

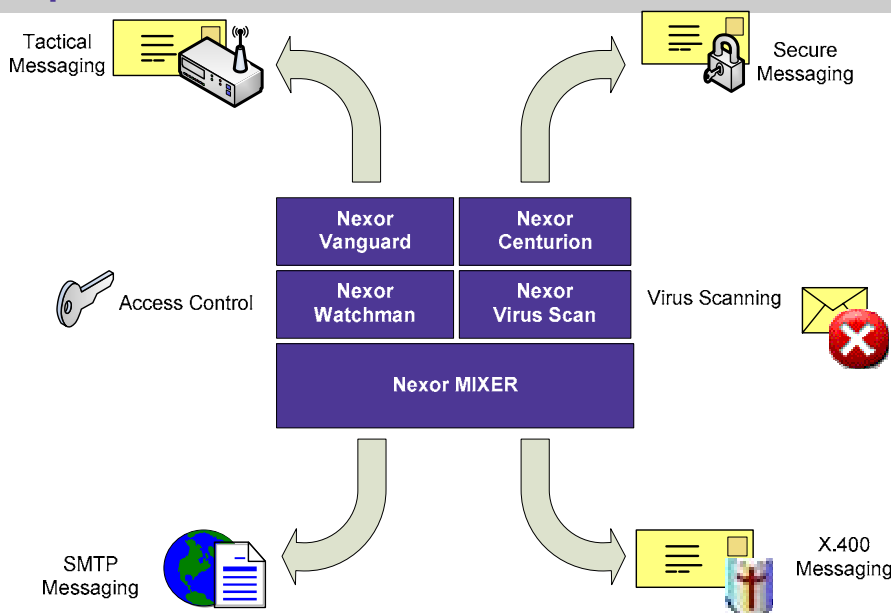
# Nexor Border Gateway

Today's climate of coalition based operations and network enabled capability means that there is a growing requirement for exchange of information between different messaging environments. Standards are emerging for secure, trusted information exchange that can be applied both within and between messaging domains to facilitate secure communications between disparate systems.

To address these existing and emerging needs, Nexor has developed the Nexor Border Gateway. Based on a brand new design, Nexor Border Gateway offers a range of components that can be selectively configured to provide a wide variety of technical solutions to meet information exchange needs, including a fully compliant ACP 145 gateway-to-gateway product. The architecture that underpins the Nexor Border Gateway components allows for complete flexibility by being platform, message transfer agent and enterprise directory agnostic. In addition to this, Nexor Border Gateway supports a range of security protocols, content types and transport protocols.

To aid cost reduction, Nexor Border Gateway is designed to work on only one server, although it can be implemented across a range of servers if desired. The deployment of the chosen gateway configuration is delivered by an intuitive installation and managed through the Nexor Management Console.

## Components



Nexor Border Gateway comprises a suite of new and existing Nexor components designed to act as a gateway between different messaging systems. Components include:

- Nexor MIXER
- Nexor Centurion
- Nexor Vanguard
- Nexor Watchman
- Nexor Virus Scan Interface

An intelligent installation allows users to select the elements that are required for their specific implementation. In combination with Nexor Border Guard products, the suite can provide total protection and control of the interfaces to external messaging systems.

## Benefits

### Interoperability

- Compliant to current and emerging standards for international interoperability including ACP145 and STANAG 4406 Annex E TMI-1.

### Reliability and Resilience

- Uses channel based architecture and makes use of O/S file system resilience to providing a proven resilient system.
- Provides a reliable multicast protocol in a connectionless oriented network.
- Demonstrates enhanced reliability in environments with up to 75% packet loss.

### Scalability and Performance

- Architecture takes advantage of multiple processors, disks, increased RAM and additional servers to scale up deployments.
- Proven high performance message switch that can be tuned for parallel message processing, message prioritisation and use of network QoS.
- Provides data compression, address mapping, and congestion control to ensure bandwidth optimisation and improved message flow.

### Security

- Provides control over the flow of information between domains by performing content verification, access controls, and policy driven security label translation.

### Low Total Cost of Operation

- Deployable on one server.
- Allows continued use of existing infrastructure by supporting ultra low bandwidths and security enablement.
- Supports multiple domain policies in one gateway.

### Reduced Risk

- Allows application of centralised security policy.
- Extends existing, proven Nexor technology.

### Platforms

Nexor Border Gateway is available on Windows 2003 / 2008 Server. Other platforms, including trusted operating systems, may be supported on request.

connect transform protect

**NEXOR**<sup>®</sup>

## Standards Compliance

### Messaging

- X.411 MTS
- X.420 IPMS
- STANAG 4406 Ed. 2
- ACP123
- STANAG 4406 Ed. 2 Annex E
- RFC 1006 ISO transport on TCP
- RFC 1521/1522 MIME
- RFC 1801 X.500 directory routing
- RFC 1869 SMTP service extensions
- RFC 1870 Message size negotiation
- RFC 1891 SMTP service extensions for DSNs
- RFC 2156 MIXER
- RFC 2197 SMTP service extension for command pipelining
- RFC 2231 Use of non-English character sets in header
- RFC 2249 Mail monitoring MIB
- RFC 2554 SMTP service extension for authentication
- RFC 2821 SMTP
- RFC 2822 Internet Message Format

### Security

- RFC 2630 CMS
- RFC 2634 ESS
- RFC 3851 - S/MIME v3.1
- RFC 3854 X400WRAP
- RFC 3855 TRANSPORT
- X.841 Security Information Objects for Access Control
- SDN.801 Access Control Concept and Mechanisms
- PKCS#12 Personal Information Exchange Syntax
- PKCS#11 Cryptographic Token Interface Standard
- CAPI Microsoft Cryptographic API

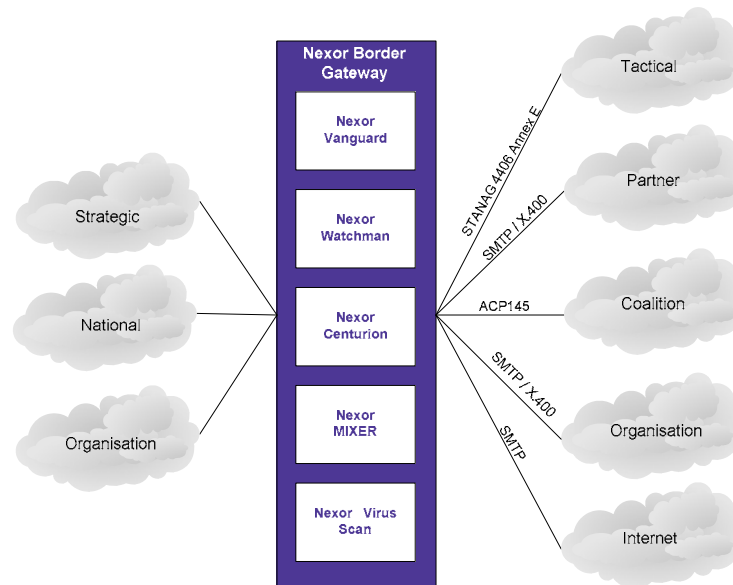
### Tactical

- RFC 2442 BATCH SMTP
- RFC 1950 ZLIB Compression
- RFC 1951 DEFLATE

### Directory

- RFC 2251 LDAP

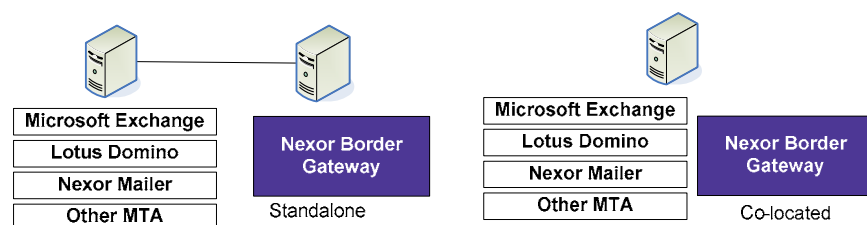
## Deployment Scenarios



The Nexor Border Gateway is designed to be deployed at the border of organisations that are required to interface to external systems. Nexor Border Gateway can be used to provide multiple different interfaces depending on the need of the organisation. It allows for any combination components to be licensed and used together to provide a fully flexible gateway.

Typical deployments include:

- **ACP145 Gateway** to provide an interface between national military message handling systems with full support for the CCEB ACP145 gateway to gateway specification
- **Tactical Messaging Gateway** to manage communications in low or unreliable bandwidths found in the tactical environment with full support for the X.400 based STANAG 4406 Annex E TMI-1 protocol and, additionally, SMTP
- **Security Policy Gateway** to prevent confidential information from passing between two connected organisations. Supporting both SMTP and X.400 and checking message security labels, message content, and addressees
- **Content Verification Gateway** to protect a domain from the threat of viruses and spam entering from external networks
- **MIXER Gateway** to transfer messages between SMTP and X.400 messaging systems.



The architecture of Nexor Border Gateway means that it is independent of the message transfer agent and can be installed either on a standalone server or co-located with a 3rd party product such as Microsoft Exchange Server.

## Product Integration

Nexor Border Gateway makes it simple to extend the information exchange functionality by allowing integration of 3rd party applications either through development using the Nexor Software Development Kits or via Nexor consultancy services.

[www.nexor.com](http://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.

© Nexor 2009

All rights reserved  
NEX1934MAR03