Implementing Information Exchange Gateways (IEGs)

Implementing NATO IEGs with Deep Secure

An Information Exchange Gateway (IEG) is a system designed to enable the flow of information between networks whilst at the same time protecting an internal domain from both inbound malware threats and outbound leakage of sensitive information. An IEG consists of a number of components implemented within a De-Militarised Zone (DMZ). The IEG hides the internal domain from the outside world, only exposing interfaces for the required information exchange. Where IEGs are implemented between two networks with a mutual distrust, a pair of IEGs is required, each one protecting its own network and connected to each other via a Wide Area Network (WAN).

Key Advantages

IEGs built on Deep Secure technologies feature:

- Content Threat Removal (CTR) using content transformation to provide the industry's first and only solution that removes sophisticated cyber threats from digital content, guaranteed.
- Policy Enforcement to enforce security policies tailored to business need, ensuring compliance, accountability and data loss protection at the boundary with policy rules that delve deep and inspect business content for potential threats.
- Data Diodes that enforce a uni-directional flow of data between networks.

NATO IEG Scenarios

In order to facilitate information sharing between NATO and its partners (NATO and non-NATO nations, International and Non-Government Organisations), NATO has defined a number of Information Exchange Gateway scenarios. The scenarios are described below and summarised in Figure 1.

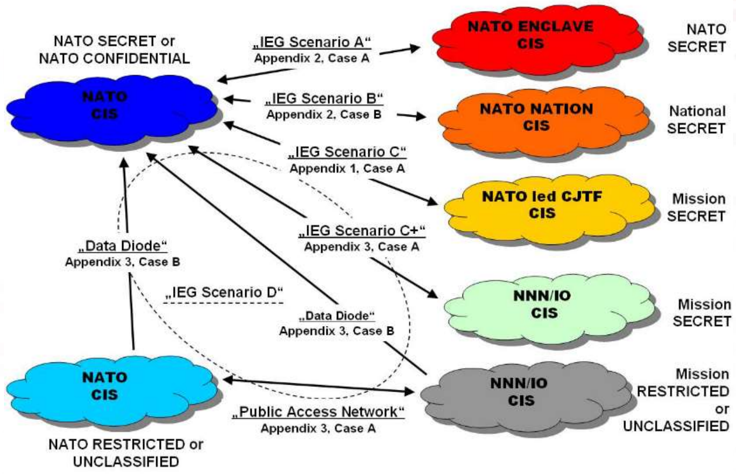


Figure 1 NATO IEG Scenarios [1]

The scenarios differ from each other based on a number of factors:

- Which organisation owns the security policy;
- What level of classification (sensitivity) each network is at;
- Which organisation manages the network.

The different scenarios are summarised in Table 1:

IEG Scenario	High Side IEG		Classification levels	Low Side IEG		Comments
	Security Policy	Network managed by		Security Policy	Network managed by	
A	NATO	NATO	Same	NATO	Nation	e.g. NATO Secret to NATO Secret enclave within a NATO nation
B (1)	Nation	Nation	Same	NATO	NATO	e.g. NATO Secret to National Secret
B (2)	NATO	NATO	Different	NATO	NATO	e.g. NATO Secret to NATO Restricted
C	NATO	NATO	Same	Non-NATO	Non-NATO	e.g. NATO Secret to Mission Secret
D	NATO	NATO	Same / Different	NGO/IO	NGO/IO	e.g. NATO Restricted to EU Restricted
E	NATO	NATO	Different	Public	Public	e.g. NATO Unclassified to Internet

Table 1 NATO IEG Scenarios

NATO IEG Architectural Approach

An IEG provides Boundary Protection Services (BPS). These services are provided by Boundary Protection Components (BPC) which perform a number of tasks for either Node Protection, Information Protection or Information Exchange as shown in Figure 2.

The core information exchange services (MMHS, Web, Email, and Directory) are necessary to support NATO business processes. A characteristic of these services is the complex nature of the protocols with the rich information that can be carried by them. Providing IPS for the core services requires deep inspection of both the underlying protocols and the information being carried to reduce the risk of malware entering into the system and sensitive information being leaked out.

[1] Image from "Guidance Document On The Implementation Of Gateways For Information Exchange Between NATO CIS and External CIS", AC/322-D(2005)0054-REV2, March 2008.

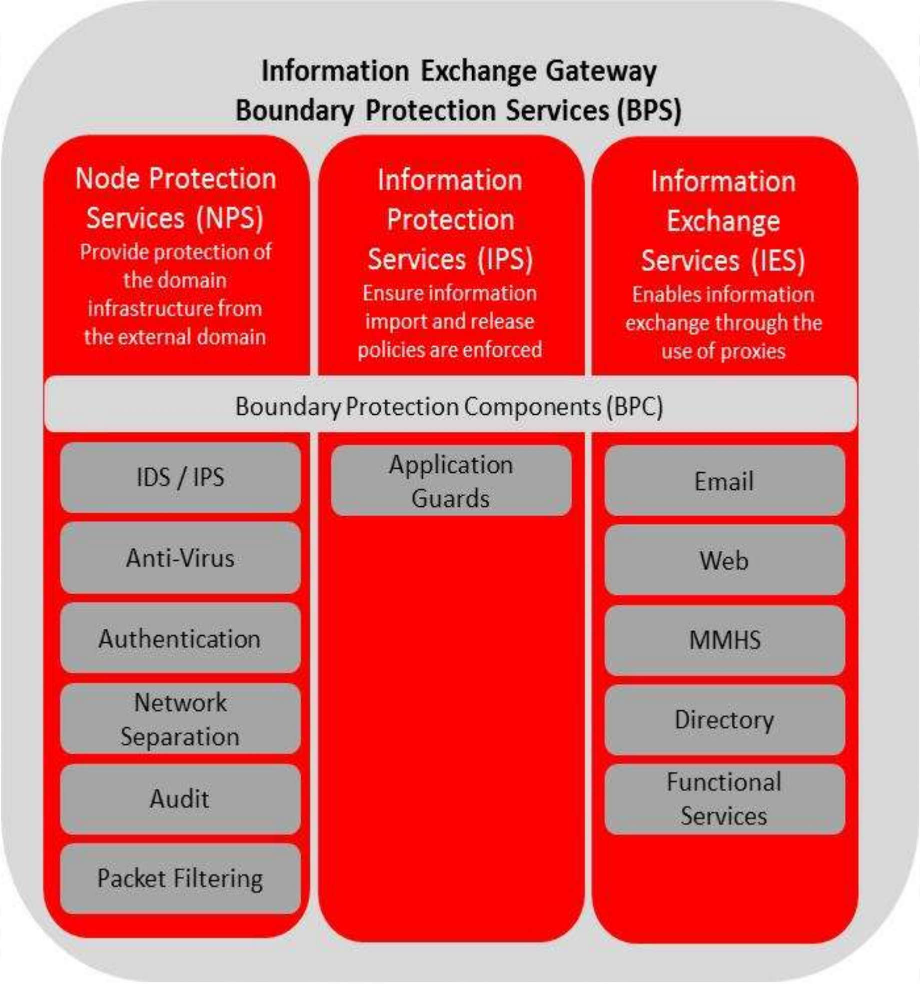

Information Exchange Gateway
Boundary Protection Services (BPS)
Node Protection Services (NPS)
Provide protection of the domain infrastructure from the external domain
Information Protection Services (IPS)
Ensure information import and release policies are enforced
Information Exchange Services (IES)
Enables information exchange through the use of proxies
Boundary Protection Components (BPC)
IDS / IPS
Anti-Virus
Authentication
Network Separation
Audit
Packet Filtering
Application Guards
Email
Web
MMHS
Directory
Functional Services

Figure 2 Boundary Protection Services

In addition to the core services, an IEG may be required to support exchange of functional services such as operational picture sharing and transport of tactical data links. A characteristic of these services is the structured nature of the data. Providing IPS for the functional services requires strong validation of the structure of the data.

Deep Secure Gateway Architectures

There are three basic architectures for a secure gateway. Each of these is suitable for different circumstances because there is a trade-off between ease of management and security. Each of these architectures is appropriate to different IEG scenarios and each can be implemented using a Deep Secure guard product to provide the Information Protection Services, the Information Exchange Services and in certain configurations the network separation component of the Node Protection Services.

DMZ Gateway

A DMZ gateway (Figure 3) is a standard pattern used to connect corporate systems to the Internet. Here the Guard is hosted in the DMZ, on a single-homed platform, along with the servers for externally visible services. The Guard provides the IPS element of the gateway. This arrangement is easy to manage but there are many ways in which it could fail, making it useful only where risks are low. In a DMZ gateway the guard may run on a virtual machine, as it does not provide the Node Protection Service of assured network separation in the solution.

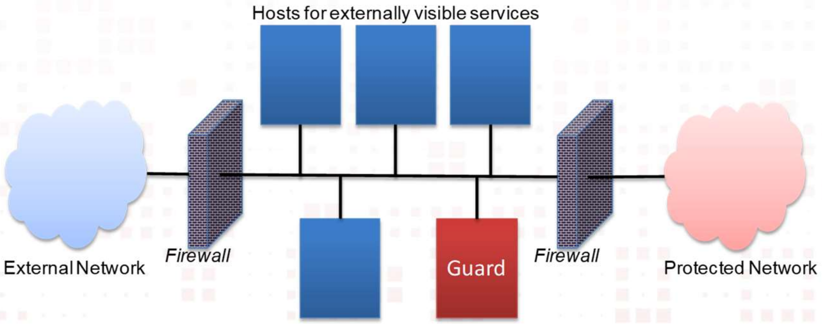


Figure 3 DMZ Gateway

Split-DMZ Gateway

A Split-DMZ secure gateway (Figure 4) is an extension of the standard pattern where separate DMZ networks are used for each network connected by a guard running on a dual-homed platform. This gives far better security, with the right Guard, because the guard is providing the Information Protection Services and the Node Protection Service of assured network separation (as well as the Information Exchange Services). The downside of this architecture is that the gateway is more difficult to manage from a central point, as management traffic must pass through the Guard. In a split-DMZ gateway the guard will be hosted on a dedicated physical machine, not a virtual machine, to avoid weaknesses in virtualisation undermining the assured separation provided by the Guard.

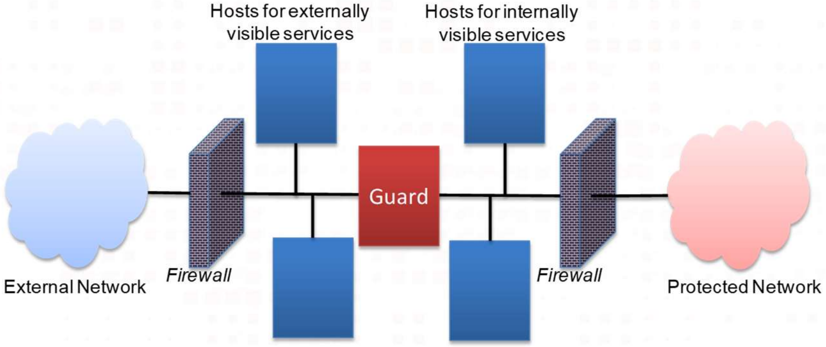

Hosts for externally visible services
Hosts for internally visible services
Guard
External Network
Firewall
Firewall
Protected Network

Figure 4 Split-DMZ Gateway

Split-DMZ with One Way Link Gateway

Where the business only needs information to pass in one direction, and security risks are very high, the Split-DMZ architecture can be made more secure by wrapping the Guard function around an optical one way link (Figure 5). The architecture is less flexible because it is uni-directional and is more difficult to manage, because the externally visible servers must be controlled from a separate management network, but security is greatly enhanced.

Security functions are centred on the Guard and the Guard's critical checks are protected from an attacker by the one way link, as any attack must work without feedback. Also, with inbound data flows, the one way link prevents any leaks of information from Protected to External and with outbound data flows the one way link blocks any attacks against the protected system. The computers hosting the guard software need to be physical computers because the variable performance of a virtualised platform makes the one way link unreliable at high speeds.

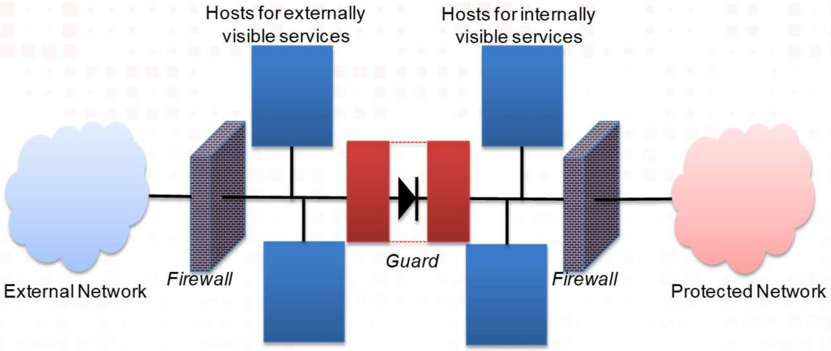
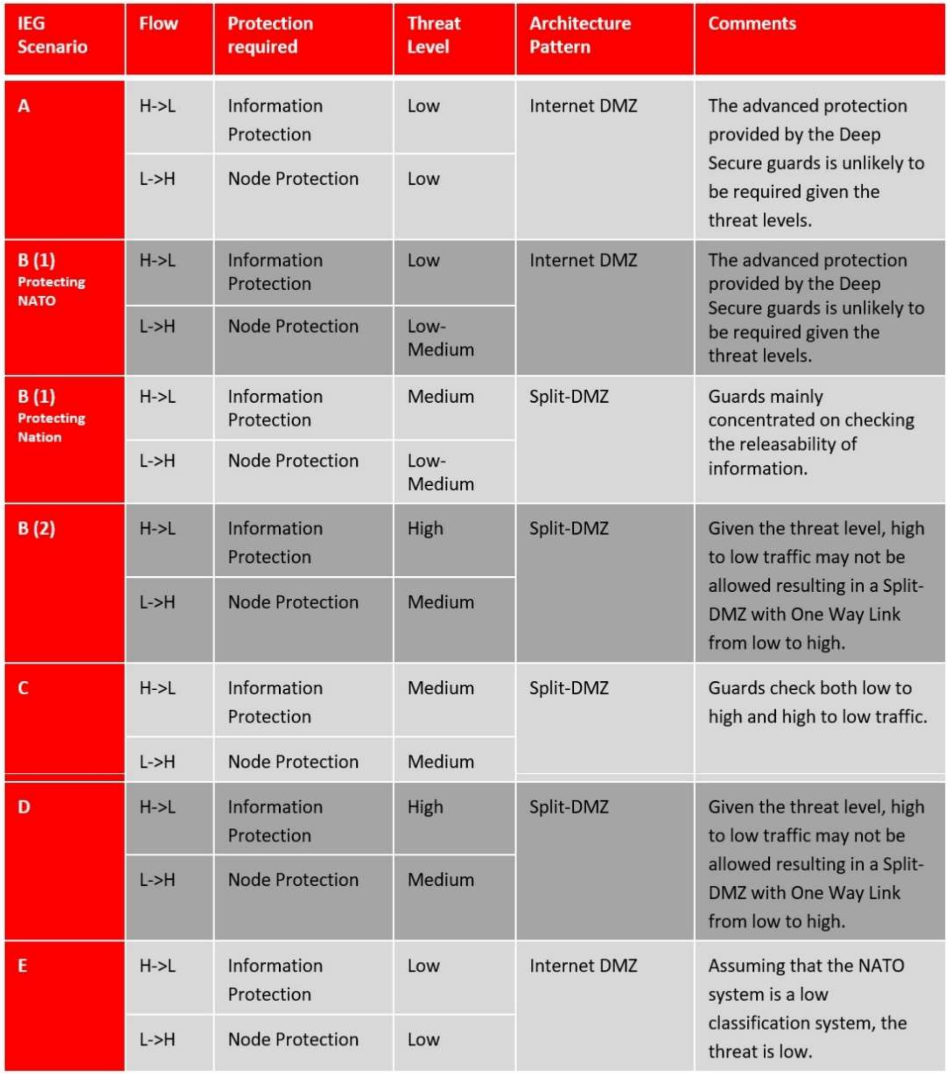

Hosts for externally visible services
Hosts for internally visible services
Guard
External Network
Firewall
Firewall
Protected Network

Figure 5 Split-DMZ with One Way Link Gateway

Unlike a Data Diode solution, this architecture provides the assured network separation Node Protection Service, the Information Protection Service and the Information Exchange Services for the gateway. It is also more performant and more manageable than a solution that places a data diode and a guard in series.

Mapping to IEG Scenarios

Using the definition of the IEG scenarios, it is possible to map each scenario to the gateway architectures above. This is shown in Table 2.



IEG Scenario	Flow	Protection required	Threat Level	Architecture Pattern	Comments
A	H->L	Information Protection	Low	Internet DMZ	The advanced protection provided by the Deep Secure guards is unlikely to be required given the threat levels.
	L->H	Node Protection	Low		
B (1) Protecting NATO	H->L	Information Protection	Low	Internet DMZ	The advanced protection provided by the Deep Secure guards is unlikely to be required given the threat levels.
	L->H	Node Protection	Low-Medium		
B (1) Protecting Nation	H->L	Information Protection	Medium	Split-DMZ	Guards mainly concentrated on checking the releasability of information.
	L->H	Node Protection	Low-Medium		
B (2)	H->L	Information Protection	High	Split-DMZ	Given the threat level, high to low traffic may not be allowed resulting in a Split-DMZ with One Way Link from low to high.
	L->H	Node Protection	Medium		
C	H->L	Information Protection	Medium	Split-DMZ	Guards check both low to high and high to low traffic.
	L->H	Node Protection	Medium		
D	H->L	Information Protection	High	Split-DMZ	Given the threat level, high to low traffic may not be allowed resulting in a Split-DMZ with One Way Link from low to high.
	L->H	Node Protection	Medium		
E	H->L	Information Protection	Low	Internet DMZ	Assuming that the NATO system is a low classification system, the threat is low.
	L->H	Node Protection	Low		

Table 2 IEG Scenario Mapping to gateway architectures

Deep Secure Guards

Deep Secure provide a range of guards to protect systems from the threat of inbound malware and outbound data leakage whilst enabling information exchange. The guards provide:

- Assured separation when using a Split-DMZ pattern;
- Full application layer proxy;
- Deep content inspection or transformation of content.

Assured Separation ensures that all communication between the connected domains is controlled and cannot bypass the content filters.
An Application Layer Proxy reduces the threat of protocol based attacks by terminating the connection on one side of the guard and creating a new connection on the other side of the guard.

The guards include deep content inspection . This reduces the threat of attacks hidden inside complex formats such as Microsoft Word and PDF by looking inside the document for known attack methods and protects against information leakage by looking for inappropriate material.

The latest range of Guards performs transformation of the content. This provides an information layer proxy by only copying the business information from the content and creating a new instance of the content on the other side of the guard. transformation ensures the protected system does not receive data that it cannot handle safely. This method reduces the threat of both known and unknown (zero day) attacks in the content format.

Policy Engine Guards
Deep Secure Policy Engine Guards provide deep content inspection of data transferred over the commonly used Web, Email and File Transfer protocols. The deep content inspection capability of the guards makes them appropriate for the complex protocols and rich data exchanged over the core Information Exchange Services.

Information Exchange Services

Deep Secure Engine Guards support SMTP, X.400 and HTTP protocols. These can be used to support a number of Information Exchange Services:

- Informal Messaging (Email);
- Formal Messaging (Military Messaging);
- Web Browsing;
- Application to Application Web Services;
- Directory Replication;
- File Transfer.

Content Inspection

Deep Secure Policy Engine Guards perform a thorough inspection of the content transferred using the above services. Complex security policies can be created to validate the content, with the ability to specify different policies for inbound and outbound traffic. Policies can be high level (one per domain) or granular down to the individual user level.

The Engine Guards perform checks to reduce the threat of inbound malware:

- Attachment Type Checking to ensure that data is one of an allowed type and that it is not masquerading as a different format (e.g. an executable);
- Attachment Filtering to ensure that the data is not corrupt, does not contain dangerous objects such as macros and does not contain an unreasonable number of embedded items;
- Virus Scanning to catch known attacks in the content;
- Server Authentication to ensure only valid servers can send or receive data;
- User Authentication and signature validation to ensure only valid users can send and receive data;
- Inspection of encrypted content to ensure malware is not hidden inside encrypted content.

The Engine Guards perform checks to reduce the threat of outbound data leakage:

- Label Checking to ensure sensitive information that is protectively marked is not sent out of the domain;
- Lexical Analysis to find sensitive information within the content;
- Detection of hidden/easily overlooked data including meta data;
- User Authentication and signature validation to ensure only authorised users can send data out of the domain.

Policy Engine Guard Architectures

Deep Secure Engine Guards can be deployed either on a physical platform or in a virtual environment depending on the risk. When deployed on a virtual platform, the guard can be installed on either a Solaris 10 or Linux operating system. When deployed on a physical platform, assured separation is provided using the Deep Secure Bastion platform. Bastion is a platform for guards which exploits the EAL4 evaluated security functionality of Oracle's Solaris 10, with Trusted Extensions, operating system.

Solaris 10 zones partition the guard host's resources so that the security critical Content Checking Engine is protected from the guard's protocol handling software (Figure 6). In addition, internal communication is constrained so that no data can pass between networks without passing through a Content Checking Engine.

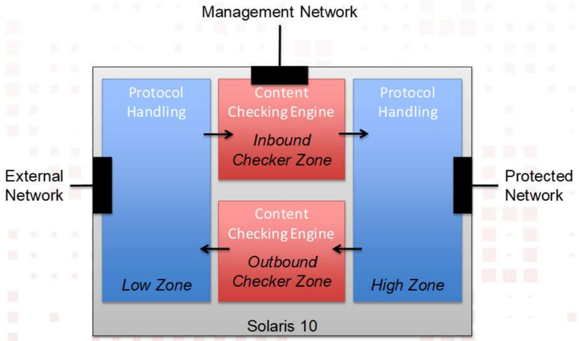


Figure 6 Bastion Zone Architecture

Deep Secure Policy Engine Guards support a number of protocols – Mail Guard for SMTP and X.400 and Web Guard for HTTP. Normally one such guard is hosted on a server, and several instances can be deployed in parallel to increase throughput and/or resilience. However it is also possible for multiple guards to be hosted on the same server, possibly with multiple instances operating in parallel.

File Transfer is enabled using Deep Secure File Transfer Management software either side of Web Guard. The Web Guard validates the files according to the security policy.

Directory Replication is enabled by transferring the required directory updates as structured data (e.g. XML) over HTTP or via file transfer. The Web Guard validates the data to ensure that it is well formed and only contains valid directory replication data.

Deep Secure Mail Guard

The Deep Secure Mail Guard is a full application layer proxy for SMTP and X.400 that provides deep content inspection of the data. It supports formal / military messaging and informal / email messaging.

Deep Secure Web Guard

The Deep Secure Web Guard is a full application layer proxy for HTTP and HTTPS that provides deep content inspection of the data. It supports both web browsing and web services as well as file transfer when used in conjunction with the Deep Secure File Transfer Manager software.

Content Threat Removal Guards

Deep Secure Content Threat Removal Guards are delivered with a hardened operating system (Deep Secure OS) and provide transformation based content handling. This makes them suitable for structured data checking and machine to machine data exchange.

Information Exchange Services

The Content Threat Removal Guards currently support SMTP, HTTP(s) DSFSP (File Transfer), framed TCP and UDP and can transform the following data formats including embedded content:

- MS Office, RTF, PDF, ZIP
- Imagery (BMP, GIF, JPG, PNG)
- Structured JSON, XML, CSV
- Extended file type support with optional sidecar facility

Using the Content Threat Removal Guards, NATO Functional Services transported over HTTP that use any of the above data formats are supported e.g. NFFI. Additional Functional Services such as Link 16 and Adat-P3 can be supported through the use of a gateway to handle the application protocol and to convert the data to one of the above data formats.

The use of content transformation means that these guards may also be appropriate for protection of the core services in secret and above systems where advanced threats can target a deep content inspection capability.

Content Transformation

Deep Secure Content Threat Removal Guards use a process called content transformation. This goes beyond deep content inspection to defend a system's applications against advanced threats that exploit weaknesses in the way they handle data. The transformation process consists of the following steps:

- A message/file/document is received from a source;
- The business content is extracted from the received message;
- The business content is verified to confirm it is appropriate to business needs;
- A new message is created that conveys the business content in a way that can be safely handled by the destination;
- The new message is delivered to its destination.

In the verification step, data passing between networks is blocked if the business content does not meet the configured policy, with full logging of the event to enable monitoring systems to detect mal-practice and attacks. As a result of transformation, a potential attacker has no influence over the way data that is delivered to the application is rendered, which means they cannot use carefully crafted data structures to exploit weaknesses in the way applications handle them.

However, many important file formats can be interpreted quite differently if they are delivered to the wrong application. The attacker generally has the opportunity to influence which application receives some data, so this leaves an avenue for attack. Deep Secure's transformation technology combats this by disrupting the way data is delivered to ensure that it will be handled safely by the wrong application as well as the right application. For example, a browser will interpret any data as an HTML web page if it is presented to it in that way. This means a file can be created that is both a valid RTF document and an HTML web page containing scripts. To deny an attacker the ability to run scripts by disguising them as RTF, Deep Secure's transformation software constructs the RTF representation so it does not contain any HTML tags if treated as HTML.

Deep Secure's transformation technology works by translating all data formats into a common format called the eXtensible Data Structure (XDS). This is a simple structure designed specifically to ease the task of creating high assurance content checkers. Use of a common representation means only one verifier is needed, so when new data formats must be supported there is no need to create additional high assurance software.

Content Threat Removal Guard Architectures

To protect itself from attack, the guard is split across two physically separate servers (Deep Secure HRB models) coupled by a hardware logic device – the High Speed Verifier (HSV) – shown in figure 7.

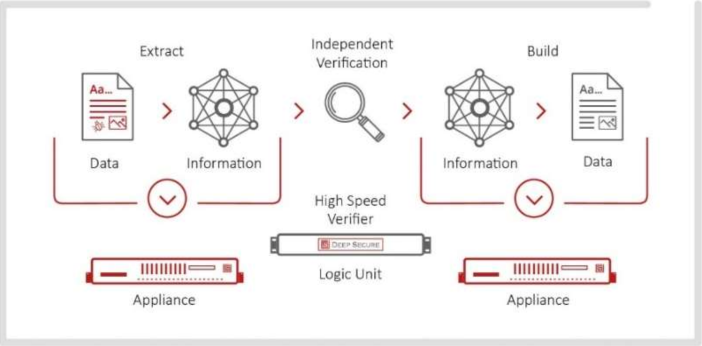


Figure 7 Content Threat Removal Guard Architecture

Each server is connected to a different network. A server extracts information from digital content that arrives from its network and passes this information to the other server via the HSV unit. The HSV verifies the simple protocol used is being followed and verifies that the information is correctly structured.

The HSV is a purely logic device. It has no processor and contains no software, so has no software attack surface. The way information is conveyed through it ensures that the HSV hides the attack surface of the destination server, so overall the guard has a minimal attack surface, making it suitable for the protection of Secret and Top Secret systems.

Deep Secure iX Guard

Deep Secure iX Guard is a full application layer proxy for protocols, including HTTP, carrying structured data, including XML and JSON. It performs content transformation to ensure the protected system does not receive data it cannot handle safely. iX Guard supports use in the following cases:

- to protect a system where access to an application in the protected system is required via a web interface;
- where a client application in a protected system has to communicate with a server application in a remote system;
- where a server application in a protected system has to communicate with a client application in a remote system.

Deep Secure Chat Guard

Deep Secure Chat Guard is an application layer proxy for XMPP controlling both the establishment of chat sessions and the flow of data during those sessions. It performs transformation to ensure the protected system does not receive any data in the chat session that it cannot handle safely.

Chat Guard supports use where XMPP chat sessions have to be made across security boundaries.

Deep Secure Network Management Guard

Deep Secure Network Management Guard is an application layer proxy for SNMP and Syslog controlling the flow of network management traffic between domains. It performs policy enforcement to ensure the protected system does not receive any network management data it cannot handle safely.
Network Management Guard supports use where network management information has to be passed between the managed network and a single management network, for example in a Split-DMZ architecture.

Deep Secure Data Diode

In cases of extreme risk, a physically uni-directional guard is required. In this case, an optical data diode could be used to ensure that data only flows in a single direction. But, even when systems are protected by optical data diodes, critical systems are still vulnerable to attack by virtue of the data delivered to them from less trusted systems through the diodes. Adding content checking functionality to the solution may still prove inadequate as it can be targeted by advanced threats and so may not provide an adequate defence for Secret and above systems.

The Deep Secure Data Diode provides a guarded one way stream of files between systems. It uses transformation to protect against attacks and leaks through the content a one way link to provide an assured one way flow of data. (Figure 8).

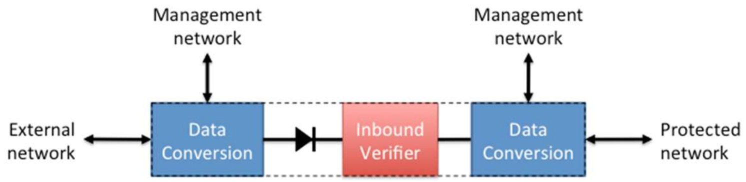


Figure 8 Uni-directional Transformation using Deep-Secure Data Diode

Requests from clients on the external network are converted to XDS, passed through the one way link to the verifier and then immediately a "success" response is generated and returned to the client. Any responses from the destination server are logged and discarded. The Data Diode guarantees no information passes from the protected to external network. The Data Diode is deployed across two computers, connected by an optical one way link or if EAL7 is required, a dedicated hardware device.

The Deep Secure Data Diode is a general purpose Guard for data feeds between applications. It supports use in High to Low or Low to High data feeds with or without an optical one way link.

File Transfer Applications

In addition to the Guards, Deep Secure offers applications to enable manual and automatic transfer of files between systems. The applications run on the customers' own equipment and transfer the files through the Deep Secure Guards for content inspection or content transformation.

Manual Transfer

File Transfer Manager is a Windows application that presents a file browser interface for manual transfer of individual files or jobs of multiple files into or out of a system.

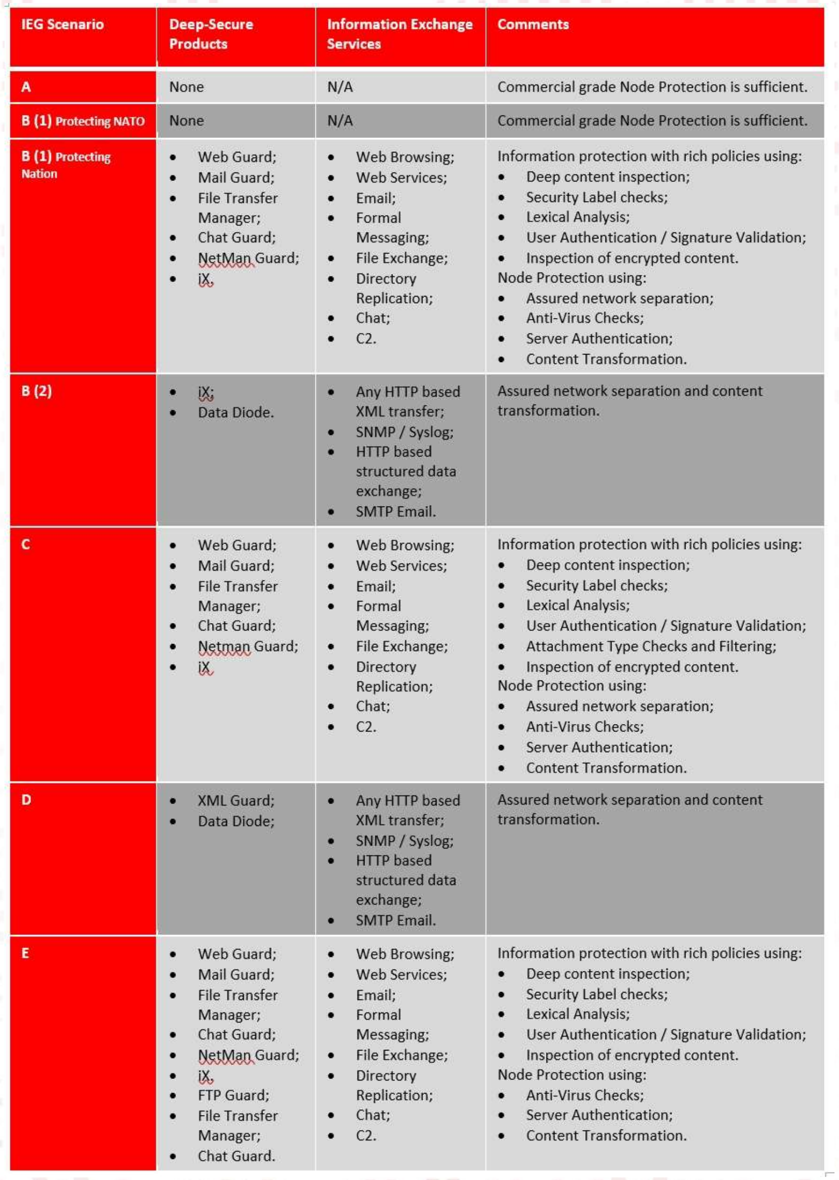
Automatic Transfer

The following applications enable automatic transfer of files between systems:

- Deep Secure Mover watches one or more folders and when files appear, moves them across the Guard to a destination folder;
- Deep Secure Copier works in the same way as Mover, but makes a copy of the file to send across to the destination;
- Deep Secure Mirror maintains a mirror of a directory on the source system on the destination system. An application script on the source system triggers the Mirror software to send updates to the destination. When the update of the mirrored data completes, the destination component runs a configured script to inform the application that the data is ready and consistent.

Mapping Deep Secure products to Information Exchange Services

Table 3 shows the mapping of the IEG scenarios and the Information Exchange Services to Deep Secure products and the relevant functionality to provide the required protection.



IEG Scenario	Deep-Secure Products	Information Exchange Services	Comments
A	None	N/A	Commercial grade Node Protection is sufficient.
B (1) Protecting NATO	None	N/A	Commercial grade Node Protection is sufficient.
B (1) Protecting Nation	• Web Guard; • Mail Guard; • File Transfer Manager; • Chat Guard; • NetMan Guard; • iX.	• Web Browsing; • Web Services; • Email; • Formal Messaging; • File Exchange; • Directory Replication; • Chat; • C2.	Information protection with rich policies using: • Deep content inspection; • Security Label checks; • Lexical Analysis; • User Authentication / Signature Validation; • Inspection of encrypted content. Node Protection using: • Assured network separation; • Anti-Virus Checks; • Server Authentication; • Content Transformation.
B (2)	• iX; • Data Diode.	• Any HTTP based XML transfer; • SNMP / Syslog; • HTTP based structured data exchange; • SMTP Email.	Assured network separation and content transformation.
C	• Web Guard; • Mail Guard; • File Transfer Manager; • Chat Guard; • Netman Guard; • iX.	• Web Browsing; • Web Services; • Email; • Formal Messaging; • File Exchange; • Directory Replication; • Chat; • C2.	Information protection with rich policies using: • Deep content inspection; • Security Label checks; • Lexical Analysis; • User Authentication / Signature Validation; • Attachment Type Checks and Filtering; • Inspection of encrypted content. Node Protection using: • Assured network separation; • Anti-Virus Checks; • Server Authentication; • Content Transformation.
D	• XML Guard; • Data Diode;	• Any HTTP based XML transfer; • SNMP / Syslog; • HTTP based structured data exchange; • SMTP Email.	Assured network separation and content transformation.
E	• Web Guard; • Mail Guard; • File Transfer Manager; • Chat Guard; • NetMan Guard; • iX. • FTP Guard; • File Transfer Manager; • Chat Guard.	• Web Browsing; • Web Services; • Email; • Formal Messaging; • File Exchange; • Directory Replication; • Chat; • C2.	Information protection with rich policies using: • Deep content inspection; • Security Label checks; • Lexical Analysis; • User Authentication / Signature Validation; • Inspection of encrypted content. Node Protection using: • Anti-Virus Checks; • Server Authentication; • Content Transformation.

Table 1 IEG Scenario Mapping to Deep-Secure Guards

Summary

NATO has defined a set of Information Exchange Gateways to enable information sharing with its partners. IEGs are typically deployed in a symmetric pair, one protecting NATO and one protecting the partner. Deep Secure can help to provide key border and information protection services to organisations that are implementing IEGs either for NATO or for partners connecting to NATO.

The Deep Secure range of guards are suited to the NATO IEG architectural approach and have established technology that is widely implemented and respected across UK MOD, UK Government and NATO. The Guards are also on the NATO Approved Products Catalogue (NIAPC). Deep Secure has committed development roadmaps that, underpinned by a technical team with the specific expertise to deliver new capability, enable solutions built around the products to adapt to changing business requirements and evolving threats. The products are designed to minimise the impact of system accreditation arising because of change.