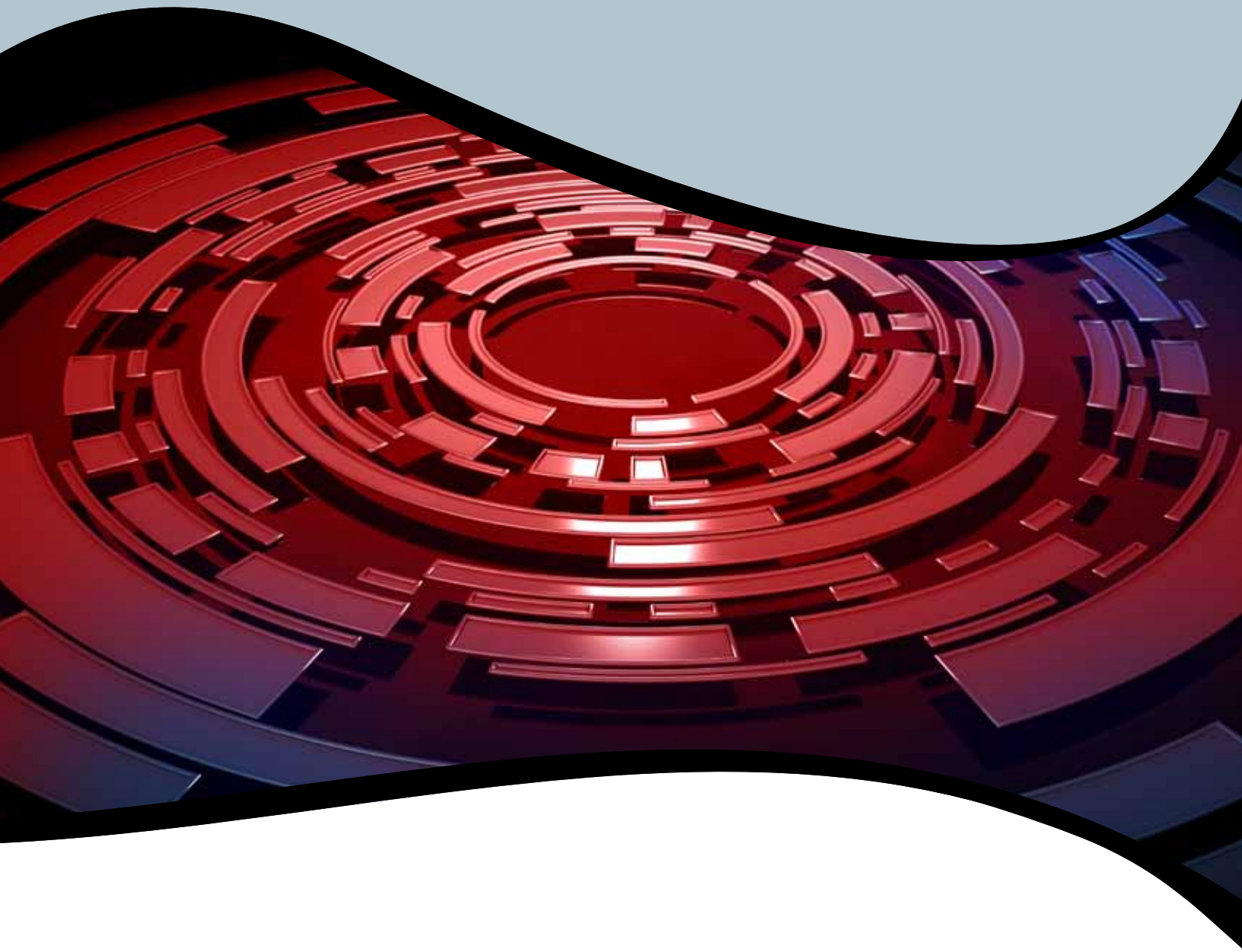
Tools

Information Assurance Tools Report

Seventh Edition

May 2, 2011

Firewalls



IATAC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-02-2011	Report	05-02-2011

4. TITLE AND SUBTITLE

Information Assurance Tools Report – Firewalls. Seventh Edition

5a. CONTRACT NUMBER
SPO700-98-D-4002-0380

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Revision by Karen Mercedes Goertzel

5d. PROJECT NUMBER

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
13200 Woodland Park Road
Herndon, VA 20171

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
A/ Distribution Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102

14. ABSTRACT

This Information Assurance Technology Analysis Center (IATAC) report provides an index of firewall tools. It summarizes pertinent information, providing users a brief description of available firewall tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and Common Criteria Evaluation Report contents and are intended only to highlight the capabilities and features of each firewall product.

15. SUBJECT TERMS
IATAC Collection, Firewall

16. SECURITY CLASSIFICATION OF:			***17. LIMITATION OF ABSTRACT***	***18. NUMBER OF PAGES***	***19a. NAME OF RESPONSIBLE PERSON***
					Tyler, Gene
a. REPORT	***b. ABSTRACT***	***c. THIS PAGE***	None	205	**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			703-984-0775

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Table of Contents

FORWARD

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with emerging scientific and technical information to support Information Assurance (IA), cyber security, and defensive information operations. IATAC is one of ten Information Analysis Centers (IAC) sponsored by DoD and managed by the Defense Technical Information Center (DTIC). IACs are formal organizations chartered by DoD to facilitate the use of existing scientific and technical information. Scientists, engineers, and information specialists staff each IAC. IACs establish and maintain comprehensive knowledge bases that include historical, technical, scientific, and other data and information, which are collected worldwide. Information collections span a wide range of unclassified, limited-distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques, including databases, models, and simulations.

IATAC's mission is to provide DoD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems, and information technology. Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As an IAC, IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities (*e.g.,* the *IAnewsletter, IA Digest, Cyber Events Calendar,* and *IA Research Update*); and publishing State-of-the-Art Reports, Critical Review and Technology Assessments, and IA Tools Reports.

The IA Tools Database is one of the knowledge bases maintained by IATAC. This knowledge base contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and antimalware tools. Information for the IA Tools Database is obtained from information available *via* open-source methods, including direct interface with various agencies, organizations, and vendors. Periodically, IATAC publishes a Tools Report to summarize and elucidate a particular subset of the tools information in the IATAC IA Tools Database that addresses a specific IA or cyber security challenge. To ensure applicability to Warfighter and Research and Development Community (Program Executive Officer/ Program Manager) needs, the topic areas for Tools Reports are solicited from the DoD IA/cyber community or based on IATAC's careful ongoing observation and analysis of the IA and cyber security tools and technologies about which that community expresses a high level of interest.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773

Email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*
SIPRNET: *https://iatac.dtic.smil.mil*

SECTION 1 ▸ Introduction

1.1 Purpose

This report provides an index of firewall tools, which are also described in the IATAC Firewalls Tools Database. Firewall tools are constantly being added to the inventory to counter new threats. The tools listed in this Report were reviewed during the period 2 February – 2 May 2011 and represents a best effort to capture all/relevant tools and corresponding information. For this report, a firewall is defined as a component or set of components that restricts access between a protected network and an unprotected network (*e.g.,* the Internet) or other sets of networks while, at the same time, it facilitates authorized access to protected network resources through proxies, filters, and other mechanisms.

This report summarizes pertinent information, providing users a brief description of available firewall tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and are intended only to highlight the capabilities and features of each firewall product. These descriptions do not represent IATAC's opinion. It is up to readers of this document to assess which product, if any, might best meet their security needs; however, the report does identify sources of product evaluations when available.

1.2 Organization

This report is organized into 5 distinct sections and one appendix as follows:

Section 1	Purpose, organization, and scope of the report
Section 2	General overview of firewalls—including a definition of what a firewall is, explanations of the various types of firewalls in existence, and discussions of how each type works
Section 3	Listing, with brief descriptions, of all available commercial and open source firewalls that could be discovered by the Report authors
Section 4	Listing of all available personal firewalls (commercial and open source) discoverable by the authors, together with information about their origins, licenses, host operating systems, and universal resource locators (URLs) to further Web-based information about them
Section 5	List of resources that provide more detailed information about specific topics touched on in this Report
Appendix	Amplifications of acronyms and abbreviations, and definitions of key terms, used in this Report

As a living document, this report will be updated periodically in digital form. It is available for download from the IATAC Web site *http://iac.dtic.mil/iatac*. Technical inquiries concerning this report may be addressed to IATAC at 703/984-0775 or via email to *iatac@dtic.mil*.

1.3 Scope

This report addresses all types of firewalls as defined and described in Section 2.1. The Report's authors recognize that a number of products being marketed as "firewalls" do not conform with this Report's definition of a firewall, but are very likely to fall into one of the categories of security applications described below; such products are not included in the listings in Section 3 or 4. Other products, though they may not be called firewalls, conform to this Report's definition of a firewall; such products are included in either Section 3 or 4 as appropriate.

This Report excludes discussions of non-firewall security applications that are designed to run in/on/as "boundary devices", except to note when such applications are integrated with a particular firewall in the same software package and co-hosted on the physical server or appliance. Such excluded applications include:

- Virtual private network (VPN) servers or gateways
- Authentication servers (including single sign-on [SSO] servers)
- Data loss prevention systems
- Intrusion detection systems (IDS) or intrusion prevention systems (IPS)—while the latter are similar to firewalls in operation, the technology evolved by extending IDS functionality to include attack blocking logic. For this reason IPS will be covered in the update of the IDS Tools Report
- Antivirus/antimalware servers/appliances—these were addressed in the 2009 Malware Tools Report
- Antispam/antiphishing servers/appliances

Also excluded from this Report are discussions of:

- Standalone proxy servers, as these are often used for purposes other than firewalling. If a proxy server is a component of a specific firewall, that fact will be mentioned in the firewall's description in Section 3.
- Policy definition and configuration scripts for iptables, Netfilter, and/or Squid, or other firewalls, as well as other kinds of utilities, toolkits, toolsets, or functional extensions to existing firewalls. While such tools add functionality to firewalls, they are not firewalls themselves, and are thus excluded from this Report.
- Open source firewalls for which no information or documentation was discoverable.
- Descriptions of personal firewalls. Such firewalls are listed in Section 4, with Universal Resource Locators (URLs) of Web pages containing information about them, but they are not described in the way that non-personal firewalls are in Section 3. Admittedly, this exclusion was somewhat arbitrary, and inspired by the concern so many new firewalls of all types have emerged, and others have been discovered since the last update of this Report and the list is changing on an almost daily basis. The authors believe that the Report will be more useful to the reader if it concentrates on firewalls that are intended to protect more than one single-user system. Section 4 does, however, provide extensive listings of desktop and mobile device firewalls and including information on their suppliers' nations of operation, the operating systems on which they are designed to run, and their licensing arrangements.

1.4 Assumptions

This report was written with a presumption that the reader would already possess an understanding of computing, information technology, and networking concepts and terms, such as "Transport Control Protocol/Internet Protocol (TCP/IP)" and other network protocols, "Open Systems Interconnect (OSI)", "application layer/layer 7", "modem", "network address translation (NAT)", "router", "packet", "demilitarized zone (DMZ)", "gateway", "boundary", "proxy", "agent", "virtual machine", "redundancy", *etc.*, as well as basic computer and network security, information assurance, and cybersecurity concepts and terms, such as "VPN", "tunnel", "cryptographic", "denial of service", "blacklist/whitelist", "spoofing", "malware", "spam", "hardened operating system", "access control", "availability", "authentication", "single sign-on", *etc.* A few primer-type resources are suggested for those readers who wish to familiarize themselves with the essentials before reading this document:

- The NetBSD Guide—Chapter 23, "Introduction to TCP/IP Networking". *http://www.netbsd.org/docs/guide/en/chap-net-intro.html*
- United States Computer Emergency Readiness Team (US-CERT). Why is Cyber Security a Problem? (National Cyber Alert System Cyber Security Tip ST04-001). *http://www.us-cert.gov/cas/tips/ST04-001.html*
- The glossary in Appendix A provides definitions of firewall-specific terms. For broader computing and networking terms, and for general information assurance and cybersecurity terms, the reader is encouraged to consult the following resources:
  - International Foundation for Information Technology. Glossary of Information Technology (IT) Terms and Phrases. *http://if4it.org/glossary.html*

- American National Standards Institute Alliance for Telecommunications Industry Solutions ATIS Telecom Glossary 2007. *http://www.atis.org/glossary*
- Navy/Marine Corps Intranet. NMCI Dictionary. *http://www.cnic.navy.mil/navycni/groups/public/@pub/@hq/documents/document/cnicd_a064707.pdf*
- World Wide Web Consortium. Web Services Glossary. *http://www.w3.org/TR/ws-gloss*
- National Institute of Standards and Technology (NIST). Glossary of Key Information Security Terms, NIST IR 7298 Revision 1, February 2011. *http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf*
- Committee for National Security Systems. National Information Assurance (IA) Glossary. *http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf*
- US-CERT. IT Security Essential Body of Knowledge (EBK) Glossary of Terms. *http://www.us-cert.gov/ITSecurityEBK/EBKGlossary08.pdf*
- Internet Engineering Task Force. Internet Security Glossary, Version 2 (Request for Comments 4949). *http://www.ietf.org/rfc/rfc4949.txt*

SECTION 2 ▸ Firewall Overview

2.1 What is a Firewall?

As defined by the Defense Information Systems Agency (DISA), "A firewall is a device that serves as a barrier between networks providing access control, traffic filtering, and other security features. Firewalls are commonly deployed between trusted and untrusted networks, for example between the Internet (untrusted) and an organization's trusted private network. They [firewalls] can also be used internally to segment an organization's network infrastructure, for example; deploying a firewall between the corporate financial information and the rest of the company network." [1]

However, the DISA definition of firewall really applies only to network firewalls. With the emergence of application-level firewalls and personal firewalls, we are adapting the DISA definition as follows:

A firewall is an application (or set of applications) that create a barrier between two domains, in whatever way "domain" is defined (i.e., physical domain, logical domain, virtual domain). All firewalls enforce an ingress control policy that is based, at least in part, on traffic filtering. Many firewalls provide other security features, but these are not necessary for an application(s) to be deemed a firewall. In all cases, the purpose of the firewall is to protect entities in one domain from threats originating in another domain.

Firewalls enforce ingress policy rules to prevent malicious and attack data from entering the domain they protect. To achieve ingress policy enforcement, firewalls often implement some limited egress policy rules, to prevent requests from being sent by an entity in the protected domain to a suspicious, anomalous, or known-malicious entity in the untrusted domain. Firewall policy rules may rely solely on an access control list that indicates which entities in an untrusted domain should be allowed to transmit traffic through the firewall to an entity in the trusted domain. Firewalls also perform analyses of the traffic itself—at least to the extent that they inspect the headers on data packets or envelopes surrounding data payloads or content. Through these analyses, the firewall determines whether the traffic satisfies various criteria by which it is deemed admissable into or releasable from the trusted domain. Such criteria may range from approving the TCP port over which the traffic was received to determining whether the traffic contains malicious or otherwise undesirable application-level content. A firewall that performs "deep packet inspection" is one that can parse and analyze traffic encoded above the network protocol layers, most often application-layer protocols.

A deep packet inspection firewall, or application firewall, must have enough knowledge of application-layer data types to determine whether the traffic's payload content conforms to the criteria for admissable (or "whitelisted") application-level traffic or the criteria for inadmissable (or "blacklisted") traffic. Depending on which type of policy is enforced (whitelist or blacklist), the firewall will admit or block the traffic as appropriate.

For a network firewall, the "domains" are two networks, to which the firewall has direct physical or routed network connections. Network firewalls are virtually always located at the outermost boundary between the network the firewall protects (trusted network) and the external (untrusted) network. Network firewall applications are often (though not always) hosted on dedicated servers or special-purpose "appliances". An appliance is a hardware platform configured especially to host a firewall (it may be "tuned" to host other types of networking or security applications as well).

For an application-level firewall, the "domains" are the application being protected, and all the systems (clients and servers) that wish to access that

1 DISA Information Assurance Support Environment. "Wireless Security Frequently Asked Questions (FAQs)". *http://iase.disa.mil/wireless/wirelessfaq.html#answer18* (accessed 27 December 2010).

application. Application-level firewalls are often located as close as possible to the application they are intended to protect, and as a result may be hosted on a dedicated server or appliance, but are often co-hosted with the application; this is especially true of Web application firewalls that are often co-hosted on the Web server.

For a personal firewall, the "domains" are the client on which the firewall runs and anything external to that client. Personal firewalls are always hosted on the client system they are intended to protect.

Network and application firewall applications are often packaged together with an operating system that has been specially "hardened" (securely configured, often with a reduced instruction set) to run the firewall application. Appliance based firewalls always include their own operating systems (OSs), which in some cases are embedded OSs (or even firmware OSs). The firewall OS may be wholly proprietary to the firewall vendor, or may be an adaptation of a general-purpose OS (sometimes with a vendor-assigned brand name to indicate the "hardened" nature of the OS). An increasing number of firewalls are hosted—or at least can be hosted—in a virtual machine (VM) environment such as VMware®, in which case they are able to act both as traditional firewalls and as firewall intermediaries between different virtual machine instances on the same physical host.

Network and application firewalls often include forwarding proxy servers and/or reverse proxy servers. A proxy server acts as an intermediary between clients and servers (applications or services); the clients may or may not be located in a different domain from the server. The proxy server can communicate in the protocol of the service/application that the client is attempting to access, and thus makes it appear to the client as if it is communicating directly with that service/application. In reality, the proxy server filters the request to validate it, sometimes altering it, before issuing it to one or more services/applications as necessary to obtain the desired response. The proxy adds a degree of disassociation between requester and responder.

For firewall purposes, it makes the most sense to implement a forwarding proxy server to enable requestors in a trusted domain to issue requests for services in an untrusted domain (such as a client requesting access to a Web site on the Internet), and a reverse proxy server to enable requestors in an untrusted domain to issue requests for services in a trusted domain (*e.g.,* such as requesting access to a Web server in a DMZ). Not only do proxy servers provide source obfuscation (similar to that implemented by NAT), with the proxy server itself appearing to be the originator of requests and responses, but in firewalls, the "gap" created by the proxy server between requestor and service provides the opportunity to "insert" a wide variety of firewall content filtering and policy enforcement logic, so that the proxy's "validation" of requests and responses can be based on a very rich set of considerations.

Firewalls are often physically located on the same physical platform as and integrated with other security applications such as:

- **Authentication servers (including SSO servers)**—These servers control access from the unprotected domain into the protected domain, allowing or preventing a requesting user from connecting into that domain based on the user's authenticated identity and associated authorizations/privileges.
- **VPN servers**—Perform authentication services as the basis for creating an encrypted session that "tunnels" over an untrusted network (*e.g.,* the Internet) any traffic transferred between a client system operated by an authenticated user and the VPN server, which then routes the traffic through a second encrypted tunnel to its desired destination—another client or server authenticated by the VPN. In this way, the VPN essentially extends the trusted domain for the requesting user by ensuring that (1) traffic can only be exchanged between members of the VPN "community" of clients and servers that can be authenticated; (2) all traffic sent *via* the encrypted VPN tunnel is protected from disclosure to unauthorized parties.

- **Data loss prevention systems**—Implement deep packet inspection of data objects that originate from within a trusted domain, and enforce egress policies to prevent the flow of any data that is determined too sensitive to leave the trusted domain (based on various criteria, such as whether it contains any text or other content strings, formats, syntax, or semantics that are associated with the data).
- **Intrusion detection and/or prevention systems**—Monitor the protected network boundary for indications of attack traffic that has managed to bypass existing firewalls. An IDS will log the suspicious/anomalous traffic and alert the administrator. An IPS may take more active measures to capture and block such traffic. To a great extent, an IPS provides firewall-like functionality; however, unlike a network-level firewall, the IPS does not implement an access control list; unlike an application-level firewall, it does not understand the details of application protocols and data syntax, and so must perform all of its possible checks against all types of traffic, regardless of whether those checks are meaningful for a specific traffic flow.
- **Antivirus, antimalware, antispyware, antispam, and antiphishing applications**—These are often integrated into relevant application firewalls to provide another means of analyzing externally-originated application traffic to determine whether it contains unacceptable content. On their own, they are not considered "firewalls" because they do not implement true ingress control policies beyond writing files that fail their checks to a "quarantine" area or "spam mailbox" instead of forwarding them to the intended recipient.

2.1.1 Specifics of Network Firewalls

In the case of a network firewall, the "domains" between which the firewall mediates are two networks, often (but not always) a private network and the Internet. To be most effective, the firewall is physically located at the outermost boundary or perimeter of the protected (private/trusted) network at its connection point with the untrusted network. All data packets ("traffic") addressed to systems within the protected network and all packets sent out of the protected network pass through the firewall, which filters (*i.e.,* parses the headers and, possibly, payloads) the traffic. As noted earlier, the firewall's primary concern is with ingress control policy—*i.e.,* whether certain traffic should be allowed to flow into the protected network, but the firewall may also enforce a policy that decides whether internally-originating requests to certain external senders should be allowed or blocked. The most common criteria for defining permissable inbound data packets are: (1) the external IP address for the traffic originator appears on the firewall's access control list or sender whitelist (or does not appear on its blacklist), and (2) the transport layer protocol used to transmit the packet appears on the firewall's whitelist (or does not appear on its blacklist).

Typically, a network firewall will be installed at each external access point on the protected network's perimeter. Though firewalls are most often implemented between a private network and the Internet, some organizations also implement network firewalls between segments of their internal private network and/or between their internal private network and a private wide-area network (WAN).

Another function of the firewall is NAT, enabled by the NAT protocol that enables the firewall to "proxy" for devices/computers on the protected network by presenting the firewall's own IP address to the external network instead of the addresses of the devices/computers whose packets the firewall is forwarding to a system on the external network. In this way, the firewall not only hides the IP addresses of the internal systems from discovery by anyone on the external network, it also prevents any direct connection between the external and internal networks, admitting only inbound traffic that is permitted by the firewall's security policy rules.

A network firewall examines all traffic routed between two networks to see if it meets certain criteria. When a firewall receives a packet from either a trusted or an untrusted source, it must determine whether or not that packet should be forwarded on to

the computer network enclave, modified before forwarding, or stopped altogether. The firewall can process the packet in several different ways, depending on the type of firewall technology it uses. In most cases, a firewall will use a pre-configured list of parameters and thresholds to permit or deny the packet transmission. Network firewalls do this in different ways, depending on what category of firewall they fall into:

- **Stateless packet filtering firewall**—A stateless packet filter considers each outbound or inbound packet individually, and does not attempt to either keep track of the "connection state" between packets sent by an internal system and those received from an external system. Aside from a few firewalls built into operating systems, and a few older open source firewalls, there are no solely packet filtering firewalls currently on the market.
- **Stateful packet inspection firewall**—Also known as stateful inspection firewalls (SIFs), as their name indicates, stateful packet inspection firewalls do keep track of "connection state" between the internal and external systems. They do this so they can ensure that any packets received from the external system correspond to a prior request sent by the internal system. Packets received from the external network that are not in direct response to an internally-originated request are considered suspicious, and most firewalls are configured to block them. Since the 1990s, the vast majority of firewalls that perform packet inspection have been stateful. Stateful packet inspection firewalls are generally referred to as stateful inspection firewalls, or SIFs.
- **Circuit-level gateway**—Unlike packet inspection firewalls that operate at the TCP/IP network layer, a circuit-level gateway (CLG) operates as a proxy server at the TCP session layer. The CLG does not filter individual packets. Instead, it provides a virtual "circuit" between an internal system and the CLG's own proxy server. All TCP session requests from that internal system are routed *via* this circuit to proxy server, which monitors the TCP handshakes between session request packets to determine whether the requested session is legitimate. If the proxy server decides to allow the session, the CLG replaces the requestor's IP address with its own and forwards the request to the external addressee.

In addition to filtering and making ingress and egress decisions about network traffic, and implementing NAT and proxy services, most network firewalls also log and report all denied traffic. Network firewalls cannot, however, make security policy decisions based on the actual semantic meaning of the content of traffic; such decisions can only be made by application-level firewalls that are able to parse and "comprehend" Layer 7 application protocols.

2.1.2 Specifics of Application Firewalls

Application firewalls (AFs) operate at the application layer of the network stack. They are proxy-based (forward and/or reverse proxy) firewalls that "run interference" between a "trusted" (internal) application and an "untrusted" (external) application. AFs operate by presenting each application with a set of proxies for all available application-level services. Like lower-layer proxy servers, application-level proxy servers give the connected applications the impression that they are communicating directly with one another when, in fact, all traffic from each application is intercepted and inspected by the AF, which either rejects that traffic (if it violates a filtering rule) or passes it to the counterpart proxy facing the other application, which then routes it to that application.

An AF's filtering and policy ruleset can be quite sophisticated. It can implement fine-grained blacklisting and whitelisting of application-level objects (*e.g.,* URLs/URIs [Uniform Resource Identifiers], email [electronic mail] addresses) and/or content conveyed *via* various application layer protocols (Hyper Text Transfer Protocol [HTTP], File Transfer Protocol [FTP], Post Office Protocol 3 [POP3], Simple Mail Transfer Protocol [SMTP], *etc.*), and can block packets received from any Web site, sender, database, *etc.* that are either on a blacklist or not on a whitelist. They can also implement more granular policies to block only certain types of content from a

specific source, or from a specific type of source. For example, they may block Internet Messaging (IM) traffic but not HTTP traffic originating from any Web site, but may block all FTP traffic originating from only certain Web sites. Some AFs can also detect anomalous content—*e.g.,* content that is incorrectly-formatted, or contains patterns that are indicative of malware/viruses, or URLs or content containing patterns indicative of known exploits of server or client software vulnerabilities. Modern application firewalls also perform various non-firewalling functions such as those listed at the end of Section 1.3.

AFs are either network- or host-based. A network-based AF is interposed not just between two applications, but between two networks, enabling it to filter application layer traffic originating from either network, and preventing undesirable application traffic from an application on the external network from reaching clients or servers on the internal protected network.

A host-based AFs is co-located on the same host as the application it protects, where it monitors all application layer input data, output data, and/or system service calls made from, to, or by the protected application. Modern personal firewalls are virtually always hybrids of host-based network and application firewalls.

AFs tend to be dedicated to certain types of applications. Currently, the most prevalent AFs are Web AFs (WAFs), [2] but there are also numerous email firewalls, as well as a growing number of XML (Web service) and database firewalls. The last of these is typically deployed to protect databases from Web-originated application attacks such as SQL injections, database rootkits, and data loss. Some database firewalls include automated Standard Query Language (SQL) learning capabilities to assist in policy configuration based on their analysis of trends found through the aggregated queries directed to a specific database.

2.1.3 Specifics of Multifunction Firewalls

A multifunction firewall is a single device that combines one or more of the firewall types described above. The vast majority of multifunction firewalls also provide additional security functions/services, such those listed at the end of Section 1.3. The most prevalent types of multifunction firewalls are:

- VPN firewalls, which are usually network firewalls with VPN server capabilities added. In many cases, the supplier of a VPN firewall also provides VPN client software for use with the firewall.
- Unified Threat Management (UTM) Gateways, which generally provide firewalling as well as most if not all of the non-firewall services described at the end of Section 1.3.

There are gradations in between, with multifunction firewalls that provide a smaller subset of end-of-Section 1.3 capabilities than is typically found on a UTM Gateway.

2.1.4 Specifics of Personal Firewalls

A personal firewall is hosted on the individual single-user computer it is intended to protect. Originally, the only function a personal firewall performed was packet filtering (stateless or stateful) of all traffic sent or received over the computer's network interface controller (NIC). Some personal firewalls also support NAT, though it is of no real use on a computer with only one NIC because all it does is obfuscate a single address through one-to-one translation. Traffic directed to the personal firewall's IP address still enters the NIC and ends up on the protected computer. NAT is more meaningful on a single-user computer that has two NICs, since the personal firewall can then provide proxy server separation between the "inside" NIC and the "outside" NIC. This configuration presumes, however, that there is some kind of network for each NIC to connect to, *e.g.,* one NIC connects to a home local-area network (LAN) and the second NIC connects to the external networking device (cable modem, Digital

2 The Web Application Security Consortium issued Version 1.0 of its Web Application Firewall Evaluation Criteria document, in part to clarify what a WAF is and its role in protecting Web sites. Download from: *http://projects.webappsec.org/w/page/13246985/Web-Application-Firewall-Evaluation-Criteria*

Subscriber Line/Asymmetric Digital Subscriber Line [DSL/ADSL] modem, wireless modem). For desktop computers with only one NIC, comparable multi-network connectivity with NAT proxying can be achieved using a personal router or hub, which connects to the computer's single NIC and to one or more other networks; the router then performs the IP address translation for the computer just as a firewall would do.

Many personal firewalls come bundled with multiple non-firewall security features, such as antivirus and antispyware, data leak prevention (DLP), antiphishing (URL blacklisting), download sandboxing, and rudimentary intrusion detection capabilities. They are, in fact, the single-user computer equivalent of UTM gateways.

A class of personal firewalls has emerged that can be hosted on mobile data devices such as personal digital assistants (PDAs) and smartphones. These are designed to protect the mobile device from threats delivered *via* the wireless network, and also to enable the device user to block certain kinds of traffic, or traffic from unknown or undesirable sources (identified by telephone number or text messaging address).

2.1.5 Other Types of Firewalls

There are other firewall types that filter traffic based on elements of network or application traffic other than IP address, protocol, or content. For example, the EdenWall Virtual Security Appliance implements a new approach to traffic filtering: it filters traffic based on the positively authenticated identities of source and destination. Firewalls such as this that do not map smoothly into the other firewall categories are provided their own subsection at the end of Section 3.

SECTION 3 ▶ **Firewall Products**

Section 3 provides a listing, with brief descriptions of available firewalls in all of the firewall categories described in Section 1. These include only commercial firewalls that are currently marketed by their vendors and open source firewalls that are actively maintained by their developers. Commercial firewalls that are still supported but no longer marketed are excluded, as are open source firewalls that are still available but no longer maintained. Also excluded are managed firewall services and managed firewall services. [3]

These descriptions are derived primarily from information published by the firewalls' suppliers. In a few cases in which supplier-provided information was insufficient, additional information was derived from reliable third-party sources, such as Common Criteria certification reports or ICSA Labs [4] testing reports.

These listings are provided for informational purposes only, and do not constitute product endorsements by IATAC, DTIC, or DOD.

3 Some examples include: (1) BinarySEC Web site Security, (2) Akamai Web Application Firewall Module, (3) iPermitMail Email Firewall, (4) Dell SecureWorks Managed Web Application Firewall, (5) BT Infonet Managed Firewall Services, (6) Proofpoint Enterprise Protection SaaS Email Security, and (7) Cloud Leverage™ Cloud IPS/Firewall, V-Firewall, and Mobile Active Defense.

4 ICSA was formerly the International Computer Security Association. ICSA Labs is now a subsidiary of Verizon.

Deerfield.com VisNetic Firewall for Servers

Abstract

For protection of Windows-based servers hosting information on the Internet, an extranet, or an intranet, VisNetic Firewall for Servers provides packet-level firewall protection. Recognizing that servers must be accessible to those with proper credentials, and perhaps open to the public anonymously, VisNetic Firewall allows legitimate requests through the firewall while denying access to packets that do not meet the rule-set. Rules within VisNetic Firewall determine whether a packet is allowed or blocked dependent upon parameters such as source and destination IP address, source and destination port, direction of traffic (i.e. inbound and/or outbound) and protocol. VisNetic Firewall also features remote administration capabilities and protection for Web servers. Remote administration allows the administration of the VisNetic Firewall server from any computer with an Internet or Intranet connection. VisNetic Firewall's Web server protection features ensure that all Web traffic is scanned for malicious activity, and is blocked upon detection.

Deerfield.com VisNetic Firewall for Servers

Type of Firewall	Packet filter/SIF
OS	Windows Server
Format	Software
License	Commercial
National Information Assurance Partnership (NIAP) Validated	
Common Criteria	
Developer	Deerfield.com
Information	*http://www.deerfield.com/products/visnetic-firewall/server/*

eSoft InstaGate Firewall

Abstract

eSoft's InstaGate firewall comes standard with stateful packet inspection and full NAT services (including Stateful Fail-over of Network Address Translation [SNAT] and Destination Network Address Translation [DNAT]), DMZ support (including a dedicated DMZ port), Voice-over-IP (VoIP) support (Session Initiation Protocol [SIP] and H.323), Point-to-Point Protocol over Ethernet (PPPoE) support, quality of service (QoS) bandwidth management. In addition, eSoft offers a number of additional VPN and AF options including (1) VPN Management, which transforms the InstaGate Firewall into a VPN firewall (IP Security [IPsec] and Point-to-Point Tunneling Protocol [PPTP]; IPsec NAT traversal); (2) Email ThreatPak and Web ThreatPak, which add intrusion detection and prevention with deep packet inspection (content filtering and antivirus/antimalware scanning) of email (envelope, content, and attachments) and Web traffic; the Web ThreatPak also performs P2P and IM blocking; (3) High Availability SoftPak, which provides automatic firewall failover and hot standby capabilities; (4) Internet Failover SoftPak, which provides automatic traffic switchover to an alternate Internet service provider in case of outage on the primary connection.

eSoft InstaGate Firewall

Type of Firewall	SIF (+ WAF and Email AF options)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	eSoft
Information	*http://www.esoft.com/network-security-appliances/instagate/*

GCIS Firewall Sentinel™ and Proxy Sentinel™

Abstract

The GCIS [General Center for Internet Services] Firewall Sentinel is a scalable intelligent IP packet filtering firewall hosted on Free BSD [Berkeley Software Distribution] Unix. The firewall continuously analyzes all inbound traffic from the Internet to determine whether it is acceptable, in which case the firewall switches to the "on" position to allow traffic to enter the protected network, or unacceptable (*i.e.,* suspicious or malicious), in which case the firewall switches itself to the "off" position, which completely blocks the traffic from entering the protected network. Proxy Sentinel includes the same stateful packet filtering firewall and adds an Internet proxy server and file caching software. Proxy Sentinel's proxy server provides a Domain Name System (DNS) server, programs for rewriting requests and for performing authentication, and management and client tools. Proxy Sentinel can also be configured to implement negative caching of failed requests. Proxy Sentinel supports Secure Socket Layer (SSL), extensive access controls, and full request logging. Both appliances can operate on cable modem, DSL/ADSL, satellite access, or dial-up connections. Customers located within a 200 kilometer radius of Montreal, Quebec, Canada, obtain free onsite configuration and installation with every firewall license they buy.

GCIS Firewall Sentinel and Proxy Sentinel

Type of Firewall	SIF
OS	Included (Free BSD)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	General Center for Internet Services (GCIS) Inc. (Canada)
Information	*http://www.internet-security.ca/firewall-sentinel.html* *http://www.internet-security.ca/proxy-sentinel.html*

Intertex SurfinBird IX67 FW Series

Abstract

The Intertex SurfinBird IX67 FW [firewall] is a SIP-capable firewall and router that performs packet filtering and stateful packet inspection, and includes a built-in SIP proxy and registrar that dynamically control the firewall and NAT for full SIP support. Optional VPN software (IPsec, PPTP and Layer 2 Tunneling Protocol [L2TP] with certificate handling) is also available for the IX67. IX67 appliances come in wireline and wireless models.

Intertex SurfinBird IX67 FW Series

Type of Firewall	SIF (with SIP proxy)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Intertex (Sweden)
Information	*http://www.intertex.se/products/list.asp?iMenuID=110&t=70*

IPFIREWALL (IPFW)

Abstract

The IPFIREWALL (IPFW), authored and maintained by FreeBSD volunteer staff members, uses the legacy stateless packet filtering rules in combination with a legacy rule-coding technique to produce "Simple Stateful" logic. A sample IPFW ruleset (stored in /etc/rc.firewall and /etc/rc.firewall6 in the standard FreeBSD install) is rather simple and not expected to be used "out of the box" without modifications. For one thing, the example does not include stateful filtering. The IPFW stateless rule syntax is technically sophisticated, and not suitable for the average firewall administrator; it requires the expertise of an expert user who understands advanced packet selection requirements and has a deep and detailed understanding of how different protocols use and create their unique packet header information.

IPFW is composed of seven components: (1) kernel firewall filter rule processor and integrated packet accounting facility, (2) the logging facility, (3) the divert rule, which triggers the NAT facility, (4) advanced special-purpose facilities, (5) "dummynet" traffic shaper facilities, (6) fwd rule forward facility, (7) bridge facility, and (8) ipstealth facility. IPFW can operate on both IP Version 4 (IPv4) and IP Version 6 (IPv6) networks.

IPFIREWALL (IPFW)

Type of Firewall	Packet filter
OS	Included (built into FreeBSD)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	FreeBSD Project
Information	*http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html*

Mac® OS X Server ipfw and Application Firewalls

Abstract

Mac OS X (Server and Client) include FreeBSD's ipfw firewall software to protect network applications hosted on the Mac OS X system. The Mac OS ipfw scans incoming IP packets and rejects or admits them based on the filters configured by the user; such filters may restrict access to any IP service running on the computer, or can be customized to allow or block inbound traffic from only certain IP addresses or from a range of IP addresses. To prevent IP address spoofing, the firewall software implements stateful packet inspection, which determines whether an incoming packet is a legitimate response to an outgoing request or part of an ongoing session. ipfw is accessible from the Terminal command line; there is no graphical user interface for configuring it.

In addition to ipfw, Mac OS X v10.5 and 10.6 includes the Application Firewall, which controls TCP and User Datagram Protocol (UDP) connections made to the protected computer by other computers on the network. The Mac OS X Application Firewall has a "stealth mode" that can also be set to block incoming Internet Control Message Protocol (ICMP) "pings". The Application Firewall does not overrule rules set by ipfw; for example, if ipfw blocks an incoming packet, the Application Firewall will not bypass ipfw to admit and process that packet.

Mac OS X Server ipfw and Application Firewalls

Type of Firewall	Packet filter/SIF
OS	Included (built into Mac OS X Server)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Apple Computer
Information	*http://support.apple.com/kb/ht1810* *http://www.apple.com/sg/server/macosx/technology/security-controls.html* *http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html*

Netfilter

Abstract

Netfilter is a packet-filtering firewall framework built into the Linux 2.4.x and 2.6.x kernels. Its packet inspection rule set is configured by iptables to specify the criteria by which packets and packet content are filtered by Netfilter. In combination with iptables, the Netfilter framework enables the system administrator to build a fully functioning firewall that implements both stateless (IPv4 and IPv6) and stateful (IPv4 only) packet inspection. Netfilter also implements NAT and Network Address Port Translation (NAPT), enables packet mangling (*i.e.,* packet manipulation), and supports tc and iproute2 systems in building sophisticated QoS and policy routers. The Netfilter framework includes multiple layers of application programmatic interfaces (APIs) for adding third-party extensions (such as numerous plug-ins and add-on modules available in the Linux "patch-o-matic" repository). When Linux is used as a workstation (*vs*. server) operating system, Netfilter can be configured as a personal firewall.

Netfilter

Type of Firewall	Packet filter/SIF
OS	built into Linux
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Netfilter.org
Information	*http://www.netfilter.org*

NetSib NetworkShield Firewall

Abstract

NetworkShield Firewall is corporate gateway stateful inspection firewall for Windows Server that protects small-to-medium-size business networks from external and internal attacks, provides Internet access to users, and includes traffic usage policy/control features. Other features include NAT, DNS forwarding, Active Directory support (for authentication), and realtime network monitoring. NetworkShield Firewall allows the administrator to configure the network based on logical objects of private (trusted) and public (untrusted) networks, with access policies for each network independent of network type (private, public) and parameters of security policies set for other networks. NetworkShield Firewall supports an unlimited number of IP addresses on a single network interface, enabling the network to be divided into logical subnets. For higher security assurance, network relationships can be established between networks beyond the firewall rules. For example, to connect a local area network (LAN) to the Internet *via* a single IP address and prevent access from the Internet to the protected network, the firewall's NAT (Network Address Translation) interaction type can be configured. To provide access between local area networks and in other cases, the "Route" interaction type can be set. The Server Publishing mechanism makes it possible to access servers in the private or perimeter (DMZ) network of the company, such as Web servers, mail servers, data servers, and to ensure protection against external attacks. NetworkShield Firewall runs as a published server (Firewall Redirect Rules are used to publish servers). NetworkShield Firewall also enables redirection of connections to other IP addresses or to other TCP/UDP ports.

NetSib NetworkShield Firewall

Type of Firewall	Packet filter/SIF
OS	Runs on Windows Server 2000/2003
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	NetSib (Hungary)
Information	*http://www.networkshield.com/*

NuFirewall

Abstract

The NuFirewall is an open source, ready-to-use firewall based on the open source Netfilter and NuFW firewalls. The NuFirewall appliance is intended to be placed between the IP networks to be protected and the untrusted network(s). NuFirewall implements both stateful packet inspection/filtering and, when integrated with an existing PKI or identity management system (which must include either an Active Directory or Lightweight Directory Access Protocol [LDAP] authentication directory), user identity-based filtering; identity-based filtering also requires installation of the NuFirewall NuFW-AS and NuAgent client modules (which interoperate with authentication software on requesting client systems).

NuFirewall

Type of Firewall	Packet filter/SIF
OS	Firewall: runs on Linux (Debian/GNU Linux Etch or later, or Ubuntu; requires X server); Agents: run on Windows XP, Vista, or 7
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	EdenWall Technologies (France)
Information	*http://www.nufw.org/projects/nufirewall*

Packet Filter

Abstract

Packet Filter (PF) is included in OpenBSD for filtering TCP/IP traffic and performance of NAT. PF can also normalize and condition TCP/IP traffic and provide QoS bandwidth control and packet prioritization.

Packet Filter (PF)	
Type of Firewall	SIF
OS	built into OpenBSD
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	OpenBSD Project
Information	*http://www.openbsd.org/faq/pf*

Qbik WinGate Proxy Server

Abstract

WinGate Proxy Server is an integrated Internet gateway, firewall, and communications server for enterprise, small business, and home networks. WinGate Proxy Server comes with a built-in packet-inspecting firewall, and can be further enhanced with optional plug-in components, to scan incoming data for viruses and filter out inappropriate Web content. WinGate Proxy Server (1) enforces access-control and acceptable use policies, (2) monitors Internet usage in real time, and maintains per-user and per-service audit logs, (3) prevents viruses, spam, and inappropriate content from entering the network, (4) provides Internet and intranet email services, (5) protects servers from internal or external threats, (6) improves network performance and responsiveness through Web and DNS caching. WinGate Proxy Server can support most types of Internet connections, from dialup modem to high-speed fiber. The Proxy Server operates transparently to users, who believe they are directly connecting to the Internet. WinGate Proxy Server supports a wide variety of Internet protocols, including HTTP, SMTP/POP3, IM, FTP, and SSL, as well as DirectPlay Internet gaming protocols and Real Time Streaming Protocol (RTSP) (for audio/video). WinGate Proxy Server's user database and policies enable administrators to limit and control per-user access to the Internet, and to log, audit, and view activity and history in real time, thereby supporting close monitoring of suspicious or non-conformant user activity.

Qbik WinGate Proxy Server

Type of Firewall	SIF (+ AF option)
OS	Runs on Windows 2000, 2003, 2008 Server, XP, Vista, and 7
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Qbik New Zealand Ltd. (New Zealand)
Information	*http://www.wingate.com/products/wingate/index.php*

ReaSoft Network Firewall

Abstract

ReaSoft Network Firewall provides small and medium-size businesses with a packet filtering/stateful inspection firewall that includes NAT, multinetwork support, servers publishing (mapping), traffic usage policy enforcement, realtime activity monitoring, event logging, system recovery, and user authentication *via* Active Directory/Windows login (Windows NT LAN Manager [NTLM]) or ReaSoft Network Firewall login. (Note: The description of the ReaSoft Network Firewall is identical to that of the NetSib NetworkShield firewall, though it is not possible to determine whether ReaSoft simply purchased and repackaged NetSib's technology.)

ReaSoft Network Firewall

Type of Firewall	Packet filter/SIF
OS	Runs on Windows 2000, XP, 2003 Server, Vista, 2008 Server, 7
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	ReaSoft Development (United States [U.S.]/Russia)
Information	*http://www.reasoft.com/products/networkfirewall*

Soft in Engines Bandwidth Management and Firewall

Abstract

Soft in Engines Bandwidth Management and Firewall is not only firewall that can allow or prohibit communication, but a traffic shaper providing QoS limitation of network speed, amount of transferred data, or priority in accessing network resources. The firewall can manage gigabit data flows. Specific product features and capabilities include: (1) Traffic shaping for Ethernet, IP, TCP, UDP, ICMP, DNS, passive FTP, HTTP, and P2P protocol flows by usernames, groupnames, organization unit names, computernames contained in Active Directory, Linux Samba NT domains, or stand-alone servers, with shaping of HTTP connections by URL; (2) SIF for TCP, UDP, ICMP, and DNS; (3) NAT (with multiple NAT support for private subnets and statically-mapped TCP/UDP ports); (4) denial of service (DoS) protection; (5) QoS (fair usage policy, data quotas); (6) content filtering for TCP/UDP traffic, with scheduling of filters possible for specific days or weeks; (7) performance monitoring; (8) connection logging for TCP, UDP, DNS, FTP, HTTP, P2P; (9) TCP connection redirection by client IP address and target TCP port; (10) support for up to 32,767 simultaneous TCP/UDP connections.

Soft in Engines Bandwidth Management and Firewall

Type of Firewall	Packet filter/SIF
OS	Runs on Windows XP/2003/Vista/2008/ Windows 7/Server 2008 R2
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Soft in Engines (Slovak Republic)
Information	*http://www.softinengines.com*

Sphinx Software Windows 7 Firewall Control Plus Server Edition

Abstract

Sphinx Software Windows 7 Firewall Control Plus Server Edition is essentially identical to the Desktop Edition in terms of protection capabilities, which include application protection from undesirable incoming and outgoing network activity, and controls Internet access by applications. The firewall manages and synchronizes port forwarding provided by external routers, and supports Ipv6 networks. However, unlike Desktop Edition, Server Edition enables an administrator to configure multiple application network access permissions on a user-by-user basis.

Sphinx Software Windows 7 Firewall Control Plus Server Edition

Type of Firewall	Packet filter/SIF
OS	Runs on Windows XP, Vista, 7
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SphinxSoftware/element5/Digital River (Germany)
Information	*http://www.sphinx-soft.com/Vista/index.html http://www.sphinx-soft.com/Vista/order.html#server*

TRENDnet 4-Port Gigabit Firewall Router

Abstract

The TRENDnet 4-Port Gigabit Firewall Router allows multiple users to share Internet access at gigabit speeds while providing a configurable firewall to protect the network from unwanted intruders. The Firewall Router can be configured to restrict Internet access based on client IP addresses, URL keywords, and service types. The Firewall Router incorporates NAT and SPI firewall technology, and protects against popular DoS attacks.

TRENDnet 4-Port Gigabit Firewall Router

Type of Firewall	Packet filter/SIF
OS	Runs on Windows XP/2003/Vista/2008/ Windows 7/Server 2008 R2
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	TRENDnet
Information	*http://www.trendnet.com/products/proddetail.asp?prod=180_TWG-BRF114&cat=41*

Windows Firewall

Abstract

Windows Firewall is built into Windows releases from XP Service Pack 2 onward, and is enabled by default for all network connections (wired, wireless, VPN, and FireWire), with some built-in exceptions to allow for connections from machines on the local network. On Windows XP, the Windows Firewall on Windows XP can only process traffic on inbound connections. With Windows Vista and Windows Server 2008 the firewall adds: (1) IPv6 connection filtering, (2) outbound packet inspection, (3) advanced packet inspection that allows rules to be specified for source/destination IP addresses, port ranges, and services (selected from a list of service names), (4) IPsec tunnel filtering (connections allowed or denied based on security certificates), (5) Kerberos authentication, (6) encryption, (7) improved management/configuration interface, (8) support for up to three separate firewall profiles per computer, (9) support for rules enforcing separate server and domain isolation policies. Windows Firewall in Windows Server 2008 Release 2 and Windows 7 added further enhancements, such as multiple active profiles. When Windows is used as a desktop (*vs.* server) operating system, Windows Firewall can be configured as a personal firewall.

Windows Firewall

Type of Firewall	SIF
OS	Built into Windows XP, Vista, Server 2003 and 2008, and 7
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Microsoft Corporation
Information	*http://technet.microsoft.com/en-us/network/bb545423.aspx*

Untangle Firewall

Abstract

The Untangle firewall is included with Untangle servers. It can also be downloaded for free as a standalone firewall. The firewall enforces simple ingress/egress rules based on IP address, protocol, and source and destination ports. Used in conjunction with a router, the Untangle firewall can create DMZ and perform NAT, or can run as a transparent bridge.

Untangle Firewall	
Type of Firewall	SIF
OS	Runs on Windows (XP, Vista)
Format	Software
License	Freeware (Commercial)
NIAP Validated	
Common Criteria	
Developer	Untangle, Inc.
Information	*http://www.untangle.com/Firewall*

Alcatel-Lucent OmniAccess 8550 Web Services Gateway

Abstract

The Alcatel-Lucent OmniAccess 8550 Web Services Gateway performs stateful run-time policy enforcement, including application access control policy enforcement for access to individual Web services, information access control policy enforcement for access to individual information records, and secured proxy point policy enforcement with cross-referenced audit for all partner activity. The Gateway's eXtensible Markup Language (XML) message validation and control ensure all messages are well formed, and its denial of service (DoS) protection prevents replay attacks. The Gateway also provides service virtualization, data protection whereby all data are digitally encrypted and signed, reliable messaging for policy-controlled, guaranteed Quality of Service for delivery of Web service messages, strong authentication for users and partner institutions (X.509, XML Key Management Specification [XKMS], Rivest-Shamir-Adelman [RSA], Data Encryption Standard [DES], Triple DES [3DES], Advanced Encryption Standard [AES], Secure Hash Algorithm [SHA], Public Key Cryptography Standards [PKCS], Certificate Revocation Lists [CRLs], Online Certificate Status Protocol [OCSP]), and user-centric auditing of each information record viewed or modified by each credentialed user. The Gateway runs on a hardened platform with no direct operating system access, an encrypted hard drive, no internal devices allowed to re-boot the system, all ports disabled, and all configuration files digitally locked. The hardware's high availability features include redundant power supplies and fans, support for Redundant Array of Independent Disks (RAID), XML processing, and SSL/TLS cryptographic hardware accelerators.

Alcatel-Lucent OmniAccess 8550 Web Services Gateway

Type of Firewall	AF (XML)
OS	Included (OmniAccess OS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Developer Alcatel-Lucent (France)
Information	*http://enterprise.alcatel-lucent.com/?product=8550WSG&page=overview*

Alt-N SecurityGateway for Exchange/SMTP Servers

Abstract

Built upon the industry standard SIEVE mail filtering language, the Alt-N SecurityGateway email firewall for Exchange/SMTP Servers incorporates multiple defense layers that deliver comprehensive protection at the edge of the network to prevent spam, phishing, viruses, and other threats to the organization's email communications. SecurityGateway's main firewalling feature is its sender blacklisting and whitelisting capability, that enables blocking (blacklisting) or admission (whitelisting) of emails from specified senders. Other standard features include antispam, anti-spoofing, email authentication, anti-abuse, message content and attachment filtering and greylisting, and data loss prevention. In addition, a ProtectionPlus option is available that extends SecurityGateway's built-in antivirus/antispam to use multiple antivirus engines (Kaspersky Antivirus Engine; Outbreak) in addition to the firewall's built-in virus and spam pattern analysis tools.

Alt-N SecurityGateway for Exchange/SMTP Servers

Type of Firewall	AF (Email)
OS	Runs on Windows XP/2000/2003/2008/ Vista/7
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Alt-N Technologies/Research In Motion, Ltd. (Canada)
Information	*http://www.altn.com/Products/ SecurityGateway-Email-Firewall*

Anchiva Secure Web Gateway A Series and Web Application Firewall S Series

Abstract

Anchiva's Secure Web Gateways provide URL filtering and Internet application control, together with a wide range of non-firewalling security functions such as antimalware protection, botnet protection, bandwidth management, Web content auditing, and keyword filtering on outbound traffic. Anchiva's Web Application Firewalls provide two-way scanning and analysis of HTTP/HTTP-Secure (HTTPS) traffic to identify and detect various types of Web coding and interactive Web technologies, URL parameters, and Web form inputs, and to block release in outbound communications of sensitive information of interest to attackers, such as server version information, and database and HTTP error messages, along with Web application code leaks and Web site directory leaks. The WAF also inspects and filters potentially dangerous file downloads and interactive Web application sessions to detect and block SQL injection attacks, cross-site scripting (XSS) attacks, command line injection attacks, weak password attacks, and buffer overflow attacks. Anchiva WAF also supports forensic monitoring and diagnosis of common security threats such as Trojan-infected Web pages, and provides realtime alerts to support attack prevention.

Anchiva Secure Web Gateway A Series and Web Application Firewall S Series

Type of Firewall	WAF
OS	Included (AnchivaOS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Anchiva Systems, Ltd. (U.S./China)
Information	*http://www.anchiva.com/us/product.asp*

Applicure dotDefender

Abstract

Applicure dotDefender complements the network firewall, IPS, and other network-based Internet security products by intercepting traffic from apparently legitimate users who attempt to abuse Web applications to commit fraud or gain unauthorized access to valuable and confidential information inside the firewall. dotDefender incorporates a series of "security engines" that enable it to inspect HTTP/HTTPS traffic for suspicious behavior. These security engines include: (1) Pattern Recognition to identify application-level attacks and malicious behavior such as SQL injection and cross site scripting; (2) Session Protection to prevent session cookie tampering and block DoS and flooding attacks; (3) DLP to inspect outgoing traffic and prevent sensitive information disclosure; the engine implements built-in traffic inspection rules, which can be extended by the customer; (4) Upload Inspection to inspect content of files downloaded (or "uploaded", depending on which direction you are thinking in) from the Internet and perform Multipurpose Internet Mail Extensions (MIME) type filtering to prevent Web shells, backdoors, rootkits, and other malicious payloads from being uploaded with seemingly benign Web content, image files, *etc.* dotDefender uses a knowledgebase of signatures for detecting requests from known-malicious sources such as bots, zombies, and spammers. The signatures also identify bad user agents and hacking tools that might attempt to gather information about vulnerabilities in Web applications protected by dotDefender. In addition to standard support for Windows 2003/2008 running Internet Information Services (IIS) and Linux running Apache Web server, dotDefender includes an Open API to enable its integration with other Web management platforms and applications.

AppliCure dotDefender

Type of Firewall	WAF
OS	Runs on Windows 2003 or 2008 running IIS V5.x or later, or Linux running Apache
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Applicure Technologies, Inc. (Israel)
Information	*http://www.applicure.com/products/dotdefender*

Armorlogic Profense

Abstract

Armorlogic's Profense is based on the positive security model. It determines allowable requests, and inputs and disallows everything else. This approach provides protection against unknown threats, simply because they are not in the white-list and thus are disallowed. A negative security model—signatures matching known attacks—can be used in combination with the firewall's positive policy rules. For example it is possible to specify (or learn) strict positive input validation rules for certain critical application components, like login.php or payment.jsp, and use more general negative signatures for the remaining part of the Web site. Profense provides out-of-the-box protection using a combination of positive and negative policy rules with adaptive learning of changes in the Web applications. The initial default protection policy improves and becomes more Web site specific as Profense learns the Web applications and consequently can create positive policy rules for critical application components. Profense's automated application profiling, or learning, engine allows for full automation of policy-building. Because of Profense's positive security model it stops exploits of vulnerabilities and weaknesses without dependence on signatures. By automatically building a positive policy based on a finite amount of information, the business content of the Web system, Profense effectively blocks attacks from hackers and worms. In other words, Profense determines whether a request is allowed based on a white-list. If a request is not in the list it is treated as if it was an attack. This means that Profense also protects from attacks targeting unpublished vulnerabilities. The Profense Web application firewall module has the following protective features: (1) Web server cloaking and customizable HTTP error handling and interception completely shield Web servers from direct Internet access and defeat fingerprinting attacks; (2) white-list based filtering of input data (including all URLs and parameters) allows for protection against threats from unpublished vulnerabilities in Web server software and Web applications; (3) validation of requests using a combination of positive and negative policy rules; (4) blocking at either the application level (request denied) or the network level (IP automatically blacklisted); (5) cross-site request forgery (CSRF) and session (hijacking) protection through session and request form origin validation based on cryptographic tokens; (6) XML and JavaScript Object Notation (JSON)-based Web services are supported; positive and negative policies and combinations thereof can be enforced on Web service requests; (7) log data masking provides compliance with requirements like Payment Card Industry Data Security Standards (PCI DSS); (8) HTTPS termination allows for white-list based protection from SSL-encrypted attacks; (9) Data leak prevention (PCI DSS 2.0 Section 6.5/6.6 compliant) using either response blocking or rewriting; (10) extensive control over what violations to block, allow, or allow and log; (11) SSL client authentication and authorization with certificate forwarding to backend servers. The firewall protects against exploits targeting all Open Web Application Security Project (OWASP) Top Ten vulnerabilities, and can be optionally extended to provide network level firewalling as well. The Profense Load Balancer module enables scalability and acceleration of even complex SSL-enabled Web applications. The Web accelerator module accelerates Web application and Web system performance by: lowering the Web and application server workload, and optimizing and reducing bandwidth usage and TCP-connection handling, and offloading SSL operations from Web servers.

Armorlogic Profense Web Application Firewall

Type of Firewall	WAF + XML AF
OS	Included (hardened, minimized OpenBSD)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Armorlogic ApS (Denmark)
Information	*http://www.armorlogic.com/profense_overview.html*

art of defence hyperguard

Abstract

art of defence's hyperguard is designed to protect Web and cloud applications against known and unknown attacks at the application layer. hyperguard enables centralized security monitoring, reporting and alerting and provides Web applications with customizable protection against external attacks. With its cluster-capability and client-capable administration, hyperguard can be deployed as a plug-in into Web servers or other Web infrastructure components (*e.g.,* as a virtual appliance) or as a cloud-based software-as-a-service (SaaS), *e.g.,* WAF SaaS on Amazon Web Services. As a plug-in, hyperguard can be deployed on all common Web servers, Java EE-Application servers, security gateways, load balancers, and network firewalls. hyperguard runs invisibly, without its own IP address; therefore it is protected from direct attack.

art of defence hyperguard

Type of Firewall	WAF
OS	Runs on Solaris, Linux, BSD Unix, and Windows
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	art of defence (United Kingdom [UK])
Information	*http://www.artofdefence.com/en/products/hyperguard.html*

Axway MailGate

Abstract

Axway (formerly Tumbleweed) MailGate offers comprehensive inbound email antispam, antivirus, and Intelligent Edge Defense, which combines anomaly detection and rate throttling with realtime zombie detection and IP reputation services to protect networks against distributed botnet attacks. The Intelligent Edge Defense module also eliminates directory harvest attacks, email DoS attacks, malformed SMTP packets, invalid recipient addresses, and other forms of malicious and invalid messages. By verifying valid recipients at the perimeter, MailGate supports IP-based block and allow lists, identifies suspicious senders, and applies intelligent traffic shaping and message throttling for invalid messages. MailGate's Domain Keys Identified Mail technology authenticates user email domains to ensure that senders within an organization are who they say they are. Bounce Address Tag Validation protects against non-delivery email attacks in which spammers spoof individual email addresses for use in spam activities. MailGate also provides content filtering and outbound email policy enforcement for data loss prevention. MailGate also provides automatic gateway-to-gateway encryption for any remote domain *via* policy-based Secure MIME (S/MIME) or Transport Layer Security (TLS) encryption or S/MIME. MailGate's digital rights management (DRM) capabilities protect the integrity of documents after they are sent by converting Microsoft Office attachments into password-protected, "locked," and watermarked PDF documents that cannot be copied, altered, or printed except by the document creator.

Axway MailGate

Type of Firewall	AF (Email)
OS	Included (hardened Linux); Virtual appliance requires VMware
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Axway/Sopra Group
Information	*http://www.axway.com/products-solutions/Email-identity-security/comprehensive-Email-security/mailgate*

BalaBit IT Security Zorp

Abstract

Zorp technology is a perimeter defense tool developed for organizations with extensive networks and demanding security requirements. During Zorp's design, the developers abandoned the traditional firewall architecture in favor of a modular architecture that enables the Zorp gateway to be extended with new modules to handle new protocols and different layers of embedded communication standards. Advanced authentication services like SSO and user-level QoS can be configured using the authentication capabilities of the product. Zorp can perform filtering, including content filtering (virus, spam), even on encrypted channels (*e.g.,* HTTPS, POP3-Secure [POP3S], Internet Message Access Protocol-Secure [IMAPS], SMTP-Secure [SMTPS], Secure FTP [SFTP], *etc.*). Zorp can also filter specialized protocols (*e.g.,* Remote Authentication Dial-In User Service [RADIUS], SIP, Microsoft Remote Procedure Call [RPC], Virtual Network Computing [VNC], Remote Desktop Protocol [RDP], *etc.*).
Zorp consists of several individual modules:
(1) Zorp application-level proxy gateway, which inspects the protocol-specific portions of network packets; (2) Zorp Content Vectoring System, which implements a content vectoring framework of several different modules (*e.g.,* virus- and spam filters) that inspect the data payloads of the network packets; (3) Zorp Management System, which provides a uniform interface to configure policy for and monitor the elements in Zorp's perimeter defense (*e.g.,* application-level gateways, content vectoring servers); (4) Zorp Management Console; (5) Zorp Authentication System, which can be configured to authenticate (*via* username/password, S/Key, CryptoCard RB1, LDAP binding, Generic Security Services Application Program Interface /Kerberos 5, or X.509 certificate) all connections passing through the network gateway; the Zorp Authentication System also mediates authentication information exchanged between Zorp components and the authentication database (*e.g.,* Microsoft Active Directory, LDAP, pluggable authentication module [PAM], RADIUS, Apache htpasswd file, Terminal Access Controller Access-Control System [TACACS]; Zorp also has its own built-in authentication database).

BalaBit IT Security Zorp

Type of Firewall	WAF
OS	Included (ZorpOS—customized version of Ubuntu Linux 6.06)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	BalaBit IT Security (Hungary)
Information	*http://www.balabit.com/network-security/zorp-gateway*

Barracuda® Spam & Virus Firewall

Abstract

The Barracuda Spam & Virus Firewall provides a solution for complete protection of an organization's email infrastructure. It eliminates spam and virus intrusions while safeguarding an organization's reputation through content inspection based on policy for both inbound and outbound email. Outbound filtering also prevents confidential or sensitive information from being purposely or inadvertently leaked outside the organization. The Barracuda Spam & Virus Firewall is compatible with all major email servers, and can be sized to support very small organizations with as few as ten employees up to extremely large organizations with as many as 200,000 employees; a single Barracuda Spam & Virus Firewall handles up to 100,000 active email users, and multiple units can be clustered together for even greater capacity and high availability. The Barracuda Spam & Virus Firewall protects the email server with twelve layers of defense, including (1) Network Denial of Service Protection; (2) Rate Control; (3) IP Reputation Analysis; (4) Sender Authentication; (5) Recipient Verification; (6) Virus Scanning; (7) Policy (User-specified rules); (8) Spam Fingerprint Check; (9) Intent Analysis; (10) Image Analysis; (11) Bayesian Analysis; and (12) Rule-Based Scoring. All Barracuda Spam & Virus Firewall models include comprehensive outbound filtering techniques including attachment scanning, virus filtering, rate controls and encryption. These features help organizations to ensure that all outgoing Email is legitimate and virus-free. In addition, Barracuda Spam & Virus Firewall includes email encryption using a cloud-based portal and Data Loss Prevention features like attachment content scanning. Barracuda Spam & Virus Firewall includes a Cloud Protection Layer to stop spam and viruses in the cloud. In this mode, inbound email messages are first scanned by the cloud before delivery. The Cloud Protection Layer also features multiple delivery options. If the primary delivery destination is unavailable, then emails are delivered to a secondary destination. If both the primary and secondary destinations are unavailable, then undelivered email is stored for later delivery.

Barracuda Spam & Virus Firewall

Type of Firewall	AF (Email)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Barracuda Networks AG (Sweden)
Information	*http://www.barracudanetworks.com/ns/products/spam_overview.php*

Barracuda® Web Application Firewalls

Abstract

The Barracuda Web Application Firewall protects Web applications and, through its integrated XML firewall, Web services from inbound malicious attacks and DLP *via* outbound traffic, Web site cloaking, and security for HTTP traffic through traffic monitoring and reporting of attack attempts. Application Profiling allows the Barracuda Web Application Firewall to automatically build and tune positive security profiles to provide zero-day protection. Administrators can create fine-grain whitelist rules to govern individual HTML elements or parameters merely by sampling Web traffic. The Firewall also includes an integrated antivirus engine. DoS protection is provided *via* sophisticated rate control policies that can be used to limit client access over time spans typical of DoS and brute force attacks. The Firewall is configured by default with "best practice" security policy, and supports further configuration of granular policies. The Firewall is designed to enforce both organizational policies and policies conformant with external data security standards such as PCI DSS. Barracuda Web Application Firewalls all support comprehensive Identity and Access Management, ranging from simple application authentication and authorization to fine grained, full featured SSO. Firewall identity and access management supports LDAP and RADIUS authentication, two-factor token-based authentication (*e.g.,* using RSA SecurID), and SSO *via* its own simple built-in capabilities, or through seamless integration with third-party SSO technologies such as CA SiteMinder. The Firewall can also increase Web application performance through SSL offloading and acceleration, load balancing, content caching, traffic compression, and connection pooling. In addition, the Firewalls can be deployed in a high-availability cluster configuration to provide redundancy.

Barracuda Web Application Firewalls

Type of Firewall	WAF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Barracuda Networks AG (Sweden)
Information	*http://www.barracudanetworks.com/ns/products/web-site-firewall-overview.php*

Bee Ware i-Suite

Abstract

Bee Ware's i-Suite is a unified threat management gateway appliance that implements Web application and Web service security management functionality, including the i-Sentry Web Application Firewall (WAF). Other i-Suite modules implement security functions such as user authentication and access control, single sign-on, and identity/access management, Web application discovery, monitoring, and vulnerability assessment, content acceleration and optimization, and data leakage prevention. i-Sentry uses Bee Ware's reverse proxy and ICX™ technology to detect and block all known and unknown attacks, including all OWASP Top Ten attacks. i-Sentry supports Web service security by providing XML conformance checking, implementation of standard XML message routing and transformation, encryption, and signature, and monitoring and attack detection for XML traffic. The "engine" driving i-Sentry is the ICX intelligent analysis technology that examines the ways in which applications are used, categorizes the observed traffic according to its threat level, and applies appropriate protection measures. ICX's correlation engine implements complex decision processes based on contextual criteria and analyses (implemented by analytic algorithms) for (1) intrusion detection based on whitelists, blacklists, and attack methodology detection; (2) behavioral analyses driven by neural networking and including session tracking, cookie tracking, and dynamic whitelisting. The administrator can configure the most appropriate actions for the firewall to perform on all security events, using a graphical representation of the security policy. Categories of available actions include (1) authorization of request, (2) rejection and redirection of request, and (3) inbound and outbound rewriting of requests and data. i-Suite can run on any of the six available i-Box appliance platforms, which also provide SSL hardware acceleration. i-Suite can also run as a virtual appliance (as a VMWare image), or can be acquired as a cloud-based SaaS offering as well.

Bee Ware i-Suite

Type of Firewall	WAF + XML AF
OS	Included (Bee Ware OS)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Bee Ware (France)
Information	*http://www.bee-ware.net/en/solutions/web-application-firewall*

BugSec WebSniper

Abstract

WebSniper protects Web servers from exposure to behavioral attack patterns such as SQL injections, buffer overflow exploits, path traversals, cross-site scripting, and many others, by implementing signature-based attack identification and blocking. WebSniper identifies and monitors requests sent *via* the Internet, and distinguishes between legitimate requests to be approved, and illegitimate requests to be interpreted as attempted attacks and blocked before they reach the Web server. WebSniper can also be used for passive monitoring of traffic (without blocking) if configured that way *via* the Information Security Manager's security policy and preferences. WebSniper can also identify attacks that are unknown in advance, and dictate their handling as defined in the configuration. WebSniper also checks and modifies responses returned from the Web server, to protect clients and prevent data leaks. WebSniper is implemented as an Internet Server Application Programming Interface (ISAPI) file to communicate efficiently with the Web server.

BugSec WebSniper

Type of Firewall	WAF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	BugSec (Israel)
Information	*http://www.bugsec.com/index.php?q=WebSniper*

Cisco® ACE Web Application Firewall

Abstract

The Cisco ACE [Application Control Engine] Web Application Firewall combines deep Web application analysis with high-performance XML inspection and management to address the full range of threats to Hyper Text Markup Language (HTML)-based and XML-based Web applications, protecting them from common attacks such as identity theft, data theft, application disruption, fraud, and targeted attacks. The Cisco ACE Web Application Firewall complies with current PCI DSS requirements sections 6.5 and 6.6. The firewall also provides authentication and authorization enforcement to block unauthorized access, positive and negative security policy enforcement to keep bad traffic patterns out and identify and allow only good traffic through, ability to deploy security policies and profiles in monitoring mode to prevent application downtime due to false positives, policy-based provisioning to increase developer productivity and improve deployment flexibility, and scalability and throughput for managing XML application traffic.

Cisco ACE XML Gateways

Type of Firewall	WAF + XML AF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Cisco Systems
Information	*http://www.cisco.com/en/US/products/ps9586/index.html*

Cisco® ACE XML Gateways

Abstract

The Cisco ACE XML Gateway delivers an integrated XML firewall that ensures that XML messages securely and efficiently reach their intended targets and provides protection at each service perimeter between un-trusted and trusted zones. With a comprehensive XML threat defense system, it protects against identity, content-based, personnel, response-compliance, message-transport, and XML DoS attacks. It integrates seamlessly with existing infrastructure such as directories, SSO, public key infrastructure (PKI), and network system management. The Cisco ACE XML Gateway also accelerates XML and application services by improving performance of the XML-based software applications, helping to ensure that all messages can be processed without compromising security, interoperability, or reliability. ACE XML Gateway runs on any of Cisco's ACE appliances.

Cisco ACE XML Gateways

Type of Firewall	AF (XML)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Cisco Systems
Information	*http://www.cisco.com/en/US/products/ps7314/index.html*

Cisco® IOS Firewall

Abstract

Cisco IOS [Internetworking Operating System] Firewall runs on the Cisco integrated services router to protect network resources and segment the network into security zones. The firewall functions include (1) detection of unwanted traffic on specific application service ports, with blocking of unwanted application-level traffic, such as IM, peer-to-peer (P2P) file-sharing, and HTTP-tunneling application traffic; (2) protocol conformance checking for HTTP, SMTP, Extended SMTP, IMAP, and POP3; (3) stateful active and standby failover between firewalls for most TCP-based services, with firewall session state maintained so that active sessions are not interrupted during a router or circuit failure. Additional security functions include: (1) HTTP inspection with Java applet filtering to block malicious content in HTTP traffic; (2) regular expression matching-based policy enforcement combined with granular application inspection and control of HTTP objects (*e.g.,* methods, URLs/URIs, header names) and values (*e.g.,* maximum URI length, maximum header length, maximum number of headers, maximum header-line length, non-American Standard Code for Information Interchange (ASCII) headers, or duplicate header fields)—these measures aid in the detection and prevention of attempts to exploit vulnerabilities, such as buffer overflows, HTTP header vulnerabilities, binary and other non-ASCII character injections, SQL injection, XSS, and worm attacks; (3) policy-map policing that applies rate limits to control network bandwidth usage; (4) session policing that limits connection rates to network hosts and helps protect against DoS attacks.

Cisco IOS Firewall

Type of Firewall	AF
OS	Included
Format	Software
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10038/*
Common Criteria	Evaluation Assurance Level (EAL) 4+
Developer	Cisco Systems, Inc.
Information	*http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/product_data_sheet09186a0080117962.html*

Cisco® IronPort® Email Security Appliances

Abstract

Cisco's IronPort Email Security Appliances combine preventive filters and signature-based reactive filters with content filtering. Cisco reputation filters provide an outer layer of defense using Cisco SenderBase® data to perform a realtime email traffic threat assessment and identify suspicious email senders. IronPort antispam uses a Context Adaptive Scanning Engine that examines the complete context of a message, including: "What" content the message contains, "How" the message is constructed, "Who" is sending the message, and "Where" the call to action of the message is intended to direct the recipient. By combining these elements, Cisco IronPort antispam stops a broad range of threats. IronPort's spam quarantine provides end-users with their own safe holding area for spam messages that integrates seamlessly with existing directory and email systems. IronPort also provides (1) virus outbreak filters that identify and stop viruses without relying on virus signatures, plus Sophos and McAfee antivirus technology to provide additional layers of protection; (2) integrated DLP provided by RSA Email DLP; (3) email encryption (TLS, Pretty Good Privacy [PGP], S/MIME) for secure communication from the email gateway to any recipient inbox, and between email gateways; (4) compliance quarantine that provides delegated access to emails flagged by the content scanning engine; (5) email authentication using DomainKeys identified Mail and DomainKeys verification and signing to digitally process messages in a way that authenticates and protects email identities of email senders and receivers on the Internet; (6) bounce verification that tags messages with digital watermarks to provide filtering of bounce attacks at the network edge; (7) directory harvest attack prevention that tracks spammers who send to invalid recipients and blocks their attempts to steal email directory information; (8) realtime email security threat monitoring and reporting that tracks every system connecting to the Cisco IronPort appliance to identify Internet threats (spam, viruses, DoS attacks, *etc.*), and monitors internal usage trends and compliance violations. Cisco IronPort email security appliances range in size to support small businesses up to Internet Service Providers (ISPs) and large enterprise networks.

Cisco IronPort Email Security Appliances

Type of Firewall	AF (Email)
OS	Included (AsyncOS®)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Cisco Systems, Inc.
Information	*http://www.cisco.com/en/US/products/ps10154/index.html*

Citrix® NetScaler® Application Firewall™

Abstract

Citrix NetScaler Application Firewall is a comprehensive Web application security solution that blocks known and unknown attacks against Web and Web services applications. NetScaler Application Firewall enforces a positive security model that permits only correct application behavior, without relying on attack signatures. It analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications. In addition to detecting and blocking common Web application threats that can be adapted for attacking XML-based applications (*i.e.,* cross-site scripting, command injection, *etc.*), NetScaler Application Firewall includes a set of XML-specific security protections. These include schema validation to thoroughly verify Simple Object Access Protocol (SOAP) messages and XML payloads, and a powerful XML attachment check to block attachments containing malicious executables or viruses. NetScaler Application Firewall also thwarts a variety of DoS attacks, including external entity references, recursive expansion, excessive nesting and malicious messages containing either long or a large number of attributes and elements. NetScaler Application Firewall technology is included in and integrated with Citrix NetScaler, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler Application Firewall is also available as a stand-alone solution on five NetScaler MPX appliances, as well as a Federal Information Processing Standard (FIPS) 140-2-compliant model. The stand-alone NetScaler Application Firewall models can be upgraded *via* software license to full NetScaler Application Delivery Controllers.

Citrix NetScaler Application Firewall

Type of Firewall	WAF + XML AF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Citrix Systems
Information	*http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=2300448*

CloudShield DNS Defender

Abstract

CloudShield DNS Defender is a DNS firewall designed specifically to safeguard DNS systems against DNS attacks (*e.g.,* DDoS, poison pill, cache poisoning, buffer overflows), and to maintain DNS availability and performance even under attack and peak loads. DNS Defender implements several deep packet inspection filters, including: (1) Protocol filters that permit only valid DNS traffic. Source and Destination filters prevent illegitimate requests; (2) Attack filters drop all traffic from known DNS attack vectors (including cache poisoning; (3) Validation filters ensure that only valid requests that conform to RFC standards are passed to the DNS; and (4) Type filters that implement flexible policy control over DNS request, requestor, and respond types. DNS Defender also implements rate limits, selective blocking, support for industry-standard blacklists, query shedding, syntax checks, DNS caching (up to 250,000 queries per second), and rate limiting of selective traffic (*e.g.,* P2P traffic). DNS Defender can be deployed on the CloudShield CS-2000 System or on the CloudShield PN41 Blade in IBM Bladecenter.

CloudShield DNS Defender

Type of Firewall	WAF (with SIF)
OS	Runs on CloudShield Packet Operating System (CPOS™)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	CloudShield/SAIC
Information	*http://www.cloudshield.com/applications/cs_dnsdefender.asp*

Deny All rWeb

Abstract

Deny All rWeb is a Web and XML application firewall designed to be deployed at the front-ends of Web applications to authenticate users and filter all inbound HTTP and HTTPS flows from the Internet or intranet. The firewall implements negative security modules (blacklist and scoring list) and protects against application-level attacks such as SQL injection, code injection, and XSS. rWeb also supports positive security modules using the "scanweb" Web site crawler and "rules wizard" whitelist generator. rWeb performs protocol inspection to protect against attacks using weaknesses in the HTTP protocol. It also protects against encoded attacks, application-level DoS, blacklisted "simple" attacks, and variable structure attacks. The firewall's whitelisting enables any traffic to be rejected that is not explicitly authorized in advance. rWeb also performs stateful tracking that protects against cookie manipulation, cookie stealing, and brute forcing to gain fraudulent access. The firewall's authentication feature enables secure implementation of an extranet using single sign-on to facilitate secure user access to resources. The firewall also includes antivirus for inbound files, and outbound filtering to prevent data loss. rWeb also supports virtual patching of application vulnerabilities without having to modify the application's source code. rWeb's XML firewall provides comparable protections against attacks that target XML-based Web services. A number of performance and availability features help offload computation and memory intensive processes from the protected Web servers, distributes traffic across multiple servers, and enables hot-swapping and automatic traffic rerouting for continuity of operation. The rWeb Reverse Proxy provides a protocol "air gap" and virtualizes the application infrastructure, while it's support for multiple DMZs enables it to simultaneously protect both public and private DMZs. Deny All rWeb can run on one of Deny All's appliances (DA-K1, DA-K2, DA-K3) or on the customer's own HP server.

Deny All rWeb

Type of Firewall	WAF + XML AF
OS	Included (hardened HP-UX Server)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Deny All Security Solutions (FR)
Information	*http://www.denyall.com/products/rweb_en.html*

Deny All rFTP

Abstract

Deny All rFTP is an application firewall that filters both unencrypted and SSL-encrypted FTP file transfers. rFTP is dedicated to protecting against attacks that exploit weaknesses in the FTP protocol, including encoded attacks. rFTP also enforces granular access control to FTP services according to user, profile, and perimeter, and performs antivirus analysis of inbound files, and outbound filtering to protect against data loss. The FTP Reverse Proxy capability provides a protocol "air gap" and virtualizes the application infrastructure. rFTP also provides the same high-availability and performance enhancements as sProxy and rWeb. Deny All rFTP can run on one of Deny All's appliances (DA-K1, DA-K2, DA-K3) or on the customer's own HP server.

Deny All rFTP

Type of Firewall	AF (File Transfer)
OS	Included (hardened HP-UX Server)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Deny All Security Solutions (FR)
Information	*http://www.denyall.com/products/rftp_en.html*

Deny All sProxy

Abstract

Deny All sProxy is a Web application firewall proxy server that protects against attacks that exploit weaknesses in the HTTP protocol, including encoded attacks, and blacklisted "simple" attacks. sProxy also protects against variable structure attacks by generating a much lower level of false positives than application firewalls that use only blacklistling. sProxy's stateful tracking capability also protects against cookie manipulation, while outgoing filtering protects against data loss. The firewall includes antivirus for analysis of all inbound files. The sProxy Reverse Proxy provides a protocol "air gap" and virtualizes the application infrastructure. The firewall supports high availability through hot-swapping and automatic traffic rerouting in the event of a hardware failure. Caching increases performance by offloading processing of static pages and SSL from the Web server, and by multiplexing TCP connections. In addition, the load balancing feature distributes heavy traffic across multiple Web servers. Deny All sProxy can run on one of Deny All's appliances (DA-K1, DA-K2, DA-K3) or on the customer's own HP server.

Deny All sProxy

Type of Firewall	WAF
OS	Included (hardened HP-UX Server)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Deny All Security Solutions (FR)
Information	*http://www.denyall.com/products/sproxy_en.html*

DigiPortal ChoiceMail Enterprise and ChoiceMail Small Business

Abstract

DigiPortal ChoiceMail is a permission-based spam blocker that uses blacklisting, permission lists, and whitelisting, which means ChoiceMail presumes all email is spam unless it originates from a whitelisted sender. ChoiceMail can be configured to automatically query unknown senders, under the assumption that only legitimate senders will respond to such a query (senders who do not are presumed to be spammers). ChoiceMail Enterprise is designed to be co-hosted with Microsoft Exchange Server, Lotus Domino, Novell GroupWise, IMail, SendMail, Netscape, and all other enterprise email servers. ChoiceMail Small Business is a POP3 antispam solution that provides the same antispam capabilities without requiring the customer organization to have its own email server; instead, the firewall can be installed on any computer on the customer's network.

DigiPortal ChoiceMail Enterprise and ChoiceMail Small Business

Type of Firewall	AF (Email)
OS	Runs on Windows NT, 2000, XP, Vista, SBS, Server 2000/2003/2008
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	DigiPortal Software
Information	*http://www.digiportal.com/products/choicemail-business.html*

eEye SecureIIS

Abstract

eEye SecureIIS provides application layer protection against known and unknown exploits, zero day attacks, and unauthorized Web access. SecureIIS inspects requests as they come in from the network layer, as they are passed up to the kernel, and at every level of processing in between. If at any point SecureIIS detects a possible attack, it can take over and prevent unauthorized access and/or damage to the Web server and host applications. SecureIIS was developed as an ISAPI filter, which allows for a tighter integration with the Web server. SecureIIS monitors data as it is processed by IIS and can block a request at any point if it resembles one of many classes of attack patterns; including SQL injection and XSS. The product leverages eEye's knowledge of the various ways in which IIS servers and Web applications can be attacked, so even undiscovered vulnerabilities are secured and thwarted. SecureIIS does not rely upon a database of attack signatures that require regular updating. Instead, it uses multiple security filters to inspect Web server traffic that could cause buffer overflows, parser evasions, directory traversals, or other attacks. Therefore, SecureIIS is able to block entire classes of attacks, including attacks that have not yet been discovered. SecureIIS provides zero-day protection for entire classes of attacks whether known or unknown. SecureIIS works with and protects all common Web-based applications such as Flash, Cold Fusion, FrontPage, Outlook Web Access, and many third-party and custom Web applications. Configurations can be modified without having to restart the Web server, thus preventing disruption of the active Web site. SecureIIS runtime logs provide detailed explanations as to why requests were denied and allow for data to be exported in any number of different formats including tab-delimited, text, and Excel. This activity can also be graphed in realtime based on class of attack. Regardless of the communications protocol, SecureIIS offers protection without affecting service levels on your Web server, and even stops attacks on encrypted sessions based on the ability to analyze the content of HTTPS sessions before and after SSL encryption.

eEye SecureIIS

Type of Firewall	WAF
OS	Runs on Windows Server (2000, 2003, or 2008) 32-bit and 64-bit
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	eEye Digital Security
Information	*http://www.eeye.com/Products/SecureIIS-Web-Server-Security.aspx*

Excelerate SpamGate

Abstract

The Excelerate SpamGate Spam Firewall appliance or software includes all the features needed to eliminate spam and protect email servers from attack. Email can be blocked, quarantined, tagged, or delivered based on the user-configured policies. SpamGate performs junk filter checks, SMTP connection checks, reputation IP checks, Bayesian filter checks, and greylisting analysis against each inbound and outbound mail message, and also includes antivirus and antimalware engines for scanning email and attachments. Filtered email messages may be deleted, rejected, copied (for forensic analysis), and bounced back to sender, quarantined on the firewall, routed to a common spam mailbox on the mail server, or appended with a "Spam" warning in the message header and forwarded to the addressee. SpamGate is based upon the open source SpamAssassin engine that performs heuristic spam analysis of the behavior of email traffic down to the packet level. SpamGate also implements: (1) Real Time Black Hole Lists and Spam URL Real Time Black Hole Lists; (2) interfaces to Vipul's Razor, Pyzor, and Distributed Checksum Clearinghouses spam signature databases; (3) greylisting; (4) an auto-learning Bayesian filter; (5) email address validation; (6) antivirus scanning; two scanners come standard; support available for up to eleven more. Additional features help to make the system effective.

Excelerate SpamGate

Type of Firewall	AF (Email)
OS	Included; Virtual Server: requires VMware
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Excelerate Software, Inc.
Information	*http://www.spamgate.us*

F5® BIG-IP® Application Security Manager

Abstract

BIG-IP Application Security Manager (ASM) includes specific, built-in validated application security policies for common applications as well as an automatic policy-building engine that can adapt to application updates. BIG-IP ASM helps virtually patch Web application vulnerabilities and maintain compliance with government and industry regulations such as PCI and HIPAA. To keep up to speed on the latest Web threats, BIG-IP ASM includes an attack expert system that provides on-the-spot knowledge of violations and attacks. BIG-IP ASM can secure any parameter from client-side manipulation and validate log-on parameters and application flow to prevent forceful browsing and logical flaws. BIG-IP ASM recognizes HTTP parameter pollution attacks and blocks these requests. BIG-IP ASM also protects against layer 7 DoS, SQL injection, XSS, brute force, zero-day Web application attacks, and other OWASP Top Ten application security risks, such as CSRF. As threats grow in number and complexity, the integrated attack expert system provides an immediate, detailed description of the attack, as well as enhanced visibility into the mitigation techniques used by BIG-IP ASM to detect and prevent the attack. BIG-IP ASM shields Web sites from Web scraping attacks that copy and reuse valuable intellectual property and information. By differentiating between a human and a bot behind a browser, BIG-IP ASM protects against automated requests to obtain data. Polices for Web applications can recognize an increase in request volumes and alert BIG-IP ASM to review whether requests are desired. Known IP addresses previously found to Web scrape can be blacklisted for detection and blocking. BIG-IP ASM also provides application-specific XML filtering and validation functions that ensure that the XML input of Web-based applications is properly structured. It provides schema validation, common attacks mitigation, and XML parser DoS prevention. BIG-IP ASM prevents the leakage of sensitive data (such as credit card numbers, Social Security numbers, and more) by stripping out the data and masking the information. In addition, BIG-IP ASM hides error pages and application error information, preventing hackers from discovering the underlying architecture and launching a targeted attack. New signatures from new attacks are frequently required to ensure up-to-date protection. BIG-IP ASM queries the F5 signature service on a daily basis and automatically downloads and applies new signatures. The most widely used security protocol for sending and receiving uploaded files for antivirus scanning is Internet Content Adaptation Protocol (ICAP). BIG-IP ASM strips an uploaded file from the HTTP request and forwards it to an antivirus server over ICAP. If the file is clean, the antivirus server responds to accept the request. If the file is not clean, BIG-IP ASM blocks the request to protect the network from virus intrusion. BIG-IP ASM eases the manageability of FTP server farms. BIG-IP ASM validates the FTP protocol, mitigates brute force attacks, and can also whitelist the enabled FTP commands. In addition, it can enforce command length limits and active-passive connections. For SMTP, BIG-IP ASM provides additional security checks at the perimeter. It also supports greylisting to prevent spam, enforces the SMTP protocol, blacklists dangerous SMTP commands, and mitigates directory harvesting attacks. The rate-limiting capabilities of BIG-IP ASM help to fight DoS attacks. BIG-IP ASM combines application optimization and acceleration technologies such as fast cache, compression, SSL offload, TCP optimization, and other performance advantages of F5's TMOS architecture. This offloads the servers, and consolidates the footprint in the data center. BIG-IP ASM can also secure FTP and SMTP traffic and provide authentication. BIG-IP ASM offloads Web services encryption and decryption as well as digital signature signing and validation, including the ability to encrypt or decrypt SOAP messages and verify signatures without the need to change application coding. BIG-IP ASM is available as a standalone appliance solution or as an add-on

module for BIG-IP Local Traffic Manager on the 11050, 8950, 8900, 6900, 3900, and 3600 appliance platforms, and as an add-on module for VIPRION®.

BIG-IP Application Security Manager

Type of Firewall	WAF + XML AF
OS	Included (TMOS™)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	F5 Networks, Inc.
Information	*http://www.f5.com/products/big-ip/application-security-manager.html.html*

Fortinet® FortiWeb™ Web Application and XML Firewalls

Abstract

Fortinet FortiWeb provides Web application firewall protection based on signature and pattern matching, parameter validation, threshold based limits, session management, flow enforcement and other technologies. Multiple attack prevention/protection capabilities are implemented by the firewall, including application signatures, HTTP request for comments (RFC) compliance, auto-learn based violations, data leak prevention, and authentication capabilities. Web defacement protection monitors protected applications for any defacement and can automatically revert to stored version. The firewall secures sensitive database content by blocking threats such as cross-site scripting, SQL injection, buffer overflows, file inclusion, denial of service, cookie poisoning, schema poisoning, and countless other attacks. The Web application firewall also includes a PCI DSS Requirement 6.6-compliant Vulnerability Scanner module. The firewall's SSL and XML encryption co-processing accelerates transaction times by offloading encryption functions. Further performance features include server load balancing and content-based routing that increase application speeds to increase server resource utilization, while active-passive high availability support implements full configuration synchronization to ensure availability of applications. The XML firewall enforces properly formed and coded pages through XML IPS, schema validation, Web Service Discovery Language (WSDL) verification, XML expression limiting, and other security technologies. Three FortiWeb models are available: FortiWeb-400B, FortiWeb-1000C, and FortiWeb-3000C; these support small-to-medium, medium-to-large, and large-to-enterprise networks, respectively.

Fortinet FortiGate Web Application and XML Firewalls

Type of Firewall	WAF + XML AF
OS	Included (FortiOS firmware)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Fortinet
Information	*http://www.fortinet.com/products/fortiweb*

Forum Sentry XML Gateway

Abstract

Forum Sentry XML Gateway features include (1) Forum XWall technology that is equipped with data authentication as well as XML IPS to actively protect against XML viruses, data corruption and denial of Web service attacks. Forum XWall ensures critical applications are appropriately accessible and continuously available by allowing network administrators to enforce perimeter policies that check the integrity of data and control access to exposed enterprise Web services. XWall peers into the "XML packet" using a unique blend of threat detection and realtime preventative countermeasures. Specifically XWall protects Web services from vulnerability discovery (e.g. through WSDL scanning), probing attacks (*e.g.,* through parameter tampering and replay attacks), coercive parsing (*e.g.,* through recursive payloads, oversize payloads, and DoS attacks), external reference attacks (*e.g.,* external URI references), and malicious content attacks (*e.g.,* schema poisoning, SQL injections). The Gateway also secures Web services communication, and provides Web services mediation and virtualization, crypto-accelerated signature, encryption, and SSL security, native protocol support for HTTP, Tibco Enterprise Message Service, IBM MQ, Java Message Service, FTP, and SMTP, and stateful request and response message processing. The Gateway's authentication and authorization capabilities include HTTP basic authentication, SSL X.509 certificate-based authentication, SAML, WS [Web Service]-Security, support for vendor identity plug-ins, and network and WSDL message-level access control. Data-level security policies are enforced through WSDL operation and URI filtering, content filtering using Xpath and regular expressions, digital signatures and encryption, composite schema validation, and antivirus scanning of attachments. Forum Sentry supports a wide range of Web services specifications including WSDL, SOAP, XML, XSLT (eXtensible Stylesheet Language Transformation), XSD (XML Schema Definition) Schema, DTD (Document Type Definition), XPath, UDDI (Universal Description, Discovery and Integration), XML Digital Signature, XML Encryption, WS-Encryption, WS-Digital Signature, WS-Trust, WS-Policy, WS-I (Web Services Interoperability organization) Basic Profile, WS-Security Token Profiles, PKCS, CRL, and XKMS.

Forum Sentry XML Gateway

Type of Firewall	AF (XML)
OS	Appliance: Included; Software version runs on Windows, Linux, Solaris, in a VM (VMware), or in an Amazon Elastic Compute Cloud (EC2) Amazon Machine Image (AMI)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Forum Systems™
Information	*http://forumsys.com/products/xmlgateway.php*

GreenSQL Express, Light, Pro, and Database Firewall

Abstract

GreenSQL offers a range of commercial database application level gateway/firewall products, including GreenSQL Pro, GreenSQL Light, and GreenSQL Express. GreenSQL commercial firewalls can protect Microsoft SQL Server, MySQL, or PostgreSQL databases and Document Management Systems. GreenSQL Pro includes database firewalling, auditing, caching, intrusion detection/prevention, monitoring, and logging and reporting solutions to protect databases and database-based document management systems from internal and external threats in real time. It enforces both positive and negative security policies, and rejects intrusion attempts for queries known or suspected to be unauthorized. The firewall's automated learning mode can automatically generate a full set of policy rules based on the specific behavior of the database to be protected. GreenSQL Light provides the same protections to single databases. GreenSQL Express is a limited free version of GreenSQL that includes a rules-based database firewall and IDS/IPS that implements a single proxy. In addition to its commercial offerings, GreenSQL offers an open source GreenSQL Database Firewall—an implementation of the GreenSQL database proxy firewall designed for protecting MySQL and PostgreSQL databases against SQL injection attacks. The logic is based on evaluation of SQL commands using a risk scoring matrix as well as blocking known database administrator commands ("drop", "create", etc).

GreenSQL Database Firewall

Type of Firewall	AF (Database)
OS	Express, Light, Pro: Windows Server 2008, Windows Server 2003, Linux (Ubuntu, CentOS, Debian); Database Firewall: Linux (Debian, Ubuntu, Red Hat, Fedora, CentOS, SuSE, Mandriva), FreeBSD
Format	Software
License	Express, Light, Pro: Commercial; Database Firewall: Open source
NIAP Validated	
Common Criteria	
Developer	GreenSQL, Ltd. (Israel)
Information	*http://www.greensql.com* *http://www.greensql.net*

Horizon Network Security™ SPAM Cracker™

Abstract

SPAM Cracker is an enterprise-grade spam and virus filter that blocks or flags most spam through context filtering (matching spammer phrases such as "get rich quick"), by known bad source IP addresses, by Sender Policy Framework *(http://www.openspf.org/)*, by checking Domain Signatures provided by Yahoo to reject false claims that the sender is a Yahoo address, by many other similar "spoofing checks", including rejecting external email claiming to be from the customer's own domain and trusted associates, and by known bad URLs in the message text. SPAM Cracker can block emails based on general domain (*e.g.,* .ru, .ro, .kr), in blacklisted foreign languages. SPAM Cracker also supports whitelisting of allowable sending domains through its No Guess Domains™ capability. The virus filter included in SPAM Cracker is signature-based, and also filters out attachments with dangerous extensions, such *as .com* and .exe. SPAM Cracker is intended to be installed on an existing Linux-based Firewall or Linux Mail server, or on a dedicated hardware platform especially configured by Horizon Network Security.

Horizon Network Security SPAM Cracker

Type of Firewall	AF (Email)
OS	Runs on Linux (Included when firewall is purchased with hardware platform)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Horizon Network Security
Information	*http://www.verysecurelinux.com/virus.html*

IBM® WebSphere® DataPower XML Security Gateway XS40

Abstract

The IBM WebSphere DataPower XML Security Gateway XS40 is a network appliance that provides a security-enforcement point for XML-based/Web services transactions, including encryption, firewall filtering, digital signatures, schema validation, WS-Security, XML access control, XPath, and detailed logging. The XS40 includes an XML firewall and XML proxy with carrier-grade features that can parse, filter, validate schema, decrypt, verify signatures, access-control, transform, sign and encrypt XML message flows. The XML firewall includes XML DoS protection, field-level message security, and Web services access control, and provides protection against XML vulnerabilities by acting as an XML proxy and performing XML well-formedness checks, buffer overrun checks, XML schema validation, XML filtering, and XML DoS protection. This DoS protection is achieved by having the XS40 validate all incoming requests and log malformed and malicious traffic to enable post-attack forensics. The XS40's field level message security capabilities enables the gateway to share information selectively, through content-based routing, encryption/decryption, and signing/verification of entire messages or of individual XML fields. These granular and conditional security policies can be based on virtually any variable, including content, IP address, hostname, or other user-defined filtering criteria. The XS40's Web services access control provides access control functions which can be used to enable secure access to Web services based applications to both internal and external clients. Both commercial and standards-based integration is supported, including LDAP, Security Assertion Markup Language (SAML), and WS-Security. The XS40 also implements fine-grained authorization, whereby the gateway interrogates every individual SOAP/XML transaction and determines whether it should be allowed through based on payload contents, security policy, and identity information; this capability is implemented using SAML, WS-Security, and Extensible Access Control Markup Language (XACML), so that fine-grained access control can be achieved in an open, cross-platform environment which joins the XS40 with other vendors' policy enforcement points and central policy repositories. The XS40 supports legacy systems such as RADIUS and LDAP, along with SAML and XACML. Service virtualization, URL rewriting, high-performance XSLT transformations, and XML/SOAP routing enable the XS40 to transparently map a rich set of services to protected back-end resources. The XS40 supports centralized policy management, and uses XSLT to create sophisticated security and routing rules. The XS40 also works with leading Policy Managers such as IBM Tivoli® Access Manager, integrating with them *via* SNMP, script-based configuration, and remote logging. The security services of the XS40 can be extended to legacy applications by running the appliance in conjunction with the DataPower Integration Server XI50 or Integration Blade XI50 Appliance. The XI50 provides XML message transformation, integration, and routing functions for legacy (non-XML) applications, and includes its own message-level security and access control functionality enabling messages to be filtered, validated, encrypted, and signed using technologies that conform to WS-Security, WS-Policy, WS-SecurityPolicy, WS-ReliableMessaging, WS-SecureConversation, WS-Trust, SAML, and LDAP standards. The XI50 also provides process acceleration, which is critical for resource-intensive, high-latency XML processing. The XS40 in combination with the XI50 made of the Target of Evaluation for the NIAP EAL4+ certification of those products.

IBM WebSphere DataPower XML Security Gateway XS40	
Type of Firewall	AF (XML)
OS	Included (firmware)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10020*
Common Criteria	EAL4+ (XS40 with XI50)
Developer	IBM
Information	*http://www-01.ibm.com/software/integration/datapower/xs40/index.html*

Igaware Web Filtering Appliance

Abstract

Igaware Web Filtering Appliance performs blocking of predefined categories of inappropriate Web sites (*e.g.,* adult, gambling), with blocking configurable per-system or per-user. The Appliance also performs blocking of dangerous content downloads, such as .exe files. Blocking can be configured through whitelists and blacklists, and the Web filter's URL databases are continuously, automatically updated. Customers with Active Directory Servers can also integrate the Igaware Web filtering appliance with Active Directory-based single sign-on, which also enables granular per-user reporting about Web usage.

Igaware Web Filtering Appliance

Type of Firewall	WAF
OS	Runs on Linux
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Igaware, Ltd. (UK)
Information	*http://www.igaware.com/products/web-filtering-appliance.php*

IMGate Mail Firewall

Abstract

IMGate is an open source email firewall with antispam and antivirus in multiple layers. IMGate performs: (1) envelope filtering with sender verification, selective greylisting, reactive SMTP blocking, and blocking of unknown recipients; (2) content filtering, including antispam, antivirus, and graphic content filtering; (3) self-monitoring and Web interface monitoring; (4) support for SMTP over TLS; and many other features.

IMGate Mail Firewall

Type of Firewall	AF (Email)
OS	Runs on FreeBSD 7
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	IMGate Project
Information	*http://www.imgate.net*

Imperva SecureSphere Database Firewall

Abstract

SecureSphere Database Firewall protects databases from attacks, data loss and theft. With realtime monitoring, alerting and blocking, pre-built security policies and audit rules SecureSphere protects the most valuable database resources and ensures data integrity. By validating access requests and identifying material variance when users perform unexpected queries SecureSphere blocks exploit attempts. The firewall can run on a SecureSphere X1000, X2000, X2500, X4500, or X6500 hardware appliance, or on an Imperva virtual appliance (V1000, V2500, V4500).

Imperva SecureSphere Database Firewall

Type of Firewall	AF (Database)
OS	Included (virtual appliances also require VMware ESX/ESXi 3.5/4.0)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Imperva
Information	*http://www.imperva.com/products/dsc_database-firewall.html*

Imperva SecureSphere File Firewall

Abstract

SecureSphere File Firewall delivers realtime file security with policy-based alerting and blocking, access activity auditing, and user rights management for files stored on file servers and network attached storage devices. SecureSphere policies complement file server access control lists (ACLs) which often fall out of synch with corporate security policy. In addition to blocking unwarranted access, SecureSphere creates a comprehensive file activity audit record which can be used to accelerate security incident response and forensic investigations. SecureSphere File Firewall helps ensure access to sensitive file data is based on a business need-to-know by identifying existing user access rights and facilitating a complete rights review. The firewall can run on a SecureSphere X1000, X2000, X2500, X4500, or X6500 hardware appliance, or on an Imperva virtual appliance (V1000, V2500, V4500).

Imperva SecureSphere File Firewall

Type of Firewall	AF (FTP)
OS	Included (virtual appliances also require VMware ESX/ESXi 3.5/4.0)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Imperva
Information	*http://www.imperva.com/products/fsc_file-firewall.html*

Imperva SecureSphere Web Application Firewall

Abstract

Imperva SecureSphere Web Application Firewall protects applications from current and future security threats by combining multiple security engines to protect against the OWASP Top Ten, including SQL Injection, XSS, and CSRF. SecureSphere Web Application Firewall automatically learns protected application and user behaviors, and updates its own Web defenses with research-driven intelligence on current threats. As a result, the firewall blocks attempts to exploit known and unknown vulnerabilities, and identifies traffic originating from known malicious sources. SecureSphere Web Application Firewall correlates request attributes across security layers and over time to detect sophisticated, multi-stage attacks, and virtually patches vulnerabilities by integrating with Web application vulnerability scanners, thereby reducing the window of exposure and impact of emergency fixes. The firewall is PCI DSS 6.6 compliant, and has been certified by ICSA Labs. The firewall can run on a SecureSphere X1000, X2000, X2500, X4500, or X6500 hardware appliance, or on an Imperva virtual appliance (V1000, V2500, V4500).

Imperva SecureSphere Web Application Firewall

Type of Firewall	WAF
OS	Included (virtual appliances also require VMware ESX/ESXi 3.5/4.0)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Imperva
Information	*http://www.imperva.com/products/wsc_web-application-firewall.html*

Intel® SOA Expressway Service Gateway

Abstract

More than a security gateway, an enterprise service bus, an XML gateway, or an XML firewall, the Intel SOA [service-oriented architecture] Expressway delivers a set of features designed to integrate, mediate, secure, and scale XML-based services in a dynamically changing application perimeter. SOA Expressway provides (1) Runtime Governance to enforce service policies and ensure compliance, (2) Security proxy, XML firewall, Authentication, Authorization, and Accounting (AAA), and trust mediation; (3) Wire-speed XML parsing reinforced by Intel chip optimizations; (4) Sophisticated service mediation for XML and non-XML data; (5) tamper-resistant hardware appliance, virtual appliance, and extensible software appliance options.

Intel SOA Expressway Service Gateway

Type of Firewall	AF (XML)
OS	Included
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Intel Corporation
Information	*http://www.dynamicperimeter.com/products/xml-security-service-gateway*

Korsmeyer Extensible Messaging Platform

Abstract

The Korsmeyer Extensible Messaging Platform (EMP) protects for Microsoft Exchange Server, Lotus Domino, and GroupWise email servers against spam, phishing, and other undesirable email content, not only preventing them from reaching users' inboxes, but also achieving a very low false-positive, thereby minimizing the amount of questionable mail that is quarantined for user intervention. EMP uses contextual pattern signatures (not simple word/phrase lists) to identify unique patterns generated unsolicited commercial email messages that have been munged or cloaked to escape detection by standard spam filters. EMP also supports whitelisting of "always deliver" senders, and includes URL reputation filtering for embedded links within email solicitations.

Korsmeyer Extensible Messaging Platform

Type of Firewall	AF (Email)
OS	Runs on Windows Server 2003/2008 or 7; UNIX/Linux; Mac OS X
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	J.A. Korsmeyer, Inc.
Information	*http://www.jak.com/antispam/enterprise-mail-security.html*

Layer 7 SecureSpan™ XML Firewall

Abstract

The SecureSpan Firewall enables security of Web 2.0, SOA, and cloud-based systems by providing a centralized enforcement point for policy-driven identity, message level security, and auditing. The SecureSpan XML Firewall provides a centralized proxy for aggregating, managing and securing SOAP and Representational State Transfer (REST) APIs. The SecureSpan XML Firewall also provides simplified implementation of leading WS*, WS-I, SAML, and XACML standards without coding. The Firewall centralizes message-level security and policy operations, including availability-based routing, XML threat protection, data cleansing and redaction, WS*, WS-I, throttling, encryption, signing, and fine-grained access control. Changes to policy can be implemented dynamically across a cluster of XML security operations, and instituted as new or updated policy rules that apply to all applications.

Layer 7 SecureSpan XML Firewall

Type of Firewall	AF (XML)
OS	Appliance: Included; Software: runs on Solaris 10, SuSE [Gesellschaft für Software-und Systementwicklung mbH] or Red Hat Linux; Virtual Appliance: requires VMWare, VMWare ESX, or Amazon EC2 AMI in addition to OS
Format	Appliance or Software
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10207/*
Common Criteria	EAL4+
Developer	Layer 7 Technologies (Canada)
Information	*http://www.layer7tech.com/products/xml-firewall*

ModSecurity

Abstract

ModSecurity is an open source WAF for Apache developed by Trustwave's SpiderLabs. It allows for HTTP traffic monitoring, logging and realtime analysis. ModSecurity can support a variety of security models, including: (1) negative security model (blacklisting); (2) positive security model (whitelisting); (3) known weaknesses and vulnerabilities model, wherein ModSecurity drives patching of the systems it protects. ModSecurity includes a flexible rule engine that implements the ModSecurity Rule Language—a specialized programming language for specifying policy rules for dealing with HTTP transaction data. ModSecurity is delivered with a set of certified ModSecurity Core Rules that provide generic protection from unknown vulnerabilities often found in Web applications; the Core Rules implement general-purpose hardening, protocol validation, and detection of common Web application security issues. ModSecurity is designed to be embeddable in existing Apache-based Web servers, and can be deployed as part of an Apache-based reverse proxy server.

ModSecurity

Type of Firewall	WAF
OS	Runs on Linux, Windows, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X, HP-UX
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Trustwave SpiderLabs
Information	*http://www.modsecurity.org/*

MONITORAPP DB INSIGHT SG™

Abstract

MONITORAPP's DB INSIGHT SG is a hardware-based appliance that is installed as a proxy on the network to provide a database firewall solution that implements a positive security model for authorization of SQL requests (controlled at the database object, SQL command, and SQL statement levels) and database accesses (controlled at the individual IP/user, database/user, and connection/time levels). Policies, including blocking policies, are automatically generated *via* DB INSIGHT SG's SQL query self-learning capability and dynamic database profiling technique. The firewall also supports full auditing of local connections, with activity tracked by IP and database user. Availability and performance are assured through the hardware appliance's fail-over/fail-open features.

MONITORAPP DB INSIGHT SG

Type of Firewall	AF (Database)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	No (South Korea National Information Service)
Common Criteria	EAL4 *(http://service2.nis.go.kr/download.jsp?t=CERTIFY&id=GOOD&t2=doc&idx=751&subIdx=0&fn=20090501175915.pdf&dn=CISS-160-ST.pdf)*
Developer	MONITORAPP Co., Ltd. (South Korea)
Information	*http://www.monitorapp.com/pro/dis.html*

MONITORAPP Web INSIGHT SG™

Abstract

MONITORAPP's Web INSIGHT SG is a hardware-based gateway appliance that is installed as a proxy on the network to provide a Web firewall solution that can detect and block external hacking attempts and attempts to exploit Web application vulnerabilities in real time. Web INSIGHT SG provides (1) Web Server Cloaking to prevent hackers from analyzing by falsifying Web server responses; (2) Cookie Security that blocks data leakage by encoding cookies; (3) Data Loss Prevention; (4) Error Page Designation to block data leakage through an error page by designating a specific error page; (5) HTTPS Security that extends the appliance's Web security functions to the HTTPS-encoded traffic. Web INSIGHT SG supports the implementation of policies, including differentiated multi-domain policies regarding Multi-Domain, and provides blocking policies for all prohibited requests. It allows the administrator to define patterns for acceptable or unacceptable Web Protocol traffic, and auto-updates Web vulnerability patterns to block exploits targeting them. Web INSIGHT SG blocks a range of Web attack types using adaptive profiling defenses that do not rely on signatures; attack types blocked include encoding bypass attacks, cross-site scripting, SQL injection, command injection, file uploading, directory traversal, buffer overflow exploits, and application-level exploits. The system's management functions include (1) monitoring of the system's own central processor unit and memory, as well as Web traffic passing through the system; (2) log management and querying; (3) statistics and reporting functions for statistical analysis of the firewall logs on an hourly, daily, weekly, or monthly basis. Availability and performance are assured through fail-over/fail-open features and Web acceleration.

MONITORAPP Web INSIGHT SG

Type of Firewall	WAF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	No (South Korea National Information Service)
Common Criteria	EAL4 *(http://service2.nis.go.kr/download.jsp?t=CERTIFY&id=GOOD&t2=doc&idx=750&subIdx=0&fn=20090430145044.pdf&dn=NISS-0159-ST.pdf)*
Developer	MONITORAPP Co., Ltd. (South Korea)
Information	*http://www.monitorapp.com/pro/wis.html*

Netop NetFilter

Abstract

Netop NetFilter implements a dynamically updated Web content filter and blocks unwanted Web sites, can be configured to block unwanted downloads, IM, chat, and file sharing programs.

Netop NetFilter

Type of Firewall	WAF
OS	Proxy server: runs on Windows NT/2000/ Server 2003/Server 2008; eClient: runs on Windows 9x/Me/2000/XP/Vista
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Netop (Denmark)
Information	*http://www.netop.com/products/administration/netop-netfilter.htm*

Oracle® Database Firewall

Abstract

Oracle Database Firewall creates a defensive perimeter around databases, monitoring and enforcing normal application behavior, helping to prevent SQL injection attacks and attempts to access sensitive application data using unauthorized SQL commands. Oracle Database Firewall (1) monitors and blocks SQL traffic on the network with white list, black list and exception list policies; (2) protects against application bypass, SQL injection and similar threats; (3) reports on database activity for Sarbanes-Oxley, PCI and other regulations, choosing from dozens of out-of-the-box reports; protects Oracle, Microsoft SQL Server, IBM DB2 for Linux, Unix, and Windows, and Sybase databases. Oracle Database Firewall requires no changes to existing applications or databases.

Oracle Database Firewall

Type of Firewall	AF (Database)
OS	Runs on Oracle Enterprise Linux
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Oracle Corporation
Information	*http://www.oracle.com/technetwork/database/database-firewall/overview/index.html*

Phantom Technologies iBoss Enterprise Web Filter

Abstract

iBoss Enterprise Web Filter implements layer 7 application proxies and deep packet inspection to perform URL, Web, and Web 2.0 content filtering, as well as drive-by spyware protection, antiphishing/antipharming, blocking of spyware and keylogger backchannels. The appliance also performs IP and port blocking, authentication with Active Directory, LDAP, and single sign-on integration, QoS/bandwidth management, extensive reporting and user desktop monitoring. It is designed for business use.

Phantom Technologies iBoss Enterprise Web Filter

Type of Firewall	WAF
OS	Included (hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Phantom Technologies, Inc.
Information	*http://myiphantom.com/ibe_overview_to.html*

Phantom Technologies iBoss Home Internet Parental Control

Abstract

iBoss Home Internet Parental Control extends URL/Web content filtering, and antimalware/antiphishing protections similar to those in iBoss Enterprise Web Filter and iBoss Pro Internet Content Filter to all Internet-accessing computers and devices in a home. It does not include firewalling or QoS features, however, and its reporting and monitoring capabilities are less extensive. It is hosted on a small-footprint wireless router appliance.

Phantom Technologies iBoss Home Internet Parental Control

Type of Firewall	WAF
OS	Included (hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Phantom Technologies, Inc.
Information	*http://myiphantom.com/ibh_overview.html*

Phantom Technologies iBoss Pro Internet Content iFilter

Abstract

iBoss Pro Internet Content Filter provides similar antimalware and content filtering to iBoss Enterprise Web Filter, plus network firewall capability, but without QoS capabilities, and with less extensive monitoring and reporting capabilities. It is hosted on a small-footprint wireless router appliance. It is designed to be used in wireless hotspots and other businesses providing public Wireless Fidelity (Wi-Fi) access.

Phantom Technologies iBoss Home Internet Parental Control

Type of Firewall	WAF (with SIF)
OS	Included (hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Phantom Technologies, Inc.
Information	*http://myiphantom.com/ibp_overview.html*

PrismTech Xtradyne I-DBC IIOP Firewall

Abstract

PrismTech's Xtradyne I-DBC [IIOP Domain Boundary Controller] IIOP [Internet Inter-Object Request Broker Protocol] Proxy Firewall is a turnkey solution for IIOP firewalling and Common Object Request Broker Architecture (CORBA) security to eliminate the risks associated with the deployment of CORBA- and Enterprise Java Bean (EJB)-based applications on the Internet or other networks outside the firewall. The I-DBC acts as a security gateway (*i.e.,* CORBA firewall) that can be integrated transparently into existing systems without modification of the existing software; For J2EE Web applications, the I-DBC constitutes an additional security barrier between the Web Server and the EJB server. The I-DBC concentrates all incoming IIOP traffic on a single transport address (1 IP address/1 port). To make CORBA/EJB and NAT interoperate, the firewall automatically and transparently adapts CORBA/EJB object references to NAT translated addresses. The I-DBC performs strong authentication using a variety of techniques, authorization, auditing, and encryption (*via* SSL). For application level firewall security, the I-DBC performs deep packet inspection for all data streams expected to be IIOP messages and blocks all traffic with incorrect, malformed, or malicious content. The I-DBC protects the internal network and applications infrastructure from attacks, protects CORBA/EJB applications from misuse and unauthorized access, and protects IIOP messages in transit on the outside network from exposure and tampering. The Xtradyne IIOP firewall is delivered with all software components necessary to operate a corporate IIOP firewall (application-level gateway), including a bastion host, the Xtradyne Security Policy Server, and the Xtradyne Administration Console. In environments with a variety of installed software middleware, the IIOP DBC can be deployed together with the Xtradyne WS-DBC [Web Services Domain Boundary Controller].

PrismTech Xtradyne I-DBC IIOP Firewall

Type of Firewall	AF (CORBA/EJB)
OS	Runs on Linux/x86 (RHEL, SuSE variants); IBM/Sun Solaris 8+
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	PrismTech, Ltd. (UK)
Information	*http://www.prismtech.com/section-item.asp?id=733*

PrismTech Xtradyne WS-DBC

Abstract

Xtradyne WS-DBC is an XML Web Services (SOAP/WSDL) application-level firewall and WS-Security gateway with extended XML/WS-Security capabilities; as such, it sits at the domain boundary and hides Web services behind virtual service endpoints and inspects all SOAP messages, blocking messages with incorrect, malformed SOAP messages, or malicious XML content to protect against externally-originated threats to internal Web Services, including malformed messages and malicious content at the domain boundary (firewall, DMZ). WS-DBC provides all security functions needed for the detailed control of access to the company's XML based application systems. It performs authentication, authorization (user-, group-, role-, and/or content-based access control), and audit functions for all service requests, thereby protecting WS applications from misuse and unauthorized access. XML and SOAP messages (Web services content) are protected in transit over the network from eavesdropping and tampering through encryption (SSL at transport level, XML Encryption) and XML Digital Signature at the data field level. WS-DBC enables centralized security administration for XML Web Service-based application systems with large numbers of (internal and external) users. The WS-DBC also implements a policy enforcement point that can be integrated transparently without any modifications to existing Web Service software.

PrismTech Xtradyne WS-DBC

Type of Firewall	AF (XML)
OS	Runs on Linux/x86 (RHEL, SuSE variants); IBM/Sun Solaris 8+
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	PrismTech, Ltd. (UK)
Information	*http://www.prismtech.com/section-item.asp?snum=3&sid=290*

Privacyware ThreatSentry

Abstract

Implemented as an IIS ISAPI extension and snap-in to the Microsoft Management Console, ThreatSentry combines a Web application firewall with behavior detection and monitoring components to block activity that falls outside of trusted parameters. The ThreatSentry system/behavior profiling and comparative analysis engine extends the intrusion detection and prevention capabilities of conventional pattern matching, rules, and policy-based systems by enabling ThreatSentry to provide protection against both known and unknown threats, internal and external to the protected network. ThreatSentry supports single or multiple server environments and protects against an array of known exploits, including directory traversal, buffer overflow, DoS, SQL injection, parser evasion, high-bit shellcode, printer protocol, and remote data services. ThreatSentry also stops any other unusual activity falling outside acceptable patterns of usage. ThreatSentry comes pre-configured with a knowledgebase of known exploitive techniques and attack characteristics. This knowledgebase is complemented by an artificial intelligence-based neural behavioral engine that continuously learns typical system activity to establish a dynamic baseline. Each server connection is compared against the knowledgebase and system baseline to identify and take action against any activity falling outside trusted parameters. ThreatSentry's intrusion prevention capabilities progressively improve as the baseline evolves automatically or based on input from the system administrator. The ThreatSentry management console provides administrators granular control over configuration settings, trusted and untrusted event management, rule and signature definition, blocked IPs, alert notification and the sensitivity level of behavioral engine.

Privacyware ThreatSentry

Type of Firewall	WAF
OS	Runs on Windows Server 2000/2003/2007 with IIS Web Server and Microsoft Management Console
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Privacyware/PWI, Inc. (US/Russia)
Information	*http://www.privacyware.com/intrusion_prevention.html*

Proofpoint Email Firewall™

Abstract

The Proofpoint Email Firewall defends against spam and malicious connections by testing numerous connection-level data points, including DNS, mail exchange record verification, Sender Policy Framework, recipient verification, and Proofpoint Dynamic Reputation™ data. Policy enforcement enables organizations to define and enforce a wide variety of acceptable usage policies for message content and attachments. The Proofpoint Email Firewall comes standard with common filters and dictionaries to help establish new corporate messaging policies or support existing policies. Examples of acceptable usage policies that can be created include: maximum message size; allowable attachment types with attachment type verification; acceptable encryption policy; monitoring for offensive language; maximum number of recipients and/or attachments; custom disclaimers or footers automatically appended to messages and disclaimers in different languages (based on the language of the email). Both inbound and outbound email messages are monitored and classified in realtime, providing organizations with proactive control of their messaging infrastructures. Any suspected or noncompliant email is flagged and can be quarantined for further review or audit before exposing the company to any liability. A point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content. Proofpoint Email Firewall rules can compare message content with dictionaries in order to protect businesses from the use of inappropriate or offensive content and other issues that can surface through email usage. Key messaging analysis functions provided by the Proofpoint Email Firewall include: (1) Policy definition; (2) Realtime compliance monitoring of email message flow, including attachments; Enterprise classification to categorize filtered messages by compliance or content-related classification; Message handling options based on an organization's defined policies and classifications, to take action on messages that violate policies. Built-in attachment scanning capabilities allow organizations to apply Proofpoint Email Firewall policies to the contents of message attachments. Policies can be enforced on content in more than 300 types of attachments, including word processing documents (such as Microsoft Word), spreadsheets (such as Microsoft Excel worksheets), Adobe Portable Document Format (PDF) documents, presentation formats (such as Microsoft PowerPoint) and documents included in archives (including .zip, .gzip, .tar, and Transport Neutral Encapsulation Format formats). In addition to the hundreds of built-in document types that Proofpoint Enterprise's Email security features natively understand, administrators can use the Proofpoint File Type Profiler to add support for new, custom or proprietary file types (*e.g.,* proprietary computer-aided design/computer-aided manufacturing formats).

Proofpoint Email Firewall

Type of Firewall	AF (Email)
OS	Included
Format	Appliance or Software (or SaaS)
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Proofpoint, Inc.
Information	*http://www.proofpoint.com/products/technology/Email-security/Email-compliance.php*

Qualys® IronBee™

Abstract

IronBee is a new collaborative open source development project the objective of which is to build a Web application firewall sensor in the cloud that will be universally accessible. As of March 2011, development had been underway for a few months within Qualys; IronBee was officially launched as a public open source project on 14 February 2011. When completed, IronBee will implement a robust framework for application security monitoring and defense, with a layered set of features at different levels of abstraction, enabling its users to choose the approach that works best for the work they need to accomplish. The framework provides the starting point for determining the exact features to be implemented. Its capabilities include (1) flexible data acquisition options (*i.e.,* deployment modes); (2) personality-based data processing that matches the parsing quirks in the back-end; (3) persistent data model that mirrors real-life entities such as applications, sessions, users, and IP addresses and that allows both short-term and long-term activity tracking; (4) aggregation of historical data (from the internal data store) as well as the information from external data sources, such as geolocation information, IP address reputation; (5) user agent profiling; (6) data retrieval and transformation engine that provides transparent optimization and rule prequalification, ensuring that no time is spent on needless or repetitive work; (7) multiple pattern matchers and support for streaming inspection; (8) a choice of approaches to implement custom security logic including flexible rule language suitable for 80% of all work, high-performing scripting platform (based on Lua) for the next 19%, support for compiled modules for the 1% of cases in which performance is of the highest importance; (9) inbound and outbound traffic analysis of protocol compliance (blacklisting and whitelisting), common attack techniques, evasion techniques (at the protocol and application levels), known exploits, exploitation of vulnerabilities in popular applications (*via* whitelisting), information leakage, error message detection; (10) virtual patching (*via* whitelisting); (11) higher-level security modules such as behavioral monitoring of IP addresses, sessions, and users, brute force detection, and DoS/Distributed DoS (DDoS) detection, cookie encryption/signing, content security policy enforcement, passive vulnerability scanning, user experience monitoring, and XML parsing/validation; (12) policy decision-making; (13) tailored defense; (14) interaction with external security systems (*e.g.,* firewalls) and data exchanges.

Qualys IronBee

Type of Firewall	WAF
OS	Included
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Qualys
Information	*https://www.ironbee.com*

Radware AppWall®

Abstract

Radware's AppWall is a Web application firewall appliance that secures Web applications and enables PCI compliance by mitigating Web application security threats, including all OWASP Top Ten threats including cross-site scripting, cross-site request forgery, broken authentication and session management, and security misconfiguration exploits. The firewall also protects against exploitation of known Web application vulnerabilities, data leaks, and zero-day attacks, and HTTP protocol exploits and evasion techniques. AppWall includes a rich set of XML and Web services security protections, including XML validity checks, Web services methods restrictions, and XML structure validation (to enforce legitimate SOAP messages and XML payloads). AppWall's DLP fully addresses PCI DSS 2.0 Requirement 6.6.

Radware AppWall

Type of Firewall	WAF + XML AF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Radware (Israel)
Information	*http://www.radware.com/Products/ApplicationDelivery/AppWall/default.aspx*

RedCondor Message Assurance Gateways

Abstract

RedCondor Message Assurance Gateways (MAGs) are network appliances that block both inbound and outbound spam, viruses (through multiple virus scanning engines), spyware, phishing, and other malicious email content before they can reach a mail server. The antispam appliance also provides a network perimeter defense system that implements greylisting and protects servers and network resources against DoS and directory harvest attacks. Suspicious email is separated from normal email stream and stored in a Web-based quarantine for up to 35 days. The MAG also provides email spooling for up to 96 hours in case of an email server outage. TLS encryption is provided as an option to protect emails processed by the MAG from unintended disclosure. Red Condor currently offers five spam filtering appliances ranging from the low-end MAG2000 to the MAG4000, which can manage more than 20,000 mailboxes and is scalable to hundreds of thousands of mailboxes when configured in a clustered multi-appliance architecture. The MAG's Vx technology implements automatic failover, and enables the MAG to be integrated into a cloud-based Hosted service.

RedCondor Message Assurance Gateways

Type of Firewall	AF (Email)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	RedCondor/St. Bernard Software, Inc.
Information	*http://www.redcondor.com/products/email-appliance.htm*

Retell Sense Voice Firewall

Abstract

Retell's Sense Voice Firewall is an anti-fraud system that is installed (in the digital video disc [DVD] drive bay of a PC positioned) between the phone system and the network termination box to monitor dialed calls and electronically disconnect any pre-set unauthorized numbers. The main features of the Sense Voice Firewall are: (1) realtime prevention of Private Automatic Branch Exchange toll fraud; (2) blocking (non-connection) of unauthorized numbers preventing connection; (3) prevention of unauthorized calls to predetermined numbers during office hours; (4) issuing an "unobtainable" number tone to blocked the callers; (5) configurable policy rules for out of hours outbound dialing, *e.g.,* to enable only calls to the emergency services for out of hours workers; (6) blocking all unspecified international numbers, 09xx and 08xx numbers, *etc.*; (7) limiting the number of incoming and outgoing out-of-hours calls.

Retell Sense Voice Firewall

Type of Firewall	AF (Voice)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Retell, Ltd. (UK)
Information	*http://www.retellrecorders.co.uk/recording/equipment/tollfraud.htm*

SafeNet® eSafe Mail Security Gateway

Abstract

SafeNet eSafe Mail Security Gateway uses a dual antispam engine with realtime reputation and deep content analysis to block spam and virus outbreaks. It also includes a user self-managed spam quarantine. The Gateway's dual antivirus engine with proactive and signature based detection blocks viruses, spyware, and malware. The gateway enables administrators will be able to assign granular security and spam policies to LDAP and Active Directory users and groups. Outbound emails and attachments are inspected to allow granular policy enforcement, preventing leakage of sensitive information. Administrators can create data leak prevention policies for LDAP/Active Directory users and groups.

SafeNet eSafe Mail Security Gateway

Type of Firewall	AF (Email)
OS	Included (Virtual appliance requires VMware)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SafeNet
Information	*http://www.safenet-inc.com/products/data-protection/content-security/esafe-mail-security-gateway*

SafeNet® eSafe Web Security Gateway

Abstract

eSafe Web Security Gateway works in realtime to filter malicious content in HTTP and FTP traffic as it enters the network, and monitors all outgoing traffic with advanced DLP features to keep information from leaking out of the organization. Modules for eSafe Web Security Gateway include: Security (includes antimalware antispyware, and antivirus); Application and Web 2.0 Control (includes AppliFilter); DLP; Content Filtering (includes URL filtering); SSL inspection; Antispam and Antiphishing; and Management and Reporting. The Application and Web 2.0 Control module provides (1) policy based control over malware/spyware "call-home" communications, P2P file sharing, IM chat and file transfer, unauthorized protocol tunneling, application (Layer 7) protocol enforcement; granular policies for appropriate Web 2.0 usage in an organization; (3) supports all the most popular Web 2.0 sites; (4) prevents Web 2.0 phishing, malware, exploits, *etc.*; (5) prevents bypassing security and content filtering policies by anonymizing proxies and applications; (6) granular security and spam policies to LDAP/Active Directory users and groups. The Content Filtering module prevents access to unauthorized, inappropriate, and malicious Web sites (more than 150 million categorized Web sites in 70 categories, with blacklist updates occurring every 2 hours). Content Filtering also controls more than 30 streaming media types by Web site category, and can be configured to fully block or merely issue a warning message to the user. The Gateway's SSL Inspection capability provides a transparent trusted man-in-the-middle to decrypt and perform deep inspection of SSL-encrypted traffic to prevent use of SSL tunneling to bypass security controls, leak sensitive data, or deliver malicious content.

SafeNet eSafe Web Security Gateway

Type of Firewall	WAF
OS	Included (Virtual appliance requires VMware)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SafeNet
Information	*http://www.safenet-inc.com/products/data-protection/content-security/esafe-web-security-gateway*

seaan.net MXtruder

Abstract

seaan.net MXtruder is hosted in front of the network firewall to filter spam and malware out of inbound email. Certain layers of the mail transfer agent header and content analysis functionality can be switched on or off as desired. MXtruder runs on a secure, high availability platform that protects against attacks such as DoS, buffer overflow exploits, and directory harvesting.

seaan.net MXtruder

Type of Firewall	AF (Email)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	seaan.net AG (Switzerland)
Information	*https://www.mxtruder.com*

SPAMINA Email Service Firewall and Email Service Firewall for MSP/ISPs

Abstract

The SPAMINA Email Service Firewall for MSP/ISPs [managed service providers/Internet service providers] is designed for deployment in private cloud computing environments. It provides multidomain antispam filtering and antiphishing and antimalware protection (the latter including perimeter virus scanning with optional quarantine accessible only by the administrator) for both incoming and outgoing email, plus antispam filtering. It also provides directory attack protection *via* delay and greylisting technologies. SPAMINA Email Service Firewall uses connection and sender filtering, heuristic, Bayesian, and content filters (SpamAssassin, BogoFilter). The email firewall policy is based on defined usage and configuration rules. The firewall can also provide complete backup of incoming email messages, and collects and reports email traffic and user activity statistics. SPAMINA performs dynamic updating of the firewall components, with realtime updating of spam filters. SPAMINA Email Service Firewall for MSP/ISPs is configured to enable ISPs or large integrators to offer email security services based on the SPAMINA Email Service Firewall.

SPAMINA Email Service Firewall and Email Service Firewall for MSP/ISPs

Type of Firewall	AF (Email)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SPAMINA/Aegis Security Group (Spain)
Information	*http://www.spamina.net/web/02products/cloud-email-firewall/spamina-email-firewall/?lang=en* *http://www.spamina.net/web/02products/cloud-email-firewall/spamina-email-service-firewall-for-mspisp%C2%B4s/?lang=en*

SpamTitan

Abstract

SpamTitan protects email systems and networks from spam, viruses, Trojans, phishing attacks, and unwanted content. SpamTitan incorporates multiple antivirus engines, including ClamAV and Kaspersky Labs, and performs multilayered antispam analyses that result in a high level of spam detection with a low false positive rate. SpamTitan also performs scanning and content filtering of inbound and outbound email, the latter providing data loss prevention. Other features include email disclaimer capability; end user spam management *via* email quarantine reports; automated updating including antivirus, antispam, version releases, and system backups; LDAP, dynamic, and alias-based file recipient verification. SpamTitan comes in two versions: SpamTitan ISO and SpamTitan for VMware. Both have identical functionality, operating systems, and support costs, but whereas SpamTitan ISO is a complete operating system and software suite image, SpamTitan for VMware® has tailored this software image to run on VMware. SpamTitan Cluster enables the deployment and management of a multinode cluster of SpamTitan for VMware virtual appliances.

SpamTitan

Type of Firewall	AF (Email)
OS	Included
Format	Software
License	Freeware (Commercial)
NIAP Validated	
Common Criteria	
Developer	SpamTitan/CopperFasten Technologies (Ireland)
Information	*http://www.spamtitan.com*

SpamWall Antispam Firewall

Abstract

Positioned in front of an existing email server, the SpamWall Antispam Firewall system provides integrated email antispam and antivirus protection at the "network perimeter" level, before unwanted or potentially dangerous email can enter the network or reach the mail server. Out of the box SpamWall is able to block and filter the majority of spam and unsolicited commercial email, as well as virus-infected emails. There are four different SpamWall models: SpamWall Lite, SpamWall Corporate/SME, SpamWall ISP/ Webhost, and SpamWall Enterprise, capable of handling capacities ranging from a few hundred messages per day up to 30 million messages per day.

SpamWall Antispam Firewall

Type of Firewall	AF (Email)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SpamWall Systems (Canada)
Information	*http://spamwall.com*

Trustwave WebDefend®

Abstract

Trustwave WebDefend is a Web application firewall appliance that provides Web applications with realtime, continuous security against attacks and data loss, and ensures they operate as intended and help them comply with industry regulations such as the PCI DSS. Using bi-directional traffic analysis, automated behavioral profiling and multiple collaborative detection engines, WebDefend identifies Web application security and availability issues, providing detection of and protection against both known vulnerabilities and emerging threats such as site scraping, malicious bots, Google hacking, and zero-day and targeted attacks. WebDefend inspects traffic entering and leaving the Web application, correlating the data from multiple attack detection engines. In this way WebDefend ensures that only valid traffic is allowed in or out of the protected Web application(s). The firewall monitors inbound uncompressed and compressed profile HTML, XML, and SOAP traffic, and inspects outgoing traffic to detect possible data loss, defacement, and security information disclosures. Application layer signatures provide actionable information on detected vulnerabilities, while realtime integrity and security issue detection catches programming mistakes, application errors, and non-secure code. The firewall also provides Web application performance monitoring for realtime visibility into the performance of Web applications at the site, URL, and session level. Three models of Trustwave WebDefend appliances are available, two that come standard with RAID support; in addition a high-availability option is available to add redundant sensors and managers for continuity of operations.

Trustwave WebDefend

Type of Firewall	WAF
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Trustwave
Information	*https://www.trustwave.com/web-application-firewall.php*

Vicomsoft InterGate Policy Manager

Abstract

Vicomsoft InterGate Policy Manager has many security features that interoperate with existing firewall installations. However, for small businesses and home businesses that have inadequate or no firewall protection, InterGate Policy Manager default settings can be configured to provide such firewall protection. InterGate implements a server-based SIF with Dynamic Host Configuration Protocol (DHCP), DNS, connection fallback and teaming, remote access server, and router capabilities. In addition to its firewalling capability, InterGate Policy Manager provides Web protocol, URL, application (including Skype, P2P file sharing, IM), and content filtering, as well as antispam and antivirus filters for email. InterGate Policy Manager also enables blocking or allowing access to such applications/URLs based on time of day.

Vicomsoft InterGate Policy Manager

Type of Firewall	WAF (with SIF)
OS	Runs on Windows 2000, XP, 2003; Mac OS X 10.4+
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Vicomsoft, Ltd./Keyfort, Ltd. (UK)
Information	*http://www.vicomsoft.com/products/firewall/index.html*

webScurity WebApp.secure™

Abstract

The WebApp.secure™ line of Web application firewalls use patent-pending Web/insite™ technology to examine HTTP traffic that flows freely through conventional perimeter defenses and compare that traffic to the protected Web site's Intended Use Guidelines™ (rules). Traffic that does not strictly adhere to the Intended Use Guidelines is automatically blocked and reported. By implementing a whitelisting approach to allowable HTTP content, Web/insite is also able to block both known and unknown HTTP-based worms and viruses, as well as attacks against application business logic, including SQL injection, URL parameter-tampering, and cookie-tampering. In addition to WebApp.secure Standard Edition and WebApp.secure Professional Edition, WebScurity offers WebApp.secure™ LiveCD, which provides a small International Organization for Standardization (ISO) image that can be used to boot any x86-based computer from compact disc (CD; native or within a VM), free of charge to organizations that want to become familiar with Web application firewall technology before purchasing.

webScurity WebApp.secure

Type of Firewall	WAF
OS	Runs on Windows 2000/2003/2007, Linux (including IBM System i, p, & z), Solaris, Mac OS X, and QNX
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	webScurity
Information	*http://www.webscurity.com/products.htm*

Aker Firewall

Abstract

The Aker Firewall implements NAT with load balancing (1-1, N-1 and 1-N or cardinalities) and Port Address Translation (PAT), and provides an HTTP proxy for filtering content and detecting viruses (normal and transparent modes), an FTP proxy with user authentication and individual and group based access control (transparent mode), SMTP/POP3 proxies for filtering email content (transparent mode). The system protects against many types of DoS, scanning, spoofing, and server attacks, and enables limiting of the number of simultaneous connections to specified source or destination IPs, for protecting against viruses and worms. The Firewall provides site-to-site and endpoint-to-site IPsec or Aker-CDP VPN using 1024-bit X.509 certificates and encryption *via* DES, 3DES, Blowfish-128, Blowfish-256, AES-128, AES-256, or proprietary encryption algorithms. The VPN's 802.1q support ensures that a single network card NIC can operate multiple VLANs. User authentication support is *via* RADIUS, Windows authentication, UNIX/Linux authentication, LDAP, or token-based authentication (smart cards, Rainbow, Aladdin, SecurID). The Aker Firewall also provides multiserver load balancing between firewalls (up to 64 firewalls), plus a Multilink Module that allows the firewall to perform network traffic load balancing among different operators' links, as well as clustering (master/slave) for fault tolerance/availability, QoS bandwidth control, and easy integration with other Aker network security modules (*e.g.,* URL Content Analyzer VPN, antivirus). Centralized management of security policies is supported for up to 64 firewalls simultaneously.

Aker Firewall

Type of Firewall	VPN firewall (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Aker Security Solutions (Brazil)
Information	*http://www.akersecurity.com/005/00502001.asp?ttCD_CHAVE=12895*

Alcatel-Lucent VPN Firewall Brick™

Abstract

The Alcatel-Lucent VPN Firewall Brick™ portfolio comprises a series of security appliances that integrate high-speed VPN, VoIP security, virtual LAN (VLAN), and virtual firewall capabilities, along with QoS bandwidth management features, a built-in IDS, and DoS protection. The VPN Firewall Brick security appliances are available in sizes suitable for small business networks up to large enterprise data centers and network edge environments. The appliance provides DDoS attack protection, support for the latest IPsec Key Exchange (IKE) v2 standards, strong authentication, and realtime monitoring, logging, and reporting. Multiple VPN Firewall Brick appliances can be centrally configured and remotely managed from a single console, using the Alcatel-Lucent Security Management Server (SMS) software. The Firewall Brick also includes an application filtering capability for deep packet inspection for command and application protocol validation, protocol anomaly detection, dynamic channel pinholes, and application-layer address translation. Application filters include HTTP, FTP, RPC, Trivial FTP (TFTP), H.323/H.323 Registration, Admission and Status, SMTP, Oracle SQL*Net, NetBIOS, Encapsulation Security Protocol, DHCP Relay, DNS, Group Transport Protocol, SIP, RTSP, and Alcatel-Lucent OmniPCX New Office Environment. In addition to its NIAP/Common Criteria EAL4+ validation, the VPN Firewall Brick has been ICSA Labs v4.1 Firewall and IPsec 1.3 certified, and FIPS 140-2-certified (VPN Firewall Brick 1200 Release 2; Release 3 certification pending).

Alcatel-Lucent VPN Firewall Brick

Type of Firewall	VPN firewall (with WAF)
OS	Included (Inferno™)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10308*
Common Criteria	EAL4+
Developer	Alcatel-Lucent (France)
Information	*http://enterprise.alcatel-lucent.com/docs/?id=7482*

Arkoon Security FAST360 Network Processor Appliances

Abstract

Arkoon's FAST360 Network Processor Appliances integrate a range of security technologies, including firewall, VPN, antivirus, antispam, Web filtering, together with network services (NAT, VLAN, dynamic routing) and QoS features (bandwidth management, link load balancing). FAST360 appliances range in size to support small businesses and branch offices up to large central offices. The FAST360's firewall engine is based on Arkoon's patented Fast Application Shield Technology, which performs realtime compliancy analysis of network, transport and application layer protocols (20 application layer modules are included with the firewall). The firewall includes an integrated IDS/IPS that detects attacks on applications based on contextual signatures. The firewall protects against phishing, malware, and abuse of tools such as Skype (hidden channels), P2P, and IM. The firewall also provides voice data protection (VoIP flows) *via* an analysis of voice data transport and signaling protocols (SIP, Media Gateway Control Protocol, Session Description Protocol, H.323, Realtime Transfer Protocol/Realtime Transport Control Protocol) and performs adaptive filtering to verify data flows against signaling flow. The voice firewalling feature can detect and/or isolate incoming and outgoing calls that are undesirable or non-compliant with policy, and can block call and IM spamming. The appliance also performs antivirus and antispyware scanning of SMTP, POP3, HTTP, and FTP traffic (Sophos antivirus/antimalware is integrated), as well as email filtering and antispam (using Commtouch technology). The FAST360 also performs URL and Web content filtering that can block a wide range of Web objects (JavaScript, ActiveX, URLs) across 50 categories, and block undesirable and dangerous content. The FAST360 also includes an IPsec VPN Gateway, network services including dynamic and static routing, VLAN and DHCP management, and Diffserv-compliant QoS. Performance and availability features include traffic optimization by flow prioritization, queue Management, and load balancing, and a clustering capability that allows parallel redundant appliances to be implemented for increased availability.

Arkoon Security FAST360 Network Processor Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	No (Agence nationale de la sécurité des systèmes d'information [SSI])
Common Criteria	EAL2+ *(http://www.commoncriteriaportal.org/files/epfiles/2004_33.pdf)*
Developer	Arkoon (France)
Information	*http://www.arkoon.net/-FAST360,111-.html*

Astaro™ Security Gateways

Abstract

Astaro Security Gateways provide comprehensive enterprise-class security applications including firewall, VPN, IPS, antivirus, antispam, email encryption, Web filter, WAF, and wireless security. All functions are integrated and run on hardened Linux on standard Intel-compatible servers or Astaro appliances. The same set of security applications, including active-active clustering, WAN link balancing, and Active Directory integration, is available on every model whether deployed as hardware, software, or virtual appliance, so even the smallest sites can obtain the same safeguards as central offices. Each Astaro Security Gateway is delivered with a free license for the Astaro Essential Firewall—a stateful packet inspection firewall that also performs secure routing, secure remote access, and networking functions. Additional security gateway functions can be purchased by subscription. These are: (1) Astaro Network Security, a configurable IPS that also includes flood protection against DoS attacks and comprehensive IPsec and SSL tunneling mechanisms for building site-to-site and remote access VPN connections (Astaro also offers licenses for VPN clients that interoperate with the Astaro Network Security VPN) ; (2) Astaro Mail Security, eliminates spam, viruses, and privacy issues from email messages before delivery to their addressees; (3) Astaro Web Security blocks spyware and viruses from entering the network in inbound Web protocol traffic or downloads; (4) Astaro Web Application Security protects Web servers and applications from attacks such as SQL injection and cross-site scripting; (5) Astaro Wireless Security simplifies the operation of secure and reliable wireless networks by implementing configuration-less access points that operate in combination with the built-in wireless controller in the Astaro Security Gateway. Every Astaro Security Gateway appliance model includes an integrated hard drive for local spam quarantine and log/reporting storage. Astaro Security Gateways are specifically designed to fulfill the needs of small to medium-sized businesses.

Astaro Security Gateways

Type of Firewall	Multifunction (with SIF [+ WAF & Email AF options])
OS	Included (hardened Linux); Virtual appliance version also requires VMware player, workstation, server, or ESX server
Format	Appliance or Software
License	Commercial
NIAP Validated	No (BSI)
Common Criteria	EAL2+ *(http://www.commoncriteriaportal.org/files/epfiles/0219a.pdf)*
Developer	Astaro GmbH & Co. KG (Germany)
Information	*http://www.astaro.com/en-us/resources/datasheets*

Barracuda® NG Firewall

Abstract

The Barracuda NG Firewall provides application-aware traffic management and prioritization across the WAN, with adaptive routing based on network traffic conditions and link status. Barracuda NG Control Center enables administrators to monitor VPN tunnels and firewall status. Standard Barracuda NG Firewall functions include: a stateful packet inspection firewall, IPS, IPsec VPN, intelligent traffic flow control, and AF. The following optional functions can be added to some or all NG Firewall models except for the low-end F10: Web security module, Web filtering module, malware protection module, SSL VPN and NAC (network access control; not available for Model F100), secure Web proxy (Models F600, F800, and F900 only). The Barracuda NG Firewall's stateful packet inspection module includes TCP proxy and NAT capabilities. The firewall's WAF module can identify and enforce security policies on applications that "hide" their traffic inside HTTP, IM, and P2P protocols. The Barracuda NG Firewall enables enforcement of policy based on user ID, group affiliation, location, and time of day. Policy actions include reporting, blocking, throttling, or enabling/disabling of specific application features. The NG Firewall's client-to-site and site-to-site VPN services can support an unlimited number of VPN client licenses. The IPS monitors network and system activities for malicious or suspicious behavior and reacts in realtime to block or prevent those activities by dropping the offending packets while allowing all other traffic to pass. Additional security options for various Barracuda NG Firewall models include: Web filters, antimalware protection, Web security, SSL VPN/NAC, and secure Web proxy. The SSL VPN and NAC option adds a customizable Web portal-based SSL VPN capability and NAC requiring a Windows client to satisfy a set of minimum security prerequisites (*e.g.,* Windows patch level, presence of antivirus and/or antispyware, user ID) before being allowed to access the network or routed to a quarantine network. Various NG Firewall F800 and F900 models are available with 1-4 optional Small Form-factor Pluggable network ports (Mini-Gigabit Interface Connector) that enable the firewall to be connected to 1Gbps fiber optic or copper networks or 10Gbps fiber optic networks. Other models are equipped with built in Wi-Fi access points (802.11b and 802.11g) that support bandwidth of up to 108Mbps. Included "click-through and login portal" functions enable kiosk style Internet or network access.

Barracuda NG Firewalls

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Barracuda Networks AG (Sweden)
Information	*http://www.barracudanetworks.com/ns/products/ng_firewall_overview.php*

BluegrassNet Voice SP100 Firewall/SIP Proxy

Abstract

BluegrassNet Voice SP100 Firewall/SIP Proxy is a stateful, pfSense-based packet inspection firewall for VoIP networks that includes a SIP proxy and media proxy daemon. The SP100 sets the DSCP markings of egress RTP packets to "Expedited Forwarding" for QoS, supports implementation of 802.1Q VLANs, and implements a DHCP Server for phone provisioning. It performs traffic shaping to reserve bandwidth for voice and other services, and implements a VPN server and client (PPTP, IPsec, OpenVPN. Advanced firewalling features include Universal Plug and Play [UPnP]), time servers, and dynamic DNS.

BluegrassNet Voice SP100 Firewall/SIP Proxy

Type of Firewall	VPN firewall (with SIF for VoIP)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	BluegrassNet Voice
Information	*http://www.bgnv.net/sip-proxy-sp100*

Check Point Power-1™ Appliances

Abstract

Check Point Power-1 appliances combine the Check Point firewall, IPsec VPN, and IPS with acceleration and networking technologies to provide a security gateway for multi-Gbps networks. Available security features are provided through Check Point's "Software Blades", *i.e.,* functional modules that can be installed on a variety of Check Point appliances or in virtualized software environments. Software Blades preconfigured in the Power-1 appliances include firewall, IPsec VPN, IPS, and various performance and advanced networking features. The Firewall Software Blade provides access control, application security, authentication, and NAT. The IPsec VPN Software Blade provides secure connectivity to corporate networks, remote and mobile users, branch offices and business partners by integrating access control, authentication, and encryption for network connections tunneled over the Internet. The IPS Blade is a multi-method threat detection engine that provides antimalware, anti-worm and other anti-threat protections for clients, servers, and operating systems.

Check Point Power-1 Appliances

Type of Firewall	Multifunction (with SIF)
OS	Included (SecurePlatform)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10329*
Common Criteria	EAL4+
Developer	Check Point
Information	*http://www.Check Point.com/products/power-1/index.html*

Check Point IP Appliances

Abstract

All Check Point IP appliances are preconfigured with the following Check Point Software Blades: firewall, IPsec VPN. All but the low-end IP282 also come preconfigured with Software Blades for application control, IPS, identity awareness, and acceleration/clustering and advanced networking. In addition, all IP Appliances support the following optional Blades: Web security; VoIP.

Check Point IP Appliances

Type of Firewall	Multifunction (with SIF)
OS	Included (IPSO)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10137*
Common Criteria	EAL4+
Developer	Check Point
Information	*http://www.checkpoint.com/products/ip-appliances/index.html*

Check Point Safe@Office UTM Appliances

Abstract

Check Point Safe@Office UTM appliances are preconfigured with the Check Point stateful packet inspection firewall, IPS, IM and P2P blocking/monitoring, port-based/tag-based virtual LAN, 802.1x Network Access Control, integrated RADIUS server, and secure wireless hotspot functionality. VPN support includes remote access clients (*via* Check Point VPN-1® SecureRemote™ L2TP, IPsec VPN, and Endpoint Connect VPN clients), L2TP VPN server, a range of IPsec features, and site-to-site VPN and remote access VPN, with support for up to 400 VPN tunnels. "Add-on services" include antivirus for HTTP, FTP, Network Basic Input/Output System over TCP/IP, POP3, Iterative Message Passing Algorithm, SMTP, and user-defined TCP and UDP ports, antispam, and Web filtering. Wireless security features include VPN over wireless, Wired Equivalent Privacy, Wi-Fi Protected Access 2 (802.11i), Wi-Fi Protected Access-Pre-Shared Key, and 802.1x. Availability features include backup ISP, load balancing, traffic shaping (for QoS), automatic gateway failover, and dialup backup.

Check Point Safe@Office UTM Appliances

Type of Firewall	Multifunction (with SIF [+ WAF option])
OS	Included (SecurePlatform hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Check Point
Information	*http://www.checkpoint.com/products/safe@office-utm-appliances/index.html*

Check Point Series 80 Appliance

Abstract

The Check Point Series 80 Appliance comes preconfigured with the Check Point firewall and IPsec VPN. IPS, antispam and email security, antivirus/antimalware, and URL filtering "Software Blades" are also available as options.

Check Point Series 80 Appliance

Type of Firewall	VPN firewall (with SIF [+ WAF & Email AF options])
OS	Included (SecurePlatform hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Check Point
Information	*http://www.checkpoint.com/products/series-80-appliance/index.html*

Check Point UTM-1™ Appliances

Abstract

All Check Point UTM-1 security appliances are preconfigured with the following Check Point Software Blades: firewall, IPsec VPN, network and endpoint policy management, and logging and status reporting. Additional Software Blades are available (in some appliances, they come preconfigured; in others they must be purchased as separate options), including: application control, identity awareness, IPS, data loss prevention, antivirus/antimalware, antispam/email security, URL filtering, Web security/object and content filtering, monitoring, and various networking and performance/availability features.

Check Point UTM-1 Appliances

Type of Firewall	Multifunction (SIF [+ WAF option])
OS	Included (SecurePlatform)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/cc-scheme/st/vid10329*
Common Criteria	EAL4+
Developer	Check Point
Information	*http://www.checkpoint.com/products/utm-1-appliances/index.html*

Cisco ASA 5500 Series Adaptive Security Appliances

Abstract

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, and 5585-X Adaptive Security Appliances. All ASA 5500 Series appliances integrate application-aware firewall, SSL/Datagram TLS and IPsec VPN (clientless and AnyConnect VPN features are licensed on a per seat and per feature basis), IPS with global correlation and guaranteed coverage, antivirus, antispam, antiphishing, and Web filtering services, and realtime reputation technology to deliver network- and application-layer security protection, user-based access control, worm mitigation, malware protection, IM and P2P control, and secure remote user and site connectivity. In addition, the Cisco ASA 5585-X model includes always-on secure mobility with integrated Web security and IPS for policy enforcement and threat protection. Using Cisco Multi-Processor Forwarding, the Cisco ASA 5500 Series enables highly customizable, flow-specific security policies to be tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series is enhanced through user-installable Security Services Modules. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention and Content Security and Control Security Services Modules. As business needs grow, customers can install a Security Plus upgrade license, enabling the Cisco ASA 5505 to scale to support a higher connection capacity and up to 25 IPsec VPN users, add full DMZ support, and integrate into switched network environments through VLAN trunking support. The upgrade license also allows support for redundant ISP connections and stateless active-standby high-availability services.

Cisco ASA 5500 Series Adaptive Security Appliances

Type of Firewall	Multifunction (with WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid6016* *http://www.niap-ccevs.org/st/vid6016/maint173* *http://www.niap-ccevs.org/st/vid6016/maint187* *http://www.niap-ccevs.org/st/vid6016/maint191*
Common Criteria	EAL4
Developer	Cisco
Information	*http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html*

Cyberoam® UTM Appliances

Abstract

Cyberoam UTM appliances offer assured security, connectivity and productivity to organizations by allowing user identity-based policy controls. Cyberoam's User Layer 8 Technology treats user-identity as the 8th Layer (the human layer) in the protocol stack. It attaches user identity to security, taking organizations a step ahead of conventional solutions that bind security to IP-addresses. Layer 8 technology functions along with each of Cyberoam security features to allow creation of identity-based security policies. Cyberoam UTM appliances include a SIF that performs deep packet inspection and protects against DoS, DDoS and IP Spoofing. In addition to the SIF module, the UTM appliances include the following modules: VPN (SSL and IPsec), IPS, antivirus, antispyware, antispam, Web content filtering, bandwidth management, application visibility and control, Third Generation Wireless Format/Worldwide Interoperability for Microwave Access connectivity (Cyberoam offers Wi-Fi appliances), IM archiving and controls, and on-appliance reporting. All appliances provide multiple link management and are IPv6-ready. Cyberoam's multi-core technology allows parallel processing of all its security features. Its Extensible Security Architecture offers a security platform that can grow with the future security needs of an organization without degrading system performance. The UTM Appliance's extensible security architecture supports feature enhancements that can be developed rapidly and deployed with minimal effort.

Cyberoam UTM Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Cyberoam (India)
Information	*http://www.cyberoam.com/utmoverview.html*

Clavister® Enterprise Security Gateway Series

Abstract

Clavister offers a series of stateful firewall appliances that perform deep packet inspection and provide built-in VPN connectivity, with optional support available for intrusion detection and prevention, antivirus, antispam, and Web content filtering. The Clavister Enterprise Security Gateway product line includes appliances for use in large telecom installations, corporate headquarters and large enterprises, small and medium-sized businesses, home offices, and virtualized cloud environments. Clavister also offers the same UTM gateway functionality in its Virtual Security Gateway series which are designed to run in a VMware virtualized environment; in this configuration, the Gateway can also provide firewall protection between virtual server instances.

Clavister Enterprise Security Gateway Series

Type of Firewall	Multifunction (with WAF)
OS	Included (Clavister CorePlus); Virtual Security Gateway also requires VMware ESXi3+
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Clavister (Sweden)
Information	*http://www.clavister.com/en/products-and-services/enterprise-security-gateways*

D-Link NetDefend Firewall/VPN UTM Appliances

Abstract

D-Link NetDefend Firewall/VPN UTM Appliances are ICSA certified. They range from small office/home office capability to large enterprise capacity. D-Link NetDefend provides several firewall features, including URL/keyword blacklists and whitelists, and access control policies. Layer 7 content inspection and protection is provided through an integrated IDS/IPS, gateway antivirus, and content filtering service; a realtime update service keeps the IPS information, antivirus signatures, and URL databases current. The integrated VPN client and server support IPsec, PPTP, and L2TP protocols in client/server mode and can handle pass-through traffic as well. Advanced VPN configuration options include DES/3DES/AES/Twofish/Blowfish/ Carlisle Adams/Stafford Tavares cipher (CAST)-128 encryption, manual or IKE/Internet Security Association and Key Management Protocol key management, quick/main/aggressive negotiation modes, and VPN authentication support using either an external RADIUS server or the internal user database.

D-Link NetDefend Firewall/VPN UTM Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	D-Link Corporation
Information	*http://www.dlink.com/category/productcategories/?cid=79* *http://www.dlink.com/category/productcategories/?cid=22*

EdenWall Security Appliances

Abstract

The EdenWall Security Appliance implements a stateful packet inspection/filtering firewall that also provides identity-based filtering (by which user identities are determined from X.509 certificates or other assured means rather than IP addresses, and access is granted or denied based on user's membership in a given directory group that reflects roles, functions, *etc*. Identity-based filtering also provides for strong accountability through traceability back to user *vs*. IP address), Deep Application Filtering (a form of deep packet inspection), network and user activity monitoring, high-availability features (load balancing, traffic shaping), site-to-site and mobile/remote access VPN, and transparent authentication (including support for authentication tokens). The EdenWall Multi-Firewall administration feature enables multiple firewall appliances to be administered from a single console. EdenWall hardware appliances range in size to support from 100 up to 8,000 simultaneous users.

EdenWall Security Appliances

Type of Firewall	VPN firewall (with SFI + AF)
OS	Included (EdenOS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	EdenWall Technologies (France)
Information	*http://www.edenwall.com/en/products/edenwall-security-appliances*

EGG Network Security Appliance

Abstract

EGG Network Security Appliance (NSA) is a high-end network perimeter protection appliance with a secure, proprietary embedded operating system, stateful inspection firewall, IDS, VPN concentrator, Web filter, and DMZ support. The EGG NSA firewall performs stateful inspection analysis of information from all communication layers, and performs complex traffic controls. EGG NSA stateful inspection defines a context based on state information generated by preexisting communications and applications. This state information is captured in state tables, which are dynamically updated by the firewall, and used as the basis upon which traffic control decisions are made. The EGG NSA examines the header fields of packets in transit and compares them with entries in the state table; only traffic associated with entries for an already-established IP session are admitted by the firewall. EGG NSA Intrusion Detection System performs realtime traffic analysis, relying on a vast knowledge base to detect suspicious activity. To date, the expanding and constantly updated IDS knowledge base contains more than 1400 signatures of attack patterns. EGG NSA integrates a complete VPN solution, acting both as server and client. EGG NSA VPN supports site-to-site and remote access VPN applications, it provides full support for mobile users. EGG NSA administration is performed with drag-and-drop operations *via* the Web Management Console, an advanced Web-based, object-oriented interface. EGG UPDATE is the system that keeps automatically updated firmware and software application features of all EGG NSA appliances, without requiring any operator intervention. QUADRO Srl also offers SENTRY outsourcing of centralized, advanced perimeter security management to purchasers of EGG NSA. SENTRY provides 24x7 network security monitoring, analysis, and alerting, performed on behalf of the customer.

EGG Network Security Appliance (NSA)

Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	QUADRO Srl (Italy)
Information	*http://www.eggnsa.it/products/appliances.php*

Endian UTM Software, Hardware, and Virtual Appliances

Abstract

Endian UTM Appliances all include the Endian Firewall, a stateful packet inspection/NAT firewall which protects the network from Internet threats while providing appropriate access to resources inside and outside the network and which also performs static and policy-based routing; IPS with Deep Packet Inspection, which protects the organization's virtual resources from malicious attacks, hackers, and most other internal or external threats; Web content and antivirus filtering that controls who can surf and where they can go on the network while protecting internal users from Web threats. The UTM also includes HTTP and FTP proxies and performs URL blacklisting, and local, RADIUS, LDAP, or Active Directory authentication and NTLM single sign-on with group-based access control; email spam (with optional upgrade to Commtouch RPD) and antivirus filtering (with optional upgrade to Sophos Antivirus) that protects against spam, phishing, and other malicious email from the network and provides protection against email-based viruses and other malware; email security also supports whitelisting/blacklisting of senders, and includes SMTP and POP3 proxies; and OpenVPN IPsec and SSL VPN with native VPN clients for Windows, Mac OS X, and Linux, DES, 3DES, AES encryption, authentication *via* preshared keys, X.509 certificates, and PPTP passthrough, and NAT traversal for IPsec traffic. The Endian UTM Virtual Appliance is optimized to run on virtualized platforms. Endian appliances also provide availability and performance features such as load balancing, hot standby (active-passive) node data/configuration synchronization, multi-WAN with automatic uplink monitoring and failover, VPN failover, automatic backup (including encrypted backups *via* email and instant recovery/backup using Universal Serial Bus [USB] sticks), and QoS.

Endian UTM Software, Hardware, and Virtual Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (hardened Linux); Virtual Appliances also need VMware, KVM, or Xen
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Endian Srl (Italy)
Information	*http://www.endian.com/en/products/software*

Entensys UserGate Proxy & Firewall

Abstract

Entensys UserGate controls Internet access, performs traffic calculations, and protects the local network against malicious activity and software, such as hacker attacks, viruses, and Trojans. UserGate is intended for use in small- and mid-sized companies. There are two antivirus engines integrated into UserGate to check incoming traffic, such as e-mail, HTTP and FTP, for malware. UserGate also incorporates a firewall, which guards the network against intrusions. UserGate incorporates NAT and application-layer proxy capabilities, and works as a point of entry to the Internet for a local network. UserGate can enforce strict Internet access policies. The integrated BrightCloud Service allows the administrator to apply Web filters, providing total control over what Web sites users can access. UserGate also includes an application filtering module that allows or denies Internet access to network applications installed on clients. User statistics are available in comprehensive reports directly accessible from within the program, or remotely *via* a Web browser. With DHCP server support, UserGate can dynamically assign IP-addresses in the local network. The resource publishing feature enables the administrator to provide access to the company's Internet-connected resources from outside the firewall. UserGate is capable of working with multiple ISPs, switching users to the secondary connection when the primary connection is broken, as well as routing different users to different ISPs. UserGate can also help manage traffic to avoid traffic congestion and make effective use of an Internet connection.

Entensys UserGate Proxy & Firewall

Type of Firewall	Multifunction (with WAF)
OS	Windows
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Entensys (Russia)
Information	*http://www.entensys.com/products/usergate*

Fortinet® FortiGate® Appliances

Abstract

FortiGate appliances provide comprehensive protection against network, content, and application-level threats. Ranging from the FortiGate-30 series for small offices to the FortiGate-5000 series for large enterprises, service providers and carriers, the FortiGate line combines the FortiOS™ security operating system with FortiASIC processors and other hardware to provide a comprehensive and high-performance array of security and networking functions including: firewall, VPN, and traffic shaping; IPS; antivirus/antispyware/antimalware; Web filtering; antispam; application control (*e.g.,* IM and P2P); VoIP support (H.323. and Skinny Client Control Protocol); layer 2/3 routing; multiple WAN interface options; virtual domain capabilities to separate various networks requiring different security policies. FortiGate appliances have attained ICSA Network Firewall, Network IPS, IPsec, and Antivirus certifications. FortiGate Appliances also include SSL Inspection technology, enabling them to filter SSL-encrypted traffic, to help prevent abuse of SSL tunneling to enable data leaks, bypass of URL blocking, or malicious content delivery.

Fortinet FortiGate Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (FortiOS firmware)
Format	Appliance
License	Commercial
NIAP Validated	No (Communications Security Establishment Canada [CSEC])
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/fortinet-v451-cert-eng.pdf)*
Developer	Fortinet
Information	*http://www.fortinet.com/solutions/firewall.html*

GajShield Unified Performance & Threat Management Appliances

Abstract

GajShield Unified Performance & Threat Management Appliances incorporates an ICSA-certified firewall, DLP, VPN, URL filtering, gateway antivirus, IPS, and performance management (traffic analysis, network behavior analysis, policy-based ISP failover and load balancing, bandwidth management).

GajShield Unified Performance & Threat Management Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	GajShield Infotech (I) Pvt. Ltd. (India)
Information	*http://www.gajshield.com/product_overview.htm*

GeNUGate Two-Tier Firewall

Abstract

GeNUGate combines a policy-based stateful packet inspection firewall with an application firewall, each hosted on a separate physical appliance that is directly connected to the other by a dedicated network connection (cross cable). The stateful inspection firewall includes circuit-level proxies for IP, TCP, and UDP, and performs NAT, QoS, queuing (traffic shaping), load balancing, packet normalization, port forwarding, distributed denial of service (DDoS), load balancing, spoofing protection, and TCP handshake offloading. The application firewall provides application-level proxies for FTP, HTTP/HTTPS, NNTP, ICMP (ping), POP3 (inbound email), SIP (VoIP), SMTP (server-server email), Telnet, and WWW [World Wide Web protocols] for Web content scanning/filtering. Content filtering is provided for Java, JavaScript, ActiveX, and user-selectable applications such as Flash (customers can also request other method filters). URL filtering is available *via* the GeNUBlock option that can block by site category (*e.g.,* gambling, porn, online auctions), and redirect blocked requests for analysis. The application firewall also supports ACLs that allow or deny access depending on the type of data object or Web object under consideration, *e.g.,* file extension, MIME type, URL, domain, or cookie. Avira AntiVir and Sophos Antivirus for GeNUGate can be purchased as an antivirus scanning option to run on the application firewall or on an external scan server. Antispam protection is also provided for email, including relay protection (sender checking/blacklisting), sender MX/IP validation, pattern blocking, greylisting, realtime blackhole listing, and Sender Policy Framework. Both the network and application firewall components support multiple authentication techniques, including Cryptocard, Kerberos, LDAP/LDAP group, local password database, RADIUS, S/Key, NTLM, and sidechannel (including timeframe). Access for protocols at all layers is provided according to source address, destination address, group authentication status, and time. High availability features include automatic configuration distribution, active-active load sharing, and automatic backups.

GeNUGate Two-Tier Firewall

Type of Firewall	Multifunction (with SIF + AF)
OS	Included (OpenBSD)
Format	Appliance
License	Commercial
NIAP Validated	No (Bundesamt für Sicherheit in der Informationstechnik [BSI])
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/0616a_pdf.pdf)*
Developer	GeNUA mbH (Germany)
Information	*http://www.netgear.com/business/products/security/UTM-series/default.aspx*

GeNUScreen Firewall & VPN Appliance

Abstract

The GeNUScreen Firewall & VPN Appliance provides the same packet inspection firewall found in the GeNUGate Two-Tier Firewall, and adds IPsec network-layer VPN that supports both tunneling and transport (packet payload only is encrypted) modes, as well as policy-based bridging and network mode (routing protocols, *e.g.,* OSPF, over VPN connections). VPN authentication is possible using RSA, preshared keys, or X.509 PKI. Encryption is provided *via* AES, 3DES, Blowfish, or CAST, with hashing *via* MD5, SHA-1, or SHA-2. As with the firewall, the VPN appliance provides high availability through active-active load balancing; the VPN appliance also implements switch trunking and hot standby for automatic failover. In addition to GeNUScreen's packet filtering firewall and VPN capabilities, optional modules are available to implement application-level capabilities such as virus scanning for HTTP and SMTP traffic, DNS and HTTP caching, and URL filtering.

GeNUScreen Firewall & VPN Appliance

Type of Firewall	VPN firewall (with SIF [+ WAF option])
OS	Included (OpenBSD)
Format	Appliance
License	Commercial
NIAP Validated	No (BSI)
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/0565a_pdf.pdf)*
Developer	GeNUA mbH (Germany)
Information	*http://www.netgear.com/business/products/security/UTM-series/default.aspx*

Gibraltar Security Gateways

Abstract

Gibraltar Security Gateways combine several important security applications into a single product that can be purchased preinstalled on one of five different hardware appliances, or as a software release. The Gateway's main features include: (1) SIF; (2) Web filter that checks Web traffic for dangerous content and viruses, and can block or restrict access to the Internet fully or partially, and log all Web traffic, based on content categories and user groups; (3) email filter that checks all email traffic for spam and viruses, identifies phishing emails, and filters out unwanted email attachments; (4) anonymization gateway that makes all internally-originated network traffic anonymous; (5) VPN gateway; (6) bandwidth management providing QoS traffic prioritization and defines bandwidth limits for different applications and users; (7) captive portal that requires users to authenticate *via* a login form before allowing them access to the network (can be used to secure wireless LANs).

Gibraltar Security Gateways

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	eSYS Informationssysteme GmbH (Austria)
Information	*http://www.gibraltar.at/content/view/2/2/lang,en*

Global Technology Associates Firewall/VPN Appliances

Abstract

The Global Technology Associates (GTA) firewall/VPN appliance product line includes a range of appliance sizes appropriate for enterprise (gigabit), corporate, and remote/branch office deployment. Standard features in all GTA firewall/VPN appliances include the following firewall capabilities: transparent NAT, stateful packet inspection, gateway failover, load balancing, DCHP server, DNS server. The appliances provide the following VPN service features: built-in IPsec VPN, LDAP, RADIUS and Active Directory Single Sign-on support. The devices also support secure remote management and provide redundancy features for high availability. In addition to the firewall and VPN features, the appliances provide the following security features: intrusion prevention system, email proxy filtering, and URL content filtering. Additional security features are available as options: content filtering, antivirus, antispam.

GTA Firewall/VPN Appliances

Type of Firewall	Multifunction (with SIF)
OS	Included (GB-OS)
Format	Appliances
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Global Technology Associates
Information	*http://www.gta.com/firewalls*

Global Technology Associates GB-Ware

Abstract

Global Technology Associates (GTA) GB-Ware software-based UTM system includes the same standard features as the GTA firewall/VPN appliance product line in a software-only implementation, *i.e.,* transparent NAT, stateful packet inspection, built-in IPsec VPN, gateway failover, load balancing, DCHP server, DNS server, LDAP, RADIUS and Active Directory single sign-on support, secure remote management, redundancy features (for high availability), and UTM features that include an intrusion prevention system, email proxy filtering, and URL content filtering. Additional optional threat management features include content filtering, antivirus, and antispam. The GB-Ware software firewall can be installed on servers running VMware or Citrix XenServer, enabling the firewall and server network services to be co-hosted on the same hardware platform.

GTA GB-Ware

Type of Firewall	Multifunction (with SIF)
OS	Included (GB-OS)
Format	Appliances and Software versions
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Global Technology Associates
Information	*http://www.gta.com/firewalls*

H3C SecPath and SecBlade

Abstract

H3C SecPath and SecBlade firewalls are ICSA-certified high-speed firewall appliances or appliance "blade" components that perform packet filtering and stateful packet inspection, and supports tens of thousands of ACL rules with high-speed ACL searching, malicious host filtering based on blacklists, Media Access Controller (MAC) address and IP address binding, Layer 4-7 application filtering capability based on Application Specific Packet Filtering technology, P2P stream detection, IPS prevention of DoS/DDoS, scanning, and snooping attacks and worm/virus propagation. The firewall also supports VoIP (H.323, SIP) detection and encryption, site-to-site and remote access VPN (IPsec, L2TP, with DES, 3DES, AES, and support for RSA SecureID; some models also support SSL/TLS tunneling), and QoS. In addition to its security functions, the SecPath firewall supports both static and dynamic routing (*e.g.,* Routing Information Protocol [versions 1 and 2], Open Shortest Path First, Border Gateway Protocol [BGP]), as well as routing policy and routing iteration. It is also a high-availability system, with support for Virtual Router Redundancy Protocol, active-active and active-backup, dual power and dual fan redundancy, and interface modules that are all hot swappable. The firewall also supports hot patching system upgrade operations that require no system downtime. Units range in size to support small businesses up to telecommunications central offices and very large enterprises.

H3C SecPath and SecBlade

Type of Firewall	VPN Firewall (with SIF)
OS	Included (Comware)
Format	Appliance or Appliance component
License	Commercial
NIAP Validated	
Common Criteria	
Developer	H3C Technologies Co., Ltd. (China)
Information	*http://www.h3c.com/portal/Products___Solutions/Products/Security_Products*

Halon SX Series Firewalls

Abstract

Halon's SX firewall appliances provide a broad range of network and application-level firewall features, including Web-based policy-based authentication, fine-grained policy-based Web (*i.e.,* HTTP) access control, anti-spoofing (inbound and outbound), hardware randomization of IP/TCP/UDP fields, protection against SYN flooding, support for multiple simultaneous per-interface policies, antispam/antivirus (Outbreak) for email (SMTP and POP3), VPN servers and clients (PPTP, IPsec) with encryption by AES, 3DES, CAST, or Blowfish, and hashing *via* Message Digest 5 (MD5), SHA-1, or Diffie-Hellman, plus RADIUS authentication, IPv6 routing, NAT traversal and protocol parsing (PPTP, FTP), dynamic BGP routing, Layer 2/3 hardware failover, Link Aggregation Control Protocol-based link aggregation or failover, and Internet failover with uplink redundancy, policy-based routing, QoS queuing, per service/per user rate limits for DoS protection, load balancing (Layer 3 TCP and ICMP and Layer 5 TCP).

Halon SX Series Firewalls

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (H/OS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Halon Security AB (Sweden)
Information	*http://www.halon.se/products/firewalls*

Hitec Fyrewall

Abstract

Hitec Fyrewall is free software based on a framework of pfSense and FreeBSD. Fyrewall offers extensive firewall capabilities with additional modules available for flow control, safe Internet navigation, and administration. Hitec Fyrewall includes: stateful packet inspection firewall, proxy server, content filter (with filtering by user or Active Directory group), Web access control email monitoring and filtering (compatible with Windows Live Messenger 2011), VPN (IPsec/PPTP/OpenVPN) with access governed by firewall rules, IDS (Squid/SquidGuard), antispam (for SMTP), DMZ capability, performance features such as traffic shaping, load balancing, redundancy (*via* Common Address Redundancy Protocol), and failover, reporting (*e.g.,* of Internet accesses, blocking events) and logging (including logging of Microsoft Network searches by keyword and contact), with integration of the Fyrewall's Squid/SquidGuard IDS with Active Directory 2003/2008.

Hitec Fyrewall

Type of Firewall	VPN firewall (with SIF)
OS	Runs on Linux or FreeBSD
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Hitec Informática (Brazil)
Information	*http://www.fyrewall.com.br*

HP ProCurve Threat Management Services (TMS) zl Module

Abstract

The HP ProCurve Threat Management Services (TMS) zl Module is a multifunction security system for the HP ProCurve Switch 5400zl and Switch 8200zl Series. It is comprised of a SIF, IDS/IPS, and an IPsec/L2TP VPN concentrator. The SIF enforces firewall policies to control traffic and filter access to network services, maintaining session information for every connection passing through it. It enforces zone-based access policies that logically group VLANs into zones that share common security policies, and supports both unicast and multicast policy settings by zone. It also performs deep packet inspection to discover IP address and service port data embedded in application data, and opening the appropriate connection for the application. The firewall also provides NAT/PAT, DoS prevention, and RADIUS- or local directory-based authentication.

HP ProCurve Threat Management Services (TMS) zl Module	
Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance subsystem
License	Commercial
NIAP Validated	
Common Criteria	
Developer	HP
Information	*http://h17007.www1.hp.com/us/en/products/network-security/index.aspx#TMSzlModule*

Huawei Quidway Eudemon Firewall Series

Abstract

Based on the Huawei carrier-class hardware platform and software platform Versatile Routing Platform, ICSA-certified Eudemon Firewalls implement anti-DoS/DDoS protection, VPN, NAT, and P2P inspection. Eudemon Firewalls can also filter and protect multimedia and VoIP traffic.

Huawei Quidway Eudemon Firewall Series

Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Huawei Technologies Co., Ltd. (China)
Information	*http://www.huawei.com/storage_networks_security/network/series.do*

IBM Security Server Protection and Virtual Server Protection for VMware

Abstract

IBM Security Server Protection combines the IBM Proventia® Server IPS and RealSecure® Server Sensor to implement deep packet inspection and blocking *via* the combination of an ICSA-certified IBM Proventia firewall that enforces allow/deny rules by address/port, named lists of objects, and complete connectivity, and an IPS augmented with the IBM protocol analysis module deep packet inspection engine that integrates multiple inspection technologies. Server Protection also implements Virtual Patch® technology, buffer overflow exploit protection, application blacklisting and whitelisting, security for Web transactions. IBM Virtual Server Protection for VMware implements the same transparent firewalling and IPS functions, along with rootkit detection and prevention, inter-VM traffic analysis, automated vulnerability assessment, network access control and policy enforcement, and virtual infrastructure auditing. In addition to providing virtual network-level protection, Virtual Server Protection for VMware can protect Mobile VMs (*e.g.,* VMotion).

IBM Security Server Protection and Virtual Server Protection for VMware

Type of Firewall	Multifunction (with SIF)
OS	Runs on Microsoft Windows, Linux, IBM AIX, UNIX, Solaris, HP-UX with VMware ESX, Windows Server 2008 Hyper-V, IBM Power Systems™ logical and workload partitions, Hewlett-Packard vPars and nPars, Solaris Container
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	IBM
Information	*http://www-01.ibm.com/software/tivoli/products/security-server-protection/index.html*

Ideco Gateway

Abstract

Ideco Gateway provides corporate networks with controlled, secure access to the Internet maintaining a database of users of the corporate network and their privileges, guarding the enterprise's servers and workstations against attacks from the Internet, filtering traffic, blocking unwanted advertising, securely connecting remote departments and users, and analyzing network traffic and setting restrictions for users. Ideco Gateway includes the following key components: (1) stateful packet inspection firewall with NAT, DNS, DHCP, *FTP,* QoS, and traffic shaper, (2) antivirus for Internet traffic and email, (3) portal/Web server, (4) mail server with Web interface, (5) proxy server, (6) VPN server.

Ideco Gateway

Type of Firewall	Multifunction (with SIF)
OS	Included (hardened Linux)
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Ideco Software (Russia)
Information	*http://www.idecogateway.com/gateway/index.php*

Igaware Network Protector

Abstract

Igaware Network Protector delivers a set of network defenses; automatic updates ensure that these defenses are always optimized against new threats as they emerge. Network Protector delivers email antispam, antivirus, and filtering of other malicious email content; VPN firewall; Web filtering that enforces Web access control policies and monitors Internet usage (integrates with Active Directory to provide single sign-on authentication); network monitoring tools.

Igaware Network Protector

Type of Firewall	Multifunction (with SIF + WAF)
OS	Runs on Linux
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Igaware, Ltd. (UK)
Information	*http://www.igaware.com/products/netprotect.php*

Ingate Firewall®

Abstract

The Ingate Firewall® 1190, 1500 series, 1660, and 2900 series are SIP-capable firewalls for enterprises that want access to SIP-based communications such as presence, instant messaging, audio and video conferencing, and VoIP. Ingate Firewalls include a SIP proxy and a SIP registrar, support NAT traversal and PAT, and have TLS support for encrypted SIP signaling—which means that instant messages are automatically encrypted. All Ingate Firewalls support stateful inspection and packet filtering with rules defined and maintained by the network security administrator. Ingate Firewalls include an encrypted VPN termination module. In addition to SIP support, Ingate Firewalls have a proxy for all standard protocols, including TCP, UDP, FTP and DHCP. The main differences between the Ingate Firewall series are the size of enterprise each is intended to support. The Firewall 1190 has three ports, and is intended for smaller office environments. The midrange Firewalls 1510, 1560 and 1660 can handle from150 up to 800 concurrent Realtime Transport Protocol (RTP) sessions (VoIP calls). An optional software upgrade module enables purchase of "capacity on demand" for the Ingate Firewall 1510 and Ingate Firewall 1560. The Firewall 2950 is a high capacity, high performance SIP security product made for large enterprises and service providers. The Firewall can handle up to 1,800 concurrent sessions, or simultaneous VoIP calls (RTP sessions), at any given time. The Firewall 2960 has an even greater capacity, handling up to 3,000 concurrent sessions/ calls at a time.

Ingate Firewalls

Type of Firewall	VPN firewall (with SIF + Voice AF)
OS	Included (hardened Linux)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Ingate (Sweden)
Information	*http://www.ingate.com/firewalls.php*

InJoy Firewall™ 4.0 Professional and Enterprise

Abstract

The InJoy Firewall performs stateful and deep packet inspection and packet filtering, intrusion detection, NAT, DNS forwarding, Web object and content filtering and HTTP URL logging, access control (with 10+ distinct security levels), port scan protection, and traffic accounting and shaping and bandwidth management (for QoS), and provides IPsec VPN server and clients with X.509 support, basic antivirus, and SafEmail email security. The Firewall also incorporates a DHCP server, and PPPoE and PPTP clients. It operates according to dynamic firewall rules, can be administered locally or remotely, and can be integrated with Windows XP Security Center. Professional edition is intended for small to medium-sized organizations; Enterprise edition is intended for enterprise users with demanding LAN topologies and VPN Gateway requirements.

InJoy Firewall 4.0 Professional and Enterprise

Type of Firewall	Multifunction (with SIF + WAF)
OS	Runs on Linux, OS/2 Warp, and Windows XP and Vista
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	F/X Communications (Denmark)
Information	*http://www.fx.dk/firewall*

iPolicy Intrusion Prevention Firewalls

Abstract

iPolicy Networks' ICSA-certified Intrusion Prevention Firewalls support multiple security services and defense mechanisms, including IPS/IDS, Layer 7 stateful firewall and URL filtering, anti-DoS/DDoS protection, URL filtering, realtime antivirus/antispyware/antiexploit protection, and VLAN and NAT support.

iPolicy Intrusion Prevention Firewalls

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	iPolicy Networks/Tech Mahindra Limited (India)
Information	*http://www.ipolicynetworks.com/products/ipf.html*

IPCop

Abstract

IPCop is a Linux-based SIF geared towards home and small office/home office users. The IPCop Web-interface is designed to be user-friendly, to accommodate non-expert users. In addition to its SIF functionality, IPCop implements a rudimentary IDS (Snort) on all interfaces, NAT (with "NAT Helper" for H.323, Internet Resource Chat, Multimedia Messaging System, PPTP, proto-gre, and !quake3 traffic), programmable port forwarding to an "orange" address, pin-hole on "green" or "blue" network, and configurable ping answering on all interfaces. IPCop also implements an IPsec VPN (Roadwarrior and Net-to-Net) that can use either X.509 certificates or pre-shared keys. IPCop also includes a Secure Shell (SSH) server (using RADIUS authentication with password or pre-shared key support) and an HTTP/FTP proxy (Squid), and a variety of networking features, including traffic shaping. It can be used on wired and wireless networks.

IPCop

Type of Firewall	VPN firewall (with SIF)
OS	Runs on Linux, BSD, UNIX, and other Portable Operating System Interface for uniX-compliant OSs
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	IPCop Team
Information	*http://www.ipcop.org*

Juniper Networks ISG Series Integrated Security Gateways

Abstract

Juniper Networks Integrated Security Gateways combine a stateful inspection firewall with IPsec VPN capabilities and DoS mitigation functions. The devices can be upgraded into full Unified Threat Management Gateways through addition of numerous optional capabilities, including: deep packet inspection for intrusion detection and prevention, includes stateful signature-based and protocol anomaly-based intrusion detection capabilities for blocking application-level attacks, and IDS/IPS packet inspection to protect against transport layer and above attacks, including zero-day, worm, Trojan, and spyware incursions; ICAP antivirus content redirection; Web filtering (provided by integrated SurfControl Web application firewall); antispam; application identification; General Packet Radio Service network support . The Gateways are manageable *via* NetScreen Security Manager, a policy-based central management system. Integrated Security Gateways range in size to support enterprises of all sizes. The appliances have also been FIPS 140-2-validated.

Juniper Networks ISG Series Integrated Security Gateways

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (ScreenOS®)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10301/*
Common Criteria	EAL4+
Developer	Juniper Networks
Information	*http://www.juniper.net/us/en/products-services/security/isg-series*

Juniper Networks NetScreen 5200 and 5400

Abstract

The Juniper Networks NetScreen 5200 and 5400 of purpose-built VPN firewall appliances are designed for large enterprise, carrier, and data center networks consists of two platforms. Both the two-slot NetScreen 5200 and the four-slot NetScreen 5400 combine firewall, VPN, traffic management, and DoS/DDoS protection into a modular chassis. Optional management module and Secure Port Modules are also available for the appliances; the latter can add integrated IPS (implementing deep packet inspection), Web filtering with redirection, and virtualization support.

Juniper Networks NetScreen Security Systems

Type of Firewall	VPN firewall (with SIF + WAF option)
OS	Included (ScreenOS)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10301*
Common Criteria	EAL4+
Developer	Juniper Networks
Information	*http://www.juniper.net/us/en/products-services/security/netscreen*

Juniper Networks SRX Services Gateways

Abstract

SRX Series Services Gateways provide perimeter security, content security, access control, and network-wide threat visibility and control. Firewall and VPN technologies secure the perimeter with minimal configuration of zones and policies. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling. For content security, SRX Series for the branch offers a UTM services consisting of Juniper's deep packet inspection technology, IPS (certain models only), antivirus and antispam (certain models only), Web filtering (integrated in some models, external in others), and data loss prevention (certain models only) *via* content filtering. The SRX Series Gateways firewall capabilities include: network attack detection; DoS and DDoS protection; TCP reassembly for fragmented packet protection; brute force attack mitigation; SYN cookie protection; zone-based IP spoofing; malformed packet protection. In addition, SRX1400 and above provide GPRS stateful inspection.

Juniper Networks SRX Services Gateways

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (Junos®)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Juniper Networks
Information	*http://www.juniper.net/us/en/products-services/security/srx-series*

Juniper Networks SSG Series Appliances

Abstract

Oracle Database Firewall creates a defensive perimeter around databases, monitoring and enforcing normal application behavior, helping to prevent SQL injection attacks and attempts to access sensitive application data using unauthorized SQL commands. Oracle Database Firewall (1) monitors and blocks SQL traffic on the network with white list, black list and exception list policies; (2) protects against application bypass, SQL injection and similar threats; (3) reports on database activity for Sarbanes-Oxley, PCI and other regulations, choosing from dozens of out-of-the-box reports; protects Oracle, Microsoft SQL Server, IBM DB2 for Linux, Unix, and Windows, and Sybase databases. Oracle Database Firewall requires no changes to existing applications or databases.

Juniper Networks SSG and NetScreen Firewall/VPN Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (ScreenOS)
Format	Appliance
License	Commercial
NIAP Validated	*http://www.niap-ccevs.org/st/vid10301*
Common Criteria	EAL4+
Developer	Juniper Networks
Information	*http://www.juniper.net/us/en/products-services/security/ssg-series*

Kerio® Control 7

Abstract

Kerio Control 7.1 is available either installed on the Kerio Control Box hardware appliance, or on a dedicated Windows server. The system incorporates a packet inspection and proxy filtering firewall/router, SNORT-based IDS/IPS, Web content filter that blocks importation of malicious or blacklisted content from the Web and blocks access to Web sites known to contain malicious content, integrated Sophos virus scanner, user activity logging, network analysis and reporting facilities, and VPN clients and services. Features include: deep inspection firewall; VPN, VPN Client, and SSL VPN; antivirus gateway protection; surf protection; content filtering; user specific access management; fast Internet sharing; VoIP and UPnP support; and Internet monitoring. Kerio Control 7 is ICSA Labs certified as a Corporate Firewall.

Kerio Control 7

Type of Firewall	Multifunction (with SIF + WAF)
OS	Windows (2000 Professional and Server, Server 2008, XP, Vista, 7) or VMWare
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Kerio
Information	*http://www.kerio.com/control*

McAfee Firewall Enterprise

Abstract

McAfee Firewall Enterprise is a direct descendant of the Secure Computing Sidewinder firewall. McAfee Firewall Enterprise provides network-level and application-level firewall capabilities and protections, including: application discovery, profiling, and visualization; fine-grained per-application/per-role access control that can also be configured based on IP reputation and geo-location; authentication services (RADIUS; LDAP; Microsoft Active Directory, Windows Domain, NTLM, and Passport; SecureID; Common Access Card support); high availability features (*e.g.,* stateful session failover, remote IP monitoring); global threat intelligence (from McAfee Labs); encrypted application filtering (filtering of encrypted content); IPS; antivirus/antispyware; Web content and object filtering; antispam; IPsec VPN. Firewall Enterprise is hosted on one of several appliance models, ranging from support for 300 users up to large enterprises. Several models incorporate redundancy features such as dual power supplies and RAID arrays. Firewall Enterprise also includes centralized firewall policy rule-creation capabilities through Firewall Profiler, which analyzes network traffic and firewall rules to provide insight into the effectiveness of the firewall's configuration in enforcing the organization's security policy, and firewall reporting *via* McAfee Firewall Reporter, which is a security event management (SEM) tool that performs central monitoring and correlated alerting and reporting consistent with regulatory requirements such as PCI DSS, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Sarbanes-Oxley, and Federal Information Security Management Act. As an option, McAfee Firewall Enterprise Control Center can be upgraded to provide centralized, enterprise-class firewall policy management for global-scale deployments.

McAfee Firewall Enterprise

Type of Firewall	Multifunction (with SIF)
OS	Included (SecureOS®)
Format	Appliance
License	Commercial
NIAP Validated	No (CESG) (Older version: *http://www.niap-ccevs.org/st/vid10089* *http://www.niap-ccevs.org/st/vid10089/maint177)*
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/crp261.pdf)*
Developer	McAfee Corporation
Information	*http://www.securecomputing.com/index.cfm?skey=232*

Microsoft Forefront Threat Management Gateway 2010

Abstract

Microsoft's Forefront Threat Management Gateway TMG 2010 is the "next generation" version of ISA Server. TMG builds upon the capabilities of ISA Server 2006, adding URL filtering (using Microsoft Reputation Services' extensive list of malicious and known-safe Web sites), HTTP/HTTPS inspection, antimalware, and intrusion-prevention technologies to protect against Web-based threats.

Microsoft Forefront Threat Management Gateway 2010

Type of Firewall	Multifunction (with WAF)
OS	Runs on Windows Server 2008
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Microsoft Corporation
Information	*http://www.microsoft.com/forefront/threat-management-gateway/en/us/default.aspx*

Microsoft® Internet Security and Acceleration Server 2006

Abstract

Microsoft Internet Security and Acceleration (ISA) Server 2006 is an integrated network boundary security gateway that helps protect IT environments from Internet-based threats while providing users secure remote access to applications and data. ISA Server contains a stateful inspection firewall that performs deep inspection of Internet protocols such as HTTP, which enables it to detect many threats that TCP/network-layer firewalls cannot. The integrated firewall and VPN architecture support stateful filtering and inspection of VPN traffic, and also supports VPN client inspection for quarantine solutions based on Microsoft Windows Server.

Internet Security and Acceleration (ISA) Server 2006

Type of Firewall	VPN firewall (with SIF)
OS	Runs on Windows Server 2003
Format	Software
License	Commercial
NIAP Validated	No (BSI)
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/0453a.pdf)*
Developer	Microsoft Corporation
Information	*http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx*

m0n0wall

Abstract

m0n0wall is developing into a complete, embedded firewall software package that, when hosted on an embedded personal computer (PC; Soekris Engineering net48xx/net55xx and PC Engines ALIX embedded operating systems are officially supported), provides features of commercial firewalls, including wireless support (including access point mode), captive portal, 802.1Q VLAN support, IPv6 support, stateful packet filtering, NAT/PAT, DHCP client, server, and relay, PPPoE, and PPTP support on the WAN interface, IPsec VPN tunnels (IKE, with support for hardware crypto cards, mobile clients and certificates), PPTP VPN (with RADIUS server support), static routing, caching DNS forwarder, Dynamic DNS client and RFC 2136-compliant DNS updater, Simple Network Management Protocol (SNMP) agent, traffic shaper and Scalable Vector Graphics-based traffic grapher, configuration backup/restore, and host/network aliases. m0n0wall is based on a stripped-down version of FreeBSD, along with a Web server, PHP, and other utilities. The m0n0wall system currently takes up less than 12MB on the Compact Flash card or Compact Disc-Read-Only Memory (CD-ROM). The recommended amount of Random Access Memory (RAM) for m0n0wall is 64MB. The entire system configuration is stored in a single XML text file.

m0n0wall

Type of Firewall	VPN firewall (with SIF)
OS	Included (hardened FreeBSD)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	m0n0wall Project (supported by BSD Perimeter LLC)
Information	*http://m0n0.ch/wall*

NETASQ U-Series and NG-Series Appliances

Abstract

NETASQ U-series appliances are designed to satisfy the network protection requirements of companies of all sizes. The Gateways provide: (1) Firewall + IPS: through contextual signature-based protocol detection and analysis, VoIP protection, DNS relay and caching, and policy-based routing; (2) IPsec VPN: uses AES encryption to provide support for 802.1Q VLANs, IPsec and SSL VPN tunnels; (3) Antivirus: embedded heuristic analysis for SMTP, POP3, *HTTP,* FTP traffic/content, plus reputation-based antispam (DNS Reverse Black List), and optional add-on Kaspersky antivirus module; (4) Content filtering: including URL filtering (15 categories), plus optional Optenet filtering (>50 categories) and NETASQ's SEISMO ("seismograph") realtime vulnerability analysis modules; (5) User authentication: *via* internal or external LDAP or Active directory, with support for transparent authentication PKI and embedded X.509 certification authority; (6) High availability: achieved through redundant system partitioning and redundant hardware. NETASQ NG-series appliances are designed to provide the same protections with a high level of assured availability and continuity of service in highly demanding environments such as high-traffic e-commerce servers and dynamic university networks. NG appliances provide the same network firewall + IPS, antivirus, and AES-based IPsec VPN capabilities as the U-Series, while adding QoS and secure routing, additional high availability and service continuity features, and an application firewall with transparent single sign-on authentication. This application firewall includes threat prevention, zero-day protection, and automatic attack quarantining capabilities, providing defenses against DoS, SQL injection, cross-site scripting, Trojan horses, session hijacking, flooding, and data evasion. The application firewall also performs realtime policy compliance checking and hourly policy scheduling.

NETASQ U-Series and NG-Series Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliances
License	Commercial
NIAP Validated	No (SSI)
Common Criteria	EAL4+ (IPS-Firewall Software Suite) *(http://www.commoncriteriaportal.org/files/epfiles/anssi_2009-30en.pdf)*
Developer	NETASQ (France)
Information	*http://www.netasq.com/en/solutions/utm.php* *http://www.netasq.com/en/firewall-services/network.php* *http://www.netasq.com/en/solutions/large-companies.php*

NetCop

Abstract

NetCop integrates open source UTM, firewall, ClamAV antivirus, Web cache, content filter, IPS/IDS, WAN link manager, bandwidth manager, anonymous proxy blocker, Wi-Fi hotspot controller, SSL VPN, and network virtualization programs into a single multifunction firewall.

NetCop	
Type of Firewall	Multifunction (with SIF + WAF)
OS	Runs on all POSIX-compliant UNIX/Linux OSs (native or in VMware)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	NetCop Project
Information	*http://sourceforge.net/projects/netcop*

NETGEAR® ProSafe Wired and Wireless VPN Firewalls

Abstract

NETGEAR's ProSafe business-class VPN Firewalls deliver protected network access between headquarter locations, remote/branch offices, and telecommuters. These appliances include a stateful packet inspection firewall, VPN, IDS/IPS, NAT, AES and 3DES Encryption, DoS protection, antispam policy enforcement (available on some models), content filtering, and more. The NETGEAR Wireless VPN Firewall adds a built-in 802.11g Access Point to the appliance's firewall and VPN capabilities.

Netgear ProSafe Wired and Wireless VPN Firewalls

Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Netgear
Information	*http://www.netgear.com/business/products/security/wired-VPN-firewalls/default.aspx* *http://www.netgear.com/business/products/security/wireless-VPN-firewalls/default.aspx*

NETGEAR® ProSecure® Unified Threat Management (UTM) Gateway Security Appliances

Abstract

NETGEAR® ProSecure® UTM appliances provide SSL & IPsec VPN Remote Access, content security, and firewall protection. The appliance's built-in SIF capabilities include a dual-WAN gigabit firewall with load balancing and failover capabilities, plus four gigabit LAN ports and one configurable hardware DMZ port. NETGEAR ProSecure UTM appliances are designed to replace existing firewalls and routers with a much broader range of content security and firewall features, including: (1) Content Security Features: scanning of Web and email protocols; stream scanning; inbound and outbound inspection; signature-less zero hour protection; malware signatures; automatic signature updates; Web content and object filters; email content filters; distributed spam analysis including supported protocols; antispam realtime blacklist; user-defined spam allow/block lists; distributed Web analysis (64 categories); IM and P2P control; and (2) Firewall Features: stateful packet inspection; IDS/IPS; WAN modes; ISP address assignment; NAT modes; routing; VoIP support.

NETGEAR UTM Gateway Security Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	NETGEAR, Inc.
Information	*http://www.netgear.com/business/products/security/UTM-series/default.aspx*

NetSentron® NS200 Lite and NS200 Pro

Abstract

NetSentron offers NS200 Lite and NS200 Pro in software-only versions, or installed on the NetSentron Server Appliance. NS200 Lite provides blacklist-based and advanced content filtering, packet filtering firewall with Web proxy and NAT, IDS, popup blocking, and malware and Trojan detection. NS200 Lite-based appliances range in size from 200 to 800 users in standard and rack-mount configurations. NS200 Pro provides all the same features as NS200 Lite (blacklist-based and advanced content filtering, packet filtering firewall with Web proxy and NAT, intrusion detection system, popup blocking, and malware and Trojan detection) plus IPsec VPN with X.509 and AES/3DES support for remote access (unlimited number of clients), wireless network support, bandwidth monitoring, restriction, and throttling, and a spam filter. As with NS200 Lite, NS200 Pro-based appliances range in size from 200 to 800 users in standard and rack-mount configurations.

NetSentron NS200 Lite and NS200 Pro

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	NetSentron (Canada)
Information	*http://www.netsentron.com/products.html*

Novell BorderManager®

Abstract

Novell BorderManager firewall and VPN technology enables secure identity management and control, acceleration, and monitoring of users' Internet activities. BorderManager leverages identity-based access control and forward proxies to protect the network against undesirable Internet content while maintaining high levels of performance. BorderManager integrates its IPsec-based VPN services and firewall capabilities to enable users to communicate securely *via* the Internet to another network protected by a Novell VPN server. Some key features of BorderManager 3.9 include: IP and IPX packet inspection; stateful inspection; NAT; VPN with NAT traversal and LDAP-based authentication; Web, *FTP,* email, DNS, Telnet, and RealAudio/RTSP application proxies (including Web and FTP reverse proxies); virus request blocking; integration with URL blocking tools (*e.g.,* SurfControl); FIPS-140-validated encryption engine.

Novell BorderManager 3.9

Type of Firewall	VPN firewall (with SIF)
OS	NetWare or Novell Open Enterprise Server
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Novell Corporation
Information	*http://www.novell.com/products/bordermanager*

O2Security SifoWorks™ Firewall/IPsec VPN Appliances

Abstract

The SifoWorks D/E/M-series are multifunction firewall systems that filter data packets at the 2nd through 7th network layers, and include the following functions: data transmission, categorization, route selection, network services categorization, security policies and access control, packet signature matching and bandwidth allocation (for QoS). Additionally, all these functions are designed to operate at full line speed. SifoWorks U-series gateway devices are equipped with a wide range of security mechanisms, integrating functions such as bandwidth management, intrusion detection, spam mail filter, content management, virus scan, *etc.* The SifoWorks U-series device also provides multiple load-balancing modes when it is connected to multiple ISPs, therefore ensuring efficient utilization of network bandwidth while providing link redundancy.

O2Security SifoWorks Firewall/IPsec VPN Appliances

Type of Firewall	Multifunction (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	O2Security Ltd./O2Micro International, Ltd. (Cayman Islands/China)
Information	*http://www.o2security.com/product/productOverview.php*

Paisley Systems Frontdoor Firewall Appliance

Abstract

The Frontdoor Firewall Appliance is a VPN firewall designed to prevent unauthorized access, secure WANs, accommodate remote workers and business partners, improve network performance and bandwidth utilization, audit and track network access, and minimize downtime. Frontdoor's firewall features allow granular control of all network traffic routed through the Frontdoor. These features include a stateful firewall that enforces access control based on blacklists or whitelists of source and destination IP addresses, source/destination ports, source/destination zones, source/destination MAC addresses, or other criteria. The firewall also performs rate limiting to defend against DoS attacks. Frontdoor also implements NAT, supports VPN tunneling, performs traffic shaping for QoS policies, and supports secure remote access. Paisley Systems Frontdoor is offered as part of a managed service package; the firewall appliance cannot be purchased separately from the managed support services.

Paisley Systems Frontdoor

Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance + managed services
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Paisley Systems
Information	*http://www.paisleysystems.com/frontdoor/frontdoor.php*

Palo Alto Networks Enterprise Firewalls

Abstract

Palo Alto Networks' next-generation firewalls provide network security by enabling enterprises to see and control applications, users, and content—not just ports, IP addresses, and packets. There are three technologies within the Palo Alto Networks' next-generation firewall that enable visibility and control over applications users and content: App-ID™, User-ID, and Content-ID. App-ID is a firewall traffic classification engine that uses as many as four different mechanisms to accurately identify exactly which applications are running on the network, irrespective of port, protocol, SSL encryption, or evasion technique employed. The determination of the application identity is the first task performed by the firewall and that information is then used as the basis for all firewall policy decisions. User-ID enables seamless integration with enterprise directory services such as Active Directory, eDirectory, LDAP, and Citrix, and enables administrators to view and control application usage based on individual users and groups of users, as opposed to just IP addresses. The firewall also implements an IPS. User information is pervasive across all features including application and threat visibility, policy creation, forensic investigation, and reporting. Content-ID is a stream-based scanning engine that uses a uniform signature format to block a wide range of threats and limit the transfer of unauthorized files and sensitive data, while a comprehensive set of URL filters and data filters controls Web surfing. Filtering also includes a network antivirus engine. The firewall also provides a complete set of traditional firewall, management, and networking features, including site-to-site IPsec VPN and SSL remote access VPN, while the identification technologies enable enterprises to create business-relevant security policies, and adopt new applications. QoS features such as traffic shaping and realtime bandwidth monitoring are also provided, as is full reporting, logging, and session tracing. Next-generation firewall model families include Palo Alto Networks' PA-4000 Series and the PA-2000 Series, along with the newly released PA-500 and range from 250Mbps to 10Gbps in throughput capacity. The appliances' Purpose-built Platform based on Palo Alto Networks' Single-Pass Parallel Processing Architecture ensures Multi-Gbps throughput through function-specific processing for networking, security, threat prevention and management, which are tightly integrated with a single pass software engine to maximize throughput. A 10Gbps data plane speeds traffic flow between processors while the physical separation of control and data plane ensures that management access is always available, irrespective of traffic load.

Palo Alto Networks Enterprise Firewalls

Type of Firewall	Multifunction
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Palo Alto Networks
Information	*http://www.paloaltonetworks.com/products*

Panda GateDefender Integra SB

Abstract

Panda GateDefender Integra harnesses the power of Panda's cloud-based Collective Intelligence database to deliver automatic realtime protection against all types of malware (viruses, worms, spyware, phishing, dialers, hacking tools, Trojans, jokes, other threats) carried in HTTP, FTP, SMTP, POP3, IMAP4, and NNTP traffic, while additional security technologies protect against targeted attacks and Internet threats. In addition to the proactive antimalware system, GateDefender Integra SB includes antispam (on SMTP, POP3, and IMAP4), content filtering of Web (*i.e.,* HTTP), file transfer (*i.e.,* FTP), and email (SMTP, POP3, IMAP4, Network News Transfer Protocol) traffic, and filtering of Web objects (URLs, using blacklisting and whitelisting, with ability to configure "Very Important Person list" exclusions), IPS, a two-way packet filtering/NAT firewall, realtime monitoring, and PPTP/L2TP/IPsec/SSL VPN tunneling with 3DES, AES, Blowfish, Twofish, and Serpent encryption.

Panda GateDefender Integra SB

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Panda Security (Spain)
Information	*http://www.pandasecurity.com/usa/enterprise/solutions/gatedefender-integra*

pfSense

Abstract

pfSense is a free, open source customized distribution of FreeBSD tailored for use as a firewall and router. pfSense implements a packet filtering and stateful inspection firewall with NAT. pfSense offers three options for VPN connectivity, IPsec, OpenVPN (SSL VPN), and PPTP Server. pfSense also offers a PPPoE server. A local user database can be used for authentication; RADIUS authentication with optional accounting is also supported. The Captive Portal feature enables pfSense to force authentication or redirection to a click-through page for network access, as is commonly done on wireless hotspot networks as well as in corporate networks needing an additional layer of security protection for wireless or Internet access. The firewall also includes DHCP Server and Relay functions.

pfSense

Type of Firewall	VPN firewall (with SIF)
OS	Included (hardened FreeBSD)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	pfSense Project (supported by BSD Perimeter LLC)
Information	*http://www.pfsense.org*

PLANET Security Gateways

Abstract

PLANET UTM Content Security Gateways use heuristic analysis to filter emails for spam and viruses. The Gateways' auto-training system can increase the identify rate of spam, while the 500GB hard drive of the appliances can support quarantining of spam mail. The antivirus application uses dual virus scan engines (ClamAV and Sophos) to detect viruses, worms and other threats in emails and Internet traffic. In addition to filtering spam and virus mail, the Gateways provide IDS/IPS and firewall functions to protect against hacking and blasting attacks from the Internet or intranet. The Gateway also performs content blocking of specific URLs, script types, IM/P2P programs; user authentication; IPsec, PPTP, and SSL VPN servers/clients (with AES and 3DES encryption), QoS and high availability features, including inbound load balancing, WAN fail-over, VPN fail-over and load balancing for VPN redundancy. The VPN Security Gateways and MH-2001 Multi-Homing Security Gateway provide all the same performance/availability features and VPN and Content Blocking functions, minus the extensive content/email filtering and IDS/IPS capabilities found in the UTM Content Security Gateways.

PLANET Security Gateways

Type of Firewall	Multifunction (with WAF + email firewall)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	PLANET Technology Corporation (Taiwan)
Information	*http://www.planet.com.tw/en/product/product_list.php?mt=menu_product_66&id2=7569 http://www.planet.com.tw/en/product/product_list.php?mt=menu_product_66&id2=7566 http://www.planet.com.tw/en/product/product_ov.php?id=7708*

Schweitzer Engineering Laboratories SEL-3620 Ethernet Security Gateway

Abstract

The substation-hardened SEL-3620 secures all Ethernet communication between your private networks and interoperates with existing business IT and control systems over an IPsec VPN (supporting up to 16 VPN network connections on three Ethernet ports). The SEL-3620 protects private networks from malicious traffic *via* an integrated firewall with strong authentication access control. The SEL-3620 secures routable protocols and data crossing the electronic security perimeter. The SEL-3620 was conceived for use with Supervisory Control and Data Acquisition (SCADA) systems, and was designed and built through a collaboration between Schweitzer Engineering Laboratories and the U.S. Department of Energy National SCADA Test Bed, EnerNex Corporation, the Tennessee Valley Authority, and Sandia National Laboratories.

Schweitzer Engineering Laboratories SEL-3620 Ethernet Security Gateway

Type of Firewall	VPN firewall (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Schweitzer Engineering Laboratories, Inc.
Information	*http://www.selinc.com/SEL-3620*

SECUI.com eXshield and NXG Firewalls

Abstract

SECUI.com firewalls range in size to support small, medium-sized, and large-scale enterprises. The SECUI.com Firewall is a deep packet inspection firewall that can detect and block hacking, worm and virus, DoS (SYN/UDP/Ping flooding), scanning attempts, session shaping, land attacks, "ping of death" attacks, IP forgery attacks, *etc.* at TCP/IP layers 2 and 3. The deep packet inspection capability also detects protocol anomalies, checks for stateful protocol signatures, and provides intrusion protection. The firewall's IPS features include traffic analysis, scanning pattern detection and blocking, session monitoring & shaping, Web application defenses (for HTTP) with command attack detection (SQL injection, LDAP injection, OS command injection, cross-site scripting, directory traversal, *etc.*), Web site cloaking, and dynamic profiling. The IPS also provides antispam with detection based on session connection (spam relay, blacklist, bulk marketing email) and content (signatures, keywords). Denial of Service attacks are blocked through protocol and pattern detection indicative of SYN/Ping/UDP flooding, "ping of death", fragmented packets, Smurf, *etc.* Clients are quarantined, and worms and viruses are isolated. Content filtering capabilities are implemented *via* external and embedded antivirus, embedded antispam, malicious URL filtering, keyword filtering, and policy-based signature pattern filtering. The firewall supports multiple operating modes (Transparent Layer 2 mode, Routing and NAT Modes and Layer 3, and Port Address Translation mode). The firewall implements a patented traffic classification algorithm, session synchronization at the kernel level, and dynamic rule-setting. The firewall also includes secure HTTP, SMTP, and POP3 proxies, split DNS (external *vs.* internal), and secure channels to applications that use dynamic ports (*e.g.,* Sun RPC, SQL*net, TFTP, FTP H.323, Dialpad, PPTP, L2TP, IPsec, ICMP/ping, RealPlayer, Windows Media Player, MSN). The firewall's high availability features include active/standby and active-active with Level 2 and Level 3 switches, redundant interfaces, session failover for routing changes, device and link failure detection. Load balancing and QoS features include traffic shaping and server load balancing. Users are authenticated *via* third-party techniques, including RADIUS, LDAP, SecureID, and S/Key, as well as SSL Web-based authentication.

SECUI.com eXshield and NXG Firewalls

Type of Firewall	Multifunction (with WAF)
OS	Included (SecuiOS)
Format	Appliance
License	Commercial
NIAP Validated	No (Republic of Korea IT Security Certification Center)
Common Criteria	EAL4 (NXG only, as WAF) *(http://service2.nis.go.kr/certify/detail.jsp?ci=GOOD.ENG&di=1615)*
Developer	SECUI.com (South Korea)
Information	*http://www.secui.com/eng/product/product_01.asp?MovieNum=FW*

SECUI.com eXshield and NXG UTM Appliances

Abstract

SECUI.com UTM appliances include SECUI.com's firewall and IPS and add an IPsec VPN that supports DES, 3DES, AES, SEED and other encryption algorithms, and SHA-1 and HAS-160 authentication hash algorithms. The VPN server implements remote-access VPNs and supports deployment of redundant VPN gateways. The VPN server prevents replay attacks, performs dead peer and dead link detection, split tunneling, and zero packet loss on SA rekeying. The UTM appliances also add session synchronization for both firewall and VPN, and multiline IPsec load balancing by VPN packet.

SECUI.com eXshield and NXG UTM Appliances

Type of Firewall	VPN firewall (with SIF)
OS	Included (SecuiOS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SECUI.com (South Korea)
Information	*http://www.secui.com/eng/product/product_01.asp?MovieNum=UTM*

Secure Crossing Zenwall-10

Abstract

The Secure Crossing Zenwall-10 Access Control Module was developed to protect SCADA and other critical infrastructure industrial control networks from standard networking threats, but also from industrial protocol-based threats from both inside and outside the protected environment. Zenwall-10 features include: Wi-Fi A/B/G wireless, Ethernet, and serial connectivity, antivirus, IDS/IPS, attack blocking, deep packet inspection field firewall, NAT, router/bridge (with advanced routing capabilities). Protocol filtering is included for the following industrial protocols: Common Industrial Protocol, Ethernet/IP, Object Linking and Embedding for Process Control, Inter-control Center Communications Protocol, Modbus, and Distributed Network Protocol-3. The Zenwall-10 includes SSL/VPN and IPsec solutions for secure remote connectivity, Active Directory integration for authentication, auto updates, automatic configuration backup, and realtime reporting with instant alerting (syslog) as well as advanced reporting for industrial historians. Secure Crossing supplies 8/5 rapid turnaround replacement for service contracts in critical situations. Remote management can be performed on a per unit basis, or multiple Zenwall-10 units across multiple locations can be managed using Secure Crossing's ZenViewer software.

Secure Crossing Zenwall-10

Type of Firewall	Multifunction (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Secure Crossing/Rockwell Automation
Information	*http://www.securecrossing.com/zenwall-10.html*

SecureLogix® ETM® System with TeleWall and Voice Firewall

Abstract

The SecureLogix ETM System includes the TeleWall telecommunications firewall and SecureLogix Voice Firewall together with other security, performance and call accounting solutions for public switched telephone network (PSTN), VoIP, and time division multiplexed (TDM) voice traffic. The TeleWall telecommunications firewall detects, logs, and controls all inbound and outbound PSTN activity based on user-defined, automated security policies. It protects enterprise data networks, phone systems, and other critical infrastructure from back-door modem access and other external attacks through the PSTN. Its granular usage policies can prevent abusive or malicious use of enterprise telecom resources by internal and external callers. The SecureLogix ETM Voice Firewall similarly secures corporate resources from telephony-borne attacks and security threats, and defends VoIP and TDM voice systems from service disruption and abuse, unauthorized access, toll fraud, and other restricted call traffic. The Voice Firewall with integrated Voice IPS capabilities can detect and block VoIP DoS attacks (signaling and media-based), malformed SIP signaling attacks against VoIP systems, toll fraud, telecommunications system tampering and voicemail/private branch exchange attacks, war dialing and other external modem attacks against data networks and other critical infrastructure, unauthorized employee dial-up connections and Internet usage over phone lines, virus infections and restricted file transfers over dial-up connections, harassing, threatening, or restricted inbound and outbound calls, fax and VoIP spam, VoIP bandwidth abuse/issues, internal voice service misuse/abuse, and fraudulent/wasteful employee calling activity.

SecureLogix ETM System with TeleWall and Voice Firewall

Type of Firewall	Multifunction (with Voice AF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	No (CSEC)
Common Criteria	EAL2+ *(http://www.commoncriteriaportal.org/files/epfiles/CR%20ETM%20v4.1.pdf)*
Developer	SecureLogix
Information	*http://www.securelogix.com/products/voice_firewall.htm* *http://www.securelogix.com/products/etm_overview.htm*

Securepoint Firewall UTM Gateways

Abstract

Securepoint Firewall UTM Gateways all include: network firewall with application proxies for HTTP, FTP (over HTTP), SMTP, POP3, VNC, and SIP/RDP, VPN gateway, virus scanner, spam filter, antiphishing filter, antispyware filter, Web filter, IDS, and other security applications. Securepoint provides an IPsec (IKEv1 and IKEv2) VPN gateway, with OpenVPN (SSL), L2TP, and PPTP support, VoIP and VLAN support, QoS, load balancing, clustering, and other high-availability features, and X.509 certificate server (for authentication). Securepoint is available in a number of appliance configurations ranging in size to support small office and branches (1-10 users) up to enterprises (200-infinite users, and as a virtual firewall software solution that runs under VMWare (for cloud environments).

Securepoint Firewall UTM Gateways

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (VMWare required for Virtual Firewall)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Securepoint GmbH (Germany)
Information	*http://www.securepoint.cc/products-utm-firewalls.html*

SmoothWall® Advanced Firewall and SmoothWall UTM

Abstract

SmoothWall Advanced Firewall is a software appliance that operates on a wide range of hardware platforms running on its own hardened GNU Linux operating system. SmoothWall UTM provides exactly the same functionality on a pre-configured hardware appliance. SmoothWall commercial firewalls are based on the open source SmoothWall Express firewall, plus numerous additional features and capabilities. The SmoothWall Advanced Firewall and UTM gateway functionality includes: IDS and IPS; stateful and deep packet inspection perimeter firewall with dynamic and static NAT; port-agile traffic blocking; internal firewall for network zoning and segregation; VPN gateway with support for SSL, IPsec, and L2TP tunnels; load balancing for inbound and outbound traffic across multiple Internet connections (includes implementation of failover protocols); authenticated Internet service access control; VB100 and Checkmark certified antimalware (SmoothWall Guardian Web Security, including a Sunbelt VIPRE antimalware engine) with high-speed scanning, realtime behavioral analysis using MX-Virtualisation™, and Genscan™ and Cobra™ heuristics, ThreatTrack™ URL, datafeed, and site blacklisting, and SteadyStream™ automatic hourly updating. The Advanced Firewall/UTM gateway's Web filtering features (provided by SmoothWall Guardian Web Filtering) include dynamic content analysis, "who, what, when, where" filtering with user/group/time/location-based controls, filetype filtering (MIME, file extension, download size), ad and cookie blocking, SSL interception, Flash filtering, URL block/blacklisting with daily updates *via* Internet Watch Foundation data feeds, Web site whitelisting, Web proxy caching, stealth mode operation, and other features. An optional module (Mailshell) can be purchased to add email antivirus and antispam capabilities, including SMTP validity checking, greylisting of unknown senders, Remote Blackhole Listing, sender domain spoofing prevention, attachment removal and content analysis, including antispam, reputation checking, bulkmail detection, and phishing detection. The Advanced Firewall and UTM gateway authentication features include support for Microsoft Active Directory, Novell eDirectory, and other LDAP-based authentication directories, as well as support for Microsoft NLTM and Windows Ident.

SmoothWall Advanced Firewall and SmoothWall UTM

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (hardened GNU Linux) (able to run under VMWare)
Format	Software and appliance versions
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Smoothwall, Ltd. (UK)
Information	*http://www.smoothwall.net/c/62/utm-advanced-firewall*

SmoothWall® Express

Abstract

SmoothWall Express is an open-source stateful inspection firewall distribution that runs on a hardened subset of the GNU/Linux operating system. SmootWall's firewall features include: support for LAN, DMZ, and wireless networks, as well as external connectivity (static Ethernet, DHCP Ethernet, PPPoE ADSL, PPPoA ADSL *via* USB or PCI DSL modem), dynamic NAT, port forwarding from external to DMZ/local IP addresses, DMZ pin-holes, outbound filtering and limited outbound traffic control, timed access, Quality-of-Service (QoS) with plus Serial Advanced Technology Attachment Serial-Attached Small Computer System Interface (SCSI), and IDE disk and hardware and SCSI RAID support, traffic statistics (per interface and per IP totals per week/per month), IDS using automatically updated Snort rules, UPnP support, IP address blacklist-based blocking. The firewall also provides several proxies: Squid caching Web proxy server, SMTP proxy (*via* SmoothZap add-on module), POP3 email proxy (*via* optional SmoothZap module) with antivirus (implemented by ClamAV open source antivirus), VoIP (SIP) proxy, DNS proxy server, IM proxy with realtime filtering and logging (with log viewing). The firewall also provides SSL VPN support for mobile ("Road Warrior") and home users and IPsec VPN support for site-to-site network connections, with 3DES (but not AES) encryption. There are also add-on modules for additional functionality: SmoothGuardian for Web content filtering, SmoothTraffic for bandwidth management/QoS, SmoothTunnel for VPN gateway functionality, SmoothRule for Internet access control and outbound rule enforcement, Smooth Monitor for incident alerting and reporting, SmoothHost for supporting multiple DMZ servers, and SmoothZap for email antispam, antivirus (*via* ClamAV), and relaying. The user interface is browser-based, and enables the administrator to use Asynchronous JavaScript and XML (Ajax) techniques to access realtime firewall and subsystem activity information and traffic graphs.

SmoothWall Express

Type of Firewall	VPN firewall (with SIF + WAF option)
OS	Included (hardened GNU/Linux) (able to run under VMWare)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Open source (funded by Smoothwall, Ltd. [UK])
Information	*http://www.smoothwall.org*

SOHOware BroadScan™ UTM Internet Security Appliance

Abstract

The SOHOware BroadScan appliance integrates multiple open source security applications (with subscription-free update service) to create an appliance-based UTM gateway solution. These applications include: stateful packet inspection firewall, email spam filter (SpamAssassin, which performs fingerprint, Bayesian self-training, greylist, and signature based filtering), email (SMTP, POP3) and Web (HTTP, FTP) antivirus (ClamAV; Sophos added on larger appliances), IDS/IPS (Snort), content blocking (URLs, scripts, HTTP and FTP uploads and downloads), DoS/DDoS prevention (based on anomalous traffic detection), DMZ port, application blocking (IM, file transfer over IM, P2P, streaming multimedia, Web mail, online gaming, VPN tunneling, remote controlling) VPN and WebVPN (IPsec, PPTP, SSL), RADIUS authentication, AAA-based user access control (database users and external users), per-user QoS and bandwidth management, multi-WAN link support with load balancing and failover, and high-availability hardware. Appliances range in size to support small business up to large enterprise networks.

SOHOware Broadscan UTM Internet Security Appliance

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	SOHOware, Inc.
Information	*http://www.sohoware.com/pro_sub_broadscan.htm*

SonicWALL® NSA and TZ Series Network Security Appliances

Abstract

All NSA and TZ Series appliances include an ICSA Firewall 4.1-certified stateful packet inspection firewall that scans more than 50 different protocols (with add-on option of SonicWALL Reassembly-Free Deep Packet Inspection™, including deep packet inspection for SSL encrypted traffic). The firewall also performs port shield (except on NSA 2400, 3500, 4500), and VoIP security, antimalware threat blocking, policy-based routing, policy-based NAT. The NSA Appliance VPN capabilities include SSL VPN clients (not available for TZ 100) and site-to-site VPN tunnels, IKEv2 VPN, route-based VPN, IPv6 support, and SSL control. The NSA Appliance supports authentication *via* X Windows Authentication /RADIUS, Active Directory, SSO, LDAP, terminal services, Citrix, and internal user database. High availability features include inbound and outbound load balancing, hardware, network, and modem failover with automated failback (no modem or hardware failover on TZ 100; no cellular modem failover on NSA 2400), and on-board QoS. Other add-on options for the NSA Series include: application intelligence and control (included in NSA E8500; not available for TZ 100/TZ 200), IPS (included in NSA E8500), gateway and enforced client antivirus/antispyware, Web content and URL filtering, comprehensive antispam, and SSL inspection (not available on 2400MX; optional in all E-series NSA appliances except NSA E8500). All NSA Appliances, with the exception of the 2400MX: EAL4+. In addition, the NSA 3500 and 4500 are FIPS 140-2-validated.

SonicWALL NSA and TZ Series Network Security Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (SonicOS)
Format	Appliance
License	Commercial
NIAP Validated	No (CSEC)
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/sonicwall-cert-e.pdf)*
Developer	SonicWALL, Inc.
Information	*http://www.sonicwall.com/us/products/Network_Security.html*

StoneSoft StoneGate™ Firewall/VPN Appliances and Virtual Firewall/VPN Appliances

Abstract

StoneGate Firewall/VPN Appliances range in size from small to medium-sized sites to remote sites, to data centers and large central network sites. The firewall functions provided by the appliances include: stateful and deep packet inspection; proxy agents for FTP, H.323, HTTP, HTTPS, IMAP4, MS RPC, NetBIOS Datagram, Oracle SQL Net, POP3, Restricted Shell, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP, ICMP; granular access control based on user, group, traffic type, target or source IP address, time of day, or day of week; seamless integration with StoneGate IPS for Web and VoIP traffic; application awareness and application-level content inspection *via* co-located or integrated antivirus, Web filter, or antispam filter. Availability features include connection/session redundancy, load balancing of ISP circuits, seamless VPN failover across multiple circuits, active-active clustering of up to 16 appliances, dynamic server load balancing, automatic backup, bandwidth management, and standards-based QoS. The Firewall also supports realtime monitoring and alerting, reporting and compliance, incident management, support for third-party event management, and rule-base optimization. VPN technologies supported include: IPsec, AES 128, AES 256, DES, 3DES, Blowfish, CAST-128, Twofish, IKE, MD5, SHA-1, and PKI (x.509). Authentication is provided *via* RADIUS, TACACS+, LDAP(S) (Microsoft Active Directory), or internal LDAP user database. ICSA certified as Firewall and Network IPS. FIPS 140-2-validated.

StoneSoft StoneGate Firewall/VPN Appliances and Virtual Firewall/VPN Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Appliance: included (Linux CentOS 5); Software: VMware ESX Server 3.5
Format	Appliance or Software
License	Commercial
NIAP Validated	No (CESG)
Common Criteria	EAL4+ *(http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/certreps/crp249.pdf)*
Developer	Stonesoft Corporation (Finland)
Information	*http://www.stonesoft.com/en/products/fw*

TeamF1 SecureF1rst Security Gateway Solution

Abstract

The SecureF1rst Security Gateway Solution (SGS) is one of TeamF1's line of prepackaged solutions marketed to Original Equipment Manufacturers and Original Design Manufacturers. To create specific instances of the SecureF1rst SGS, TeamF1 uses pre-existing software blocks that have been proven effective in numerous deployments, thus minimizing risk for original equipment manufacturers and original design manufacturers. TeamF1 offers its comprehensive set of SGS features as completely modular packages to enable full customization of the SGS to satisfy an OEM's specific requirements. The available security features for the SecureF1rst SGS include: (1) stateful packet inspection firewall with port/service blocking, support for multiple firewall zones, one-to-one and many-to-one NAT, and IPv6 support; (2) DoS attack resistance; (3) replay attack prevention; IDS/IPS (including wireless IPS); (4) gateway antivirus; (5) Web content filtering with URL/Java/ActiveX blocking; (6) DNSsec server and proxy; (7) IPsec and SSL VPN (10,000+ tunnels) with fully-qualified/absolute domain name-based connections, IPsec NAT traversal (RFCs 3947/3948), site-to-site (hub, spoke, mesh) and remote access (client-to-site), VPN ModeConfig Support authentication, and VPN redundancy and backup; support for multiple authentication and access control technologies, including IKE authentication supported by manual key and IKE Security Associations (with key and IKE lifetime settings, IKE keep-alive, and main/aggressive/quick IKE modes), preshared keys, and RSA signatures, choice of advanced encryption and integrity algorithms (DES, 3DES, AES, Blowfish, RSA/DSA, MD5, SHA-1, SHA-256/384/512, Rivest Cipher-4, X.509 v.3, Diffie-Hellman Groups 1,2,5,14, Diffie-Hellman, Perfect Forward Secrecy), Authentication Header/ Authentication Header-Encapsulating Security Payload (ESP) support, Microsoft Challenge-Handshake Authentication Protocol, Port-based NAC), Kerberos Authentication Agent, X-Windows Authentication, External RADIUS server, and internal local user database, SMTP authentication for Email; among others.

TeamF1 SecureF1rst Security Gateway Solution

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	TeamF1, Inc.
Information	*http://www.teamf1.com/products/sgs/sgs_highlights.htm*

Trlokom OmniVPN and Katana Gateway

Abstract

Trlokom OmniVPN is an integrated VPN/firewall/IDS/IPS gateway that controls inbound and outbound network access at the network perimeter. The Katana firewall controls the nature of network traffic entering and leaving the network, and ensures that all unauthorized traffic is blocked. Support for NAT-traversal in Katana gateways ensures that remote nodes and gateways behind NATs will be able to establish VPN connections with other VPN gateways. The Gateway also implements and IDS/IPS system that controls which applications can access the network and the types of traffic they can generate. VPN features include remote-access and site-to-site VPN with support for 300,000+ simultaneous network connections, with no limits placed on the number of VPN tunnels; it has been shown to sustain 50Mbps for 256 bit AES or 3DES-encrypted traffic when operating at full capacity. Katana Gateway has been tested and proven interoperable with VPN gateways from Checkpoint, Cisco, D-Link, Fortinet, Linksys, NetGear, Juniper NetScreen, SonicWALL, and WatchGuard. The VPN gateway's support for dynamic IP addressing means it does not require static IP addresses for VPN gateways with which it interoperates. The gateway also supports X.509 certificate-based authentication, and requires domain login for teleworkers, with enforcement of policies to limit their access. OmniVPN Gateway also provides central management of subnet-based VPN/firewall and group-based IDS/IPS policies, with support for policy server clustering for high availability, and monitoring and shaping of traffic at any point in the network, as well as support for dynamic remote installation/upgrade of software on all network nodes, and ability to pull IDS/IPS policies from any network node. Trlokom Katana Gateway is intended for small business or personal firewall use; it provides the same VPN gateway, firewalling, and IDS/IPS features as OmniVPN without the central management features. Katana Gateway can be installed on any PC with two NICs to use as an enterprise VPN firewall (*vs.* a personal firewall).

Trlokom OmniVPN and Katana Gateway

Type of Firewall	Multifunction (with SIF)
OS	Runs on Windows
Format	Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Trlokom, Inc.
Information	*http://www.trlokom.com/product/katana-gateway.php*

Tutus Färist Firewall

Abstract

The Färist Firewall is a high assurance application layer firewall. The Färist Firewall enforces high-level security policies and creates fine-grained audit trails. The firewall is an application-level proxy-based firewall with VPN capabilities. It supports proxies for most common network services and protocols including DNS, DHCP, FTP, HTTP, LDAP, Line Printer Daemon protocol, Network Time Protocol, ICMP/ping, Remote Frame Buffer, SIP (VoIP), SMTP, SNMP, syslog, TCP, UDP, Telnet, Internet Group Management Protocol, multicast NTP, multicast, Independent Computing Architecture (Citrix), Notes RPC (Lotus Notes), Convolutional Ambiguity Multiple Access, and certain North Atlantic Treaty Organization (NATO) information exchange protocols (*e.g.,* NATO Friendly Force Information protocol). The Färist Firewall also features VPN encryption using IPsec ESP tunneling at both the link and network layers; automatic key exchanges using X.509 certificates; encryption using AES-256 in Cipher-Block Chaining mode. The firewall has built-in failover functionality to enable high availability configurations.

Tutus Färist Firewall

Type of Firewall	Multifunction (with WAF)
OS	Included (FreeBSD version 6.2)
Format	Software
License	Commercial
NIAP Validated	No (Försvarets Materielverk)
Common Criteria	EAL4+ *(http://www.commoncriteriaportal.org/files/epfiles/20080527_CR2006001_Farist.pdf)*
Developer	Tutus Digital Gatekeepers (Sweden)
Information	*http://www.tutus.se/products/farist-firewall.html*

Ubiq-Freedom

Abstract

Ubiq-Freedom is an open source UTM gateway that includes a firewall, proxy server, VPN, IDS, email security, antispam, and antivirus.

Ubiq-Freedom	
Type of Firewall	Multifunction
OS	Included (Linux From Scratch)
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	wep Solutions India (India)
Information	*http://sourceforge.net/projects/ubiq-freedom/*

Untangle Server with Lite, Standard, or Premium Package

Abstract

Untangle Server provides a security appliance to run one of Untangle's Multifunction firewall packages—the entry-level Lite, Standard, or Premium Packages, all of which comprise a set of freeware, open-source, and commercial security applications. Untangle Lite Package provides entry-level multifunctional firewall functionality, including a packet inspection firewall (Untangle Firewall, which is also available separately as freeware), Web Filter, Virus Blocker, Spam Blocker, DoS Attack Blocker, Phish Blocker, Spyware Blocker, P2P and IM Protocol Control, Captive Portal (enforces access control based on defined terms of service), IPS, OpenVPN, and reporting function. Untangle Standard Package adds to the above a Directory Connector (integrates Standard Package reporting and policy tools with existing RADIUS or Microsoft Access Directory servers) and Automatic Configuration Backup capability, plus live phone technical support (*vs*. email/online only). Premium Package adds Policy Manager (for defining user and time-based Web and remote access policies), Kaspersky Virus Blocker (for enhanced antivirus protection), Commtouch Spam Booster (for further reduction in spam incidence), WAN load balancing and failover, bandwidth control, and Web cache. Untangle's Server appliances are Dell Computer-manufactured Pentium- and Xeon-based devices with RAID and hardware redundancy to increase availability.

Untangle Server with Lite, Standard, or Premium Package

Type of Firewall	Multifunction (with SIF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Untangle, Inc.
Information	*http://www.untangle.com/Products/untangle-libitem-lite-package* *http://www.untangle.com/Products/untangle-libitem-standard-package* *http://www.untangle.com/Products/untangle-libitem-premium-package*

Vordel® Gateway

Abstract

Vordel Gateway is a purpose-built Gateway, often referred to as an XML Gateway or SOA appliance, available in multiple form factors, designed to accelerate, secure and integrate all types of traffic on the SOA network. It offers policy-driven processing of SOAP, REST, XML and other data formats; protocol and content transformation; XML filtering and access control to services to support governance of the SOA infrastructure. The Gateway's XML firewall provides threat prevention *via* realtime XML validation and threat scanning that can detect and block following attacks: XML entity expansion and recursion attacks, XML document size/width/depth attacks, XML well formedness-based parser attacks, coercive parsing, jumbo payloads, recursive elements, MegaTags (also known as jumbo tag names), public key DoS attacks, XML flooding, XML encapsulation, XML virus, replay attacks, resource hijacking, dictionary attack, message, data, and parameter tampering, falsified message, message snooping, XPath, Xquery, and SQL injection, WSDL enumeration, routing detour, schema poisoning, malicious morphing and XML morphing, malicious Include (also known as an XML external entity attack), memory space breach, WSDL scanning, XML bomb attacks, rogue SOAP attachments, XML clogging, and traffic throttling. The firewall also performs field-level validation, IP address and SOAP operation filtering, HTTP header and query string analyses, outgoing message scanning for sensitive content based on metadata or regular expression patterns, schema validation, and detection of viruses and malicious code (based on a malicious content signature library) in messages, data, and SOAP attachments. The Gateway is available as a hardened network appliance, software, virtual appliance, or an Amazon AMI. It is deployable standalone or as an integral component of a strategic enterprise SOA infrastructure, and can interface with existing enterprise service buses, enterprise management systems, and identity management platforms.

Vordel Gateway

Type of Firewall	Multifunction (with XML AF)
OS	Appliance: Included (VX platform OS); Software: Runs on Windows 7/Vista/XP/ Server 2003/Server 2008, Linux (Red Hat, SuSE Enterprise Server, Ubuntu, Debian, Oracle), Solaris 10 SPARC [Scalable Processor ARChitecture]; Virtual appliance: Also requires VMware
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Vordel Ltd. (Ireland)
Information	*http://www.vordel.com/products/gateway*

Vyatta Core

Abstract

Vyatta Core software provides basic routing, stateful packet inspection firewall, IPsec and SSL-Based VPN (using OpenVPN software), and WAN load balancing. The Vyatta firewall features IPv4/IPv6 stateful packet inspection to intercept and inspect network activity and protect data. Vyatta's firewall capabilities include stateful failover, zone and time-based firewalling, P2P filtering, and more. Vyatta also offers a number of Vyatta PLUS Enhanced Security Services within its VyattaGuard Secure Web Filtering software subscription edition—which includes Web/Web 2.0 content inspection and Web transaction filtering capable of implementing parental controls and identifying and blocking pornography, hate speech, social media/online shopping misuse, excessive bandwidth consumption (*e.g.,* associated with P2P and streaming media), and Web-based threats such as malware and phishing. Vyatta also offers a software subscription edition package comprising Sourcefire Vulnerability Research Team IPS rules and IPS/IDS to provide non-signature-based protection against known and unknown vulnerability exploitations.

Vyatta Core

Type of Firewall	VPN firewall (with SIF + WAF option)
OS	Included (Vyatta NOS)
Format	Appliance or Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Vyatta
Information	*http://www.vyatta.com/products/software_subscriptions.php*

WatchGuard® Extensible Threat Management Series

Abstract

WatchGuard (formerly BorderWare) Extensible Threat Management (XTM) Series multifunction firewall appliances include WatchGuard's proprietary Fireware® XTM or XTM Pro (XTM 1050 only) operating system, which implements the firewall features. All WatchGuard XTM Appliances provide: ICSA-certified IPsec VPN (also supports SSL, PPTP), single sign-on (Radius, LDAP, Active Directory, VASCO, RSA SecureID), HTTPS inspection, VoIP security (H.323. SIP, call setup and session security), application usage control (including Web 2.0 applications), reputation-based defense (for blocking malicious Web sites), role-based access control, realtime and self-health monitoring, and management and reporting features. Wireless models feature dual-band 802.11n for Wi-Fi. Specific firewall capabilities include: NAT, QoS, policy-based routing, stateful packet inspection, deep packet inspection, proxy firewall; Application proxies for HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3; Blocks spyware, DoS attacks, fragmented packets, malformed packets, blended threats, and other attack patterns; optional Security Bundle provides the following additional threat protections: WebBlocker, spamBlocker, gateway antivirus, and IPS. WatchGuard appliances range in size to support small offices and wireless hotspots at the low end up to large businesses and data centers at the high end. All appliances are ICSA and FIPS 140-2 certified, with Common Criteria EAL4+ evaluations underway.

WatchGuard XTM Series

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (Fireware XTM or XTM Pro)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	WatchGuard
Information	*http://www.watchguard.com/products/xtm-main.asp*

XRoads Edge2WAN Cloud Firewall Appliances

Abstract

Edge2WAN Cloud Firewall Appliances are multifunction firewalls specifically engineered to run in a cloud computing environment. They provide stateful, policy-based packet inspection, content filtering (including Web content, spyware, and virus filtering), remote access VPN and site-to-site VPN (<15 tunnels on low-end appliance, up to 100 tunnels on high-end appliance; larger EdgeXOS UBM appliances are also available that can support up to 1,000 concurrent VPN tunnels and from 100-10,000 active DNS domains). Performance and availability features include WAN link bonding (for Internet traffic acceleration), site-to-site VPN failover, and multiple ISP failover.

XRoads Edge2WAN Cloud Firewall Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included (EdgeXOS)
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	XRoads Networks, Inc.
Information	*http://www.cloudfirewalls.com/cf/products/prod_comparison.xrn*

Zentyal Gateway

Abstract

Zentyal Gateway is an open source network gateway that provides an integrated collection of open source networking (Ethernet, Wi-Fi, PPPoE, and VLAN), firewall (NAT, redirection, DMZ, *etc.*), routing, QoS (layer 7 traffic shaping, load balancing), availability (redundancy with WAN fail-over), proxy server (HTTP proxy with cache, content filtering, and antivirus), access control (policies according to users, groups, and subnets), and RADIUS authentication tools, designed to implement a virtual network gateway appliance. Zentyal Gateway's networking and availability features are provided by multiple Linux networking subsystems. The firewall is Netfilter. Routing is provided by Iproute2. QoS is provided by L7filter and Iproute2. The proxy service is provider by Squid, with Dansguardian and ClamAV for content filtering. Access control is provided by Squid, and authentication by FreeRADIUS.

Zentyal Gateway

Type of Firewall	Multifunction (with SIF + WAF)
OS	runs under VMware, VirtualBox, or KVM [Kernel-based Virtual Machine]
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Zentyal/Ebox Technologies S.L. (Spain)
Information	*http://www.zentyal.com/en/products/server/gateway*

Zentyal UTM

Abstract

Zentyal UTM is an open source UTM gateway that provides an integrated collection of open source firewall, content filtering (email: antivirus, antispam, and greylisting; Web: antivirus, content analysis, whitelisting and blacklisting), VPN, and IDS tools, designed to implement a virtual UTM gateway appliance. The firewall included in Zentyal UTM is Netfilter. Email content filtering is provided by ClamAV, Spamassassin, Postgrey, Amavisd-new and P3scan. Web content filtering is provided by Squid, Dansguardian, and ClamAV. The VPN is provided by OpenVPN, and the IDS is Snort.

Zentyal UTM	
Type of Firewall	Multifunction (with SIF + WAF)
OS	Runs under VMware, VirtualBox, or KVM
Format	Software
License	Open source
NIAP Validated	
Common Criteria	
Developer	Zentyal/Ebox Technologies S.L. (Spain)
Information	*http://www.zentyal.com/en/products/server/utm*

ZyXEL ZyWALL Unified Security Gateways and Internet Security Appliances

Abstract

ZyXEL's ZyWALL Unified Security Gateways include IPsec VPN concentrators and SSL or L2TP remote access VPN support, ICSA-certified stateful inspection firewall, ICSA-certified ZyXEL Antivirus or Kaspersky Labs antivirus, Application Patrol upgrade option to add application level firewall controls such as IM/P2P blocking, application access control down to individual user/application feature level, IDS/IPS including malware detection and blocking, Web link protection including blocking of sites known/suspected to deliver malware, email antispam, user-aware access control to applications or resources, including security scans by user or user group, bandwidth management with QoS prioritization, and high availability features (device HA, redundant power module, multiple ISP links in a single WAN trunk). ZyWALL Internet Security Appliances provide the same features, and add VoIP security, more granular Web site/content blacklisting (according to Web site categories, *e.g.,* pornography, racial intolerance) and firewall zoning with layer 3 virtualization (for VLAN and virtual/alias interfaces).

ZyXEL ZyWALL Unified Security Gateways and Internet Security Appliances

Type of Firewall	Multifunction (with SIF + WAF)
OS	Included
Format	Appliance
License	Commercial
NIAP Validated	
Common Criteria	
Developer	ZyXEL Communications
Information	*http://us.zyxel.com/Business/Products-Business-User.aspx#Firewall,%20IPSEC,%20and%20SSL*

EdenWall Virtual Security Appliance

Abstract

EdenWall Virtual Security Appliance implements EdenWall's identity-based filtering method in virtual environments ranging from workstations to servers. Thanks to the agent embedded in each virtual session, EdenWall Virtual Security Appliance can grant specific rights to each user and provide full visibility over actions triggered by the user in the virtual environment to which he has access. By associating an EdenWall agent with each VM, EdenWall Virtual Security Appliance can distinguish between sessions according to the associated user identity and ensure that users access only the resources they are entitled to. Identity-based filtering enables the EdenWall Virtual Security Appliance to secure VM pools with dynamic IP addresses, instead of relying solely on application-level or network-level packet filtering.

EdenWall Virtual Security Appliance

Type of Firewall	Identity filtering firewall
OS	Appliance: Included (EdenOS); Software agents: Citrix, VMware, TSE
Format	Appliance + Software
License	Commercial
NIAP Validated	
Common Criteria	
Developer	EdenWall Technologies (France)
Information	*http://www.edenwall.com/en/products/edenwall-virtual-security-appliance*

SECTION 4 ▶ **Personal Firewalls**

As with the firewalls in Section 3, the personal firewalls listed in this section exclude firewalls that, even though available, appear not to have been updated in the past two years, or appear to be no longer supported, or to run only on no-longer-supported operating systems.

Personal firewall products change so rapidly that descriptive information about them provided by their vendors becomes obsolete almost as soon as it is published. For this reason, the authors of this Report believe that including such information, when it will become inaccurate so quickly, would be of questionable value to the reader. Therefore, we have not provided abstracts on these tools. However, we have provided Web links to such information, along with some basic data points on the national origins of the firewall developers, the operating systems on which they are hosted, and the licensing arrangements under which they are available.

Section 4.1 focuses on computer-based personal firewalls. Section 4.2 focuses on personal firewalls for mobile devices such as smartphones.

4.1 Personal Firewalls for Computers

Table 4-1 lists all known personal firewalls designed to run on computers (PCs, laptops, notebooks, netbooks). All are commercially-licensed unless otherwise noted as exceptions. All are developed in the U.S. unless otherwise noted as exceptions. All run on Windows unless otherwise noted as exceptions.

Note that firewalls built into operating systems (e.g., Windows Firewall, IPCop), and their ability to be used as personal firewalls when those operating systems are run in single-user mode, were discussed in Section 3.

Firewall	Exceptions	Information
AGAVA Firewall	Origin: Russia	*http://www.agfirewall.ru*
Agnitum Outpost Firewall Pro™ and Network Security	Origin: Russia	*http://www.agnitum.com/products/outpost/index.php* *http://www.agnitum.com/products/networksecurity/index.php*
Alcatel-Lucent IPSec Client (with built-in firewall)	Origin: France	*http://enterprise.alcatel-lucent.com/docs/?id=9825*
Ashampoo® FireWall FREE and PRO	Origin: Germany; License: Freeware (FireWall FREE only)	*http://www.ashampoo.com/en/usd/pin/0050/Security_Software/Ashampoo-FireWall-FREE* *http://www.ashampoo.com/en/usd/pin/0150/Security_Software/Ashampoo-FireWall-PRO*
AVS4YOU (Online Media Technologies) AVS Firewall	Origin: UK; License: Freeware	*http://www.avs4you.com/AVS-Firewall.aspx*
BitDefender® Internet Security and Total Security	Origin: Romania	*http://www.bitdefender.com/solutions/internet-security.html* *http://www.bitdefender.com/solutions/total-security.html*
Bullet Proof Soft PC Internet Firewall Security		*http://www.bulletproofsoft.com/firewall-securty.html*
BullGuard® Internet Security	Origin: UK	*http://www.bullguard.com*
C&C Software 8Signs Firewall	Origin: Canada	*http://www.ccsoftware.ca/8signs*
CA® eTrust Internet Security Suite Plus		*http://shop.ca.com/ca/products/internetsecurity/internetsecurity_suite.asp*
Check Point ZoneAlarm® Free Firewall, ZoneAlarm Pro, and ZoneAlarm Internet Security Suite		*http://www.zonealarm.com/security/en-us/computer-security.htm*
Comodo Personal Firewall	License: Shareware	*http://personalfirewall.comodo.com*
Deerfield.com Visnetic Firewall		*http://www.deerfield.com/products/visnetic-firewall*
Defender Pro™ 15-in-1 and 5-in-1		*http://www.defender-pro.com*
DigiPortal ChoiceMail One		*http://www.digiportal.com/products/homehome-office.html*
Emsisoft Online Armor Premium, ++, and Free Firewall	Origin: Austria; License: Freeware (Free Firewall only)	*http://www.online-armor.com*
ESET Smart Security	Origin: Ireland	*http://www.eset.ie/smartsecurity*
Filseclab Personal Firewall Professional Edition	Origin: China; License: Freeware (source code available for one-time license fee)	*http://www.filseclab.com/eng/products/firewall.htm* *http://www.filseclab.com/eng/products/sourcecode.htm*

Firewall	Exceptions	Information
Fortinet® FortiClient™		*http://www.fortinet.com/products/endpoint/forticlient.html*
F-Secure® Internet Security	Origin: Finland	*http://www.f-secure.com/en_EMEA/products/home-office/internet-security/index.html*
F/X Communications InJoy Firewall™ 4.0 Personal	Origin: Denmark; OS: Linux, OS/2 (Warp 3 and 4), Windows (XP and Vista)	*http://www.fx.dk/firewall/license.html*
G Data InternetSecurity and NotebookSecurity	Origin: Germany	*http://www.gdatasoftware.com/products/anti-virus-produkte/shop/123-private-user/1274-g-data-internetsecurity-2011.html* *http://www.gdatasoftware.com/products/anti-virus-produkte/shop/123-private-user/1450-g-data-notebooksecurity-2011.html*
GFI Sunbelt Personal Firewall™	License: Freeware	*http://www.sunbeltsoftware.com/Home-Home-Office/Sunbelt-Personal-Firewall*
Ghost Security GhostWall	License: Freeware	*http://www.ghostsecurity.com/ghostwall*
IBM Proventia Desktop Endpoint Security		*http://www-01.ibm.com/software/tivoli/products/desktop-endpoint-security*
InfoExpress CyberArmor Personal Firewall		*http://www.infoexpress.com/security_products/firewall_overview.php*
Innovative Startup Firewall		*http://www.innovative-sol.com/firewall*
Intego VirusBarrier X6 and Internet Security Barrier X6 (Single or Dual Protection)	Origin: U.S./France; OS: Mac OS X (Dual Protection presumes presence of Windows under Boot Camp, Parallels Desktop, or VMware Fusion VM)	*http://www.intego.com/internet-security-barrier* *http://www.intego.com/isbDP* *http://www.intego.com/virusbarrier* *http://www.intego.com/virusbarrierDP*
iSafer Firewall	License: Open source	*http://isafer.sourceforge.net*
Jetico Personal Firewall™	Origin: Finland	*http://www.jetico.com/firewall-jetico-personal-firewall*
Jiangmin Firewall	Origin: China	*http://global.jiangmin.com/products.htm*
Kaspersky® Internet Security	Origin: Russia	*http://www.kaspersky.com/kaspersky_internet_security*
Lavasoft Personal Firewall	Origin: Sweden	*http://www.lavasoft.com/products/lavasoft_personal_firewall.php*
Malware Guard System Firewall	License: Freeware	*http://malwareguard.com*
McAfee® Internet Security for Mac	OS: Mac OS X	*http://home.mcafee.com/Store/PackageDetail.aspx?pkgid=358*
MCS Firewall	Origin: Poland; License: Freeware/Shareware	*http://www.mcsstudios.com/en*
MicroWorld Technologies eScan™ Internet Security Suite		*http://www.escanav.com/english/content/products/generic_eScan/eScan.asp*
Mil Firewall	Origin: Bulgaria	*http://www.milincorporated.com/mil-firewall.html*
NETGATE FortKnox Personal Firewall	Origin: Slovak Republic; License: Freeware	*http://www.fortknox-firewall.com/index.php?option=com_content&task=view&id=18&Itemid=41*
Norman Personal Firewall	Origin: Norway	*http://www.norman.com/home/all_products/personal_firewall/norman_personal_firewall/en-us*

Firewall	Exceptions	Information
OMNIQUAD Personal Firewall	Origin: UK	*http://www.omniquad.com/newsite/consumer/personalfirewall/index.asp*
Open Door Networks DoorStop X Firewall	OS: Mac OS X	*http://www.opendoor.com/doorstop*
Panda Antivirus Pro and Internet Security for Netbooks, Internet Security, and Global Protection	Origin: Spain	*http://www.pandasecurity.com/usa/homeusers/solutions/antivirus* *http://www.pandasecurity.com/usa/homeusers/solutions/antivirus-netbooks* *http://www.pandasecurity.com/usa/homeusers/solutions/internet-security* *http://www.pandasecurity.com/usa/homeusers/solutions/global-protection*
PCSecurityShield Security Shield		*http://www.pcsecurityshield.com/PP/dspSecurityShield.aspx*
PC Tools™ Firewall Plus and Internet Security	Origin: UK; License: Freeware (Firewall Plus only)	*http://www.pctools.com/firewall* *http://www.pctools.com/internet-security*
Preventon® Personal Firewall Pro	Origin: UK	*http://www.preventon.com/firewall.php*
PrivacyWare Privatefirewall	Origin: U.S./Russia; License: Freeware	*http://www.privacyware.com/personal_firewall.html*
Rising Firewall and Rising Internet Security	Origin: China	*http://www.rising-global.com/products/Rising-Firewall-2011.html* *http://www.rising-global.com/products/Rising-Internet-Security-2011.html*
r-tools technology R-Firewall	Origin: Canada	*http://www.r-tt.com/r-firewall*
SecurStar SecurWall	Origin: Germany	*http://www.securstar.com/products_swall.php*
Soft4Ever Look 'n' Stop		*http://www.soft4ever.com/LooknStop/En/index2.htm*
SoftPerfect® Personal Firewall	Origin: Australia; License: Freeware	*http://www.softperfect.com/products/firewall/*
Sophos Endpoint Security and Control/ Endpoint Security and Data Protection	Origin: UK	*http://www.sophos.com/products/enterprise/endpoint/index2.html*
Sphinx Windows 7 Firewall Control and Firewall Control Plus	Origin: Germany; License: Firewall Control (not Plus): Freeware	*http://www.sphinx-soft.com/Vista/index.html*
Symantec Norton® Internet Security for Macintosh®	OS: Mac OS X	*http://www.symantec.com/norton/macintosh/internet-security*
Symantec Norton® Personal Firewall within Norton® Internet Security		*http://www.symantec.com/norton/products/internet-security.jsp*
Trend Micro® Internet Security		*http://us.trendmicro.com/us/products/personal/internet-security/index.html*
Trlokom Katana		*http://www.trlokom.com/product/katana-client.php*
TrustPort Internet Security	Origin: Czech Republic	*http://www.trustport.com/en/products/trustport-internet-security*
Webroot® Desktop Firewall		*http://www.webroot.com/consumer/products/desktopfirewall*

4.2 Personal Firewalls for Mobile Devices

Table 4-2 lists all known personal firewalls designed to run on mobile devices (ads, smartphones, personal digital assistants). All are commercially-licensed unless otherwise noted as exceptions. All are developed in the U.S. unless otherwise noted as exceptions.

Firewall	Exceptions	Operating System(s)	Information
Airscanner Mobile Firewall		Windows Mobile®	*http://www.airscanner.com/products/firewall*
Anguanjia Security Guarder	Origin: Unable to determine (Vietnam?); License: Freeware	Android	*http://www.androidapps.com/tech/apps/351260-security-guarder-anguanjia*
BlackBerry® Device Firewall		built into BlackBerry OS	*http://docs.blackberry.com/en/smartphone_users/deliverables/14194/BlackBerry_device_firewall_763467_11.jsp*
CA Mobile Firewall		Symbian S60, Windows Mobile	*http://cainternetsecurity.net/KB/KD.aspx?KDId=1217*
DroidX Advanced Call Filter, Super Call Blocker, Super Call Blocker Pro	License: Advanced Call Filter/Super Call Blocker: Freeware; Call Blocker Pro: Shareware	Android	*http://www.appbrain.com/app/advanced-call-filter/com.droidx.advancedcallfilter http://www.appbrain.com/app/super-call-blocker/com.droidx.blocks http://www.appbrain.com/app/super-call-blocker-pro/com.droidx.gblockspro*
Fortinet® FortiMobile™		Symbian S60, Windows Mobile	*http://www.fortinet.com/products/endpoint/fortimobile.html*
FruitMobile Bluetooth Firewall for Android	License: Freeware	Android	*http://www.fruitmobile.com/products.html*
Guardam GBlocker and Mobile Application SmsGuard	License: Shareware	Android	*http://www.guardam.com/2010/06/23/mobile-aplication-gblocker http://www.guardam.com/2010/06/23/mobile-aplication-smsguard http://www.intego.com/virusbarrier*
Intego VirusBarrier X6 iPad upgrade	Origin: U.S./France; Prerequisite: Intego VirusBarrier X6 for Mac OS X	iPad	*http://www.intego.com/virusbarrier http://www.intego.com/news/intego-updates-virusbarrier-x6-to-scan-the-apple-ipad.asp*
Lucky-Dog Xing aFirewall	Origin: China (Hong Kong); License: Shareware	Android	*http://androidfirewall.appspot.com*
MYMobile Protection Premium	Origin: UK	Android, Symbian S60, Windows Mobile	*https://www.mymobilesecurity.com/us/en/mms/eshop/product-info/my-mobile-protection/basemp*
SlideMe AndFire	License: Freeware	Android	*http://slideme.org/en/application/andfire*
Symantec Norton® Mobile Security™		Android	*http://us.norton.com/mobile-security*
Velurex Firewall	Origin: Unable to determine; License: Shareware	Android	*http://www.velurex.net/firewall.aspx*
Trend Micro™ Mobile Security		Symbian S60, Windows Mobile	*http://us.trendmicro.com/us/products/enterprise/mobile-security*

Firewall	Exceptions	Operating System(s)	Information
Yllier Firewall iP	License: Shareware	iPhone and iPad	*http://yllier.webs.com/firewall.html http://cydia.saurik.com/package/com.yllier.firewall*
Logic Unlimited™ Call Firewall	Origin: India; License: Freeware	Windows Mobile	*http://logic-unlimited.in/callfirewall.php*
F-Secure® Mobile Security	Origin: Finland	Android, Symbian S60, Windows Mobile	*http://www.f-secure.com/en/web/home_global/protection/mobile-security*
ProtectStar™ Mobile Firewall		Windows Mobile	*http://www.protectstar.com/2_73_60_products-mobilefirewall.html*

SECTION 5 ▶ Firewall Resources

The following sections list English-language print and online resources that provide more extensive, in-depth information about firewalls. Excluded are information sources that predate 2001 or that focus on a specific firewall product or supplier.

5.1 Books

The following are books in print that should be of interest to those wishing to obtain further information on the technical aspects of firewalls, or guidance on the acquisition or use of firewalls.

- Amon, Cherie and Thomas W. Shinder, and Anne Carasik-Henmi. *The Best Damn Firewall Book Period,* Second Edition (2007, Syngress Publishing).
- Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker,* Second Edition (2003, Addison Wesley Professional).
- Komar, Brian, Ronald Beekelaar, and Joern Wettern. *Firewalls for Dummies,* Second Edition (2003, For Dummies).
- Liu, Alex X. *Firewall Design and Analysis,* First Edition (2010, World Scientific Publishing Company).
- Noonan, Wes and Ido Dubrawsky. *Firewall Fundamentals,* First Edition (2006, Cisco Press).
- Pohlmann, Norbert and Tim Crothers. *Firewall Architecture for the Enterprise,* First Edition (2002, Wiley).
- Stewart, J. Michael. *Network Security, Firewalls, and VPNs,* First Edition (2010, Jones & Bartlett Learning).
- Whitman, Michael E. and Herbert J. Mattord. *Guide to Firewalls and Network Security,* Third Edition (2011, Delmar Cengage Learning).

5.2 Online Publications and Other Web-Based Resources

The following are downloadable technical papers and articles, Web sites, and Web pages pertaining to general firewall information, specific firewall technical topics and issues, and guidance and best practices for firewall selection, configuration, and administration. The reader is also encouraged to search YouTube for the numerous instructional videos focusing on firewalls.

5.2.1 General Firewall Information

- Department of Homeland Security National Cyber Security Division and Multi-State Information Sharing and Analysis Center. "Local Government Cyber Security: Beginners Guide to Firewalls", 19 June 2006. *http://www.esrmo.scio.nc.gov/CyberSecurity/library/pdfs/FirewallGuide.pdf* (accessed 27 December 2010).
- "Internet Firewalls: Frequently Asked Questions", Revision 10.9, April 2009. *http://www.interhack.net/pubs/fwfaq/* (accessed 27 December 2010).
- James Madison University. Personal Firewalls (work in progress). *http://www.jmu.edu/computing/security/info/pfw.shtml* (accessed 16 March 2011).
- Markus, Henry S. Home PC Firewall Guide page. *http://www.firewallguide.com/* (accessed 16 March 2011).
- National Infrastructure Security Co-ordination Centre (NISCC). "Understanding Firewalls: Technical Note 10/04", Revised 23 February 2005. *http://www.cpni.gov.uk/Documents/Publications/2005/2005007_TN1004_Understanding_firewalls.pdf* (accessed 16 March 2011).

- NISCC. "Firewalls: Viewpoint 02/2006", 31 March 2006. *http://www.cpni.gov.uk/documents/publications/2006/2006032-vp0206_firewalls.pdf* (accessed 16 March 2011).
- National Security Agency (NSA) Information Assurance Directorate (IAD) Systems and Network Analysis Center (SNAC). "Enterprise Firewall Types" (I73-001-06). *http://www.nsa.gov/ia/_files/factsheets/I73-001-06.pdf* (accessed 27 December 2010).
- OWASP. Web Application Firewall page. *http://www.owasp.org/index.php/Web_Application_Firewall* (accessed 27 December 2010).

5.2.2 Firewall Technology Resources

- Elfarag, Ahmed Abou, A. Baith M., and Hassan H. Alkhishali. "Description and Analysis of Embedded Firewall Techniques". In World Academy of Science Engineering and Technology Journal, Volume 58, 2009. *http://www.waset.org/journals/waset/v58/v58-75.pdf* –or– *http://www.waset.ac.nz/journals/waset/v58/v58-75.pdf* (accessed 16 March 2011).
- Ingham, Kenneth and Stephanie Forrest. "Network Firewalls". In Vemuri, V. Rao and V. Sreeharirao, eds. *Enhancing Computer Security with Smart Technology,* pp. 9-35 (2005, CRC Press). *http://www.cs.unm.edu/~forrest/publications/firewalls-05.pdf* (accessed 27 December 2010).
- Lipson, Howard and Ken van Wyk. "Application Firewalls and Proxies—Introduction and Concept of Operations". For Department of Homeland Security Build Security In portal, 27 September 2008. *https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/assembly/30-BSI.html* (accessed 27 December 2010).
- Liu, Alex X. "Firewall Policy Verification and Troubleshooting". *In Computer Networks,* Volume 53, Issue 16, November 2009, pp. 2800-2809. *http://www.cse.msu.edu/~alexliu/publications/FirewallVerification/verificationjournal.pdf* (accessed 16 March 2011).
- Martinsen, Pål-Erik. *Configuration and Implementation Issues for a Firewall System Running on a Mobile Handset.* Master of Information Technology Research Thesis, Queensland University of Technology, 2005. *http://eprints.qut.edu.au/16095/1/Pal-Erik_Martinsen_Thesis.pdf* (accessed 16 March 2011).
- Pabla, Inderjeet, Ibrahim Khalil, and Jiankun Hu. "Intranet Security *via* Firewalls". Chapter 11 in Stavroulakis, Peter and Mark Stamp, eds. *Handbook of Information and Communication Security* (2010, Springer). *http://www.cs.rmit.edu.au/~jiankun/Sample_Publication/Intranet.pdf* (accessed 16 March 2011).
- Peisert, Sean, Matt Bishop, and Keith Marzullo. "What Do Firewall's Protect?: An Empirical Study of Firewalls, Vulnerabilities, and Attacks". Technical Report CSE-2010-8, 30 March 2010. *http://www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-8.pdf* (accessed 16 March 2011).
- Raja, Fahimeh, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, Kellogg S. Booth. "Expectations, Perceptions, and Misconceptions of Personal Firewalls". Presented at Sixth Symposium on Usable Privacy and Security, Redmond, WA, 14-16 July 2010. *http://cups.cs.cmu.edu/soups/2010/posters/13.pdf* (accessed 16 March 2011).
- Rezvani, Mohsen and Ramtin Aryan. "Specification, Analysis, and Resolution of Anomalies in Firewall Security Policies". In *World Applied Sciences Journal,* Volume 7 (Special Issue for Computer and IT), 2009, pp. 188-198. *http://www.idosi.org/wasj/wasj7(c&it)/25.pdf* (accessed 16 March 2011).
- US-CERT National Cyber Alert System. "Understanding Firewalls" (Cyber Security Tip ST04-004). *http://www.us-cert.gov/cas/tips/ST04-004.html* (accessed 27 December 2010).

- Xu, Haiping, Abhinay Reddyreddy, and Daniel F. Fitch. "Defending Against XML-Based Attacks Using State-Based XML Firewall". Report for Computer and Information Science Dept., University of Massachusetts at Dartmouth, 14 February 2011. *http://www.cis.umassd.edu/~hxu/Papers/UMD/JCP-XU-2011.pdf* (accessed 16 March 2011).

5.2.3 Firewall Guidance

- Naidu, Krishni. "SANS Institute Security Consensus Operational Readiness Evaluation Firewall Checklist". *http://www.sans.org/score/checklists/FirewallChecklist.pdf* (accessed 16 March 2011).
- NISCC. "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks", Revision 1.4, 15 February 2005. *http://www.cpni.gov.uk/docs/re-20050223-00157.pdf* (accessed 27 December 2010).
- NSA IAD SNAC. "Desktop or Enterprise Firewall?" (Fact Sheet I73-002-06). *http://www.nsa.gov/ia/_files/factsheets/I73-002-06.pdf* (accessed 27 December 2010).
- NSA IAD SNAC. "Enterprise Firewalls in Encrypted Environments" (Fact Sheet I73-003-06). *http://www.nsa.gov/ia/_files/factsheets/I73-003-06.pdf* (accessed 27 December 2010).
- OWASP. "Best Practices: Use of Web Application Firewalls". *http://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls* (accessed 27 December 2010).
- Patterson, Don . "XML Firewall Architecture and Best Practices for Configuration and Auditing", SANS Institute GSEC Gold Certification paper, 2007. *http://www.sans.org/reading_room/whitepapers/firewalls/xml-firewall-architecture-practices-configuration-auditing_1766* (accessed 27 December 2010).
- Scarfone, Karen and Paul Hoffmann, National Institute of Standards and Technology (NIST). *Guidelines on Firewalls and Firewall Policy,* Special Publication SP 800-41, Revision 1, September 2009. *http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf* (accessed 27 December 2010).

5.2.4 Firewall Product Selection and Acquisition Resources

- Common Criteria Portal. Certified Products: Boundary Protection Devices and Systems list. *http://www.commoncriteriaportal.org/products/#BP* (accessed 16 March 2011).
- Common Criteria Portal. Certified Products: Network and Network-Related Devices and Systems list. *http://www.commoncriteriaportal.org/products/#NS* (accessed 16 March 2011).
- ICSA Labs. Certified Products: Network Firewalls list. *https://www.icsalabs.com/products?tid[]=4217* (accessed 16 March 2011).
- ICSA Labs. Certified Products: PC Firewalls list. *https://www.icsalabs.com/products?tid[]=4220* (accessed 16 March 2011).
- ICSA Labs. Certified Products: Web Application Firewalls list. *https://www.icsalabs.com/products?tid[]=4227* (accessed 16 March 2011).
- NIAP Common Criteria Evaluation and Validation Scheme. Validated Products List: Firewalls. *http://www.niap-ccevs.org/vpl/?tech_name=Firewall* (accessed 16 March 2011).
- *PC Magazine.* (Personal) Firewalls Product Finder page. *http://www.pcmag.com/category2/0,2806,4722,00.asp* (accessed 16 March 2011).
- Web Application Security Consortium. "Web Application Firewall Evaluation Criteria 1.0". *http://projects.webappsec.org/w/page/13246985/Web-Application-Firewall-Evaluation-Criteria* (accessed 27 December 2010).

APPENDIX ▸ **Acronyms, Abbreviations, Glossary**

The table in section A.1 lists and amplifies all acronyms and abbreviations used in this document. The table in section A.2 provides a glossary of firewall-related terms used in this document. As noted in Section 1.3, this glossary provides definitions for firewall-specific terms only. For broader computing and networking terms, the reader is encouraged to consult the following resources:

- International Foundation for Information Technology. Glossary of Information Technology (IT) Terms and Phrases. *http://if4it.org/glossary.html*
- American National Standards Institute Alliance for Telecommunications Industry Solutions. ATIS Telecom Glossary 2007. *http://www.atis.org/glossary*
- Navy/Marine Corps Intranet. NMCI Dictionary. *http://www.cnic.navy.mil/navycni/groups/public/@pub/@hq/documents/document/cnicd_a064707.pdf*
- World Wide Web Consortium. Web Services Glossary. *http://www.w3.org/TR/ws-gloss*

For general information assurance and cybersecurity terms, the reader is encouraged to consult the following resources:

- National Institute of Standards and Technology (NIST). Glossary of Key Information Security Terms, NIST IR 7298 Revision 1, February 2011. *http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf*
- Committee for National Security Systems. National Information Assurance (IA) Glossary. *http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf*
- US-CERT. IT Security Essential Body of Knowledge (EBK) Glossary of Terms. *http://www.us-cert.gov/ITSecurityEBK/EBKGlossary08.pdf*
- Internet Engineering Task Force. Internet Security Glossary, Version 2 (Request for Comments 4949). *http://www.ietf.org/rfc/rfc4949.txt*

A.1 Acronyms and Abbreviations

Acronym/Abbreviation	Amplification
®	Registered Trademark Symbol
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ACE	Application Control Engine
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AF	Application Firewall
Ajax	Asynchronous JavaScript and eXtensible Markup Language
AMI	Amazon Machine Image (of Linux)
API	Application Programmatic Interface
ApS	Anpartsselskab (Limited Liability Company)
ASCII	American Standard Code for Information Interchange
ASM	Application Security Manager
BGP	Border Gateway Protocol
BSD	Berkeley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAST	Carlisle Adams/Stafford Tavares Cipher
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CLG	Circuit-Level Gateway
CORBA	Common Object Request Broker Architecture
CRLs	Certificate Revocation List
CSEC	Communications Security Establishment Canada
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLP	Data Leak (or Loss) Prevention
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DNS	Domain Name System

Acronym/Abbreviation	Amplification
DoD	Department of Defense
DoS	Denial of Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DTD	Document Type Definition
DVD	Digital Video Disc
e.g.	Exempli Gratia (For Example)
EAL	Evaluation Assurance Level
EC2	Elastic Compute Cloud
EJB	Enterprise Java Bean
email	Electronic Mail
EMP	Extensible Messaging Platform
ESP	Encapsulating Security Payload
etc.	et cetera (and so forth)
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FW	Firewall
GB	Gigabyte
Gbps	Giga Bits Per Second
GCIS	General Center for Internet Services
GmbH	Gesellschaft mit beschränkter Haftung (company with limited liability)
GTA	Global Technology Associates
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol-Secure
I-DBC	Internet Inter-Object Request Broker Protocol Domain Boundary Controller
i.e.	id est (that is)
IA	Information Assurance
IAC	Information Analysis Centers
IAD	Information Assurance Division
IATAC	Information Assurance Technology Analysis Center
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IIOP	Internet Inter-Object Request Broker Protocol

Acronym/Abbreviation	Amplification
IIS	Internet Information Services
IKE	Internet Protocol Security Key Exchange
IM	Internet Messaging
IMAP	Internet Message Access Protocol
IMAPS	Internet Message Access Protocol -Secure
Inc.	Incorporated
IOS	Internetworking Operating System
IP	Internet Protocol
IPFW	Internet Protocol Firewall
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISA	Internet Security and Acceleration
ISAPI	Internet Server Application Programming Interface
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
JSON	JavaScript Object Notation
KVM	Kernel-based Virtual Machine
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLC	Limited Liability Company
Ltd.	Limited (Company)
MAC	Media Access Controller
MAG	Message Assurance Gateways
MB	Megabyte
mbH	mit beschränkter Haftung (with Limited Liability [Business])
Mbps	Mega Bits Per Second
MD5	Message Digest Five
MIME	Multipurpose Internet Mail Extensions
MSP	Managed Service Provider
NAC	Network Access Control
NAPT	Network Address Port Translation

Acronym/Abbreviation	Amplification
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NIAP	National Information Assurance Partnership
NIC	Network Interface Controller
NISCC	National Infrastructure Security Co-ordination Centre
NIST	National Institute of Standards and Technology
NSA	Network Security Appliance; National Security Agency
NTLM	(Windows) NT Local area network Manager
OCSP	Online Certificate Status Protocol
OS	Operating System
OWASP	Open Web Application Security Project
P2P	Peer-To-Peer
PAM	Pluggable Authentication Modules
PAT	Port Address Translation
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Digital Assistant
PDF	Portable Document Format
PF	Packet Filter
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POP3	Post Office Protocol-3
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
Pvt. Ltd.	Private Limited (Company)
QoS	Quality Of Service
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request For Comments (Internet Engineering Task Force)
RPC	Remote Procedure Call

Acronym/Abbreviation	Amplification
RSA	Rivest-Shamir-Adelman (Protocol)
RTP	Realtime Transport Protocol
RTSP	Real Time Streaming Protocol
SaaS	Software-As-A-Service
SAML	Security Assertion Markup Language
SCADA	Supervisory Control And Data Acquisition
SCSI	Small Computer System Interface
SFTP	Secure File Transfer Protocol
SGS	Security Gateway Solution
SHA	Secure Hash Algorithm
SIF	Stateful Inspection Firewall
SIP	Session Initiation Protocol
S.L.	Sociedad Limitada
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol -Secure
SNAC	Systems and Network Analysis Center
SNAT	Stateful Fail-over of Network Address Translation
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SPARC	Scalable Processor ARChitecture
SQL	Standard Query Language
Srl	Società a responsabilità limitata (limited liability company)
SSH	Secure Shell
SSI	Agence nationale de la sécurité des systèmes d'information
SSL	Secure Socket Layer
SSO	Single Sign-On
SuSE	Gesellschaft für Software-und Systementwicklung mbH
TACACS	Terminal Access Controller Access-Control System
TCP	Transport Control Protocol
TDM	Time Division Multiplexed
TFTP	Trivial FTP
TLS	Transport Layer Security
™	Trademark Symbol

Acronym/Abbreviation	Amplification
U.S.	United States
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UK	United Kingdom
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Universal Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VoIP	Voice-over-Internet Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide-Area Network
Wi-Fi	Wireless Fidelity
WS-	Web Service-*standard* (*e.g.,* WS-Security, WS-Encryption)
WS-I	Web Services Interoperability Organization
WSDL	Web Service Discovery Language
WWW	World Wide Web (protocols)
XACML	eXtensible Access Control Markup Language
XKMS	eXtensible Markup Language Key Management Specification
XML	eXtensible Markup Language
XSD	eXtensible Markup Language Schema Definition
XSLT	eXtensible Stylesheet Language Transformation
XSS	Cross-Site Scripting
XTM	Extensible Threat Management

A.2 Glossary

Term	Definition
Appliance	Hardware device specifically designed and/or configured to host a particular application or class of applications, such as a firewall.
Application Firewall	Firewall that operates at the application level of the TCP/IP stack to intercept all traffic traveling to or from a given type of application (Web application, database application, Web service, *etc.*), dropping all packets that are not transmitted *via* a protocol supported by the firewall's application type, and blocking the application traffic that does not conform to the firewall's security policy; also referred to as an application-level gateway or application-layer firewall. Increasingly, application firewalls inspect the application traffic for improper content to determine whether it does conform to policy. A Web application firewall can process traffic transmitted *via* popular Web protocols (*e.g.,* HTTP, FTP, POP3, IM, P2P protocols, *etc.*). A database firewall can process SQL traffic. An email firewall can process email protocols (*e.g.,* SMTP, POP3). An XML firewall can process traffic transmitted *via* popular XML-based Web service/Web 2.0 protocols (*e.g.,* SOAP, WSDL, UDDI, *etc.*). There is a class of operating system utilities that block execution of certain types of applications installed on the operating system; these too are sometimes referred to as application firewalls.
Blocking	Preventing or denying access based on a security policy. Blocking may be performed on inbound traffic, to prevent it from reaching the protected network, or it may be performed on outbound traffic, to prevent users on the internal network from accessing external systems, services, or Web sites on the external network.
Boundary	Physical or logical perimeter of a system or network.
Content Filtering	Processing and blocking or allowing the admittance from the external network of material that contains specified text strings (words and phrases) or data types, or that originates from specified addresses or hosts. Web content filters generally compare requested Web site addresses (URLs) against a list of addresses of known bad or indesirable Web sites in order to block requested access to those Web sites.
Deep Packet Inspection	Processing of packet payload rather than packet header, in order to make a decision about disposition of the packet. In firewalls and IDS/IPS, DLP, *etc.*, deep packet inspection is used to determine whether the content of network traffic conforms to policy rules governing its admissability or releasability.
Demilitarized Zone (DMZ)	Host or network segment inserted physically or logically as a "neutral zone" between an organization's private network and an external network (most often the Internet). The DMZ's purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to information and services provided by the internal network while shielding the internal network from attacks originating on the external network.
Firewall	Hardware/software gateway capability that, in accordance with a specific security policy, limits access and controls the flow of traffic between networks, hosts, or systems that exhibit different security attributes or postures. A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.
Gateway	Intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. A gateway operates by converting/translating transmission speeds, protocols, codes, or security measures from one network to the other. A security gateway separates trusted (or relatively more trusted) hosts on one side from untrusted (or less trusted) hosts on the other side. A firewall is a type of security gateway.
Hardened Operating System	Host operating system that has been configured to reduce its security weaknesses or to minimize the accessibility of its security weaknesses to potential exploiters.
Intrusion Detection System	Hardware or software system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, including both intrusions (attacks from outside the system/network) and misuse (attacks from within the system/network).

Term	Definition
Intrusion Prevention System	Hardware or software system that can detect an intrusive activity and attempt to stop it, ideally before the activity reaches its target.
Multifunction Firewall	Firewall that performs more than one firewalling function, often as well as other non-firewalling security functions, such as VPN server functions, virus/malware/spam/phishing detection, user authentication, *etc.*, and sometimes also non-security functions. Multifunction firewalls are increasingly referred to as unified threat management gateways.
Network Address Translation (NAT)	Routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema that maps those internal addresses to the firewall's own external address for purposes of providing a return address to the external network. The firewall keeps track of the actual internal addresses so that inbound packets intended for those internal systems can have the firewall's address stripped off and replaced with the correct internal system address for routing to the internal system.
Network Firewall	Firewall that operates on traffic below the application layer, generally traffic transmitted *via* protocols at Layers 2 and 3 of the TCP/IP protocol stack.
Packet Filtering	Processing a flow of data and selectively blocking or permitting passage of individual packets according to a security policy.
Personal Firewall	Utility or application on a personal computer or mobile computing device that monitors network activity and blocks unauthorized communications. Most personal firewalls are, in fact, multifunction firewalls that perform a number of non-firewalling content checking, authentication, encryption, and access control functions.
Proxy	Application often used as, or as part of, a firewall. A proxy relays application transactions or a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. In a firewall, a proxy server may support proxies for several applications and protocols (*e.g.,* FTP, HTTP, and TELNET). Instead of a client in the protected enclave connecting directly to an external server, the internal client connects to the proxy server, which in turn connects to the external server. The proxy server waits for a request from inside the firewall, forwards the request to the server outside the firewall, gets the response, then sends the response back to the client. The proxy may be transparent to the clients, or they may need to connect first to the proxy server, and then use that association to also initiate a connection to the real server. In this way, the proxy "breaks" the connection between a client and server and effectively blocks the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the internal network. A proxy can provide security service beyond that which is normally part of the relayed protocol, such as access control based on peer entity authentication of clients, or peer entity authentication of servers when clients do not have that ability. A proxy at OSIRM Layer 7 can also provide finer-grained security service than can a filtering router at Layer 3. For example, an FTP proxy could permit transfers out of, but not into, a protected network.
Proxy Agent	Software application running on a firewall or dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the host device
Quality Of Service (QoS)	measurable end-to-end performance properties of a network service, which can be guaranteed in advance according to a Service-Level Agreement. These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, *etc.* QoS functions may adjust traffic prioritization, and other QoS attributes in order to satisfy their QoS guarantees.
Stateful Firewall	Firewall that keeps track of the context of a connection between two IP addresses, *i.e.,* it keeps track of the interchange of packets for the entire duration of that connection, thus enabling it to make security policy decisions based on whether a packet received from an IP address is associated with an existing connection or indicates the existence of a new connection. If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.
Stateful Inspection Firewall	Stateful firewall that performs packet inspection; also referred to as a stateful packet inspection firewall.

Term	Definition
Stateless Firewall	Firewall that does not keep track of connection context. A stateless firewall treats every packet as if it belongs to a new connection, and thus must evaluate each packet individually according to the same ruleset for new connections.
Tunneling	Technology enabling one network to send its data *via* another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. When tunneling is used in VPNs, the encapsulation mechanism is encryption.
Virtual Appliance	A software image that contains a software stack designed to run inside an existing VM on a virtualization platform such as VirtualBox, Xen, VMware, or Parallels that can be hosted on a commodity hardware platform (Intel-based PC, Apple Macintosh). Like a physical appliance, a virtual appliance provides a platform for running an application such as a firewall. Unlike a physical appliance, the hardware that hosts the virtual appliance has not been specifically "tuned" for use by the application that runs on the virtual appliance.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks. In addition to cryptographic tunneling, VPNs use other security controls (*e.g.,* certificate-based authentication) together with endpoint address translation to give the user the impression that she/he is communicating *via* a dedicated line. VPNs are often used to create VPN tunnels between firewalls, enabling private networks connected to those firewalls to transmit their traffic *via* the firewall-to-firewall encrypted VPN tunnels over the Internet.
Vpn Firewall	Firewall that also hosts a VPN server and, possibly, one or more VPN clients, enabling it to also perform as a VPN gateway.