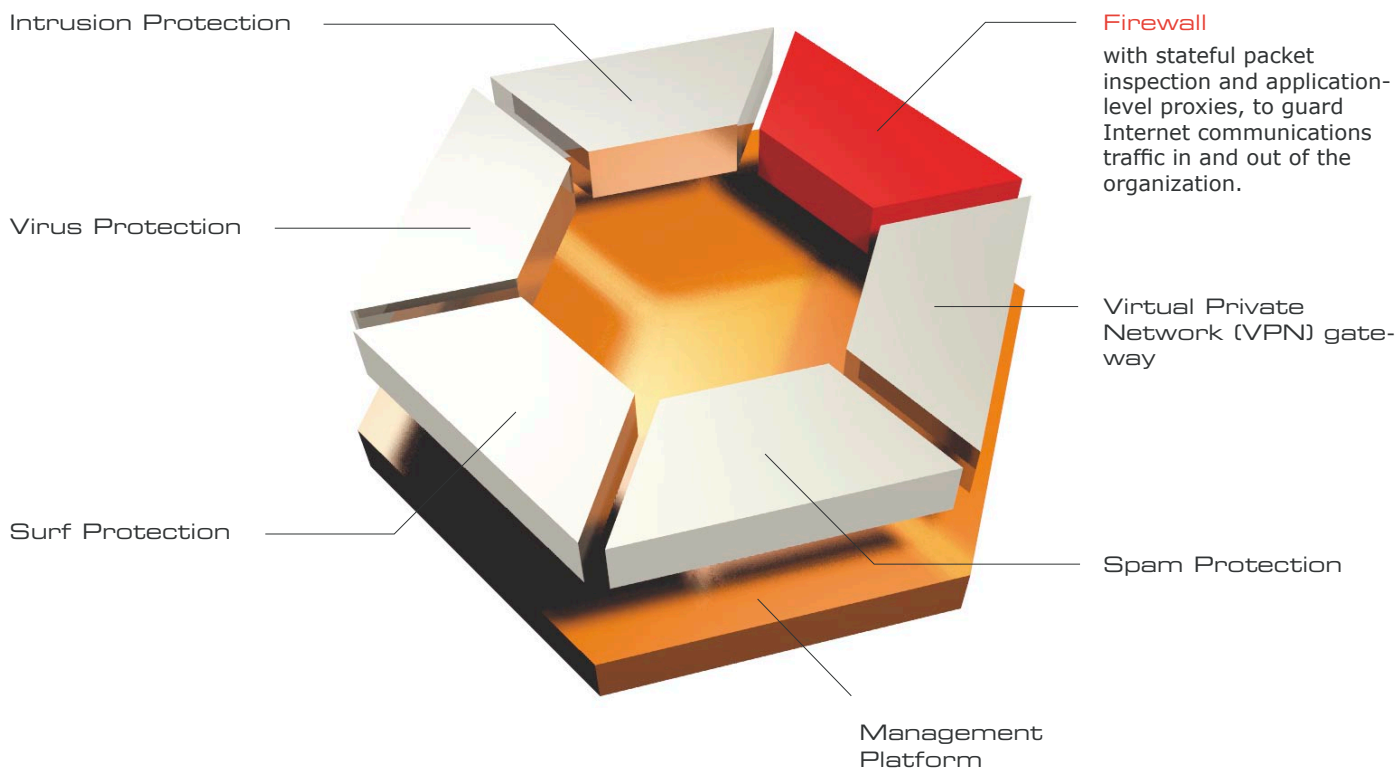


Astaro Security Linux V5 Firewall

Network security affects everyone. In the 2003 CSI/FBI Computer Crime and Security Survey, 78% of respondents reported attacks through their Internet connection, leading to financial losses from information theft, financial fraud, disabled web sites and networks (denial of service), viruses, sabotage, and other threats.

A firewall is an essential foundation for network security. The Astaro Security Linux firewall manages all communications traffic between the Internet and internal networks to block unauthorized access. Stateful packet inspection and application-level deep packet filtering ensure that both network and application behavior conform to rules and policies set by the administrator.



Description

The Astaro Security Linux firewall manages inbound and outbound communications traffic. Administrators can block or allow access, for each protocol, to each internal network, server, service, and user group. The firewall inspects both networking information (packet headers) and application information (payloads) to detect and block suspicious traffic.

Stateful Packet Inspection

Astaro Security Linux inspects network packet headers to manage traffic between the Internet and internal networks, servers, and users.

With the easy-to-use WebAdmin graphical interface, administrators can quickly set rules to block or allow traffic, by protocol and by port, between pairs of source and destination addresses.

Astaro Security Linux examines individual packet headers to make sure that they conform to the rules of the appropriate protocol (packet filtering), and tracks the sequence of events during ongoing connections to detect violations of normal processes (stateful packet inspection).

Application-Level Deep Packet Filtering

The Astaro Security Linux firewall utilizes application-level proxies to scan the application-related content of communications packets (payloads) to ensure conformance with rules specific to web traffic, email, DNS, and other broad application types.

The optional Astaro Security Linux Intrusion Protection detects additional threats related to specific applications and protocols. This is activated by sub-

scribing to the separately-priced Astaro Intrusion Protection service.

Security Proxies

Astaro Security Linux provides comprehensive proxies for a variety of protocols, including:

- ▶ HTTP
- ▶ DNS
- ▶ SOCKS
- ▶ POP3
- ▶ Ident
- ▶ SMTP

These proxies simplify management by allowing administrators to quickly and easily enable and disable protocols and features such as content filtering, caching, whitelists and blacklists, file extension filtering, and MIME error checking.

Firewall

NAT and Masquerading

Dynamic and static Network Address Translation (NAT) and masquerading conceal internal IP addresses behind a "public" IP address, to prevent hackers from learning about internal networks, servers, and users.

DoS Protection

Astaro Security Linux protects against common Denial of Service (DoS) attacks like TCP SYN flood, ICMP flood, UDP flood, Smurf, Trinoo, and IP spoofing.

Traffic Shaping and QoS

Administrators can increase or decrease the priority of different types of traffic between specific endpoints, providing quality of service (QoS) for critical transactions.

Detailed Reporting

Astaro Security Linux provides detailed reporting on network traffic, connections, packet filter violations, hardware utilization on the firewall system, and other information for managing the firewall.

Accounting reports provide detailed data on traffic to and from network segments.

Detailed logs can be stored and viewed in text format, or exported to spreadsheets and reporting systems for ad-hoc or specialized analysis.

Foundation of a Complete Network Security Solution

The firewall is the foundation of the six security applications included in Astaro Security Linux. Applications such as Intrusion Protection and Virus Protection work with the firewall so that traffic related to security threats can be blocked immediately, before infecting internal networks.

Operating all six applications in-line on the same system can improve performance by eliminating delays vectoring files back and forth to separate systems for virus, spam, and intrusion scanning.

Astaro Security Linux administration is simple and management costs are low because all six applications share:

- ▶ One installation process
- ▶ One management interface
- ▶ One update mechanism
- ▶ One set of logs and reports

About Astaro

Astaro provides a network security solution that is complete, simple to manage, affordable, and effective. Astaro selects and integrates the best of open source security software to provide the widest range of innovative security technology available in a single package. Astaro's software has won numerous awards, and is in use on over 20,000 networks in more than 60 countries. Astaro Security Linux is distributed by a worldwide network of solutions partners who offer local support and services.



www.astaro.com

Americas

Astaro Corporation
3 New England Executive Park
Burlington, MA 01803
USA

T: +1 781 272 8787
F: +1 781 272 8989
americas@astaro.com

Offices in Kelowna, BC and
Sunnyvale, CA

Europe, Middle East, Africa (EMEA)

Astaro AG
Pfinztalstrasse 90
76227 Karlsruhe
Germany

T: +49 721 490 069 0
F: +49 721 490 069 55
emea@astaro.com

Offices in Pinneberg/Germany,
Paris/France and Reading/UK

Asia Pacific (APAC)

T: +49 721 490 069 0
F: +49 721 490 069 55
apac@astaro.com

Your Astaro Partner