What's New In Astaro Security Linux V6

Transparent Firewall Mode

Packets can traverse the firewall without modifying any of the source or destination information in the IP packet header (acting like a layer 2 switch or bridge). There is no need to reconfigure IP space from currently assigned addresses. (Previously a subnet had to be split in at least two different subnets in order to put ASL in between). It is easy to pull a firewall out of the loop to diagnose network problems and to accurately map problem IP addresses.

Time-Based Packet Filter and Surf Protection Configuration

You can apply configuration options for packet and URL filters for specified time periods. For example, you can enable a set of firewall rules that allows a specific group access to specific servers only on Monday through Friday, from 8:00AM to 5:00PM.

Support for the Linux Kernel 2.6

Astaro Security Linux V6 utilizes the new Linux kernel 2.6. Benefits include:

- Support for S-ATA disks
- Increased performance for multithreaded applications (e.g. the content filter) via use of new thread library and support of Hyper-Threading Technology. This enables a single physical processor to execute two or more separate code streams (threads) concurrently.
- Support of new hardware and new devices

Policy-Based Routing

Traffic can be forwarded and routed based on source IP address, source port and destination port (in addition to normal routing, which is based on the destination IP address). With this feature traffic can be spread over multiple Internet uplinks to improve application performance, improve the use of bandwidth, and control costs.

SIP (Session Initiation Protocol) Proxy

The SIP Proxy increases flexibility, security and performance when supporting Voice over IP (VoIP) communications. SIP software clients (like kphone, xlite) and SIP hardware clients (Voice over IP phones which are SIP-compatible, such as those from Cisco, Grandstream or Snom) can work behind an IP masquerading firewall or NAT router.

Anomaly-Based Intrusion Protection

Increased protection against "zero-day-attacks"(malicious threats that attack enterprise networks before signatures have been developed). To guard against these early attacks, Astaro Security Linux analyzes the behavior of "normal" traffic via statistical and heuristic analysis and identifies anomalies that indicate a possible new attack, for example, new services, previously unseen hosts, and unusual amounts of traffic.

Novell eDirectory Support

New functionality is provided to allow easier integration of ASL into existing eDirectory environments. You can now define containers/contexts to specify a starting point within the directory tree where the users that should be authenticated are included. You can also define eDirectory groups that can be used for various authentication clients (WebAdmin, HTTP Proxy, SMTP Proxy, SOCKS) and you can apply content filter rules (profiles) to specific eDirectory groups.

Enhanced IPSec VPN Status View

A new, user-friendly view on the current VPN status, for example, active tunnels.

IPSec Dead Peer Detection

Automatic detection of IPSec gateways and clients that become unavailable, even if the IPSec SA has not yet expired. This feature allows faster detection of network outages and IPSec peer crashes.

Accelerated High Availability Take-Over

For systems in a high availability configuration, the time is reduced for the back-up system to take over when the primary system fails.

Enhanced Denial of Service (DoS) Protection

The release includes enhanced configuration options and supported protocols (TCP, UDP and ICMP) to protect against DoS/Flood attacks.

Bypass List for the Transparent Proxies

The implementation of transparent HTTP in Astaro Security Linux V5 redirected every request coming from an "Allowed Network" into the proxy. With V6 you can configure an exclude list of certain sources and destinations that should not be redirected to HTTP, POP3 or SMTP proxies, specified by IP addresses or hostnames.

Up2Date Supports Resuming Downloads

System Up2Dates can resume a previously broken download of a package to decrease total transfer times.

Pattern Up2Dates also remember which patterns have already been downloaded if a previous download was interrupted.

Distribution of PPTP & L2TP over IPSec roadwarrior IP addresses received by DHCP server

This feature allows the use of DHCP served IP addresses for remote access.

SSL-LDAP

Connections to LDAP servers can be encrypted using SSL/TLS standards. This allows using LDAP authentication over public networks such as the Internet

Astaro Portscan Detection PSD

The firewall detects portscans that are targeted either towards the firewall or towards a protected network behind the device. If the device detects a portscan, it either notifies the system administrator or blocks the relevant packets. This means the device can filter out portscans that are targeted against other machines, so the scanning packets never reach their destination. Even a machine with many open ports (like a default Windows system) does not reveal any ports.

Spyware reporting

A "Spyware" line has been added to the Reporting->Content Filter->HTTP graph.

Extend DNS Network Object

You can now create DNS network objects (hostnames).that have multiple resource records (IP addresses). This enhances the capabilities of using DNS hostnames within packet filter rules, bypass lists etc.

SMTP Proxy File Extension Filter

The Content Filter Frontend now provides an advanced parsing of e-mails and their actual MIME content, so that it is now possible to match against Chinese or other non-standard character sets. It can now also match against filenames with encoded MIME strucutre, e.g. including escape sequences or filenames which are forged to be written in multiple lines etc.

Wipe Local Log File Archives

A button in Local Logs Settings has been added to make it easy to delete the local log file archives. This allows to remove log information that's no longer needed from disk.

POP3 Proxy Enhancements

The reporting on blocked POP3 messages has been enhanced to include more details (sender, subject, date…) providing easier administration and search capabilities.

Detailed Notification E-mail for Intrusion Protection

The automatic notification e-mail which is generated by Astaro Security Linux has been enhanced so that it is easier to read and contains more useful information.

Roadwarrior CA Virtual Address Pool

The Roadwarrior CA connection type is suitable for large IPSec setups with hundreds or thousands of clients. You can now specify a virtual IP address pool for these clients.

Support of Multiple PPPoE uplinks

You can now configure more than one WAN interface running PPPoE (typically for DSL uplinks to ISPs). This allows for more flexible network configurations e.g. for policy-based routing or uplink-failover.

SMTP Proxy Transparent Mode

The SMTP proxy can now be operated transparent mode. The great advantage of proxies operating in transparent mode is the possibility to offer an additional security for specific services without losing the flexibility and without modifying any of the clients or server. It is also possible to exclude certain source/destination networks from being proxied