Public Copy

# Quotation

| Date | Quote # |
|---|---|
| 3/30/2015 | 114 |

The Well Connected Office

| Name / Address |
|---|
| San Mateo County Harbor District<br>Attn: Accounts Payable<br>400 Oyster Point Blvd<br>Suite 300<br>South San Francisco, CA 94080 |

| Project |
|---|
| Firewall Option 4 |

| Item | Description | Qty | Unit Price | Total |
|---|---|---|---|---|
| Maintenance Re-up | Support for Products currently in place at the district Plaza office and the Pillar Point Harbor Harbormaster's office. Includes reinstatement and 1 year of 24x7 support and upgrades | 1 | 5,380.00 | 5,380.00 |
| CPAP-SG2200-NGTP | CheckPoint 2200 Next Generation Threat Prevention Appliance with 11 blades suite | 1 | 3,800.00 | 3,800.00T |
| CPES-SS-PREMIUM-A... | Premium Direct Enterprise Support | 1 | 1,000.00 | 1,000.00T |
| | Sales Tax - South San Francisco, CA | | 9.00% | 432.00 |

Pls. Do not remove

**Total** $10,612.00

Unless otherwise specified, this quotation is valid for up to 30 days after the Quotation date. Please note that quotations typically do not include labor and shipping charges. All prices shown for labor and shipping, if shown, are estimates only and may change. The Well Connected Office is not responsible for loss of business, loss of profits, downtime, or other items beyond our reasonable control due to the purchase/use of these items. Please note that items are typically under the support of the manufacturer for a period of 90 days post purchase, and any additional support beyond that period should be arranged before the expiration of the 90 day warranty period. Longer warranties will be noted on the individual items shown.

# Quotation

| Date | Quote # |
|---|---|
| 3/30/2015 | 115 |

The Well Connected Office

Name / Address

San Mateo County Harbor District
Attn: Accounts Payable
400 Oyster Point Blvd
Suite 300
South San Francisco, CA 94080

| Project |
|---|
| Firewall Option 5 |

| Item | Description | Qty | Unit Price | Total |
|---|---|---|---|---|
| CPAP-SG2200-NGTP | CheckPoint 2200 Next Generation Threat Prevention Appliance with 11 blades suite | 3 | 3,800.00 | 11,400.00T |
| CPES-SS-PREMIUM-A... | Premium Direct Enterprise Support | 3 | 1,000.00 | 3,000.00T |
| | Sales Tax - South San Francisco, CA | | 9.00% | 1,296.00 |

| | |
|---|---|
| **Total** | $15,696.00 |

Unless otherwise specified, this quotation is valid for up to 30 days after the Quotation date. Please note that quotations typically do not include labor and shipping charges. All prices shown for labor and shipping, if shown, are estimates only and may change. The Well Connected Office is not responsible for loss of business, loss of profits, downtime, or other items beyond our reasonable control due to the purchase/use of these items. Please note that items are typically under the support of the manufacturer for a period of 90 days post purchase, and any additional support beyond that period should be arranged before the expiration of the 90 day warranty period. Longer warranties will be noted on the individual items shown.

# Quotation

| Date | Quote # |
|---|---|
| 3/30/2015 | 116 |

The Well Connected Office

Name / Address

San Mateo County Harbor District
Attn: Accounts Payable
400 Oyster Point Blvd
Suite 300
South San Francisco, CA  94080

| Project |
|---|
| Firewall Option 6 |

| Item | Description | Qty | Unit Price | Total |
|---|---|---|---|---|
| 01-SSC-3863 | Dell SonicWALL NSA2600 Series Firewall with TotalSecure with 1 year CGSS Bundle (Threat Prevention, Content Filtering, 24x7 support) | 2 | 3,300.00 | 6,600.00T |
| 01-SSC-4662 | Dell SonicWALL NSA250M TotalSecure Appliance Bundle -- Includes 1 year gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Services, Premium Content Filtering Service, and 24x7 Dynamic Support | 1 | 1,900.00 | 1,900.00T |
|  | Sales Tax - South San Francisco, CA |  | 9.00% | 765.00 |

**Total** $9,265.00

Unless otherwise specified, this quotation is valid for up to 30 days after the Quotation date. Please note that quotations typically do not include labor and shipping charges. All prices shown for labor and shipping, if shown, are estimates only and may change. The Well Connected Office is not responsible for loss of business, loss of profits, downtime, or other items beyond our reasonable control due to the purchase/use of these items. Please note that items are typically under the support of the manufacturer for a period of 90 days post purchase, and any additional support beyond that period should be arranged before the expiration of the 90 day warranty period. Longer warranties will be noted on the individual items shown.

# UTM-1 Edge NW Series Features

UTM-1 Edge NW Series Features

| Feature | UTM-1 Edge NW | UTM-1 Edge NW ADSL |
|---|---|---|
| SKU Prefix | CPUTM-EDGE-NWn | CPUTM-EDGE-NWn-ADSL |
| Concurrent Users | 32 / Unlimited | |
| **Capacity** | | |
| Firewall Throughput | 1 Gbps | |
| VPN Throughput | 200 Mbps | |
| Concurrent Firewall Connections | 60,000 | |
| **Hardware Features** | | |
| 4-Port LAN Switch | Ethernet 10/100/1,000 Mbps | |
| WAN Port | Ethernet 10/100/1000 Mbps | ADSL2+ |
| ADSL Standards | — | ADSL2, ADSL2+, T.1413 G.DMT (G.992.1)<br>G.Lite (G.992.2)<br>ANNEX A (ADSL over POTS), ANNEX B (ADSL over ISDN) |
| DMZ/WAN2 Port | Ethernet 10/100/1,000 Mbps | |
| Dialup Backup (Req. Ext. Modem) | ✓ | |
| Console Port (Serial) | ✓ | |
| ExpressCard Port | — | ✓ |
| Print Server | ✓ | |
| USB 2.0 Ports | 2 | 1 |
| **Firewall & Security Features** | | |
| Check Point Stateful Inspection Firewall | ✓ | |
| Application Intelligence (IPS) | ✓ | |

| | |
|---|---|
| Intrusion Detection and Prevention using Check Point SmartDefense | ✓ |
| Network Address Translation (NAT) | ✓ |
| Four Preset Security Policies | ✓ |
| Anti-spoofing | ✓ |
| Voice over IP Support | SIP, H.323 |
| Unlimited INSPECT Policy Rules | ✓ |
| Instant Messenger Blocking / Monitoring | ✓ |
| P2P File Sharing Blocking / Monitoring | ✓ |
| Port-based, Tag-based, and Other VLAN | 5 / 64 |
| Port-based Security (802.1x) | ✓ |
| Web Rules | ✓ |
| Secure HotSpot (Guest Access) | ✓ |

PALO ALTO NETWORKS: **PA-500 Specsheet**

# PA-500

## Key Security Features:

**CLASSIFY ALL APPLICATIONS, ON ALL PORTS, ALL THE TIME WITH APP-ID™.**

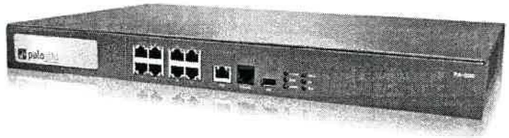
- Identify the application, regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Use the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, apply traffic shaping.
- Categorize unidentified applications for policy control, threat forensics, custom App-ID creation, or packet capture for App-ID development.

**EXTEND SAFE APPLICATION ENABLEMENT POLICIES TO ANY USER, AT ANY LOCATION, WITH USER-ID™ AND GLOBALPROTECT™.**

- Agentless integration with Active Directory, LDAP, eDirectory Citrix and Microsoft Terminal Services.
- Easily integrate firewall policies with NAC, 802.1X wireless, Proxies and NAC solutions.
- Deploy consistent policies to local and remote users running Microsoft Windows, Mac OS X, Linux, Android or iOS platforms.

**PROTECT AGAINST ALL THREATS—BOTH KNOWN AND UNKNOWN—WITH CONTENT-ID™ AND WILDFIRE™.**

- Block a range of known threats including exploits, malware and spyware, across all ports, regardless of common threat evasion tactics employed.
- Limit unauthorized transfer of files and sensitive data, and control non work-related web surfing.
- Identify unknown malware, analyze it based on more than 230 malicious behaviors, then automatically create and deliver protection in the next content update.



PA-500

The Palo Alto Networks® PA-500 is a platform for enterprise branch offices and medium sized businesses.

The controlling element of the PA-500 is PAN-OS™, a security-specific operating system that natively classifies all traffic, inclusive of applications, threats and content, then ties that traffic to the user, regardless of location or device type. The application, content, and user—in other words, the business elements that run your business—are then used as the basis of your security policies, resulting in an improved security posture and a reduction in incident response time.

| PERFORMANCE AND CAPACITIES[1] | PA-500 |
|---|---|
| Firewall throughput (App-ID enabled) | 250 Mbps |
| Threat prevention throughput | 100 Mbps |
| IPSec VPN throughput | 50 Mbps |
| New sessions per second | 7,500 |
| Max sessions | 64,000 |

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 6.0.

To view additional information on the PA-500 security features and associated capacities, please visit www.paloaltonetworks.com/products

paloalto networks.

CASPIAN IT GROUP

# Estimate

| Date | Estimate # |
|---|---|
| 3/31/2015 | 550 |

| Name / Address |
|---|
| San Mateo County Harbor District<br>400 Oyster Point Blvd Ste. 300<br>South San Francisco, CA 94080 |

Caspian IT Group
1326 White Oaks RD.
Campbell CA 95008
408-780-0900

| Customer Contact | Rep |
|---|---|
|  | SS |

| Item | Description | Qty | Rate | Total |
|---|---|---|---|---|
|  | Project Description:<br>The following proposal is to connect 3 offices of San Mateo County Harbor District via secured VPN. Caspian IT Group will provide the following:<br>- Install each VPN Firewall in each office.<br>- Configure VPN to connect to Admin Office<br>- Test the connection<br>- Configure throughput on each Firewall<br>- Configure Security on each firewall<br>The above configuration will connect 3 offices together through VPN Tunnel as well as concurrent SSL VPN through Client for mobile users up to 10 users. |  |  |  |
| ZyWALL USG10... | ZyWALL USG100-PLUS 1 Year Security Service Bundle (Commtouch CF, Commtouch AS, Kaspersky AV, ZyXEL IDP) with ZyWALL USG100-PLUS SSL Upgrade from 2 to 10 Users | 3 | 1,299.99 | 3,899.97T |

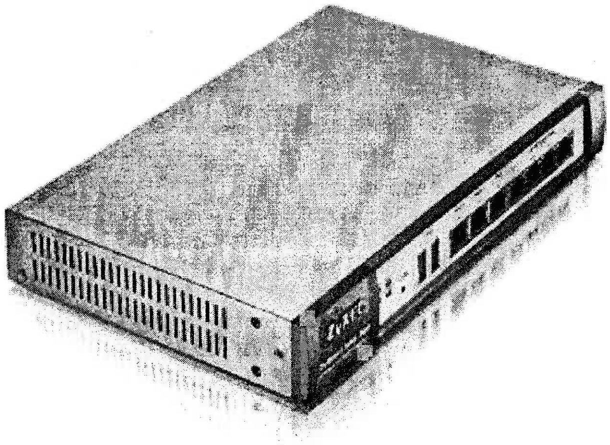
**Please Note that the price indicated is based on a Cash or a Check payment.**
**An additional %3.5 Transaction fee will be added to the total amount if paid by Credit Card.**

Signature ______________________

|  |  |
|---|---|
| Subtotal | $3,899.97 |
| Sales Tax (9.0%) | $351.00 |
| Total | $4,250.97 |

# ZyWALL USG 100

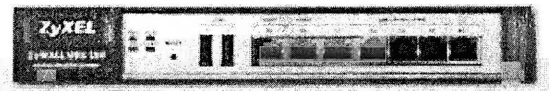
Unified Security Gateway



## Unified Security Gateway for small businesses

- Flexible hybrid VPN (IPSec/L2TP VPN and SSL VPN in one box)
- 7 Gigabit ports
- Scalable UTM/VPN performance
- IM/P2P management (application patrol)
- Bandwidth management
- Unique extension card slot for 3G and WLAN

Content Control from Blue Coat



**ZyWALL USG 100**
Entry-level firewall, 50 VPN tunnels with 50Mbps, firewall 100Mbps

## Advantages

**Strong UTM Performance**
The ZyWALL USG 100 is a high-performance, deep packet inspection security platform for small to medium-sized offices (recommended 10~25 PC users). It embodies a firewall, Intrusion Detection and Prevention (IDP), content filtering, anti-virus, anti-spam and VPN in one box. This multi-layered security safeguards your organisation's customer and company records, intellectual property and critical resources against external and internal threats. Its fanless design allows quiet heat dissipation, making it the perfect choice for desktop deployments.

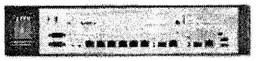
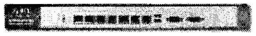
**Flexible Hybrid VPN**
With streamlined integration of both IPSec VPN and SSL VPN technologies, the ZyWALL USG 100 is an ideal solution for organisations requiring intensive VPN applications across distributed networks. No matter whether you are in a remote branch office or at an unreliable hotel hotspot, the ZyWALL USG 100 can establish secure communication tunnels with IPSec and/or SSL protection.

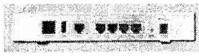
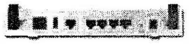
**Ensure Policy Compliance**
Another major benefit of the USG 100 is that user-aware access control, scheduling, bandwidth usage and anti-threat security features can be enforced against inbound and outbound traffic of the protected network resources, whilst multi-ISP links, wireless cards and 3G support can provide more network connectivity.

**Highlights**
- High-performance multi-layer threat protection powered by cutting-edge SecuASIC hardware accelerator
- Hybrid VPN (IPSec, SSL and L2TP) secures connections to branch offices, partners and headquarters
- ICSA-certified ZyXEL or Kaspersky Labs-powered anti-virus for protection against viruses and spyware
- Application patrol controls IM and P2P application usage, even who can use which features within an application
- Extension card slot and USB ports for multiple 3G wireless WAN connections

## Key Features

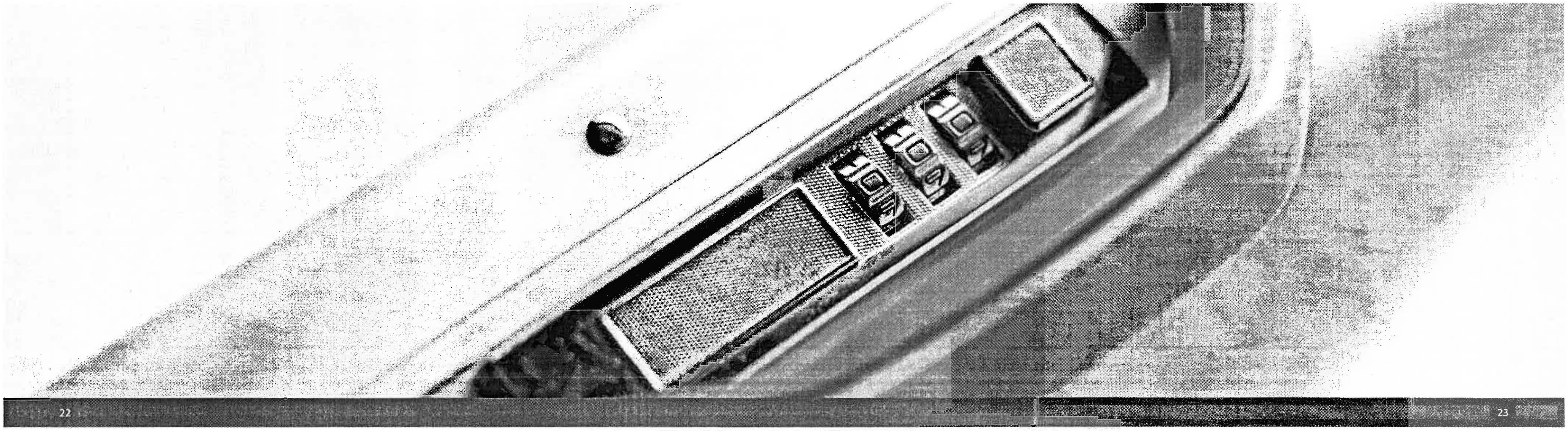
| | |
|---|---|
| **SPI firewall throughput** | 100Mbps |
| **VPN AES/3DES throughput** | 50Mbps |
| **Interfaces** | 5 x LAN/DMZ, 2 x WAN (all GbE) |
| **Concurrent sessions** | 20,000 |
| **No. of user licences** | Unlimited |
| **Max. no. of simultaneous IPSec VPN connections** | 50 |
| **Max. no. of simultaneous SSL VPN users** | 5 |
| **Operating mode** | Routing/NAT/SUA mode |
| **UTM support** | Content filter incl. Web firewall feature, anti-spam, anti-virus (optional ZyXEL AV or Kaspersky AV), IDS/IDP |
| **Bandwidth management** | Multiple WANs for load balancing |
| **Security** | Firewall, IPSec VPN, UTM, IM/P2P management, user-aware management |
| **Network** | Bridge mode/mix mode (routing + bridge), VLAN tagging (802.1q), 3G/WLAN support |
| **Management** | Web GUI (HTTP and HTTPS), CLI, Vantage CNM, Vantage Report |
| **Redundancy** | Device HA (A/P), VPN HA, auto failover, failback, dial backup |
| **Authentication method** | Local database, Radius, LDAP, Microsoft AD |
| **Special feature** | Supports ZyXEL OTP system |
| **Mounting** | 19", 1U |
| **Power supply** | 12V DC, 3.5A |
| **Dimensions** | 242 x 75 x 35.5mm (WxDxH) |

| Series | Product name | Duration | ZyXEL anti-virus | Kaspersky anti-virus |
|---|---|---|---|---|
| ZyWALL USG series | | | | |
|  | ZyWALL USG 2000 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |
| | ZyWALL USG 1000 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |
|  | ZyWALL USG 300 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |
| | ZyWALL USG 200 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |
| | ZyWALL USG 100 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |

| Series | Product name | Duration | ZyXEL anti-virus | Kaspersky anti-virus |
|---|---|---|---|---|
| ZyWALL UTM series (with turbo card) | | | | |
| | ZyWALL 50 | 1 year<br>2 years | -<br>- | ✓<br>✓ |
|  | ZyWALL 20 | 1 year<br>2 years | -<br>- | -<br>- |
|  | ZyWALL 20W | 1 year<br>2 years | -<br>- | -<br>- |

| Product name | Duration | IDP | Content filtering | Free RBL/DNSBL AS | SSL VPN |
|---|---|---|---|---|---|
| | | | | | |
| ZyWALL USG 2000 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ | Free RBL/DNSBL AS<br>Free RBL/DNSBL AS | ✓<br>✓ |
| ZyWALL USG 1000 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ | Free RBL/DNSBL AS<br>Free RBL/DNSBL AS | ✓<br>✓ |
| ZyWALL USG 300 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ | Free RBL/DNSBL AS<br>Free RBL/DNSBL AS | ✓<br>✓ |
| ZyWALL USG 200 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ | Free RBL/DNSBL AS<br>Free RBL/DNSBL AS | ✓<br>✓ |
| ZyWALL USG 100 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ | Free RBL/DNSBL AS<br>Free RBL/DNSBL AS | ✓<br>✓ |

| Product name | Duration | Content filtering | SSL VPN |
|---|---|---|---|
| | | | |
| ZyWALL 50 | 1 year<br>2 years | ✓<br>✓ | ✓<br>✓ |
| ZyWALL 20 | 1 year<br>2 years | ✓<br>✓ | -<br>- |
| ZyWALL 20W | 1 year<br>2 years | ✓<br>✓ | -<br>- |



NETWORK STRATEGY

2096 Walsh Avenue, #B-1
Santa Clara, CA 95050
Tel./Fax: 866-836-4675
E-Mail: info@ntstrategy.com

# Proposal

| Date | Proposal # |
|---|---|
| 3/31/2015 | 274 |

Name / Address

San Mateo County Harbor District
400 Oyster Point Blvd. Ste. 300
South San Francisco, CA 94080

| Customer Phone | Rep |
|---|---|
|  | Ata |

| Item | Description | Qty | Rate | Total |
|---|---|---|---|---|
|  | Project Description:<br>San Mateo County Harbor District requires to connect 3 offices through VPN in the bay area. |  |  |  |
| Materials | XTM 25 Series Security Bundle, 3-Year<br>* Includes Appliance, Gateway AV/IPS, SpamBlocker, WebBlocker, LiveSecurity, Application Control and Reputation Enabled Defense | 3 | 1,699.99 | 5,099.97T |
| Small Busine... | The Following service were performed:<br>- Configure the VPN to connect 3 offices through VPN | 10 | 145.00 | 1,450.00 |

I hereby authorize the service work and materials noted above and agree to pay the estimated charges. Because Network Strategy custom orders all products based on customer need, returns are not allowed after the order has been placed. I acknowledge reading and approving Network Strategy's Warranty and Terms & Conditions of sale as posted on its website - ntstrategy.com. I acknowledge that the estimated amount may change due to additional time spent or additional materials needed to complete the service project.

| | |
|---|---|
| **Subtotal** | $6,549.97 |
| **Sales Tax (9.25%)** | $471.75 |
| **Total** | **$7,021.72** |

Customer Signature: ____________________ Date: ______________

CASPIAN IT GROUP

# Estimate

| Date | Estimate # |
|---|---|
| 3/31/2015 | 551 |

**Name / Address**

San Mateo County Harbor District
400 Oyster Point Blvd Ste. 300
South San Francisco, CA 94080

Caspian IT Group
1326 White Oaks RD.
Campbell CA 95008
408-780-0900

| Customer Contact | Rep |
|---|---|
| | SS |

| Item | Description | Qty | Rate | Total |
|---|---|---|---|---|
| | Project Description:<br>The following proposal is to connect 3 offices of San Mateo County Harbor District via baasic secured VPN. Caspian IT Group will provide the following:<br>- Install each VPN Firewall in each office.<br>- Configure VPN to connect to Admin Office<br>- Test the connection<br>The above configuration will connect only 3 offices together through VPN Tunnel. | | | |
| Netgear Prosafe... | NETGEAR FVS318G-100NAS ProSafe VPN Firewall | 3 | 499.99 | 1,499.97T |

**Please Note that the price indicated is based on a Cash or a Check payment.**
**An additional %3.5 Transaction fee will be added to the total amount if paid by Credit Card.**

| | |
|---|---|
| Subtotal | $1,499.97 |
| Sales Tax (9.0%) | $135.00 |
| Total | $1,634.97 |

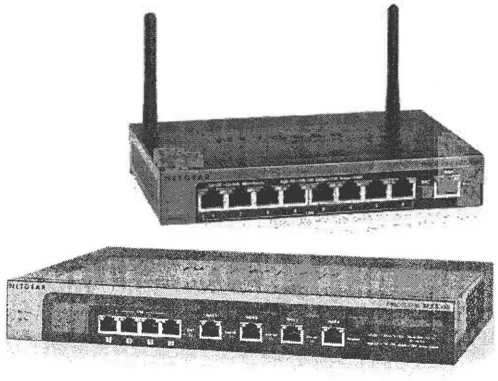
Signature ______________________

NETGEAR®

# ProSAFE® VPN Firewall Series

Data Sheet

FVS318G, FVS318N, FVS336G and SRX5308



## Essential Business-class Network Protection

NETGEAR® ProSAFE® business-class VPN Firewalls are high performing routers that deliver Stateful Packet Inspection (SPI), Virtual Private Network (VPN), Network Address Translation (NAT), AES and 3DES Encryption, Denial of Service (DoS) protection and provide full secure network access between headquarter locations, remote/branch offices and remote workers. This makes it the ideal solution to provide businesses with the essential network security needed to stop unwanted intrusions.

## Highlights

### Secure

NETGEAR ProSAFE VPN Firewalls provide both secure IPsec site-to-site tunnels and IPsec secure access for remote clients and also support client-less SSL VPN as well as secure L2TP and PPTP connections. Employing a true SPI firewall with customizable firewall rules, this VPN router is a high-performance, SNMP-manageable, network solution that furnishes multidimensional security including denial-of-service (DoS) protection, stateful packet inspection (SPI), URL keyword filtering, logging, reporting, and real-time alerts.

### Flexible

ProSAFE VPN Firewalls work perfectly with ISP modems, including cable or DSL broadband connections. Wireless-N connectivity[1] and Gigabit LAN/WAN ports keep your data moving at top speed and a configurable DMZ port allows for flexible server deployment. With Network Address Translation (NAT) routing and classical routing, all the users in your small office can access your broadband connection at the same time. VLAN support allows for guest networks plus better network segmentation and IPv6 support will enable you to future proof your network.

### Reliable

Models with multiple WAN ports can operate in either a load-balancing or fail-over configuration. The load-balancing configuration enables maximum throughput by utilizing WAN connections to distribute traffic across two broadband connections, possibly with different ISP providers. Alternatively, a second WAN port may be configured as a failover connection in case the primary connection fails, for another method of providing high reliability.

The rugged metal unit houses advanced, high-quality electronics, and is backed by the industry-best ProSAFE Lifetime Hardware Warranty*, Lifetime Technical Support[3], and Lifetime Next Business Day Replacement*.

ICSA labs CERTIFIED FIREWALL-SMB

VPNC CERTIFIED Basic Interop AES Interop

LIFETIME Warranty

LIFETIME Tech Support

LIFETIME Next Business Day

[1] On Supported Models

## Features and Benefits

### Hardware Accelerated Network Processor

- High Performance LAN-to-WAN throughput for today's and tomorrow's broadband speeds

### Essential Business Networking Features

- IPv4/IPv6 Support
- 802.1Q VLAN
- QoS
- NAT and Classical Routing
- SIP ALG, VPN Passthrough

### Secure Firewall

- Stateful Packet Inspection (SPI)
- DoS attack protection
- Block TCP/UDP packet floods
- Port/service blocking
- Hardware DMZ port
- MAC Address filter
- Web object and keyword blocking

### Secure VPN Remote Access

- SSL VPN – clientless remote access, anywhere, anytime
- IPsec VPN – secure site-to-site tunnels and client-based remote access
- Industry-strength encryption algorithms
- IKE authentication protects against unauthorized remote access
- L2TP and PPTP Server

### Bandwidth Management

- Control end user bandwidth consumption with Bandwidth Profiles
- Prioritize traffic with Quality of Service (QoS)
- WAN Traffic Metering

### Dual or Quad WAN Ports[1]

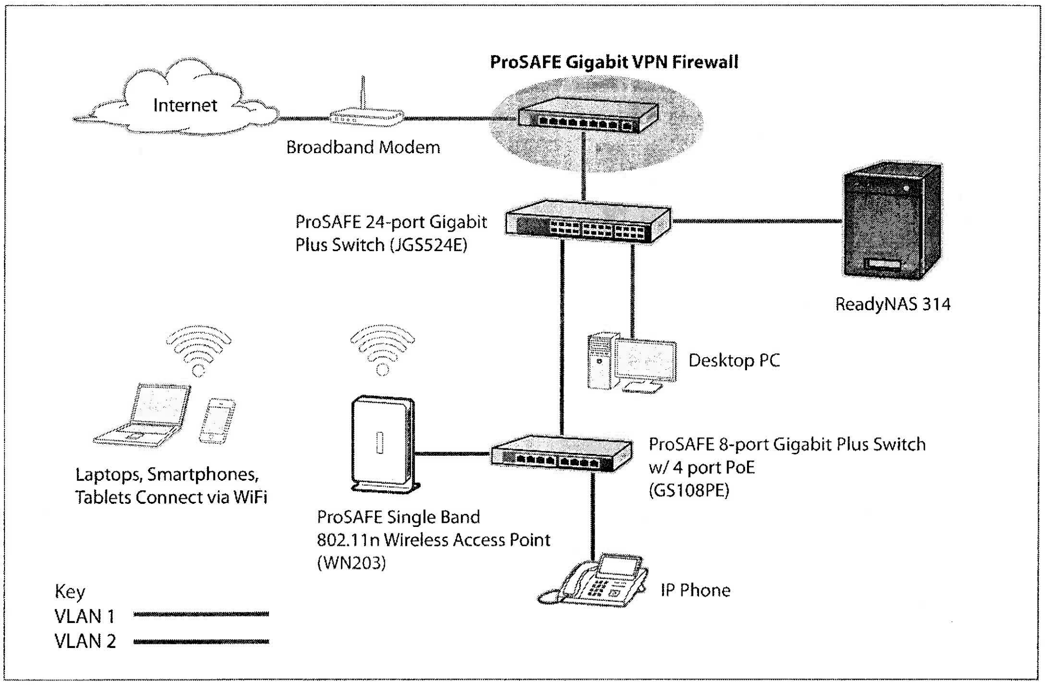
- Connect multiple broadband connections simultaneously
- 2 modes of session-based WAN load balancing
- WAN failover for maximum uptime

### Easy to use

- Auto Detect connects to your ISP quickly
- DHCP (client and server) for fast deployment
- Intuitive Web management GUI
- IPsec VPN Wizard allows for easy VPN setup
- SNMP, telnet management support
- SYSLOG and emailed logs enable thorough network monitoring

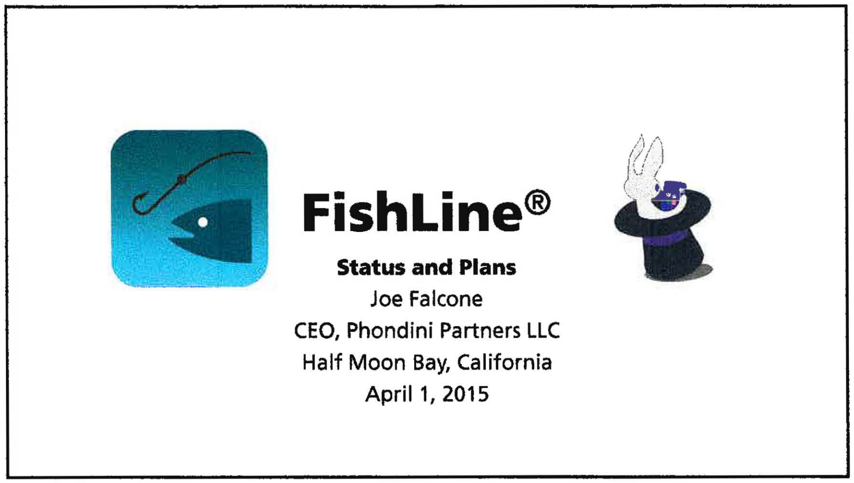
### Reliable NETGEAR Hardware

- Industry-grade metal casing
- High-quality electronics
- Lifetime Hardware Warranty
- Lifetime Technical Support
- Lifetime Next Business Day Replacement


ProSAFE Gigabit VPN Firewall
Internet
Broadband Modem
ProSAFE 24-port Gigabit Plus Switch (JGS524E)
ReadyNAS 314
Desktop PC
Laptops, Smartphones, Tablets Connect via WiFi
ProSAFE 8-port Gigabit Plus Switch w/ 4 port PoE (GS108PE)
ProSAFE Single Band 802.11n Wireless Access Point (WN203)
IP Phone
Key
VLAN 1
VLAN 2

*ProSAFE VPN Firewall Deployment Diagram*

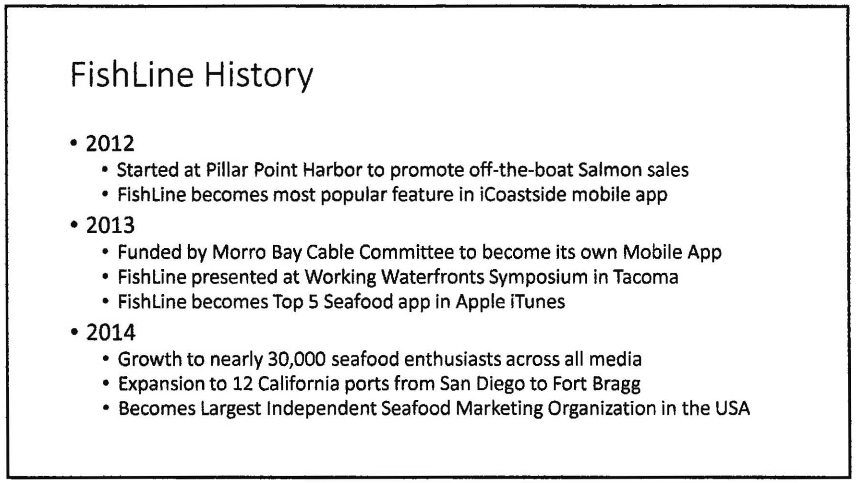
[1] On Supported Models



# FishLine®

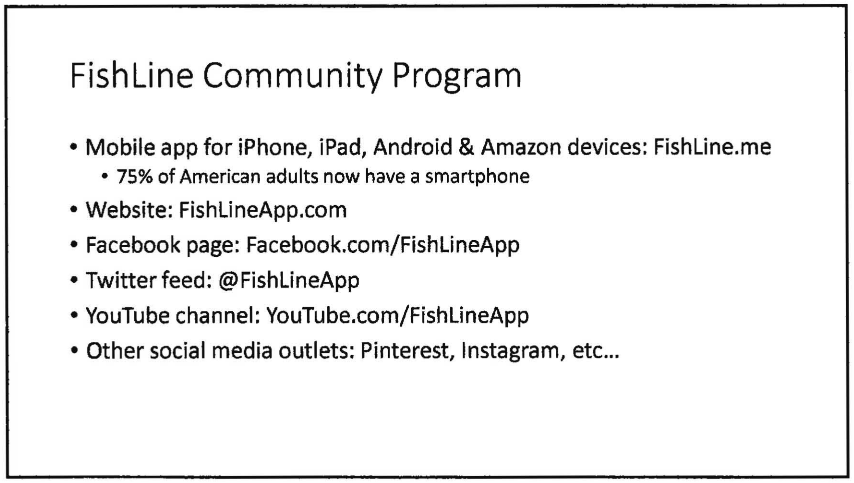
**Status and Plans**

Joe Falcone
CEO, Phondini Partners LLC
Half Moon Bay, California
April 1, 2015



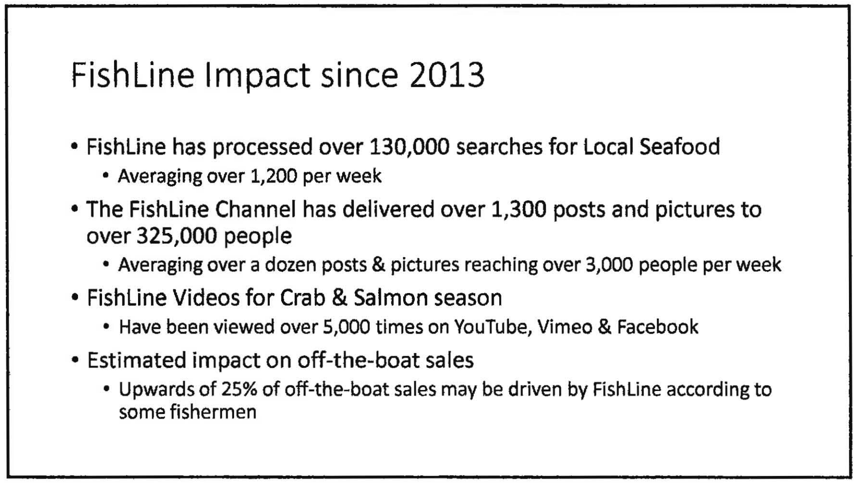
## FishLine History

- 2012
  - Started at Pillar Point Harbor to promote off-the-boat Salmon sales
  - FishLine becomes most popular feature in iCoastside mobile app
- 2013
  - Funded by Morro Bay Cable Committee to become its own Mobile App
  - FishLine presented at Working Waterfronts Symposium in Tacoma
  - FishLine becomes Top 5 Seafood app in Apple iTunes
- 2014
  - Growth to nearly 30,000 seafood enthusiasts across all media
  - Expansion to 12 California ports from San Diego to Fort Bragg
  - Becomes Largest Independent Seafood Marketing Organization in the USA



## FishLine Community Program

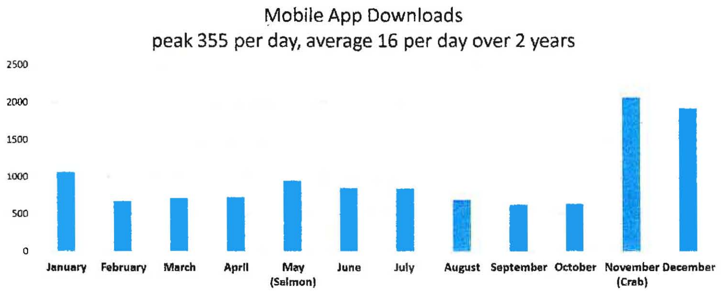
- Mobile app for iPhone, iPad, Android & Amazon devices: FishLine.me
  - 75% of American adults now have a smartphone
- Website: FishLineApp.com
- Facebook page: Facebook.com/FishLineApp
- Twitter feed: @FishLineApp
- YouTube channel: YouTube.com/FishLineApp
- Other social media outlets: Pinterest, Instagram, etc…



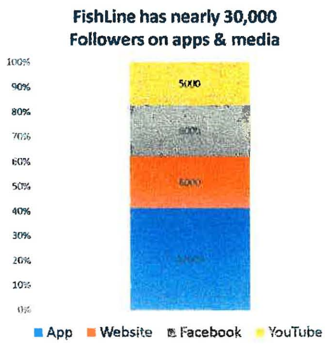
## FishLine Impact since 2013

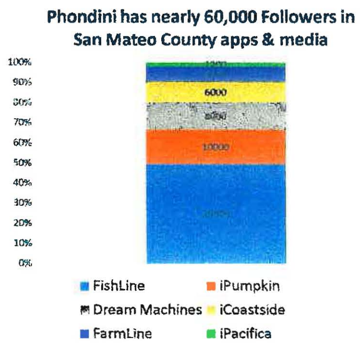
- FishLine has processed over 130,000 searches for Local Seafood
  - Averaging over 1,200 per week
- The FishLine Channel has delivered over 1,300 posts and pictures to over 325,000 people
  - Averaging over a dozen posts & pictures reaching over 3,000 people per week
- FishLine Videos for Crab & Salmon season
  - Have been viewed over 5,000 times on YouTube, Vimeo & Facebook
- Estimated impact on off-the-boat sales
  - Upwards of 25% of off-the-boat sales may be driven by FishLine according to some fishermen

## FishLine Seasons

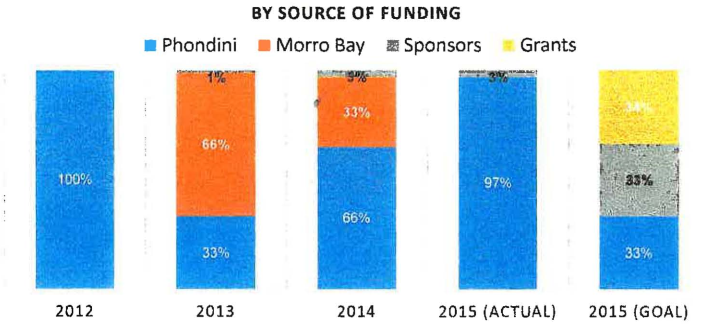


## FishLine & Phondini Media Followers



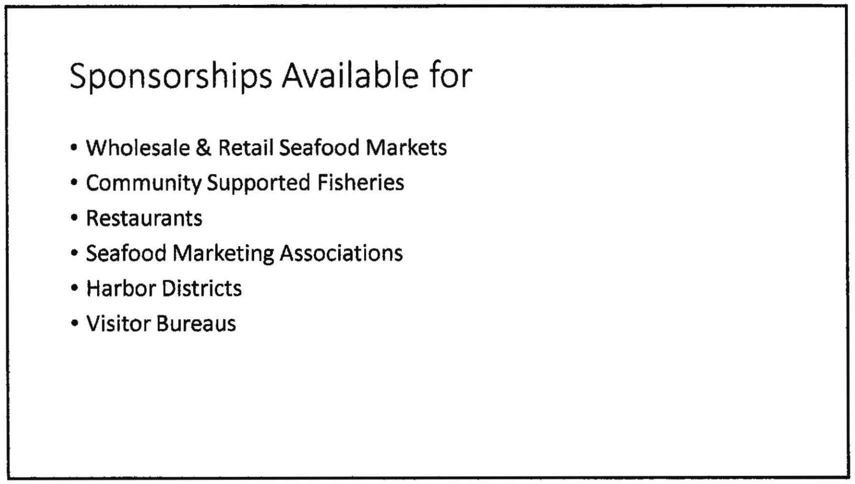


## Who Pays for FishLine?



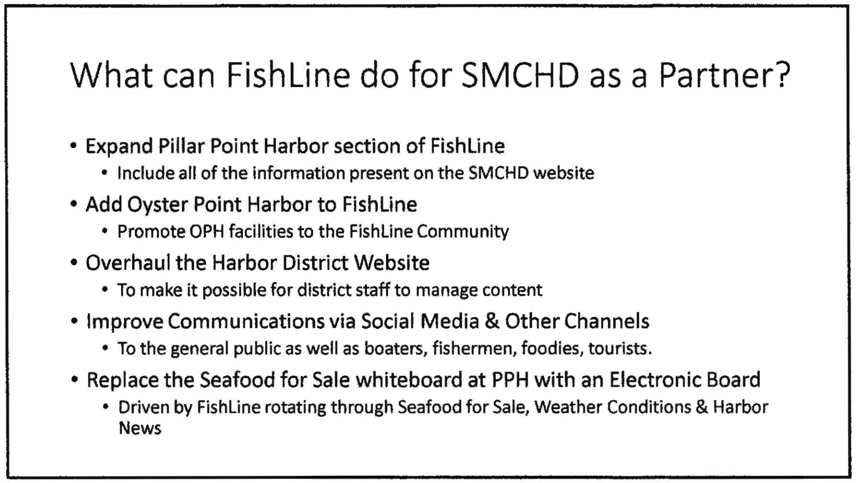
## Grants

- **National Fish and Wildlife Foundation – Fisheries Innovation Fund**
  - Electronic Monitoring and Reporting RFP
  - **Phondini is proposing to add Charter Boats & Sportfishing to FishLine**
  - Seeking Charter Boat & Sportfishing Partners for this Proposal
  - Would like "Letter of Support" from Harbor District
  - Deadline is April 13 (RFP went out March 24!)
- **Fish Locally Collaborative & Northwest Atlantic Marine Alliance**
  - Know Your Fisherman Nationwide Initiative RFQ
  - **Phondini is proposing to expand FishLine nationwide**
  - Drive content marketing & branding campaign to promote small-to-mid-scale domestic commercial fishermen and their catch
  - Phondini is a finalist.



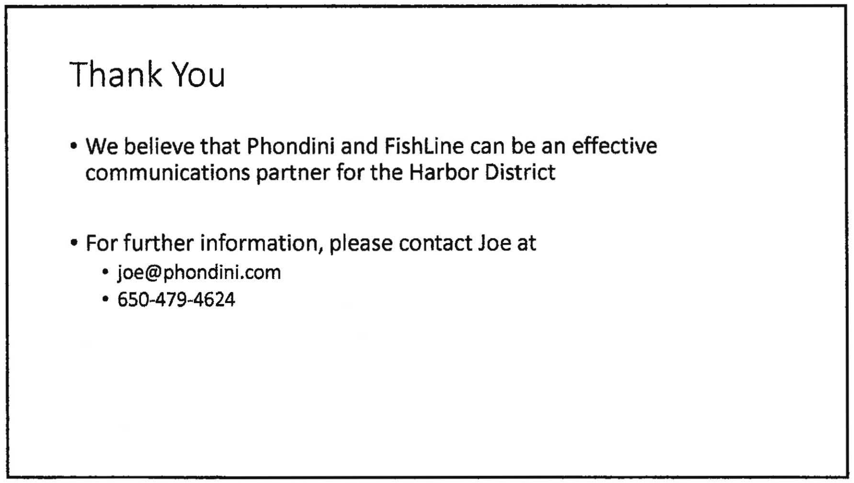
## Sponsorships Available for

- Wholesale & Retail Seafood Markets
- Community Supported Fisheries
- Restaurants
- Seafood Marketing Associations
- Harbor Districts
- Visitor Bureaus



## What can FishLine do for SMCHD as a Partner?

- Expand Pillar Point Harbor section of FishLine
  - Include all of the information present on the SMCHD website
- Add Oyster Point Harbor to FishLine
  - Promote OPH facilities to the FishLine Community
- Overhaul the Harbor District Website
  - To make it possible for district staff to manage content
- Improve Communications via Social Media & Other Channels
  - To the general public as well as boaters, fishermen, foodies, tourists.
- Replace the Seafood for Sale whiteboard at PPH with an Electronic Board
  - Driven by FishLine rotating through Seafood for Sale, Weather Conditions & Harbor News



## Thank You

- We believe that Phondini and FishLine can be an effective communications partner for the Harbor District

- For further information, please contact Joe at
  - joe@phondini.com
  - 650-479-4624