

## Astaro Security Linux V5 Intrusion Protection

Hackers are becoming continuously more skillful at finding and exploiting weaknesses in every type of technology and at creating “blended attacks” that evade traditional security products.

Astaro Security Linux Intrusion Protection identifies and blocks over 1,500 different kinds of probes and attacks. It can notify administrators of suspicious activities, or have the firewall stop attacks immediately.

### Intrusion Protection

Protection to detect and stop hostile probes and application-based attacks.

### Virus Protection

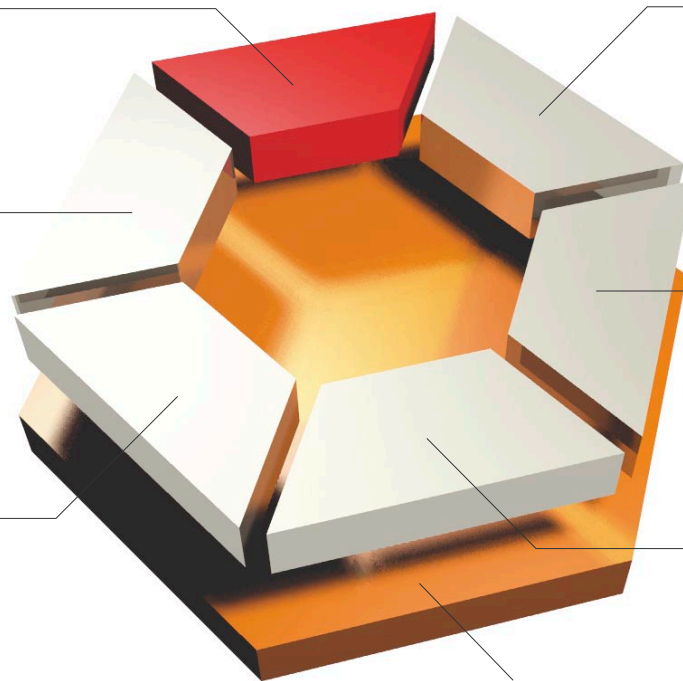
### Surf Protection

### Firewall

### Virtual Private Network (VPN) gateway

### Spam Protection

### Management Platform



## Description

Astaro Security Linux Intrusion Protection scans inbound network traffic and uses pattern recognition technology to detect over 1,500 types of probes, denial of service (DoS) attacks, and attempts to exploit application vulnerabilities. Administrators can set thresholds for being notified about incidents, have suspicious traffic blocked, and enable and disable rules for maximum performance.

### Extensive Detection Rules

Astaro Security Linux utilizes a database of over 1,500 rules to detect patterns indicating:

- ▶ Hostile probing, port scans, backdoor probes, illegitimate interrogations, host sweeps and other activities.

- ▶ Denial of Service (DoS) attacks like SYN flood.
- ▶ Protocol exploitations, leveraging weaknesses in DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, x11 and other network protocols.
- ▶ Application attacks, exploiting programming errors in internally developed software and CGI scripts, and in popular applications and databases such as Oracle, MySQL server, ColdFusion and FrontPage.
- ▶ Targeted attacks that exploit the vulnerability of messaging and chat traffic.

### Intrusion Detection and Prevention

Astaro Security Linux performs intrusion detection by identifying suspicious behavior and notifying the system administrator about incidents.

The software can also provide intrusion prevention by working with the firewall to immediately block incoming traffic associated with intrusions.

Intrusion detection and prevention can be employed simultaneously.

New threat patterns are installed frequently through the Astaro Up2Date service. Astaro monitors and adopts new threat patterns posted to the database of the Snort project, the largest open source intrusion detection project.

## Intrusion Protection

### Performance and Control

By putting intrusion protection in-line with the firewall, Astaro Security Linux ensures that all Internet and VPN traffic is inspected, and that there are no delays as traffic is routed to a separate sensor.

The administrator can also tailor testing to each network and server by:

- ▶ Enabling or disabling any of the over 1,500 rules.
- ▶ Customizing existing rules or creating new ones.
- ▶ Performing certain classes of tests only on specific networks or traffic from specific servers (for example, executing email-related tests only on traffic to and from email servers).

Rule changes are applied immediately, without any need to reboot the firewall or change network configurations.

### Astaro Intrusion Protection Subscription

Intrusion Protection is an optional subscription that is installed as part of Astaro Security Linux and activated by a license key.

### Selected Classes of Intrusion Detection Rules

Probes and Attacks

- ▶ Backdoor software
- ▶ Denial of service
- ▶ Distributed denial of service

- ▶ Network scanning
- ▶ Unwanted traffic

### Applications and Services

- ▶ Messaging and chat
- ▶ MySQL server database
- ▶ Oracle database
- ▶ CGI scripts
- ▶ Command shell code
- ▶ ColdFusion
- ▶ FrontPage
- ▶ Microsoft IIS
- ▶ Multimedia streaming software
- ▶ P2P networks (Napster, Kazaa)

### Protocols

- ▶ DNS
- ▶ FTP
- ▶ ICMP
- ▶ IMAP
- ▶ NetBIOS
- ▶ NNTP
- ▶ P2P
- ▶ POP2
- ▶ POP3
- ▶ RPC
- ▶ SMTP
- ▶ SQL
- ▶ TFTP
- ▶ X11

## Part of a Complete Network Security Solution

Intrusion Protection is one of six security applications included in 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.

### 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



[www.astaro.com](http://www.astaro.com)

### Asia Pacific (APAC)

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

Your Astaro Partner