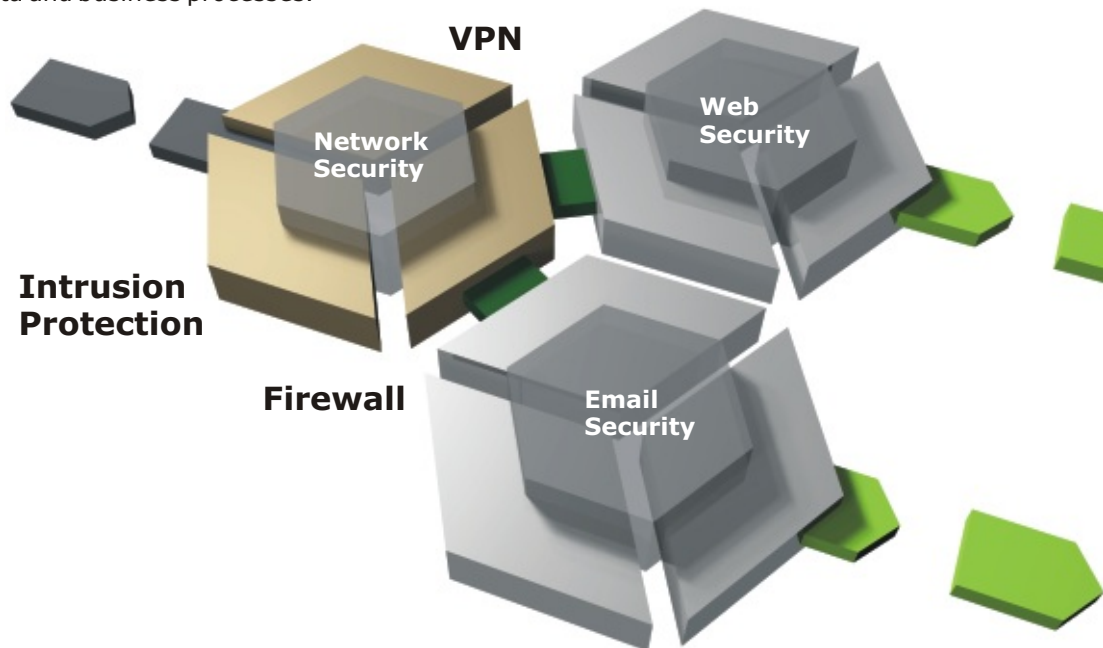


# Network Security



## Network Security

New vulnerabilities in computer applications are being announced every day. Emerging technologies are creating gaps in network security. Hackers and criminals are becoming more skillful at exploiting weaknesses for fun and for financial gain. Organizations need the best possible defenses against attacks on their networks and applications in order to protect their data and business processes.



## Astaro Network Security

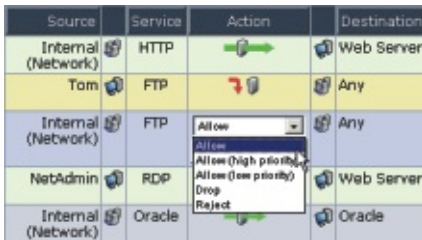
- ▶ **Firewall**, with stateful packet inspection and application-level proxies, guards Internet communications traffic in and out of the organization.
- ▶ **Intrusion Protection** detects and blocks probes and application-based attacks using heuristics, anomaly detection, and pattern-based techniques.
- ▶ **Virtual Private Network Gateway** assures secure communications with remote offices and "road warriors".

Astaro Security Gateway appliances and software include a firewall, an intrusion protection system and a VPN gateway. These core security applications ensure that network traffic conforms to rules set by the administrator, block over 3,000 different threats, stop "zero day attacks" by detecting sudden changes in network behavior, and reduce costs by assuring secure Internet communications with remote offices and employees.

These applications are fully integrated with the other parts of Astaro Security Gateway appliances and software, so they are easy to deploy, configure and manage as part of a complete network security infrastructure.

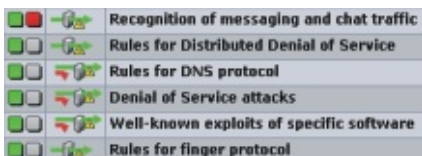
# Firewall

The Astaro firewall manages inbound and outbound communications traffic, as well as traffic between internal networks. 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.



Source	Service	Action	Destination
Internal (Network)	HTTP	Allow	Web Server
Tom	FTP	Deny	Any
Internal (Network)	FTP	Allow	Any
NetAdmin	RDP	Allow	Web Server
Internal (Network)	Oracle	Deny	Oracle

Easy Configuration



Recognition of messaging and chat traffic
Rules for Distributed Denial of Service
Rules for DNS protocol
Denial of Service attacks
Well-known exploits of specific software
Rules for finger protocol

Complete Protection

## Application-Level Deep Packet Filtering

Astaro's firewall provides both stateful packet inspection and application-level deep packet filtering. Packet headers are inspected, and ongoing connections are monitored, to make sure that they conform to the appropriate policies. Application-level proxies scan content (payloads) to ensure conformance with rules specific to web traffic, email,

DNS, and other broad application types.

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.

## Security Proxies

A comprehensive set of proxies are provided for HTTP, SMTP, POP3, DNS, SIP and SOCKS. These proxies simplify management by allowing administrators to quickly and easily enable and disable protocols and features such as virus scanning, content filtering, caching, whitelists and blacklists, file extension filtering, and MIME error checking. Web and email proxies can be run in transparent mode, so that each users' packets can be redirected to the proxy without having to reconfigure desktop settings.

## NAT, Masquerading and DoS Protection

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.

Astaro's firewall protects against common Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks such as TCP SYN flood, ICMP flood, UDP flood, Smurf, Trinoo, and IP spoofing.

## Transparent Firewall Mode

Packets can traverse the firewall in transparent mode without modifying

any of the source or destination information in the packet header. The firewall can be inserted or removed from the network without needing to reconfigure IP addresses.

## Time-Based Rules and Policy-Based Routing

Packet filter rules can be set for specified time periods. User groups can be granted access to networks and servers at certain times of day and denied access at others.

Astaro's firewall can forward and route packets based on destination IP address, source IP address, source port, and destination port. Traffic can be spread over multiple Internet uplinks to improve application performance, reduce bandwidth use, and control costs.

## 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 Gateway 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.

## Intrusion Protection

Astaro's Intrusion Protection application scans inbound network traffic and uses pattern recognition technology and anomaly detection to identify over 3,000 types of probes and attacks.

### Extensive Detection Rules

Astaro's Intrusion Protection utilizes a database of over 3,000 rules to detect patterns indicating:

- ▶ Hostile probing, port scans, backdoor probes, illegitimate interrogations, and host sweeps.
- ▶ Exploitations of weaknesses in DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, x11 and other network protocols.
- ▶ Application attacks, exploiting vulnerabilities in home-grown software and popular applications such as IIS, Oracle, MySQL server, and Frontpage.
- ▶ Activities relating to messaging, chat traffic, and Peer-2-Peer (P2P) networking.

### Anomaly Detection

"Zero-day-attacks" are malicious threats that attack networks before signatures have been developed. To protect against them, Astaro's Intrusion Protection identifies typical network traffic patterns via statistical and heuristic analysis. It then alerts administrators when it detects anomalies that indicate attacks, such as new network services or previously unseen hosts.

### Intrusion Detection and Prevention

Astaro's Intrusion Protection application can notify administrators about suspicious behavior ("intrusion detection") and work with the firewall

to immediately block incoming traffic associated with intrusions ("intrusion prevention").

New threat patterns are installed frequently through the Astaro Up2Date service. Astaro utilizes new threat patterns from the Snort project and from Sourcefire, the leading Open Source and commercial sources of intrusion patterns.

### Performance and Control

Because intrusion protection is in-line with the firewall, all Internet and VPN traffic is inspected, and there are no delays as traffic is routed to a separate sensor. Rule changes are applied immediately, without any need to reboot the firewall or change network configurations.

The administrator can also tailor intrusion testing to each network by:

- ▶ Enabling or disabling any of the over 3,000 rules.
- ▶ Customizing existing rules and creating new ones.

- ▶ Performing tests only where they are needed (for example, email-related tests only on traffic to email servers).

### 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
- ▶ P2P networks (Napster, Kazaa)
- ▶ Coldfusion
- ▶ FrontPage
- ▶ Microsoft IIS
- ▶ Multimedia streaming software

### Protocols

DNS, FTP, ICMP, IMAP, NetBIOS, NNTP, P2P, POP2, POP3, RPC, SMTP, SQL, TFTP, X11.

## About Astaro

Astaro was founded in 2000, with the goal of creating integrated, easy-to-use network security products. The company's leading Unified Threat Management product, Astaro Security Gateway, protects more than 25,000 customers, ranging from small businesses, to government and non-profit agencies, to global enterprises. Astaro's firewall is **ICSA Labs certified**. The company's technology has received recognition and awards such as **Editors' Choice** and **Best Business Security Solution of the Year** from PC Magazine, **Best Security Solution** from LinuxWorld Expo, **10 Stars** and **Test Center Recommended** from CRN Magazine, **Five Stars** from SC Magazine, "**Extremely Cost-Effective**" from The Tolly Group, and "**Excellent**" from InfoWorld Magazine. Astaro is co-headquartered in Karlsruhe, Germany and Boston, United States, with offices and solutions partners in over 40 countries.



## VPN

The Astaro VPN (Virtual Private Network) gateway uses a variety of data encryption methods to create a secure communications "tunnel" over the public Internet.

### Multiple Architectures

To accommodate the needs of branch offices, home users, and "road warriors", the VPN gateway supports a variety of VPN architectures, including Net-to-Net, Host-to-Net, and Host-to-Host.

### Broad Protocol and Client Support

The Astaro VPN gateway supports VPN protocols like IPSec, L2TP over IPSec, and PPTP. Administrators can select from a broad range of VPN clients, including the native Windows and Windows Mobile PPTP and L2TP over IPSec clients, the Mac OS X VPN client, and other VPN clients that follow the

IPSec standard, including the Astaro Secure Client. Different clients can be mixed in an Astaro VPN environment.

### Certificate Authority

The Astaro Security Gateway includes an internal certificate authority with authentication based on PKI-trustchain.

### Simplified Remote Access

Dynamic IP addresses and DNS/WINS server addresses, taken from a virtual address pool or provided by an DHCP server, can be distributed automatically to simplify remote access. IPSec client configurations can be distributed from a central point, simplifying mass rollouts of IPSec VPNs.

### Integrates Into Existing Environments

Astaro's VPN gateway is easy to integrate into existing environments. It can authenticate VPN users against local

databases, Radius Servers, Novell eDirectory, Microsoft Active Directory, and LDAP-compliant enterprise directories. It can also apply access policies based on users and groups, IPs and networks, and PKI-based IPSec user groups.

### Firewall Integration

Astaro's VPN gateway is fully integrated with Astaro's firewall. IPSec VPNs can utilize NAT traversal and virtual IP addresses. Firewall settings are generated automatically when VPN clients are configured. Packet filter policies can be specified on a per-user basis. VPN user groups can be created and used to grant access rights.

## Summary of Supported Algorithms and Protocols

Encryption algorithms supported:

- ▶ AES (Rijndael)
- ▶ DES
- ▶ 3DES
- ▶ Blowfish
- ▶ Serpent 128-bit
- ▶ Twofish 128-bit
- ▶ MPPE (40 and 128 bit)

Authentication methods include:

- ▶ Passphrase (PSK)
- ▶ Certificates (X.509v3)
- ▶ Raw RSA Keys
- ▶ CHAP, MSCHAP, MSCHAPv2, and PAP
- ▶ RADIUS (for L2TP, IPSec and PPTP)

IPSec protocols include:

- ▶ Internet Key Exchange (IKE)
- ▶ Encapsulated Security Payload (ESP)
- ▶ Layer 2 Tunneling Protocol (L2TP)
- ▶ NAT-Traversal

## Learn More

Download the free trial software at [www.astaro.com](http://www.astaro.com) or request a free trial appliance today! Contact Astaro at:

### The Americas

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

T: +1 781 345 5000  
F: +1 781 345 5100  
[americas@astaro.com](mailto:americas@astaro.com)

### Europe, Middle East, Africa

Astaro AG  
Amalienbadstrasse 36  
76227 Karlsruhe  
Germany

T: +49 721 255 16 0  
F: +49 721 255 16 200  
[emea@astaro.com](mailto:emea@astaro.com)

### Asia Pacific Region

Astaro Corporation  
30th Floor Bank of China Tower  
1 Garden Road, Central  
Hong Kong, China

T: +852 2251 8514  
F: +852 2251 8515  
[apac@astaro.com](mailto:apac@astaro.com)

## Your Astaro Solutions Partner

