

Security Appliance

SecFW

The SecFW appliance is optimized to be used as a central network protection between the Internet and the internal network. SecFW is the combination of hardware and software that can physically and logically separate and control the flow travelling different segments with respect to different security levels. The SecFW can accept up to ten Ethernet segments, offering each one 100 Megabits per second of firewall throughput.

Besides the fact that SecFW offers all standard firewalling functionalities (packet filtering, stateful inspection, ...) SecFW has outstanding features like the possibility to specify rules by interface (not only based on IP addresses), transparent routing and transparent proxy. SecFW provide also customize extensive logging.

SecFW is designed for maximum network uptime and security by integrating all fire-wallling functionalities over a Conostix standard component -SecCORE- which is composed of a secure Operating System, a local IDS (Intrusion Detection System), MAC (Mandatory Access Control) and a High Availability module.

The system can be easily managed from a standard Web browser or via a SSH tunnel.

Key features

- explicitly deny/permit any packet from passing through
- distinguish between various interfaces filter by IP networks or hosts
- selectively filter any IP protocol
- selectively filter fragmented IP packets
- selectively filter packets with IP op-

tions

- send back an ICMP error/TCP reset for blocked packets
- keep packet state information for TCP, UDP and ICMP packet flows (stateful inspection)
- keep fragment state information for any IP packet, applying the same rule to all fragments
- act as a Network Address Translator (NAT)
- use redirection to setup true transparent proxy connections
- provide packet header details to a user program for authentication
- in addition, supports temporary storage of pre-authenticated rules for passing packets through
- Extensive logging facilities : logging packets to a network devices is supported for both packets being passed through the filter and those being blocked
- Managed from a standard Web browser or from encrypted SSH tunnel

System security

SecCORE is the standard component base for all security appliances offered by Conostix. As most important functionalities can be considered the secure hardened operating system (SecOS), high-availability (HA Mod).

SecOS is a hardened operating system derived from Linux. SecOS is optimized for packet forwarding and handling of these packets. SecOS adds a lot of standard security features like :

- Local IDS to detect file change, configuration change and malicious activities
- MAC (Mandatory access control) at the operating system level by standard (control of each file, process, tcp port...)
- Stripped operating system with no additional libraries and binaries.

The High-Availability module (HA Mod) provides network redundancy and fail-over for all services running on the appliance. The module uses High-Availability IP routing services. The HA Mod is compliant to VRRPv2 (RFC2338). It provides dynamic fail-over of IP addresses from one appliance to another in the event of failure.



The appliance

Dimension :

- Compact 1U rack-optimized
- 1.70"H x 24"L x 16.75"W

Standard :

- Intel Quad core 2 processor
- 1024 DDR2 1
- 2 x 10/100/1000 BT network adapters
- 2 x 73 GB HDD SAS
- 24X DVD/RW
- Floppy drive
- SVGA, Serial RS232C port, PS/2 keyboard/mouse connectors

Optional :

- Up to 4 GB SDRAM 133 Mhz
- Up to 2 Quad Ethernet 10/100/1000 BT cards
- RAID controller

CONOSTIX S.A.

Luxembourg

Tel : ++352 26103061

Fax : ++352 26103062

E-mail : info@conostix.com

Web : www.conostix.com