PROVINCIA DI COMO

S1.02 SETTORE AFFARI GENERALI ISTITUZIONALI E LEGALI
S2.04 SERVIZIO SISTEMI INFORMATIVI

DETERMINAZIONE N. 620 / 2020

OGGETTO: AFFIDAMENTO DEL SERVIZIO DI SICUREZZA PERIMETRALE DELLA RETE INFORMATICA DELLA PROVINCIA DI COMO. IMPEGNO DI SPESA EURO 147.568,20 (IVA inclusa). Codice CIG: 8328653DDE

IL RESPONSABILE

Premesso che:

- per una corretta e sicura gestione delle comunicazioni (intranet, extranet ed internet) ed una certa erogazione dei servizi, nonché per la salvaguardia delle banche dati, è imprescindibile garantire la protezione della rete interna da attacchi esterni e la possibilità di comunicare con l'esterno attraverso opportuni filtri e protezioni;

- con determina n. 323 del 30/03/2018 è stato affidato alla Società IFInet srl di Verona, mediante procedura negoziata ai sensi del D.L. 50/2016 art. 3 comma uuu) con il criterio dell'offerta economicamente più vantaggiosa ai sensi dell'art. 95 comma 2 con richiesta di offerta sulla piattaforma tecnologica di e-procurement SINTEL messa a disposizione da ARCA Regione Lombardia, il servizio per la sicurezza perimetrale della rete informatica della Provincia di Como dal 1/03/2018 al 29/02/2020;

- con determina n. 166 del 27/2/2020 si è prorogato il servizio di 4 mesi con la medesima ditta in quanto i tempi necessari per aderire alla Convenzione CONSIP "Reti Locali 6", tramite MEPA, attraverso la richiesta di valutazione preliminare al fornitore contraente, Telecom Italia, si sono dimostrati più lunghi rispetto allo scadenziario programmato;

- con successiva determinazione n. 478 del 8/07/2020 è stato nuovamente prorogato per altri tre mesi il servizio in oggetto, permanendo le condizioni di cui alla precedente proroga ed in conseguenza delle condizioni legate alla diffusione del contagio COVID 19 ;

Considerato che si rende necessario procedere all'affidamento del servizio di sicurezza perimetrale della rete informatica della Provincia di Como in scadenza al 30.09.2020;

Dato atto che:

- in data 15/01/2020 è stata inviata, tramite la piattaforma Acquisti in Rete P.A., la

richiesta di valutazione preliminare per i seguenti dispositivi e servizi per la sicurezza delle reti: n. 4 apparati firewall e n. 1 sandbox, servizi di fornitura - consegna - installazione degli apparati attivi (firewall, sandbox), servizio di configurazione, servizio di assistenza e manutenzione, servizio di gestione e sistema di monitoraggio, servizio di gestione da remoto della rete per i dispositivi per la sicurezza acquistati, aggiornamento dei dispositivi per la sicurezza. Le esigenze in termini di servizi complementari aggiuntivi, previsti nella richiesta di valutazione preliminare, sono i seguenti servizi: gestione della sicurezza totalmente a carico del fornitore, protezione della posta elettronica da virus e spam - NAT - sicurezza della DMZ, gestione e SLA migliorativi per la sede di via Volta (servizi critici della Protezione Civile, Lavoro e Centri per l'Impiego), accesso in sola lettura alla console di gestione degli apparati di sicurezza.

- in data 22/05/2020 prot. n. 16318 TELECOMITALIA SPA ha inviato il Piano di Esecuzione preliminare comprendente i servizi richiesti ad eccezione delle licenze software per il sistema di protezione della posta elettronica da virus e spam, non previste nella Convenzione Consip e da acquistare separatamente.
- in data 26/05/2020 prot. n. 16675 TELECOMITALIA SPA ha inviato il Piano di Esecuzione definitivo (All. 1) comprendente i servizi richiesti;
- in data 8/06/2020 è stato effettuato l'ordine del servizio in oggetto tramite la piattaforma Acquisti in Rete P.A. da cui risultava ancora un sufficiente residuo disponibile per le adesioni
- il fornitore ha rifiutato l'ordine con la seguente motivazione: "l'ordine non può essere accettato poiché si registra la saturazione del contratto".

Visto il Decreto Legislativo n. 76/2020, c.d. "decreto semplificazioni", che ha derogato l'art 36 co 2 lettera a) del Codice dei Contratti Pubblici, prevedendo che fino al 31 luglio 2021 l'affidamento diretto sia possibile per importi fino a 150.000 euro e comunque, per servizi e forniture, nei limiti delle soglie ex art 35;

Considerato che il Piano di Esecuzione definitivo della Convenzione (allegato) rispondeva e risponde a tutte le necessità rappresentato dall'Ente ed espresse nella richiesta di valutazione preliminare e che il fornitore ha confermato la disponibilità ad erogare il servizio in oggetto alle medesime condizioni e costi della Convenzione esaurita ;

Considerato inoltre che i costi del servizio rispecchiamo il Piano di Esecuzione definitivo con il seguente piano di spesa:

- dal 1° ottobre 2020 al 31 dicembre 2020: 99.405,27 € (IVA inclusa) per l'acquisto dei dispositivi di sicurezza di fascia media (firewall e sandbox) ed i relativi servizi di manutenzione, configurazione, subscrition per l'uso e l'aggiornamento dei dispositivi di sicurezza; 8.580,89 € (IVA inclusa) per i servizi di gestione e assistenza.
- dal 1° gennaio 2021 al 31 dicembre 2021: 10.887,45 € (IVA inclusa) per il servizio annuale di gestione e assistenza;
- dal 1° gennaio 2022 al 31 dicembre 2022: 10.887,45 € (IVA inclusa) per il servizio annuale di gestione e assistenza;
- dal 1° gennaio 2023 al 31 dicembre 2023: 10.887,45 € (IVA inclusa) per il servizio annuale di gestione e assistenza;
- dal 1° gennaio 2024 al 30 settembre 2024: 6.919,69 € (IVA inclusa) per il servizio di gestione e assistenza;

Ritenuto pertanto, anche in ottica di razionalizzazione e contenimento della spesa, che per l'Ente sia conveniente procedere con l'affidamento diretto del servizio in quanto lo stesso ha conservato le condizioni economiche della convenzione originaria stipulata in esito ad una procedura aperta di rilievo comunitario e , pertanto , sulla base di condizioni contrattuali

validate dal mercato ed all'esito di un confronto competitivo aperto ;

Viste:

- la Deliberazione del Consiglio Provinciale n. 4 del 29.04.2020 con la quale è stato approvato il Bilancio di previsione per il triennio 2020-2022;
- la Deliberazione del Presidente n. 37 del 07/05/2020 di approvazione del Piano esecutivo di Gestione 2020/2022;
- la Deliberazione del Presidente n. 49 del 09/06/2020 di integrazione del Piano esecutivo di Gestione 2020/2022;

D E T E R M I N A

1) che la premessa è parte integrante e sostanziale del presente atto;

2) di affidare in via diretta , ai sensi dell'art. 1 comma 2 lettera a) del D.L. 76/2020 contenente '' Misure urgenti per la semplificazione e l'innovazione digitale'' e per le motivazione ampiamente espresse in premessa , a Telecom Italia SPA via Gaetano Negri, 1 – 20123 Milano il servizio di sicurezza perimetrale della rete informatica dell'Ente, per un periodo di 48 mesi decorrenti dall' 1 ottobre 2020 , per un importo di Euro 120.957,54 (IVA esclusa);

3) di approvare il Piano di Esecuzione definitivo presentato da Telecom Italia SPA via PEC prot. n. 16675 allegato al presente provvedimento (All. 1);

4) di impegnare la spesa complessiva prevista di Euro 147.568,20 (IVA inclusa) con la seguente ripartizione annuale:

anno 2020 Euro 107.986,16 (IVA inclusa):

cap. 23950/3 Missione 01 Programma 08 Piano dei Conti 2020107	Euro 33.884,72
cap. 22300/1 Missione 15 Programma 01 Piano dei Conti 2020105	Euro 65.520,55
cap. 1450/19 Missione 01 Programma 08 Piano dei Conti 1030219	Euro 8.580,89

anno 2021 Euro 10.887,45 (IVA inclusa)
cap. 1450/19
Missione 01 Programma 08 Piano dei Conti 1030219

anno 2022 Euro 10.887,45 (IVA inclusa)
cap. 1450/19
Missione 01 Programma 08 Piano dei Conti 1030219

anno 2023 Euro 10.887,45 (IVA inclusa)

anno 2024 Euro 6.919,69 (IVA inclusa)

la somma prevista per il 2023 e 2024 sarà impegnata successivamente a carico dei pertinenti esercizi finanziari ;

5) di dare atto che il pagamento avverrà a seguito di ricevimento di regolare fattura , nei termini previsti dal capitolato d'oneri ;

6) di trasmettere il presente provvedimento al Settore Finanziario per gli adempimenti conseguenti ed in copia al Servizio Controllo di Gestione.

Lì, 18/08/2020

IL RESPONSABILE
ACCARDI MATTEO
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

PIANO DI ESECUZIONE PER LA REALIZZAZIONE DI UNA RETE LOCALE IN CONVENZIONE CONSIP RETI LOCALI 6

PROVINCIA DI COMO

- PIANO DI ESECUZIONE DEFINITIVO –

REDATTO: (Autore)	**MEB-M/NO.PSV Convenzioni**	**Luciano Arioli**
APPROVATO: (Proprietario)	**MEB-M/NO.PSV Convenzioni**	
LISTA DI DISTRIBUZIONE:	**MEB-M/NO.PALL**	**Raimondo Ortega**
	GdP TI della Convenzione CONSIP LAN 6	**info.retilocali6@telecomitalia.it**
	Provincia di Como (Innovazione Tecnologica)	**Laura Cigardi Via Borgo Vico, 148 22100 - Como (CO)**
DESCRIZIONE ALLEGATI:	**Nell'indice**	

Il presente documento è stato redatto in coerenza con il Codice Etico e di Condotta ed il Modello Organizzativo 231 del Gruppo TIM

INDICE

1. Registrazione modifiche documento....3
2. Sommario....4
3. Riferimenti della Convenzione....5
4. Premessa....6
4.1 Servizi tecnici:....6
4.2 Servizio di gestione:....8
4.3 Infrastruttura della sede di Via Volta....10
4.4 SLA attuali....10
4.5 Migrazione....11
5. Soluzione proposta....12
5.1 Soluzione proposta per gli apparati attivi....12
5.2 Dispositivi per la sicurezza delle reti....14
6. Servizi....22
6.1 Servizio di supporto al collaudo....22
6.2 Servizi di assistenza, manutenzione....22
6.3 Servizi di addestramento e formazione....23
6.4 Servizio di intervento su chiamata su PDL....24
7. Project Management e piano di realizzazione....26
8. Piani di Sicurezza....27
9. Oneri di progettazione....28
10. Allegati....29

1. REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	REVISIONE	DATA
Prima emissione	0	26/05/2020

2. SOMMARIO

Il presente documento descrive il Piano di Esecuzione Definitivo (Progetto Esecutivo) di Telecom Italia relativamente alla richiesta di fornitura di Servizi e Sistemi LAN attivi e passivi da effettuare presso il Cliente Provincia di Como in accordo a quanto previsto dalla Convenzione CONSIP "Reti Locali 6".
Quanto descritto, è stato redatto in conformità alle richieste dell'Amministrazione e sulla base delle esigenze emerse e delle verifiche effettuate durante le seguenti riunioni tecniche svolte in presenza dell'Amministrazione nelle sedi interessate:

- riunione del 28 novembre 2019;
- riunione del 14 gennaio 2020;
- call del 20 gennaio 2020 con i referenti di Via Volta (servizio Lavoro e Protezione Civile);
- riunione del 13 maggio 2020 (sede Provincia di Como).

3. RIFERIMENTI DELLA CONVENZIONE

La fornitura degli apparati attivi e passivi oggetto della soluzione tecnica descritta avviene attraverso l'adesione alla Convenzione CONSIP "Reti Locali 6".
I documenti di riferimento della Convezione suddetta sono pubblicati sul sito www.acquistinretepa.it nella sezione INIZIATIVE- CONVENZIONI - AREA MERCEOLOGICA: INFORMATICA, ELETTRONICA, TELECOMUNICAZIONI E MACCHINE PER UFFICIO – RETI LOCALI 6 – DETTAGLIO LOTTI.

Di seguito sono indicate le persone di riferimento che saranno coinvolte durante la messa in opera del Progetto:

- **Referente dell'Amministrazione (Capo Progetto)**

- Referente amministrazione:
  dott. Matteo Accardi (Dirigente) matteo.accardi@provincia.como.it

- Referenti tecnici per la sede di via Borgo Vico:
  Laura Cigardi, laura.cigardi@provincia.como.it ,
  Gian Battista Clerici, gianni.clerici@provincia.como.it ,
  Giovanni Scandella, giovanni.scandella@provincia.como.it

- Referenti tecnici per la sede di via Volta:
  Guendalina Camozzi (Lavoro / Centri per l'Impiego), guendalina.camozzi@provincia.como.it
  Tiziana Arena (Protezione Civile), tiziana.arena@provincia.como.it

- PEC istituzionale: protocollo.elettronico@pec.provincia.como.it

- **Referente di Telecom Italia (Responsabile di commessa)**

  Luciano Arioli
  Via Tonale, 11 - 20125 - Milano
  Tel: 026212056 - cell. 3351365995
  Email: lucianoaristide.arioli@telecomitalia.it

- **Referente di Telecom Italia (Responsabile per la realizzazione)**

  Italo Finocchio
  Corso Giuseppe Garibaldi 120 - 20025 – Legnano (MI)
  Tel: 0331391556 - cell. 3357689721
  Email: italo.finocchio@telecomitalia.it

4. PREMESSA

Il Cliente Provincia di Como ha rischiesto il Piano di Esecuzione Definitivo (Progetto Esecutivo) in convenzione CONSIP LAN6 che prevede la fornitura e installazione di apparati Firewall di fascia media con relativo dispositivo di Sandbox e l'installazione di nuove licenze antispam su gateway TrendMicro (a completamento della soluzione e che il Cliente dovrà acquistare fuori dalla Convenzione CONSIP LAN6), in quanto il servizio di protezione della posta elettronica da virus e spam (TrendMicro) non è incluso.

I paragrafi successivi descrivono la situazione attualmente in essere dal Cliente nelle sedi di Via Borgo Vico n. 148, Via Alessandro Volta n. 44 e nelle sedi Periferiche collegate relativamente ai prodotti e servizi di sicurezza perimetrale.
La nuova proposta dovrà soddisfare i requisiti dell'attuale soluzione sia in termini di caratteristiche e performance degli apparati che in termini di servizi erogati.
Di seguito sono elencati i servizi attualmente attivi presso la Provincia di Como.

4.1 Servizi tecnici:

Firewall

- Apparati attualmente in uso: Check Point 4600, Check Point 1470; tali apparati si prevede di sostituirli con i nuovi Fortinet serie 300E);
- application level firewall (header + contenuto del pacchetto);
- configurazione ridondata;
- regole a livello di network/singolo IP/singolo utente o gruppo di utenti di Active Directory;
- regole distinte per la sede centrale di via Borgo Vico e la sede periferica di via Volta.
- stazione di management esterna all'amministrazione, console di controllo, server di log;
- report sintetici (es. statistiche generali, allarmi, dati sulle connessioni VPN, log eventi, …);
- caratteristiche avanzate della stazione di management: quality of service, controllo delle applicazioni, data loss prevention, user access identity, sistema di revisione delle politiche di sicurezza, integrazione del database utenti con Microsoft Active Directory;
- PAT management (nascondere le porte effettive di ascolto con porte fittizie).

Intrusion detection system, intrusion prevention system

- Prodotto in uso: Check Point IPS;
- Protocolli Ethernet, TCP/IP;
- capacità di rilevazione degli attacchi garantendo la minore percentuale possibile di falsi positivi e falsi negativi;
- raccolta e conservazione delle tracce di avvenuti attacchi, raccolta di eventi relativi a tentativi di
- attacco;
- analisi predeterminata degli eventi rilevati attraverso l'utilizzo di "signature analysis", gestione e aggiornamento del database delle "signature";
- monitoraggio proattivo degli eventi segnalati dal sistema IDS/IPS ed analisi degli attacchi rilevati;
- notifica specifica a fronte dell'identificazione di un evento di attacco;
- architettura ridondata ed integrata negli apparati di sicurezza perimetrale;
- tipologie di protezione implementate: attacchi malware; DoS e DDoS; vulnerabilità di server e applicazioni; protocol misuse; traffico generato da applicazioni non desiderate (incluse IM e P2P),…;
- correlazione degli eventi IPS con vulnerabilità presenti su server e servizi pubblicati su Internet;
- aggiornamento settimanale signature IPS.

Servizio di protezione del traffico HTTP (s) /FTP (s) da virus

- Prodotto in uso: Antivirus software blade di Check Point - servizio ThreatCloud;
- protezione da attacchi veicolati tramite i protocolli HTTP, HTTPS, FTP, FTPS;
- controllo traffico web 2.0;
- protezione da attacchi phishing, malware, spyware, keyloggers, ...;
- protezione da attacchi veicolati tramite Botnet;
- blocco di comunicazioni verso siti con rischi elevati per la sicurezza;
- blocco di tentativi di tunnelling su HTTP, HTTPS;
- scansione di file compressi (7zip, zip, gzip, tgzip, rar);
- supporto file exe, vbs, bat, ...
- scansione in tempo reale;
- differenziare il controllo su traffico in ingresso/uscita;
- funzionalità di SSL Decryption;
- creazione di regole di eccezione per siti/categorie di siti.3

Servizio di rilevamento BOT

- Prodotto in uso: Anti-Bot software blade di Check Point - servizio ThreatCloud;
- identificare i computer infettati da BOT, bloccare le comunicazioni provenienti dai server C&C (Comando e Controllo);
- analisi complete delle infezioni da BOT con log avanzati.

Servizio di protezione della posta elettronica da virus e spam

- Prodotto in uso: Trend Micro InterScan Messaging Security Virtual Appliance;
- scansione in tempo reale della posta elettronica;
- antispam e antivirus;
- supporto blacklist, interrogazione di ulteriori database di blacklist in aggiunta a quelli offerti dal produttore del sistema di sicurezza;
- controllo sui file allegati ai messaggi di posta elettronica;
- filtri configurabili tramite espressioni regolari.

Servizio di gestione e controllo dell'accesso alla navigazione Internet

- Prodotto in uso: Check Point URL filtering e application control;
- blocco della navigazione verso i siti appartenenti a specifiche categorie;
- controllo del contenuto dinamico e real time delle pagine;
- controllo accesso Internet sia in HTTP, HTTPS FTP, FTPS, oltre a tutti i protocolli incapsulabili;
- controllo dei servizi "social networking" (es. consentire la lettura di Facebook ma non la pubblicazione di post);
- politiche di navigazione associate a singoli utenti / gruppi di utenti / IP / sottorete;
- integrazione con Active Directory;
- policy distinte per la sede centrale di via Borgo Vico e la sede periferica di via Volta.

Servizio di Network Address Translation (NAT) management

- analisi del piano di indirizzamento, configurazione NAT;
- gestione del servizio NAT.

Servizio di VPN management

- Prodotto in uso: Check Point VPN;
- Data origin authentication, data integrity, data confidentiality, replay protection;
- configurazione e gestione di connessioni VPN;
- VPN site-to-site, client-to-site;
- gestione autonoma da parte del fornitore / cooperativa (interazione con eventuali fornitori terzi per l'instaurazione della VPN);
- generazione di report con i dettagli delle connessioni VPN (stato, traffico, ...).

Servizio di gestione della banda Internet

- Prodotto in uso: Check Point QoS;
- gestione della banda Internet (ottimizzazione della banda per garantire, ad esempio, la disponibilità di banda per applicazioni maggiormente sensibili alla latenza come ad esempio il sistema di videoconferenza);
- limitare la banda per alcune tipologie di traffico / garantire una banda minima per altre tipologie di traffico / assegnare dinamicamente ad altro traffico la banda riservata a servizi e non utilizzata;
- policy basate su IP / sottoreti, legate ad orari.4

Servizio di gestione della DMZ

- gestione della sicurezza della DMZ;
- configurazione di nuovi apparati e servizi (indirizzamento pubblico, regole firewall, …).

Servizio di event & log monitoring management

- monitoraggio e gestione di allarmi;
- configurazione di notifiche;
- monitoraggio proattivo;
- raccolta, verifica, correlazione, analisi e storicizzazione degli eventi raccolti nei file di log dei sistemi di sicurezza;
- generazione di report dettagliati (sorgente dell'evento/allarme, tipologia dell'evento/allarme, descrizione, gravità, istante temporale, …).

4.2 Servizio di gestione:

La gestione del sistema di sicurezza copre i seguenti servizi:

- firewall, IDS/IPS, protezione del traffico da virus, bot, spam, controllo navigazione Internet, NAT management, VPN management, gestione banda Internet, gestione della DMZ, monitoraggio. Inoltre, si occupa di tutte le attività correlate necessarie per il corretto funzionamento dei sistemi di sicurezza quali configurazione, aggiornamento, monitoraggio da remoto, throubleshooting, change management e manutenzione.

4.2.1 Monitoraggio da Remoto

- Software di monitoraggio in uso: PRTG;
- monitoraggio del corretto funzionamento di sistemi, servizi applicativi e della rete nell'ambito dei sistemi di sicurezza, verifica della raggiungibilità degli apparati, con l'evidenziazione dei tempi totali di effettivo utilizzo e di eventuale disservizio;
- monitoraggio proattivo dei dispositivi, da remoto, ed intervento tempestivo in caso di guasto o malfunzionamento;
- generazione di alert a fronte del verificarsi di eventi definiti in fase di configurazione del servizio;
- possibilità di consultare via web le informazioni relative agli apparati monitorati;
- installazione di patch e hot-fix e nuove versioni software del sistema di monitoraggio, ove queste introducano nuove funzionalità necessarie per il monitoraggio degli apparati e servizi;
- backup delle configurazioni, sia in occasione della conclusione della prima installazione e successivamente ad ogni modifica sostanziale;
- possibilità di implementare numerosi controlli su apparati e servizi, quali, ad es., informazioni su utilizzo delle risorse (RAM, CPU, ecc.), traffico sulle interfacce, sovraccarichi, stato dei servizi, ecc.…

4.2.2 Troubleshooting

- Analisi e risoluzione delle problematiche a seguito di attività di monitoraggio effettuate dal fornitore o di una richiesta da parte della Provincia;

- aggiornamento / adeguamento dei sistemi di sicurezza in caso di modifiche alle infrastrutture ed ai servizi in uso da parte della Provincia (es. server, apparati attivi, connettività Internet, ...).

4.2.3 Change Management

- attività sistemistica per la modifica / implementazione di regole e configurazioni dei sistemi di sicurezza;
- tale servizio copre qualsiasi necessità di modifica dei dati di configurazione e applicativi nell'ambito del sistema (esempio: creazione/modifica delle regole del firewall); le regole sono create e gestite autonomamente dal fornitore per la risoluzione di una problematica/richiesta (es. mancata raggiungibilità di un sito web);
- possibilità di accedere alle console di management dei sistemi di sicurezza forniti, in un ambiente dedicato, e di modificare in autonomia le configurazioni dei sistemi stessi;
- definizione granulare dei privilegi d'accesso ai sistemi da parte degli amministratori (es. utenze per la sola visualizzazione della configurazione, utenze per la sola modifica delle configurazioni, ecc. ...).

4.2.4 Servizio di Manutenzione:

- Manutenzione correttiva: riparazione di guasti, blocco o altri inconvenienti; messa a disposizione di parti di ricambio (identiche alle parti sostituite che verranno ritirate dal fornitore) in sostituzione; eventuali modifiche tecniche necessarie; esecuzione di prove e controlli atti a garantire il ripristino del pieno funzionamento del sistema. La manutenzione si estende alle parti di ricambio. Se il ripristino del problema richiede tempi superiori a quelli indicati nelle SLA, il fornitore provvede, a propria cura e spese, alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali;
- manutenzione preventiva comprende gli interventi (concordati) per consentire la perfetta funzionalità del sistema di sicurezza e prevenire malfunzionamenti (quali ad es.: aggiornamento software, risoluzione bug,...);
- Redazione del report di intervento, per ogni intervento di manutenzione effettuato dai tecnici.
- La Provincia di Como avrà accesso alla console degli apparati (firewall/sandbox), eventualmente anche in sola lettura.

4.2.5 Servizio di ticketing:

- Inoltro delle richieste di assistenza (telefonicamente o via mail);
- l'apertura del ticket comporta l'invio di una mail alla Provincia di Como contenente il numero del ticket, data e ora, descrizione e l'identificativo del referente;
- la modifica dello stato del ticket (esempio: chiusura attività) viene notificata via email.

4.2.6 Servizio remoto:

- I servizi di sicurezza sono erogati da remoto, con connessione VPN tra il fornitore e la Provincia di Como.

4.2.7 SLA:

- Monitoraggio: da lunedì a domenica, 24 h. In caso di malfunzionamento della componente hardware/software utilizzata per il monitoraggio: intervento entro 1 ora;
- Troubleshooting: da lunedì a domenica, 24 h (minimo: da lunedì a sabato, 8:00-20:00)
  - 30 minuti per la presa in carico;
  - 3 ore per la risoluzione da remoto;
  - 6 ore per l'intervento on-site;
  - il ripristino avviene comunque entro 24 ore solari dalla segnalazione del guasto;
- Change management: da lunedì a venerdì, dalle 8:30 alle 18:30, con esclusione dei giorni festivi
  - 30 minuti per la presa in carico;
  - 1 ora per l'implementazione della modifica;

- Manutenzione correttiva: da lunedì a domenica, 24 h (minimo: da lunedì a sabato, 8:00-20:00)
    - malfunzionamento bloccante: intervento entro 1 ora, ripristino on site entro 8 ore;
    - malfunzionamento non bloccante: intervento entro 8 ore, ripristino on site entro 16 ore.

4.3 Infrastruttura della sede di Via Volta

Per la sede di Via Volta – settore Lavoro e Protezione Civile, ci sono le seguenti integrazioni da prevedere:

- Connettività Internet in fibra, 20 Mbps, con IP pubblici;
- connettività MPLS (gestita da altro operatore telefonico) con la sede di Via Borgo Vico, 148 e con i cinque Centri per l'Impiego (di seguito CPI) ove sono attive una linea di 2Mb in ciascun CPI;
- connettività satellitare di back-up a servizio della Sala Operativa Unificata Provinciale di Protezione Civile (SOUP) condivisa con la Prefettura da attestare comunque sui firewall. Gli utenti sono circa 80, tra sede di via Volta e CPI, ma sono in previsione 72 assunzioni. Gli utenti dei CPI escono su Internet tramite la connettività Internet della sede di via Volta. Ogni CPI ha un proprio indirizzamento IP interno. È presente una DMZ con Portale Internet che eroga servizi H24 con circa 80.000 utenti registrati. I servizi erogati rispondono a dettati normativi ed hanno scadenze stringenti e perentorie. Sono presenti VPN client to site. Vi è un'estensione della rete verso la confinante Prefettura che dovrà essere attestata sul firewall. L'infrastruttura è costituita da una LAN dedicata, in parte cablata, in parte wireless, e da una DMZ dedicata con servizi on-line H24 con circa 1000 utenti. Si dovranno garantire l'accesso ad Internet, i servizi VPN, l'accesso ad alcuni server e la pubblicazione del server di front end. Sono inoltre presenti due centralini VOIP in alta affidabilità. Nella sede di via Volta sono presenti tre domini (2 domini 2012R2 e un dominio 2016) senza relazione di trust con il dominio della sede di via Borgo Vico. Gli apparati di sicurezza in uso nella sede di Via Volta sono n. 2 appliance rack "Check Point 1470", verranno sostituiti da n°2 firewall Fortinet serie 300E (FW/IPS/ACPL/AV/ABOT/URLF/VPN/QOS).

4.3.1 Firewall

I valori attualmente garantiti sono:

- production performance
    - 1.6 Gbps firewall throughput
    - 175 Mbps threat prevention throughput network connectivity
    - IPv4 e supporto IPv6
    - numero VLAN supportate: 1024
    - supporto dei protocolli di routing dinamici BGP, OSPF, RIPv1, RIPv2
    - supporto di due connettività Internet distinte in modo da poter assicurare la continuità di traffico sia in ingresso che in uscita
    - RFC 3511, 2544, 2647, 1242 Performance Tests (LAB)
    - 3.2 Gbps on firewall throughput, 1518 byte UDP
    - 0.5 Gbps on VPN throughput, AES-128 175 Mbps of threat prevention throughput (IPS, application control, URL filtering, antivirus, anti-bot antispam, sandboxing) 0.5 million of concurrent transitions, 64 byte HTTP response 30.000 connections per second, 64 byte HTTP response.

E' necessario verificare i valori di throughput di via Volta alla luce dell'incremento del numero di utenti e servizi.

4.4 SLA attuali

Monitoraggio remoto:

- da lunedì a sabato, 24x24
- SLA: entro 2 ore dall'evento. Comunicazione della causa del problema, classificazione della severità secondo i livelli critico (il sistema non è operativo) / serio (parti del

sistema non sono operative), indicazione e condivisione dei passi e delle tempistiche necessarie alla risoluzione.

Troubleshooting (risoluzione problemi):
- da lunedì a sabato, 8:00 - 20:00
- SLA: 2 ore per la presa in carico e la prima analisi del problema, 4 ore lavorative per la risoluzione da remoto, 8 ore lavorative per intervento on-site in caso di impossibilità di risolvere il problema da remoto ed eventualmente per attivare il servizio di manutenzione per il ripristino del sistema. Il ripristino del sistema dovrà comunque avvenire entro 24 ore solari dalla segnalazione del guasto, ad eccezione del malfunzionamento dei componenti software non dipendenti dal fornitore del servizio.

Change management (modifica configurazioni):
- da lunedì a venerdì, 9:00-13:00; 14:00-18:00
- SLA: 1 ora per la presa in carico, 2 ore per l'implementazione della modifica.

Per le specificità della SOUP il servizio di troubleshooting deve essere garantito H24 con gli SLA ivi indicati (che con riferimento alla Convenzione CONSIP si ritiene siano quelli correlati al profilo HP).
Per tutti i servizi si richiede il profilo HP della Convenzione (H24, 7 giorni su 7).

NOTE: si ribadisce la necessità di garantire comunque il funzionamento di tutti i servizi per Via Volta in caso di
DOWN della Sede Centrale di via Borgo Vico.

4.5 Migrazione

- almeno 15 giorni di preavviso;
- la migrazione dovrà essere effettuata nei giorni in cui i CPI sono chiusi al pubblico. Le giornate disponibili sono: martedì o giovedì pomeriggio indicativamente dalle 14:30/15:00 a seguire.

5. SOLUZIONE PROPOSTA

La soluzione proposta, in relazione delle esigenze espresse dall'Amministrazione, si compone dei seguenti elementi, che verranno valorizzati, per quanto non incluso nella configurazione base consip, nella componente "DEI servizi":

Realizzazione della Rete LAN (apparti attivi)

- fornitura, installazione e configurazione delle seguenti apparati attivi:
  a. apparati per la sicurezza delle reti;
- servizio di assistenza al collaudo;
- realizzazione della pubblicazione su internet per portale protezione civile SOUP (Reverse PROXY) attraverso, come condiviso durante l'ultimo incontro del 13 05 u.s., implementazione politiche di NAT – In caso di variate o ulteriori esigenze , si valuteranno sviluppi.

Servizi di assistenza, manutenzione e gestione

- assistenza e manutenzione del nuovo, come descritto nel paragrafo 4.2;
- servizio di monitoraggio da remoto, come descritto nel paragrafo 4.4;
- servizio di Troubleshooting, come descritto nel paragrafo 4.4;
- servizio di Change management, come descritto nel paragrafo 4.4;
- Servizio di ticketing, come descritto nel paragrafo 4.2.

Servizi di addestramento e formazione:

- servizio di addestramento sulla fornitura;
- servizio di formazione sulle reti locali.

Il dimensionamento del progetto e le caratteristiche della soluzione saranno tali da assicurare una elevata scalabilità e flessibilità che tenga conto dell'evoluzione presunta sul carico di lavoro dell'Amministrazione.
Nella fase di progettazione si è tenuto conto delle possibili ottimizzazioni in termini di efficienza e di risparmio energetico della rete locale e delle infrastrutture collegate.

5.1 Soluzione proposta per gli apparati attivi

Il dimensionamento del progetto e le caratteristiche della soluzione saranno tali da assicurare una elevata scalabilità e flessibilità che tenga conto dell'evoluzione presunta sul carico di lavoro dell'Amministrazione.
Nella fase di progettazione si è tenuto conto delle possibili ottimizzazioni in termini di efficienza e di risparmio energetico della rete locale e delle infrastrutture collegate.
Si prevede di fornire n°4 firewall Fortinet della serie 300E dei quali n° 2 verranno installati nella sede di Via Borgo Vico e n° 2 nella sede di Via Volta. Tali apparati saranno configurati in Business Continuity l'uno rispetto all'altro e a supporto verrà anche fornita una Sandbox che verrà gestita dai Firewall di Via Borgo Vico. Ciò significa che normalmente le due sedi lavoreranno entrambe tramite la Sandbox di Borgo Vico e, in caso di failover di una delle due sedi, la Sandbox continuerà ad erogare il servizio se la sede di Borgo Vico è attiva, contrariamente non erogherà il servizio di Sandboxing se la sede attiva sarà quella di Via Volta. Questo non pregiudicherà comunque il servizio di sicurezza della sede in quanto, anche se non sarà possibile raggiungere la Sandbox, il firewall non permetterà ad eventuali attori malevoli di entrare nella rete, bloccando download da siti o gli allegati presenti nelle mail non autorizzate.
Note: gli apparati sono stati uniformati per rispettare le esigenze richieste dal progetto ed ottimizzarne la sostituzione ed i tempi di intervento in caso di guasti.

5.1.1 Descrizione della fornitura delle componenti attive della Rete LAN

Famiglia	Codice Articolo Convenzione	Descrizione Articolo Convenzione	Produttore	Quantità
Dispositivi di sicurezza - FORTINET	RL6L2_FG-300E-BDL-C	Fornitura in opera dispositivi di sicurezza fascia media	FORTINET TELECOM ITALIA	4

Dispositivi di sicurezza - FORTINET	RL6L2_FC-10-00306-900-02-12	Aggiornamento dei dispositivi per la sicurezza di fascia media	FORTINET	12
Dispositivi di sicurezza - FORTINET	RL6L2_FSA-1000D-BDL-C	Fornitura in opera Sandbox	FORTINET TELECOM ITALIA	1
Dispositivi di sicurezza - FORTINET	RL6L2_Configurazione FSA-1000D-BDL-C	Configurazione Sandbox	TELECOM ITALIA	1
Dispositivi di sicurezza - FORTINET	RL6L2_FC-10-SA01K-969-02-12	Aggiornamento del dispositivo Sandbox	FORTINET	3
Listino DEI	RL6L2_DEISERVIZI	Lavori di realizzazione di opere civili accessorie alla fornitura - Servizi	TELECOM ITALIA	1

5.1.2 Servizio di installazione degli apparati attivi della Rete LAN

Gli apparati attivi, che consentono l'alloggiamento su rack, saranno installati nel seguente modo:

- inserimento di eventuali moduli interni ed esterni all'apparato;
- montaggio su rack: gli apparati saranno ancorati ai montanti utilizzando le apposite staffe di sostegno. La posizione dell'apparato all'interno del rack e delle staffe relative (nella parte frontale, centrale o posteriore dell'apparato) sarà determinata dalla maggior convenienza in termini di accessibilità alle porte dell'apparato e di stabilità dello stesso;
- inserimento di eventuali moduli esterni all'apparato;
- messa a terra dell'apparato conformemente allo standard NEC, che prevede l'utilizzo di un cavo di rame di dimensioni minime pari a 14 AWG e di un terminale ad anello da collegare all'apparato con un diametro interno pari a circa 7mm. L'altra estremità del cavo sarà collegata ad un punto di messa a terra appropriato;
- connessione dei cavi di rete e di alimentazione. La connessione dei cavi di rete includerà le operazioni di etichettatura degli stessi.

Nel caso di apparati attivi che non consentano l'ancoraggio ai montanti del rack, essi saranno alloggiati su appositi ripiani, mantenendo adeguato spazio libero per le operazioni di esercizio e manutenzione sugli stessi e per consentire un appropriato riflusso di aria.

5.1.3 Servizio di configurazioni degli apparati attivi della Rete LAN

Il servizio di configurazione comprende tutte le attività necessarie a garantire il corretto funzionamento dell'apparato in rete secondo le politiche dettate dall'Amministrazione e, pertanto, consentirà di ottenere un sistema "chiavi in mano" stabile e funzionante per consentire il normale esercizio.
Le attività di configurazione che saranno garantite al termine dell'installazione sono:

- aggiornamento all'ultima versione stabile di sistema operativo;
- inserimento dell'apparato in rete conformemente al piano di indirizzamento dell'Amministrazione;
- configurazione delle VLAN necessarie ed inserimento delle porte nelle VLAN relative;

La configurazione degli apparati attivi verrà eseguita a seguito del buon esito dell'installazione degli stessi.
Descrizione generale degli apparati attivi proposti
Nei paragrafi successivi sono descritte le caratteristiche sintetiche degli apparati attivi proposti per la realizzazione della rete locale.

5.1.4 Descrizione generale degli apparati attivi proposti

Nei paragrafi successivi sono descritte le caratteristiche sintetiche degli apparati attivi proposti per la realizzazione della rete locale.

5.2 Dispositivi per la sicurezza delle reti

5.2.1 Dispositivi di sicurezza fascia alta

Requisiti minimi dispositivi di sicurezza fascia alta
Funzionalità Antivirus
Funzionalità Antispam
Funzionalità di Application Control
Funzionalità di Intrusion Prevention System
Funzionalità Firewall
VPN IPSec
Funzionalità web/url filtering
Almeno 10 interfacce 1000Base-T
Intrusion Prevention throughput almeno pari a 2 Gbps
Firewall throughput almeno pari a 10 Gbps
VPN throughput almeno pari a 4 Gbps
Almeno 4 milioni di sessioni contemporanee
Almeno 140.000 nuove sessioni al secondo

Caratteristiche migliorative dispositivi di sicurezza fascia alta
Supporto per configurazioni High Availability
Protezione da Advanced Persistent Threat (APT)
Funzionalità VPN SSL
Supporto IPv6
Funzionalità di traffic shaping (gestione QoS)
Presenza di almeno 10 contesti virtuali
Miglioramento di almeno il 30% delle prestazioni minime previste per l'Intrusion Prevention throughput
Miglioramento di almeno il 30% delle prestazioni minime previste per Firewall throughput
Miglioramento di almeno il 30% delle prestazioni minime previste per VPN throughput
Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di sessioni contemporanee
Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di nuove sessioni al secondo

5.2.2 Fortinet Fortigate

L'apparato proposto da Telecom Italia come dispositivo per la sicurezza di fascia alta è il FortiGate 300E, che è un appliance di fascia Enterprise, con architettura interna basata sulle seguenti tipologie di processori ASIC:

- Content Processor CP9, che accelera le funzionalità di content inspection basate su signatures e le attività di encryption/decryption offloading;
- Network Processor NP6, che accelera le funzionalità di firewall statefull inspection sia in ambiente IPv4 che IPv6, il traffico SCTP e Multicast, l'IPSec, le funzionalità di Traffic Shaping, e il CAPWAP.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi di fascia alta.

Requisiti minimi:

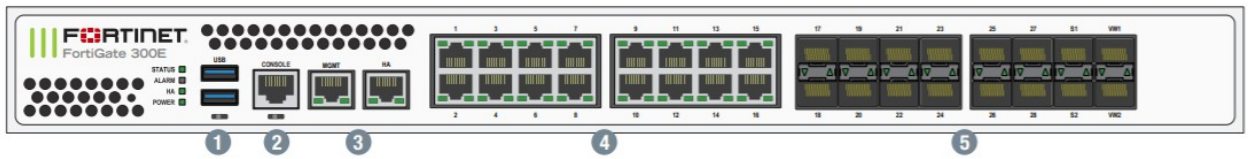
- Funzionalità Antivirus
- Funzionalità Antispam
- Funzionalità di Application Control
- Funzionalità di Intrusion Prevention System
- Funzionalità Firewall
- VPN IPSec
- Funzionalità web/url filtering
- Almeno 10 interfacce 1000Base-T
- Intrusion Prevention throughput almeno pari a 2 Gbps
- Firewall throughput almeno pari a 10 Gbps
- VPN throughput almeno pari a 4 Gbps
- Almeno 4 milioni di sessioni contemporanee
- Almeno 140.000 nuove sessioni al secondo

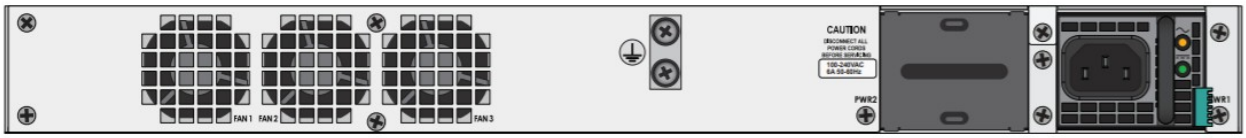
Le caratteristiche indicate come migliorative per i dispositivi di sicurezza di fascia alta richiesti dalla gara sono le seguenti:

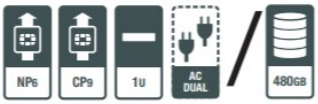
- Supporto per configurazioni High Availability
- Protezione da Advanced Persistent Threat (APT)
- Funzionalità VPN SSL
- Supporto IPv6
- Funzionalità di traffic shaping (gestione QoS)
- Presenza di almeno 10 contesti virtuali
- Miglioramento di almeno il 30% delle prestazioni minime previste per l'Intrusion Prevention throughput (2.6 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per Firewall throughput (13 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per VPN throughput (5.2 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di sessioni contemporanee (5.2 M)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di nuove sessioni al secondo (182.000)

Il Fortigate 300E é un appliance di fascia media che soddisfa i suddetti requisiti, sia minimali che migliorativi.

FortiGate 300E/301E







Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 16x GE SFP Slots

Questo dispositivo é dotato di 16 interfacce 1000 base-T, 16 slot SFP. Il sistema viene offerto completo di subscription Fortiguard per i servizi di Application Control, IPS, AV, Web Filtering ed Antispam.
La tabella seguente fornisce un dettaglio delle specifiche tecniche e prestazionali della macchina:

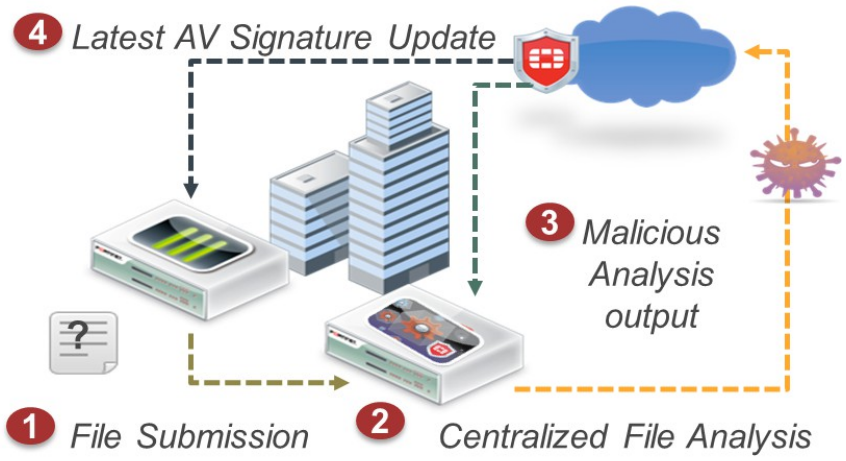
Specifiche hardware	
Interfacce GE RJ45	16
GE SFP Slots	16
Porte Console (RJ45)	1
Performance di Sistema	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	32 / 32 / 20 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	32 / 32 / 20 Gbps
Latenza Firewall (64 byte UDP packets)	3 µs
Firewall Throughput (Pacchetti per Secondo)	30 Mpps
Sessioni Concorrenti (TCP)	4 Million
Nuove Sessioni/Secondo (TCP)	300,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	2,5 Gbps
SSL Inspection Throughput (IPS, HTTP)	3,9 Gbps
Application Control Throughput (HTTP 64K)	7 Gbps
Virtual Domains (Default / Maximum)	10/10
Numero Massimo di FortiSwitches Supportati	48
Numero Massimo di FortiAPs (Totali / Tunnel Mode)	512/256
Numero Massimo di FortiTokens	5000
Numero Massimo di FortiClient registrati	600
Configurazioni di High Availability	Active/Active,Active/Passive, Clustering
Dimensioni	
Altezza x Larghezza x Lunghezza (mm)	44.45 x 432 x 380
Peso	7.3 kg
Form Factor	1 RU

Riferimenti documentali pubblici:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_500E.pdf

5.2.3 Fortisandbox

Fortisandbox è la soluzione progettata da Fortinet proprio per la rilevazione di tale tipologia di attacchi altamente mirati e confezionati ad hoc, che si annidano nelle reti e vengono ignorati dalle difese tradizionali. In genere questi attacchi sono noti con il nome di APT (Advanced Persistent Threat) e per contrastarli è necessario un approccio multilivello: Fortisandbox offre la più recente tecnologia che impiega una combinazione di mitigazione proattiva, visibilità avanzata delle minacce e reporting completo; si avvale delle tecnologie Fortinet di scansione antimalware, sandboxing a due livelli (lightweight e full) e cloud query ai Fortiguard Labs per individuare le tecniche di evasione e avere una protezione dalle minacce allo stato dell'arte. Le tecniche di scansione dinamica di Fortinet si basano sul brevetto CPRL (Compact Pattern Recognition Language) che permette di rilevare con una singola signature decine di migliaia di variazioni del codice virale.
FortiSandbox offre una protezione altamente efficace contro questa classe emergente di minacce oltre ad avere una notevole flessibilità di deployment e semplicità di gestione.
Le caratteristiche principali del FortiSandbox includono:

- Motore Antimalware dinamico e aggiornamenti/query verso il cloud Fortinet: gli aggiornamenti vengono effettuati dai FortiGuard Labs, a cui può inviare query in tempo reale, permettendo così di rilevare in modo veloce minacce esistenti ed emergenti;
- Emulazione di Codice: esegue in tempo reale una ispezione di tipo "lightweight sanboxing", in cui riescono ad identificare tipologie di malware che utilizzano tecniche di evasione e/o si attivano solo in presenza di versioni software specifiche;
- Ambiente virtuale completo (detonazione): fornisce un ambiente isolato per analizzare codice sospetto o ad alto rischio, permettendo di esplorare e verificare l'intero ciclo di vita della minaccia;
- Visibilità avanzata: fornisce un quadro globale in una vasta gamma di reti, sistemi e attività di file classificati per livello di rischio, per migliorare la velocità di risposta agli incidenti;
- Network Alert: controlla il traffico di rete e rileva le richieste verso siti "malicious", che stabiliscono comunicazioni con server C&C e altre attività che sono indice di compromissione della sicurezza;
- Analisi Manuale: consente agli amministratori di sottomettere manualmente campioni di malware per effettuare sandboxing virtuale senza la necessità di avere un dispositivo separato;
- Submission al FortiGuard (opzionale): i tracer report, i file malicious e altre informazioni possono essere sottomesse ai FortiGuard Labs per ricevere raccomandazioni di bonifica e protezioni in linea aggiornate.



La soluzione Fortisandbox è molto flessibile, offrendo diversi scenari di deployment che permettono di adattarsi alle esigenze e ai requisiti dei clienti.

Essa prevede principalmente tre metodi di input con cui può esaminare il traffico di rete ed analizzare i file:

- On demand

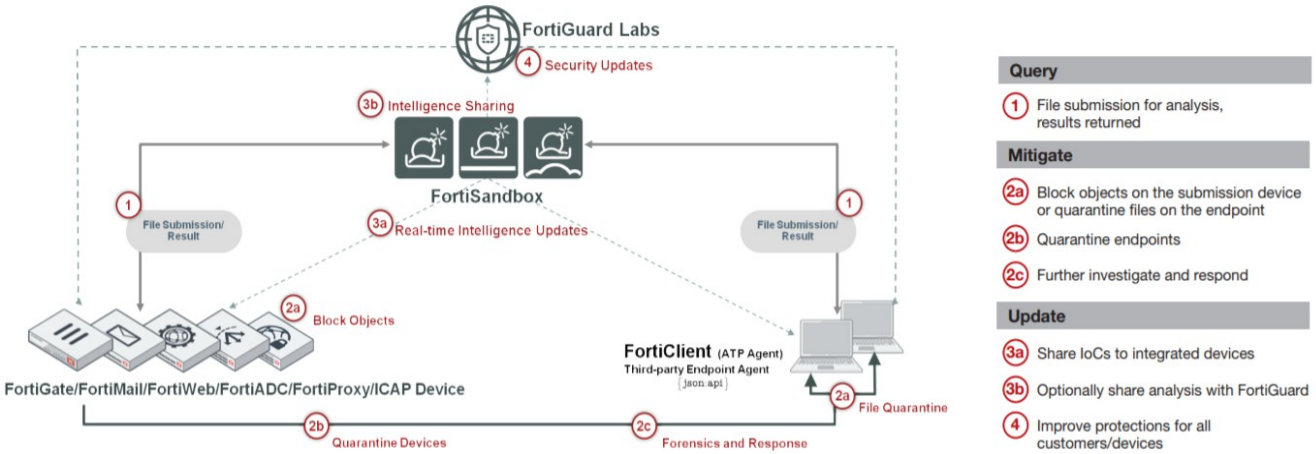
In questa modalità gli amministratori possono sottomettere manualmente campioni di malware per effettuare attività di analisi in sandboxing e verificarne i risultati in un ambiente isolato.

- Sniffer Mode

In questa modalità Fortisandbox riceve il traffico che viene spillato da porte in SPAN di switch di rete o utilizzando TAP: è in grado di analizzare i protocolli HTTP, FTP, POP3, IMAP, SMTP e numerose estensioni di files.

- Device Mode

Soluzioni Fortinet, quali FortiGate, FortiMail, FortiWeb, FortiClient (ATP Agent), FortiADC e fornitori di sicurezza di terze parti (tramite API) possono intercettare e inviare i contenuti sospetti al FortiSandbox che effettuerà una serie di analisi volte a rilevare malware di tipo zero-day e APT. L'integrazione fornirà anche tempestive capacità di alert, remediation e reporting che sono caratteristiche della soluzione offerta.



In particolare, l'integrazione con il FortiGate permette anche l'analisi dei protocolli supportati con crittografia ssl, utilizzando le funzionalità di SSL deep inspection.

Le tre modalità di input possono essere attivate contemporaneamente su interfacce diverse dell'appliance.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi sandbox di tipo appliance:
Requisiti minimi:

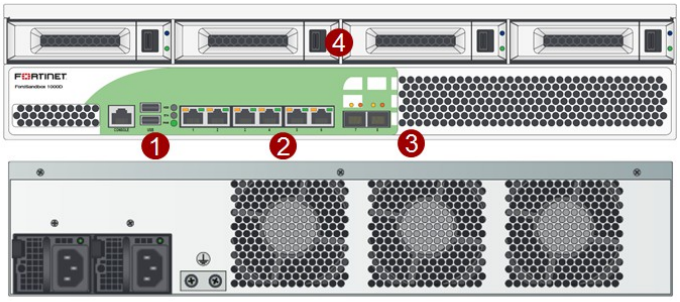
- Deve essere dello stesso brand dei dispositivi di sicurezza offerti e completamente interoperabile con almeno quelli di fascia alta e di fascia top
- Supporto di almeno le seguenti tipologie di file: .rar, .cab, .zip, .gz, .bz2, .exe, .dll, .bat, .pdf, .jar, .doc, .docx,.xls, .xlsx, .ppt, .pptx, .php, .mp3, .mp4, .avi, .mov, .jpeg, .gif, .png
- Supporto di almeno i seguenti protocolli e applicazioni: HTTP, FTP, SMTP, IMAP, POP3
- Virtual Machine - scansione di almeno 100 files/ora
- Supporto di almeno 4 macchine virtuali
- Storage interno almeno 4TB
- Almeno 4 interfacce 10/100/1000Base-T
- Almeno 2 porte 1Gb SFP
- Supporto IPv6

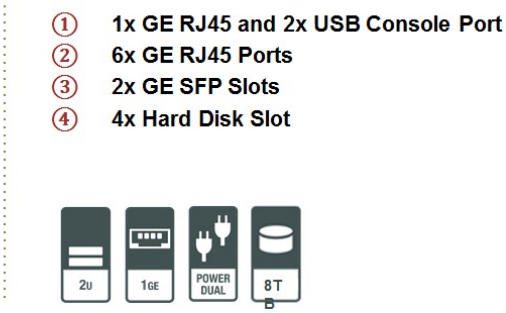
Le caratteristiche indicate come migliorative per i dispositivi Sandbox richiesti dalla gara sono le seguenti:

- Power supply ridondata
- Supporto di almeno 8 macchine virtuali

- Storage interno almeno 8TB
- Virtual Machine - scansione di almeno 150 files/ora

La FortiSandobx 1000D, dotata di complessivi 4 hard-disk da 2 TB ciascuno 3.5 " SATA, é un appliance sandbox che soddisfa tutti i suddetti requisiti, sia minimali che migliorativi.





Questo dispositivo é dotato di 6 interfacce rame RJ45 ports e due slot GE SFP; supporta 8 VM ed un VM Sandboxing Throughput di 160 Files/ora.

	FSA-1000D
VM Sandboxing (Files/Hour)	160
AV Scanning (Files/Hour)	6,000
Number of VMs	
Interfaces	6x GE RJ45 ports, 2x GE SFP slots
File type support	.7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
Input methods	FortiGate, FortiMail Integration, FortiWeb Integration FortiClient Integration, Sniffer mode, manual on-demand file upload, submission API, network file share inspection
Status & Analysis Visibility	Full (rating, source, destination, MD5/SHA, observed behaviors, full logs, pcap, etc) on-box, statistics overview on FGT only
Info submission to FortiGuard Labs	None or all information related to analysis of “low/medium/high risk” objects, based on customer configuration
File Quarantine	On-box file quarantine for network file share scanning. FortiMail submits and queues mails for suspicious content
Protection	Manual policy configuration, FortiGuard AV signature update, requires FortiGuard premium service for SLA

Riferimenti documentali pubblici:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

6. SERVIZI

6.1 Servizio di supporto al collaudo

Il fornitore procederà autonomamente alla verifica funzionale di tutti gli apparati e servizi oggetto della fornitura e al termine di tale verifica consegnerà all'Amministrazione Contraente il «**Verbale di Fornitura**»;
L'amministrazione Contraente procederà al collaudo della fornitura:

- Richiedendo a Telecom Italia di effettuare il collaudo tramite una propria commissione interna producendo, a completamento della fase di collaudo, la relativa documentazione di riscontro (autocertificazione). L'Amministrazione sottoscriverà entro 20 giorni il «**Verbale di Collaudo**».
- Nominando una propria Commissione di collaudo entro 15 giorni dalla data riportata sul «**Verbale di Fornitura**». I lavori dovranno concludersi entro 15 giorni dalla data di costituzione della Commissione di collaudo con la stesura del «**Verbale di Collaudo**»

Nel caso di esito positivo, la data del «**Verbale di Collaudo**» avrà valore di «**Data di accettazione**» della fornitura.

6.1.1 Collaudo degli apparati attivi

Per quanto riguarda le procedure tecniche di collaudo degli apparati attivi, in caso di semplice fornitura, l'installazione sarà eseguita a seguito del buon esito del collaudo del cablaggio passivo. Gli apparati attivi saranno messi in funzione dopo la verifica preventiva del buon funzionamento delle linee di alimentazione di servizio e di backup. Il collaudo degli apparati attivi verrà eseguito con le seguenti modalità:

- verifica corretta tensione di alimentazione;
- accensione apparato e verifica funzionamento degli alimentatori;
- verifica accensione dei LED.

In caso di esito positivo del processo di autotest, verrà compilata la scheda di avvenuto collaudo.
Verranno eseguiti dei test di simulazione di interruzione della rete elettrica per mostrare ai responsabili dell'amministrazione richiedente, il perfetto funzionamento dell'apparato.

6.2 Servizi di assistenza, manutenzione

6.2.1 Servizi di Manutenzione

I servizi di assistenza e manutenzione sul nuovo per la tipologia di apparati attivi previsti in convenzione, **sono gestiti dal CNA** ed eseguiti dai fornitori con le modalità indicate nel capitolato tecnico e annessi chiarimenti nel rispetto degli SLA previsti e riportati dal progettista nel CNI, e sono comprensivi di:

- manutenzione preventiva, che include interventi per evitare l'insorgere di malfunzionamenti;
- manutenzione evolutiva comprendente tutte le attività inerenti il costante aggiornamento delle componenti software/firmware dei sistemi all'ultima release disponibile sul mercato;
- manutenzione correttiva che include le azioni volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità anche attraverso attività di supporto on-site.

Nel corso degli interventi di manutenzione saranno essere eseguite almeno le seguenti attività:

- eliminazione degli inconvenienti che hanno determinato la richiesta di intervento;
- controllo e ripristino delle normali condizioni di funzionamento;

- fornitura ed applicazione delle parti di ricambio della stessa marca, modello e tipo e nuove di fabbrica per la manutenzione del nuovo, o equivalenti per la manutenzione dell'esistente,
- aggiornamento della documentazione relativa;
- redazione del relativo "verbale di intervento".

6.2.2 Servizi di Assistenza e Manutenzione del nuovo

Per tale servizio vengono definite tre differenti fasce di performance:

- Low Performance (LP): con finestra di erogazione del servizio
  Lun-Ven 08.00-17.00 oppure 09.00-18.00
- Medium Performance (MP): con finestra di erogazione del servizio
  Lun-Ven 08.00-17.00 oppure 09.00-18.00 e Sab. 08.00-14.00
- High Performance (HP): con finestra di erogazione del servizio
  H24 7 giorni su 7

Le fasce LP, MP e HP rappresentano i livelli di servizio opzionali relativi all'assistenza e alla manutenzione che l'Amministrazione potrà richiedere separatamente.
Il livello di gravità del guasto segnalato sarà codificato attraverso dei Severity Code assegnati dal Call Center del Concorrente. Il Severity Code dovrà essere repentinamente segnalato dal Call Center ai referenti mediante gli strumenti di comunicazione disponibili (telefono, posta elettronica) assieme ad una diagnosi di massima del disservizio e ad una stima sulle modalità e sulle tempistiche di ripristino.
I Severity Code sono di seguito identificati:

- **Severity Code 1 - Guasto Bloccante**: le funzionalità di base e/o maggiormente rilevanti non sono più operative.
- **Severity Code 2 - Disservizio**: le funzionalità di base sono operative ma il loro utilizzo non è soddisfacente.

Si precisa che il servizio di manutenzione sarà eseguito nel rispetto degli SLA riportati nella Guida alla Convenzione.

La presente proposta tecnica per i dispositivi di sicurezza (Firewall e Sandbox) è previsto un servizio di Mautenzione profilo **HP per la durata di 48 mesi (4 anni).**

Famiglia	Codice Articolo Convenzione	Descrizione Articolo Convenzione	Produttore	Quantità
Dispositivi di sicurezza FORTINET	RL6L2_Manutenzione HP Anno 1 FG-300E-BDL-C	Manutenzione mensile HP Anno 1 Dispositivi di sicurezza fascia media	TELECOM ITALIA	4 (per 12 mesi)
Dispositivi di sicurezza FORTINET	RL6L2_Manutenzione HP successivo anno 1 FG-300E-BDL-C	Manutenzione mensile HP anno successivo Dispositivi di sicurezza fascia media	TELECOM ITALIA	4 (per 36 mesi)
Dispositivi di sicurezza FORTINET	RL6L2_Manutenzione HP Anno 1 FSA-1000D-BDL-C	Manutenzione mensile HP Anno 1 Sandbox	TELECOM ITALIA	1 (per 12 mesi)
Dispositivi di sicurezza FORTINET	RL6L2_Manutenzione HP successivo anno 1 FSA-1000D-BDL-C	Manutenzione mensile HP anno successivo Sandbox	TELECOM ITALIA	1 (per 36 mesi)

6.3 Servizi di addestramento e formazione

I servizi di "addestramento e formazione" sono costituiti da addestramento sulla fornitura, formazione di base e formazione avanzata sulle reti locali.

Si distinguono due diversi servizi:

- un **servizio di addestramento** all'uso del Sistema installato, da effettuarsi nella sede dell'Amministrazione
- un **servizio per la fruizione di sessioni formative** impartite presso le sedi dell'Amministrazione che permettano di istruire i discenti su tematiche inerenti il networking

Sarà cura di Telecom Italia la predisposizione di una scheda di valutazione che rispecchi gli argomenti riportati nel programma dello specifico corso e preveda una valutazione del trattamento degli stessi da parte del personale dell'Amministrazione partecipante al corso con tre livelli di gradimento, di cui uno insufficiente.
Al termine di ciascuna sessione l'Amministrazione potrà valutare le schede compilate dai partecipanti e, in caso di una valutazione che non sia almeno sufficiente per almeno il 20% dei partecipanti e almeno buona per almeno il 20% dei partecipanti (scala insufficiente, scarso, sufficiente, buono, ottimo), potrà chiedere la ripetizione della sessione per gli argomenti che hanno avuto gradimento negativo.
A conclusione dei corsi Telecom Italia rilascerà all'Amministrazione un Verbale di erogazione del Corso attestante la data di effettiva erogazione del servizio, la durata effettiva, il programma effettivamente seguito ed eventuali criticità emerse.

Famiglia	Codice Articolo Convenzione	Q.tà ore
Servizio di addestramento e formazione	RL6L2_Addestramento fornitura	4

6.3.1 Servizio di addestramento sulla fornitura

Telecom Italia organizzerà un servizio di addestramento all'uso del sistema installato, da effettuarsi nella sede dell'Amministrazione che, in particolare, dovrà perseguire gli obiettivi seguenti:

- Conoscenza della configurazione degli apparati forniti ed installati, nonché le funzionalità del sistema di gestione, qualora fornito e mettere in grado il personale designato dall'Amministrazione di gestire in maniera autonoma ed ottimale la rete installata sia per la parte attiva che per la passiva, ma soprattutto come da richiesta la possibilità e la capacità di estrapolare eventualli report dal sistema di gestione.
- La durata complessiva del corso non potrà comunque superare il numero di ore massimo di seguito elencate riferite ad ogni tipologia di apparato

Tipologia fornitura	Q.tà ore
Dispositivi per la sicurezza delle reti	4

6.4 Servizio di intervento su chiamata su PDL

Ricadono nelle specifiche di tale servizio tutte le lavorazioni ordinarie relative alle PDL quali:

- modifica delle configurazioni di una PDL esistente;
- ripristino in esercizio delle seguenti componenti del cablaggio relative alla singola PDL:
  - cablaggio orizzontale;
  - collegamenti verticali o di dorsale (sia in rame, sia in fibra);
  - funzionalità degli armadi rack;
  - tutti gli elementi costituenti il cablaggio strutturato.
  - Tutti i servizi compresi come descritto nel paragrafo 4.2 e 4.4.

La validità del pacchetto è limitata a 48 mesi dalla data di ordinativo della fornitura.

L'elemento minimo di servizio è costituito da un pacchetto per 25 PDL nell'ambito del quale non potranno essere richiesti più di 5 interventi.
L'Amministrazione Contraente dovrà richiedere un sufficiente numero di pacchetti di intervento su PDL, sulla base delle lavorazioni previste e a copertura della propria rete LAN. lo stesso

pacchetto potrà essere utilizzato su PDL che appartengano a differenti reti locali purchè appartenenti allo stesso comune.
La validità del pacchetto è limitata a 48 mesi dalla data di avvio del servizio di fornitura.

Si precisa che il servizio di intervento su PDL sarà eseguito nel rispetto degli SLA e **secondo le modalità** riportati nella Guida alla Convenzione.

Tipologia fornitura	Q.tà pacchetti
Servizi MAC per PDL	55

7. PROJECT MANAGEMENT E PIANO DI REALIZZAZIONE

Le attività saranno espletate senza interruzioni in conformità al piano delle attività seguente, salvo problemi legati all'approvviggionamento dei materiali, a partire dalla data di avvio lavori preventivamente concordata con l'Amministrazione che decorrerà dalla data in cui l'Amministrazione renderà disponibili i locali ove andranno realizzate le attività descritte nel Progetto esecutivo ed eventualmente i titoli edilizi necessari.
Tale data, definita come **"Data di disponibilità dei locali**", sarà indicata dall'Amministrazione nell'Ordinativo di fornitura oppure attraverso l'emissione di un apposito "Verbale di disponibilità dei locali" successivo all'emissione dell'Ordinativo di fornitura.
Pertanto, tutte le date riportate nel piano di attivazione o cronoprogramma sono espresse in termini di lasso temporale intercorrente dalla Data di disponibilità dei locali.
Si precisa che alcune delle attività previste potranno essere svolte anche in parallelo tra loro.

Il piano delle attività, se necessario, potrà essere verificato ed aggiornato a cura dei responsabili delle parti anche durante la fase realizzativa.

Macro attività	Durata attività (giornate lavorative)
Fornitura e lavori di posa in opera di apparati passivi	20 gg
Lavori di realizzazione di opere civili accessorie alle forniture	20 gg
Fornitura e installazione di apparati attivi	20 g
Certificazione e collaudo Impianti	20 gg

Relativamente ai lavori di realizzazione di opere civili accessorie alle forniture, eventuali criticità, non prevedibili e/o
pianificabili in fase progettuale, potranno essere oggetto di riesame tra le parti in relazione agli impatti sulla
pianificazione temporale nonché la eventuale revisione di spesa richiesta.

8. PIANI DI SICUREZZA

In relazione al progetto in oggetto, in ottemperanza alle disposizioni di cui ai Decreti in vigore, (art.7 D.Lgs. 626/94 - art.26 D.Lgs. 81/08), il Piano Operativo di Sicurezza che sarà messo in atto dal personale di impresa da noi comandato ad operare presso le Vostre sedi Vi sarà inviato successivamente.

Con l'occasione Vi comunichiamo che il personale TIM, che interverrà presso le Vostre sedi per le attività di progettazione, coordinamento lavori e collaudo, è stato formato in merito agli articoli di legge suddetti, è stato reso consapevole dei rischi da Voi elencati e non introduce a sua volta eventuali rischi con la propria attività.

9. ONERI DI PROGETTAZIONE

Nel caso in cui l'Amministrazione Contraente decidesse di non approvare il presente Piano di Esecuzione Definitivo e quindi di non procedere all'emissione dell'Ordinativo di fornitura, l'Amministrazione Contraente dovrà comunque corrispondere all'Aggiudicatario un corrispettivo per le attività preliminari svolte, secondo quanto indicato nella seguente tabella:

PDL	Importo
≤ 100 oppure solo fornitura	**1.000 €**
tra 100 e ≤ 200	**2.000 €**
> 200	**5.000 €**

Tabella - Remunerazione costo del Piano di esecuzione definitivo

Le PDL che devono essere valutate per il computo del costo della pianificazione operativa sono quelle indicate dall'Amministrazione nella Lettera d'ordine per la redazione del Piano di esecuzione definitivo.
Si precisa che i corrispettivi indicati nella tabella sopra riportata sono fissi, invariabili ed omnicomprensivi di ogni onere e spesa inerenti tutte le attività preliminari svolte e non sono oggetto di offerta e, quindi, di ribasso da parte dei Fornitori.
L'Amministrazione Contraente potrà non procedere con l'Ordinativo di Fornitura, senza alcun onere a suo carico, qualora la quotazione riportata nel Piano di esecuzione definitivo risulti superiore del 10% (dieci per cento) rispetto alla quotazione del preventivo economico preliminare (riportata nel Piano di Esecuzione Preliminare).

10. ALLEGATI

Allegato 1 - Richiesta Progetto Preliminare/Valutazione Preliminare.

df

via Volta.pdf

Allegato 2 - Piano di Esecuzione Preliminare

Provincia di Como.p

Allegato 3 - Richiesta Progetto Definitivo/Valutazione Definitiva.

DF

Allegato 4 - Preventivo Economico Definitivo (IVA esclusa) relativi ai prodotti e ai servizi richiesti sulla base del Listino di fornitura della Convenzione Reti Locali 6 ed ai lavori di realizzazione di opere civili accessorie alle forniture (listini DEI).

definitivo Provincia

Codice Articolo Convenzione	Quantità
RL6L2_FG-300E-BDL-C	4
RL6L2_Configurazione FG-300E-BDL-C	4
RL6L2_Manutenzione HP Anno 1 FG-300E-BDL-C	4
RL6L2_Manutenzione HP successivo anno 1 FG-300E-BDL-C	4
RL6L2_FC-10-00306-900-02-12	12
RL6L2_FSA-1000D-BDL-C	1
RL6L2_Configurazione FSA-1000D-BDL-C	1
RL6L2_Manutenzione HP Anno 1 FSA-1000D-BDL-C	1
RL6L2_Manutenzione HP successivo anno 1 FSA-1000D-BDL-C	1
RL6L2_FC-10-SA01K-969-02-12	3
RL6L2_DEISERVIZI	1
RL6L2_Addestramento fornitura	4
RL6L2_Intervento25PDL	55

Durata	Prezzo Totale
	19867,20
	1192,04
12	582,24
36	1997,28
	22021,68
	20771,04
	1246,26
12	608,88
36	2087,64
	13163,28
	7050,00
	120,00
	30250,00
TOTALE	**120957,54**

Famiglia

Dispositivi di sicurezza - FORTINET

Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET

Dispositivi di sicurezza - FORTINET

Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET
Dispositivi di sicurezza - FORTINET
Listino DEI
Servizio di addestramento e formazione
Servizi MAC per PDL

Codice Articolo Convenzione

RL6L2_FG-300E-BDL-C

RL6L2_Configurazione FG-300E-BDL-C
RL6L2_Manutenzione HP Anno 1 FG-300E-BDL-C
RL6L2_Manutenzione HP successivo anno 1 FG-300E-BDL-C
RL6L2_FC-10-00306-900-02-12

RL6L2_FSA-1000D-BDL-C

RL6L2_Configurazione FSA-1000D-BDL-C
RL6L2_Manutenzione HP Anno 1 FSA-1000D-BDL-C
RL6L2_Manutenzione HP successivo anno 1 FSA-1000D-BDL-C
RL6L2_FC-10-SA01K-969-02-12
RL6L2_DEISERVIZI
RL6L2_Addestramento fornitura
RL6L2_Intervento25PDL

Descrizione Articolo Convenzione

Fornitura in opera dispositivi di sicurezza fascia media

Configurazione Dispositivo sicurezza fascia media
Manutenzione mensile HP Anno 1 Dispositivi di sicurezza fascia media
Manutenzione mensile HP anno successivo Dispositivi di sicurezza fascia media
Aggiornamento dei dispositivi per la sicurezza di fascia media

Fornitura in opera Sandbox

Configurazione Sandbox
Manutenzione mensile HP Anno 1 Sandbox
Manutenzione mensile HP anno successivo Sandbox
Aggiornamento del dispositivo Sandbox
Lavori di realizzazione di opere civili accessorie alla fornitura - Servizi
Addestramento sulla fornitura
Pacchetto per 25 postazioni di lavoro

Produttore	Quantità	Durata	Unità di misura	Prezzo senza IVA
FORTINET TELECOM ITALIA	4		pezzo	4966,80
TELECOM ITALIA	4		pezzo	298,01
TELECOM ITALIA	4	12	pezzo/mese	12,13
TELECOM ITALIA	4	36	pezzo/mese	13,87
FORTINET	12		pezzo	1835,14
FORTINET TELECOM ITALIA	1		pezzo	20771,04
TELECOM ITALIA	1		pezzo	1246,26
TELECOM ITALIA	1	12	pezzo/mese	50,74
TELECOM ITALIA	1	36	pezzo/mese	57,99
FORTINET	3		pezzo	4387,76
TELECOM ITALIA	1		Ordinativo	7050,00
TELECOM ITALIA	4		Ora di docenza	30,00
TELECOM ITALIA	55		Pacchetto	550,00
				TOTALE
				TOTALE GENERALE

UT Totale	Canone Anno 1 Totale	Canone Anno 2 Totale
19867,20		
1192,04		
	582,24	
		665,76
22021,68		
20771,04		
1246,26		
	608,88	
		695,88
13163,28		
7050,00		
120,00		
30250,00	30250	
###	**1191,12**	**1361,64**
###		

Canone Anno 3 Totale	Canone Anno 4 Totale
665,76	665,76
695,88	695,88
1361,64	**1361,64**

Codice Articolo Acquisto
FG-300E-BDL-C
Installazione FG-300E-BDL-C
Configurazione FG-300E-BDL-C
Man. HP Anno 1 FG-300E-BDL-C
Man. HP s.a. 1 FG-300E-BDL-C
FC-10-00306-900-02-12
FSA-1000D-BDL-C
Installazione FSA-1000D-BDL-C
Configurazione FSA-1000D-BDL-C
Man. HP Anno 1 FSA-1000D-BDL-C
Man. HP s.a. 1 FSA-1000D-BDL-C
FC-10-SA01K-969-02-12
DEISERVIZI
Addestramento fornitura
Intervento25PDL

Descrizione Articolo Acquisto

Fornitura dispositivi di sicurezza fascia media
Installazione dispositivi di sicurezza fascia media
Configurazione Dispositivo sicurezza fascia media
Manutenzione mensile HP anno 1 Dispositivi di sicurezza fascia media
Manutenzione mensile HP anno successivo Dispositivi di sicurezza fascia media
Aggiornamento dei dispositivi per la sicurezza di fascia media
Fornitura Sandbox
Installazione Sandbox
Configurazione Sandbox
Manutenzione mensile HP anno 1 Sandbox
Manutenzione mensile HP anno successivo Sandbox
Aggiornamento del dispositivo Sandbox
Lavori di realizzazione di opere civili accessorie alla fornitura - Servizi
Addestramento sulla fornitura
Pacchetto per 25 postazioni di lavoro

Provincia di Como

VISTO DI REGOLARITA' CONTABILE

DETERMINAZIONE DIRIGENZIALE N. 620 / 2020

UNITA' PROPONENTE: S2.04 SERVIZIO SISTEMI INFORMATIVI
OGGETTO: AFFIDAMENTO DEL SERVIZIO DI SICUREZZA PERIMETRALE DELLA RETE INFORMATICA DELLA PROVINCIA DI COMO. IMPEGNO DI SPESA EURO 147.568,20 (IVA INCLUSA). CODICE CIG: 8328653DDE.

Visto di regolarità contabile attestante la copertura finanziaria ai sensi dell'art. 147 bis del D.Lgs. n. 267 del 18.08.2000 e s.m.i. cap. 23950/3 imp. 1565/2020 per € 33.884,72 in entrata da avanzo vincolato

cap. 22300/1 imp. 1566/2020 per € 65.520,55 in entrata da cap. 7170 acc. 887/2020 per € 65.520,55

cap. 1450/19 imp. 1567/2020 per € 8.580,89

cap. 1450/19 imp. 46/2021 per € 10.887,45
cap. 1450/19 imp. 7/2022 per € 10.887,45

sull'esercizio 2023 l'importo di euro 10.887,45 sarà impegnato sul cap. 1450/19 ad approvazione del bilancio 2021/2023

sull'esercizio 2024 l'importo di euro 6.919,69 sarà impegnato sul cap. 1450/19 ad approvazione del bilancio 2022/2024

ESITO: **FAVOREVOLE**

Lì, 18/08/2020

IL DIRIGENTE/IL RESPONSABILE DEI SERVIZI FINANZIARI
GALETTI DARIO
(Sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.)