

Nexor Watchman 7.0

Introduction

Nexor Watchman provides content checking and verification technology to prevent confidential information being transferred by unauthorised parties between specified domains. For example, this could be deployed between a company intranet and the Internet to prevent confidential information leaving the organisation.

This functionality augments a standard Nexor Mailer and can be used on both SMTP and X.400 messages.

Nexor Watchman enables three key checks to be performed:

- Validation of the message originator, based upon information contained within an LDAP Directory.
- Validation of the message recipients, based upon:
 - their classification clearance,
 - or
 - the policy set for the originator.
- Determination of the classification of the message, based upon a weighted hit-word count of the message content and the security label.

Each check can be performed independently to ensure that the message is processed correctly.

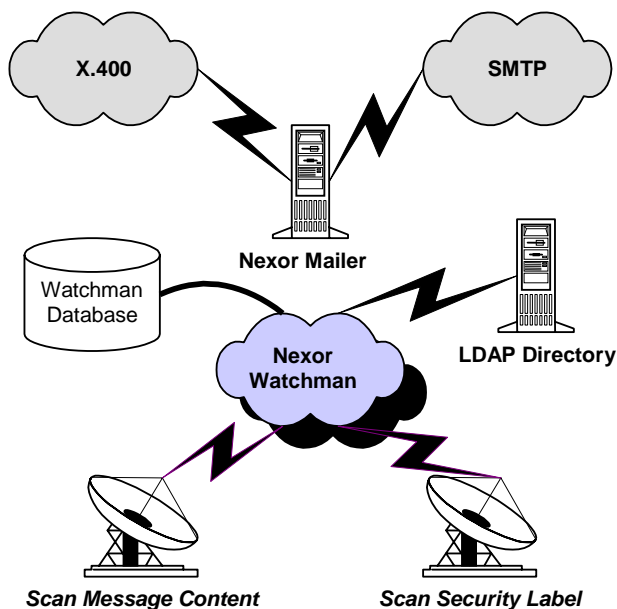


Figure 1: High level architecture

Configuration

Nexor Watchman enables the verification of the user's chosen group of messages to be configured using the standard functionality of the Nexor Mailer.

For example, the user can choose to check all messages, or just those destined for a specific domain.

Additional configuration modules are built into a separate database. If required, multiple configurations can be supported on the same Nexor Mailer. This modular approach adopts proven components of the Nexor Mailer, whilst providing customer flexibility, enabling the system to be tailored to the customer's specific requirements.

Platforms

- Windows 2003 / 2008 Server

Other platforms, including trusted operating systems, may be supported on request.

Project Features

Originator Validation

Nexor Watchman enables the customer to determine if the originator is internal or external. When the originator is internal a directory lookup is performed to find a "sites" attribute, which states the domains that the originator is cleared to send to.

An internal originator will be deemed to be invalid if there is not a corresponding entry for that person within the LDAP directory. This will result in the non-delivery of the message and notification being sent to a pre-determined administrator.

Recipient Classification Clearance

Nexor Watchman enables the customer to determine if the recipients are internal or external.

Internal recipients will be queried in the LDAP Directory to determine what classification of message they can receive.

External recipients will be cleared to a pre-configured classification stored in the database.

Message Classification

The classification of a message is calculated based upon the number and weight of the hit words it contains.

The exploding of the message content involves:

- removing any RFC-822 MIME or X.400 FTBP / bilateral encoding;
- extracting any files from zip files;
- decoding TNEF attachments;
- extracting text "strings" from binary files, for example Microsoft Word.

The text files will then be scanned using Nexor Mailer verify-word program.

Recipient Validation

A check is then performed using the classification calculated for the message, to determine if that recipient has the appropriate classification clearance.

If the recipient is not cleared for that message then the message will not be delivered to that recipient.