

# Security Appliance

## SecRPX

The SecRPX reverse proxy is to be used outside the firewall or on a DMZ to represent a secure content server to outside clients, preventing direct, unmonitored access to your core server's data from outside your company. SecRPX can protect multiple different Web servers simultaneously, ideal for companies who want to protect unsecured Web servers. SecRPX can add SSL connectivity to ensure strong and performant encryption to the web traffic. SecRPX can add high-level authentication mechanisms on internal Web servers (SecureID, LDAP, ...) and can also do caching and load-balancing.

SecRPX is designed for maximum network uptime and security by integrating all reverse proxy functionalities over a Conostix standard component -SecCORE- which is composed of a secure Operating System, a local Firewall, 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

- High encryption level (128 bit SSLv3) between client browser and SecRPX or/and between SecRPX and internal Web servers
- Clients authentication methods : Basic authentication, X509 client certificates, LDAP, SecureID, TACACS+, Radius, Oracle 7&8, PostgreSQL, mSQL, Windows NT, NDS, **Luxtrust compliant**
- Authentication information can be bridged to internal Web servers via Cookies or HTTP headers
- Automatically compress HTTP (GZIP

algorithm) to browsers that can handle compression to optimize bandwidth usage

- Rules based URL filtering (HTTP method, URI, query string, body content)
- Rules based URL rewriting
- Can add, replace, merge or remove HTTP request and response headers
- Extensive logging facilities in W3C format (customize)
- 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) and packet filtering (SecFW).

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.

SecFW is a standard firewall solution running on SecOS. Firewalling is running on every security appliance and not only on a central point. SecFW is a stateful inspection firewall and provide customize extensive logging.



## 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**