

# SecurActive NSS-500

Network and Security Surveillance platform



## SecurActive NSS Solution

SecurActive NSS is a network and security surveillance platform based on an innovative analysis engine. It captures network traffic and analyzes it, making the understanding of network activity easier.

With a graphic interface that is both intuitive and simple to use, SecurActive NSS provides a panel display which shows the type of traffic that flows through the network, detecting network anomalies and risks such as attacks, incoherent traffic, illegitimate traffic, threshold limits, etc.

The SecurActive NSS product line brings together 4 different solutions for network owners and administrators so that they can respond to effective network monitoring requirements regardless of network size.

## NSS-500: Behaviour analysis of high-sized LAN networks

The SecurActive NSS-500 appliance is ideal for large company networks (up to 70 000 session flows\*), integrating all the network surveillance and security functions required to accommodate this type of structure.

## Modularity and transition

The technical configuration of the SecurActive NSS-500 appliance provides a wide margin of flexibility to monitor the growth of your company's network architecture. Thanks to its 7 Gigabyte Ethernet listening ports, SecurActive NSS-500 is the perfect solution for large company networks and for growing companies in any industry.

\* A TCP/UDP flow is a type of communication between two IP machines during time intervals of two minutes.

## SecurActive NSS-500 solution: major advantages

### • A SIMPLE AND COMPLETE SOLUTION

SecurActive NSS-500 was designed and produced to include the following features: network view, security view, web view, alerts and reports.

#### **Benefits:**

- No unforeseen or hidden costs
- Simplicity of integration and no-fuss operation
- Assured efficiency and streamlining of its different features

### • A FULLY INTUITIVE ADMINISTRATION SET-UP

SecurActive NSS-500 appliance was designed for any user to go up from general information (synthesis) to a more detailed perspective in a simple and intuitive manner. The numerous wizard tools that are available facilitate the immediate and full use of the NSS-500 solution.

#### **Benefits**

- Acquisition of simplified competencies
- No added requirement for other resources to support the solution's administration
- Self-training for team users
- Ease of use by all authorised operators
- Reduced time dedicated to network administration

### • PASSIVE POSITIONING ON THE NETWORK

SecurActive NSS-500 can be positioned on the network via a port mirroring using your own switch or can be built in via a TAP switch. The totality of your network traffic is duplicated and then transmitted to SecurActive NSS-500 to be analysed.

#### **Benefits**

- Transparency mode
- Non-intrusive integration
- No supplementary traffic generated
- No network disruption or disturbance during installation of SecurActive NSS-500.

### • NETWORK AND SECURITY PERSONALISED ALERTS

SecurActive NSS-500 can be configured to accommodate a company's unique network alerts and security measures based on its operations, its requirements, and its IT's code of ethics. The alerts are uploaded through SecurActive's interface and/or transmitted by e-mail to administrators.

#### **Benefits**

- Possibility of supervision mode while using SecurActive NSS-500
- Significant decrease in attack risks
- Immediate resolution of network incidents and security breaches as soon as they occur.

- **CONFIGURATION ADAPTED TO NETWORK REQUIREMENTS**

SecurActive NSS-500 can also be configured so that it is adapted to meet your network's unique requirements for both infrastructure (zones and sites) and service definition requirements (identification of services and priority applications).

**Benefits**

- Easy and quick grasp of your network's functions and operations
- More rapid and efficient analysis of your network's activity

SecurActive NSS-500 appliance integrates the following standard functionalities:

**Network Display**

- Changes in observed time intervals (2 min / 2 h / 2 d / last month)
- Global traffic distribution (by IP protocol volumes, service volumes)
- Exchanged traffic by zone (volumes exchanged by zone)
- Matrix of volumes exchanged by zone
- Distribution of IP protocols
- Volume of traffic exchanged by host
- Active sessions
- Uncategorised flows
- Direct access to an IP address
- Historical records of network alerts
- Bandwidth by protocols
- Bandwidth by applicable service category
- Bandwidth for traffic < than 5%
- Bandwidth for traffic > than 5%
- Monitoring filters on IP source, destination, hours
- Alerts by network threshold limits

**Security Display**

- Incidents by category
- Incidents by signature
- TOP of hostile hosts
- TOP of target hosts
- Historical records of security alerts
- Incidents by alert level

**Web Display**

Consultation by:

- web site
- family
- category
- zone
- source
- export in CSV file

### Response Time Management

- Measurement of both application and network latency periods
- Identification of network deteriorations

### Configuration

- Configuration of the context (zone and services)
- Configuration of upstream network alerts (triggering of threshold limits)
- Configuration of upstream security alerts
- 5 levels of alerts from 1 to 5 (critical to informative)
- Management of users (access to the administrator or user box, creation of group profiles)

### Reports

- Historisation of reports
- Generation of reports via assistant launch
- Generation of standard reports
- Generation of personalised reports
- Planning for the generation and transmission of reports
- Push via e-mail
- Generation of reports in HTML
- Reading of reports through Firefox or Internet Explorer

### Expertise

- Generation of frame capture files
- Automatic triggering of the capture/ parameter set-up through a wizard
- Capture of up to a maximum of 10,000 frames per capture
- Stocking of local file captures
- File recovery for reading in PCAP format

### Services

- Client Support DHCP
- DNS resolution support
- SMTP support
- Configuration of working hours
- NTP support
- Consideration of HTTP proxy
- Possibility of time freeze
- Automatic updates from URL classifications and security

### Logging/Monitoring

- Real time monitoring of the appliance's parameters
- Secured access via login/password
- Notification by e-mail

### Management

- Access to the administration of the NSS-500 solution in either WEB HTTP or HTTPS
- Two access levels: administrator or user
- Access to manage the solution via the administration port
- Console port access series interface
- Access to support via remote maintenance service in Stunnel mode
- Access log to the solution

### Specifications and performance

- 7 listening interface 10/100/1000 Mbits base T copper
- 2 extension slots SFP (Optical fibre) - option
- 1 administration port interface 10/100/1000 Mbits base T copper
- Connectivity of the administration port via a "port mirroring" or a TAP
- Approximately 100,000 session flows\*
- Network accommodates up to 5000 workstations
- Over 9,000 supported security signatures
- Support for OLFE0 categories in URL consultation

### Hardware specifications

- Quad Core Intel E5310, Speed up to 1,6 GHz (4MB Cache)
- RAM Type & Max. Capacity 2 x DDRII 533/667/800 DIMM, standard: 8 Go
- Ethernet interfaces 10/100 LAN (8 Giga Ethernet ports RJ45 Copper)
- HDD (Hard disk) 2.5" HDD 500 GB (supports SATA II, 1x3)
- Serial port (1 console port - RJ-45)
- LCD Module (2x16, PIO)
- Power: 350 W ATX Power Supply
- Double Power Supply
- Rackable: 2 U
- Dimensions: 427 x 458 x 44 mm
- Certifications: CE FCC Class A