

Nexor Sentinel

Nexor Sentinel is a high assurance mail guard, single-box appliance designed to protect an organisation by validating that inbound and outbound electronic messages conform to the security policy of the protected domain. Nexor Sentinel is supplied on two secure platform options, one evaluated to Common Criteria EAL4+, the other to EAL5+. The underlying secure platform ensures network separation of the connected domains, while the base mail guard application, originally designed and tested to EAL4, ensures only policy conformant messages can pass between these connected networks.

Nexor Sentinel products have been deployed worldwide by national defence forces and organisations such as NATO.



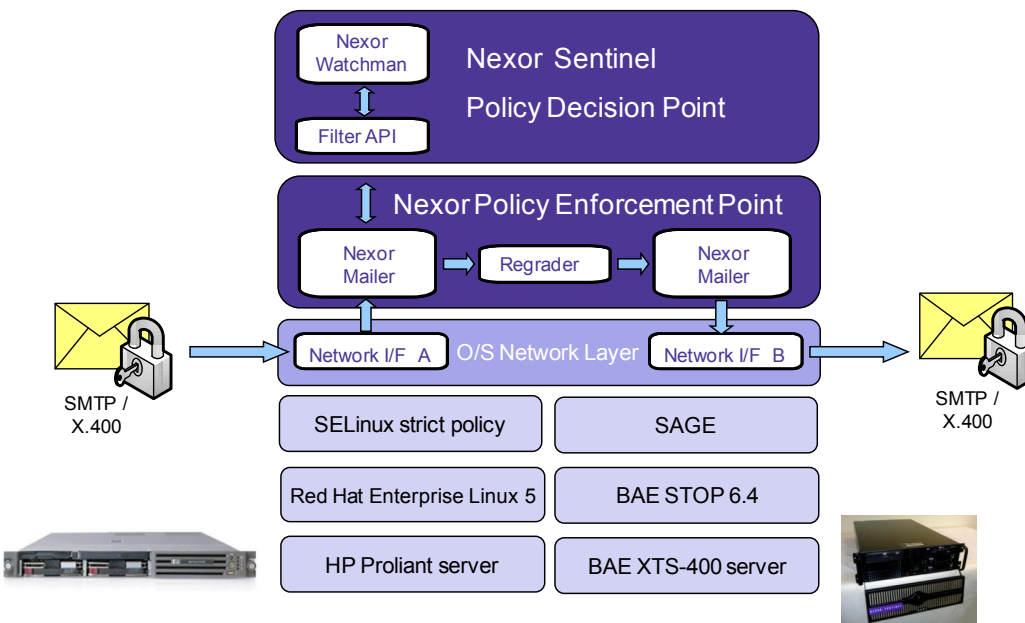
Sentinel 2



Sentinel 3

Security

Designed with security in mind, Nexor Sentinel appliances make use of the evaluated security functionality provided by the underlying platform to ensure an electronic message can only pass from one domain to the other via a trusted path. The trusted path includes ensuring all messages are scanned by the Nexor Watchman policy enforcement module which validates the messages conform to the defined security policy. Non conformant messages are rejected, preventing the potential damage caused by outbound data loss or inbound malicious content.



Nexor Sentinel - Architecture

To meet the interoperability and security needs of the world's most demanding organisations, Nexor separates content and protocol conversions from message security. Nexor Sentinel provides message security, while Nexor Border Gateway provides content and protocol conversion. This approach reduces solution assurance and accreditation costs.

Benefits

Nexor Sentinel connects and protects messaging domains by:

- preventing data loss via email
- protecting an organisation from downstream denial-of-service
- validating cryptographic security controls
- allowing control of who is able to send what to whom
- providing traceability of communication exchanges

Standards Compliance

- RFC 2821 SMTP
- RFC 2822 Internet Message Format
- RFC 2045/2046/2047 MIME
- RFC 3851 S/MIME v.3.1
- RFC 2634 Enhanced Security Services
- X.411 Message Transfer System
- X.420 Interpersonal Messaging System
- STANAG 4406 Ed. 2 (P772)
- SDN.801 Access Control Concept and Mechanisms
- X.841 Security Information Objects for Access Control
- WP7 (AC/322-D (2004) 0021) Electronic Labelling of NATO Information
- PKCS#12 Personal Information Exchange Syntax
- RFC 4250-4254 Secure Shell v2.0 (SSH)
- RFC 2571 SNMP v3
- RFC 2249 Mail Monitoring MIB
- W3C XML 1.0
- W3C XML Schema 1.0

Platform Options

- Nexor Sentinel 2 is supplied on BAE XTS-400 hardware, running STOP 6™ (EAL5+)
- Nexor Sentinel 3 is supplied on HP Proliant hardware running SELinux (EAL4+)

connect transform protect

NEXOR®

www.nexor.com

Features

- SMTP and X.400 message guarding
- Supports S/MIME v3 signed, encrypted and triple wrapped messages
- Supports Protecting Content Type (PCT) wrapped messages
- Policy enforcing filters for message transport
 - Message envelope checks
 - Access Control Lists
 - Return of Content in reports
- Policy enforcing filters for message content:
 - Allowed attachment types
 - Allowed body part types
 - Dirty word searching
 - Message precedence
 - XML schema validation for XML attachments
- Policy enforcing filters for message security:
 - Message signature
 - Message encryption
 - Signed Receipts
 - Security label
 - Originator and recipient clearance
- Multiple security label locations supported:
 - S/MIME ESS
 - X.400 P772 content
 - X.400 envelope
 - First Line of Text
 - Attachments
- Multiple security label formats supported:
 - SDN.801
 - X.841 / NATO WP7
 - Free format text

Policy Enforcement

Nexor Sentinel enforces organisational security policy by verifying:

- **Transport:** Message envelope checks including originator and recipient access control list checks (black and white list).
- **Content:** Checks to ensure there is no unauthorised or inappropriate information flowing into or out of the organisation. Message exchange may be permitted or denied based on checks on message precedence, "dirty word" searching, and analysis of message body parts. Policies can be enforced to ensure only specific types of messages, attachments and/or reports are allowed to pass through Nexor Sentinel. Validation of XML attachments can ensure that the data conforms to a known schema and is well formed. Virus scanning of the complete message is also supported using the Sophos Anti-Virus engine. Custom content checking is possible by integration of 3rd party message content filters including office file inspection using PuriFile.
- **Security Labels:** Access controls based on labels contained in messages to ensure the contained information is allowed to be released. Nexor Sentinel can handle labels in different formats and locations including plug-ins to handle complex text based labels in multiple languages as well as P1, P772 and ESS. Sentinel can also process labels in Microsoft Office documents.
- **Message Security:** Checks to ensure the confidentiality, integrity and non-repudiation of information, including the validation of message security labels, S/MIME signatures (both inner and outer signed data), S/MIME encryption and S/MIME signed receipts.

Journaling, Audit and Rejection

Nexor Sentinel's journaling function provides an archiving capability of messages traversing the mail guard. A secure audit trail is also kept of messages passing through the system. When a message fails to pass one or more message filters, a secure rejection message is sent to an administrator detailing the reasons for rejection.

Management and Monitoring

Nexor Sentinel can be managed either locally on the appliance or remotely using an intuitive user interface.



Sentinel 2



Sentinel 3

- A server provides for remote access allowing secure copying of files on and off of the appliance.
- An SNMP server provides real time information to remote monitoring tools on the state of the mail guard.
- Full remote access to the appliance can also be provided using a secure KVM switch.

Deployment Scenarios

Nexor Sentinel 2 provides network separation for up to 4 domains, Nexor Sentinel 3 provides network separation for up to 8 domains.

Nexor Sentinel is typically deployed behind a network firewall and will interoperate with many standards compliant messaging systems including Microsoft Exchange.

www.nexor.com

Information in this document is provided "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement.