

CAPITOLATO TECNICO

Infrastruttura di sicurezza

Sommario

1	PREMESSA.....	4
1.1	Sigle e acronimi.....	4
1.2	Definizioni.....	5
2	AMBITO DELLA FORNITURA.....	6
2.1	Descrizione dell'ambito.....	6
2.2	Utenza.....	6
2.3	Sedi.....	6
2.4	Infrastruttura.....	6
3	DEFINIZIONE DELLA FORNITURA.....	7
3.1	Oggetto della fornitura.....	7
3.2	Requisiti di conformità dell'infrastruttura.....	7
4	CARATTERISTICHE DELLA FORNITURA.....	9
4.1	Infrastruttura di sicurezza.....	9
4.1.1	Architettura Hardware.....	10
4.1.2	Funzionalità base.....	10
4.1.3	Funzionalità Evolute.....	11
4.1.4	Sandbox (opzionale).....	12
4.1.5	Management ed elementi di gestione.....	12
4.2	Cablaggio.....	13
4.3	Servizi di consegna e installazione.....	13
4.4	Servizi di configurazione.....	14
4.5	Supporto specialistico.....	14
4.6	Formazione.....	15
5	SERVIZI DI MANUTENZIONE.....	16
5.1	Manutenzione hardware.....	16
5.2	Manutenzione software.....	16
5.3	Modalità di esecuzione.....	17
6	VERIFICA DI CONFORMITÀ.....	18
7	CRITERIO DI AGGIUDICAZIONE.....	19
7.1	Definizione dell'offerta economica.....	19
7.2	Definizione dell'offerta tecnica.....	20
8	BASE D'ASTA E MODALITA' DI PRESENTAZIONE DELL'OFFERTA.....	22
8.1	Offerta Tecnica.....	22
8.2	Offerta Economica.....	22



Indice delle Tabelle

Tabella 1 - Architettura Hardware	10
Tabella 2 - Funzionalità di base.....	10
Tabella 3 - Funzionalità Evolute	12
Tabella 4 - Criteri di aggiudicazione	19
Tabella 5 – Punteggi offerta tecnica	21
Tabella 6 - Offerta economica	22

Indice delle Figure

Figura 1 - Infrastruttura di sicurezza	9
--	---



1 PREMESSA

Il presente capitolato definisce gli aspetti tecnici della fornitura di sistemi hardware e software e dei relativi servizi necessari per l'aggiornamento dell'infrastruttura di sicurezza del Dipartimento della Pubblica Sicurezza.

Fanno parte della fornitura anche le attività di consegna, installazione, configurazione e supporto alla verifica di conformità. Dovrà essere erogato un periodo di formazione e formazione del personale dell'Amministrazione per poter mettere in condizioni gli amministratori del sistema di essere autonomi nella gestione quotidiana dell'infrastruttura.

Le attività di personalizzazione verranno eseguite dal Fornitore, su richiesta del Committente, facendo ricorso al supporto specialistico, anche questo compreso nell'oggetto della fornitura.

Il presente documento è strutturato nei seguenti capitoli:

- Nel capitolo 2 è descritto il contesto in termini di caratteristiche applicative e di ambienti tecnologici.
- Nel capitolo 3 vengono descritte le componenti e i servizi oggetto della fornitura.
- Nel capitolo 4 vengono riportate le caratteristiche tecniche della fornitura, in termini di requisiti generali, di caratteristiche minime obbligatorie e di requisiti di conformità a cui devono necessariamente rispondere le apparecchiature fornite.
- Nel capitolo 5 vengono riportate le caratteristiche della manutenzione e dei relativi livelli di servizio.
- Nel capitolo 6 sono descritte le attività di verifica della conformità.
- Nel capitolo 7 sono descritti i criteri di aggiudicazione.
- Nel capitolo 8 viene descritta la base d'asta e la modalità di aggiudicazione delle offerte.

1.1 Sigle e acronimi

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

ACRONIMO	DESCRIZIONE
AS	AntiSpyware
AV	AntiVirus
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
LdS	Livello/i di Servizio
POP3	Post Office Protocol
SMB	Server Message Block
QoS	Quality of Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
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:

- **Amministrazione:** l'Amministrazione contraente, ovvero il Ministero dell'Interno;
- **Capitolato Tecnico:** il presente documento;
- **Committente:** l'Amministrazione responsabile del contratto, ovvero il Dipartimento di Pubblica Sicurezza;
- **Fornitore:** l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Fornitura:** quanto indicato come Oggetto di Fornitura e descritto dettagliatamente;
- **Impresa:** l'Impresa aggiudicataria della gara, eventualmente mandataria di un RTI;
- **Manutenzione:** l'insieme delle operazioni volte a mantenere in efficienza e/o ripristinare la piena funzionalità dei Sistemi richiesti nel Capitolato Tecnico;
- **Responsabile del progetto/servizio:** soggetto individuato dal Committente, che per una determinata attività progettuale o per un servizio, assume la responsabilità della conduzione dello stesso e, in particolare, costituisce l'interlocutore principale del Fornitore nell'esecuzione delle attività.
- **Servizio/i:** il servizio o l'insieme dei servizi connessi alla Fornitura in oggetto.
- **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.
- **Sistema di sicurezza (o Sistema),** espressione architettuale di una o più funzionalità dell'Infrastruttura di sicurezza, per esempio firewall, IPS, ecc.; ogni Sistema può essere costituito da uno o più Componenti di sicurezza;
- **Componente di sicurezza (o Componente),** un qualunque elemento hardware o software (per esempio nodo firewall, licenza software, interfaccia di rete, console di gestione, ecc.) dei Sistemi facenti parte dell'Infrastruttura di sicurezza;



2 AMBITO DELLA FORNITURA

2.1 Descrizione dell'ambito

L'obiettivo del presente capitolato tecnico è quello di descrivere i prodotti da acquisire per le esigenze del sistema di sicurezza del Ministero dell'Interno al fine di aumentare il livello di sicurezza delle trasmissioni informatiche e di diminuire il rischio di incidenti informatici.

2.2 Utenza

I prodotti oggetto della fornitura interessano principalmente gli utenti del Dipartimento della Pubblica Sicurezza e più in generale del Ministero dell'Interno.

2.3 Sedi

La Sede del servizio è presso il:

- Compendio Viminale (Piazza del Viminale 1, Roma)

2.4 Infrastruttura

A titolo indicativo di seguito vengono riportati i sistemi/apparecchiature attualmente in dotazione dell'Amministrazione, con indicazione della marca, modello e quantità con le quali i prodotti oggetto della Fornitura dovrà essere sostituito.

MARCA	MODELLO	QUANTITÀ
FORTINET	FortiManager 3000B	2
FORTINET	FortiAnalyzer 2000A	2
FORTINET	FortiSwich Blade	4
FORTINET	FortiGate FG5001A-FA2	18

3 DEFINIZIONE DELLA FORNITURA

3.1 Oggetto della fornitura

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

- Infrastruttura di sicurezza, secondo quanto descritto al paragrafo 4.1;
- Installazione e configurazione dell'infrastruttura, secondo quanto descritto nei paragrafi 4.3 e 4.4;
- Manutenzione in garanzia dell'Infrastruttura di Sicurezza, secondo quanto descritto al capitolo 5;
- Supporto specialistico di prodotto, secondo quanto descritto al paragrafo 4.5;
- Formazione, secondo quanto descritto al paragrafo ~~Errore. L'origine riferimento non è stata trovata.~~

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

1. tutti i componenti dovranno soddisfare i requisiti e presentare caratteristiche tecniche non inferiori a quanto riportato nel presente capitolato tecnico;
2. i componenti, laddove di pertinenza, dovranno essere forniti secondo le quantità, indicate al capitolo 4 del presente capitolato tecnico;
3. 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 3.2.

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

- per ciascun prodotto l'Impresa fornirà una copia della manualistica tecnica completa, edita dal produttore; la documentazione dovrà essere in lingua italiana, oppure, se non prevista, in lingua inglese;
- l'Impresa dovrà garantire l'interoperabilità e la compatibilità di tutti i sistemi che costituiscono la soluzione proposta.

3.2 Requisiti di conformità dell'infrastruttura

Il Fornitore dovrà garantire la conformità delle apparecchiature alle normative CEI o ad altre disposizioni internazionali riconosciute e, in generale, alle vigenti norme legislative, regolamentari e tecniche disciplinanti i componenti e le modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori.

Tutto il materiale hardware previsto nel presente appalto dovrà rispondere ai seguenti requisiti di carattere generale:

- essere consegnato completo di quanto necessario per il corretto avviamento, interconnessione con i sistemi esistenti ed utilizzo (cavi di alimentazione, cavi di connessione, adattatori, materiali di consumo di prima dotazione, ecc.);
- rispettare i requisiti stabiliti nel D.Lgs. 19 settembre 1994, n. 626;



- operare con una alimentazione di rete da 230V $\pm 10\%$, 50 Hz, secondo le caratteristiche dell'alimentazione della rete italiana ed i componenti dovranno rispettare le norme EPA;
- operare nell'intervallo di temperatura da 0°C a + 40°C e nell'intervallo di umidità compresa dal 20% all'90% senza condensazione;
- essere conforme:
 - o alle norme CEI 74-2 (EN60950), di sicurezza del prodotto;
 - o alla direttiva CEE 90/270 recepita con legge nr. 142 del 19 Febbraio 1992;
 - o ai requisiti di immunità definiti dallo Standard EN55024;
 - o ai requisiti di sicurezza (es. IMQ) e di emissione elettromagnetica (es. FCC) certificati da Enti riconosciuti a livello europeo;
- dove essere munito dei marchi di certificazione riconosciuti da tutti i paesi dell'Unione Europea e dove essere conforme alle norme relative alla compatibilità elettromagnetica;
- corredato della documentazione, sia in forma cartacea che digitale, per ciascun componente (e.g.: manuale d'uso e manutenzione) includendo la descrizione delle eventuali architetture realizzate.
- Le parti elettriche delle apparecchiature dovranno essere conformi allo standard EPA ENERGY STAR.

4 CARATTERISTICHE DELLA FORNITURA

I prodotti oggetto della fornitura dovranno attenersi ai requisiti illustrati nel presente capitolo. Si rappresenta che laddove vengano riportate caratteristiche tecniche, queste sono sempre da intendersi come requisiti minimi della Fornitura, se non diversamente specificato.

4.1 Infrastruttura di sicurezza

Il sistema di sicurezza deve essere in alta affidabilità e consiste di una soluzione cosiddetta Next-Generation in grado di filtrare tutti i flussi di traffico che attraversano l'infrastruttura e consentire il transito solo a quelli che rispondono alle regole definite.

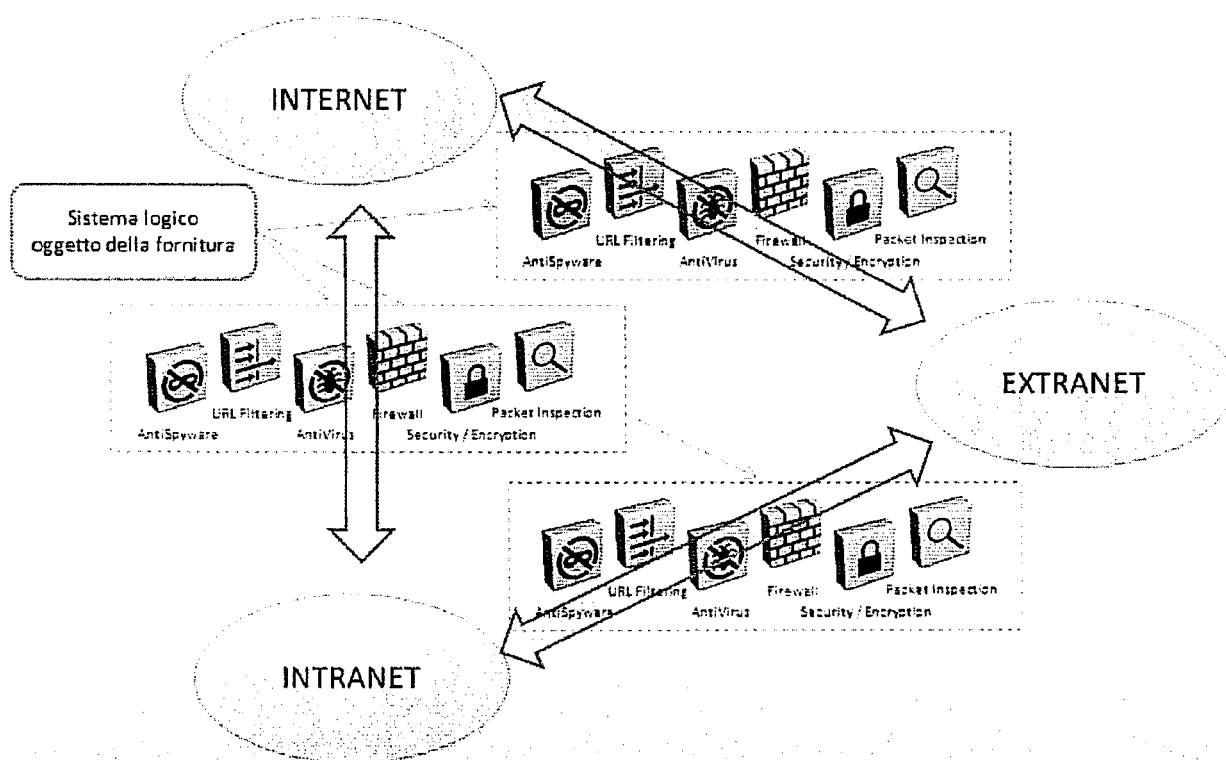


Figura 1 - Infrastruttura di sicurezza

Il sistema potrà essere formato da più componenti e nel suo complesso dovrà avere funzionalità di:

- firewall;
- concentratore VPN IPSec e SSL;
- protezione dalle vulnerabilità (IPS) o da malware (Antivirus/Antispyware);
- analisi dei contenuti in generale (File blocking; Data filtering);
- controllo della navigazione (URL filtering e Web filtering);
- controllo delle applicazioni (Application control);
- controllo della qualità del servizio (QoS) [opzionale].

I requisiti e le funzionalità si articolano su differenti argomenti che verranno dettagliati nei prossimi sottoparagrafi.

4.1.1 Architettura Hardware

Gli apparati devono essere basati su appliance con risorse hardware distinte e dedicate per il piano di controllo ed il piano di inoltro per garantire la massima affidabilità. Il traffico deve essere gestito esclusivamente sulle risorse hardware dedicate al piano di inoltro senza interessare il piano di controllo.

Le caratteristiche hardware sono da intendersi minime e relative ad ogni singolo componente.

Tabella 1 - Architettura Hardware

ID	CARATTERISTICA e FUNZIONALITA'	VALORE RICHIESTO
R.1	Marca/Modello	Dichiarare il valore
R.2	Quantità di apparati	Dichiarare il valore (≥ 2)
R.3	Struttura	Modello per Rack
R.4	Rack Unit Occupate	Dichiarare il valore
Q.1	Interfacce	- 4 porte GE base-T - 8 porte GE base-SX
R.5	Interfaccia di management	1 GE dedicata
R.6	Interfaccia di HA	Dedicata
R.7	Storage	Disco Solido (SSD) – dichiarare quantità e dimensione
R.8	Alimentazione AC	Ridondata e Hot-swap
R.9	Ventole di raffreddamento	Hot-swap
R.10	Temperatura operative	Da 0° a 40°C
R.11	Umidità	Da 20% a 90%

4.1.2 Funzionalità base

Gli apparati dovranno garantire funzionalità di firewalling, VPN IPSec e VPN SSL. Le politiche di sicurezza dovranno garantire la gestione completa del flusso di traffico e quindi essere in grado di gestire differenti livelli della pila ISO/OSI.

Le caratteristiche e le funzionalità sono da intendersi minime (salvo ove specificato) e relative ad ogni apparato.

Tabella 2 - Funzionalità di base

ID	CARATTERISTICA e FUNZIONALITA'	VALORE RICHIESTO
R.12	Modalità di funzionamento	- L2 (trasparent) - L3 (routing) - Monitoring
R.13	Routing	- OSPF (dichiarare il numero di rotte) - RIP (dichiarare il numero di rotte) - BGP (dichiarare il numero di rotte) - Statico

R.14	Multicast	- PIM-SM - IGMP
R.15	Alta affidabilità	- Active/Active - Active/Standby
R.16	Aggregazione di interfacce	802.3ad
R.17	VLAN	802.1q
R.18	Modalità di NAT	- NAT 1:1 - NAT n:n - NAT m:n
R.19	Crittografia	3DES – AES (128-bit, 192-bit, 256-bit)
R.20	Autenticazione	MD5 – SHA-1
R.21	Modalità di VPN	- IPSEC - SSL
R.22	Firewalling	stateful inspection
Q.2	Stateful Inspection Throughput	≥ 5 Gbps
R.23	3DES/AES VPN Throughput	≥ 1 Gbps
Q.3	Numero di sessioni concorrenti	≥ 1.000.000
Q.4	Nuove connessioni/secondo	≥ 120.000
R.24	Numero di tunnel VPN (IPSEC-SSL)	≥ 2.000
Q.5	Sistemi Virtuali	≥ 10
Q.6	QoS	8 classi di traffico con parametri per la larghezza di banda garantita, massima e prioritaria

Di seguito vengono riportate alcune precisazioni in merito alle funzionalità base richieste.

Le tre differenti modalità di funzionamento riportate nella tabella, al requisito R.12, devono poter essere configurate contemporaneamente sugli apparati e su interfacce, fisiche o logiche, differenti.

Ogni singola macchina deve garantire il forwarding del traffico in base a specifiche regole indipendentemente dai percorsi riportati in tabella di routing (funzionalità nota come Policy Based Routing) e calcolate su base IP (sorgente e destinazione), applicazione ed utente.

Al fine di ottimizzare e semplificare la fase di configurazione le regole di NAT devono essere indipendenti dalle regole di firewall.

Gli apparati devono supportare la possibilità di controllare applicazioni sconosciute sia mediante politiche di sicurezza specifiche che mediante la creazione di signature personalizzate. Inoltre tramite le policy di firewalling deve essere possibile decidere se le applicazioni sconosciute sono permesse.

4.1.3 Funzionalità Evolute

Gli apparati devono integrare funzionalità di IPS, Antivirus e Antispyware, File Blocking e Data filtering, URL filtering e Web filtering, Application control. Tali funzionalità devono essere aggiornate con modalità automatiche e manuali.

In particolare le funzionalità di Antivirus e IPS dovranno essere effettuate in hardware.

Gli apparati devono supportare almeno un throughput di 2Gbps con attive tutte le funzionalità IPS, Anti-Virus, Application Control, Url Filtering e AntiSpyware.

Tabella 3 - Funzionalità Evolute

ID	CARATTERISTICA e FUNZIONALITA'	VALORE RICHIESTO
Q.7	Throughput con tutte le funzionalità attive	≥ 2 Gbps

Le funzionalità di IPS serviranno per individuare i flussi anomali che attraversano l'infrastruttura di rete e deve essere possibile definire molteplici profili di sicurezza da applicare a policy di firewalling distinte.

Le caratteristiche obbligatorie del sistema IPS sono specificate di seguito:

- pacchetti formati in modo non corretto
- connessioni incomplete o non standard
- sovraccarico delle interfacce
- rilevazione di attacchi DoS
- controllo granulare delle applicazioni
- comportamento anomalo delle applicazioni (L7)
- comportamento anomalo dei protocolli (L3/L4)

Gli apparati devono supportare funzionalità di AV e AS su tutti i seguenti protocolli: HTTP, FTP, POP3, IMAP, SMTP e SMB. Inoltre devono essere in grado di riconoscere i file scaricati o spediti e bloccarli o generare un alert quando vengono rilevati.

La funzionalità di URL Filtering deve avere un database mantenuto a bordo dell'apparato per facilitare la gestione del sistema di categorizzazione.

4.1.4 Sandbox (opzionale)

Opzionalmente potrà essere messo a disposizione un servizio/funzionalità che permetta di verificare il comportamento di alcune tipologie di file che attraversano il nodo. In caso tale verifica risultasse positiva, dovrà essere resa disponibile una contromisura per tale malware entro le successive 48 ore. I file da controllare localmente o in remoto dovranno essere gestibili direttamente dalle politiche di sicurezza del nodo. Se la verifica viene effettuata tramite l'invio del file all'esterno, l'amministratore dell'apparato dovrà poter configurare le informazioni da inviare insieme al file (ad esempio source/destination port/IP address, utente, file name, url).

4.1.5 Management ed elementi di gestione

Le componenti del sistema dovranno avere una interfaccia grafica per la fase di configurazione, troubleshooting ed estrazioni di eventuali report. Queste funzionalità potranno essere sia embedded o essere installate su macchine di gestione esterne.

Di seguito viene riportata una lista dei protocolli minimi che devono essere supportati per la gestione del sistema:

- SSH
- SSL
- SNMP

- Syslog
- NTP

Deve poter essere permesso l'accesso agli apparati attraverso la configurazione e la profilazione di utenti locali.

Gli apparati devono poter autenticare gli utenti sia attraverso captive portal per permettere l'autenticazione di client non basati sul sistema operativo Microsoft Windows che mediante server Kerberos, Active-Directory, server LDAP e server RADIUS.

Il riconoscimento dell'utente deve poter essere usato dal device per decidere quali profili di firewalling, IPS, Anti-Virus e QoS, se presente, applicare.

Gli apparati devono supportare il salvataggio di configurazioni per poterle richiamare nel caso si renda necessario ristabilire velocemente un servizio interrotto a causa di una configurazione errata. Tutte le modifiche effettuate non dovranno essere immediatamente operative ma dovrà essere necessario forzare (tramite opportuno comando) il salvataggio della nuova configurazione.

L'apparato, tramite interfaccia grafica o console di gestione, deve mettere a disposizione strumenti che consentano il confronto fra due configurazioni salvate.

Sulla pagina iniziale dell'interfaccia grafica di management del nodo devono essere disponibili e riportate in maniera chiara le principali informazioni sulla stato del sistema.

Gli apparati devono mettere a disposizione strumenti di verifica delle politiche di sicurezza e di troubleshooting dell'apparato, tali strumenti devono essere presenti o sulla console di gestione o sull'interfaccia grafica del singolo componente.

4.2 Cablaggio

Per tutti gli apparati oggetto della fornitura sono richiesti tutti i cavi necessari alla realizzazione di tutti i collegamenti tra gli apparati di fornitura e la loro interconnessione con i dispositivi di rete esistenti, per assicurarne il corretto funzionamento, con una scorta del 20%.

Inoltre è richiesta la verifica funzionale dei collegamenti effettuati con gli apparati in fornitura.

4.3 Servizi di consegna e installazione

Dovrà essere erogato un servizio di installazione necessario alla messa in opera del sistema, si precisa che l'attività di consegna e di installazione si intende comprensiva di ogni onere relativo all'imballaggio, trasporto, facchinaggio, consegna al piano, posa in opera, installazione e asporto dell'imballaggio.

Tale servizio include:

- trasporto presso la sede dell'Amministrazione di tutti i materiali;
- assemblaggio, laddove necessario degli apparati;
- installazione degli apparati di rete e delle interfacce;
- attestazione di tutti i cavi necessari all'interconnessione degli apparati secondo uno schema di dettaglio che sarà concordato con l'Amministrazione.

4.4 Servizi di configurazione

Dovrà essere erogato un servizio di configurazione del sistema, tale servizio include :

- configurazione del sistema di sicurezza in alta affidabilità;
- configurazione delle interfacce di rete e dei processi di routing;
- configurazione del NAT;
- configurazione delle politiche di sicurezza;

Le specifiche di cui sopra devono essere intese al solo livello indicativo, la configurazione di dettaglio dovrà essere concordata con l'Amministrazione.

Per le attività di configurazione dovranno esser forniti un congruo numero di giorni uomo di un mix di figure professionali con conoscenza dei sistemi in argomento.

4.5 Supporto specialistico

Per tutta la durata del contratto, il Committente potrà richiedere l'erogazione a consumo di un numero di giornate di Supporto Specialistico fino ad un massimo di 20 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 dell'Infrastruttura 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.

Il Supporto Specialistico potrà essere richiesto dal Committente 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 erogata con i seguenti livelli di servizio:

- tempo di presa in carico, 1 (uno) giorno lavorativo dalla ricezione della richiesta: l'Impresa deve prendere in carico la chiamata inviando una email di conferma alla persona di riferimento indicata dal Committente;
- 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 l'Impresa 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.

Il personale di cui l'Impresa si avvarrà dovrà essere in possesso di determinati requisiti e competenze professionali e nello specifico:

- almeno n. 1 figura professionale con almeno 5 anni di esperienza nella progettazione, e realizzazione di architetture di rete;

- almeno n. 1 figura professionale con 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;

L'Impresa dovrà produrre, in fase di presentazione dell'offerta tecnico-economica, curriculum vitae in formato europeo per consentire al Committente di comprovare il possesso dell'organico aziendale delle figure professionali richieste.

Il servizio comprende tutti gli oneri necessari per la perfetta e puntuale esecuzione del medesimo.

Tutte le attività e gli interventi richiesti ed erogati saranno consuntivati mediante apposita Relazione delle attività di Supporto Specialistico svolte, redatta a cura dell'Impresa 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).

4.6 Formazione

L'Impresa 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 Next-Generation Firewall inseriti all'interno dell'infrastruttura.

L'Impresa dovrà erogare una sessione di formazione della durata di 5 (cinque) giorni su tutte le componenti del sistema oggetto di fornitura. Inoltre dovrà provvedere alla fornitura della documentazione didattica per i discenti, sia su supporto cartaceo, sia su supporto elettronico.

La sessione di formazione dovrà essere svolta da personale certificato sui prodotti offerti e verrà tenuta presso un apposito locale, adeguatamente attrezzato, sito in Roma e messo a disposizione dall'Amministrazione.

L'Impresa dovrà produrre, di volta in volta, quanto necessario per consentire al Committente di comprovare l'esistenza della suddetta certificazione.

Le sessioni di Formazione dovranno essere erogate, previo accordo con il committente, 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.

5 SERVIZI DI MANUTENZIONE

Per tutte le apparecchiature in fornitura deve essere fornito un servizio di assistenza e garanzia per un periodo di trentasei (36) mesi decorrendo dalla data di emissione del certificato di conformità.

Il servizio di manutenzione 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.

La prestazione dei servizi di manutenzione deve garantire una copertura di 7 giorni la settimana con orario continuativo H24, l'Impresa, durante il periodo di validità contrattuale, dovrà effettuare il servizio di manutenzione hardware e software secondo le modalità sotto descritte.

Tale servizio potrà essere esteso a discrezione dell'Amministrazione per ulteriori massimo diciotto (18) mesi (con periodo minimo di tre (3) mesi) al costo massimo pari alla metà del valore della "Manutenzione" come riportato nella tabella economica. Se il periodo richiesto è inferiore a diciotto (18) mesi, il costo del servizio sarà proporzionale ai mesi richiesti.

5.1 Manutenzione hardware

L'impresa si impegna alla fornitura delle parti di ricambio e gli interventi dovranno essere di tipo on-site.

Per quanto riguarda i guasti bloccanti:

- Tempi di ripristino entro 12 ore solari dalla chiamata

Per quanto riguarda i guasti non bloccanti:

- Tempi di ripristino entro 48 ore solari dalla chiamata

Uno specialista hardware provvederà ad una prima analisi del problema, a raccogliere le informazioni essenziali per poterlo gestire nel modo più efficiente e rapido.

5.2 Manutenzione software

L'Impresa 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 software installati.

Per quanto riguarda i guasti bloccanti:

- Tempi di ripristino entro 12 ore dalla chiamata

Per quanto riguarda i guasti non bloccanti:

- Tempi di ripristino entro 48 ore dalla chiamata

Uno specialista software provvederà ad una prima analisi del problema, a raccogliere le informazioni essenziali per poterlo gestire nel modo più efficiente e rapido.

5.3 Modalità di esecuzione

Il servizio di manutenzione dovrà prevedere l'attivazione da parte del Fornitore della predisposizione e comunicazione di un numero telefonico di contatto ed email (PEC) per l'apertura delle chiamate in caso di guasto/malfunzionamento 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 il Committente comunicherà al Fornitore 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 email da parte dell'Amministrazione è considerato il riferimento temporale di apertura della chiamata.

Il Fornitore inserirà tale richiesta nel proprio sistema di gestione Trouble Ticket System (TTS) evidenziandone il livello di servizio ed assegnando ad essa un identificativo che dovrà comunicare 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.

Le parti di ricambio, che dovranno essere nuove di fabbrica, identiche alle parti sostituite, verranno fornite dal Fornitore senza alcun onere aggiuntivo; le parti sostituite verranno ritirate dallo stesso che ne acquisirà la proprietà, assicurandone il trattamento in conformità alle norme vigenti.

Nel caso in cui, a fronte di un guasto di un apparato, il Fornitore sia sprovvisto 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) che dovrà essere approvato dall'Amministrazione se presenta caratteristiche tecniche inferiori. Tale soluzione è da considerarsi sempre e comunque provvisoria e non svincola il Fornitore dall'obbligo di fornire l'apparato (o la componente) richiesto per la riparazione entro e non oltre 10 giorni lavorativi dal ripristino temporaneo del servizio, verbalizzato nel "Rapporto di fine intervento".

6 VERIFICA DI CONFORMITÀ

Le verifiche di conformità saranno eseguite da una Commissione istituita con apposito decreto dell'Amministrazione.

Il Fornitore deve presentare un "Piano dei Test", con l'indicazione di un efficiente programma di verifiche che sarà sottoposto ad approvazione da parte dell'Amministrazione.

Il Fornitore garantisce tutta l'assistenza necessaria e mette a disposizione della Commissione tutte le apparecchiature e mezzi necessari alla effettuazione delle verifiche.

I collaudi vengono eseguiti con le modalità previste nel piano, fatta salva la facoltà della Commissione di richiedere ulteriori verifiche.

7 CRITERIO DI AGGIUDICAZIONE

La gara viene aggiudicata a favore del concorrente che presenta l'offerta economicamente più vantaggiosa ai sensi dell'art. 83 del D.lgs. 163/2006 e s.m.i., da individuare sulla base dei parametri e con i pesi di seguito elencati:

Tabella 4 - Criteri di aggiudicazione

CRITERIO	PUNTEGGIO MASSIMO
Punteggio tecnico	70
Punteggio economico	30
TOTALE	100

Il punteggio totale viene determinato dalla somma algebrica del punteggio dell'offerta economica (P_E) e del punteggio tecnico (P_T) 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 nelle tabelle di valutazione tecnica.

I punteggi ottenuti dall'esame tecnico ed economico saranno quindi sommati al fine di ottenere la graduatoria finale, aggiudicando la gara al concorrente che ha ottenuto il punteggio maggiore.

La gara viene aggiudicata all'offerta che consegue la massima valutazione totale. Tutti i calcoli saranno arrotondati alla seconda cifra decimale. A parità di punteggio complessivo l'aggiudicazione avviene a favore dell'offerente che ha ottenuto il maggiore punteggio tecnico.

7.1 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:

$$P_E = 30 \times \left(\frac{P_{\max} - P_{\text{off}}}{P_{\max} - P_{\min}} \right)$$

Dove:

- P_E è il punteggio economico assegnato all'offerta in esame;
- P_{off} è il prezzo offerto oggetto di valutazione;
- P_{\max} è il prezzo massimo offerto;

- P_{\min} è il prezzo minimo offerto;

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

7.2 Definizione dell'offerta tecnica

Il fornitore dovrà produrre una Relazione Tecnica descrittiva della soluzione proposta e dovrà rispondere a tutti i quesiti, a prescindere dalla tipologia R/Q, fornendo indicazioni circa la prestazione offerta dal prodotto disponibile già in fase di gara. Le risposte ai quesiti dovranno essere riportate in tabelle analoghe a quelle presenti nei paragrafi precedenti, introducendo il testo nei rispettivi riquadri. Si precisa che tutte le soluzioni proposte devono essere nella piena disponibilità dell'impresa, senza oneri aggiuntivi per l'Amministrazione e che quanto descritto nella Relazione Tecnica costituisce di per sé dichiarazione di impegno dell'impresa all'esecuzione nei tempi e modi descritti nella relazione stessa.

In caso di conformità parziale al requisito il fornitore dovrà esporre tutte le informazioni necessarie a chiarire il comportamento del prodotto ed i limiti della funzionalità effettivamente supportata rispetto alla funzionalità richiesta.

Ai fini di una più uniforme valutazione delle offerte, i Fornitori concorrenti sono chiamati, pena l'esclusione, a valorizzare le schede in allegato contenenti il riepilogo della fornitura ed il riferimento in offerta.

Il punteggio relativo all'offerta tecnica sarà calcolato sulla base della seguente formula:

$$P_T = \sum P_i$$

Dove:

- P_T è il punteggio tecnico assegnato all'offerta in esame
- P_i è il punteggio assegnato al requisito opzionale Q_i

A loro volta tutti i requisiti opzionali Q_i , salvo ove espressamente definito, verranno calcolati con la seguente formula lineare:

$$Q_i = \begin{cases} P_{\max} \times \left(\frac{V_o - V_{\text{base}}}{V_{\max} - V_{\text{base}}} \right) & \text{se } V_{\max} > V_{\text{base}} \\ P_{\max} & \text{se } V_{\max} = V_{\text{base}} \end{cases}$$

Dove:

- P_{\max} è il punteggio massimo assegnabile al requisito Q_i
- V_{\max} è il valore massimo assegnato al requisito tra tutte le offerte
- V_{base} è il valore minimo richiesto della Q_i
- V_o è il valore offerto nel requisito

Di seguito vengono riportati i punteggi assegnati ai requisiti opzionali:

Tabella 5 – Punteggi offerta tecnica

ID	CARATTERISTICHE E FUNZIONALITÀ	VALORE RICHIESTO	PUNTEGGIO
Infrastruttura di sicurezza			
Q.1	Interfacce	- 4 porte GE base-T - 8 porte GE base-SX	- 1 per ogni interfaccia GE base-T aggiuntiva (max 4 punti) - 2 per ogni interfaccia GE base-SX aggiuntiva (max 6 punti)
Q.2	Stateful Inspection Throughput	≥ 5 Gbps	10
Q.3	Numero di sessioni concorrenti	≥ 1.000.000	5
Q.4	Nuove connessioni/secondo	≥ 120.000	5
Q.5	Sistemi Virtuali	≥ 10	10
Q.6	QoS	Presente	5 se presente
Q.7	Throughput con tutte le funzionalità attive	≥ 2 Gbps	15
Q.8	Sandbox	Presente	10 se presente

8 BASE D'ASTA E MODALITA' DI PRESENTAZIONE DELL'OFFERTA

L'importo a base d'asta complessivo è fissato in €600.000, IVA esclusa; non saranno, quindi, ammesse offerte economiche che comportano una spesa superiore.

8.1 Offerta Tecnica

L'offerta tecnica dovrà essere presentata preferibilmente mediante la compilazione delle tabelle del paragrafo 4.1, ovvero, in qualsiasi altra forma stilistica purché rappresenti, a pena di esclusione, i medesimi livelli di dettaglio e di informazioni.

8.2 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 6 - Offerta economica

SOCIETÀ			
CODICE FISCALE			
OGGETTO	OFFERTA ECONOMICA per la partecipazione alla Gara con procedura ristretta e accelerata ai sensi del D. Lgs. 163 del 12 aprile 2006.		
	Q.TA'	COSTO UNITARIO	PREZZO COMPLESSIVO
Infrastruttura di Sicurezza (inserire per ogni riga il dettaglio di ogni singola appliance fornita)			
Servizi di configurazione/Installazione			
Supporto Specialistico	20 giorni		
Manutenzione	36 mesi		
Formazione	5 giorni		
TOTALE OFFERTA IVA ESCLUSA			
TOTALE OFFERTA IVA INCLUSA			