IT MODERNISATION RECOVERY INCREMENT 1

WP07 - SYSTEMS INTEGRATION AND CORE CAPABILITIES

NATO OPERATIONAL NETWORK (ON) INFRASTRUCTURE AS A SERVICE (IAAS)

SERVICE DESIGN PACKAGE (SDP)

Effective date..... : 30-Jun-23
Version No..... : 1.2
Issued by ..... : ITM Project Office
Approved by ..... : Martin Diepstraten, POLARIS Technical Design Authority

Document Control

Title:	NATO Operational Network (ON) Infrastructure as a Service (IaaS)
Version:	1.2
Date:	30-Jun-23
Classification:	NATO UNCLASSIFIED
Filename:	NU-ITMRC1-Service Design Package (SDP) IaaS
Storage location:	ITM-RC1 Portal

Table of Amendments

Version	Date	Description
0.1	9th May 22	NCI Agency initial update of SDP to align with architecture and new project scope.
0.17	14th Nov 22	Updates after initial comments.
0.18	13th Dec 22	QA Validation, adaptation to standard document and naming
1.0	20th Dec 22	Initial release for Checkpoint-1.
1.1	19th April 23	Update following change of Datacenter location (CR1)
1.2	23rd June 23	Update to align with Architecture clarifications.

Stakeholders Details

Role	Name	Signature
Author	Jean-Francois Suret Jean-Francois.Suret@ncia.nato.int Senior Architect, NCI Agency	Jean-Francois Suret Digitally signed by Jean-Francois Suret Date: 2023.06.30 11:45:46 +02'00'
Author	Marc Mengerink Marc.Mengerink@ncia.nato.int Senior Engineer, NCI Agency	Marc Mengerink Digitally signed by Marc Mengerink Date: 2023.06.30 11:54:00 +02'00'
Approver	Martin Diepstraten Martin.Diepstraten@ncia.nato.int POLARIS Technical Design Authority, NCI Agency	Martin Diepstraten Digitally signed by Martin Diepstraten Date: 2023.06.30 11:50:49 +02'00'

Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY

0001 Infrastructure as a Service (IaaS), provided as part of the NATO Operational Network (ON), is providing services to end users up to and including the NS classification. IaaS provides the foundation required for other services e.g. Client Provisioning Services (CPS), Enterprise Core Services (ECS) and Service Management and Control (SMC) Services. This Service Design Package (SDP) provides an integrated NATO ON IaaS design.

0002 IaaS comprises the main infrastructure installed at the Data Centres (DCs), Enhanced Nodes (ENs) and Standard Nodes (SNs), while Remote Nodes (RNs) and Service Operation Centres (SOC) rely on the DC for infrastructure services.

0003 The DC hosts the majority of the applications supporting ENs, SNs and RNs. The centralized IaaS solution reduces the need for individual projects to provide, operate and maintain hardware to support their capabilities.

0004 The IaaS solution adopts the following set of architecture principles defined in the Architecture Design Package (ADP) for the NATO ON and more specifically:

- Continuity
- Secure multi-tenancy
- Flexibility
- Scalability
- Virtualisation
- Automation
- Remote administration
- Future Proofing
- Standardisation
- user experience
- Green IT

2. INTRODUCTION

0005 The goal of the IaaS design is to detail how the IaaS deployment are and will be implemented (technical design) and operated to provide a private IaaS cloud infrastructure usable from any location within the NATO enterprise.

0006 IaaS consists of 8 services which will be detailed further in the document:

- Infrastructure Networking Services.
- Infrastructure Processing Services.
- Infrastructure Storage Services.
- Infrastructure CIS Security Services.
- Infrastructure Archive Storage Services.
- Backup and Recovery Services.
- Infrastructure SMC*, also referenced as IaaS Domain SMC.*
- Reference Environment (IREEN) *specific* Services.

2.1. Purpose and Scope

0007 The IaaS SDP describes the infrastructure services design aspects, including associated management services and interfaces, required to provide the infrastructure foundation of the NATO Enterprise ON Private cloud.

2.2. Document Organisation

0008 The organisation of this documents is as follow:

- ***Section 3 Service Design and Topology*** – Describes service internal architecture and key service/subservice concepts, implementation strategy and provides the distribution of services to IaaS locations
- ***Section 4 Service Solution*** – Describes each subservice solution and component implementation design for hardware/software, security measures and implementation design rationale for service levels
- ***Section 5 Service Management and Tools*** – Describes the detailed implementation for hardware/software component design of subservice area domain management and element management
- ***Section 6 Service Processes*** – Provides the list of standard operating procedures (SOPs) associated with NATO ON processes for design
- ***Section 7 Service Organisation Skill Level Requirements*** – Provides the level of manpower linked to skill levels
- ***Section 8 Service Measurement*** – Describes solution to collect, analyse and report the required KPI information
- ***Appendix A (Sub)Services Interface Control Document (ICD)*** – Provided for each subservice where the service is subdivided into multiple subservices
- ***Appendix B Component to ICD Mapping Table*** – Describes mapping of each hardware/software component (interface) to service interfaces that are identified either in internal subservices ICD or the external services ICD in the architecture design document ICD appendix
- ***Appendix C NATO ON Procedures and Work Instructions*** – Provides procedures associated with NATO ON processes related to the NATO ON technical services groups (IaaS, CPS, ECS, SMC)
- ***Appendix D NATO ON NCI Agency Roles and Responsibilities*** – Provides manpower required to undertake NATO ON operational and support task

- ***Appendix E NATO ON Service Placement Architecture*** – Provides the high-level service distribution architecture of the NATO ON capability.
- ***Appendix F NATO ON IaaS Service Placement Architecture*** – Provides the high-level Infrastructure services distribution architecture of the NATO ON capability.

2.3. Points of Contact

0009 The IaaS SDP is under the responsibility and maintained by ITM Engineering Team itm.engineering@ncia.nato.int .

0010 Changes to future design must be approved by Polaris Technical Design Authority (TDA).

POC	Role	Responsibility
itm.engineering@ncia.nato.int	Organizational Ownership	Shared Ownership of the SDP
POLARIStda@nr.ncia.nato.int	Polaris Technical Design authority	Approve the SDP

2.4. Glossary

0011 The common abbreviations found throughout this document are listed in Table 1 below. The reader is also invited to refer to the ITM Glossary of Abbreviations (link) and the NATO Glossary of Abbreviations (link).

Acronym or Term	Definition
AAA	Authentication, Authorisation, Accounting
ACL	Access Control List
AD	Active Directory
ARP	Address Resolution Protocol
ASM	Application Security Manager (BIG-IP)
ATC	Aggregated Transport Classes
AWS S3	Amazon Web Service Simple Storage Service
BGP	Border Gateway Protocol
BMS	Background Media Scan
BPS	Boundary Protection System
CA	Certificate Authority
CMP	Cloud Management Platform
CoI	Community of Interest
CPU	Central Processing Unit
DBRR	Data Backup, Replication and Recovery
DC	Data centre
DCI	Data centre Interconnect
DEM	Distributed Execution Manager
DFW	Distributed Firewall (VMware)

Acronym or Term	Definition
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoD	Department of Defence (US)
DR	Disaster Recovery
DRS	Distributed Resource Scheduling (VMware)
DSCP	Differentiated Services Code Point
DSM	Dual Stack Model
dvSwitch	Distributed vSphere Switch (VMware)
ECS	Elastic Cloud Storage
ECS SDP	Enterprise Core Service Service Design Package
EN	Enhanced Node
ESG	Edge Services Gateway
ESXi	Enterprise-class, type-1 hypervisor
GE	Gigabit Ethernet
GTM	Global Traffic Manager (BIG-IP)
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapters
HTML	Hyper Text Mark-up Language
HTTPS	Hyper Text Transfer Protocol Secure
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
ILB	The Integrated Load Balancer
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IPAM	IP Address Manager
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
iSCSI	Internet Small Computer System Interface
ITM	Information Technology Modernisation
LAN	Local Area Network
LB	Load Balancer
LDAP	Lightweight Directory Access Protocol
LTM	Local Traffic Manager
LUN	Logical Unit Number (SAN)
MAPI	Messaging Application Programming Interface

Acronym or Term	Definition
MIB	Management Information Base
MM	Model Manager
MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NDMP	Network Data Management Protocol
NFS	Network File System
NIC	Network Interface Controller
NII	Networking and Information Infrastructure
NR	NATO Restricted
NSX	VMware Network Virtualisation and Security Platform
NTP	Network Time Protocol
NU	NATO Unclassified
NVGRE	Network Virtualisation using Generic Routing Encapsulation
NVMe	Non-Volatile Memory Express
NVRAM	Non-volatile RAM
OOB	Out of band
OS	Operating System
ON	Operational Network
OSPF	Open Shortest Path First
PCIe	Peripheral Component Interconnect Express
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PBN	Protected Business Network
PSU	Power Supply Unit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RBD	Reliability Block Diagram
RE	Reference Environment
REST	Representative state transfer
RLO	Recovery Level Objectives
RN	Remote Node
RP	Rendezvous Point
RPO	Recovery Point Objective
RSTP	Rapid Spanning Tree Protocol
RTO	Recovery Time Objective
RU	Rack Unit

Acronym or Term	Definition
SAN	Storage Area Network
SAS	Serial Attached System Component Small Computer System Interface
SATA	Serial Advanced Technology Attachment
SCCM	System Centre Configuration Manager
SCSM	Storage Compartmented Security Mode
SDRS	Storage Distributed Resource Scheduling
SFTP	Secure File Transfer Protocol
SIOP5	Service Interoperability Point 5
SLA	Service Level Agreement
SMB	Server Message Block
SMC	Service Management and Control
SMTP	Simple Mail Transfer Protocol
SN	Standard Node
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SR-IOV	Single Root Input/Output Virtualisation
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
SSO	Single Signed On
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ToR	Top of Rack
UDP	User Datagram Protocol
UMDS	Update Manager Download Service
UTP	Unshielded Twisted Pair
VASA	vStorage APIs for Storage Awareness
VCHA	vCenter High Availability
vCPU	Virtual Central Processing Unit
VDI	Virtual Desktop Infrastructure
vDS	Virtual Distributed Switch
VLAN	Virtual Local Area Network
VLT	Virtual Link Trunking
VM	Virtual Machine
VMDK	Virtual Machine Disk
VoIP	Voice over Internet Protocol

Acronym or Term	Definition
VPN	Virtual Private Network
vRA	vRealise Automation
VRF	Virtual Router Forwarding
vRLI	vRealise Log Insight
vROP	vRealise Operation Manager
VRRP	Virtual Router Redundancy Protocol
vSAN	Virtual Storage Area Network
VTC	Video Teleconference
VTEP	Virtual Tunnel End Point
VxLAN	Virtual Extensible LAN
WAF	Web Application Firewall
WAN	Wide Area Network

Table 1 - Glossary of Terms and Abbreviations

2.5. Reference Documents

0012 The following documents pertinent to the IaaS are listed in Table 2.

Document	Description
Architecture Design Package (ADP)	Describes the NAT ON architecture, services, systems, organisational entities, and their relationships to each other and to their environment
Service Design Package – Client Provisioning Services (CPS)	Describes the NATO ON desktop delivery and management capabilities, application delivery, mobile device management, print, and scanning services, and wireless local-area network (LAN) connectivity for all NATO users.
Service Design Package – Enterprise Core Services (ECS)	Describes the NATO ON directory services, email messaging, unified communications, and portal services.
Service Design Package – SMC	Describes the NATO ON Enterprise SMC services and processes to monitoring and metering all NATO ON infrastructure and services
Service Placement	The Service placement details where the Service and sub-services are deployed in addition to detailing major dependencies with other services. The Service placement is complementary to the Service Design Package.
Service Placement Architecture	The Service Placement Architecture in Appendix E and F provide, at a conceptual level, a visualization of how/where services are implemented.

Table 2 - Reference Documents

3. SERVICE DESIGN AND TOPOLOGY

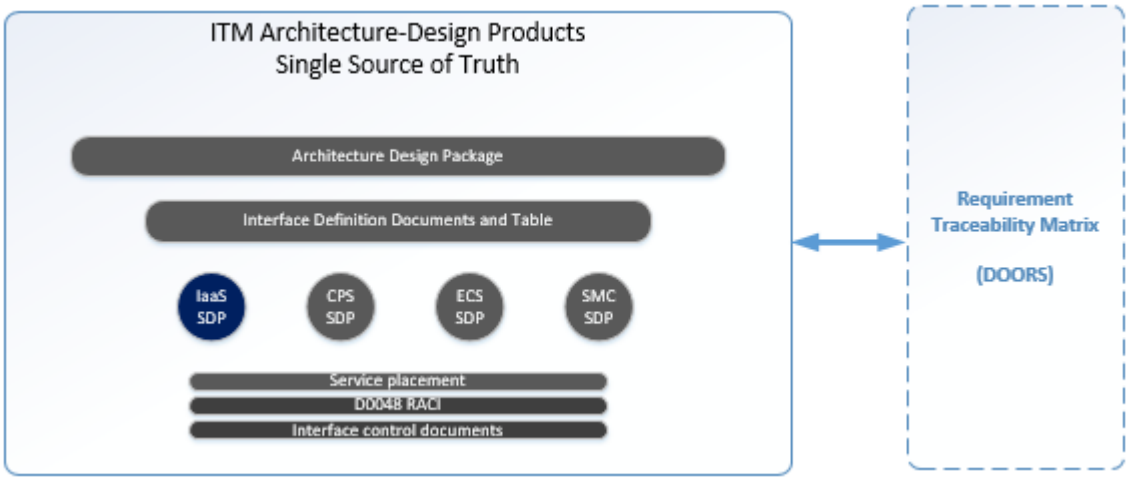
0013 The ADP is the overarching document describing the services implemented and/or leveraged to establish the NATO ON.

0014 This SDP details the IaaS services and subservices required to implement the NATO ON as per: Annex E NATO ON Service Placement Architecture v 1.0

0015 and,

Annex F NATO ON IaaS Service Placement Architecture v 1.0

0016 This SDP is part of the authoritative source of information regarding Architecture and Design aspects.



0017

Figure 1 - Architecture-Design Products

3.1. NATO Operational Network Infrastructure as a Service (NATO ON IaaS) General Aspects

0018 The NATO Operational Network Infrastructure as-a Service (NATO ON IaaS) is designed to provide centrally managed, secure, highly resilient and highly available services to support NATO.

0019 The NATO ON IaaS is composed of:

- A centralized Private IaaS cloud service instance at Data Centre (DC) locations (**NS Infra DC Node**).
- Locally deployed IaaS footprints at Enhance Nodes (EN) (**NS Infra Enhanced Node**) and Standard Nodes (SN) (**NS Infra Standard Node**).
- Remote Nodes (RN) are not hosting Infrastructure services, the only have a Campus LAN Segment providing user access to the NATO ON IaaS provided and hosted services.

0020 All services deployed at all nodes are implementing IPv6 (by default) and IPv4.

3.1.1. IaaS Node Relationship

0021 The Centralized NATO ON IaaS service at Data Centre (DC) locations is intended to host Enterprise services such as:

- Core Services (C3T - Core Services).
- Functional Application Services (C3T - Community of Interest Services).

- Backup and Recovery Services (to support EN/SN disaster recovery plans)
- Backup and Archive Services.

0022 (While limited to initially providing IaaS, the centralized cloud infrastructure is aimed at supporting PaaS, SaaS services in the future.)

0023 The ON IaaS is also composed of local footprints, to host essential services, at the various EN and SN Nodes. The IaaS local footprints, while ultimately part of the extended NATO IaaS cloud, are meant to host essential services to the local entity in order to ensure business continuity:

- Local Essential Core services (EN/SN).
- Local Essential Functional Application services (EN).

0024 ENs, SNs and RN's are logically paired to a DC for core service access. For ENs and SNs this also include disaster recovery. DCs themselves act as fail-over domain for each-other. The pairing between Nodes and Data Centre Locations is based on NCI network topology. (Best connectivity)

0025 The Figure below depicts the type of Services hosted on the IaaS at the various Node location, noting the location of the DC Nodes may still change depending on external factors (e.g. availability of the facility).

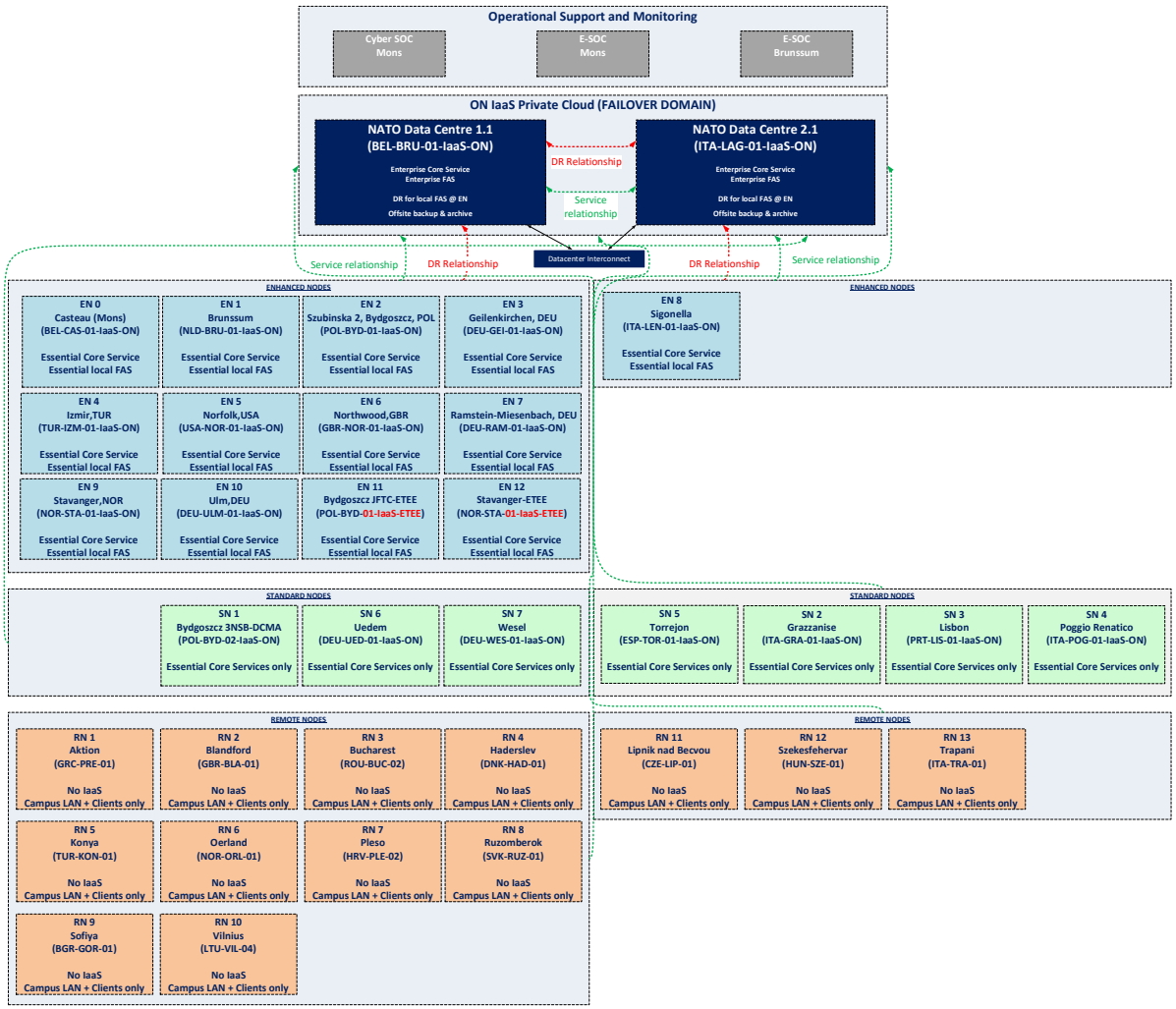


Figure 2 - Hosted Services per Node

And below the current list of sites /node types.

Site ID (location)	Node ID	Infrastructure Node Type	NS Infrastructure Node ID
BEL-BRU-01	BEL-BRU-01	NS DC Node	BEL-BRU-01-Infra-ON
BEL-CAS-01	BEL-CAS-01	NS Infra Enhanced Node	BEL-CAS-01-Infra-ON
BGR-GOR-01	BGR-GOR-01	NS Infra Remote Node	BGR-GOR-01-Infra-ON
CZE-LIP-01	CZE-LIP-01	NS Infra Remote Node	CZE-LIP-01-Infra-ON
DEU-GEI-01	DEU-GEI-01	NS Infra Enhanced Node	DEU-GEI-01-Infra-ON
DEU-RAM-01	DEU-RAM-01	NS Infra Enhanced Node	DEU-RAM-01-Infra-ON
DEU-UED-01	DEU-UED-01	NS Infra Standard Node	DEU-UED-01-Infra-ON
DEU-ULM-01	DEU-ULM-01	NS Infra Enhanced Node	DEU-ULM-01-Infra-ON
DEU-WES-01	DEU-WES-01	NS Infra Standard Node	DEU-WES-01-Infra-ON
DNK-HAD-01	DNK-HAD-01	NS Infra Remote Node	DNK-HAD-01-Infra-ON
ESP-TOR-01	ESP-TOR-01	NS Infra Standard Node	ESP-TOR-01-Infra-ON
GBR-BLA-01	GBR-BLA-01	NS Infra Remote Node	GBR-BLA-01-Infra-ON
GBR-NOR-01	GBR-NOR-01	NS Infra Enhanced Node	GBR-NOR-01-Infra-ON
GRC-PRE-01	GRC-PRE-01	NS Infra Remote Node	GRC-PRE-01-Infra-ON
HRV-PLE-02	HRV-PLE-02	NS Infra Remote Node	HRV-PLE-02-Infra-ON
HUN-SZE-01	HUN-SZE-01	NS Infra Remote Node	HUN-SZE-01-Infra-ON
ITA-GRA-01	ITA-GRA-01	NS Infra Standard Node	ITA-GRA-01-Infra-ON
ITA-LAG-01	ITA-LAG-01	NS DC Node	ITA-LAG-01-Infra-ON
ITA-LEN-01	ITA-LEN-01	NS Infra Enhanced Node	ITA-LEN-01-Infra-ON
ITA-POG-01	ITA-POG-01	NS Infra Standard Node	ITA-POG-01-Infra-ON
ITA-TRA-01	ITA-TRA-01	NS Infra Remote Node	ITA-TRA-01-Infra-ON
LTU-VIL-04	LTU-VIL-04	NS Infra Remote Node	LTU-VIL-04-Infra-ON
NLD-BRU-01	NLD-BRU-01	NS Infra Enhanced Node	NLD-BRU-01-Infra-ON
NOR-ORL-01	NOR-ORL-01	NS Infra Remote Node	NOR-ORL-01-Infra-ON
NOR-STA-01	NOR-STA-01	NS Infra Enhanced Node NS Infra Enhanced Node	NOR-STA-01-Infra-ON NOR-STA-01-Infra-ETEE
POL-BYD-01	POL-BYD-01	NS Infra Enhanced Node NS Infra Enhanced Node	POL-BYD-01-Infra-ON POL-BYD-01-Infra-ETEE
POL-BYD-02	POL-BYD-02	NS Infra Standard Node	POL-BYD-02-Infra-ON
PRT-LIS-01	PRT-LIS-01	NS Infra Standard Node	PRT-LIS-01-Infra-ON
ROU-BUC-02	ROU-BUC-02	NS Infra Remote Node	ROU-BUC-02-Infra-ON
SVK-RUZ-01	SVK-RUZ-01	NS Infra Remote Node	SVK-RUZ-01-Infra-ON
TUR-IZM-01	TUR-IZM-01	NS Infra Enhanced Node	TUR-IZM-01-Infra-ON
TUR-KON-01	TUR-KON-01	NS Infra Remote Node	TUR-KON-01-Infra-ON
USA-NOR-01	USA-NOR-01	NS Infra Enhanced Node	USA-NOR-01-Infra-ON

Table 3 - Current Location to Infrastructure Node Mapping

3.1.2. Centralized NATO ON IaaS: Cloud Regions and Availability zones

0026 The NATO ON IaaS infrastructure is designed to meet the cloud essential characteristics:

- On demand self-service (which maturity will evolve over time)
- Broad network access
- Resource pooling (Multi-tenancy support)
- Rapid elasticity (however constrained by physical facilities)
- Measured service

0027 In order to achieve its objectives, a cloud infrastructure is deployed according to Region, Data centre and Availability zone building blocks.

0028 **Regions** are defined by distinct locations. The distance between regions can be rather large. Regions contain one or more availability zones.

0029 **Availability Zones** are collections of infrastructure components, which could be hosted in data centres in a metropolitan area, or two safety zones within the same (large-scale) data centre. Availability zones are physically separated so that physical disasters only affect one zone at a time. An availability zones runs on its own, physical distinct, independent infrastructure (incl. power, cooling, security) and is engineered to be highly reliable.

0030 The current assigned NATO ON Data Centre locations (BEL-BRU-01, Brussels, and ITA-LAG-01, Lago Patria) are defined as separate regions due to the physical distance (~1700km) and network latency (>25ms). In addition, these locations currently do not provide the means to host multiple availability zones.

0031 This architecture and design of the ON IaaS takes into account that multiple availability zones per region will not be available. This means there are limitations to how applications and services are designed and implemented to meet availability requirement, and it is affecting how business continuity can be achieved.

0032 The NATO Centralized ON Private cloud is designed based on 2 Regions, in which at least a Data centre with one availability zone is implemented. The NATO ON Private cloud must take into account the need for future availability improvement and growth by adding availability zones in either the initial data centre or additional data centres in very close proximity to initial ones (to allow for high bandwidth/low latency between availability zones).

0033 With the initial data centres being in two different regions, and therefore be subject to high latency, the infrastructure itself does not provide synchronous replication of services between the two datacentres. Services hosted on the infrastructure will need to be designed and deployed based on such constraint. To deploy services in an active/active topology, services need to handle themselves the replication (when capable of handling high latency and potentially leveraging global load balancing capabilities).

0034 The two single availability zone datacentres act only as “paired” regions/availability zone to allow for the recovery of services as part of disaster recovery scenarios (but not without loss of data).

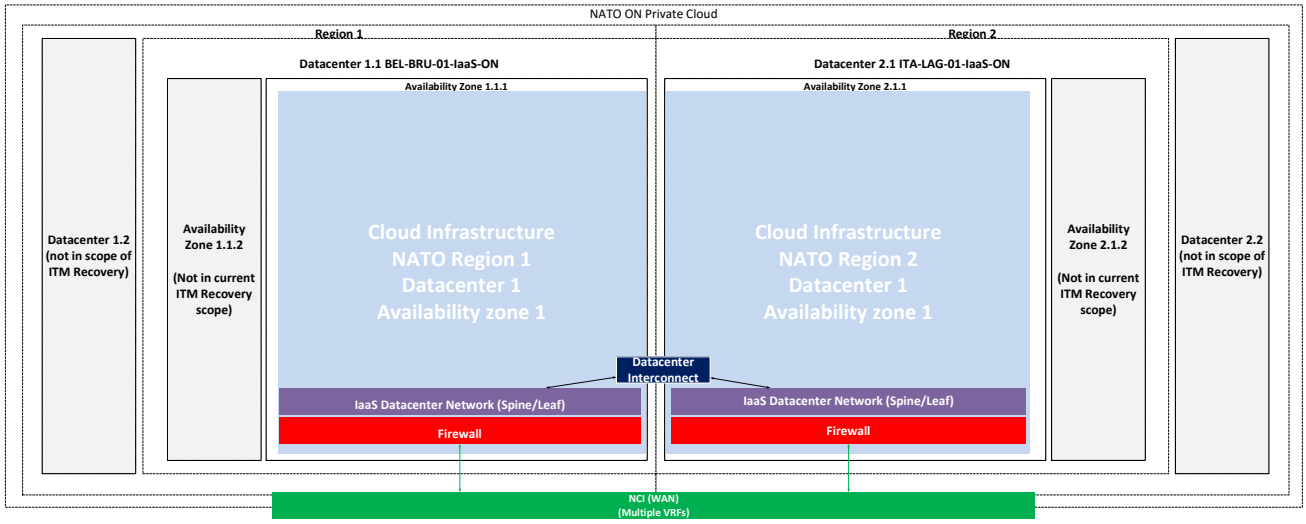


Figure 3 - NATO ON Private Cloud – Region, Datacentre, Availability Zone

3.1.3. IaaS Local footprints (Edge): Enhanced Nodes and Standard Nodes

0035 Due to the distributed nature of NATO sites (e.g. distance implying lack of high bandwidth/low latency between sites), only the datacenters meet the requirements to establish a Cloud capability.

0036 The Local Infrastructure as a Service footprints or Edge deployment, required to be deployed at the sites to ensure business continuity requirement for local entities, are therefore not part of the centralized NATO ON IaaS.

0037 Those IaaS Local footprints are considered an extension or edge cloud deployment, and will be dedicated to the provision of service to the Local entity. While the IaaS local footprint is scaled to only support the local entity, it is envisioned that the configuration could evolve to support multi-tenancy.

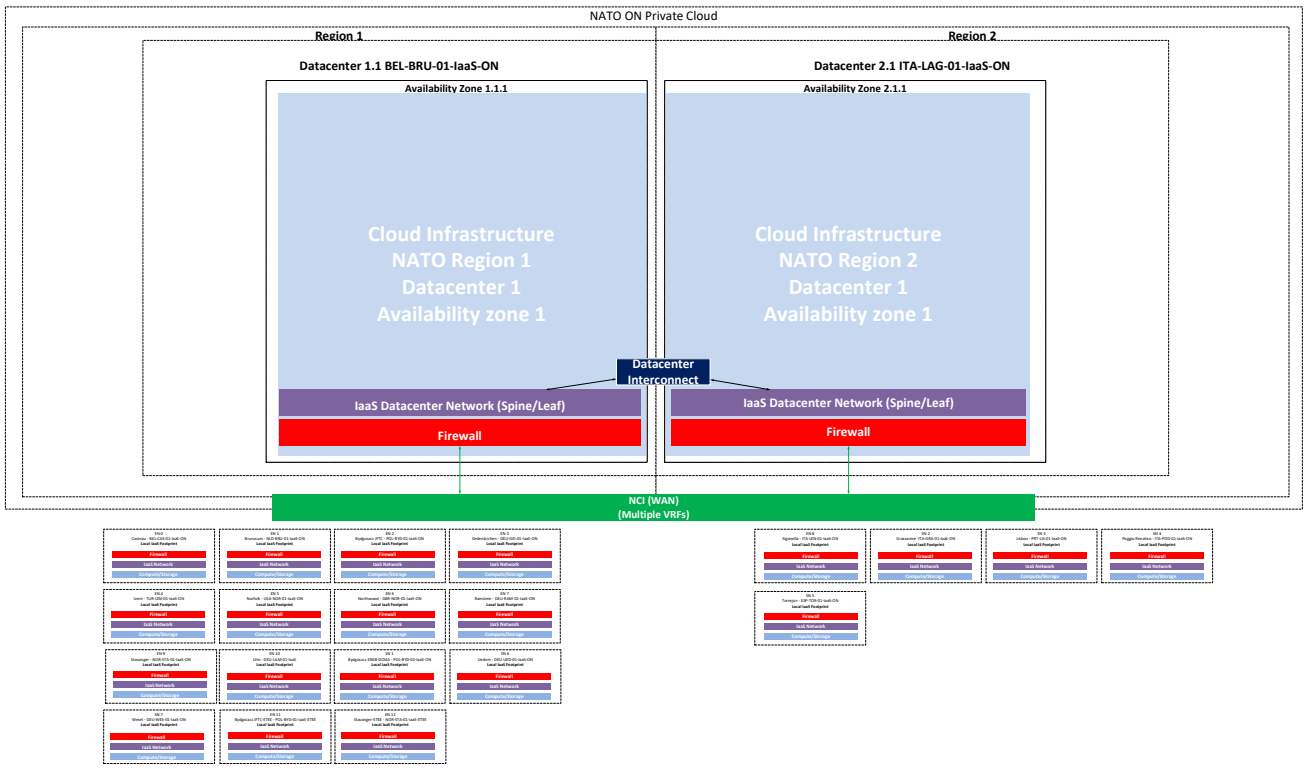


Figure 4 - NATO ON Private Cloud and IaaS Local footprints

3.1.4. Multi-Tenancy and Security zones

0038 This paragraph describes the NATO ON IaaS security zones and the concept of multi/single tenancy IaaS.

3.1.4.1. Multi-tenancy infrastructure:

0039 IaaS multi-tenancy infrastructures allows different tenants to share the same physical infrastructure (compute, storage and networking), while still keeping their business logic and data separate and secure.

0040 On a multi-tenancy IaaS, a Tenant will have its resources logically separated from other tenants, requiring appropriate security measures in order to protect data and restrict access between tenant services. (Security zoning, Firewalling, Virtual Resource Pools separation, encryption etc.)

3.1.4.2. Single-tenancy infrastructure:

0041 Single-tenancy is considered for complete physical isolation of compute and storage (and potentially the network physical infrastructure and BPS).

0042 A required single-tenancy infrastructure is the Infrastructure serving the Reference Environment, as this environment will require complete isolation of the operational environments to allow isolated testing of infrastructure software and hardware implementations/upgrades.

3.1.4.3. Management infrastructure:

0043 Multi-tenancy is not applicable to the infrastructure that hosts the tools which manage the IaaS. The Management domains that contain the tools and services to manage the IaaS service run on a dedicated physically separated infrastructure.

3.1.4.4. Security Segment:

0044 A security segment is a logical security boundary internal to a tenant (e.g. VLANs).

3.1.4.5. Tenant resources:

0045 Tenant resources are logical or physical resources allocated to a specific Tenant. A Tenant may be allocated resources from multi-tenancy and/or single-tenancy infrastructures.

3.1.4.6. Security Zone:

0046 A security zone in the context of the NATO ON IaaS refers to the logical extension of an IaaS Tenant resources across all locations (Datacentre Availability Zones, ENs, SNs). Security zones are also defined when resource need to be logically isolated as for example the management services.

0047 While the security zones and their tenancy mapping may be updated as part of the development of a cyber-security design during future phases, the NATO ON Private IaaS cloud provides Secure IaaS and is expected to initially support the following security zones:

- ACT/ACO (Bi-SC) (NATO-ON-SZ-TNT-001)
- Exercise and Training environments (ETEE), which are initially deployed as Single Tenant Enhance Nodes in 2 locations. (NATO-ON-SZ-ETEE-001)

- Reference environment(s), which is initially deployed on Single-Tenancy Infrastructure(s). (NATO-ON-SZ-REF-001)
- Common Infrastructure and Common Core Services: common services for all end-users, devices, and applications facing services. (NATO-ON-SZ-SRV-001)
- NATO ON Management Services: Infrastructure management services, excluding Organization tenant services, only accessible from infrastructure administrators and Cyber security services. (NATO-ON-SZ-MGT-001)
- NATO Cyber Security Services. (NATO-ON-SZ-SEC-001)

0048 Table 4 below shows the initial NATO ON IaaS mapping to security zones and tenancies.

	Available on Tenancy type(s)		Security zone at specific node type		
Security Zone	**Multi-Tenancy**	**Single-Tenancy**	**DC site**	**EN site**	**SN site**
ACT/ACO (Bi-SC) (NATO-ON-SZ-TNT-001)	yes	no	yes	yes for all ACT/ACO ENs	yes for all ACT/ACO SNs
Exercise and Training environment(s) (ETEE) (NATO-ON-SZ-ETEE-001)	not initially	yes	not initially	limited to 2 locations	no
Reference environment(s) (NATO-ON-SZ-REF-001)	no	yes	yes	no	no
NATO ON Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	yes	no	yes	yes for all	yes for all
NATO ON Management Services (NATO-ON-SZ-MGT-001)	No (to be revisited during HLD)	yes	yes	yes	no (to be revised during HLD)
NATO Cyber Security Services (NATO-ON-SZ-SEC-001)	For distributed services	For centralized services	yes	For distributed services	no

Table 4 - ON IaaS Initial Security Zones and Tenancy type mapping

0049 While there are initially only single Datacentre/Availability zone deployments, the tenants would be extended between Availability zones of a single region if additional availability zones were implemented.

0050 The NATO ON Private IaaS cloud leverage the Datacentre interconnect to extend the security zones **across regions**.

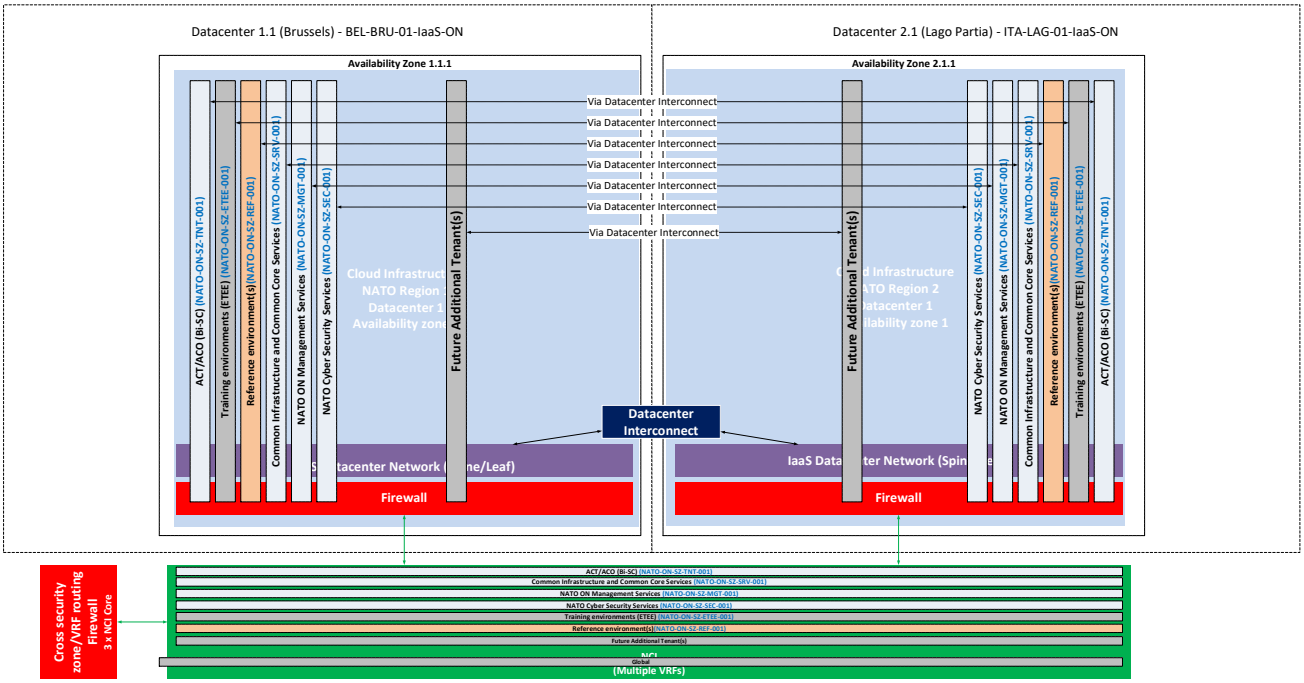


Figure 5 - ON IaaS Initial Security Zones

0051 The “Extension” of the tenants over the WAN (NCI) to other Nodes will leverage dedicated NCI VRF per security zone in order to maintain the traffic separated over the WAN.

3.2. Service Model [Pending Updates During Detailed Design and Implementation]

The IaaS service consists of 8 subservices. **Figure 6** depicts the current hierarchy and known characteristics.

Figure 6 - Service Architecture Hierarchy (Visio)

0052 The subsequent sections outline the subservice topology and design of all components that make up IaaS.

0053 ITILv3 2011 was used in the development of the IaaS solution to deliver upon the five service lifecycle stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service improvement. Table 5 lists the high level activities and needs of the service throughout its life cycle to orchestrate successful service creation, transition to production, management of work, and service improvement. Additional and specific details related to the service life cycle activities, schedules, and needs shall be contained within the document such as the Project Management, Implementation, Risk and Configuration Management Plans.

Service Needs Throughout its Lifecycle:	Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Strategy, goals and objectives defined	X				
Policies defined	X	X	X	X	X
Business and service requirements defined	X				
Management of risks and issues	X	X	X	X	X
Common architecture for consistent design		X			
Define and translate business requirements		X			

Service Needs Throughout its Lifecycle:	Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement
Service and process design and development activities		X			
Personnel/group roles, responsibilities, and skills		X	X	X	
Project management, coordination and integration with other services or processes		X	X		
Communication and training plans		X	X	X	
Service integration and testing activities			X		
Quality and control of service delivery			X		
Gantt chart with project stages and timelines			X		
Service transition and acceptance criteria planning		X	X	X	
Transition service into production without disruption			X		
Service operational acceptance test			X	X	
End-to-end best practices for responsive and stable services				X	
Day-to-day service support and management functions				X	
Deliver services to customers at agreed levels with minimal interruptions				X	
Service operational monitoring				X	
Align services with the business needs	X	X	X	X	X
Recognise service improvement opportunities and change	X	X	X	X	X
Continual service and process assessments	X	X	X	X	X

Table 5 - Service Needs Throughout Each ITIL Lifecycle Stage

3.3. Subservice Topology

0054 This section discusses the distribution of IaaS subservices of processing, storage, networking, infrastructure SMC, CI security, Infrastructure Archive Storage, Backup and Recovery, Infrastructure SMC to the NATO ON DCs including IREEN and SOCs, ENs, SNs.

0055 While the NATO ON service placement identifies all services and sub services and their relationship with nodes and dependencies with other major services, Table 6, shows a

simplified overview of the relationship between systems and subservices to deliver functionalities at DCs, ENs and SNs.

System/ Subservice	Sub-system/sub process	IaaS Component	DC IaaS	EN IaaS	SN IaaS
Infrastructure Processing	Virtualised Processing	Processing	vSAN Ready Node	vSAN Ready Node	vSAN Ready Node
Infrastructure Processing	Operating System	Hypervisor and OS	VMware ESXi	VMware ESXi	VMware ESXi
Infrastructure Storage	Block-Level Storage	Storage	vSAN Ready Node optional: SAN/NAS (external to VSAN)	vSAN Ready Node optional: SAN/NAS (external	vSAN Ready Node
VDI Storage	Block-Level Storage	Storage	vSAN Ready Node	vSAN Ready Node	vSAN Ready Node
Infrastructure Storage	File-system storage	Storage	vSAN Ready Node optional: SAN/NAS (external	vSAN Ready Node optional: SAN/NAS (external	vSAN Ready Node
Infrastructure Networking	Switching	Core Switching	Cisco ACI, VMware NSX	Cisco ACI, VMware NSX	Cisco ACI, VMware NSX
Infrastructure Networking	DDI	DNS	Windows Server	Windows Server	Windows Server
Infrastructure Networking	DDI	DHCP	Windows Virtual Machine and Global Load balancing	Windows Virtual Machine	Windows Virtual Machine
Infrastructure Networking	DDI	IPAM	Infoblox DDI	Managed from Datacentre	Managed from Datacentre
Infrastructure Networking	Global Load Balancing	Load Balancer	F5 GSLB and/or Infoblox	Managed from Datacentre	Managed from Datacentre
Infrastructure Networking	Local Load Balancing	Load Balancer	LTM virtual appliances, F5 Big IQ and	LTM virtual appliance	LTM virtual appliance

System/ Subservice	Sub-system/sub process	IaaS Component	DC IaaS	EN IaaS	SN IaaS
			F5 physical appliance		
Infrastructure Networking	Data Transfer	Data replication	Veeam, VMware vSphere Replication	Veeam, VMware vSphere Replication	Veeam,
Infrastructure SMC		Configuration Management	BMC Service Management (Remedy)	BMC Service Management	BMC Service Management
Infrastructure SMC		Event Management	BMC TrueSight vRLI	BMC TrueSight vRLI	BMC TrueSight vRLI
Infrastructure SMC		Performance & Capacity	BMC TrueSight VMware vRops	From DC	From DC
Infrastructure SMC		Automation & orchestration	vRealize Automation, Ansible, Git, Terraform and others VMware SRM	vRealize Automation VMware SRM	vRealize Automation
Infrastructure SMC		Backup and Archiving	VEAM/vSAN ready node/T1&T2/3 backup server and T4 Object Storage	VEAM/vSAN ready node/T1&T2 backup server	VEAM/vSAN server/T1&T2 backup server
Infrastructure CIS Security	BPS	BPS1 Firewall	Palo Alto	Palo Alto	Palo Alto

Table 6 - IaaS Design Relationship between Systems and Subservices to Functionality

0056 The capacity aspects will be detailed as an annex of the SDP since capacity management shall not impact the service design itself.

3.4. Infrastructure Processing Subservice Topology

0057 The NATO ON infrastructure processing solution consists of the compute platform, virtualisation layer, and the orchestration layer.

0058 In term of server and storage, the IaaS is to use a virtualization solution leveraging commodity hardware to implement Hyper converged infrastructure solutions (e.g. vSAN ready nodes, Openstack, etc.) for ease of deployment and maintenance.

0059 While dedicated storage system/appliance may be more adapted for application requiring a lot of storage, the IaaS itself will benefit from standardized commodity hardware, allowing to provide scalability and flexibility as per the architecture principals.

3.4.1. Centralized NATO ON IaaS

0060 The Centralized private cloud consist of the following building blocks per availability zone:

3.4.1.1. Management domain

- One or multiple Management cluster(s) to isolate the cloud management services (required from security and business continuity point of view).
- The management clusters are not to host Tenant services but only cloud management services.

0061 The management resource clusters are required to be physically separated to meet AC/322-D/0048-REV3 "POS2-10 Administration tools, if virtualized, are done so on dedicated physical servers"

3.4.1.2. Workload domain:

- One or multiple “General” cluster(s) for multi-tenant workloads (Multi-Tenancy IaaS)
- One or multiple “Database” cluster(s) for multi-tenant database workload (allowing to optimize license costs), but excluding databases used by cloud management services. (Multi-Tenancy IaaS)
- One or multiple “Security” cluster(s) for hosting Cyber Security services for the NATO ON (Single-Tenancy IaaS *unless the services are later approved to run on Multi-tenant IaaS*)
- One or multiple VDI clusters for supporting local users and act as VDI disaster recovery resource pool (Multi-Tenant PaaS)
- One or multiple disaster recovery clusters to support EN disaster recoveries (Multi-Tenancy IaaS).
- One or multiple DMZ clusters, dedicated for proxy/reverse proxies and other communications between tenants and to external CIS (Multi-Tenancy IaaS by default unless Single-Tenancy required).
- One or multiple clusters for container specific clusters.
- One or multiple clusters for Pre-production specific clusters (to support Reference Environment (IREEN) Services Subservice Topology).

0062 The DMZ clusters are required to meet AC/322-D/0048-REV3 "NWS2-3 For system components providing services which are accessible from another CIS, the CIS implements a DMZ to separate those components from other CIS components" and “POS2-9 BPC are not hosted on the same physical server as the VMs they protect"

3.4.1.3. Other building blocks:

0063 While not part of the multi-tenant virtual infrastructure itself, additional servers and storage are providing services allowing to implement the NATO ON IaaS.

- Physical servers for domain controllers (to support business continuity).
- Physical Boundary Protection Devices (e.g. Firewalls)

- Management servers (for services not part of the cloud infrastructure and to support business continuity)
- Physical servers for services not supported on the virtual infrastructure (originally Exchange services were planned as non-virtual services, such design aspect **will be re-assessed**).
- The NATO SIEM based on Splunk, which exist today part of NCSC infrastructure and is to be scaled up to support the new load and services.
- Physical load balancers, used for at least physical workload and DMZs.
- Backup storage and services (Hardware already procured need to be scaled up and change of software compared to NATO ON initial baseline).
- Archive storage and services (Elastic cloud storage for which the already procured capacity need to be reviewed)

0064 In addition to those building blocks, interfaces to other existing system and services are required.

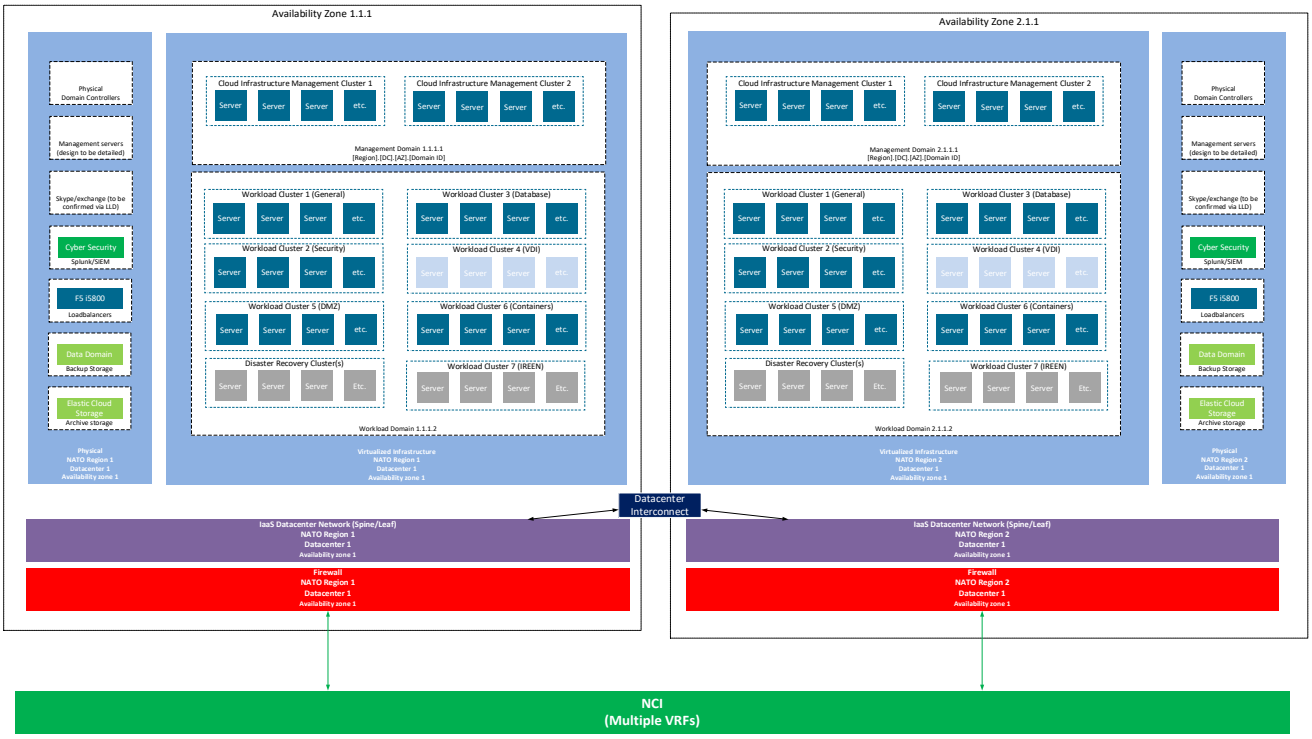


Figure 7 - NATO ON Private Cloud Resource Pools (NS Infrastructure DC Node)

3.4.2. IaaS Local footprints

0065 While the IaaS local footprints for the Enhanced Nodes are critical for business continuity and are composed of workload and management domain/resource clusters, the Standard Nodes will be composed only of a centrally managed Workload cluster and/or a shared Workload/Management domain/resource cluster.

3.4.2.1. Enhanced Nodes IaaS (NS Infrastructure EN Node)

0066 Enhanced Nodes IaaS are composed of both a Workload and Management Domain with at least one resource cluster each (dependent on the sizing required at the local site):

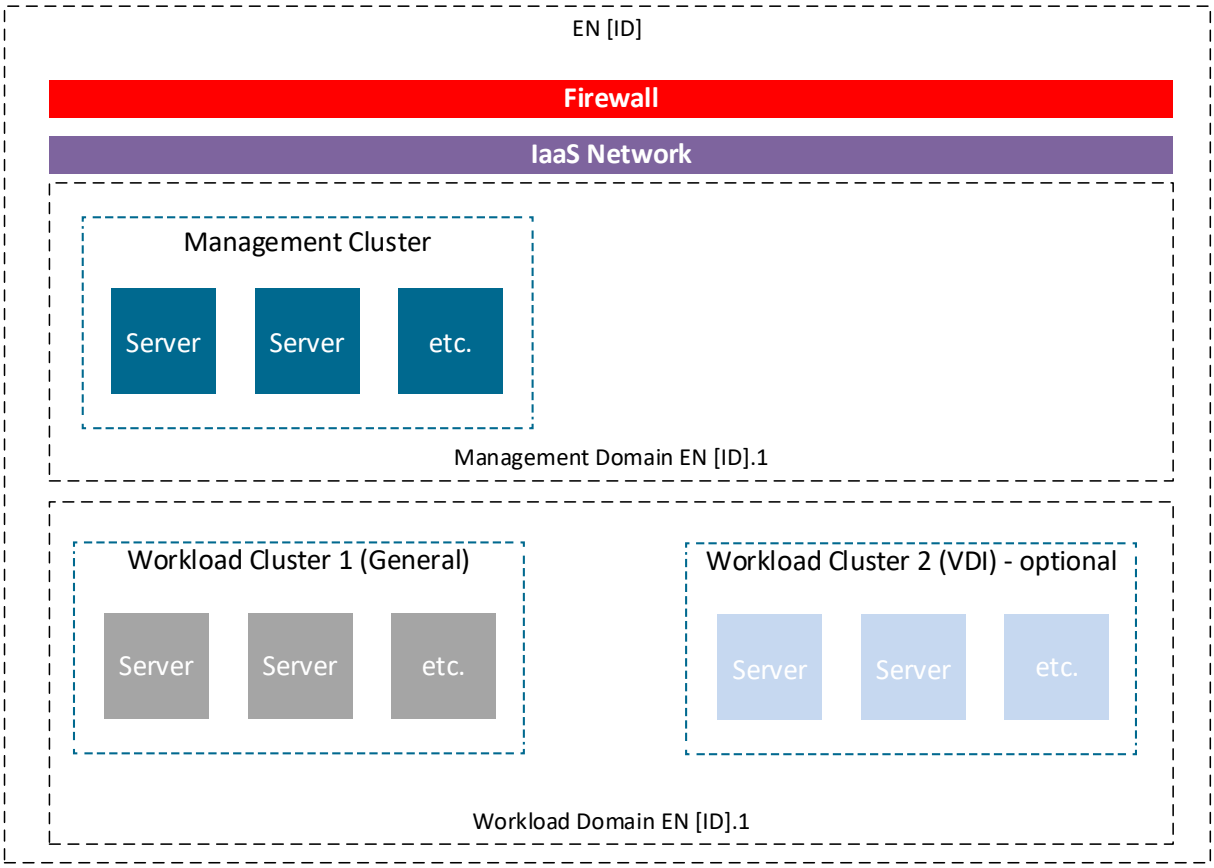


Figure 8 - IaaS Local Footprint (Edge) - Enhanced Node Resource Pools

0067 Some ENs are provided with VDI capabilities and will require dedicated VDI resource cluster.

3.4.2.2. Standard Nodes (NS Infrastructure SN Node)

0068 Standard Nodes IaaS are composed of a single multi-tenant Workload domain resource cluster managed from a centrally hosted management system. *(Depending on the deployment models defined during High-level design development, it may be required to change this to a single consolidated Management/Workload Domain resource cluster*)

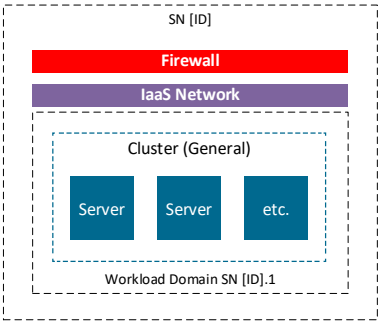


Figure 9 - IaaS Local Footprint (Edge) - Standard Node Resource Pools

3.4.3. Resource pooling overview

0069 The figure below depicts the initial resource clusters expected at each site to implement the ON IaaS services.

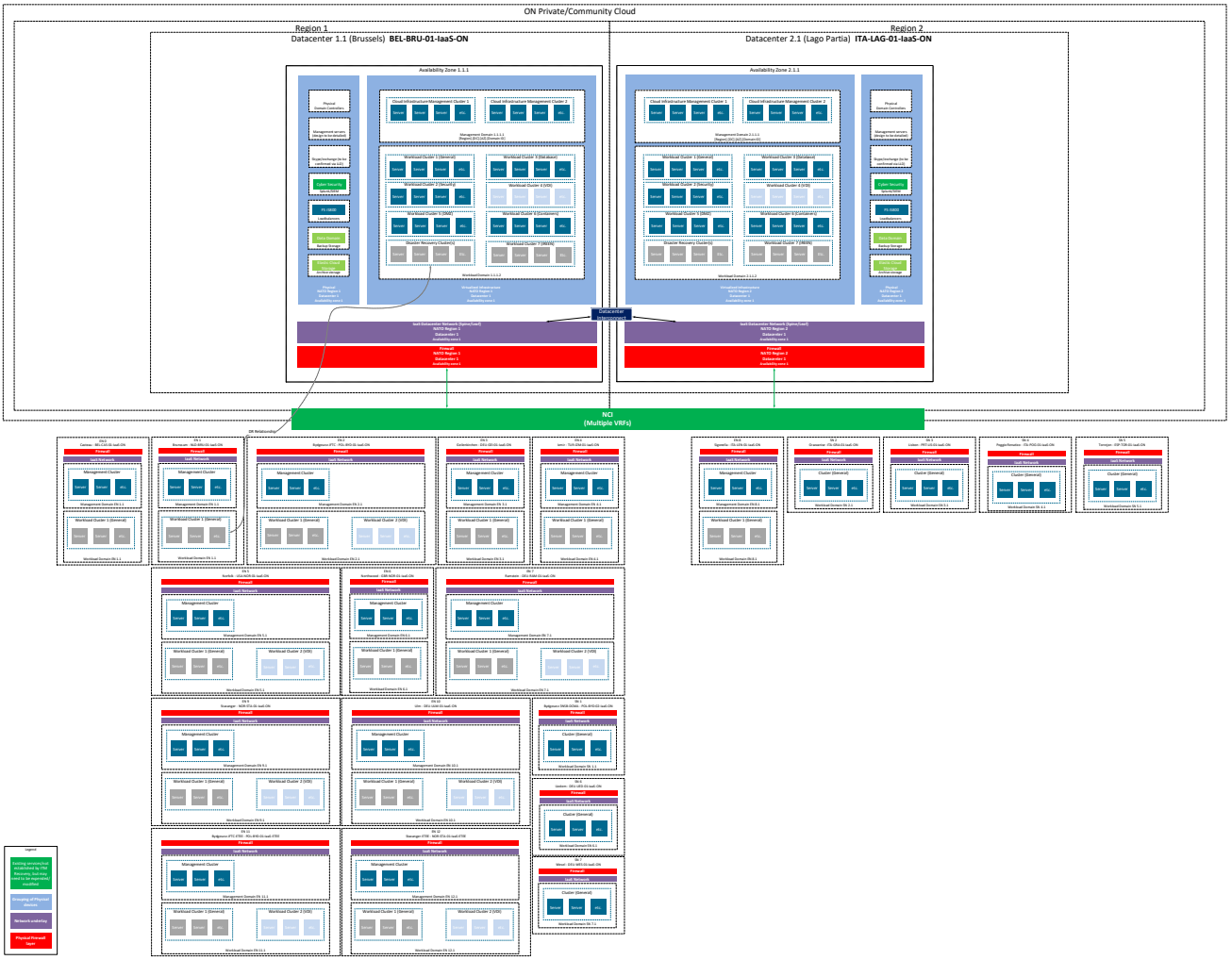


Figure 10 - Resource Pools overview

0070 The NATO ON compute platform service is standardised on VSAN Ready nodes for all virtual services. The server configuration for IaaS is standardised to allow flexibility when allocating or reallocating resources between node types.

0071 While server models are leveraging vSAN ready nodes, different builds are defined per usage to allow for better licensing and investment efficiencies (e.g. database clusters and VDI clusters have a different configuration)

3.4.4. Virtualisation Layer Topology

0072 The NATO ON Virtualisation service is mainly built leveraging vSAN validated servers and VMware vCloud Suite. The VMware vCloud suite leveraged for the NATO ON is depicted below[1]:

1 NOTE: VMware is changing their products names, this will be reflected in the next SDP.

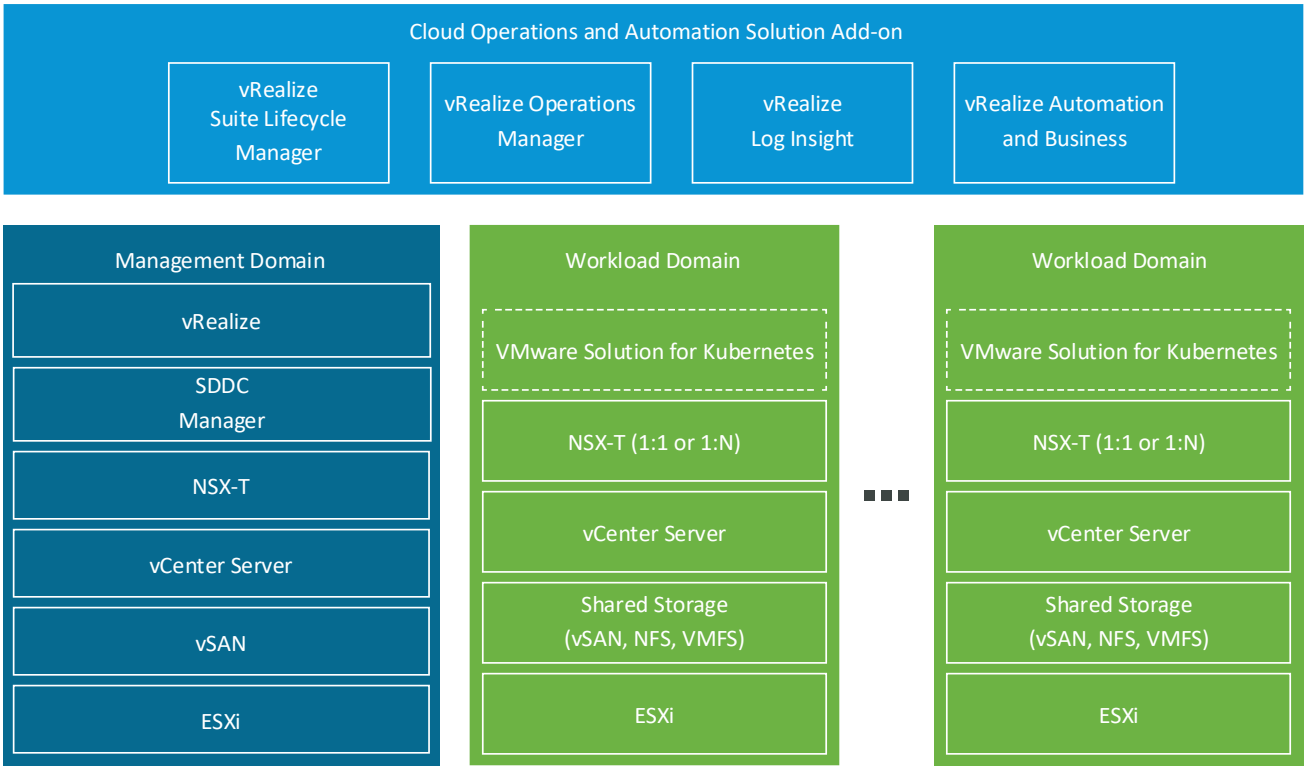


Figure 11 - NATO ON VMware vCloud suite

0073 While VMWare workspace one (part of vCloud) is not depicted, the component will be considered during implementation phase if it is identified as required and decreases the complexity/allow for quicker implementation.

0074 Table 7 lists the specific VMware components deployed by site and cluster:

Sub-service/component	Clustering Domain	Resource Cluster	Site
VMware vCenter (Management)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
VMware vCenter (Workload)(DC)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
VMware vCenter (Workload)(EN)	Management Domain	Cloud Infrastructure Management cluster [ID]	EN
VMware vCenter (Workload)(SN)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
VMware Update Manager	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
vRealize Automation (vRA)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
vRealize Operations Manager (vROps)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
vRealize Operations Manager (vROps) collectors	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
NSX-T Manager Global	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
NSX-T Manager (MGT)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
NSX-T Manager (Workload)(DC)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
NSX-T Manager (Workload)(EN)	Management Domain	Cloud Infrastructure Management cluster [ID]	EN
NSX-T Manager (Workload)(SN)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
vRealize Log Insight	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
vRealize Network Insight	Management Domain	Cloud Infrastructure Management cluster [ID]	DC

VMware Site Recovery Manager (MGT)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
VMware Site Recovery Manager (Workload)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
vRealize Suite Lifecycle Manager	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
vRealize Business	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
SDDC Manager (To be defined during implementation)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN

Table 7 - VMware components per Node type

0075 VMware services are hosted on the Cloud Infrastructure Management cluster to provide resource isolation.

0076 Production, test and end user facing applications shall not use the Management cluster resources reserved for management, monitoring and infrastructure services.

0077 Placing all management, monitoring and infrastructure services in a dedicated highly available cluster provides higher availability for these critical services.

0078 Access controls and permissions are configured to limit access to only administrators (Physical BPS, micro segmentation, and authentication). This protects access to the VMs running the management, monitoring and infrastructure services.

Figure 12 - NATO ON Major VMware components per Node.

3.4.4.1. VMware vCenter

0079 VMware vCenter is used for the centralized management of the VMware resources. While the intent is to centralize and automate the deployment of virtual resources, VMware vCenter is required to be deployed locally at ENs in order to allow for management and monitoring of the virtual platform in case of WAN outages.

0080 The vCenter(s) managing Standard Nodes will be deployed in the DC IaaS as per the DR mapping depicted in 3.1.1.

0081 Each vCenter is deployed as a vCenter HA cluster.

3.4.4.2. VMware Update Manager (VUM)

0082 VMware Update Manager is part of VMware vSphere. VUM is leveraged either for manual or orchestrated updates and upgrades. VUM is now bundled as part of vCenter appliance and does not need to be deployed separately.

3.4.4.3. vRealize Automation (vRA) / Aria Automation Orchestrator

0083 vRealize Automation enables administrators to automate the deployment of a set of VMs, or a blueprint of the way a particular set of VMs should be deployed. It provides a secure portal where authorised administrators, developers or business users can request new IT services and manage specific cloud and IT resources, while affirming compliance with business policies.

0084 The vRA services are deployed in the centralized DC IaaS and protected with SRM for disaster recovery (vRA is only active in one region at a time).

0085 vRealize automation is configured in order to allow for tenant self-provisioning of VMs with the latest approved operating systems.

0086 Additional automation is added over time to expend the self-provisioning to core and functional services.

3.4.4.4. NSX-T

0087 On the NATO ON, NSX-T is mainly used to implement the network virtualization and micro-segmentation. The intent is to leverage Cisco ACI for the overlay network, limiting the deployment of edge nodes to only necessary scenarios.

0088 NSX-T Managers are deployed for each node according to the breakdown in 3.4.4. In addition global managers are deployed in the IaaS DC to federates the instances and allow for a single pane of glass management.

3.4.4.5. vRealize Operations Manager (vROps)

0089 vRealize Operation Manager allows to have a detailed oversight of the capacity and usage of the resources. It is deployed as large cluster in the main datacentre (Region 1) with remote collectors deployed at each DC and EN locations.

3.4.4.6. vRealize Log Insight

0090 vRealize Log Insight clusters are deployed in each DC IaaS. The configuration allows for high availability and increased log ingestion rates.

0091 All VMware specific syslog data are first collected by Log Insight and then forwarded to the SIEM/central logging (based on Splunk).

3.4.4.7. Tanzu (Kubernetes)

0092 Tanzu is deployed on dedicate workload cluster(s) at the datacentres locations in order to provide kubernetes cluster(s) (container orchestration).

0093 Tanzu Grid is deployed on the management cluster(s) at the datacentre to manage the kubernetes cluster(s) and allow to maintain consistency of the Tanzu clusters and ease the deployment of containers.

3.4.4.8. vRealize Network Insight

0094 vRealize Network Insight clusters are deployed in each DC IaaS.

0095 It is used to provide analytics regarding network traffic and allow for troubleshooting issues.

0096 The primary datacentre will host the active Platform cluster, while the secondary DC will be used in case of outage at the primary DC.

0097 Agents will be deployed at least in both datacentres and potentially at EN and SNs.

3.4.4.9. VMware Site Recovery Manager

0098 VMware Site Recovery Manager is used to orchestrate business disaster recovery procedures and enable business continuity. VMware SRM leverages the vSphere replication and backup replication services as described in 3.9.3 Infrastructure Replication Services - Disaster Recovery .

3.5. Infrastructure Networking Subservice Topology

0099 The infrastructure networking subservice consists of core switching, Border protection services, load balancing, IP addressing, and Quality of Service (QoS) policy services. It shall be noted that all networking services must be implemented as dual stack supporting IPv6 and IPv4.

3.5.1. Core Switching Topology

0100 The physical network, used as Underlay network, is composed of a cost effective and reliable **2 Tier Leaf and Spine switching topology**.

0101 Cisco networking switches are leveraged to implement the network core switching for the DC, EN and SN.

0102 In leaf and spine switch design, the spine switch acts as a data centre aggregation switch providing Layer 2 Ethernet switching and Layer 3 routing services. The leaf switch acts as the datacentre access-edge switch, providing Layer 2 Ethernet switching service to end devices.

0103 Dedicated Leaf switches are used for external connectivity, towards the Physical firewalls.

0104 External switches are used for external connectivity, between the Physical firewalls and NATO WAN (NCI).

0105 Out of band management switches are expected to be deployed in each rack and connected to NCI, however for large deployment, an Out of band management aggregation switch will be required to reduce the number of interfaces towards NCI our of band management network.

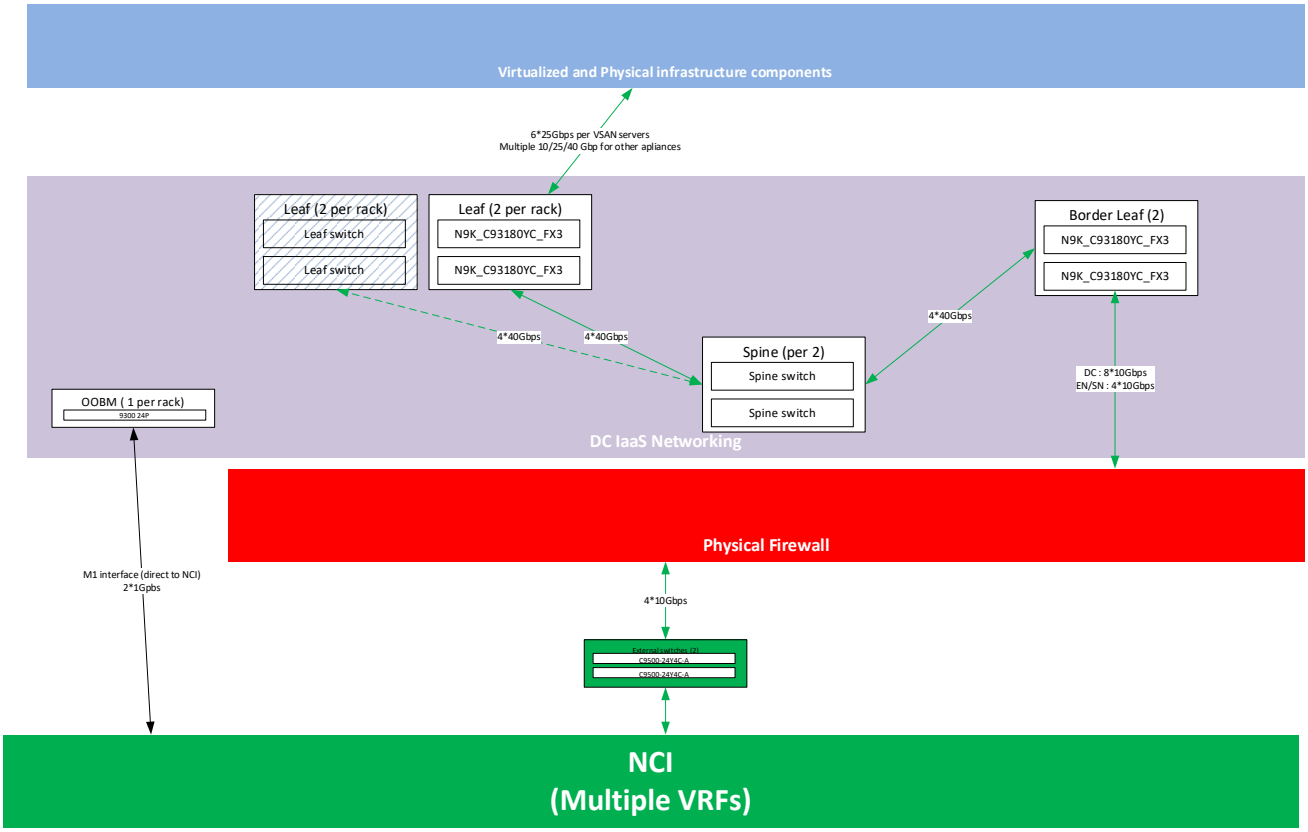


Figure 13 - Leaf and Spine Topology

0106 NATO ON core switching equipment listed below detail the product models and their corresponding use case.

Product	Use Case	Performance	Density	Resiliency
Cisco N9K_C9364C_GX_	DC Spine	12.84 Tbps	64*40/100 Gbps 2* 1/10G SFP+	Redundant hot swappable power supplies and fans
Cisco N9K_C93600CD_GX	EN/SN Spine Switch	12.8 Tbps	28*40/100 Gbps (QSFP28) 8*40/100 (QSFP-DD)	Redundant hot swappable power and fan
Cisco N9K_C93180YC_FX3	Leaf switch	3.6 Tbps	48 x 1/10/25 Gbps 6 x 40/100 Gbps	Redundant hot swappable power and fan
Cisco C9300_24T_A	Out of band management switches	208 Gbps	24*10/100/1000	Redundant power
Cisco C9500_24Y4C_A_	External switches	2 Tbps	24*1/10/25 4*40/100	Redundant hot swappable power and fan

Table 8 - NATO ON Core Switching Equipment

0107 The current topology requires from the design:

- Each Leaf to have 40Gbps uplinks to each of the Spine switches.
- Leafs do not directly connect to other leaves.
- Leaf switches are also known as the Top of Rack switch (TOR), connecting Hardware Servers (e.g. ESXI Hosts) to the underlay network using 25Gbps interfaces.

- Each Hardware Server has minimum four physical 25Gbps Network Interface Cards (NIC) but may require 6 or more interfaces.
- Appliances and Bare Metal servers connect in a similar way as Hosts to the Leaf Switches with 10G, 25G and/or 40Gbps interfaces (the quantity of Physical interfaces will vary).
- Connections outside of the IaaS is performed by designated Border Leaf switches. The Border Leaf switches interface via the physical firewall through 10/25/40/100 Gbps interfaces depending on the type of Node and its size.
- The Data Centre Interconnect (DCI) is provided through a Border leaf switch via a 100Gbps interface at NATO ON DC IaaS locations only.

0108 The components required to implement and manage the switches are described in the Domain SMC chapter 3.10.3.

3.5.2. Network, Firewall and Security – Border Protection Services

0109 The following are 3 major aspects driving the IaaS architecture and design:

- Certified Firewall are required at the boundary of a CIS/security zone and cannot be virtualized on the same hardware hosting services ("*BPC are not hosted on the same physical server as the VMs they protect* "from AC/322-D/0048-REV3 (INV)).
- The implementation of software define networking and virtualization requires an underlay and an overlay network and must rely on a cost efficient and reliable solutions.
- There shall be no single point of failure.

3.5.2.1. Intra Security Zone

0110 As part of the Centralized NATO ON IaaS or Local IaaS footprint, segmentation within a Tenant/Security zone is mainly performed via micro-segmentation capabilities (e.g. VMWare distributed firewall, Cisco ACI EPGs and/or virtualized security controls).

0111 When a Tenant is deployed across multiple infrastructures hosted at different Nodes, the information flow within the security zone will in addition cross the physical boundary protection Firewall and the WAN.

0112 Automated provisioning of Virtual Machine is expected to allow specifying not only the Security zone to which the Virtual Machine belongs, but the logical/micro-segmented zone parameters, load balancing, reverse proxy and additional settings, which will be defined over time.

3.5.2.2. Inter Security Zone

0113 As part of the Centralized NATO ON IaaS or Local IaaS footprint, segmentation between security zones is performed via a layer of certified Firewall. As part of ITM Recovery increment 1, this is realized by physical Palo Alto Firewalls. The figure below depicts the boundaries of security zones and how traffic must flow from one security zone to the other.

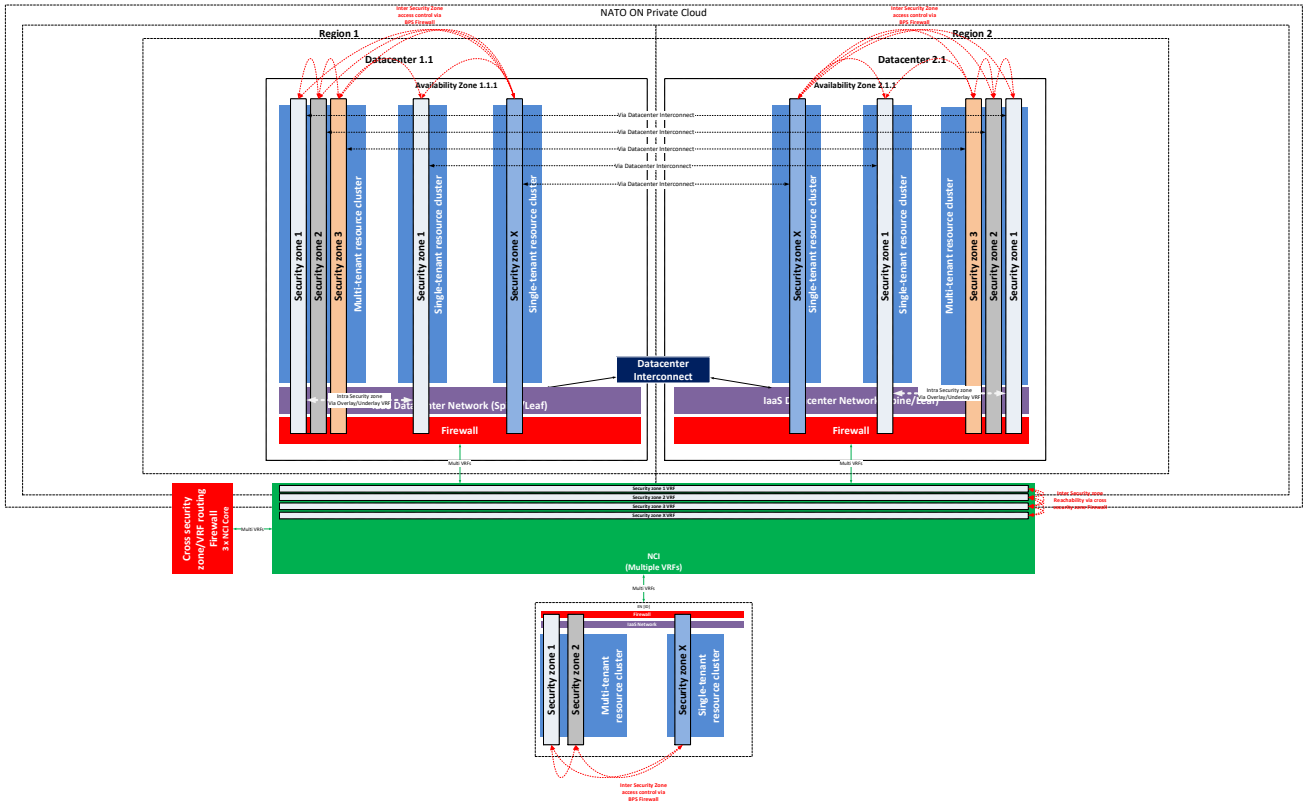


Figure 14 - Inter and Intra Security Zone

0114 Services deployed in a NATO ON IaaS Security zone must further be designed in a secure manner (e.g. taking into account micro-segmentation, virtual security zones, reverse proxies, WAF etc.)

3.5.3. Load Balancing/Application Delivery Controller Topology

0115 This section addresses the load balancing, also known as Application Delivery Controller (ADC) solution for the NATO ON infrastructure. The Load Balancing/ADC components are providing more than traditional load balancing, they are leveraged as part of the intent to build cloud based services leveraging zero trust security architecture models.

0116 The Load balancers/ADC components provide:

- Local Load balancing capabilities.
- Global Load balancing capabilities based on DNS.
- SSL interception and Web Application Firewall capabilities.
- Authentication of consumers and application access control.

0117 Multiple components are leveraged in order to implement the capability:

- Physical F5 appliance for physical workloads in the Datacentre.
- Virtual appliance for the Global Load balancers (either F5 or infoblox could be leveraged)
- Virtual appliance for Local Load balancers/ADC for Virtual Loads.
- Integrated Load balancing capabilities provided by other components (e.g. in case VMware Edge being used) for Local Load balancers/ADC.
- Istio as the Ingress load balancer container for Kubernetes deployments.

0118 The Virtual appliances for Local and global load balancing and WAF capabilities are expected to be aligned with the physical Load balancer (F5) however since those are not

hardware based, and previously purchased virtual appliance licenses are expired, the solution may be re-defined during implementation (e.g. leveraging VMware loadbalancing services). It is to be noted that for the global load balancers, Infoblox (the DDI) solution may be an alternative.

Sub-service/component	Security zone	Resource Cluster	Site
Local Load balancer/ADC and WAF (virtual appliance)	Every security zone	Workload Cluster 1 (General)	DC,EN,SN
Local Load balancer/ADC and WAF (virtual appliance) (DMZ)	Every security zone	Workload Cluster 5 (DMZ)	DC,EN,SN
Global Load balancers/ADC (virtual appliance) internal	Every security zone	Workload Cluster 1 (General)	DC
Global Load balancers/ADC (virtual appliance) external	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Workload Cluster 5 (DMZ)	DC
Physical Load balancers/ADC and WAF	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Not applicable	DC
Load balancing (integrated)	Every security zone (When applicable)	Not applicable	DC,EN,`SN

Table 9 - Load balancing/ADC component per Node Type

0119 The Load balancing/ADC service is further detailed in 4.2.1.

3.5.4. DDI (DNS, DHCP, IP Address Management)

0120 The DDI solution is implemented on the NATO ON to provide:

- IP address management, which integrates with Active Directory DNS and DHCP servers.
- DNS services, integrating with Global load balancers.
- DHCP management and delegation of pools.

0121 In order to align with currently deployed DDI solution in NATO, the NATO ON relies on Infoblox (NIOS) for DNS, DHCP.

0122 The DDI solution is deployed in a DMZ in every Datacentre location.

Sub-service/component	Security zone	Resource Cluster	Site	DC Availability
DDI (DHCP, DNS, IPAM - Infoblox)	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Workload Cluster 1 (General)	DC	Active – Active
DDI (DNS ext - Infoblox)	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Workload Cluster 5 (DMZ)	DC	Active – Active

Table 10 - DDI component per Node Type

0123 The DDI solution integrates with NATO ON enterprise windows Active Directory DNS and DHCP servers to provide a holistic view of the NATO ON enterprise IP infrastructure, and identifying which user and/or device is or was using a specific IP Address.

0124 To be noted: The DDI solution will also be replacing the current NATO NS Root DNS (for which a migration will need to take place), and DNS SEC will require to be implemented.

3.5.5. QoS Topology

0125 The NATO ON QOS implementation follows the NATO IP QoS Standard for the Networking and Information Infrastructure (NII) as described in Technical Note 1417. TN 1417 is an end-to-end QOS reference architecture for NATO NII.

0126 As a segment of NATO NII, the NATO ON solution is designed to support existing NATO QoS model.

0127 All network switches, physical or virtual, are configured to ensure end-to-end support in honouring the DSCP markings as they enter and exit the environment.

0128 The NATO ON datacentre core switching enforce QoS policies, while services must mark traffic according to the NATO QoS reference architecture. Each service or application

0129 Identifying trust boundary (source of the marking, often the application or the system running the application)

0130 Identify classification and marking for the specific application network flows (as per NATO QOS Reference architecture)

0131 Ensure marking is maintained up to the Interface with NCI (via SIOP5 interfaces) to pass approved DSCP marking to NCI WAN.

0132 In general, trust boundary is established close to the source as much as possible. As such, trust boundary begins at the datacentre edge (leaf switches). The leaf switches either trust the incoming 802.1P marking or align the traffic to the NCI hardware queue QOS/COS markings. The switches and Firewall then pass the DSCP marking to NCI as depicted in **Figure 15**.

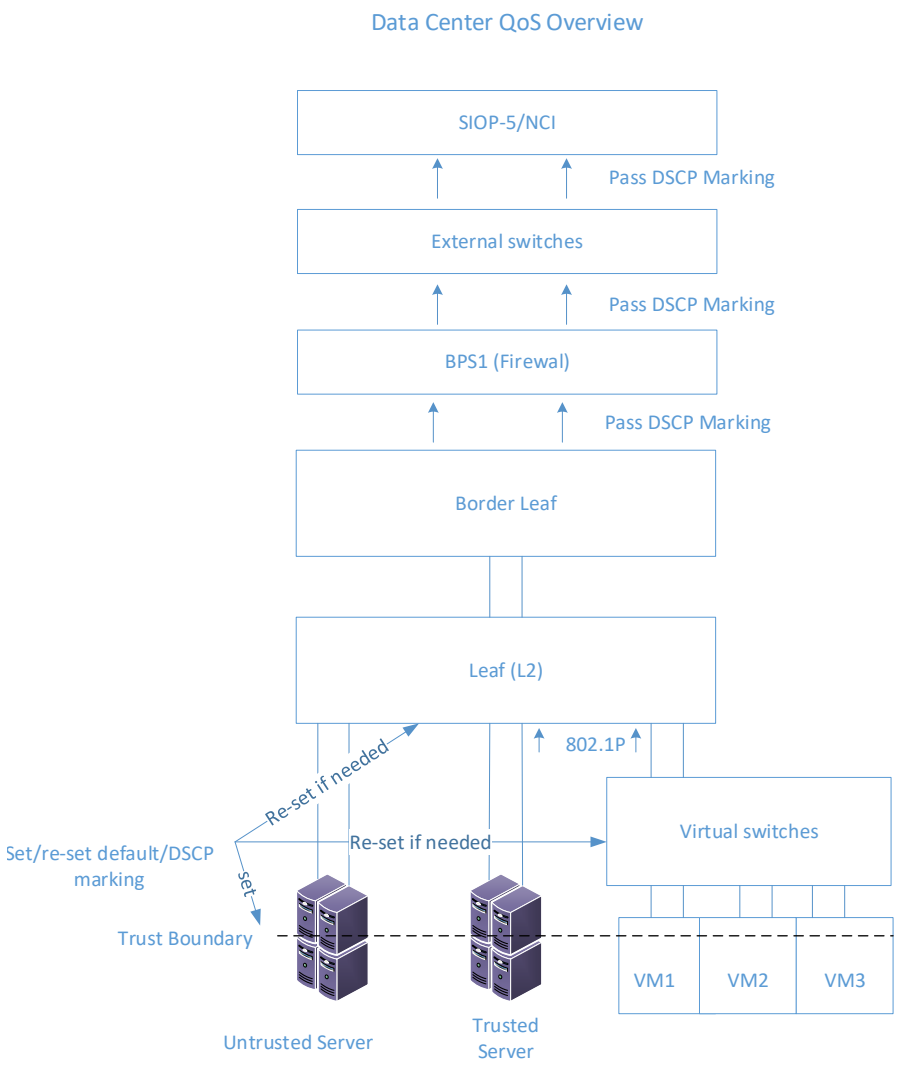


Figure 15 - Datacentre QoS Overview

3.5.6. Network Overlay

0133 As described in 3.4.4.4 the intent is to leverage Cisco ACI for the network overlay and limit the usage of NSX-T for security/micro-segmentation capabilities. This allow to leverage the same network capabilities and align network configuration for both VMware and non-VMware workloads.

0134 The network overlay will be implemented to extend the datacentre networks between each other's to allow for improved high availability and disaster recovery responses.

0135 However it will not be possible to extend the networks between DC(s) and other node types due to the latency and current MTU limitations (Hardware crypto limitation) which may be revised once/if limitations do not exist anymore.

0136 The design of the overlay will be adjusted during implementation in order to optimize it taking into account automation and ease of management.

3.5.7. NCI WAN Interface

0137 Each Node IaaS will require to interface with the NATO WAN (NCI). This is performed by the implementation of multiple SIOP-5 interfaces or sub-interfaces (one SIOP-5 per security zone) between the external switches and the NCI NS CCA routers.

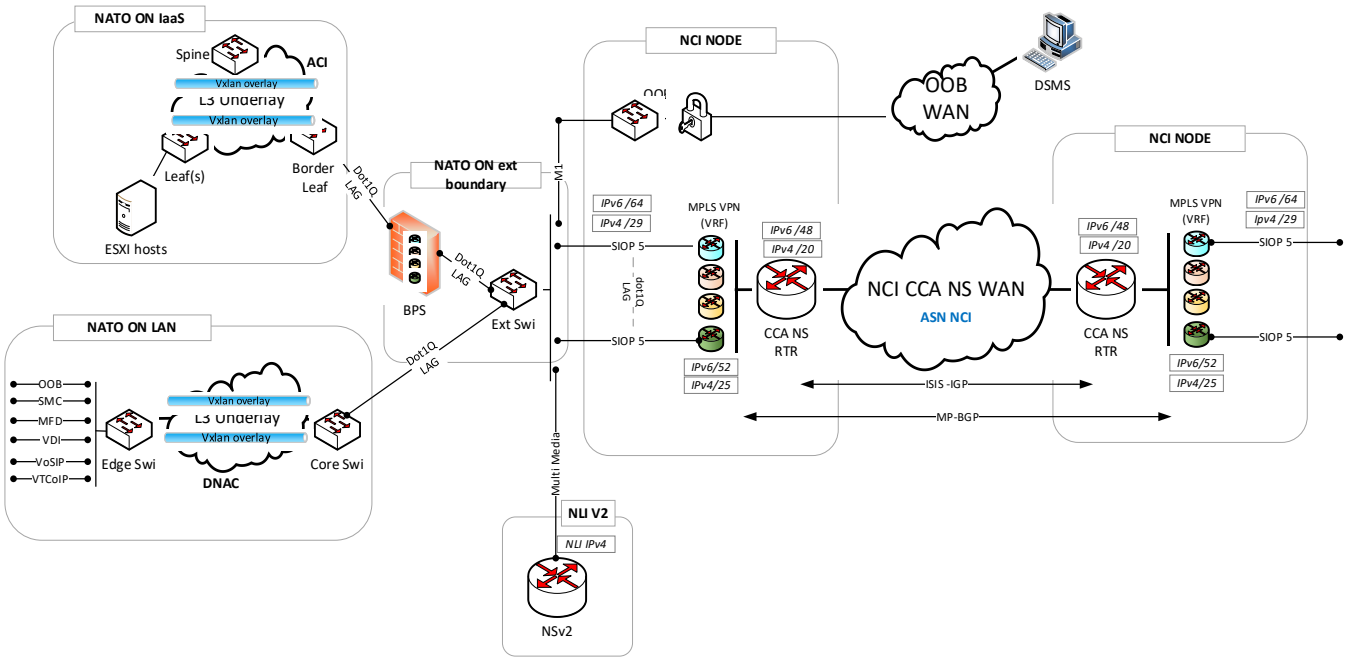


Figure 16 - NATO ON and NCI SIOP-5 interfaces

0138 The routing is implemented leveraging OSF and BGP to allow for dynamic routing to be implemented.

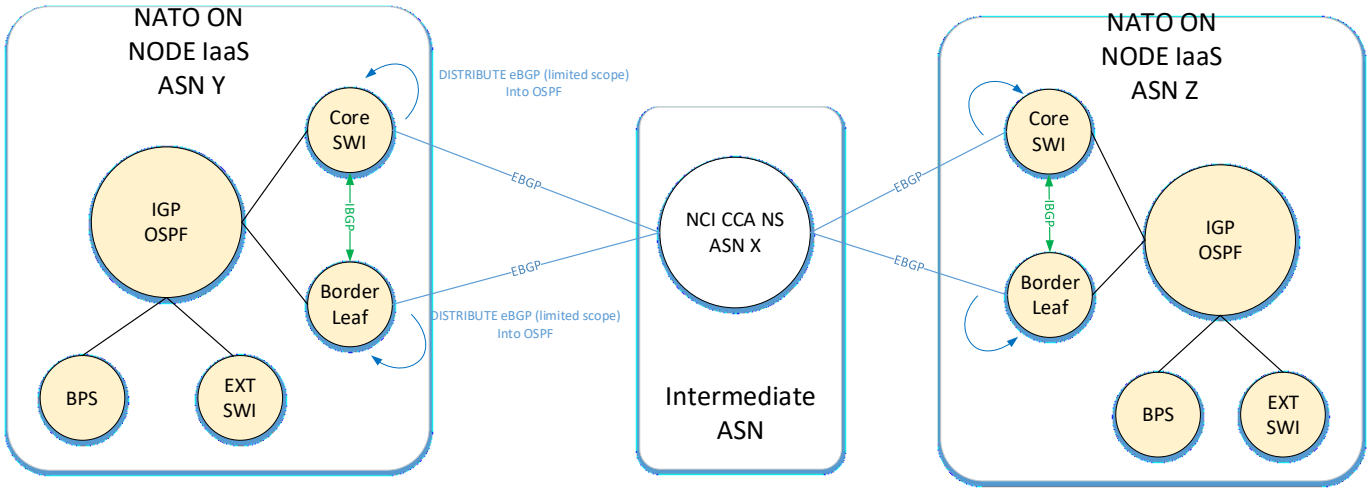


Figure 17 - NATO ON and NCI routing concept

0139 Further details regarding the detailed implementation are to be developed in the ICDs.

3.6. Infrastructure Storage Subservice Topology

3.6.1. Virtualized platform

0140 The NATO ON is mainly established based on VMware vSAN clusters (vSAN Ready Nodes). The vSAN building blocks provide the storage required for all applications and services running on the virtualized infrastructure. Dedicated storage appliances are not excluded and will be leveraged based on use case requirements for efficient use for large storage requirements (where VSAN technology will not provide the most cost-effective solution).

0141 The vSAN clusters are specified to provide appropriate amount of capacity and performance, and capacity will be increased over time to meet the changing demand.

3.6.1.1. Virtual Machine data

0142 The vSAN storage is leveraged for VM disks and contribute to meeting the multi-tenancy and security requirements.

0143 Tenants VMs data is isolated by default via the vSAN architecture.

0144 VMware Storage Policy Based Management (SBPM) is configured to use tags to map and host VMs on the appropriate vSAN clusters (e.g. for DMZ or SQL database VMs) and required disaster and failure tolerance policies.

0145 Tenant VMs are hosted on dedicated vSAN clusters when required (as per the architecture security zone concept)

0146 Data In Transit encryption is implemented (DIT).

0147 Data at Rest Encryption (DRE) is implemented when required by leveraging SBPM policies and VMware Native Key Provider. (vSAN Ready nodes allow to leverage VMware Native Key Provider (NKP) for data at rest encryption without the need for additional KMS).

3.6.1.2. File shares

0148 As part of ECS services, Windows Distributed File System (DFS) servers are implemented (leveraging the Virtualized platform).

3.6.2. Physical platform

0149 The physical services are leveraging both their internal storage and when needed the file shares established by ECS (Windows DFS).

3.7. Infrastructure Cyber Security Subservice Topology

0150 While Security is part of many services, specific security components and services are required to be deployed and or integrated with. This paragraph details those component and services.

0151 The boundary protection services are built based on the implementation of Firewall, DMZ infrastructure and DMZ services. The boundary between the NATO ON IaaS services and the NCI Wide Area Network is named BPS-1. The boundary between the lower classification and NATO ON is named BPS-4 and is based on the use of a network diode.

3.7.1. BPS-1 Topology

0152 BPS-1 is composed of all system and services allowing for the secure communication between security zones and from/with external system and services.

0153 BPS-1 physical firewalls model differs between sites based on expected traffic load but provide the same functionalities. Newer models will be considered over time.

Vendor	Model	Site	Function	Max Throughput with Threat Prevention	Interfaces
Palo Alto	3260 *(or newer)*	EN/SN	BPS1 Firewall	4.3Gbps	10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)

Vendor	Model	Site	Function	Max Throughput with Threat Prevention	Interfaces
Palo Alto	5250 *(or newer)*	DC	BPS1 Firewall	21.4Gbps	10/100/1000 (2), 40G/100G QSFP28 HA (1), 10/100/1000 out-of-band management (1), RJ45 console port (1)

Table 11 - BPS-1 Physical Firewalls

0154 As described in 3.5.2.2, the Firewalls (Palo Alto) are contributing to the multi-tenancy by segregating the different security zone in separate VRFs.

0155 The DMZ virtual services are deployed on the dedicated vSAN DMZ clusters, and segregated from internal resource (in the same tenant) they protect by leveraging VMware NSX-T distributed firewall (micro-segmentation) as well as Cisco EPGs and Traffic contracts.

0156 Some of the Virtual services deployed in the DMZ are described in the IaaS SDP (e.g. DDI and Load balancer components) but many are described as part of the other relevant SDPs (e.g. Skype, SharePoint etc.)

3.7.2. Integration with NATO Cyber Security threat prevention service.

0157 The Firewalls (Palo Alto) are not only used for implementing firewall capabilities, but as part of the Cyber Security Architecture they are used for Intrusion detection and prevention (Palo Alto Threat prevention functionality) and interface with the NATO SIEM.

3.7.3. Integration with NATO Enterprise Logging and SIEM.

0158 All IaaS services are integrating with the NATO Enterprise logging/SIEM based on Splunk.

0159 The VMware logs will be centralized first in Log Insight and then forwarded to the NATO SIEM.

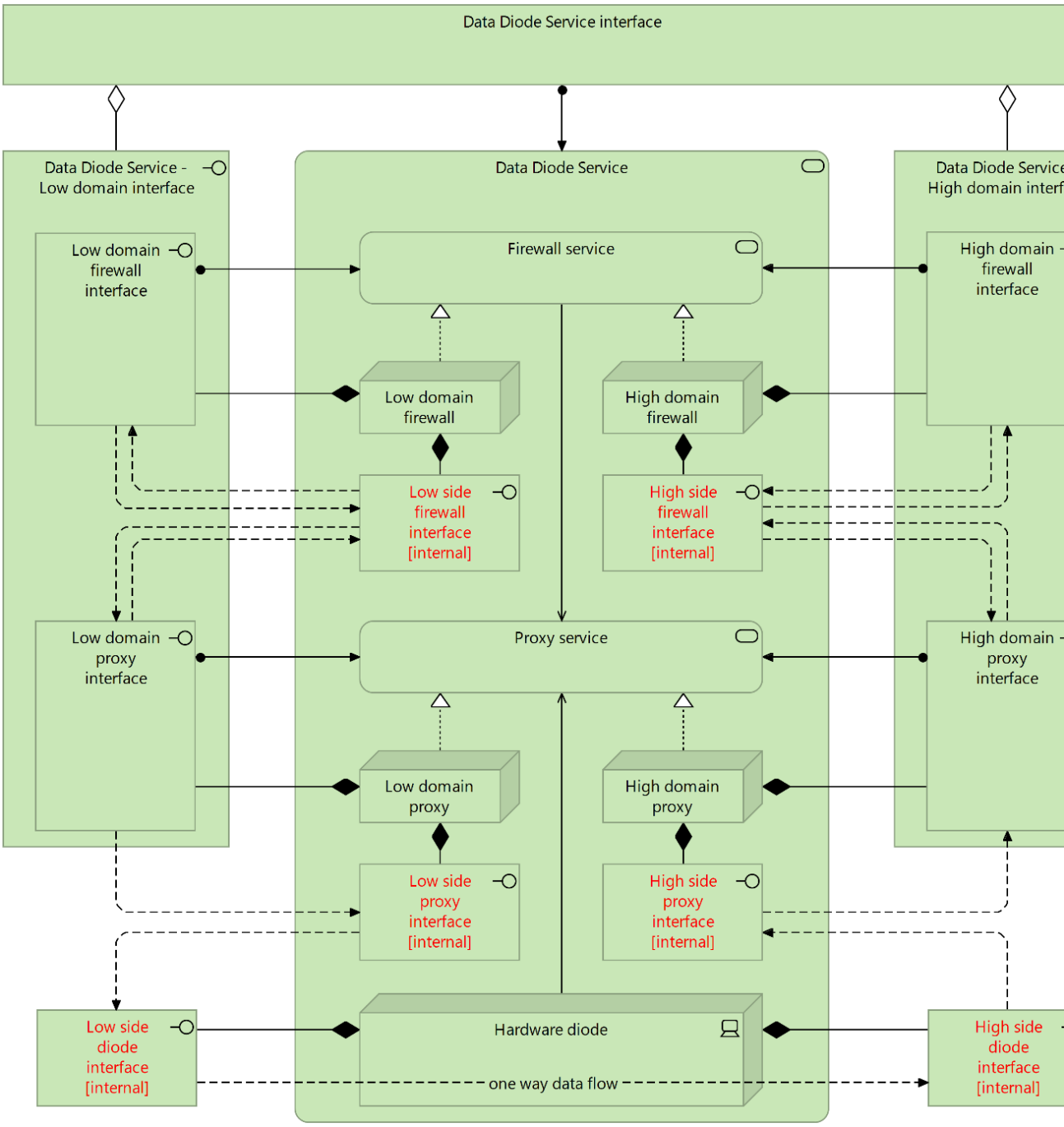
0160 Other systems are configured either to :

- Send the logs to the logging server/forwarder
- Provide a mechanism to allow the Splunk heavy forwarder to pull the logs from the target.

3.7.4. Data Diode as a Service - BPS4 Topology [Will be updated during design work of Diode as a Service]

0161 The BPS4 function is re-designed as a Diode as a Service as part of the ON cyber Security services. The IaaS services will leverage the Diode as a Service in order to enable file transfer between lower classification system and services and higher classification system and services (e.g. as part of lifecycle management to transfer patches/firmware/updates etc.) as well as enable email transfer from lower to higher classification.

0162 The following figure depicts the “Data Diode Service” Technical Architecture.



0163

Figure 18 - 'Data Diode Service' Technical Architecture

0164 The Data Diode as a service is implemented in each of the Datacentre and deployed as an high available service as depicted in the technical topology below :

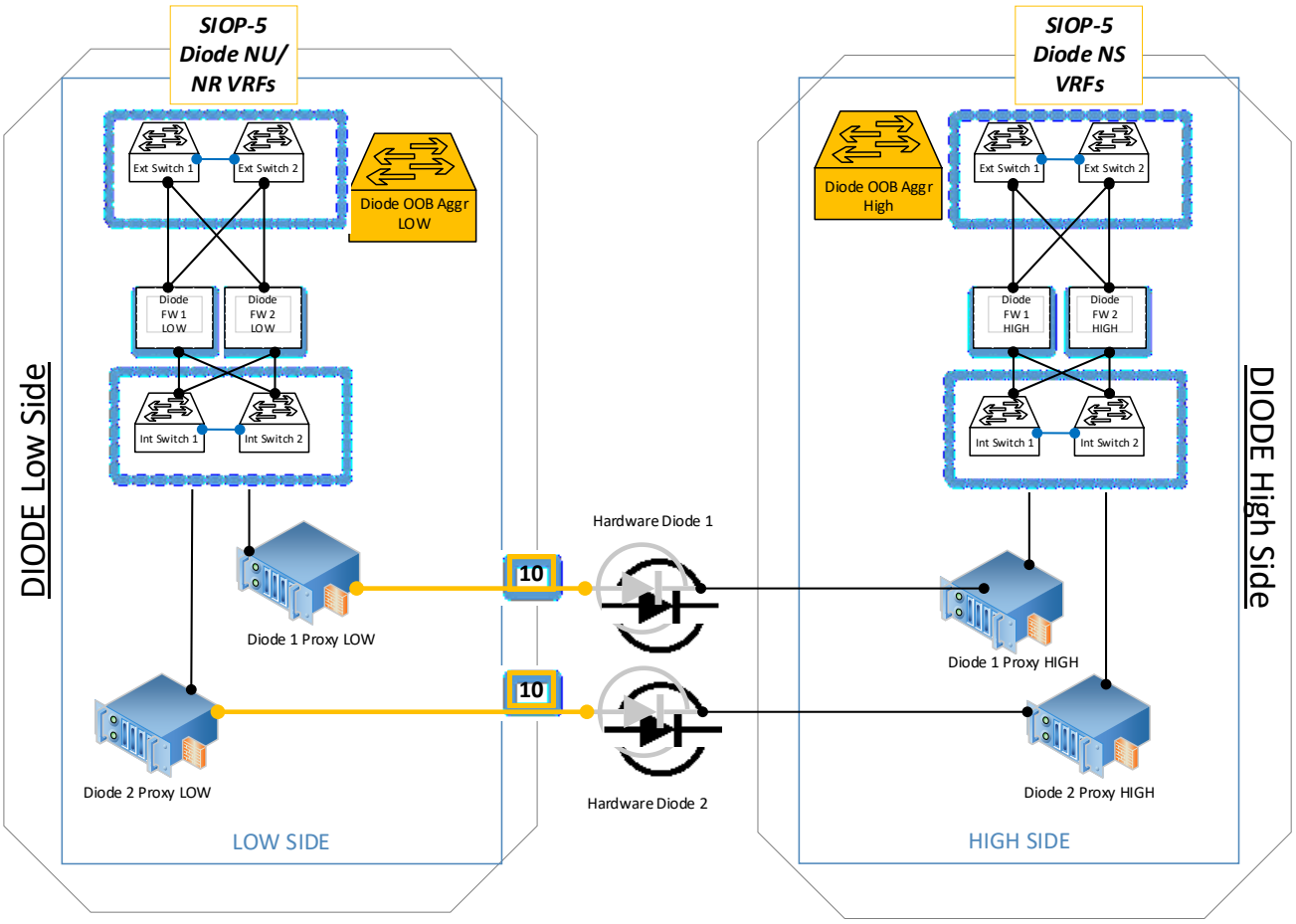


Figure 19 – Data Diode as a Service Technical topology

3.7.5. Security hardening

0165 All services deployed are required to be hardened, so that only required functions are enabled, and that access to services are authorized only from applicable consumers (user, device and/or service).

0166 Security hardening is developed and implemented as part of the automation and orchestration.

0167 Security hardening include the implementation of:

- NCIRC Hardening guides.
- DISA guides.
- Vendor specific hardening guidance.
- Remediation to identified vulnerabilities.

0168 Dashboards must be available to provide an overview of the security compliance of services and components deployed, including compliance to directive (e.g. **AC/322-D/0048-REV3**)

3.7.6. NATO Cyber Security Services Integration

0169 The NATO Cyber Security Centre (NCSC) is delivering, managing and operating NATO Cyber Security Services. The NATO ON IaaS and the services deployed inside the IaaS must integrate with those services.

3.7.6.1. Information flow between NATO ON IaaS and NCSC Cyber Security services

0170 The delivery, management, and operation of NATO Cyber Security Services by NCSC relies on cyber security enclaves (local deployment) and a centralized Cyber Security Operations Centre (CSOC) capability. The enclaves facilitate monitoring of infrastructures as well as the execution of online vulnerability assessments (OVA) and online computer forensics (OCF). The figure below highlights the information flow between the NATO ON IaaS and the CSOC, required for monitoring, OVA, and OCF. (In the figure, enclaves are referred to as Tier 3 (T3), and the CSOC as Tier 2 (T2)).

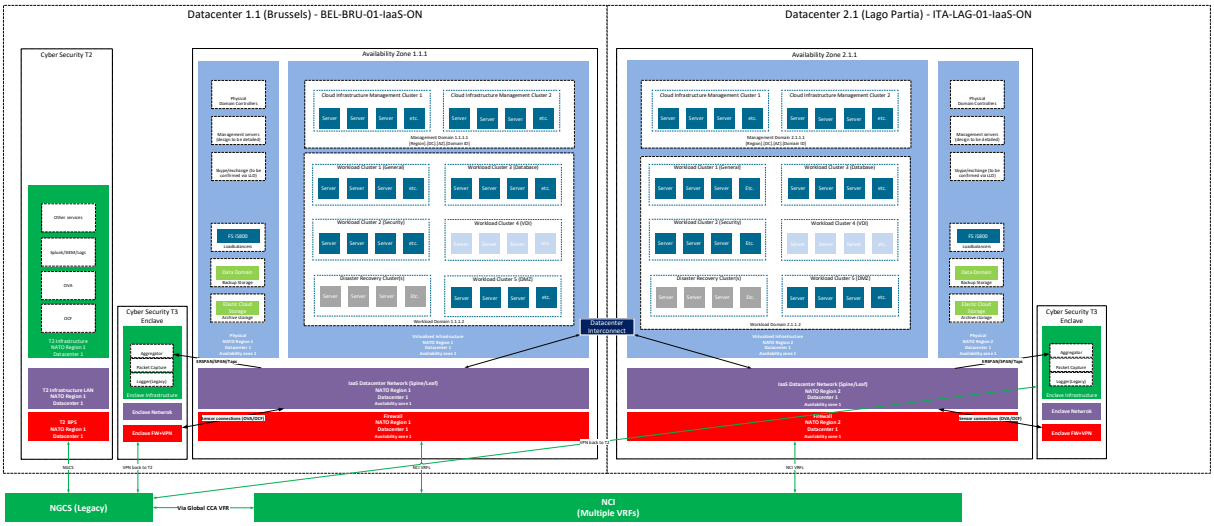


Figure 20 - Information flow between NATO ON IaaS and NCSC T2 and T3 infrastructure

3.7.6.2. Monitor and Detect

0171 The core of the NCSC Monitor and Detect service is based around a Security Information and Event Management (SIEM) system.

0172 The type of interfaces (at the Data Centres) between NATO ON IaaS and the capabilities that deliver the Monitor and Detect service, including the SIEM (based on Splunk), are depicted in the figure below. (While the figure depicts only the Data Centres, the same architecture applies for all sites).

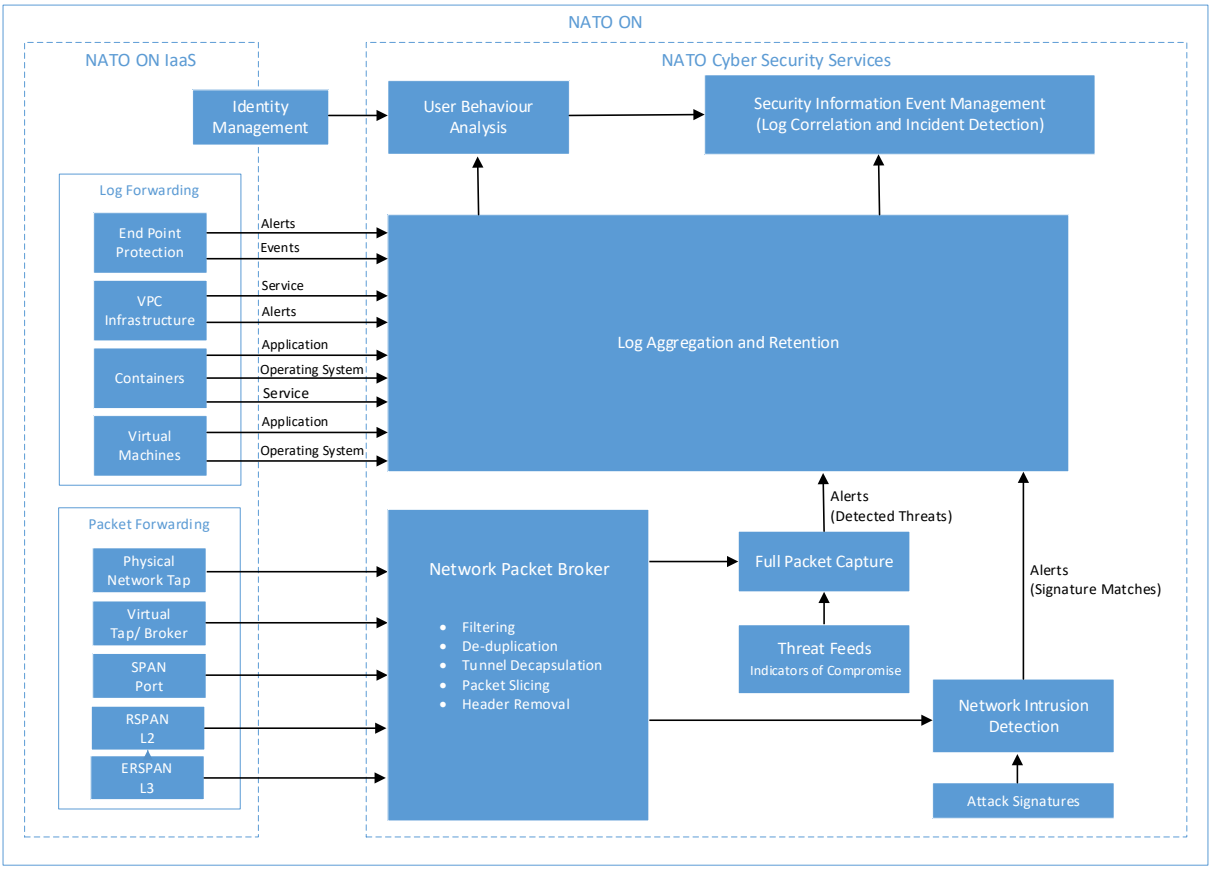


Figure 21 - NATO ON IaaS and NCSC interfaces

0173 While the figure above depicts only the datacentres, the same architecture applies for all sites.

3.7.6.3. Prevent

0174 The NATO ON IaaS services integrate with NCSC services in order to support the Prevent capability. The services and process implemented for the NATO ON are to be aligned with NCSC procedures and require coordination with NCSC to develop SOPs.

3.8. Infrastructure Archive Storage Subservice Topology

0175 Specific Archiving storage is deployed in the Datacentre only and leverage an object storage solution. The NATO ON is currently planned to re-use Dell EMC Elastic Cloud storage (ECS) platform for all Tier 4 storage.

0176 Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation and analysis of unstructured data on a massive scale on commodity hardware. Dell EMC ECS is specifically designed to support mobile, cloud, big data and social networking applications.

0177 The initial Archive Storage must support long term archiving of backup for at least 5 years for forensic purposes. And it shall support other type of back-ups for 2 years. This will require identification of the detailed requirement per application and or services either part of IaaS or services hosted on the IaaS.

Sub-service/component	Security zone	Resource Cluster	Site
Tier-4 Archive storage (ECS)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not applicable	DC

Table 12 - Archive Storage component per Node Type

3.9. Backup and Recovery Subservice Topology

0178 Backup, archive and disaster recovery mechanisms apply to all infrastructure nodes to support business continuity in case of loss of data or service. In addition it provides long term (5 years) archiving retention for specific data sets. The envisaged solution is driven by the service level targets, disaster recovery requirements and date retention per application or data set.

0179 The service level targets for data loss are specified in 4 service level targets (L1-L4) as depicted in Table 13 below. Each level specifies the required Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Service level target levels are assigned per service / application.

Service Level Target	RTO (hrs)	RPO (hrs)
1	1	1
2	4	8
3	12	24
4	48	48

Table 13 - CIS service recovery requirements

0180 Note that Level 1 (L1) is specified not to allow any data loss nor downtime in SOR/MER 2021. Such requirement is not possible to meet (close to zero is achievable, but would require architecture/including facilities to be designed for such requirement). And since the current facilities do not provide the means to allow for multiple availability zones nor synchronous replication between the existing data centre locations, which would reduce data loss and downtime for L1 services, there will be a need for future improvement and implementation of new underlying physical DC infrastructure and IaaS.

0181 In addition, the disaster recovery mechanisms enable data recovery in case of total data loss at any site taking into account the service level target requirements per service.

3.9.1. Backup and archive Tier Topology

0182 To facilitate the backup and archive service and key requirements for service level target 2, 3 and 4, the following backup components are utilized:

- 1st tier – local copy: Primary backup servers/appliances with local direct attached storage providing fast local backup and restore capabilities for short term data recovery (7 days retention)
- 2nd tier – local copy: Secondary backup storage are dedicated local backup storage appliances providing a 2nd copy of the data on a different device at the local site for near-term data recovery (up to 6 months retention).
- 3rd tier – off site copy: The 3rd copy of backup data is provided in the data centre that is paired with the remote site (based on best Wide Area Network path or Datacentre interconnect). Backup data is replicated from the 2nd tier backup storage and shall allow data recovery in case of data loss at any site. Note that this 3er tier backup storage device shall also function as 2nd tier backup storage for the data centre itself.

- 4th tier – local + off site copy: Optionally available for specific data is the archive storage located only at the Data Centre locations. Backup data may be offloaded to the archive storage from the backup at the datacentre, or from a specific service directly. Archive storage is fully replicated between the data centre locations and provides data retention for up to 5 years.

0183 Figure 22 below depicts these components in each node.

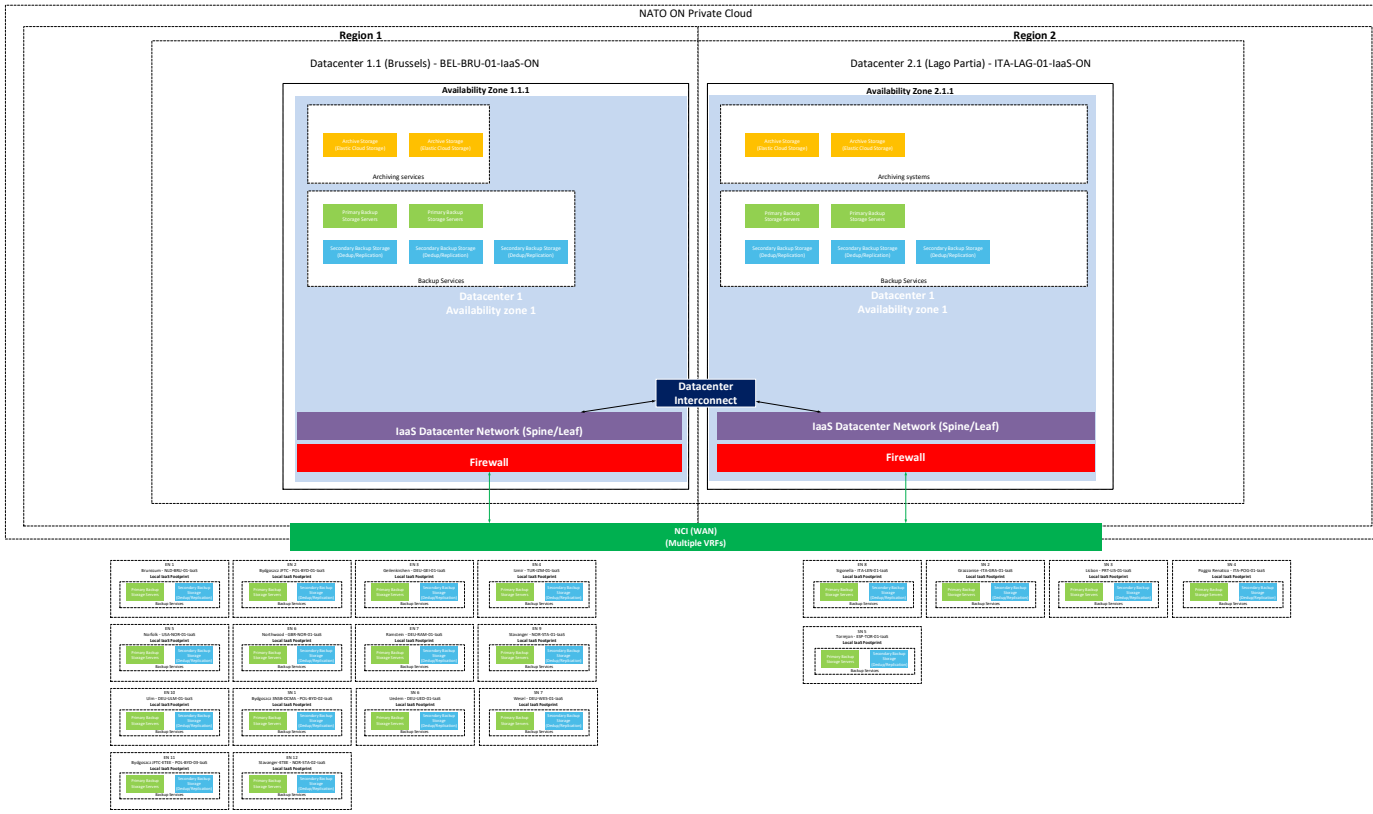


Figure 22 - Backup and Archive storage components

0184 The Primary (Tier 1) storage solution is based on HPE servers, running Oracle Linux operating system to allow for immutable backups to be enabled

0185 The Secondary (Tier 2/3) storage remains to be defined as part of the implementation (based on the most cost effective solution and replication architecture (Backup software based replication versus Tier 2 Storage Appliance replication)), however an initial deployment with HPE Store Once is expected in the datacentre.

Sub-service/component	Security zone	Resource Cluster	Site
Tier-1 Backup Storage	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not applicable	DC,EN,SN
Tier-2/3 Backup Storage	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not applicable	DC,EN,SN

Table 14 - Backup Tier1/2/3 component per Node Type

3.9.2. Backup and archive Orchestration

0186 VEEAM is deployed as a virtual appliance and configured at each site to backup and allow the recovery of data as per the Tier model descried in 3.9.1.

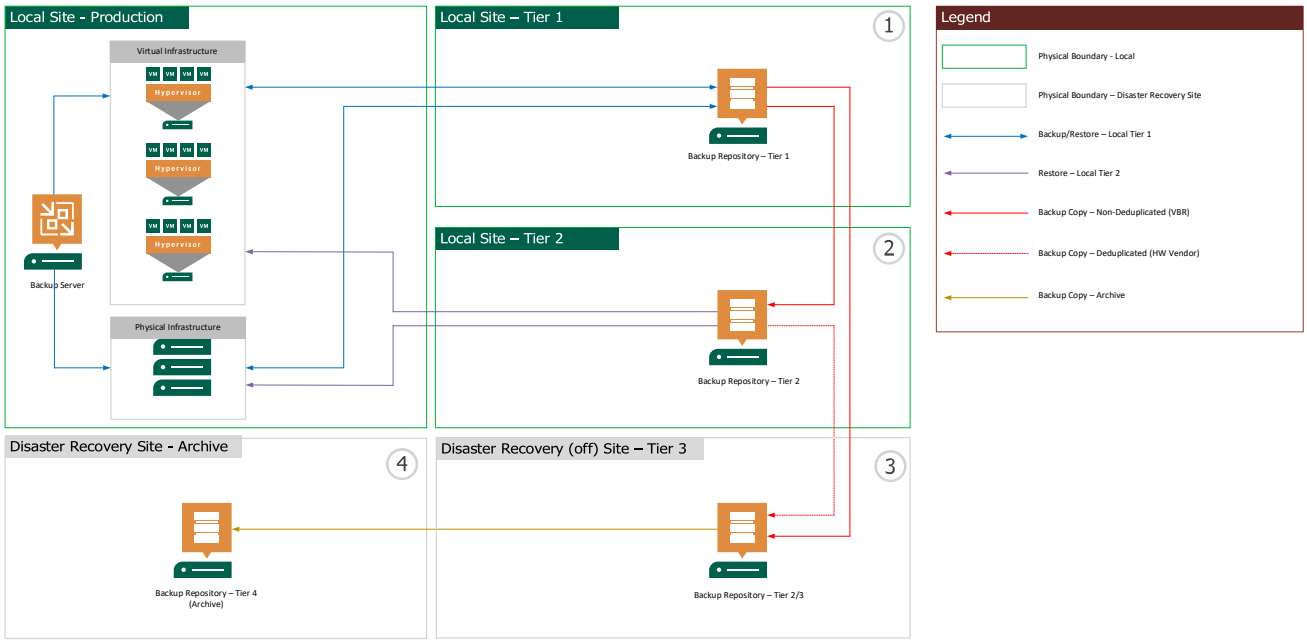


Figure 23 - VEEAM Backup/Recovery Orchestration

0187 VEEAM is configured to backup different type of data:

- Virtual machines.
- Application data.
- Databases.
- Any required artefact.

0188 For replication of backup data between the local site and the Disaster Recovery site, it is yet to be determined whether to leverage the built-in replication functionality of VEEAM (avoiding vendor lock-in for Tier 2 storage but more overhead/less performant), or whether to leverage the replication functionality of the hardware vendor for the Tier 2 storage (Requiring same Tier 2 storage vendor to be used in the enterprise, but providing better performant replication).

3.9.3. Infrastructure Replication Services - Disaster Recovery

0189 To support disaster recovery in the event of loss of a service or complete site, applications and data with target service level L2, L3 and L4 need to be made available in the paired recovery site (data centre), which shall have capacity reserved for these applications by means of dedicated disaster recovery clusters.

0190 To meet the required RTO for target service level 2 and 3 applications, it is foreseen that these applications are made available in the recovery site by means of a-synchronous replication leveraging the VMware vSphere replications service.

0191 To meet the disaster recovery requirements for L4 applications, the backup and archive service shall be utilised in combination with the backup replication mechanism. This will allow a copy of the backup to be available in the recovery site for restore within the L4 specified RTO and RPO values.

0192 The orchestration for failover of services is handled by VMware Site Recovery Manager.

0193 Figure 24 below provides an overview of the foreseen replication streams.

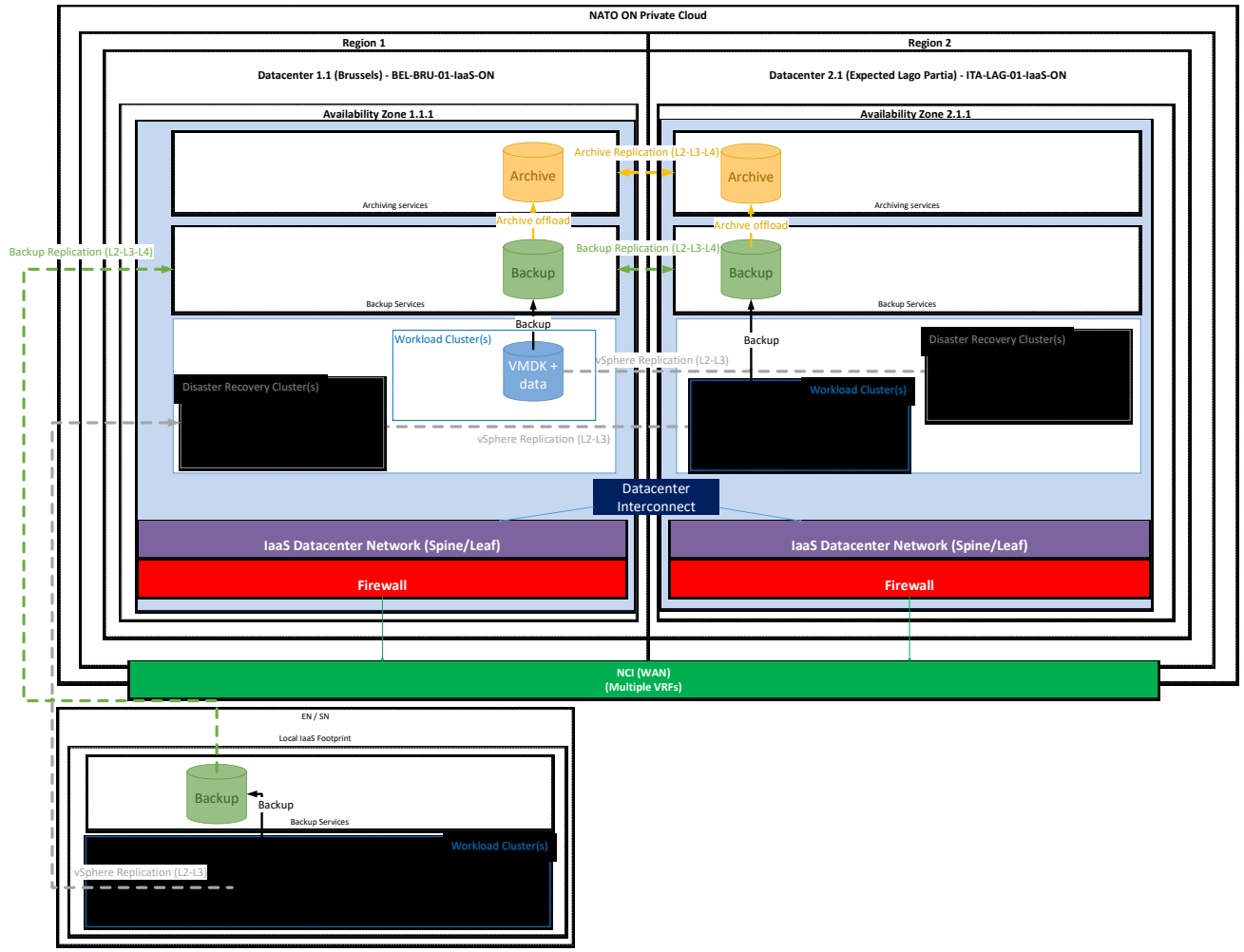


Figure 24 - NATO ON IaaS Replication overview

3.10. Infrastructure Service Management and Control (SMC) - IaaS Domain SMC Subservice Topology

0194 The NATO ON IaaS is to leverage Infrastructure DevOps (DevSecOps) concepts in order to provide benefits related to automation and agility.

0195 The ON IaaS is therefore leveraging Software defined solutions in order to orchestrate and automate changes.

0196 The configuration and changes need to be implemented via infrastructure as code and via configuration management scripts except when not possible.

0197 Interfaces with Enterprise SMC (enterprise level functionalities and enterprise scope) will be required, however domain SMC services and tools need to allow for an enterprise wide management (domain level functionalities and enterprise scope).

3.10.1. Overarching IaaS Automation and Orchestration.

0198 In order to benefit from Software Defined solutions and infrastructure as a code, and to support business continuity and implement appropriate lifecycle management, components and process are required to ensure at least the following functions are implemented.

- Infrastructure as Code (e.g. Terraform)
- Artefact Repository (e.g. Nexus, Artifactory)
- Source code management (e.g. GitLab).
- Configuration management (e.g. Ansible)
- End to end Automated Release and Deployment (CI/CD).
- Automated configuration and security compliance reporting (e.g. Runecast analyzer).
- Vulnerability scanning and reporting.
- Logging and monitoring.

0199 The overall NATO ON Orchestration and Automation is implemented leveraging components including Ansible Terraform, Jenkins and Git to standardize, control and automate the deployment of IaaS components, be harmonized with tools used for PaaS, SaaS and other NATO environment automation tools, and better support disaster recovery procedures. Those tools further integrates with other system including for example vRealize Automation (vRA) described in paragraph 3.4.4.3.

0200 Additional component and systems are expected to be used to further improve the overall automation and orchestration of infrastructure changes which will need to be further detailed during the implementation phase and sprints.

Sub-service/component	Security zone	Resource Cluster	Site	DC Availability
Git repository	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active - Passive
Ansible	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active - Passive
Terraform	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active - Passive
Jenkins	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active – Passive
Artefact Repository (tbd)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active – Passive
Compliance Reporting system	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Cloud Infrastructure Management cluster [ID]	DC	Active – Passive

Table 15 - IaaS Automation and Orchestration Component per Node Type

3.10.2. Infrastructure Processing

0201 The domain SMC components used to implement and manage the physical servers and virtualization services are described below.

3.10.2.1. Physical Compute Platform management

0202 The initial implementation of vSAN ready nodes is performed based on HP vSAN Ready node servers.

0203 In order to manage the physical hardware platform, HP One View will be leveraged to maintain the firmware of the physical servers up to date except in the case where the servers are automatically updated via another mechanism (e.g. in case of use of VMWare Virtual Cloud Foundation).

0204 HP One View is deployed as a virtual appliance in each DC and EN IaaS Node, and all instances are part of a federation to allow for a single pane of glass management (through

the global dashboard deployed at the Datacentre Node) of the Enterprise IaaS physical devices.

0205 SN IaaS will be managed through instances deployed in the DC IaaS Nodes.

0206 Each instance can manage up to 640 devices, and therefore additional instances will be required at nodes were the number of devices is higher.

Sub-service/component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
HP One View	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN

Table 16 - Physical Hardware Platform per Node Type

3.10.2.2. Virtual Compute Platform management

0207 It was initially envisioned to leverage VMWare Virtual Cloud Foundation (VCF) to deploy and manage resource clusters based on VSAN Ready nodes.

0208 However the impact of deploying VMware components leveraging the SDDC Manager need to be further evaluated, since it has architecture and design constrains.

0209 The main reason for considering VMWare VCF SSDC Manager is that multiple components are deployed automatically including Vcenter, vRealize Suite (including vRealize Automation, Operations, Log insights) and NSX-T.

0210 The current expectation is that if using the SDDC Manager, DCs and ENs would require single site VCF deployment topologies. VCF Stretched deployments would require multiple availability zones in the same region (which we do not have for the initial NATO ON IaaS deployment). While VCF Multi-site (VCF Federation) gives the possibility to have a VCF single pane of glass, this is currently limited to 25 VCF deployments.

0211 While the use of VCF SDDC Manager reduces the manpower required to configure, change, and maintain the environment as it allows to automate the lifecycle management (update/upgrade) of the compute/storage and the virtualization services, the complexity of meeting the NATO ON Architecture with VCF may bring **inefficient use of resources and go against the benefits NATO is looking for with the establishment of the NATO ON.**

0212 It is expected to further develop this aspect during the project sprints to implement the services in an automated and efficient manner.

3.10.3. Infrastructure Networking

0213 The domain SMC components used to implement and manage the network overlay and underlay are described below.

3.10.3.1. Cisco APIC Controllers

0214 The Network IaaS is based on Cisco ACI. Cisco APIC controllers are deployed at each site to control the IaaS Networking.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site

Cisco APIC (Large)(DC)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not Applicable	Global NS (Admin)	Not Applicable	Not Applicable	DC
Cisco APIC (Medium)(EN)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not Applicable	Global NS (Admin)	Not Applicable	Not Applicable	EN
Cisco APIC (Small)(SN)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not Applicable	Global NS (Admin)	Not Applicable	Not Applicable	SN

Table 17 - Cisco APIC controllers per Node Type

0215 The Datacentre will initially leverage a Large cluster (L3), the Enhanced Node will use a Medium cluster (M3), while the Standard node will either depend on the datacentres or leverage a Small 1U (XS) cluster (This will need to be validated upon implementation).

3.10.3.2. Cisco Nexus Dashboard

0216 The Nexus Dashboard allows to have an overview (single pane of glass) of all the Cisco ACI deployments. Two functionalities are provided, Orchestrator (NDO) and Insight (NDI).

0217 While the two functionalities may require dedicated clusters for performance reasons, the initial deployment will leverage a Large Nexus Dashboard deployment to host both NDO and NDI.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
Nexus Dashboard (Large)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Not Applicable	Global NS (Admin)	Not Applicable	Not Applicable	DC

Table 18 - Nexus Dashboard per Node Type

0218 The Initial cluster supporting NDO and NDI will be deployed in 1 DC only. This will be revised once additional cluster(s) are deployed (or extended).

3.10.3.3. NSX-T

0219 NSX-T will be leveraged for at least the Distributed firewall and require the NSX-T Managers to be deployed.

0220 A NSX-T Manager cluster will be required to control each site and controlled via a Global Manager deployed at the DC.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
NSX-T Manager Global	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC
NSX-T Manager (MGT)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC,EN
NSX-T Manager (Workload)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
NSX-T Manager (Workload)(EN)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	EN
NSX-T Manager (Workload)(SN)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC

Table 19 - NSX-T Manger per Node Type

3.10.3.4. Load balancing / ADC

0221 Depending on the solution chosen to implement the load balancing/ADC components described in 3.5.3, specific monitoring and management component may be required.

0222 For the management of the centralized F5 appliances, f5 BIG-IP IQ is implemented in the datacentres.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
F5 BIG-IP IQ (Centralized Management)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC

Table 20 - Load Balancing/ADC per Node Type

0223 When leveraging NSX-T load balancers, the management will be performed via the NSX-T managers described in 3.10.3.3.

3.10.4. Backup and Recovery

0224 In order to monitor and provide reporting, Veeam ONE is deployed as an active/passive solution in the datacentre locations.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
Backup and Archive (Veeam ONE)	NATO ON Management Services (NATO-ON-SZ-MGT-001)	Single-Tenant	Global NS (Admin)	Management Domain	Cloud Infrastructure Management cluster [ID]	DC

Table 21 - (Enterprise) Backup and Archiving per Node Type

0225 The T1 storage is relying on Oracle Linux and an Oracle Linux update repository is deployed in each datacentre as an active/active service. The repository requires updates to be automatically sent via the diode (BPS4) from a repository deployed on the lower classification network.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
Oracle Linux update repository	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Multi-Tenant	Global NS (Admin)	Workload domain	Workload Cluster 1 (General)	DC

Table 22 – Oracle Linux Repository per Node Type

3.10.5. Infrastructure CIS Security

0226 With the deployment of Palo Alto firewall, Panorama will be required to orchestrate changes across the various IaaS deployments. The target is to merge both NATO ON IaaS and existing NS Firewalls under a single Enterprise wide domain SMC instance (Panorama).

0227 The security mechanism provided by the IaaS extend beyond the physical boundaries and Palo Alto. Micro segmentation leverage functionalities from VMWare NSX (distributed firewall) as well as Cisco ACI and its capability to perform policy based traffic redirection. Panorama, Cisco ACI and NSX-T must be integrated to provide a harmonized management of the security policies and segmentation.

0228 DMZ services will be managed through their associated domain SMC services.

0229 In addition the NATO SIEM and its implementation are used (and will need to be modified and configured) to provide dashboard (including security compliance dashboard) for all services part of the NATO ON.

3.10.6. Rack Management

0230 Devices are planned in each rack (APC Netbotz Rack Monitor and APC Metered PDU's) for the monitoring of the power consumption and monitor and control access to each rack. The events are consolidated in the central logging and IaaS Domain SMC to allow for alerts to be appropriately generated and dashboards providing visibility of the events.

3.10.7. Identity and Access Management

3.10.7.1. Authentication

0231 The NATO ON IaaS Services integrates with different authentication providers. IaaS components will be integrated with a new management/service forest as described in the ECS SDP.

3.10.7.2. Privilege Access Management (PAM)

0232 The access control to IaaS Domain SMC components is performed via a new Privilege and Access Management (PAM) system. All IaaS Domain SMC services leverage PAM and are configured to support Role base access.

3.10.7.3. NATO PKI Services

0233 NATO policies mandate the use of the NATO PKI for all PKI certificates. While manual certificate requests are supported, automation will require the Integration of Element and domain SMC services with the NPKI services.

0234 The NPKI support the following mechanism:

- SCEP
- WNES (for windows domain joined devices)

0235 Identification of the type of integration required will need to be detailed during implementation phases.

3.10.8. Enterprise SMC

0236 The NATO ON IaaS domain SMC services integrate with the Enterprise SMC services. For each domain SMC service/tool, identification of the required type of interface will be defined as part of the detailed design.

0237 The interfaces will follow the approach described below:

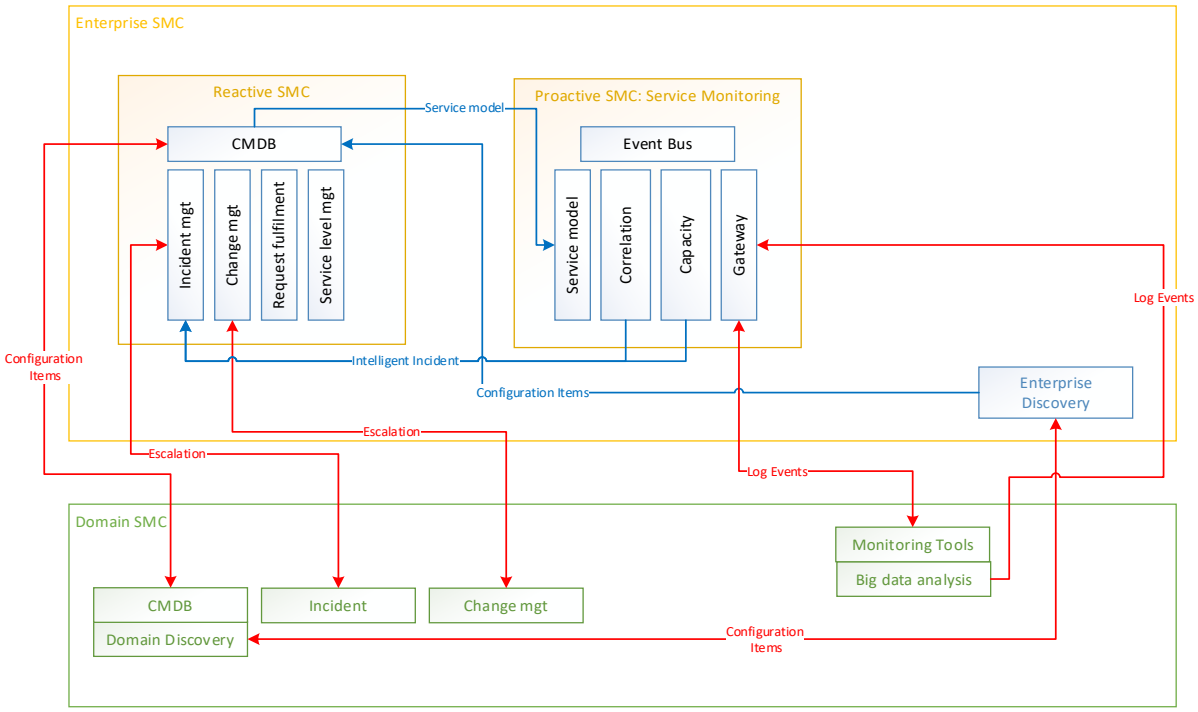


Figure 25 - Interfaces types between domain SMC and Enterprise SMC

0238 The relationship between Enterprise SMC tools and Domain SMC is described below:

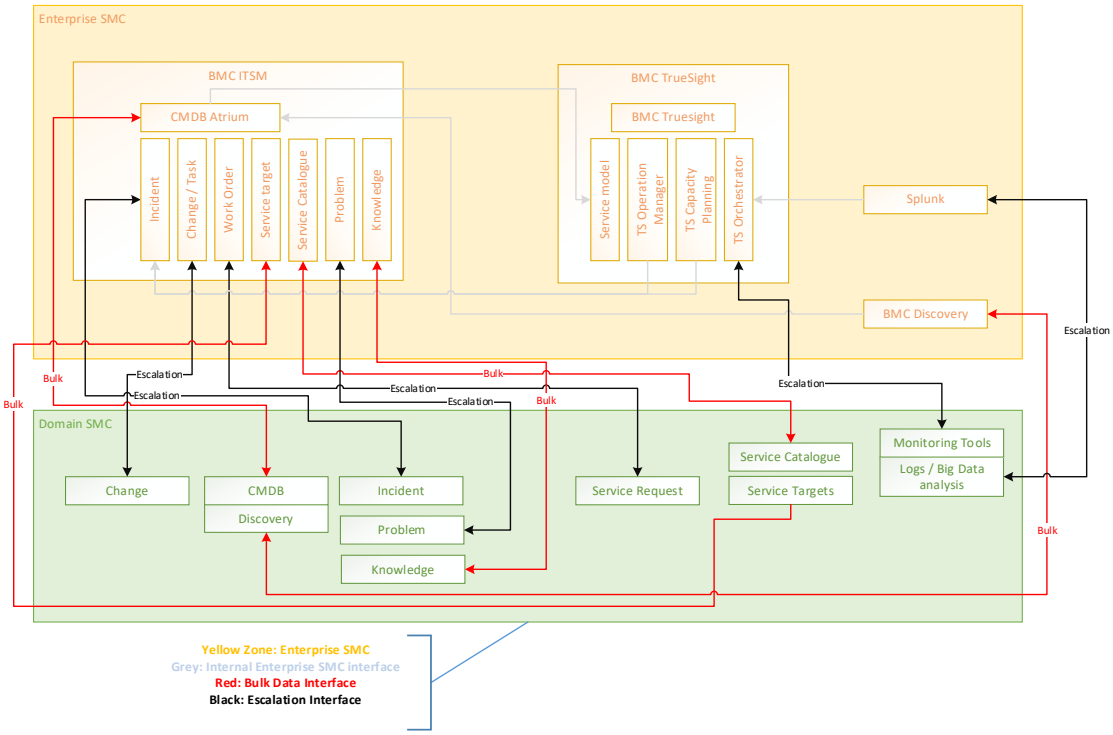


Figure 26 - Enterprise SMC and Domain SMC relationship

3.11. Reference Environment (IREEN) Services Subservice Topology

0239 Two Reference environment infrastructures are implemented and leveraged for non-production testing and validation activities.

0240 IREEN ON@NS it the NATO ON Reference Tenant/security zone composed of a dedicated set of component running at NS allowing to develop, test and validate changes leveraging classified data.

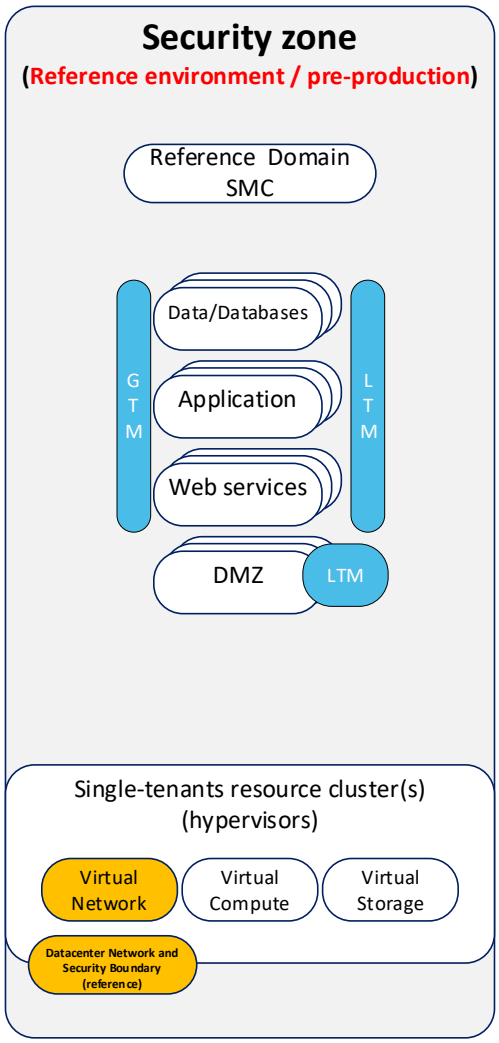


Figure 27 - NATO ON Reference environment Tenant (NS)

0241 IREEN ON@NU is the reference environment of the NATO ON services, operating at NU.

0242 IREEN ON@NU is a logical element of the NATO Software Factory (NSF) Computer Information System (CIS) which is composed of on-premise infrastructure hardware and NATO Public Cloud Services operating at NU.

0243 The NATO Public Cloud Services are based on the NSF, which is NCI Agency 'Development and Integration Environment', in order to develop and test software based components.

0244 On-premise Hardware is leveraged for developing and testing the automated deployment and change management of hardware related components.

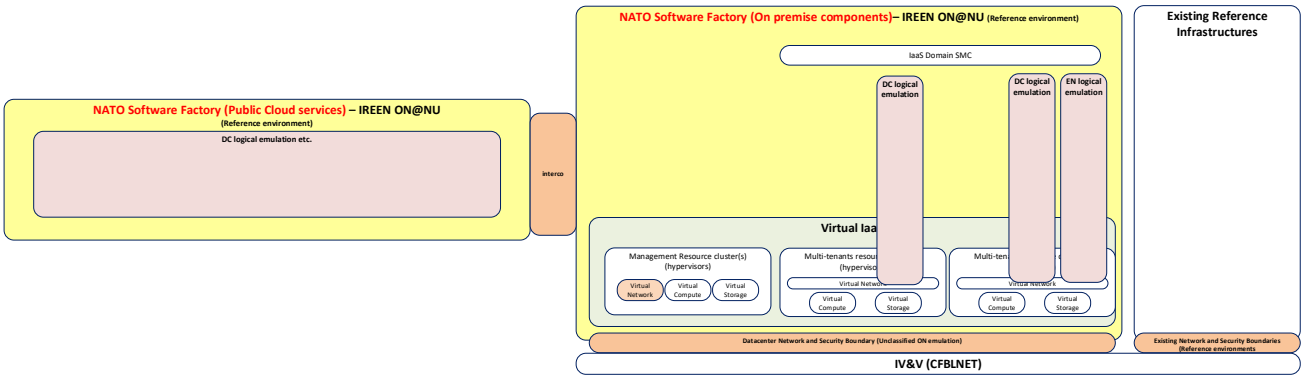


Figure 28 - Unclassified NATO ON Reference environment (IREEN ON@NU)

0245 Both reference infrastructures are used for application and infrastructure life cycle management and for which the details will need to be defined as part of the definition and implementation of DevOps (DevSecOps). In addition, NATO is leveraging a cloud DevOps environment (NSF/Azure cloud) which is expected to be leveraged as part of the DevOps lifecycles.

4. SERVICE SOLUTION – IMPLEMENTATION DETAILS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0246 This section is used to describe the implementation details of the services identified in Section 3.

0247 With major updates of the components and solutions required to implement the NATO ON, this section need to be revised/adjusted.

4.1. Infrastructure Processing Service Solution

0248 The infrastructure processing subservice contains the physical computer hardware, as well as the virtualisation and orchestration layers. These designs are outlined in detail below.

4.2. Infrastructure Networking Service Solution

4.2.1. Load Balancing/Application Delivery Controller Design

0249 As described in 3.5.3 the load balancing/ ADC capabilities are leveraging multiple components.

0250 All F5 LTMs are enabled to provide:

- Web Application Firewall (ASM)
- Access Policy Manager (APM)
- Advanced Firewall Manager (AFM)

0251 The figure below describes the components expected to be implemented per node:

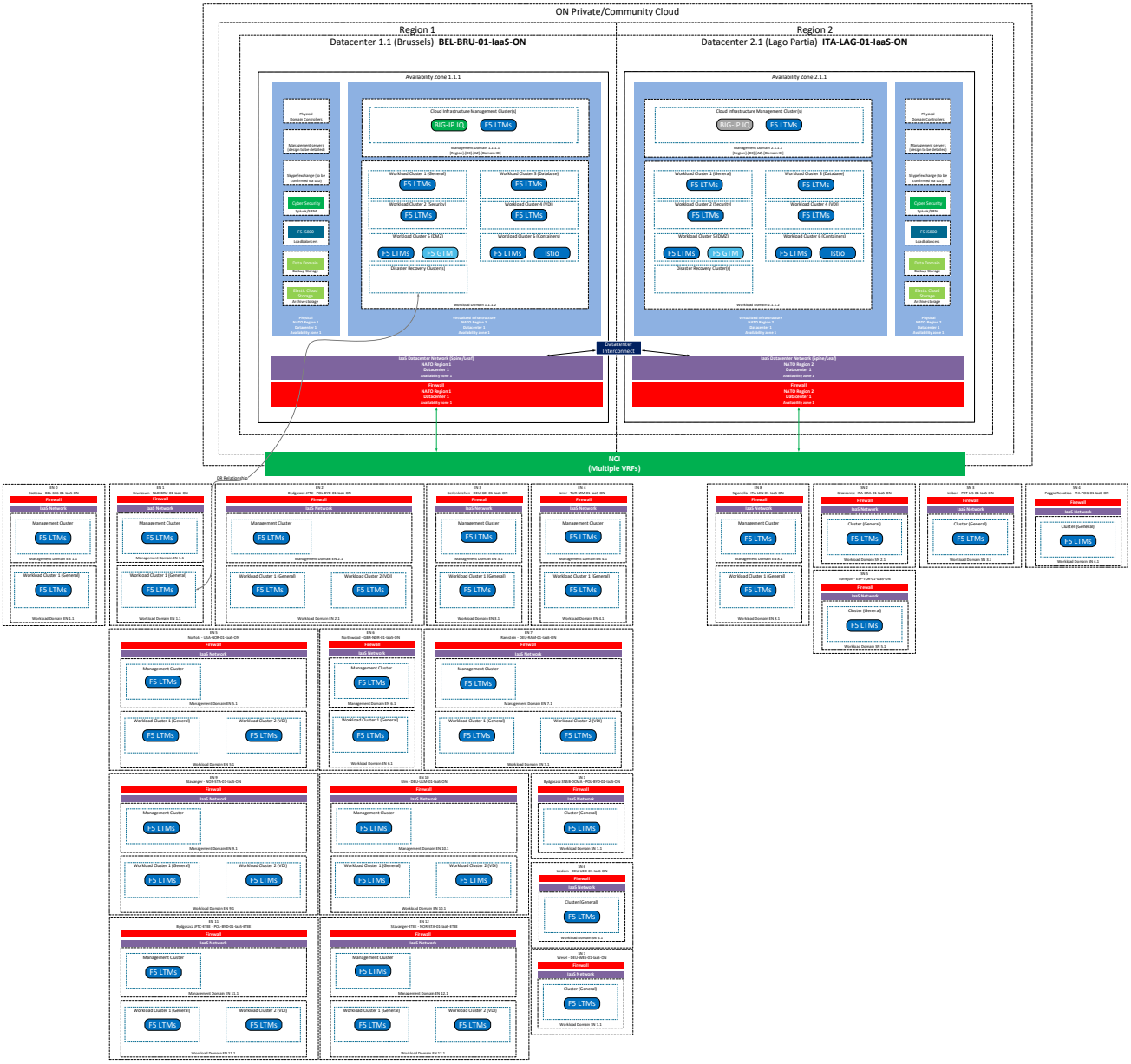


Figure 29 - F5 Load Balancing / ADC deployment per node

4.2.1.1. Global load balancers:

0252 F5 Global load balancers are deployed in order to provide DNS/Geographical load balancing of all applications leveraging distributed or centralized models.

0253 Since Global load balancing is based on DNS, the Root DNS services must be configured to delegate resolvable DNS names/zones to the GSLBs.

0254 Internal global load balancing clusters are deployed per datacentre, per global security zone (tenant) and maintains awareness of the status of all tenant internal services required to be globally load balances.

0255 One External global load balancing cluster is deployed per datacentre and maintains awareness of the status of all external services load balanced by local DMZ instances to redirect users to the appropriate DMZ service.

0256 The redirection is based on:

- Geographical preference (based on latency and/or fixed pairing of Node to service instance).
- Active/passive architectures.
- Detection of application failures.
- Automated or Manual Maintenance/Disaster response activities.

0257 During implementation, the F5 GSLB may be replaced by Infoblox or other alternative if it is deemed as a more appropriate.

4.2.1.2. Local load balancers:

0258 Local Load balancers are implemented to provide not only high availability of service, but SSL interception, web application firewall, user authentication and application access controls.

0259 Load balancing instances require to be dedicated to the tenant/global security zone and separated between DMZs and other internal security zones.

0260 F5 LTMs instances are deployed per global security zone and for each DMZ and application security zones.

0261 When leveraged, NSX Advance load balancing must be deployed as part of the edge nodes.

0262 The Local load balancers are integrating with ADFS in order to allow for claim based authentication for users. For F5 LTM, this is performed leveraging the Application Policy manager (APM).

0263 During the implementation, F5 LTMs may be replaced by NSX-T load balancers if it is demonstrated that implementing VMware Edge services and leveraging VMware Load balancing instead of F5 LTMs is more efficient and respond to security requirements

4.2.1.3. Datacentre Physical load balancers:

0264 In the datacentres F5 i5800 Physical load balancer clusters are deployed to load balance physical workloads. The F5 i5800 are deployed as clusters in each of the datacentre IaaS.

0265 Cisco ACI and F5 are used in a complementary manner, to enable policy based load balancing of traffic (Traffic is routed towards the F5 appliances based on ACI policies).

0266 Each physical load balancer is connected via a 4*10Gbps interface aggregate to Leaf switches. The physical connectivity is as follows:

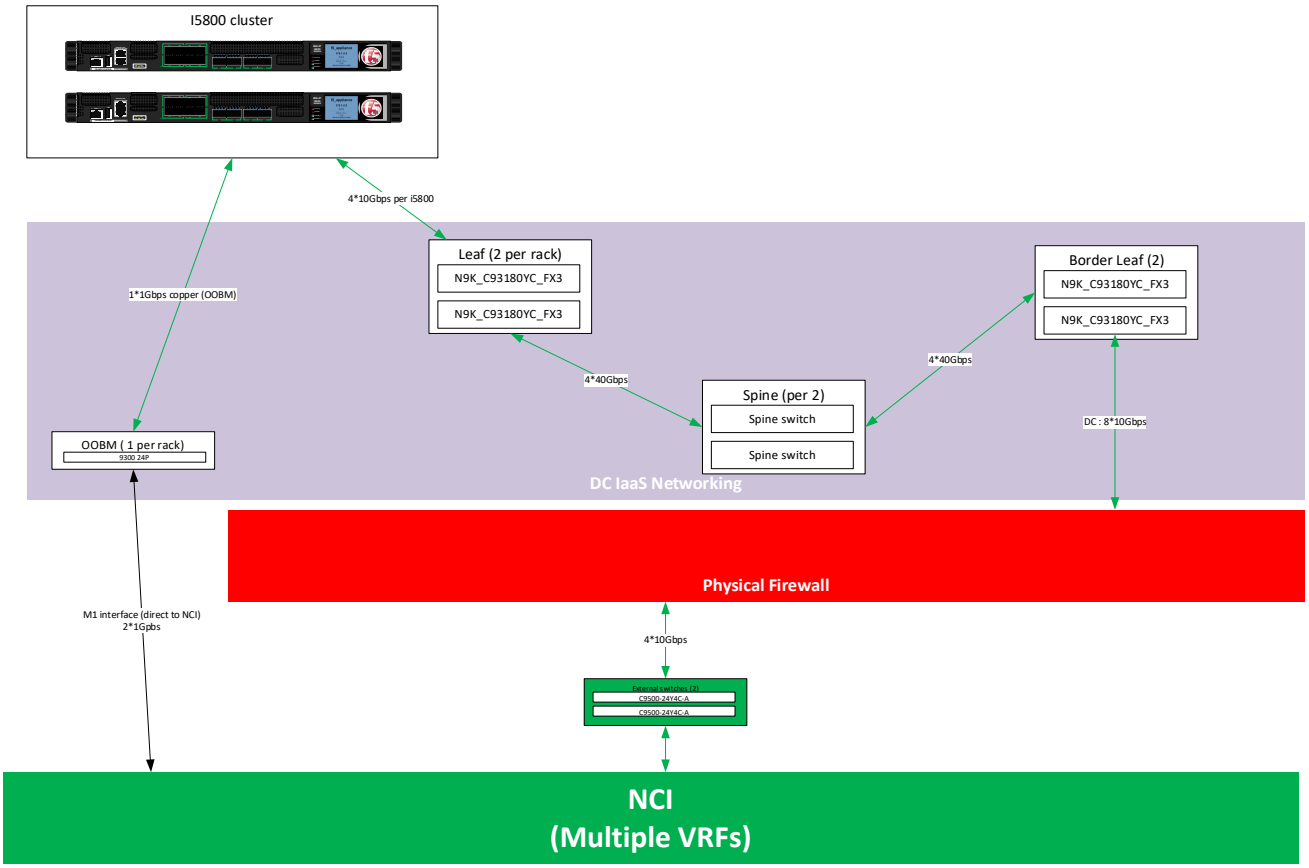


Figure 30 - DC Physical Load Balancer Connectivity

0267 The F5 i5800 clusters are configured to implement the same capabilities as per the Local Load balancer description in 4.2.1.2

0268 Multi-tenancy is supported by using dedicated virtual instance (vCMP) per security zone.

4.2.1.4. Load Balancing Security Mechanisms

0269 The security measures that apply to the load balancing sub-service are articulated in Table 23.

Security Mechanisms	NATO ON Solution
SM01a - Malware protection for server	Load balancing contains web application firewall features which protect servers from outside threats, including payload analysis that can protect against malware threats.
SM14 - Firewall (FW) for Outer Perimeter/Border Protection	The Local Load balancers deployed in the DMZ and in the application segments provide WAF capabilities.
SM15 - Firewall (FW) for Inner Perimeter	The Local Load balancers deployed in the DMZ and in the application segments provide WAF capabilities.
SM21a - System and Security Logging & Auditing	All load balancers configured to forward logs to the enterprise central SIEM/log collector (Splunk).
SM21b - System and Security Logging & Auditing - Applications	All load balancers configured to forward logs to the enterprise central SIEM/log collector (Splunk).

Security Mechanisms	NATO ON Solution
SM22 - Configuration and Hardening of network devices	All components are configured following existing NCI Agency hardening guideline (if it exist), DISA guidance and/or vendor best practices.
SM25 - Storage Compartmented Security Mode (SCSM)	N/A
SM26 - Data Backup, Replication and Recovery (DBRR)	Device level backups for configuration kept by the BIG IQ management application. And further backup via the backup/archive services.
SM28 - IT Forensic	Logs from load balancer appliances sent to the enterprise central SIEM/log collector (Splunk).
SM29 - Encryption-Decryption/Cryptography	Load balancer devices participate in the overall PKI solution for the enterprise. SSL is intercepted, payload analysed and re-encrypted to the server (if applicable).
SM30b - NPKI Devices, in conjunction with SM17	
SM31 - Security Zones	Dedicated load balancing instances are used per security zone.
SM32 - Policies, directives and procedures (PDP)	Follows the NCI Agency policies, directives and procedures to configured and implement NATO ON components.
SM33 - Load Balancing/Failover (LB/FO)	The load balancers is the central devices providing this service. Both local load balancing at a site, but also inter-datacentre failover provided by the F5 solution. The load balancers themselves set up in a cluster for stateful failover between the different components.
SM35 - Data Loss/Leak Prevention (DLP) for Devices	The ADC and Loadbalancing services are configured to contribute to DLP whenever required.
SM36 - Vulnerability Scanning & Compliancy	
SM42 - Identity & Access Management (IAM)	The load balancer appliances adhere to the MS AD identity management solution.
SM44 - Network Time Protocol (NTP)	Load balancer components leverage NCI Agency provided Stratum 1 time source for NTP.
SM45 - Logical Unit Number (LUN) Management for Storage Area Network (SAN)	N/A
SM47 - Data Activity Monitoring (DAM) and File Server Activity Monitoring (FSAM) using the Data Safeguarding mechanism	N/A
SM49 - Identity & Authentication, Access Control (IAAC)	As part of the WAF, Firewall and reverse proxy functions, identities are beings checked to provide access to services whenever applicable.
SM50 - DDoS	The ASM feature set of F5 provides DDOS protection for the services that it provides load balancing of other WAF support for.

Table 23 - Load Balancing Security Mechanism

5. SERVICE MANAGEMENT AND TOOLS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0270 The integration touch point between SMC Enterprise management and the IaaS services are shown in Table 24. This includes sending live health, performance, availability and capacity information to SMC components through such protocols as Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP). Further details on each component can be found in the SMC SDP.

Requirement Detail	Integration
The Infrastructure SMC service shall be provided through the following SMC components: a. IaaS Configuration Management System.	IaaS will be incorporated into the NATO ON Configuration Management System.
The Infrastructure SMC service shall be provided through the following SMC components: b. IaaS Event Management System.	IaaS will be incorporated into the NATO ON Event Management System.
The Infrastructure SMC service shall be provided through the following SMC components: c. IaaS Performance and Capacity System.	IaaS will be incorporated into the NATO ON Performance and Capacity System.
Although the underlying IaaS components may differ per node, the IaaS SMC Component shall provide standard interfaces for management and control of all IaaS SMC functionalities.	IaaS will use standard SNMP interfaces and COTS tools found on the NCI Agency approved products lists. These COTS tools use SNMP to collect management and control information.
The IaaS SMC Components shall have the ability to control pools of compute, storage and networking resources throughout the IaaS footprint from a consolidated set of applications and user interfaces.	IaaS uses Infoblox and vRealize to control pools of compute, storage and networking resources. See tables in section 4.1 and 4.2 for more detail.
Enhanced Nodes shall host IaaS SMC components to remotely manage and control limited IaaS capabilities in those nodes.	IaaS uses Infoblox and vRealize to host the IaaS SMC components for remote manage and control.
The Standard Nodes shall host SMC Element Manager Components only to allow remote management and control for the limited IaaS capabilities in those nodes	The Standard Nodes hosts SMC Element Manager Components only to allow remote management and control for the limited IaaS capabilities in those nodes.
The IaaS SMC components shall have a system/service monitoring ability that is able to collect information from the Purchaser's communication services monitoring and facilities support monitoring (see data-pack (Section 16) to provide the end-to-end services view.	IaaS uses Splunk, Infoblox and vRealize to deliver system and service monitoring. See section 4.1 and 4.2 for more detail.
The IaaS SMC Components shall provide the following management and control functions: Support Configuration Management: support configuration management of Infrastructure Services by providing discovery of infrastructure assets and configuration items (CI).	IaaS uses Splunk, Infoblox and vRealize to support configuration management. The SMC controls the configuration management process. See SMC SDP for more detail.

Requirement Detail	Integration
The IaaS SMC Components shall provide the following management and control functions: Support Cyber Security compliance: support the required CIS Security services.	IaaS uses Splunk and Palo Alto to report cyber security compliance to SMC for the CIS Security Services.
The IaaS SMC Components shall provide the following management and control functions: Monitor system/service behaviour: provide monitoring toolset for abnormal system/service behaviour defined by either thresholds or sets of system events.	IaaS uses Infoblox and vRealize to monitor and report system events to SMC.
The IaaS SMC Components shall provide the following management and control functions: Alert: generate alert if any of the thresholds are breached or any abnormal behaviour pattern is captured. Alert generation and escalation mechanism shall be customizable for different type of monitoring, users and situations.	IaaS uses Infoblox and vRealize to monitor thresholds and send alerts to SMC.
The IaaS SMC Components shall provide the following management and control functions: Trend/Correlation Analysis: provide analysis and correlation toolset for IaaS logs.	IaaS uses Splunk to collect data and send the information to SMC for trend analysis and correlation.
The IaaS SMC Components shall provide the following management and control functions: Record/Archive Events: record/archive pre-defined set of events generated by IaaS related systems.	IaaS uses Splunk to collect data and send to SMC. SMC uses ITSM to record and archive events.
The IaaS SMC Components shall provide the following management and control functions: Filter Events and Detect Anomalies: filter events for priority, criticality and deduplication and detect exceptions, faults, warnings within the logs.	IaaS uses Splunk to record the data and send it to SMC. SMC uses Remedy and ITSM processes to filter events and detect anomalies.
The IaaS SMC Components shall provide the following management and control functions: Meter Resource/Service Utilisation: record consumption of resources and utilisation of services for metering purposes. Provide data to IT Cost Management System.	IaaS uses Splunk to collect data to send to SMC to support the meter and resource and service utilisation.
The IaaS Configuration Management (CM) System shall support Enterprise Configuration Management by providing access to infrastructure assets and configuration items (CI).	IaaS uses Splunk and Infoblox to collect configuration information and send it to SMC. SMC performs the configuration management updates using ITSM implemented in Remedy.
The IaaS CM System shall provide the toolset to discover all IaaS Assets and their configuration information.	IaaS performs CM using SMC. Splunk collects the information and sends to SMC to perform the CM process.
The discovery and inventory shall not be limited to Microsoft Windows systems but shall also include Linux, UNIX and Apple systems.	IaaS uses Splunk to collect information and send it to SMC for this process.

Requirement Detail	Integration
IaaS CM System shall provide the ability to change, capture, duplicate, backup or restore the configuration of IaaS Systems.	IaaS integrates with E-SMC to perform the CM process which provides the ability to change, capture, duplicate, backup or restore the configuration of IaaS Systems.
IaaS CM System shall provide a dashboard with overall view of the IaaS infrastructure inventory items.	IaaS integrates with E-SMC to perform the CM process. SMC provides the dashboard configured with the overall view of the IaaS infrastructure inventory items
The IaaS Event Management (EM) System shall collect events generated from all IaaS Components and forward them to the Enterprise Event Management System.	IaaS uses Splunk, Infoblox and vRealize to collect information and send it to SMC. SMC uses Remedy to perform event management.
The IaaS EM System shall provide toolset for the operators to define, filter, correlate and group events according to their context, criticality, source and impacts	IaaS integrates with E-SMC toolset to enable operators to define, filter, correlate and group events.
The IaaS EM System shall provide toolset to automatically generate alarms, escalate and trigger for automated actions.	IaaS integrates with E-SMC to automatically generate alarms, escalate and trigger for automated actions.
The IaaS EM System shall provide customizable dashboards and report building toolset to the operators.	IaaS integrates with E-SMC to customize dashboards and the report building toolset to the operators.
The IaaS EM System shall provide automated processing and filtering of events to enhance performance and optimize resources.	IaaS integrates with E-SMC to provide automated processing and filtering of events to enhance performance and optimize resources.
The IaaS EM System architecture shall allow distributed and hierarchical deployment that will support resilience of the event management process.	IaaS integrates with E-SMC to allow distributed and hierarchical deployment support resilience or the event management process.
The IaaS EM System shall provide event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns in IaaS.	IaaS integrates with E-SMC to provide the event correlation toolset to customize or adapt detection normal and abnormal behaviour patterns.
The IaaS EM System shall provide policy and rule based event filtering, alarm triggering and report generating capabilities.	IaaS integrates with E-SMC to provide policy and rule-based event filtering, alarm triggering and report generating capabilities.
The IaaS Performance and Capacity Management System shall provide visibility on usage patterns over daily, monthly and variable periods. This toolset shall support trend and abnormal behaviour analysis.	IaaS integrates with E-SMC for the performance and capacity process.

Requirement Detail	Integration
The IaaS Performance and Capacity Management System shall provide toolset to trigger automated actions when resource utilisation thresholds are breached.	IaaS integrates with E-SMC for the performance and capacity management process. The individual configuration item that has a Service Level agreement associated with its performance is configured to send event data. This event data is configured to alert when resource utilization thresholds are breached.
The Performance and Capacity Management System shall support both current and projected capacity assessments.	IaaS integrates with E-SMC for the performance and capacity management process.
The Performance and Capacity Management System shall provide the following functionality: Integration with Enterprise SMC to provide visibility on enterprise level.	IaaS integrates with E-SMC for the performance and capacity management process.
The Performance and Capacity Management System shall provide the following functionality: Reserve capacity and performance of IaaS resources per tenant and per service.	IaaS integrates with E-SMC for the performance and capacity management process.
The IaaS Automation and Orchestration System shall provide the toolset to automate IaaS provisioning tasks via a single user interface for networking, storage and processing services.	IaaS integrates with E-SMC for the automation and orchestration system to meet this requirement.
The IaaS Automation and Orchestration System shall include template based automatic creation of application server roles for NATO and Enterprise Core Service Applications.	IaaS integrates with E-SMC for the automation and orchestration system to meet this requirement.
The IaaS Automation and Orchestration System shall accept triggers from IaaS Event, Configuration, Capacity and Performance Management Systems.	IaaS integrates with E-SMC for the automation and orchestration system to meet this requirement.
The IaaS Automation and Orchestration System shall provide workflow mechanism that enables multiple operators to be involved in acknowledgement and authorization of the automated tasks	IaaS integrates with E-SMC for the automation and orchestration system to meet this requirement
The IaaS Automation and Orchestration System shall enable the operators to execute tasks for remote nodes from Service Operation Centre(s).	IaaS integrates with E-SMC for the automation and orchestration system to meet this requirement.
The processing component shall log and report the capacity at least in terms of: processing time, RAM, storage device capacity, storage device time, network interfaces utilisation, logical queues for the physical capacity available, logical capacity used by guests.	vSphere provides the relevant statistics as required. In addition, this information will be available with the BMC management suite.

Table 24 - Service Management and Tools Requirements

5.1. Service Area Management

0271 The integration between IAAS Element Management and Enterprise Service Management & Control is focused on TrueSight Capacity & Operations Management. TrueSight provides visibility into the performance and capacity management of NATO ON Services.

0272 Enterprise Splunk provides event management collection for the Enterprise.

0273 The integration touch point between SMC enterprise management (TrueSight) and the IaaS Element Management services is shown in Table 25 and element management metric collection is detailed within Section 7.3 Measurement Collection.

0274 For integrated interface between Element and Enterprise Management, See NATO ON Service Management & Control SDP Section 4.0.

Subservice	Component	Connection Point	Description
Core Switching	Network Switch	BMC TSCOM	Capacity and performance management
Core Switching	Network Switch	IPAM system (Infoblox)	IP management and configuration management.
Core/Campus Switching	Network Switch	Cisco APIC	Monitor network and configure management
Load Balancing	LTM/GTM	BIG-IQ	Monitor load balancing services, create new iRules or modify existing iRules. View performance of the system and keep policies synced between devices.
Load Balancing	LTM	vRealise Orchestration To be further defined	Automatically create new VIPs, change load balancing policy based on an application blueprint.
IP Addressing	Infoblox DDI	BMC Service Portal	Request new IP address space or allocate space to a function or project.
Compute Platform	Compute Server	BMC Remedy	Request for a server configuration.
Virtualisation	ESXi	TSCOM and vRealize	Monitor hypervisor host performance (CPU, Memory and network).
Virtualisation	vCenter	TSCOM and vRealize	Monitor virtualisation layer performance.
Virtual Networking	NSX	vRealize	Create network overlays for new systems or applications.
Automation	To be further defined	To be further defined	To be further defined
Infrastructure Storage	vCenter	TSCOM and vRealize	Manage performance and exceptions on the storage.
VDI Storage	vCenter	TSCOM and vRealize	Manage performance and exceptions on the storage.
Backup Storage	Data Domain	TSCOM and vRealize	Manage performance and exceptions on the storage array.

Subservice	Component	Connection Point	Description
Archive Storage	To be defined	TSCOM and vRealize	Manage performance and exceptions on the archive storage service.
BPS1	PA Firewall	TSCOM and Panorama	Manage performance and exceptions on the BPS1 firewall.

Table 25 - IaaS Management

5.2. Subservice Area and Element Management

0275 Subservices require technology specific element management tools for regular administrative tasks and operation. The tools required to manage each subservice and element are shown in Table 26.

Subservice	Software/Device	Tool	User	Purpose
Compute Platform	vSAN ready node servers	HP One View	Server Admin	Remote access to console.
Virtualisation Platform	VMware ESXi	vCenter	Server Admin	Manage VMs and ESX servers.
Infrastructure Storage	VMware ESXi	vCenter	Storage Admin	Manage EMC Unity Infrastructure Arrays.
Infrastructure Storage	VMware ESXi	vCenter	Storage Admin	Manage EMC Unity Infrastructure Arrays.
VDI Storage	VMware ESXi	vCenter	Storage Admin	Manage EMC XtremIO Arrays.
Backup Storage	T1/T2/T3 backup storage	Veeam TBD	Backup Admin / Storage Admin	Manage Data Domain Arrays.
Backup Storage	All Data Domain Arrays	System CLI/SSH Console	Backup Admin / Storage Admin	Manage Data Domain Arrays.
Archive Storage	To be defined	Veeam TBD	Backup Admin/Storage Admin	Manage archiving storage and rules
Backup and Archiving	Veeam	Veeam console	Backup Admin	Manage Backup and Recovery configuration and jobs.
Core Switching	Switch OS	Secure Shell	Network Admin	Remote access to device.
OOB Management switch	Switch OS	Secure Shell	Network Admin	OOB remote access to device.
Core Switching	Switch OS	Secure Shell/SNMPv3	Network Admin	Access, monitor and edit configuration.
Core Switching	SNMPv3	SCOM/Solar Winds	Network team/SOC/Auditor	Network monitoring.

Subservice	Software/Device	Tool	User	Purpose
Core Switching	Syslog	Splunk/Solar Winds	Network team/SOC/Auditor	Log file management, troubleshooting and analytic.
Core Switching	Cisco ISE	TACACS+ Device Authentication	Network Admin, SOC Operator, Service Desk Personnel	Provide AAA services for core switching equipment.
AD DNS	IPAM	AD-DNS Server	Network Admin, System Admin	Provide central and integrated DNS Management.
AD DHCP	IPAM	AD-DHCP Server	Network Admin, System Admin	Provide central and integrated DHCP Management.
Load Balancing	F5 i5800 and virtual load balancers	F5 BigIQ Portal TBD	Network Admin	Manage F5 virtual and physical load balancers.
IP Addressing	Infoblox DDI	Infoblox DDI	Network Admin	Manage IP Address within NATO ON environment.
BPS1	Palo Alto 5XXX and 3XXX	Palo Alto Panorama	Network Admin	Manage Palo Alto Firewall Devices.
	VMware ESXi	vCenter	Server Admin	Manage VMs and ESX servers.

Table 26 - Subservice Management Tools

6. SERVICE PROCESSES [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0276 This section provides the mapping of ITIL processes with NATO ON Capabilities.

6.1. Process Design

0277 Five category 1 and twelve category 2 ITIL processes have been designated to support the NATO ON process implementation and NATO ON Services implementation (total of 17 ITIL processes). Each of the 17 ITIL process documents (SOPs/Steps/Work Instructions) need to be developed as a separate set of artefacts to provide the information requirements of SDP Section 5.1 and SDP Appendix 3 for each of the NATO ON Services. The ITIL process documents and the associated processes, procedures and work instructions are for inclusion in the Operations Manual. Each ITIL process document will include a process overview diagram with initial roles identified to manage each process and a list of the KPIs to support the process objectives. Table 27 provides a reference for the ITIL processes directly supporting each NATO ON Service operating in a production environment. Refer to the separate ITIL Process Documentation Artefacts for process overview and workflow. SMC is listed in Table 27 as an NATO ON Capability, as it provides the integrated toolsets and processes utilised in NATO ON Service support and delivery.

ITIL Lifecycle Stage	ITIL Processes Directly Supporting NATO ON Services Operating in Production Environment	Notes for CPS, ECS, IaaS Services	NATO ON Service / NATO ON Capability			
			IaaS	CPS	ECS	SMC
SS	Financial Management for IT Services	Charge back and cost information.	X	X	X	X
SD	Service Level Management	Provide information for service reviews and improvement opportunities.	X	X	X	X
SD	Availability Management	Monitor and report actual service and infrastructure availabilities to meet service levels.	X	X	X	X
SD	Capacity Management	Monitor and report service and infrastructure performance and capacities to meet service levels.	X	X	X	X
SD	IT Services Continuity Management	Test and support continuity plans.	X	X	X	X
SD	Information Security Management	Repeatedly validate security control effectiveness.	X	X	X	X
ST	Change Management	Raise RFC to add, modify or remove anything with impact on the service.	X	X	X	X
ST	Service Asset and Configuration Management	Provide Asset/CI information and configuration control.	X	X	X	X
ST	Release and Deployment Management					X

ITIL Lifecycle Stage	ITIL Processes Directly Supporting NATO ON Services Operating in Production Environment	Notes for CPS, ECS, IaaS Services	NATO ON Service NATO ON Capability			
			IaaS	CPS	ECS	SMC
ST	Service Validation and Testing					X
ST	Change Evaluation					X
ST	Knowledge Management	Collect and manage the Know How of the IT Organisation to support and deliver the service.	X	X	X	X
SO	Request Fulfilment					X
SO	Incident Management	Log incident for unplanned interruption to the service.	X	X	X	X
SO	Access Management	Manage user permission.	X	X	X	X
SO	Problem Management	Detect and eliminate the cause of the problem.	X	X	X	X
SO	Event Management	Monitor and resolve alerts or notifications with impact to the service.	X	X	X	X

Table 27 - ITIL Processes Directly Supporting NATO ON Service in Production

7. SERVICE ORGANISATIONAL SKILL LEVELS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0278 To maintain consistency and avoid conflicting information between design documents containing the same information, please refer to SMC SDP document for Section 6.0 content.

7.1. Service Organisational Skill Levels Requirements

0279 To maintain consistency and avoid conflicting information between design documents containing the same information, please refer to SMC SDP document for Section 6.1 content. See Annex D of this SDP for service specific man-power level and skills (Role).

8. SERVICE MEASUREMENT [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0280 This section details the mechanisms for collecting, analysing and reporting on component and service metrics and measures that feed into and support agreed-upon KPIs.

8.1. KPI Analysis and Reporting [To be further updated during implementation]

0281 The objective of service measurement is identification and collection of data/information that identifies and quantifies service value-adds and contributions to achieving organisation goals. Service measurement identifies indicators of service risks, issues and improvement opportunities. The objective of service reporting is to analyse and deliver service measurement information (reports) in a format to facilitate action by decision makers.

0282 Service measurement will gather the data from approved NATO ON/SMC monitoring tools or from manual data/information gathering methods and report on progress toward achieving agreed-upon KPIs. The service measurement information will provide linkage between higher-level NATO ON service or process goals and objectives, critical success factors, metrics, and measures. As used in this KPI design, a measure (raw data) is defined as a number derived from taking a measurement, such as the weight or temperature of something, the number of website visits or the number of logged incidents. In contrast, a metric is defined as a calculation between two measures. The calculation is typically a form of division and the result is expressed as a percentage, ratio, fraction, decimal or the like.

0283 Table 28 is the KPI design for service measurement data and information as an exemplar of what will be provided as part of updating and optimisation of KPI design and metrics for each service, monitoring service-based testing, and as part of FSA.

Critical Success Factor 1.0 [what (actions) must happen to succeed] (Performance Objective)	**Maintain Storage Capacity to Meet Current and Future Operational Needs**
KPI ID	1.0.1
KPI Description [If our actions are succeeding (effect)] (Desired Outcome/Result)	Tier 3 storage capacity adequate to back up all data, per classification
Component Measure 1 (what to measure at the component level)(what would prevent success/outcome/result/ dependencies)	Storage capacity (Gigabytes/Terabytes/Petabytes)
Component Measure 2	Usable free disk space (percentage of total capacity)
KPI Metric (Formula)	(Storage capacity/usable free disk space) x 100
KPI Target	>25% storage scalability, per classification
Frequency	Data collection frequency: daily (7 days per week)
	Reporting frequency: monthly (calendar), by 10th of following month
Responsible Parties	Data/Information Collector: TBC
	Data/Information Customer: NCI Agency Capacity Manager

Critical Success Factor 1.0 [what (actions) must happen to succeed] (Performance Objective)	Maintain Storage Capacity to Meet Current and Future Operational Needs
Data Source	SCOM
Reporting Format	For one-time snapshot report – stacked bar chart showing proportion of storage capacity required to total usable free disk space

Table 28 - IaaS – Storage Sub-service Objective – Provide Scalable Storage Capacity for the NATO ON Enterprise

0284 The approved NATO ON/SMC Toolsets, as mapped to NATO processes and service components, will be used to capture, store and process (threshold monitoring) the service-specific KPI measurement data for use in standardised reports and dashboards in compliance with the NCI Agency's information quality and classification standards. Access control-levels will be used to ensure service measurement data and reports are transparent and available across management and functions based on defined roles and responsibilities.

IaaS Service KPI will need to be further defined/refined with linkage to NATO ON service goals and objectives as the detailed design is further developed.

The KPI design solution for service measurement and service reporting will include the below activities and provide the basis for a standard measurement and reporting process.

- Build, test and deploy measurement data collection, storage, processing, analysis and reporting to satisfy KPI requirements.
- Review and evaluate service-critical success factors and KPIs for 'what should be measured' and 'what can be measured', adjusting or (re)negotiating requirements and/or expectations as necessary.
- Provide early life support for transition and review tasks, which includes how to request a report or make changes to a report.
- Deploy measurement and reporting change request and incident reporting procedures as part of process tailoring.
- Update the Service Catalogue if applicable.
- Publish service measurement and service reporting standards.
- Establish service measurement and service reporting controls and governance.
- Provide information to NCI Agency staff/users/support staff so they are aware of service measurement and service reporting capabilities.
- Establish access control levels for reports based on organisation information classification standards.
- Verify service measurement and reporting requirements map to NATO ON standard tool capabilities for capturing, processing and analysing data and reporting the data/information.
- Continually identify capability gaps and propose design solution(s) for gap closure.

8.2. KPI Measures and Metrics Analysis and Reporting

0285 Measures and metrics for service-level defined KPIs will be monitored and collected via four main methods. They are:

- A combination of real-time automated alerts from SMC tools and report generated by Enterprise monitoring personnel.
- Manual review of automated alerts via SOPs implemented by system administrators.
- User report through service desk and service desk ticket tends analysis.

- Review of vendor service and equipment maintenance (RMA) activities.

0286 All information related to KPI measurement for availability, capacity and performance will be consolidated in the enterprise management dashboard and analysed as required to ensure that system targets for confidentiality, integrity and availability are maintained.

8.3. Measurement Collection

0287 Measurements to support KPIs will be collected on all IaaS subservices. The following sections outline the measurements for initially defined KPI availability, capacity and performance of the service subservices, dependencies and the monitoring/collection toolset.

8.3.1. Infrastructure Processing

0288 The following KPIs will be collected for the processing subservice.

Subservice	Measure	Data	Monitoring/Collection
Processing	Host CPU Utilisation	70%	vROPs & TSOM / Splunk
Processing	Host Average Memory Utilisation [18.2.1.12]	80%	vROPs & TSOM / Splunk
Processing	Host Peak Memory Utilisation [18.2.1.13]	percentage	vROPs & TSOM / Splunk
Processing	Host Datastore utilisation	70%	vROPs & TSOM / Splunk
Processing	Host I/O Reads	Requires baselining	vROPs & TSOM / Splunk
Processing	Host I/O Writes	Requires Baselining	vROPs & TSOM / Splunk
Processing	Host Interface utilisation	70%	vROPs & TSOM / Splunk
Processing	Host Storage latency	5ms	vROPs & TSOM / Splunk
Processing	Host Intake temperature	TBD	vROPs & TSOM / Splunk
Processing	VM Ready Time	10ms	vROPs & TSOM / Splunk
Processing	VM CPU utilisation [18.2.1.10]	70%	vROPs & TSOM / Splunk
Processing	VM Memory Utilisation [18.2.1.11]	80%	vROPs & TSOM / Splunk
Processing	VM Network Utilisation	2gbps	vROPs & TSOM / Splunk

Table 29 - KPI Infrastructure Processing

8.3.2. Infrastructure Networking

0289 The following KPIs will be collected for the networking subservice.

Subservice	Measure	Data	Monitoring/Collection
Core Switching	Round trip time [18.2.1.6]	ms	ONM & TSOM/Splunk
Core Switching	Usable Bandwidth [18.2.1.7]	MB	ONM & TSOM/Splunk
Core Switching	Latency and Jitter [18.2.1.8]	ms	ONM & TSOM/Splunk
Core Switching	Spine Switches availability- uptime	99.99%	ONM & TSOM/Splunk
Core Switching	Leaf Switches availability- uptime	99.99%	ONM & TSOM/Splunk
Core Switching	Leaf to Leaf Latency	5ms	ONM & TSOM/Splunk
Core Switching	Leaf to WAN Latency	5ms	ONM & TSOM/Splunk

Subservice	Measure	Data	Monitoring/Collection
Core Switching	Leaf Uplink Utilisation	70%	ONM & TSOM/Splunk
Core Switching	Leaf Switch Port capacity	80%	ONM & TSOM/Splunk
Core Switching	Spine switch Port capacity	80%	ONM & TSOM/Splunk
DCI	Leaf to DCI latency	<5ms?	ONM & TSOM/Splunk
DCI	Datacentre to Datacentre Latency	ms	ONM & TSOM/Splunk
Core switching	Supplier RMA	Next Business Day	Remedy

Table 30 - KPI Infrastructure Networking

8.3.3. Infrastructure Storage

0290 The following KPIs will be collected for the storage subservice.

Subservice	Measure	Data	Monitoring/Collection
All Storage	Capacity [18.2.1.1]	Gigabytes / Terabytes / Petabytes	vROPs & TSCM / Splunk
All Storage	Usable Free Disk Space [18.2.1.2]	% of total capacity	vROPs & TSCM / Splunk
All Storage	5GB file retrieval time [18.2.1.3]	ms	vROPs & TSOM / Splunk
All Storage	5MB file retrieval time [18.2.1.4]	ms	vROPs & TSOM / Splunk
All Storage	Input/ Output per Second (IOPS) [18.2.1.5]	iops	vROPs & TSOM / Splunk
Infrastructure Storage	SMB Average Read Latency	<15ms	vROPs & TSOM / Splunk
Infrastructure Storage	SMB Average Write Latency	<5ms	vROPs & TSOM / Splunk
Infrastructure Storage	NFS Average Read Latency	<15ms	vROPs & TSOM / Splunk
Infrastructure Storage	NFS Average Write Latency	<5ms	vROPs & TSOM / Splunk
Infrastructure Storage	MAX Port Throughput	<900MB/s	vROPs & TSOM / Splunk
Infrastructure Storage	Average Port Throughput	<700MB/s	vROPs & TSOM / Splunk
Infrastructure Storage	SP Processor Utilisation	<70%	vROPs & TSOM / Splunk
Infrastructure Storage	SP Cache Utilisation	<70%	vROPs & TSOM / Splunk
Infrastructure Storage	Disk Utilisation	<70%	vROPs & TSOM / Splunk

Subservice	Measure	Data	Monitoring/Collection
Infrastructure Storage	Pool Capacity Utilisation	<90%	vROPs & TSOM / Splunk
VDI Storage	System Capacity Utilisation	<85%	vROPs & TSOM / Splunk
VDI Storage	MAX Port Throughput	<900MB/s	vROPs & TSOM / Splunk
VDI Storage	Average Port Throughput	<700MB/s	vROPs & TSOM / Splunk
Backup Storage	MAX Port Throughput	<900MB/s	vROPs & TSOM / Splunk
Backup Storage	Average Port Throughput	<700MB/s	vROPs & TSOM / Splunk
Backup Storage	System / Storage Pool Capacity Utilisation	<85%	vROPs & TSOM / Splunk
Backup Storage	System CPU Utilisation	<70%	vROPs & TSOM / Splunk
Archive Storage	Storage Pool Capacity	<95%	vROPs & TSOM / Splunk
Archive Storage	CPU Utilisation	<70%	vROPs & TSOM / Splunk
Archive Storage	Relative NIC %	>%10	vROPs & TSOM / Splunk
Backup Service	Backup interval [18.2.1.9]	Seconds	vROPs & TSOM / Splunk
Backup Service	Backup type (incremental, full) [18.2.1.9]	type	vROPs & TSOM / Splunk
Backup Service	Backup time to recover [18.2.1.9]	seconds	vROPs & TSOM / Splunk
Backup Service	backup media [18.2.1.9]	Storage/archive	vROPs & TSCM / Splunk
Backup Service	Backup archive interval [18.2.1.9]	days	vROPs & TSOM / Splunk

Table 31 - KPI Infrastructure Storage

8.3.4. Infrastructure CI Security

0291 The following KPIs will be collected for the CI Security subservice.

Subservice	Measure	Data	Monitoring/Collection
BPS1	CPU utilisation	75%	Panorama & TSOM / Splunk
BPS1	Interface utilisation	75%	Panorama & TSOM / Splunk
BPS1	Blocked malicious traffic	requires baselining	Panorama & TSOM / Splunk
BPS1	TCP connections	requires baselining	Panorama & TSOM / Splunk
BPS1	Packets per second/interface	requires baselining	Panorama & TSOM / Splunk
BPS1	Firewall denies	requires baselining	Panorama & TSOM / Splunk
BPS1	Blocked URLs	Requires baselining	Panorama & TSOM / Splunk
BPS1	Blocked applications	Requires baselining	Panorama & TSOM / Splunk

Table 32 - KPI Infrastructure CIS

Annex A (SUB)SERVICES INTERFACE CONTROL DOCUMENT [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

A.1. Introduction

0292 This appendix describes the ICDs for the IaaS subservices and will be updated during the development and implementation of the solution.

Annex B COMPONENT TO ICD MAPPING [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

Annex C NATO ON PROCEDURES AND WORK INSTRUCTIONS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0293 NCI Agency requires complete procedures and work instructions to fulfil the operational tasks associated with the design that this SDP articulates. It is further understood that these procedures and work instructions will be completed to the point that a knowledgeable administrator will be able to take the procedures and effectively operate and maintain the environment, given the skill levels outlined in section 6 of this SDP.

0294 Below is a list of typical procedures that will need to be carried out for each service lane.

0295 However it is expected with the implementation of the DevOps approach and automation, that the majority of the SOPs listed below will not be required and/or not required to be triggered manually.

C.1. Core Switching

0296 IaaS Core Switching SOPs are presented in Table 33, including description, actors, frequency of execution, tools, and reference number.

SOP Description	Actor	Frequency	Tool	SOP Ref
Create VLAN and/or VLAN interface	Network Operator	As needed		
Create VRF	Network Admin	As needed		
Delete VLAN and/or VLAN interface	Network Admin	As needed		
Delete VRF	Network Admin	As needed		
Advertise VLAN subnet in OSPF	Network Admin	As needed		
Remove VLAN subnet in OSPF	Network Admin	As needed		
Add static route	Network Admin	As needed		
Remove static route	Network Admin	As needed		
Remove static route	Network Admin	As needed		
Assign VLAN to access port	Network Admin	As needed		
Remove VLAN to access port	Network Admin	As needed		
Assign VLAN to trunk port	Network Admin	As needed		
Remove VLAN from trunk port	Network Admin	As needed		
Create layer 2/3 port channel	Network Admin	As needed		
Delete layer 2/3 port channel	Network Admin	As needed		
Create VLT domain	Network Admin	As needed		
Delete VLT domain	Network Admin	As needed		
Create read-only Network Admin account	Network/System Admin	As needed		
Delete read-only Network Admin account	Network Admin	As needed		
Create privilege Network Admin account	Network Admin	As needed		

SOP Description	Actor	Frequency	Tool	SOP Ref
Delete privilege Network Admin account	Network Admin	As needed		

Table 33 - Core Switching SOP Definition

C.2. Load Balancing

0297 Load Balancing SOPs are presented in Table 34, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Upgrade BIG IP OS	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-001
Web Browser	Power off the system	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-002
Web Browser	Power on the system	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-003
Web Browser	Replace power supply	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-004
Web Browser	Replace fan tray	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-005
Web Browser	Replace cable	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-006
Web Browser	Replace SFP	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-007
Web Browser	Replace cable	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-008
Web Browser	Promote standby unit to active	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-009
Web Browser	Add new self-IP	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-010
Web Browser	Create UCS archive file	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-011
Web Browser	Restore to previous UCS archive file	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-012
Web Browser	Provision BIG-IP system resources	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-013
Web Browser	Create a new pool	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-014
Web Browser	Create a new node	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-015
Web Browser	Remove a node	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-016
Web Browser	Add a new pool member	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-017

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Remove a pool member	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-018
Web Browser	Create a new virtual server	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-019
Web Browser	Enable local traffic objects	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-020
Web Browser	Disable local traffic objects	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-021
Web Browser	Create new profile	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-022
Web Browser	Edit existing profile	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-023
Web Browser	Create new iRule	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-024
Web Browser	Create new iApp	Network Admin L3	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-025
Web Browser	Provision new application	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-026
Web Browser	Add new user	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-027
Web Browser	Remove/edit existing user	Network Admin L2	As needed	BIG IP Web GUI	NATO-ON-SOP-LB-028

Table 34 - Load Balancing SOP Definition

C.3. IP Addressing

0298 IP Addressing SOPs are presented in Table 35, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
IPAM	Allocate IP address assignment	Network/System Admin	As needed		
IPAM	Remove IP address assignment	Network/System Admin	As needed		
IPAM	Delegate per site/CoI IP address manager	Network/System Admin	As needed		
IPAM	Remove delegate per site/CoI IP address manager account	Network/System Admin	AS needed		

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
IPAM	Discover active subnets on network	Network/System Admin	Monthly		
IPAM	Recover unused subnets	Network/System Admin	Monthly		

Table 35 - Addressing SOP Definition

C.4. Infrastructure Processing Process Design

0299 The SOPs specific to the IaaS Infrastructure Processing subservice have been broken up into the appropriate subservice and addressed herein.

C.5. Compute Platform

0300 Compute Platform SOPs are presented in Table 36, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
	Rack and cable server	Tier-2 compute	As needed		
	Replace HDD	Tier-2 compute	As needed		
	Replace memory	Tier-2 compute	As needed		
	Harden server	Tier-2 compute	As needed		
	Configure Active Directory authentication	Tier-2 compute	As needed		
	Boot from ISO image	Tier-2 compute	As needed		
	Update server firmware	Tier-2 compute	As needed		

Table 36 - Compute Platform SOP Definition

C.6. Virtualisation Platform

0301 Virtualisation Platform SOPs are presented in Table 37, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
vCenter Server	Create/update vSphere template	Template Admin	As needed	vCenter Server	NATO-ON-SOP-VIRT-001
vCenter Server	Create/update customisation specification	Template Admin	As needed	vCenter Server	NATO-ON-SOP-VIRT-002
vCenter Server	Increase/decrease VM resources	vSphere Admin	As needed	vCenter Server	NATO-ON-SOP-VIRT-003
Update Manager	Upgrade VM hardware	Update Admin	As needed	Update Manager	NATO-ON-SOP-VIRT-004
Update Manager	Upgrade VM tools	Update Admin	As needed	Update Manager	NATO-ON-SOP-VIRT-005

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
vROPs	Monitor resource requirements	vSphere Admin	As needed	vROPs	NATO-ON-SOP-VIRT-006
vCenter	Create/apply host profiles	vSphere Admin	As needed	vCenter	NATO-ON-SOP-VIRT-007
ESXi & vCenter	Apply security settings to ESXi/vCenter components	vSphere Admin	As needed	ESXi & vCenter	NATO-ON-SOP-VIRT-008
vROPs & vCenter	Manage/monitor host resources	vSphere Admin	Daily	vROPs & vCenter	NATO-ON-SOP-VIRT-009
vROPs & vCenter	Manage/monitor cluster resources	vSphere Admin	As needed	vROPs & vCenter	NATO-ON-SOP-VIRT-010
ESXi	Redeploy/deploy ESXi hosts	vSphere Admin	As needed	ESXi	NATO-ON-SOP-VIRT-011
vROPs	Review performance metrics	Operations Centre, Help Desk, vSphere Admin, Storage Admin, Network Admin	Daily	vROPs	NATO-ON-SOP-VIRT-012
vCenter	Enable/disable DRS	vSphere Admin	As needed	vCenter	NATO-ON-SOP-VIRT-013
vCenter	Enable/disable HA	vSphere Admin	As needed	vCenter	NATO-ON-SOP-VIRT-014
vCenter	Create/update DRS affinity rules	vSphere Admin	As needed	vCenter	NATO-ON-SOP-VIRT-015
vROPs	Resource forecasting	Resource Manager	As needed	vROPs	NATO-ON-SOP-VIRT-016
vCenter	Manage resource pools	vSphere Admin	As needed	vCenter	NATO-ON-SOP-VIRT-017
UMDS	Set up/manage UMDS server	Update Admin	As needed	UMDS	NATO-ON-SOP-VIRT-018
UMDS	Configure/manage UMDS downloads	Update Admin	As needed	UMDS	NATO-ON-SOP-VIRT-019
Update Manager	Subscribe update manager to UMDS web site	Update Admin	As needed	Update Manager	NATO-ON-SOP-VIRT-020
Update Manager	Push updates to ON	Update Admin	Monthly/as needed	UMDS	NATO-ON-SOP-VIRT-021
Update Manager	Remediate hosts, appliances, and virtual machines hardware and tools	Update Admin	As needed	Update Manager	NATO-ON-SOP-VIRT-022

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Update Manager & UMDS	Maintain/manage regular update cycle	Update Admin	As needed	Update Manager & UMDS	NATO-ON-SOP-VIRT-023
vCenter	Create/publish content library	Template Admin	As needed	vCenter	NATO-ON-SOP-VIRT-024
vCenter	Create/subscribe to content library	Template Admin	As needed	vCenter	NATO-ON-SOP-VIRT-025
vCenter	Upload templates and ISOs to the content library	Template Admin	As needed	vCenter	NATO-ON-SOP-VIRT-026
vCenter	Create templates	Template Admin	As needed	vCenter	NATO-ON-SOP-VIRT-027
Operating System	Update templates	Template Admin	As needed	Operating System	NATO-ON-SOP-VIRT-028
vCenter & Operating System	Test template updates	Template Admin	As needed	vCenter & Operating System	NATO-ON-SOP-VIRT-029
NSX Manager	Create/manage logical switches	Virtual Network Admin	As needed	NSX Manager	NATO-ON-SOP-VIRT-030
NSX Manager	Manager dynamic routing	Virtual Network Admin	As needed	NSX Manager	NATO-ON-SOP-VIRT-031
NSX Manager	Create new network segments	Virtual Network Admin	As needed	NSX Manager	NATO-ON-SOP-VIRT-032
NSX Manager & ESG	Create/manage edge service gateways (routing and FW)	Virtual Network Admin	As needed	NSX Manager & ESG	NATO-ON-SOP-VIRT-033
NSX ESG	Create/manage firewall rules	Virtual Network Admin	As needed	NSX ESG	NATO-ON-SOP-VIRT-034
NSX Service Composer	Create security groups	Virtual Network Admin	As needed	NSX Service Composer	NATO-ON-SOP-VIRT-035
NSX Service Composer & NSX Manager	Configure service composer integrations (IPAM, FW, AV, etc.)	Virtual Network Admin	As needed	NSX Service Composer & NSX Manager	NATO-ON-SOP-VIRT-036
NSX Manager & Active Directory	Manage NSX roles and responsibilities	Virtual Network Admin	As needed	NSX Manager & Active Directory	NATO-ON-SOP-VIRT-037
NSX Manager	Prepare ESXi hosts for NSX when adding new	Virtual Network Admin	As needed	NSX Manager	NATO-ON-SOP-VIRT-038
vRA & vCenter	Create/manage vRA blueprints	Blueprint Architect	As needed	vRA & vCenter	NATO-ON-SOP-VIRT-039

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
vRA & vRO	Create/manage vRA subscriptions	Blueprint Architect	As needed	vRA & vRO	NATO-ON-SOP-VIRT-040
vRA	Create/manage vRA business groups	Tenant Admin	As needed	vRA	NATO-ON-SOP-VIRT-041
vRA	Create/manage vRA fabric groups	Fabric Admin	As needed	vRA	NATO-ON-SOP-VIRT-042
vRA & vCenter	Create/manage vRA reservations	Fabric Admin	As needed	vRA & vCenter	NATO-ON-SOP-VIRT-043
vRA & vRO	Create/manage vRA catalogue	Catalogue Admin	As needed	vRA & vRO	NATO-ON-SOP-VIRT-044
vRA & Infoblox	Create/manage vRA network profiles	Fabric Admin	As needed	vRA & Infoblox	NATO-ON-SOP-VIRT-045
vRA	Create/manage custom properties	Blueprint Architect	As needed	vRA	NATO-ON-SOP-VIRT-046
vRA	Create/manage property groups	Blueprint Architect	As needed	vRA	NATO-ON-SOP-VIRT-047
vRO	Create/manage automation workflows	Workflow Developer	As needed	vRO	NATO-ON-SOP-VIRT-048
vRO	Configure/manage vRO plugins	vRO Admin	As needed	vRO	NATO-ON-SOP-VIRT-049
vROPs	Create/manage custom dashboards	vROPs Admin	As needed	vROPs	NATO-ON-SOP-VIRT-050
vROPs	Forecast resource availability	Resource Manager	Monthly	vROPs	NATO-ON-SOP-VIRT-051
vRLI	Configure Syslog sources	vSphere Admin	As needed	vRLI	NATO-ON-SOP-VIRT-052
Active Directory, vCenter, vRA, NSX, vROPs, vRLI & SRM	Review/manage roles and responsibilities	vSphere Admin, Network Admin vROPs Admin Disaster Recovery Admin	Monthly	Active Directory, vCenter, vRA, NSX, vROPs, vRLI & SRM	NATO-ON-SOP-VIRT-053
SRM	Create and manage protection groups	Disaster Recovery Admin	As needed	SRM	NATO-ON-SOP-VIRT-054
vSphere Replication	Create/manage vSphere replication	Disaster Recovery Admin	As needed	vSphere Replication	NATO-ON-SOP-VIRT-055

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
SRM & vCenter	Configure/manage inventory mappings	Disaster Recovery Admin	As needed	SRM & vCenter	NATO-ON-SOP-VIRT-056
SRM & vSphere Replication	Perform failover tests	Disaster Recovery Admin	As needed	SRM & vSphere Replication	NATO-ON-SOP-VIRT-057
SRM	Perform disaster recovery	Disaster Recovery Admin	As needed	SRM	NATO-ON-SOP-VIRT-058
vSphere Replication & SRM	Re-protect after disaster	Disaster Recovery Admin	As Needed	vSphere Replication & SRM	NATO-ON-SOP-VIRT-059

Table 37 - Virtualisation Platform SOP Definition

C.7. Infrastructure Storage Subservice

0302 The SOPs specific to the IaaS Infrastructure Storage subservice have been broken up into the appropriate subservice and addressed herein.

C.8. Infrastructure Storage Process Design

0303 Infrastructure Storage SOPs are presented in Table 38, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
AD-DS	Add a new user	Storage Admin L2	As needed		
AD-DS	Delete an existing user	Storage Admin L2	As needed		
Web Browser	Upgrade Unity OS	Storage Admin L3	As needed		
Web Browser	Power off the system	Storage Admin L3	As needed		
Web Browser	Power on the system	Storage Admin L3	As needed		
Web Browser	Replace hard drive	Storage Admin L2	As needed		
Web Browser	Replace power supply	Storage Admin L2	As needed		
Web Browser	Create storage pool	Storage Admin L2	As needed		
Web Browser	Expand storage pool	Storage Admin L2	As needed		
Web Browser	Add a new block host	Storage Admin L2	As needed		
Web Browser	Create an NFS export	Storage Admin L2	As needed		
Web Browser	Expand an NFS export	Storage Admin L2	As needed		
Web Browser	Shrink an NFS export	Storage Admin L2	As needed		
Web Browser	Delete an NFS export	Storage Admin L2	As needed		
Web Browser	Create an SMB share	Storage Admin L2	As needed		
Web Browser	Expand an SMB share	Storage Admin L2	As needed		
Web Browser	Shrink an SMB share	Storage Admin L2	As needed		

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Set a share or user level quota	Storage Admin L2	As needed		
Web Browser	Monitor system hardware alerts	Storage Admin L2	Daily		
Web Browser	Monitor pool usage	Storage Admin L2	Weekly		
Web Browser	Monitor host connections	Storage Admin L2	Daily		
Web Browser	Monitor key performance metrics	Storage Admin L2	Daily		
Web Browser	Monitor NAS quota usage	Storage Admin L2	Weekly		
Web Browser	Monitor replication	Storage Admin L2	Daily		
Web Browser	Monitor snapshots	Storage Admin L2	Daily		

Table 38 - Infrastructure Storage SOP Definition

C.9. Backup Storage

0304 Backup Storage SOPs are presented in Table 39, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Reboot the system	Backup Admin L2	As needed		
Web Browser	Power on the system	Backup Admin L2	As needed		
Web Browser	Power off the system	Backup Admin L2	As needed		
AD-DS	Add a new user	Backup Admin L2	As needed		
AD-DS	Delete an existing user	Backup Admin L2	As needed		
Web Browser	Create a user	Backup Admin L2	As needed		
Web Browser	Delete a DD Boost user	Backup Admin L2	As needed		
Web Browser	Manage client access	Backup Admin L2	As needed		
Web Browser	Modify a storage unit	Backup Admin L2	As needed		
Web Browser	Create a storage unit	Backup Admin L2	As needed		
Web Browser	Delete a storage unit	Backup Admin L2	As needed		
Web Browser	Create an interface group	Backup Admin L2	As needed		
Web Browser	Delete an interface group	Backup Admin L2	As needed		
Web Browser	Add a client to an interface group	Backup Admin L2	As needed		
Web Browser	Add a new cloud tier unit	Backup Admin L3	As needed		
Web Browser	Delete a cloud tier unit	Backup Admin L2	As needed		

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Add a cloud tier data movement policy to an Mtree	Backup Admin L3	As needed		
Web Browser	Move data to the cloud manually	Backup Admin L2	As needed		
Web Browser	Move data to the cloud automatically	Backup Admin L2	As needed		
Web Browser	Recall a file from the cloud tier	Backup Admin L2	As needed		
Web Browser	Create a new remote Mtree replication job	Backup Admin L3	As needed		
Web Browser	Delete a remote Mtree replication job	Backup Admin L3	As needed		
Web Browser	Upgrade the system	Backup Admin L3	As needed		
Web Browser	Monitor system hardware alerts	Storage Admin L2	Daily		
Web Browser	Monitor storage usage	Storage Admin L2	Weekly		
Web Browser	Monitor cloud tiering usage	Storage Admin L2	Daily		
Web Browser	Monitor key performance metrics	Storage Admin L2	Daily		
Web Browser	Monitor replication	Storage Admin L2	Daily		

Table 39 - Backup Storage SOP Definition

C.10. Archive Storage

0305 Archive Storage SOPs are presented in Table 40, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
AD-DS	Add a new user	Storage Admin L2	As needed		
AD-DS	Delete an existing user	Storage Admin L2	As needed		
Web Browser	Add a new object user	Storage Admin L2	As needed		
Web Browser	Power on the system	Storage Admin L3	As needed		
Web Browser	Power off the system	Storage Admin L3	As needed		
Web Browser	Create a bucket	Storage Admin L2	As needed		
Web Browser	Edit a bucket	Storage Admin L2	As needed		
Web Browser	Set a bucket ACL	Storage Admin L2	As needed		
Web Browser	Create a VDC	Storage Admin L3	As needed		
Web Browser	Delete a VDC/failover site	Storage Admin L3	As needed		
Web Browser	Create a replication group	Storage Admin L3	As needed		

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Web Browser	Modify a replication group	Storage Admin L3	As needed		
Web Browser	Delete a replication group	Storage Admin L3	As needed		
Web Browser	Create a storage pool	Storage Admin L2	As needed		
Web Browser	Delete a storage pool	Storage Admin L2	As needed		
Web Browser	Monitor system alerts	Storage Admin L2	Daily		
Web Browser	Monitor VDC replication	Storage Admin L2	Daily		
Web Browser	Monitor storage pool usage	Storage Admin L2	Daily		
Web Browser	Monitor traffic metrics	Storage Admin L2	Daily		

Table 40 - Archive Storage SOP Definition

C.11. Backup and Archiving

0306 Backup and Archiving SOPs are presented in Table 41, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
System GUI	Reboot the system	Backup Admin L2	As needed		
System GUI	Power on the system	Backup Admin L2	As needed		
System GUI	Power off the system	Backup Admin L2	As needed		
AD-DS	Add a new user	Backup Admin L2	As needed		
AD-DS	Delete an existing user	Backup Admin L2	As needed		
System GUI	Replace power supply	Backup Admin L2	As needed		
System GUI	Replace cable	Backup Admin L2	As needed		
System GUI	Replace disk drive	Backup Admin L2	As needed		
System GUI	Upgrade Avamar administrator	Backup Admin L2	As needed		
System GUI	Register new client machine	Backup Admin L2	As needed		
System GUI	Move client machine to different domain	Backup Admin L2	As needed		
System GUI	Enable a client machine	Backup Admin L2	As needed		
System GUI	Disable a client machine	Backup Admin L3	As needed		
System GUI	Retire a client machine	Backup Admin L3	As needed		
System GUI	Delete a client machine	Backup Admin L3	As needed		
System GUI	Create an on-demand backup	Backup Admin L2	As needed		

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
System GUI	Create a new backup schedule	Backup Admin L3	As needed		
System GUI	Create new retention policy	Backup Admin L2	As needed		
System GUI	Edit existing retention policy	Backup Admin L2	As needed		
System GUI	Create new backup policy rule (for auto assignment)	Backup Admin L2	As needed		
System GUI	Validate a backup	Backup Admin L2	As needed		
System GUI	Delete a backup	Backup Admin L3	As needed		
System GUI	Restore data from a backup	Backup Admin L2	As needed		
System GUI	Suspend backup jobs	Backup Admin L2	As needed		
System GUI	Resume backup jobs	Backup Admin L2	As needed		
System GUI	Suspend restore jobs	Backup Admin L2	As needed		
System GUI	Resume restore jobs	Backup Admin L2	As needed		
System GUI	Create a system checkpoint	Backup Admin L2	As needed		
System GUI	Perform an on-demand replication	Backup Admin L2	As needed		
System GUI	Schedule a new replication	Backup Admin L2	As needed		
System GUI	Cancel a replication task	Backup Admin L3	As needed		
System GUI	Restore from a replica backup	Backup Admin L2	As needed		
System GUI	Recover a VM using instant access	Backup Admin L2	As needed		
System GUI	Edit cloud tiering policy	Backup Admin L2	As needed		

Table 41 - Backup and Archiving SOP Definition

C.12. Infrastructure CIS Subservice

0307 The SOPs specific to the IaaS Infrastructure CIS subservice have been broken up into the appropriate subservice and addressed herein.

C.13. BPS1

0308 BPS1 SOPs are presented in Table 42, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
ADUC	Add a new administrator	Firewall Administrator	As needed	Active Directory Users and Computers	NATO-ON-SOP-PA-001
ADUC	Remove an administrator	Firewall Administrator	As needed	Active Directory Users and Computers	NATO-ON-SOP-PA-002
Panorama	Add device to panorama	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-003
Panorama	Remove device from panorama	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-004
Panorama	Add device to device group	Tier-2 Firewall Operator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-005
Panorama	Review threat index	Tier-2 Firewall Operator	Daily	Panorama Web GUI	NATO-ON-SOP-PA-006
Panorama	Review connectivity to each firewall	Tier-2 Firewall Operator	Daily	Panorama Web GUI	NATO-ON-SOP-PA-007
Panorama	Create policy template	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-008
Panorama	Apply policy template	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-009
Panorama	Update firewall policy	Tier-2 Firewall Operator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-010
Panorama	Review firewall policy	Firewall Administrator	Monthly	Panorama Web GUI	NATO-ON-SOP-PA-011
Panorama	Modify policy privileges	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-012
Panorama	Upgrade PANOS	Firewall Administrator	As needed	Panorama Web GUI	NATO-ON-SOP-PA-013

Table 42 - BPS1/BPS2 SOP Definition

Annex D OPERATION ROLES AND RESPONSIBILITIES [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

Role	FTE	Education	Experience	Certifications

Table 43 - Specific Roles and Responsibilities

Annex E NATO ON SERVICE PLACEMENT ARCHITECTURE V 1.0

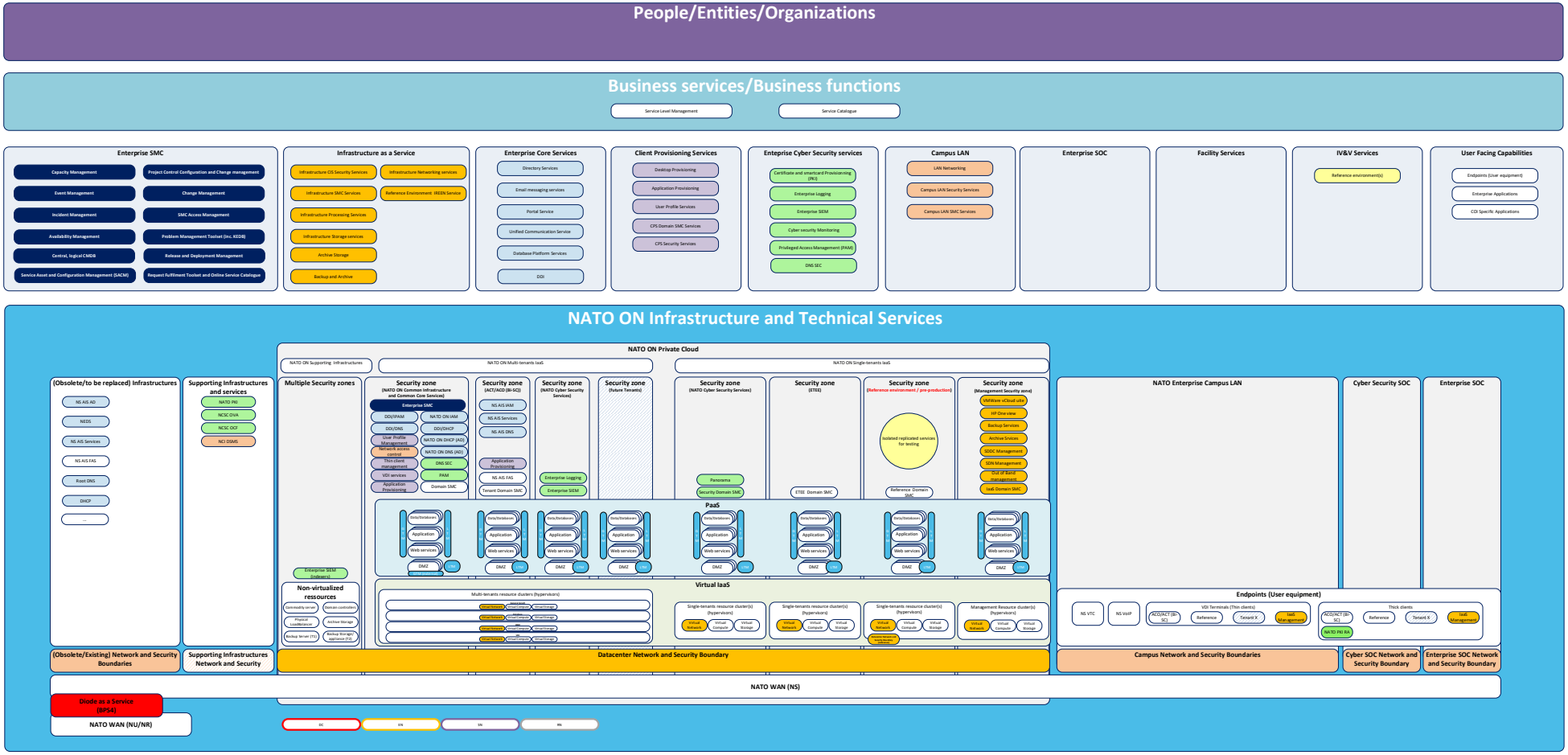


Figure 31 - NATO ON Service Placement Architecture

Annex F NATO ON IaaS Service Placement Architecture v 1.0

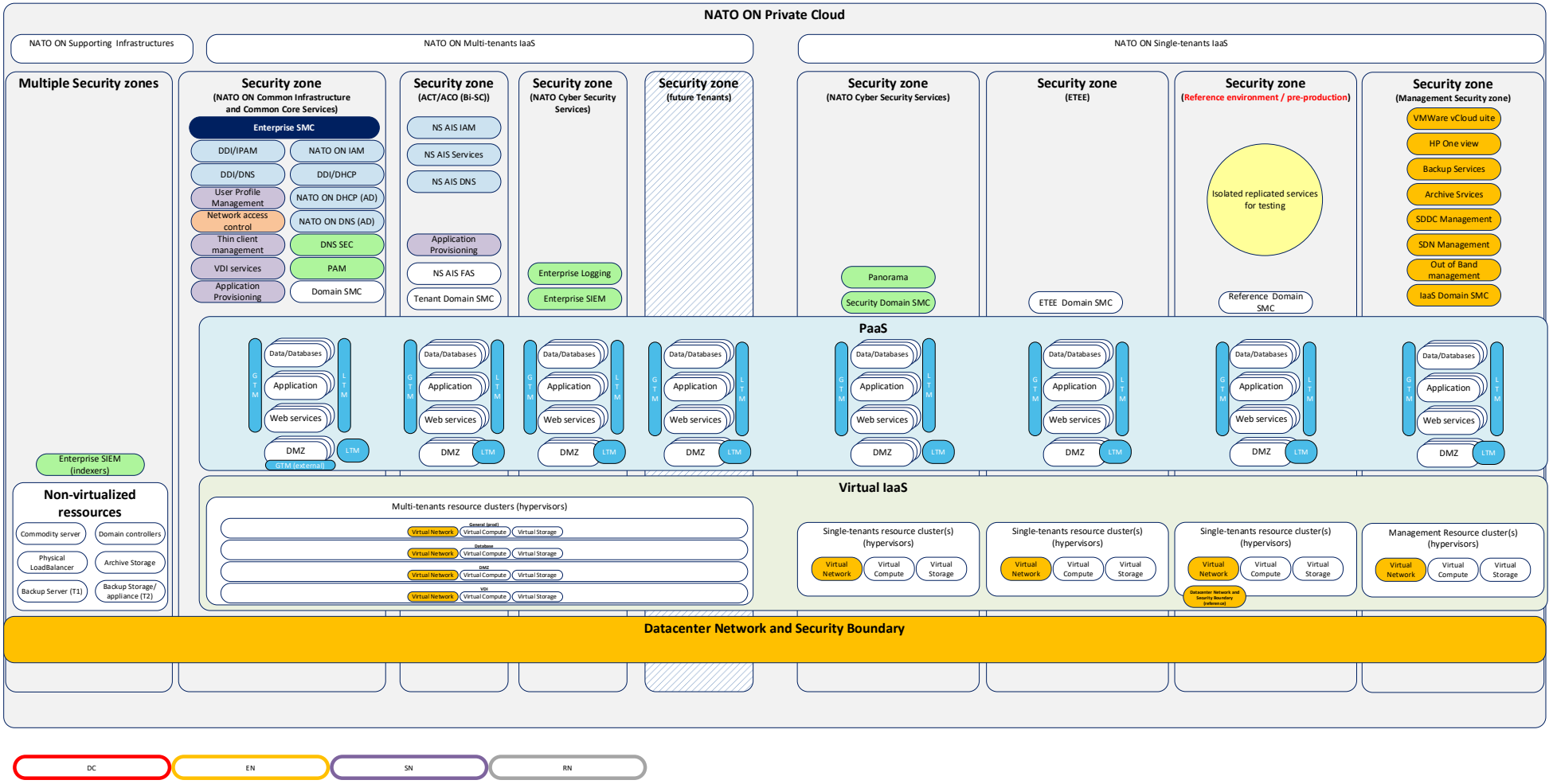


Figure 32 - NATO ON IaaS Service Placement Architecture