

Network and Security infrastructure

Industry Day, Bologna, 16 January 2019

Ahmed Benallegue

Networks and Security Workstream Leader

Bologna January 16, 2019

Agenda

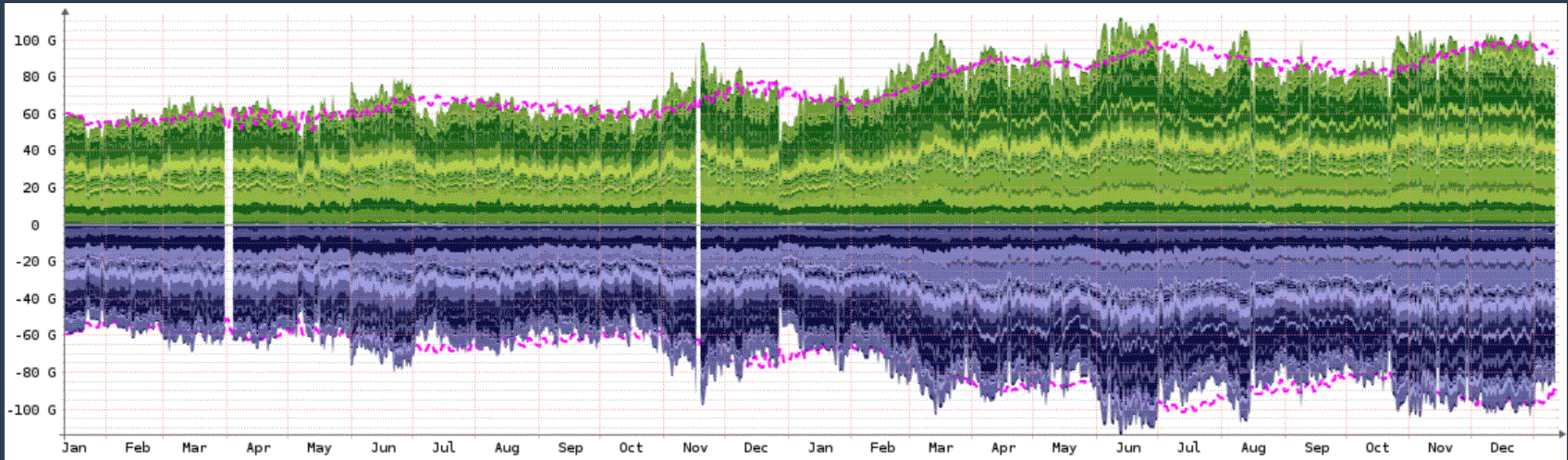
- Introduction
- HLD Overview
- Fabric Layer
- Internet Edge Layer
- Security Layer: Firewall Nodes
- Auxiliary Services: DDI and NTP
- Auxiliary Services: Application Control and Load Sharing
- Procurement approach
- Q&A

Introduction

- The LAN network infrastructure is composed of the following components:
 - **Fabric Layer** (or High Performance Network): used for the exchange of large amounts of operational data, most of which is hosted within our own data centres
 - Architecture: IP Fabric or “Spine-Leaf”
 - **Offices Network**: connects end-user devices such as workstations, telephones and printers, into the High Performance Network
 - Architecture: two-tier collapsed core design
 - 2 networks: Offices Network in Reading and **Offices Network in Bologna**
 - **Management & Monitoring** Network: physically segregated network used to supports the administration and the monitoring of the IT systems operated by ECMWF at all sites
 - Architecture: two-tier collapsed core design

Introduction

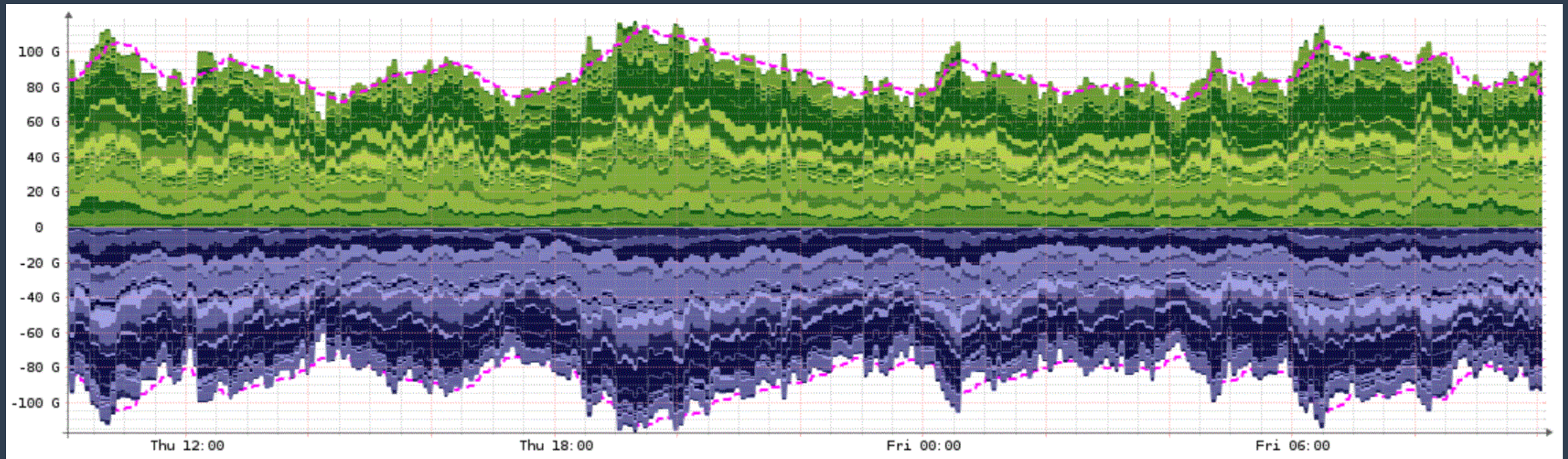
- ECMWF's HPN traffic trend over the last two-year (Jan 2017-Dec)
 - Data traffic increase factor: **1.5** from 240Gbps to 360Gbps
 - Total traffic handled by **one** of the two core switches:



- Expected data traffic increase multiplier factor for period 2017-2023: **3.6** from 240Gbps to 864Gbps

Introduction

- ECMWF's HPN daily traffic trend
 - Peaks at around 6am and 6pm: ECMWF products dissemination
 - Total traffic handled by **one** of the two core switches over a 24h-period, 10-11 January 2019:



Introduction

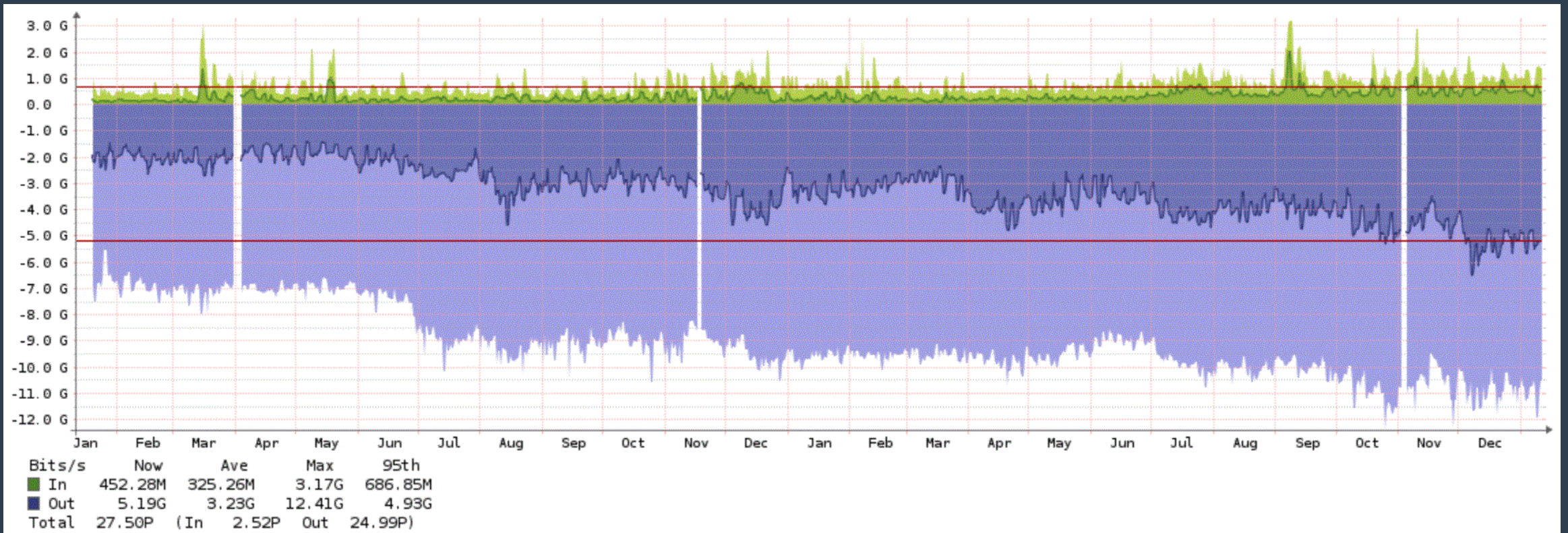
- The WAN aspects
 - ECMWF's Internet connection comprises dual links to JANET in Reading and GARR in Bologna, respectively the United Kingdom's and Italy's National Research and Education Network (NREN)
 - JANET and GARR have high speed connections to the rest of the Internet, especially to the GÉANT network, which provides a high speed backbone between most research networks within Europe and the US
 - ECMWF is also connected to the RMDCN (Regional Meteorological Data Communication Network), a private IPVPN that provides a computer network infrastructure for the meteorological community in World Meteorological Organisation Region VI, and beyond in its capacity as one of the WMO community's Core Networks
- The **Internet Edge Layer**: the component that connects the LAN infrastructure to the WAN

Introduction

- The Internet connections are used for a variety of activities:
 - Exchange of meteorological data between ECMWF's site located in Reading, UK, and ECMWF's Data Centre site located in Bologna, Italy;
 - Dissemination of meteorological data to ECMWF's Member and Cooperating States as per ECMWF's convention;
 - Acquisition of meteorological data from ECMWF's Member and Cooperating States as per ECMWF's convention;
 - Web-browsing and specific VPN services offered by ECMWF to ECMWF staff, contractors and other relevant personnel to provide and maintain ECMWF services;
 - Generic web-browsing services offered by ECMWF to ECMWF staff, contractors and other relevant personnel;
 - Transfer of meteorological data between ECMWF and its partners through various tools provided by ECMWF;
 - Dissemination of meteorological data to other ECMWF partners, including commercial customers.

Introduction

- ECMWF's Internet traffic trend over the last two-year (Jan 2017-Dec)
 - Total traffic going through ECMWF's Internet circuits



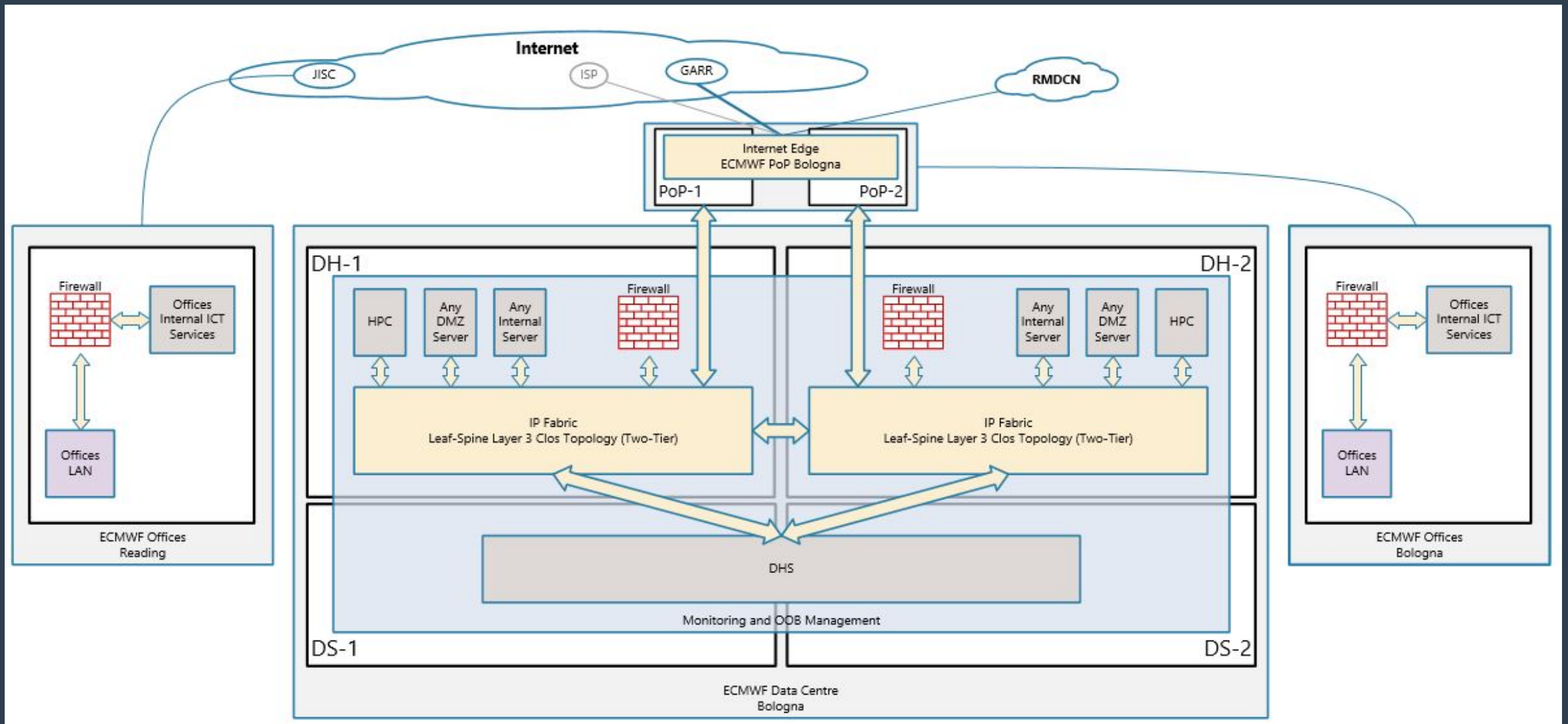
Introduction

- The **Security Layer** protects ECMWF IT systems from internal and external threats
 - Defence in depth approach
 - **Security Layer: Firewall Nodes**
 - Network security layer – NGFW firewall
 - Application-layer firewall
 - VPN
 - NAT
 - Intrusion Protection System (IPS)
 - Management of elephant flows
 - Offices security layer – Offices firewall
 - Unified Threat Management (UTM): Web filtering and application control
 - Management and monitoring of the security layer

Introduction

- The Network and Security infrastructure is also used to provide essential enabling **Auxiliary Services**
 - **Auxiliary Services: DDI and NTP**
 - **Auxiliary Services: Application Control and Load Sharing**
- Operational needs
 - 24/7/365 service availability

HLD – Overview



Fabric Layer

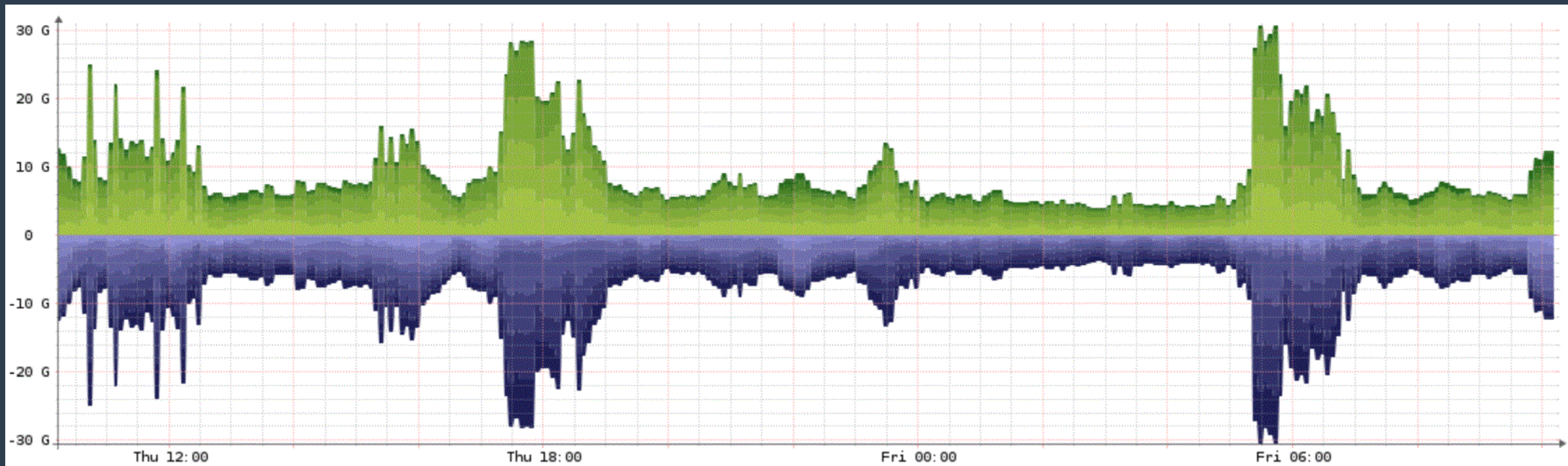
- The network backbone that interconnects the other network components together to provide connectivity to all IT systems
- It will be based on an “IP Fabric” or “Leaf-Spine” architecture
- It will be based on a multi-site topology with two physically segregated networks deployed in the two Data Halls
 - Very high service availability of the resulting infrastructure
 - Highly scalable as it can easily scale and expand to interconnect with other sites
- Connectivity types: 10GbE, 25GbE and 100GbE
- Number of ports – **Very rough figures** based on fully populated racks:
 - Network connectivity: ~300 x 10GbE, ~50 x 25GbE and ~400 x 100GbE
 - Server connectivity: ~1600 x 10GbE/25GbE (mainly 25GbE)

Internet Edge Layer

- Joins the data centre to the WAN through ECMWF's Internet, RMDCN and SIP-based telephony circuits
 - 2x100Gbps Internet circuits provided by GARR
 - 2x1Gbps RMDCN circuits provided by GTT (formerly known as Interoute)
 - Telephony SIP trunks connectivity
- Used to provide the Reading-Bologna site-to-site connectivity

Security Layer: Firewall Nodes

- Monitors and controls the flow of data traffic to protect ECMWF from internal and external threats
- Includes various hardware and software elements to protect the data centre and other network infrastructures such as Offices and M&M networks
- Total traffic handled by the current firewall cluster over a 24h period (13-14 January 2019):



Auxiliary Services

- Provides essential enabling auxiliary services for other IT service providers at ECMWF
 - Auxiliary Services: DDI and NTP
 - DDI: DNS, DHCP and IPAM services
 - NTP services
 - Auxiliary Services: Application Control and Load Sharing
 - Service delivery services
 - Load balancing services

Procurement approach

- Two ITTs for the following component groups

Component Groups
<ul style="list-style-type: none">• Fabric Layer• Internet Edge Layer
<ul style="list-style-type: none">• Offices Network in Bologna• Management & Monitoring

- Three ITTs for the following components

Component
Security Layer: Firewall Nodes
Auxiliary services: DDI and NTP
Auxiliary services: Application Control and Load Sharing

Q&A
Grazie mille!