MINISTERO DELL'INTERNO

MINISTERO
DELL'INTERNO

CAPITOLATO TECNICO

Next Generation Firewall

Messa in sicurezza dell'infrastruttura di rete mediante acquisizione di sistemi firewall per il CED di Napoli e per il sito di DR di Bari.

Sommario

Indice delle Tabelle

Indice delle Figure

1 PREMESSA

Il presente capitolato definisce gli aspetti tecnici della fornitura di sistemi hardware e software e dei relativi servizi necessari per l'aggiornamento tecnologico dei sistemi firewall del CED della Polizia di Stato, ubicato presso il CEN di Napoli, e del sito di DR (Disaster Recovery), ubicato presso il CUB di Bari; tale aggiornamento tecnologico abiliterà la messa in sicurezza dell'infrastruttura di rete dell'Amministrazione.
La fornitura prevede l'acquisizione di due coppie di Next Generation Firewall, di un sistema di gestione centralizzato e dei relativi servizi di installazione, configurazione e assistenza. Inoltre dovrà essere erogato un periodo di formazione del personale dell'Amministrazione per poter mettere in condizioni gli amministratori del sistema di essere autonomi nella gestione quotidiana dell'infrastruttura.

1.1 Sigle e acronimi

Nell'ambito del presente Capitolato Tecnico sono stati usati i seguenti acronimi:

Tabella 1 - Sigle e acronimi

ACRONIMO	DESCRIZIONE
AS	AntiSpyware
AV	AntiVirus
AM	AntiMalware
DNS	Domain Name System
DR	Disaster Recovery
FTP	File Transfer Protocol
FW	Firewall
HLD	High Level Design
HTTP	HyperText Transfer Protocol
IPS	Intrusion Prevention System
LdS	Livello/i di Servizio
LLD	Low Level Design
NAT	Network Address Traslation
QoS	Quality of Service
RDP	Remote Desktop Protocol
RTI	Raggruppamento Temporaneo di Impresa
SAL	Stato Avanzamento Lavori
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

1.2 Definizioni

Nel corpo del presente documento i termini e le espressioni di seguito indicati devono essere interpretati secondo le seguenti definizioni:

- Fornitore: l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- Assistenza: l'insieme delle operazioni volte a mantenere in efficienza e/o ripristinare la piena funzionalità dei sistemi richiesti nel Capitolato Tecnico;
- Guasto bloccante: Si intende per guasto bloccante un malfunzionamento per cui è impedito l'uso di tutto il sistema o di una o più funzioni essenziali.
- Guasto non bloccante: Si intende per guasto non bloccante un malfunzionamento per cui è impedito l'uso di funzionalità non essenziali o critiche del sistema in alcune condizioni per cui non si ha un effetto penalizzante sull'operatività degli utenti.
- Incidente: evento che non è parte delle operazioni standard di un servizio, e che causa, o potrebbe causare, un interruzione o una riduzione della qualità del servizio stesso
- Malfunzionamento: è un impedimento all'esecuzione dell'applicazione /funzione o gli effetti che un errore ha causato sulla base dati o il riscontro di differenze fra l'effettivo funzionamento del software applicativo e quello atteso, come previsto dalla relativa documentazione.

2 SITUAZIONE ATTUALE

Il livello firewall attuale del CEN, distribuito nelle quattro sale CED che costituiscono il DataCenter, è costituito per ciascuna sala da una coppia di Cisco FWSM blade active-standby in modalità routed multicontext, ogni coppia di apparati blade è alloggiata in due Cisco Catalyst 6509 configurati in modalità stand-alone.
In ogni sala, sui firewall Cisco FWSM, sono stati creati, in base alle esigenze, un numero diverso di contesti i quali si contendono dinamicamente le risorse del sistema. Attualmente sono attivi complessivamente n.39 contesti firewall, per un numero totale di ACL-Rules implementate di c.a. 3000 col un massimo di c.a. 300 ACL-Rules per singolo contesto.
Per completezza si riportano di seguito il layout fisico (Figura 1) e logico (Figura 2) del Datacenter. In particolare nel layout fisico lo schema riportato della Sala CED è replicato per ciascuna della 4 sale che costituiscono il datacenter.

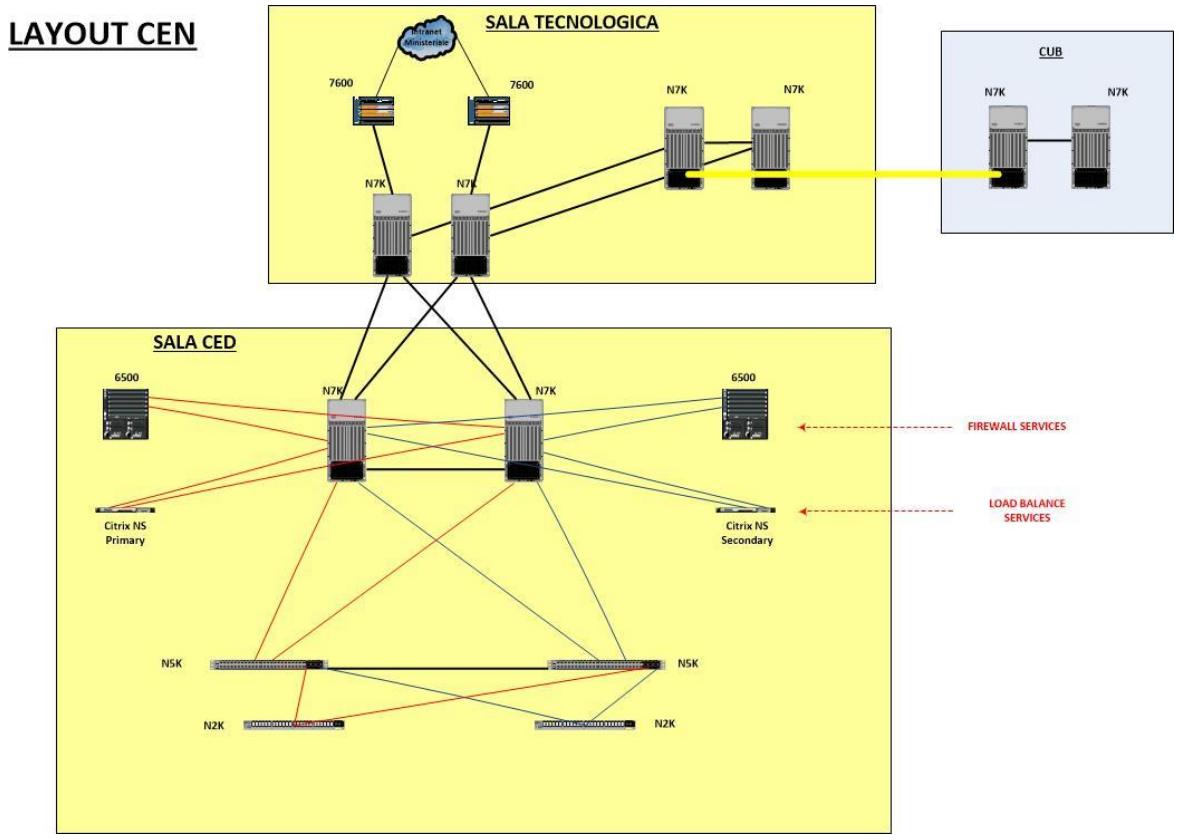

Figura 1 - Layout fisico

Il layout "logico" del Datacenter è riportato in figura 2.

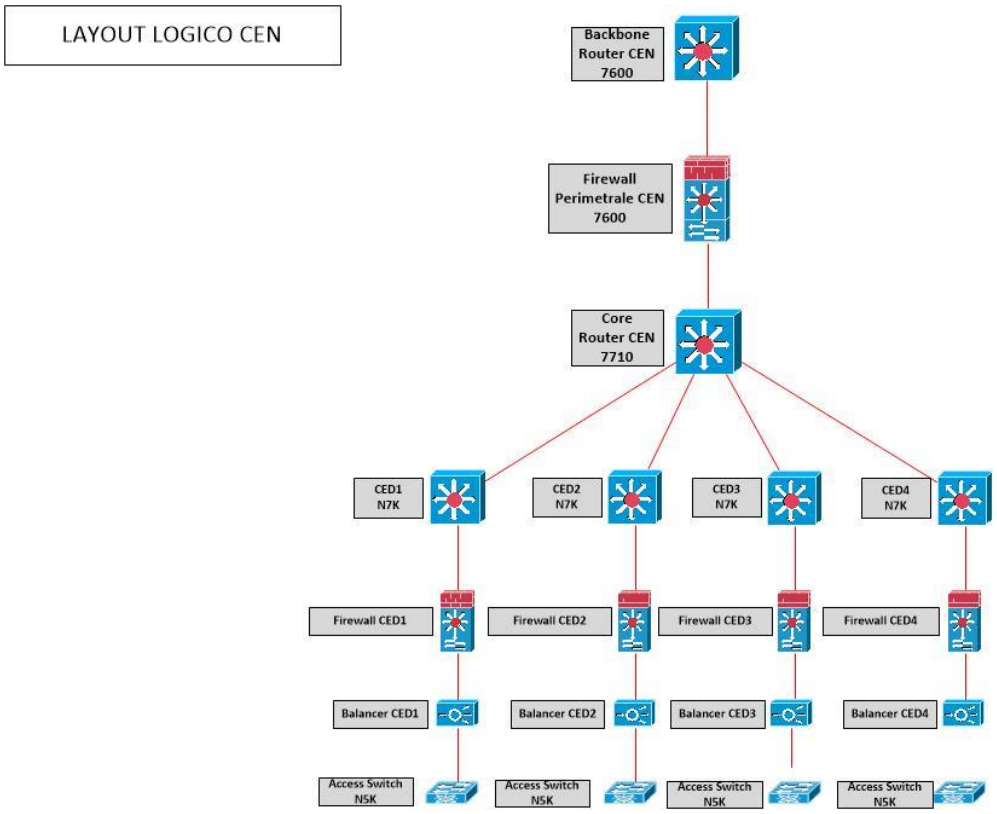

Figura 2 - Layout logico

Per quanto riguarda il CUB di Bari, l'architettura è identica al CEN di Napoli, con la sola differenza che le sale CED sono 2 invece che 4.

3 OGGETTO DELLA FORNITURA

L'oggetto della fornitura è rappresentato dal complesso degli apparati, dei servizi e delle attività come descritti nel presente capitolato:

- Fornitura di due coppie di Next Generation Firewall
- Fornitura di un sistema di gestione centralizzato
- Attività di progettazione
- Attività di installazione
- Attività di migrazione e configurazione
- Servizio di assistenza
- Supporto specialistico
- Formazione.

La fornitura dovrà conformarsi ai requisiti di base di seguito indicati:

- tutti i componenti dovranno soddisfare i requisiti e presentare caratteristiche tecniche non inferiori a quanto riportato nel presente capitolato tecnico;
- i componenti, laddove di pertinenza, dovranno essere forniti secondo le quantità, indicate nel presente capitolato tecnico;
- l'infrastruttura di sicurezza nel suo complesso ed i servizi ad essa correlati dovranno rispettare le normative vigenti in materia di sicurezza dell'informazione, di privacy, emissioni elettromagnetiche e sicurezza sul lavoro specificati nel paragrafo 4.6.

Il fornitore dovrà individuare un Responsabile della Fornitura, che costituirà il singolo punto di contatto nei confronti dell'Amministrazione. Il Responsabile della Fornitura dovrà coordinare tutte le attività e produrre resoconti periodici, che saranno presentati durante i SAL di progetto.

- per ciascun prodotto il fornitore fornirà una copia della manualistica tecnica completa, edita dal produttore; la documentazione dovrà essere in lingua italiana, oppure, se non prevista, in lingua inglese;
- il produttore, attraverso il progetto di alto (HLD) e basso livello (LLD), dovrà garantire l'interoperabilità e la compatibilità di tutti i sistemi che costituiscono la soluzione proposta e l'integrazione con l'ambiente esistente.

3.1 Etichette sugli apparati

Il fornitore dovrà posizionare apposite targhe (etichette) su tutte le apparecchiature hardware in fornitura; queste dovranno essere fissate in modo permanente e ben visibili. Le suddette etichette devono riportare fedelmente il design riportato nell'immagine seguente:

Le etichette devono avere una dimensione di 50mm di larghezza e 80mm di lunghezza. L'etichetta deve essere a colori e in particolare: per la bandiera dell'Unione Europea fondo blu RGB:0/0/153 e stelle dorate RGB:255/204/0 mentre per la bandiera della Repubblica Italiana colore verde RGB:0/146/70 e colore rosso RGB:206/43/55.

3.2 Sedi

Le attività saranno svolte presso il Centro Elettronico Nazionale della Polizia di Stato di Napoli, sito in via Miano 2 Napoli c/o il Real Bosco di Capodimonte e presso il Centro Unico di Backup della Polizia di Stato di Bari sito in via Cacudi 3 Bari c/o Centro Polifunzionale della Polizia di Stato secondo le modalità indicate nel presente documento.

4 INFRASTRUTTURA DI SICUREZZA

Nel presente capitolo sono riportati i requisiti minimi che dovranno obbligatoriamente essere rispettati e supportati nella soluzione proposta dal fornitore.
La soluzione deve essere composta da due coppie di apparati Next Generation Firewall da installare e configurare presso i CED primario e secondario della Polizia di Stato indicati nel paragrafo 3.2.

4.1 Architettura Hardware

Tutte le funzionalità richieste devono essere presenti su ognuno degli apparati proposti. Tali apparati dovranno essere basati su macchine fisiche con hardware dedicato (non sarà possibile proporre apparati su macchine virtuali) e il piano di inoltro del traffico dovrà essere costituito da hardware dedicato (es. CPU, ASIC, FPGA).
Ognuno degli apparati oggetto della fornitura dovrà essere dotato delle seguenti interfacce di rete (i transceiver devono essere inclusi nella fornitura):

- n.16 porte 10 Gigabit SFP+ (Short Range)
- n.2 porte 40 Gigabit QSFP+ (Short Range)
- n.1 porta in rame 10/100/1000 per la gestione
- n.1 porta Console.

Gli apparati devono essere dotati di almeno un disco di tipo SSD.
Gli apparati devono avere alimentazione e ventole di raffreddamento ridondate ed estraibili a caldo, inoltre devono poter operare a temperature tra 10° e 40°C con un tasso di umidità compreso tra 20% e 70%.
Gli apparati dovranno avere larghezza adatta a rack standard 19".

4.2 Funzionalità di base

Il Sistema Operativo degli apparati oggetto della fornitura dovrà essere basato su un'architettura software proprietaria, opportunamente progettata.
Gli apparati dovranno garantire le seguenti modalità di funzionamento:

- Livello 2 (trasparente): due interfacce, entrambe configurate per operare senza indirizzo IP, sono definite una di ingresso e l'altra di uscita. Il forwarding sarà effettuato inoltrando sull'interfaccia fisica di uscita ciò che viene ricevuto dall'interfaccia fisica di ingresso, previa verifica delle politiche di sicurezza;
- Livello 3: l'interfaccia è configurata per operare con indirizzo IP. Il forwarding sarà basato su modalità di inoltro al livello 3 della pila ISO/OSI (routing).

Gli apparati dovranno garantire contemporaneamente le funzionalità base di Firewalling, IPSec VPN e SSL VPN.

4.2.1 Alta Affidabilità (HA)

L'architettura deve prevedere la ridondanza dei servizi su due o più apparato, per assicurare l'alta affidabilità dei servizi stessi. I servizi non devono essere impattati nel caso di guasto di un singolo apparato o di un aggiornamento dell'architettura stessa.

- Modalità' operative tra gli apparati: Active/Passive, Active/Active (con condivisione del carico)
- Sincronizzazione delle configurazioni
- Sincronizzazione delle sessioni
- Failover del traffico tra gli apparati senza perdita di servizio
- Supporto del Link Aggregation Control Protocol (LACP), IEEE (802.3ad) su singolo apparato.

4.2.2 Virtualizzazione

È richiesto che l'architettura supporti la separazione logica di ogni apparato in almeno 40 contesti virtuali: deve essere possibile partizionare ogni apparato in differenti apparati virtuali che agiscano in maniera indipendente.
Gli apparati devono supportare le interfacce logiche con la separazione del traffico tramite 802.1q.

4.2.3 Stateful inspection

Gli apparati proposti dovranno essere in grado di riconoscere le applicazioni (livello 7 della pila ISO/OSI) indipendentemente dalla porta TCP/UDP utilizzata tenendo traccia delle connessioni attive.
Le regole di sicurezza dovranno permettere la gestione completa del flusso di traffico, intesa come possibilità di gestione di differenti livelli della pila ISO/OSI.
Dovrà essere possibile attivare o disattivare le regole *a caldo*, senza inficiare il funzionamento dell'apparato.

4.2.4 Network Address Traslation

Gli apparati proposti devono supportare i seguenti tipi di NAT:

- Destinazione o sorgente
- Statico o dinamico

4.2.5 Routing

Gli apparati dovranno essere in grado di supportare funzionalità di routing statico e routing dinamico (RIP, OSPF, BGP).
Gli apparati dovranno garantire la funzionalità di inoltro del traffico in base a specifiche regole indipendentemente dai percorsi riportati in tabella di routing (funzionalità nota come Policy Based Routing). Il traffico deve essere selezionato sulla base di regole di livello 3 e livello 4.

4.2.6 Virtual Private Network

Gli apparati dovranno supportare funzionalità di IPSec VPN, in modalità Gateway-to-Gateway e in modalità Client-to-Gateway, e di SSL VPN. Inoltre devono supportare gli algoritmi riportati di seguito:
Retrocompatibilità con algoritmi non raccomandati (fonte NSA e NIST)

- Algoritmi di cifratura DES, 3DES

- Algoritmi di autenticazione MD5, SHA-1
- IKEv1
- Perfect forward secrecy (DH groups) – 1, 2

Altri algoritmi

- Algoritmi di cifratura AES (128), AES (256)
- Algoritmi di autenticazione SHA-256
- Manual key, IKEv2, PKI (X.509)
- Perfect forward secrecy (DH) – 5 (1536 bits), 14 (2048 bits)
- Perfect forward secrecy (ECDH) – 19 (256-bit elliptic curve), 20 (384-bit elliptic curve)

Deve essere possibile configurare i gateways VPN in modalità ridondata.

4.3 Funzionalità evolute

Gli apparati oggetto della fornitura dovranno poter integrare le funzionalità di base, descritte nel paragrafo 4.2, con le seguenti funzionalità avanzate:

- Quality of Service
- SSL Inspection
- Intrusion Prevention System
- Anti Malware
- Application Control

4.3.1 Quality of Service

E' richiesto che l'architettura supporti le seguenti funzioni di QoS per la prioritizzazione del traffico.

- Configurazione di banda massima per indirizzo IP (Sorgente e destinazione) e servizio (Livello 4);
- RFC 2474 IP DiffServ in IPv4;
- Configurazione di filtri per determinare la Class of Service (CoS);
- Classificazione del traffico.

4.3.2 SSL Inspection

Gli apparati dovranno poter decifrare le sessioni SSL, in ingresso e uscita, per poter applicare le politiche e i controlli di sicurezza sul contenuto del traffico in transito.

4.3.3 Intrusion Prevention System

Gli apparati dovranno supportare funzionalità di IPS in modo da poter identificare minacce all'interno dei flussi di traffico che attraversano gli apparati stessi:

- Stateful protocol signatures: il traffico viene confrontato esclusivamente con le signature compatibili con il contesto del protocollo.
- 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
- Meccanismi di notifica degli attacchi: syslog
- 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.
- Protezione contro la proliferazione dei sistemi infetti con integrazione automatica con sistemi SIEM
- Possibilità di realizzare signature personalizzate
- Possibilità di configurare soglie di traffico per protocollo
- Frequenza degli aggiornamenti giornaliera in caso di emergenza per la diffusione di una nuova minaccia.

L'aggiornamento delle signature deve avvenire sia in modalità automatica che manuale.

4.3.4 AntiMalware

Gli apparati dovranno supportare funzionalità di AM in modo da poter identificare minacce all'interno dei contenuti del traffico che attraversa gli apparati stessi.
Gli apparati devono supportare la funzionalità sui seguenti protocolli: HTTPS, HTTP, FTP, SMTP e SMB.
Gli apparati dovranno essere in grado di analizzare il contenuto del traffico (es. file scaricati, file spediti, ecc.), identificare eventuali elementi malevoli e in caso positivo generare un alert e/o bloccare gli stessi contenuti malevoli in maniera automatizzata.
Dovrà essere possibile permettere, bloccare e controllare in maniera flessibile i tipi di file che vengono trasportati, attraverso la rete, tramite applicazioni.
L'aggiornamento delle signature deve avvenire sia in modalità automatica che manuale

4.3.5 Application Control

Gli apparati devono permettere il controllo sui flussi applicativi per permettere o negare il traffico di una o di un gruppo di applicazioni mediante le specifiche politiche di sicurezza.
Inoltre dovranno supportare la possibilità di controllare applicazioni sconosciute. In particolare dovrà essere possibile decidere se le applicazioni sconosciute possono attraversare l'apparato, da quali sorgenti oppure verso quali destinazioni possano essere abilitate.

4.4 Performance

Ogni singolo apparato dovrà raggiungere almeno i seguenti livelli di performance:

1. Gli apparati dovranno supportare singolarmente un throughput di almeno 70Gbps. Tale dato di throughput dovrà essere considerato per traffico UDP (64 Byte Frames) con la sola funzionalità di firewall abilitata.
2. Gli apparati devono avere una latenza massima di 30µs. Tale misurazione dovrà essere effetttuata per traffico UDP (64 Byte Frames) con la sola funzionalità di firewall abilitata, per un massimo di 1.500.000 di frames per secondo per gigabit di traffico.
3. Gli apparati dovranno supportare singolarmente un throughput di almeno 50Gbps. Tale dato di throughput dovrà essere considerato con la sola funzionalità di firewall abilitata e il seguente MIX di protocolli (Traffico TCP a 1024 bytes)
    - SMB 10%
    - RDP 2%
    - HTTPS 40%
    - HTTP 30%
    - FTP 3%
    - SSH 5%
    - DNS 5%

- SMTP 5%

4. Gli apparati dovranno supportare singolarmente un throughput di almeno 12Gbps. Tale dato di throughput dovrà essere considerato con tutte le funzionalità abilitate (FW – IPS – AM) e il seguente MIX di protocolli (Traffico TCP a 1024 bytes)
    - SMB 10%
    - RDP 2%
    - HTTPS 40%
    - HTTP 30%
    - FTP 3%
    - SSH 5%
    - DNS 5%
    - SMTP 5%
5. Gli apparati dovranno supportare singolarmente almeno 400k nuove sessioni TCP per secondo e 30M di sessioni contemporanee complessive.
6. Gli apparati devono supportare almeno 500 tunnel IPSec VPN
7. Gli apparati dovranno supportare singolarmente un throughput di almeno 12Gbps per la funzionalità di IPSec VPN con la seguente configurazione:
    - IPSec site-to-site
    - IKEv2
    - Pre-shared key
    - IKE & ESP encryption – AES(128)
    - IKE & ESP integrity – SHA256
    - IKE Diffie-Hellman – Group 5
    - Traffico TCP a 1024 bytes
8. Gli apparati dovranno supportare singolarmente almeno 40 contesti virtuali.

Il throughput dei punti 1, 3 e 4 deve essere misurato considerando le funzionalità attive in base al test richiesto e un insieme di politiche di sicurezza composto da almeno 100 regole distribuite in maniera omogenea tra regole FW (access list), NAT e IPS/AM. Tutte le regole devono avere il log attivato e solo l'ultima deve individuare il traffico interessante ai fini della misurazione.
Il throughput del punto 7 deve essere misurato considerando tutte le funzionalità attive e un insieme di politiche di sicurezza composto da almeno 100 regole. Tutte le regole devono avere il log attivato e solo l'ultima deve individuare il traffico interessante ai fini della misurazione.

4.5 Funzionalità di gestione

Gli apparati dovranno supportare il salvataggio di almeno due configurazioni di sistema per poterle richiamare nel caso si renda necessario ripristinare velocemente un servizio interrotto a causa di una configurazione errata (tale funzionalità può essere effettuata anche con il sistema di gestione centralizzato).

4.5.1 Autenticazione

Si chiede che sia obbligatoria l'autenticazione locale per la gestione degli apparati, tale autenticazione deve permettere la distinzione tra un profilo amministratore e un profilo utente (sola lettura).
Gli apparati firewall dovranno supportare l'autenticazione degli utenti mediante integrazione con server LDAP e RADIUS.
Il riconoscimento dell'utente dovrà essere utilizzato dall'apparato per selezionare il tipo di profilo e i permessi di accesso.

4.5.2 Monitoraggio e Logging

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

- SNMP V2 e V3
- Syslog (Gli apparati dovranno disporre della funzionalità di inoltro dei log verso un Syslog Server remoto, in caso di fault del sistema centrale di gestione i log devono essere memorizzati sugli apparati).
- NTP

4.5.3 Management

Gli apparati devono supportare i seguenti sistemi di management:

- Interfaccia Web per amministrazione del singolo nodo o del cluster accessibile in SSL/TLS
- Interfaccia CLI per amministrazione del singolo nodo o del cluster accessibile in SSH

Attraverso le suddette interfacce deve essere possibile effettuare le operazioni di configurazione, monitoraggio e troubleshooting. In particolare sul cruscotto dell'interfaccia grafica del singolo apparato o del cluster dovranno essere disponibili e riportate in maniera chiara le principali informazioni sulla stato del sistema.

4.6 Certificazioni e conformità

Tutto il materiale, pezzi o componenti non esplicitamente indicati nel presente capitolato, ma necessari per integrare le apparecchiature fornite con l'infrastruttura esistente, dovrà essere fornito, senza nessun altro costo aggiuntivo dovuto a mancanza di parti non indicate esplicitamente. Sarà pertanto cura del fornitore evidenziare e inserire in offerta eventuali componenti aggiuntivi, ritenuti essenziali per il corretto montaggio e funzionamento degli apparati, anche laddove questi non siano stati esplicitamente citati nel presente documento.
Tutte le apparecchiature e le opzioni eventualmente fornite dovranno essere nuove di fabbrica ed essere costruite utilizzando parti nuove.
Le apparecchiature offerte dovranno possedere marchi di certificazione riconosciuti da tutti i Paesi dell'Unione Europea, essere conformi alle norme concernenti la compatibilità elettromagnetica, alle normative CEI e, in generale, alla vigente normativa che disciplina i componenti e le relative modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori. A titolo esemplificativo e non esaustivo, le apparecchiature fornite dovranno rispettare i requisiti indicati nella Direttiva CEE 90/270 recepita dalla legislazione italiana con Legge 19 febbraio 1992, n. 142 e quelli relativi:

- alla riduzione dell'uso di sostanze pericolose previsto dalla normativa vigente, ed in particolare dalla direttiva 2002/95/CE, (RoHS), recepita con D .Lgs. 151/2005;
- ai requisiti di immunità definiti dalla EN55024;
- alla conformità alle Direttive di Compatibilità Elettromagnetica (89/336 e 92/31 - EMC) e conseguentemente essere marchiate e certificate CE;
- ai requisiti di sicurezza (es.: IMQ) e di emissione elettromagnetica (es.: FCC classe A) certificati da Enti riconosciuti a livello europeo.

5 SISTEMA DI GESTIONE

La soluzione di gestione centralizzata dovrà essere integrata con gli apparati firewall oggetto della fornitura. Il sistema di gestione potrà essere installato su una macchina fisica dedicata oppure su una macchina virtuale. Nel primo caso sarà onere del fornitore fornire l'intera soluzione mentre nel secondo caso sarà cura dell'Amministrazione fornire sia l'hardware che le licenze di virtualizzazione, il fornitore dovrà preoccuparsi della compatibilità con la soluzione di virtualizzazione presente al CEN (VMware vCenter 6.5).
Tale soluzione di gestione dovrà, nello specifico, abilitare:

- La gestione centralizzata delle configurazioni di sistema degli apparati (Configuration Management)
- La definizione centralizzata e la distribuzione delle politiche di sicurezza verso tutti gli apparati gestiti. Il sistema deve essere in grado di distribuire le regole su più cluster parametrizzando gli oggetti, in modo tale che uno stesso oggetto abbia valori differenti su differenti cluster.
- Il sistema dovrà disporre di strumenti per la verifica delle politiche di sicurezza configurate. In particolare deve generare degli alert in caso di regole che sovrascrivono altre successive.
- La raccolta e la correlazione centralizzata delle informazioni (log) degli apparati gestiti
- Logiche di autorizzazione di diversi profili di amministrazione basate su ruoli (RBAC - Role Based Access Control)
- Tutti gli alert generati dal sistema devono poter essere inviati via anche tramite SMTP/SNMP v2 o v3
- La generazione di report predefiniti o personalizzati relativi agli apparati gestiti. I report generati dovranno essere esportati nei formati CSV, PDF o XML
- Per ogni singolo apparato dovranno essere disponibili e riportate in maniera chiara le principali informazioni sulla stato del sistema. Tali informazioni dovranno almeno comprendere tutte le seguenti voci: interfacce con relativo stato, quantità di risorse attualmente utilizzate, modello hardware, identificativo univoco dell'apparato (es. numero di serie), informazioni generali sui parametri IP di gestione del nodo (es. IP Address, Default Gateway, Subnet Mask), utenti loggati, log di sistema e di configurazione.

6 SERVIZI

Al fine di assicurare la continuità e l'efficienza del servizio reso, il fornitore deve garantire l'installazione e la configurazione dei sistemi (paragrafi 6.2 e 6.3) e l'assistenza tecnica necessaria (paragrafo 6.3.1).
L'Amministrazione organizzerà un primo incontro con i responsabili del fornitore al fine di pianificare le attività successive. La data del kick-off meeting sarà assunta come data di inizio lavori.
L'attività lavorativa non potrà essere interrotta se non per brevi intervalli di tempo e durante particolari orari, questo comporterà che tutte le attività che implicheranno fermi macchina dovranno essere preventivamente concordate con l'Amministrazione.

6.1 Progettazione

Il progetto di alto livello (HLD) e il progetto di basso livello (LLD) relativo alle attività di installazione, configurazione, migrazione e rilascio della infrastruttura deve essere redatto dal produttore, il quale deve altresì fornire la documentazione relativa alle configurazioni di dettaglio di tutti i sottosistemi coinvolti nonché alle specifiche tecniche.
L'architettura e le configurazioni definite e documentate nel HLD e nel LLD saranno oggetto di verifica da parte dell'Amministrazione. Il produttore si impegnerà ad apportare eventuali modifiche e integrazioni che l'Amministrazione potrà eventualmente richiedere al fine di approvare i due progetti; l'approvazione finale del HLD prima e del LLD sarà vincolante per il prosieguo delle attività.

6.1.1 HLD

Questo documento deve descrivere la soluzione di alto livello in base ai vincoli dell'Amministrazione e ai requisiti fisici e logici. Il HLD deve contenere una descrizione dei concetti chiave del progetto, una panoramica della soluzione e un cronoprogramma; inoltre deve evidenziare la topologia che verrà utilizzata e quali protocolli saranno coinvolti.

6.1.2 LLD

Questo è un documento particolareggiato che verrà utilizzato dal fornitore al fine di implementare il progetto; esso dovrà contenere tutti i dettagli necessari ad implementare la soluzione e configurare i dispositivi.
In particolare il LLD dovrà contenere il seguente dettaglio:

- Architettura di rete
- Topologia di rete
- Servizi di rete
- Considerazioni di progettazione
- Naming Convention
- Progetto fisico della rete
- Progetto logico della rete.

Dovrà includere altresì un piano dettagliato e sarà composto almeno dalle seguenti attività:

- Cablaggio
- Installazione nuovo hardware
- Configurazione hardware
- Integrazione dei sistemi con gli apparati esistenti
- Migrazione
- Test di funzionamento di tutti i sistemi
- Collaudo finale di tutti i sistemi

Per ciascuna delle fasi deve essere presentata una scheda dettagliata comprensiva delle seguenti informazioni:

- Obiettivo
- Responsabilità
- Prerequisiti e dipendenze
- Tempi di esecuzione
- Risorse impiegate
- Potenziali disservizi e criticità
- Rollback in caso di problemi.

6.2 Installazione

La consegna degli apparati dovrà avvenire presso le sedi indicate dall'Amministrazione al paragrafo 3.2, secondo le tempistiche definite nel paragrafo 7; i materiali di risulta d'imballo saranno prelevati e smaltiti a cura del fornitore.
Sarà cura del fornitore fornire cavetteria, cablaggi e quant'altro necessario per la posa in opera e l'installazione di tutte le apparecchiature ai fine della loro corretta configurazione.
L'installazione e il cablaggio dell'intera infrastruttura dovrà terminare secondo le tempistiche definite nel paragrafo 7.

6.3 Migrazione e configurazione

Al completamento della fase di installazione il fornitore dovrà procedere alle attività di configurazione di tutti i sistemi previsti in fornitura e alla migrazione delle regole di sicurezza dall'ambiente esistente.
Il fornitore si impegna a nominare un responsabile tecnico incaricato di curare il coordinamento tecnico delle attività in fase di realizzazione e di migrazione dei primi ambienti, nonché di svolgere la funzione di unico referente nei confronti dell'Amministrazione.
Per le attività di migrazione e configurazione dovrà esser fornito un gruppo di lavoro formato da figure professionali con conoscenza dei sistemi in argomento.
Nell'ambito delle prove finalizzate alla verifica funzionale, il fornitore dovrà redigere e consegnare, entro il termine delle attività di configurazione, un rapporto contenente l'articolazione delle prove per la verifica dei requisiti.
L'Amministrazione si riserva la facoltà di rivedere e modificare l'articolazione ed il tipo dei test proposti.
La fase di configurazione e migrazione dei servizi dalla infrastruttura attuale a quella in fornitura si dovrà avvenire secondo le tempistiche definite nel paragrafo 7.

6.3.1 Gruppo di lavoro

Il gruppo di lavoro deve essere composto da sistemisti esperti e specialisti di prodotto che abbiano almeno 5 anni di esperienza nell'ambito delle attività sistemistiche e di networking, nel gruppo di lavoro deve essere presente almeno una figura che abbia conseguito la più alta certificazione, in ambito sicurezza, del produttore degli apparati proposti.
L'Amministrazione, al fine di assicurare un'adeguata copertura del servizio, richiede che il gruppo di lavoro sia costituito da figure professionali con conoscenze approfondite sulla soluzione di sicurezza oggetto della fornitura.
Le variazioni della composizione delle risorse professionali nel corso del progetto dovranno essere approvate dall'Amministrazione ed in ogni caso non potranno essere di spessore inferiore a quanto offerto in sede di gara.

6.4 Assistenza

Per tutte le apparecchiature in fornitura deve essere fornito un servizio di assistenza e garanzia per un periodo di trentasei mesi (36) decorrendo dalla data di verifica di conformità.
Il servizio di assistenza degli apparati consiste nel ripristino delle complete funzionalità, nella messa a disposizione di tutte le parti di ricambio in sostituzione e nell'esecuzione delle prove e dei controlli necessari a garantire il ripristino del pieno funzionamento degli apparati di proprietà dell'Amministrazione, entro i LdS di seguito indicati.
Il ripristino degli apparati deve avvenire a fronte di un guasto, blocco o altro inconveniente non bloccante, intendendosi per guasto qualsiasi anomalia funzionale che, direttamente o indirettamente, provochi l'interruzione o la non completa disponibilità delle funzionalità del sistema in questione o, in ogni caso, qualsiasi difformità del prodotto in esecuzione dalla relativa documentazione tecnica e manualistica d'uso.
Il fornitore, durante il periodo di validità contrattuale, dovrà effettuare il servizio di assistenza hardware e software secondo le modalità descritte nei seguenti paragrafi.

6.4.1 Gestione e assistenza dei sistemi

Sono comprese nel servizio di gestione e assistenza tutte le attività di:

- Installazione dell'hardware e del software, la loro configurazione e personalizzazione.
- Allineamento dei sistemi hardware e software alle più recenti innovazioni tecnologiche rilasciate dal produttore, nonché attivazione di tutte le attività necessarie per prevenire potenziali guasti dei sistemi e ripristino del funzionamento a fronte di eventuali guasti al fine di assicurare la regolare erogazione del servizio. Va precisato che le attività di innovazione tecnologica, come pure quelle relative alle correzioni, si riferiscono essenzialmente alla capacità di mantenere aggiornato ed in regolare stato di funzionamento sia il software che il firmware dell'hardware. A seguito del rilascio, da parte del produttore, di un aggiornamento e/o di una correzione software, l'attività di assistenza deve essere svolta in sinergia con quella di gestione, per l'esecuzione ed il controllo delle operazioni di modifica e upgrade dei sistemi in esercizio.

Dovranno essere previste, quindi, attività di assistenza preventiva (attività di assistenza atta a prevenire l'occorrenza di errori, malfunzioni e guasti) e di assistenza correttiva (attività di assistenza a seguito di segnalazioni di malfunzioni o guasti). Sono comprese in queste anche le attività volte al miglioramento o arricchimento funzionale, a seguito di migliorie decise e introdotte dal fornitore stesso che non comportano oneri contrattuali.

6.4.2 Assistenza hardware e software

Il fornitore deve garantire la fornitura di patches e aggiornamenti durante il periodo di copertura del contratto, inoltre deve permettere l'accesso gratuito al sito aziendale, dal quale sia possibile ricevere informazioni su nuove versioni e aggiornamenti dei prodotti hardware e software installati.
Il servizio di assistenza deve garantire una copertura di 7 giorni la settimana con orario h24.
Un tecnico provvederà ad una prima analisi del problema, a raccogliere le informazioni essenziali per poterlo gestire nel modo più efficiente e rapido ed infine a stimare i tempi di intervento.

6.4.3 Modalità di esecuzione

Il servizio di assistenza dovrà prevedere l'attivazione da parte del fornitore di un numero telefonico di contatto, di un indirizzo email e di un Trouble Ticket System (TTS) per la gestione dei guasti e malfunzionamenti di un apparato o di una componente di esso, attivo h24, sette giorni su sette, per 365 giorni l'anno. Entro la data di inizio dei servizi l'Amministrazione comunicherà alla società

aggiudicataria dell'appalto i nominativi e i gruppi di lavoro abilitati all'apertura delle chiamate da parte dell'Amministrazione.
Si precisa che, ai fini della misurazione dei livelli di servizio, l'orario di inoltro della chiamata via telefono o dell'email da parte dell'Amministrazione è considerato il riferimento temporale di apertura del ticket.
Il fornitore inserirà tale richiesta nel proprio TTS evidenziandone il livello di servizio ed assegnando ad essa un identificativo che dovrà comunicare all'Amministrazione all'apertura del guasto. Il sistema di gestione dovrà garantire il tracciamento della richiesta (stato dell'intervento) in tutte le sue fasi, fino alla chiusura dell'intervento stesso.
Il fornitore dovrà utilizzare parti di ricambio nuove di fabbrica, identiche alle parti sostituite e, ove esistenti, prodotte dallo stesso costruttore delle apparecchiature. Le parti di ricambio, il ritiro e lo smaltimento dovranno essere fornite dalla società aggiudicataria dell'appalto senza alcun onere per l'Amministrazione.
Nel caso in cui, a fronte di un guasto di un apparato, il fornitore non sia provvisto della parte di ricambio richiesta per la riparazione, potrà, al fine di ripristinare il servizio, operare la sostituzione con un altro sistema (o con un'altra componente) avente le medesime caratteristiche ed in grado di ristabilire la corretta e completa funzionalità. Tale soluzione è da considerarsi sempre e comunque provvisoria e non svincola il fornitore dall'obbligo di fornire l'apparato (o la componente) necessario per la riparazione. Il fornitore dovrà quindi intervenire nuovamente per operare la corretta sostituzione entro e non oltre 15 giorni lavorativi dal ripristino temporaneo del servizio.

6.5 Supporto specialistico

Per tutta la durata del contratto, l'Amministrazione potrà richiedere l'erogazione a consumo di un numero di giornate di supporto specialistico fino ad un massimo di 80 giornate, che potranno essere utilizzate per la realizzazione di diverse attività. A titolo esemplificativo ma non esaustivo, ne sono riportate di seguito alcune:

- implementazione di nuove funzionalità derivanti da specifiche esigenze di evoluzione dei sistemi di sicurezza non note al momento;
- stesura di procedure e politiche di sicurezza inerenti il funzionamento in esercizio della nuova infrastruttura;
- realizzazione di integrazioni personalizzate tra i sistemi forniti e quelli presenti attualmente all'interno dell'infrastruttura di rete.

Il supporto specialistico potrà essere richiesto dall'Amministrazione mediante e-mail (PEC), dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 e il sabato dalle ore 9.00 alle ore 13.00.
Il supporto specialistico dovrà essere erogato con i seguenti livelli di servizio:

- tempo di presa in carico, 1 (uno) giorno lavorativo dalla ricezione della richiesta: il fornitore deve prendere in carico la chiamata inviando una email di conferma alla persona di riferimento indicata dall'Amministrazione;
- tempo di intervento 5 (cinque) giorni solari dalla presa in carico: per intervento s'intende la presenza fisica della risorsa nella sede indicata nella chiamata.

Per l'espletamento delle suddette attività il fornitore dovrà avvalersi di personale certificato nella tecnologia oggetto di intervento (e comunque compresa nell'ambito della fornitura), ed in possesso di competenza ed esperienza su tematiche inerenti sia aspetti tecnologici sia aspetti di sicurezza informatica.
A seconda delle attività da svolgere, l'Amministrazione potrà richiedere che il personale sia in possesso di determinati requisiti e competenze professionali. A titolo esemplificativo ma non esaustivo di seguito vengo indicati alcuni dei requisiti professionali che di volta in volta potrebbero essere richiesti:

- almeno 5 anni di esperienza nella progettazione, e realizzazione di architetture di rete;

- esperienza comprovata di configurazione e tuning relativa alle componenti dell'Infrastruttura oggetto di fornitura;
- almeno 5 anni di esperienza in materia di sicurezza informatica, con particolare riferimento alla componente organizzativa, per la progettazione/realizzazione di Sistemi di Gestione della Sicurezza delle Informazioni;

Il fornitore dovrà produrre, di volta in volta, quanto necessario per consentire all'Amministrazione di comprovare l'esistenza della suddetta certificazione e dei requisiti professionali richiesti.
Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante apposita Relazione delle attività di Supporto Specialistico svolte, redatta a cura del fornitore ed accettata dall'Amministrazione, nella quale verranno indicati l'orario di inizio, l'oggetto e la durata dell'intervento stesso (mezza giornata o giornata intera a seconda della durata dell'intervento).

6.6 Formazione

Il fornitore dovrà erogare un servizio di formazione rivolto al personale tecnico dell'Amministrazione, o eventuale personale di società da questa designate, con lo scopo di fornire loro una adeguata conoscenza delle nuove tecnologie offerte, tale da consentire la gestione delle apparecchiature e dei prodotti software previsti nell'ambito della fornitura.
La formazione dovrà essere volta all'approfondimento di temi riguardanti l'utilizzo e la gestione dei nuovi prodotti oggetto di fornitura comprendendo le caratteristiche e le funzionalità salienti, con particolare riferimento alle configurazioni hardware e software adottate. Inoltre dovrà comprendere le comuni problematiche riscontrabili nell'implementazione della tecnologia nell'ambiente applicativo dell'Amministrazione.
Le nuove tecnologie oggetto di formazione devono essere legate ai nuovi apparati Next Generation Firewall inseriti all'interno dell'infrastruttura e al Sistema di gestione centralizzato.
Il fornitore dovrà erogare quattro sessioni di formazione (due a Napoli e due a Bari) della durata di 5 (cinque) giorni su tutte le componenti del sistema oggetto di fornitura, la prima sessione sarà di livello base mentre la seconda di livello avanzato. Inoltre dovrà provvedere alla fornitura della documentazione didattica per i discenti, sia su supporto cartaceo, sia su supporto elettronico.
Le sessioni di formazione dovrà essere svolta da personale certificato sui prodotti offerti e verrà tenute presso un apposito locale, adeguatamente attrezzato, messo a disposizione dall'Amministrazione.
Il fornitore dovrà produrre, di volta in volta, quanto necessario per consentire all'Amministrazione di comprovare l'esistenza della suddetta certificazione.
Le sessioni di formazione dovranno essere erogate, previo accordo con l'Amministrazione, entro un tempo massimo di 2 (due) mesi dalla data di accettazione della fornitura.
Il completo e corretto espletamento delle sessioni di formazione sarà certificato mediante apposita relazione sulla formazione svolta comprendente un questionario che indichi il livello di gradimento del corso da parte dei discenti, redatta a cura dell'Impresa di concerto con l'Amministrazione.
Il fornitore al termine di ogni sessione rilascerà ai partecipanti un attestato di partecipazione.

7 TEMPISTICHE E LIVELLI DI SERVIZIO

Si riepilogano di seguito le tempistiche caratterizzanti i servizi descritti nel capitolo 6.

- Kick off meeting: l'Amministrazione, nella persona del Direttore dell'Esecuzione Contrattuale, provvederà ad indire tale incontro entro 5 giorni lavorativi dalla data di esecutività del contratto. In tale sede il Fornitore dovrà presentare un piano di test per la verifica preventiva (paragrafo 8.1).
- Verifica preventiva: il laboratorio dovrà essere predisposto, pronto per l'utilizzo, entro e non oltre 15 giorni dall'accettazione del piano di test.
- Consegna degli apparati: dovrà avvenire entro 45 giorni solari dalla data di esecuzione con esito positivo della verifica preventiva.
- Installazione: entro 10 giorni solari dalla consegna degli apparati.
- High Level Design: il documento dovrà essere presentato entro 30 giorni solari dal Kick-off meeting.
- Low Level Design: il documento dovrà essere presentato entro 60 giorni solari dall'approvazione del documento HLD da parte dell'Amministrazione.
- Migrazione e configurazione: entro 120 giorni solari dal termine dell'installazione.

Si riportano di seguito, suddivisi per le voci oggetto della fornitura e relativamente al periodo di erogazione del servizio riportato nel presente capitolato, i livelli di servizio minimi attesi.

Tabella 2 - Livelli di Servizio

INDICATORE DEL SERVIZIO	VALORI DI SOGLIA	PERIODO DI OSSERVAZIONE
Tempistiche di progetto	Come da paragrafo 7	Una tantum
Numero di roll-back	Numero di rollback previsti a fronte della migrazione di un servizio: = 0	Per ogni servizio migrato
Servizi di assistenza e assistenza (guasti bloccanti)	Tempo di ripristino dell'infrastruttura o del servizio: ≤ 4 ore nel 95% dei casi ≤ 12 ore nel 5% dei casi	Trimestrale
Servizi di assistenza e assistenza (guasti non bloccanti)	Tempo di ripristino dell'infrastruttura o del servizio: ≤ 24 ore nel 95% dei casi ≤ 72 ore nel 5% dei casi	Trimestrale

8 VERIFICA DI CONFORMITÀ

Le operazioni di verifica di conformità saranno eseguite da una specifica commissione, a tal fine designata formalmente dall'Amministrazione, che dovrà verificare la piena funzionalità di tutti i sistemi e la loro corrispondenza ai requisiti imposti.
La verifica di conformità verrà suddivisa in due fasi:

1) verifica preventiva
2) verifica finale

8.1 Verifica preventiva

Nella verifica preventiva verranno verificate le funzionalità e le prestazioni degli apparati proposti nell'Offerta Tecnica. Il fornitore dovrà provvedere a propria cura e spese, ivi comprese le spese di viaggio, vitto ed alloggio per il personale della commissione, alla messa in opera di un laboratorio di test, per verificare dette funzionalità e prestazioni.
Al personale della commissione, durante le fasi di verifica di funzionalità delle suddette apparecchiature, dovrà essere fornita assistenza in lingua italiana o in lingua inglese.
Il fornitore deve presentare entro 5 giorni dalla firma del contratto un piano di test completo della topologia di rete, con l'indicazione di un efficiente programma di verifiche che sarà sottoposto ad approvazione da parte dell'Amministrazione. Le verifiche saranno eseguite secondo le modalità previste nel piano, fatta salva la facoltà della commissione di richiedere ulteriori accertamenti.
Il laboratorio dovrà prevedere la presenza degli stessi apparati offerti al fine di testare tutte le funzionalità richieste nel presente capitolato (requisiti minimi e requisiti migliorativi).
Tali apparati dovranno essere interconnessi tra loro e quindi bisognerà prevedere l'utilizzo di ottiche opportune, così come specificato nel Capitolato Tecnico.
Dovranno essere inoltre previsti misuratori di performance dello stesso tipo di quelli utilizzati per la stesura dei report secondo gli standard "Benchmarking Methodology Working Group (BMWG)" IETF:2544 (IPv4), 2889 (LAN switch), 3918 (Multicast), 5180 (IPv6) e 5965 (IP/MPLS).
Il laboratorio dovrà essere predisposto, pronto per l'utilizzo, entro e non oltre 15 giorni dall'accettazione del piano di test.
Sarà ritenuto accettabile uno scostamento delle performance dichiarate di ±5%, tuttavia nel caso in cui, a seguito delle necessarie verifiche effettuate in contraddittorio con il fornitore, risultassero non soddisfatti i requisiti dichiarati in sede di gara, si procederà alla rescissione del contratto.

8.2 Verifica finale

Per dare avvio alle operazioni di verifica finale, l'Amministrazione dovrà ricevere da parte del fornitore una formale comunicazione di approntamento al collaudo al termine della fase di migrazione e configurazione (Capitolo 7). Tale comunicazione dovrà essere corredata da un Piano dei Test Funzionali.
Nel corso della verifica di conformità, la Commissione avrà la facoltà di eseguire verifiche anche differenti da quanto indicato nella documentazione fornita a supporto. Inoltre, per facilitare le operazioni di collaudo, la Commissione potrà richiedere la presenza del DEC e di personale inviato dal fornitore.
All'atto dell'accettazione della fornitura, in caso di esito positivo della verifica di conformità, verrà redatto e sottoscritto dall'Amministrazione il verbale di collaudo ed accettazione, cui sarà allegato il documento rapporto di collaudo in cui sono tracciate le attività svolte durante il collaudo stesso.
La presenza di anomalie che, a giudizio dell'Amministrazione, per gravità o numerosità, non consentano lo svolgimento o la prosecuzione delle attività di collaudo provocherà la sospensione del collaudo stesso. La suddetta sospensione potrebbe comportare il mancato rispetto della data prevista di fine collaudo, per cause imputabili al fornitore. Le anomalie emerse in fase di collaudo devono essere rimosse entro il termine massimo di 15 giorni lavorativi.

9 AGGIUDICAZIONE

Le operazioni di aggiudicazione saranno eseguite da una specifica commissione, a tal fine designata formalmente dall'Amministrazione, che dovrà effettuerà le verifiche sulla base della documentazione tecnica prodotta dai concorrenti.
La commissione dovrà assegnare i punteggi sia tecnici che economici secondo i criteri previsti nel paragrafo 9.1. Al termine delle valutazioni deve essere stilata una graduatoria provvisoria.

9.1 Criteri di aggiudicazione

La gara viene aggiudicata a favore del concorrente che presenta l'offerta economicamente più vantaggiosa ai sensi dell'art. 95 comma 2 del D.lgs. 50/2016 e s.m.i., da individuare sulla base dei parametri e con i pesi di seguito elencati:

Tabella 3 - Criteri di aggiudicazione

CRITERIO	PUNTEGGIO MASSIMO
Punteggio tecnico	80
Punteggio economico	20
TOTALE	100

Il punteggio totale viene determinato dalla somma algebrica del punteggio dell'offerta economica (PE) e del punteggio tecnico (PT) calcolato applicando la seguente formula:

$$Y = P_E + P_T$$

La commissione giudicatrice procederà alla valutazione delle offerte tecniche e all'attribuzione del relativo punteggio con riguardo alle caratteristiche tecniche migliorative rispetto a quanto previsto dal Capitolato Tecnico in base ai criteri indicati nella tabella di valutazione tecnica Tabella 4 - Punteggi offerta tecnica.
I punteggi ottenuti dall'esame tecnico ed economico saranno quindi sommati al fine di ottenere la graduatoria provvisoria, aggiudicando la gara al concorrente che ha ottenuto il punteggio maggiore.
La gara viene aggiudicata all'offerta che consegue la massima valutazione totale. A parità di punteggio complessivo l'aggiudicazione avviene a favore dell'offerente che ha ottenuto il maggiore punteggio tecnico.

9.1.1 Definizione dell'offerta economica

Il punteggio relativo all'offerta economica sarà calcolato sulla base della seguente formula di tipo lineare che tiene conto del prezzo a base d'asta:

$$P_E = 20 \times \left(\frac{R_{off}}{R_{max}}\right)^{\alpha}$$

Dove:

- P_E è il punteggio economico assegnato all'offerta in esame;
- R_{off} è il ribasso dell'offerta in analisi rispetto al prezzo a base d'asta;
- R_{max} è il massimo ribasso rispetto al prezzo a base d'asta tra tutte le offerte pervenute;
- α è pari a 0,1;

SI precisa che saranno considerate le prime due cifre dopo la virgola senza procedere a alcun arrotondamento (es. PE: 3,2345 punteggio attribuito 3,23)

9.1.2 Definizione dell'offerta tecnica

Si sottolinea che l'assegnazione di ogni singolo punteggio deve essere il risultato non di una valutazione complessiva del servizio sotto esame, ma esclusivamente degli eventuali elementi migliorativi presentati rispetto alle caratteristiche minime richieste. Il mancato rispetto, oggettivamente riscontrato, di una o più di tali caratteristiche deve infatti portare ad una esclusione dell'offerta dalla procedura di gara e non, bensì, ad una discrezionale valutazione di inadeguatezza.
Di seguito vengono proposti i criteri che verranno utilizzati dalla Commissione per la valutazione delle Offerte Tecniche.

Tabella 4 - Punteggi offerta tecnica

	CRITERIO	PUNTEGGIO MASSIMO
Architettura Hardware		
1	Gli apparati dovranno avere risorse hardware distinte e dedicate per il piano di controllo (Management Plane) e per il piano di inoltro (Data Plane). Il traffico dovrà essere gestito esclusivamente sulle risorse hardware dedicate al piano di inoltro senza interessare il piano di controllo.	2
2	Verrà assegnato un punteggio migliorativo in base al numero di interfacce aggiuntive in dotazione al singolo apparato. - 0,2 punti per ogni interfaccia 10 Gigabit SFP+ aggiuntiva (max 3 punti) - 1 punto per ogni interfaccia 40 Gigabit QSFP+ aggiuntiva (max 2 punti)	5
3	Gli apparati dovranno disporre delle funzionalità base ed evolute descritte nei paragrafi 4.2 e 4.3, senza necessità di utilizzare alcun modulo software o hardware aggiuntivo o ulteriore apparato esterno.	2
4	Possibilità di creare un cluster composto da almeno 4 apparati fisici. Le performance totali del cluster devono essere: - FW traffico UDP (par.4.4 punto 1) - Throughput x 0.9 x numero di apparati - FW traffico MIX (par.4.4 punto 3) - Throughput x 0.8 x numero di apparati - NGFW traffico MIX (par.4.4 punto 4) - Throughput x 0.6 x numero di apparati Per Throughput si intende quello dichiarato nella sezione delle performance	5
Funzionalità di base		
5	Le modalità di funzionamento base dell'apparato proposto (Livello 2, Livello 3) descritte nel paragrafo 4.2 dovranno poter essere configurate contemporaneamente	2

	sull'apparato, su interfacce differenti, senza necessità di utilizzo di diversi contesti virtuali.	
Funzionalità evolute		
6	Gli apparati dovranno supportare la possibilità di controllare applicazioni sconosciute (che non sono all'interno del database dell'apparato) anche mediante la creazione di signature personalizzate. Inoltre dovrà essere possibile realizzare signature specifiche per applicazioni proprietarie in base a specifici campi che identificano l'applicazione all'interno del pacchetto TCP.	2
7	Dovrà essere possibile configurare la QoS per indirizzo IP (Sorgente e destinazione) e applicazione (Livello 7).	2
Performance		
8	Throughput FW tra 70Gbps (MIN) e 105Gbps (MAX) con traffico UDP come descritto al punto 1 del paragrafo 4.4	5
9	Throughput FW tra 50Gbps (MIN) e 100Gbps (MAX) con traffico MIX come descritto al punto 3 del paragrafo 4.4	15
10	Throughput NGFW (FW + IPS + AM) tra 12Gbps (MIN) e 36Gbps (MAX) con traffico MIX come descritto al punto 4 del paragrafo 4.4	15
11	Throughput VPN tra 12Gbps (MIN) e 40Gbps (MAX) come descritto al punto 7 del paragrafo 4.4	5
Funzionalità di gestione		
12	Gli apparati dovranno supportare l'autenticazione degli utenti mediante integrazione nativa con server LDAP e RADIUS, senza necessità di impiego di ulteriori moduli software hardware aggiuntivi o apparati distinti.	1
13	Gli apparati dovranno disporre della funzionalità di inoltro dei log verso più Syslog Server esterni	1
14	Gli apparati dovranno disporre della funzionalità di Captive Portal per abilitare l'autenticazione di client esterni non basati su sistemi di autenticazione Microsoft.	1
Sistema di gestione centralizzato		
15	Il sistema dovrà disporre di un motore di correlazione di oggetti ed eventi relativi a tutte le diverse funzioni di sicurezza attive sugli apparati e che garantisca una vista in tempo reale e aggregata delle attività sospette o eventi relativi ad attività malevole.	5
16	Il sistema deve supportare funzionalità di remediation automatiche e integrarsi con tool di vulnerability assessment. Inoltre deve fornire strumenti di controllo, risposta e gestione degli incidenti.	1
17	Il sistema deve permettere di confrontare due configurazioni (sia di sistema che dell'insieme di regole di sicurezza) ed evidenziare le differenze.	1
18	Il sistema deve integrare funzionalità di reportistica evoluta, tali funzionalità dovranno prevedere: - Almeno 30 report differenti che comprendano almeno 4 differenti categorie di informazioni.	2

	- La possibilità di creare report che evidenzino l'attività di un singolo specifico utente, selezionando un intervallo di tempo. - La possibilità di creare report (live) che si aggiornano con un refresh al più ogni 10 minuti	
19	Il sistema dovrà fornire un report sugli eventuali "botnet" presenti in rete, che evidenzi i comportamenti anomali e azioni malevole quali utilizzo di DNS dinamici, accesso a siti di recente registrazione, siti di Malware, ecc.	1
20	Il sistema deve permettere l'analisi della priorità delle regole sulla base dell'utilizzo delle stesse e fornire delle evidenze sulla migliore sequenza possibile delle regole	2
Servizi		
21	Oltre alla formazione descritta nel paragrafo 6.6, il fornitore deve fornire due corsi per 5 discenti, un corso base e uno avanzato, tra quelli ufficiali rilasciati dal produttore. I corsi devono avere una durata minima di 4 giorni ciascuno ed essere tenuti presso un training center da un istruttore certificato.	5

L'attribuzione del Punteggio Tecnico (P_T) sarà data dalla somma algebrica dei punteggi assegnati.

$$P_T = \sum_{1}^{21} P_i$$

Dove:

- P_i è il punteggio relativo al criterio i-esimo.

L'attribuzione dei punteggio (P_i) della sezione Performance (con i=8÷11) avverrà secondo la seguente formula:

$$P_i = \frac{P}{MAX - MIN} \quad (V_O - MIN)$$

Dove:

- P è il punteggio massimo attribuibile al criterio i-esimo;
- MAX è il massimo del valore di Throughput;
- MIN è il minimo del valore di Throughput;
- V_O è il valore di Throughput legato all'apparato offerto.

Si precisa che saranno considerate le prime due cifre dopo la virgola senza procedere a alcun arrotondamento (es. PE: 3,2345 punteggio attribuito 3,23).

10 MODALITÀ DI PRESENTAZIONE DELL'OFFERTA

Si riportano di seguito i criteri che ciascuna società concorrente deve seguire nel redigere la propria offerta.

10.1 Offerta Tecnica

L'offerta tecnica dovrà essere prodotta in lingua italiana priva di qualsiasi indicazione di carattere economico, dalla quale dovranno evincersi in maniera dettagliata le caratteristiche del servizi offerto. Lo schema di offerta tecnica richiesto, dovrà avere la struttura del capitolato tecnico (rispettando la sequenza dei capitoli e paragrafi), dalla quale si evincono in maniera diretta e dettagliata le caratteristiche di quanto offerto, mettendo a confronto le caratteristiche tecniche minime richieste e quelle offerte, le modalità di fornitura e di presentazione dei servizi oggetto di fornitura, con riferimento dei requisiti indicati nel capitolato tecnico.
Tale relazione dovrà:

- essere presentata su fogli singoli di formato DIN A4, non in bollo, con una numerazione progressiva ed univoca delle pagine;
- essere fascicolata con rilegatura non rimovibile e contenuta entro le 100 (cento) pagine;

Alla relazione in originale dovrà essere aggiunta una copia in formato elettronico non modificabile con la possibilità di eseguire ricerche di testo.

10.2 Offerta Economica

L'offerta economica dovrà essere presentata mediante la compilazione della seguente tabella, ovvero, in qualsiasi altra forma stilistica purché rappresenti, a pena di esclusione, i medesimi livelli di dettaglio e di informazioni:

Tabella 5 - Offerta economica

	Q.TA'	IMPORTO UNITARIO	IMPORTO TOTALE
Apparati Hardware			
Licenze (IPS – AM) - (Inserire per ogni riga il dettaglio dei servizi o licenze fornite)			
Licenze contesti virtuali			
Sistema di gestione			
Progettazione			
Installazione			
Migrazione			
Configurazione			
Assistenza			
Supporto Specialistico			
Formazione presso CEN Napoli			
Formazione presso CUB Bari			
TOTALE OFFERTA IVA ESCLUSA			
di cui oneri specifici per la sicurezza aziendale, di cui all'art. 95, comma 10 del D.Lgs. n. 50/2016			