,930 | $2,930 |
| 90 | NA | Hardware Token Licensing for 5 Years | Included with Above | |
| 90 | Included with Above | 1 Year Technical Support/Phone Consulting | Included with Above | |
| | Misc. items | List additional items needed for the solutions to coexist and meet all specs | NA | NA |
| | | | | |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | | | | |
| 4 | FP10-INS02-000-02-00 | Installation and Configuration of both solutions (Remote installation) | $709.00 | $2,836 |
| | | | | |
| | | | Subtotal | $37,460 |
| | | | Shipping | |
| | | | Total | |

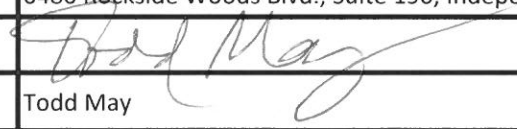
********** Please sign and complete ALL of the information below. **********

| | |
|---|---|
| Vendor's Name | AdvizeX Technologies, LLC |
| Vendor's Address | 6480 Rockside Woods Blvd., Suite 190, Independence, OH, 44131 |
| Authorized signature for Vendor |  |
| Authorized printed name for Vendor | Todd May |
| Vendor's Phone/Fax # | 216-901-1818/216-901-1447 |
| Vendor's Email address: | tmay@advizex.com |

***** Lowest cost vendor meeting specifications will be awarded the contract. ******

| TAX14006 COST SHEET | | | | |
|---|---|---|---|---|
| **Qty** | **Product Number** | **Description** | **Unit Price** | **Extended Price** |
| 2 | FG-1000C-BDL-950-12 | SSL VPN Hardware Appliance | $15,847 | $31,694 |
| 2 | Included with Above | 1 Year Extended Service Agreement for VPN Appliance | Included with above. | |
| 2 | Included with Above | SSL VPN Licensing for 100 Concurrent Users with the Physical Devices in Separate Locations | Included with above. | |
| | | | | |
| 2 | Included with Above | Hardware Appliances for Multi Factor Authentification using hardware tokens | Included with Above | |
| 90 | NA | Application Base Software Licensing | Included with Above | |
| 1 | FTK-200-100 | Hardware Tokens with 5 year Programmable Lifespan (Qty. 100 per pack) | $2,930 | $2,930 |
| 90 | NA | Hardware Token Licensing for 5 Years | Included with Above | |
| 90 | Included with Above | 1 Year Technical Support/Phone Consulting | Included with Above | |
| | Misc. items | List additional items needed for the solutions to coexist and meet all specs | NA | NA |
| | | | | |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | Additional items | | NA | NA |
| | | | | |
| 4 | FP10-INS02-000-02-00 | Installation and Configuration of both solutions (Remote installation) | $709.00 | $2,836 |
| | | | | |
| | | | Subtotal | $37,460 |
| | | | Shipping | |
| | | | Total | |

********** Please sign and complete ALL of the information below. **********

| | |
|---|---|
| Vendor's Name | AdvizeX Technologies, LLC |
| Vendor's Address | 6480 Rockside Woods Blvd., Suite 190, Independence, OH, 44131 |
| Authorized signature for Vendor |  |
| Authorized printed name for Vendor | Todd May |
| Vendor's Phone/Fax # | 216-901-1818/216-901-1447 |
| Vendor's Email address: | tmay@advizex.com |

***** Lowest cost vendor meeting specifications will be awarded the contract. ******

# ATTACHMENT F – AGREEMENT ADDENDUM FOR SOFTWARE

WV-96A
Rev. 12/12

## AGREEMENT ADDENDUM FOR SOFTWARE

In the event of conflict between this addendum and the agreement, this addendum shall control:

1. **DISPUTES** - Any references in the agreement to arbitration or to the jurisdiction of any court are hereby deleted. Disputes arising out of the agreement shall be presented to the West Virginia Court of Claims.
2. **HOLD HARMLESS** - Any provision requiring the Agency to indemnify or hold harmless any party is hereby deleted in its entirety.
3. **GOVERNING LAW** - The agreement shall be governed by the laws of the State of West Virginia. This provision replaces any references to any other State's governing law.
4. **TAXES** - Provisions in the agreement requiring the Agency to pay taxes are deleted. As a State entity, the Agency is exempt from Federal, State, and local taxes and will not pay taxes for any Vendor including individuals, nor will the Agency file any tax returns or reports on behalf of Vendor or any other party.
5. **PAYMENT** - Any references to prepayment are deleted. Fees for software licenses, subscriptions, or maintenance are payable annually in advance. Payment for services will be in arrears.
6. **INTEREST** - Any provision for interest or charges on late payments is deleted. The Agency has no statutory authority to pay interest or late fees.
7. **NO WAIVER** - Any language in the agreement requiring the Agency to waive any rights, claims or defenses is hereby deleted.
8. **FISCAL YEAR FUNDING** - Service performed under the agreement may be continued in succeeding fiscal years for the term of the agreement, contingent upon funds being appropriated by the Legislature or otherwise being available for this service. In the event funds are not appropriated or otherwise available for this service, the agreement shall terminate without penalty on June 30. After that date, the agreement becomes of no effect and is null and void. However, the Agency agrees to use its best efforts to have the amounts contemplated under the agreement included in its budget. Non-appropriation or non-funding shall not be considered an event of default.
9. **STATUTE OF LIMITATION** - Any clauses limiting the time in which the Agency may bring suit against the Vendor, lessor, individual, or any other party are deleted.
10. **SIMILAR SERVICES** - Any provisions limiting the Agency's right to obtain similar services or equipment in the event of default or non-funding during the term of the agreement are hereby deleted.
11. **FEES OR COSTS** - The Agency recognizes an obligation to pay attorney's fees or costs only when assessed by a court of competent jurisdiction. Any other provision is invalid and considered null and void.
12. **ASSIGNMENT** - Notwithstanding any clause to the contrary, the Agency reserves the right to assign the agreement to another State of West Virginia agency, board or commission upon thirty (30) days written notice to the Vendor and Vendor shall obtain the written consent of Agency prior to assigning the agreement.
13. **LIMITATION OF LIABILITY** - The Agency, as a State entity, cannot agree to assume the potential liability of a Vendor. Accordingly, any provision in the agreement limiting the Vendor's liability for direct damages is hereby deleted. Vendor's liability under the agreement shall not exceed three times the total value of the agreement. Limitations on special, incidental or consequential damages are acceptable. In addition, any limitation is null and void to the extent that it precludes any action for injury to persons or for damages to personal property.
14. **RIGHT TO TERMINATE** - Agency shall have the right to terminate the agreement upon thirty (30) days written notice to Vendor. Agency agrees to pay Vendor for services rendered or goods received prior to the effective date of termination. In such event, Agency will not be entitled to a refund of any software license, subscription or maintenance fees paid.
15. **TERMINATION CHARGES** - Any provision requiring the Agency to pay a fixed amount or liquidated damages upon termination of the agreement is hereby deleted. The Agency may only agree to reimburse a Vendor for actual costs incurred or losses sustained during the current fiscal year due to wrongful termination by the Agency prior to the end of any current agreement term.
16. **RENEWAL** - Any reference to automatic renewal is deleted. The agreement may be renewed only upon mutual written agreement of the parties.
17. **INSURANCE** - Any provision requiring the Agency to purchase insurance for Vendor's property is deleted. The State of West Virginia is insured through the Board of Risk and Insurance Management, and will provide a certificate of property insurance upon request.
18. **RIGHT TO NOTICE** - Any provision for repossession of equipment without notice is hereby deleted. However, the Agency does recognize a right of repossession with notice.
19. **ACCELERATION** - Any reference to acceleration of payments in the event of default or non-funding is hereby deleted.
20. **CONFIDENTIALITY** -Any provision regarding confidentiality of the terms and conditions of the agreement is hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act.
21. **AMENDMENTS** - All amendments, modifications, alterations or changes to the agreement shall be in writing and signed by both parties. No amendment, modification, alteration or change may be made to this addendum without the express written approval of the Purchasing Division and the Attorney General.

**ACCEPTED BY:**

| **STATE OF WEST VIRGINIA** | **VENDOR** |
|---|---|
| Spending Unit: _____ | Company Name: AdvizeX |
| Signed: _____ | Signed: Todd May |
| Title: _____ | Title: Account Manager |
| Date: _____ | Date: 10-8-13 |

## ATTACHMENT G – ENTIRE PARTY AGREEMENT

Attachment
PO#_____

This agreement constitutes the entire agreement between the parties, and there are no other terms and conditions applicable to the licenses granted hereunder.

Agreed

Todd May 10-8-13
Signature Date

ACCOUNT MANAGER
Title

ADVIZEX
Company Name

_____
Signature Date

_____
Title

_____
Agency/Division

# ATTACHMENT D – VENDOR PREFERENCE CERTIFICATE

State of West Virginia

## VENDOR PREFERENCE CERTIFICATE

Rev. 07/12

Certification and application* is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Resident Vendor Preference, if applicable.

1. ___ **Application is made for 2.5% resident vendor preference for the reason checked:**
Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**
___ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; or 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**
___ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. ___ **Application is made for 2.5% resident vendor preference for the reason checked:**
Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. ___ **Application is made for 2.5% resident vendor preference for the reason checked:**
Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

4. ___ **Application is made for 5% resident vendor preference for the reason checked:**
Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. ___ **Application is made for 3.5% resident vendor preference who is a veteran for the reason checked:**
Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. ___ **Application is made for 3.5% resident vendor preference who is a veteran for the reason checked:**
Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. ___ **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**
Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) reject the bid; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

**Under penalty of law for false swearing (West Virginia Code, §61-5-3), Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.**

**Bidder:** AdvizeX **Signed:** Todd May

**Date:** 10/8/13 **Title:** Acct. Manager

# ATTACHMENT E – PURCHASING AFFIDAVIT

RFQ No. TAX14006

STATE OF WEST VIRGINIA
Purchasing Division

## PURCHASING AFFIDAVIT

**MANDATE:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

**AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.**

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: ADVIZEX Date: 10-8-13

Authorized Signature: Todd Mag

State of Ohio

County of Cuyahoga, to-wit:

Taken, subscribed, and sworn to before me this 7 day of Oct, 2013.

My Commission expires _____, 20___.

NOTARY PUBLIC _____

AFFIX SEAL HERE

PATRICIA A. TOMMER
Notary Public
State of Ohio
My Commission Expires February 06, 2017

Purchasing Affidavit (Revised 07/01/2012)

## ATTACHMENT H – CERTIFICATION AND SIGNATURE PAGE

### CERTIFICATION AND SIGNATURE PAGE

By signing below, I certify that I have reviewed this Solicitation in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this bid or proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

AdvizeX
(Company)

Todd May
(Authorized Signature)

TODD MAY, ACCOUNT MANAGER
(Representative Name, Title)

216-901-1818 216-901-1447
(Phone Number) (Fax Number)

10-8-13
(Date)

## ATTACHMENT I – ADDENDUM ACKNOWLEDGEMENT FORM

**ADDENDUM ACKNOWLEDGEMENT FORM**
**SOLICITATION NO.:** TAX14006

**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.

AdvizeX
Company

Todd May
Authorized Signature

10-8-13
Date

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

Revised 07/25/2013