CONTRACT FOR THE BIDDING OF ONE (1) LOT NETWORK SECURITY DEVICE

THIS AGREEMENT made on the ____ day of ____ **2014** between **PHILIPPINE HEALTH INSURANCE CORPORATION,** a government owned and controlled corporation created and existing by virtue of R.A. 7875, otherwise known as the "National Health Insurance Act of 1995", with office address. at 18th Floor, City State Center Building, 709 Shaw Blvd corner Oranbo Drive, Pasig City, represented herein by its **Chief Information Executive CELERINO S. CABRERA , JR.,** (hereinafter called **"PHILHEALTH"**).

-and-

TRENDS AND TECHNOLOGIES, INC., a stock corporation, organized and registered with the Securities and Exchange Commission under Sec. Reg. No. AS092-07351, issued on October 30, 1992 and existing under the laws of the Republic of the Philippines, with business address at 6/flr. Trafalgar Plaza, 105 H.V. Dela Costa St., Salcedo Vill., Makati City, represented herein by its **Head, Financial Services Group, VICTOR L. TIU,** (hereinafter called **"TRENDS"**).

WHEREAS, PHILHEALTH invited Bids for the ***Bidding on the Procurement of One (1) Lot Network Security Device*** and has accepted a Bid by **TRENDS AND TECHNOLOGIES, INC.** for the supply of those goods in the sum of ***SEVEN MILLION EIGHTY EIGHT THOUSAND NINE HUNDRED NINETY NINE PESOS (PhP7,088,999.00),*** (hereinafter called **"the Contract Price"**).

WITNESSETH: That -

NOW, THEREFORE, for and in consideration of the foregoing premises, the parties hereto have agreed as they hereby agree and bind themselves as follows:

1. In this Contract, words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Contract, viz.:

   (a) TRENDS' Schedule of Requirements **(Annex "A")**;
   (b) TRENDS' Bid Form **(Annex "B")**;
   (c) TRENDS' Technical Proposal **(Annex "C")**;
   (d) Notice of Award **(Annex "D"); [for signature]**
   (e) BAC-ITR Resolution No. **23**, s. 2014 **(Annex "E")**;
   (f) General Conditions of the Contract (GCC) **(Annex "F")**;
   (g) Special Conditions of the Contract (SCC) **(Annex "G"); and**
   (h) Performance Security **(Annex "H").**

3. In consideration of the payments to be made by **PHILHEALTH** to **TRENDS** as hereinafter mentioned, **TRENDS** hereby covenants with **PHILHEALTH** to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract;

4. **PHILHEALTH** hereby covenants to pay **TRENDS** in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the time and in the manner prescribed by the contract;

10/11

CELERINO S. CABRERA JR.
Chief Information Executive

VICTOR L. TIU
Head, Financial Services Group
Trends and Technologies, Inc.

SVP EDGAR JULIUS ASUNCION
Chief Legal Executive

OIC-SM RONALD ALLAN C. PABLO
Corporate Information Security Department

HANNAH LORRAINE DALISAY
Division Chief
Accounting and Internal Control

WITNESS for TRENDS
SHIRLEY Z. AMATA

WITNESS for TRENDS
ROSE S. HERNANDEZ

5. The contract price covers the costs of all Deliverable Items and Services and includes all applicable taxes, including the 12% Value Added Tax (VAT), customs duties, license fees, freight, insurance, cost of importation and delivery at the time and locations specified and other charges which may be imposed on the Product by foreign and local authorities

6. **TRENDS** hereby covenants to deliver in favor of **PHILHEALTH** the **One (1) Lot Network Security Device** and the services related thereto, in accordance with the technical specifications as stated in attached Annexes of this Contract.

7. **Within Thirty (30) Calendar Days** after complete delivery to and acceptance by **PHILHEALTH, TRENDS** shall submit the **STATEMENT OF BILLING ACCOUNT** and other documentary requirements as may be required by the former as condition for payment. **PHILHEALTH** shall thereafter pay the sum of to **Six Million Three Hundred Eighty Thousand Ninety Nine Pesos and Ten Centavos (PhP6,380,099.10) only**, which is ninety percent (90%) of the total contract price.

   As obligation for the warranty, **PHILHEALTH** shall withhold **ten percent (10%) of the total contract price** as **retention money** or as obligation for **"Warranty"** in an amount equivalent to **Seven Hundred Eight Thousand Eight Hundred Ninety Nine Pesos and Ninety Centavos (PhP708,899.90) only. Said amount shall only be released after the lapse of the Three (3) year warranty period** for non-expendable supplies as required under Section 62 (Warranty) of the Revised IRR of R.A. 9184 . Provided, however, that the goods supplied are free from patent and latent defects and all the conditions imposed under this Contract have been fully met. Provided further, that **TRENDS** may opt to post a **special bank guarantee** equivalent to at least ten percent (10%) of the total contract price. The said special bank guarantee must have a **validity period of three (3) years** covering the whole duration of the warranty period.

8. All other terms, conditions and stipulations accompanying this Contract together with all proposals and all mandatory provisions of the Revised Implementing Rules and Regulations of R.A. 9184, shall form an integral part of the contract between the PARTIES hereto.

   The PARTIES hereby certify that they have read or caused to be read to them each and every provision of the foregoing Contract and that they had fully understood the same.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

PHILIPPINE HEALTH INSURANCE CORPORATION

10/11

CELERINO S. CABRERA, JR.
Chief Information Executive

TRENDS AND TECHNOLOGIES, INC.

VICTOR L. TIU
Head, Financial Services Group

Signed in the presence of:

SVP EDGAR JULIO S. ASUNCION
Chief Legal Executive

SM RONALD ALLAN C. PABLO
Corporate Information Security Department

HANNAH LORRAINE DALISAY
Division Chief
Accounting and Internal
Control Department
CAF #2014-11-02

____
Witness for **TRENDS**
ROSE S. HERNANDEZ

____
Witness for **TRENDS**
SHIRLEY Z. AMATA

ACKNOWLEDGEMENT

REPUBLIC OF THE PHILIPPINES)
CITY OF MAKATI CITY **) S.S.**

BEFORE ME, this ___ day NOV 2 1 2014 2014, personally appeared the following persons exhibiting to me their respective Government issued ID's, to wit:

CELERINO S. CABRERA, JR. PHILHEALTH I.D. #
Philippine Health Insurance Corp.

VICTOR L. TIU PHILHEALTH ID # 0190506904254
Trends and Technologies, Inc.

Known to me to be the same persons who executed the foregoing Contract Agreement consisting of ***one hundred eleven (111) pages*** including the annexes and this page on which the acknowledgement is written and they acknowledged that the same is their free act and deed and that of the corporations being represented.

WITNESS MY HAND AND SEAL on the date and place first above written.

ATTY. VIRGILIO R. BATALLA
NOTARY PUBLIC FOR MAKATI CITY
APPOINTMENT NO. M-35
UNTIL DECEMBER 31, 2014
ROLL OF ATTORNEY 48348
MCLE COMPLIANCE NO. IV-0015333/4-10-2013
IBP NO. 706762 – LIFETIME MEMBER
PTR. NO. 422-5505 JAN 2, 2014
EXECUTIVE BLDG. CENTER
MAKATI AVE., COR., JUPITER

Doc No. 460
Page No. 93
Book No. 42
Series of 2014

ANNEX "A"

Section VI. Schedule of Requirements

The schedule of services expressed as weeks/months stipulates hereafter a date which is the date of the maintenance service to the project site.

Item Number	Description	Quantity	Total	Delivered, Weeks/Months
	Network Security Device	One (1) Lot	One (1) Lot	Within Thirty (30) Calendar Days after the issuance and receipt of the winning bidder of the Notice to Proceed.

I hereby certify to comply and deliver all the above requirements.

Trends and Technologies,Inc. — Shirley Z. Amata — July 9, 2014

Name of Company/Bidder — **Signature over Printed Name of Representative** — **Date**

Annex "B"

Bid Form

Date: JULY 14, 2014
Invitation to Bid No.: NSD 2014-003-IT

The Chairperson
Bids and Awards Committee
PHILHEALTH

Gentlemen and/or Ladies:

Having examined the Bidding Documents including Bid Bulletin Numbers *[insert numbers]* N/A, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply/delivery/perform ***One (1) Lot Network Security Device*** in conformity with the said Bidding Documents for the sum stated hereunder:

PARTICULARS	COST per Lot (Inclusive of VAT)	Total Cost (Inclusive of VAT)
PLEASE SEE ATTACHED BILL OF MATERIALS		
TOTAL (In Words) SEVEN MILLION EIGHTY EIGHT THOUSAND NINE HUNDRED NINETY NINE PESOS ONLY.	PhP 7,088,999.00	PhP 7,088,999.00

We undertake, if our Bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in BDS provision for ITB Clause 0 and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the lowest or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements as per ITB Clause 5 of the Bidding Documents.

Dated this 14th day of JULY 2014.

SZAmata
[signature] SHIRLEY Z. AMATA

ACCOUNT MANAGER
[in the capacity of]

Duly authorized to sign Bid for and on behalf of TRENDS AND TECHNOLOGIES INC.

E003.001

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

TRENDS & TECHNOLOGIES, INC.

Bidding for the Procurement of ONE (1) LOT NETWORK SECURITY DEVICE
Invitation to Bid No.: NSD 2014-003-IT

Bill of Materials

Item	Product Description	Qty	Cost per item (Inclusive of VAT)	TOTAL COST (Inclusive of VAT)
	Appliance			
1	FG-60D-BDL. Bundle: 10xGE RJ45 Ports (including 7xInternal Ports, 2xWAN Ports, 1xDMZ Port). Max managed FortiAPs (Total/Tunnel) 10/5.	50	Php81,155.98	Php4,057,799.00
	Subscription Licenses/ Upgraded Support 24x7 for 3 years			
2	1 Year Hardware Premium Bundle Upgrade to 24x7 Comprehensive Support for FG-60D-BDL	50	Php10,215.00	Php510,750.00
3	Additional 2 years: UTM Bundle (24x7 FortiCare plus NGFW, AV, Web Filtering and AntiSpam Services)	50	Php50,409.00	Php2,520,450.00
	INCLUSIONS:			
	Section VII. Technical Specifications:			
4	Item Number 2. Delivery, installation, testing and maintenance (page 42 of 61 Bid Douments)	1	Php0.00	Php0.00
5	Item Number 5. Project Management (page 48 of 61 Bid Documents)	1	Php0.00	Php0.00
6	Item Number 6. Warranty for 3 years (page 49 of 61 Bid Documents)	1	Php0.00	Php0.00
7	Item Number 7. After Sales Support (page 49 and 50 of 61 Bid Documents)	1	Php0.00	Php0.00
8	Item Number 8. Technology Transfer & Workshop for 10 participants (page 50 of 61 Bid Documents)	1	Php0.00	Php0.00
9	Item Number 10. Documentation (page 51 of 61 Bid Documents)	1	Php0.00	Php0.00
	TOTAL (Inclusive of VAT)			Php7,088,999.00

Prepare by:

Shirley Z. Amata
Account Manager
Financial Services Group

July 14, 2014

ANNEX "C"

Section VII. Technical Specifications

SPECIFICATIONS	Statement of Compliance
* Statement of Compliance- Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of ITB Clause 3.1(a)(ii) and/or GCC Clause 2.1(a)(ii).	
1. GENERAL FEATURES	**Statement of Compliance** *
The network security device should have the following general features to comply with the requirements:	
• Network access control;	Comply
• Packet handling layer;	Comply
• Firewall;	Comply
• Intrusion detection and prevention.	Comply
Flexible deployment options:	
• Standalone firewall, standalone IPS, and firewall/IPS combination products;	Comply
• SBR Service Provider Series products tailored for needs of wireline, Code Division Multiple Access (CDMA), and Global System for Mobile Communications (GSM) service providers;	Comply
Broad range of protocol support including:	
• Control and signalling layer security (SIP, H.323, MGCP, SIGTRAN, SOAP);	Comply
• Mobile protocols including GPRS Tunnelling Protocol (GTP), Generic Routing Encapsulation (GRE), IP-IP encapsulation, Point-to-Point Protocol (PPP);	Comply
• Stream Control Transmission Protocol (SCTP) for SS7 telephony.	Comply
As **Philippine Health Insurance Corporation** is also envisioned to have a centralized management of all its network security devices in the future: from the central office to regional offices and service offices, the solution should be capable to integrate to a central management system/tools to effectively manage its current, new and additional network security devices to further improve the organization's security posture. Whether deploying several new devices and agents, distributing updates, or installing security policies across managed assets, it will drastically reduce management costs and overhead.	Comply

PhilHealth will be utilizing this device to take advantage of the benefits this will provide not only to the Corporation but also to the millions of its members, stakeholders, and partners in delivering quality health care services.	Comply
2. SCOPE OF THE PROJECT	
This project will cover the delivery, installation, testing, maintenance, documentation, and support of the Corporate Security Devices and peripherals. Specifically, the vendor shall provide the deliverables.	Comply
3. TECHNICAL SPECIFICATIONS	
1. **Technical Specifications 50 devices for Remote Offices**	

Number of Devices	**Fifty (50) Unified Threat Management Device**	Comply
General Specifications	The Device must support an upgradeable firmware. or can be converted to next generation firmware or OS	Comply
	Must support IPv4 and IPv6	Comply
	Must have High Availability or Clustering capability	Comply
	Must be hardware-based or appliance type	Comply
	Operation System (OS) and/or the security software must be integrated with the firewall device to remove overhead extra platform layers found on general-purpose commercial systems.	Comply
Concurrent Connections	Must have at least 500,000 concurrent connections	Comply
Unified Threat Management (UTM)	Must have integrated anti-virus, URL and application filter, and intrusion prevention system licenses for three (3) years.	Comply
Network Interfaces	Must have at least seven (7) x 10/100/1000 Ethernet ports and at least two (2) x 10/100/1000 WAN interfaces	Comply
Performance and Capacity	Must have at least 1.5Gbps firewall throughput	Comply

		Must have at least 35 Mbps antivirus throughput		Comply
		Must have at least 200 Mbps IPS throughput		Comply
		Must support at least 500,000 concurrent firewall sessions		Comply
		Must support at least 4,000 firewall sessions per seconds		Comply
		Must support at least 5,000 firewall policies		Comply
		Must support Voice Over IP traffic		Comply
		Must be able to support unrestricted number of user		Comply
	Firewall Operation	Must support virtual domains		Comply
		Must support multiple zones security (i.e. at different security levels)		Comply
		Must support VoIP protection such as: H.323. SIP, MGCP, SCCP, ALG.		Comply
		Must support policy based Source and Destination NAT.		Comply
		Must support 802.1q VLAN		Comply
		Must support MAC and IP MAC filtering and spoof prevention.		Comply
		Must support Dos and DDOS attack prevention.		Comply
	Anti-Virus/Anti-Spyware	Must be able to block, remove, and detect virus, worm and Trojan.		Comply
		Must protect against spyware, malware and phishing.		Comply
		Must have database update for virus signature.		Comply
		Must support file quarantine		Comply
		Must be able to block by file size or type.		Comply
		Must be able to scan HTTP, FTP, SMTP, POP3, IMAP, and VPN Tunnels.		Comply
	Intrusion Prevention System (IPS)	Must support block attacks such as DoS, port scanning. IP/ICP/TCP related		Comply
		Must support block attacks such as DNS, FTP bounce and improper commands.		Comply
		Must support protection from at		Comply

		least 3,000 threats.		Comply
		Must support protocol anomaly detection.		Comply
		Must support Custom signature.		Comply
	Application Control	Must identify and control popular IM/P2P applications regardless of port/protocol: AOL-IM, Yahoo, MSN, KaZaa, ICQ, Gnutella, BitTorrent, WinNY, Skype, eDonkey, Facebook... and other similar sites.		Comply
	Gateway Antispam	Must support Real Time Blocking (RTB) and MIME header check.		Comply
		Must support IP address Black list/white list.		Comply
		Must support real-time blacklist/open relay database server, MIME Header Check , Keyword/Phrase Filtering		Comply
		Must support automatic updates.		Comply
		Must support SMTP/SMTPS, POP3/POP3S, IMAP/ IMAPS		Comly
	URL Filtering	Must support URL keyword and phrase blocking.		Comply
		Must have HTTP proxy capability.		Comply
		Must support Java applet, cookies and active x blocking.		Comply
		Must have at least 76 Unique Categories		Comply
		Must be able to support custom based categories		Comply
	SSL VPN	Must have URL database		Comply
		Must support at least 30 Mbps SSL-VPN throughput		Comply
		Must have support TCP and UDP Tunneling		Comply
		Must have support Active Directory, LDAP and radius authentication.		Comply

№003.001

Office of the Secretariat
BAC Central Office

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

Site to Site VPN (IPSec VPN)	Must support at least 1GbpsIPSec VPN throughput	Comply
	Must have support DES, 3DES, AES and SHA-1/MD5 Authentication	Comply
	Must support PPTP, L2TP, VPN Client Pass Through SSL Single Sign-On Bookmarks Two-Factor Authentication	Comply
	Must have support IKE Certificate Authentication: Digital Certificates and pre-shared key.	Comply
	Must support at least Remote access VPN, L2TP within IPSec, and IPSec NAT trasversal.	Comply
	Must have Hub and Spoke VPN Support	Comply
	Must have the capability to auto-connect VPN and support redundant VPN gateways.	Comply
Traffic Management	Must have BGP, OSPF, RIP v1, v2 routing protocols capability.	Comply
	Must have policy based routing (Source Destination, Port/Service).	Comply
	Must have support for guaranteed bandwidth settings per policy.	Comply
	Must have support for maximum bandwidth settings per policy.	Comply
	With diffserv marking support per policy.	Comply
Networking	Must have support gateway failover selector (Multiple WAN supports)	Comply
	Must have support policy based routing.	Comply
	Must have IPv6 Support (Firewall, DNS, Transparent Mode, SIP,Dynamic Routing, Admin Access, Management)	Comply
	Must have support DDNS and PPPoE client.	Comply
	Must have support parent proxy with FQDN.	Comply

High-Availability	Must have high availability features. High availability can be configured as active/active and active/passive mode.		Comply
	Must support VRRP, session synchronization for firewall and VPN, session failover for routing change.		Comply
	Must be able to detect device failures and link failure.		Comply
User Authentication	Must have local database.		Comply
	Must support active directory integration.		Comply
	Must support external radius/LDAP database integration.		Comply
	Must support Xauth over RADIUS for IPSEC VPN		Comply
System Management	Must have command line interface (console, telnet, and SSH)		Comply
	Management via VPN tunnel		Comply
	Must be able to manage via enterprise network management.		Comply
	Must be manageable locally by multiple administrators.		Comply
Administration	Must be capable with different user access level (administrator/user).		Comply
	Must support software upgrades and configuration changes thru web and TFTP.		Comply
	Must have configuration rollback capability.		Comply
	Must be able to integrate with Syslog servers.		Comply
Logging/Monitoring	Must support email alerts		Comply
	Must support SNMP		Comply
	Must support VPN tunnel monitoring		Comply
Power Supplies Accessories	Input voltage must be 100/240 Volts alternating current autosense		Comply
	Must have management cables		Comply
	Must have power cables, manuals, utility drivers and other accessories		Comply

	Must have complete rack mounting accessories (brackets, screws &etc.	Comply
Security Certification	The firewall must at least be certified and complied with the specifications of ICSA Laboratory in terms of Antivirus, IPS, and IPSec VPN.	Comply
	Must be ICSA Labs Certified (Enterprise Firewall)	Comply
	Must be ICSA Labs Certified (Network IPS)	Comply
	Must be ICSA Labs Certified (IPSec)	Comply
	Must be ICSA Labs Certified (Gateway Antivirus)	Comply
Other Pertinent Requirements	Must be at least in the leaders, challengers and visionaries quadrant for ability to execute and completeness of vision in the Gartner's Magic Quadrant for Unified Threat Management as of July 2013	Comply
	Must be at least in the challengers, leaders and visionaries quadrant for ability to execute of Gartner's Magic Quadrant for Enterprise Network Firewalls as of February 2013	Comply
Other Hardware Requirements	- Must have at least 1 USB port	Comply
	- Must have console port for management (RJ45)	Comply
	- Internal Storage: at least 8GB	Comply
Compliance	Must be FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB compliant	Comply

4. INSTALLATION AND TESTING

a) The vendor must ensure that the proposed solution is compatible with the existing equipment of PhilHealth. — Comply

b) Intensive testing should be done by the vendor to achieve the functionality and benefits of the new devices. The vendor must provide an actual result of the testing of the installed devices. — Comply

c) The winning vendor will work in parallel with PhilHealth Network Engineers during the installation and testing of all the security devices to secure the corporate network infrastructure.	Comply
d) The winning vendor must be the highest level of partnership with the proposed solution	Comply
e) The winning vendor must be capable to integrate the proposed Network Security Devices to PhilHealth's current IP Telephony to allow calls from Central Office to PRO and vice versa.	Comply
f) Must have four (4) certified engineers of the proposed solution.	Comply
g) Must have two (2) installed base in governments within the last two (2) years from the time of bidding.	Comply
5. PROJECT MANAGEMENT	
a) The winning vendor should provide a PMP Certified Project Management team that will handle the planning, design, installation, and maintenance of the Network Security Devices of PhilHealth and will work in parallel with PhilHealth Network Engineersand InfoSec Representatives for the duration of the project.	Comply
b) The Project Management team will be composed of a Project/Team Leader, Assistant Team Leader, and team member representatives from the vendor,PhilHealth Network team and InfoSec Representatives.	Comply
c) The Project Management team and PhilHealthNetwork Engineers will be responsible for the formulation and configuration of the security policies of the Corporation based on the existing IT Policies and Standards and/or Information Security Policies being implemented by PhilHealth.	Comply
d) Both parties (vendor and PhilHealthProject Management Team) should agree to the formulated policies before the implementation/rollout proper.	Comply

6.WARRANTY	
a) The equipment should be covered by warranty on parts and service for at least three (3) years and for software patches and firmware updates. The warranty period for the hardware supplied shall commence upon acceptance. A comprehensive maintenance program for the first three-year period shall be included in the proposal.	Comply
b) The comprehensive maintenance shall include replacements for all parts which should be locally available. The vendor shall ensure continuous inventory of all critical parts of the equipment. Critical parts of the equipment shall include: main board, memory, modules, power supplies etc.	Comply
c) The vendor must ensure that PhilHealth would be given the following:	
o Firmware updates, software patches, driver updates and agents for the management software – FREE (via www or CD)	Comply
o Parts replacement – FREE for the duration of the warranty period.	Comply
o Preventive Maintenance – FREE at least twice a year for the duration of the warranty period. Shall be done remotely.	Comply
o Configuration – FREE assistance on product reconfiguration (on-site Central Office Pasig) for the duration of the warranty period.	Comply
7. AFTER SALES SUPPORT	
a) During the warranty period, the vendor shall provide highly technical personnel to service the security devices and all of its components/peripherals whenever hardware and/or any related problem should occur.	Comply
b) On call support shall be available 24 hours a day, 7 days a week. A one (1) hour response from time of the call (through telephone call) shall be provided. Onsite support must have a response time of not more than 4 hours from the time of the call in cases where in the phone support could not solve the problem. Onsite support in Central Office Pasig since deployment of devices will be nationwide.	Comply

<table>
<tr><td>c) On hardware repair, testing shall be done in Central Office Pasig to know the extent of the problem. All components beyond repair shall be replaced at no cost during the effectivity and conditions of the warranty. Service units should be available for the system and peripherals within a day after testing and diagnosis for temporary replacement of the defective unit(s). Delivery of replacement and pull out of defective only in Central Office Pasig.

d) The winning bidder shall coordinate with PhilHealth Network Engineers regarding the technical support and other matters after the awarding of the project. This is to facilitate faster response in case problem/s is/are needed to be resolved immediately.</td><td>Comply

Comply</td></tr>
<tr><td><b>8. TECHNOLOGY TRANSFER & WORKSHOP</b></td><td></td></tr>
<tr><td>a) FREE in-depth technical workshop should be provided for PhilHealth Network Engineers and designated InfoSec Personnel. The training should be conducted by the competent engineer(s) with at least 2 years of experience in the implementation of the said devices on the Training Centers in relation to the security devices and other tools that will be used to manage the said NETWORK SECURITY DEVICES. The technical workshop is listed below:

<table>
<tr><th>Course Title</th><th>No. of Participants</th></tr>
<tr><td>At least 2 days workshop in the management, installation and configuration of Firewall devices. The workshop should be hands-on and reflects the actual environment of PhilHealth.

Participants will consists of:
• eight (8) PhilHealth ITMD Network Personnel and;
• two (2) from Infosec Department.</td><td>10</td></tr>
</table></td><td>Comply

Comply

Comply

Comply</td></tr>
</table>

b) In the event proposed training is outside Metro Manila, all accommodation and transportation expenses of the participants of the workshop should be shouldered by the winning bidder.	Comply
9. OTHER REQUIREMENTS	
a) A certification must be provided by the bidder that his/her company is an authorized reseller/partner of the manufacturer of all proposed products.	Comply
b) A certification must be provided by the bidder that his/her company is an authorized support services provider of the manufacturer of all proposed products.	Comply
10. DOCUMENTATION	
The bidder must provide user and system manuals and technical materials of each device. Complete documentation of software and licenses, utility and recovery CDs must also be provided including the inventory of the server systems' components and serial numbers.	Comply
11. ACCEPTANCE	
PhilHealth technical personnel must review and conduct a physical testing of the delivered equipment based on its functions. All deliverables mentioned above should be checked by PhilHealth and complied by the vendors before the final acceptance and turnover of the project.	Comply
12. DELIVERY ADDRESS AND DATE	
a) The NETWORK SECURITY DEVICES must be delivered at 14th floor, Room 1410,Citystate Centre Building, #709 Shaw Blvd., Oranbo, Pasig City.	Comply
b) Delivery of all equipment should not be more than thirty (30) calendar days after the issuance of Notice to Proceed. The proponent shall indicate the details of installation for the entire project. •Both parties will determine the installation and implementation based upon the agreed schedule. The winning proponent shall guarantee installation and testing of the equipment within the specified period of agreed schedule.	Comply

I hereby certify to comply with all the above Technical Specifications

Trends and Technologies, Inc.	Shirley Z. Amata	July 10, 2014
Name of Company/Bidder	Signature over Printed Name of Representative	Date

Item # 3. Technical Specifications Pages 42-47

Technical Specifications		Statement of Compliance
General Specifications	Upgradeable Firmware	COMPLY. Firmware is upgradable to the latest firmware/OS.
	ipv4/ipv6	Comply. Fortigate supports ipv4 and ipv6. refer to FortiOS Brochure page 6 (FortiOS Networking Services)
	High Availability/Clustering	COMPLY. High Availability (active/active, Active/Passive, Clustering) are supported. Refer to Fortigate-60D Datasheet page 4.
	Hardware-based	COMPLY. Fortigate firewall is a hardware-based appliance. Refer to Fortigate-60D Datasheet page 1.
	Operation System	COMPLY. Security system is integrated in the hardware appliance. Refer to Fortigate-60D Datasheet.
Concurrent Connections	500,000 concurrent	COMPLY. Concurrent Sessions: 500,000. Refer to Fortigate-60D Datasheet page 4.
UTM	must have integrated antivirus	COMPLY. The Fortigate Firewall have integrated antivirus, url, application filter, IPS licenses. Refer to FortiOS Brochure page 6 (FortiOS Security Services).
Network Interfaces		COMPLY. Refer to Fortigate-60D Datasheet page 4 10/100/1000 Internal Interfaces: 7 10/100/1000 WAN Interfaces: 2 10/100/1000 DMZ Interfaces: 1
Performance and Capacity	1.5 Gbps Firewall throughput	COMPLY. Refer to Fortigate-60D Datasheet page 4 Firewall Throughput (1518 / 512 / 64 byte UDP packets): 1.5 Gbps
	35 Mbps ativirus throufhput	COMPLY. Refer to Fortigate-60D Datasheet page 4 Antivirus Throughput (Proxy Based / Flow Based): 35Mbps/50Mbps
	200 Mbps IPS throughput	COMPLY. Refer to Fortigate-60D Datasheet page 4 IPS Throughput: 200 Mbps.
	500,000 concurrent firewall sessions	COMPLY. Refer to Fortigate-60D Datasheet page 4 Firewall Concurrent Sessions: 500,000
	4000 firewall sessions	COMPLY. Refer to Fortigate-60D Datasheet page 4 Firewall Session per second: 4000
	5000 firewall policies	COMPLY. Refer to Fortigate-60D Datasheet page 4 Firewall Policies: 5000

	support VoIP	COMPLY. VoIP Security (SIP Firewall / RTP Pinholing). Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	unrestricted number of user	COMPLY. Fortigate supports unrestricted number of user.
Firewall Operation	virtual domains	COMPLY. Virtual Domains (NAT/Transparent mode) Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	multiple zones	COMPLY. Multi-Zone Support Refer to FortiOS Brochure page 6 (FortiOS Networking Services)
	VoIP protections	COMPLY. VoIP Security (SIP Firewall / RTP Pinholing) and SIP/H.323 /SCCP NAT Traversal. Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	Source and Destination NAT	COMPLY. Support NAT (source and destination) Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	802.1Q VLAN	COMPLY. VLAN Tagging (802.1Q) Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	MAC, IPMC filtering	COMPLY. Assigning IP address by MAC address. Refer to FortiOS Handbook page 456
	DOS and DDOS protection	COMPLY. Defending against DoS attacks Refer to FortiOS Handbook page 630-632
Antivirus/Antispyware	block/remove	COMPLY. Fortigate can able to block, remove, and detect viruses, worms and trojan. Refer to FortiOS Handbook page 862-866
	spyware/malware	COMPLY. Fortigate can protect against spyware, malware and phishing. Refer to FortiOS Handbook page 862-873
	database update	COMPLY. The antivirus scan engine has a database of virus signatures it uses to identify infections. Refer to FortiOS Handbook page 862
	file quarantine	COMPLY. Fortigate supports file quarantine. Refer to FortiOS Brochure page 6 (FortiOS Security Services)
	block file size	COMPLY. Fortigate can checking for a file size, name, or type, or for the presence of a virus or grayware signature. Refer to FortiOS Handbook page 862
	HTTP,FTP	COMPLY. FortiGate unit apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, IM, and NNTP sessions. Refer to FortiOS Handbook page 862
	block attacks such as DOS, port scanning	COMPLY. Fortigate IPS can block DOS, port scan. IP/ICP/TCP related Refer to FortiOS Handbook page 626, page 630

IPS	block attacks such as DNS, FTP bounc	COMPLY. Please refer to Fortiguard Encyclopedia. http://www.fortiguard.com/encyclopedia/#term=DNS http://www.fortiguard.com/encyclopedia/#term=FTP
	protection from 3000 threats	COMPLY. Fortigate IPS can support from at least 3000 threats. Refer to FortiOS Brochure page 6.
	support protocol anomaly detection	**COMPLY. Fortigate IPS support protocol anomaly detection.** Refer to FortiOS Brochure page 6.
	support custom signature	COMPLY. Fortigate IPS support custom signature. Refer to FortiOS Brochure page 6.
Application Control	identify and control popular IM/P2P	COMPLY. Fortigate Application control can identify and control popular IM.P2P. Refer to FortiOS Brochure page 6.
Gateway Antispam	Real Time Blocking (RTB) and MIME	COMPLY. Fortigate Antispam support real time blocking and MIME header detection. Refer to FortiOS Brochure page 6.
	IP Address Black List/White List	COMPLY. Fortigate Antispam support IP Address BlackList/Exempt List Refer to FortiOS Brochure page 6.
	real time blacklist/open relay	COMPLY. Fortigate Antispam support Real-Time Blacklist/Open Relay Database Server **MIME Header Check** Keyword/Phrase Filtering Refer to FortiOS Brochure page 6.
	support automatic updates	COMPLY. Fortigate Antispam support Automatic Real-Time Updates From FortiGuard Network. Refer to FortiOS Brochure page 6.
	support SMTP/SMTPS	COMPLY. Fortigate Antispam support for SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS. Refer to FortiOS Brochure page 6.
URL Filtering	URL Keyword/phrase	COMPLY. Fortigate Web Filtering support for URL/Keyword/Phrase Block. Refer to FortiOS Brochure page 6.
	HTTP proxy capability	COMPLY. Fortigate have http proxy capability. Refer to FortiOS Handbook page 2489
	Java applet, cookies, active-X blocking	COMPLY. Fortigate Web Filtering blocks Java Applet, Cookies, Active X. Refer to FortiOS Brochure page 6.
	76 Unique Categories	COMPLY. Fortigate Web Filtering have at least 76 unique content categories. Refer to FortiOS Brochure page 6.

	custom based categories	COMPLY. Fortigate Web Filter supports custom based categories. Refer to FortiOS Handbook page 926
	URL Database	COMPLY. FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages. Refer to FortiOS Brochure page 6.
SSL VPN	30 Mbps SSL Throughput	COMPLY. SSL VPN Throughput - 30 Mbps. Refer to Fortigate-60D Datasheet page 4.
	TCP and UDP Tunneling	COMPLY. Fortigate support TCP and UDP tunneling.
	support Active Directory, LDAP and radius Auth	COMPLY. Fortigate SSL VPN supports Active Directory, LDAP and radius authentication. Refer to FortiOS Handbook page 1439
Site to Site VPN	1Gbps IPSEC VPN Throughput	COMPLY. IPSEC VPN Throughput - 1 Gbps. Refer to Fortigate-60D Datasheet page 4.
	DES, 3DES	COMPLY. FortiGate IPSEC VPN supports DES, 3DES, and AES Encryption and SHA-1/MD5 Authentication. Refer to FortiOS Brochure page 6.
	PPTP L2TP	COMPLY. FortiGate IPSEC VPN supports: PPTP, L2TP, VPN Client Pass Through Hub and Spoke VPN Support SSL Single Sign-On Bookmarks SSL Two-Factor Authentication Refer to FortiOS Brochure page 6.
	IKE Cert Auth	COMPLY. FortiGate IPSEC VPN supports IKE Certificate Authentication (v1 & v2). Refer to FortiOS Brochure page 6.
	support Remote access VPN	COMPLY. Fortigate VPN supports remote access VPN, L2TP within IPSEC, and IPSec NAT Traversal. Refer to FortiOS Brochure page 6.
	Hub and spoke	COMPLY. Fortigate VPN have Hub and Spoke VPN support. Refer to FortiOS Brochure page 6.
	auto-connect VPN and support redundant	COMPLY. Fortigate VPN have capability to auto connect and support redundant VPN gateways. Refer to FortiOS Handbook page 1233
	BGP, OSPF, RIP v1,v2	COMPLY. Fortigate supports Dynamic Routing for IPv4 (RIP, OSPF, IS-IS, BGP, & Multicast protocols). Dynamic Routing for IPv6 (RIP, OSPF, & BGP). FortiOS Brochure page 6.

Traffic Management	policy based routing	COMPLY. Fortigate supports policy based routing. FortiOS Brochure page 6.
	guaranteed bandwidth	COMPLY. Fortigate supports Guarantee/Max/Priority Bandwidth.refer to FortiOS Brochure page 6.
	maximum bandwidth	COMPLY. Fortigate supports Guarantee/Max/Priority Bandwidth.refer to FortiOS Brochure page 6.
	diffserv marking support	COMPLY. Fortigate have Differentiated Services (DiffServ) Support. refer to FortiOS Brochure page 6.
Networking	gateway failover selector	COMPLY. Fortigate has Multiple WAN Link Support. refer to FortiOS Brochure page 6.
	ipv6 support	COMPLY. IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Admin Access, Management). refer to FortiOS Brochure page 6.
	DDNS and PPPoE client	COMPLY. Fortigate support DDNS and PPPOE client. DDNS refer to FortiOS Handbook page 1295 PPPoE refer to FortiOS Brochure page 6.
	parent proxy with FQDN	COMPLY. Fortigate supports FQDN. Refer to FortiOS Handbook page 564
High Availability	Active/active Active/Passive	COMPLY. Fortigate supports High Availability Active-Active, Active-Passive. refer to FortiOS Brochure page 6.
	VRRP, session synchronization	COMPLY. Fortigate supports VRRP, session failover (session pickup). Refer to refer to FortiOS Brochure page 6. Refer to FortiOS Handbook page 1988
	detect device failover and link failure	COMPLY. Fortigate supports device failure detection and notification and Link Failover. refer to FortiOS Brochure page 6.
User Authentication	local database	COMPLY. Fortigate have Local Database refer to FortiOS Brochure page 6.
	AD integration	COMPLY. Fortigate have Windows Active Directory (AD) Integration (w/ FSAE). refer to FortiOS Brochure page 6.
	external radius/LDAP database integration	COMPLY. Fortigate have External RADIUS/LDAP/TACACS+ Integration. refer to FortiOS Brochure page 6.
	Xauth over RADIUS	COMPLY. Fortigate have Xauth over RADIUS for IPSEC VPN. refer to FortiOS Brochure page 6.

System Management	command line interface	COMPLY. Fortigate supports management via Telnet / Secure Command Shell (SSH), and Command Line Interface (CLI). refer to FortiOS Brochure page 6.
	management via VPN	COMPLY. Fortigate can be manage via VPN.
	manage via Enterprise Network Management	COMPLY. Fortigate can be manage via Enterprise Network Management. Central Management via FortiManager (optional). refer to FortiOS Brochure page 6.
	manageable locally by multiple admin	COMPLY. Fortigate can be manage by Multiple Administrators and User Levels. refer to FortiOS Brochure page 6.
Administration	different user access level	COMPLY. Fortigate can be manage by Multiple Administrators and User Levels. refer to FortiOS Brochure page 6.
	software upgrades and config change	COMPLY. Fortigate supports firmware upgrade and config changes via Web and TFTP. Firmware upgrade Refer to FortiOS Handbook page 322 Configuration revision Refer to FortiOS Handbook page 318
	config rollback	COMPLY. Fortigate supports restoring configurations. Refer to FortiOS Handbook page 321.
	intergate with syslog server	COMPLY. Fortigate supports logging via Local and Remote Syslog/WELF server logging. refer to FortiOS Brochure page 6.
Logging/Monitoring	email alerts	COMPLY. Fortigate supports Email Notification of Events. refer to FortiOS Brochure page 6.
	SNMP	COMPLY. Fortigate supports logging via SNMP. refer to FortiOS Brochure page 6.
	VPN tunnel monitoring	COMPLY. Fortigate supports VPN Tunnel Monitoring. refer to FortiOS Brochure page 6.
Power Supplies Accessories	100/240 volts AC	COMPLY. Power Required: 100-240 VAC. Refer to Fortigate-60D Datasheet page 4
	management cables	COMPLY, included in the box. Refer to 60D-Quickstart Guide
	power cables, manuals, utility drivers	COMPLY, included in the box. Refer to 60D-Quickstart Guide
	complete rack mounting access	COMPLY. Provisioned.
	ICSA Laboratory	COMPLY. Fortigate is certified and complied by ICSA Laboratory. refer to FortiOS Brochure page 6.

Security Certification	Enterprise FW	COMPLY. ICSA Labs Certified (Enterprise Firewall). refer to FortiOS Brochure page 6.
	Network IPS	COMPLY. ICSA Labs Certified (NIPS). refer to.FortiOS Brochure page 6.
	IPSEC	COMPLY. ICSA Labs Certified (IPSec/SSL-TLS). refer to FortiOS Brochure page 6.
	Gateway Antivirus	COMPLY. ICSA Labs Certified (Gateway Antivirus). refer to FortiOS Brochure page 6.
Other Pertinent Requirements	Magic Quadrant July 2013	COMPLY.refer to http://www.gartner.com/technology/reprints.do?id=1-1HH2PVB&ct=130722&st=sb
	Magic Quadrant Feb 2013	COMPLY. refer to 2013-Magic-Quadrant-Next-Generation-Firewalls.
Other HW Req	1 USB, console and internal storage 8GB	COMPLY. Fortigate 60D has 1 USB port and 1 console port. Refer to Fortigate-60D Datasheet page 4
Compliance	FCC Part 15	COMPLY. Fortigate is comply with FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB. Refer to Fortigate-60D Datasheet page 4

Prepared by:

Shirley Z. Amata
Account Manager
Financial Services Group
Trends and Technologies, Inc.
11-Jul-14

FURTINET.

FortiGate/FortiWiFi®-60D Series

Integrated Threat Management for Small Networks

The FortiGate/FortiWiFi-60D Series are compact, all-in-one security appliances that deliver Fortinet's Connected UTM. Ideal for small business, remote, customer premise equipment (CPE) and retail networks, these appliances offer the network security, connectivity and performance you need at a single low per-device price.

Advanced Protection and Wireless Connectivity

You get advanced threat protection, including firewall, application control, advanced threat protection, IPS, VPN, and web filtering, all from one device that's easy to 'leploy and manage. With our FortiGuard® security subscription services you'll have automated protection against today's sophisticated threats.

Reduce the need for additional wireless access points by integrating a high-bandwidth "fat-client" into your FortiGate with the FortiWiFi-60D. It's also a great option to secure mobile devices in BYOD environments with automatic device identification and customizable access and security policies.

VDOMs on the FortiGate/FortiWiFi-60D let you segment networks to enable guest and employee access, or protect things like cardholder data. You get the flexibility to match your business needs and meet compliance standards like PCI and HIPAA.

All-in-one High Performance Network Security

Built on the foundation of the FortiASIC System on a Chip 2 (SoC2) and FortiOS 5, the 60D series provides an integrated set of essential security technologies to protect all of your applications and data. You get the industry's best firewall plus the latest in Advanced Threat Protection, Intrusion Protection, Web-filtering and many new features like Sandboxing, Feature Select Options for simplifying configurations and deployments, and Contextual Visibility for enhanced reporting and management.

Key Features & Benefits

Unified Security	Multi-threat protection from a single device increases security and lowers costs
Simplified Licensing	Unlimited user licensing and comprehensive features
Multi-Port Interfaces	Multiple network interfaces and optional wireless connectivity enable data segmentation for compliance and flexible deployment

Enterprise-Class Protection that's Easy to Deploy and Manage

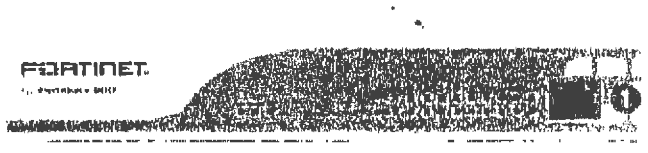
- 1.5 Gbps throughput performance ensures your network security won't be a bottleneck
- Integrated switch and options for PoE simplify your network infrastructure
- Up to 2x WAN, 7x LAN and 1x DMZ interface ports (2x Power Over Ethernet ports on POE models)
- Runs on FortiOS 5 – the most powerful security operating system in the world delivers more security to fight advanced threats, more control to secure mobile devices, and more intelligence to build secure policies

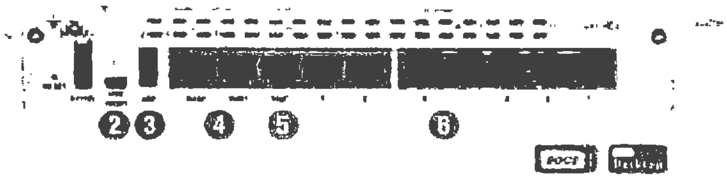
ICSA labs
ICSA labs
ICSA labs
ICSA labs
ICSA labs

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

/ARDWARE

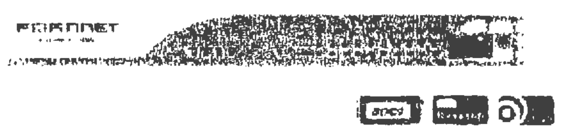
FortiGate-60D



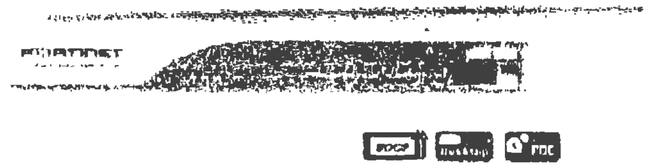


1. Console Port
2. USB Management Port for FortiExplorer
3. USB Port
4. 2 x GE RJ45 WAN Ports
5. 1x GE RJ45 DMZ Ports
6. 7 x GE RJ45 Internal Ports / 5 x GE RJ45 Internal and 2 x GE PoE Ports on POE models

FortiWiFi-60D



FortiGate-60D-POE



FortiWiFi-60D-POE

Powered by FortiASIC SOC2

- Combines a RISC-based CPU with Fortinet's proprietary FortiASIC™ content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed, secure remote access

Install in Minutes with FortiExplorer

The FortiExplorer™ wizard enables you to easily and quickly set up and configure FortiGate and FortiWiFi platforms with easy-to-follow instructions. The application runs on Windows, Mac OS X desktops and laptops as well as popular mobile devices. Simply connect to the appropriate USB port on the appliance, and be fully protected in minutes.

3G/4G WAN Connectivity

The FortiGate/FortiWiFi-60D series includes a USB port that allows you to plug in a compatible 3rd party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Superior Wireless Coverage

A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi-60D and provides speedy 802.11n coverage on both 2.4 GHz and 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

IIGHLIGHTS

FortiOS — The World's Most Advanced Security Operating System

- **Feature Select**
Instantly fine-tunes the FortiGate based on desired deployment needs using feature presets. Simplifies user administration and configurations while providing flexibility for different deployment modes.

- **Contextual Visibility**
Presents critical deep insights into historic or real-time network activities with data on threat details, IPs, users, devices, applications and more. Allows administrators to quickly understand threats and stop them.

- **Advanced Security**
Multiple advanced technologies can be coordinated to look for and stop today's blended, targeted or unknown attacks. Efficient packet handling improves performance while lowering latencies and reducing network complexities.

For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet

Industry Validation

The FortiGate family of physical and virtual appliances has earned more certifications than any other vendor by consistently meeting rigorous third-party standards. Our industry-leading technology provides you with air-tight security which you can safely count on.

More Protection and Better ROI

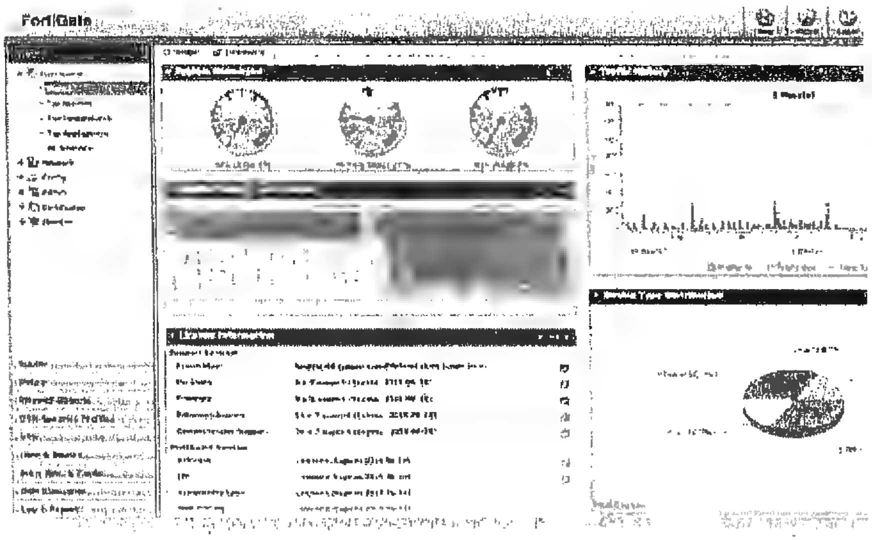
The FortiGate constantly evolves itself in its mission to provide more value for users. Extended features such as WiFi controller, integrated token server, endpoint control and WAN optimization add more security to organizations without incurring additional cost.

Complete and Real-time Security

Fortinet FortiGuard Subscription Services provide automated, real-time, up-to-date protection against the latest security threats. Our threat research labs are located worldwide, providing 24x7 updates when you most need it.

World-Class Technical Support and Documentation

Fortinet FortiCare support offerings provide comprehensive global support for all Fortinet products and services. You can rest assured your Fortinet security products are performing optimally and protecting your users, applications, and data around the clock.



FortiOS Dashboard — Single Pane of Glass Management

ORDER INFORMATION

Product	SKU	Description
FortiGate-60D	FG-60D	10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port). Max managed FortiAPs (Total / Tunnel) 10 / 5
FortiWiFi-60D	FWF-60D	10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port), Wireless (802.11a/b/g/n). Max managed FortiAPs (Total / Tunnel) 10 / 5
FortiGate-60D-POE	FG-60D-POE	10 x GE RJ45 ports (including 5 x Internal ports, 2 x WAN ports, 1 x DMZ port, 2 x PoE ports). Max managed FortiAPs (Total / Tunnel) 10 / 5
FortiWiFi-60D-POE	FWF-60D-POE	10 x GE RJ45 ports (including 5 x Internal ports, 2 x WAN ports, 1 x DMZ port, 2 x POE ports). Wireless (802.11a/b/g/n). Max managed FortiAPs (Total / Tunnel) 10 / 5

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

SPECIFICATIONS

	FORTIGATE-60D	FORTIWIFI-60D	FORTIGATE-60D-POE	FORTIWIFI-60D-POE
Hardware Specifications				
GbE RJ45 WAN Ports	2			
GbE RJ45 Internal Ports	7	7	5	5
GbE RJ45 PoE Ports	-	-	2	2
GbE RJ45 DMZ Ports	1			
Wireless Interface	-	802.11 a/b/g/n	-	802.11 a/b/g/n
USB Ports (Client / Server)	1 / 1			
Console (RJ45)	1			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	1.5 / 1.5 / 1.5 Gbps			
Firewall Latency (64 byte UDP packets)	4 μs			
Firewall Throughput (Packets Per Second)	2.2 Mpps			
Concurrent Sessions (TCP)	500,000			
New Sessions/Sec (TCP)	4,000			
Firewall Policies	5,000			
IPSec VPN Throughput (512 byte packets)	1 Gbps			
Gateway-to-Gateway IPSec VPN Tunnels	200			
Client-to-Gateway IPSec VPN Tunnels	500			
SSL-VPN Throughput	30 Mbps			
Concurrent SSL-VPN Users (Recommended Max)	100			
IPS Throughput	200 Mbps			
Antivirus Throughput (Proxy Based / Flow Based)	35 / 50 Mbps			
Virtual Domains (Default / Max)	10 / 10			
Max Number of FortiAPs (Total / Tunnel Mode)	10 / 5			
Max Number of FortiTokens	100			
Max Number of Registered FortiClients	200			
High Availability Configurations	Active / Active, Active / Passive, Clustering			
Dimensions				
Height x Width x Length (in)	1.50 x 8.50 x 5.83 in	1.50 x 8.50 x 6.18 in	1.50 x 8.50 x 5.83 in	1.50 x 8.50 x 6.18 in
Height x Width x Length (mm)	38 x 216 x 148 mm	38 x 216 x 157 mm	38 x 216 x 148 mm	38 x 216 x 157 mm
Form Factor	Desktop			
Weight	1.9 lbs (0.9 kg)			
Environment				
Power Required	100-240 VAC, 50-60 Hz			
Max Current	110 V / 1.5 A, 220 V / 0.75 A	110 V / 1.5 A, 220 V / 0.75 A	110 V / 1.5 A, 220 V / 0.75 A	110 V / 1.5 A, 220 V / 0.75 A
Total Available PoE Power Budget	-	-	30.8 W	30.8 W
Power Consumption (Avg / Max)	11.7 / 14 W	11.7 / 14 W	27.4 / 45.2 W	29.9 / 48.2 W
Heat Dissipation	40 BTU/h	40 BTU / h	154 BTU / h	165 BTU / h
Operating Temperature	32 - 104 °F (0 - 40 °C)			
Storage Temperature	-31 - 158 °F (-35 - 70 °C)			
Humidity	20 to 90% non-condensing			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Compliance				
	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications				
	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN			

Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files.

FORTINET.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FORTINET

BROCHURE

FortiOS™ 4.0 Software

Redefining Enterprise Network Security

Updated for FortiOS 4.0 MR3

FortiOS 4.0 Software — Redefining Enterprise Network Security

Today's Security Challenges

Networks are faster than ever, carrying more information and rich content - as well as potentially malicious payloads. The volume and sophistication of attacks have also increased, requiring more accurate detection methods and the ability to block threats before they can do any damage. Simultaneously, cost-reduction programs are forcing IT departments to consolidate network equipment and operating expenses wherever possible.

Fortinet Offers A Simple, Powerful Solution

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of all FortiGate® consolidated security platforms. FortiOS 4.0 software leverages the hardware acceleration provided by custom FortiASIC™ processors, delivering the most comprehensive suite of IPv6-ready security and networking services available within a single device. FortiGuard® Security Subscription Services ensure that FortiOS threat protections are always up to date, defending your network against the latest, most sophisticated and dynamic attacks.

FortiOS 4.0 Security Features

- Enterprise-class Firewall - IPv6-Ready
- Application Control
- Integrated Intrusion Prevention
- Identity-based Policy Enforcement
- SSL-encrypted Traffic Inspection
- VPN - IPSec and SSL
- Antivirus / Antispyware
- Antispam
- Data Loss Prevention (DLP)
- Flow-based Inspection Options
- Web Filtering
- Endpoint Network Access Control (NAC)
- Vulnerability Management
- Monitoring, Logging and Reporting
- WAN Optimization
- Integrated Wireless Controller
- VoIP Security
- Centralized Management
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services
- FortiGuard Security Updates

> ***"A further disrupting factor is the rate of change within enterprise networking — inexorably increasing throughput, more Web-based applications, more complex connections within applications, more complex data centers and more data being presented to customers means that firewalls have had to keep up with features and performance to meet these changing needs".***
>
> Greg Young and John Pescatore
> Gartner Magic Quadrant for Enterprise Network Firewalls - March 2010.

Complete Security

Fortinet designed and built FortiOS 4.0 security services from the ground up to deliver integrated performance and effectiveness that standalone products simply cannot match. The services work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before theft and damage can occur.

Purpose-Built for Performance

FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC processors. This combination of custom hardware and software gives you the best security and performance possible from a single device.

Simplified Deployment and Management

FortiOS 4.0 software lowers costs and reduces IT staff workloads. Centralized management and analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges. You gain the flexibility of having a unified security policy at the device level along with an appliance-based centralized management platform for large deployments.

Unique Visibility and Control

Advanced security features such as Flow-based Inspection and Wireless Controller capability allow you to monitor and protect your network from endpoints to core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

FortiOS 4.0 Software — Complete Content and Network Protection

Fortinet continues to increase the breadth and depth of security and networking services included in the FortiOS purpose-built operating system. By adding new functionality and enhancing the performance of existing services, FortiOS software continues to demonstrate why it remains the gold standard for multi-threat security. FortiOS 4.0 software includes many advanced security and networking features, some of which are highlighted below:

Application Control

Application control enables you to define and enforce policies for thousands of applications running on your network and endpoints. Newer Web-based applications such as Facebook, Skype, Twitter and Salesforce.com can be detected and controlled at a granular level, regardless of ports and protocols used. Application classification and control is essential to manage the explosion of new Internet-based technologies bombarding networks today.

Antivirus / Antispyware

In addition to three proxy-based antivirus databases, FortiOS also includes a high-performance flow-based antivirus option. The flow-based option allows you to scan files of any size while maintaining the highest levels of performance. In addition, flow-based inspection enables scanning of files within compressed files to detect hidden threats. By providing you the flexibility to choose your antivirus engine, you can balance your performance and security requirements for your environment.

Data Loss Prevention (DLP)

Fortinet DLP identifies sensitive information and blocks transmission to points outside of your network perimeter. A sophisticated pattern-matching engine monitors traffic from multiple applications, such as Web-based email and encrypted instant messaging, and provides audit trails to aid in policy compliance. You can select from a wide range of configurable actions to log, block and archive data, as well as ban or quarantine rogue users. Flow-based DLP options are also available.

Web Filtering

Inappropriate Web surfing and use of Web-based applications can result in lost productivity, network congestion, malware infection and data loss. Web Filtering controls user access to Web-based applications such as instant messaging, peer-to-peer file sharing and streaming media, while blocking phishing sites and blended network attacks. In addition, botnet command and control traffic and fast flux file downloading can be blocked. Flow-based Web filtering options are available.

Wireless Controller

All FortiGate and FortiWiFi™ consolidated security platforms have an integrated wireless controller, enabling centralized management of FortiAP™ secure access points and wireless LANs. Unauthorized wireless traffic is blocked, while allowed traffic is subject to identity-aware multi-threat security inspection. You can control network access, quickly update security policies, and identify and suppress rogue access points - all from a single console.

WAN Optimization

Wide area network (WAN) optimization accelerates applications over your wide area links while ensuring multi-threat security enforcement. FortiOS 4.0 software eliminates unnecessary and malicious traffic and optimizes legitimate traffic by reducing the amount of information transmitted between applications and servers. This improves performance of applications and network services while reducing bandwidth requirements.

Firewall

Fortinet firewall technology combines ASIC-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block complex threats. FortiGate firewall protection integrates with other key security features such as virtual private network (VPN), antivirus, intrusion prevention, Web filtering, antispam and traffic shaping to deliver multi-layered security that scales from small business appliances to multi-gigabit core network and data center platforms.

Intrusion Prevention

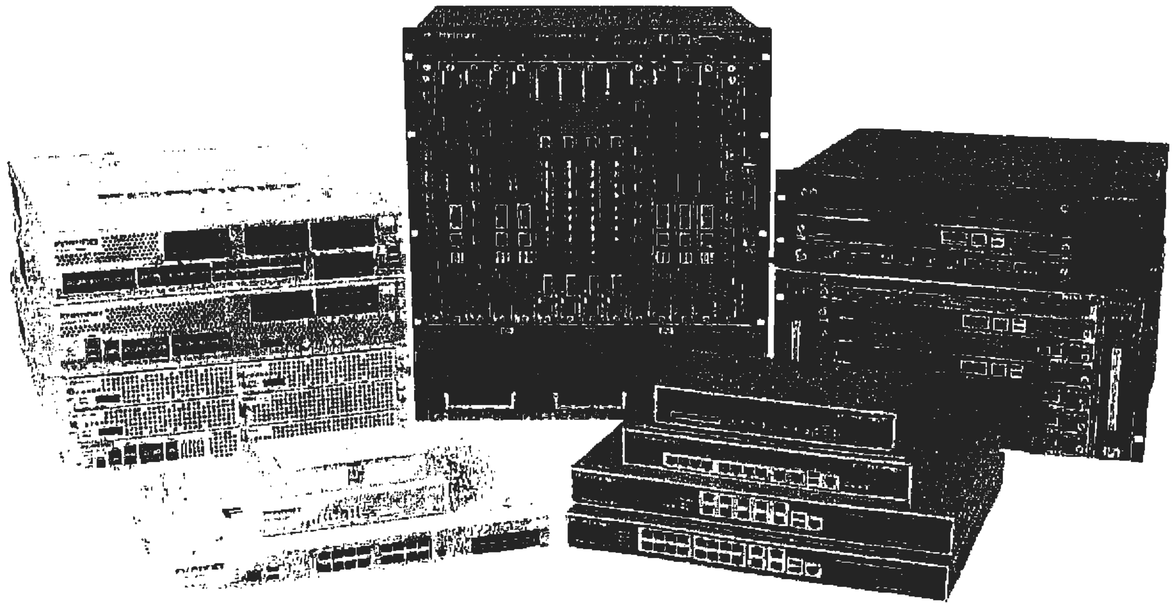
Intrusion prevention system (IPS) technology provides protection against current and emerging network level threats. In addition to signature-based detection, we perform anomaly-based detection whereby our system alerts users to traffic that fits a specific profile-matching the attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that are incorporated into our FortiGuard services.

VPN

Fortinet virtual private network technology provides secure communications between multiple networks and hosts using IPSec and SSL VPN protocols. Both services leverage custom FortiASIC processors to accelerate encryption and decryption network traffic. Once the traffic has been decrypted, multi-threat inspection including antivirus, intrusion prevention, and Web filtering can be applied and enforced for all content.

Antispam

Fortinet antispam technology offers a wealth of features to detect, tag, quarantine, and block spam messages and malicious attachments generated by spambots and compromised systems. FortiGate and FortiWiFi platforms and FortiClient endpoint security agents offer integrated antispam functionality as part of their multi-layered protection, backed by the FortiGuard Antispam Service.



TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

Fortinet's Security Solution

Today's organizations need more network protection than traditional firewalls can provide. Stand-alone security solutions add complexity and cost without providing comprehensive protection.

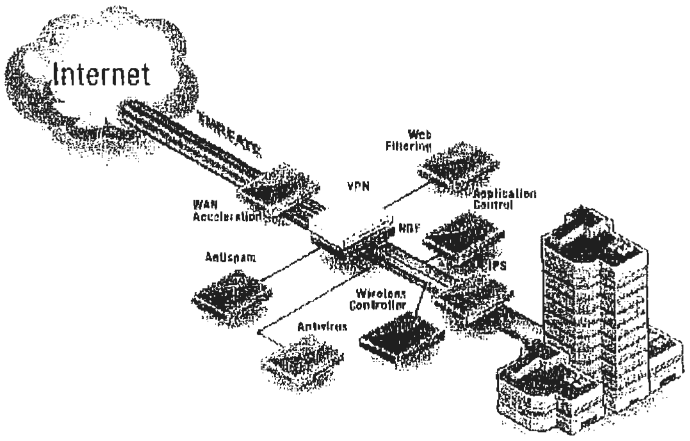
FortiOS integrates many functions together into a single security platform, including firewall, VPN, application control, intrusion prevention, and web filtering. Fortinet delivers complete content protection, which is more than simply identifying applications and allowing or denying the traffic. It is application control coupled with identity-based policy enforcement of all content.

Complex & Costly

Typical Adhoc Model

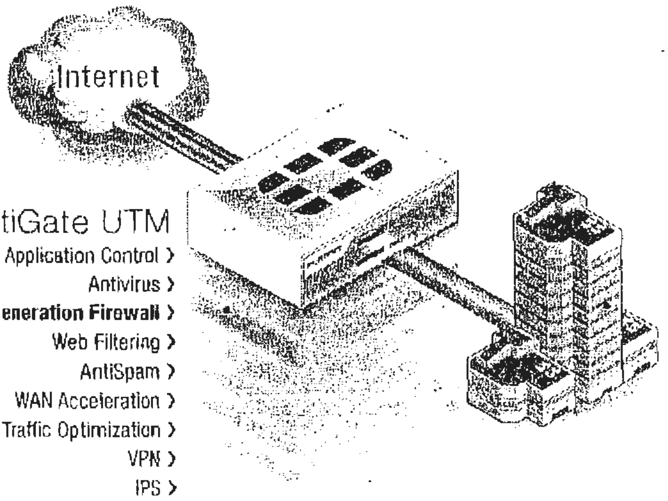
Typical Adhoc Model

Numerous stand-alone security products from different vendors are costly to deploy, complex to manage, and degrade network performance and reliability.



Simple & Cost Effective

Fortinet UTM Model



FortiGate UTM

Application Control ›
Antivirus ›
Next Generation Firewall ›
Web Filtering ›
AntiSpam ›
WAN Acceleration ›
Traffic Optimization ›
VPN ›
IPS ›
DLP ›
WiFi Controller ›

The Fortinet UTM Model

Fortinet's fully integrated security technologies offer increased protection, improved performance, reduced costs, and greater reliability.

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

FortiOS Security Services

FIREWALL

ICSA Labs Certified (Enterprise Firewall)
NAT, PAT, Transparent (Bridge)
Routing Mode (RIP, OSPF, BGP, Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
Group-based Authentication & Scheduling
SIP/H.323 /SCCP NAT Traversal
WINS Support
Explicit Proxy Support (Citrix/TS etc.)
VoIP Security (SIP Firewall / RTP Pinholing)
Granular Per-Policy Protection Profiles
Identity/Application-Based Policy
Vulnerability Management
IPv6 Support (NAT / Transparent mode)

VIRTUAL PRIVATE NETWORK (VPN)

ICSA Labs Certified (IPSec/SSL-TLS)
PPTP, IPSec, and L2TP + IPSec Support
SSL-VPN Concentrator (including iPhone client support)
DES, 3DES, and AES Encryption Support
SHA-1/MD5 Authentication
PPTP, L2TP, VPN Client Pass Through
Hub and Spoke VPN Support
IKE Certificate Authentication (v1 & v2)
IPSec NAT Traversal
Automatic IPSec Configuration
Dead Peer Detection
RSA SecurID Support
SSL Single Sign-On Bookmarks
SSL Two-Factor Authentication
LDAP Group Authentication (SSL)

ANTIVIRUS / ANTISPYWARE

ICSA Labs Certified (Gateway Antivirus)
Includes Antispyware and Worm Prevention

Protocols:	HTTP/HTTPS	SMTP/SMTPS
	POP3/POP3S	IMAP/IMAPS
	FTP	Major IM Protocols

Flow-Based Antivirus Scanning Mode
Automatic "Push" Content Updates
File Quarantine Support
Databases: Standard, Extended, Extreme, Flow
IPv6 Support

WEB FILTERING

76 Unique Content Categories
FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages
HTTP/HTTPS Filtering
Web Filtering Time-Based Quota
URL/Keyword/Phrase Block
URL/Category Exempt
Blocks Java Applet, Cookies, Active X
MIME Content Header Filtering
IPv6 Support
Flow-based Web Filtering

APPLICATION CONTROL

Identify and Control Over 1400 Applications
Traffic-Shaping (Per Application)
Facebook Application and Category Control
Differential Services Support Per-Application
Control Popular Apps Regardless of Port/Protocol:

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

INTRUSION PREVENTION SYSTEM (IPS)

ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update
IPv6 Support

DATA LOSS PREVENTION (DLP)

Identification and Control of Sensitive Data in Motion
Built-In Pattern Database
RegEx-based Matching Engine for Customized Patterns
Configurable Actions (block/log)
Customized Patterns
Supports IM, HTTP/HTTPS, and More
Many Popular File Types Supported
International Character Sets Supported
Document Fingerprinting
Flow-Based DLP Scanning Mode

ANTISPAM

Support for SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
Real-Time Blacklist/Open Relay Database Server
MIME Header Check
Keyword/Phrase Filtering
IP Address Blacklist/Exempt List
Automatic Real-Time Updates From FortiGuard Network

ENDPOINT COMPLIANCE AND CONTROL

Monitor & Control Hosts Running FortiClient Endpoint Security
Vulnerability Scanning of Network Nodes

FortiOS Networking Services

NETWORKING/ROUTING

Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing for IPv4 (RIP, OSPF, IS-IS, BGP, & Multicast protocols)
Dynamic Routing for IPv6 (RIP, OSPF, & BGP)
Multi-Zone Support
Route Between Zones
Route Between Virtual LANs (VLANs)
Multi-Link Aggregation (802.3ad)
IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Admin Access, Management)
VRRP and Link Failure Control
sFlow Client

TRAFFIC SHAPING

Policy-based Traffic Shaping
Application-based and Per-IP Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth
Shaping via Accounting, Traffic Quotas

VIRTUAL DOMAINS (VDOMs)

Separate Firewall/Routing Domains
Separate Administrative Domains
Separate VLAN Interfaces
10 VDOM License Std. (more can be added)

DATA CENTER OPTIMIZATION

Web Server Caching	TCP Multiplexing
HTTPS Offloading	WCCP Support

HIGH AVAILABILITY (HA)

Active-Active, Active-Passive
Stateful Failover (FW and VPN)
Device Failure Detection and Notification
Link Status Monitor
Link failover
Server Load Balancing

WAN OPTIMIZATION

Bi-Directional / Gateway to Client/Gateway
Integrated Caching and Protocol Optimization
Accelerates CIFS/FTP/MAPI/HTTP/HTTPS/Generic TCP
Requires a FortiGate device with Hard Drive

FortiOS Management Services

MANAGEMENT/ADMINISTRATION OPTIONS

Web UI (HTTP/HTTPS)
Telnet / Secure Command Shell (SSH), and Command Line Interface (CLI)
Role-Based Administration
Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
Multiple Administrators and User Levels
System Software Rollback
Configurable Password Policy
Customizable Dashboard Widgets (Web UI)
Central Management via FortiManager (optional)

LOGGING/MONITORING/VULNERABILITY MGMT

Network Vulnerability Scanning
Graphical Report Scheduling Support
Graphical Real-Time and Historical Monitoring
Local and Remote Syslog/WELF server logging
SNMP Support
Email Notification of Events
VPN Tunnel Monitor
Optional FortiAnalyzer Logging (including per-VDOM)
Optional FortiGuard Analysis and Management Service

FIREWALL USER AUTHENTICATION OPTIONS

Local Database
Windows Active Directory (AD) Integration (w/ FSAE)
External RADIUS/LDAP/TACACS+ Integration
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support
LDAP Group Support
FortiToken Support

WIRELESS CONTROLLER

Unified WiFi and Access Point Management
Automatic Provisioning of APs
On-wire Detection and Blocking of Rogue APs
Virtual APs with Different SSIDs
Multiple Authentication Methods

Note: The list above is comprehensive and may contain FortiOS features which are not available on all FortiGate appliances. Consult FortiGate system documentation to determine feature availability.

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

Fortinet Advantages

Consolidated,Comprehensive Security

Consolidated security technologies enable higher throughput and lower latency, with greater visibility and control over users, applications, and data.

Hardware-Accelerated Performance

Custom FortiASIC processors accelerate the processing-intensive tasks required to secure networks in today's sophisticated threat environment.

Global Threat Research and Support

FortiGuard® Labs threat research and FortiCare™ support teams deliver the 24/7 real-time protection and support you need to stay ahead of a constantly evolving threat landscape and an ever-changing networking environment.

Rigorous 3rd Party Certifications

Fortinet is the only unified threat management vendor to earn certifications across all core security technologies. These independent certifications demonstrate our ability to consolidate multiple security technologies into a single device while still meeting the highest standards of performance and accuracy.

Fortinet Certifications

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

FIPS VALIDATED 140-2

COMMON CRITERIA
EAL 4+ CERTIFIED

ICSA labs CERTIFIED IPSEC - BASIC

ICSA labs CERTIFIED ANTI-SPAM

ICSA labs CERTIFIED NETWORK IPS

IPv6 READY

NSS approved

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, web application firewall, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with hardware return for replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel +65-6513-3734
Fax +65-6295-0015

FORTINET

Magic Quadrant for Enterprise Network Firewalls

7 February 2013 ID:G00229302

Analyst(s): Greg Young

VIEW SUMMARY

Advances in threats have driven mainstream firewall demand for next-generation firewall capabilities. Buyers should focus on the quality, not quantity, of the features and the R&D behind them. This market includes mature vendors and new entrants.

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built appliances and virtualized models for securing corporate networks. Products must be able to support single-enterprise firewall deployments and large global deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles, products, and a sales and support ecosystem focused on the enterprise.

The firewall market has evolved from simple stateful firewalls to NGFWs, incorporating full-stack inspection to support intrusion prevention, application-level inspection and granular policy control. Such NGFWs will eventually subsume mainstream deployments of stand-alone network intrusion prevention system (IPS) appliance technology at the enterprise edge. Gartner already sees this shift in the form of reduced IPS buying activity and a flattening of IPS market growth, but Gartner believes the security-conscious segment of the market will continue to use separate IPSs. The reality of product life spans cannot be ignored in this market shift, however: Enterprises refresh individual firewalls, on average, every five years, and IPSs are refreshed about four years or less, so the market won't shift quickly.

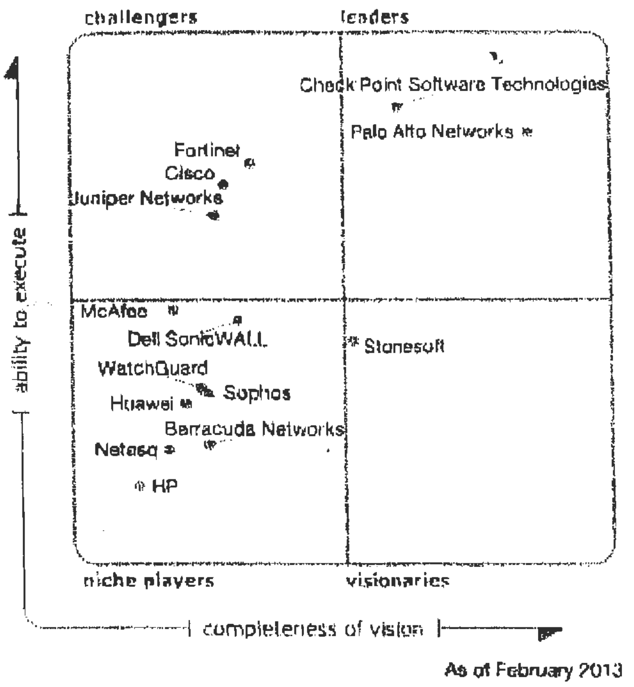
Although firewall/VPN and IPS are converging, other security products are not. All-in-one or unified threat management (UTM) products are suitable for small or midsize businesses (SMBs) but *not*for the enterprise: Gartner forecasts that this separation will continue until at least 2016. Branch-office firewalls are becoming specialized products, diverging from the SMB products (for more information, see "Magic Quadrant for Unified Threat Management").

Gartner has successively increased the Magic Quadrant evaluation weighting for NGFW features. This edition signals a significant increase in the weighting of NGFW capabilities reflecting the changing markets and enterprise needs.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (February 2013)

Return to Top

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks (www.barracudanetworks.com) acquired European firewall vendor phion in 2009. Barracuda has been focused primarily on selling to the low end of the midsize-enterprise market at low cost. The former phion firewall is now branded as the Barracuda NG Firewall family across a range of appliances and a virtual version. Barracuda is assessed as a Niche Player for enterprises, mostly because it serves a set of placements when the Leaders are otherwise not welcome. We do not see the Barracuda NG Firewall frequently displacing Leaders otherwise. The firewall has application control and reputation services, and the Barracuda NG Firewall Vx is a virtual version.

Strengths

- The Barracuda NG Firewall is a good option for Barracuda customers who want to get a firewall product from the same vendor, especially for those organizations that are outgrowing their current UTM and/or moving into point products.
- The Barracuda NG Firewall unit support staff offer good local language support, especially in Germany, Switzerland and Austria.
- The Barracuda NG Firewall is a strong competitor in situations where price is highly weighted in the selection.

Cautions

- Barracuda customers are primarily SMBs, and the vendor does not yet have well-established enterprise network security channels or support.
- No vendor we surveyed listed Barracuda as a significant enterprise competitive threat. Barracuda has not been visible on the firewall shortlists of Gartner customers. Most interest has been instead via incumbent customers who have other Barracuda products.
- Full Internet Protocol version 6 (IPv6) still needs to be implemented. Some clients Gartner interacted with commented that the IPS reporting could be improved.

Return to Top

Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is a well-known, pure-play security company with the largest firewall installed base, and strong and broad channel support.

The majority of enterprises choose to use Check Point-branded appliances, although options are also available for a software install on self-sourced servers, a virtual machine install (Secure Gateway Virtual Edition [VE]), or the remaining partners, such as Crossbeam (recently acquired by Blue Coat Systems). The IPSO and SecurePlatform operating systems are unified under the new GAiA operating system release.

Check Point has continued to expand its software "blade" strategy (that is, preloaded software modules enabled through subscription keys). Gartner believes that the blades, which match NGFW features (for example, IPS, user identity, application control and anti-bot), will continue to have high attach rates, but there will be little demand for some blades that enable other features (for example, email security and Web antivirus).

Check Point is assessed as a Leader for enterprises, because we continuously see the vendor competing in demanding selections, providing an NGFW development path that customers are asking for, and retaining customers based on its features and channel strength.

Strengths

- Check Point scored high as a significant enterprise competitive threat by all vendors Gartner surveyed. Gartner observes that Check Point is in most shortlists in which security protection is weighted highly. The Check Point Experience user events continue to be an effective platform for new announcements and maintaining loyalty.
- The Check Point management console is ranked highly by customers with a large number of firewalls with differing configurations or a significant compliance burden: Check Point continues to invest considerable intellectual property into the management console, in recognition of the importance configuration has to administrators in enterprise deployments. Surveyed clients were consistently managing complex environments with many firewalls and users.
- Check Point has a strong field of product options, such as Virtual Systems for virtualized firewalling, VE for running in virtualized environments, and its SmartEvent correlation product. The wide availability of appliance models and software options enables Check Point to meet the requirements for complex enterprise networks. Check Point has performed favorably on third-party IPS testing, and Gartner clients comment that the IPS is a significant improvement over previous Check Point IPS products.
- Check Point has good capability for meeting large-enterprise requirements with the newer high-end 21000 and 61000 series appliances.
- Check Point continues to have the strongest third-party ecosystem of security products that integrate easily with Check Point's management platform. Gartner has received positive feedback from clients regarding the stability and use of Check Point's GAiA operating system release.

Cautions

- High price is a common reason provided by Gartner customers for replacing or considering replacing Check Point firewalls. This is not an issue in new placements, in which a premium firewall function is required and justifies the investment. In firewall selections and support renewals, Gartner often hears that support pricing is complex, and price negotiations are difficult.
- Gartner views the Check Point Software Blade architecture as having only short-term attractiveness; it is a difficult long-term strategy option for enterprises. Enterprises are cautious about adding new functions to firewalls. With 12 blades now available for the Check Point firewall, Gartner believes charging for features that are included by competitors is challenging and can appear "UTM-like," thus alienating enterprises.
- In the survey to vendors, Check Point was listed second most often as the vendor they replace. Although a longtime Magic Quadrant Leader, Check Point needs to take a more aggressive R&D and marketing path if it wishes to change its current trajectory.
- Gartner believes the new managed security service provider (MSSP) offering will likely alienate some MSSP partners.

Return to Top

Cisco

Cisco (www.cisco.com) has an exceptionally broad network security product portfolio across the network security, Web security and email security tiers. Cisco has chosen to retain the Adaptive Security Appliance (ASA) firewall brand, and it has added application control under the CX feature brand and has appended the X designator as a suffix to newer models that include IPS. Cisco is assessed as a Challenger for enterprises over the evaluation period, because we did not see it frequently displacing Leaders based on vision or feature, and it does not effectively compete in the NGFW field that is visible to Gartner. Instead, Gartner sees Cisco winning mostly procurements through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not highly weighted evaluation criteria (that is, as part of a solution sell in which security is one component). Gartner expects IPS to be added to the CX models in 2013, whereas currently a choice must be made: either application control or IPS. Also in 2013, a single management console is likely (for more information, see "Vendor Rating: Cisco").

Strengths

- Cisco has significant market share in security. The new option for an Enterprise License Agreement (ELA) for security software and hardware is of interest to Cisco security customers who are undertaking multiyear deployments and wish to maintain a timetable and product flexibility.
- Gartner clients consistently rate as excellent the Cisco support network, which is the most-often-cited reason for loyalty to Cisco security products. The vendor has strong channels, broad geographic support and the availability of other security products. Surveyed Cisco firewall clients consistently ranked having other products from this vendor as the most important factor in the selection.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, with firewalls also available via the Firewall Services Module blade for 6500 series switches, Cisco ASA 1000V Cloud Firewall, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router.
- The integration of reputation features across Cisco security products is a differentiator that is often missed in enterprise selections. Although many competitors have reputation features, the breadth of the Cisco reputation feed is a quality factor.

Cautions

- Cisco firewall products are selected more often when security offerings are added to Cisco's infrastructure, rather than when there is a shortlist with competing firewall appliances. Cisco was listed by competitors as the product they most often replace. Gartner does not view Cisco's security strategy as messaging effectively in the broader NGFW market.
- The requirement to add a hardware module (the Advanced Inspection and Prevention Security Services Model [AIP-SSM]) to add IPS capability to some models of ASA firewall appliance remains a barrier to deployment and a competitive disadvantage for branch-office deployments. The add-in module does, however, provide processing help with the deep inspection load. If the SSM module is used for IPS, then it cannot be used for other content inspection. However, Gartner does not expect Cisco to continue selling the non-X models beyond 2014.
- The security strategy, product offering nomenclature and product descriptions are often cited by Gartner clients as confusing and orthogonal to competitors' terms and road maps. By using terms such as "context-aware" and "CX" rather than application control or NGFW, Cisco is sometimes excluded as clients experience confusion in comparing Cisco's offering to competitors' offerings.

Return to Top

Dell SonicWALL

SonicWALL (www.sonicwall.com), formerly owned by Thoma Bravo and acquired in 2012 by Dell, is now renamed Dell SonicWALL and is headquartered in California. Although the majority of Dell SonicWALL's business had been selling UTM to SMBs, the SuperMassive line is aimed at the high end at very competitive price/performance points. Other Dell SonicWALL security products include Secure Sockets Layer (SSL) VPN, email security gateways, clean wireless and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class Network Security Appliance (NSA), NSA and TZ. Dell SonicWALL is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well (for example, retail, upper-midsize businesses and service providers), and we do not see it often displacing Leaders.

Strengths

- Dell SonicWALL's broad model range is a good option for wide remote-office deployments requiring many smaller devices, such as in retail or franchise outlets, or with Type C enterprises (see Note 1). The Dell acquisition represents a broader channel for SonicWALL products, especially into midsize organizations or organizations that already have a strong Dell relationship.
- Dell SonicWALL has improved its enterprise go-to-market ability, rather than attempting to push an SMB UTM upmarket, by aligning product lines specifically to the horizontal — SuperMassive for data centers, service providers and ISPs, and the E-Class NSA for enterprises.
- The SuperMassive line has achieved market traction in high-throughput firewall deployments, such as carriers and service providers, in which firewall throughput, low latency and price are foremost. Clients that Gartner surveyed liked the high performance of the SuperMassive appliance.

Cautions

- Most of Dell SonicWALL's firewall and other security product lines have been primarily SMB-focused and not competitive in most enterprises. Dell SonicWALL does not yet have a broad-enough enterprise channel, support and management console features to be considered in competition with the Leaders and to become a bigger part of the NGFW conversation. Some clients that Gartner interacts with have reported that the console management of the SuperMassive appliance needs integration improvements for the lower-tier firewall appliances.
- Dell SecureWorks presents a channel conflict for sales to other MSSPs, which can view Dell SonicWALL as part of a competitor. Gartner rarely sees Dell SonicWALL in most Type A and Type B enterprise firewall selections.
- Dell SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in the Gartner customer base. Although it has a good NGFW feature set, Dell SonicWALL has not been visible in NGFW selections as seen by Gartner.

Return to Top

Fortinet

California-based Fortinet (www.fortinet.com) has long focused on using purpose-built hardware to produce UTM appliances at strong price/performance points. Although the firewall features in its UTM products met most of the needs of firewall-focused large-enterprise buyers, Fortinet's approach and philosophy continue to be focused on "everything in one box," which has caused its brand and channel support to be slow to evolve from its SMB base. Fortinet continues to make progress within the Gartner customer base, usually by expanding out from branch-office or retail deployments to capture the primary or core firewalls, and it is seen winning some data center implementations. Fortinet is a significant threat to competitors in this market because of the company's hardware expertise, competitive pricing and steady revenue growth. Fortinet is a viable shortlist contender for most of the enterprise firewall market. It is assessed as a Challenger mostly because we see it displacing competitors on value and performance, but not often beating Leaders in mainstream enterprise selections. Fortinet has steadily been expanding its support offerings to be better-aligned to the enterprise, including options for dedicated technical account managers.

Strengths

- Fortinet has a large R&D team and uses this to outmaneuver competitors that often rely on OEM arrangements. Fortinet continuously delivers new features in the application-specific integrated circuit (ASIC) and operating system, providing extensive pressure on competitors and pleasing the channel. Fortinet maintains road map agility to get to the market quickly, with new features that are fully console-integrated. This also has enabled Fortinet to expand its portfolio of nonfirewall network security offerings, which provides increasing cross-selling opportunities.
- Fortinet continues to increase its wins against the larger firewall incumbents when customers are deploying in emerging areas — such as in-the-cloud firewalls, MSSPs and service providers — and carriers and ISPs are deploying in areas in which high-end performance is required. Fortinet is price-competitive, especially when using multiple virtual domains, and appliance reliability is reported as very high. Fortinet has invested significantly in obtaining and completing certifications.
- Its firewalls have high-end performance from purpose-built hardware and a wide model range, including bladed appliances for large enterprises and carriers, as well as SMB and branch-office solutions. Although many competitors are increasing their reliance on chips from Intel or other third-party providers for their future performance gains, Fortinet (much as in its software development) maintains control of its own dual processors — one ASIC for network security operations and the second for content inspection.
- The Fortinet Mezzanine Card (FMC) and Advanced Mezzanine Card (AMC) accelerated interface modules (AIMs) are options for some enterprises and carriers to expand performance or networking interfaces without having to resort to appliance replacements.

Cautions

- Management capabilities were most often listed as the reason when Fortinet was shortlisted but not selected in enterprises. However, where aggressive console use is not required, or where multiple firewalls share the same policy, the Fortinet console is highly competitive.
- Fortinet does not have a dedicated NGFW, but instead presents its UTM product, expecting a subset of product features to be used. Fortinet's marketing focus on using UTM for enterprises has persisted in what is effectively an attempt to change enterprise buying behavior. This can steer away enterprise customers. Fortinet also has historically defined enterprises as 500 users — about half the number used by Gartner and competitors. The UTM messaging also has enterprises excluding

Fortinet from NGFW shortlists, even when the necessary capabilities (such as application control) are present.

- Gartner believes Fortinet does not have a strong third-party security vendor ecosystem, and Fortinet does not hold any customer conferences.

Return to Top

HP

Acquired in 2009 as part of HP's acquisition of 3Com, China-based H3C Technologies was formed as a joint partnership between Huawei and 3Com, and it has been shipping firewalls since 2003. Now that H3C is part of HP (www.hp.com), the former H3C firewalls are being leveraged by HP, especially in its current customer base. Models include the HP F5000 and F1000 (also called the A Series Firewalls in some marketing material), an add-in module for switches, the HP Threat Management Services zl module, and firewall software that can be added to the HP E5400 zl and E8200 zl series switches. HP is assessed as a Niche Player primarily because of its geographic sales and presence, and the current absence of NGFW features, such as IPS and application control. (See "Vendor Rating: HP" for more information.)

Strengths

- HP and legacy H3C have a strong regional presence in China and the Asia/Pacific region, and sales are increasing for incumbent HP networking customers. HP and H3C firewalls will be of most interest to China-based enterprises, especially where other H3C or 3Com networking equipment is used.
- There is a wide range of models (including a high-throughput, blade-based chassis), branch-office models and enterprise models, all with a flat-fee URL model.
- It has broad IPv6 support.

Cautions

- HP firewalls are not visible outside the Asia/Pacific region, and HP has to address concerns from many geographies about relying on technology developed in China. This situation has led to HP having to recommend competitors' firewall products as optional replacements for HP firewall products' end of life.
- The firewall lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation, which is usually seen in enterprise contenders.
- HP does not currently have a coherent network security strategy that is able to challenge market Leaders.

Return to Top

Huawei

China-based Huawei (www.huawei.com) has been shipping firewall products for almost a decade (for more information, see "Vendor Rating: Huawei").The range of appliances and models is extensive, especially for higher-throughput options, and for customers who already have Huawei products and wish to expand that business to firewalls. Unified security gateway (USG) is the primary enterprise line, and Eudemon is the line for carriers and service providers. The majority of Huawei firewalls are sold to carriers, ISPs and cloud and service providers. Although Huawei has received negative coverage in North America and Europe regarding suspicions of "back doors," this is not a concern in all regions and verticals.

Strengths

- Gartner assesses Huawei as having a very good overall network security strategy.
- Customers whose networks are based primarily on Huawei infrastructure products can include Huawei firewalls.
- The top end of the Huawei firewall line has a very high throughput and is a good shortlist candidate for carriers.

Cautions

- The majority of Huawei firewalls have very little visibility outside the Asia/Pacific region; however, placements in EMEA represent a significant share.
- Despite significant steps undertaken by Huawei to address concerns about relying on technology developed in China, the concerns remain for many prospective customers.

Return to Top

Juniper Networks

Firewall offerings of California-based Juniper Networks (www.juniper.net/us/en) are in multiple model lines: SRX, SSG, ISG and vGW. The Juniper SRX firewall, the primary firewall offering, offers a router as a basic element of the firewall, and it runs the same Junos operating system as is on other

Juniper infrastructure components. Having routing in the firewall is of interest to a narrow segment of customers. Juniper has AppSecure for application control and visibility, and it has added a hypervisor-based stateful firewall under the vGW product name. Juniper's Junos Space Security Design is the successor product for the current security management within Juniper Network Security and Manager (NSM). Juniper is assessed as a Challenger for enterprises, because we see Juniper selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features. Juniper is, however, often shortlisted and/or selected in mobile service provider deployments and enterprise data center deployments, primarily because of price and high throughput on its largest appliances. Gartner sees Juniper mostly selected as an adjunct to the Juniper network infrastructure business.

Strengths

- Customers whose networks are already standardized on Juniper's Junos-based infrastructure products can benefit from the Space Security Design console, as it is part of the Junos Space network management platform.
- Where Juniper was selected, clients cited a global logistics channel and/or good price for high firewall throughput.
- Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models. Juniper has a strong range of branch-office firewalls complementing the enterprise products. Its branch-office firewalls include WAN optimization controller and an Avaya voice gateway.

Cautions

- As a network infrastructure vendor, Juniper is sometimes at a disadvantage selling into Cisco networks, where buying any Juniper security equipment can be resisted as a Cisco network equipment replacement. Some Gartner clients report that having Security Design as part of Space can be perceived as a challenging proposition versus pure-play dedicated firewall consoles. Juniper clients that Gartner interacts with have commented that Space Security Design is not yet fully featured.
- Gartner does not assess Juniper as having a highly compelling or differentiated security vision, or one well-known to non-Juniper customers. Juniper's emphasis on the Mykonos technology is not effective with network buyers in competing with the NGFW messaging of Leaders. Gartner rarely sees Juniper considered on shortlists by customers looking for an NGFW and instead sees Juniper more often mentioned by customers looking to replace a firewall.
- Gartner believes that most enterprises want an operating system in their security products that differs from the one in infrastructure components.

Return to Top

McAfee

McAfee (www.mcafee.com/us) was acquired by Intel in early 2011. McAfee obtained its firewall products through the acquisition of Secure Computing in late 2008. The former Sidewinder product has been renamed to the McAfee Firewall Enterprise. McAfee has seven product models and a VX virtualized version. The McAfee Firewall Enterprise is certified for use on Crossbeam X-Series blades, CloudShield CS-4000 and Riverbed Steelhead appliances.

The road map for Firewall Enterprise is more important for consideration than the current features in the product. A re-engineered Firewall Enterprise integrated with the McAfee IPS on a purpose-built hardware platform will be the milestone for which to watch and a road map toward an NGFW. McAfee is assessed as a Niche Player for enterprises, mostly because it serves a set of placements when the Leaders are otherwise not welcome.

Strengths

- The wide breadth of the McAfee Global Threat Intelligence (GTI) reputation feed is a positive quality element, as is the TrustedSource feature used to block known bad Internet Protocol (IP) addresses.
- The McAfee Event Reporter for Firewall provides guidance on firewall configuration and is included with the product. MFE has good identity and geolocation options.
- Visibility of ePolicy Orchestrator (ePO) host information within the firewall reporting and console tools is of interest to current McAfee ePO customers.
- The "one price" of Firewall Enterprise is an advantage versus the complex pricing schemes of many competitors. URL filtering is included at no charge.

Cautions

- Gartner believes that the Intel acquisition has presented a significant distraction for the McAfee network security unit. Gartner security analysts always believed that the network security appliance business made no sense for Intel and believe that this has proven true in the market.

- Although it has been four years since the acquisition of Secure Computing, the McAfee IntruShield IPS engine, available in the stand-alone IPS appliances, is not yet integrated into the Firewall Enterprise. The current Firewall Enterprise IPS capabilities are not competitive with leading NGFW vendors' capabilities, and users generally comment negatively to Gartner on the IPS configuration and performance.
- McAfee is rarely seen on Gartner client network firewall shortlists; however, when it is, the time taken to navigate the general McAfee support system is the most often listed criticism heard from Gartner clients during the selection process. McAfee was not listed by any vendor we surveyed as a significant enterprise competitive threat. Declining to participate in NSS Labs' firewall evaluation has not helped McAfee's visibility.

Return to Top

Netasq

Netasq (www.netasq.com) has been a pure-play network security vendor headquartered in France for more than a decade, selling firewalls, vulnerability management and messaging security gateways. The acquisition of Netasq by Cassidian CyberSecurity (an EADS company) is now completed. Netasq will continue to operate as an independent company. Netasq products mostly appeal to both EU-based midsize businesses and enterprise companies. Virtual versions are also available in the V line. Netasq is assessed as a Niche Player for enterprises, mostly because it best serves midsize businesses, and agencies in portions of EMEA, or when the Leaders or Challengers do not have the usual advantages. Feature sets are divided between enterprise and UTM lines.

Strengths

- By not using traditional signatures and, instead, focusing on heuristics, Netasq has innovated on an IPS path that is different from mainstream firewall vendors, which has positioned it more uniquely for countering new kinds of attacks. Users report that they like its policy-based management and real-time policy warning.
- It is VPN-certified for "EU Restricted" use in the EU, which is of interest to governments and agencies looking for simpler procurement.
- Netasq gets good marks from midsize enterprises for features and ease of use, and it has good channel support in EMEA.
- Netasq users comment to Gartner that the branded training and EU support are very good. Cassidian projects can include Netasq firewalls as part of the solution.

Cautions

- The majority of Netasq's penetration, visibility and channel is focused on EMEA, especially France.
- Although having a good feature set, Netasq has not been part of NGFW selections as seen by Gartner because of the company's low visibility in other geographies.

Return to Top

Palo Alto Networks

Palo Alto Networks (www.paloaltonetworks.com) is a California-based pure-play network security company. Palo Alto Networks had a widely publicized initial public offering (IPO) in July 2012, added a virtual version, and held its first user conference. Palo Alto Networks continues to both drive competitors to react in the firewall market and to move the overall firewall market forward. It is assessed as a Leader, mostly because of its NGFW design, direction of the market along the NGFW path, consistent displacement of competitors, rapidly increasing revenue and market share, and market disruption that forces competitors in all quadrants to react.

Strengths

- A crisp focus on enterprise NGFW features and messaging is viewed positively by firewall operators in enterprises.
- Gartner clients consistently rate the Palo Alto Networks application identification (App-ID) and IPS higher than competitors' offerings for ease of use and quality. The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream. This "single pass" is a design advantage versus unnecessary inspection that can occur in competing products that process traffic in serial order — from firewall to IPS, and then to application control.
- Palo Alto Networks continued through 2012 to generate the most firewall inquiries among Gartner customers by a significant margin. Palo Alto Networks was consistently on most NGFW competitive shortlists, and we observed high customer loyalty and satisfaction from early adopters. A simple pricing structure helps in procurements versus competitors who charge for features that Palo Alto includes.

- Most firewall vendor road maps are following the Palo Alto Networks NGFW road map, placing these vendors at a competitive disadvantage.

Cautions

- The PA series of firewalls do not yet have certification at the EAL4+ level for the Common Criteria for Information Technology Security Evaluation.
- Palo Alto Networks does not have appliances with the higher throughput of some competitors, meaning they are less often considered for larger data center placements.
- The company does not have products in adjacent security markets, which would allow for cross-selling opportunities. The company has room to develop a third-party product support ecosystem.
- With product pricing higher than that of competitors that have fewer features, Palo Alto Networks is challenged to win RFPs, whereby price is the greatest weighted factor, especially for selections that are firewall only (that is, no IPS or application control).

Return to Top

Sophos

Security company Sophos (www.sophos.com) has co-headquarters in the U.K. and the U.S. The Sophos UTM necessarily targets SMBs. Gartner observes Sophos usually scoring highly where price is the primary factor and where Sophos products are already in place. Sophos is assessed as a Niche Player for enterprises, mostly because it wins over Leaders in some selections based on features or with a very specific channel. The Sophos UTM is available as an appliance or software load, and as a certified Amazon Virtual Private Cloud connector, and it has application control.

Strengths

- Sophos' endpoint product customers can have the same vendor provide them their UTM solution.
- Users like Sophos' price, and surveyed users consistently comment on the ease of installation as a strong point.
- A free firewall is available in the "UTM Essential Firewall" edition that includes firewall, network-address translation (NAT), routing and Web GUI. The free edition runs on a PC, within a virtual machine or in the VMware vSphere Edition.
- The Sophos blog has been a visible medium in the security ecosystem for establishing Sophos as a broader security participant.

Cautions

- The Sophos firewall is not often seen in enterprise selections in the Gartner client base. As a UTM, the product is not a match for most enterprises and instead is seen more often in SMBs. The Sophos UTM usually competes with other SMB firewall vendors' solutions.
- Sophos was not listed by any vendor we surveyed as a significant enterprise competitive threat, and it has not been highly visible on NGFW shortlists among Gartner clients.

Return to Top

Stonesoft

Headquartered in Finland, public company Stonesoft (www.stonesoft.com) has expanded its operations into North America and other geographies, especially Eastern Europe. Stonesoft is focused on network security and has been very innovative in analyzing threat evasion techniques, and it is known for its well-functioning clustering and active-active options. Stonesoft is assessed as a Visionary for enterprises, because it has firewall features that are not seen in many competitors' products, and its firewall features are both innovative against modern and advanced threats and focused on the enterprise. Stonesoft also provides stand-alone IPS and SSL VPN products. The StoneGate brand has been dropped in favor of the Stonesoft name. The Stonesoft NGFW product is offered across a wide range of appliances, including branch office and a virtualized firewall version that is certified for VMware. Furthermore, the MIL-320 model was introduced as a military-grade ruggedized appliance.

Strengths

- Stonesoft's threat research concerning evasive attacks has increased security credibility and visibility for the company and products. As a company headquartered neither in the U.S. or China, Stonesoft is being shortlisted where enterprise operations span multiple countries, including the U.S. and China.
- Stonesoft has a long legacy with high-availability technology, and it has very reliable clustering and active-active deployability. Almost all surveyed Stonesoft clients ranked these features as important in their selections.
- The Stonesoft Management Center console can send and receive logs in multiple formats — such as syslog, Common Event Format (CEF), Log Event Enhanced Format (LEEF), Common Log Format

(CLF) and WebTrends Enhanced Log File Format (WELF) — from non-Stonesoft devices to aid in correlation and reporting.

- Support pricing is slightly lower than the industry average, and it has a loyal customer base.

Cautions

- Stonesoft has limited market visibility and channel strength outside of EMEA, and it has low visibility within the Gartner customer base, although its firewall and company revenue has increased also outside of EMEA.
- Although the Stonesoft product has many next-generation features, the Stonesoft brand is not yet widely known.

Return to Top

WatchGuard

WatchGuard (www.watchguard.com) is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM series of products span performance and feature ranges demanded by large enterprises; however, WatchGuard's branding, channel support and management capabilities tend to be more oriented toward SMBs. A well-established security-focused company, WatchGuard also has products that include SSL VPN and the Extensible Content Security (XCS) email and Web security line. The XTM-branded firewall models fall into two categories. The XTM 2 Series and XTM 5 Series are UTM, and the XTM 8 Series and the XTM 1050 and 2050 models are targeted for the enterprise. One important strategic improvement has been WatchGuard's introduction of the "NGFW Bundle" option for appliances that is better-suited to enterprise buyers than the UTM-only approach. WatchGuard is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing Leaders. In May 2012, WatchGuard obtained EAL4+ Common Criteria certification for the XTM line.

Strengths

- WatchGuard's strong price/performance has enabled it to win price-sensitive competitions across retail, branch-office, remote-office and Type C enterprise deployments. Gartner has observed an increase in visibility of WatchGuard in client inquiries since the last report.
- Users report high satisfaction with the reporting function in the WatchGuard management console. Enterprise models are correctly targeted at NGFW, rather than UTM functionality.
- WatchGuard's products have a low rate of product vulnerabilities compared with most competitors' products.
- The new RapidDeploy feature is of interest in areas where many firewalls will be deployed, such as in franchises or retail, or via an MSSP.

Cautions

- Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections. Enterprise channel and support will need to be expanded if WatchGuard wishes to compete in a broader segment of enterprises.
- Although having a good NGFW feature set, WatchGuard has not been part of many NGFW selections as seen by Gartner. WatchGuard clients that Gartner interacts with generally reported the IPS quality as being average.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed and has low visibility in the Gartner customer base.

Return to Top

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Return to Top

Added

Huawei was added.

Dell acquired SonicWALL, which was in the previous Magic Quadrant, but the name has now changed.

Return to Top

Dropped

No vendors were dropped. AhnLab, Sourcefire, Cyberoam and F5 were examined as part of this analysis but did not yet meet the inclusion criteria at the time of the analysis of this report.

Return to Top

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet the market definition and description were considered for this report under the following conditions:

- Gartner analysts assess that the company has an ability to effectively compete in the enterprise firewall market.
- Gartner clients generate inquiries about the company.
- The company regularly appears on shortlists for selection and purchases.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than $10 million and within a customer segment that is visible to Gartner.

Exclusion Criteria

Network firewall companies that were not included in this report may have been excluded for one or more of the following conditions:

- The company did not meet the inclusion criteria.
- The company has minimal or negligible apparent market share among Gartner clients, or it is not actively shipping products.
- The company is not the original manufacturer of the firewall product. That includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and ISPs that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and we do not rate platform providers separately.
- The company's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs, such as UTM firewalls or those for small office/home office placements, are not targeted at the market this Magic Quadrant covers (enterprise) and are excluded.
- The company has primarily a network IPS with a non-enterprise-class firewall.
- The company has personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls (WAFs; see Note 2) — all of which are distinctly separate markets.

Return to Top

Evaluation Criteria

Ability to Execute

- *Product or service:* This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continuously deployed in enterprises, and the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a company's ability to execute. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is foremost over revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and being able to support complex deployments and modern demilitarized zones. Having a low rate of vulnerabilities in the firewall is important. Logistical capabilities for managing appliance delivery, product service and port density matter. Support is rated on quality, breadth and value of offerings through the specific lens of enterprise needs.
- *Overall viability:* Overall business viability includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (and the wins are compared with Gartner data on such competitions held by our

customers), and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of enterprise clients and presence on competitive shortlists.

- *Sales execution/pricing:* We evaluate the company's pricing, deal size, installed base and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. Presales and postsale support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, including the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains. Cost of ownership over a typical firewall life cycle (three to five years) was assessed, as was the pricing model for conducting a refresh while staying with the same product and replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.
- *Market responsiveness and track record:* This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in the firewall market and how enterprises deploy network security.
- *Market execution:* Competitive visibility is a key factor, including which vendors are most commonly considered top competitive solutions, during the RFP and selection process, and which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking looks at which vendors consider each other to be direct competitive threats, such as driving the market on innovative features co-packaged within the firewall, or offering innovative pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and the inability of a product to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.
- *Customer experience and operations:* This includes management experience and track record, as well as the depth of staff experience specifically in the security marketplace. The greatest factor in this category is customer satisfaction throughout the sales and product life cycle. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Evaluation Criteria	**Weighting**
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Table 1. Ability to Execute Evaluation Criteria

Source: Gartner

Completeness of Vision

- *Market understanding and strategy:* This includes providing a track record of delivering on innovation that precedes customer demand rather than an "us too" road map. We also evaluate the vendor's overall understanding and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning road maps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put a plan in place, show that they are following their plan and modify their plan as they forecast the market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive road map and delivery of NGFW is weighted very highly. The NGFW capabilities are expected to be integrated to achieve both correlation improvement and functional improvement.

- *Sales strategy:* Sales strategy includes preproduct and postproduct support, value for pricing, and providing clear explanations and recommendations for detection events. Building loyalty through credibility with full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and to do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.
- *Offering strategy:* This criterion focuses on a vendor's product road map, current features, NGFW integration, virtualization and performance. Credible independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integration with other security components is also weighted, as well as product integration into other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office. Innovation such as introducing practical new forms of intelligence that the firewall can apply policy to is highly rated.
- *Business model:* This includes the process and success rate for developing new features and innovation, and R&D spending.
- *Vertical, industry and geographic strategy:* This includes the ability and commitment to service geographies and vertical markets, such as complex enterprise international deployments, MSSPs, carriers or governments.
- *Innovation:* This includes R&D and quality differentiators, such as:

o Performance, which includes low latency, new firewall mechanisms and achieving high IPS throughput and low appliance latency

o Firewall virtualization and securing virtualized environments

o Integration with other security products

o Management interface and clarity of reporting — the more a product mirrors the workflow of the enterprise operation scenario, the better the vision

o "Gives back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity

Products that are not intuitive in deployments or operations are difficult to configure or have limited reporting, and they are scored accordingly.

The more a product mirrors the workflow of the enterprise operation scenario, the better the vision. Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Low

Table 2. Completeness of Vision Evaluation Criteria
Source: Gartner (February 2013)

Quadrant Descriptions

Leaders

The Leaders quadrant contains a mix of large and midsize vendors, with the common element of making products that are built for enterprise requirements. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rules/policy minimization. An NGFW capability is an important element as enterprises move away

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safeguarding features, providing expert capability, rather than treating the firewall as a commodity, and having a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss and options for hardware acceleration.

Return to Top

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not leading with features. Many Challengers are slow to work toward or do not plan for an NGFW capability, or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challenger products are often well-priced and, because of their strength in execution, vendors can offer economic security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they are obligated to place security or firewall products as a lower priority in their overall product sets. Firewall market Challengers will often have significant market share but trail smaller market share Leaders in the release of features.

Return to Top

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with leaders and challengers. Most visionary products have a good NGFW capability but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations willing to update products more frequently and switch vendors if required. Where firewalling is a competitive element for an enterprise, Visionaries are good shortlist candidates. Vendors that do not have NGFW capabilities are adding them in a defensive move, while those with strong NGFW offerings are focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better identification of malicious protocols at multi-Gbps rates.

Return to Top

Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls, makers of multifunction firewalls for SMBs, or branch-office-only product makers attempting to break into the enterprise market. Many Niche Players are making larger SMB products, with the mistaken hope that this will satisfy enterprises. Some enterprises that have the firewall needs of an SMB (for example, some Type C "risk-averse" enterprises) may consider products from Niche Players, although other models from Leaders and Challengers may be more suited. If local geographic support is a critical factor, then Niche Players can be shortlisted.

Return to Top

Context

The enterprise firewall market is one of the largest and most mature security markets. It is populated with both mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization and use of the cloud, have increased demand for new firewall features and capabilities. Organizations' final product selection decisions must be driven by their specific requirements, especially in the relative importance of management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, and integration with the established security and network infrastructure.

Return to Top

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding both to changes in threats and changes in enterprise network speed and complexity. The firewall market is highly penetrated in the larger markets (North America and Western Europe), which means to protect their installed base, incumbents must add improved capabilities and increase performance, or face either replacement by innovative new market entrants or commoditization by low-cost providers. Firewall policy management (FPM) products are increasingly used for managing complexity (see Note 3).

Next-Generation Firewalls

One key area of firewall evolution has been support for what Gartner called in 2009 "next-generation firewall" features — namely, integrated deep packet inspection intrusion detection, application identification and granular control. The key differentiators in these areas are IPS effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and fine-grained policy enforcement in about the top 25 business applications. Identity-based policy enforcement or abilities to enforce policy on thousands of applications have been highly touted but rarely used.

Because it is highly penetrated, the firewall market is driven by refresh cycles. We have seen some common patterns in the firewall market as enterprises with three- to five-year-old firewalls and IPSs evaluate replacement:

- Enterprises not currently using IPS at all migrate to NGFW with minimal use of advanced features.
- Enterprises with firewalls and stand-alone IPSs employed primarily in detection mode (that is, using minimal signature sets) migrate to NGFW using the built-in IPS capabilities.
- Enterprises with firewalls and stand-alone IPS used for active prevention with large signature sets and some custom signatures migrate to NGFW for the firewall but continue using stand-alone IPS.
- High-security environments upgrade to NGFW for the firewall and upgrade IPS to next-generation IPS (NGIPS; see "Defining Next-Generation Network Intrusion Prevention").

Virtualized Firewalls

As data center virtualization has continued, demand for virtual appliance support has grown. Performance and the ability to manage firewall policy through a single integrated management console for stand-alone appliances or virtual appliances are key differentiators. Gartner has not seen the firewall features of virtualization platforms, such as those offered with VMware, as major competitors to firewall vendors, as the need for separation of duties drives reluctance to trust the infrastructure to protect the infrastructure. As other virtualization platforms, such as Xen and Hyper-V, gain traction, managing heterogeneous virtualized firewalls will present a challenge. Performance remains a barrier to wider deployment: Almost all network firewalls today are delivered on purpose-built appliances because of the poorer performance of running firewalls on general-purpose servers. Almost all operating systems within firewall appliances are uniquely hardened, subject to stringent third-party security evaluations. Security-minded enterprises are also rightly skeptical of running firewalls within a hypervisor that is between the threat and the firewall.

New Firewall Players

Acquisitions continued during the evaluation period, but there were also new entrants into the firewall market. Dell acquired SonicWALL, and Cassidian CyberSecurity (an EADS company) acquired Netasq. Palo Alto Networks had its IPO in July 2012. In December 2011, Sourcefire announced a firewall product, and in January 2012, F5 announced that the Big-IP data center firewall had been certified as a network firewall by ICSA Labs. Asia-based vendors, such as Huawei, began to explore expanding outside of their home geographies, with the Mideast and Eastern European markets the initial target geographies.

During the evaluation period, the firewall market grew to $6.3 billion in 2011. This is on target with our estimate in the previous Magic Quadrant. For 2012, Gartner estimates the firewall market will have grown 10% to reach $6.93 billion. For 2013, Gartner expects the enterprise firewall market will grow 11%, reaching $7.7 billion. We forecast this market will reach a compound annual growth rate of 10% through 2016.

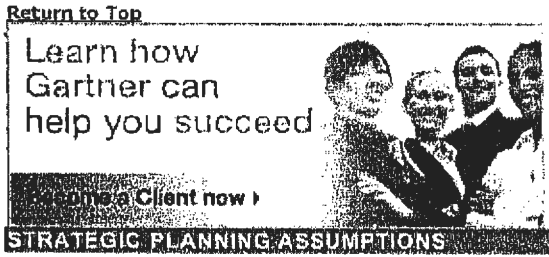
Confusing Use of "Application" and "Firewall" in Three Distinct Products

Overlapping terminology and confusing marketing can lead to confusion between the three distinct issues of application control, WAFs and firewalls on application delivery controllers (ADCs). The firewall application control approaches by most NGFW vendors, such as Check Point, Fortinet, Palo Alto Networks and Dell SonicWALL, are mostly about controlling external applications, such as Facebook and peer-to-peer (P2P) file sharing.

WAFs are different: WAFs are placed primarily in front of Web servers in the data centers. Pure-play WAF companies, such as Imperva, or data center infrastructure vendors that provide WAF technology within their ADCs are concerned with custom internal Web applications.

While some ADC vendors, such as F5, are now introducing network firewalling within their ADCs as well, Gartner does not see NGFW and WAF technologies converging because they are for different tasks at different placements. As Gartner advises clients, most enterprises have a single brand of network firewall for all the placements, including Internet-facing, virtualized, data center and branch (see "One Brand of Firewall Is a Best Practice for Most Enterprises"). These data center firewalls will be challenged to gain any noteworthy share until they can provide competitive firewalling for all enterprise placements; they can, however, serve a very niche set of placements, such as in cases in which the data center is a separate business with its own firewall operations staff.

Return to Top



STRATEGIC PLANNING ASSUMPTIONS

Virtualized versions of enterprise network safeguards will not exceed 20% of unit sales by year-end 2016.

Through 2015, more than 75% of enterprises will continue to seek network security from a vendor different from their infrastructure vendor.

Less than 10% of Internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.

ACRONYM KEY AND GLOSSARY TERMS

ADC	application delivery controller
AIM	accelerated interface module
AMC	Advanced Mezzanine Card
AIP-SSM	Advanced Inspection and Prevention Security Services Model
ASA	Adaptive Security Appliance
ASIC	application-specific integrated circuit
CEF	Common Event Format
CLF	Common Log Format
ELA	Enterprise License Agreement
ePO	ePolicy Orchestrator
FPM	firewall policy manngement
FIPS	Federal Information Processing Standard
FMC	Fortinet Mezzanine Card
Gbps	gigabits per second
GTI	Global Threat Intelligence
IOS	Internetwork Operating System
IP	Internet Protocol
IPO	initial public offering
IPS	intrusion prevention system
IPv6	Internet Protocol version 6
ISP	Internet service provider
LEEF	Log Event Enhanced Format
MFE	McAfee Firewall Enterprise
MSSP	managed security service provider
NAT	network-address translation
NGFW	next-generation firewall
NSM	Network Security and Manager
P2P	peer-to-peer
SMB	small or midsize business
NSA	Network Security Appliance
SSL	Secure Sockets Layer
USG	unified security gateway
UTM	unified threat management

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

VE	Virtual Edition
WELF	WebTrends Enhanced Log File Format
XCS	Extensible Content Security

EVIDENCE

This Magic Quadrant was conducted in accordance with Gartner's well-defined methodology. The analysis in this report was based primarily on interviews and interactions during firewall inquiries with Gartner clients since the last report. We also consider surveys completed by vendors, vendor briefings conducted at the vendors' request throughout the year, interviews with references provided by the vendors, and supporting Gartner quantitative research on market share.

Guidelines for responding to the full survey were provided at the time of issue of the survey. Responses were nevertheless of variable quality. Responses that were lower quality (for example, ignored the question, poor grammar, inability to explain key concepts, inability to provide high-quality explanations of use cases, and inability to go beyond technical capabilities and demonstrate an understanding of the business environment) or did not meet the guidelines generally tended to score lower. Vendors that declined to provide a survey response were assessed by Gartner as to what the likely reply would have been (usually this is in relation to specific revenue breakdowns). Some vendors declined to answer certain questions due to market restrictions and therefore did not fare as well under some of the scoring criteria.

We asked for a specific number of references from each vendor, and each reference customer is supplied with a structured survey. References are scored on the basis of both the quality of the reference and what they tell us. For each vendor, we take into account comments from both that vendor's own references, and what other vendors' customers say about that particular vendor. Vendors can be notably affected by the inability to have sufficient reference customers provide input.

NOTE 1
TYPE A, B AND C ENTERPRISES

Enterprises vary in their aggression and risk-taking characteristics. Type A enterprises seek the newest security technologies and concepts, tolerate procurement failure and are willing to invest for innovation that might deliver lead time against their competition; this is the "lean forward" or aggressive security posture. For Type A enterprises, technology is crucial to business success. Type B enterprises are "middle of the road." They are neither the first, nor the last, to bring in a new technology or concept. For Type B enterprises, technology is important to the business. Type C enterprises are risk-averse for procurement, perhaps are investment-challenged and are willing to cede innovation to others. They wait, let others work out the nuances and then leverage their learning; this is the "lean back" security posture more accustomed to monitoring rather than blocking. For Type C enterprises, technology is critical to the business and is clearly a supporting function.

NOTE 2
CONFUSION OF BUYERS CONCERNING WAFS

The advent of application control in firewalls has led to some natural confusion between the NGFW and WAF markets in the minds of buyers. These markets today remain very distinct. The critical difference is of direction: application control in NGFW is concerned primarily with applications external to the enterprise (for example, peer-to-peer and Facebook), whereas WAF is concerned with protecting custom Web applications on servers internal to the enterprise. Although a few firewalls offer optional WAF modules, these are rarely enabled; instead, we see WAF deployed either as a stand-alone product (such as from Imperva), an off-premises service (such as from Akamai), or within an ADC (such as from F5).

NOTE 3
FPM TOOLS

Third-party FPM vendors (such as AlgoSec, Tufin and FireMon) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the FPM market is still somewhat small, the customers requiring help with complexity are the very largest, and the market is growing. Additionally, very large enterprises may have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single vendor solution is usually the best choice. All FPM vendors support multiple firewall products, whereas no firewall vendor will effectively manage a competing product, and FPM vendors are expanding into managing other network security devices, such as IPS.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

© 2013 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website,http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.

About Gartner | Careers | Newsroom | Policies | Site Index | IT Glossary | Contact Gartner

Magic Quadrant for Unified Threat Management

19 July 2013 ID:G00245469

Analyst(s): Greg Young, Jeremy D'Hoinne

VIEW SUMMARY

Unified threat management devices provide small or midsize businesses with multiple network security functions in a single appliance. Buyers should focus on performance when every targeted feature is enabled, and on total cost of ownership instead of initial purchase price.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees, with revenue ranging from $50 million to $1 billion. UTM products for the SMB market must provide the following functions at a minimum:

- Standard network stateful firewall functions
- Remote access and site-to-site virtual private network (VPN) support
- Secure Web gateway (SWG) functionality (anti-malware, URL and application control)
- Network intrusion prevention focused on workstation protection

All UTM products contain various other security capabilities, such as email security, Web application firewalls (WAFs) and data loss prevention. However, the vast majority of SMBs only utilize the firewall, intrusion prevention and SWG functionalibes. They also request a basic level of application control, mostly to restrict the use of Web applications and cloud services (such as social media, file sharing and so on). Features related to the management of mobile devices create a potentially attractive differentiator for this market (see "How Unified Threat Management Tackles the Consumerization of IT"). Browser-based management, basic embedded reporting, and localized software and documentation, which don't appeal to large enterprises, are highly valued by SMBs in this market. SMBs should evaluate UTM devices based on the controls they will actually use, the performance they will get for those features, and the quality of vendor and channel (and managed services) support that is available.

Given the continuing economic uncertainty, most SMBs have strong IT budgetary and staffing constraints. This causes them to highly value ease of deployment and use, strong local channel support, and flexible pricing. Leading UTM vendors will:

- Be aggressive and flexible in pricing, reducing upfront costs, eliminating hidden fees, and ensuring durable software and hardware support.
- Focus on midsize businesses' need for the right network security at the right price, rather than trying to upsell them to enterprise products and capabilities.
- Provide product management features that simplify deployment and ongoing operations.
- Make it easy for customers with evolving security needs to add licenses to existing platforms by unifying their support contract renewal dates.
- Offer efficient vendor technical support and easy-to-diagnose systems to value-added resellers (VARs), which often handle a large number of devices with understaffed technical teams.
- Be early to add new security features that are showing up as separate point products.

Many UTM vendors are heading toward the console and management being fully in the cloud. Gartner

STRATEGIC PLANNING ASSUMPTIONS

Replacement of UTM by cloud options will remain at less than 5% through 2016; however, by then, most UTM devices will leverage cloud-assisted security and management features.

By 2016, 15% of SMBs will use mobile device management capabilities from their UTM platforms to handle mobility — up from less than 1% today

NOTE 1
UTM REVENUE DIFFERENTIATION

Gartner does not include branch office firewall revenue as UTM revenue.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and believes that, although it's convenient for the vendors to do so, a portion of the SMB market will not accept this exclusively cloud model for reasons of latency, trust, and being able to access the console when under attack. Reporting and log retention are well-suited to the cloud, but not exclusively.

For 2012, Gartner estimates that worldwide revenue in the UTM market totaled approximately $1.53 billion, which represents an 18.7% growth over our estimate for 2011 (see Note 1). Gartner believes that the UTM market will continue to grow faster than many other security markets, but we also see a number of trends applying downward pressure on market growth. Regardless, we forecast continued growth in the UTM market of approximately 15% compound annual growth rate through 2018

We see the following positive trends continuing to drive growth in the UTM market:

- A steady number of new, small (that is, fewer than 100 employees) organizations.
- SMBs in emerging countries buying their first UTM products to secure increasingly faster and more highly business-critical broadband Internet connections. This scenario represents "greenfield" growth for the market — often with a preference for country or region-specific vendors.
- A continued refresh of first-generation UTM products by SMBs — especially midsize businesses (100 to 999 employees), and especially in North America and Western Europe — due to product aging and the demand for higher-speed Internet connectivity. This demand drives the replacement of existing product with the incumbent's newer version, or replacement of the incumbent by a competitor.

Some trends will limit market growth:

- The increased use of smartphones, tablets and even 4G-equipped laptops moves more small business Internet traffic to direct connections to wireless data service providers, as opposed to through UTM appliances to wired Internet service providers (ISPs).
- The pricing and features of cloud-based SWG services (see "Magic Quadrant for Secure Web Gateways") are very attractive to small businesses because they offer flexible pricing and meet the needs for securing mobile users. While most of those services only deal with Secure Sockets Layer (SSL) and HTTP traffic, they represent most of the needs of many small businesses, and can reduce their UTM needs to a simple firewall/router. However, the SWG market is smaller than the UTM market and follows a slightly slower growth.
- The increased use of cloud-based email (such as Google Apps for Business or Microsoft Office 365) reduces the demand for email security, since those services include integrated email antivirus functionality
- As lower-midsize companies grow to become upper-midsize and enterprise size, their security needs will get more complex, and they will outgrow their UTM appliances and deploy enterprise network security platforms, such as next-generation firewalls and SWGs.

Gartner believes that the downward trends now balance the positive trends and might put increased pressure on the market in the future, thereby causing us to maintain our UTM market growth forecast from our previous outlook. These trends have also led to limited entries/exits of vendors into/from this market. In 2012, Cassidian CyberSecurity, a subsidiary of the EADS Group, acquired Netasq. Arkoon Network Security, Barracuda Networks, Endian and eSoft did not meet the inclusion criteria.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management

services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements

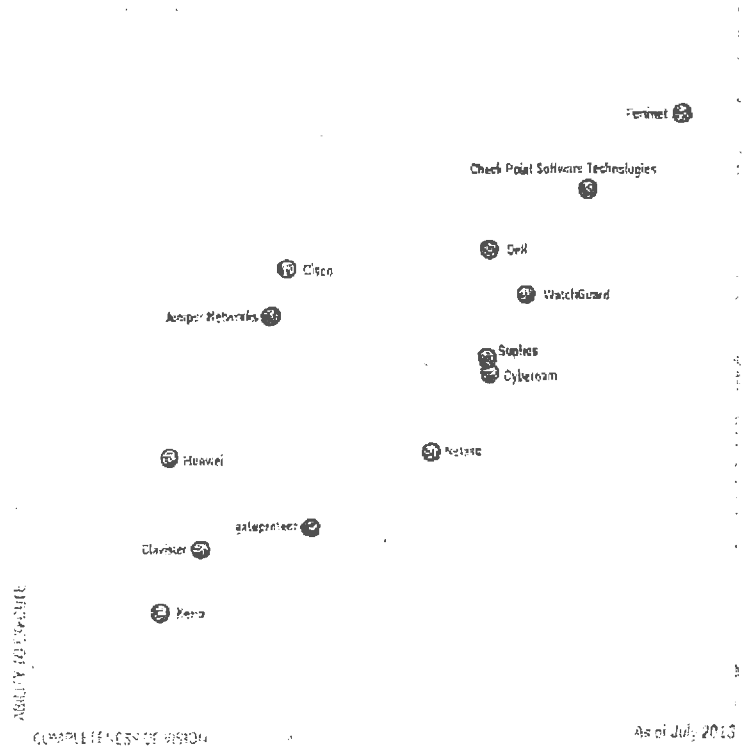
Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

TRENDS AND TECHNOLOGIES, INC
CERTIFIED TRUE COPY



Source: Gartner (July 2013)

Return to Top

Vendor Strengths and Cautions

Check Point Software Technologies

Check Point Software Technologies is one of the largest pure-play security companies, and has been expanding from the enterprise security market to the UTM market since 2004. Check Point has been very active in the UTM segment. In the past 18 months, it has targeted SMBs with new appliances (primarily the 600 and 1100 series), with part of a global product line update (referred to as the "2012 appliances") and with the release of a common operating system (OS) for every security gateway (GAiA) Its SMB portfolio now includes 11 appliances and a cloud-based security service. Fundamental to Check Point firewall offerings is the set of software options referred to as Software Blades.

Strengths

Check Point's reporting and management console is highly rated by midsize companies. Known primarily as an enterprise security provider, Check Point has expanded into the SMB space for midsize companies that are seeking premium firewall products.

Check Point's UTM solutions benefit from its enterprise-level security features, such as ThreatCloud and Anti-Bot. The Software Blades approach allows for customization of features.

Selective direct user involvement with its UserCheck technology improves security awareness and reduces the risk of policy infringement.

The consolidation of the appliance portfolio and the unification of the different Software Blades under the GAiA OS will ease maintenance and reduce the learning curve for SMB resellers and end users.

Check Point has very strong capabilities for virtualized versions and securing virtualization.

Cautions

- Price is often cited as the primary reason for not selecting Check Point solutions.
- Check Point has approximately 30 different Software Blades. Having so many options creates an overly complex pricing scheme for many SMBs and small resellers, compared with the competition. Blade packages, however, are available for the purpose of simplification.

Return to Top

Cisco

Cisco uses its network infrastructure placements as an entree to bundle in adjunct security solutions for SMBs. Cisco now addresses SMBs with the ISA500 Series for small businesses (four models), the ASA 5500-X Series for midsize companies (two models) and the cloud-managed MX series (six appliances) based on the Meraki solutions (acquired in 2012). In addition to the dedicated security solutions, Cisco has a large portfolio of network solutions that can provide security features, such as the Integrated Services Router (ISR).

Strengths

- Cisco support is rated well by Gartner customers; its entrenchment in the network infrastructure makes it easy to find well-trained staff to support Cisco security implementations.
- The ISA500 Series and ASA 5500-X Series show feature improvements compared with the previous generations of products; the removal of the requirement for hardware add-in modules for intrusion prevention or content inspection allows the new ASA product line to compete with other midsize UTM devices.
- The cloud-based MX series provides an easy way to centrally manage distributed organizations looking for PCI compliance.
- The integration of Cisco AnyConnect with the ISA500 Series and the ASA 5500-X Series, in addition to the existing Cisco client for mobile devices, makes Cisco a good choice for SMBs with many mobile users.

Cautions

- Cisco's UTM devices have low visibility among Gartner SMB clients and do not generate many inquiries, because clients view Cisco primarily as an enterprise security player. The vendors we surveyed continue to identify Cisco as one of the most replaced brands.
- Cisco's 2012 UTM refresh showed that it could catch up with basic SMB needs, but it still has to demonstrate its ability to drive the market.

Return to Top

Clavister

Clavister, which is headquartered in Sweden, targets primarily ISPs with its cloud services. It addresses SMBs through its branded security appliances, the Eagle Series and Wolf Series. Also, Clavister's technology is provided as an OEM solution.

Strengths

- The security quality of Clavister's products is often mentioned by its customers. Also, its ISO 9001:2008 certification and two-year standard return-and-repair warranty appeal to SMBs that weight reliability highly.
- The Clavister X8 series of rugged appliances is a good fit for specific midsize vertical industries.

Cautions

- The focus on core firewall needs, rather than completeness of features, translates into a competitive gap for specific use cases.
- Gartner has not observed notable client interest outside of Europe, and Clavister has generated a very low level of inquiry from Gartner clients over the past 12 months.
- Clavister was never cited as a competitive threat by surveyed vendors.

Return to Top

Cyberoam

Based in India, Cyberoam is a pure-play vendor for the UTM market, focusing solely on SMBs. Over the

MA
TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

past nine months, it released its NG Series with 12 new appliances and five virtual appliances. Cyberoam consistently communicates about the integration of user identity in every component of the UTM configuration, and about the availability of Web Application Firewall on the UTM.

Strengths

Cyberoam's product development approach of providing competitive pricing, coupled with the regular addition of new features, has proved to be a successful choice for the SMB market.

Its well-organized management interface minimizes the burden implied by the presence of numerous features.

Cloud-based centralized management, which is free for certified partners, can be a valuable asset for managed security service providers (MSSPs).

Users report that they like the built-in reporting capabilities.

Cautions

Cyberoam's visibility remains low with Gartner clients, and it is not yet cited as a threat by surveyed vendors and resellers.

Cyberoam does not yet have a significant sales presence in North America.

Gartner believes that Cyberoam's channel marketing is overly focused on perceived competitor shortcomings, rather than on promoting its own brand and benefits to customers.

Return to Top

Dell

Dell acquired SonicWALL in 2012 and kept SonicWALL as the name of its firewall product line. Dell sells two product lines to the SMB market: the SonicWALL TZ Series for the smallest businesses and the SonicWALL NSA Series for small and midsize companies. It also targets the enterprise market with its SonicWALL SuperMassive Series, competing with established enterprise players on the price/performance ratio. Dell also provides SSL VPN and email security gateway.

Strengths

Gartner often sees Dell shortlisted based on the SonicWALL brand being well-established in the SMB market.

Many customers report to Gartner that the TZ Series product line is a cost-effective solution with very good overall performance. Low total cost of ownership (TCO) is often cited as a reason for choosing Dell SonicWALL products.

The TZ Series' clean wireless features are available for smaller locations, and Gartner has observed that retailers are interested in these noteworthy features.

Dell's overall focus on midsize organizations aligns well with a UTM offering, and Dell's broad logistical capabilities assist with deployments involving multiple geographies.

Cautions

Surveyed vendors claimed that Dell SonicWALL is a brand they often replace. Gartner has observed that SonicWALL's acquisition by Dell has caused disruption for prospects that don't have an existing Dell relationship because of changes in the channel.

Gartner views Dell's efforts to move toward the enterprise markets as alienating the SMBs. The latest SonicOS releases — which have an increased number of features targeting the higher-end of midsize markets and enterprises, as well as a marketing focus on the SuperMassive Series — increase this perception.

Return to Top

Fortinet

Fortinet is a security vendor based in California. It offers 10 FortiGate UTM appliance models aimed at the small and midsize market. The security product portfolio, including tokens and host agents (FortiClient), is designed to appeal to VARs as the route to SMB sales. With two new models in 2012 (FortiGate-60D and FortiGate-100D), Fortinet continues to rely on its custom application-specific integrated circuit (ASIC) architecture to provide a high price/performance ratio. The fifth major version of Fortinet's OS brought a new set of features aimed at managing phones and tablets, trying to further expand the scope of UTM and to pressure competitors with advanced features.

Strengths

Fortinet continues to have the highest visibility of UTM providers among Gartner clients, and it is the company most frequently mentioned by the vendors we surveyed as a significant SMB competitive threat.

Because Fortinet designs and builds its own ASIC (FortiASIC), and uses little OEM software (compared with most UTM vendors), it provides a very aggressive price/performance proposition, which is important to SMBs that typically have limited security budgets.

Fortinet has a very large R&D team. Gartner views Fortinet as setting the cadence in the UTM market, driving its competitors to react.

Fortinet has a strong channel presence and provides local support in numerous countries.

Cautions

The frequent hardware and software updates make it harder to maintain a consistent level of expertise across Fortinet's widely distributed channel, which sometimes causes support issues.

Users often report a noticeably greater-than-documented impact on performance when using Web antivirus and URL filtering. Customers should take this into account and assess actual performance when doing competitive evaluations and product sizing.

Return to Top

gateprotect

Gateprotect is a German company, headquartered in Hamburg. It focuses on the SMB and MSSP markets, with nine models targeting companies composed of 10 to 10,000 users. Gateprotect emphasizes its management interface, and uses its proprietary solution (eGUI) to configure the UTM. It develops the core of its software (v.9), but relies on OEM partners that are specialized in their field for some security inspections. In 2012, gateprotect secured a new round of investment that was intended to accelerate its international expansion. It provides virtual images of its appliances and a centralized management tool for MSSPs.

Strengths

Gateprotect visual configuration emphasizes the ease of creation of security policies, focusing on saving time for end-user and technical support services.

Gateprotect maintains what Gartner views as a very competitive software release cycle to answer the needs of SMBs.

Cautions

Gateprotect has low visibility and rarely appears on Gartner client shortlists (although there is a slight increase in Latin America).

Increased efforts to expand beyond EMEA are still developing within the markets Gartner observes.

Return to Top

Huawei

Huawei is a China-based company with a primary focus on network infrastructure solutions. Its Unified Security Gateway (USG) product line includes seven models targeting SMBs. Huawei operates in 40 countries, and its revenue comes mainly from China, Africa and the Middle East. The company recently invested significantly in developing its channel to better address SMBs.

Strengths

Existing customers of Huawei's network solutions will get a good price for value and a shorter learning curve with its UTM devices.

The USG product line includes a comprehensive set of network options (such as 3G, xDSL and Wi-Fi).

Huawei is leveraging its hardware and software to deliver a very attractive price/performance proposition. Because the vendor has a very large security portfolio, other offerings (such as its secure wireless and tablet containers) can provide end-to-end security options for SMBs.

Cautions

Like most infrastructure vendors, Huawei's main focus remains network and larger enterprises or carriers. To address the SMB market, it has yet to shift its road map priorities toward core SMB market needs.

- Huawei has low visibility outside the Asia/Pacific region for its security products.
- Its investment in the UTM market is still recent, resulting in software that is lagging behind other solutions. However, Gartner views the Huawei UTM road map as very positive.

Return to Top

Juniper Networks

Juniper Networks is a network infrastructure vendor based in California. It has a broad portfolio that covers network and security solutions. Its UTM offering (SRX Series) includes seven models and relies on the Junos OS, which is the common platform for network and security appliances of Juniper's portfolio. The vendor has enhanced its Web filtering with reputation-based scoring, and made application control and visibility (AppSecure) available to the SRX Series.

Strengths

- The use of a common OS for security and network components reduces training costs and complexity for UTM buyers that have other Juniper products in place.
- Users often cite good performance as the top reason to select Juniper.

Cautions

- As an enterprise vendor, Juniper's road map and product strategy are not focused on the SMB market.
- Compared with its enterprise/carrier channel, Juniper has a limited dedicated channel focused on the UTM market.

Return to Top

Kerio

Kerio is a U.S. company based in California. It has been selling UTM devices since 2004. The Kerio Control Box appliance is offered in two models: as a software appliance (ISO file) or as a virtual appliance. Kerio has added URL filtering, IPv6 and IPsec VPN support.

Strengths

- Users report to Gartner ease of use and product quality as the main reasons for choosing Kerio.
- Vendor support is also highly rated.

Cautions

- Kerio generates a very low level of inquiry from Gartner clients, and it does not have an extensive specialized channel to address the UTM market.
- Kerio's default license is limited to five users. The competition frequently offers unlimited users out of the box.
- Kerio provides a limited set of features and appliance choices, compared with its competitors.

Return to Top

Netasq

Netasq, founded in 1998, is a French UTM vendor that was acquired by Cassidian CyberSecurity, a subsidiary of the EADS Group. The U Series, its product offering for SMBs, includes six appliances along with virtual appliances. Netasq developed its own intrusion prevention system (IPS) and application detection engine. In 2012, Netasq completely renewed the UTM product lines (the S models) with increased performance and IPsec hardware acceleration. It also changed its service offer — extending it for up to five years.

Strengths

- Netasq has a simple service offering with a low-cost bundle that's often cited as good for TCO.
- Integration of application versioning and vulnerability detection are often cited as criteria for choosing Netasq.
- Users consistently say that support from Netasq and channel partners is very good.

Cautions

- The majority of Netasq's customers are in EMEA, and the company has low visibility among

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

Gartner customers.

Gartner believes that the acquisition by Cassidian will lead to a shift in Netasq's focus from SMBs to larger enterprises and governments, potentially taking the development and capability focus away from SMB customers.

Return to Top

Sophos

Sophos is headquartered in Boston and in Oxford, U.K. It was initially providing endpoint security solutions, and in 2011, it integrated a UTM offer with the acquisition of the German-based company Astaro. The acquisition went smoothly and did not slow the pace of new releases. Sophos now offers eight UTM appliances to protect companies with 10 to 5,000 users. Version 9.1, the latest release of its OS, adds management features for Sophos endpoints. The vendor continues to offer free UTM software (software appliance or virtual appliance) for home usage, and it benefits from an active community that provides quick feedback on emerging needs.

Strengths

Sophos' ease of use consistently rates high among customers that Gartner has interviewed. Monitoring and configuration are well-integrated.

The interface contains general guidance on what each feature does. This recognizes the SMB reality that not all operators are firewall experts.

Sophos Remote Ethernet Device (Red) appliances are a competitive advantage when it comes to secure small branch offices.

New Wi-Fi features added in Version 9 make it easy to manage temporary guests with vouchers and time or quota limits.

Cautions

Customers report to Gartner that quality of service, VPN features and visibility into user activity need improvement.

Sophos' UTM device is present less often on Gartner clients' shortlists than other Leaders' UTM devices.

Sophos' application control features need to be expanded beyond the Web and better integrated with users in the firewall policy.

Return to Top

WatchGuard

WatchGuard, a U.S. company with headquarters based in Seattle, was one of the first to ship UTM platforms to the market. Its portfolio for SMBs is composed of 11 models (XTM 2, 3, 5 and 8 Series). WatchGuard's comprehensive offer also includes Web- and email-dedicated gateways. WatchGuard is a well-established UTM vendor with a strong focus on the SMB market. It has launched virtual appliances, and has extended its offer to MSSPs with a new program and a specific cloud-based solution for initial deployment (RapidDeploy).

Strengths

Customers often cite the low initial price as a reason to select WatchGuard.

WatchGuard has a strong and loyal channel presence in many countries.

Recent hardware and software upgrades have brought significant performance improvements.

An increased focus on MSSP needs reflects positively on the overall user experience.

Cautions

WatchGuard offers a large number of products and services that are often very similar. Channel partners and buyers tell Gartner this is confusing.

WatchGuard scored low as a significant UTM competitive threat by the vendors we surveyed.

Return to Top

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change.

As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Return to Top

Added

Huawei was added.

Dell acquired SonicWALL, which was in the previous Magic Quadrant, and the brand name has changed to Dell.

Return to Top

Dropped

Trustwave was not included because it sells UTM primarily as an element of a bundled managed service offering rather than as appliances.

Netgear was dropped because it focuses on a subset of the SMB market.

Return to Top

Inclusion and Exclusion Criteria

Inclusion Criteria

The following minimum requirements were used to determine which UTM companies met the criteria to be included in this Magic Quadrant under the following conditions:

They shipped UTM software and/or hardware products — targeted to midsize businesses — that included capabilities in the following feature areas at a minimum:

Network security (stateful firewall and intrusion prevention)

Web security gateway

Remote access for mobile employees (VPNs)

Email security

They regularly appeared on Gartner midsize client shortlists for final selection.

They achieved UTM product sales (not including maintenance or other service fees) of more than $7 million in 2012, and within a customer segment that's visible to Gartner. They also achieved this revenue on the basis of product sales, exclusive of managed security service (MSS) revenue.

Exclusion Criteria

There was insufficient information for assessment, and the companies didn't otherwise meet the inclusion criteria, or aren't yet actively shipping products for revenue.

Products aren't usually deployed as the primary Internet-facing firewall (for example, proxy servers and network IPS solutions).

Products are built around personal firewalls, host-based firewalls, host-based IPSs and WAFs — all of which are distinct from this market.

Solutions are delivered primarily as an integral part of MSSs, to the extent that product sales didn't reach the $7 million threshold.

Return to Top

Evaluation Criteria

Ability to Execute

Product/Service: Key features — such as ease of deployment and operation, console quality, price/performance, range of models, secondary product capabilities (for example, logging, integrated Wi-Fi support and remote access), and the ability to support multifunction deployments — are weighted heavily.

Overall Viability: This includes a vendor's overall financial health, prospects for continuing operations,

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

company history, and demonstrated commitment to the multifunction firewall and network security market. Growth of the customer base and revenue derived from sales are also considered. All vendors are required to disclose comparable market data, such as UTM revenue, competitive wins versus key competitors (which is compared with Gartner data on such competitions held by our clients), and devices in deployment. The number of UTM devices shipped isn't a key measure of execution. Instead, we consider the use of these solutions and the features deployed to protect the key business systems of Gartner midsize business clients.

Sales Execution/Pricing: This includes pricing, the number of deals, the installed base, and the strength of sales and distribution operations in the vendors. Presales and postsales support is evaluated. Pricing is compared in terms of a typical midsize business deployment, including the cost of all hardware, support, maintenance and installation. Low pricing won't guarantee high execution or client interest. Buyers want value more than they want bargains, although low price is often a factor in building shortlists. The TCO during a typical multifunction firewall life cycle (which is three to five years) is assessed, as is the pricing model for adding security safeguards. In addition, the cost of refreshing the products is evaluated, as is the cost of replacing a competing product without intolerable costs or interruptions.

Market Responsiveness and Track Record: This includes the ability to respond, change direction, be flexible, and achieve competitive success as opportunities develop, competitors act, customer needs evolve, and market dynamics change. This criterion also considers the provider's history of responsiveness.

Marketing Execution: This addresses awareness of the product in the market. We recognize companies that are consistently identified by our clients and often appear on their preliminary shortlists.

Customer Experience and Operations: These include management experience and track record, and the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycles. Also important are ease of use, overall throughput across different deployment scenarios, and how the firewall fares under attack conditions (see Table 1).

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	High
Market Responsiveness and Track Record	Standard
Marketing Execution	Low
Customer Experience	Standard
Operations	Standard

Source: Gartner (July 2013)

Completeness of Vision

Market Understanding and Marketing Strategy: These include providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" road map and an overall understanding and commitment to the security market (specifically the SMB network security market). Gartner makes this assessment subjectively by several means, including via interactions with vendors in briefings and via feedback from Gartner clients on information they receive concerning road maps Incumbent vendor market performance is reviewed yearly against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors can't merely state an aggressive future goal. They must enact a plan, show that they're following it and modify the plan as they forecast how market directions will change.

Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detection events and deployment efficacy. Building loyalty through credibility with a full-time midsize business security and research staff demonstrates the ability to assess the next generation of requirements.

Offering (Product) Strategy: The emphasis is on the vendor's product road map, current features, leading-edge capabilities, virtualization and performance. The quality of the security research labs behind the security features is considered. Credible, independent third-party certifications, such as Common Criteria, are included. Integrating with other security components is also weighted, as well as product integration with other IT systems. As threats change and become more targeted and complex, we weight vendors highly if they have road maps to move beyond purely signature-based, deep packet inspection techniques. In addition, we weight vendors that are looking to add cloud-based services to their offerings.

Business Model: This includes the process and success rate of developing new features and innovation, along with R&D spending.

Innovation: This includes product innovation (such as R&D) and quality differentiators (such as performance, virtualization, integration with other security products, a management interface and clarity of reporting).

Geographic Strategy: This includes the ability and commitment to service geographies.

The more a product mirrors the workflow of the midsize business operations scenario, the better the vision. Products that are counterintuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and beating competitors to market with new features are very important components of a good vision (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Standard
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Low

Source: Gartner (July 2013)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors at the forefront of making and selling UTM products that are built for midsize business requirements. The requirements necessary for leadership include a wide range of models to cover midsize business use cases, support for multiple features, and a management and reporting capability that's designed for ease of use. Vendors in this quadrant lead the market in offering new safeguarding features, and in enabling customers to deploy them inexpensively without significantly affecting the end-user experience or increasing staffing burdens. These vendors also have a good track record of avoiding vulnerabilities in their security products. Common characteristics include reliability, consistent throughput, and products that are intuitive to manage and administer.

- Return to Top

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they aren't leading with features. Many Challengers have other successful security products in the midsize world and are counting on the client relationship or channel strength, rather than the product, to win deals. Challengers' products are often well-priced, and because of their strength in execution, these vendors can offer economic security product bundles that others can't. Many Challengers hold themselves back from becoming Leaders because they're obligated to set security or firewall products as a lower priority in their overall product sets.

Return to Top

Visionaries

Visionaries have the right designs and features for the midsize business, but lack the sales base, strategy or financial means to compete globally with Leaders and Challengers. Most Visionaries' products have good security capabilities, but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and switch vendors, if required. Where security technology is a competitive element for an enterprise, Visionaries are good shortlist candidates.

Return to Top

Niche Players

Most vendors in the Niche Players quadrant are enterprise-centric or small-office-centric in their approach to UTM devices for SMBs. Some Niche Players focus on specific vertical industries or geographies. If SMBs are already clients of these vendors for other products, then Niche Players can be shortlisted.

Return to Top

Context

SMBs have significantly different network security requirements from those of large enterprises, due to different threat environments and different business pressures. Although the branch offices of some larger enterprises have requirements that are similar to midsize businesses, this is not always the case. The UTM market consists of a wide range of suppliers that meet the common core security requirements of SMBs, but businesses need to make their decisions by mapping their threat and deployment patterns to optimal offerings.

Return to Top

Market Overview

UTM appliances are used by midsize businesses to meet the requirements for secure Internet connectivity. For many small businesses, those requirements are often driven by regulatory demands (such as the PCI Data Security Standard), driving low to medium levels of security. Gartner sees very different demands from the enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls"), which generally require more-complex network security features, and show very different selection criteria.

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute that is used most often is the number of employees. Small businesses usually have fewer than 100 employees, while midsize businesses are usually defined as companies with fewer than 1,000 employees. The secondary attribute that is used most often is annual revenue. Small businesses are usually defined as those with less than $50 million in annual revenue, while midsize businesses are defined as those with less than $1 billion in annual revenue. Typically, 80% of the companies that Gartner analysts speak with have between 100 and 999 employees, and revenue between $100 million and $500 million.

The primary characteristic of midsize companies is that they are organizations with resource-constrained IT departments. They have a relative constraint in capital expenditures, operational budgets, number of IT staffers and depth of IT skills when compared with large enterprises. In keeping with this, UTM appliances are frequently used across midsize businesses as a low-cost way of meeting their network security requirements. Midsize businesses look at security differently, and show different buying behaviors compared with larger enterprises. The primary areas of difference are the following (in order of importance):

- A limited or nonexistent skilled security staff drives the need for ease of installation, configuration and use of channel-managed solutions.
- Less complex use of the Internet results in lower demand for high-end security features, such as application-level security and custom intrusion prevention filters.
- Limited security budgets drive acquisition costs to represent more than 60% of the overall decision weighting.
- Small businesses often perceive that they are not visible to attackers and, therefore, don't require as much security. However, financially motivated attackers have targeted small businesses, and the publicity over successful attacks has changed these businesses' perception.

The branch offices of larger companies have very different network security demands from midsize businesses, even though they may be of similar size. Gartner views branch offices' firewalls as extensions of the central firewall strategy (see "Bring Branch Office Network Security Up to the Enterprise Standard"). This drives large enterprises to often use low-end enterprise products at their branch offices to ensure interoperability, and to take advantage of economies of scale in getting larger discounts from their firewall vendors. This is not true in all cases, but in general, it is one of the major reasons why firewall vendors that sell successfully to the enterprise and SMB markets tend to have separate product lines for each market. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market.

Small businesses with fewer than 100 employees have even more budgetary pressures and even fewer security pressures. Most security procurement decisions are driven by nontechnical factors and rarely feature competitive comparisons. For these reasons, this Magic Quadrant focuses on the UTM products used by midsize businesses, as defined above.

Return to Top

About Gartner | Careers | Newsroom | Policies | Site Index | IT Glossary | Contact Gartner

FORTINET®

Certificate of Authorized Reseller

Tender/Project: Bidding For The Procurement Of One (1) Lot Network Security Device [ITB No. NSD 2014-003-IT]·

Company: Philippine Health Insurance Corporation

Fortinet, Inc. hereby recognizes that: Trends & Technologies, Inc.;

Having its registered place of business at: 6th Floor Trafalgar Plaza, No. 105 HV dela Csta Street, Salcedo Village, Makati City, 1227, Philippines; is a Certified Gold FortiPartner and is currently authorized to bid, sell, and support Fortinet products which include proposed Fortigate Firewall FG-60D.

Notwithstanding anything to the contrary herein, authorized FortiPartners do not represent Fortinet and can not make statements that are binding on behalf of Fortinet.

This certification is being issued upon the request of Philippine Health Insurance Corporation.

Sincerely,

Jeff Castillo
Country Manager, Philippines
Fortinet International, Inc

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

FORTINET®

CERTIFICATE OF AUTHORIZED SUPPORT SERVICES PROVIDER

Project Name: Bidding For The Procurement of One (1) Lot Network Security Device [ITB No. NSD 2014-003-IT]

Company: Philippine Health Insurance Corporation

Fortinet, Inc. hereby recognizes that: Trends & Technologies, Inc.

Having its registered place of business at: 6th Floor Trafalgar Plaza, No. 105 HV dela Csta Street, Salcedo Village, Makati City, 1227, Philippines;

Is currently an authorized GOLD FortiPARTNER and is currently authorized throughout the Philippines to provide support services for Fortinet Products, which include proposed Fortigate Firewall FG60D.

This certification is issued upon the request of Philippine Health Insurance Corporation.

Should you have questions, please do not hesitate to contact the undersigned.

Sincerely,

Jeff Castillo
Country Manager, Philippines
Fortinet International, Inc

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

Trends & Technologies, Inc.

Project Management Team

for Philippine Health Insurance Corporation

Bidding for the Procurement of ONE (1) LOT NETWORK SECURITY DEVICE

ITB No. NSD 2014-003-IT

Project/Team Leader: Maynard Cefre (Project Manager)

Assistant Team Leader: Anthony N. Pagalanan
(Security Implementation Engineer and
Training Instructor)

Team Members:

Jasper Franco
(Customer Care Engineer)

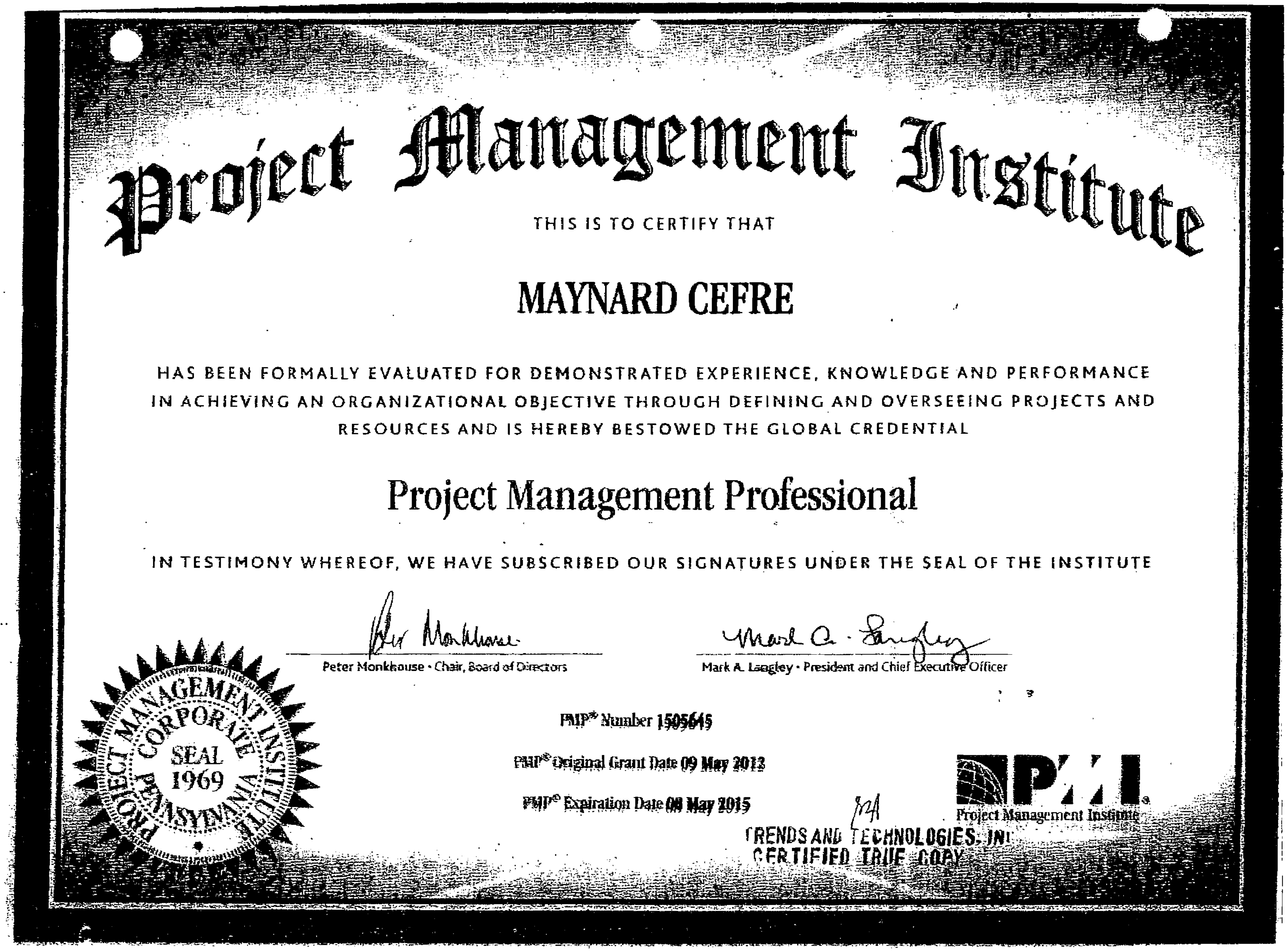
Kleffens Quiambao
(Customer Care Engineer)

Raquel Rellebo
(Design Engineer)

Shirley Z. Amata
(Account Manager)

Prepared by:

Shirley Z. Amata
Account Manager
Financial Services Group
July 11, 2014



Project Management Institute

THIS IS TO CERTIFY THAT

MAYNARD CEFRE

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL

Project Management Professional

IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE

Peter Monkhouse

Peter Monkhouse • Chair, Board of Directors

Mark A. Langley

Mark A. Langley • President and Chief Executive Officer

PROJECT MANAGEMENT INSTITUTE
CORPORATE
SEAL
1969
PENNSYLVANIA

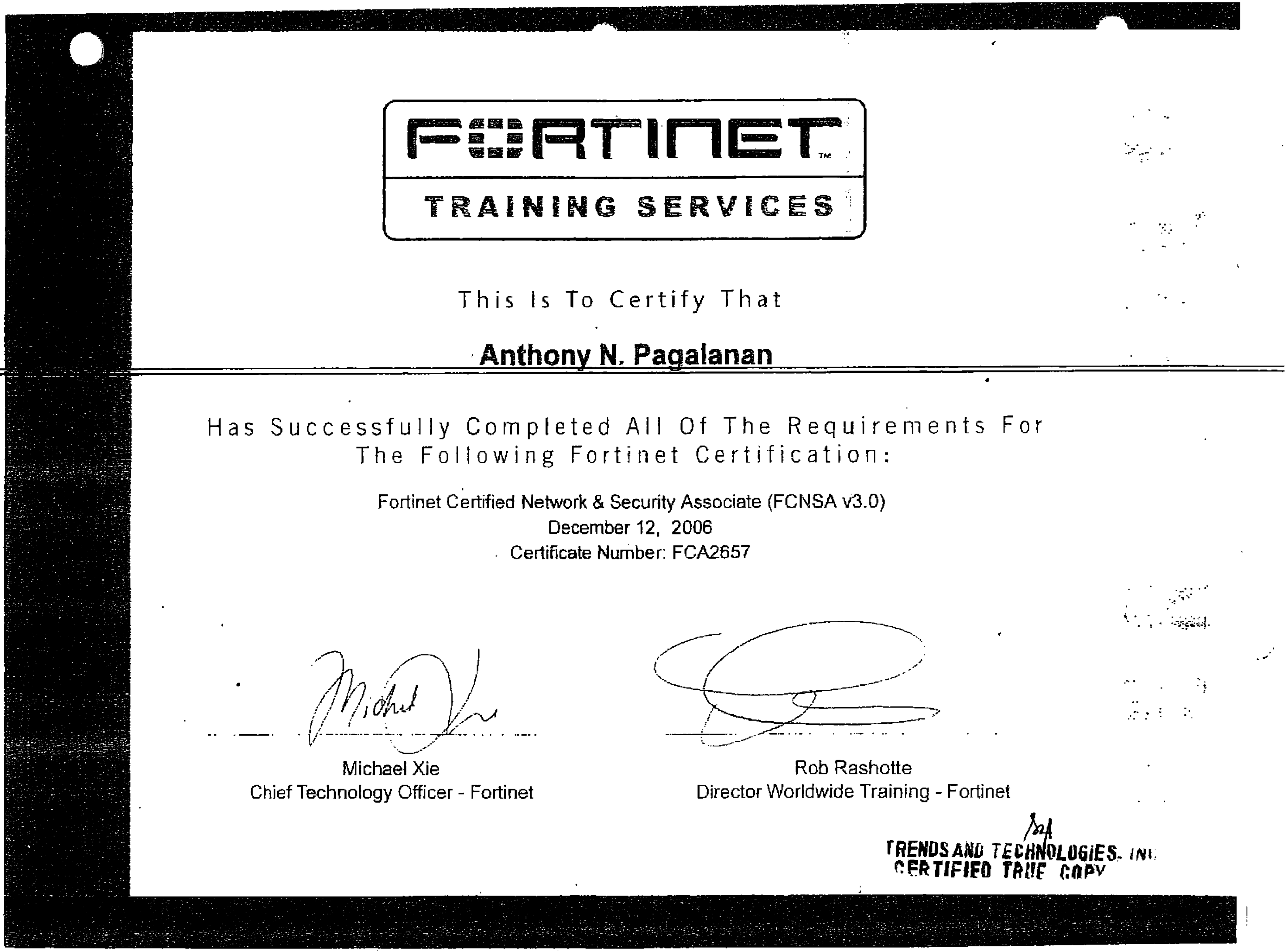
PMP® Number 1505645

PMP® Original Grant Date 09 May 2012

PMP® Expiration Date 08 May 2015

PMI®
Project Management Institute

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY



FORTINET™

TRAINING SERVICES

This Is To Certify That

Anthony N. Pagalanan

Has Successfully Completed All Of The Requirements For The Following Fortinet Certification:

Fortinet Certified Network & Security Associate (FCNSA v3.0)
December 12, 2006
Certificate Number: FCA2657

Michael

Michael Xie
Chief Technology Officer - Fortinet

Rob Rashotte
Director Worldwide Training - Fortinet

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

FORTINET®

TRAINING SERVICES

This Is To Certify That

Jasper Franco

Has successfully completed all of the requirements for the following Fortinet Certification:

Fortinet Certified Network Security Administrator

Date: 10/4/2013

Certification ID: FCNSA-2013-16046

Michael Xie
Chief Technology Officer - Fortinet

Michael Anderson
Vice President, Global Services and Support - Fortinet

TRENDS AND TECHNOLOGIES, INC
CERTIFIED TRUE COPY

FORTINET®

TRAINING SERVICES

This Is To Certify That

KLEFFENS A. QUIAMBAO II

Has successfully completed all of the requirements for the following Fortinet Certification:

Fortinet Certified Network Security Professional

Date: 11/28/2013

Certification ID:FCNSP-2013-16718

Michael Xie
Chief Technology Officer - Fortinet

Michael Anderson
Vice President, Global Services and Support - Fortinet

TRENDS AND TECHNOLOGIES, IN
CERTIFIED TRUE COPY

FORTINET™

TRAINING & CERTIFICATION

This Is To Certify That

Raquel Rellebo

Has Successfully Completed All Of The Requirements For The Following Fortinet Certification:

Fortinet Certified Network Security Professional (V4.x)

Date: January 28, 2011

Certification ID: FCNSP8217

Michael Xie
Chief Technology Officer - Fortinet

Michael Anderson
Vice President, Global Services and Support - Fortinet

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

I. PERSONAL INFORMATION

NAME: CEFRE (LAST NAME) MAYNARD (FIRST NAME) DE GUZMAN (MIDDLE NAME)

POSITION: Project Director

JOB GRADE:

DATE HIRED: FEBRUARY 08, 2002

AFFILIATE COMPANY: TTI

DEPARTMENT: Project Management Office

SECTION: PROFESSIONAL SERVICES GROUP

CITY ADDRESS: 2363 Raymundo St. Sta. Ana, Manila

HOME PHONE NO.: 02-561-8373

MOBILE NO.: 0917-852-0888

PROV'L ADDRESS:

TELEPHONE NO.:

DATE OF BIRTH: 23 MAY 1977

PLACE OF BIRTH: Manila

CIVIL STATUS: SINGLE

SSS NUMBER: 33-5503647-0

TIN NO.: 911-678-423

BLOOD TYPE: O

PASSPORT NO.: WB3725394

PLACE OF ISSUE: DFA Manila

DATE OF ISSUE: 24 SEPT 2011

VALID UNTIL: 23 SEPT 2016

CTC NO.:

PLACE OF ISSUE:

DATE OF ISSUE

DRIVER'S LICENSE NO.: N03-01-320037

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY: Purita G Cefre

RELATIONSHIP: Mother

ADDRESS: 2363 Raymundo St. Sta. Ana, Manila

TELEPHONE NO.: 02-561-8373

NAME OF DEPENDENTS	DATE OF BIRTH	RELATIONSHIP

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1	Jan 2013 to Present	Trends & Technologies, Inc.	Project Director	Direct, plan and lead a team of Project Managers for the successful performance of different projects for the company Review project status of Project Managers and modifies plans and schedules as required
2	Sept 2004 to Dec 2012	Trends & Technologies, Inc.	Project Manager	Project Management and Implementation of various ICT projects
3	Apr 2003 to Sept 2004	Trends & Technologies, Inc.	Systems Engineer	Pre-sales engineer for wireless communication systems
4	Feb 2002 to Apr 2003	Technologies Specialist, Inc.	Systems Engineer	Pre-sales engineer for access devices and wireless communication systems design.
5	Jun 2000 to Feb 2002	Universal Telecommunications Services, Inc. (Mobilcom)	Engineering & Operations Supervisor	Supervision of operations of the Metro Manila Switching and BTS Network of Mobilcom.
6	Feb 1998 to Jun 2000	Universal Telecommunications Services, Inc. (Mobilcom)	Switch Engineer	Part of the Switching Operations of MPT1327 for Metro Manila

III. EDUCATIONAL BACKGROUND

	DATES	INSTITUTION	DEGREE
ELEMENTARY	April 1989	Justo Lukban Elementary School	Primary Education
HIGH SCHOOL	June 1989 to March 1993	Manila Science High School	Secondary Education
COLLEGE	June 1993 to April 1998	Pamantasan ng Lungsod ng Maynila	BSECE

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS

ITEM	COURSE NAME	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	Veraz IG4K	Trends & Technologies	Singapore	November 2006
2.				

B. FOREIGN SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.				
2.				

C. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	Nokia Actionet Switching & Base Station Operations	Nokia / UTSI	Cebu City	March 06, 98 - April 04, 98
2.	Nokia DMR2000 Microwave Installation & Operations	Nokia / UTSI	Cebu City	July 1999
3.	Spectrum Analyzer Operations	Advantest / UTSI	Makati	
4.	Communications Service Monitor Operations	Marconi / UTSI	Makati	
5.	Lucent Definity G3SI Basic Administrator's Course	Alliance Technologies / UTSI	Makati	February 1999
6.	People Handling Skills	Jebssen / UTSI	Pasay City	September 2001
7.	Cisco WLAN	Cisco / TSI	Makati	September 2002
8.	Project Management Workshop	UAP / TTI	Pasig	April 2003
9.	Project Management Essentials	Global Knowledge / TTI	Makati	February 2007
10.	CAPM Certification Workshop	PM Partners / TTI	Makati	April 2008
11.	PMP Certification Workshop	Element K / TTI	Makati	April 2012
12.	Managing for Results Workshop	Trends Net / TTI	Makati	June 29, July 6, & July 13, 2013

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

D. CERTIFICATIONS / PROFESSIONAL LICENSE

ITEM	DESIGNATION	COMPANY/SPONSOR	EXAMINATION	INCLUSIVE DATES
1.	Project Management Professional (PMP) #1505645	Project Management Institute	09 May 2012	May 9, 2012 to May 8, 2015
2.	Certified Associate in Project Management (CAPM) #1333020	Project Management Institute	04 May 2010	May 4, 2010 to May 3, 2015
3.	Registered Electronics and Communications Engineer ECE #18799	Professional Regulations Commission	09 April 1999	

TRENDS AND TECHNOLOGIES, INC
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

I. PERSONAL INFORMATION

NAME: PAGALANAN (LAST NAME) ANTHONY (FIRST NAME) NAVARRO (MIDDLE NAME)

POSITION: TECHNICAL SUPPORT ENGINEER
JOB GRADE:
DATE HIRED: OCT 21, 2004

AFFILIATE COMPANY: TTI
DEPARTMENT: TECHNICAL SERVICES
SECTION:

CITY ADDRESS: 107 UPO ST. BRGY.NAPICO LIFEHOMES SUBD., PASIG CITY, METRO MANILA 1609

HOME PHONE NO.:
MOBILE NO.: +639178581659

PROV'L ADDRESS: 9-184 ALMEDA ST. IBABA DEL NORTE PAETE, LAGUNA 4016

TELEPHONE NO.:

DATE OF BIRTH: JULY 9, 1979
PLACE OF BIRTH: PAETE,LAGUNA
CIVIL STATUS: MARRIED

SSS NUMBER:
TIN NO.:
BLOOD TYPE: O

PASSPORT NO.:
PLACE OF ISSUE:
DATE OF ISSUE:
VALID UNTIL:

CTC NO.:
PLACE OF ISSUE:
DATE OF ISSUE
DRIVER'S LICENSE NO.:

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY: AMELITA A. PAGALANAN
RELATIONSHIP: SPOUSE
ADDRESS: 107 UPO ST. BRGY.NAPICO LIFEHOMES SUBD., PASIG CITY, METRO MANILA 1609
TELEPHONE NO.: +639172730331, +639297117633

NAME OF DEPENDENTS	DATE OF BIRTH	RELATIONSHIP
ARON MIGUEL A. PAGALANAN	NOV. 19, 2004	SON

MA

TRENDS AND TECHNOLOGIES. INC
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1	2001 - 2004	WOLFPAC MOBILE INC.	PROGRAMMER	DEVELOP MOBILE APPLICATIONS
2				
3.				
4				
5				

III. EDUCATIONAL BACKGROUND

	DATES	INSTITUTION	DEGREE
ELEMENTARY			
HIGH SCHOOL			
COLLEGE	1999	DLSU-DASMARINAS	BS COMSCI

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS

ITEM	COURSE NAME	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	F5 BIG-IP LTM ESSENTIALS AND BIG-IP LTM ADVANCE TOPICS V9.X	TTI	SINGAPORE	JULY 22 - 25, 2008
2.	PACKETEER SPECIALIST COURSE - LEVEL 1 & 2	TTI	SINGAPORE	FEB. 23-27, 2009
3.				

B. FOREIGN SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.				
2.				
3.				
4.				
5.				

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

C. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	COMCLARK - SME 100-101 TECHNICAL TRAINING	TTI		NOV 23-25, 2005
2.	MCAFEE INTRUSHIELD ESSENTIALS	TTI		JAN.13-16, 2009
3.	MCAFEE FOUNDSTONE ENTERPRISE ADMINISTRATION	TTI		MAR. 2 - 3, 2009
4.	MCAFEE EPOLICY ORCHESTRATOR ADMINISTRATION	TTI		MAR. 4 - 6, 2009
5.	F5 BOOTCAMP 1A: CORE FUNDAMENTALS (LTM, GTM, IRULES) AND BOOTCAMP 2A: ACTIVE- ACTIVE DATA CENTRE SOLUTION WORKSHOP	TTI	*MAKATI*	SEPTEMBER 2 TO 6, 2013

D. CERTIFICATIONS

ITEM	DESIGNATION	COMPANY/SPONSOR	EXAMINATION	INCLUSIVE DATES
1.	CA ETRUST IDENTITY AND ACCESS MANAGEMENT BASIC FOUNDATIONS	TTI		NOV. 27, 2006
2.	FORTINET CERTIFIED NETWORK SECURITY ASSOCIATE (FCNSA)	TTI		DEC. 12, 2006
3.	F5 CERTIFIED PRODUCT CONSULTANT	TTI	F5 BIG-IP V9 LOCAL TRAFFIC MANAGEMENT EXAM	OCT. 3, 2008
4.	BLUE COAT PACKETSHAPER CERTIFIED SPECIALIST	TTI	PACKETSHAPER CERTIFIED SPECIALIST EXAM	DEC. 1, 2009
5.	FORTINET CERTIFIED NETWORK SECURITY PROFESSIONAL	TTI		DECEMBER 17, 2010
6.	F5 PRODUCT CONSULTANT- ASM	TTI	(BIG-IP ASM V10X) APPLICATION DELIVERY NETWORK TEST	JULY 13, 2012
7.	F5 CERTIFIED BIG IP ADMINISTRATOR	TTI		OCTOBER 25, 2013

TRENDS AND TECHNOLOGIES, INC
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

I. PERSONAL INFORMATION

NAME:	FRANCO (LAST NAME)	JASPER (FIRST NAME)	YAPE (MIDDLE NAME)

POSITION:	CADET ENGR.	JOB GRADE:	LEVEL 1	DATE HIRED:	SEPTEMBER 6, 2010
AFFILIATE COMPANY	TTI	DEPARTMENT:	CUSTOMER CARE GROUP	SECTION:	CCG – ON SITE

CITY ADDRESS:	2942 F. MANALO ST. PUNTA STA. ANA MANILA		
HOME PHONE NO.:	N/A	MOBILE NO.:	0917-5763547 / 0915-6831525
PROV'L ADDRESS:	737 RIZAL ST. MALAPIT, SAN ISIDRO, NUEVA ECIJA		
TELEPHONE NO.:	SAME AS ABOVE		

DATE OF BIRTH:	OCTOBER 23, 1987	PLACE OF BIRTH:	SAN ISIDRO, NUEVA ECIJA	CIVIL STATUS:	SINGLE
SSS NUMBER:	33-9829233-6	TIN NO.:	242-929-860	BLOOD TYPE:	

PASSPORT NO.:	N/A	CTC NO.:	N/A
PLACE OF ISSUE:	N/A	PLACE OF ISSUE:	N/A
DATE OF ISSUE:	N/A	DATE OF ISSUE	N/A
VALID UNTIL:	N/A	DRIVER'S LICENSE NO.:	N/A

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY:	GERARDO FRANCO
RELATIONSHIP:	FATHER
ADDRESS:	737 RIZAL ST. MALAPIT, SAN ISIDRO, NUEVA ECIJA
TELEPHONE NO.:	09179369576

NAME OF DEPENDENTS	DATE OF BIRTH	RELATIONSHIP

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1	Sept. 2006	Jollibee	Service Crew	Serve Customers
2	Sept. 2007	Boni Vibes Internet Cafe	Cashier/Technician	Assist and Support Customers
3	July 2009	Knowledge and System Integration Corp.	IT Specialist	Support Clients through Helpdesk, Networking and Web Development
4				
5				
6				

III. EDUCATIONAL BACKGROUND

	DATES	INSTITUTION	DEGREE
ELEMENTARY	1994-2000	Malapit East Elementary School	Graduate
HIGH SCHOOL	2000-2004	General de Jesus College	Graduate
COLLEGE	2004-2009	Rizal Technological University	B.S. Computer Engineering
POST GRADUATE STUDIES			

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS

ITEM	COURSE NAME	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	Fortinet Administration and Content Inspection and Basic VPN Access	TTI	Kuala Lumpur, Malaysia	March 11-12, 2013
2.	Fortinet Secured Network Deployment and VPNs	TTI	Kuala Lumpur, Malaysia	March 13-15, 2013
3.	Blue Coat Certified PacketShaper Administrator and BlueCoat Certified PacketShaper Professional	TTI	Singapore	May 27 -31, 2013
4.	Checkpoint Security Administrator and Expert Training	TTI	Singapore	February 11 to 19, 2014

B. FOREIGN SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.				
2.				
3.				
4.				
5.				

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

C. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	CCNA Boot Camp Cisco 1-4	Packetlink	Taguig City	June 2010
2.	Window Server	RTU	Mandaluyong City	February 2009
3.	My SQL	RTU	Mandaluyong City	February 2009
4.	3D Blender Training	RTU	Mandaluyong City	March 2009
5.	Advance PC Troubleshooting	RTU	Mandaluyong City	February 2009
6.	Riverbed Steelhead Appliance Deployment & Management (SADM) training	TTI	Makati City	July 16 to 19, 2013

D. CERTIFICATIONS

ITEM	DESIGNATION	COMPANY/SPONSOR	EXAMINATION	INCLUSIVE DATES
1.	Cisco Certified Network Associate	TTI	640-802	July 29, 2011
2.	CCNA – Security	TTI	Implementing Cisco IOS Network Security	June 1, 2012
3.	CCNP- Security	TTI	• Securing Networks with Cisco Routers & Switches	July 16, 2012
			• Implementing Cisco Intrusion Prevention System (IPS) v7.0	June 20, 2012
			• Deploying Cisco ASA Firewall Features	January 18, 2013
			• Deploying Cisco ASA VPN Solutions	March 21, 2013
4.	Fortinet Certified Network Security Administrator	. TTI	FCNSA	October 4, 2013

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

I. PERSONAL INFORMATION

NAME:

QUIAMBAO	KLEFFENS II	AGBULOS
(LAST NAME)	(FIRST NAME)	(MIDDLE NAME)

POSITION: CADET ENGINEER
JOB GRADE:
DATE HIRED: NOVEMBER 04, 2010
AFFILIATE COMPANY: TTI
DEPARTMENT: CUSTOMER CARE SERVICE
SECTION:

CITY ADDRESS: 5363 BEN HARRISON ST. PIO DEL PILAR MAKATI CITY
HOME PHONE NO.:
MOBILE NO.: 0917-8092850
0927-6684784
PROV'L ADDRESS: PALLMALL ST. LEONCIA VILLAGE ANGELES CITY
TELEPHONE NO.:

DATE OF BIRTH: MAY 11, 1981
PLACE OF BIRTH: ANGELES CITY
CIVIL STATUS: MARRIED
SSS NUMBER: 0221140626
TIN NO.: 000229087981
BLOOD TYPE: O

PASSPORT NO.:
PLACE OF ISSUE:
DATE OF ISSUE:
VALID UNTIL:

CTC NO.:
PLACE OF ISSUE:
DATE OF ISSUE
DRIVER'S LICENSE NO.: C10-03-0006211

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY: JOANNE M. QUIAMBAO
RELATIONSHIP: SPOUSE
ADDRESS: BAGONG POOK LEMERY, BATANGAS
TELEPHONE NO.: 09151157579

NAME OF DEPENDENTS	DATE OF BIRTH	RELATIONSHIP
KYLA KHLOE M. QUIAMBAO	12/23/2007	CHILD
JOANNE M. QUIAMBAO	06/03/1981	SPOUSE
KLEFFENS C. QUIAMBAO	08/01/1947	PARENT

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1	JUNE 22, 2009 – NOV 01, 2010	WEST CONTACT SERVICES INC.	CUSTOMER SERVICE REPRESENTATIVE	TAKE IN CUSTOMER CALLS AND PROCESS CREDIT CARD APPLICATIONS
2	MARCH 19, 2007 – JANUARY 30, 2009	ETELECARE GLOBAL SOLUTIONS	SALES SERVICE REPRESENTATIVE	HANDLES CUSTOMER CALLS IN A TIMELY MANNER, PROVIDE SOLUTIONS TO CUSTOMER CONCERN AND MEET EXPECTED SALES QUOTA.
3	JULY 06, 2005 – JULY 05, 2006	YONYU PLASTIC CO LTD.	GENERAL WORKER	WORK AS PRINTING MACHINE OPERATOR, DO QUALITY CHECKING AND FACTORY WORK.

III. EDUCATIONAL BACKGROUND

	DATES	INSTITUTION	DEGREE
ELEMENTARY	1998 - 1994	LEONCIA VILLAGE ELEMENTARY SCHOOL	
HIGH SCHOOL	1994 - 1998	CHEVALIER SCHOOL	
COLLEGE	1998 - 2003	AMA COMPUTER COLLEGE	BS COMPUTER ENGINEER
POST GRADUATE STUDIES			

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS

ITEM	COURSE NAME	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	FORTINET TECHNICAL BOOT CAMP	TTI	KOTA KINABALU, MALAYSIA	OCTOBER 7 TO 11, 2013
2.				
3.				
4.				
5.				

B. FOREIGN SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.				
2.				
3.				
4.				
5.				

TRENDS AND TECHNOLOGIES. INC.
CERTIFIED TRUE COPY

C. LOCAL TRAININGS/SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	NETWORKING LOCAL ARE NETWORKING	AMA COMPUTER COLLEGE	TESDA, TAGUIG	FEB. 15, 2003
2.	INDUTRIAL AUTOMATION	AMA COMPUTER COLLEGE	TESDA, TAGUIG	MARCH14, 2003
3.	PC TROUBLESHOOTING	AMA COMPUTER COLLEGE	AMA COMPUTER COLLEGE, MAKATI	MARCH 15, 2003
4.	CHECK POINT SECURITY ADMINISTRATOR	TTI	MANILA	AUGUST 28- 31, 2012
5.	CHECK POINT SECURITY EXPERT	TTI	MANILA	SEPTEMBER 3- 5, 2012

D. CERTIFICATIONS

ITEM	DESIGNATION	COMPANY/SPONSOR	EXAMINATION	INCLUSIVE DATES
1.	CISCO CERTIFIED NETWORK ASSOCIATE	TTI	640-802	MARCH 8, 2012
2.	FORTINET CERTIFIED NETWORK AND SECURITY ASSOSCIATE	TTI	FCNSA EXAM	AUGUST 24, 2012
3.	FORTINET CERTIFIED NETWORK AND SECURITY PROFESSIONAL	TTI	FCNSP EXAM	FEBRUARY 05, 2013
4.	CHECKPOINT CERTIFIED SECURITY ADMINISTRATOR	TTI	CHECKPOINT CERTIFIED SECURITY ADMINISTRATOR EXAM	APRIL 11, 2013
5.	CCNA- SECURITY	TTI	CISCO CERTIFIED NETWORK ASSOCIATE- SECURITY	NOVEMBER 28, 2013
6.	FORTINET CERTIFIED NETWORK SECURITY PROFESSIONAL	TTI	FCNSP EXAM	
7.	CISCO IOS SECURITY SPECIALIST	TTI		APRIL 15, 2014 TO APRIL 15, 2016

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

I. PERSONAL INFORMATION

NAME:	RELLEBO (LAST NAME)	RAQUEL (FIRST NAME)	QUILILAN (MIDDLE NAME)

POSITION:	CADET ENGINEER	JOB GRADE:		DATE HIRED:	FEB. 22, 2010
AFFILIATE COMPANY	TRENDS & TECHNOLOGIES, INC	DEPARTMENT:	DESIGN AND ENGINEERING GROUP	SECTION:	DE – SOS / CA

CITY ADDRESS:	23 AVELINO, JOAQUIN, SR. ST. BALANGKAS, VALENZUELA CITY		
HOME PHONE NO.:	(02) 443-1519	MOBILE NO.:	0917-5913212
PROV'L ADDRESS:	N.A.		
TELEPHONE NO.:	N.A.		

DATE OF BIRTH:	NOV. 27, 1987	PLACE OF BIRTH:	VALENZUELA CITY	CIVIL STATUS:	SINGLE
SSS NUMBER:		TIN NO.:		BLOOD TYPE:	A

PASSPORT NO.:		CTC NO.:	
PLACE OF ISSUE:		PLACE OF ISSUE:	
DATE OF ISSUE:		DATE OF ISSUE	
VALID UNTIL:		DRIVER'S LICENSE NO.:	

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY: ROGELIO S. RELLEBO

RELATIONSHIP: FATHER

ADDRESS: 23 AVELINO, JOAQUIN, SR. ST., BALANGKAS,VALENZUELA CITY

TELEPHONE NO.: (02) 443-1519

NAME OF DEPENDENTS	DATE OF BIRTH	RELATIONSHIP
ROGELIO S. RELLEBO	DEC. 24, 1954	FATHER
CRISTITA Q. RELLEBO	MARCH 2, 1949	MOTHER

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

COMPANY CONFIDENTIAL

TRENDS AND TECHNOLOGIES HOLDING, INC.

II. WORK EXPERIENCES

ITEM	INCLUSIVE DATES	COMPANY NAME	POSITION	DESCRIPTION OF FUNCTION
1				
2				
3				

III. EDUCATIONAL BACKGROUND

	DATES	INSTITUTION	DEGREE
ELEMENTARY	1994-2000	PIO VALENZUELA ELEMENTARY SCHOOL	
HIGH SCHOOL	2000-2004	POLO NATIONAL HIGH SCHOOL	
COLLEGE	2004-2009	POLYTECHNIC UNIVERSITY OF THE PHILIPPINES	B.S. ELECTRONICS AND COMMUNICATIONS ENGINEERING
POST GRADUATE STUDIES			

IV. SEMINARS AND TRAININGS ATTENDED

A. FOREIGN TRAININGS

ITEM	COURSE NAME	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.				
2.				
3.				
4.				
5.				

B. FOREIGN SEMINARS

ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	RIVERBED APJ PARTNER CONFERENCE	TTI ; RIVERBED	PHUKET, THAILAND	MARCH 5-8, 2012
2.	FORTINET TECHNICAL BOOT CAMP	TTI	KOTA KINABALU, MALAYSIA	OCTOBER 7 TO 11, 2013
3.				
4.				
5.				

TRENDS AND TECHNOLOGIES, INC
CERTIFIED TRUE COPY

TRENDS AND TECHNOLOGIES HOLDING, INC.

C. LOCAL TRAININGS/SEMINARS

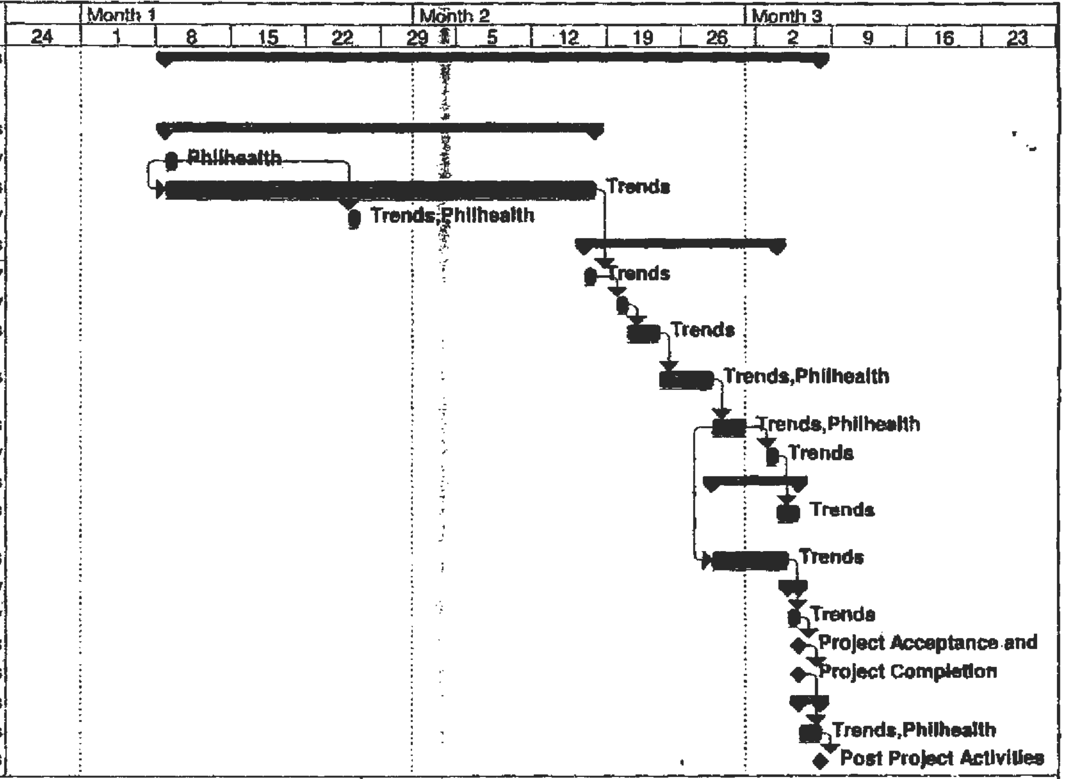
ITEM	SEMINAR TITLE	COMPANY/SPONSOR	VENUE	INCLUSIVE DATES
1.	301 - FORTIGATE MULTI-THREAT SECURITY SYSTEMS II (SECURED NETWORK DEPLOYMENT AND VIRTUAL PRIVATE NETWORKS) AND 303 – DIAGNOSTICS AND TROUBLESHOOTING	TTI	MANILA	AUGUST 16-20, 2010
2.	BLUE COAT CERTIFIED PROXYSG ADMINISTRATOR AND PROFESSIONAL	TTI	MANILA	OCTOBER 26-30, 2010
3.	MCAFEE BOOTCAMP		MANILA	2011
4.	RIVERBED STEELHEAD APPLIANCE DEPLOYMENT & MANAGEMENT (SADM)	TTI	MANILA	JULY 16 TO 19, 2013
5.	F5 BOOTCAMP 1A: CORE FUNDAMENTALS (LTM, GTM, IRULES) AND BOOTCAMP 2A: ACTIVE ACTIVE DATA CENTRE SOLUTION WORKSHOP	TTI	MANILA	SEPTEMBER 2 TO 6, 2013

D. CERTIFICATIONS

ITEM	DESIGNATION	COMPANY/SPONSOR	EXAMINATION	INCLUSIVE DATES
1.	CISCO CERTIFIED NETWORK ASSOCIATE	TTI		MAY 7, 2010
2.	BLUE COAT CERTIFIED PROXYSG ADMINISTRATOR	TTI	BCCPA V.3.4.1 CERTIFICATION	OCTOBER 29, 2010
3.	FORTINET CERTIFIED NETWORK SECURITY PROFESSIONAL	TTI		NOVEMBER 4, 2010
4.	SOLARWINDS CERTIFIED PROFESSIONAL	TTI		DECEMBER 22, 2010
5.	FORTINET CERTIFIED NETWORK SECURITY ADMINSITRATOR	TTI		JANUARY 2011
6.	F5 LTM ESSENTIALS V10 EXAM	TTI		7-OCT-11
7.	F5 CERTIFIED SYSTEM ENGINEER (F5 LTM ADVANCE V10 EXAM)	TTI		28-OCT-11
8.	F5 PRODUCT CONSULTANT-ASM	TTI	(BIG-IP ASM V10X EXAM) APPLICATION DELIVERY NETWORK EXAM	JULY 9, 2012
9.	BLUE COAT CERTIFIED PACKETSHAPER ADMINISTRATOR	TTI	BCPSA-3.3.1-26572	AUGUST 11, 2012
10.	CISCO SALES EXPERT	TTI	646-206	JULY 15, 2013

TRENDS AND TECHNOLOGIES, INC.
CERTIFIED TRUE COPY

ID	Task Name	Duration
1	**Bidding For The Procurement of One (1) Lot Network Security Device [ITB No. NSD 2014-003-IT].**	**45 days**
2	Initiation	**30 days**
3	Issuance of Notice to Proceed	1 day
4	Ordering of Equipment	30 days
5	Kick-off Meeting	1 day
6	**Execution**	**12 days**
7	Equipment Delivery	1 day
8	Onsite Inventory (HO)	1 day
9	Upgrade FortiGate firmware of 50 x FG60D	3 days
10	Conduct IPSECVPN Testing on Philhealth H.O And IPVPN Failover Testing	3 days
11	Conduct HAT (Hardware Acceptance Test)	3 days
12	Save and Back-up configuration	1 day
13	**Monitoring and Controlling**	**6 days**
14	Preparation of installation manual for Fortigate IPSECVPN And Initial configuration	2 days
15	Preparation of Project Documentation	5 days
16	**Closing**	**1 day**
17	Submission of Project Documentation	1 day
18	Project Acceptance and Closure	0 days
19	Project Completion	0 days
20	**Post Project Activities**	**2 days**
21	Training	2 days
22	*Post Project Activities Completed*	0 days



Bidding for the Procurement of
(1) One Lot Network Security Device

Task	▬	Milestone	◆	External Tasks	▬
Split	─	Summary	▬	External Milestone	◇
Progress	▬	Project Summary	▬	Deadline	⇩

ANNEX "D"

Republic of the Philippines
PHILIPPINE HEALTH INSURANCE CORPORATION
Citystate Centre Building, 709 Shaw Boulevard, Pasig City
Healthline 441-7444   www.philhealth.gov.ph

NOTICE OF AWARD

Date Issued: 01 SEP 2014

Ms. SHIRLEY Z. AMATA
TRENDS AND TECHNOLOGIES, INC.
6/F Trafalgar Plaza, 105 H.V. Dela Costa,
Salcedo Village, Makati City
Tel.No.: 814-0130

Ms. **Amata**:

We are pleased to notify you that your bid proposal for the bidding on the procurement of ***One (1) Lot Network Security Device*** for the execution of *Trends and Technologies, Inc.* at the Contract Price equivalent to **Seven Million Eighty Eight Thousand Nine Hundred Ninety Nine Pesos (PhP7,088,999.00)**is hereby accepted.

You are hereby required to provide within ten (10) calendar days the ***performance security*** in the form and amount stipulated in the Bid Documents of the said procurement. Failure to provide the performance security shall constitute sufficient ground for cancellation of the award and forfeiture of the bid security.

Very truly yours,

ALEXANDER A. PADILLA
President and CEO

Conforme:

Ms. SHIRLEY Z. AMATA
TRENDS AND TECHNOLOGIES, INC.
Date: SEPT. 2, 2014

CCCD - 08-15-14-4524

ANNEX D

Republic of the Philippines
PHILIPPINE HEALTH INSURANCE CORPORATION
Citystate Centre Building, 709 Shaw Boulevard, Pasig City
Healthline 441-7444 www.philhealth.gov.ph

NOTICE OF AWARD

Date Issued: 01 SEP 2014

Ms. SHIRLEY Z. AMATA
TRENDS AND TECHNOLOGIES, INC.
6/F Trafalgar Plaza, 105 H.V. Dela Costa,
Salcedo Village, Makati City
Tel.No.: 814-0130

Ms. **Amata**:

We are pleased to notify you that your bid proposal for the bidding on the procurement of ***One (1) Lot Network Security Device*** for the execution of *Trends and Technologies, Inc.* at the Contract Price equivalent to **Seven Million Eighty Eight Thousand Nine Hundred Ninety Nine Pesos (PhP7,088,999.00)**is hereby accepted.

You are hereby required to provide within ten (10) calendar days the ***performance security*** in the form and amount stipulated in the Bid Documents of the said procurement. Failure to provide the performance security shall constitute sufficient ground for cancellation of the award and forfeiture of the bid security.

Very truly yours,

ALEXANDER A. PADILLA
President and CEO

Conforme:

Ms. SHIRLEY Z. AMATA
TRENDS AND TECHNOLOGIES, INC.
Date: SEPT. 2, 2014

LCRD - 08-15-14-4524

[illegible] n O. IV-DK-20-1598

Republic of the Philippines
PHILIPPINE HEALTH INSURANCE CORPORATION
Citystate Centre Building, 709 Shaw Boulevard, Pasig City
Healthline 441-7444 www.philhealth.gov.ph

BIDS AND AWARDS COMMITTEE FOR INFORMATION TECHNOLOGY RESOURCES (BAC-ITR)
RESOLUTION NO. 23, S. 2014

RESOLUTION RECOMMENDING THE DECLARATION OF TRENDS AND TECHNOLOGIES, INC. AS THE BIDDER WITH THE SINGLE CALCULATED AND RESPONSIVE BID (SCRB) AND THE AWARD THERETO OF THE CONTRACT FOR THE PROCUREMENT ONE (1) LOT NETWORK SECURITY DEVICE

WHEREAS, based on the approved Request and Issue Voucher (RIV) No. 14-0332 dated April 29, 2014 the Corporate Information Security Department (CISD) requested procurement of One (1) Lot Network Security Device with an Approved Budget for the Contract (ABC) of Seven Million Five Hundred Sixty Five Thousand One Hundred Three Pesos (PhP7,565,103.00);

WHEREAS, procurement of the abovementioned project was advertised on June 16, 2014 at the Philippine Star (PS) and was posted at the Phil-GEPS and PhilHealth Corporate website and at conspicuous places located at the PhilHealth Head Office on June 16- July 4, 2014;

WHEREAS, in response to the said invitation, one (1) bidder secured the bidding documents, namely Trends and Technologies, Inc.;

WHEREAS, a Pre-Bid Conference was held on July 1, 2014 to address requests for clarifications and other queries with regard to the project where no queries was raised;

WHEREAS, the Opening of Bids was held on July 14, 2014 wherein Trends and Technologies, Inc. submitted its bid;

WHEREAS, during the said Opening of Bids, Trends and Technologies, Inc. offered a financial bid proposal of Seven Million Eighty Eight Thousand Nine Hundred Ninety Nine Pesos (PhP7,088,999.00) and was adjudged as the proponent with the Single Calculated Bid (SCB). The BAC-ITR instructed the Technical Working Group (TWG) to proceed with the post-qualification of CT Link Systems, Inc.;

WHEREAS, the TWG conducted post-qualification evaluation on July 23, 2014 and presented the results during the BAC-ITR meeting on August 5, 2014 declaring that the bid proposal of Trends and Technologies, Inc. was found to be compliant with the eligibility, technical and financial requirements of PhilHealth;

WHEREAS, upon further review , the BAC-ITR concurred with the recommendation of the TWG to declare Trends and Technologies, Inc. as the bidder with the Single Calculated and Responsive Bid;

NOW, THEREFORE, the BAC-ITR resolved to recommend to the President and CEO the award of the contract for **One (1) Lot Network Security Device** to **TRENDS AND TECHNOLOGIES, INC.** in the amount of **Seven Million Eighty Eight Thousand Nine Hundred Ninety Nine Pesos (PhP7,088,999.00).**

Signed this 5th day of **August 2014** at Pasig City

SVP EDGAR JULIO S. ASUNCION
Chairperson

OIC-VP LEIZEL P. LAGRADA
Vice-Chairperson

SM MARIO S. MATANGUIHAN
Member

SM ALFREDO B. PINEDA II
Member

SM MA. SOPHIA B. VARLEZ
Member

OIC-SM RONALD ALLAN C. PABLO
Member/End-user

[✓] APPROVED
[ ] DISAPPROVED
[ ] Others ________

ALEXANDER A. PADILLA
President and CEO
Date Signed: ________

RESOLUTION RECOMMENDING THE DECLARATION OF TRENDS AND TECHNOLOGIES, INC. AS THE BIDDER WITH THE SINGLE CALCULATED AND

ANNEX "F"

Section IV. General Conditions of Contract

1. Definitions

1.1. In this Contract, the following terms shall be interpreted as indicated:

(a) "The Contract" means the agreement entered into between the Procuring Entity and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

(b) "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.

(c) "The Goods" means all of the supplies, equipment, machinery, spare parts, other materials and/or general support services which the Supplier is required to provide to the Procuring Entity under the Contract.

(d) "The Services" means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Supplier covered under the Contract.

(e) "GCC" means the General Conditions of Contract contained in this Section.

(f) "SCC" means the Special Conditions of Contract.

(g) "The Procuring Entity" means the organization purchasing the Goods, as named in the SCC.

(h) "The Procuring Entity's country" is the Philippines.

(i) "The Supplier" means the individual contractor, manufacturer distributor, or firm supplying/manufacturing the Goods and Services under this Contract and named in the SCC.

(j) The "Funding Source" means the organization named in the SCC.

(k) "The Project Site," where applicable, means the place or places named in the SCC.

(l) "Day" means calendar day.

(m) The "Effective Date" of the contract will be the date of receipt by the Supplier of the Notice to Proceed or the date provided in the Notice to Proceed. Performance of all obligations shall be reckoned from the Effective Date of the Contract.

(n) "Verified Report" refers to the report submitted by the Implementing Unit to the Head of the Procuring Entity setting forth its findings as to the existence of grounds or causes for termination and explicitly stating its recommendation for the issuance of a Notice to Terminate.

2. Corrupt, Fraudulent, Collusive, and Coercive Practices

2.1. Unless otherwise provided in the SCC, the Procuring Entity as well as the bidders, contractors, or suppliers shall observe the highest standard of ethics during the procurement and execution of this Contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for the purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the Government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in Republic Act 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) "collusive practices" means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede au administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevaut to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights. of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

2.2. Further the Funding Source, Borrower or Procuring Entity, as appropriate, will seek to impose the maximum civil, administrative and/or criminal penalties available under the applicable law on individuals and organizations deemed to be involved with any of the practices mentioned in GCC Clause 2.1(a).

3. Inspection and Audit by the Funding Source

The Supplier shall permit the Funding Source to inspect the Supplier's accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Funding Source, if so required by the Funding Source.

4. Governing Law and Language

4.1. This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

4.2. This Contract has been executed in the English language, whicb shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

5. Notices

5.1. Any notice, request, or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request, or consent sball be deemed to have been given or made when received by the concerned party, either in person or througb an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the SCC, which shall be effective when delivered and duly received or on the notice's effective date, whichever is later.

5.2. A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to the provisions listed in the SCC for GCC Clause 5.1.

6. Scope of Contract

6.1. The GOODS and Related Services to be provided shall be as specified in Section VI. Scbedule of Requirements.

6.2. This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. Any additional requirements for the completion of this Contract shall be provided in the SCC.

7. Subcontracting

7.1. Subcontracting of any portion of the Goods, if allowed in the BDS, does not relieve the Supplier of any liability or obligation under this Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants or workmen.

7.2. Subcontractors disclosed and identified during the bidding may be changed during the implementation of this Contract, subject to compliance with the required qualifications and the approval of the Procuring Entity.

8. Procuring Entity's Responsibilities

8.1. Whenever the performance of the obligations in this Contract requires that the Supplier obtain permits, approvals, import, and other licenses from local public authorities, the Procuring Entity shall, if so needed by the Supplier, make its best effort to assist the Supplier in complying with such requirements in a timely and expeditious manner.

8.2. The Procuring Entity shall pay all costs involved in the performance of its responsibilities in accordance with GCC Clause 6.

9. Prices

9.1. For the given scope of work in this Contract as awarded, all bid prices are considered fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances and upon prior approval of the GPPB in accordance with Section 61 of R.A. 9184 and its IRR or except as provided in this Clause.

9.2. Prices charged by the Supplier for Goods delivered and/or services performed under this Contract shall not vary from the prices quoted by the Supplier in its bid, with the exception of any change in price resulting from a Change Order issued in accordance with GCC Clause 29.

10. Payment

10.1. Payments shall be made only upon a certification by the Head of the Procuring Entity to the effect that the Goods have been rendered or delivered in accordance with the terms of this Contract and have been duly inspected and accepted. Except with the prior approval of the President no payment shall be made for services not yet rendered or for supplies and materials not yet delivered under this Contract. Ten percent (10%) of the amount of each payment shall be retained by the Procuring Entity to cover the Supplier's warranty obligations under this Contract as described in GCC Clause 17.

10.2. The Supplier's request(s) for payment shall be made to the Procuring Entity in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and/or Services performed, and by documents submitted pursuant to the <u>SCC</u> provision for GCC Clause 6.2, and upon fulfillment of other obligations stipulated in this Contract.

10.3. Pursuant to GCC Clause 10.2, payments shall be made promptly by the Procuring Entity, but in no case later than sixty (60) days after submission of an invoice or claim by the Supplier.

10.4. Unless otherwise provided in the <u>SCC</u>, tbe currency in which payment is made to the Supplier under this Contract shall be in Philippine Pesos.

11. Advance Payment and Terms of Payment

11.1. Advance payment shall be made only after prior approval of the President, and shall not exceed fifteen percent (15%) of the Contract amount, unless otherwise directed by the President or in cases allowed under Annex "D" of RA 9184.

11.2. For Goods supplied from abroad, the terms of payment shall be as follows:

(a) On Contract Signature: Ten percent (10%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms.

(b) On Delivery: Seventy percent (70%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents.

(c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by the Procuring Entity's authorized representative. In the event that no inspection or acceptance certificate is issued by the Procuring Entity's authorized representative within forty five (45) days of the date shown on the delivery receipt the Supplier shall have the right to claim payment of the remaining twenty percent (20%) subject to the Procuring Entity's own verification of the reason(s) for the failure to issue documents (vii) and (viii) as described in the SCC provision on Delivery and Documents.

11.3. All progress payments shall first be charged against the advance payment until the latter has been fully exhausted.

12. Taxes and Duties

The Supplier, whether local or foreign, shall be entirely responsible for all the necessary taxes, stamp duties, license fees, and other such levies imposed for the completion of this Contract.

13. Performance Security

13.1. Within ten (10) calendar days from receipt of the Notice of Award from the Procuring Entity but in no case later than the signing of the contract by both parties, the successful Bidder shall furnish the performance security in any the forms prescribed in the ITB Clause 33.2.

13.2. The performance security posted in favor of the Procuring Entity shall be forfeited in the event it is established that the winning bidder is in default in any of its obligations under the contract.

13.3. The performance security shall remain valid until issuance by the Procuring Entity of the Certificate of Final Acceptance.

13.4. The performance security may be released by the Procuring Entity and returned to the Supplier after the issuance of the Certificate of Final Acceptance subject to the following conditions:

(a) There are no pending claims against the Supplier or the surety company filed by the Procuring Entity;

(b) The Supplier has no pending claims for labor and materials filed against it; and

(c) Other terms specified in the SCC.

13.5. In case of a reduction of the contract value, the Procuring Entity shall allow a proportional reduction in the original performance security, provided that any such reduction is more than ten percent (10%) and that the aggregate of such reductions is not more than fifty percent (50%) of the original performance security.

14. Use of Contract Documents and Information

14.1. The Supplier shall not, except for purposes of performing the obligations in this Contract, without the Procuring Entity's prior written consent, disclose this Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring Entity. Any such disclosure shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

14.2. Any document, other than this Contract itself, enumerated in GCC Clause 14.1 shall remain the property of the Procuring Entity and shall be returned (all copies) to the Procuring Entity on completion of the Supplier's performance under this Contract if so required by the Procuring Entity.

15. Standards

The Goods provided under this Contract shall conform to the standards mentioned in the Section VII. Technical Specifications; and, when no applicable standard is mentioned, to the authoritative standards appropriate to the Goods' country of origin. Such standards shall be the latest issued by the institution concerned.

16. Inspection and Tests

16.1. The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Contract specifications at no extra cost to the Procuring Entity. The <u>SCC</u> and Section VII. Technical Specifications shall specify what inspections and/or tests the Procuring Entity requires and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

16.2. If applicable, the inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the goods' final destination. If conducted on the premises of the Snpplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Entity. The Supplier shall provide the Procuring Entity with results of such inspections and tests.

16.3. The Procuring Entity or its designated representative shall be entitled to attend the tests and/or inspections referred to in this Clause provided that the Procuring Entity shall bear all of its own costs and expenses incurred in connection with such attendance including, but not limited to, all traveling and board and lodging expenses.

16.4. The Procuring Entity may reject any Goods or any part thereof that fail to pass any test and/or inspection or do not conform to the specifications. The Supplier shall either rectify or replace such rejected Goods or parts thereof or make alterations necessary to meet the specifications at no cost to the Procuring Entity, and shall repeat the test and/or inspection, at no cost to the Procuring Entity, upon giving a notice pursuant to GCC Clause 5.

16.5. The Supplier agrees that neither the execution of a test and/or inspection of the Goods or any part thereof, nor the attendance by the Procuring Entity or its representative, shall release the Supplier from any warranties or other obligations under this Contract.

17. **Warranty**

17.1. The Supplier warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the Procuring Entity provides otherwise.

17.2. The Supplier further warrants that all Goods supplied under this Contract shall have no defect, arising from design, materials, or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.

17.3. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier for a minimum period specified in the SCC. The obligation for the warranty shall be covered by, at the Supplier's option, either retention money in an amount equivalent to at least ten percent (10%) of the final payment, or a special bank guarantee equivalent to at least ten percent (10%) of the Contract Price or other such amount if so specified in the SCC. The said amounts shall only be released after the lapse of the warranty period specified in the SCC; provided, however, that the Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.

17.4. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, within the period specified in the SCC and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the Procuring Entity.

17.5. If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in GCC Clause 17.4, the Procuring Entity may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Entity may have against the Supplier under the Contract and under the applicable law.

18. **Delays in the Supplier's Performance**

18.1. Delivery of the Goods and/or performance of Services sball be made by the Supplier in accordance with the time schedule prescribed by the Procuring Entity in Section VI. Schedule of Requirements.

18.2. If at any time during the performance of this Contract, the Supplier or its Subcontractor(s) should encounter conditions impeding timely delivery of the Goods and/or performance of Services, the Supplier shall promptly notify the Procuring Entity in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, and upon causes provided for under GCC Clause 22, the Procuring Entity shall evaluate the situation and may extend the Supplier's time for performance, in which case the extension shall be ratified by the parties by amendment of Contract.

18.3. Except as provided under GCC Clause 22, a delay by the Supplier in the performance of its obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to GCC Clause 19, unless an extension of time is agreed upon pursuant to GCC Clause 29 without the application of liquidated damages.

19. **Liquidated Damages**

Subject to GCC Clauses 18 and 22, if the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. The maximum deduction shall be ten percent (10%) of the amount of contract. Once the maximum is reached, the Procuring Entity shall rescind the Contract pursuant to GCC Clause 23, without prejudice to other courses of action and remedies open to it.

20. Settlement of Disputes

20.1. If any dispute or difference of any kind whatsoever shall arise between the Procuring Entity and the Supplier in connection with or arising out of this Contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

20.2. If after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Procuring Entity or the Supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

20.3. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause shall be settled by arbitration. Arbitration may be commenced prior to or after delivery of the Goods under this Contract.

20.4. In the case of a dispute between the Procuring Entity and the Supplier, the dispute shall be resolved in accordance with Republic Act 9285 ("R.A. 9285"), otherwise known as the "Alternative Dispute Resolution Act of 2004."

20.5. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the Supplier any monies due the Supplier.

21. Liability of the Supplier

21.1. The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines, subject to additional provisions, if any, set forth in the SCC.

21.2. Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent rights, if applicable, the aggregate liability of the Supplier to the Procuring Entity shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

22. Force Majeure

22.1. The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that the Supplier's delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure*.

22.2. For purposes of this Contract the terms "*force majeure*" and "fortuitous event" may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the Contractor could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the Contractor. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

22.3. If a *force majeure* situation arises, the Supplier shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for perfomance not prevented by the *force majeure*.

23. Termination for Default

23.1. The Procuring Entity shall terminate this Contract for default when any of the following conditions attends its implementation:

(a) Outside of *force majeure*, the Supplier fails to deliver or perform any or all of the Goods within the period(s) specified in the contract, or within any extension thereof granted by the Procuring Entity pursuant to a request made by the Supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contact price;

(b) As a result of *force majeure*, the Supplier is unable to deliver or perform any or all of the Goods, amounting to at least ten percent (10%) of the contract price, for a period of not less than sixty (60) calendar days after receipt of the notice from the Procuring Entity stating that the circumstance of force majeure is deemed to have ceased; or

(c) The Supplier fails to perform any other obligation under the Contract.

23.2. In the event the Procuring Entity terminates this Contract in whole or in part, for any of the reasons provided under GCC Clauses 23 to 26, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Entity for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of this Contract to the extent not terminated.

23.3. In case the delay in the delivery of the Goods and/or performance of the Services exceeds a time duration equivalent to ten percent (10%) of the specified contract time plus any time extension duly granted to the Supplier, the Procuring Entity may terminate this Contract, forfeit the Supplier's performance security and award the same to a qualified Supplier.

24. Termination for Insolvency

The Procuring Entity shall terminate this Contract if the Supplier is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity and/or the Supplier.

25. Termination for Convenience

25.1. The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience. The Head of the Procuring Entity may terminate a contract for the convenience of the Government if he has determined the existence of conditions that make Project Implementation economically, financially or technically impractical and/or unnecessary, such as, but not limited to, fortuitous event(s) or changes in law and national government policies.

25.2. The Goods that have been delivered and/or performed or are ready for delivery or performance within thirty (30) calendar days after the Supplier's receipt of Notice to Terminate shall be accepted by the Procuring Entity at the contract terms and prices. For Goods not yet performed and/or ready for delivery, the Procuring Entity may elect:

(a) to have any portion delivered and/or performed and paid at the contract terms and prices; and/or

(b) to cancel the remainder and pay to the Supplier an agreed amount for partially completed and/or performed goods and for materials and parts previously procured by the Supplier.

25.3. If the Supplier suffers loss in its initial performance of the terminated contract, such as purchase of raw materials for goods specially manufactured for the Procuring Entity which cannot be sold in open market, it shall be allowed to recover partially from this Contract, on a ***quantum merit*** basis. Before recovery may be made, the fact of loss must be established under oath by the Supplier to the satisfaction of the Procuring Entity before recovery may be made.

26. Termination for Unlawful Acts

26.1. The Procuring Entity may terminate this Contract in case it is determined *prima facie* that the Supplier has engaged, before or during the implementation of this Contract, in unlawful deeds and behaviors relative to contract acquisition and implementation. Unlawful acts include, but are not limited to, the following:

(a) Corrupt, fraudulent, and coercive practices as defined in ITB Clause 3.1(a);

(b) Drawing up or using forged documents;

(c) Using adulterated materials, means or methods, or engaging in production contrary to rules of science or the trade; and

(d) Any other act analogous to the foregoing.

27. Procedures for Termination of Contracts

27.1. The following provisions shall govern the procedures for termination of this Contract:

(a) Upon receipt of a written report of acts or causes which may constitute ground(s) for termination as aforementioned, or upon its own initiative, the Implementing Unit shall, within a period of seven (7) calendar days, verify the existence of such ground(s) and cause the execution of a Verified Report, with all relevant evidence attached;

(b) Upon recommendation by the Implementing Unit, the Head of the Procuring Entity shall terminate this Contract only by a written notice to the Supplier conveying the termination of this Contract. The notice shall state:

(i) that this Contract is being terminated for any of the ground(s) aforementioned, and a statement of the acts that constitute the ground(s) constituting the same;

(ii) the extent of termination, whether in whole or in part;

(iii) an instruction to the Supplier to show cause as to why this Contract should not be terminated; and

(iv) special instructions of the Procuring Entity, if any.

(c) The Notice to Terminate shall be accompanied by a copy of the Verified Report;

(d) Within a period of seven (7) calendar days from receipt of the Notice of Termination, the Supplier shall submit to the Head of the Procuring Entity a verified position paper stating why this Contract should not be terminated. If the Supplier fails to show cause after the lapse of the seven (7) day period, either by inaction or by default, the Head of the Procuring Entity shall issue an order terminating this Contract;

(e) The Procuring Entity may, at any time before receipt of the Supplier's verified position paper described in item (d) above withdraw the Notice to Terminate if it is determined that certain items or works subject of the notice had been completed, delivered, or performed before the Supplier's receipt of the notice;

(f) Within a non-extendible period of ten (10) calendar days from receipt of the verified position paper, the Head of the Procuring Entity shall decide whether or not to terminate this Contract. It shall serve a written notice to the Supplier of its decision and, unless otherwise provided, this Contract is deemed terminated from receipt of the Supplier of the notice of decision. The termination shall only be based on the ground(s) stated in the Notice to Terminate;

(g) The Head of the Procuring Entity may create a Contract Termination Review Committee (CTRC) to assist him in the discharge of this function. All decisions recommended by the CTRC shall be subject to the approval of the Head of the Procuring Entity; and

(h) The Supplier must serve a written notice to the Procuring Entity of its intention to terminate the contract at least thirty (30) calendar days before its intended termination. The Contract is deemed terminated if it is not resumed in thirty (30) calendar days after the receipt of such notice by the Procuring Entity.

28. Assignment of Rights

The Supplier shall not assign his rights or obligations under this Contract, in whole or in part, except with the Procuring Entity's prior written consent.

29. Contract Amendment

Subject to applicable laws, no variation in or modification of the terms of this Contract shall be made except by written amendment signed by the parties.

30. Application

These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of this Contract.

Annex" G"

Section V. Special Conditions of Contract

GCC Clause	
1.1(g)	The Procuring Entity is ***Philippine Health Insurance Corporation.***
1.1(i)	The Supplier is *[to be inserted at the time of contract award].*
1.1(j)	The Funding Source is: **Philippine Health Insurance Corporation's Corporate Operating Budget (COB) for CY 2014** in the amount of ***Seven Million Five Hundred Sixty Five Thousand One Hundred Three Pesos (PhP7,565,103.00)***
1.1(k)	The Project Site is *at PhilHealth Head Office*
5.1	The Procuring Entity's address for Notices is: ***EDGAR JULIO S. ASUNCION,*** *Senior Vice-President, Chief Legal Executive, and BAC-ITR Chairperson, Room 1002, 10th Floor CityState Centre,709 Shaw Boulevard, Pasig City*
6.2	Delivery of the Goods and Services shall be made by the Supplier in accordance with the terms specified in Section VI. **Delivery and Documents –** The Delivery terms of this Contract shall be as follows: **One (1) Lot Network Security Device** shall be delivered to Room 1503, 15th Floor Citystate Centre Bldg., 709 Shaw Blvd., Bgy. Oranbo, Pasig City. Risk and title will pass from the Supplier to PhilHealth upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods and Services shall be made by the Supplier in accordance with the terms specified in Section VI. Schedule of Requirements. The details of shipping and/or other documents to be furnished by the Supplier are as follows: Upon delivery of the Goods and Services to the Project Site, the Supplier shall notify PhilHealth and present the following documents to PhilHealth: (i) Original and four copies of the Supplier's invoice showing Goods' description, quantity, unit price, and total amount; (ii) Original and four copies delivery receipt/note, railway receipt, or truck receipt; (iii) Original Supplier's factory inspection report; (iv) Original and four copies of the Manufacturer's and/or Supplier's warranty certificate; (v) Original and four copies of the certificate of origin (for imported Goods); (vi) Delivery receipt detailing number and description of items received signed by the authorized receiving personnel; (vii) Certificate of Acceptance/Inspection Report signed by the Procuring Entity's representative at the Project Site; and (viii) Four copies of the Invoice Receipt for Property signed by the Procuring Entity's representative at the Project Site. **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: (a) performance or supervision of on-site assembly and/or start-up of the supplied Goods; (b) furnishing of tools required for assembly and/or maintenance of the supplied Goods; (c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; (d) performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not

	relieve the Supplier of any warranty obligations under this Contract; and The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Spare Parts –** The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier: The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spares for the Goods for a period of *three (3) years.* **Packaging –** The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the GOODS' final destination and the absence of heavy handling facilities at all points in transit. The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: PHILIPPINE HEALTH INSURANCE CORPORATION Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Insurance –** The Goods supplied under this Contract shall be fully insured by the Supplier in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery. The Goods remain at the risk and title of the Supplier until their final acceptance by the Procuring Entity. **Transportation –** PhilHealth accepts no liability for the damage of Goods during transit. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to PhilHealth until their receipt and final acceptance at the final destination. **Patent Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
10.2	NO FURTHER INSTRUCTIONS

10.4	NO FURTHER INSTRUCTIONS
13.4(c)	NO FURTHER INSTRUCTIONS
16.1	The bidders should be able to comply with the following: • The winning bidder should work in parallel with PHILHEALTH Corporate Information Security Department (InfoSec) during the installation, testing, and commissioning of the Project. • The bidders must ensure that the proposed **One (1) Lot Network Security Device** is compatible with the existing equipment of PHILHEALTH. • Intensive testing should be done by the winning bidder to achieve the functionality and benefits of the **One (1) Lot Network Security Device.**
17.3	• The maintenance period will be for a period of three (3) years. • All software/hardware should be covered by warranty on services, upgrades and updates on the **One (1) Lot Network Security Device** within the maintenance period which shall commence upon acceptance of the delivered goods.
17.4	The period for correction of defects within the warranty period are: • The bidders should be able to provide expert personnel to service the **One (1) Lot Network Security Device** whenever problems should occur. • The winning bidder should provide a 24x7 phone and technical support to PhilHealth within the three (3) years contract. • Expenses for the technical personnel who will provide the technical service on-site to PHILHEALTH shall be at the expense of the winning bidder.
21.1	NO ADDITIONAL PROVISION.

ANNEX "H"

Prudential Guarantee

Prudential Guarantee and Assurance, Inc.

COYIUTO HOUSE
119 Palanca Legaspi Village
Makati City, Philippines
Tel.: (632) 810 4916 to 35
Fax: (632) 819 2991
coyiutohouse@pga.com.ph
www.prudentialguarantee.com

LINE & SUBLINE	
BONDS	
PERFORMANCE	
ENDORSEMENT NO.	BD-G13-HOM-0018875N
POLICY NO.	BD-G13-HOM-0037124
POLICY JACKET NO.	ASHOM14012297
ISSUE DATE	SEP 18, 2014
EFFECTIVITY DATE	SEP 03, 2014
EXPIRY DATE	JAN 01, 2015
INTERMEDIARY	12000

PREMIUM	
DOC STAMPS	
PREMIUM TAX	
FIRE SERVICE TAX	
VALUE ADDED TAX	
LOCAL GOV'T TAX	
OTHER CHARGES	
AMOUNT DUE	
CURRENCY	PHILIPPINE PESO

INSURED: TRENDS AND TECHNOLOGIES, INC.
6TH FLOOR TRAFALGAR PLAZA
105 H.V. DELA COSTA STREET
SALCEDO VILLAGE, MAKATI CITY

OBLIGEE : PHILIPPINE HEALTH INSURANCE CORPORATION

BOND AMOUNT : Php 2,126,699.70

IT IS HEREBY DECLARED AND AGREED that the following clause stated under this bond is hereby DELETED:

"xxx shall not be liable for any claim not discovered and presented to the company within fifteen (15) days from the expiration of this bond or occurrence of the default or failure of the Principal, whichever is the earliest, and that the obligee hereby waives his right to file any claim against the Surety after the termination of the period xxx"

Except as above-mentioned, all other terms and conditions of this bond remain the same.

CONFORME:

TRENDS AND TECHNOLOGIES, INC.

PRUDENTIAL GUARANTEE AND ASSURANCE INC.

GUIA LAGUIO-FLAMINIANO
VICE PRESIDENT

Authorized Signature

Blg. 2013/53-R
(No.) 2013/53-R

Republika ng Pilipinas
Republic of the Philippines
Kagawaran ng Pananalapi
Department of Finance
KOMISYON NG SEGURO
INSURANCE COMMISSION

KATIBAYAN NG PAGKAMAYKAPANGYARIHAN
CERTIFICATE OF AUTHORITY

ITO AY PATUNAY na ang PRUDENTIAL GUARANTEE AND ASSURANCE, INC.
(This is to certify that

NG LUNGSOD NG MAKATI, PILIPINAS

na isang [illegible]
a [illegible]
(FIRE, MARINE, CASUALTY, SURETY)

na kompanya ng seguro ay nakatugon sa lahat ng mga kailangang itinakda ng batas
insurance company, has complied with all requirements of law

ng Pilipinas kaugnay sa gayong mga kompanya ng seguro, kung kaya pinagkakaloob an
of the Philippines relative to such insurance companies, and it is hereby granted

nitong KATIBAYAN NG PAGKAMAYKAPANGYARIHAN upang makipagnegosyo ng
this ***CERTIFICATE OF AUTHORITY*** *to transact*

uri ng seguro na itinakda sa itaas hanggang ikalabindalawa ng hatinggabi, ng ikatatlumpung
the class of insurance business above set forth until twelve o'clock midnight, on the thirtieth

araw ng Hunyo, taong dalawampung libo't labing-apat
day of June, year 2014

maliban kung agad na bawiin o pigilin ng may makatuwirang dahilan.
unless sooner revoked or suspended for cause.)

Bilang KATUNAYAN NITO, inilagda ko ang aking pangalan
(In WITNESS WHEREOF, I have hereunto subscribed my name

at ikinintal ang Opisyal na Tatak ng aking Tanggapan
and caused my Official Seal to be affixed,

sa Lungsod ng Maynila, Pilipinas. Ito ay may bisa
at the City of Manila, Philippines. This becomes

simula ika-isa ng Hulyo 2013
effective on 1 July 2013.)

EMMANUEL F. DOOC
Insurance Comm

GUARANTEE AND ASSURANCE,
CERTIFIED TRUE COPY
GUIA LAGUIO-FLAMINIANO
Vice President

VALID UNTIL
DECEMBER [illegible]
PURSUANT TO R.A. NO. [illegible]

[illegible]
[illegible] Commissioner

*AO No. 117 issued on
May 1, 1950

Date Issued: 070113

KOMISYON NG SEGURO
1949

Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila

1 August 2014

PRUDENTIAL GUARANTEE AND ASSURANCE, INC.
Coyiuto House, 119 C. Palanca Street
Legaspi Village, Makati City 1229

Attention: Atty. Celestino L. Ang
President

Gentlemen:

We are sending herewith Certificate of Authority of Prudential Guarantee and Assurance, Inc.

The Certificate of Authority shall be valid from **July 1, 2014 until** December 31, 2015, pursuant to the New Insurance Code (R.A. No. 10607), unless sooner suspended or revoked for cause.

Please acknowledge receipt.

Very truly yours,

VIDA T. CHIONG
Deputy Insurance Commissioner
Officer-In-Charge

Encls., a/s

ANNEX "H"

Prudential Guarantee

Prudential Guarantee and Assurance, Inc.

COYIUTO HOUSE
119 Palanca, Legaspi Village
Makati City, Philippines
Tel.: (632) 810 4916 to 35
Fax: (632) 819 2991
coyiutohouse@pga.com.ph
www.prudentialguarantee.com

LINE & SUBLINE BONDS PERFORMANCE		**PREMIUM**	
		DOC STAMPS	
		PREMIUM TAX	
ENDORSEMENT NO.	BD-G13-HOM-0018875N	**FIRE SERVICE TAX**	
POLICY NO.	BD-G13-HOM-0057124	**VALUE ADDED TAX**	
		LOCAL GOV'T TAX	
POLICY JACKET NO.	ASHOM14012297	**OTHER CHARGES**	
ISSUE DATE	SEP 18, 2014		
EFFECTIVITY DATE	SEP 03, 2014	**AMOUNT DUE**	
EXPIRY DATE	JAN 01, 2015		
INTERMEDIARY	12000	**CURRENCY**	PHILIPPINE PESO

INSURED: TRENDS AND TECHNOLOGIES, INC.
6TH FLOOR TRAFALGAR PLAZA
105 H.V. DELA COSTA STREET
SALCEDO VILLAGE, MAKATI CITY

OBLIGEE : PHILIPPINE HEALTH INSURANCE CORPORATION

BOND AMOUNT : Php 2,126,699.70

IT IS HEREBY DECLARED AND AGREED that the following clause stated under this bond is hereby DELETED:

"xxx shall not be liable for any claim not discovered and presented to the company within fifteen (15) days from the expiration of this bond or occurrence of the default or failure of the Principal, whichever is the earliest, and that the obligee hereby waives his right to file any claim against the Surety after the termination of the period xxx"

Except as above-mentioned, all other terms and conditions of this bond remain the same.

CONFORME:

TRENDS AND TECHNOLOGIES, INC.

PRUDENTIAL GUARANTEE AND ASSURANCE INC.

GUIA LAGUIO-FLAMINIANO
VICE PRESIDENT
Authorized Signature

Blg. 2013/53-R
(No.) 2013/53-R

Republika ng Pilipinas
Republic of the Philippines
Kagawaran ng Pananalapi
Department of Finance
KOMISYON NG SEGURO
INSURANCE COMMISSION

KATIBAYAN NG PAGKAMAY-KAPANGYARIHAN
CERTIFICATE OF AUTHORITY

ITO AY PATUNAY na ang **PRUDENTIAL GUARANTEE AND ASSURANCE, INC.**
(This is to certify that

NG LUNGSOD NG MAKATI, PILIPINAS

na isang
a
pang [illegible]
NON-LIFE
(FIRE, MARINE, CASUALTY, SURETY)

na kompanya ng seguro ay nakatugon sa lahat ng mga kailangang itinakda ng batas
insurance company, has complied with all requirements of law

ng Pilipinas kaugnay sa gayong mga kompanya ng seguro, kung kaya pinagkakaloban
of the Philippines relative to such insurance companies, and it is hereby granted

nitong KATIBAYAN NG PAGKAMAY-KAPANGYARIHAN upang makapagnegosyo ng
this CERTIFICATE OF AUTHORITY to transact

uri ng seguro na itinakda sa itaas hanggang ikalabindalawa ng hatinggabi, ng ikatatlumpung
the class of insurance business above set forth until twelve o'clock midnight, on the thirtieth

araw ng Hunyo, taong dalawampung libo't labing-apat
day of June, year 2014

maliban kung agad na bawiin o pigilin ng may makatuwirang dahilan.
unless sooner revoked or suspended for cause.)

Bilang KATUNAYAN NITO, nilagda ko ang aking pangalan
(In WITNESS WHEREOF, I have hereunto subscribed my name

at ikinintal ang Opisyal na Tatak ng aking Tanggapan
and caused my Official Seal to be affixed,

sa Lungsod ng Maynila, Pilipinas. Ito ay may bisa
at the City of Manila, Philippines. This becomes

simula ika-isa ng Hulyo 2013.
effective on 1 July 2013.)

EMMANUEL F. DOOC
Insurance Commissioner

TEE AND ASSURANCE, I
CERTIFIED TRUE CO
GUIA LAGUIO-FLAMINIANO
Vice President

VALID UNTIL
DECEMBER 31, [illegible]
PURSUANT TO R.A. No. [illegible]

For [illegible]
Insurance Commissioner

*AO No. 117 issued on
May 1, 1950

Date Issued: 070113

Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila

1 August 2014

PRUDENTIAL GUARANTEE AND ASSURANCE, INC.
Coyiuto House, 119 C. Palanca Street
Legaspi Village, Makati City 1229

Attention: Atty. Celestino L. Ang
President

Gentlemen:

We are sending herewith Certificate of Authority of Prudential Guarantee and Assurance, Inc.

The Certificate of Authority shall be valid from **July 1, 2014 until** December 31, 2015, pursuant to the New Insurance Code (R.A. No. 10607), unless sooner suspended or revoked for cause.

Please acknowledge receipt.

Very truly yours,

VIDA T. CHIONG
Deputy Insurance Commissioner
Officer-In-Charge

Encls.: a/s

Prudential Guarantee

OIC BOND NO. G(13)101696

PGA BOND NO. BD-G13-HOM-0057124

DOCUMENTARY STAMPS
"PAID"
SEP 09 2014

Premium		[illegible]696.85
Doc Stamps		1,461.11
EVAT		1,403.62
Local Tax		23.38
Other Charges		200.00
TOTAL	₱	14,785.97

PERFORMANCE BOND

KNOW ALL MEN BY THESE PRESENTS:

That **TRENDS AND TECHNOLOGIES, INC.** of **6TH FLOOR TRAFALGAR PLAZA 105 H.V. DELA COSTA STREET SALCEDO VILLAGE, MAKATI CITY**, as PRINCIPAL and **PRUDENTIAL GUARANTEE AND ASSURANCE INC.**, a corporation duly organized and existing under and by virtue of the laws of the Philippines, as SURETY, are held and firmly bound unto **PHILIPPINE HEALTH INSURANCE CORPORATION** as OBLIGEE in the sum of PESOS: **TWO MILLION ONE HUNDRED TWENTY SIX THOUSAND SIX HUNDRED NINETY NINE AND 70/100 ONLY (P2,126,699.70)** Philippine Currency, for the payment of which sum, well and truly to be made, we bind ourselves, our heirs, executors, administrators, successors, and assigns jointly and severally, firmly by these presents.

WHEREAS, The above-named Principal was awarded the Bid/Contract to ____________________ *;*

To guarantee the full and faithful performance by the Principal to complete the One (1) Lot Network Security Device project, as per Notice of Award dated September 1, 2014, a copy of which is hereto attached to form an integral part of this bond;

WHEREAS, this bond is Callable on Demand;

PROVIDED, HOWEVER, that the liability of SURETY under this bond shall in no case exceed the total sum of PESOS: TWO MILLION ONE HUNDRED TWENTY SIX THOUSAND SIX HUNDRED NINETY NINE AND 70/100 ONLY (Php 2,126,699.70), Philippine Currency;

WHEREAS, said OBLIGEE requires said PRINCIPAL to give a good and sufficient bond in the above stated sum to secure the full and faithful performance on his part of said **contract;**

NOW THEREFORE, if the PRINCIPAL shall well and truly perform and fulfill all the undertakings, covenants, terms, conditions and agreements stipulated in said **contract** then, this obligation shall be null and void; otherwise it shall remain in full force and effect.

The liability of **PRUDENTIAL GUARANTEE AND ASSURANCE INC.**, under this bond will expire on **January 1, 2015**; Furthermore, it is hereby agreed and understood that **PRUDENTIAL GUARANTEE AND ASSURANCE INC.**, shall not be liable for any claim not discovered and presented to the company within fifteen (15) days from the expiration of this bond or occurrence of the default or failure of the principal, whichever is the earliest, and that the obligee hereby waives his right to file any claim against the Surety after the termination of the period of fifteen days above mentioned after which time this bond shall definitely terminate and be deemed absolutely cancelled.

IN WITNESS WHEREOF, we have set our hands this **03rd day of September, 2014**.

TRENDS AND TECHNOLOGIES, INC.
Principal

By:

JOSE DANIEL L. BALAJADIA
CORPORATE SECRETARY

PRUDENTIAL GUARANTEE AND ASSURANCE INC.
TIN 000-431-813

By:

GUIA LAGUIO-FLAMINIANO
Vice President

MARC OCAMPO-TAN
Manager

Signed in the Presence of :

____________________ ____________________

DOCUMENTARY STAMPS "PAID" SEP 0 9 2014

REPUBLIC OF THE PHILIPPINES } S.S. BD-G13-HOM-0057124
CITY OF MAKATI

On this 09th day of September, 2014, personally appeared before me:

Name	*Valid ID No.*	*Issued on*	*Issued at*
JOSE DANIEL L. BALAJADIA			
MARC OCAMPO-TAN	33-5553010-8		
GUIA LAGUIO-FLAMINIANO	33-3013743-3		
PRUDENTIAL GUARANTEE AND ASSURANCE INC.	CI-00142975	Jan. 03, 2014	Makati City

known to me to be the same persons who executed the foregoing instrument and they acknowledged to me that the same is their free and voluntary act and deed and the free and voluntary act and deed of the corporation they represent.

ATTY. ROGEL R. ATIENZA
Notary Public for Makati City
Until December 31, 2014
Appointment No. M-175 (2013-2014)
G/F Caylum House, #159C. Palanca St.,
Legaspi Village, Makati City, Metro Manila
PTR No. 4215789-Jan. 2, 2014-Makati City
IBP No. 949619-Jan. 2, 2014-Pasig City
Roll of Attorney No. 22649
MCLE Compliance No. IV-0007948-Sept. 18, 2012

Doc. No.	264
Page No.	54
Book No.	CIV
Series of	2014

REPUBLIC OF THE PHILIPPINES } S.S.
CITY OF MAKATI

Ms. & Mr. GUIA LAGUIO-FLAMINIANO and MARC OCAMPO-TAN of PRUDENTIAL GUARANTEE AND ASSURANCE INC. with TIN 047-000-491-813 having been duly sworn, state and depose that PRUDENTIAL GUARANTEE AND ASSURANCE INC. is actually worth the amount specified in the foregoing undertaking to wit: TWO MILLION ONE HUNDRED TWENTY SIX THOUSAND SIX HUNDRED NINETY NINE AND 70/100 ONLY (Php 2,126,699.70) Philippine Currency, over and above all just debts and obligations and property exempt from execution.

GUIA LAGUIO-FLAMINIANO MARC OCAMPO-TAN
(Affiant/s)

SUBSCRIBED AND SWORN TO before me this 09th day of September, 2014 at Makati, Philippines, Affiant/s having exhibited to me their valid Identification No. as above indicated.

WITNESS MY HAND AND SEAL.

ATTY. ROGEL R. ATIENZA
Notary Public for Makati City
Until December 31, 2014
Appointment No. M-175 (2013-2014)
G/F Caylum House, #159C. Palanca St.,
Legaspi Village, Makati City, Metro Manila
PTR No. 4215789-Jan. 2, 2014-Makati City
IBP No. 949619-Jan. 2, 2014-Pasig City
Roll of Attorney No. 22649
MCLE Compliance No. IV-0007948-Sept. 18, 2012

Doc. No.	265
Page No.	54
Book No.	CIV
Series of	2014