

TrafficShield

Application Firewall

TrafficShield® is a web application firewall that provides comprehensive, proactive, network and application-layer protection from generalized and targeted attacks by understanding the user interaction with the application firewall. TrafficShield employs a positive security model ('deny all unless allowed') to permit only valid and authorized application transactions, while automatically protecting critical web applications from attacks such as Google hacking, cross-site scripting, and parameter tampering.

Key Benefits

Comprehensive Web Application Security – Protects against entire classes of HTTP and HTTPS-based threats (both known and unknown) rather than guarding against a limited list of known attacks.

Hardened Appliance Protection – Protects servers from attacks and ensures that only valid responses get through.

Targeted Attack Protection – Protects scanners and other automated devices that can't defend themselves against targeted attacks because these attacks involve a malicious user seeking vulnerabilities unique to a particular session. TrafficShield detects and mitigates pattern-less exploits in real time, adding complementary protection to existing firewalls and Intrusion Detection Systems, which cannot efficiently address HTTP and HTTPS-borne threats.

Random Attack Protection – Application layer packet inspection and behavioral logic protect against counterfeit application activity, providing precise attack mitigation and granular blocking against script kiddies, known worms and vulnerabilities, requests for restricted object and file types, and other known exploits.

Security Policy Management – Automatically generates and enforces application security policies that are easy to manage, intuitive, and incredibly accurate.

Comprehensive Network Security Services – Provides a secure reverse proxy, including SSL acceleration, termination, and re-encryption to web servers, key management and failover handling, and basic network firewalling capabilities.

Web Server Protection – Hides your web infrastructure so that hackers can't tell what servers you're running. Strips out identifying operating system and web server information from message headers, conceals any HTTP error messages from users, and removes application error messages from pages sent to users while checking to make sure no server code leaks out onto web pages.

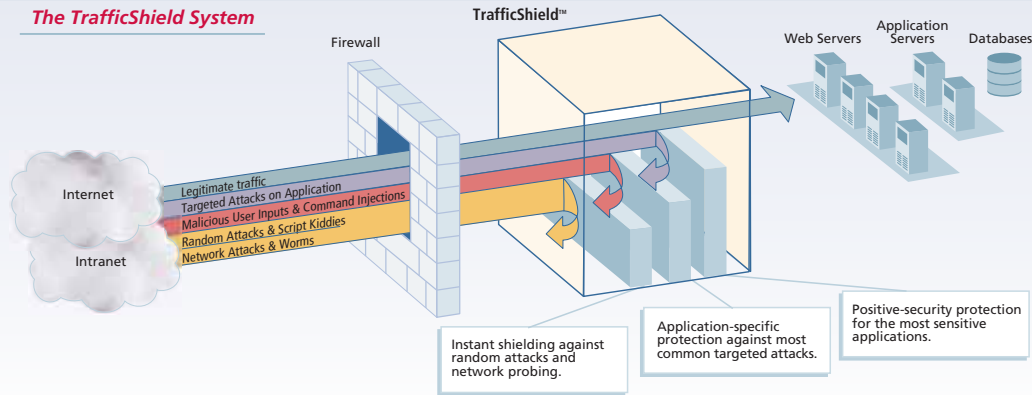
VLAN support – Delivers maximum flexibility for easier deployments.

Total Protection

TrafficShield protects against application, infrastructure, and network threats such as:

- SQL Injection
- Command Injection
- Buffer Overflow
- Google Hacking (Forceful Browsing)
- Application Platform Exploits
- Cross-Site Scripting
- Cookie/Session Poisoning
- Parameter/Form Tampering
- Error Message Interception
- Zero Day Attacks

The TrafficShield System



Based On The Powerful TMOS Architecture

Integrated with F5's powerful TMOS operating system, TrafficShield can now leverage many of the pre-existing capabilities of TMOS, including:

- **SSL Acceleration**
SSL key exchanges, certificate management and AES encryption are processed through the TMOS architecture while extending the capability of TrafficShield.
- **iRules**
A scripting language that gives IT professionals unparalleled application awareness and network control.
- **Network Administration**
TMOS enables TrafficShield to configure and manage network level functionality such as VLANs, failover and routing.
- **Client Authentication**
LDAP, RADIUS, TACACS+, Client Certificate-based LDAP and OSCP authentication profile types are now supported on TrafficShield.
- **Packet Filtering**
Enables TrafficShield to identify and filter traffic at the packet level, providing exhaustive security at both the network and application layers.
- **TCP Stack Optimization**
With TrafficShield on TMOS, end users can also enjoy the advantages of F5's highly optimized TCP stack, reducing the effects of chattiness, congestion, and packet loss recovery.

Positive Security Protects Against Targeted Attacks

Scanners and other automated devices can't defend against targeted attacks because these attacks involve a malicious user seeking vulnerabilities unique to a particular application. Only an application-specific security policy can protect against this type of threat. TrafficShield's purpose-built hardware and patent-pending software detect and mitigate patternless exploits in real time, adding accurate,

complementary protection to existing firewalls and Intrusion Detection Systems (IDS), which cannot address HTTP and HTTPS-borne threats efficiently.

Comprehensive Network Security Services

TrafficShield provides a secure reverse proxy, including SSL acceleration, termination and re-encryption to web servers, key management and failover handling, and basic network firewalling capabilities.

Web Server Protection (Cloaking)

TrafficShield hides your web infrastructure so that hackers can't tell what servers you're running. It strips out identifying OS and web server information from message headers, conceals any HTTP error messages from users and removes application error messages from pages sent to users, and checks to make sure no server code leaks out onto web pages.

F5 Application Traffic Management

TrafficShield is complementary to F5's FirePass SSL VPN Remote Access and BIG-IP Traffic Management product lines. As FirePass secures user-to-application access, the TrafficShield product ensures that only valid traffic reaches the application. Combine with F5's BIG-IP for a powerful, holistic approach to the secure and optimized delivery of your applications.

Flexible Deployment Options

TrafficShield can be deployed in a variety of security postures depending on customer needs. A standard implementation can take less than a day and provides protection against the most common application attacks. Our optional 'Advanced Policy Customization' module allows customers to fully tailor their policy as required, providing the most granular protection in the industry.

Availability

TrafficShield is available as a stand alone solution on TMOS, or through the BIG-IP® Application Security Module (ASM), which is a software solution that runs on the BIG-IP v9 system. Please contact your F5 representative for more details.



Specifications

Supported Content:

HTML 4.0
Client side scripting (JavaScript, VBScript, etc.)
Dynamic content
Single-object applications
Rich media content (Flash, Shockwave, Applets, etc.)

Compatibility:

All major servers (Netscape, IIS, Apache, etc.)
All major browsers (Netscape, Internet Explorer, etc.)
Any application server (Sun, Oracle, IBM, etc.)
All major load balancers

Supported Protocols:

HTTP 1.0 and HTTP 1.1
HTTPS

Management Interfaces:

Command Line Interface (CLI) – for initial configuration
Web based (SSL) – advanced configuration, control and monitoring
SNMP traps
Syslog
OPSEC

Weight:

~36 lbs.

Dimensions:

17.5" w x 24.5" (OAL)/23.5" behind mounting ears x 3.5"

Power Supply:

400W with redundant option



F5 Networks, Inc. Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks Asia-Pacific

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd Europe/Middle-East/Africa

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeinfo@f5.com

F5 Networks Japan K.K.

+81-3-5447-3350 Voice
+81-3-5447-3351 Fax
info@f5networks.co.jp