CINECA

G00328

CAPITOLATO TECNICO

FORNITURA E REALIZZAZIONE RETE E SERVIZI DI SICUREZZA PER I SISTEMI HPC CINECA

CIG 8974369B92

CINECA Consorzio Interuniversitario

C.F. 00317740371 - P. IVA 00502591209

Sede legale amministrativa e operativa:

Via Magnanelli, 6/3 - 40033 Casalecchio di Reno (BO)
Tel. +39 051.6171411 - Fax +39 051.2130217

Altre sedi operative:

Via R. Sanzio, 4 - 20090 Segrate (MI)
Tel. +39 02.269951

Via dei Tizi, 6/B - 00185 Roma
Tel. +39 06.444861

Via F. Imparato, 198 - 80146 Napoli
Tel. +39 081.5593711

INDICE

Art. 1. Generalità contesto HPC e obiettivi progetto Leonardo

L'Italia ha una lunga tradizione nella scienza computazionale e nel calcolo ad alte prestazioni. CINECA fu istituito cinquant'anni fa, con la missione statutaria di un centro nazionale di supercalcolo per supportare l'eccellenza nella scienza e nell'innovazione tecnologica.

Grazie alla visione di lungo termine del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) e al persistente impegno del suo sistema di governance, CINECA ha assunto un ruolo di primo piano a livello mondiale, introducendo sistemi di supercalcolo di livello internazionale classificati nel segmento più alto della TOP500, e in due occasioni nella top ten.

Assieme alle altre istituzioni della Ricerca e dell'Università sul territorio ha contribuito a rendere Bologna uno dei più importanti poli per l'HPC e il Big Data in Europa. Attualmente tutte le principali azioni europee in ambito HPC e Big Data coinvolgono CINECA, come ad esempio le seguenti iniziative: l'Accesso Transnazionale dell'infrastruttura di ricerca HPC, PRACE, ETP4HPC, Human Brain Project e il progetto ICEI FENIX per la Federazione dei sistemi europei di supercalcolo, EOSChub per l'open data infrastructure, HPC Center of Excellence in Material Design, MAX, in solid Earth, Cheese, in Engineering, Excellerat, in IoT e big data processing guidato dall'industria, IoTwins.

La partnership con il datacenter HPTC INFN - CNAF, leader Tier1 in WLCG per l'elaborazione dei dati raccolti dagli esperimenti LHC al CERN, anch'esso a Bologna, ha iniziato l'evoluzione di una iniziativa di sviluppo strategico incentrata sull'espansione/trasferimento di entrambi i centri di calcolo (CINECA e INFN) nel Tecnopolo del Parco Scientifico di Bologna. Questa evoluzione è indirizzata all'adozione di infrastrutture di classe Exascale nel medio termine, e concepita per affrontare i prossimi cicli tecnologici nel dominio del supercalcolo e nuovi campi applicativi emergenti come AI e ML, sicurezza informatica, medicina di precisione, industria 4.0, ambiente e cambiamento climatico.

La visione sinergica e condivisa tra governo nazionale e governo locale, facendo leva sulla concentrazione delle competenze, garantisce la contemporanea presenza a Bologna del CINECA e dell'INFN e la visione di sviluppo di alto profilo elaborata sull'espansione complessiva del Tecnopolo. Questa visione ha anche sostenuto una proposta di successo per ospitare il datacenter ECMWF.
È in questo contesto che CINECA, tramite la nuova infrastruttura presso il Tecnopolo di Bologna, fungerà da "hosting member" di uno dei precursori dei supercomputer di classe Exascale europei, acquisiti dalla "EuroHPC Joint Undertaking". Iniziativa questa basata da un lato sul sostegno politico, economico e istituzionale del MIUR, e dall'altro, sulla collaborazione scientifica a lungo termine con l'INFN e la SISSA.
La nuova infrastruttura che ospiterà il sistema pre-exascale dell'iniziativa EuroHPC, progetto "Leonardo", sarà quindi dislocata in uno degli edifici del "Tecnopolo di Bologna", di proprietà al 100% della Regione Emilia-Romagna, insediamento industriale esistente (100.000 mq) in fase di adeguamento nell'ambito di un masterplan cittadino che destina l'area per le attività di ricerca. L'area per il Centro di calcolo dedicata a "Leonardo" comprende 890 mq di sala macchine principale, 350 mq di magazzini, impianti elettrici e di raffreddamento e ventilazione, uffici e spazi ausiliari, ed è progettata

per un'estrema efficienza energetica, con un PUE inferiore a 1,1. L'impiantistica elettromeccanica per 20 MW IT ma, nella prima fase di esercizio sarà dotata di un'infrastruttura capace di 10 MW IT. Come programmato dalla roadmap nazionale, in una successiva fase di esercizio, il sito è quindi in grado di ospitare un sistema full Exascale a seguito di un upgrade delle infrastrutture di distribuzione elettrica e di raffreddamento per adeguarsi ai 20 MW IT.

È nel quadro complessivo precedentemente delineato che si colloca la fornitura oggetto della presente gara, per dotare il nuovo centro di calcolo CINECA presso il Tecnopolo di Bologna di tutti gli apparati necessari a fornire la connettività generale e sicurezza verso la rete internet, le reti della ricerca mondiale e l'integrazione con gli apparati di rete esistenti presso il centro di calcolo CINECA in Casalecchio di Reno, questi ultimi per i servizi generali e di salvataggio dati.

È di fondamentale importanza, per la buona risuscita del progetto, considerare che la fornitura in oggetto costituirà il tramite verso cui il nuovo sistema di calcolo "tra i primi in Europa" sarà acceduto dalle istituzioni di ricerca italiane, europee e mondiali.

Poiché le infrastrutture di supercalcolo sono riconosciute sia a livello nazionale che a livello europeo come infrastrutture strategiche, la loro sicurezza informatica è pertanto posta al centro dell'attenzione; per questo, oltre che alla sicurezza della nuova infrastruttura che verrà realizzata presso il Tecnopolo di Bologna, questa fornitura vuole indirizzare anche la sicurezza dell'infrastruttura di supercalcolo tutt'ora in essere presso la sede di Casalecchio di Reno.

Art. 2. Sedi CINECA destinazioni della fornitura

Gli apparati oggetto della fornitura sono da destinarsi:

- alla sede CINECA presso Casalecchio di Reno in via Magnanelli 6/3(di seguito semplicemente indicata sede CINECA di Casalecchio di Reno)
- alla sede CINECA presso Bologna in via Stalingrado s.n.c. (senza numero civico) - Tecnopolo Bologna (di seguito semplicemente indicata sede CINECA Tecnopolo)

Art. 3. Oggetto della Fornitura

3.1 Fornitura richiesta

Oggetto del presente contratto è la fornitura di:

- Apparati firewall per la sede CINECA Casalecchio di Reno (in seguito abbreviati FWCx) da collegare agli apparati di frontiera già presenti (Juniper MX204) a protezione del perimetro; la fornitura dovrà includere tutte le componenti necessarie anche per gli apparati CINECA (cavi, componenti ottiche, licenze, etc.)
- Apparati firewall per la sede CINECA Tecnopolo (in seguito abbreviati FWTx) da collegare agli apparati di rete oggetto della fornitura inclusivi di tutte le componenti necessarie (ottiche, cavi, licenze, etc.)

- Apparati di rete per la sede CINECA Tecnopolo (in seguito abbreviati RTx e SWTx) necessari per garantire al supercalcolatore "Leonardo" la connettività locale, verso internet e verso le reti della ricerca afferenti a GÉANT e per realizzare l'interconnessione tra i datacenter CINECA di Casalecchio di Reno e CINECA Tecnopolo.
- Switch ethernet per la sede CINECA Tecnopolo (in seguito SWT-Sx) per il collegamento delle postazioni di lavoro (PDL), degli Access Point e di quanto necessario per realizzare la rete di Management per la gestione e l'accesso agli apparati oggetto della fornitura
- Access Point (APx) inclusivi di tutte le componenti necessarie (es. controller) per la realizzazione di un servizio di accesso WiFi con gestione centralizzata delle configurazioni che consenta di accedere a internet e all'infrastruttura di management per la sede di CINECA Tecnopolo
- Redazione ed implementazione del progetto tecnico ed esecutivo per la soluzione architetturale proposta dalla ditta concorrente
- Tutte le componenti hardware/software necessarie per la realizzazione dell'architettura proposta e del relativo cablaggio (es. rack, patch panel, cavi in fibra ottica, cavi UTP, cavi DAC cavi, cavetteria di vario tipo, componenti ottiche, licenze software, etc.)
- servizi professionali per installazione e implementazione del progetto
- servizi professionali di supporto post-implementazione
- servizio di formazione del personale;
- servizi di manutenzione e assistenza per 60 mesi per tutte le risorse HW e SW incluse nella fornitura.

3.2 Definizione e acronimi

Per agevolare la lettura del documento viene di seguito riportato il glossario dei termini più frequentemente utilizzati:

Committente: CINECA;

Esecutore: operatore economico affidatario;

FC: fibre channel;

iSCSI: internet Small Computer Systems Interface;

Gbit/s, Gb/s: Gigabit per secondo;

Mbit/s, Mb/s: Megabit per secondo

VRF (Virtual Routing and Forwarding): tecnologia che consente di definire istanze di routing table distinte sugli apparati di rete

VRF Leaking: funzionalità software che consente lo scambio controllato di informazioni di routing tra le varie tabelle di routing associate alle VRF

LACP (Link Aggregation Control Protocol): protocollo di aggregazione di più porte fisiche in un singolo canale logico definito nello standard IEEE 802.3ad e successivamente 802.1ax-2008;

MLAG (Multi Chassis Link Aggregation Group): protocollo che consente di realizzare aggregazioni di porte fisiche (LACP) attestate su switch differenti;

ESI (Ethernet Segment Identifier) LAG: evoluzione standard della funzionalità di MLAG

FHRP (First Hop Redundancy Protocol): protocollo per la gestione HA di un gruppo di router attraverso la selezione automatica di un master router (virtual router).
VRRP (**Virtual Router Redundancy Protocol**): implementazione standard del FHRP
HSRP (**Hot Standby Routing Protocol**): implementazione Cisco proprietaria del FHRP
OSPF (**Open Shortest Path First**): protocollo di routing dinamico interno utilizzato per garantire la propagazione dinamica delle reti IP e la riconvergenza su percorsi alternativi in caso di guasto di apparati o di collegamenti di rete;
uRPF (Unicast Reverse Path Forwarding): funzionalità di sicurezza normalmente utilizzata per implementare la protezione anti-spoofing consentendo agli apparati di rete di bloccare il traffico proveniente da indirizzi IP sorgenti che gli apparati raggiungerebbero utilizzando una interfaccia differente da quella da cui i pacchetti sono stati ricevuti.
MP-BGP (**Multiprotocol BGP**): estensione del protocollo BGP (RFC 4760) che consente il trasporto di informazioni di routing dei protocolli IPv4, IPv6, Multicast e la configurazione di MPLS L3 VPN
NBD (**Next Business Day**): fornitura delle parti sostitutive entro il giorno lavorativo successivo alla richiesta;
HA (**High availability**): insieme di tecnologie volte a garantire la massima continuità e disponibilità dei servizi erogati
PDL: Postazione di lavoro portatile o fissa
GÉANT: GÉANT pan-European network – https://www.geant.org
DEISA:Distributed_European_Infrastructure_for_Supercomputing_Applications-https://en.wikipedia.org/wiki/Distributed_European_Infrastructure_for_Supercomputing_Applications. Nel seguito l'acronimo sarà utilizzato per indicare reti della ricerca in uso per follow up del progetto
PRACE: Partnership for Advanced Computing in Europe - https://prace-ri.eu/. Iniziativa europea in ambito HPC
GARR: Consortium GARR – fornitore di connettività per enti di ricerca, scuole e universtià italiane - https://www.garr.it
OMN (Operational Management Nodes): server per la gestione del cluster del supercalcolatore Leonardo
FEN (Frontend Nodes): server di frontend per l'accesso ai servizi offerti dal supercalcolatore Leonardo
SG (Skyway Gateways): gateways tra reti infiniband e reti ethernet
DAC: Direct Attach Copper – cavo di interconnessione ad alte prestazioni con trasceiver integrati
IDC: Inter Datacentre Connection – collegamenti di interconnessione tra datacenter

Art. 4. Caratteristiche tecniche della fornitura

4.1 Architettura di rete CINECA Casalecchio di Reno esistente

Architettura di rete generale

L'architettura di rete CINECA presso la sede di Casalecchio di Reno a supporto delle aree operative HPC e ICT si basa su un classico modello gerarchico che prevede i livelli di internet border, core, distribution e access (vedi Figura 1).
Il livello di internet border è costituito da apparati collocati sul "bordo" che garantiscono la connettività verso la rete internet e le reti della ricerca con una banda aggregata di 20Gb/s verso GARR (accesso istituzionale) e 400Mb/s verso Fastweb. Gli internet border router, n.2 Juniper MX204 (I03 e I04 in figura), utilizzano sessioni external BGP verso GARR e Fastweb per annunciare le reti pubbliche di CINECA e per ricevere le informazioni di routing esterno dai provider. Inoltre sono configurati tra loro e con gli internet border router della sede CINECA di Roma con sessioni internal BGP per realizzare scenari di tipo active-backup: in caso di guasto del router primario di accesso alla rete internet istituzionale via GARR (I03) o dei suoi collegamenti di rete, il traffico viene automaticamente re-instradato su router secondario (I04) e utilizza i link di backup; in caso di guasto del router primario di accesso alla rete internet commerciale via Fastweb, il traffico viene re-instradato sui border router della sede CINECA di Roma e inoltrato su internet tramite Retelit, l'Internet Service Provider utilizzato per l'accesso alla rete internet commerciale dalla rete di Roma. Infine, per garantire la corretta separazione tra gli ambienti istituzionale e commerciale e per sfruttare al massimo le capacità dell'hardware, gli internet border, come anche tutti gli altri apparati di rete che svolgono funzioni di livello 3, sono configurati per utilizzare processi di routing distinti all'interno di istanze di routing separate (VRF). In questo modo gli internet border router realizzano i seguenti scenari per l'instradamento del traffico degli apparati del sottostante livello core:

- Per l'ambito istituzionale ridistribuiscono, nel protocollo OSPF verso il livello core, la default route ricevuta via BGP dal GARR con pesi distinti, per garantire che, in condizioni di normale funzionamento, il default gateway per gli apparati di switching del livello core sia il router I03
- Per l'ambito commerciale originano, nel protocollo OSPF verso il livello core, una default route con pesi distinti, per garantire che, in condizioni di normale funzionamento il default gateway per gli apparati di switching del livello core sia il router I04

Dopo il livello di internet border, troviamo (vedi Figura 1) il livello di core che è costituito da n.2 apparati Extreme Networks BD-X8 (C03 e C04) che realizzano l'aggregazione degli apparati di distribuzione verso le aree HPC, tramite n.2 apparati Mellanox MSN2700 (D19/D20) e ICT, tramite n.2 apparati Cisco Nexus 9504 (D11/D12).

A completamento della descrizione sommaria dell'architettura di rete generale di CINECA presentata è importante riportare che:

- le funzionalità di livello 3 sono distribuite sugli apparati di rete dei livelli border, core, e distribution all'interno dei quali, come già anticipato, sono configurate istanze di routing distinte per ogni VRF (protocolli OSPF e BGP);
- le funzionalità di livello 2 sono invece utilizzate nei livelli border, core e distribution per il tagging delle VLAN 802.1q (utilizzate per realizzare i collegamenti punto-punto L3 delle VRF sui collegamenti fisici) e dagli apparati del livello di access per il collegamento dei server.

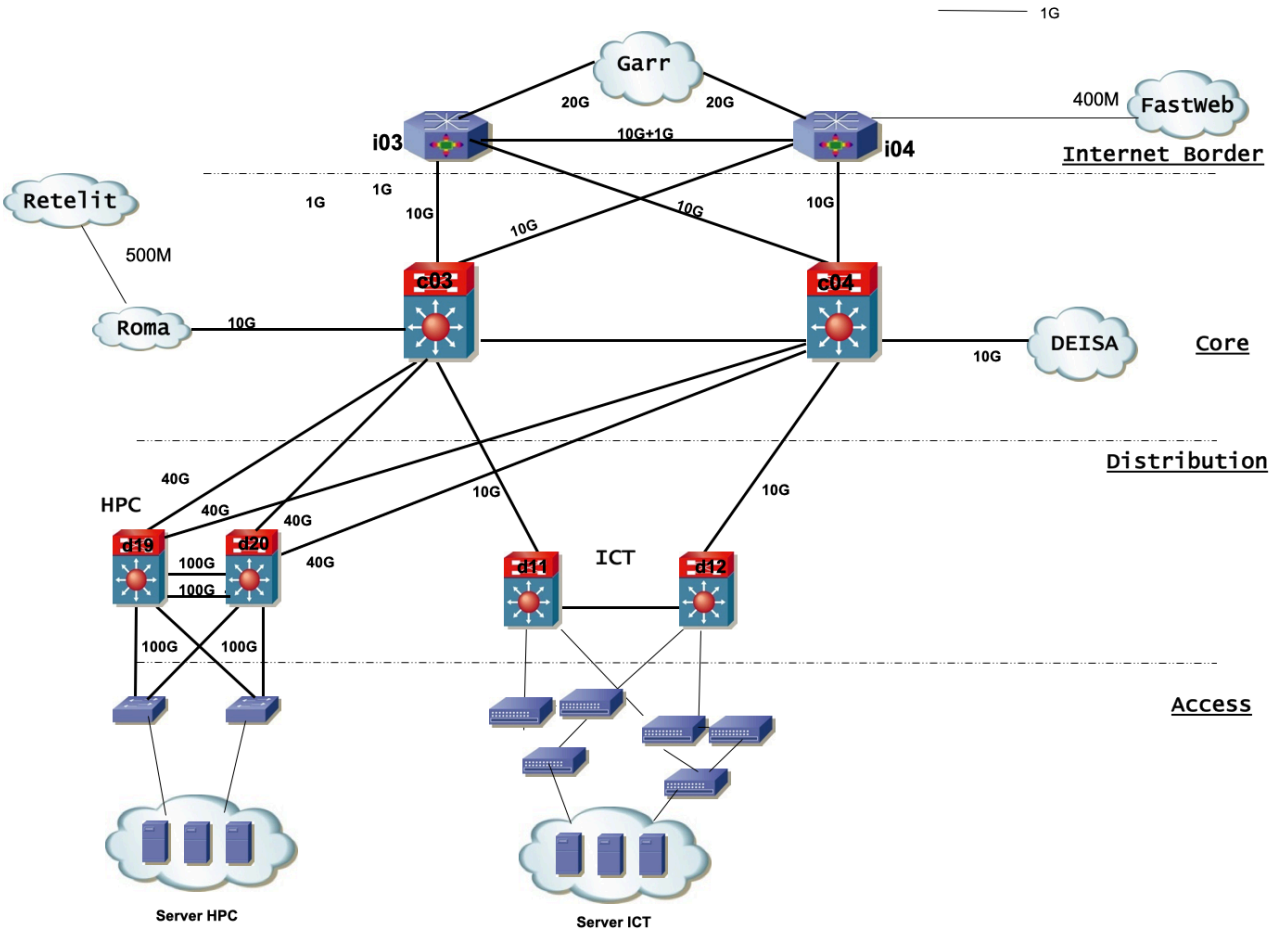

Figura 1: Architettura di rete generale CINECA

Architettura di rete HPC

In Figura 2 e in Figura 3 sono riportati gli schemi di dettaglio dell'architettura di rete dei servizi dell'area HPC i cui punti principali sono riportati di seguito:

- L'interconnessione degli apparati di livello distribution (D19/D20) con il livello core (C03/C04) è realizzata mediante n.4 link ethernet da 40Gb/s ciascuno configurati come link punto-punto di livello 3 su cui è attivo il protocollo di routing OSPF per garantire il routing corretto e la necessaria riconvergenza in caso di guasti di link o di parte degli apparati coinvolti
- Gli apparati di distribuzione D19 e D20:
  - sono configurati tra loro in modalità MLAG
  - sono connessi a tutti gli apparati del livello di access tramite link a 100Gb/s
  - svolgono il ruolo di gateway L3 per le VLAN implementate nel livello access
  - sono configurati per implementare policy di filtraggio IP (ACL) tra le VLAN utilizzate nel livello access
  - gestiscono due VRF distinte, la VRF "Academic" utilizzata per la connettività dei sistemi istituzionali e la VRF DEISA (vedi Figura 3) utilizzata per consentire la connettività diretta di determinati sistemi HPC verso alcune reti GÉANT (centri di ricerca afferenti ora afferenti al progetto PRACE / EuroHPC) tramite un link fisico dedicato fornito dal GARR e attestato fisicamente su uno dei due core switch (C04).
  - ricevono dai core switch la default route via OSPF in VRF "Academic" e le reti IP DEISA in VRF "DEISA" (vedi Figura 3), tramite un processo di ridistribuzione di BGP in OSPF realizzato dal core switch C04. I sistemi HPC finali sono poi configurati per utilizzare come "default gateway" gli indirizzi IP di D19/D20 in VRF "Academic" e come "gateway" per raggiungere le reti di ricerca DEISA, gli indirizzi IP di D19/D20 in VRF DEISA. Questo scenario di routing, che prevede l'utilizzo di blocchi di indirizzamento IP distinti associati alle VRF e annunciati separatamente via BGP verso la general internet e verso la rete GÉANT, sarà lo stesso richiesto anche per i sistemi HPC che installati presso il tecnopolo (vedi 4.2.2)
- Gli apparati di accesso:
  - svolgono unicamente funzioni di livello 2 e sono connessi verso gli altri apparati (di accesso o di distribuzione) tramite link multipli aggregati da 100Gb/s o 10gb/s in MLAG (vedi link in viola o link in nero in Figura 2)
  - forniscono l'accesso alla rete ai sistemi HPC, più in generale a quegli host e/o reti interne dei cluster, che necessitano di I/O esterno.

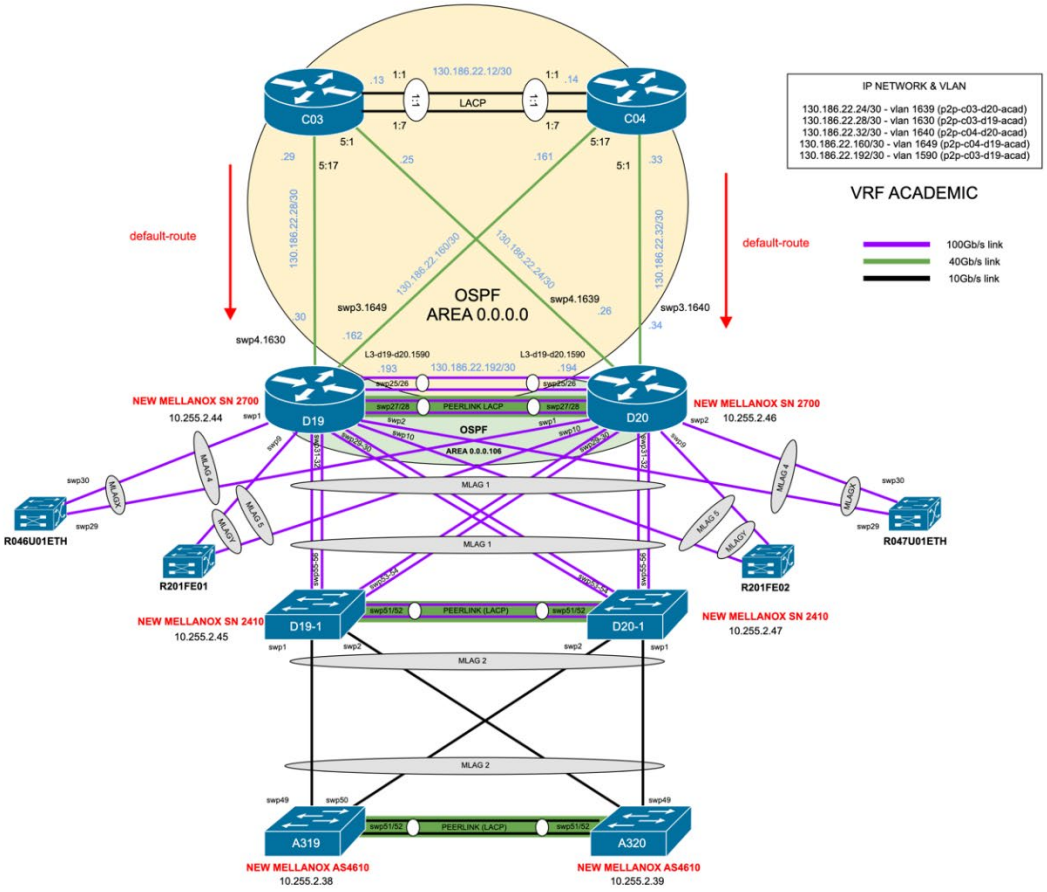

Figura 2: Architettura di rete HPC

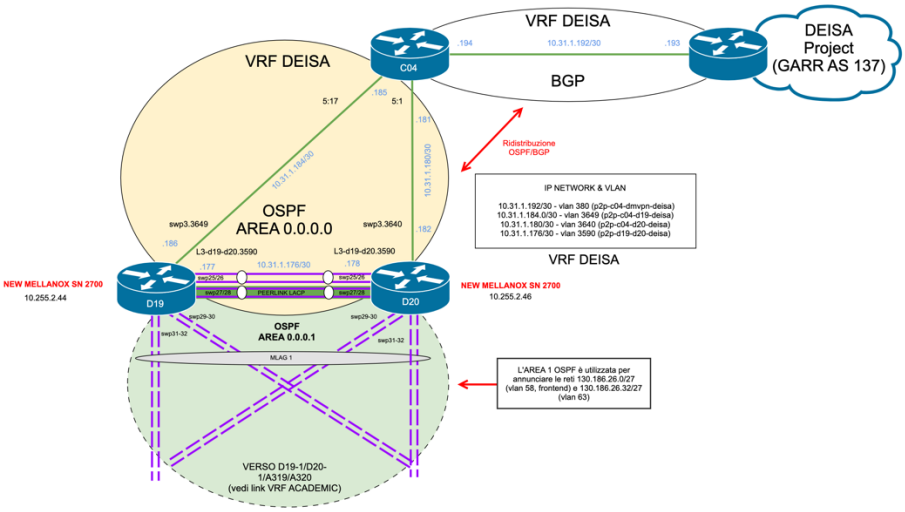

Figura 3: Architettura HPC - progetto DEISA

4.2 Disegno di architettura di rete

Scopo di questo paragrafo è descrivere l'ipotesi di architettura che per CINECA dovrebbe consentire il raggiungimento degli obiettivi generali di progetto. È importante sottolineare che l'architettura proposta costituisce una architettura di alto livello che dovrà quindi essere sviluppata e dettagliata dalla ditta concorrente in ciascuna delle componenti descritte e che dovrà tenere conto degli obiettivi e dei requisiti funzionali e tecnologici riportati nel presente documento. La ditta concorrente dovrà pertanto produrre il progetto tecnico di dettaglio e occuparsi dell'implementazione della soluzione proposta compatibilmente con i tempi e le modalità descritte all'interno del progetto esecutivo.

In Figura 4 è stata riportata l'architettura di rete di alto livello disegnata da CINECA in cui con il nome in rosso sono stati evidenziati gli apparati oggetto della fornitura, i cui requisiti minimi funzionali e tecnologici sono stati specificati nel paragrafo 4.3 Requisiti tecnici minimi della fornitura

La descrizione dell'architettura ipotizzata è stata suddivisa nei seguenti sotto paragrafi:

- 4.2.1 Architettura rete di produzione - CINECA Casalecchio
- 4.2.2 Architettura rete di produzione - CINECA Tecnopolo
- 4.2.3 Architettura rete servizi - CINECA Tecnopolo
- 4.2.4 Architettura interconnessione - CINECA Casalecchio di Reno - Tecnopolo

all'interno dei quali oltre alla descrizione dell'architettura sono stati esplicitati anche gli obiettivi che si intende realizzare con il presente progetto

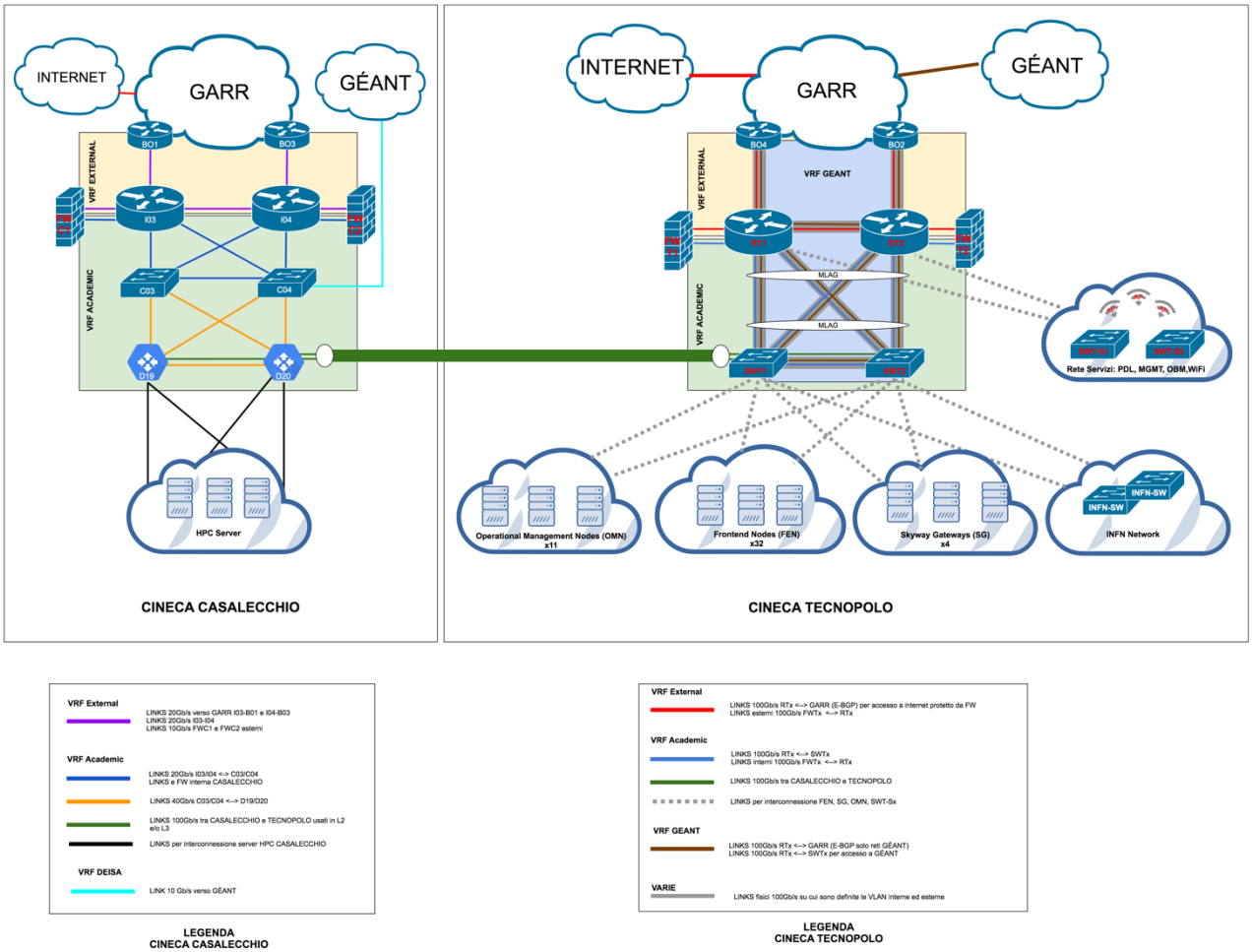

Figura 4: Architettura CINECA Casalecchio-Tecnopolo

4.2.1 Architettura rete di produzione - CINECA Casalecchio di Reno

Obiettivi

- introduzione nell'infrastruttura esistente di apparati di firewalling (FWCx) configurati in alta affidabilità in grado di analizzare e proteggere il traffico in ingresso/uscita dal datacenter
- opportuna riconfigurazione del routing degli apparati in esercizio per il corretto instradamento del traffico in ingresso/uscita dal datacenter verso/dagli apparati di firewalling

Descrizione architettura

Per evitare di dover cambiare radicalmente le configurazioni di routing degli apparati pre-esistenti (core switch "Extreme Networks BDX8" C03/C04 e border router "Juniper MX204" I03/I04) e semplificare l'attività di introduzione dei nuovi apparati, i firewall FWCx dovranno essere collegati direttamente ai router Juniper MX204 (I03/I04). Sarà quindi necessario configurare sui router una nuova istanza di routing , VRF "External" in Figura 4, per il corretto instradamento del traffico da e verso i Firewall perimetrali

Nello specifico nella VRF "External" saranno configurate (vedi collegamenti in viola in Figura 4):

- le interfacce dei router CINECA utilizzate per i peering E-BGP con i router GARR (20Gb/s aggregati su due link fisici per ciascun router)
- le interfacce utilizzate per il peering I-BGP tra i router CINECA (20Gb/s aggregati su due link fisici per ciascun router)
- le interfacce dei router CINECA da collegare alle interfacce "esterne" dei firewall oggetto della fornitura (vedi 4.3.2.1 Requisiti minimi rete di produzione - CINECA Casalecchio e 4.3.3 Requisiti minimi dei Firewall)

mentre nella VRF "Academic" oltre alle interfacce già presenti andranno configurate le interfacce dei router CINECA da collegare alle interfacce "interne" dei firewall oggetto della fornitura.

La ditta concorrente dovrà meglio specificare all'interno del progetto tecnico:

- le modalità di realizzazione del routing inter-VRF e del routing interno insieme allo scenario di configurazione dei Firewall in alta affidabilità ritenuto più adeguato (es. active-standby, active-active, ecc. vedi anche 4.3.3 Requisiti minimi dei Firewall).
- quante e quali interfacce fisiche intende utilizzate per i collegamenti tra firewall FWCx e router Juniper MX204. Tra le opzioni possibili, che andranno comunque opportunamente giustificate nella descrizione dell'offerta tecnica, la ditta concorrente avrà la possibilità di utilizzare interfacce 40Gb/s o interfacce 10Gb/s da utilizzare eventualmente in modalità aggregata (vedi anche 4.3.2.1 Requisiti minimi rete di produzione - CINECA Casalecchio)

4.2.2 Architettura rete di produzione - CINECA Tecnopolo

Obiettivi

- introduzione di apparati di firewalling (FWTx) configurati in alta affidabilità in grado di ispezionare e proteggere il traffico in ingresso/uscita dal datacenter
- introduzione e configurazione di apparati di routing (RTx) per garantire
    - l'interconnessione al GARR via BGP, per accesso alle reti della ricerca italiane, a internet, e alle reti della ricerca afferenti a GÉANT
    - il collegamento degli apparati di firewalling (FWTx)
    - il collegamento degli apparati Gateway[1] (SWTx)

[1] Gli apparati SWTx dovranno poter svolgere sia funzionalità di livello 2 che di livello 3 (vedi 4.3.2.2 Requisiti minimi rete di produzione - sede CINECA Tecnopolo)

  - il collegamento degli apparati di rete SWT-Sx a supporto della rete servizi (vedi anche 4.2.3 Architettura rete servizi - CINECA Tecnopolo)
  - l'opportuna riconvergenza del routing interno (verso gli SWTx) ed esterno (verso GARR) in caso di guasti hardware degli apparati o dei collegamenti di rete
  - l'eventuale bypass del firewall per il traffico destinato o originato a/da reti della ricerca afferenti a GÉANT
- introduzione e configurazione di apparati Gateway[1] (SWTx) per garantire (vedi Figura 4)
  - il collegamento dei FEN
  - il collegamento dei SG
  - il collegamento dei OMN
  - il collegamento dei link geografici di interconnessione verso il datacenter CINECA di Casalecchio di Reno (vedi anche 4.2.4 Architettura interconnessione - CINECA Casalecchio di Reno - Tecnopolo)
  - il collegamento verso gli apparati di routing (RTx) per consentire l'accesso dai/ai sistemi presso il datacenter tecnopolo alle/dalle reti internet e GÉANT
  - opportuna riconvergenza del routing interno (verso gli RTx) in caso di guasti hardware degli apparati o dei collegamenti di rete

Descrizione architettura

L'ipotesi è di replicare il modello architetturale simile a quello presente del datacenter CINECA di Casalecchio di Reno dimensionando e configurando opportunamente i collegamenti e gli apparati di rete per supportare flussi di traffico con banda complessiva pari almeno a 200Gb/s verso GARR (ovvero verso reti general internet e reti GÉANT). In questo caso però, si richiede anche di predisporre l'infrastruttura per poter eseguire, in caso di necessità futura, il bypass dei firewall perimetrali per il raggiungimento delle sole reti della ricerca afferenti a GÉANT. L'architettura dovrà pertanto consentire i seguenti scenari:

- instradamento di flussi di traffico soggetti alla protezione dei firewall perimetrali, originati da sistemi configurati con indirizzi IP all'interno di un prefisso IPv4 specifico, CINECA IPv4 Prefix 1, e destinati a internet, alle reti della ricerca afferenti a GARR e alle reti della ricerca afferenti a GÉANT. I prefissi IPv4 saranno forniti da CINECA in fase di configurazione.
- instradamento di flussi di traffico NON soggetti alla protezione dai firewall perimetrali (firewall bypass), originati da sistemi configurati con indirizzi IP all'interno di un prefisso IPv4 specifico, CINECA IPv4 Prefix 2, e destinati esclusivamente alle reti della ricerca afferenti a GÉANT. I prefissi IPv4 saranno forniti da CINECA in fase di configurazione.

Gli apparati del livello border (RTx) dovranno pertanto essere configurati, ciascuno, con (almeno) due sessioni E-BGP con il GARR, la prima configurata in VRF "External" su cui annunceranno il prefisso CINECA IPv4 Prefix1 e da cui riceveranno la default route (vedi link in rosso RTx-BOx in Figura 7), la seconda configurata in VRF "GÉANT" su cui annunceranno il prefisso CINECA IPv4 Prefix2 e da cui riceveranno le sole reti afferenti a GÉANT (vedi link in colore marrone RTx-BOx in Figura 7). Il traffico diretto/originato al/dal datacenter Tecnopolo dovrà essere bilanciato sui due link a 100Gb/s verso il GARR e, tra i router RTx dovranno essere configurate le necessarie sessioni I-BGP (in VRF "External" e in VRF "GÉANT") per garantire, in caso di guasto di uno dei due link di

accesso al GARR o degli apparati su cui il link è terminato, la riconvergenza automatica del traffico sul restante link attivo.

Per semplificare l'architettura rispetto al datacenter di Casalecchio, il collegamento tra il livello border (RTx) e il sottostante livello core (SWTx) si ipotizza di utilizzare almeno n.4 link ciascuno a 100Gb/s configurati in MLAG per definire un unico aggregato logico da 400Gb/s. L'ipotesi è di attivare processi di routing dinamici su base VRF (OSPF) per realizzare gli scenari sopra citati come meglio illustrato nelle figure seguenti

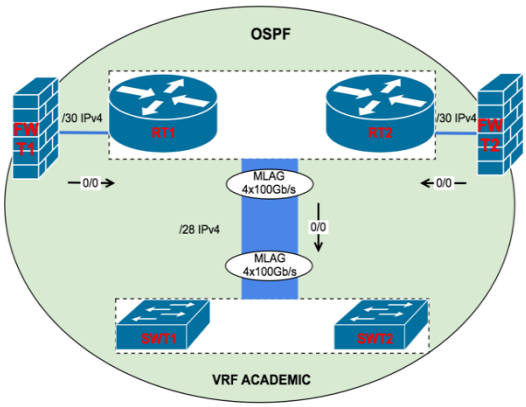

Figura 5: Schema logico routing interno VRF ACADEMIC

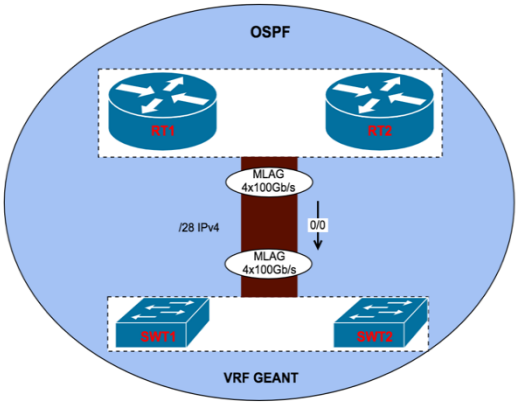

Figura 6: Schema logico routing interno VRF GÉANT

In particolare la Figura 5 descrive l'ipotetico routing per i sistemi soggetti alla protezione del firewall perimetrale. In questo caso la default route viene distribuita internamente fino al livello di core (via OSPF e/o routing statico) utilizzando una VLAN dedicata trasportata sull'aggregato MLAG tra RTx e SWTx e associata ad una rete IP /28. Tale rete sarà inserita in VRF "ACADEMIC" e utilizzata dagli apparati di rete RTx, SWTx e FWTx per poter stabilire le adiacenze OSPF. In questo modo il traffico in uscita degli host soggetti alla protezione perimetrale (configurati con IP inclusi nel prefisso CINECA IPv4 "Prefix1") sarà instradato in VRF "ACADEMIC" verso i firewall i quali, dopo aver eseguito le opportune operazioni di analisi e filtraggio, lo instraderanno verso le interfacce dei router RTx configurate in VRF "EXTERNAL". I router RTx a loro volta instraderanno il traffico sulla prima sessione BGP (vedi collegamento in rosso RTx-BOx in Figura 7); il traffico di ritorno seguirà il percorso inverso.

La Figura 6 descrive invece l'ipotetico routing per i sistemi NON soggetti alla protezione perimetrale. In questo caso la default route viene distribuita internamente fino al livello di core (via OSPF e/o routing statico) utilizzando una VLAN dedicata trasportata sull'aggregato MLAG tra RTx e SWTx e associata ad una subnet IP /28. Tale rete sarà inserita in VRF "GÉANT" e utilizzata dagli apparati di rete RTx, SWTx e FWTx per poter stabilire le adiacenze OSPF. In questo modo il traffico in uscita degli host NON soggetti alla protezione perimetrale (configurati con IP appartenenti al range incluso nel prefisso CINECA IPv4 "Prefix2") sarà instradato in VRF "GÉANT" fino ai router RTx che a loro

volta lo instraderanno sulla seconda sessione BGP (vedi collegamento in marrone RTx-BOx in Figura 7); il traffico di ritorno seguirà il percorso inverso.

Per quanto riguarda il secondo scenario (vedi Figura 6) è importante sottolineare che la maggior parte dei centri di ricerca raggiungono normalmente la general internet e le altre reti della ricerca utilizzando un unico accesso condiviso, ovvero utilizzando un unico peering BGP con il provider (GARR per l'Italia) per instradare entrambi i flussi di traffico (verso le reti general internet e verso le reti della ricerca). Per questo motivo il GARR, non potendo utilizzare VRF distinte per separare i due contesti, non potrà evitare di inoltrare il traffico proveniente dalla general internet anche sul collegamento dedicato per il raggiungimento delle sole reti afferenti a GÉANT (vedi collegamento in colore marrone in Figura 7). Quel traffico dovrà pertanto essere bloccato dagli apparati RTx ad esempio con ACL o con l'attivazione della funzionalità di Unicast Reverse Path Forwarding (uRPF). Si ricorda infatti che il GARR annuncerà su quel peering le sole reti della ricerca GÉANT.

Per concludere in Figura 7 è rappresentata la modalità con la quale un host di frontend (FEN), in caso di necessità potrà utilizzare entrambe le connessioni, quella protetta da firewall per l'accesso alla rete internet e alle reti della ricerca afferenti al GARR, e quella non protetta da firewall per raggiungere le reti della ricerca afferenti a GÉANT. In questo caso il server dovrà disporre di due interfacce di rete fisiche o logiche (es. interfacce VLAN sulla stessa interfaccia fisica), la prima configurata con un indirizzo IP del range CINECA IPv4 "Prefix1", e la seconda configurata con indirizzo IP del range CINECA IPv4 "Prefix2". Le interfacce saranno connesse agli apparati SWTx, la prima in VRF "ACADEMIC" e la seconda in VRF "GÉANT". Infine il server dovrà essere configurato per utilizzare come default gateway un indirizzo IP di SWTx in VRF ACADEMIC e con rotte statiche esplicite per raggiungere le reti afferenti a GÉANT utilizzando come gateway un indirizzo IP di SWTx configurato in VRF "GÉANT".

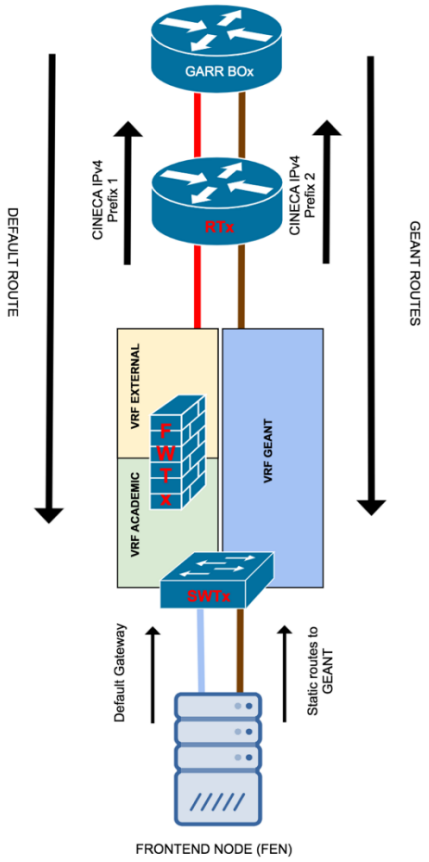

Figura 7: Accesso protetto (verso internet e GARR) e non protetto (verso GÉANT)

La ditta concorrente dovrà meglio specificare all'interno del progetto tecnico le modalità di realizzazione del routing e lo scenario di configurazione dei Firewall in alta affidabilità ritenuto più adeguato (active-standby, active-active, vedi anche 4.3.3 Requisiti minimi dei Firewall).

4.2.3 Architettura rete servizi - CINECA Tecnopolo

Obiettivi

La rete dei servizi dovrà:

- implementare una infrastruttura ethernet/IP di management per il collegamento, la gestione e il monitoraggio di tutti gli apparati di rete/firewall e delle componenti a supporto della rete (es. sistema di gestione WiFi, piattaforme di management rete/firewall, console server, ecc.) oggetto della presente fornitura.
- implementare reti IP wireless e collegare l'esistente rete cablata per il personale CINECA e per eventuale personale ospite garantendo differenti privilegi di accesso alle risorse
- implementare le seguenti tipologie di accesso alle risorse interne/esterne (vedi anche 4.3.2.3 Requisiti minimi rete servizi - CINECA Tecnopolo):
  a) accesso alla infrastruttura ethernet/IP di management:

- dalle postazioni (PDL) cablate e wireless del personale autorizzato
- dalle reti del datacenter CINECA di Casalecchio utilizzando i link dedicati tra i due datacenter
- dall'esterno tramite VPN terminate sui firewall perimetrali FWTx

b) accesso ad Internet e alle reti risorse interne (es. FEN, OMN, etc..) dalle Postazioni di Lavoro (PDL) cablate e wireless del personale autorizzato presso il Tecnopolo.
c) accesso ad Internet delle postazioni mobili (Laptop, Tablet, Smartphone etc.) per gli ospiti

L'accesso a tali servizi dovrà avvenire sia tramite rete cablata che mediante rete wireless e realizzata tramite gli switch SWT-Sx e l'infrastruttura wireless necessaria oggetto della fornitura (vedi anche 4.3.2.3 Requisiti minimi rete servizi).

Descrizione architettura

Il design dell'architettura della rete servizi è a discrezione della ditta concorrente purché soddisfi gli obbiettivi e i requisiti minimi funzionali e tecnologici richiesti (vedi anche 4.3.2.3 Requisiti minimi rete servizi)

4.2.4 Architettura interconnessione - CINECA Casalecchio di Reno - Tecnopolo

Obiettivi

- I datacenter CINECA di Casalecchio di Reno e del Tecnopolo necessitano di essere connessi direttamente (IDC). Un provider di servizi di connettività MAN fornirà gli apparati fisici e i link ottici in tecnologia Ethernet (all'utilizzatore) fino alle sale macchine dei suddetti datacenter. I link saranno due per ottenere una piena ridondanza funzionale e di cammino e si desidera attivarli con una capacità di trasporto di 100Gb/s ciascuno per essere poi utilizzati in modalità active/active.

Descrizione architettura

L'interconnessione tra i datacenter di CINECA Casalecchio e CINECA Tecnopolo sarà realizzata mediante due collegamenti geografici ethernet da 100Gb/s ciascuno e attestati, lato Casalecchio su una coppia di apparati Mellanox MSN2700 (D19, D20) con sistema operativo Cumulus Linux v.3.7.6, lato Tecnopolo sugli apparati di rete SWTx oggetto della fornitura
Gli apparati lato Tecnopolo saranno poi configurati tra loro in MLAG per consentire la configurazione di un aggregato logico da 200Gb/s verso i corrispettivi apparati lato Casalecchio (attualmente già configurati in MLAG) per consentire il trasporto di VLAN o la definizione di punto-punto L3 tra i due datacenter e garantire bilanciamento di carico e la ridondanza.

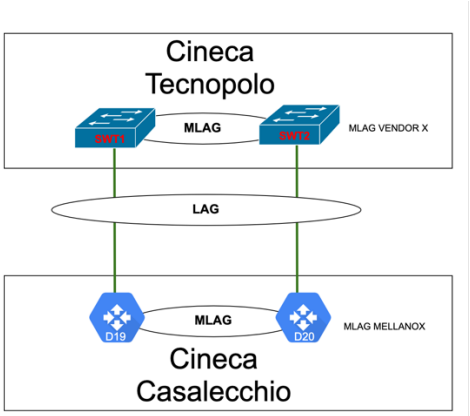

Figura 8 interconnessione tra i datacenter CINECA

La ditta concorrente dovrà meglio specificare all'interno del progetto tecnico le modalità necessarie che andranno implementare per garantire la connettività richiesta tra le reti dei due datacenter.

4.3 Requisiti tecnici minimi della fornitura

L'esecutore dovrà obbligatoriamente garantire la fornitura di apparati e di tutte le componenti necessarie garantendo i requisiti minimi generali e specifici indicati nei sotto paragrafi che seguono

4.3.1 Requisiti minimi generali

Seguono i requisiti minimi generali richiesti:

- Gli apparati forniti dovranno essere nuovi (non usati e/o rigenerati) e realizzati con componenti prodotte da primari costruttori a livello mondiale;
- Le componenti software integrate nelle risorse hardware oggetto della fornitura dovranno essere fornite all'ultima release stabile;
- La fornitura dovrà comprendere i servizi di installazione e configurazione;
- La fornitura dovrà comprendere le eventuali licenze software necessarie per la durata di 60 mesi;
- La fornitura dovrà comprendere i servizi di assistenza e manutenzione per tutte le componenti hardware e software fornite per la durata di 60 mesi come maggiormente dettagliato in 0 Art. 6. Servizi di manutenzione e assistenza

Per quanto riguarda gli aspetti di logistica, si specifica che:

- Gli apparati di rete ed i Firewall dovranno essere di tipo rack-mounted ossia installabile in rack standard da 19" ed essere dotati ciascuno di alimentazione ridondata per consentire l'alimentazione a due sorgenti elettriche distinte;
- La fornitura dovrà comprendere tutto il necessario per la realizzazione dell'architettura proposta, ovvero a titolo puramente esemplificativo e non esaustivo: componenti HW, componenti software, cavetteria varia, patch in fibra ottica, eventuali slitte e materiali necessari per

il collegamento sia alla rete dati che alla rete elettrica (ovvero cavi in fibra ottica, cavi UTP, cavi DAC, ecc.) e per l'installazione all'interno dei rack;
- Ogni risorsa HW di tipo rack-mounted oggetto della fornitura dovrà prevedere un sistema di dissipazione del calore basato su flussi d'aria nella direzione fronte – retro;
- Tutti i cablaggi richiesti sia in fibra ottica che in rame dovranno essere attestati su patch panel installati all'interno dei rack coinvolti o con presa RJ45 a muro per gli Access Point

In particolare:

- Gli apparati FWCx forniti presso la sede di Casalecchio di Reno verranno installati in due rack già esistenti e quindi non oggetto di fornitura. Tali rack saranno di dimensioni 800mm x 1000mm (LxP) e posizionati a non più di 60 metri l'uno dall'altro. Gli apparati potranno occupare un massimo di 8 Rack Unit ciascuno, ed avere almeno due (massimo 6) prese di alimentazione di tipo C13. In caso di alimentazioni di tipologia differente (es. C19) il fornitore dovrà prevedere anche la fornitura delle PDU con alimentazione monofase 2P+T connettività CEE 32A.
- Gli apparati SWTx forniti presso il Tecnopolo verranno installati in due rack oggetto di fornitura (vedi SWTx nella Sala "HPC Leonardo" di Figura 9) .Tali due rack dovranno ciascuno
  - Avere dimensioni: 800mm x 1000mm da 42RU
  - Essere dotati di almeno n.2 PDU con alimentazione monofase 2P+T connettività CEE 32A
  - Ospitare apparati che non devono complessivamente assorbire più di 6 KW totali
- Gli Access Point (APx) forniti presso il Tecnopolo andranno installati nella Sala "HPC Leonardo" e collegati agli apparati SWT-Sx installati nelle "Sale reti" (vedi Figura 9)
- Le piattaforme di management e tutti gli altri apparati forniti presso la sede del Tecnopolo, verranno installati in una coppia di rack che dovranno far parte della fornitura e che saranno dislocati in due "Sale reti" distinte (vedi Figura 9) ad una distanza massima di 20 metri l'uno dall'altro e di 90 metri dalla sala che ospiterà gli apparati SWTx e gli Access Point (APx) al fine di garantire la necessaria ridondanza fisica; i rack dovranno ciascuno:
  - Avere dimensioni: 800mm x 1000mm da 42RU
  - Essere dotati di almeno n.2 PDU con alimentazione monofase 2P+T connettività CEE 32A
  - Ospitare apparati che non devono complessivamente assorbire più di 6 KW totali
- La ditta concorrente, oltre ai cablaggi necessari per realizzare le interconnessioni richieste dal progetto, dovrà anche fornire:
  - dorsale 12 porte rame cat. 6 da ognuna delle due sale reti verso il rack che contiene gli apparati SWTx (vedi Figura 9)
  - n. 10 cavi MPO-12 fibre ottiche multimodali e relativi patch-panel tra ognuna delle due sale reti verso il rack che contiene gli apparati SWTx (vedi Figura 9)
  - n. 5 cavi MPO-12 fibre ottiche monomodali e relativi patch-panel tra ognuna delle due sale reti verso il rack che contiene gli apparati SWTx (vedi Figura 9)
  - i cavi necessari per interconnettere il centro stella (già esistente, non oggetto della presente fornitura), su cui sono stati accentrati i collegamenti delle postazioni di lavoro cablate (PDL), verso le due "Sale reti" (vedi Figura 9). In particolare si richiede di

fornire almeno i seguenti collegamenti di lunghezza massima pari a 90m tra la sala in cui si trova il centro stella delle PDL e ognuna delle due "Sale reti":

- n.8 cavi in rame UTP almeno cat.6 e relativi patch-panel rack-mounted
- n.1 cavo MPO-12 fibre ottiche multimodali e relativi patch-panel con 6 connettori LC-LC

Figura 9: Planimetria datacenter Tecnopolo

4.3.2 Requisiti minimi rete

I requisiti minimi funzionali e tecnologici riportati nei sotto paragrafi che seguono sono stati strutturati in forma tabellare per garantire una maggiore facilità di riferimento utilizzando specifici codici di requisito

4.3.2.1 Requisiti minimi rete di produzione - CINECA Casalecchio di Reno

Per la sede di Casalecchio la fornitura dovrà consentire di raggiungere gli obiettivi indicati in 4.2.1 Architettura rete di produzione - CINECA Casalecchio di Reno e garantire i seguenti requisiti minimi funzionali e tecnologici:

Cod. Req.	Ambito	Descrizione
R.1	Funzionalità Posiziona-mento	Al fine da preservare l'architettura di routing attualmente in esercizio i firewall oggetto della fornitura dovranno essere posizionati sul livello internet border ovvero collegati ai border router Juniper MX204 con un numero di interfacce opportunamente dimensionato per garantire una banda aggregata complessiva adeguata (vedi 4.3.2.1 Requisiti minimi rete di produzione - CINECA Casalecchio e 4.3.3 Requisiti minimi dei Firewall)
R.2	Hardware	Al fine da garantire la massima scalabilità e flessibilità in merito alle connessioni dei firewall con gli apparati Juniper MX204 pre-esistenti si richiede per ciascun MX204 la fornitura di: o n.2 transceiver ethernet 40Gb/s Juniper QSFPP-40GBASE-SR4 o n.2 transceiver ethernet 40Gb/s Juniper QSFPP-4X10GE-SR o n.8 transceiver ethernet 10Gb/s Juniper SFPP-10G-SR-C da utilizzare su interfacce fisiche già disponibili sul MX204 e su quelle realizzabili tramite cavi breakout (richiesti nel punto successivo) o n.2 cavi da 3mt per suddividere una porta ethernet 40Gb/s (QSFPP-4X10GE-SR) in 4 porte ethernet 10Gb/s senza transceiver saldati alle estremità (es. cavo breakout MPO-12 to 4 x LC) Nota: in base alla architettura di erogazione del servizio Firewall proposta dalla ditta concorrente (active-active o active standby) potrà essere necessario procedere con la configurazione in MLAG degli apparati MX204. Tale attività sarà eventualmente sempre a carico della ditta concorrente che dovrà preoccuparsi di fornire anche tutte le componenti aggiuntive che si dovessero rendere necessarie per il corretto dimensionamento della banda tra i MX204. A tal fine si anticipa che sugli MX204 sono disponibili, ovvero utilizzabili, le sole 4 interfacce QSFP28 mentre il modulo da 8 porte 10Gb/s è già completamente utilizzato.
R.3	Integrazione	Si richiede la fornitura di n.4 transceiver ethernet 100GBASE-SR4[2], NVIDIA MMA1B00-C100D (https://store.mellanox.com/products/nvidia-mma1b00-c100d-optical-transceiver-100gbe-qsfp28-mpo-850nm-sr4-up-to-100m-ddmi.html), da utilizzare sugli switch Mellanox MSN2700 (D19/D20): n.1 per ciascuno switch più n.2 transceiver spare da utilizzare come backup, per la realizzazione dell'interconnessione geografica a 200Gb/s tra i datacenter CINECA Casalecchio e Tecnopolo.

4.3.2.2 Requisiti minimi rete di produzione - CINECA Tecnopolo

[2] Si richiedono transceiver 100GBASE-SR4 (copertura fino a 100m) in quanto l'illuminazione delle tratte geografiche a lunga distanza è delegata al fornitore dei circuiti fisici esterni (circuiti non oggetto della presente fornitura)

Per la sede del Tecnopolo la fornitura dovrà consentire di raggiungere gli obbiettivi indicati in 4.2.2 Architettura rete di produzione - CINECA Tecnopolo e garantire i seguenti requisiti minimi funzionali e tecnologici:

Cod. Req.	Ambito	Descrizione
R.4	Funzionalità Posizionamento	i firewall FWTx dovranno essere posizionati sul livello internet border ovvero connessi agli apparati RTx per garantire la protezione sul perimetro; le policy di sicurezza tra le reti interne saranno invece implementate dagli apparati SWTx

R.5	Funzionalità Rete	• utilizzo di VRF distinte per separare le seguenti tipologie di flussi di traffico
		  ○ flussi protetti dai firewall perimetrali (VRF "External" e "Academic")
		  ○ flussi non protetti (bypass) dai firewall perimetrali per l'accesso alle sole reti afferenti a GÉANT (VRF "GÉANT")
		• aggregazione in MLAG di almeno n.4 link 100Gb/s ethernet tra gli apparati RTx e SWTx da utilizzare per trasportare VLAN e/o realizzare connessioni punto-punto L3.
		• implementazione di opportuni filtri (es. ACL e/o funzionalità di uRPF, Unicast Reverse Path Forwarding) sugli apparati RTx per evitare di ricevere traffico da host non afferenti alle reti GÉANT sul collegamento di accesso dedicato a GÉANT (collegamento marrone Figura 4) come meglio specificato nella sezione "Descrizione architettura"

R.6	Funzionalità Comunicazioni Server HPC	• i FEN potranno essere configurati con indirizzamento IP pubblico o con indirizzamento IP privato ed esposti su Internet tramite i FWTx. Per entrambe le tipologie di FEN sarà possibile attivare una seconda interfaccia (fisica o logica) configurata con indirizzamento IP pubblico per raggiungere le sole reti della ricerca afferenti a GÉANT bypassando i Firewall FWTx (vedi anche sotto "Descrizione Architettura" e Figura 7):
		Figura 7
		Indipendentemente dalla tipologia i FEN dovranno poter:
		  ○ contattare ed essere contattati da internet e dalle reti GÉANT
		  ○ essere raggiunti direttamente dalle reti CINECA del datacenter di Casalecchio sul link IDC (vedi 4.2.4)
		• gli OMN saranno configurati con IP privati e dovranno poter:
		  ○ accedere alla general internet via NAT
		  ○ essere raggiunti da internet via VPN

		○ essere raggiunti direttamente sul link IDC tra i datacenter CINECA (vedi 4.2.4) • i server SG saranno utilizzati come gateway tra il mondo ethernet e mondo infiniband e, almeno nella fase iniziale, forniranno servizi a server su rete INFN. Gli SG saranno probabilmente connessi in LAG verso gli switch SWTx e su tali LAG saranno realizzate delle connessioni punto-punto L3[3]. Il requisito funzionale sarà quindi quello di configurare gli apparati di rete per garantire il routing verso le reti infiniband tramite le connessioni punto-punto L3. Il traffico verso i SG potrà comunque arrivare oltre che dai sistemi INFN anche da alcune reti CINECA del datacenter di Casalecchio di Reno e da alcune reti esterne
R.7	Hardware	Si richiede la fornitura di n.2 apparati di rete di tipo RTx (vedi Figura 4): • basati, ciascuno, su architetture di tipo non blocking wirespeed, ovvero con backplane dimensionati in grado da garantire la trasmissione alla velocità massima consentita (wirespeed) e senza limitazioni (non-blocking) per almeno le seguenti interfacce (che dovranno essere incluse nella presente fornitura, per singolo apparato): ○ n.1 interfaccia ethernet 100Gb/s inclusiva di transceiver 100GBASE-SR4[2] per connessione geografica verso il POP GARR. ○ n.4 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4[2] per connessione verso apparati SWTx (2 interfacce) e apparato gemello RTx (2 interfacce) ○ n.2 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per connessione verso apparati firewall (FWT1, FWT2) ○ n.4 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per espansione futura/backup ○ n.2 interfacce ethernet 10Gb/s inclusive di transceiver 10GBASE-SR per collegamento degli switch SWT-Sx ○ n.6 interfacce 10Gb/s 10Gb/s inclusive di transceiver 10GBASE-SR per espansione future/backup • dotati di interfaccia di management ethernet 1000BaseT e di interfaccia console • con alimentazione ridondata • con tutte le licenze necessarie per supportare le funzionalità di networking sia di Layer 2 (L2) sia di Layer3 (L3) con riferimento

[3] La configurazione degli SG è in carico al fornitore del supercalcolatore Leonardo che non ha ancora fornito a CINECA i dettagli tecnici. Tali dettagli saranno condivisi con la ditta concorrente in una fase successiva

		al modello OSI su rete Ethernet ed in particolare almeno le seguenti: ○ Routing IPv4 e IPv6 ○ OSPF v2/v3 ○ MP-BGP ○ Supporto per almeno n.4 VRF con ▪ possibilità di realizzare import/export di prefissi di rete tra le VRF (VRF leaking) sulla base di criteri definibili dall'utente che non richiedano necessariamente all'utente l'inserimento di elenchi statici (es. possibilità di import/export in/da una VRF di tutti i prefissi ricevuti da un determinato protocollo di routing) ▪ possibilità di gestire tabelle di routing con almeno 30.000 reti unicast per almeno una VRF ○ uRPF (Unicast Reverse Path Forwarding) ○ FHRP (es. VRRP, HSRP, ecc.) ○ Possibilità implementare regole di filtraggio del traffico di policy su base IP (es. ACL, security policy, etc.) ○ MLAG o tecnologia di aggregazione su chassis differenti similare (es. ESI LAG, vedi anche 4.2.2) ○ LACP ○ Switching L2 ○ VLAN (IEEE802.1Q) ○ L2 e L3 Multicast ○ Supporto Jumbo frame ○ Funzionalità per il controllo del broadcast storm Funzionalità di campionamento dei flussi di traffico ed inoltro ad apparati terzi per attività di analisi e monitoring (es. Netflow, Jflow, ecc.)
R.8	Hardware	Si richiede la fornitura di n.2 apparati di rete di tipo SWTx (vedi Figura 4): • basati su architetture di tipo non blocking wirespeed, ovvero dimensionati con backplane in grado da garantire ciascuno la trasmissione alla velocità massima consentita (wirespeed) e senza limitazioni (non-blocking) ad almeno le seguenti interfacce (che dovranno essere incluse nella presente fornitura, per singolo apparato): ○ n.1 interfaccia ethernet 100Gb/s inclusiva di transceiver 100GBASE-SR4[2] per connessione geografica verso il corrispettivo switch Mellanox MSN2700 di Casalecchio (D19/D20). ○ n.8 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per connessione verso apparati RTx (2 interfacce) e apparato gemello SWTx (6 interfacce)

		○ n.16 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per connessione verso gli SG. Si fa presente che in questo caso la ditta concorrente non dovrà fornire i cavi in fibra ottica necessari per il collegamento degli SG in quanto già oggetto di altra fornitura. ○ n.8 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per rilancio dei collegamenti di n.2 apparati SG verso infrastruttura INFN ○ n.2 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 per espansione futura/backup ○ n.32 interfacce ethernet 100Gb/s inclusive di transceiver 100GBASE-SR4 da collegare verso altrettanti server (FEN) dotati di scheda di rete NVIDIA MCX516A-CCAT ConnectX-5 EN https://store.mellanox.com/products/nvidia-mcx516a-ccat-connectx-5-en-adapter-card-100gbe-dual-port-qsfp28-pcie3-0-x16-tall-bracket-rohs-r6.html e posti ad una distanza massima di 20 metri dagli apparati SWTx. La scelta della tipologia di cavi da utilizzare per realizzare le connessioni (es. cavi DAC, transceiver e cavi in fibra con connettori MPO o LC, ecc.) è lasciata alla ditta concorrente che dovrà fornire tutto il necessario per realizzare i collegamenti richiesti ○ n.6 interfacce ethernet 10Gb/s inclusive di transceiver 10GBASE-SR per il collegamento degli OMN. Si fa presente che in questo caso la ditta concorrente non dovrà fornire i cavi in fibra ottica necessari per il collegamento degli OMN in quanto già oggetto di altra fornitura. ○ n.2 interfacce ethernet 10Gb/s inclusive di transceiver 10GBASE-SR per espansione futura/backup In caso di fornitura di apparati SWT che prevedano solo interfacce ethernet a 400 Gb/s, dovrà essere fornito tutto il necessario (es. cavi di breakout, patch panel, ecc.) per ricavare le interfacce 10Gb/s e 100Gb/s minime richieste. Tali interfacce da 10Gb/s e 100Gb/s dovranno essere attestate su patch panel dedicati, inclusi nella fornitura, e installati all'interno dei rack contenenti gli apparati SWT. • dotati di interfaccia di management ethernet 1000BaseT e di interfaccia console • con alimentazione ridondata • con tutte le licenze necessarie per supportare le funzionalità di networking sia di Layer 2 (L2) sia di Layer3 (L3) con riferimento

		al modello OSI su rete Ethernet ed in particolare almeno le seguenti: ○ Routing IPv4 e IPv6 ○ OSPF v2/v3 ○ Supporto per almeno n.4 VRF ○ FHRP (es. VRRP, HSRP, ecc.) ○ Possibilità implementare regole di filtraggio del traffico di policy su base IP (es. ACL, security policy, etc.) ○ MLAG o tecnologia di aggregazione su chassis differenti similare (es. ESI LAG, vedi anche 4.2.2) ○ LACP ○ Switching L2 ○ VLAN (IEEE802.1Q) ○ L2 e L3 Multicast ○ Supporto Jumbo frame ○ Funzionalità per il controllo del broadcast storm ○ Funzionalità di campionamento dei flussi di traffico ed inoltro ad apparati terzi per attività di analisi e monitoring (es. Netflow, Jflow, ecc.)
R.9	Gestione	Si richiede che gli apparati di rete RTx e SWTx siano dotati delle seguenti funzionalità amministrative a livello di sistema operativo: • Shell di amministrazione con comandi per la gestione del sistema, dei file locali, del monitoraggio • Client SSHv2 e Telnet • Definizione di utenze amministrative multiple configurabili per differenziare i privilegi di accesso e gestione degli apparati. • Autenticazione degli utenti e dei gruppi sia locale che remoto mediante protocollo Radius • Logging di eventi e anomalie • Supporto di inoltro log su server remoto tramite protocollo Syslog • Supporto protocolli SNMPv2 e v3 e “Management Information Base” (MIB)
R.10	Omogeneità	Gli apparati RTx e SWTx dovranno essere prodotti dallo stesso vendor (che dovrà essere anche lo stesso degli apparati SWT-Sx, vedi switch rete servizi, vedi 4.3.2.3.1 Requisiti tecnologici switch ethernet)
R.11	Completezza	Si richiede la fornitura delle ulteriori risorse software o hardware (es. server, interfacce fisiche, transceiver, licenze, etc..) che si dovessero rendere necessarie sugli apparati RTx/SWTx/FWTx per la realizzazione dell’architettura della rete servizi proposta dalla ditta concorrente (vedi anche 4.2.3 Architettura rete servizi - CINECA Tecnopolo e 4.3.2.3 Requisiti minimi rete servizi - CINECA Tecnopolo)

4.3.2.3 Requisiti minimi rete servizi - CINECA Tecnopolo

La rete dei servizi da realizzare presso la sede CINECA del Tecnopolo dovrà consentire di raggiungere gli obiettivi indicati in 4.2.3 Architettura rete servizi - CINECA Tecnopolo e garantire seguenti requisiti minimi funzionali e tecnologici.

Si ricorda che le ulteriori risorse software o hardware (es. server, interfacce fisiche, transceiver, licenze, etc..) che si dovessero rendere necessarie per la realizzazione dell'architettura della rete servizi proposta (oltre a quelle descritte nel presente paragrafo e nei relativi sotto paragrafi) dovranno essere incluse all'interno della presente fornitura, ovvero la soluzione dovrà essere di tipo "chiavi in mano"

Cod. Req.	Ambito	Descrizione
S.1	Funzionalità Rete di Management	Realizzazione di una infrastruttura ethernet/IP di management sulla quale collegare principalmente le interfacce di Management degli apparati di rete/firewall, le relative piattaforme di Management e il console server (vedi 4.3.3.2 Requisiti funzionali obbligatori per la gestione dei Firewall e 4.3.2.3.3 Requisiti tecnologici network managemen) e che possa: • consentire l'accesso agli apparati di rete via IP e tramite console server dedicato raggiungibile via IP sia su rete locale che su rete 4G/LTE per avere le possibilità di realizzare un accesso diretto out-of-band in caso di indisponibilità della rete IP locale . • avere accesso alla general internet • essere raggiunta dall'esterno via VPN • essere raggiunta dalle reti PDL CINECA del datacenter di Casalecchio utilizzando il link diretto tra i due datacenter (vedi anche 4.2.4 Architettura interconnessione - CINECA Casalecchio di Reno - Tecnopolo) • essere raggiunta dalle postazioni autorizzate cablate o con accesso WiFi del datacenter tecnopolo
S.2	Funzionalità di Management e Monitoring rete	Realizzazione almeno delle seguenti funzionalità di network monitoring/management: • Gestione e monitoraggio centralizzato della disponibilità, dell'utilizzo delle principali risorse HW (es. CPU, RAM, ecc.) e dell'utilizzo di banda delle interfacce di rete degli apparati SWTx, RTx, SWT-Sx

		• Monitoraggio centralizzato della disponibilità, dell'utilizzo delle principali risorse HW (es. CPU, RAM, ecc.) e dell'utilizzo di banda delle interfacce di rete degli apparati FWTx, FWCx • Monitoraggio centralizzato della disponibilità degli apparati APx • La ricezione e possibile consultazione dei log degli apparati SWTx, RTx, SWT-Sx • Backup delle configurazioni degli apparati di rete (SWTx/RTx/SWT-Sx) con possibilità di verificare le differenze tra versioni differenti ed eseguire il ripristino di configurazioni precedenti
S.3	Funzionalità di Management e Monitoring WiFi	Realizzazione almeno le seguenti funzionalità di network monitoring/management per la rete WiFi: • Gestione e monitoraggio centralizzato della disponibilità del sistema di accesso WiFi. • Raccolta e possibile consultazione dei log del servizio • Backup delle configurazioni del servizio
S.4	Funzionalità Rete cablata e wireless	Realizzazione di infrastruttura cablata e wireless mediante la fornitura e configurazione di tutti gli apparati, i sistemi, i software e licenze utili per fornire accesso dedicato ai servizi specificati in 4.2.3 Architettura rete servizi - CINECA Tecnopolo (vedi sezione Obiettivi, casi: a, b, c) e che garantisca almeno: • Isolamento logico tra le varie reti da realizzare mediante utilizzo di VLAN e SSID dedicati. • Accesso alle reti wireless (servizi dei casi a e b) mediante protezione di tipo WPA2/WPA3 ENTERPRISE e autenticazione IEEE802.1X basata su protocollo Radius, configurato in alta disponibilità su sistemi inclusi nella presente fornitura, per autenticare le utenze sia in locale che sui sistemi di autenticazione della sede CINECA di Casalecchio di Reno. Il sistema di autenticazione Radius dovrà essere configurato per mantenere anche i dati di accesso al servizio WiFi degli utenti. • Accesso alle reti wireless per gli ospiti (caso c) mediante apposito captive-portal
S.5	Funzionalità Posizionamento	Collegamento fisico degli switch ethernet SWT-Sx sugli apparati RTx

4.3.2.3.1 Requisiti tecnologici switch ethernet

Cod. Req.	Ambito	Descrizione
S.6	Hardware	Si richiede la fornitura di almeno n.2 switch ethernet (SWT-Sx in Figura 4): • basati su architetture di tipo non blocking wirespeed, ovvero dimensionati con backplane in grado da garantire ciascuno la trasmissione alla velocità massima consentita (wirespeed) e senza limitazioni (non-blocking) ad almeno le seguenti interfacce (che dovranno essere incluse nella presente fornitura, per singolo apparato) o n.8 interfacce ethernet 10Gb/s inclusive di transceiver 10GBASE-SR o n.16 interfacce ethernet 1Gb/s 1000BASE-T con supporto degli standard IEEE802.3af (POE) e IEEE.802.3at (POE+) o n.16 interfacce ethernet 1Gb/s 1000BASE-T • dotati di interfaccia di management ethernet 1000BaseT e di interfaccia console • con alimentazione ridondata • che supportino le funzionalità di o VLAN (IEEE802.1Q) o L2 e L3 Multicast o Jumbo frame o Controllo del broadcast storm • che supportino le seguenti funzionalità amministrative a livello di sistema operativo: o Shell di amministrazione con comandi per la gestione del sistema, dei file locali, del monitoraggio o Client SSHv2 e Telnet o Definizione di utenze amministrative multiple configurabili per differenziare i privilegi di accesso e gestione degli apparati. o Autenticazione degli utenti e dei gruppi sia locale che remoto mediante protocollo Radius o Logging di eventi e anomalie o Supporto di inoltro log su server remoto tramite protocollo Syslog o Supporto protocolli SNMPv2 e v3 e “Management Information Base” (MIB)

S.7	Omogeneità	Gli apparati SWT-Sx dovranno essere prodotti dallo stesso vendor degli apparati RTx e SWTx (apparati descritti in 4.2.2 Architettura rete di produzione - CINECA Tecnopolo)

4.3.2.3.2 Requisiti tecnologici servizio WiFi

Cod. Req.	Ambito	Descrizione
S.8	Hardware	Si richiede la fornitura di n.8 access point e di quanto necessario (es. controller) per la implementazione di un servizio WiFi per l'accesso a internet e ai sistemi installati presso il datacenter del Tecnopolo come meglio richiesto e specificato nei requisiti funzionali indicati in 4.2.3). Gli access point dovranno: • supportare i protocolli IEEE 802.11ax, 802.11ac, 802.11a/g/n • supportare almeno 4 SSID • garantire il supporto Radio 2.4Ghz e 5Ghz • supportare WPA3 e WPA2 nelle modalità "Enterprise" con autenticazione sia RADIUS (802.1X) che PSK (Pre-Shared Key) • supportare i protocolli IEEE802.3af (POE) e IEEE.802.3at (POE+) • supportare il montaggio sia a parete che a soffitto. In caso di soluzioni WiFi basate su controller on-premise è richiesta la fornitura di controller ridondati e configurati in alta disponibilità. Soluzioni basate su servizi in cloud saranno accettate limitatamente alla parte di configurazione centralizzata del servizio e alla raccolta dei dati necessari per verificarne funzionamento e performance come meglio specificato in S.9
S.9	Piattaforma di Management WiFi	Si richiede al fornitura di una piattaforma di management per il servizio WiFi in grado di realizzare le funzionalità indicate nel requisito S.3 (vedi par. 4.3.2.3 Requisiti minimi rete servizi - CINECA Tecnopolo). La piattaforma di management potrà essere fornita a discrezione della ditta concorrente in modalità on-premise o cloud. In caso di fornitura on-premise si richiede che il servizio sia configurato in alta disponibilità con almeno 2TB di spazio per la raccolta dei log. In particolare si ricorda che i log di accesso degli amministratori dovranno essere conservati a norma di legge e disponibili per almeno 6 mesi secondo quanto previsto dal Garante Privacy

		In caso di erogazione del servizio in cloud dovranno essere rispettate le seguenti condizioni: • Il traffico degli utenti connessi agli AP non dovrà essere inviato sul cloud ma essere gestito esclusivamente in locale. Non saranno pertanto ammesse soluzioni che prevedano l'invio del traffico utente verso il cloud • Le configurazioni degli AP e dei dati necessari per il monitoraggio dei livelli di servizio e per il troubleshooting dovranno essere opportunamente cifrate e protette. La ditta concorrente dovrà meglio dettagliare all'interno dell'offerta tecnica le modalità e le policy di sicurezza implementate sul cloud per la protezione e trasmissione di tali informazioni al fine da assicurare che siano accessibili esclusivamente da utenze CINECA. • Il servizio in cloud dovrà essere ospitato al più su server localizzati in territorio europeo e dovrà rispettare le normative vigenti in termini di conservazione, integrità e riservatezza dei dati e quanto previsto dal regolamento europeo GDPR • La piattaforma di management dovrà raccogliere e consentire la visualizzazione dei log di accesso degli amministratori (login/logout) avvalendosi, se necessario, di ulteriori componenti hardware e software on premise. In particolare si ricorda che i log di accesso degli amministratori dovranno essere conservati a norma di legge e disponibili per almeno 6 mesi secondo quanto previsto dal Garante Privacy In entrambi i casi la piattaforma di management dovrà comprendere tutte le componenti hardware e software (inclusive di eventuali licenze per 60 mesi) utili al suo funzionamento

4.3.2.3.3 Requisiti tecnologici network management

Cod. Req.	Ambito	Descrizione
S.10	Piattaforma di Management Rete	Si richiede la fornitura di una piattaforma di network management per la gestione e il monitoraggio della rete in grado di realizzare le funzionalità indicate nel requisito S.2 (vedi Requisiti Funzionali del par. 4.3.2.3 Requisiti minimi rete servizi - CINECA Tecnopolo). La piattaforma di management: • dovrà essere fornita esclusivamente in modalità on-premise, non saranno pertanto ammesse soluzioni basate su cloud

		• potrà avvalersi di componenti differenti (es. per la gestione, per il monitoraggio, per la raccolta dei log, ecc.) ciascuna delle quali dovrà essere ridondata e configurata in alta disponibilità • dovrà garantire almeno 4TB di spazio disco per la raccolta dei log; in particolare si ricorda che i log di accesso degli amministratori dovranno essere conservati a norma di legge e disponibili per almeno 6 mesi secondo quanto previsto dal Garante Privacy Il sistema di network management/monitoring richiesto dovrà comprendere tutte le componenti hardware e software (inclusive di eventuali licenze per 60 mesi) utili al suo funzionamento
S.11	Accesso	Si richiede la fornitura di un console server per l'attestazione delle interfacce seriali degli apparati di rete (RTx, SWTx, SWT-Sx (inclusiva delle eventuali licenze per 60 mesi) che disponga di almeno 32 interfacce seriali e consenta di raggiungere le console degli apparati ad esso connessi via IP sulla LAN e out-of-band (OBM) via LTE/4G. La scheda SIM LTE/4G sarà fornita da CINECA.

4.3.2.4 Requisiti minimi rete interconnessione - CINECA Casalecchio di Reno - Tecnopolo

Per l'interconnessione tra i due datacenter CINECA di Casalecchio e Tecnopolo la fornitura dovrà consentire di raggiungere gli obiettivi indicati in 4.2.4 Architettura interconnessione - CINECA Casalecchio di Reno - Tecnopolo e garantire i seguenti requisiti minimi funzionali (i requisiti tecnologici per gli apparati sono stati già specificati nei precedenti paragrafi)

Cod. Req.	Ambito	Descrizione
I.1	Attivazione	L'offerente dovrà attivare sui due link che interconnetteranno i datacenter CINECA, ovvero gli apparati D19/D20 di produzione del datacenter di Casalecchio e gli apparati SWTx oggetto della fornitura, un canale aggregato di capacità complessiva pari a 200Gb/s fornendo gli apparati, le ottiche, i cablaggi di sala e in generale tutto l'occorrente che sarà meglio specificato nel seguito. Le tecnologie impiegate dovranno permettere la realizzazione di reti con protocolli layer 2 e layer 3 (in particolare VLAN stretching fra i datacenter)
I.2	Configurazione	L'offerente dovrà inizialmente configurare gli apparati di entrambi i datacenter CINECA per garantire le seguenti interconnessioni: • dalle reti CINECA del datacenter di Casalecchio verso le reti dei FEN (pubbliche e private, vedi requisiti funzionali par. 4.2.2). L'obiettivo è di realizzare delle connessioni dirette che consentano agli utenti

		connessi ai sistemi del datacenter Casalecchio di raggiungere direttamente i FEN ed evitare di impattare sui Firewall FWTx. • dalle reti PDL CINECA e da alcuni sistemi di backup del datacenter di Casalecchio verso i OMN (vedi anche requisiti funzionali OMN in 4.2.2) e verso la rete di management (vedi anche 4.2.3) • da alcune reti CINECA del datacenter di Casalecchio e da alcune reti INFN attestate sugli apparati SWTx al Tecnopolo verso gli SG

4.3.3 Requisiti minimi dei Firewall

4.3.3.1 Requisiti tecnologici obbligatori dei Firewall

La fornitura prevede n.2 istanze di Firewall, una destinata alla sede di CINECA Casalecchio (FWC)e l'altra alla sede di CINECA Tecnopolo (FWT).
Ai fini del seguente capitolato, per "istanza di Firewall" s'intende una soluzione di sicurezza perimetrale avente le caratteristiche minime obbligatorie, ed eventualmente anche migliorative, descritte nella documentazione di gara. L'istanza deve essere intesa come una "black box" costituita da un determinato numero di apparati (e quindi non necessariamente due come riportato nello schema di Figura 4) per l'analisi del traffico (i veri e propri Firewall) e da eventuali atri apparati e/o dispositivi di supporto, lasciando all'offerente la piena libertà - nei limiti dei requisiti espressi dal capitolato – di definirne l'architettura "interna", come, ad esempio, il numero, la tipologia e le caratteristiche degli apparati di cui è composta..La descrizione dell'architettura di suddetta "istanza", e non solo l'elenco delle sue componenti, deve essere presente nell'Offerta Tecnica al fine di permettere alla stazione appaltante la necessaria valutazione della proposta.

Cod. Req.	Ambito	Descrizione
F.1	Prestazioni richieste	L'istanza FWC deve assicurare in esercizio le seguenti prestazioni: • Almeno 10Gbps di traffico protetto dall'istanza firewall con tutte le funzionalità fornite tra quelle elencate in "4.3.3.3 Requisiti funzionali obbligatori per la sicurezza" contemporaneamente attive. Il totale del traffico minimo protetto deve poter essere formato da almeno 5Gbps di traffico VPN IPsec (IPv4) oppure, in alternativa, da almeno 5Gbps di traffico TLS/SSL da ispezionare. • Il numero di utenze VPN IPsec e SSL contemporaneamente attive (cfr "4.3.2.1 Requisiti tecnologici obbligatori dei Firewall") che l'istanza dovrà garantire dovrà essere almeno pari a 400 (quattrocento). • Le prestazioni indicate devono essere mantenute anche in presenza di guasti che affliggono non più del 50% dei dispositivi di una istanza (cfr. Architettura e HA) L'istanza FWT deve assicurare in esercizio le seguenti prestazioni:

		• Almeno 60Gb/s di traffico protetto dall'istanza firewall con tutti gli apparati funzionanti e con tutte le funzionalità fornite tra quelle elencate in "4.3.3.3 Requisiti funzionali obbligatori per la sicurezza" contemporaneamente attive, accettando un degrado massimo di non oltre il 50% del traffico protetto in caso di guasto di non più del 50% degli apparati. Il totale del traffico minimo protetto dal firewall deve poter essere formato da almeno 30Gb/s di traffico VPN IPsec (IPv4) oppure, in alternativa, da almeno 30Gbps di traffico TLS/SSL da ispezionare. Il numero di utenze VPN IPsec e SSL contemporaneamente attive (cfr "4.3.2.1 Requisiti tecnologici obbligatori dei Firewall") che l'istanza dovrà garantire dovrà essere almeno pari a 800 (ottocento). L'ispezione del traffico TLS/SSL deve poter essere effettuata sia per il traffico inbound (verso le risorse aziendali protette, tramite la installazione sul firewall dei loro certificati digitali X509 e relative chiavi private) sia per quello outbound (dalle risorse aziendali protette, es. PdL, verso Internet).
F.2	Architettura e HA	Le istanze FWC e FWT sono costituite entrambe da cluster con caratteristiche di Alta Affidabilità (HA). Questo implica che ciascuna istanza può essere formata da un numero di nodi a scelta dell'offerente, ma nel rispetto dei seguenti requisiti: 1. La modalità di HA offerta deve essere tale da non richiedere l'uso del multicast nella LAN tra l'istanza e la rete del CINECA. 2. L'istanza FWC deve garantire le prestazioni minime richieste (vedi sopra) anche in caso di guasto di non più del 50% degli apparati che le costituiscono (c.d. ridondanza 1:1).
F.3	Hardware	Tutte le componenti e tutte le istanze firewall devono essere dello stesso vendor, essere installabili in rack standard 19" e dotate di tutti gli accessori idonei allo scopo. Devono essere anche dotate di alimentatori ridondati (AC. 220V/50Hz). Le istanze devono avere almeno le seguenti interfacce per potersi collegare alla rete del CINECA. Da tale conteggio sono escluse tutte le porte di backend dell'istanza, ovvero quelle necessarie al suo corretto funzionamento interno in relazione all'architettura proposta. Sarà cura dell'offerente includere le componenti di rete necessarie (ad esempio moduli sui firewall, SFP, switch, cavi, ecc.) alla realizzazione della soluzione offerta. Si osservi anche che il requisito sulla numerosità e tipologia delle porte di rete non si applica alla piattaforma di gestione, ma solo alle componenti che sono incaricate della protezione del traffico. La piattaforma

		di gestione dovrà essere configurata dall'offerente in modo che possa rispondere ai requisiti indicati nel successivo paragrafo 2.3.2.2: • FWC: almeno n.4 porte 40Gb/s; almeno n.8 porte 10Gb/s; almeno n.4 porte 1Gb/s rame o 10Gb/s (per la gestione) • FWT: almeno n.4 porte 100Gb/s; almeno n.16 porte 10 Gb/s; almeno n.4 porte 1Gb/s rame o 10 Gb/s (per la gestione) Le porte indicate sopra, ad esclusione di quelle 1Gb/s, dovranno essere fornite complete di transceiver SR. Si richiedono inoltre i seguenti ulteriori transceiver da utilizzare per scopi futuri/backup: • n.2 transceiver 40Gb/s SR per l'istanza FWC • n.2 transceiver 100Gb/s SR per l'istanza FWT Le istanze devono supportare almeno i protocolli: • LACP (IEEE 802.3ad) per aggregare almeno n.4 interfacce per il collegamento con la rete del CINECA • VLAN (IEEE 802.1Q) • MP-BGP • OSPFv2/v3

4.3.3.2 Requisiti funzionali obbligatori per la gestione dei Firewall

La piattaforma di gestione, parte integrante della fornitura delle istanze Firewall, deve soddisfare i requisiti elencati di seguito.

Cod. Req.	Ambito	Descrizione
F.4	Gestione centralizzata e funzionalità	Le istanze FWC e FWT devono essere gestite da un'unica piattaforma di gestione che sarà dislocata obbligatoriamente on-premise presso una sede CINECA a Casalecchio o a Tecnopolo (a scelta della stazione appaltante durante la fase d'installazione). La piattaforma di gestione dovrà consentire: • La configurazione, tramite interfaccia web e/o console proprietaria unificata, delle istanze firewall oggetto del capitolato incluse le policy di sicurezza; • La ricezione e la indicizzazione dei log dalle istanze firewall;

		• La possibilità, tramite interfaccia web e/o console proprietaria, di effettuare ricerche personalizzate trai i log ricevuti. La piattaforma di gestione dev'essere fornita con tutto l'hardware, il software, le licenze e i servizi di manutenzione (per 60 mesi) necessari al suo pieno e corretto funzionamento.
F.5	Architettura e HA	La piattaforma di gestione deve essere costituita da n.2 appliance hardware dedicate configurate in alta disponibilità active/stand-by senza richiedere l'uso del multicast nella LAN tra suddetta piattaforma e la rete del CINECA. Per il collegamento della piattaforma di gestione con la rete del CINECA nel datacenter Casalecchio, la stazione appaltante metterà a disposizione dell'offerente al massimo n.4 porte 1Gbps in rame.
F.6	Prestazioni	Ogni appliance dovrà essere dotata di almeno 24TB (raw) per la memorizzazione dei log ed avere risorse computazionali e di memoria adeguate alla ricezione, indicizzazione e memorizzazione in modo sostenuto (non di picco) di almeno 20.000 (ventimila) righe di log al secondo. Le appliance, inoltre, dovranno essere alimentate AC 220V/50Hz e dovranno essere installabili in rack standard 19" (l'offerente dovrà fornire tutti gli accessori idonei allo scopo).

4.3.3.3 Requisiti funzionali obbligatori per la sicurezza realizzata dai Firewall

Di seguito sono elencati i requisiti funzionali per gli aspetti di sicurezza. Devono essere soddisfatti per tutti i 60 (sessanta) mesi di durata delle licenze e della manutenzione delle istanze Firewall.
Le funzionalità di seguito elencate devono essere comuni ad entrambe le istanze Firewall fornite.

Cod. Req.	Ambito	Descrizione
F.7	Network Firewall	Possibilità di configurare regole di filtraggio su base indirizzo IPv4/IPv6, protocollo, porta. Le regole devono anche consentire di identificare l'origine del traffico su base geografica ed implementare meccanismi configurabili di rate limiting.
F.8	Gestione e verifica dell'identità	Possibilità di abilitare regole di filtraggio condizionate dalla verifica dell'identità di utenti e/o dispositivi. Si richiede l'integrazione almeno con Active Directory e la disponibilità di servizi di autenticazione locali al Firewall (es. Captive Portal) e di client proprietari da distribuire almeno su postazioni di lavoro Windows 10 o superiore.

F.9	Application-aware Firewall	Possibilità di configurare regole di filtraggio basate sul riconoscimento delle maggiori applicazioni. Detto riconoscimento deve avvenire tramite l'analisi L7 del traffico di rete e non con la mera associazione IANA porta-applicazione.
F.10	Ispezione TLS/SSL	Possibilità di configurare regole di filtraggio con le quali abilitare l'analisi del traffico cifrato TLS/SSL. La funzionalità deve essere presente sia per il traffico inbound (verso le risorse aziendali protette, tramite la installazione sul firewall dei loro certificati digitali X509 e relative chiavi private) e sia per quello outbound (dalle risorse aziendali protette, es. PdL, verso Internet).
F.11	Filtraggio Web	Possibilità di configurare regole di filtraggio basate sulla classificazione delle risorse web (URL). La classificazione delle risorse deve avvenire in maniera dinamica, eventualmente anche per mezzo di un servizio Cloud del vendor in contatto continuo/periodico con il Firewall.
F.12	Intrusion Prevention System (IPS)	Il Firewall deve essere dotato di un servizio di Intrusion Prevention almeno basato su: IoC (anche signature relative a CVE noti ed IP reputation), identificazione di uso anomalo dei protocolli (DNS incluso), identificazione di anomalie nell'utilizzo delle risorse di rete o dei comportamenti utente. Il servizio deve anche avere la capacità di identificare e bloccare l'attività di Bot mediante il controllo dei canali di Command & Control attivi all'interno del traffico analizzato. La lista delle minacce (IoC, pattern, ecc.) deve essere aggiornata in modo dinamico, eventualmente anche per mezzo di un servizio Cloud del vendor in contatto continuo/periodico con il Firewall.
F.13	Antivirus	Il Firewall deve poter analizzare il traffico per identificare e bloccare, tramite Antivirus, la trasmissione di eseguibili o documenti malevoli (virus, malware, trojan, ecc.). L'antivirus deve almeno essere basato su signature. La lista delle firme deve essere costantemente aggiornata. La protezione può eventualmente anche essere fornita tramite l'integrazione con un servizio Cloud del vendor in contatto continuo/periodico con il Firewall.
F.14	VPN	Possibilità di configurare VPN sia IPsec che SSL. Il protocollo IPv6 deve essere supportato almeno per VPN SSL. La configurazione di VPN client-to-site deve supportare l'autenticazione a più fattori, una modalità clientless SSL (con portale di accesso integrato nel firewall), e una modalità che richiede l'installazione di un client proprietario (almeno per Windows 10 o superiore).

4.3.4 Requisiti servizi professionali

Dovranno far parte della fornitura i seguenti servizi professionali:

- servizi professionali per installazione e configurazione dei dispositivi conferiti
- servizi professionali di supporto post-implementazione di almeno n.10 giornate (es. per supporto nell'implementazione di configurazioni di rete atte a soddisfare requisiti non previsti nel progetto iniziale, per analisi e troubleshooting di anomalie funzionali, ecc.)
- servizio di formazione del personale Cineca sull'architettura tecnologica realizzata e sulla gestione operativa degli apparati forniti
- servizi di manutenzione e assistenza come meglio specificato nell'Art.6

L'offerente deve essere certificato o concessionario dei produttori del materiale oggetto della fornitura, che ne attesti la capacità di condurre con successo le attività previste dal presente Capitolato. Tutto il personale dell'offerente che effettuerà le attività di installazione, supporto, formazione dovrà essere in possesso delle certificazioni professionali rilasciate dai produttori delle tecnologie oggetto delle attività stesse.

4.4 Conformità alla normativa di riferimento

4.4.1 Le apparecchiature fornite dovranno obbligatoriamente essere munite dei marchi di certificazione riconosciuti da tutti i paesi dell'Unione Europea e dovranno obbligatoriamente essere conformi alle norme relative alla compatibilità elettromagnetica.
4.4.2 L'Esecutore dovrà obbligatoriamente garantire la conformità delle apparecchiature alle normative CEI o ad altre disposizioni internazionali riconosciute e, in generale, alle vigenti norme legislative, regolamentari e tecniche disciplinanti i componenti e le modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori.

4.5 Caratteristiche generali delle forniture

L'Esecutore dove garantire la completezza e l'omogeneità della fornitura stessa, indipendentemente dalla eterogeneità delle componenti dei servizi base e delle opzioni previste dalla fornitura.
La fornitura dovrà conformarsi ai requisiti di seguito indicati:

- tutte le apparecchiature eventualmente previste e le opzioni dovranno essere nuove di fabbrica, fornite dallo stesso produttore, ed essere costruite utilizzando parti nuove;
- tutta la fornitura dovrà risultare conforme ai requisiti di conformità indicati in precedenza;
- qualora l'erogazione del servizio prevedesse la fornitura di prodotti o apparecchiature all'utente finale, per ciascuna apparecchiatura dovrà essere fornita una copia della manualistica tecnica completa in formato elettronico, edita dal produttore; la documentazione dovrà essere in lingua italiana se disponibile oppure, se non prevista, in lingua inglese.

Art. 5. Piano di fornitura

5.1 L'Esecutore si deve attenere a quanto offerto.

5.2 Collaudo

Al termine della consegna della fornitura e dell'installazione e configurazione degli apparati, il Fornitore dovrà comunicare formalmente di essere pronto al collaudo.

Il collaudo sarà svolto dal personale del CINECA in contraddittorio con l'Esecutore ed avrà lo scopo di verificare il rispetto dell'Offerta Tecnica e del documento di progetto esecutivo.
Il collaudo deve dare esito positivo rispetto ai seguenti punti:

- coerenza del progetto rispetto agli obiettivi dell'Azienda;
- corrispondenza della fornitura con l'Offerta Tecnica e il rispetto degli obblighi contrattuali;
- verifica dell'opportunità di varianti.

A tal fine il Fornitore deve includere nel piano di progetto la proposta di un piano di collaudo, che deve essere preventivamente approvato e può essere pertanto modificato secondo le esigenze del CINECA.

Nel piano di collaudo **dovrà obbligatoriamente** essere inserito il test funzionale da eseguire.
CINECA si riserva inoltre la possibilità di effettuare ulteriori test funzionali e di carico con strumenti e metodologie proprie.

I test di accettazione che CINECA reputa necessari per considerare il collaudo concluso con esito positivo devono comprendere almeno i seguenti punti:

- test funzionali dimostranti la **compatibilità** delle componenti hardware/software fornite con quelle in essere al CINECA e specificate in precedenza;
- test operativi relativi alle **funzionalità** richieste dal presente capitolato tecnico;
- test operativi rispetto alle funzionalità aggiuntive a quelle minime previste e presenti nella offerta proposta che CINECA riterrà di interesse collaudare;
- test funzionali di continuous availability che verifichino la continuità di servizio. Di seguito un elenco non esaustivo ma esemplificativo di possibili test:
  - Guasto simulato ad una linea elettrica di alimentazione (esterna).
  - Guasto simulato di una ventola.
  - Guasto simulato di un alimentatore interno.
  - Guasto simulato di un intero switch/router.
  - Guasto simulato di un link e verifica della riconvergenza.

A positiva conclusione della fase di collaudo dovrà essere fornito un documento sintetico di collaudo (con una check list di punti che evidenzino che i test sono avvenuti con successo) e opportuna documentazione in lingua italiana contenente la rilevante descrizione tecnica dell'infrastruttura, comprendente:

- descrizione dell'architettura risultante;
- esplicitazione dettagliata dei task di implementazione e delle procedure operative propedeutiche alla gestione e manutenzione ordinaria dell'architettura, in particolare:
  - monitoraggio delle componenti hardware e software;
  - reportistica e analisi delle performance;
  - gestione degli upgrade dei componenti;
  - utilizzo delle funzionalità avanzate.
- certificazione del costruttore attestante che tutte le componenti installate sono coperte da supporto e manutenzione per tutto il periodo contrattuale individuato dalla gara.

5.3 Tempi di attivazione della fornitura

L'esecutore deve completare l'attivazione della fornitura in termini di apparati, installazione, configurazione, collaudo entro e non oltre i **45 (quarantacinque) giorni solari** dalla stipula del contratto.

5.4 Tempi di erogazione della formazione e dei servizi professionali

Relativamente alla formazione questa dovrà essere erogata entro e non oltre i **60 (sessanta) giorni solari** dalla stipula del contratto, a meno di diversi accordi tra le parti.

5.5 Relazioni con il Committente

Ad aggiudicazione avvenuta e ai fini della stipula del Contratto, l'Esecutore aggiudicatario deve nominare un proprio Referente con compito di interfaccia unica verso il CINECA.
Il Referente dell'Esecutore dovrà relazionarsi con l'Azienda relativamente a tutte le problematiche che il CINECA riterrà non risolte nell'ambito del normale rapporto con l'Esecutore.
Il Referente dell'Esecutore è unico anche nel caso di aggiudicazione ad Associazione temporanea/Consorzio/GEIE, e dovrà farsi carico di gestire la relazione fra le varie imprese partecipanti, fungendo da interfaccia unica verso il CINECA; in questo caso l'Esecutore dovrà illustrare come intende gestire il coordinamento fra le diverse imprese.
Il Referente dell'Esecutore, costituendo il punto di riferimento contrattuale per l'Azienda, parteciperà se richiesto ad incontri regolari con i suoi rappresentanti per l'aggiornamento sullo stato di avanzamento del contratto e per condividere ogni azione correttiva che si rendesse necessaria per il rispetto del contratto. Sarà inoltre responsabile di assicurare al CINECA la disponibilità di tutta la documentazione necessaria per il corretto accesso e utilizzo dei servizi (credenziali di accesso, etc.).
Il Referente dell'Esecutore dovrà possedere caratteristiche professionali di gradimento al CINECA, e lo stesso dovrà fornire, entro la stipula del Contratto, un recapito telefonico, un numero di cellulare ed un riferimento e-mail.

Art. 6. Servizi di manutenzione e assistenza

L'Esecutore deve includere i servizi di manutenzione di seguito descritti per una durata minima di **60 (sessanta) mesi** dalla data di consegna dei materiali oggetto del presente procedimento di gara, senza oneri aggiuntivi a carico di CINECA.
L'Esecutore deve garantire:

- le caratteristiche generali dei servizi di manutenzione e assistenza indicati nel seguito
- l'erogazione delle prestazioni contrattualmente definite per i servizi di manutenzione e assistenza, anche nel caso siano pendenti controversie con CINECA.

6.1 Caratteristiche generali

6.1.1 I servizi devono comprendere le seguenti attività:

- supporto alla risoluzione dei malfunzionamenti a carico di componenti hardware o software (ove previste) dei prodotti forniti;
- invio delle parti sostitutive secondo le SLA più avanti riportate;

- rilascio di aggiornamenti software (firmware, driver, microcodici) per la correzione di bug o l'aggiunta di nuove funzionalità; si precisa che per aggiornamento si intende anche il passaggio ad una nuova versione ("release") del firmware;
- assistenza alla configurazione, tuning e al migliore utilizzo dei prodotti forniti da parte dei tecnici CINECA preposti alla sua gestione.

6.1.2 Il servizio di manutenzione e assistenza si intende "a corpo" e relativo a tutti i prodotti che verranno acquisiti da CINECA nell'ambito della fornitura.

6.1.3 Nel servizio di manutenzione devono essere comprese tutte le attività necessarie ad assicurare gli adeguamenti normativi dei software e delle attrezzature, con riferimento a tutta la normativa europea, nazionale e regionale. Così come i beni compresi nel servizio al suo avvio, anche i beni riparati o sostituiti dovranno essere conformi alle normative vigenti e alla loro evoluzione.

6.1.4 Tutti gli interventi di manutenzione e assistenza devono essere opportunamente documentati. L'Esecutore o suo incaricato è tenuto a prestare la necessaria assistenza tecnica rispettando rigorosamente le condizioni e i tempi di intervento richiesti nel Capitolato.

L'Esecutore risponde della professionalità dei tecnici incaricati.

Il personale tecnico inviato on-site dall'Esecutore o da suo incaricato:

- deve essere dotato, senza oneri aggiuntivi per CINECA, di tutte le strumentazioni necessarie per svolgere in piena autonomia gli interventi che saranno richiesti;
- deve essere dotato, senza oneri aggiuntivi per CINECA, di telefono cellulare in grado di ricevere chiamate e di effettuare le chiamate necessarie a relazionarsi con i colleghi e con il personale dell'Azienda e con altri fornitori;
- deve essere dotato, senza oneri aggiuntivi per CINECA, di mezzi di locomozione adeguati allo svolgimento del servizio.

6.1.5 In relazione al servizio di gestione dei malfunzionamenti si fa presente che l'Esecutore o suo incaricato potrà intervenire secondo le seguenti modalità:

- intervento da remoto per la risoluzione dei malfunzionamenti;
- manutenzione on-site, qualora il malfunzionamento non permetta una correzione attraverso l'intervento da remoto. Le attività di fault management che richiedano intervento diretto dovranno essere concordate con il CINECA.

6.1.6 L'intervento deve garantire il completo ripristino della piena operatività, incluse analisi e diagnosi dei malfunzionamenti, e potrà svolgersi in collaborazione con il personale del CINECA o di altre aziende o personale da essa incaricati, qualora necessario.

La manutenzione ordinaria include tutto l'hardware, con obbligo di sostituzione di qualsiasi parte guasta senza eccezioni, senza alcun onere per CINECA.

Un intervento si intende eseguito soltanto quando siano state ripristinate tutte le funzionalità precedenti l'intervento stesso e le condizioni operative precedenti al guasto siano completamente ristabilite.

Solo in casi adeguatamente motivati da parte dell'Esecutore o suo incaricato sarà possibile adottare soluzioni alternative (per es. in caso di guasti su componenti obsolete non più reperibili sul mercato).

CINECA, qualora lo ritenga opportuno, potrà mettere a disposizione dell'Esecutore o suo incaricato, presso le proprie sedi, uno o più magazzini adatti allo *spare-part* management, secondo modalità che verranno concordate tra le parti.

6.1.7 I servizi di manutenzione e assistenza dovranno essere erogati direttamente da parte dai produttori delle componenti fornite

6.2 SLA dei servizi di manutenzione e assistenza

L'Esecutore dovrà garantire i livelli di servizio di seguito indicati, indipendentemente dal fatto che il servizio sia erogato direttamente, o dai produttori delle varie componenti, o da altre società specializzate in questo tipo di servizi.

6.2.1 Periodo di ricezione e sottomissione delle chiamate: giorni feriali (Lun−Ven) nell'orario 9−18;

6.2.2 Tempo di intervento: l'Esecutore dovrà garantire l'intervento, cioè almeno l'inizio della diagnosi di eventuali malfunzionamenti segnalati da CINECA entro il giorno lavorativo successivo la ricezione della segnalazione. Pertanto, il CINECA dovrà essere ricontattato entro il giorno lavorativo successivo dalla ricezione della segnalazione per iniziare le fasi di *"problem determination"*.

6.2.3 Tempo di sostituzione delle componenti HW: l'Esecutore dovrà garantire la sostituzione delle componenti HW entro almeno il giorno lavorativo successivo alla diagnosi del guasto, con sostituzione delle parti che avvenga in giorni feriali (Lun−Ven) nell'orario 9−18;

6.2.4 Tutti i tempi sopra riportati devono intendersi indipendenti dal numero di disservizi simultanei: in caso di più occorrenze di guasti contemporanei, l'Esecutore dovrà garantire supporto tecnico e logistico e il rispetto delle tempistiche su ogni singolo intervento.

6.3 Call Center per Servizi di Help Desk

Nell'ambito dei servizi di manutenzione e assistenza devono essere disponibili all'attivazione del Contratto uno o più Call Center per il servizio di Help Desk, accessibili mediante uno o più numeri telefonici ed erogati in lingua italiana e/o inglese.

6.3.1 Tali Call Center devono svolgere funzioni di Help Desk riguardo alle seguenti attività:

1. supporto alla risoluzione dei malfunzionamenti a carico di componenti hardware o software dei prodotti oggetto di fornitura;
2. coordinamento dell'invio delle parti sostitutive in caso di guasto;
3. coordinamento dell'invio del tecnico on-site per la sostituzione di parti hardware in caso di guasto;
4. assistenza alla configurazione, al tuning e al migliore utilizzo dei prodotti oggetto di fornitura da parte dei tecnici CINECA preposti alla sua gestione;
5. richieste relative a informazioni sull'utilizzo, funzionalità delle componenti, documentazione.

6.3.2 Per queste funzionalità, i Call Center devono consentire una rapida individuazione della natura della problematica, anche attraverso strumenti di interazione col chiamante (IVR) ovvero operatori di accoglienza della chiamata. L'Esecutore deve garantire la presenza di operatori competenti in tutte le fasce orarie di copertura del servizio. Il Call Center rilascerà un identificativo della chiamata (*ticket*) da utilizzarsi per il tracciamento delle attività e la successiva rendicontazione.

6.3.3 Per ciascun Call Center coinvolto nell'erogazione del servizio, devono essere comunicati al CINECA:

1. Il numero telefonico del Call Center per la ricezione delle chiamate;
2. un eventuale indirizzo e-mail dedicato al servizio di ricezione chiamate;

3. un eventuale sito Web ad accesso riservato dedicato alla apertura e monitoraggio dello stato di avanzamento delle chiamate;
4. procedure per l'effettuazione delle chiamate, comprensive di tutte le informazioni che il CINECA dovrà produrre per accreditare la richiesta di manutenzione o assistenza tecnica.

Casalecchio di Reno (BO), 15 Novembre 2021

Paolo Malfetti
CINECA Consorzio Interuniversitario
Il Responsabile Unico del Procedimento
(Documento firmato digitalmente)