MINISTERO DELL'INTERNO
Dipartimento della Pubblica Sicurezza

DIREZIONE CENTRALE DEI SERVIZI TECNICO LOGISTICI E DELLA GESTIONE PATRIMONIALE

Capitolato Tecnico

Fornitura di una Piattaforma "Web Security gateway" con relativi servizi professionali a supporto per il Dipartimento della Pubblica Sicurezza

INDICE

1. Premessa 2

2. Prescrizioni in materia di sicurezza 2

3. Definizioni 2

4. Oggetto della fornitura 3

5. Descrizione della fornitura 4

6. Requisiti sistema di Web Security Gateway 4

7. Requisiti Gestionali e di Reporting 4

8. Requisiti Funzionali 6

9. Deployment e dimensionamento 9

10. Consegna, installazione, posa in opera. 11

11. Descrizione dei servizi 11

12. Formazione 13

13. Assistenza e manutenzione 13

14. Livelli di servizio 14

15. Verifica di conformità 14

16. Base d'asta 14

17. Criterio di Aggiudicazione delle Offerte 15

18. Presentazione dell'offerta economica 15

1. Premessa

Il presente documento disciplina gli aspetti tecnici, relativi la fornitura di una piattaforma di **Web Security gateway** per le esigenze del Dipartimento della Pubblica Sicurezza. L'obbiettivo primario è quello di garantire in sicurezza la navigazione sulla rete internet, delle postazioni di lavoro istituzionali.
La durata del contratto è di **36 mesi.**

Si rappresenta che in caso di **eventuale** discrepanza tra documenti tecnici, farà fede questo documento denominato *"**Capitolato Tecnico parte seconda".***

2. Prescrizioni in materia di sicurezza

Tutte le apparecchiature hardware fornite devono essere conformi alla normativa vigente che regolamenta la loro produzione, commercializzazione ed utilizzo; in particolare devono rispettare, ciascuna per le singole specifiche caratteristiche, le seguenti prescrizioni in materia di sicurezza:

- Legge 1 marzo 1968, n. 186 "disposizioni concernenti la produzione di materiali, apparecchiature, macchinari, installazioni e impianti elettrici ed elettronici";
- Legge 18 ottobre 1977, n. 791, così come modificata dal D. Lgs. 25 novembre 1996 n. 626, "attuazione della direttiva 93/68/CEE in materia di marcatura CE del materiale elettrico destinato ad essere utilizzato entro alcuni limiti di tensione";
- D. Lgs. 25 luglio 2005, n. 151, "attuazione delle direttive 2002/95/CE, 2002/96/CE e 2003/108/CE, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti";
- D. Lgs. 3 aprile 2006, n. 152, "Norme in materia ambientale";
- D. Lgs. 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro";
- Norme UNI e CEI di riferimento.

Il fornitore deve garantire che il prodotto fornito sia nuovo di fabbrica, corredato di marchio CE, devono corrispondere all'ultima versione in commercio, devono essere corredate di informazioni utili al loro smaltimento integrale o di parti di esse, in conformità con la vigente normativa in materia.

Il Fornitore dovrà produrre idonea documentazione in merito alla sicurezza di quanto fornito; in particolare, dovrà documentare l'eventuale presenza di sostanze nocive o cancerogene.

3. Definizioni

Nel seguito del documento si ricorrerà più volte ad alcuni termini cui è attribuito il seguente significato:

- **Amministrazione**: l'Amministrazione contraente, ovvero il Ministero dell'Interno;
- **Capitolato Tecnico parte seconda**: il presente documento**;**
- **Committente**: l'Amministrazione responsabile del contratto, ovvero il Dipartimento della 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;
- **Listini:** elenchi di prodotti e di servizi, corrispondenti a varie tecnologie, predisposti dal Committente oppure offerti dall'Impresa sulla base dei requisiti del presente Capitolato, da cui è possibile attingere gli oggetti delle varie acquisizioni;
- **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**: eventi negativi che compromettono alcuni aspetti dell'asset, della rete o della sicurezza.
- **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.

4. Oggetto della fornitura

Sono oggetto della fornitura:

- Nr. 30.000 Licenze di Web Security Gateway. (configurazione e gestione appliance, log, integrazione con sistemi di terze parti, feed intelligence) **ONPREMISE**.
- Nr. >= 3 Appliance fisiche per Web Security Gateway al fine di prevedere un sistema in alta affidabilità almeno di tipo 2 +1.
- Nr. 1 Sistema di gestione, con appliance fisico oppure con server dedicato.
- Nr.1 Sistema di gestione di backup
- 30.000 licenze che includono le seguenti funzionalità avanzate: Url Filtering, antivirus, visibilità, (analisi avanzata dei malware e security analitycs) "threat intelligence".
- Nr.1 Rack contenente l'hw totale e che sia compatibile con le appliances oggetto della fornitura.
- Servizi professionali 40gg.
- Servizi di manutenzione.
- Giornate di Formazione.

5. Descrizione della fornitura

Di seguito sono indicate le caratteristiche tecniche **minime** da rispettare a **pena esclusione**. Si precisa che per alcune caratteristiche è indicato un **valore minimo**, per altre è riportato l'esatto valore richiesto.

Criterio di aggiudicazione	Minor Prezzo
Ordinamento delle offerte	Al ribasso
Unità di misura delle offerte	Valuta euro
Valore Appalto specifico	**€ 510.000,00 IVA esclusa**
Durata del contratto	36 mesi
Soglia rilevanza comunitaria	Sopra soglia
Numero di lotti	1
Nome commerciale	• Zscaler • Symantec • Cisco • Forcepoint. • McAfee

6. Requisiti sistema di Web Security Gateway

I requisiti della piattaforma di Web Security Gateway sono suddivisi come di seguito:

• **Requisiti Gestionali e di Reporting**
• **Requisiti Funzionali**
• **Deployment**

7. Requisiti Gestionali e di Reporting

La piattaforma **deve** offrire almeno le seguenti funzionalità:

Requisito	**Conformità al requisito**
La soluzione deve avere un sistema di gestione sia direttamente sull'apparato/appliance (on box management) che centralizzato. E richiesto di fornire un sistema di gestione centralizzato delle appliance e dei log.	

Deve essere offerta una soluzione capace di gestire (aggiornamenti software, configurazioni) ed effettuare reports sia a livello di singolo apparato che in maniera centralizzata.	
L'appliance deve essere gestibile via interfaccia grafica in Https e da comand line in SSH.	
L'appliance deve supportare i seguenti meccanismi per trasferire i file log: FTP, SCP e Syslog.	
La soluzione deve supportare reports sul traffico utente, sul filtraggio di url, utente a maggior traffico e i maggiori threats malevoli riportati.	
Devono essere disponibili reports sulla banda utilizzata dagli utenti.	
Devono essere disponibili reports sulle richieste web bloccate dalla funzionalità di web reputation o dalla componente di anti-malware.	
Devono essere disponibili report sull'utilizzo della CPU delle appliance, utilizzo della RAM e disponibilità del disco fisso con la percentuale di utilizzo per reports e file di logs.	
I report devono essere generati almeno in formato pdf e in formato CSV.	
I report devono essere schedulabili per giorno/settimana/mese.	
La soluzione deve supportare il "rollover" automatico dei file di log quando è raggiunta la dimensione massima definita dall'amministratore o intervallo di tempo per la raccolta dei log. I file di log archiviati devono poter essere compressi per limitare occupazione di memoria sul disco fisso.	
L'appliance dei Web Security Gateway deve supportare un'interfaccia web che include un tool per simulare le richieste http degli utenti a scopo di troubleshooting in modo da analizzare il comportamento della soluzione di web proxy. Devono essere simulate richieste HTTP GET e Post.	

8. Requisiti Funzionali

Requisito	**Conformità al requisito**
La soluzione deve avere capacità di effettuare sullo stesso hardware le seguenti funzionalità: web proxy, url filtering, decryption del traffico TLS ed anti-malware.	
Il Web Proxy deve poter supportare implementazioni in modalità esplicita (expliciti proxy) che trasparente contemporaneamente. Inoltre deve essere capace di nascondere il client IP verso Internet.	
La soluzione deve fornire almeno 80 differenti categorie di contenuto (es. Adult, Pornography etc) e 20 categorie di Security Threats (includendo la categoria di "New Seen Domains" tendezialmente utilzzati come base di nuovi attacchi informatici).	
La soluzione deve supportare il controllo della banda in maniera granulare per utente, url, gruppi di utente, indirizzi IP sorgente/destinazione e tale controllo deve essere applicabile su base temporale.	
Devono essere supportati i seguenti servizi di proxy:http/https/FTP e SOCKS v5.	
La soluzione deve supportare la funzione di web traffic tap: una sua interfaccia fisica deve poter essere usata per inviare selettivamente traffico http e https (de-cifrato) verso una piattaforma esterna (es. IDS/IPS).	
La soluzione deve poter supportare categorie di URL di tipo "custom" ossia definite per specifici host name ed indirizzi IP	
La soluzione deve poter importare liste di specifici host name ed indirizzi IP (IoC) da server esterni per definire un'apposita categoria di feed esterni.	
La soluzione deve fornire uno score di reputation per ogni URL analizzato, lo score associato è stabilito in base a parametri come categorizzazione del url, presenza di virus/spam/spyware/phishing,	

registrazione del dominio,indirizzi ip associati al URL. Il web score derivato deve essere usato per attività di filtraggio delle url.	
Lo score di Web Reputation deve essere customizzabile in base a specifiche esigenze in modo che amministratore possa impostare cosa è permesso, bloccato o ulteriormente analizzato tramite engine di anti-malware	
La soluzione deve poter mostare verso gli utenti un messaggio personalizzabile sulle motivazione perché la richiesta web è stata bloccata	
La soluzione deve identificare e bloccare le pagine Web con script JavaScript, applicazioni ActiveX dannose (o non autorizzate), blocco di programmi o software eseguibili potenzialmente dannosi.	
La soluzione deve essere configurata per bloccare donwload di file basandosi su caratteristiche come file size e tipo di file (pdf,xml,zip,exe,mp4,avi,wmv).	
La soluzione si deve integrare con Active Directory, LDAP e Radius server per autenticazione utente, con possibilità di gestire autenticazioni e autorizzazioni su attributi e gruppi del direttorio.	
La soluzione deve permettere il signle sign on per utenti di dominio autenticati via AD	
La soluzione deve fornire almeno due diversi motori di anti-virus per analisi inboud che outbound del traffico web.	
La soluzione deve fornire un database di Url per bloccare liste di categorie di url di phishing, malevoli (etc) con aggiornamenti di tipo real-time.	
La soluzione deve fornire funzionalità anti-malware, anti-virus e anti-bot sia per il traffico in-bound che out-bound includendo l'analisi per file compressi.	
La soluzione deve supportare funzionalità avanzate di anti-malware che permettono di verificare la reputazione del file in transito (es. identificandolo tramite SHA-256) tramite feedback dalla Threat Intelligence del vendor proposto. La soluzione	

deve essere capace di monitorare continuamente i file analizzati ed in caso di modifica del verdetto (es. da "clean" a "bad") eseguito dalla Threat Intelligence del vendor proposto, deve notificarlo sul sistema di gestione tramite opportuno messaggio identificando utente che ha scaricato il file.	
La soluzione deve supportare TLS 1.3 sia in passthrough che in decrypt mode. In passthrough, è il client che stabilisce la sessione TLS con il server (WWW) mentre in modalità decrypt, la soluzione mantiene due sessioni una con il client e l'altra con il server (WWW) tramite funzionalità di "man in the middle".	
La soluzione deve poter essere integrata con soluzione DLP di terze parti.	
Per analisi evoluta dei threats malevoli, la soluzione di web proxy deve essere integrabile con soluzioni avanzate di machine learning a cui inviare i log (formato W3C) in forma anominizzata (ossia cifrando gli identificativi dell'utente come ip address e username tali da renderli non identificabili sulla piattaforma di machine learning) . La soluzione di machine learning deve essere offerta ed integrata nella soluzione di web proxy proposta tramite opportuna licenza.	
La soluzione deve supportare i seguenti proxy log:Apache, Squid and W3C.	
La soluzione deve supportare IPv6.	
La soluzione deve poter bloccare accesso ad Internet su base IP addresses, range di indirizzi IP, subnet e CIDR. Inoltre deve poter forzare l'autenticazione per sessioni provenienti da specifici IP, subnet o CIDR.	
Deve supportare la funzionalità di bloccare applicazioni che effettuano la tunnellizzazione di traffic non HTTP su porte tipicamente utilizzate per traffico HTTP	
La soluzione deve essere nativamente integrata con almeno una soluzione NAC (Network Access Control) in modo da definire le politiche di accesso ai siti web sulla base delle informazioni di	

contesto condivise dalla piattaforma NAC tramite tramite API	
La soluzione deve gestire on board il deployment dei PAC file, in modo che i web browser utente possono automaticamente scegliere il corretto web proxy.	
La soluzione deve supportare meccanismi di alta affidabilità sia in un deployment di tipo trasparente (es. tramite protocollo WCCP) che in modalità esplicita (es. PAC File, DNS)..	
Il portale di supporto del vendor deve permettere all'amministatore della soluzione di controllare la categoria associata ad un URL e sottomettere nuovi URL per un'opportuna categorizzazione	
La soluzione di Web Proxy deve essere integrata nativamente con una soluzione di Threat Hunting inclusa all'interno della fornitura.	

9. Deployment e dimensionamento

Requisito	**Conformità al requisito**
Il sizing della soluzione deve supportare 30000 utenti che generano almeno 3000 sessioni http/https per secondo, di cui il 60% di tipo https, con le funzionalità di Url Filering, Reporting, due motori di antivirus abilitati. La soluzione proposta deve poter gestire almeno 9000 connessioni per secondo (senza alta affidabilità) e 6000 connessioni per secondo considerando un appliance dedicato alle funzionalità di backup. La soluzione proposta deve poter supportare almeno 330000 connessioni contemporanee (senza alta affidabilità) e 220000 connessioni contemporanee considerando un appliance dedicato alle funzionalità di backup. Tale soluzione deve essere impiegabile con almeno 3 appliances fisici includendo meccanismi di alta affidabilità di tipo N+1 (dove N è pari almeno 2).	

Si richiede di fornire informazione del vendor da cui si evince la fattibilità del dimensionamento della fornitura, per quanto concerne sia traffico indicato, sia le appliances necessarie alla sua gestione, eventualmente tramite un simulatore messo a disposizione dal vendor.	
Gli appliances fisici in fornitura devono avere la ridondanza dell'alimentazione (power dupply), almeno 6 porte 1Gbps di tipo 1000BaseT ed 2 porte 10Gbps di tipo 10GbaseSR, ed avere i dischi H/D di tipo "hot swappable".	
Appliance di web security gateway deve essere composto da una piattaforma con doppia CPU, almeno 64GB di RAM, almeno 9.6 TB per lo storage HD in configurazione RAID10	
Appliance o server per il sistema di gestione deve essere composto da una piattaforma con doppia CPU, almeno 32GB di RAM, almeno 9.6 TB di storage HD in configurazione RAID10. Deve essere supportata la ridondanza dell'alimentazione, 6 porte 1Gbps Base T ed i dischi storage (HD) devono essere di tipo "hot swappable".	
Il sistema di gestione centralizzato deve essere basato su un appliance o server dedicato al management, deve poter essere possibile effettuarte il backup dei dati di web tracking e reporting su un sistema di gestione secondario.	
Il sistema di gestione deve effettuare la retention dei log (web tracking e reporting) per almeno 60 giorni.	
Sia le appliance di web security gateway che il sistema di gestione devono poter essere installati in rack standard di tipo 19-in (larghezza)	
.Deve essere fornito accesso al supporto del vendor in modalità **24x7 per la diagnostica di problematiche software**, mentre il replacement del hardware malfunzionante deve essere di tipo 8x5 con spedizione del componente di ricambio al massimo il giorno lavorativo successivo all'apertura del guasto	

10. Consegna, installazione, posa in opera.

La consegna degli apparati deve avvenire presso la sede di Roma indicata dall'Amministrazione.
Sarà cura dell'aggiudicatario 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.

La realizzazione e l'installazione dell'intera infrastruttura, ovvero, il processo di migrazione degli attuali 25000 utenti, verso la piattaforma offerta dovrà avvenire entro un **massimo di 20 gg** solari dalla consegna di tutto il materiale e dalla data di esecuzione del contratto. La consegna dovrà avvenire al piano indicato della relativa sede.

Per motivi di segretezza, le informazioni relative alle attuali configurazioni da migrare veranno condivise solo con l'aggiudicatario della gara.

11.Descrizione dei servizi

Al fine di garantire la continuità e l'efficienza del servizio reso, il fornitore deve garantire l'installazione e la configurazione dei sistemi della fornitura e l'assistenza tecnica necessaria.

Piano di progetto

L'Amministrazione organizzerà un primo incontro (kick-off meeting) con i responsabili della ditta 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.
Il piano di lavoro per l'installazione di tutti i sistemi sarà composto almeno dalle seguenti attività:

1. Cablaggio
2. Installazione nuovo hardware
3. Configurazione hardware
4. Integrazione dei sistemi con gli apparati esistenti
5. Test di funzionamento di tutti i sistemi
6. Collaudo finale di tutti i sistemi

Analisi, progettazione e pianificazione.

Il fornitore ha l'onere di redigere il progetto esecutivo relativo alle attività di installazione, configurazione, e rilascio della infrastruttura. 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 progetto esecutivo saranno oggetto di verifica da parte dell'Amministrazione. Il fornitore si impegnerà ad apportare eventuali modifiche e integrazioni su indicazione dell'Amministrazione al fine di approvare il progetto esecutivo: l'approvazione finale del progetto esecutivo sarà vincolante per il prosieguo delle attività.
Si specifica che il progetto esecutivo deve includere un piano dettagliato delle attività comprensivo delle fasi di installazione, configurazione, test, collaudo, formazione ed addestramento.

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.

Inoltre 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.

Configurazione sistemi.
Al completamento della fase di installazione il fornitore dovrà procedere alle attività di configurazione di tutti i sistemi previsti in fornitura.

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.

Per attività di configurazione sono richiesti **nr. 40 gg a consumo da erogarsi nell'arco di 36 mesi,** di un mix di figure professionali con conoscenza dei sistemi in argomento **per attività varie di analisi, configurazione, progettazione e tuning della piattaforma.**
Tale servizio si svolgerà nell'ambito della settimana lavorativa articolata in cinque giorni dal lunedì al venerdì. L'orario di lavoro coinciderà per quanto possibile con l'orario dell'Amministrazione (09.00/18.00).
Si fa presente che eventuali giornate residuali, potranno essere erogate anche post verifica inventariale.

L'Amministrazione richiederà tale servizio con un preavviso di almeno 7 giorni solari.

Le configurazioni definite saranno oggetto di verifica da parte dell'Amministrazione. Il fornitore si impegnerà ad apportare eventuali modifiche e integrazioni su indicazione dell'Amministrazione

Modalità di erogazione del servizio

La regolamentazione contrattuale del servizio è **su richiesta a chiamata.** Per l'erogazione del servizio si dovrà garantire la presenza di personale con competenze certificate a soddisfare con professionalità il servizio richiesto presso le sedi indicate dall'Amministrazione.

Monitoraggio sull'erogazione del servizio

Le singole presenze del personale impiegato nell'erogazione dei servizi oggetto della fornitura saranno registrate e dovrà essere redatto per l'amministrazione un riepilogo delle giornate lavorative prestate.

L'Amministrazione potrà verificare la professionalità del personale impiegato nell'erogazione dei servizi durante il periodo in esame, utilizzando come parametri di qualità l'adeguatezza delle competenze, l'efficacia e l'efficienza degli interventi. Qualora una singola valutazione risultasse insufficiente, il fornitore su richiesta dell''Amministrazione dovrà sostituire il personale coinvolto senza aver riconosciuto l'onere della prestazione eseguita.

Nella presentazione dell'offerta economica il concorrente dovrà indicare **il costo unitario della singola giornata, pena esclusione.**

12. Formazione

Attraverso personale certificato è richiesta la formazione al personale della Polizia di Stato tramite un corso da svolgere nelle sede di Roma presso i locali dell'Amministrazione oppure in modalità e-learning.

Il corso, da tenersi in lingua italiana, prevedere la partecipazione di massimo 10 discenti e dovrà essere organizzato in un'unica sessione della durata minima di 5 giorni lavorativi (8 ore dalle 8.00 alle 17.00); l'Amministrazione si riserva il diritto di far partecipare numero 3 (tre) osservatori.

Il Fornitore dovrà organizzare il corso:

- fornendo tutto il materiale didattico necessario
- prevedendo l'alternarsi di fasi teoriche e pratiche, allo scopo di illustrare tutte le funzionalità offerte dal sistema.

Le date di inizio e le modalità di svolgimento dei attività di formazione dovranno esser concordate con l'Amministrazione. In particolare il Fornitore dovrà definire un **Piano Formativo** per un adeguato addestramento teorico e pratico per il personale, approvato dall'Amministrazione.

Sono a carico del Fornitore i costi di eventuali trasferte, trasferimenti, vitto ed alloggio.

13. Assistenza e manutenzione

Per tutte le apparecchiature in fornitura deve essere fornito un servizio di assistenza e manutenzione per un periodo di trentasei mesi (36) decorrendo dalla data di verifica 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.

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.

Modalità di esecuzione

Il servizio di manutenzione 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.

Deve essere fornito accesso al supporto del vendor in modalità **24x7 per la diagnostica di problematiche software**, mentre il replacement del hardware malfunzionante deve essere di tipo

8x5 con spedizione del componente di ricambio al massimo il giorno lavorativo successivo all'apertura del guasto

Il fornitore deve garantire la fornitura di *patch* 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.

14. Livelli di servizio

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 e le penali connesse in caso di superamento delle soglie.

INDICATORE DEL SERVIZIO	VALORI DI SOGLIA	PERIODO DI OSSERVAZIONE
Servizi di assistenza e manutenzione (guasti bloccanti)	Tempo di ripristino dell'infrastruttura o del servizio: ≤ 4 ore nel 95% dei casi ≤ 24 ore nel 5% dei casi	trimestrale
Servizi di assistenza e manutenzione (guasti non bloccanti)	Tempo di ripristino dell'infrastruttura o del servizio: ≤ 24 ore nel 95% dei casi ≤ 72 ore nel 5% dei casi	trimestrale

15. Verifica di conformità

Le operazioni di verifica di conformità saranno eseguite dall'Amministrazione che dovrà esaminare la fornitura. In generale, per dare avvio alle operazioni di collaudo, l'Amministrazione dovrà ricevere da parte del fornitore una formale comunicazione di approntamento al collaudo entro 30 giorni solari dalla ricezione dell'ordine. Nel corso del collaudo, l'Amministrazione avrà la facoltà di eseguire verifiche anche differenti da quanto indicato nella documentazione fornitagli a supporto. All'atto dell'accettazione della fornitura, in caso di esito positivo del collaudo, 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. La presenza di anomalie riscontrate durante la fase di collaudo viene registrata ai fini della misurazione degli indicatori di qualità applicabili. In ogni caso le anomalie emerse in fase di collaudo devono essere rimosse entro il termine massimo di 15 giorni lavorativi.

16. Base d'asta

L'importo a base d'asta complessivo è fissato in **510.000,00 IVA esclusa;** non saranno, quindi, ammesse offerte economiche che comportano una spesa superiore.

17. Criterio di Aggiudicazione delle Offerte

Considerato che i prodotti con le caratteristiche necessarie all'Amministrazione sono individuati con specifiche tecniche puntualmente identificate, la richiesta di offerta verrà aggiudicata con il criterio del minor prezzo, ai sensi dell'art. 95 comma 4, lett.b), del D.lgs. 50/2016.

18. Presentazione dell'offerta economica

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

PRODOTTO	**Q.TA'**	**COSTO UNITARIO** ***(€ iva esclusa)***	**PREZZO COMPLESSIVO** ***(€ iva esclusa)***
Piattaforma Web Security Gateway	30.000 Licenze		
Licenze funzionalità avanzate	30.000 Licenze		
Appliance fisiche per Web Security Gateway	>=3		
Appliance o server dedicato per sistema di gestione	1		
Appliance o server dedicato per sistema di gestione di backup	1		
Rack compatibile e contenente l'hw totale	1		
Formazione	1		
Servizi professionali	40gg		
Servizio di manutenzione	36 mesi		
TOTALE			
oneri relativi ai rischi di sicurezza aziendali ai sensi dell'art. 95, comma 10, del D. Lgs.vo nr.50/2016			