Allegato – Capitolato Tecnico
CIG: 7462641E28

Sommario

1. Introduzione

1.1. *Il progetto "Datacenter Security and Infrastructure services for Registro.it CIG 7462641E28"*

1.1.1. *Oggetto della fornitura*

Oggetto della presente procedura di gara è la fornitura degli apparati di sicurezza e di infrastruttura di switching per data center che andranno a costituire la nuova architettura del data center di Pisa del *Registro. it*.
Si precisa che, date le caratteristiche della fornitura oggetto della gara, l'operatore economico aggiudicatario dovrà garantire la partnership con il produttore per tutta la durata del contratto.

Gli apparati necessari alla realizzazione del progetto sono divisi in tre categorie:

1. ***Apparati Sicurezza Datacenter (tipologia Security-FW): 2 apparati Firewall***
2. ***Apparati per Infrastruttura Datacenter (tipologia DC-Infra): 6 apparati Switch***
3. ***Piattaforma di Gestione (tipologia Gestione): 2 apparati MGT e 2 apparati LOG per un totale di 4 server.***

Oltre alla fornitura dovrà essere previsto il servizio di assistenza specialistica e di manutenzione degli apparati sopra indicati.

1.1.2. *Apparati Sicurezza Datacenter*

Gli apparati per la sicurezza di tipo Security-FW, che indicheremo nel seguito come apparati di tipologia Security-FW, sono adibiti alla realizzazione della sicurezza Edge e Core del Datacenter di Pisa e saranno identificati nel seguito del documento come Security-FW.
Gli apparati per la sicurezza del Datacenter, due in totale, saranno ubicati nel Datacenter del *Registro .it* e forniranno i servizi di sicurezza per i flussi di traffico da e per il Datacenter.
Gli apparati Security-FW saranno installati presso l'Area della Ricerca del CNR di Pisa. Nella Tabella 1 sono specificati i nodi con la relativa nomenclatura e ubicazione

Security-FW	
Nodo L3: NIC-R1	data center di Pisa del Registro .it
Nodo L3: NIC-R2	data center di Pisa del Registro .it

Tabella 1: Apparati Sicurezza Data center

1.1.3. Apparati per Infrastruttura Data center

Gli apparati per l'ampliamento dell'infrastruttura di data center, che indicheremo come apparati di tipologia DC-Infra, oggetto del presente bando, saranno sei in totale. Essi saranno posizionati all'interno del data center e saranno dedicati a raccogliere le connettività dei server esistenti e e degli apparati di instradamento, ponendosi come elemento abilitante all'integrazione dei servizi di sicurezza.

Gli apparati DC-Infra saranno installati presso l'Area della Ricerca del CNR di Pisa. Nella Tabella 2 sono specificati i nodi con la relativa nomenclatura e ubicazione.

DC-Infra	
Nodo L2: NIC-PI-32T-1	Data center di Pisa del Registro .it
Nodo L2: NIC-PI-32T-2	Data center di Pisa del Registro .it
Nodo L2: NIC-PI-32T-3	Data center di Pisa del Registro .it
Nodo L2: NIC-PI-32T-4	Data center di Pisa del Registro .it
Nodo L2: NIC-PI-32T-5	Data center di Pisa del Registro .it
Nodo L2: NIC-PI-32T-6	Data center di Pisa del Registro .it

Tabella 2: Apparati per Infrastruttura DC-Infra

1.1.4. wApparati Piattaforma di Gestione

Gli apparati che costituiscono la piattaforma di Gestione, che indicheremo nel seguito come apparati di tipologia Gestione, oggetto del presente bando, possono essere distinti in due diverse tipologie, per i quali si richiedono dispositivi fisici dedicati:

- funzioni di configurazione, controllo, monitoraggio e allarmistica e controllo dello stato degli apparati oggetto del bando (nodi MGT);
- funzioni di raccolta, analisi, correlazione e reportistica dei log e dei flussi di traffico dell'intera infrastruttura del Registro .it (nodi LOG).

Gli apparati di tipologia Gestione, dedicati ai servizi sopra indicati, saranno installati presso l'Area della Ricerca del CNR di Pisa. Nella Tabella 3 sono specificati i nodi con la relativa nomenclatura e ubicazione.

Apparati MGT e LOG	
Nodo Gestione: MGT-1	Data center di Pisa del Registro .it
Nodo Gestione: MGT-2	Data center di Pisa del Registro .it
Nodo Log: LOG-1	Data center di Pisa del Registro .it
Nodo Log: LOG-2	Datacenter di Pisa del Registro .it

Tabella 3: Apparati per Piattaforma di Gestione .

2. Caratteristiche della fornitura - Requisiti minimi generali

2.1. *Indicazioni generali*

I seguenti punti costituiscono i requisiti minimi e sono quindi vincolanti per la fornitura.
Per ogni punto dovranno essere fornite le specifiche e i dettagli a dimostrazione della conformità alle richieste. La valutazione sarà effettuata sulla documentazione fornita e la mancanza anche di un solo requisito minimo comporterà l'esclusione dalla gara.
È importante sottolineare che, oltre ai requisiti minimi generali di seguito indicati, i requisiti minimi specifici per i singoli apparati, di cui alla fornitura oggetto del bando, sono descritti nei relativi capitoli.

2.1.1. *Unico produttore*

Gli apparati oggetto della fornitura devono essere realizzati tutti dallo stesso produttore al fine di garantire un elevato livello di integrazione tra le componenti ed una efficacia del supporto nel suo insieme: tutte le parti hardware e software della fornitura devono comparire nel listino del produttore senza nessun avviso di uscita di produzione o di termine di manutenzione o supporto specialistico.

2.1.2. *Unico sistema operativo*

Tutti gli apparati di tipologia Security-FW devono essere dotati dello stesso sistema operativo e utilizzare la stessa versione e revisione dello stesso.
Tutti gli apparati di tipologia DC-Infra devono essere dotati dello stesso sistema operativo e utilizzare la stessa versione e revisione dello stesso.

2.1.3. *Omogeneità apparati hardware*

Gli apparati di tipologia Security-FW, all'interno del portafoglio del produttore, devono appartenere alla stessa linea/serie di prodotti.
Gli apparati di tipologia DC-Infra, all'interno del portafoglio del produttore, devono appartenere alla stessa linea/serie di prodotti.

2.1.4. *Vincoli progettuali*

Tutti gli apparati delle tipologie Security-FW e DC-Infra devono soddisfare i seguenti requisiti architetturali necessari ad ottemperare le richieste prestazionali e di alta disponibilità. Per completezza si riportano le definizioni dei concetti e dei termini utilizzati:

- Piano di controllo (Control plane) - L'insieme delle funzioni preposte alla definizione delle informazioni che un apparato utilizza per l'inoltro dei pacchetti di dati. È rappresentato dalle istanze dei protocolli di routing con la struttura dati derivante: Routing Information Base (RIB);
- Piano di inoltro (Forwarding/data plane) - L'insieme delle funzioni e delle informazioni, derivate dal piano di controllo, atte all'inoltro dei pacchetti di dati è rappresentata dalla Forwarding Information Base (FIB) per le operazioni di routing e switching.

2.1.4.1.Separazione dei piani di controllo e di inoltro

È richiesta la separazione dei piani di controllo e di inoltro al fine di avere l'ottimizzazione delle strutture dati, dei processori e delle componenti hardware e software nel complesso, in funzione delle prestazioni richieste (tipicamente relative a operazioni di aggiornamento e modifica, da parte del control plane, e operazioni time-critical, come "table lookup" e "multi-field classification packet processing", da parte del forwarding plane).
Tale separazione, implicando il disaccoppiamento anche fisico delle parti hardware e software preposte alle due funzioni, garantisce inoltre che il malfunzionamento dell'uno non impatti sull'altro.

2.1.4.2.Architettura a forwarding distribuito (distributed forwarding)

È richiesta un'architettura di tipo "distributed forwarding", che consente ad un apparato di mantenere le informazioni di inoltro, pertinenti alla funzione dell'apparato nello stack OSI

(comprese le politiche di filtraggio e di trattamento differenziato del traffico), sui moduli di I/O (line cards) e/o, in generale, sui moduli preposti al forwarding.

2.1.4.3.Metodologie per la valutazione delle prestazioni

Gli apparati interessati da questa funzionalità sono appartenenti alla tipologia Security-FW e DC-Infra.

Per la valutazione delle performance degli apparati ci si avvale delle metodologie e delle definizioni standard proposte nell'ambito del "Benchmarking Methodology Working Group (BMWG)" IETF: 2544 (IPv4), 2889 (LAN switch), 3918 (Multicast), 5180 (IPv6), 5695 (IP/MPLS) e 3511 (Firewall).

Nella documentazione fornita dovrà essere specificato se i dati di throughput sono al netto dei 20 Byte di overhead dovuti al preambolo e allo "inter-packet gap".

Nei dati di performance dichiarati il throughput massimo di sistema deve essere al netto dell'overhead introdotto per lo switching interno all'apparato (non deve quindi essere utilizzato il dato relativo al "raw bitrate").

3. Apparati tipologia Security-FW - Requisiti minimi

Costituiscono requisito minimo e quindi sono condizioni vincolanti per la fornitura, pena l'esclusione dalla gara, le seguenti prestazioni funzionali.

3.1. *Servizi di Sicurezza*

3.1.1. *Firewall Stateful inspection*

Gli apparati devono tenere traccia dello stato delle connessioni da e per il DC e devono poter riconoscere i pacchetti che appartengono alle connessioni attive.

3.1.2. *Network Address Translation*

Gli apparati devono supportare i seguenti tipi di Network Address Translation (NAT):

- Destination;
- Source;
- Static;
- Persistent NAT;
- IPv6 address translation.

3.1.3. *Funzionalità IPsec VPN*

Gli apparati devono supportare le seguenti caratteristiche per VPN IPsec:

- Supporto per architetture del tipo: Site-to-Site, Hub/Spoke, Hub/Spoke e on-demand Spoke-to-Spoke, Full Mesh;
- Algoritmi di cifratura: DES, 3DES, AES-128, AES-192, AES-256;
- Algoritmi di autenticazione: MD5, SHA-1, SHA-128, SHA-256 ;
- Protocolli SA: manual key, IKEv1, IKEv2, PKI (X.509);
- Perfect forward secrecy (DH groups): 1, 2, 5,14;
- Replay attack prevention;
- Redundant VPN gateways;
- Tunneling di tipo IP-Sec, IP-IP and GRE (Generic Routing Encapsulation);
- Supporto del routing dinamico (BGP, OSPF) all'interno dei tunnel per lo scambio delle informazioni di routing tra i vari peer;
- Supporto meccanismi di cifratura e accelerazione in hardware;
- Supporto di soluzioni di Accesso Remoto attraverso l'utilizzo di un client in grado di gestire connessioni VPN sia con protocollo IPsec che SSL.

3.1.4. *Intrusion Prevention System (IPS)*

Gli apparati devono supportare le seguenti funzionalità di IPS:

- Meccanismo di rilevazione degli attacchi: Stateful signatures, protocol anomaly detection e application identification;
- Meccanismi di risposta agli attacchi: drop connection, close connection, session packet log e session summary;
- Meccanismi di notifica degli attacchi: possibilità di inviare ad un server remoto (syslog server) i log generati dall'analisi IDP;
- Protezione contro la proliferazione dei sistemi infetti con integrazione automatica con sistemi SIEM;
- Possibilità di realizzare signature personalizzate;
- Frequenza degli aggiornamenti giornaliera, cosí da essere sempre up-to-date con gli aggiornamenti che il produttore mette a disposizione;
- Applicazione della funzione di Packet capture alle regole di IPS.

3.1.5. *Controllo Applicativo*

Gli apparati devono permettere l'identificazione e il controllo delle applicazioni (layer 7) che transitano da e per il DC. In particolare devono supportare:

- Visibilità applicativa: analisi dettagliata sull'utilizzo delle applicazioni in termini di bytes, pacchetti e sessioni;
- Controllo delle applicazioni: specifico controllo sui flussi applicativi per permettere o negare il traffico di una o di un gruppo di applicazioni;
- QoS a livello applicativo: prioritizzazione del traffico in base all'applicazione e al suo contesto;
- Advanced Policy-Base Routing: possibilità di scelta del percorso di routing in base alla applicazione identificata;
- SSL Proxy: possibilità di decifrare il traffico SSL in entrambe le direzioni per il controllo e la visibilità delle applicazioni che utilizzano il protocollo SSL, utilizzando meccanismi in grado di discriminare le sessioni a cui applicare l'inspection.

3.1.6. Funzionalità Unified Threat Management (UTM)

Gli apparati devono supportare le seguenti funzionalità UTM:

- Antivirus: deve poter identificare spyware, adware, viruses, keyloggers e altri malware per i protocolli http, POP3, SMTP, IMAP e FTP;
- Web Filtering: categorizzazione e controllo del traffico Web. La soluzione deve poter discriminare tra traffico permesso e vietato in base alla categorizzazione;
- Content filtering: filtraggio dei contenuti in base a MIME type ed estensione del file;
- Protezione Worm: signature che rilevano il traffico generato dai sistemi compromessi da Worm o il loro transito sulla rete;
- Protezione dai Trojan: rilevazione del traffico generato dai sistemi compressi da Trojan o il loro transito sulla rete;
- Protezione da Spyware, Adware e Keylogger: rilevazione del traffico generato dai software elencati o rilevazione del loro transito sulla rete.

3.1.7. Servizi di sicurezza avanzati

Gli apparati devono supportare le seguenti funzionalità contro minacce di tipo "zero-day":

- Protezione contro le Botnet tramite il monitoraggio delle comunicazioni di tipologia Command&Control;
- Protezione contro gli zero-day attack utilizzando tecnologie di macchine learning analisys per i file trasferiti utilizzando i protocolli HTTP, HTTPS, SMTP e IMAP;
- Possibilità di filtraggio dei flussi in ingresso e uscita utilizzando regole di geolocalizzazione IP;
- Supporto di REST API per l'integrazione con altri componenti/produttori e per lo scambio delle informazioni (feeds).

3.1.8. Architettura di Sicurezza Integrata

La soluzione deve potersi interfacciare con l'architettura di rete e sicurezza già presente presso il Registro .it. In particolare, deve supportare le seguenti funzionalità:

- Third-party Log Integration: supporto per l'integrazione con i sistemi di logging di altri dispositivi/applicazioni.;
- Automatic Remediation: supporto per l'applicazione di regole dinamiche per il blocco dei flussi di traffico in base agli eventi gestiti dal Log Manager. Il processo di Automatic Remediation deve essere aperto e deve potersi integrare con dispositivi/applicazioni di altri produttori;
- Disponibilità di meccanismi di protezione contro attacchi DOS, in particolare protezione contro attacchi del tipo: ICMP/UDP/TCP flood, TCP syn attack, ICMP/UDP/TCP sweep.

3.1.9. Public Key Infrastructure (PKI)

È richiesto che gli apparati supportino le seguenti funzionalità di PKI:

- PKI certificate requests (PKCS#7);
- Automated certificate enrollment (SCEP);
- Supporto alle Autorità di Certificazione;

- Certificati Self-signed.

3.1.10. Funzioni Logiche Routing/Switching

È richiesto che gli apparati supportino i seguenti sistemi di virtualizzazione:

- Supporto per istanze virtuali di routing e zone di sicurezza;
- Supporto per interfacce logiche con separazione del traffico tramite 802.1q.

3.2. *Servizi di rete*

3.2.1. Funzionalità IPv6

È richiesto che gli apparati supportino le seguenti funzioni IPv6:

- Firewall stateful e stateless filters;
- Dual stack IPv4/IPv6 firewall;
- RIPng;
- BGP;
- BFD;
- ICMPv6;
- OSPFv3;
- CoS;
- Supporto VPN IPsec per tunnel IPv6.

3.2.2. Qualità del Servizio (QoS)

È richiesto che gli apparati supportino le seguenti funzioni di qualità del servizio per la prioritizzazione del traffico:

- Classificazione del traffico;
- Possibilità di configurare soglie di traffico per protocollo
- Configurazione di banda massima per servizio e/o applicazione e/o indirizzo IP;
- Configurazione di banda massima per singolo indirizzo IP;
- RFC 2474 IP DiffServ in IPv4;
- Configurazione di filtri per determinare la Class of Service (CoS);
- Politiche di scheduling in base al COS;
- Politiche di shaping in base al COS;
- Prioritizzazione dei protocolli di routing dinamico.

È richiesto che gli apparati supportino le regole di QoS a livello applicativo (layer 7). Le regole devono permettere di assegnare un valore nel campo DSCP in base al traffico applicativo al fine di applicare le politiche di CoS, sia sull'apparato che rappresenta il punto di ingresso al dominio di QoS che nel resto dell'architettura di rete.

3.2.3. Policing and Scheduling

È richiesto che gli apparati supportino le seguenti funzioni:

- Supporto per classificazione 802.1p, DiffServ code point (DSCP) ed EXP;
- Classificazione del traffico in base a VLAN, data-link connection identifier (DLCI), interfacce, interfacce logiche e filtri multicampo layer3/4;
- Supporto per il rewrite 802.1p, DSCP ed EXP;
- Supporto per policy per banda massima e garantita.

3.2.4. Modalità Operative

Gli apparati devono supportare le seguenti modalità operative:

- Layer 2 Stateful: modalità trasparente L2;
- Layer 3 Stateful: modalità routed L3;
- Layer2/Layer3 Stateful: modalità mixed trasparente/routed;
- Packet mode: possibilità di disabilitare la funzione Stateful per l'intero apparato.

3.2.5. Routing

Gli apparati devono supportare i seguenti protocolli e funzionalità di routing:

- BGP;
- IS/IS;
- OSPF;
- RIP v1/v2;
- Static routes;
- Source-based routing;
- Policy-based routing;
- Application Policy-based routing;
- Equal cost multipath (ECMP);
- Reverse path forwarding (RPF);
- Multicast.

Deve inoltre essere garantito il supporto alle estensioni di Graceful Restart (GR) relative ai protocolli di routing: OSPF, BGP e IS-IS.

3.2.6. Alta Affidabilità

L'architettura deve prevedere la ridondanza dei servizi, sui due nodi, per assicurare l'alta affidabilità dei servizi stessi. I servizi non devono essere impattati nel caso di guasto di un nodo o di un aggiornamento dell'architettura stessa. Devono essere supportate le seguenti funzionalità:

- Modalità operative tra i nodi: attivo/passivo, attivo/attivo;
- Sincronizzazione delle configurazioni;
- Sincronizzazione delle sessioni;
- Failover del traffico tra i nodi senza perdita di servizio;
- Identificazione di possibili guasti hardware su un nodo ed eventuale failover del traffico;
- Identificazione di eventuali guasti sui link di upstream ed eventuale failover del traffico;
- Supporto LACP sia sul singolo nodo che tra i due nodi;
- Possibilità di riavviare i singoli processi a "runtime".

3.2.7. Aggiornamento Software

Gli apparati devono supportare i seguenti meccanismi e funzionalità durante l'aggiornamento del software:

- Processo di aggiornamento dei componenti del Cluster che non causi il riavvio contemporaneo di tutte le unità del Cluster stesso ma il riavvio selettivo di ogni singolo componente.

3.2.8. Dynamic Host Configuration Protocol (DHCP)

Gli apparati devono supportare le seguenti funzionalità DHCP:

- DHCP Server;
- DHCP Relay.

3.2.9. Monitoraggio e Logging

Gli apparati devono supportare i seguenti protocolli di monitoraggio e logging:

- SNMP v2 e v3, trap ed inform;
- Structured Syslog;
- Debugging: il livello di dettaglio delle attività di debug deve poter essere configurabile così come il suo output (file, CLI ...) e il livello di debug non deve avere impatto sulle prestazioni dell'apparato.

3.2.10. Management

Gli apparati devono supportare i seguenti sistemi di management:

- Interfaccia Web per l'amministrazione del singolo nodo o del cluster;
- Interfaccia CLI per l'amministrazione del singolo nodo o del cluster;
- Interfaccia NETCONF per integrazione con sistemi di automazione;
- Console centralizzata per gestire sia i singoli nodi, sia più di un cluster.

3.3. *Sistema Operativo e Strumenti di Monitoraggio*

3.3.1. *Architettura sistema Operativo (OS)*

3.3.1.1.Caratteristiche sistema

È richiesto che il sistema operativo degli apparati proposti possegga le seguenti proprietà:

- Sistema operativo di rete e sicurezza ad architettura modulare;
- Multitasking;
- Multiutente.

3.3.1.2.Gestione Ridondanza

Gli apparati Security-FW devono essere dotati di meccanismi e di processi per la gestione della sincronizzazione degli stati logici e dei processi distribuiti su elementi fisicamente distinti dell'architettura.

3.3.2. *Amministrazione Sistema Operativo e configurazioni*

3.3.2.1.Amministrazione sistema, utenti e sicurezza

È richiesto che il sistema operativo sia dotato delle seguenti funzionalità:

- Interfaccia utente (shell) con comandi per system administration, file manipulation, system monitoring e troubleshooting;
- Client: Telnet e SSHv2;
- Protocolli AAA quali Radius e TACACS+ con fallback su database utenti locale al nodo;
- Definizione di profili;
- Gestione di utenti e gruppi;
- Gestione dei permessi con granularità a livello di singolo comando e regex;
- Registrazione (logging) di tutte le informazioni rilevanti circa le possibili anomalie riguardanti la sicurezza.

3.3.2.2.Amministrazione delle Configurazioni

È richiesto che il sistema operativo sia dotato delle seguenti funzionalità:

- Interfaccia utente (shell) con ambiente separato per la modifica delle configurazioni (e.g. configuration mode);
- Accesso e modifica per utenti concorrenti con possibilità di modifica esclusiva ("lock" su tutta o su parte della configurazione);
- Possibilità di modifica di più configurazioni con funzione di confronto (analogamente al comando unix "diff"), funzione di controllo sintattico e semantico delle stesse prima della loro operatività;
- Salvataggio automatico delle configurazioni e backup su un server remoto e accessibile anche localmente tramite la shell utente "Command Line Interface" (CLI);
-

4. Apparati tipologia DC-Infra - Requisiti minimi

Costituiscono requisito minimo e quindi sono condizioni vincolanti per la fornitura, pena l'esclusione dalla gara, le seguenti prestazioni funzionali.

4.1. *Vincoli progettuali*

4.1.1. *Piattaforma non bloccante (wire speed o, equivalentemente, non-blocking).*

È richiesto che gli apparati abbiano la capacità di:

- operare le decisioni di filtering e forwarding del traffico in condizioni di massimo carico su tutte le porte di I/O simultaneamente;
- distribuire arbitrariamente la totalità delle capacità delle porte di I/O tra tutte le porte dell'apparato.

Affinché la piattaforma sia wire speed (non-blocking) le prestazioni di table lookup performance (1) e data flow capacity (2) devono essere entrambe rispettate in assenza di perdita di pacchetti.

4.1.2. *Architettura distribuita (Stack)*

È richiesto che l'architettura proposta sia tale per cui gli apparati possano agire come un unico dispositivo logico con il Control Plane e i File di Configurazione unificati e con un'unica immagine di sistema operativo che opera su tutti gli apparati. Nello stesso tempo l'architettura deve fornire dei meccanismi di ridondanza di Control Plane e Management Plane (es. Master/Backup), meccanismi di resilienza per la gestione del Forwarding Plane e la convergenza in caso di eventuali link failure.
L'obiettivo principale è la fornitura di un'architettura Datacenter costituita da un unico livello topologico e quindi da un unico apparato a livello logico, atta ad ottimizzare l'inoltro del traffico tra le diverse utenze afferenti.
Un altro obiettivo di questa architettura sarà quella di evitare l'uso di protocolli che inibiscano l'occupazione di tutta la banda disponibile, quali per esempio lo Spanning Tree.
Suddetta architettura sarà denominata, d'ora in avanti, di tipo Stack.

4.1.3. *Line rate packet forwarding*

L'esecuzione dei compiti di packet forwarding all'interno di un apparato, che lavora a line rate, implica che tale operazione sia implementata con dei network processor ottimizzati per tali funzioni e dotati di hardware dedicato[1] alle operazioni di table lookup, pattern matching e header rewriting.
La latenza introdotta dalla catena di processing dei pacchetti deve essere quindi trascurabile, nei limiti dello stato dell'arte dei sistemi per il packet forwarding di categoria carrier-class attuali, rispetto alla latenza teorica dell'apparato al layer OSI al quale esso opera.

4.1.4. *Line rate packet processing*

Oltre alle funzioni di packet forwarding, implementate a line rate per gli apparati DC-Infra, si includono nel fast path dell'apparato le funzioni di multi-field classification, filtering, metering e policing tipiche delle esigenze di traffic management e security degli operatori di rete.
Le attività di packet classification, filtering e policing in ambiente misto IPv4 ed IPv6, configurate in aggiunta alle operazioni di inoltro di protocolli non proprietari, non devono introdurre latenze che impattino sul throughput dichiarato dell'apparato e delle sue interfacce di rete.

4.2. *Funzionalità di Stacking*

Non sono accettati meccanismi di stacking che permettano di offrire servizi di ridondanza a livello 3 e che garantiscano la disponibilità delle capacità di forwarding dei pacchetti all'interno dell'intero stack mediante protocolli standard in modalità attivo/passivo o proprietari in modalità attivo/attivo.

4.3. *Modularità Stack*

---

1 Senza entrare nell'ambito progettuale dei sistemi adibiti alla funzione di Packet Forwarding, dei meccanismi di parallelizzazione e di multithreading dei processori utilizzati, qui si intende la dotazione interna al processore in termini di componenti hardware per task specifici (ASIC, CAM, TCAM...).

È richiesto che l'architettura di stacking preveda la possibilità di interconnettere in stack almeno 10 apparati per la tipologia DC-Infra. Nel complesso l'architettura offerta dovrà essere in grado di supportare almeno 400 porte alla velocità di 10GbE (in grado di supportare connettività in fibra SFP+, DAC o rame RJ45) e, in aggiunta, almeno 20 porte dedicate alla definizione dello stack mediante interconnessioni locali, ognuna con capacità superiore a 50Gbps.

4.3.1. *Connettività Stack*

Le connessioni fisiche per la realizzazione dello stack devono potere essere implementate sia attraverso connessioni locali, utilizzando interfacce proprietarie dedicate, sia attraverso connessioni geografiche con interfacce ottiche standard 10 Giga SFP+ e 1 Giga SFP, supportando e rispettando i vincoli di distanza indicati nelle specifiche delle ottiche stesse. Queste due modalità di connessione devono poter convivere contemporaneamente. Di seguito il dettaglio delle ottiche standard richieste per poter implementare l'interconnessione geografica degli apparati in stack:

- 1GE-SX (fino a 550m con fibra MMF OM2);
- 1GE-LX (fino a 10km con fibra SMF);
- 10GE-USR (fino a 100m con fibra MMF OM3);
- 10GE-SR (fino a 400m con fibra MMF OM4);
- 10GE-LRM (300m con fibra SMF);
- 10GE-LR (fino a 10 km con fibra SMF);
- 10GE-ER (fino a 40 km con fibra SMF);
- 10GE-ZR (fino a 80 km con fibra SMF);
- 10GE-DAC 1m/3m/5m/7m (10-Gbps full-duplex serial transmission).

4.3.2. *Forwarding distribuito*

All'interno dello stesso stack, deve essere possibile inoltrare il traffico tra porte appartenenti allo stesso apparato e tra porte appartenenti ad apparati diversi senza che il forwarding del traffico richieda interventi e, più in generale, risorse computazionali dell'apparato su cui risiedono le funzionalità di controllo del piano di routing e/o forwarding.

4.4. *Sistema Operativo e Strumenti di Monitoraggio*

4.4.1. *Architettura Sistema Operativo*

4.4.1.1.Caratteristiche sistema

È richiesto che il sistema operativo degli apparati proposti abbia le seguenti proprietà:

- Sistema operativo di rete ad architettura modulare, dove ogni modulo è in grado di processare in maniera indipendente specifiche risorse e di eseguirle all'interno di un segmento di memoria protetto e che non può andare in conflitto con le altre risorse del sistema;
- Multitasking;
- Multiutente.

4.4.1.2.Gestione ridondanza

È richiesto che il sistema operativo degli apparati sia dotato di meccanismi e di processi per la gestione della sincronizzazione degli stati tra due kernel in configurazione fisicamente ridondata (propedeutici ai meccanismi di switchover tra l'unità master e l'unità backup). Per configurazione fisicamente ridondata si intende un sistema costituito da almeno due apparati (unità master e unità backup) appartenenti al medesimo stack con funzionalità centralizzate di Route Processor e Control Board.

4.4.2. *Amministrazione Sistema Operativo e configurazioni*

4.4.2.1.Amministrazione sistema, utenti e sicurezza

È richiesto che il sistema operativo sia dotato delle seguenti funzionalità:

- Interfaccia utente (shell) con comandi per system administration, file manipulation, system monitoring e troubleshooting;

- Client: Telnet e SSHv2;
- AAA Radius e TACACS+ con fallback su database utenti locale al nodo;
- MAC Radius authentication;
- Definizione di profili;
- Gestione di utenti e gruppi;
- Registrazione (logging) di tutte le informazioni rilevanti circa le possibili anomalie riguardanti la sicurezza;
- Supporto di un meccanismo per filtrare e limitare il traffico destinato al "Piano di Controllo" dell'apparato.

4.4.2.2.Amministrazione delle Configurazioni

È richiesto che il sistema operativo sia dotato delle seguenti funzionalità:

- Interfaccia utente (shell) con ambiente separato per la modifica delle configurazioni (e.g. configuration mode);
- Accesso e modifica per utenti concorrenti con possibilità di modifica esclusiva ("lock" su tutta o su parte della configurazione);
- Possibilità di modifica di più configurazioni con funzione di confronto (analogamente al comando unix "diff") delle stesse prima della loro operatività;
- Log con inoltro del flusso dati su un server remoto tramite protocollo Syslog ed accessibile anche localmente tramite la shell utente (CLI - Command Line Interface);
- Linguaggio di scripting: con possibilità di sviluppo di script locali sul nodo per la personalizzazione di comandi, per la schedulazione automatica di modifiche di elementi di configurazione.

4.4.3. *Alta affidabilità*

- I dispositivi offerti devono essere predisposti allo stacking ed implementare le funzioni centralizzate di Route Processor e Control Board su almeno due apparati fisicamente distinti (unità master e unità backup) e in configurazione ad alta disponibilità. Per maggiori dettagli tecnici sull'architettura si consulti il capitolo "Architettura e dotazione hardware - Requisiti minimi (Cap.6)";
- I dispositivi offerti devono supportare la funzionalità di Failover/Switchover: lo switchover tra gli apparati dedicati al Piano di Controllo e di Gestione Centralizzato (Master/Backup) deve essere completamente trasparente al resto degli apparati dello stack;
- Disponibilità di un processo di aggiornamento unificato per gli apparati dello Stack che non causi il riavvio contemporaneo di tutti gli apparati che compongono lo Stack stesso ma il riavvio selettivo e sequenzialedi ogni singola unità. Tale processo deve garantire la continuità del Piano di Controllo attraverso meccanismi in grado di preservare le informazioni e gli stati generati dai protocolli di routing e dal kernel;
- Possibilità di riavviare i singoli processi a "runtime" (Process Restart);
- Supporto di un meccanismo di gestione dello stack che eviti, in caso di guasti, la generazione di un split dello stack stesso e la duplicazione del Piano di Controllo e di Gestione;
- L'interfaccia appartenente ad un LAG, condiviso tra una unità che sta effettuando il reboot ed una unità attiva, deve mantenere attivo il processo di forwarding;
- La procedura di aggiornamento dei dispositivi che compongono lo Stack deve permettere la convivenza momentanea di unità con release di sistema operativo diverse, senza alcuna interruzione del processo di forwarding dei pacchetti sulle unità che non sono coinvolte nella procedura di reboot.

4.4.4. *Monitoraggio, amministrazione e gestione (OA&M)*

4.4.4.1.Strumenti di controllo

È richiesto che il sistema operativo sia dotato delle seguenti funzionalità:

- Comandi ICMP: ping, traceroute;
- Supporto SNMPv2 e v3, SNMP Trap e SNMP Inform. In particolare è richiesto il supporto delle "Management Information Base" (MIB) previste dagli standard IETF e IEEE e delle relative estensioni proprietarie;
- Debugging: il livello di dettaglio delle attività di debug deve poter essere configurabile così come il suo output (file, CLI...) e il livello di debug non deve avere impatto sulle prestazioni dell'apparato.

4.4.4.2.Traffic Mirroring e Sampling

È richiesto che il sistema operativo supporti le funzionalità di mirroring del traffico e dei protocolli della famiglia sFlow o equivalenti. Le operazioni di campionamento del traffico devono poter avvenire in tempo reale e senza degrado delle prestazioni.

4.4.4.3.Strumenti di OA&M

Gli apparati devono prevedere strumenti (anche attraverso l'uso di MIB SNMP proprietarie) per la misura, in tempo reale, di parametri prestazionali di rete quali: delay, jitter e packet loss;
Gli apparati devono supportare il protocollo "Bidirectional Forwarding Detection" (BFD) almeno per i protocolli OSPF, BGP, IS-IS, RIP.

4.5. *Funzionalità layer2 OSI*

4.5.1. *LLDP*

Gli apparati devono supportare i protocolli Link Layer Discovery Protocol (LLDP) e LLDP-MED (Media Endpoint Discovery).

4.5.2. *MTU*

Gli apparati devono supportare l'invio di trame Ethernet con payload di dimensione superiore ai 1500 Byte. In particolare il payload deve raggiungere i 9000 Byte.

4.5.3. *Data center Bridging (DCB)*

Gli apparati devono rispettare lo standard IEEE DCB per fornire funzionalità di FCoE Transit Switch.

4.5.4. *Routing & Bridging congiunto*

Sugli apparati devono essere supportate interfacce con funzionalità di layer2 configurabili con VLAN tag. Le singole porte devono poter essere configurate sia in "access mode" sia in "802.1Q trunking mode".
È richiesto il supporto di layer2 bridging e di layer3 routing sulla stessa interfaccia. Le trame Ethernet devono essere trattate a livello 2 se non sono inviate al MAC address dello switch. Le trame Ethernet devono essere trattate a livello 3 e quindi ruotate alle altre interfacce di livello 3, laddove inoltrate al MAC address dello switch su cui sono abilitate le funzionalità di livello 3.

4.5.5. *Spanning Tree Protocols*

Gli apparati devono supportare tutti i protocolli standard IEEE di tipo Spanning Tree Protocols (xSTP). In particolare devono essere implementate tutte le evoluzioni in accordo con gli standard IEEE 802.1D (Spanning Tree Protocol), IEEE802.1s (Multiple Spanning Tree Protocol), IEEE 802.1w (Rapid Spanning Tree Protocol) e VSTP (Vlan Spanning Tree Protocol).

4.5.6. *802.1Q - Virtual LANs e CoS*

Gli apparati devono gestire VLAN ID e le funzionalità di vlan tagging in accordo con la raccomandazione IEEE 802.1Q senza alcuna limitazione.
Gli apparati devono avere la capacità di trasportare sui LAG sia traffico di tipo untagged che traffico di tipo tagged 802.1Q (Tagged ports support in LAG).
Gli apparati devono gestire CoS in accordo con la raccomandazione IEEE 802.1p marking.

4.5.7. *Link Aggregation*

Gli apparati devono supportare la funzionalità di link aggregation in accordo con lo standard IEEE 802.3ad e garantire un numero di link aggregation group (LAG) non inferiore a 110 in modalità stack. Inoltre il numero di membri per singolo LAG deve scalare fino ad 8. È richiesto inoltre il

supporto della funzionalità di Link Aggregation Control Protocol (LACP). Deve essere possibile realizzare aggregati di porte 1GbE o 10GbE sia tra porte dello stesso nodo, che tra porte appartenenti a nodi diversi dello Stack.
La configurazione degli aggregati non deve avere alcun impatto sulle prestazioni individuali e complessive dei nodi in termini di throughput e di funzionalità.
Il sistema deve disporre di meccanismi di bilanciamento del traffico (load balancing) all'interno di un link aggregato, sia se formato staticamente che se formato dinamicamente utilizzando LACP.

4.5.8. Port authentication

Il sistema deve implementare, in modo esaustivo, le raccomandazioni per il "Port-based Network Access Control" (PNAC) secondo lo standard IEEE 802.1X. È richiesto il supporto per i seguenti metodi di autenticazione:

- protocollo 802.1X e framework di autenticazione EAP;
- "MAC Authentication";
- autenticazione tramite "Captive Portal".

Deve essere inoltre supportata l'autenticazione concorrente di utenti multipli per singola porta di rete e deve essere possibile l'utilizzo dei tre metodi di autenticazione (sopra descritti) sulla stessa porta di rete.
Si deve fornire il supporto di "RADIUS authentication" (RFC 2138), "RADIUS Extensible Authentication Protocol (EAP) support for 802.1X" (RFC 3579) e "Dynamic authorization extensions to RADIUS" (RFC 5176).
Si deve fornire il supporto di "RADIUS Accounting" come da RFC 2139 e, in particolare, devono essere supportati i seguenti stati e attributi:

- Tipologia Accounting Status Type:
    - Accounting Start;
    - Accounting Stop;
- Attributi Radius richiesti:
    - User-Name;
    - NAS-Port;
    - Framed-IP-Address;
    - Filter-ID;
    - Framed-MTU;
    - Client-System-Name;
    - Session-Timeout;
    - Idle-Timeout;
    - Called-Station-ID;
    - Calling-Station-ID;
    - NAS-Identifier;
    - Acct-Status-Type
    - Acct-Session-Id;
    - Acct-Authentic;
    - Event-Timestamp;
    - NAS-Port-ID.

4.5.9. Edge Virtual Bridging

Deve essere possibile implementare la funzionalità di Edge Virtual Bridging che permette a diverse virtual machine di comunicare tra loro e con host esterni utilizzando l'infrastruttura sottostante. I server che utilizzano il protocollo VEPA (Virtual Ethernet Port Aggregator) inviano i pacchetti da una virtual machine ad un altra utilizzando un virtual bridge presente su uno switch adiacente. La funzionalità di Edge Virtual Bridging permette di ricevere i pacchetti sulla stessa interfaccia dalla quale sono stati inoltrati.

4.6. *Funzionalità di Routing IPv4 e IPv6*

4.6.1. DHCP

Gli apparati devono supportare le seguenti funzionalità DHCP:

- DHCP server;
- DHCP relay (configurabili per interfaccia e per VLAN).

4.6.2. Routing IP

Gli apparati devono supportare le funzionalità di indirizzamento, routing e forwarding dei pacchetti IP, unicast e multicast, in conformità alle specifiche di Classless Routing con Variable Length Subnet Masking e agli standard IETF rilevanti.
Gli apparati devono supportare la configurazione del routing statico (static routes) di una default route e il routing dinamico tramite le famiglie di protocolli EGP e IGP.
È richiesto il supporto dei protocolli BGP, IS-IS, OSPFv2.
Gli apparati devono permettere la configurazione della ridistribuzione delle informazioni di routing tra differenti protocolli con la possibilità di applicare filtri per la selezione delle rotte.
Gli apparati devono supportare funzionalità di filtering delle rotte dai processi EGP/IGP alle tabelle di routing.
Gli apparati devono supportare la configurazione di equal cost multipath ECMP per le rotte.
Le funzionalità specificate nei paragrafi seguenti sono previste, anche se non esplicitamente citate, in conformità agli standard IEEE e IETF.
Nel caso in cui la conformità agli standard richiesti non sia completa, o non sia contemplata l'aderenza a particolari funzionalità avanzate incluse nello standard, se ne dettaglino le motivazioni.

4.6.2.1.RIP

Gli apparati devono supportare i protocolli di routing RIPv2, secondo lo standard RFC 2453, e RIPv1, secondo lo standard RFC 1058.

4.6.2.2.OSPF

Gli apparati devono supportare gli standard OSPFv2 (RFC 2328) con le estensioni OSPF NSSA Option (RFC 1587) e "OSPF Opaque LSA Option" (RFC 2370).

4.6.2.3.IS-IS

Gli apparati devono supportare il protocollo di routing Intermediate System to Intermediate System (IS-IS).

4.6.2.4.BGP

Gli apparati devono supportare il protocollo di routing Border Gateway Protocol (BGP).

4.6.3. Routing Multicast

Gli apparati devono supportare i protocolli Protocol Independent Multicast - Sparse Mode (PIM-SM), Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) e Protocol Independent Multicast - Dense Mode (PIM-DM).
Si deve fornire il supporto dei protocolli IGMPv1(RFC 1112), IGMPv2(RFC 2236), IGMPv3(RFC 3376) e delle relative funzionalità di Snooping per IGMP v1, v2 e v3.
Gli apparati devono supportare i meccanismi configurabili di filtering IGMP.

4.6.4. Policy Routing

Gli apparati devono supportare il "Policy Based Routing": consentire l'instradamento del traffico alterando il processo decisionale standard, previsto dallo specifico protocollo, basandosi quindi su policy configurate dall'amministratore dei sistemi.

4.6.5. Virtual Routing e Forwarding

Gli apparati devono supportare le funzionalità di "Virtual routing and forwarding" (VRF), comunemente denominate VRF-lite.

4.6.6. Funzionalità IPv6

Gli apparati devono supportare i seguenti protocolli IPv6, eventualmente soggetti a licenza di attivazione:

- OSPFv3
- BGP IPv6;
- IS-IS IPv6;
- RIPng;
- DHCPv6 server/relay;
- IPv6 PIM; IPv6 MLDv1/v2;
- VRRP IPv6;
- NDP (RFC 4861).

4.6.7. Funzionalità MPLS

Gli apparati devono supportare le seguenti funzionalità MPLS:

- Label-switching router (LSR);
- RSVP, RSVP-TE;
- LDP tunneling over RSVP;
- Layer3 VPN;
- Static LSPs;
- BGP L2 VPN;
- Circuit Cross Connect.

4.7. *Amministrazione, gestione (OA&M), protezione e sicurezza*

Gli apparati devono implementare una suite di protocolli e meccanismi di monitoraggio e controllo per la rilevazione e la gestione dei guasti, dei malfunzionamenti e delle anomalie. Tali meccanismi, oltre a fornire strumenti per il monitoraggio delle performance, devono collaborare in maniera strutturata con i meccanismi automatici di protezione e recovery ad ogni livello del modello di riferimento OSI.

4.7.1. Layer2: Ethernet

Gli apparati devono supportare meccanismi di storm control per traffico unicast, broadcast e multicast.

Sono inoltre richieste funzionalità layer2 per la gestione e il controllo dei MAC address a livello di porta e la possibilità di mantenere elementi in modo permanente (persistent MAC learning).

4.7.2. Layer3: IP

Gli apparati devono supportare il Virtual Router Redundancy Protocol (VRRP) secondo lo standard RFC 2338.

Gli apparati devono supportare il protocollo Bidirectional Forwarding Detection (BFD).

Gli apparati devono supportare le estensioni per i meccanismi di “Graceful Restart” (GR), secondo lo standard “Graceful OSPF Restart” (RFC 3623).

È richiesta l’implementazione delle MIB come da RFC 2011 "SNMPv2 Management Information Base for the Internet Protocol using SMIv2" e, in particolare, il supporto completo della tabella “ipNetToMediaTable”.

4.8. *Qualità del Servizio (QoS)*

4.8.1. Packet filtering

Gli apparati devono supportare la funzionalità di packet filtering e Access Control List (ACL) sulle interfacce fisiche e logiche a “line rate” in ingresso e in uscita, con funzioni di classificazione del traffico ad elevata granularità, configurando i campi 802.1p, DSCP e IP Precedence dell’intestazione protocollare IP, i parametri di livello 2 (mac-address), livello 3 (IP), livello 4 (porte) , o qualsiasi combinazione delle precedenti.

Devono essere configurabili almeno le seguenti operazioni “post pattern matching”:

- Accept;
- Discard.

Devono essere configurabili almeno le seguenti azioni associate:

- Count.

4.8.2. Policing & Scheduling

Gli apparati devono supportare il protocollo CoS in accordo con la raccomandazione IEEE 802.1p: "LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization".
Gli apparati devono supportare i meccanismi di QoS secondo il modello DiffServ e poter operare sul campo DSCP dell'header IP per il trattamento differenziato del traffico in classi di servizio (precedence trust and marking).
Gli apparati devono prevedere, per il traffico in uscita, la possibilità di configurare sulle interfacce il accodamento su almeno 8 code hardware.
Gli apparati, per le operazioni di "traffic policing" e "scheduling", devono supportare sulle interfacce di ingresso funzioni di classificazione del traffico sulla base di combinazioni di "header field" protocollari a layer2, layer3 e layer4.
Gli apparati devono supportare la definizione del rate limiting in ingresso ed uscita delle interfacce.

5. Apparati tipologia Gestione - Requisiti minimi

Costituiscono requisito minimo e quindi sono condizioni vincolanti per la fornitura, pena l'esclusione dalla gara, le seguenti caratteristiche e funzionalità.

5.1. *Singola Piattaforma di Gestione*

La piattaforma proposta deve prevedere una soluzione di configurazione unica per tutti gli apparati Security-FW e per tutti gli apparati DC-Infra. Inoltre la piattaforma di gestione deve permettere il monitoraggio delle prestazioni dei dispositivi e prevedere una soluzione di log management unica per tutti gli apparati Security-FW e per tutti gli apparati DC-Infra. Entrambe le soluzioni, configurazione e log management, devono essere fornite con dispositivi fisici dedicati e non in soluzioni virtualizzate.

5.2. *Graphical User Interface*

La Piattaforma di Gestione deve essere disponibile via interfaccia Web e non deve richiedere l'installazione di nessuna applicazione con funzione di Console sui dispositivi degli amministratori dei sistemi. In particolare, deve supportare almeno uno dei seguenti Browser: Internet Explorer, Chrome, Firefox o Safari.

5.3. *Scalabilità e Alta Affidabilità*

La soluzione per la gestione dell'Architettura proposta deve essere in alta affidabilità 1+1 e deve essere già predisposta per gestire almeno 100 dispositivi.
Deve inoltre integrare sistemi di storage esterni mediante protocollo NFS o iSCSI per la componente di Log Collector sia per aumentare il retention period dei log, sia per la funzionalità di archiviazione dei log stessi.

5.4. *Operatività*

La Piattaforma di Gestione deve possedere le caratteristiche specificate nei seguenti paragrafi.

5.4.1. *API pubbliche per integrazione con sistemi di terze parti*

La Piattaforma di Gestione deve supportare API pubbliche per l'integrazione con software di terze parti, come ad esempio sistemi di OSS/BSS.
Il produttore deve fornire la documentazione pubblica relativa alle API in questione.

5.4.2. *Monitoraggio e azioni di remediation*

La Piattaforma di Gestione deve prevedere il monitoraggio, in tempo reale, dello stato di salute dell'intera architettura proposta e, in caso di eventi particolari, deve poter eseguire delle azioni di remediation in automatico.
In particolare, deve supportare le seguenti azioni in automatico:

- Rilevazione eventi: la piattaforma deve poter ricevere e gestire eventi relativi a guasti e/o malfunzionamenti generati dall'architettura in questione;
- Raccolta dati: la piattaforma deve essere in grado di raccogliere automaticamente le informazioni relative agli eventi generati al punto precedente e necessarie per l'analisi del problema in corsa da parte del produttore;
- Apertura case: la piattaforma deve poter aprire "case" automaticamente verso il supporto del produttore e condividere le informazioni raccolte nella fase di rilevazione del problema.

La Piattaforma di Gestione deve prevedere anche dei meccanismi di prevenzione dei problemi tramite il monitoraggio costante degli apparati, correlando in automatico i dati con le informazioni rilasciate dal produttore. Le informazioni rilasciate dal produttore da utilizzare durante la fase di correlazione sono:

- End of Support per le versioni software utilizzate;
- Notifica di bug sia hardware che software scoperti dal produttore che possano impattare sull'operatività dell'architettura proposta e sulle configurazioni utilizzate;
- Gestione dei contratti di supporto e delle licenze. In caso di scadenza dei supporti e/o delle licenze, la Piattaforma di Gestione deve proattivamente generare degli alert.

5.5. *Requisiti per la gestione dei dispositivi di tipologia Security-FW*

La Piattaforma di Gestione deve supportare le seguenti funzionalità:

- Configurazione dei dispositivi Security-FW in tutte le sue componenti di sicurezza descritte nel capitolo 6;
- Performance Monitoring: monitoraggio in tempo reale delle performance degli apparati Security-FW;
- Visibilità: possibilità di visualizzare le informazioni ricevute dai dispositivi Security-FW sia in forma statistica (dashboard) sia in forma raw.

5.6. *Requisiti per la gestione dei dispositivi di tipologia DC-Infra*

La Piattaforma di Gestione deve supportare le seguenti funzionalità:

- Configurazione completa dei dispositivi di tipologia DC-Infra;
- Performance Monitoring: monitoraggio in tempo reale delle performance degli apparati DC-Infra relativamente allo stato dell'apparato stesso e delle interfacce di fisiche/virtuali;

5.7. *Log Management*

La Piattaforma di Gestione deve supportare la gestione dei Log generati anche da dispositivi di altri produttori. Il collettore dei Log (nodi LOG) deve essere integrabile per poter supportare diversi produttori di sistemi e applicazioni di rete e sicurezza. In particolare deve supportare almeno i seguenti produttori divisi per tipologia:

- Firewall: Cisco, Juniper, Fortinet, CheckPoint;
- Antivirus: McAfee, Symantec;
- DDos protection: Arbor, Radware;
- Networking: Cisco, Juniper;
- Load Balancer: F5;
- Client Operating Systems: Windows, Mac OS, GNU/Linux;
- Server Operating Systems: Windows, GNU/Linux (Red Hat, Ubuntu, Debian);
- Web Server: Apache;
- DB: MySQL, PostgreSQL;
- Mail server: Postfix;
- DNS server: Bind.

5.7.1. *Analisi dei Log*

La Piattaforma di Management deve supportare almeno le seguenti funzionalità:

- Reporting: possibilità di generare dei report, sia da template standard che da template personalizzati, esportabili nei seguenti formati: PDF, HTML, RTF, Word, XML;
- Possibilità di configurare i tempi di retention anche in base allo spazio di archiviazione disponibile;
- I log ricevuti devono essere protetti contro possibili modifiche/manipolazioni del log stesso e devono essere salvati in formato raw;
- Correlazione dei log: il sistema di log Management deve supportare la possibilità di correlare i log ricevuti da varie sorgenti per generare degli allarmi relativi a possibili attacchi informatici;
- Supporto dei seguenti protocolli per il monitoraggio dei flussi dati: IPFIX, Netflow e sFlow.

5.7.2. *Funzionalità avanzate di correlazione*

La piattaforma di Log Management deve supportare le seguenti funzionalità avanzate di correlazione dei log:

- capacità di integrazione di "threat intelligence feed", in grado di arricchire le informazioni acquisite dalle sorgenti con ulteriori informazioni di "intelligence" provenienti dal produttore, terze parti o da community pubbliche (ad esempio IP/domain reputation, indicatori di compromissione, etc);

- funzionalità di “vulnerability scan”, che consente di effettuare la ricerca di vulnerabilità sui nodi che compongono l’infrastruttura informatica e correli le medesime vulnerabilità con le minacce rilevate dall’infrastruttura di sicurezza, al fine di ridurre il perimetro di analisi del rischio: la piattaforma deve rendere disponibile la funzionalità su almeno 255 nodi.

5.8. *Element Management Systems*

La Piattaforma di Gestione deve poter supportare il ruolo di Element Management System (EMS) secondo la definizione del ETSI relativo al “Network Functions Virtualisation (NFV); Architectural Framework”.

6. Architettura e dotazioni hardware/software - Requisiti minimi

All'interno di questo capitolo sono dettagliate, oltre ai vincoli architetturali, le richieste minime in termini di capacità, modularità e numero interfacce di rete degli apparati oggetto del presente bando. Tali requisiti sono vincolanti ai fini della fornitura.

6.1. *Tipologia Security-FW*

Gli apparati della tipologia Security-FW devono rispettare i requisiti progettuali e le specifiche tecniche riportati nei capitoli precedenti i quali sono maggiormente dettagliati nei successivi paragrafi.

6.1.1. *Prestazioni e Connettività per i dispositivi Security-FW Datacenter*

6.1.1.1.Prestazioni

È richiesto che l'architettura soddisfi le seguenti performance:

- Firewall performance: 80 Gbps;
- VPN performance IMIX: 9 Gbps;
- L7 Application FW: 32 Gbps;
- IPS performance massime: 20 Gbps,
- Advanced Security Services (zero-day attack, C&C, IPS) - 3,5 Gbps (traffico HTTP 44kB);
- Analisi file contro zero-day attack: 30.000 al giorno;
- Maximum concurrent sessions IPv4/IPv6:10 milioni;
- New sessions/second: 300.000.

6.1.1.2.Connettività

L'architettura deve avere almeno le seguenti interfacce:

- 8 x 10 GE SFP+: traffico dati;
- 1 x 1 GE: management port out of band;
- 2 x 10 GE SFP+: control e data link per le comunicazioni tra i nodi (HA);
- 1 x porta console RJ45
- 1 x USB.

6.1.1.3.Capacità minime

- Firewall policy: 60.000;
- Zone di sicurezza: 2.000;
- Tunnel IPSec site-to-site: 2.000;
- Utenti concorrenti per accesso remoto VPN: 50;
- BGP peers: 250;
- BGP routes RIB: 2 milioni;
- Adiacenze OSPF: 256;
- Rotte OSPF: 250.000;
- RIP v1/v2 neighbors: 256;
- RIP v2 table size: 8.000;
- VLANs per interfaccia fisica: 4.000;
- VLAN supportate: 4.000.

6.1.2. *Quantità*

La fornitura dovrà prevedere i seguenti apparati:

Apparati	Tipologia	Quantità
Firewall DC Pisa	Security-FW Data center	2

6.1.3. *Caratteristiche fisiche dei nodi*

Tutti gli apparati con funzionalità di nodo della tipologia Security-FW devono appartenere alla stessa famiglia all'interno del portafoglio del produttore prescelto, devono poter essere installati in rack standard 800x1000 mm e non devono superare 1 Rack Unit (RU) in altezza ciascuno.

Tutti gli apparati della tipologia Security-FW devono essere forniti con un livello di ridondanza sullo storage costituito da almeno due dischi SSD in configurazione RAID1/mirroring.
Si devono fornire alimentatori con alimentazione in schema di ridondanza 1+1.
Gli alimentatori installati all'interno dei nodi devono essere:

- Hot-swappable (rimozione di moduli senza impatto sul funzionamento del sistema);
- Hot-pluggable (inserimento di nuovi moduli senza impatto sul funzionamento del sistema).

Presenza di un sistema di raffreddamento ridondato e con flusso dell'aria *front-to-back*.
I moduli di ventole installate all'interno dei nodi devono essere:

- Hot-swappable (rimozione di moduli senza impatto sul funzionamento del sistema);
- Hot-pluggable (inserimento di nuovi moduli senza impatto sul funzionamento del sistema).

6.1.3.1. Transceiver per nodi di tipologia Security-FW

Nella tabella seguente sono riportate le quantità richieste per il Datacenter di Pisa:

Standard	Tipo di transceiver	Quantità richieste
SFP-10GE-LR	SFP+	20

6.1.3.2.Alta disponibilità e prestazioni dei nodi

I singoli nodi devono prevedere la possibilità di essere in configurazione ridondata almeno 1+1, cioè almeno due nodi devono poter costituire un unico apparato logico per il collegamento verso il data center o verso dispositivi di rete esterni tramite aggregazione di interfacce (Link Aggregation Group).
Pertanto le funzioni di Network e Security devono poter essere eseguite su almeno due nodi fisicamente distinti appartenenti allo stesso Cluster in configurazione attivo/passivo o attivo/attivo.
Il singolo nodo deve essere collegato all'altro nodo con almeno due link dedicati.
Il singolo nodo deve essere in grado di fornire le prestazioni, capacità e connettività descritte al paragrafo 6.1.1. In caso di guasto di un nodo, l'architettura non deve scendere sotto le prestazioni richieste.

6.1.4. *Servizi di sicurezza*

I servizi di sicurezza descritti al Capitolo 3.1 possono essere forniti in modalità licenza-perpetua o attraverso licenze commerciali della durata di 5 anni.

6.2. *Tipologia DC-Infra*

Gli apparati della tipologia DC-Infra devono rispettare i requisiti progettuali e le specifiche tecniche riportati nei capitoli precedenti i quali sono maggiormente dettagliati di seguito:

- Apparati costituiti da multilayer Ethernet switch a elevata densità di porte di rete. I modelli dovranno essere composti rispettivamente da porte 1G/10G SFP+ e da porte 100M/1G/10G RJ45;
- Apparati basati su piattaforme non bloccanti con piano di controllo separato da quello di inoltro;
- Apparati dove la commutazione del traffico, tra nodi diversi appartenenti allo Stack, non deve impegnare le unità centralizzate della stessa;
- Apparati dove le funzioni di packet forwarding e packet processing devono essere implementate a line rate su tutti gli apparati componenti lo Stack;
- Gli apparati dello stack che svolgono il ruolo di Piano di Controllo e Gestione Centralizzato devono gestire:

    - L’inizializzazione e la gestione dei processi di gestione dell’intero stack;
    - Il calcolo, la gestione e la distribuzione su tutto lo stack delle tabelle di forwarding;
    - La gestione del traffico di controllo per la condivisione degli instradamenti tra i diversi componenti dello Stack;
- Gli apparati dello stack aventi funzionalità di Piano di Controllo e di Gestione Centralizzato devono essere in configurazione active/backup, in modo da garantire la ridondanza sia per quanto riguarda l’hardware che per quanto riguarda le funzionalità di alta affidabilità;
- Gli apparati dello stack aventi funzionalità di Piano di Controllo e di Gestione Centralizzato devono mantenere tra loro la sincronizzazione degli stati per essere in grado di assumere uno il ruolo dell’altro;
- Gli apparati dello stack, che non ricoprono il ruolo di Master/Backup all’interno dello stack stesso, devono essere in grado di ricevere ed elaborare i dati di forwarding ricevuti dall’apparato con funzionalità di Piano di Controllo e di Gestione Centralizzato in modalità Master. Devono inoltre poter individuare ed inoltrare tutte le informazioni di fault/errore, locali all’apparato, verso l'apparato con funzionalità di Piano di Controllo e di Gestione Centralizzato in modalità Master.

In generale, tutti i nodi dello stack devono poter essere in grado, in caso di fault, di assumere uno qualunque dei possibili ruoli previsti dal protocollo di stacking.
Deve essere possibile definire, in maniera deterministica, il ruolo dei singoli switch facenti parte dello stack, individuando quali switch assumeranno il ruolo di Master/Backup con funzionalità di Piano di Controllo e Gestione ridondato;
Tutti i nodi devono avere lo stesso sistema operativo e le stesse funzionalità.

6.2.1. Quantità

La fornitura dovrà prevedere i seguenti apparati per il data center di Pisa:

Apparati	Tipologia	Quantità
Nodo Multilayer Ethernet Switch 100M/1G/10G RJ-45 1G/10G SFP/SFP+	DC-Infra	6

6.2.2. Caratteristiche fisiche dei nodi

Tutti gli apparati con funzionalità di nodo della tipologia DC-Infra devono essere predisposti con ridondanza 1+1 sugli alimentatori.
Gli alimentatori devono avere la possibilità di supportare direzione del flusso dell’aria sia di tipo front-to-back che back-to-front.
Gli alimentatori devono fornire alimentazione in schema di ridondanza 1+1.
Gli alimentatori installati all’interno dei nodi devono essere:

- Hot-swappable (rimozione di moduli senza impatto sul funzionamento del sistema);
- Hot-pluggable (inserimento di nuovi moduli senza impatto sul funzionamento del sistema).

Presenza di un sistema di raffreddamento ridondato e con flusso dell’aria *front-to-back*.
I moduli di ventole installate all’interno dei nodi devono essere:

- Hot-swappable (rimozione di moduli senza impatto sul funzionamento del sistema);
- Hot-pluggable (inserimento di nuovi moduli senza impatto sul funzionamento del sistema).

6.2.3. Alta disponibilità e prestazioni dei nodi

L’architettura di stacking deve poter costituire un unico apparato logico per il collegamento di server o dispositivi di rete esterni anche tramite aggregazione di interfacce (Link Aggregation Group) senza l'utilizzo di tecniche non ottimizzate quali lo Spanning Tree (STP) o simili.
Tutti i nodi della tipologia DC-Infra devono appartenere alla stessa famiglia all’interno del portafoglio del produttore prescelto, devono poter essere installati in rack standard 800x1000 mm e non devono superare 1 RU (RU, Rack Unit) in altezza.

6.2.4. *Moduli Uplink dei nodi*

I singoli nodi, al fine di garantire una maggior flessibilità architetturale, devono potere ospitare contemporaneamente tutte le possibili combinazioni di due moduli di uplink (integrati o di espansione) aventi le seguenti caratteristiche:

- modulo con almeno 8 interfacce 1/10 GbE SFP/SFP+ (il modulo a 8 interfacce 1/10 GbE SFP/SFP+ deve poter supportare il protocollo MACsec nelle modalità switch-to-switch e switch-to-host);
- modulo con almeno 8 interfacce 100M/1G/10G BASE-T RJ-45;
- modulo con almeno 2 interfacce 40 GbE QSFP+;
- modulo con interfacce proprietarie dedicate alla realizzazione di uno Stack.

6.2.5. *Configurazione dei nodi di tipologia DC-Infra*

Tutti i nodi devono prevedere almeno:

- 32x porte 100M/1G/10G BASE-T RJ-45;
- 8x porte 1/10G SFP/SFP+;
- 2x porte dedicate all'interconnessione locale degli apparati in stack;
- alimentatori in configurazione di ridondanza 1+1.

6.2.5.1.Transceiver per nodi tipologia DC-Infra

Nella tabella seguente sono riportate le quantità richieste per il Datacenter di Pisa:

Standard	Tipo di transceiver	Quantità richieste
SFP-10GE-LR	SFP+	22

Nota 1: le ottiche SFP-10G-LR saranno utilizzate per la connessione ai Firewall oggetto di questo capitolato.

6.2.6. *Requisiti di compatibilità ottiche*

Fermo restando l'adesione ai relativi Multi-Source Agreement (MSA), deve essere certificata la compatibilità dei transceiver SFP e SFP+ con gli omologhi di altri produttori.

Deve essere possibile utilizzare transceiver di differenti produttori a patto che sia garantito il supporto di tutte le funzionalità e le prestazioni richieste (per esempio come nel caso di "Digital Diagnostics Monitoring").

L'utilizzo di transceiver di differenti produttori non deve invalidare alcun servizio di manutenzione o SLA attivato per l'apparato in oggetto, se non per guasti riguardanti il transceiver stesso o la fibra ottica ad esso collegata.

6.3. *Tipologia Gestione*

Gli apparati della tipologia Gestione devono rispettare i requisiti progettuali e le specifiche tecniche riportati nei capitoli precedenti e che sono maggiormente dettagliati nei successivi paragrafi.

6.3.1. *Alta disponibilità*

La Piattaforma di Gestione deve garantire l'alta affidabilità 1+1 a livello di servizio per le funzioni descritte nel paragrafo 1.1.4 e maggiormemente specificate nel capitolo 5. La soluzione deve prevedere dispositivi fisici per l'erogazione dei servizi di tipologia Gestione.

6.3.2. *Prestazioni e Scalabilità*

La Piattaforma di Management deve garantire le seguenti performance e scalabilità:

- Gestione per 10 dispositivi di tipologia Security-FW e 100 dispositivi di tipologia DC-Infra;
- Supporto per 2500 Eventi Per Secondo (EPS) con possibilità di scalare raddoppiando gli EPS supportati sullo stesso hardware;

- Supporto per 25000 Flussi Per Minuto (FPM) con possibilità di scalare fino a 200000 FPM sullo stesso hardware mediante opportuna licenza facoltativa.

6.3.3. Caratteristiche fisiche dei nodi

Tutti gli apparati della tipologia Gestione devono poter essere installati in rack standard 800x1000 mm e non devono superare le 2RU (RU, Rack Unit) di altezza ciascuno.
Per tutti gli apparati della tipologia Gestione (nodi MGT e nodi LOG) si devono fornire alimentatori con alimentazione in schema di ridondanza 1+1.
Gli alimentatori installati all'interno dei nodi devono essere:

- Hot-swappable (rimozione di moduli senza impatto sul funzionamento del sistema);
- Hot-pluggable (inserimento di nuovi moduli senza impatto sul funzionamento del sistema).

In particolare, per ogni nodo di tipo MGT è richiesto:

- Un numero minimo di 4 porte RJ-45 10/100/1000 Mbps;
- Almeno una porta console RJ-45;
- Capacità di storage non inferiore a 6 TB con un numero di dischi non inferiore a 6;
- Meccanismo di ridondanza storage tale da poter aumentare le prestazioni, la sicurezza ed anche la tolleranza contro eventuali guasti di tipo RAID10.

In particolare, per ogni nodo di tipo LOG, è richiesto:

- Un numero minimo di 4 porte RJ-45 10/100/1000 Mbps;
- Un numero minimo di 2 porte 10G SFP+;
- Almeno una porta IPMI LAN RJ-45;
- Capacità di storage non inferiore a 6 TB;
- Meccanismo di ridondanza storage tale da poter aumentare le prestazioni, la sicurezza ed anche la tolleranza contro eventuali guasti di tipo RAID10.

6.3.4. Quantità

La fornitura dovrà prevedere i seguenti apparati per il Datacenter di Pisa:

Apparati	Tipologia	Quantità
Cluster di nodi MGT	Gestione	2
Cluster di nodi LOG	Gestione	2

7. Servizio di assistenza specialistica e manutenzione - Requisiti minimi

La fornitura degli apparati deve prevedere un servizio di assistenza specialistica e di manutenzione atto a garantire l'esercizio corretto e continuativo delle funzionalità implementate sull'infrastruttura da realizzare.
Esso deve comprendere servizi di assistenza sistemistica (correzione bug software, rilascio relative patch, aggiornamenti release OS e supporto tecnico al troubleshooting) e procedure per la gestione e sostituzione delle parti hardware nel caso in cui queste non rispettino parametri di performance dichiarati o in caso di guasto.
Il contratto di assistenza specialistica e manutenzione deve avere una durata di 60 mesi dalla data di consegna degli apparati e delle piattaforme software oggetto della presente fornitura.
Le modalità e le tempistiche, alle quali devono essere soggette tali attività, costituiscono gli SLA (Service Level Agreement) che l'Operatore economico sarà tenuto a rispettare e che sono definiti nei paragrafi seguenti.

7.1. *Definizioni*

Sono fornite le definizioni di alcuni termini utilizzati:

- Network Operations Center (NOC): struttura preposta alle attività riguardanti il corretto funzionamento della rete telematica;
- Technical Assistance Center (TAC): centro di supporto tecnico del produttore;
- Return Materials Authorization (RMA): autorizzazione alla spedizione delle componenti hardware in sostituzione di quelle riconosciute guaste a seguito dell'analisi della TAC;
- Business Day (BD): giorno lavorativo utilizzato dalla stazione appaltante per la parametrizzazione dello SLA e corrispondente all'intervallo temporale 8:30 am - 5:00 pm (UTC+1) dei giorni feriali (Lun - Ven);
- Next Business Day (NBD): entro il giorno lavorativo successivo;
- Service Level Agreement (SLA): modalità e tempistiche, che definiscono le metriche contrattuali per l'erogazione del servizio di assistenza. Di seguito la definizione dei tipi di SLA:
    - 24x7x365: 24 ore al giorno per tutti i giorni dell'anno;
    - 24x7x1h: entro il tempo massimo di 1 ora a qualunque orario della giornata;
    - 8x5xNBD: entro massimo il giorno lavorativo successivo nella fascia oraria BD;
- Troubleshooting: il processo di analisi e ricerca delle cause dei guasti;
- Guasto: malfunzionamento o degrado di prestazioni parziale o totale del sistema, inteso come entità hardware e software preposta all'espletamento di determinate funzionalità. Nel seguito sono definiti quattro livelli di guasto:
    - Severity1: sistema compromesso nell'esercizio delle proprie funzioni e/o blocco di un servizio ritenuto critico;
    - Severity2: sistema parzialmente compromesso nell'esercizio delle proprie funzioni, che risultano degradate ma con disponibilità dei servizi o perdita di ridondanza nei componenti del sistema;
    - Severity3: sistema soggetto a malfunzionamenti o anomalie occasionali che non impattano sui servizi erogati;
    - Severity4: attività riguardanti configurazioni particolari o implementazione di nuovi servizi;
- Hardware Delivery: il processo di consegna presso il committente delle parti hardware giudicate guaste. Tipicamente facente parte delle metriche soggette a SLA in alternativa alla semplice spedizione (shipment) che contrariamente al delivery non offre garanzie temporali di ricezione.

7.2. *Caratteristiche del servizio*

L'operatore economico deve garantire che il servizio di assistenza specialistica e manutenzione sia erogato direttamente dal produttore degli apparati.

Gli apparati oggetto del servizio saranno consegnati nelle sedi e i punti di presenza della stazione appaltante.

Sedi della stazione appaltante: *IIT- CNR, Pisa*

Il delivery delle parti in sostituzione di quelle giudicate guaste, laddove previsto dagli specifici servizi di assistenza, prevederà come indirizzo di consegna le sedi della stazione appaltante.

7.2.1. *Registrazione codici prodotto*

L'Operatore Economico deve garantire che tutte le parti hardware e software proposte nella fornitura siano registrate ufficialmente sotto il contratto di assistenza specialistica e manutenzione del produttore, tramite il proprio codice identificativo (numero seriale).

Alla stazione appaltante deve essere garantita visibilità di tale registrazione tramite accesso su base 24x7x365 a una sezione riservata nel portale web del produttore degli apparati.

La lista dei codici identificativi deve essere sempre sincronizzata con le attività di sostituzione delle parti ritenute guaste a seguito di emissione dei codici RMA.

7.2.2. *Knowledge base & software*

L'operatore economico deve garantire che il produttore degli apparati metta a disposizione, con accesso 24x7x365, la manualistica completa degli apparati e piattaforme software, con esempi di configurazione, la knowledge base relativa, la rendicontazione di tutte le anomalie e limitazioni, note tecniche del produttore, bollettini di sicurezza ed avvisi sul rilascio di nuove release del sistema operativo.

L'operatore economico deve garantire che il produttore degli apparati e delle piattaforme software metta a disposizione su base 24x7x365 il servizio di download e di aggiornamento delle release software e firmware degli apparati e delle piattaforme software oggetto del servizio di supporto.

L'operatore economico deve garantire che il produttore metta a disposizione la possibilità di iscriversi ai technical bulletin per ricevere, in maniera tempestiva, alert via email relativamente a bug o notifiche di sicurezza.

L'operatore economico deve garantire che tutti questi servizi siano resi disponibili dal produttore attraverso un portale web accessibile dalla stazione appaltante; tale portale web deve essere lo stesso utilizzato per il servizio al paragrafo 7.2.3.

7.2.3. *Trouble ticket system*

Per le attività di troubleshooting deve essere garantita la relazione diretta tra il NOC dello IIT-CNR e la TAC del produttore; non è ammessa nessuna forma di mediazione all'interno del processo di supporto, tra questi due soggetti. La segnalazione di un malfunzionamento o di un guasto deve prevedere l'assegnazione di un ticket di segnalazione e deve essere tracciabile e gestita tramite un sistema di "Trouble Ticket System".

Le comunicazioni tra il NOC dello IIT-CNR e la TAC del produttore, nel processo di supporto, devono essere veicolate indifferentemente tramite i seguenti canali di comunicazione: telefono, posta elettronica e/o interfaccia web.

Il servizio di assistenza specialistica e manutenzione deve prevedere un unico punto di contatto per ogni mezzo di comunicazione previsto: unico numero telefonico, unico indirizzo di posta elettronica e di accesso al portale web. In particolare il NOC della stazione appaltante deve avere accesso al sistema di ticketing del produttore per avere completa visibilità del processo di troubleshooting in tempo reale; l'accesso al sistema di ticketing deve essere garantito almeno su canale web.

7.2.4. *Apertura ticket*

È richiesto l'accesso al sistema di apertura dei ticket secondo la modalità 24x7x365 e deve essere rispettato un tempo massimo di presa in carico della segnalazione di un'ora, cioè secondo la modalità 24x7x1h.

Per tutti i ticket, indipendentemente dal canale di sottomissione utilizzato, è richiesto che vengano emessi secondo la severity richiesta dal NOC dello IIT-CNR ed eventualmente scalati ad altra

severity solo dopo un'analisi congiunta tra il NOC dello IIT-CNR stesso e il personale della TAC del produttore.

7.2.5. *Technical escalation e supporto evoluto*

È richiesta la possibilità di attivare un processo di escalation all'interno della TAC del produttore per la gestione dei trouble ticket; tale escalation deve essere possibile via telefono e via medesimo portale web di cui ai paragrafi 7.2.3 e 7.2.4.

È richiesta la possibilità di un accesso diretto al secondo livello dell'engineering della TAC del produttore già all'apertura del "trouble ticket".

7.3. *Livelli di servizio*

È richiesta la seguente tipologia di SLA in caso di guasto per tutti gli apparati hardware:

Servizio Standard: NBD (Next Business Day).

7.3.1. *Servizio Standard: NBD*

Per tutti gli apparati hardware è richiesto lo SLA minimo di seguito dettagliato:

- servizio di hardware delivery delle parti in sostituzione di quelle ritenute guaste, secondo modalità 8x5xNBD dalla diagnosi finale del processo di troubleshooting aperto direttamente con il produttore.

Le eventuali spese di consegna e di ritiro delle parti hardware devono essere a carico dell'operatore economico.

7.3.2. *Servizi di Configurazione*

Per tutti gli apparati oggetto del capitolato l'operatore economico deve garantire un servizio di configurazione e messa in servizio erogato direttamente dal personale specializzato del produttore presso la sede della stazione appaltante, per un massimo di 5 giorni eseguiti in orario lavorativo.

8. CRITERI DI AGGIUDICAZIONE DELL'OFFERTA-PRESTAZIONI MGLIORATIVE

8.1 CRITERIO DI AGGIUDICAZIONE

L'appalto è aggiudicato in base al criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo, ai sensi dell'art. 95, comma 2 del Codice.

La valutazione dell'offerta tecnica e dell'offerta economica sarà effettuata in base ai seguenti punteggi.

	PUNTEGGIO MASSIMO
Offerta tecnica	*80*
Offerta economica	*20*
TOTALE	**100**

Criteri di valutazione dell'offerta tecnica

Le offerte tecniche devono rispettare i requisiti tecnici minimi richiesti a pena di esclusione.

Il punteggio dell'offerta tecnica è attribuito sulle prestazioni migliorative elencate e descritte di seguito al successivo paragrafo 8.4 con la relativa ripartizione dei punteggi.

Metodo di attribuzione del coefficiente per il calcolo del punteggio dell'offerta tecnica

Agli elementi è assegnato un punteggio tabellare definito, automaticamente e in valore assoluto, sulla base della presenza o assenza nell'offerta, dell'elemento richiesto.

Si procederà poi a riparametrare il punteggio maggiore al massimo dei punti assegnabili (80 su 100) riproporzionando linearmente i punteggi delle offerte, secondo la seguente formula:

C(i)R = [C(i)/C(imax)] * Pmax

Dove:

C(i)R = offerta i-esima riproporzionata
C(i) = offerta i-esima
C(imax) = offerta con punteggio maggiore
Pmax = punteggio massimo attribuibile (80,00 punti)

Calcolo del punteggio dell'offerta economica

Il Punteggio relativo all'offerta Economica (PE) è di un massimo di 20 punti e verrà calcolato secondo la seguente formula:

PE =Valmin/ Val offerta* YY

dove

- Valmin è il valore dell'offerta risultata più bassa fra tutte le offerte economiche pervenute dalle Ditte Concorrenti

• Val offerta è il "Valore complessivo dell'Offerta" di ciascuna Ditta Concorrente.

• YY è il punteggio assegnato all'offerta economica, nella fattispecie corrispondente a 20.

PUNTEGGIO FINALE

Il Punteggio complessivo sarà dato dalla somma del punteggio dell'offerta tecnica e dell'offerta economica

8.2 Valutazione dell'offerta tecnica

La valutazione tecnica degli elementi migliorativi, come per i requisiti minimi, sarà effettuata in base al contenuto della documentazione presentata.

Ogni requisito tecnico o prestazionale non presente o non chiaramente dettagliato nella documentazione fornita, sarà considerato mancante. Si raccomanda la compilazione ordinata e puntuale dell'allegato Offerta Tecnica. È richiesto di allegare i report dei test di performance prodotti da tester ad alte prestazioni (e.g. Agilent, Ixia e Spirent). Si sottintende che tali tester abbiano throughput e parametri di precisione adeguati all'esecuzione delle misure per la categoria degli apparati oggetto di questo bando di gara. In caso contrario i report non avranno validità ed il requisito sarà considerato mancante.

Nei report deve essere chiaramente specificato, onde permettere la valutazione dell'idoneità dello strumento, marca e modello del tester usato. Nel caso i tester utilizzati siano sottodimensionati allo scopo, i report allegati saranno considerati come mancanti.

L'IIT verificherà, congiuntamente con il personale tecnico dell'operatore economico aggiudicatario, i dati tecnici relativi alle capacità e le prestazioni degli apparati oggetto del presente bando, mediante verifica dinamica in laboratorio secondo le metodologie indicate nel paragrafo "2.1.4.3 Metodologie per la valutazione delle prestazioni". Il laboratorio dovrà essere allestito con oneri a carico dell'operatore economico.

8.3.Requisiti Hardware, Prestazionali e di Supporto

Con riferimento agli apparati di tipologia Security-FW e DC-Infra, nella valutazione delle performance, gli elementi migliorativi verranno considerati alla luce del valore aggiunto apportato alle prestazioni del sistema nel suo complesso. A titolo di esempio, si consideri il caso in cui si propongano interfacce aggiuntive ma con dati di performance scadenti (e.g. prestazioni modeste nella classificazione del traffico in presenza di politiche complesse o limiti eccessivi nell'inoltro in presenza di ACL composte da un elevato numero di termini).

Si considera limitato il vantaggio fornito dalla larghezza di banda disponibile, in quanto non sfruttabile in contesti richiedenti elevata capacità di forwarding in presenza di politiche di filtraggio o di "multi-field classification" di una certa complessità.

Allo stesso modo si considera limitato l'utilizzo di link aggregati, in quanto non sempre utilizzabili per limiti nella configurabilità di funzionalità avanzate e nel bilanciamento del traffico (nonché nella gestione delle code) all'interno del bundle, soprattutto in contesti ad elevata complessità nel "packet processing".

8.4.Criteri di valutazione

Le soluzioni migliorative che l'operatore economico può proporre compilando l'allegato Offerta Tecnica sono individuate nella tabella che segue e spiegate nei paragrafi successivi 9-12 (il numero del paragrafo corrispondente è indicato nella prima colonna della tabella prima della descrizione). La tabella indica i punteggi assegnati per ogni elemento offerto (diversamente il punteggio assegnato sarà pari a 0).

Le offerte tecniche presentate devono raggiungere una soglia minima di punteggio complessivo di 15 punti per l'ammissione alla successiva fase di valutazione economica.

Categorie	Punteggio
9 Apparati tipologia Security-FW - Requisiti migliorativi	**39,1**
9.1 Architettura di sicurezza integrata	1,5
Importazione "threat intelligence feed"	0,5
Dynamic Distributed Enforcement	1
9.2 Zero-day malware protection	9,2
Analisi statica e dinamica di file "inviati dalla stazione appaltante"	1
Analisi files	7,2 max
per ogni estensione specificata in tabella al par. 9.2	0,1
Dimensione files	1 max
fino a 10 MByte	0,1
fino a 20 MByte	0,3
oltre 30 MByte	1
9.3 Next Generation Firewall Services	1,2
Web Filtering	0,6
Meccanismi di protezione	0,2
Signature del IDP	0,2
Supporto requisiti FIPS 140-2	0,2
9.4 Configurazione, Backup e Gestione	12,6
Archiviazione automatica delle configurazioni	2
Attivazione configurazioni per tempo limitato	6
Controllo sintattico della configurazione runtime	4
Definizione MIB personalizzate	0,2
Esecuzione di script per configurazione e gestione apparato	0,2
Supporto di REST API pubbliche via HTTPS	0,2
9.5 Strumenti di monitoraggio	0,5
Supporto a: Python, Ansible e Chef	0,4
Collezionare di informazioni statistiche per interfaccia, etc	0,1
9.6 Resilienza ed Alta affidabilità	0,3
9.6.1 Alta disponibilità layer2/3	

Monitoraggio della raggiungibilità IP dei nodi del Cluster	0,1
Equal Cost Multi Path (ECMP)	0,2
9.7 Qualità del Servizio (QoS), Routing and Filtering	10,6
9.7.1 Route filtering	0,2
9.7.2 Packet filtering	0,2
9.7.3 Policing & Scheduling	0,2
9.7.4 Funzionalità di rete	8 max
Funzionalità MPLS	5
L2VPN VPLS	2
L3VPN e NGMVPN multicast VPN	1
9.7.5 IP tunneling e overlay	2
9.8 Virtualizzazione e sistemi di convergenza	0,2
9.9 Caratteristiche fisiche	3
Quantità di calore media dissipata	1 max
pari o inferiore a 700 BTU/hr	1
maggiore di 700 BTU/hr fino a 1000 BTU/hr	0,3
maggiore di 1000 BTU/hr	0,1
Quantità media di potenza assorbita	1 max
pari o inferiore a 200W	1
maggiore di 200W ed inferiore o uguale a 400W	0,3
maggiore di 400W	0,1
MTBF degli apparati	1 max
pari o superiore a 100000 ore	1
inferiore a 100000 ore	0,3
10 Apparati tipologia DC-Infra - Requisiti migliorativi	**26,4**
10.1 Configurazione, Backup e Gestione	12,4
Archiviazione automatica delle configurazioni	2
Attivazione configurazioni per tempo limitato	6
Controllo sintattico della configurazione runtime	4
Definizione MIB personalizzate	0,2
Esecuzione di script per configurazione e gestione apparato	0,2
10.2 Strumenti di monitoraggio	0,7

Monitoraggio tramite: Python, Ansible e Chef	0,4
Remotizzazione del traffico in mirroring	0,1
Configurazione di politiche di accounting e mirroring	0,2
10.3 Alta disponibilità Layer2	4,4
10.3.1 Link Aggregation	1,5 max
Garanzia di banda di interconnessione stack	0,5
Algoritmi per bilanciamento traffico all'interno dello stack	0,5
Inoltro traffico unicast in uno stack	0,5
10.3.2 Stacking	2,5 max
Possibilità di estensione di uno stack	2
Mantenimento automatico delle informazioni dei membri di uno stack	0,5
10.3.3 Traffic load balancing	0,4 max
Equal Cost Multi Path (ECMP)	0,2
Algoritmi per traffico burst	0,2
10.4 Qualità del Servizio (QoS), Routing and Filtering	0,5
10.4.1 Interfacce di Livello 3	0,1
10.4.2 Route filtering	0,2
10.4.3 Packet filtering	0,2
10.5 Virtualizzazione e sistemi di convergenza	3,5
Plugin per Openstack	0,5
Supporto standard IEEE DCB e con lo standard FC-BB-5 del gruppo di lavoro T11	1,5
Supporto protocollare quali Priority-based Flow Control (PCF), 802.1Qbb, FCoE Inizialization Protocol (FIP) snooping e data center Bridging Exchange (DCBX)	1,5
10.6 Capacità Switching	2
10.7 Caratteristiche fisiche	2
Potenza assorbita	1 max
pari o inferiore a 450W	1
superiore a 450W ed inferiore a 600W	0,3
pari o superiore a 600W	0,1
Valore di MTBF	1 max

superiore a 145000 ore	1
pari o superiore di 100000 ore e minore di 145000 ore	0,3
inferiore a 100000 ore	0,1
10.8 Prestazioni globali architettura DC-Infra	1 max
Mac Entry Scale - almeno 1800	0,2
IPv4 RIB entries – almeno 8500	0,2
ARP Entry – almeno 3000	0,1
BGP routes – almeno 3500	0,2
Multicast Group – almeno 720	0,1
BGP Peers – almeno 100	0,1
OSPF neighbors – almeno 60	0,1
11 Apparati tipologia Gestione - Requisiti migliorativi	**4**
11.1 Log Management	1,5
Correlazione eventi	1
Esecuzione script	0,5
11.2 Virtualizzazione e sistemi di convergenza	0,5
11.2.1 Scalabilità della piattaforma di Gestione	
Numero dispositivi addizionali	1 max
110 < num dispositivi >= 200	0,1
200 < num dispositivi >= 500	0,3
num dispositivi > 500	1
Numero eventi acquisiti da Log Collector	1 max
2.500 < num eventi >= 50.000	0,3
num eventi> 50.000	1
12 Requisiti migliorativi generali	**10,5**
12.1 Consolidamento Sistema operativo	10
12.2 Technical Assistance Center	0,5
	Totale 80

9 Apparati tipologia Security-FW - Requisiti migliorativi

9.3.Architettura di sicurezza integrata

- Possibilità di importare "threat intelligence feed" provenienti dal produttore, da terze parti o da community pubbliche (IP, Domain Reputation) e possibilità di aggiornare dinamicamente tali feed sugli apparati per l'applicazione dinamica delle policy sul controllo del traffico, senza richiedere cambi di configurazione; ***(punti 0,5)***
- Dynamic Distributed Enforcement: supporto di meccanismi per la distribuzione automatica di regole di sicurezza anche agli switch e router presenti in rete, generate dinamicamente in funzione della presenza di minacce, al fine di garantire l'isolamento della minaccia stessa il più vicino possibile alla sorgente. ***(punti 1)***

9.4.Zero-day malware protection

- Possibilità di fare eseguire, all'architettura remota del produttore, l'analisi statica e dinamica di file "inviati dalla stazione appaltante". I file dovranno poter essere caricati tramite REST API pubbliche; ***(punti 1)***
- Supporto dell'analisi, all'interno dell'architettura remota del produttore, di file che transitano sulla rete locale con estensioni diverse *(saranno assegnati **punti 0,1** per ogni estensione supportata, fino ad un massimo di **punti 7,2**)*:

.swf	*.zip*	*.gzip*	*.rar*	*.tar*	*.inf*	*.ini*	*.reg*	*.plist*
.xap	*.bin*	*.com*	*.tar*	*.apk*	*.ipa*	*.dll*	*.kext*	*.ko*
.xbap	*.exe*	*.dat*	*.mst*	*.msm*	*.pyc*	*.a*	*.so*	*.o*
.bat	*.js*	*.pl*	*.py*	*.sct*	*.sh*	*.tcl*	*.java*	*.plsm*
.pyo	*.c*	*.cc*	*.cpp*	*.cxx*	*.h*	*.htt*	*.pdf*	*.ocx*
.chm	*.doc*	*.docx*	*.dotx*	*.xslt*	*.email*	*.mbox*	*.pdfa*	*.ear*
.ppt	*.pptsm*	*.pptx*	*.ps*	*.html*	*.pot*	*.xsl*	*.class*	*.war*
.rtf	*.txt*	*.xlsx*	*.xml*	*.pps*	*.ppa*	*.jar*	*.deb*	*.dmg*

- Supporto per l'analisi, all'interno dell'architettura remota del produttore, di file con dimensione superiore a 30 MByte per tutte le tipologie di cui sopra:
    - Fino a 10 MByte ***(punti 0,1)***
    - Fino a 20 MByte ***(punti 0,3)***
    - Oltre i 30 MByte ***(punti 1)***

9.5.Next Generation Firewall Services

- Possibilità di configurare almeno 500 profili diversi per la funzionalità di Web filtering; ***(punti 0,6)***

- Disponibilità di meccanismi di protezione contro attacchi e/o tecniche di evasion che si basano su pacchetti non compliance con gli RFC. In particolare: IP bad option, ICMP fragmentation, TCP no flag o una combinazione non conforme di flag e IP spoofing; ***(punti 0,2)***

- Possibilità di importare/utilizzare le signature del IDP open source Snort; ***(punti 0,2)***

- Possibilità di configurare il dispositivo in compliance con i requisiti FIPS 140-2 senza la necessità di hardware e/o licenze aggiuntive. ***(punti 0,2)***

9.6.Configurazione, Backup e Gestione

- Archiviazione automatica delle configurazioni applicate all'apparato, per un numero pari o superiore a 50; ***(punti 2)***

- Possibilità di eseguire sull'apparato (in maniera nativa mediante un singolo comando dedicato sul sistema operativo e senza l'utilizzo di script aggiuntivi) una configurazione per un periodo di tempo predefinito (definibile dall'utente) al termine del quale, se non esplicitamente confermata, l'apparato ritorna automaticamente alla precedente configurazione attiva; ***(punti 6)***

- Possibilità di eseguire sull'apparato (in maniera nativa mediante un singolo comando dedicato sul sistema operativo e senza l'utilizzo di script aggiuntivi) un controllo sintattico della configurazione runtime (definita in memoria ma non attiva); ***(punti 4)***

- Possibilità di definire MIB personalizzate, ovvero MIB che siano popolate da informazioni definite dall'utente; ***(punti 0,2)***

- Possibilità di definire degli script (es. configuration script, event policies/script, operation script, SNMP/MIB script) al fine di eseguire in maniera autonoma processi di configurazione e gestione dell'apparato. Per la corretta valutazione del requisito in oggetto devono essere dettagliate le funzionalità degli strumenti di scripting disponibili; ***(punti 0,2)***

- Supporto di REST API pubbliche via HTTPS per consentire il controllo, la configurazione e la gestione del dispositivo integrando diversi meccanismi o sistemi di terze parti utili ad esempio all'esecuzione di remote procedure call (rpc) sull'apparato, alla gestione delle procedure di read/write, monitoraggio e troubleshooting. ***(punti 0,2)***

9.7.Strumenti di monitoraggio

- Possibilità di monitorare lo stato e le performance degli apparati da remoto tramite i seguenti strumenti e linguaggi di automation: Python, Ansible e Chef; ***(punti 0,4)***

- Possibilità di collezionare informazioni statistiche per interfaccia logica/fisica, firewall policies (hit e quantità di traffico), applicazioni layer 7 (hit e quantità di traffico) e classi QoS sorgente/destinazione. ***(punti 0,1)***

9.8.Resilienza ed Alta affidabilità

9.8.1. Alta disponibilità layer2/3

- Disponibilità di meccanismi di monitoraggio della raggiungibilità IP dei nodi del Cluster in grado di innescare in maniera autonoma, nel caso di mancata raggiungibilità, il failover dei nodi del cluster; ***(punti 0,1)***
- Per la funzionalità definita Equal Cost Multi Path (ECMP) i percorsi paralleli disponibili devono essere almeno 8. ***(punti 0,2)***

9.9.Qualità del Servizio (QoS), Routing and Filtering

9.9.1. Route filtering

Disponibilità delle seguenti funzionalità al fine di configurare ed implementare politiche di manipolazione del routing per mezzo della mutua redistribuzione tra diversi protocolli, sia dinamici che statici. La mutua redistribuzione deve essere configurabile mediante: ***(punti 0,2)***

- Scelta del protocollo di origine con supporto esplicito dei seguenti protocolli:
    - Bgp;
    - Direct;
    - Local;
    - IS-IS;
    - OSPFv2;
    - OSPFv3;

    - Static;
- scelta tramite l'utilizzo di prefissi di rete puntuali o aggregati;
- supporto almeno dei seguenti criteri per protocollo:
    - OSPFv2/3: area, route-type ed external-type;
    - IS-IS: level e route-type;
    - BGP: as-path, community, local-preference, origin, med e neighbor.

9.9.2. Packet filtering

Possibilità di poter effettuare le seguenti operazioni/azioni a seguito del "pattern matching" basato sulle regole di classificazione: ***(punti 0,2)***

- accept;
- discard;
- reject (Discard sending ICMP destination unreachable message);
- count (conteggio dei pacchetti che soddisfano l'access-list);
- Dscp (setting DSCP);
- Traffic Class (setting traffic class);
- rate-limiting;
- log;
- selezione di una routing table alternativa per effettuare policy routing.

9.9.3. Policing & Scheduling

Supporto del meccanismo Weighted Random Early Detection (WRED). ***(punti 0,2)***

9.9.4. Funzionalità di rete

- Supporto dei seguenti protocolli e funzionalità MPLS: RSVP, LDP, Fast Reroute (FRR), Point-to-Multipoint LSP; ***(punti 5)***
- Supporto dei protocolli Circuit cross-connect (CCC), translational cross-connect (TCC) e L2VPN VPLS, pseudowires; ***(punti 2)***
- Supporto dei protocolli L3VPN e NGMVPN multicast VPN. ***(punti 1)***

9.9.5. IP tunneling e overlay

- Supporto delle seguenti tecniche di encapsulation per estensione Layer 2/3 su rete pubblica IP: CCC over GRE over IPsec, L2VPN over GRE over IPsec, L3VPN over GRE over IPsec. ***(punti 2)***

9.10. Virtualizzazione e sistemi di convergenza

Supporto dei plugin per l'integrazione con l'orchestratore Openstack. ***(punti 0,2)***

9.11. Caratteristiche fisiche

- Presenza di documentazione tecnica che documenti che la quantità di calore media dissipata da ogni apparato in configurazione massima, espressa in Btu/hr sia:
    - pari o inferiore a 700 BTU/hr. ***(punti 1)***
    - maggiore di 700 BTU/hr ed inferiore o uguale a 1000 BTU/hr. ***(punti 0,3)***
    - maggiore di 1000 BTU/hr. ***(punti 0,1)***

- Presenza di documentazione tecnica che documenti che la quantità media di potenza assorbita sia:
    - pari o inferiore a 200W. ***(punti 1)***
    - maggiore di 200W ed inferiore o uguale a 400W. ***(punti 0,3)***
    - maggiore di 400W. ***(punti 0,1)***

- Presenza di documentazione tecnica che documenti che i valori di MTBF degli apparati sia:
    - pari o superiore a 100000 ore. ***(punti 1)***
    - inferiore a a 100000 ore. ***(punti 0,3)***

10 Apparati tipologia DC-Infra - Requisiti migliorativi

10.3. Configurazione, Backup e Gestione

- Archiviazione automatica delle configurazioni applicate all'apparato, per un numero pari o superiore a 50; ***(punti 2)***
- Possibilità di eseguire sull'apparato (in maniera nativa mediante un singolo comando dedicato sul sistema operativo e senza l'utilizzo di script aggiuntivi) una configurazione per un periodo di tempo predefinito (definibile dall'utente) al termine del quale, se non esplicitamente confermato, l'apparato ritorna automaticamente alla precedente configurazione attiva; ***(punti 6)***
- Possibilità di eseguire sull'apparato (in maniera nativa mediante un singolo comando dedicato sul sistema operativo e senza l'utilizzo di script aggiuntivi) un controllo sintattico della configurazione runtime (definita in memoria ma non attiva); ***(punti 4)***
- Possibilità di definire MIB personalizzate, ovvero MIB che siano popolate da informazioni definite dall'utente; ***(punti 0,2)***
- Possibilità di definire degli script (es. configuration script, event policies/script, operation script, SNMP/MIB script) al fine di eseguire in maniera autonoma processi di configurazione e gestione dell'apparato. Per la corretta valutazione del requisito in oggetto devono essere dettagliate le funzionalità degli strumenti di scripting disponibili. ***(punti 0,2)***

10.4. Strumenti di monitoraggio

- Possibilità di monitorare lo stato e le performance degli apparati da remoto tramite i seguenti strumenti e linguaggi di automation: Python, Ansible e Chef; ***(punti 0,4)***
- Disponibilità della funzionalità di remotizzazione del traffico in mirroring; ***(punti 0,1)***
- Possibilità di configurare le politiche di accounting e mirroring selezionando il traffico sulla base degli header a livello 2, 3 e 4 della pila OSI. ***(punti 0,2)***

10.5. Alta disponibilità Layer2

10.5.1. Link Aggregation

- Disponibilità di un meccanismo in grado di preservare la capacità di banda di interconnessione dello stack eseguendo il forwarding del traffico sulla stessa interfaccia dalla quale viene ricevuto il medesimo traffico, anche in presenza di un LAG configurato su differenti apparati dello stack; ***(punti 0,5)***
- Disponibilità di algoritmi che operano sia in modalità Layer 2 che Layer 3, finalizzati al bilanciamento del traffico che insiste sui membri del LAG, tali da incrementare la banda disponibile sul LAG stesso. ***(punti 0,5)***
  Tali algoritmi devono basarsi su campi di questo tipo:
  - IPv4 packet: Source IP, Destination IP, Source Port e Destination Port;
  - IPv6 packet: Source IP, Destination IP, Source Port, Destination Port e IPv6 Flow Label;
  - Non-IP frame: Source MAC e Destination MAC;
- Possibilità di configurare l'inoltro del traffico di tipo unicast sul membro locale del LAG dove è ricevuto tale traffico, ottimizzando quindi l'uso dei collegamenti dello Stack senza l'impiego dei membri non locali di tale LAG. ***(punti 0,5)***

10.5.2. Stacking

- Possibilità di estendere l'architettura inserendo all'interno dello stesso stack apparati differenti da quelli indicati nel capitolo 6.2 e che siano in grado di fornire almeno interfacce native in rame 10/100/1000 Mbps Base-T. ***(punti 2)***
- Implementazione di un meccanismo in grado di verificare e mantenere automaticamente tutte le informazioni relative ai membri dello stack e alla loro raggiungibilità, attraverso delle metriche di shortest-path che utilizzano meccanismi di hello-interval per reagire ed evidenziare qualsiasi cambiamento nella topologia dello stack stesso. ***(punti 0,5)***

10.5.3. Traffic load balancing

- Per la funzionalità definita Equal Cost Multi Path (ECMP) i percorsi paralleli disponibili devono essere almeno 8. ***(punti 0,2)***

- Presenza di un algoritmo, all'interno dell'architettura Stack, che permetta di rilevare flussi di traffico di tipo burst (flussi che proporzionalmente sono di dimensioni molto più grandi dei normali flussi) e che trasformi gli stessi in flussi di dimensioni ridotte. ***(punti 0,2)***

10.6. Qualità del Servizio (QoS), Routing and Filtering

10.6.1. Interfacce di Livello 3

Possibilità di configurare almeno 1024 interfacce di Livello 3 per permettere la comunicazione tra i diversi domini di broadcast di Livello 2. ***(punti 0,1)***

10.6.2. Route filtering

Disponibilità delle seguenti funzionalità al fine di configurare ed implementare politiche di manipolazione del routing per mezzo della mutua redistribuzione tra diversi protocolli, sia dinamici che statici. La mutua redistribuzione deve essere configurabile mediante: ***(punti 0,2)***

- Scelta del protocollo di origine con supporto esplicito dei seguenti protocolli:
    - Bgp;
    - Direct;
    - Local;
    - IS-IS;
    - OSPFv2;
    - OSPFv3;
    - Static;
- scelta tramite utilizzo di prefissi di rete puntuali o aggregati;
- supporto almeno dei seguenti criteri per protocollo:
    - OSPFv2/3: area, route-type ed external-type;
    - ISIS: level e route-type;
    - BGP: as-path, community, local-preference, origin, med e neighbor.

10.6.3. Packet filtering

Possibilità di effettuare le seguenti operazioni/azioni a seguito del "pattern matching" basato sulle regole di classificazione: ***(punti 0,2)***

- accept;
- discard;
- reject (Discard sending ICMP destination unreachable message);
- routing-instance (reindirizzamento di pacchetti verso una specifica virtual routing instance);
- vlan (reindirizzamento pacchetti ad una specifica vlan);
- count (conteggio dei pacchetti che soddisfano l'access-list);
- Dscp (setting DSCP);
- Forwarding Class (setting traffic class);
- interface;
- loss-priority;
- log.

10.7. Virtualizzazione e sistemi di convergenza

- Supporto dei plugin per l'integrazione con l'orchestratore Openstack; ***(punti 0,5)***
- Possibilità di configurare qualsiasi tipo di nodo dello Stack come FCoE transit switch in accordo con lo standard IEEE DCB e con lo standard FC-BB-5 del gruppo di lavoro T11; ***(punti 1,5)***

- Supporto protocollare quali Priority-based Flow Control (PCF), 802.1Qbb, FCoE Inizialization Protocol (FIP) snooping e data center Bridging Exchange (DCBX). ***(punti 1,5)***

10.8. Capacità Switching

Disponibilità di capacità switching non inferiore a 960 Gbps Full-Duplex sia per protocolli Layer2 che Layer3 (per full-duplex si intende un tipo di connessione che permette la comunicazione in due direzioni contemporaneamente alla massima velocità prevista dalla singola porta; quindi nel caso specifico lo switch deve poter gestire traffico in ingresso pari a 480Gbps e traffico in uscita pari a 480Gbps). ***(punti 2)***

10.9. Caratteristiche fisiche

- Presenza di documentazione tecnica che specifichi che la quantità media di potenza assorbita sia:
    - pari o inferiore a 450W. ***(punti 1)***
    - superiore a 450W ed inferiore a 600W. ***(punti 0,3)***
    - pari o superiore a 600W. ***(punti 0,1)***
- Presenza di documentazione tecnica che specifichi che il valore di MTBF sia:
    - superiore a 145000 ore. ***(punti 1)***
    - pari o superiore di 100000 ore e minore di 145000 ore. ***(punti 0,3)***
    - inferiore a 100000 ore. ***(punti 0,1)***

10.10. Prestazioni globali architettura DC-Infra

Supporto almeno delle seguenti prestazioni per motivi di scalabilità: ***(punti 1)***

Caratteristiche	**Valori minimi**	**Punti assegnati**
Mac Entry Scale	18000	0.2
IPv4 RIB entries	8500	0.2
ARP Entry	3000	0.1
BGP routes	3500	0.2
Multicast group	720	0.1
BGP Peers	100	0.1
OSPF neighbors	60	0.1

11 Apparati tipologia Gestione - Requisiti migliorativi

11.3. Log Management

- Possibilità di correlare eventi generati da differenti sorgenti (cap 5.7), sia tramite regole rilasciate dal produttore, sia tramite la creazione di regole personalizzate dalla stazione appaltante ***(punti 1)***

- Possibilità di eseguire script (python, perl, bash) automatici e personalizzati in base agli eventi rilevati. ***(punti 0,5)***

11.4. Virtualizzazione e sistemi di convergenza

Integrazione con architetture cloud Openstack (Newton) almeno per le funzioni di monitoring, host e network discovery, topology e visibility. ***(punti 0,5)***

11.4.1. Scalabilità della piattaforma di Gestione

- Possibilità di gestire contemporaneamente un numero crescente di dispositivi di tipologia DC-Infra e/o Security-FW con la sola aggiunta delle licenze necessarie, senza modifiche architetturali o aggiunta di altri nodi, secondo le seguenti fasce:
    - numero di dispositivi maggiore di 110 e inferiore o pari a 200. ***(punti 0,1)***
    - numero di dispositivi maggiore di 200 ed inferiore o pari di 500. ***(punti 0,3)***
    - numero di dispositivi maggiore di 500. ***(punti 1)***

- Possibilità di gestione, da parte del Log Collector, di un numero crescente di eventi per secondo, con la sola aggiunta di altri nodi all'architettura corrente, secondo le seguenti fasce:
    - numero di eventi maggiore di 2500 e minore di 50.000. ***(punti 0,3)***
    - numero di eventi maggiore di 50.000. ***(punti 1)***

12 Requisiti migliorativi generali

12.3. Consolidamento Sistema operativo

Utilizzo del medesimo sistema operativo per entrambe le tipologie di apparati: Security-FW, DC-Infra. ***(punti 10)***

12.4. Technical Assistance Center

Disponibilità, sugli apparati di tipologia Gestione, di sistemi di monitoraggio a carattere proattivo e di metodi di automazione nella gestione dei trouble ticket (ad esempio la generazione automatica di report sugli apparati per la diagnosi dei guasti o delle anomalie). In particolare sarà valutata la disponibilità di script, in esecuzione sui dispositivi forniti, che rilevano eventuali problemi (hardware, software e funzionali) sui dispositivi e che raccolgono informazioni sugli apparati stessi utili alla risoluzione dei problemi. Di seguito una descrizione più dettagliata delle caratteristiche e funzioni che, se presenti, costituiranno un requisito migliorativo: ***(punti 0,5)***

- gli script devono inviare, nella forma di incident/case, le informazioni raccolte ad una console software centrale oggetto della presente fornitura;
- la stazione appaltante deve poter identificare, sulla console, gli incident di interesse e per questi aprire in automatico via web casi tecnici presso la TAC del produttore; il sistema dovrà allegare al ticket tutte le informazioni rilevanti in termini di log, file diagnostica, support-information, ecc di cui tipicamente una TAC necessita per gestire le problematiche;
- la console, utilizzando i dati di inventario delle versioni software installate e dello stato di salute dei dispositivi e dei dati raccolti attraverso gli script sopra descritti, dovrà offrire funzionalità di gestione proattiva, come:
    - notifica di bug ai quali gli apparati della stazione appaltante e le loro relative configurazioni hardware e software potrebbero essere soggette;
    - l'analisi e la segnalazione di stati di EOL end of life / EOS end of support, ai quali la propria infrastruttura hardware/software potrebbe essere soggetta.