Sprawling enterprise applications and the broad, fast-changing attack surface of Web 2.0 call for a new approach to firewall security. First-generation firewalls were limited to port, protocol, and IP addresses. Today, Forcepoint high assurance firewalls let you confidently see and control new and existing applications for efficient, effective rules. And to detect complex threats within these applications, we integrate proactive threat intelligence with multiple inspection technologies in one cost-effective, easy-to-manage appliance.

Firewalls are traditionally only as strong or as weak as the policies you define. But effective security policies for today’s complex Web 2.0 traffic depend on fine-grained understanding that can be hard to come by. You need rapid insight that goes far beyond port and protocol to encompass different web applications and users and the sophisticated threats that target them.

Where in the past you could await signatures, the breakneck pace of threat evolution today demands proactive, predictive diagnosis of risk. Multiple attributes, such as source reputation, content, and behavior should be assessed to reveal malicious intent before a new threat is confirmed.

It’s not enough to predict the threat. Accurate, timely blocking demands concerted action that crosses conventional product silos. These demands — plus the call to prove compliance — increase the operational burden on the network team. Yet budgets remain under pressure. Something has to change.

THE BIGGEST FIREWALL INNOVATION IN 15 YEARS

With version 8 of the Forcepoint Firewall Enterprise, Forcepoint reinvents the firewall. Three innovations deliver unprecedented protection at an affordable price. We combine full application visibility and control, reputation-aware threat intelligence, and multivector attack protection to improve network security while shaving effort and expense. The firewall solution includes the Forcepoint Firewall Enterprise appliances and Forcepoint Firewall Enterprise Control Center centralized management.

Today, the weakest link in network security is the application layer. We have taken our proven, high-assurance firewall — trusted by ultrasecure environments all over the world — and have added broad application discovery and control. You can now protect new and existing Web 2.0 applications from the risks of data leakage, network abuse, and malicious attacks. With Forcepoint technology, you can ensure the applications using your network benefit your business.

Application Visibility

Forcepoint AppPrism technology allows you to identify all traffic and reveal the applications that are really in use, with helpful context such as source, bandwidth, and destination. By inspecting encrypted application-level traffic, you can eliminate loopholes favored by cyberthieves and attackers.

Application Control

Fine-grained control allows comprehensive enforcement of policy based on business needs. Instead of policies matched just to IP address, port, or protocol, you can now place a user name with a role and a set of applications.
FORCEPOINT FIREWALL ENTERPRISE FEATURES

Forcepoint AppPrism™ application visibility and control including:
- Packet, stateful, and full application filtering
- Full application visibility and control
- Multiple delivery options, including multi-firewall (one appliance managing up to 32 virtual firewalls), Forcepoint Firewall Enterprise for Crossbeam, and a virtual firewall appliance
- Network address translation [NAT] Forcepoint AppPrism categories
- Anonymizers/proxies
- Authentication services
- Business web applications
- Content management
- Commercial monitoring
- Database
- Directory services
- Email
- Encrypted tunnels
- Enterprise resource planning [ERP]/customer relationship management [CRM]
- File sharing
- Gaming
- Instant messaging
- Infrastructure services
- IT utilities
- Mobile software
- Peer-to-peer [P2P]
- Photo/video sharing
- Remote administration
- Remote desktop/terminal services
- Social networking
- Software/system updates
- Storage
- Streaming media
- Toolbars and PC utilities
- Voice over IP [VoIP]
- VPN
- Webmail
- Web browsing
- Web conferencing

Construct application usage rules that combine attributes such as:
- Business or recreational purpose
- User identity
- Embedded application control
- Whitelisting
- Geo-location

User Identity
Without visibility into and control over users and the context of their use, firewalls cannot defend against increasingly port-agile, evasive, targeted applications.

Forcepoint Firewall Enterprise applies user-aware rules and control over applications. When a user connects, the system validates entitlements in real time from your existing user directory. The firewall quickly applies policies mapped to user identity that grant explicit use of an application.

By tracking to the user, rules are granular enough for modern business operation. And identity-based rules make good operational sense. More and more enterprises rely heavily on unified use of user directories and identity management to support access controls. User changes happen once and propagate out. Security policies stay up to date as the user community changes.

Embedded Application Control
Embedded application control gives you the power to tailor rights within an application. For instance, you might allow Yahoo!, but block Yahoo! IM, or allow IM only for specific user groups, perhaps customer support or sales or locations, such as the head office.

You can also support appropriate corporate use and blackout policies by specifying when an application can or cannot be used. Rules could allow MySpace use during lunchtime, for example, for customer service teams, while financial applications are not available to anyone via VPN on weekends.

Many exploits try to benefit from the lax security in social networking sites by concealing their payloads within trendy applets. With Forcepoint, you can allow access to the beneficial elements of sites like Facebook, but still minimize the risk of compromised applications within each site.

Whitelisting
For advanced control, application whitelisting lets you explicitly allow only traffic from applications that have been approved as necessary or appropriate. Compared to lengthy blacklists, whitelisting whittles down the number of rules you need to write and maintain.
FORCEPOINT FIREWALL ENTERPRISE FEATURES CONT.

Authentication
- Local
- Microsoft Active Directory
- Transparent identities for Active Directory (Forcepoint logon collector)
- LDAP (Sun, Open LDAP, Custom LDAP)
- RADIUS
- Microsoft Windows domain authentication
- Microsoft Windows NTLM authentication
- Passport [single sign-on]
- Strong authentication (SecurID)
- Supports CAC authentication

High Availability
- Active/active
- Active/passive
- Stateful session failover
- Remote IP monitoring

Global Threat Intelligence
- Forcepoint Global Threat Intelligence™ network connection reputation
- Geo-location filtering
- Forcepoint Labs™

Encrypted Application Filtering
- SSH
- SFTP
- SCP
- Bidirectional HTTPS decryption and re-encryption

Intrusion Prevention System (IPS)
- More than 10,000 signatures
- Automatic signature updates
- Custom signatures
- Preconfigured signature groups

Anit-Virus and Anti-Spyware
- Protects against spyware, Trojans, and worms
- Heuristics
- Automatic signature updates

Geo-location
As botnets proliferate through popular social networking applications, it has become more important to be able to lock down rogue applications that attempt to communicate to certain locations. Geo-location lets you cut off this contact to keep your data from exfiltrating and prevent your systems from being used for mischief.

We give you this fine-grained control while making rules development less complex. In fact, there’s just one policy in one view. One straightforward console presents the options required to efficiently manage all rules and add defenses. This unified model is especially beneficial over time and across teams, as we also highlight rule interactions and overlaps. With colored fields highlighting potential conflicts, you avoid errors and enhance performance.

Protection
Forcepoint AppPrism helps you reduce risks from application-level threats while you optimize use of corporate bandwidth. Behind Forcepoint AppPrism stands the power of Forcepoint Labs™. Our threat researchers use threat research and intelligence data to continually recognize and assess risk for 31 categories of applications, ranging from anonymizers to video and photo sharing.

By assigning dynamic reputations for sites, senders, and locations, we can block an average 70 percent of undesirable traffic before you ever see it. Because of this capability, it can even spot the subtle command and control (C&C) channel of botnets.

THE ONLY FIREWALL WITH REPUTATION ANALYSIS AND GLOBAL THREAT INTELLIGENCE
Only Forcepoint includes reputation technology in a firewall, and it is just one element of Forcepoint Global Threat Intelligence™. At Forcepoint, more than 400 researchers collaborate across web, spam, vulnerability, host and network intrusion, malware, and regulatory compliance research. This breadth allows them to characterize every new threat and vulnerability.

Their efforts, informed by more than 100 million sensors around the world, deliver real-time predictive risk analysis to guard you against evolving multifaceted threats.

Unlike old-fashioned firewalls that rely on signatures, automated threat feeds from Forcepoint Labs keep you up to date without taking your firewall off-line. With the increase in advanced persistent threats like Operation Aurora, Forcepoint Global Threat Intelligence is the most sophisticated protection you can own, helping you mitigate vulnerabilities, avoid regulatory violations, and lower the cost of remediation.
Web Filtering
- Integrated Forcepoint URL filtering and management
- Block Java, Active-X, JavaScript, SOAP

Anti-Spam
- Forcepoint Global Threat Intelligence network connection reputation

VPN
- IKEv1 and IKEv2
- DES, 3DES, AES-128, and AES-256 encryption
- SHA-1 and MD5 authentication
- Diffie-Hellman groups 1, 2, and 5
- Policy-restricted tunnels
- NAT-T
- Xauth

FORCEPOINT SecurityOS® OPERATING SYSTEM

Features
- Forcepoint Type Enforcement® technology
- Preconfigured operating system (OS) security policy
- OS compartmentalization
- Network stack separation

Forcepoint Firewall Enterprise Control Center
- Windows graphical user interface
- Local console
- Full command line
- USB disaster recovery configuration backup and restore

Logging and Monitoring
- On-box logging
- Scheduled log archiving and exporting
- Forcepoint Firewall Enterprise log software extract format (SEF)
- Export formats (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP v1, v2c, and v3

MULTIVECTOR SECURITY IN ONE INTEGRATED APPLIANCE
One reason customers choose Forcepoint is our extensive security and compliance portfolio. Now, we place this might right at your door. Facing off against the complex threats in Web 2.0 applications, exploit cocktails, phishing, and targeted attacks, Forcepoint Firewall Enterprise now combines multiple crucial threat protections in every firewall appliance.

Before, firewalls were limited to access control and segmentation. Adequate protection required the expense of implementing and maintaining several separate products. Now, one appliance combines:
- Forcepoint AppPrism for full application discovery and control
- Intrusion prevention
- Global reputation analysis
- Industry-leading Forcepoint URL filtering
- Encrypted application filtering
- Antivirus, antispyware, and antispam

Our experience building multivector solutions has helped us deliver all these protections without compromising performance or productivity — and without adding to the cost.

FINE-GRAINED CONTROL MADE MANAGEABLE
Reliable security must also be easy to configure. The intuitive Forcepoint Firewall Enterprise administrative console lets your administrators create rules and selectively apply defenses such as application filters, IPS signatures, and URL filtering from a single screen. New software feature updates are delivered automatically via the Internet, reducing maintenance effort. Simply determine the schedule with a single click.

The Forcepoint Firewall Enterprise product line includes an additional tool for simplifying management. Sold separately, Forcepoint Firewall Enterprise Control Center offers centralized firewall policy management for multiple Forcepoint Firewall Enterprise appliances. It helps you maximize operational efficiency, simplify policy control, optimize rules, streamline software updates, and demonstrate regulatory compliance. You can even compare policy configurations on all of your Forcepoint Firewall Enterprise Control Center-managed devices to ensure consistency across your network. Robust configuration management lets you centrally track, trace, and validate all policy changes.

Furthermore, Forcepoint Firewall Enterprise Control Center integrates with Forcepoint ePolicy Orchestrator® (Forcepoint ePO™) software, providing visibility into firewall health data and reports.
Firewall Enterprise Appliance

Network and Routing
- IPv6 compliant
- Dynamic routing (RIP v1 and v2, OSPF, BGP, and PIM-SM)
- Static routes
- 802.1Q VLAN tagging
- DHCP client
- Default route failover
- QoS

Secure Servers
- Secure DNS (single or split)
- Secure sendmail (single or split)

Appliances and Hardware
- Upgrade warranty to four-hour response for most models
- Virtualization solutions available
- Single-, dual-, and quad-core processors
- ASIC-based acceleration
- RAID HDD configurations
- Redundant power supplies

Technical Support
- 24/7 telephone-based technical support
- 24/7 technical support with web-based ticketing and knowledgebase

FORCEPOINT FIREWALL ENTERPRISE PRODUCT LINE
The Firewall Enterprise product line includes appliances appropriate for businesses of all sizes, as well as companion products, such as Forcepoint Firewall Enterprise Control Center. Our Control Center and Firewall Enterprise appliances work together to streamline management activities and reduce operational costs. Flexible hybrid delivery options include physical appliances, multi-firewall appliances, and virtual appliances. Carrier-class security performance with speeds up to 40 Gbps is delivered by our Forcepoint Firewall Enterprise for Crossbeam solution running on Crossbeam’s X-Series hardware. Ask your sales representative for more information.

THE MOST SECURE FIREWALL HARDWARE PLATFORM
At its core, Forcepoint Firewall Enterprise runs on the high-speed, high-assurance Forcepoint SecureOS operating system. Patented Forcepoint Type Enforcement technology secures the OS itself for an unparalleled level of platform security. Perhaps it is why Forcepoint SecureOS has an unparalleled CERT advisory record: no emergency security patches have ever been required.

The preconfigured operating system security policy prevents compromises, and the entire operating system is compartmentalized so attackers cannot disrupt its work.

These extra steps allowed us to be the first firewall to achieve Common Criteria EAL 4+ certification with US DoD Protection Profile compliance.

Because of our innovation and advanced security, the Forcepoint Firewall Enterprise protects 15,000 networks around the world, including thousands of government agencies, Fortune 500 organizations, and seven of the top 10 financial institutions. Put Forcepoint to work protecting you.
<table>
<thead>
<tr>
<th>HARDWARE SPECS(^1)</th>
<th>S1104</th>
<th>S2008</th>
<th>S3008</th>
<th>S4016</th>
<th>S5032</th>
<th>S6032</th>
<th>S7032-XX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>Small 1U</td>
<td>1U</td>
<td>1U</td>
<td>Enterprise 1U</td>
<td>Enterprise 2U</td>
<td>Enterprise 2U</td>
<td>Enterprise 2U</td>
</tr>
<tr>
<td>Unlimited User Licenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Recommended Users</td>
<td>200</td>
<td>300</td>
<td>600</td>
<td>Medium–Large(^1)</td>
<td>Medium–Large(^1)</td>
<td>Large(^2)</td>
<td>Large(^3)</td>
</tr>
<tr>
<td>RAID</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Network Modules</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2(^5)</td>
</tr>
<tr>
<td>1 Gb Copper Interfaces</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>8/16</td>
<td>8/32</td>
<td>8/32</td>
<td>8/16(^6)</td>
</tr>
<tr>
<td>1 Gb Fiber Interface Option</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>8</td>
<td>24</td>
<td>24</td>
<td>8(^7)</td>
</tr>
<tr>
<td>10 Gb Fiber Interface Option</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>6</td>
<td>18</td>
<td>18</td>
<td>4(^8)</td>
</tr>
<tr>
<td>Encrypted Filtering Acceleration</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Integrated</td>
<td>Integrated</td>
<td>Integrated</td>
<td>N/A</td>
</tr>
<tr>
<td>Out-of-Band Management</td>
<td>Serial Console Only</td>
<td>Serial Console Only</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**PERFORMANCE\(^1\)**

<table>
<thead>
<tr>
<th>Firewall Performance (maximum)(^2)</th>
<th>750 Mbps</th>
<th>2.0 Gbps</th>
<th>4.0 Gbps</th>
<th>9.0 Gbps</th>
<th>12.0 Gbps</th>
<th>15.0 Gbps</th>
<th>12.0 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Prevention(^3)</td>
<td>250 Mbps</td>
<td>1.0 Gbps</td>
<td>2.0 Gbps</td>
<td>3.0 Gbps</td>
<td>5.0 Gbps</td>
<td>6.0 Gbps</td>
<td>5.0 Gbps</td>
</tr>
<tr>
<td>Forcepoint AppPrism(^2)</td>
<td>250 Mbps</td>
<td>1.0 Gbps</td>
<td>2.0 Gbps</td>
<td>7.5 Gbps</td>
<td>10.0 Gbps</td>
<td>12.0 Gbps</td>
<td>10.0 Gbps</td>
</tr>
<tr>
<td>Concurrent Sessions(^2)</td>
<td>200,000</td>
<td>500,000</td>
<td>750,000</td>
<td>1,500,000</td>
<td>3,000,000</td>
<td>4,000,000</td>
<td>3,000,000</td>
</tr>
<tr>
<td>New Sessions per Second(^4)</td>
<td>5,000</td>
<td>15,000</td>
<td>20,000</td>
<td>35,000</td>
<td>50,000</td>
<td>70,000</td>
<td>50,000</td>
</tr>
<tr>
<td>IPsec VPN Throughout [AES](^3)</td>
<td>60 Mbps</td>
<td>250 Mbps</td>
<td>350 Mbps</td>
<td>400 Mbps</td>
<td>450 Mbps</td>
<td>500 Mbps</td>
<td>450 Mbps</td>
</tr>
<tr>
<td>IPsec VPN Maximum Number of Tunnels(^3)</td>
<td>250</td>
<td>1,000</td>
<td>2,000</td>
<td>4,000</td>
<td>8,000</td>
<td>10,000</td>
<td>8,000</td>
</tr>
</tbody>
</table>
### Dimensions, Weight, Environmental

<table>
<thead>
<tr>
<th></th>
<th>Width</th>
<th>Depth</th>
<th>Height</th>
<th>Weight</th>
<th>Power Supply Details</th>
<th>Operating Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16.9 in</td>
<td>8.5 in</td>
<td>1.7 in</td>
<td>10.93 lbs</td>
<td>100 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>42.93 cm</td>
<td>21.59 cm</td>
<td>4.32 cm</td>
<td>4.96 kg</td>
<td>350 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>16.9 in</td>
<td>28.0 in</td>
<td>1.7 in</td>
<td>25 lbs</td>
<td>Dual 400 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>42.93 cm</td>
<td>71.12 cm</td>
<td>4.32 cm</td>
<td>11.34 kg</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>16.9 in</td>
<td>28.0 in</td>
<td>1.7 in</td>
<td>25 lbs</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>42.93 cm</td>
<td>71.12 cm</td>
<td>4.32 cm</td>
<td>11.34 kg</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>17.2 in</td>
<td>24.4 in</td>
<td>1.7 in</td>
<td>22 lbs</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>43.8 cm</td>
<td>61.87 cm</td>
<td>4.32 cm</td>
<td>9.98 kg</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>18.9 in</td>
<td>30.0 in</td>
<td>3.4 in</td>
<td>40 lbs</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
<tr>
<td></td>
<td>48.04 cm</td>
<td>76.21 cm</td>
<td>8.71 cm</td>
<td>18.14 kg</td>
<td>Dual 750 W 110/220 V</td>
<td>10° C–35° C 50° F–95° F</td>
</tr>
</tbody>
</table>

1. All specification and performance results are based on the S series of appliances.
2. Version 8 performance data represents the maximum capabilities of the systems as measured under optimal testing conditions. Deployment and policy considerations may impact performance results.
3. Please contact your Forcepoint representative to determine proper sizing for your needs.
4. Maximum of two network modules supported (of any type), maximum of one 10 Gb network module supported (with a maximum of four transceivers populated).