esrin

Via Galileo Galilei, 00044 Frascati, ITALY

DOCUMENT

ESA Earth Observation PDGS
Implementation of the EO Network Security Policy

GMGT-SENE-EOPG-PD-10-0004 ESA_EOP-G-NW_Policy_Implementation-v1.2

Prepared by	**EO Network Security Office**
Reference	**GMGT-SENE-EOPG-PD-10-0004**
Issue	**1**
Revision	**2**
Date of Issue	**22/Sep/2010**
Status	**Approved/applicable**
Document Type	**EO Policy Document**
Distribution	**EOP-G, OPS-ERO**

European Space Agency
Agence spatiale européenne

APPROVAL

Title Earth Observation PDGS - Implementation Of The EO Network Security Policy	
Issue 1	**Revision** 2
Author EO security team	**Date**
Approved by	**Date**
Gioacchino Buscemi, ESA, EOP-GS Maria Eugenia Forcada Arregui, ESA, H/EOP-GS	24/09/2010 29/9/2010
Authorized by	**Date**
Gunther Kohlhammer, ESA, H/EOP-G	18/10/2010

CHANGE LOG

Reason for change	Issue	Revision	Date
Initial version	1	0	31-Mar-2006
First update	1	1	14-Nov-2007
Second update	1	2	22-Sep-2010

CHANGE RECORD

Issue 1	Revision 2		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
• See section 5 for details • Update of the ESA Document Templates	22-Sep-2010	All	All

Table of contents:

List Of Figures:

List of Tables:

1 INTRODUCTION

Over the years, ESA Earth Observation (EO) has deployed an effective environment to allow quick and effective acquisition, processing, storage, distribution and access to the various Earth Observation products. All these services are connected to the various EO networks. To protect these interconnected EO assets, a network security policy is required that sets the baseline against which implementations of these networked services, their management and security controls are deployed.

This policy document fits in the overall ESA Earth Observation (EO) Ground Segment Security Framework depicted below. It is in line with the higher level policies. It addresses the more practical security aspects when connecting systems and services to the EOP-G networks.

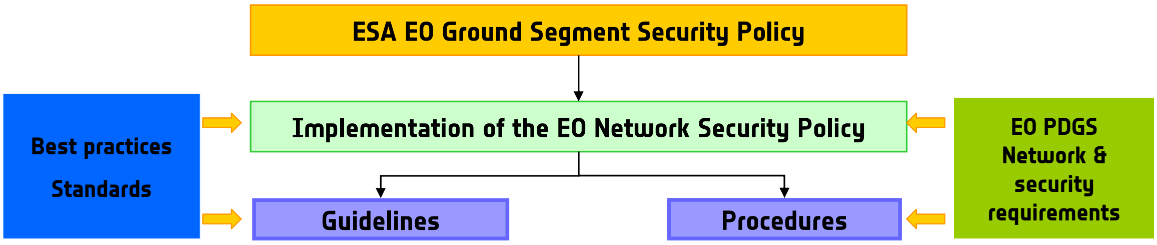
ESA EO Ground Segment Security Policy
Implementation of the EO Network Security Policy
Best practices
Standards
Guidelines
Procedures
EO PDGS Network & security requirements

Figure 1 - The EO Information Services Security Policy Framework

Procedural aspects on how to implement the network security policy are provided in EOP-G Network Security Procedures. Likewise, guidelines that may help in successfully implement the EOP-G security policy are provided in separate EOP-G Network Security Guidelines.

Standards and best practices are followed as much as possible and applicable to the EO environment.

EO PDGS network and security requirements influence the implementation of the EOP-G network security policy, its corresponding guidelines and operational procedures.

This document replaces ESA_EOP-GNW_Policy_Implementationv1.1.3 issued 14-11-2007. The current document enters immediately into force and remains applicable until next revision.

The current document will be subject under yearly review, unless a major need requires anticipating it.

The review will take into account acquired experience and lessons learnt during the year, new/changed services and business needs to be implemented or existing services that have been extended/changed/improved. The emerging needs and related secure solutions identified to satisfy them will be integrated into the baseline described in this document.

2 SCOPE AND APPLICABILITY

This document applies to all services, systems and users of the EOP-G Networks, commonly referred to as EO Networks for brevity. It maps the “ESA Earth Observation Ground Segment Security Policy” [AD1] to the networked infrastructure and services that are deployed and provided in the context of the Earth Observation projects on the EO Networks.

The scope of the document is limited to the EOP-G Networks.

All EO networks owned by the Agency are also subject to the ESA Corporate Network Security Policy [RD1] and corresponding implementation document [RD2], in as far as they apply to the EOP-G Networks.

3 DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

Community
A group of EO users and/or services that share a common network infrastructure with the same security baseline.

DMZ
A DMZ, or demilitarized zone, refers to a perimeter network that can be a physical or logical subnetwork containing systems that expose services to a network of lower security class. Likewise it may offer screened and restricted access to services residing on networks of another security class. Traffic to and from the DMZ is screened by a Firewall.

EO Centre
Refers to one of the currently known EOP-G Centres:

1. Frascati, Italy - ESRIN
2. Kiruna Salmijarvi, Sweden - SSC
3. Kiruna, Sweden - ESRANGE
4. Farnborough, UK - Infoterra
5. Oberpfaffenhofen, Germany DLR
6. Neustrelitz, Germany - DLR
7. Matera Station ,Italy - Telespazio
8. Maspalomas, Spain - INTA
9. Toulouse, France - CNES
10. Tromsø, Norway - KSAT
11. Svalbard, Norway - KSAT
12. Sodankylä, Finland –FMI
13. Villafranca de Castillo, Spain - ESAC.

ESN
ESA External Services Networks. See [RD1] – section 5.7.1 “ESA Network Security Hierarchy Classification”

ISN
ESA Internal Services Networks. See [RD1] – section 5.7.1 “ESA Network Security Hierarchy Classification”

Off-site network
Refers to an EO network at non-ESA premises; e.g. Serco Frascati Office, Advanced Computer Systems, ElsagDatamat.

Remote network
A network not located at one of the EO Centres.

3.2 Abbreviations

ACL	Access Control List
ACS	Assertion Consumer Service
Corp. DMZ	Corporate DMZ
DAP	Data Access Portal
DDoS	Distributed Denial of Service
DNS	Domain Name System
DMZ	De-Militarized Zone
E-Serv	External ICT Services LAN
EO	Earth Observation
EO NSO	Earth Observation Network Security Officer
EOP-G	Earth Observation Department – Ground Segment
EO-SSO	Earth Observation Single Sign On
ESACERT	ESA’s Computer and Communications Emergency Response Team
ESN	ESA (Corporate) External Services Networks
FTP	File Transfer Protocol
HiSEEN	High-Speed ESA Earth Observation Network
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL/TLS
I-PSN	Internal Projects and Services Network(s)
I-Serv	Internal ICT Services LAN
IP	Internet Protocol
IPSec	Internet Protocol security architecture
IDS	Intrusion Detection System
IPS	Intrusion Protection System
ISN	ESA (Corporate) Internal Services Networks
L1 DMZ	Level 1 or Restricted Trust DMZ
L2 DMZ	Layer 2 or Interconnection DMZ
L3 DMZ	Layer 3 or Inter Trust DMZ
LAN	Local Area Network

LDAP	Lightweight Directory Access Protocol
MGT DMZ	Management DMZ
ODAD	On-Line Data Access and Distribution
ODAD-NS	ODAD-Network Services
PSTN	Public Switched Telephone Network
RAS	Remote Access Service
SDSR	Security Delta Service Request
SFTP	Secure FTP
SLDAP	LDAP over SSL/TLS
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

4 RELATED DOCUMENTS

4.1 Applicable Documents

[AD1] ESA Earth Observation Ground Segment Security Policy – GMGT-SECR-EOPG-PD-07-0001

[AD2] GMES Space Component Data Access principles, ESA/PB-EO(2008)65, May 8 2008.

[AD3] Revised ESA Data Policy for ERS, Envisat and Earth Explorers missions, ESA/PB-EO(2010)54, May 11 2010.

[AD4] Network and ICT Security requirements for the EO PDGS v1.1, GMGT-SENE-EOPG-RS-09-0002

[AD5] EO PDGS data categorization guidelines and security rules v.1.0, GMGT-SENE-EOPG-TN-10-0006

[AD6] EO PDGS Users classification v.1.0, GMGT-SENE-EOPG-TN-10-0007

4.2 Reference Documents

[RD1] ESA Security Directives – ESA/ADMIN/IPOL(2008)6

[RD2] Implementation Of The ESA Network Security Policy, EISD-EPNS-00003, Version 2, Revision 2(.3), 28/09/2004

[RD3] EO Network Security Interconnection Agreement template, issue 1, rev 2

[RD4] EO Network Security Waiver template, issue 1, rev 0

[RD5] Technical Description of the EO network and ICT security infrastructures v1.0 – GMGT-SENE-EOPG-TN-09-0003

[RD6] Solution Definition for the new SMOS DMZ, ref. EISD-ESAC-0012-1, v1.0, 20/5/2008

[RD7] Annex to Solution definition for the new SMOS DMZ.xls, 9/04/09

[RD8] EO SDSR processing procedure v2.3

[RD9] EOSEC-SDSR-Form-r1.4

[RD10] Solution definition for off-site relocation of EOP-G's contractors v1.3 - EISD-OSR-0002

[RD11] UM-SSO Installation Guide for SP Integration, ref. SIE-UMSSO-SP-INT-001,

v.1.4.6, 17-3-2010

[RD12] EO op UM-SSO Interface Control Document, Ref. SIE-EO-OP-UM-SSO-ICD-002, v. 2.2.1, 17-3-2010

5 CHANGES TO PREVIOUS VERSION

This section summarizes the main differences with v1.1.3 of this document.

5.1 The New EO Network Reference Architecture

In order to meet and manage the requirements of EO projects, the EO network reference architecture has been upgraded. Instead of the black-and-white internal and external security zones, there are now several grades of security zones. Details are provided in section 6, 7 and 8.

5.2 Promoted Hosts

The concept of promoted hosts was introduced ad-hoc at times that the EO networks were still being engineered. The concept was never defined and security practices that should apply to these hosts were never defined nor applied. Over the years, promoted hosts became a synonym for a quick and easy way to bypass the EO network security baseline for some hosts. However, no consideration was given to the security impact on these promoted hosts and all other systems on EO networks, the continuous confusion and discussions about promoted hosts, the extra cost and effort required handling promoted hosts from the security and operational teams and the impact on the EO front-end.

In those early days, there was no coordinated EO network and security governance and clear organization. ESA corporate security policies were not adhered to.

Since 2006, all the above has been put in place in line with and under supervision of EO Management. In addition, the EO networks have evolved significantly - see section 5.1 - such that promoted hosts have become an unnecessary and obsolete practice. Last but not least, the ESA Security Directives were released in 2008 and are applicable to ESA as a whole.

As from the first release (v1.0) of the “Implementation of the EO Network Security Policy” on 31-Mar-2006, projects and design authorities were requested to cease using promoted hosts and services. Since v1.1 of this document, released on 17-Sep-2007, the concept of promoted hosts was not supported anymore.

As of this release, v1.2, the concept of promote hosts is formally withdrawn. With this release of the policy, no new promoted hosts are granted or implemented anymore.

Implementations of existing promoted hosts shall either:

- be decommissioned, when the system and/or service is not necessary anymore;
- be migrated to the supported network reference architecture and practices as described in sections 6, 7 and 8;
- or remain in place until decommissioning of the system and services. This option requires as of now an approved waiver. See section 8.16.)

The intention is to phase out all promoted hosts over time.

5.3 Direct Access To The Internet

As of this release, v1.2, direct access from systems on the EO internal networks (I-PSNs, L3, MGT, I-Serv) to the Internet for the baseline services, is decommissioned as a baseline service. The baseline services to the Internet can be obtained via the proxies and gateways residing on the E-Serv LAN. See section 6, 7 and 8.3.1.

5.4 Telnet

As of this release, v1.2, the use of telnet to access systems on the EO networks is decommissioned as a baseline service. Interactive console access is supported via SSH.

If telnet is required on a permanent basis and it cannot be migrated to SSH, the service will need to be requested via an EO-SDSR.

5.5 PoP

As of this release, v1.2, the use of PoP to pick up client mail on the EO networks is decommissioned as a baseline service. Supported client side mail services are based on the EO Lotus Notes services.

If other mail services are required they are to be requested via a Change Request and an EO-SDSR.

5.6 Ping - Traceroute

As of this release, v1.2, the use of ping and traceroute to networks of different security classification is decommissioned as a baseline service. These services belong to the network management services and are supported from the EO Management DMZ (see section 6 and 8.3.7.

If ping and/or traceroute is required on a permanent basis from a system on the other EO networks, the service will need to be requested via an EO-SDSR.

5.7 EO Security Framework

While former versions of this document presented the entire EO security framework in progress for networks, data, and several other potential security policies, this revision highlights the framework for network security only. See section 1.

5.8 Procedures

All previous versions of this document were based on a security framework that clearly separates policies from procedures and guidelines. This is common best security governance practice applied everywhere in the world. Indeed, procedures are operational related items are bound to change according to entirely different mechanisms then those applicable to a policy. Procedures are produced and maintained by different entities. This was also clear for EO over the last years. Hence, all procedural items have been removed from this policy document.

5.9 Network Security Baseline Numbering

A renumbering of the network security baselines was required in order to take into considerations all possible traffic flows. Each rule in the new EO network baseline numbering scheme is identified by:

- source network name
- Destination network name
- progressive ID

A cross-reference is provided in Appendix A to trace back old security baseline numbers towards the new ones.

5.10 Editorial change

The document title has been changed to better reflect the scope of the document.
The previous title “Earth Observation Implementation of the EO Network Security policy” has been changed into “ESA Earth Observation PDGS Implementation of the EO Network Security policy.

6 THE EO CENTER NETWORK REFERENCE ARCHITECTURE

In Figure 2 the reference network architecture for an EO Centre is presented. It shows the different network types that may be implemented at an EO Centre.
Note that not all network types need to be present at every EO centre.

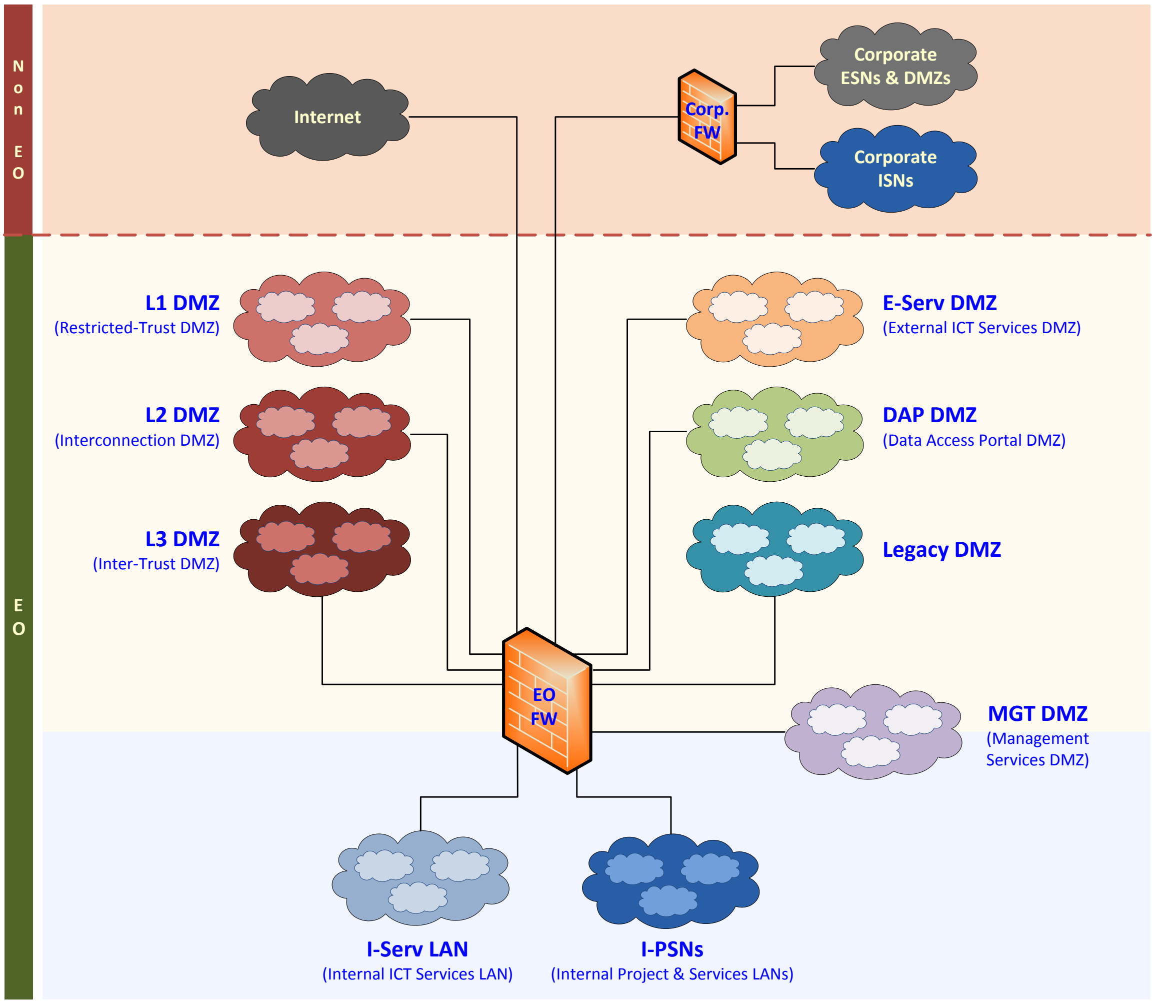

Figure 2 - EO Centre High-Level Network Reference Architecture

Each network zone represents a different network security level. Figure 2 represents the EO Network Security Classification.

The EO network security classes are discussed below.

7 EO NETWORK SECURITY CLASSIFICATION

A network connecting to the EO networks is classified as:

- An external network
- A non-EO network
- An EO demilitarized zone
- An EO internal network.

The security level of each zone is determined by the network security baseline and not by the physical or logical connection to screening devices; e.g. some EO DMZ's are more secure then an EO internal network. (See section 9.)

EO networks may be deployed at EO Centres as well as on remote sites. See section 8.5.

7.1 External networks

The External Networks are networks outside ESA's administrative control. Examples of such networks can be, but are not limited to:

- Any type of Internet connectivity.
- Networks owned by other Space Agencies External entity like NASA, JAXA that connect to EO networks.
- Networks owned by industrial partners offering some kind of services to EO (like hosting, outsourcing).

All communication between the external network and the other networks shall be screened by the EO firewall.

7.2 Non-EO Networks

The Non-EO Networks are ESA networks outside EO's administrative control. Examples of such networks can be, but are not limited to:

- ESA External Services Networks,
- ESA Internal Services Networks,
- FOS DMZs (internal and external), etc.

All communication between Non-EO Networks and EO DMZs and EO Internal LANs, shall be screened by the EO Firewalls.

7.3 EO centres

7.3.1 Demilitarized Zones

A demilitarized zone refers to a perimeter network that can be a physical or logical sub-network containing systems that expose services to a network of lower security class. Likewise it may offer screened and restricted access to services residing on networks of another security class. Currently the following EO DMZs are defined:

- The External ICT Services DMZ
- The DAP DMZ
- The Legacy DMZ
- The Level-1 (Restricted-Trust) DMZ
- The Level-2 (Interconnection) DMZ
- The Level-3 (Inter-Trust) DMZ
- The Management DMZ

Traffic to and from these DMZs is screened and policed in both directions. Each of these DMZs serves a particular purpose and/or community. They have each a different security grading. (See sections 8.3.1 – 8.3.7) The baseline network security policy is provided in section 9.

7.3.2 EO Internal Networks

The EO Internal Networks are networks where systems and services are hosted that require a higher protection then systems on the DAP DMZ and which do not need direct access to the Internet. Currently the following EO Internal networks are defined:

- The Internal ICT Services LAN
- The Internal Project and Services LANs.

Communication between these internal networks and EO networks of another security class, is ruled and controlled by the EO Firewalls. Traffic to and from these LANs is screened and policed in both directions. The baseline network security policy is provided in section 9.

8 IMPLEMENTATION OF THE EO NETWORK SECURITY POLICY

The EO Network Security Policy is implemented through the following security controls:

- EO Firewalls
- EO Security Belts
- EO DMZs
- EO Internal LANs
- (Remote) Off-site EO Networks
- A 3-tier application approach
- Layer 2 network segmentation
- EO Remote Access Services
- Centralized general networks services
- Single sign-on
- IDS/IPS
- DDoS defense
- Proxy
- EO Network Security Baseline Services
- EO Network Security Delta Services

Each of these security controls are discussed below.

8.1 EO Firewalls

An important security control through which the EO Network Security Policy is implemented and enforced, is the EO Firewall.

Note that the term “firewall” does not necessarily refer to the physical firewall infrastructure elements. The EO Firewalls are to be seen as a security architecture composed of several physical devices that are able to segment networks in different security domains, to implement traffic screening in all directions and enforce access restrictions between EO networks of different security classification.

An EO Firewall may screen network traffic originating at the same or from another physical geographical location. An example of the latter can be an EO internal network at an EO centre that communicates through the WAN with an EO DMZ at another EO Centre.In such case it is necessary that the EO Firewall and the remote EO network are connected via a network link that does not change the security class of the screened network along the way. Encryption of the link is desirable but not mandatory.

8.2 EO Security Belts

EO Networks of the same security classification and nomenclature that are deployed at different EO Centres have full connectivity amongst each other by default.

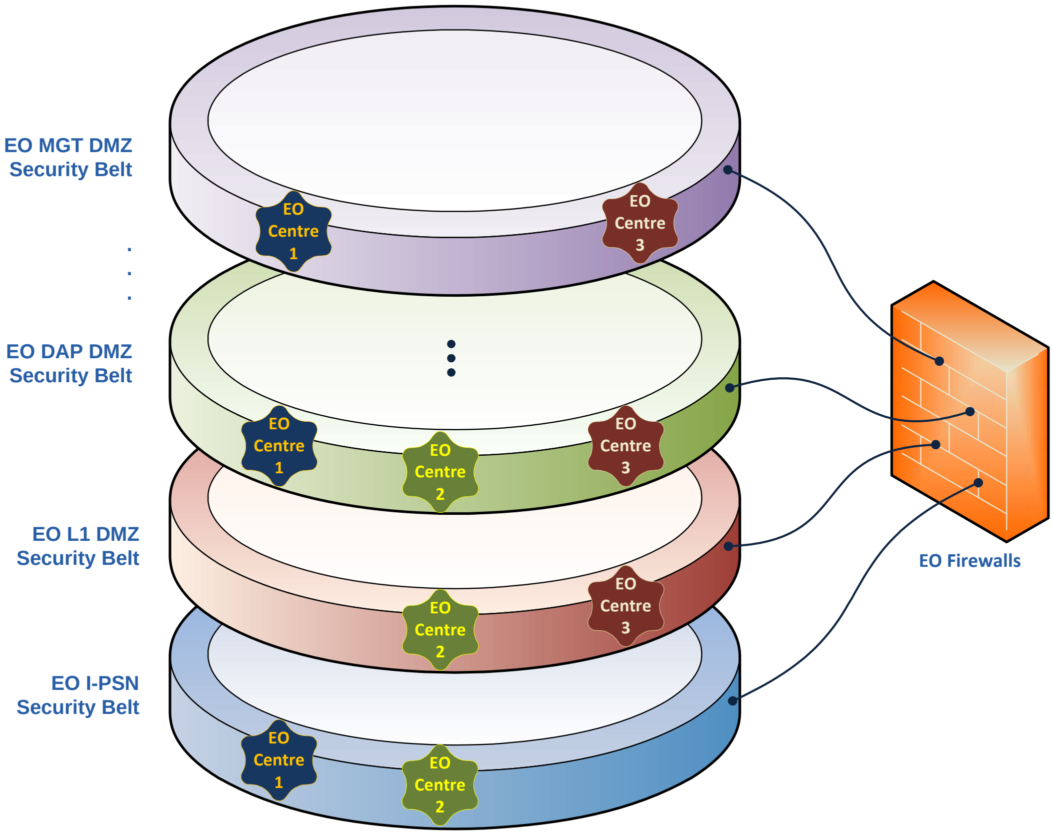

Figure 3 - EO Security Belts Conceptual Example

Note that:

- Security Classification refers to the EO network types described in section 7.
- Nomenclature refers to the different network types inside the main security classes that are discussed in sections 8.3 to 8.8.

Concretely, this means that there are no traffic restrictions for EO networks in the same security belt, irrespective of where these EO networks are physically located.

8.3 EO Demilitarized Zones

DMZs are another means to improve network and service security by placing systems, applications and services in a DMZ that protects them best according to their connectivity requirements.

Projects and support teams need to understand the differences between the different EO DMZs in order to architect, develop and deploy their systems and services in line with the EO Network Security policy.

Following sections explain the different types of EO DMZs available together with their typical use.

8.3.1 E-Serv DMZ (External ICT Services DMZ)

This DMZ hosts only supporting ICT services that are necessary for all EO networks and systems. An External ICT Services DMZ is deployed at least in one EO centre (ESRIN) and may be replicated at other centres if the need arises; for instance for business continuity and disaster recovery purposes. All EO networks shall use the common ICT services deployed in this DMZ in case they require the provided functionality.

The services provided to the external EO networks, are:

Group 1:

- DNS (future)
- NTP services (future)

Group 2:

- SMTP mail relay services
- Lotus Notes mail services

Group 3:

- Proxy services
- Application gateways

The services groups are segmented according to the scheme described in section 8.7 after consultation and agreement with the EO-NSO.

Strict traffic restrictions do apply on this DMZ, according to its baseline security policy – see section 9.4. By default, SDSR’s are not granted for systems and services deployed on this DMZ – see section 8.15. If connectivity requirements change, the security baseline is to be amended. However, this is only possible after entering a Change Request and/or Evolution activity. The new security baseline is to be approved by the EO-NSO. An EO-

SDSR will only be a temporary means to bridge the period from requirement to acceptance and update of this document.

8.3.2 DAP DMZ (Data Access Portal DMZ)

A DAP DMZ is deployed at least in one EO centre (ESRIN) and may be implemented in other centres if the need arises.

Systems and services that need to be accessed from anywhere on the Internet, are to be placed on the DAP DMZ. Examples can be, but are not limited to:

- web portals
- file and data exchange servers
- product catalogues front-ends
- on-line product ordering front ends
- customer and user registration front-ends
- authentication front-ends
- data dissemination servers
- Presentation/tier-1 systems (see Section 8.6)

Systems and services deployed on this DMZ shall only store public non-sensitive data and information. Data classification details are reported in [AD4]

All systems and services shall be deployed on registered ESA DAP DMZ public IP addresses ranges and shall always have an up-to-date forward and reverse DNS entry in the EO DNS. DNS resolution for these systems shall be available from any public accessible network.

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.5.

8.3.3 Legacy DMZ

This EO DMZ is optional and only required in case existing legacy services are deployed at the EO Centre that are agreed not to be migrated. This DMZ is intended to be decommissioned over time when all hosted legacy systems and services have been decommissioned or migrated.

The Legacy-Freeze DMZ is intended to support existing systems and services that:

- support on-going missions
- provide services to the internal and external user communities that cannot be amended until decommissioning

By default, all existing network connectivity is maintained without any modification. Changes to the network architecture, extensions and additions to the existing DMZ are not allowed, nor supported

In case the EO legacy systems and services are deployed on the DAP DMZ, they will be shielded from the rest of the DAP-DMZ, using the approach described in section 8.7. The existing connectivity with DAP systems will be still guaranteed.

Newly deployed systems and services designed after the release date of this policy document are not supported on this DMZ. Instead all evolutions necessary to maintain the currently provided services will be supported in the Legacy DMZ.

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.6.

8.3.4 Level-1 (Restricted-Trust) DMZ

A Level-1 or “Restricted-Trust” DMZ is deployed in at least one EO Centre and may be implemented in other centres if the need arises.

In general, this DMZ hosts server-type systems and services that can only communicate with well identified peers on the EO DAP DMZ, the ESA networks, the Internet etc.

- Services and systems with specific communication needs with public addressable peers.
- Non-general purpose ICT services for EO that are supporting the entire EO user community.
- Systems and services that require an enhanced level of network security protection.
- Tier-2 systems (see Section 8.6)

General purpose workstations and client systems are not allowed in this DMZ.

Systems and services deployed on this DMZ can only store up to public non-sensitive data and information. Examples of data that that can not be stored on this DMZ can be, but are not limited to:

- Non-local authentication credentials
- System and service management related data that is not necessary for or the result of normal operations.
- Mission critical non-public data

Data classification details are reported in [AD4]
Projects shall take this into account when designing their services.

Systems and services shall be deployed on registered ESA public IP address ranges. Every system connected to the DMZ shall have an up-to-date forward and reverse DNS entry in the EO DNS services. DNS resolution for these systems shall be available from any public accessible network

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.7.

8.3.5 Level-2 (Interconnection) DMZ

A Level-2 or "Interconnection" DMZ is deployed in at least one EO Centre and may be implemented in other centres if the need arises.

This DMZ has the sole purpose to host interconnection networks; i.e. networks that interconnect non-trusted EO networks and EO networks in a controlled and secure way.

This DMZ is fully in line with the "Interconnection Network" concept in the ESA Security Directives [RD1] and will also need to implement the concepts laid out there (i.e. point-to-point only, choke points, IDS).

The following equipment and services are typically found in an interconnection network:

- state-of-the-art remote access servers
- local authentication services
- IDS/IPS probes

This DMZ is the main vehicle to interconnect networks of different ownership and under different management. Examples can be but are not limited to:

- The DMZ hosts the EO RAS which is the main interconnection mechanism for remote service providers and partner organizations to connect specific networks at their side to specific EO networks at an EO Centre.
- The DMZ may host also other VPN end-points, PSTN, ISDN ADSL modems, access servers and services etc. that facilitate the connectivity with and from a remote party, that cannot be addressed via the EO RAS services.

This DMZ is not used for:

- hosting end-user systems
- IP interconnections with other ESA networks that are routed over the normal ESA Intra -or Internet access and for which no additional authentication and/or screening are required.
- any other services then the ones mentioned above.

The different interconnection networks are separated from each other in this DMZ, using the approach described in section 8.7.

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.8. For the moment only RAS access baseline has been defined. Any other connection type (see sections 8.5.3 and 8.5.4) from this zone to the EO network will be defined case-by-case based on the connectivity matrix.

8.3.6 Level-3 (Inter-Trust) DMZ

A Level-3 or “Inter-Trust” DMZ is deployed in at least one EO Centre and may be implemented in other centres if the need arises.

In general, this DMZ hosts server-type systems and services of the following g type:

- Systems and services that act as the intermediary between well identified systems and services on the local EO Centre Internal Networks and the Restricted Trust DMZ.
- Systems and services that host sensitive data that is to be used on the EO DMZs and Internal Networks.
- Systems and services that require the strongest level of network security protection.
- Tier-3 systems

In general, server-type systems and services of the highest security classification that can only communicate with well identified peers and services on the EO Restricted Trust DMZ and EO Internal Networks and this for well identified business reasons.

General purpose servers, workstations and client systems are not allowed in this DMZ.

Systems and services deployed on this DMZ shall store only data that is necessary to fulfil its role as intermediary between the EO Centre Internal Networks and the Restricted Trust DMZ.
Examples of data that can be stored on this DMZ can be, but are not limited to:

- Authentication credentials
- Configurations
- Mission related data

Data classification details are reported in [AD4]
Systems and services shall be considered as critical and shall meet the highest security standards in the EO Networks. Consequently, before systems and services are connected to this DMZ, they shall be screened extensively in terms of best security practices with regard to Operating System, applications, operations and maintenance, staffing, data classification and treatment, disaster recovery and risks related to the communications. These best

practices are verified when the owner requests connectivity to the DMZ. Best Security Practice guidelines are found on the ESACERT web pages, CIS, NIST, vendor pages etc. If a particular EO best practice is to be followed, a Guideline and/or Procedure will be provided. (See Figure 1 in section 1.)

Projects shall take this into account when designing their services.

Systems and services shall be deployed on registered ESA private IP address ranges. Every system connected to the DMZ shall have an up-to-date forward and reverse DNS entry in the EO DNS services. DNS resolution for these systems shall be available only on the EO and ESA networks.

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.9.

8.3.7 MGT DMZ (Management DMZ)

The EO management DMZ is deployed in at least one EO centre and may be implemented in other centres if the need arises.

By default, management of EO systems and services is to be performed from this management DMZ.

This DMZ is a collection of management sub-networks. Each of these sub-networks host systems and services that manage the systems and services on the other EO networks.

Management systems and services are grouped on internal and external management sub-networks. Management sub-networks may also be grouped further according to:

- Service provider
- Project requirements
- Management services
- Access requirements

The different management sub-networks are separated from each other in this DMZ, using the approach described in section 8.7.

Management traffic runs between the management network interface(s) of the systems to be managed and the management stations on the management sub-network. Management traffic shall not be run over the service network interface of the managed system(s)/service(s). One may use separate physical and/or logical network interfaces to accomplish this.

Remote service providers can access management systems deployed on the EO Management DMZ through the Remote Access Services on the L2 (Interconnection) DMZ. See sections 8.3.5 and 8.8.

Systems and management services shall be deployed on registered ESA private IP address ranges. Every system connected to the DMZ shall have an up-to-date forward and reverse DNS entry in the EO DNS services. DNS resolution for these systems shall be available only on the EO and ESA networks.

Traffic restrictions apply on this DMZ according to the corresponding baseline security policy – see section 9.10.

8.4 EO Internal Networks

The EO internal networks host systems and services that are useful to the ESA EO user community only.

Projects and support teams need to understand the differences between the different use of EO Internal networks and DMZs in order to architect, develop and deploy their services in line with the EO Network Security policy.

Following sections explain the different types of EO Internal LANs available together with their typical use.

8.4.1 I-Serv LAN (Internal ICT Services LAN)

These LANs host only common support ICT services for systems and applications connected to the EO Internal Networks. An Internal ICT Services LAN is deployed at least in one EO centre (ESRIN) and may be replicated in other centres if the need arises; for instance business continuity and disaster recovery purposes. Networks at other EO centres shall use the common ICT services deployed in this LAN in case they require the functionality.

The services provided to the EO Internal Networks are:

Group 1:

- DNS services
- NTP services

Group 2:

- SMTP mail relay services

The services groups are segmented according to the scheme described in section 8.7 after consultation and agreement with the EO-NSO.

Strict traffic restrictions do apply on this LAN, according to the baseline security policy – see section 9.2. Should connectivity requirements change, the security baseline is to be amended. However, this is only possible after entering a Change Request and/or Evolution activity. The new security baseline is to be approved by the EO-NSO and the update is to be reflected also in an update of this document.

8.4.2 I-PSNs (Internal Project and Service LANs)

Internal project LANs are deployed in different EO Centres according to the project need.

They have the purpose to provide an environment that groups all project and/or service related systems and applications in their own secured internal LAN. Inside the project or service LAN, communication is free. But communication with other networks is restricted according to the baseline security policy. See section 9.3.

Examples of EO internal project and service LANs can be, but are not limited to:

- EO internal services
- data processing, archiving, distribution, handling, quality control
- mission and production planning
- application development, testing and release
- hosting and processing of sensitive EO data
- EO internal user services
- EO internal support services (helpdesk, order handling, quality control, statistics and reporting, etc.)
- general purposes workstation clients
- operator consoles

The different project and service LANs are separated from each other, using the approach described in section 8.7 after consultation and agreement with the EO-NSO.

All systems and services on these internal LANs, shall be deployed on registered ESA private IP addresses ranges and shall always have an up-to-date forward and reverse DNS entry in the EO Internal DNS. .

8.4.3 Staging area

This area allows preparing systems before they can be operationally connected to the EO security zone, where:

- applications can be finally integrated and tested in their target environment
- the systems security plan can be prepared.

The staging area is a layer 2 subnet (see section 8.7), completely isolated from all productions subnets (internal and external) and from other staging areas.

The staging area baseline is to block all traffic by default except for:

- Internet connectivity via the HTTP proxy located in the E-Serv
- DNS resolution, if required
- Specific traffic documented in a traffic matrix and agreed with the EO NSO.

The requested connectivity will be granted for the necessary time period over this area..

It is not necessary to submit an SDSR. A request shall be submitted to the EO Security Officer.

8.5 (Remote) Off-Site EO Networks

EO has the requirement to allow external 3rd parties to support EO activities from an agreed location that is not necessarily an EO Centre. Likewise, collaborations between ESA and external parties may require deployment of an EO network at a remote site or the interconnection of the EO network to other networks.

By default, remote networks are considered external Networks and the corresponding security baseline applies.

In the following cases, the remote off-site networks belong to one of the following EO Network classes:

- New EO centre
- Remote Access facility (RAS node)
- Hosting/housing/outsourcing providers (external service provider)
- Space community partners (scientific or government organization)

The policy to support these set ups is discussed below.

8.5.1 EO centre

An EO centre is a facility directly connected to the EO network that hosts an EO network extension under the direct control of EOP.

This EO node implements one or more of the security zones described in sections 8.3 and 8.4 and comply with the related baselines (see Section 9).

The centre is managed by an operator who has signed a specific contractual agreement with ESA.

8.5.2 Remote Access facility

In this scenario, an EO network of a specific security class (internal, DMZ) is extended to a remote location to allow remote maintenance activities over EO systems. The Remote Access Service is described in Section 8.8.

Current RAS sites are:

- HP-EDS
- Serco Frascati Office
- Advanced Computer Systems (ACS)
- ElsagDatamat

The RAS solution implemented at each site is described in [RD10]

The procedure and requirements for connecting and/or extending these remote networks to an EO network of a specific security class is decided on a case-by-case basis by the EO-NSO.

Following elements may be enforced by the EO-NSO:

- An Interconnection Agreement is to be prepared and signed off between the interconnecting parties. The EO Network Security Officer and ESA Security Office need to confirm the interconnection agreement.
- An audit is performed by a party appointed by ESA in order to verify compliance. The audit shall be performed as agreed in the Interconnection Agreement. Note that the audit addresses both the off-site EO network side as well as the side at the EO Centre.
- The remote off-site network is considered an extension of the EO network and hence the same security baseline policy applies.
- The remote off-site network does not have any other network connectivity.
- The remote off-site EO network is connected to the on-site EO network via a protected link[1].
- The off-site remote EO network can be of one security class only.
- If the remote party hosts EO networks of different security classes, they shall be at least separated logically and they shall be connected via separated protected links.

Depending on the situation, the EO-NSO may decide to add other requirements in addition to the above or replacing them.

The RAS baseline policy is detailed in Section 9.8.

[1] A protected link can be implemented either via encryption over public network (e.g. VPN over Internet) or via a dedicated private link (e.g.: direct link, MPLS)

8.5.3 Interconnection with External Service Provider

Some EO services may be outsourced, hosted or housed by an external industry, named in the following as Business partner.

In this case the business partner network is not an EO network extension and:

- it may connect to EO network for data exchange
- it may offers service to end users on behalf of ESA

Examples are, but not limited to:

- NETCETERA that host some ESA web services,
- Infoterra that supports operations of the GMES-SCI service

The procedure and requirements for connecting these remote networks and authorizing the service provision on ESA behalf is decided on a case-by-case basis by the EO-NSO.

Following elements has to be considered by the service provider:

- Risk assessment of the threats posed to the Provided Service, ESA and third parties
- Implementation of the security measures necessary to cope with the assessed risks (like network segmentation, authentication/authorization measures, systems hardening, intrusion prevention, link encryption, etc.)
- An Interconnection Agreement to be signed off between the interconnecting parties. The EO Network Security Officer and ESA Security Office need to confirm the interconnection agreement.
- Specific network and system requirements imposed to the business partner network based on the provided service needs and risks. The requirements are agreed and subscribed in the Interconnection Agreement;
- An audit is performed by ESA or a third party appointed by ESA in order to verify compliance. The audit shall be performed as agreed in the Interconnection Agreement. Note that the audit addresses both the off-site network side as well as the side at the EO Centre.

Depending on the situation, the EO-NSO may decide to add other requirements in addition to the above or replacing them.

This kind of partners will be connected through the L2 DMZ. The security baseline for this type of end point is to block all traffic by default except for network flows approved and agreed with the EO NSO[2] and documented through a connectivity matrix in the Interconnection Agreement.

[2] This baseline will be standardized if a common set of communications services and requirements is identified for this kind of interconnection.

8.5.4 Interconnection with a Scientific/Government Partner

Typically, this situation arises when collaboration is established between ESA and an external organization. Examples can be but are not limited to:

- NASA
- JAXA
- ASI

The procedure and requirements for connecting these remote networks is agreed with the partner organization on a case-by-case basis, approved by the EO-NSO and documented in an Interconnection Agreement signed off between the interconnecting parties.
The EO Network Security Officer and ESA Security Office need to confirm the interconnection agreement.

This kind of partners will be connected through the L2 DMZ. The security baseline for this type of connectivity is that all traffic is blocked by default. All necessary connectivity has to be specified in a traffic matrix (documented in the Interconnection Agreement) and is implemented case-by-case.

8.6 A 3-Tier Application Approach

Services that are offered to the Internet community and which meet any of the following conditions:

- require authentication
- require database access
- require middleware services
- process or require the use of sensitive information

are required to agree on the architecture and design with the EO-NSO before deployment (see [AD4]).

These kinds of services and applications are typically to be deployed according to a 3-tier approach. In summary, this entails:

1. a “Presentation Tier” (also known as Tier-1), deployed on a DAP-DMZ project or service subnet.

   This tier gives the user access to applications through a front-end (G)UI; e.g. a browser. This is the layer were front-end related scripting and mark-up languages are used. It also implements a first layer of sanitation and scrubbing of all user input provided though the applications in order to minimize abuse.

2. a “Logic” or “Application Tier” (also known as Tier-2), deployed on a L1 (Restricted-Trust) DMZ.

   This tier addresses the necessary logic process to be applied upon or with the user provided input to satisfy the request. It also provides translation or brokering of the user requests to the back-end, implements mediation between the front-end and the back-end and implements sanitation and scrubbing of the request offered to the back-end. This tier acts as a server for the user requests coming from the presentation tier and acts as client to the data tier to obtain the necessary data. This is the tier where object and rules are defined and programming takes place.

3. a “Data Tier” (also known as Tier-3), deployed on a L3 (Inter-Trust) DMZ or I-PSN.

   This tier stores the data to be accessed and provides access to the various databases and kinds of sensitive data. On this tier, one will find all kinds of database query programming languages and communications. These data and databases may be hosted on systems directly deployed on the L3 DMZ or on an EO internal project or service subnet.

The above serves as a well-known and best security practice example of a multi-tier approach. Depending on the application, one may define less or more tiers.

Wherever possible, projects shall take into account this multi-tier approach in architecting, designing and deploying their services and applications from the initial phase of the project.

8.7 OSI Layer 2 Network Segmentation and Protection

8.7.1 OSI Layer 2 Network Segmentation

Each of the main types of EO networks (see section 6 and 7, 8.2 and 8.4) are segmented into sub-networks along boundaries that shield these sub-networks from others that may be deployed inside the same main EO network.

This segmentation may be implemented to group systems and services belonging to the same:

- Project
- Application - Service

- Provider
- Access requirements
- Security requirements

This segmentation is implemented at Layer-2 of the OSI network model, using state-of-the art network equipment.

By default, there is no communication between the several sub-networks on the same main EO network type, unless there is a specific communication need. The latter will be granted.

8.7.2 OSI Layer 2 Protection

By default all EO networks shall implement Layer-2 port protection at the network switches to avoid abuse of and attacks to VLANs, trunks, MAC and IP addresses, DHCP services, CAM tables, ARP etc.

Hubs are not allowed on the EO Networks.

8.7.3 Network Connectivity

Systems can be connected to the EO networks only when the network connectivity has been requested to the service desk and when they have allocated the switch port. When the switch port is active, the system needs to assure that the IP address and the DNS entries are immediately properly configured.

A Layer-2 subnet can be requested to the service desk. The request is to be approved by the EO Network Security Officer. A procedure is to be put in place for handling such requests.

8.8 EO Remote Access Services

There is a business need to interconnect off-site remote networks with EO networks for remote maintenance purposes (See also section 8.5). For this reasons, EO provides Remote Access Services.
Remote access facilities described in 8.5.2 have been implemented to provide this service.

The EO RAS are implemented in the L2 (Interconnection) DMZ.

Remote Access to the EO networks is currently provided in two ways:

- A LAN-to-LAN connection
- A remote client to EO LAN connection

The high-level concept is shown in Figure 4 below.

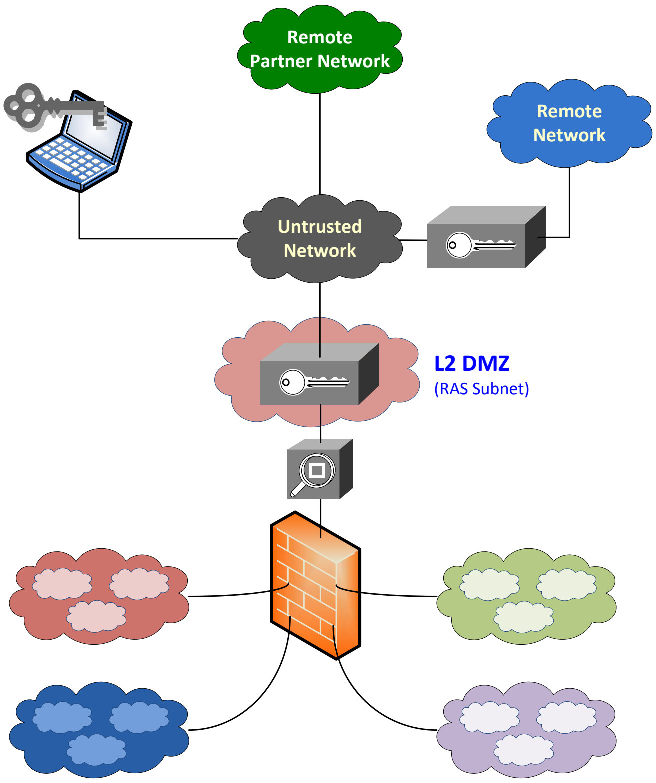

Figure 4 - EO Remote Access Services concept

Both types of remote access scenarios are subject to the following common policy:

- Traffic between the remote side and the EO network may be transmitted over an untrusted network; e.g. the Internet.
- Traffic in transit between the two sites shall always be encrypted.
- Traffic arriving at the EO Centre shall first be decrypted and then be screened by an Intrusion Detection Service before being screened by the EO Firewall.
- Traffic leaving the EO Centre shall first be screened by the EO Firewall; then it will be screened by an Intrusion Detection Service before it is encrypted and sent to the remote site.
- By default, the baseline security policy described in section 9.8 is applied on the EO Firewall.

The common policy that applies to all the EO RAS services is augmented with a specific policy for each of the scenarios.

8.8.1 EO RAS LAN-to-LAN Connection

Besides the common EO RAS policy, described above, the following specific policy for LAN-to-LAN EO RAS connections applies:

- This remote access scenario connects a remote 3rd party LAN to an EO network of one specific security class. The latter can be an EO internal network or an EO DMZ.
- The remote 3rd party LAN becomes a screened extension of the EO network to which it connects.
- The remote 3rd party LAN and the EO network to which it connects have the same security classification.
- Besides the connection to the EO network, the remote LAN shall have no other connections.
- The connection between the remote LAN and the EO network is established through an up-to-date, industry best practices VPN service that protects all traffic between EO dedicated VPN end-points at either side of the link.
- By default, the VPN Service is provided by ESA at both ends. However, other 3rd party VPN services may be used as long as there is an agreement with the EO-NSO.
- All traffic that is not intended for local systems on the remote LAN is routed through this dedicated VPN connection to the EO Firewall, where it will be screened and routed.
- Any system on the remote 3rd party LAN is allowed to connect to any system on the EO LAN of the same security classification, as long as it is a business related activity that is within the scope of the work trusted to the remote 3rd party.
- The EO Project Manager or EO Customer Representative, responsible for the activities of the remote 3rd party and the EO Network Security Officer shall approve the deployment of an EO LAN-to-LAN RAS connection.

8.8.2 EO RAS Client-PC Connection

Besides the common EO RAS policy, described above, the following specific policy for PC Client-to-LAN RAS connections applies:

- This remote access scenario connects a remote client PC to systems connected to an EO network of one specific security class.
- In terms of security classification, the client-PC becomes as such the same as any other system on the EO network to which it connects.
- The client PC is allowed to connect to any system on the EO network as long as it is a business related activity that is within the scope of the work trusted to the user of the client PC.
- At the time of the connection, the remote client PC is only connected to the EO network.
- The connection is established through an up-to-date, industry best practices Client VPN service that encrypts all traffic between the remote client PC and the EO dedicated VPN end-point at the ESA Site.
- Strong authentication is mandatory for the client PC when setting up the VPN connection to the EO dedicated VPN end-point. For EO, PC Client RAS strong

authentication implies the use of an RSA hardware token that will be provided by ESA, after the request has been approved.

An EO guideline can be provided to the remote party which explains the security requirements expected to be in place at the remote PC.

8.9 Centralized General Network Services

In order to improve security and management of common IT services have been grouped together and put on a specific network segment (E-Serv DMZ and I-Serv LAN).

The services made available, are described in section 8.3.1 and 8.4.1. In summary it concerns following services:

- EO DNS servers for **DNS resolution**:
  - ESA Corporate DNS at ESRIN is authoritative for eo.esa.int domain and serves systems on the external DMZs (DAP, L1, E-Serv)
  - Two Internal EO DNS servers reside on the I-Serv to offer a resolution service to internal systems only (I-PSN, L3 and Management LAN). Internal systems thus are able to solve internal names directly and external names via the ENVISAT DNS relay or Corporate DNS that will act as forwarders as well towards Public DNS.

- EO NTP servers for **NTP synchronization**:
  - ESA Corporate provides an NTP source on a ESA ESN
  - Each EO mission/project that needs an NTP service has the following possibilities:
    - implement its own NTP service in the I-Serv DMZ that will serve all the Mission PDGS/ project;
    - leverage on the NTP service provided by the EO NTP server located in the I-Serv and synchronized with the ESA Corporate NTP
  - DMZs servers can connect to the Mission/project NTP server or the EO NTP server, both located in the I-Serv.

- EO mail relays for relaying any SMTP mail. These **EO mail relay**:
  - Inbound mail arrives from the corporate E-mail servers and is relayed to the final EO system
  - Outbound mail arrives from an EO system and is relayed via the corporate E-mail servers to the final destination.

- **EO email services** for EO operators:
  - Email services for operators are provided by two Lotus Notes servers (*Eopnotes*) residing in the E-Serv DMZ
  - The EOPnotes servers communicate with the ESA Corporate email system to enable email exchange for the EOP operators.

- **EO proxies** to allow internal systems to access http and ftp resources on non-EO networks.

- EO web reverse proxy that will serve as a front-end from non-EO networks and relays the HTTP(S) and possible tunnelled CORBA and SOAP requests to the EO web servers on the DAP and L1 DMZs (future implementation).

By default, all EO systems are expected to configure their systems to make use of these centralized network services unless agreed differently with the EO-NSO. The use of http/ftp proxy in particular is granted to internal systems that cannot access directly the Internet.

The network security baseline services are taking the use of these centralized services into account. The EO Firewalls are configured to enforce this policy. Only in specific cases where the use of these services is not possible, deviations may be granted via an SDSR (section 8.15) or via a waiver (section 8.16).

8.10 Earth Observation Web Single Sign On

The EO SSO framework is introduced to provide a single sign on process for EO web applications. Integration of web application/services into the EO SSO framework is expected to take place incrementally by all EO existing Web applications/services and to be deployed by default for new Web applications/services. Related documentation can be found in [RD11] and [RD12].

EO SSO Service Providers (typically Web Applications/Services containers) shall install a predefined CFI (EO SSO CAS Checkpoint available for the Apache web server).
The EO SSO CAS Checkpoint shall be customized by Service Providers to:
a. establish a secure and trusted connection (via digital Certificates)
b. be able to "outsource" the Authentication process to the EO SSO Identify Provider component located in the L1 DMZ.
EO Service providers shall be able to inter-connect from their location (Source: Internet, DAP, ISN and Off-Site EO networks) to the L1 EO SSO IDP using https/soap as defined in the following.

The baseline for EO Service Providers is the following and it is reported in the reletad baselines (Section 9).

Service	Source	Destination	Protocol	Port
End user authentication	Any	EO-SSO-IDP	HTTPS	TCP/443
EO-SSO-CAS module access to EO-SSO IDP	EO-SSO-CAS	EO-SSO-IDP	SOAP over SSL	TCP/8110
SP access to EO-SSO IDP	EO-SSO-CAS	EO-SSO-IDP	SOAP over SSL	TCP/8104

Table 8-1: EO Web SSO baseline

8.11 IDS/IPS

A managed Intrusion Detection/Prevention System Service (IDS/IPS) is provided to protect EO networks and applications from threats such as:

- An intrusion attempt
- The transmission of malicious code
- Backdoor activity
- Network based threats.

The IDS/IPS monitors and inspects traffic flows related to:

- DAP DMZ
- L1 DMZ
- L2/RAS DMZ

- E-Serv DMZ.

The IPS/IDS can work contemporarily in two modes:

- prevention over a specified set of servers
- detection only over another set of servers

Whenever a malicious activity is detected in **prevention** mode, the IPS:

- notify the Interoute Security Operation Centre (SOC) with alerts according to the detected event
- notify the specified ESA representative
- take actions, like block, ignore, log, quarantine, etc according to the configured action/alarm severity combination.

When “Blocking” action is configured, only packets matching specific signatures are dropped (thus any subsequent valid attempt is allowed, without disrupting legitimate traffic).

When “Quarantine” action is configured, specific traffic based on source and/or destination and/or protocol port is blocked. This kind of action is used to prevent attacks that are recognised only by correlating several flows (e.g. UPD flooding).
The quarantine reverts to default when the threat is over or is manually unblocked. The manual unblocking can be requested by the identified ESA representative using the Service Provider ticketing system.

The identified ESA representative is always notified whenever some kind of traffic is blocked or quarantined.

Default severity levels for signatures and associated actions are fine-tuned by the Service Provider together with ESA technical responsible of each domain during the learning phase.
The tuning process allows defining baseline traffic and reducing the level of false positive/negatives.

The IDS/IPS is configured to operate in **detection** mode over special type of traffic that should not be automatically blocked.
In this case alerts generated by the IDS are displayed in real-time in the SOC, where alarms are assessed and assigned a severity level (low, medium, high or critical) depending on the type of attack, age, threat and impact of the attack.
This assessment will determine the action taken by the SOC, the response time and notification method (phone, email, sms) to the identified ESA representative.

Business Impact	Event Description	Action Taken by the SOC

Low	No direct threat, but may contain information indicative of intrusive activity	Store for a period of time for forensic purposes. Analysis may provide details essential to identify source address or timelines of attack.
Medium	A malevolent packet (a deprecated attack or intrusive enumeration) sent to the target, which represents no direct threat to operation. A medium alert would not impact the operation or the logical access controls of a system.	Post event analysis and review by security engineer. Trend analysis and correlation with other events.
High	Attack on the target, representing a real potential threat and having an impact on the availability or security of a systems and its data i.e. Service interruption, data integrity loss or data exposure, injection of malicious code or software, etc.	Event analysis by security engineer and action taken to stop or reduce the threat and prevent further attack. Target must be analysed to identify if it was compromised.
	Significant evidence of ongoing actual system compromise. Multiple high events corroborated by supporting system evidence (i.e. defaced website, system unavailable or maxed bandwidth/cpu).	Immediate escalation to the ESA representative.

Table 8-2: Response policy for IDS identified threats

The IPS/IDS system is directly connected to the Service Provider management network.

When the IPS/IDS device fails, it will behave like a physical short circuit, allowing all traffic to flow without disrupting the service.

A Host Intrusion Prevention system is also in place to protect file system integrity and monitor suspicious activities on deployed systems over all DMZs and internal network. The HIPS management system is located in the EO Management LAN where it collects logs and status information. The management system can take actions on system to block identified attacks and threat. The HIPS system is controlled by the system administrator that decide if and what action to take, in agreement with the EO technical responsible of the system. No automatic actions can be configured or allowed towards controlled systems.

8.12 DDoS

DDoS or Distributed Denial of Service is a form of attack on the network where a hacker(s) attempts to make a network resource(s) unavailable to its intended users.

The EO network is protected via a DDoS protection system. The traffic is monitored 24/7 and can react to new attacks in real time.

The system is placed in learning mode at a periodic schedule for a set time (4 hrs every 6 months), to build a baseline traffic database to detect anomalies in case of an attack. This process is followed for every EO publicly addressable subnets (i.e. EO DMZs). The baseline traffic can be defined for set of servers within each DMZ.

The DDoS device monitors all ongoing customer traffic, flagging an alert to the Service Provider NOC (Network Operation Centre) when anomaly is detected. The NOC will then analyze the anomaly, which if considered genuine will lead to the following:

- Contact the ESA representative via email or phone, based on type of attack and severity (as defined in the ESA profile)
- The Zone under attack will be manually put into 'Protect' mode. This will be triggered only by ESA consent – The ESA representative is required to phone the NOC to initiate and authorize the action.

In "protect mode", traffic identified as anomalous will be diverted, while traffic for all other destinations will remain in the same paths without being diverted.

The DDoS device analyzes the diverted zone traffic in search for anomalies and identifies an anomaly when the flow violates the policy threshold. A set of dynamic filters are then created by the guard that continuously adapt to the zone traffic and type of attack. Filters can operate at single IP granularity level , allowing to filter only the malicious traffic and inject back towards the final destination the cleaned traffic.

When an attack is detected, mitigation starts within two minutes and full protection will normally be in place within 3-5 minutes.

The zone is manually set to "unprotect" once the filters are no longer in use (the attack is terminated) and the ESA representative will be informed.
The traffic will be returned to the normal routing path within one hour of attack termination.

8.13 Proxy

Two types of proxy are currently enabled:

- http proxy (*eomailesr1* and *eoproxyesr3*)
- ftp proxy (*eomailesr2*)

The http proxy is reachable on port 3128 and it forwards connections only on a set of ports specified in the baselines (Section 9).
Its main purpose is to allow software updates of internal systems that are not allowed to access the internet directly (such as I-PSN, I-Serv, MGT and E-Serv).
An access control list filters the subnets allowed to use it.
Basic filtering, based on regular expression ACL, is applied to block contents belonging to the following Internet categories:

- Internet Radio and TV
- Adult content
- Gambling
- Illegal Peer-to-Peer File Sharing
- Social networking
- Web chat

- Personal webmail
- Message Boards and Forums
- Streaming Media.

The http proxy is provided in a high availability configuration.
The http proxy shall not be used as a reverse proxy.

The ftp proxy can be used by all internal subnets for specific operational reasons. No filters are applied on this proxy except for IP filtering provided by the local host-firewall.

8.14 EO Network Security Baseline Services

EO Network Security Baseline Services are network services that are the default traffic screening rules implemented on the EO Firewalls to police the traffic between the directly or indirectly connected systems and networks of different security classes.

The baseline services are available and applicable to all systems, services and users without the need for requesting the connectivity.

The EO network security baseline services are specified in Section 9 and this for each EO network of a specific security class.

8.15 EO Network Security Delta Services

Connectivity requirements that are not covered by the EO Network Security Baseline services need to be requested through a EO-SDSR.

An EO-SDSR is assessed by an EO-NSO appointed security entity. Based on the security assessment and other business and/or project related requirements that are brought the attention of the EO-NSO, the EO-SDSR may be approved or denied.

In general, requesting EO-SDSRs is strongly discouraged. Usually, the request is the result of a service definition or architecture that has not taken into account the EO Network Security Policy and its implementation. Therefore, before anything else, EO projects and users are requested to consult the policy documents and verify with their experts how the design and architecture can modified to avoid requesting an EO-SDSR.

This document will be periodically updated to accommodate new and changed business needs identified from the different projects and to include into the baseline the secure approach identified to take them into account.

The EO SDSR procedure is detailed in [RD8], the EO SDSR template is provided in [RD9].

8.16 EO Network Security Waiver

If it is impossible to connect a system to the EO networks according to the EO G/S Security Policy [AD1] or its implementation (this document), a waiver can be requested to the EO-NSO.

Besides the administrative details, this waiver needs to provide sound justifications, technical details and liability statement for risks and costs related to implement the waiver and recovery handling after an incident due to a waived service/solution. The EO Network Security waiver template [RD4] is to be used.

The waiver needs to be signed by EO management and the EO Network Security Officer and its validity period is not longer then 1 year after which it is to be decommissioned or renewed.

A waiver [RD4] is to be used with caution and should never serve as a way to bypass the EO Network Security Policy or its implementation (this document).

9 EO NETWORK SECURITY BASELINES

In the following sections the network security baselines are presented for the different EO networks – see sections 6, 7 and 8.3 to 8.4.

9.1 Common Network Security Baseline

- The EO Network Security Baseline consists of the following:

  1. A network security baseline identifier.
  2. An indication of a source network and the source system(s) on the network
  3. An indication of a destination network and the destination system(s) on the network
  4. The application protocol and the underlying transport protocol
  5. For TCP and UDP based connections the allowed source and destination ports.
  6. Notes that accompany the baseline rule

- The security baselines defined in the following sections are valid for all systems in the same security belt, irrespective of their location – see section 8.2.

- Only traffic from the source initiated to the destination is mentioned in the baseline. Return traffic related to the same communication is assumed to be allowed by default. (This is in line with the state-of-the-art Firewall technology.)

- Communications not mentioned in following sections and tables are not part of the baseline and hence are blocked.

- Inside a main network security class, EO Networks can be segmented at OSI Layer 2 (See section 8.7). Routing between these subnets is not enabled by default. Routing between these Layer-2 subnets can be enabled on a need-to-have basis and after filing a CR and approval of the EO Network Security Officer.

- In the security baseline tables below, connection can be specified for:

  - **Any:** the baseline policy applies to any system on the specified EO network

  - **Single:** the baseline policy applies only to a single registered system on the specified EO network. No EO-SDSR is required though, but the Firewall rules are to be configured from/to this single system. It is at the discretion of the EO Network Services operations team to implement this in the most efficient manner and to group rules as much as possible to avoid impact on the Firewall performance.

- None of the protocols are to be used as permanent connections or tunnels for traffic that is not documented, approved or has the purpose to bypass the EO Network Security Baseline; e.g. it is not allowed to set up connections to EO systems on the I-PSN from a non-EO network through SSH or HTTPS tunnels.

- When references are made to SSH in the following tables, it includes SFTP and SCP as they are different applications of using the same SSH protocol.

- In the following tables, SOAP is included in the security baseline for HTTP(S) as it is tunnelled over these protocols.

- Management traffic runs between the management network interface(s) of the systems to be managed and the management stations on the management sub-network. Management traffic shall not be run over the service network interface of the managed system(s)/service(s). One may use separate physical and/or logical network interfaces to accomplish this.

- It must be noted that SOAP protocol is allowed based on a waiver that temporarily permits its use until a new SOAP proxy/firewall will be in place. After that, SOAP will be screened and policed by this proxy and the policy will be updated accordingly.

- Following sections detail all baseline rules associated to each network zone. The baseline rules are grouped on source network basis, e.g. I-Serv security baseline collect all rules from the I-Serv towards the rest of the networks.

- Each baseline set is identified by the tag <source-network-name> / <destination-network-name>.

- Each network baseline identifier is formatted according to the following scheme:

  <source-network-name>><destination-network-name>#*nn*

  where *nn* is the progressive identifier of the requirement object

The following abbreviations are used to identify the source/destination network:

External ICT Services DMZ	**E-Serv**
The DAP DMZ	**DAP**
The Legacy DMZ	**Legacy**
The Level-1 (Restricted-Trust) DMZ	**L1**
The Level-2 (Interconnection) DMZ	**L2**
The Level-3 (Inter-Trust) DMZ	**L3**
The Management DMZ	**MGT**
The Internal ICT Services LAN	**I-Serv**

• The Internal Project and Services LANs	**I-PSN**
• ESA External Services Networks	**ESN**
• ESA Internal Services Networks	**ISN**
• Internet	**EXT**

Appendix B shows an overall baseline traffic matrix, that highlights all baseline rules applicable to each specific source-destination flow.

9.2 I-Serv LAN Security Baseline

I-Serv DMZ Security Baseline

ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
I-Serv>I-Serv							
I-Serv>I-Serv#01	I-Serv/DNS Servers	I-Serv/DNS Servers	DNS	TCP, UDP	53	53	(1)
I-Serv>I-Serv#02	I-Serv/NTP Servers	I-Serv/NTP Servers	NTP	UDP	123	123	
I-Serv>I-Serv#03	I-Serv/SMTP Servers	I-Serv/SMTP Servers	SMTP	TCP	25	25	
I-Serv>E-Serv							
I-Serv>E-Serv#01	I-Serv/SMTP Servers	E-Serv/SMTP Servers	SMTP	TCP	25	25	
I-Serv>E-Serv#02	I-Serv/any	E-Serv/HTTP Proxies	HTTP(S)	TCP	80, 81, 443, > 1023	80, 443	(2)
I-Serv>ESN							
I-Serv>ESN#01	I-Serv/DNS Servers	ESN/DNS Servers	DNS	TCP, UDP	53	53	
I-Serv>ESN#02	I-Serv/NTP Servers	ESN/NTP Servers	NTP	UDP	123	123	
I-Serv>MGT							
I-Serv>MGT#01	I-Serv/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(3)
I-Serv>MGT#02	I-Serv/any	MGT DMZ/single	ICMP reply	IP			(4)
I-Serv>MGT#03	I-Serv/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(5)
I-Serv>MGT#04	I-Serv/any	MGT DMZ/single	syslog	UDP	>1023	514	
I-Serv>MGT#05	I-Serv/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(6)

Table 9-1: I-Serv DMZ Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between similar network service servers at I-Serv subnets at local and remote EO Center(s).

(2) Further necessary destination ports will be added and implemented upon request. It is not necessary to submit an SDSR to use other ports. Proxy is contacted through port 3128.

(3) (3)SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(4) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the I-Serv subnets. All other ICMP types/codes from the systems connected to the I-Serv LAN are blocked.

(5) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(6) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

9.3 I-PSN Security Baseline

I-PSN Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
I-PSN>I-PSN							
I-PSN>I-PSN#01	I-PSN/any	I-PSN/any	any	IP	any	any	(1)
I-PSN>I-Serv							
I-PSN>I-Serv#01	I-PSN/any	I-Serv/DNS Servers	DNS	TCP, UDP	> 1023	53	(2)
I-PSN>I-Serv#02	I-PSN/any	I-Serv/NTP Server	NTP	UDP	123, > 1023	123	(3)
I-PSN>I-Serv#03	I-PSN/any	I-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(4)
I-PSN>E-Serv							
I-PSN>E-Serv#01	I-PSN/any	E-Serv/HTTP Proxies	HTTP(S)	TCP	80, 81, 443, > 1023	80, 443	(5)
I-PSN>E-Serv#02	I-PSN/any	E-Serv /FTP Proxies	FTP	TCP	> 1023	21, 20, 2121, 2020	(6)
I-PSN>E-Serv#03	I-PSN/Operators VLANs	E-Serv/LN Servers	LN	TCP	1352	1352	(7)
I-PSN>DAP							
I-PSN>DAP#01	I-PSN/any	DAP DMZ/any	FTP	TCP	> 1023	21, 20	
I-PSN>DAP#02	I-PSN/any	DAP DMZ/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(8)
I-PSN>DAP#03	I-PSN/any	DAP DMZ/any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
I-PSN>DAP#04	I-PSN/any	DAP DMZ/single	SSH	TCP	> 1023	22	(9)
I-PSN>DAP#05	I-PSN/any	DAP DMZ/single	SQL*Net	TCP	> 1023	1521	(10)
I-PSN>DAP#06	I-PSN/any	DAP DMZ/ GANTT Tool Servers	GANTT	TCP	> 1023	20000, 20010, 20100	(11)
I-PSN>Legacy							
I-PSN>Legacy#01	I-PSN/Exisiting	Legacy DMZ/Exisiting	Existing	Existing	Existing	Existing	(12)
I-PSN>L1							
I-PSN>L1#01	I-PSN/Operators VLANs	L1 DMZ/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30210	(8)
I-PSN>L1#02	I-PSN/any	L1 DMZ/any	HTTPS	TCP	80, 81, 443, > 1023	443, 8110, 8104	
I-PSN>L1#03	I-PSN/Operators VLANs	L1 DMZ/any	SSH, SFTP	TCP	> 1023	22	
I-PSN>L3							
I-PSN>L3#01	I-PSN/any	L3 DMZ/any	HTTPS	TCP	80, 81, 443, > 1023	443, 8110, 8104	
I-PSN>L3#02	I-PSN/single	L3 DMZ/single	LDAPS	TCP	636, > 1023	636	(13)
I-PSN>ESN							
I-PSN>ESN#01	I-PSN/single	Corp ESN/single	FTP	TCP	> 1023	21, 20	(14)
I-PSN>ESN#02	I-PSN/single	Corp ESN/single	FTPS	TCP	> 1023	21, 20, 990, 30200-30210	(8)
I-PSN>ESN#03	I-PSN/single	Corp ESN/single	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	(15)
I-PSN>ESN#04	I-PSN/single	Corp ESN/FOS LAN single	SSH	TCP	> 1023	22	(9)
I-PSN>MGT							
I-PSN>MGT#01	I-PSN/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(16)
I-PSN>MGT#02	I-PSN/any	MGT DMZ/single	ICMP reply	IP			(17)
I-PSN>MGT#03	I-PSN/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(18)
I-PSN>MGT#04	I-PSN/any	MGT DMZ/single	syslog	UDP	>1023	514	
I-PSN>MGT#05	I-PSN/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(19)
I-PSN>MGT#06	I-PSN/single	MGT DMZ/single	LDAPS	TCP	49152 -65535	636	(20)

Table 9-2: I-PSN Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between similar network service servers at I-Serv subnets at local and remote EO Center(s), if routing is enabled between the subnets.

(2) All I-PSN systems need to configure their DNS resolvers with the I-Serv DNS servers.

(3) All I-PSN systems need to be NTP synchronized. The time synchronization may leverage on the I-Serv NTP servers or on an ad-hoc NTP server if more stringent timing requirements are to be satisfied.

(4) Systems on the I-PSN can send mail via the I-Serv mail relay only.

(5) The use of the E-Serv web proxy is the default configuration for http(s). Further necessary destination ports will be added and implemented upon request. It is not necessary to submit an SDSR to use other ports. Proxy is contacted through port 3128.

(6) The use of the E-Serv FTP proxy is the default configuration for FTP file transfers.

(7) End-user mail support is via native Lotus Notes only.

(8) FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.

(9) SSH is allowed for service related communication only. System administration via SSH is to be performed from the MGT DMZ, not from the I-PSN.

(10) SQL*Net is still in this security baseline but it is intended to remove it in future policy releases. New application designs should avoid putting databases on the DAP DMZ.

(11) Any system on the I-PSN can access the GANTT Applications servers on the DAP DMZ.

(12) The connectivity configured on the Firewall between the I-PSN and the Legacy DMZ at the date of the release of this version of the policy is the Network Security baseline.

(13) LDAP over SSL/TLS. Not intended for end-user systems. End-user systems shall access an application or service on an I-PSN that will perform the LDADS request on behalf of the end-user.

(14) Direct FTP to Corporate ESN servers which cannot support proxied FTP connections.

(15) Direct HTTP(S) to Corporate ESN servers which cannot support proxied HTTP(S) connections.

(16) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(17) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the I-PSN subnets. All other ICMP types/codes from the systems connected to the I-PSN LAN are blocked.

(18) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(19) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

(20) LDAP authentication flow from systems located in any DMZ to the LDAP replica server located in a dedicated subnet of the Management DMZ

9.4 E-Serv Security Baseline

E-Serv DMZ Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
E-Serv>E-Serv							
E-Serv>E-Serv#01	E-Serv/NTP Servers	E-Serv/NTP Servers	NTP	UDP	123	123	(1)
E-Serv>E-Serv#02	E-Serv/SMTP Servers	E-Serv/SMTP Servers	SMTP	TCP	25	25	
E-Serv>E-Serv#03	E-Serv/LN Servers	E-Serv/LN Servers	LN	TCP	1352	1352	
E-Serv>I-Serv							
E-Serv>I-Serv#01	E-Serv/any	I-Serv/NTP Servers	NTP	UDP	123	123	(2)
E-Serv>I-Serv#02	E-Serv/SMTP Servers	I-Serv/SMTP Servers	SMTP	TCP	25	25	
E-Serv>ESN							
E-Serv>ESN#01	E-Serv/SMTP Servers	ESN/SMTP Servers	SMTP	TCP	25	25	(3)
E-Serv>ESN#02	E-Serv/HTTP Proxies	ESN/any	HTTP(S)	TCP	80, 81, 443, 8000-8999	80, 443	(6)
E-Serv>ESN#03	E-Serv/FTP Proxies	ESN/any	FTP	TCP	21, 20, > 1023	21, 20, > 1023	
E-Serv>ISN							
E-Serv>ISN#01	E-Serv/LN Servers	ISN/LN Servers	LN	TCP	1352	1352	(4)
E-Serv>EXT							
E-Serv>EXT#01	E-Serv/SMTP Servers	Internet/Corporate External SMTP gateways	SMTP	TCP	25	25	(5)
E-Serv>EXT#02	E-Serv/HTTP Proxies	Internet/any	HTTP(S)	TCP	80, 81, 443, 8000-8999	80,443	(6)
E-Serv>EXT#03	E-Serv/FTP Proxies	Internet/any	FTP	TCP	21, 20, > 1023	21, 20, > 1023	
E-Serv>Legacy							
E-Serv>Legacy#01	E-Serv/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	if any
E-Serv>MGT							
E-Serv>MGT#01	E-Serv/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(7)
E-Serv>MGT#02	E-Serv/any	MGT DMZ/single	ICMP reply	IP			(8)
E-Serv>MGT#03	E-Serv/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(9)
E-Serv>MGT#04	E-Serv/any	MGT DMZ/single	syslog	UDP	>1023	514	
E-Serv>MGT#05	E-Serv/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(10)

Table 9-3: E-Serv Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between similar network service servers at E-Serv subnets at local and remote EO Center(s).

(2) NTP synchronization obtained through an internal NTP server (provided.

(3) One of the mail exchange options for the E-Serv SMTP mail gateways is via the mail relays on the Corporate DMZ.

(4) Applicable between well identified Lotus Notes server(s) on the E-Serv DMZ and the ESRIN Internal Services Networks. Note that a Corporate SDSR is required.

(5) One of the mail exchange options for the E-Serv SMTP mail gateways is via the Off-Site Corporate mail gateways.

(6) E-Serv proxies intended to hand-off the requests of EO internal networks to external world servers (Internet, ESN). Further necessary destination HTTP(s) ports will be added and implemented upon request. It is not necessary to submit an SDSR to use other ports. HTTP Proxy is contacted through port 3128.

(7) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(8) ICMP Type 0 are supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the E-Serv DMZ. All other ICMP types/codes from the systems connected to the E-Serv DMZ is blocked.

(9) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(10) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

9.5 DAP DMZ Security Baseline

DAP DMZ Security Baseline							
ID	**Source**	**Destination**	**Protocol**		**Port or Number**		**Notes**
	Network/System	Network/System	Application	Transport	Source	Destination	
DAP>DAP							
DAP>DAP#01	DAP DMZ subnet/any	DAP DMZ subnet/any	any	any	any	any	(1)
DAP>E-Serv							
DAP>E-Serv#01	DAP DMZ/any	E-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(2)
DAP>I-Serv							
DAP>I-Serv#01	DAP DMZ/any	I-Serv/NTP Servers	NTP	UDP	123, > 1023	123	(3)
DAP>EXT							
DAP>EXT#01	DAP DMZ/any	Internet/any	FTP	TCP	> 1023	21, 20	
DAP>EXT#02	DAP DMZ/any	Internet/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(4)
DAP>EXT#03	DAP DMZ/single	Internet/single	SSH, SFTP, SCP	TCP	> 1023	22	(5)
DAP>EXT#04	DAP DMZ/any	Internet/any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
DAP>ESN							
DAP>ESN#01	DAP DMZ/any	Corp ESN/any	FTP	TCP	> 1023	21, 20	
DAP>ESN#02	DAP DMZ/any	Corp ESN/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(4)
DAP>ESN#03	DAP DMZ/any	Corp ESN/any	SSH, SFTP, SCP	TCP	> 1023	22	(5)
DAP>ESN#04	DAP DMZ/any	Corp ESN/any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
DAP>ESN#05	DAP DMZ/any	Corp ESN/DNS server	DNS	TCP, UDP	> 1023	53	(6)
DAP>ESN#06	DAP DMZ/G-POD	ESN/G-POD	GRIDFTP	TCP	> 1023	2811 20000-20200	(7)
DAP>ESN#07	DAP DMZ/G-POD	ESN/G-POD	SSH	TCP	> 1023	22	
DAP>ESN#08	DAP DMZ/G-POD	ESN/G-POD	MySQL	TCP	> 1023	3306	(8)
DAP>ESN#09	DAP DMZ/G-POD	ESN/G-POD	PostgresSQL	TCP	> 1023	5432	(9)
DAP>ESN#10	DAP DMZ/G-POD	ESN/G-POD	USCP	UDP	> 1023	5000	(10)
DAP>L1							
DAP>L1#01	DAP DMZ/any	L1 DMZ/single	HTTP(S)	TCP	80, 81, 443, > 1023	443	
DAP>L1#02	DAP DMZ/single	L1 DMZ/single	HTTP(S)	TCP	80, 81, 443, > 1023	8110, 8104	
DAP>I-PSN							
DAP>I-PSN#01	DAP DMZ/any	I-PSN/any	FTP	TCP	> 1023	21, 20	
DAP>I-PSN#02	DAP DMZ/any	I-PSN/any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
DAP>I-PSN#03	DAP DMZ/single	I-PSN/single	SQL*Net	TCP	> 1023	1521	(11)
DAP>I-PSN#04	DAP DMZ/any	I-PSN/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(4)
DAP>I-PSN#05	DAP DMZ/single	I-PSN/single	CORBA	TCP, UDP		1080	(12)
DAP>Legacy							
DAP>Legacy#01	DAP/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	(13)
DAP>MGT							
DAP>MGT#01	DAP DMZ/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(14)
DAP>MGT#02	DAP DMZ/any	MGT DMZ/single	ICMP reply	IP			(15)
DAP>MGT#03	DAP DMZ/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(16)
DAP>MGT#04	DAP DMZ/any	MGT DMZ/single	syslog	UDP	>1023	514	
DAP>MGT#05	DAP DMZ/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(17)
DAP>MGT#06	DAP DMZ/single	MGT DMZ/single	LDAPS	TCP	49152 -65535	636	(18)

Table 9-4: DAP DMZ Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between DAP DMZ subnets at local and remote EO Center(s) if routing is enabled between the subnets.
(2) Systems on the DAP DMZ can send mail via the E-Serv mail relay(s) only.
(3) All DAP DMZ systems need to be NTP synchronized. The NTP server, wether provided by the project or by EO is always located in the I-Serv.
(4) Direct FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.
(5) SSH, SFTP and SCP only to well identified systems on the Internet. See also section 9.1.
(6) DMZs systems relay on Corporate DNS for name resolution.
(7) GridFTP is a GPOD specific protocol and constitutes an extension of the standard FTP transfer protocol for GRID purposes. This protocol uses TCP 2811 for the control channel and port range 20000-20200 for data exchange. GridFTP authentication is performed via user certificates X509 certificates issued by GRID-FR (CNRS).
(8) MySQL is used to perform G-POD catalogue operations (query, registration).
(9) PostgresSQL is used to perform new G-POD catalogue registration operations.
(10) USCP stands for Udp Secure Channel Protocol and it is a GPOD specific protocol. It provides a Single Packet Authentication protocol: each control packet is digitally signed (using X509 certificates) and verified separately from all the others. The Grid-cache-system (a client/server application developed to provide access to remote file repositories using a cache based optimization) leverages on this protocol to authenticate each GridFTP request.
(11) Direct SQL*Net from a DAP-DMZ system to a server on the I-PSN is allowed.
(12) This is considered a Legacy protocol, it will not be supported in the future implementations
(13) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.
(14) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.
(15) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the DAP DMZ. All other ICMP types/codes from the systems connected to the DAP DMZ are blocked.
(16) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.
(17) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.
(18) LDAP authentication from systems located in any DMZ to the LDAP replica server located in a dedicated subnet of the Management DMZ

9.6 Legacy DMZ Security Baseline

Legacy DMZ Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
Legacy>Legacy							
Legacy>Legacy#01	Legacy DMZ/any	Legacy DMZ/any	any	any	any	any	(1)
Legacy>E-Serv							
Legacy>E-Serv#01	Legacy DMZ/any	E-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(2)
Legacy>E-Serv#02	Legacy DMZ/any	E-Serv/HTTP Proxies	HTTP(S)	TCP	80, 81, 443, 8000-8999	80, 443	(3)
Legacy>E-Serv#03	Legacy DMZ/any	E-Serv/FTP Proxies	FTP	TCP	21, 20, > 1023	21, 20, > 1023	(4)
Legacy>E-Serv#04	Legacy DMZ/any	E-Serv/LN Servers	LN	TCP	> 1023	1352	(5)
Legacy>I-Serv							
Legacy>I-Serv#01	Legacy DMZ/any	I-Serv/NTP Servers	NTP	UDP	123, > 1023	123	(6)
Legacy>EXT							
Legacy>EXT#01	Legacy DMZ/Existing	Internet/Existing	Existing	Existing	Existing	Existing	(8), (7)
Legacy>DAP							
Legacy>DAP#01	Legacy DMZ/Existing	DAP DMZ/ Existing	Existing	Existing	Existing	Existing	(7)
Legacy>I-PSN							
Legacy>I-PSN#01	Legacy DMZ/Existing	I-PSN/Exisiting	Existing	Existing	Existing	Existing	(7)
Legacy>ESN							
Legacy>ESN#01	Legacy DMZ/Existing	ESN/Existing	Existing	Existing	Existing	Existing	(7)
Legacy>ISN							
Legacy>ISN#01	Legacy DMZ/Existing	ISN/Existing	Existing	Existing	Existing	Existing	(7)
Legacy>MGT							
Legacy>MGT#01	Legacy DMZ/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(9)
Legacy>MGT#02	Legacy DMZ/any	MGT DMZ/single	ICMP reply	IP			(10)
Legacy>MGT#03	Legacy DMZ/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(11)
Legacy>MGT#04	Legacy DMZ/any	MGT DMZ/single	syslog	UDP	>1023	514	
Legacy>MGT#05	Legacy DMZ/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(12)

Table 9-5: Legacy DMZ Security Baseline

(1) Applicable between Legacy DMZ subnets at local and remote EO Center(s) if routing is enabled between the subnets.
(2) Systems on the Legacy DMZ can send mail via the E-Serv mail relay(s) only.
(3) The use of the E-Serv web proxy is the default configuration for http access.
(4) The use of the E-Serv FTP proxy is the default configuration for FTP file transfers.
(5) End-user mail support is via native Lotus Notes only.
(6) All Legacy DMZ systems need to be NTP synchronized. The NTP server, whether provided by the project or by EO is always located in the I-Serv.
(7) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.

(8) Direct FTP and HTTP(S) to Internet servers which cannot support proxied HTTP(S) connections

(9) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(10) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the Legacy DMZ. All other ICMP types/codes from the systems connected to the Legacy DMZ are blocked.

(11) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(12) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

9.7 L1 (Restricted Trust) DMZ Security Baseline

L1 DMZ Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
L1>L1							
L1>L1#01	L1 DMZ/any	L1 DMZ/any	any	any	any	any	(1)
L1>E-Serv							
L1>E-Serv#01	L1 DMZ /any	E-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(2)
L1>I-Serv							
L1>E-Serv#01	L1 DMZ/single	I-Serv/NTP Server single	NTP	UDP	123, > 1022	122	(3)
L1>ESN							
L1>ESN#01	L1 DMZ/any	Corp ESN/ DNS	DNS	TCP, UDP	> 1023	53	(4)
L1>L3							
L1>L3#01	L1 DMZ/single	L3 DMZ/ single	LDAPS	TCP	49152 -65535	636	(5)
L1>MGT							
L1>MGT#01	L1 DMZ/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(6)
L1>MGT#02	L1 DMZ/any	MGT DMZ/single	ICMP reply	IP			(7)
L1>MGT#03	L1 DMZ/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(8)
L1>MGT#04	L1 DMZ/any	MGT DMZ/single	syslog	UDP	>1023	514	
L1>MGT#05	L1 DMZ/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(9)
L1>MGT#06	L1 DMZ/single	MGT DMZ/single	LDAPS	TCP	49152 -65535	636	(10)

Table 9-6: L1 (Restricted Trust) DMZ Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between L1 DMZ subnets at local and remote EO Center(s) if routing is enabled between the subnets.

(2) Systems on the L1 DMZ can send mail via the E-Serv mail relay(s) only.

(3) All L1 DMZ systems need to be NTP synchronized. The NTP server, wether provided by the project or by EO is always located in the I-Serv.

(4) All L1 DMZ systems need to configure their DNS resolvers with the Corporate DNS servers.

(5) Authentication databases reside on the L3 DMZ. Only LDAP over SSL/TLS is supported.

(6) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(7) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the L1 DMZ. All other ICMP types/codes from the systems connected to the L1 DMZ are blocked.

(8) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(9) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

(10) LDAP authentication flow from systems located in any DMZ to the LDAP replica server located in a dedicated subnet of the Management DMZ.

9.8 L2 (Interconnection) DMZ Security Baseline

L2 DMZ Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
L2>E-Serv							
L2>E-Serv#01	EO RAS PC/any EO RAS LAN/any	E-Serv/HTTP Proxies	HTTP(S)	TCP	80, 81, 443, 8000-8999	80, 443	(1)
L2>E-Serv#02		E-Serv/FTP Proxies	FTP	TCP	21, 20, > 1023	21, 20, > 1023	(2)
L2>DAP							
L2>DAP#01	EO RAS PC/any	DAP DMZ/ any	FTP	TCP	> 1023	21, 20	
L2>DAP#02	EO RAS LAN/any		FTPS	TCP	> 1023	21, 20, 990, 30200-30210	(3)
L2>DAP#03			SSH, SFTP, SCP	TCP	> 1023	22	
L2>DAP#04			HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
L2>DAP#05			SQL*Net	TCP	> 1023	1521	
L2>L1							
L2>L1#01	EO RAS PC/any	L1 DMZ/ any	FTP	TCP	> 1023	21, 20	
L2>L1#02	EO RAS LAN/any		FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(3)
L2>L1#03			SSH, SFTP, SCP	TCP	> 1023	22	
L2>L1#04			HTTP(S)	TCP	80, 81, 443, > 1023	80, 443, 8110, 8104	
L2>I-Serv							
L2>I-Serv#01	EO RAS PC/any	I-Serv/DNS Servers	DNS	TCP, UDP	> 1023	53	(4)
L2>I-Serv#02	EO RAS LAN/any	I-Serv/NTP Servers	NTP	UDP	123, > 1023	123	(5)
L2>I-Serv#03		I-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(6)
L2>I-PSN							
L2>I-PSN#01	EO RAS PC/any	I-PSN/ any	FTP	TCP	> 1023	21, 20	
L2>I-PSN#02	EO RAS LAN/any	I-PSN/ any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(3)
L2>I-PSN#03		I-PSN/ any	SSH, SFTP, SCP	TCP	> 1023	22	
L2>I-PSN#04		I-PSN/ any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
L2>I-PSN#05		I-PSN/ any	SMB	TCP	> 1023	445	(7)
L2>I-PSN#06		I-PSN/ any	SQL*Net	TCP	> 1023	1521	
L2>I-PSN#07		I-PSN/ any	MSSQL	TCP	> 1023	1433	
L2>I-PSN#08		I-PSN/ any	LDAPS	TCP	49152 -65535	636	(8)
L2>I-PSN#09		I-PSN/ any	RDP	TCP	> 1023	3389	(9)
L2>I-PSN#10		I-PSN/ any	ICA	TCP	> 1023	1494	
L2>L3							
L2>L3#01	EO RAS PC/any	L3/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(3)
L2>L3#02	EO RAS LAN/any	L3/any	SSH, SFTP, SCP	TCP	> 1023	22	
L2>L3#03		L3/any	HTTPS	TCP	> 1023	single	(10)
L2>L3#04		L3/any	LDAPS	TCP	49152 -65535	636	(8)
L2>Legacy							
L2>Legacy#01	EO RAS PC/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	(11)
L2>Legacy#02	EO RAS LAN/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	
L2>MGT							
L2>MGT#01	EO RAS PC/any	MGT DMZ/any	SNMP	TCP, UDP	161, 162	161, 162	(12)
L2>MGT#02	EO RAS LAN/any	MGT DMZ/any	ICMP reply	IP			(13)
L2>MGT#03		MGT DMZ/any	ICA	TCP	> 1023	1494	(14)
L2>MGT#04			RDP	TCP	> 1023	3389	
L2>MGT#05			SSH, SFTP, SCP	TCP	> 1023	22	
L2>MGT#06		MGT DMZ/any	TFTP	UDP	69, >1023	69	(15)
L2>ANY							
L2>TBD#1	Custom rules to be defined case by case						

Table 9-7: L2 (Interconnection) DMZ

(1) The use of the E-Serv web proxy is the default configuration for all systems connecting through the L2 DMZ to the Internet. Further necessary destination ports will be added and implemented upon request. It is not necessary to submit an SDSR to use other ports. Proxy is contacted through port 3128.

(2) The use of the E-Serv FTP proxy is the default configuration for all systems connecting through the L2 DMZ to the Internet.

(3) FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.

(4) All systems connecting through the EO RAS at the L2 DMZ, need to configure their DNS resolvers with the I-Serv DNS servers.

(5) All systems connecting through the EO RAS at the L2 DMZ to access EO DMZs need to be NTP synchronized with the connected systems. They can use the NTP servers on the I-Serv DMZ.

(6) If system connecting through the EO RAS at the L2 DMZ need to send mail, they will use the I-Serv SMTP mail relay.

(7) Windows resource sharing via NetBIOS of TCP is supported. Older Windows sharing mechanisms are not supported.

(8) LDAP over SSL/TLS from a remote system to a server is allowed However, it is not intended for end-user systems. End-user systems should access an application or service that will perform the LDADS request on behalf of the end-user.

(9) Access from a trusted remote party, passing through the L2 DMZ via the EO RAS services, to a Windows systems connected to the I-PSN is supported via native Microsoft Terminal Server (also known as Remote Desktop Protocol). System administration via RDP has to be performed from the MGT DMZ.

(10) Application server web access between peers only on a specific TCP port. No EO-SDSR is required, but the communication needs to be explicitly configured in the Firewall rule base.

(11) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.

(12) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO. Note that this concerns SNMP from devices located on/in the L2 DMZ only; SNMP from systems on networks that are interconnected is not falling under this security baseline.

(13) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the L2 DMZ. All other ICMP types/codes from the systems connected to the L2 DMZ are blocked. Note that this concerns ICMP replies from devices located on/in the L2 DMZ only; ICMP replies from systems on networks that are interconnected do not fall under this security baseline.

(14) Management clients systems connecting through the EO RAS at the L2 DMZ, can access management systems on the Management DMZ via ICA, RDP or SSH. Tunnels and/or permanent connections are not permitted though.

(15) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

9.9 L3 (Inter Trust) DMZ Security Baseline

L3 DMZ Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
L3>L3							
L3>L3#01	L3 DMZ/any	L3 DMZ/any	LDAPS	TCP	49152 -65535	636	(2), (1)
L3>L3#02	L3 DMZ/any	L3 DMZ/any	HTTPS	TCP	single	single	
L3>I-Serv							
L3>I-Serv#01	L3 DMZ/any	I-Serv/DNS Servers	DNS	TCP, UDP	> 1023	53	(3)
L3>I-Serv#02	L3 DMZ/any	I-Serv/NTP Servers	NTP	UDP	123, > 1023	123	(4)
L3>I-Serv#03	L3 DMZ/any	I-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(5)
L3>MGT							
L3>MGT#01	L3 DMZ/any	MGT DMZ/single	SNMP	TCP, UDP	161, 162	161, 162	(6)
L3>MGT#02	L3 DMZ/any	MGT DMZ/single	ICMP reply	IP			(7)
L3>MGT#03	L3 DMZ/single	MGT DMZ/single	TFTP	UDP	69, >1023	69	(8)
L3>MGT#04	L3 DMZ/any	MGT DMZ/single	syslog	UDP	>1023	514	
L3>MGT#05	L3 DMZ/any	MGT DMZ/single	HIPS log	UDP	>1023	1514	(9)
L3>MGT#06	L3 DMZ/single	MGT DMZ/single	LDAPS	TCP	49152 -65535	636	(10)

Table 9-8: L3 (Inter Trust) DMZ Security Baseline

(1) Applicable within the same security belt (see section 8.2); i.e. between similar network service servers at L3 subnets at local and remote EO Center(s) if routing is enabled between the subnets.

(2) Application server web access between peers only on a specific TCP port. No EO-SDSR is required, but the communication needs to be explicitly configured in the Firewall rule base.

(3) All L3 DMZ systems need to configure their DNS resolvers with the I-Serv DNS servers.

(4) All L3 DMZ systems need to be NTP synchronized. The NTP server, whether provided by the project or by EO is always located in the I-Serv.

(5) Systems on the L3 DMZ can send mail via the E-Serv mail relay(s) only.

(6) SNMPv3 with security features enabled is required. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. Other SNMP versions and configurations are to be requested to the EO-NSO.

(7) ICMP Type 0 is supported. This allows for ping and traceroute functionality from the EO MGT DMZ to the L3 DMZ. All other ICMP types/codes from the systems connected to the L3 DMZ are blocked.

(8) TFTP is to be used for system configuration and only when there is no other way to transfer file(s) to and from a dedicated management system.

(9) HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

(10) LDAPS feeding communication from the Master LDAP DB to the replica LDAP DB to allow population of the replica DB

9.10 MGT DMZ Security Baseline

ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
MGT DMZ Security Baseline							
MGT>MGT#01	MGT DMZ/any	MGT DMZ/any	any	any	any	any	(1)
MGT>I-Serv							
MGT>I-Serv#01	MGT DMZ/any	I-Serv/DNS Servers	DNS	TCP, UDP	> 1023	53	(2)
MGT>I-Serv#02	MGT DMZ/any	I-Serv/NTP Servers	NTP	UDP	123, > 1023	123	(3)
MGT>I-Serv#03	MGT DMZ/any	I-Serv/SMTP Servers	SMTP	TCP	25, > 1023	25	(4)
MGT>E-Serv							
MGT>E-Serv#01	MGT DMZ/any	E-Serv/HTTP Proxies	HTTP(S)	TCP	80, 81, 443, 8000-8999	80, 443	(5)
MGT>Any (***)							
MGT>ANY#01	MGT DMZ/single	E-Serv DMZ/single DAP DMZ/ single Legacy DMZ/single L1 DMZ/single L2 DMZ /single L3 DMZ /single I-Serv/single I-PSN/single	SNMP	TCP, UDP	161, 162	161, 162	(6)
MGT>ANY#02			ICMP	IP			(7)
MGT>ANY#03			FTP	TCP	> 1023	21, 20	(8)
MGT>ANY#04			FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(9)
MGT>ANY#05			SSH, SFTP, SCP	TCP	> 1023	22	(10)
MGT>ANY#06			HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	(11)
MGT>ANY#07			RDP	TCP	> 1023	3389	(12)
MGT>ANY#08	MGT DMZ/single	E-Serv DMZ/any DAP DMZ/ any Legacy DMZ/any L1 DMZ/any L2 DMZ /any L3 DMZ /any I-Serv/any I-PSN/any	HIPS log	UDP	>1023	1514	(13)
MGT>EXT							
MGT>EXT#01	MGT DMZ/single	Internet ESN	ICMP T8/C0	IP			(14)
MGT>EXT#02			ICMP T3/Cx	IP			
MGT>EXT#03			ICMP T4/C0	IP			
MGT>EXT#04			ICMP T5/Cx	IP			
MGT>EXT#05			ICMP T11/Cx	IP			
MGT>EXT#06			ICMP T30	IP			

Table 9-9: MGT DMZ Security Baseline

(***) All the protocols listed in rules from #01 to #07 are available for all the destinations listed in the related column (e.g. SNMP is possible from a specific MGT system to specific systems in the E-Serv, DAP, Legacy, L1, L2, L3, I-Serv, I-PSN). Protocols listed for #08 are available for all destinations listed in the related column (e.g. UDP is available from a specific MGT system to any systems in the listed zones)

(1) Applicable within the same security belt (see section 8.2); i.e. between similar network service servers at MGT subnets at local and remote EO Center(s) to allow management of remote systems, if routing is enabled between the subnets.

(2) All MGT DMZ systems need to configure their DNS resolvers with the I-Serv DNS servers.

(3) All MGT DMZ systems need to be time synchronized with the managed systems. The NTP server, wether provided by the project or by EO is always located in the I-Serv.

(4) Systems on the MGT DMZ can send mail via the I-Serv mail relay(s) only.

(5) Web access for systems connected on the MGT DMZ can be obtained via the web proxies on the E-Serv DMZ. Further necessary destination ports will be added and implemented upon request. It is not necessary to submit an SDSR to use other ports. Proxy is contacted through port 3128.

(6) SNMPv3 with security features enabled is supported. SNMPv2c is allowed until SNMPv3 will be officially supported by OS. SNMP to service interfaces of the devices is not supported. Other SNMP versions and configurations than the SNMPv3 are to be requested to the EO-NSO.

(7) ICMP is supported towards the management interfaces of devices on the EO networks. ICMP to the service interfaces of the devices is not supported. ICMP all types and codes are supported to network gear. Towards systems connected to the EO networks, only ICMP echo requests are supported.

(8) Direct FTP to the management interfaces of the systems connected to the EO networks is supported. FTP from the MGT DMZ toward the service interfaces of the systems connected to the EO networks is not supported.

(9) Direct FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports. FTPS from the MGT DMZ toward the management interfaces of the systems connected to the EO networks is supported. FTPS from the MGT DMZ toward the service interfaces of the systems connected to the EO networks is not supported.

(10)SSH, SFTP and SCP only between well identified systems only. See also section 9.1. SSH, SFTP and SCP from the MGT DMZ toward the management interfaces of the systems connected to the EO networks is supported. SSH, SFTP, SCP from the MGT DMZ toward the service interfaces of the systems connected to the EO networks is not supported.

(11)HTTP(S) from the MGT DMZ toward the management interfaces of the systems connected to the EO networks is supported. HTTP(S) from the MGT DMZ toward the service interfaces of the systems connected to the EO networks is not supported.

(12)RDP from the MGT DMZ toward the management interfaces of the systems connected to the EO networks is supported. RDP from the MGT DMZ toward the service interfaces of the systems connected to the EO networks is not supported.

(13)HIPS alarm and configuration protocol used by the HIPS system to retrieve information and perform actions in case of attacks.

(14)Towards the Internet and the ESA External Services Networks, the following ICMP traffic is supported for diagnostic purposes:

- ICMP Type 8 (Echo)
- ICMP Type 3 (Destination Unreachable) – All codes
- ICMP Type 4 (Source Quench)
- ICMP Type 5 (Redirect) – All codes
- ICMP Type 11 (Time Exceeded) – All codes
- ICMP Type 30 (Traceroute)

9.11 Internet Security Baseline

Internet Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
EXT>E-Serv							
EXT>E-Serv#01	Internet/Corporate External SMTP gateways	E-Serv/SMTP Servers	SMTP	TCP	25	25	(1)
EXT>DAP							
EXT>DAP#01	Internet/any	DAP DMZ/ any	FTP	TCP	> 1023	21, 20	
EXT>DAP#02	Internet/any	DAP DMZ/ any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(2)
EXT>DAP#03	Internet/single	DAP DMZ/ single	SSH, SFTP, SCP	TCP	> 1023	22	(3)
EXT>DAP#04	Internet/any	DAP DMZ/ any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
EXT>DAP#05	Internet/single	DAP DMZ/ GANTT Tool Servers	GANTT	TCP	> 1023	20000, 20010, 20100	(4)
EXT>DAP#06	Internet/single	DAP DMZ/ DDS C-band	RRMP	TCP, UDP	> 1023	10000-10100	(5)
EXT>L1							
EXT>L1#01	Internet/any	L1/single	HTTPS	TCP	80, 81, 443, > 1023	443	(6)
EXT>L1#02	Internet/single	L1/single	HTTPS	TCP	80, 81, 443, > 1023	8110, 8104	(7)
EXT>Legacy							
EXT>Legacy#01	Internet/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	(8)

Table 9-10: Internet Security Baseline

(1) Corporate Mail Gateways forwards email to the E-Serv SMTP mail gateways

(2) Internet systems can access file servers on the DAP or L1 DMZ via FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.

(3) Systems on the Internet can access servers on the DMZ via SSH.

(4) Well identified systems on the Internet can access the GANTT Applications servers on the DAP DMZ.

(5) Well identified Envisat DDS stations can use RRMP (Restricted Reliable Multicast Protocol) to provide NACX to the DDS C-band servers located at ESRIN.

(6) Internet systems can access Web SSO on L1 only via HTTPS.

(7) Only point-to point connections are allowed towards SSO servers over the other service ports.

(8) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.

9.12 ESN Security Baseline

ESN Security Baseline							
ID	Source	Destination	Protocol		Port or Number		Notes
	Network/System	Network/System	Application	Transport	Source	Destination	
ESN>E-Serv							
ESN>E-Serv#01	ESN/any	E-Serv/SMTP servers	SMTP	TCP	25	25	
ESN>DAP							
ESN>DAP#01	ESN/any	DAP DMZ/ any	FTP	TCP	> 1023	21, 20	(1)
ESN>DAP#02	ESN/any	DAP DMZ/ any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(2)
ESN>DAP#03	ESN/single	DAP DMZ/ single	SSH, SFTP, SCP	TCP	> 1023	22	(3)
ESN>DAP#04	ESN/any	DAP DMZ/ any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	(4)
ESN>DAP#05	ESN/any	DAP DMZ/ GANTT Tool Servers	GANTT	TCP	> 1023	20000, 20010, 20100	(5)
ESN>DAP#06	ESN/G-POD	DAP DMZ/G-POD	GRIDFTP	TCP	>1023	2811 20000-20200	(6)
ESN>DAP#07	ESN/G-POD	DAP DMZ/G-POD	Ganglia XML	TCP, UDP	>1023	8649	(7)
ESN>DAP#08	ESN/G-POD	DAP DMZ/G-POD	SSH	TCP	>1023	22	
ESN>DAP#09	ESN/G-POD	DAP DMZ/G-POD	USCP	UDP	>1023	5000	(8)
ESN>L1							
ESN>L1#01	ESN/any	L1/single	HTTPS	TCP	80, 81, 443, > 1023	443	(9)
ESN>L1#02	ESN/ single	L1/single	HTTPS	TCP	80, 81, 443, > 1023	8110, 8104	
ESN>Legacy							
ESN>Legacy#01	ESN/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	(10)

Table 9-11: ESN Security Baseline

(1) ESN systems can access file servers on the DAP DMZ via FTP.

(2) ESN systems can access file servers on the DAP DMZ via FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.

(3) Systems on the ESNs can access servers on the DAP DMZ via SSH on a point-to-point basis, no SDSR is requested.

(4) ESN systems can access web portals on the DAP DMZ via HTTP(S).

(5) Well identified systems on the ESNs can access the GANTT Applications servers on the DAP DMZ.

(6) GridFTP is a GPOD specific protocol and it constitutes an extension of the standard FTP transfer protocol for GRID purposes. This protocol uses TCP 2811 for the control channel and port range 20000-20200 for data exchange. GridFTP authentication is performed via user certificates X509 certificates issued by GRID-FR (CNRS).

(7) Ganglia XML is a protocol specific of the GPOD environment. Ganglia is an open-source scalable distributed monitoring system for high-performance computing systems such as clusters and Grids

(8) USCP stands for Udp Secure Channel Protocol and it is a GPOD specific protocol. It provides a Single Packet Authentication protocol: each control packet is digitally signed (using X509 certificates) and verified separately from all the others. The Grid-cache-system (a client/server application developed to provide access to remote file repositories using a cache based optimization) leverages on this protocol to authenticate each GridFTP request.

(9) ESN systems can access Web SSO on L1 only via HTTPS. Only point-to point connections are allowed towards SSO servers over the other service ports.

(10) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.

9.13 ISN Security Baseline

ISN>E-Serv							
ISN>E-Serv#01	ISN/LN Servers	E-Serv/LN Servers	LN	TCP	1352	1352	(1)
ISN>DAP							
ISN>DAP#01	ISN/any	DAP DMZ/any	FTP	TCP	> 1023	21, 20	
ISN>DAP#02	ISN/any	DAP DMZ/any	FTPS	TCP	> 1023	21, 20, 990, 30200-30220	(2)
ISN>DAP#03	ISN/any	DAP DMZ/single	SSH, SFTP, SCP	TCP	> 1023	22	(3)
ISN>DAP#04	ISN/any	DAP DMZ/any	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
ISN>DAP#05	ISN/any	DAP DMZ/GANTT Tool Servers	GANTT	TCP	> 1023	8300, 20000, 20010, 20100	
ISN>I-PSN							
ISN>I-PSN#01	ISN/any	I-PSN/single	FTP	TCP	> 1023	21, 20	
ISN>I-PSN#02	ISN/any	I-PSN/single	FTPS	TCP	> 1023	21, 20, 990, 30200-30210	(2)
ISN>I-PSN#03	ISN/any	I-PSN/single	SSH, SFTP, SCP	TCP	> 1023	22	(3)
ISN>I-PSN#04	ISN/any	I-PSN/single	HTTP(S)	TCP	80, 81, 443, > 1023	80, 81, 443, 8000-8999	
ISN>I-PSN#05	ISN/any	I-PSN/single	SQL*Net	TCP	> 1023	1521	(4)
ISN>I-PSN#06	ISN/single	I-PSN/single	SMB	TCP	> 1023	445	(5)
ISN>L1							
ISN>L1#01	ISN/any	L1/single	HTTPS	TCP	80, 81, 443, > 1023	443	(6)
ISN>L1#02	ISN/ single	L1/single	HTTPS	TCP	80, 81, 443, > 1023	8110, 8104	
ISN>Legacy							
ISN>Legacy#01	ISN/Existing	Legacy DMZ/Existing	Existing	Existing	Existing	Existing	(7)

Table 9-12: ISN Security Baseline

(1) Applicable between well identified Lotus Notes server(s) on the E-Serv DMZ and the ESRIN Internal Services Networks. Note that a Corporate SDSR is required.

(2) SN systems can access file servers via FTP over SSL/TLS, both explicit and implicit. The server side must run data connection on the high unprivileged ports.

(3) ISN systems can access well identified servers via SSH. SSH towards client systems on the I-PSNs is not allowed.

(4) ISN systems can access well identified databases on the I-PSNs via SQL*Net. Note that a Corporate SDSR will be required.

(5) Well identified ISN systems can set up resource sharing via NetBIOS over TCP sessions towards well identified Microsoft systems. Note that a Corporate SDSR will be required.

(6) ISN systems can access Web SSO on L1 only via HTTPS. Only point-to point connections are allowed towards SSO servers over the other service ports. HTTPS access will be performed according to the Corporate Firewall rules (e.g. Proxy or NAT)

(7) Only existing connectivity, in place at the release of this version of the policy is a baseline security service for the Legacy subnets. Other communications require an EO-SDSR.

APPENDIX A SECURITY BASELINE CROSS-REFERENCE

A cross reference of the security baseline rule numbers between the old (v1.1.3) and the new (v1.2) version of the policy is provided below. Obviously, **the old numbering is deprecated and not to be used henceforth.** Likewise all qualifications and ambiguous notations to source and destinations on the old IDs are deprecated and not valid henceforth. Wherever possible or applicable, a reference is provided.
Three possible statuses are specified for each old baseline rule:

- Active
- Withdrawn
- Replaced.

If a rule is ACTIVE, it means it is still valid and only the ID has changed.
If a rule is WITHDRAWN, it is not implemented in the new baseline, as such there is no corresponding rule.
If a rule has been REPLACED, it means that the old rule is withdrawn but the communication is achieved via a different model, represented by one or more new rules associated to it.

Old-ID	Source	Destination	Protocol	Status	New rule ID	Reference
SB-01	Internal LAN	Internal LAN	Any	Active	**I-PSN / I-PSN 01**	Table 9-2
SB-02	Internal LAN (local Centre and only for promoted hosts)	DAP DMZ (remote Centre)	FTP (both passive and active)	Active	**I-PSN / DAP 01**	
			HTTP/HTTPS	Active	**I-PSN / DAP 03**	
			SSH/SFTP	Active	**I-PSN / DAP 04**	
			FTPS-explicit mode	Active	**I-PSN / DAP 02**	
			Traceroute (ICMP)	Withdrawn	-	
			Ping	Withdrawn	-	
SB-03	DAP DMZ	DAP DMZ	FTP	Active	**DAP / DAP 01**	Table 9-4
			HTTP/HTTPS	Active		
			SSH/SFTP	Active		
SB-04	Internal LAN	Internet	FTP (both passive and active)	Replaced	**I-PSN / E-Serv 01**	Table 9-2

Old-ID	Source	Destination	Protocol	Status	New rule ID	Reference
	(only for promoted hosts)		HTTP/HTTPS	Replaced	I-PSN / E-Serv 02	See Sections 5.4 , 8.3.7, 9.3.
			DNS (towards ESA)	Replaced	I-PSN / I-Serv 01	
			Corporate FW baseline rules	Withdrawn	-	
			Traceroute (ICMP)	Replaced	MGT / EXT 06	
			Ping	Replaced	MGT / EXT 01	
SB-05	DAP DMZ	Internet	FTP	Active		Table 9-4
					DAP / EXT 01	Table 9-3
			SSH/SFTP	Replaced	DAP / EXT 03	
			FTPS-explicit mode	Active	DAP / EXT 02	
			HTTP/HTTPS	Active		
					DAP / EXT 04	
			Telnet	Withdrawn	-	
			SMTP (towards ESA)	Replaced	DAP / E-Serv 01 E-Serv / EXT 01	
			DNS (towards ESA)	Replaced	E-Serv / ESN 01	
SB-06	Internet	DAP DMZ	FTP	Active	EXT / DAP 01	Table 9-10
			SMTP (specific hosts, delta)	Replaced	EXT / E-Serv 01	
			HTTP/HTTPS	Active	EXT / DAP 04	
			Telnet (peer2peer, delta)	Withdrawn		Section 5.4
			SSH/SFTP (peer2peer, delta)	Active	EXT / DAP 03	Table 9-10
			FTPS-explicit mode	Active	EXT / DAP 02	

Old-ID	Source	Destination	Protocol	Status	New rule ID	Reference
			GANTT tool – ports : 20000,20010, 20100	Active	EXT / DAP 05	
SB-07	Internal LAN	DAP DMZ	Telnet	Withdrawn	-	Section 5.4
			FTP	Active	I-PSN / DAP 01	Table 9-2
			SSH/SFTP	Active	I-PSN / DAP 04	and sections, 5.2, 8.2, 8.9
			FTPS-explicit mode	Active	I-PSN / DAP 02	
			HTTP/HTTPS	Active	I-PSN / DAP 03	
			SMTP (specific hosts, delta)	Replaced	I-PSN / I-Serv 03	
			SNMP (specific hosts, delta)	Replaced	MGT / ANY 01	Table 9-9 and Section 8.3.7
			POP3 (specific hosts, delta)	Withdrawn	-	Sections 5.5 and 9.3.
			Traceroute (ICMP)	Replaced	MGT / ANY 02	Table 9-9 and Section 5.4
			Ping	Replaced	MGT / ANY 02	
			DNS (specific hosts, delta)	Replaced	I-PSN / I-Serv 01	Table 9-2
			GANTT tool (20000, 20010, 20100)	Active	I-PSN / DAP 06	
SB-08	DAP DMZ	Internal LAN	FTP	Active	DAP / I-PSN 01	Table 9-4
			Telnet (peer2peer, delta)	Withdrawn	-	Section 5.4
			Corba (peer2peer, delta)	Active	DAP / I-PSN 05	Table 9-4
			SQLnet (peer2peer, delta)	Active	DAP / I-PSN 03	
			SMTP	Replaced	DAP / E-Serv 01	Table 9-4
					E-Serv / I-Serv 02	Table 9-3
			NTP	Replaced	DAP / I-Serv 01	Table 9-4

Old-ID	Source	Destination	Protocol	Status	New rule ID	Reference
			SNMP-trap	Replaced	DAP / MGT 01	Table 9-4, Section 8.3.7
SB-09	ISN	DAP DMZ	Telnet	Withdrawn	-	Section 5.4
			FTP	Active	ISN / DAP 01	Table 9-12
			SSH/SFTP	Active	ISN / DAP 03	
			FTPS-explicit mode	Active	ISN / DAP 02	
			Corporate FW baseline rules	Withdrawn	-	Section 9.13.
			GANTT tool (8300)	Active	ISN / DAP 05	Table 9-12
SB-10	Internal LAN (only for promoted hosts)	ESN	FTP (both passive and active)	Active	I-PSN / ESN 01	Table 9-2
			HTTP/HTTPS	Active	I-PSN / ESN 03	
			Traceroute (ICMP)	Replaced	MGT / EXT 06	Section 5.4
			Ping	Replaced	MGT / EXT 01	Table 9-9
SB-11	ESN	Internal LAN (only for promoted hosts)	FTP (peer2peer, delta)	Withdrawn	-	Section 9.12
SB-12	DAP DMZ	ESA External Services Networks	FTP	Active	DAP / ESN 01	Table 9-4
			SSH/SFTP	Active	DAP / ESN 03	
			FTPS-explicit mode	Active	DAP / ESN 02	
			HTTP/HTTPS	Active	DAP / ESN 04	
			SMTP (included in EOR5)	Replaced	DAP / E-Serv 01	
			DNS (included in EOR5)	Active	DAP / ESN 05	
			Telnet	Withdrawn	-	Section 5.4
SB-13	ESN	DAP DMZ	FTP	Active	ESN / DAP 01	Table 9-11

Old-ID	Source	Destination	Protocol	Status	New rule ID	Reference
			SMTP (specific hosts, delta) (included in EOR6)	Replaced	ESN / E-Serv 01	
			HTTP/HTTPS	Active	ESN / DAP 04	
			SSH/SFTP (peer2peer, delta)	Active	ESN / DAP 03	
			FTPS-explicit mode (peer2peer, delta)	Active	ESN / DAP 02	
			Telnet (peer2peer, delta)	Withdrawn	-	Section 5.4
			GANTT tool (20000, 20010, 20100)	Active	ESN / DAP 05	Table 9-11
RAS-01	Remote LAN Remote Client-PC	EO Internal LAN	SSH, SFTP, SCP	Active	L2 / I-PSN 03	Table 9-7
			FTP (normal and passive)	Active	L2 / I-PSN 01	
			FTPS-explicit mode	Active	L2 / I-PSN 02	
			Microsoft File sharing (SMB)	Active	L2 / I-PSN 05	
			HTTP	Active	L2 / I-PSN 04	
			HTTPS, SSL	Active	L2 / I-PSN 04	
			ICA	Active	L2 / I-PSN 10	
			SQL*Net	Active	L2 / I-PSN 06	
RAS-02	Remote LAN Remote Client-PC	EO DAP-DMZ	SSH, SFTP, SCP	Active	L2 / DAP 03	Table 9-7
			FTP (normal and passive)	Active	L2 / DAP 01	
			FTPS-explicit mode	Active	L2 / DAP 02	
			HTTP	Active	L2 / DAP 04	
			HTTPS, SSL	Active	L2 / DAP 04	
			SQL*Net	Active	L2 / DAP 05	

Table 9-13: Security baseline cross-reference between the previous policy and the current one.

APPENDIX B OVERALL BASELINE MATRIX

Table 9-14 summaries the overall baseline connectivity between each couple of zones. In particular each cell specifies the baseline set of rules associated to the specific source (first column) →destination (first row) flow.
Each set is identified by the couple <*source net name*> / < *destination net name*> and it is specified in the different sections 9.x, where each baseline is identified by the source network.

Destination Source	I-SERV	E-SERV	DAP-DMZ	ESN	ISN	I-PSN	Internet	Management LAN	L1-DMZ	L2 DMZ (RAS)	L3-DMZ	Legay DMZ
I-Serv	I-SERV>I-SERV	I-SERV>E-SERV	▨	I-SERV>ESN	▨	▨	▨	I-SERV>MGT	▨	▨	▨	▨
E-Serv	E-SERV>I-SERV	E-SERV>E-SERV	▨	E-SERV>ESN	E-SERV>ISN	▨	E-SERV>EXT	E-SERV>MGT	▨	▨	▨	E-SERV>LEGACY
DAP DMZ	DAP>I-SERV	DAP>E-SERV	DAP>DAP	DAP>ESN	▨	DAP>I-PSN	DAP>EXT	DAP>MGT	DAP>L1	▨	▨	DAP>LEGACY
ISN	▨	ISN>E-SERV	ISN>DAP	☒	☒	ISN>I-PSN	☒	▨	ISN>L1	▨	▨	ISN>LEGACY
ESN	▨	ESN>E-SERV	ESN>DAP	☒	☒	▨	☒	▨	ESN>L1	▨	▨	ESN>LEGACY
I-PSN	I-PSN>I-SERV	I-PSN>E-SERV	I-PSN>DAP	I-PSN>ESN	▨	I-PSN>I-PSN	▨	I-PSN>MGT	I-PSN>L1	▨	I-PSN>L3	I-PSN>LEGACY
Internet	▨	EXT>E-SERV	EXT>DAP	☒	☒	▨	☒	▨	EXT>L1	▨	▨	EXT>LEGACY
Management LAN	MGT>ANY	MGT>E-SERV MGT>ANY	MGT>ANY	MGT>EXT	▨	MGT>ANY	MGT>EXT	MGT>MGT	MGT>ANY	MGT>ANY	MGT>ANY	MGT>ANY
L1 DMZ	L1>I-SERV	L1>E-SERV	▨	L1>ESN	▨	▨	▨	L1>MGT	L1>L1	▨	L1>L3	▨
L2 DMZ (RAS)	L2>I-SERV	L2>E-SERV	L2>DAP	☒	☒	L2>I-PSN	▨	L2>MGT	L2>L1	N/A	L2>L3	L2>LEGACY
L3 DMZ	L3>I-SERV	▨	▨	▨	▨	▨	▨	L3>MGT	▨	▨	L3>L3	▨
Legacy DMZ	LEGACY>I-SERV	LEGACY>E-SERV	LEGACY>DAP	LEGACY>ESN	LEGACY>ISN	LEGACY>I-PSN	LEGACY>EXT	LEGACY>MGT	▨	▨	▨	LEGACY>LEGACY

Table 9-14: Overall baseline connectivity view.

Legenda:

- Grey cells communications not allowed
- Crossed cells: communications out of scope of the EO baseline