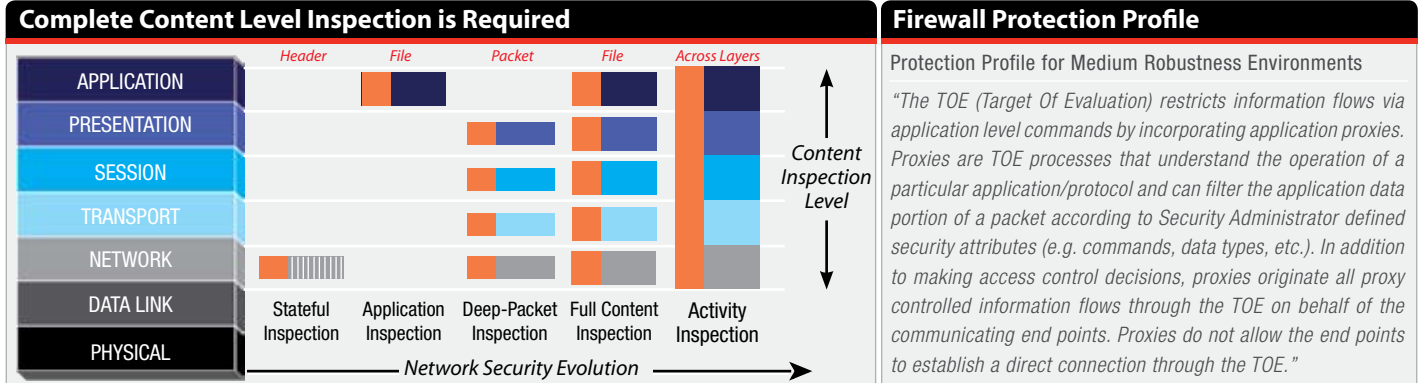


FortiGate[®] Application Proxy Firewalls

**Complete Security
for Federal Systems**

A New Security Environment – New Security Requirements

Security threats to networks and computing resources have evolved into sophisticated multi-vectored attacks. Proxy firewalls provide the advantages of restricting information flows at the application level and the benefit of better security by not allowing end points to establish direct connections. However single-focused security techniques such as stateful inspection, deep-packet inspection or traditional proxy firewalls no longer provide adequate protection to meet the requirements of the latest U.S. Government security mandates and provide protection from multi-vectored attacks.



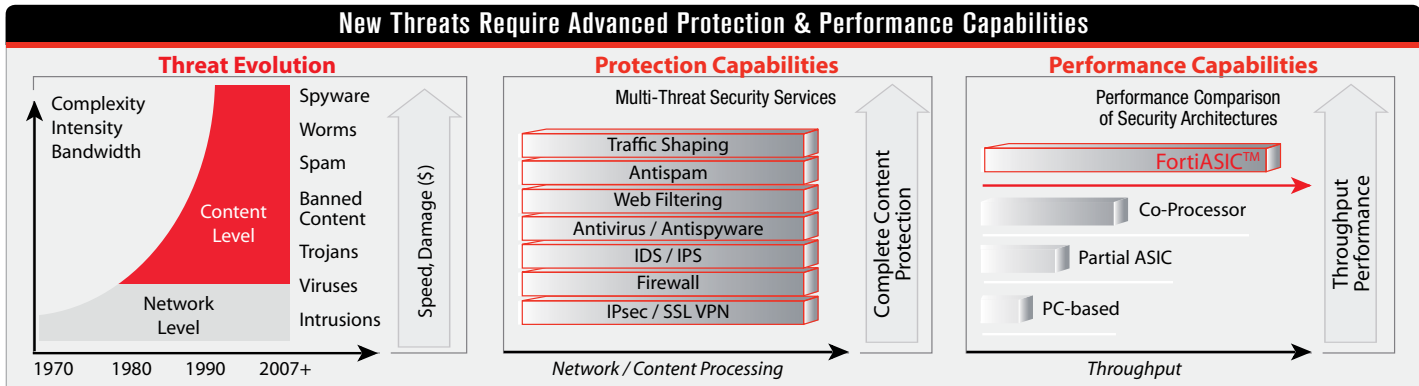
Firewall Protection Profile

Protection Profile for Medium Robustness Environments

"The TOE (Target Of Evaluation) restricts information flows via application level commands by incorporating application proxies. Proxies are TOE processes that understand the operation of a particular application/protocol and can filter the application data portion of a packet according to Security Administrator defined security attributes (e.g. commands, data types, etc.). In addition to making access control decisions, proxies originate all proxy controlled information flows through the TOE on behalf of the communicating end points. Proxies do not allow the end points to establish a direct connection through the TOE."

New Threats are Driving New Security Requirements

New threats warrant new protection methodologies that provide multi-layered security services and complete content level protection to meet the requirements of the latest U.S. Government Common Criteria Firewall Protection Profile. Furthermore as network traffic continues to grow in volume protection must cost-effectively scale to higher levels of throughput without compromising security defenses or network performance.



Fortinet Next-Generation Application Proxy Firewalls

FortiGate security systems operate as a hybrid stateful and proxy firewall, leveraging the benefits of both, to provide a complete Unified Threat Management (UTM) solution. A purpose-built security operating system provides multi-layered security services powered by a hardware platform with ASIC-based acceleration that delivers unprecedented levels of performance.

FortiGate is the only application-level firewall that meets the current CCEVS Criteria

FortiGate products have achieved impartial and independent validation at the EAL 4+ level of the Common Criteria Evaluation and Validation Scheme (CCEVS) Scheme.

FortiGate is currently under evaluation for conformance with the latest Medium Robustness Protection Profile for both traffic-filter firewall and for application-level firewalls:

- ✓ U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, January 09, 2006 (PP_FW_TF_MR2.0_V1.1)
- ✓ U.S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0, October 28, 2003. (PP_FW_MR2.0_V1.0)



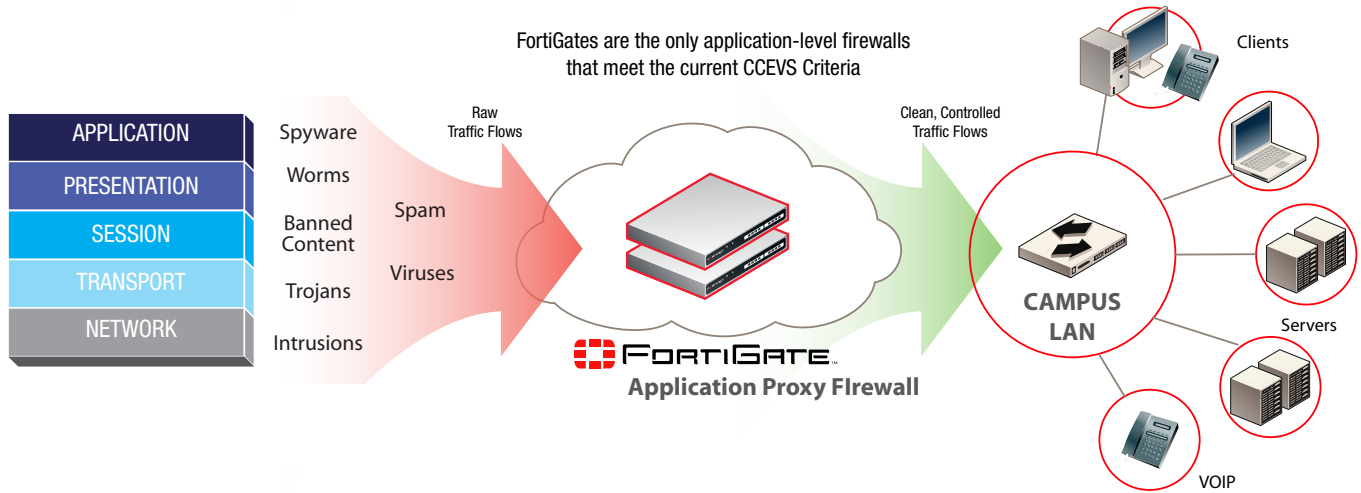
FortiGate Application Proxy Firewalls

FortiGate platforms are based on an integrated hardware and software architecture specifically designed for high-performance, application-level content processing. FortiOS™ Security Services can be selectively enabled to provide a unique set of services or a full suite of UTM security services all within a single application proxy enabled platform. FortiOS Security Services include firewall, IPsec and SSL VPNs, Intrusion Prevention System (IPS), antivirus, antispam, antispyware, and Web filtering. Unlike traditional firewalls and proxy devices that operate on individual packets, FortiGate complete content reassembly and inspection provides advanced protection. Entire traffic flows are examined to provide unparalleled scanning, detection and protection from even the most sophisticated blended threats. The Fortinet FortiASIC™ family of processors are purpose-built Application Specific Integrated Circuits (ASIC) that deliver the high-performance network and content processing required to provide this sophisticated level of security without impact to network or application performance. The FortiGuard® Network provides dynamic updates to ensure system software and security services such as antivirus/antispyware, antispam, Web filtering, and intrusion prevention software are always up to date.



FortiGate Application Proxy Firewalls in the Network

Granular security policies can be defined to provide complete content-level inspection and multi-layered security protection to ensure clean controlled information and traffic flows that meet the requirements of the latest U.S. Government Common Criteria Firewall Protection Profile.



"Fortinet's defining difference from its competitors is the architecture of its UTM appliances. UTMs typically include a stateful inspection firewall, intrusion prevention/detection systems, antimalware (antivirus, antispyware, antispam), and content filtering and VPN (IPsec and SSL). Fortinet built its own antimalware software, and its ASIC-based hardware provides the power to ensure efficient inline traffic scanning. Most other UTM vendors must partner with antivirus companies for their scanners, and the process power is based more on piled-on memory."

— Lawrence Walsh, Editor VARBusiness & GovernmentVAR Magazine
(Jan 2007, www.crn.com)



FORTINET™

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
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel: +65-6513-3730
Fax: +65-6223-6784