Paper

NATO automated information system co-operative zone technologies

Martin Diepstraten and Rick Parker

Abstract — The core components of NATO's automated information systems (AIS) include directory services (DS), e-mail, web services, and military message handling systems (MMHS) to exchange information with similar capabilities in NATO's member nation systems or systems that are under control of multi-national coalitions. NATO has developed the concept of information exchange gateways (IEGs) to meet this requirement. This paper introduces the concept of combining symmetric co-operative zones (CZs) to form these information exchange gateways. A generic framework for the co-operative zone network and security architecture is introduced in support of co-operative zone development. It is shown how a co-operative zone network interface can be integrated with the NATO general-purpose segment communications system (NGCS). Development of the NATO co-operative zones is based on an evolutionary approach. A baseline co-operative zone configuration, supporting directory services, e-mail and web services, has been tested and validated on the allied systems interoperability testbed (ASIT). This paper reports the results of the test and validation program. The paper concludes with an overview of planned evolutionary steps for co-operative zone development. Subjects covered in this overview are extension of information services, enhancement of security architecture, and operational deployment (i.e., scalability and manageability).

Keywords — information exchange, firewall technologies, directory services, messaging services, web services, INFOSEC.

1. Introduction

NATO's changing operational environment has caused a dramatic change in the way commanders use their supporting command control and information systems (CCIS) to exchange information. As CCIS's evolve from single-purpose systems in single-level secure environments to multi-purpose systems in multiple-level secure environments, it becomes impossible to build custom interfaces for each possible permutation of information exchange and still remain flexible and responsive to change.

Within NATO's automated information system, the concept of an information exchange gateway through symmetric co-operative zones been introduced with the aim to manage and control all information exchange through a single secure entity with well-defined interfaces.

This paper will focus on the initial architecture of the IEG concept that has been tested and validated in the NC3A allied systems interoperability testbed and the evolution of the concept into operational and more advanced variations.

2. Information exchange gateway operational view

From the operational point of view an IEG can be characterised by two features:

1) the information services that are passed through the gateway;

2) the business case identifying the difference in security level that is bridged by the IEG.

Information services can be end-user related services, such as mail and web, but also be infrastructure or management services, such as domain name service (DNS) and simple network management protocol (SNMP).

Within the scope of the IEG program of work [1] three configuration cases have been identified so far:

- **Case A**. NATO-SECRET to NATO-SECRET enclaves that reside in environments under control of NATO or NATO member nations. There are no interconnections to national CCIS networks. The Case A gateway is sometimes classified as a NATO point of presence (POP). From the POP boundary, the nation has the responsibility to deliver the information service to the user.

- **Case B**. NATO-SECRET to NATO National Secret-HIGH systems that reside in environments under control of NATO member nations.

- **Case C**. NATO-SECRET to coalition secret systems that fall under the responsibility of a Combined Joint Task Force in which NATO is in the lead.

3. Information exchange gateway architecture

The basic conceptual framework of the information exchange gateway through symmetric co-operative zones is illustrated in Fig. 1.

Information exchange between a sender and receiver, both residing in separate local CCIS networks, will always take place via the sender's own CZ and through a symmetric CZ under control of the receiver. No direct traffic is allowed between two local CCIS networks other than that relayed through the source and destination CZs.

The example in Fig. 1 shows this information flow from a nation-X CCIS supporting service A to its counterpart in

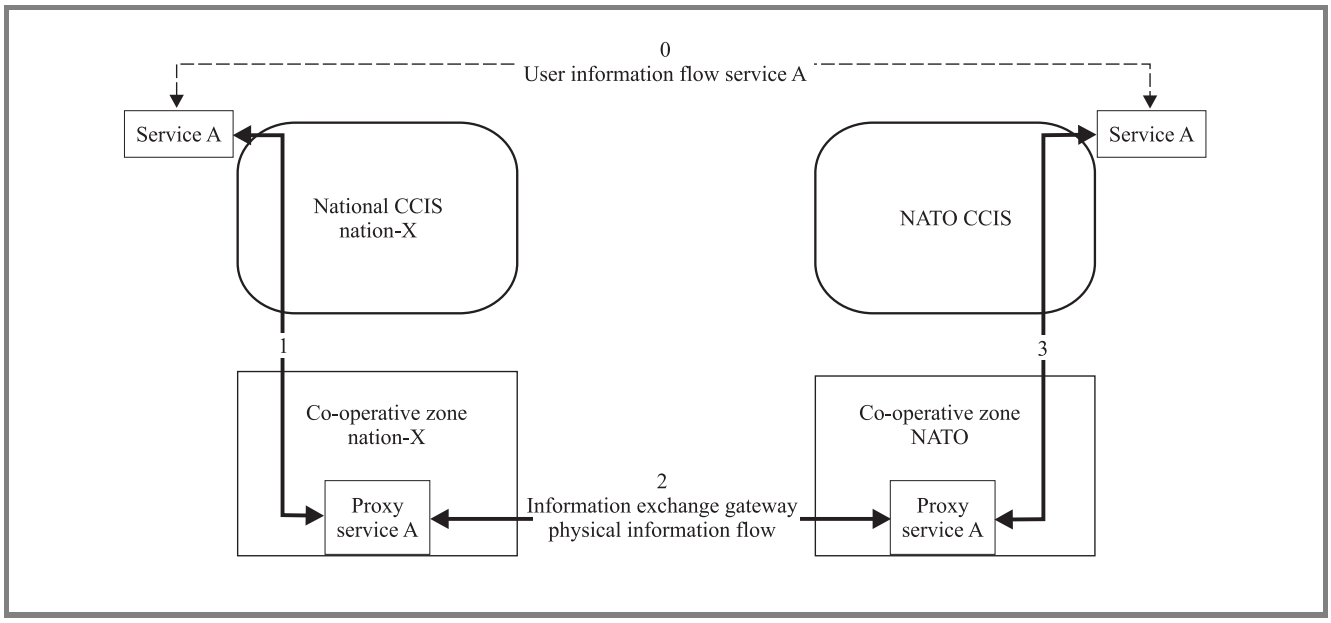

Fig. 1. Information exchange gateway through co-operative zones.

the NATO local CCIS (dashed information flow labelled 0). This information flow that consists of 3 logical connections (labelled 1 up to 3 in Fig. 1):

1) nation-X CCIS service A to nation-X CZ proxy service A;

2) nation-X CZ proxy service A to NATO CZ proxy service A;

3) NATO CZ proxy service A to NATO CCIS service A.

The information services that will be shared through a CZ are to be established on a trustworthy network and security architecture. One of the basic principles of trustworthy computing is to work with well-defined restricted interfaces. Another important principle is to avoid unnecessary complexity (keep it simple). Therefore, the architecture that has been adopted for the information exchange gateway employs **symmetric** co-operative zone modules (CZMs) at both ends of the IEG. This symmetry requirement holds the number of CZM interfaces to a minimum.

In addition to symmetry the following design principles are applied for the further development of the CZMs:

- Minimise the number of protocols that run across the IEG.
- Minimise the volume of network traffic overhead that is generated by a certain service.
- Standardise on common protocols.
- Avoid services or features that carry great risk with respect to security vulnerabilities.

The following categories of IEG architecture will be explained in more detail:

1) security architecture;

2) network architecture;

3) backbone and management services architecture.

3.1. Security architecture

The CZ security architecture most closely resembles a "screened subnet firewall configuration" based on a bastion host that provides authentication and proxy services [2]. Figure 2 illustrates the security elements comprised by a CZM. These are:

- A boundary protection device (firewall) that provides the source environment (i.e., local CCIS) with the protection required under NATO's "self-protecting node" guidance [3].
- A second boundary protection device (filtering router) that manages and secures network paths, protocols and ports to other co-operative zones between service peers at the fixed IP-to-IP-number level.
- An intrusion detection system (IDS) to detect attempted exploitation of (emerging) security flaws that occur in the CZM component systems.

The bastion host capability (providing both authentication and proxy services) has been implemented in the following fashion:

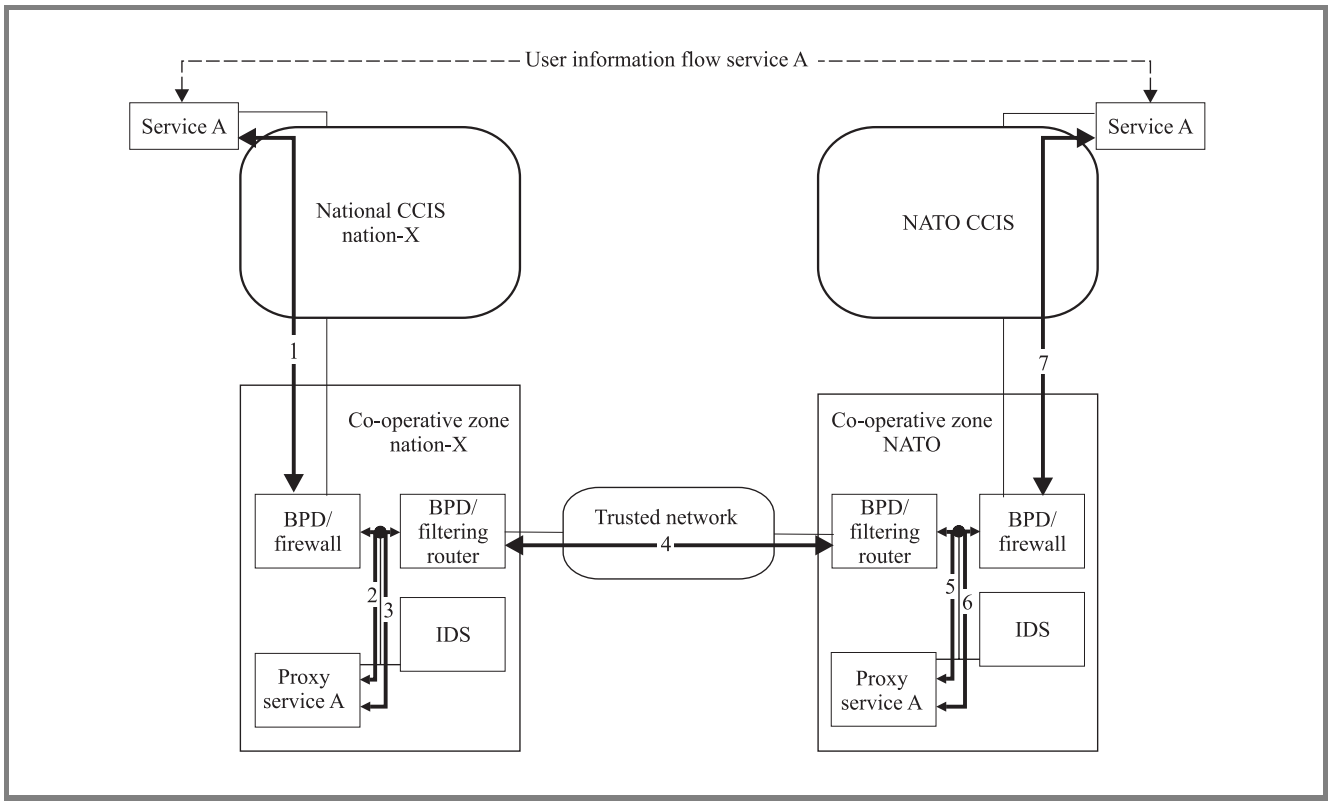

Fig. 2. Co-operative zone INFOSEC components.

- CZ proxy servers to relay traffic from/to the source/target servers in the local CCIS domain (through the BPD/firewall).
- Proxy authentication by the BPD or as part of the local CCIS system.

The chosen approach provides a high level of security, because there are three levels of defence to thwart intruders:

- The filtering router only advertises (limited) IP-numbers of the CZ subnet – the local CCIS network is invisible from the outside.
- The firewall only advertises and supports connection from local CCIS concentrator servers and counterpart proxy servers in the CZ.
- Potential emerging vulnerabilities are pro-actively detected by the IDS.

The user information flow (Fig. 2) is redirected through these three levels by seven consecutive connection steps.

3.2. Network architecture

For Cases A and B, where CZs of NATO or NATO member nation controlled entities are involved, the NATO policies for interconnection [4] prescribe the application of network encryption facilities to establish a trusted interconnected CZ WAN.

NATO will establish a "backbone" infrastructure of NATO CZs to which other, NATO national CZs, can connect. This backbone infrastructure will be based on the draft NATO general purpose communication segment architecture [5]. NATO national sites get connected to the NATO network through the nearest NGCS access router. The CZs will share one common (private) IP-space.

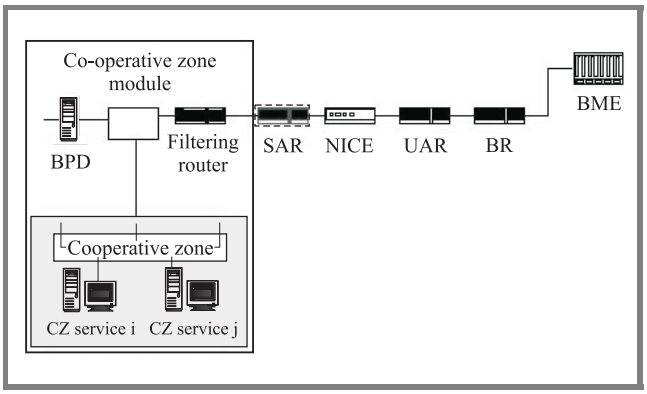

Fig. 3. Co-operative zone module NGCS interface.

Co-operative zones get integrated into the NGSC network through IP-encryption, using the NATO IP-crypto equipment (NICE) [6] and hooking into the nearest NGCS access router. Figure 3 shows which network and security devices a CZ uses to connect to the physical bearer network.

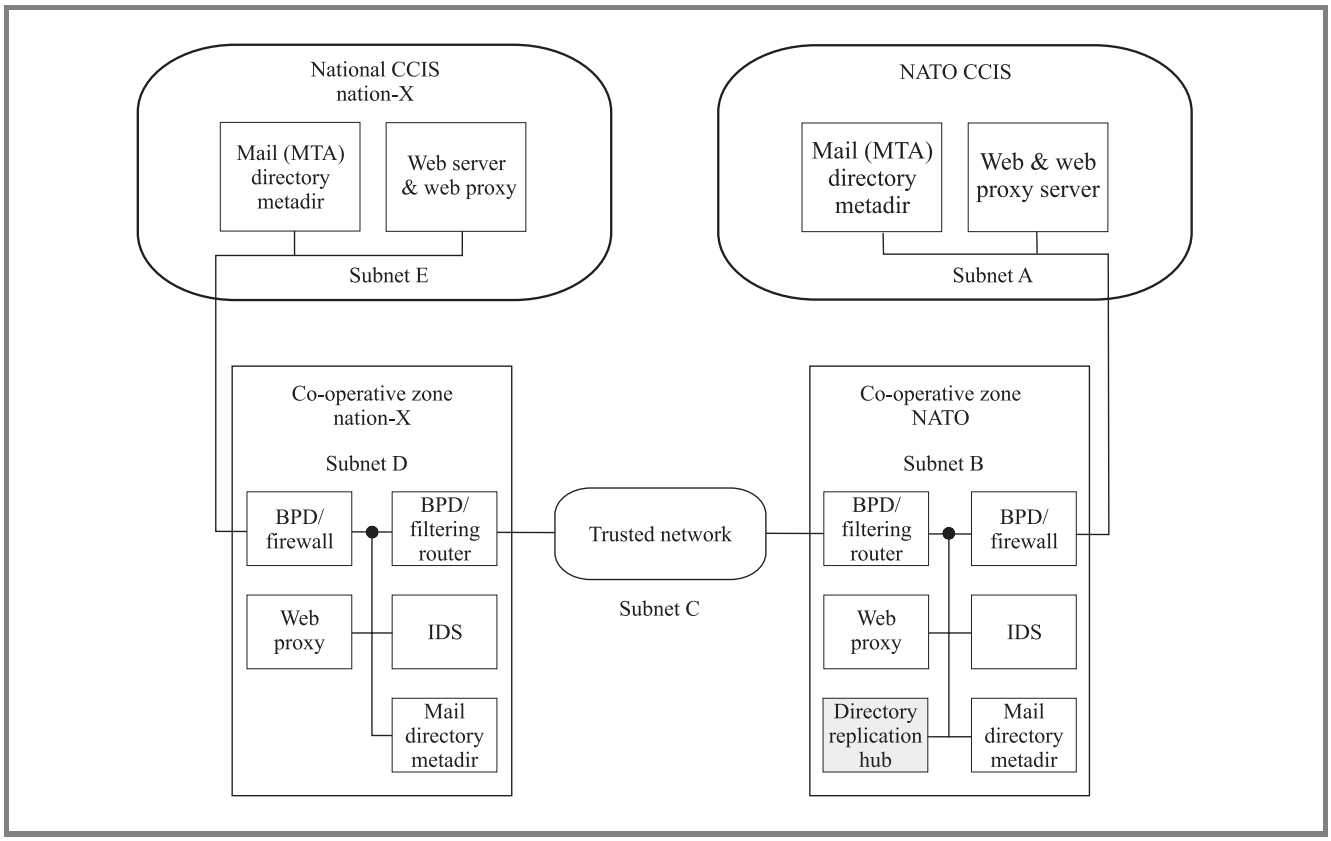

Fig. 4. Information exchange gateway ASIT system diagram.

The configuration comprises the following devices:

- secure access (Fig. 3 – dashed line) router, used for tunnelling through the IP-network;
- the NATO IP-crypto device (NICE);
- an unclassified access router (UAR);
- backbone router (BR);
- bandwidth management equipment (BME).

3.3. Backbone and management services architecture

In addition to the core IEG user services, backbone and management services are needed to maintain the potentially large network of CZM nodes. Examples of backbone services are:

- time services (based on NTP);
- distributed replication services for some of the involved user services and supporting services (e.g. directory services, DNS, etc.);
- redundant network and server backbone infrastructure.

Examples of management services are:

- naming and addressing (performed by the NATO naming and addressing authority);
- network, systems, and services monitoring (e.g. through SNMP);
- software and hardware configuration management and distribution.

4. Baseline configuration

An IEG baseline configuration has been established in the ASIT, to test and validate the concept of an IEG through symmetric CZs. The baseline configuration simulates a Case A IEG providing the following information services:

- e-mail based on X-400;
- web supporting HTTP and HTTPS;
- directory services based on LDAP version 3.

The directory service basically supports the e-mail address book capability, and directory replication is supported.
A system diagram depicting the server, network and security components of the ASIT configuration is shown in Fig. 4. The following IEG network domains were

implemented based on the IP-subnet distribution as shown in Table 1.

Tables 2–4 specify the ASIT components in further detail[1].

The remainder of this chapter describes the detailed configurations and lessons learned of the mail, web, directory, and security services.

Table 1
ASIT IP-subnets

Subnet	Specification
A	NATO CCIS LAN
B	NATO CZ
C	Routing domain in between the back-to-back filtering routers
D	Nation-X CZ
E	Nation-X CCIS LAN

Table 2
NATO/nation-X CCIS components

NATO and nation-X CCIS components	Product specification
Web server	Microsoft IIS 5.0
Web proxy server	MS ISA 2000 server
Mail server (MTA)	Microsoft Exchange 5.5
Directory server	MS Exchange 5.5 GAL
Meta-directory	Microsoft MMS 2.2

Table 3
Nation-X CZ components

Nation-X CZ	Specification
Filtering router	CISCO 2500
IDS	RealSecure
Firewall	Checkpoint Firewall-1
Web proxy	MS ISA 2000 server
Mail server (MTA)	Microsoft Exchange 5.5
Directory server	MS Exchange 5.5 GAL
Meta-directory	Microsoft MMS 2.2

Table 4
NATO CZ components

NATO CZ	Specification
Filtering router	CISCO 2500
IDS	RealSecure
Firewall	Checkpoint Firewall-1
Web proxy	MS ISA 2000 server
Mail server	Microsoft Exchange 5.5
Directory server	DCL (X500)
Directory replication hub	DCL (X500)

[1]The Microsoft Windows 2000 Advanced Server SP2 OS was used unless it is specified otherwise.

4.1. E-mail

The e-mail service is based on X-400. Each CZM contains an X-400 mail transfer agent (MTA), based on the MS Exchange 5.5 product [7], with two X-400 connectors connecting to the local CCIS MTA and a peer co-operative zone MTA. Figure 5 shows the mail flow and Exchange 5.5 site addressing as have been used in the testbed.

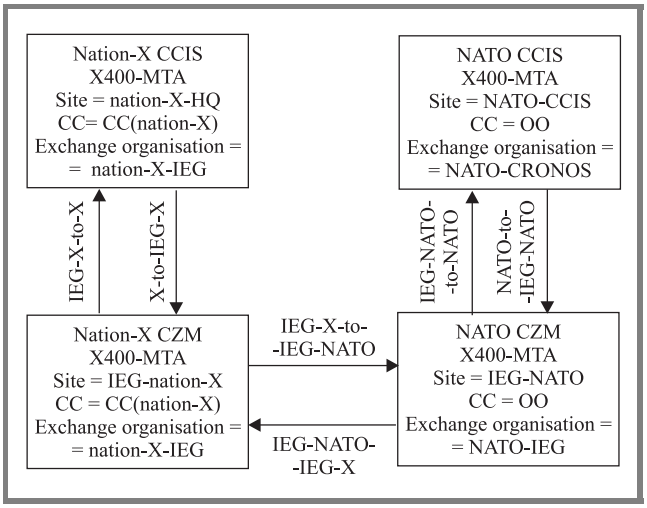

Fig. 5. Testbed e-mail configuration.

Table 5 gives an example specification of the X-400 connector labelled as "NATO-TO-IEG-NATO".

Table 5
Example X-400 connector specification

Feature	Specification
Routing	X400: C=OO;a= ;p=NATO-IEG;o= IEG-NATO;X400: C=CC(nation-X); a=;p=nation-X-CCIS;o=*
MTA conformance	1988 normal mode
X400 link options	BP-15 (in addition to BP-14) Two way alternate Allow exchange format
X400 body part	IA5
	Use the GDI from site addressing

Configuration of the e-mail infrastructure was straightforward. One issue that had to be resolved was related to passing X-400 through the firewall that is configured with NAT. X-400 connectors at both ends need to be configured as if they are communicating on a fixed IP-path. Therefore, an additional firewall rule had to be added enforcing advertisement of a fixed IP-number for incoming X-400 traffic.

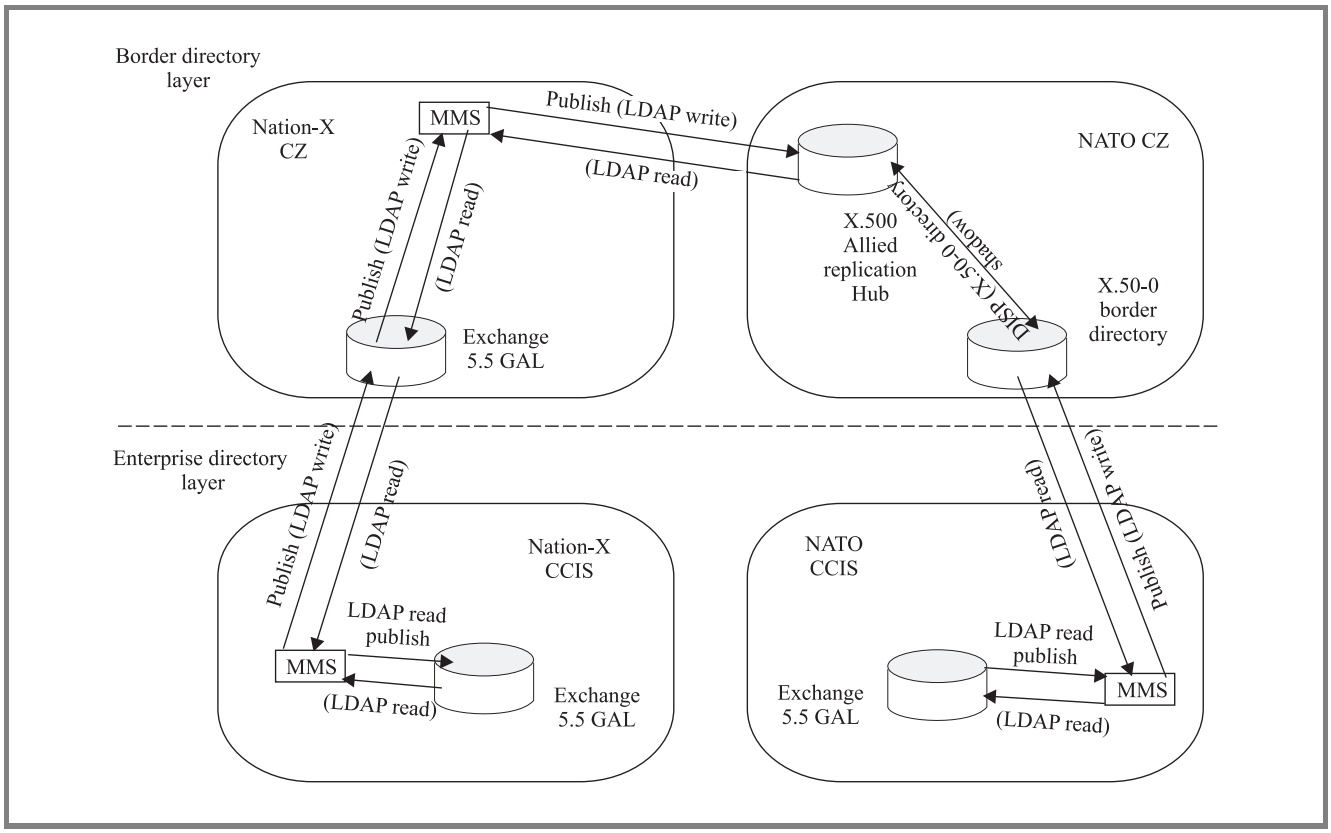

Fig. 6. Directory replication.

4.2. Directory services

The testbed's directory services closely follow the NATO directory services interoperability model [8]. This model is based on three layers of directory services:

1) custom system and application directories (lowest layer);

2) enterprise directory, supporting all enterprise common directory information (middle layer);

3) border directories, created for sharing certain directory information with other organisations (top layer).

NATO and the nations have agreed to use a schema based on ACP 133 [9] in the alliance domain. Also, the current guidance is to use X.500 replication (DISP) to ensure that all the DS data published into the alliance domain is available on every participating border directory service agent (DSA). As every nation is responsible for its own border DSA, it is very likely that they will be based on many different products, and multi-vendor X.500 DISP interoperability is not guaranteed. Some nations may therefore need to employ other replication techniques, e.g. based on meta-directory technology, to ensure that their border DSA is as well populated as those that are able to participate in the automatic X.500 replication.
The filtering and synchronisation processes that control the flow between the application and enterprise layers, and between the enterprise and border layers in the DS architecture, are commonly implemented using meta-directory technology (based on LDAP version 3).
The following mapping of DS interoperability model entities has been implemented in the testbed:

- The NATO (enterprise) and NATO nation enterprise directory are represented as the Exchange 5.5 global address list (GAL), which is an LDAP version 3 readable/writable directory.

- The NATO border directory is based on X-500 (DCL product) [10] and uses the agreed ACP133 schema.

- The nation-X border directory is based on an Exchange 5.5 GAL as a low-cost, easy to implement LDAP readable/writable directory.

- An allied replication hub directory has been implemented to facilitate directory synchronisation of border directories using the directory information shadowing protocol (DISP). This directory provides subtrees for NATO and NATO nations in which only the owner of the information has write access and all others have read access.

- Meta-directory technology has been implemented to facilitate directory synchronisation.

The test exercise that was executed on the testbed was to synchronise e-mail recipients information in support of an "allied recipients" subcontainer of the exchange e-mail address list. Figure 6 shows the directory synchronisation flow.
Information publication was achieved through:

- Publishing releasable mail recipient information from the enterprise directory layer to the border directory layer.
- Shadowing the published border directory mail recipient information (subtree) to the counterpart subtree in the hub directory.

Information download was achieved through:

- Shadowing the mail recipient information in the non-owned subtrees of the NATO replication hub directory the border directory into the equivalent subtrees in the border directory.
- Synchronising the mail recipient information in the non-owned subtrees in the border directory with the "allied recipients" container of the Exchange 5.5 (enterprise) directory.

The two protocols used for directory synchronisation were:

- DISP to synchronise the NATO replication hub X-500 directory information with the NATO border X-500 directory.
- LDAP version 3 to synchronise local CCIS directories with the border directories and to synchronise the nation-X border directory with the NATO hub X-500 directory. For configuration management and control of LDAP based directory synchronisation the Microsoft meta-directory services tool was used [11] by applying the Exchange 5.5 and generic LDAP management agents.

An important lesson learned from the directory synchronisation work is that the directory attribute-flow in between diverse systems (MMS processing rules, X-500 and exchange GAL directory schema) requires a rigorous mapping scheme of attributes and attribute translation rules.

4.3. Web services

Since Case A users require seamless web services, there must be a collaborating chain of local CCIS and CZ web proxy services for HTTP(S) traffic. The web proxy servers are responsible for routing of HTTP-traffic from/to browser to/from the target web server, through the CZ web proxy servers. No direct web server to browser traffic is allowed.
The web proxy server chain (Fig. 7) handles HTTP-requests for a "foreign" web page in the following way:

- An HTTP-request for a NATO CCIS web page hosted by a NATO CCIS web server is made by a nation-X user. It is redirected through the nation-X proxy server to the nation-X CZ proxy server and forwarded to the NATO CZ proxy server.
- The NATO CZ proxy server routes the request to the downstream NATO CCIS proxy server that will then finally connect to the target web server.
- The NATO CCIS target web server response is returned through the NATO web proxy server and the NATO CZ web proxy server to the nation-X CZ web proxy.
- The nation-X CZ proxy routes the response back to nation-X CCIS web proxy. This proxy will then finally route the response to the requesting web browser.

In the testbed experiment the Microsoft Internet acceleration server (ISA) [12] was used to implement the required web proxy server capability.

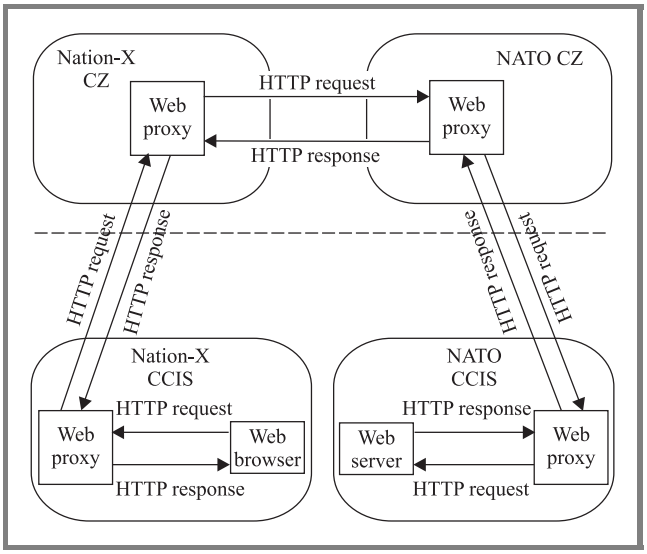

Fig. 7. Allied systems interoperability testbed web proxy chain.

Since the implementation is fully symmetric we will only give the configuration settings of the NATO local CCIS proxy server and the NATO CZ proxy server in Tables 6 and 7, respectively.
The configuration of the web proxy services (routes) was straightforward in the test configuration. It is expected that the live installation will need to be tuned (using caching, etc.) to establish acceptable response times to the end-user. It need to be noted that web browsing based on IP-addresses in "external" domains is not supported through this method.

Table 6
NATO local CCIS proxy settings

Attribute	Setting
Client sets	• NATO clients: subnet A • NATO CZ clients: IP-address NATO CZ web proxy server
Destination sets	• NATO sites: *.nato.int • Nation-X sites: *.nation-x
Protocol rules	• Access allowed to HTTP(S) for NATO clients and NATO CZ clients • Access denied for FTP/Gopher for both NATO and NATO CZ clients
Site and content rules	• Access to nation-X sites allowed to NATO clients • Access to NATO sites allowed to NATO CZ clients • Access to NATO sites allowed to NATO clients
Routing for web browser applications	• Requests to NATO sites retrieved directly from specified destination • Requests to nation-X sites are routed to a specified upstream server: IP-address NATO CZ web proxy server port: 8080

Table 7
NATO CZ proxy server settings

Attribute	Setting
Client sets	• NATO clients: NAT IP-address advertised by NATO CZ firewall (B.x) • Nation-X CZ clients: IP-address nation-X CZ web proxy server
Destination sets	• NATO sites: *.nato.int • Nation-X sites: *.nation-x
Protocol rules	• Access allowed to HTTP(S) for NATO clients and nation-X CZ clients • Access denied for FTP/Gopher for both NATO clients and nation-X CZ clients
Site and content rules	• Access to nation-X sites allowed to NATO clients • Access to NATO sites allowed to nation-X CZ clients
Routing for web browser applications	• Requests to NATO sites are routed to a specified upstream server: NATO IP-address advertised by NATO CZ firewall (B.x) • Requests to nation-X sites are routed to a specified upstream server: IP-address nation-X CZ web proxy server

4.4. Security and network services

In order to achieve the required level of security for Case A the following features have been implemented on the testbed:

- A firewall, based on an EAL-4 assurance level [13] product, checkpoint firewall-1 [14], installed on a C2 configured Windows NT-4 (service pack 3) platform [15]. In the testbed NAT has been implemented to hide the local CCIS system address space. As a measure of verification both NATO and nation-X IP subnets were assigned the same IP address range with identical IP addresses for the mail, directory, and web servers on either side of the firewall. The firewall rules support X-400, LDAP, HTTP, HTTPS.
- The filtering router has been setup to only allow connections between peer servers in the NATO and nation-X co-operative zone (e.g. MTA to MTA, proxy server to proxy server, directory server to hub directory).
- The intrusion detection system based on the realsecure product [16] has been connected to the CZ LAN as a stealth (receive-only) probe and console. The IDS monitors the traffic across the CZ in both directions, detecting incidents of known exploit attempts against the CZ proxy servers or the security components.

One important note to be made is that DNS is not required as a supporting service to resolve names to IP-numbers, because all routing is done based on fixed configured "routes" on an IP-to-IP basis through proxy routes, X-400 connectors, and DISP/LDAP connections.

5. Co-operative zone technologies evolution

The Information exchange gateway configuration that was tested and verified in the ASIT is considered to be a base line configuration. This baseline configuration will evolve in the following technology areas:

- Addition of AIS functional services.
- Adding security services by hardening security and developing Case B and Case C gateways.
- Development of backbone services.

The addition of functional services is a requirement that is very much dependent on further developments in the following areas:

- Migration of present custom interfaces from NATO to NATO nations and coalitions.
- Deployment of new allied systems.

- Operational requirements that lead to a requirement for additional functional services. For example, a new NATO system that will be deployed in the next couple of years is the NATO messaging services (NMS) system. The NMS will introduce the requirement for additional services to pass through the CZ to support a military message handling system (MMHS) [17] and, potentially, a NATO public key infrastructure (NPKI) [18].

Other services that are identified to be developed as a part of the Bi-SC AIS core capabilities [1] might also be candidates to get deployed as gateway services. Examples are:

– conferencing services (based on H323);

– real-time data streams (RMP, RAP);

– distributed database (SQL);

– middleware and XML web services communications features.

The two driving forces behind the further development of security services are:

1) optimisation of security features of the Case A baseline configuration;

2) additional security features required for Case B and Case C.

Optimisation of Case A security services includes:

- Further development of intrusion detection patterns and matching intrusion detection information at a central level.

- Configuring the server installation templates up to the C2 level [13].

- Shielding of the CZ IP-space to the local CIS network IP-space. For this it is considered to implement either NAT from CZ to local CIS or to run an IP-proxy service in front of the BPD.

- Prescribe usage of security tools such as security templates, virus checkers, vulnerability scanners for configuration and operation of information services.

- Develop a concept for centralised monitoring of intrusion detection consoles.

For Case B it is envisioned that the security services will not differ from Case A with the exception of the implementation of web publishing rules. The reverse proxy service will be restricted based on access controls. A request will be authenticated to the BPD/firewall that provides access to the local CCIS web services by impersonating a guest account in the local CCIS domain, based on the authenticated service, group, or individual user account level. The establishment of authentication services may be supported through the implementation of a NATO public key infrastructure [18] and the establishment of an allied PKI interoperability profile. Initially, though, it is anticipated that identification and authentication of authorized users will be left as a locally-selected and operated function, with support from the NATO/national AIS staff as required.

For Case C, the picture for security features looks very different from the Case A security features. Case C is only in a very early stage of concept development and it is anticipated that the services supported across the CZ will begin with 2-way messaging and directory services. Additionally, (one-way) coalition-to-NATO file transfer, much like the current interfaces between NATO and SFOR/KFOR will need to be implemented. Security options for bidirectional file transfer and web services are currently under study.

Scalability and availability are very important features that go together if the amount of interconnected CZs increases. The following solutions are considered to master scalability and availability aspects by establishing an IEG backbone infrastructure:

– redundant CZs per NATO nation;

– multiple NATO CZs (covering regions and are in hot-standby for backup);

– high availability requirements for the underlying network layer (NGCS QOS);

– redundant paths (creating secondary connectors) for MTA's;

– distribution of NATO hub directory.

6. Conclusion

A baseline configuration for an information exchange gateway has successfully been tested and validated in the allied systems interoperability testbed. Lessons learned are taken for the further evolution and the operational deployment of the information exchange concept. The NATO C3 Agency is looking forward to a very busy period with the NATO nations to test and implement the information exchange gateway concept and contribute to allied systems interoperability.

References

[1] Capability Package 5A0050/9B0020 "Provide Bi-SC Static AIS Core Capability".

[2] W. Stallings, "Network Security Essentials, Applications and Standards". Upper Saddle River, NJ: Prentice Hall, 1999.

[3] Paragraph 23 of the "Primary Directive on Security", jointly issued as AC/35-D/2004 under the NATO Security Committee and AC/322-D/0052 by the NATO C3 Board, 17 June 2002.

[4] NATO Information Management Policy (ref. a Annex II to PO(99) 189).

[5] NATO GPS Communications System Programme. Vol. II: Technical System Plan, ed. 3, Jan. 1999.

[6] NATO General Purpose Segment (GPS) Communications System (NGCS), Security Architecture, Version 1.31, 3 May 2001.

[7] Microsoft Exchange 5.5 (SP 4). Microsoft corporation, http://www.microsoft.com/exchange/default.asp

[8] NC3B ISSC DS WG, "NATO directory interoperability model", June 2001, http://nra.nacosa.nato.int/ds/zdocs/dsahwg45.zip

[9] Combined Communications Electronics Board (CCEB) Allied Message Handling (AMH) International Subject Matter Experts (ISME), "Allied Communication Publication (ACP) 133 – Common Directory Services and Procedures", March 2000.

[10] Data connection limited. DS directory version 2.4.01., http://www.dataconnection.com/dirs/diridx.htm

[11] Microsoft metadirectory services, Microsoft corporation, http://www.microsoft.com/windows2000/technologies/directory/MMS/default.asp

[12] Microsoft Internet security and acceleration server 2000 SP1, Microsoft corporation, http://www.microsoft.com/isaserver/

[13] Common criteria website, http://www.commoncriteria.org/cc/cc.html

[14] Firewall 1, checkpoint, http://www.checkpoint.com/products/protect/firewall-1.html

[15] Windows NT 4.0 security set-up for NATO classified systems (NR to NS), Version 4 (includes SP6), INFOSEC Command NACOSA, July 2000.

[16] Realsecure managed intrusion protection service (ISS), http://www.iss.net/products_services/managed_services/service_intrusion.php

[17] Standard NATO Agreement (STANAG) 4406, "Military message handling service edition 1", Dec. 1998.

[18] AC/322 (NPMA-PAC) WP-2, "NATO PKI CONOPS, v. 1.3", 5 July 2001.

Martin Diepstraten is a Principal Scientist in the Core Information Systems Technology branch of NC3A's Communications and Information System Division. Prior to joining NC3A in 2000, he worked on a number of Dutch Government and NATO communication and information system development and integration projects. His current activities focus on operating system kernel services, information systems integration and information interoperability.
e-mail: martin.diepstraten@nc3a.nato.int
Communications and Information Systems Division
NATO Consultation, Command and Control Agency
The Hague, The Netherlands

Rick Parker is a Principal Scientist in the Communications Security Techniques branch of NC3A's Communications and Information System Division. Prior to joining NC3A in 1995, he worked on a number of US and NATO Information Security projects, including R&D, standards and architecture. His current activities focus on security aspects of the CCIS and the underlying networks, vulnerability analysis and forensics.
e-mail: rick.parker@nc3a.nato.int
Communications and Information Systems Division
NATO Consultation, Command and Control Agency
The Hague, The Netherlands