CAPITOLATO SPECIALE D'APPALTO PER L'AFFIDAMENTO DELLA FORNITURA, INSTALLAZIONE, CONFIGURAZIONE, GESTIONE E MANUTENZIONE DI UN SISTEMA DI SICUREZZA PERIMETRALE PER LA PROVINCIA DI COMO

RISERVATEZZA

1. Introduzione

Il presente capitolato contiene le specifiche tecniche relative all'affidamento della fornitura, installazione, configurazione, gestione e manutenzione di un sistema di sicurezza perimetrale per la Provincia di Como, per 30 mesi, dall'1/01/2012 al 30/06/2014;
Nel corpo del capitolato, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:
Capitolato tecnico, il presente documento;
Soluzione, l'insieme delle componenti hardware, dei relativi sistemi operativi, delle licenze software applicative, delle software subscriptions e dei servizi connessi;
Committente, Provincia di Como;
Concorrente, Impresa invitata alla gara;
Fornitore, l'Impresa aggiudicataria.

1.1. Scopo del documento

Le specifiche indicate nel presente capitolato tecnico sono finalizzate alla stipula, da parte del Committente, di un contratto di fornitura, installazione, configurazione, gestione e manutenzione di un sistema di sicurezza informatica perimetrale e servizi correlati per la Provincia di Como.
Il presente documento ha quindi lo scopo di fornire alle aziende concorrenti (di seguito "Concorrenti/e") il riferimento per predisporre l'offerta economica richiesta.

1.2. Modalità dì selezione del fornitore

La selezione della soluzione finale seguirà le seguenti fasi temporali:
- Risposta domande Concorrenti: i Concorrenti potranno richiedere chiarimenti al Committente sui requisiti presenti all'interno del documento. Tempistiche e modalità di interazione sono riportate nel Disciplinare di gara.
- Valutazione delle offerte: le risposte dei Concorrenti giunte all'interno delle tempistiche definite verranno valutate secondo la modalità dell'offerta economicamente più vantaggiosa.
- Selezione del Concorrente vincitore: a valle delle valutazioni avverrà la selezione definitiva del Fornitore e la stipula del contratto di fornitura tra il Committente e il Fornitore.
- Fornitura, configurazione e messa in esercizio: in questa fase verrà consegnata e configurata la soluzione sulla base delle esigenze del Committente.
- Collaudo dell'implementazione realizzata: a valle della messa in servizio, la soluzione del Fornitore verrà sottoposta a collaudo e, in caso di successo, passata in produzione.

2. Obblighi del fornitore

Presentando offerta i Concorrenti riconoscono di:
- aver preso visione, condividere, accettare ed impegnarsi a rispettare nella fornitura tutte le specifiche definite;
- riconoscere fin d'ora, nel caso, per qualsiasi motivo, l'offerta tecnica dovesse risultare in alcune sue parti non congruente o carente rispetto ai contenuti in seguito specificati, che tali parti dell'offerta saranno ritenute nulle.

Le informazioni relative al contesto Committente sono da intendersi come indicative e sono state introdotte al fine di mettere il Concorrente nella condizione di poter formulare un'offerta.

2.1. Garanzia

La garanzia richiesta per tutte le componenti della fornitura è di 30 (trenta) mesi, quindi per tutta la durata del contratto.

2.2. Formazione

Dovrà essere fornita una formazione introduttiva generale sui prodotti oggetto della fornitura. Si richiedono almeno n. 3 giornate di formazione erogate da personale certificato sulle tecnologie oggetto dell'offerta.
Il Concorrente potrà proporre ulteriori attività di formazione specifiche sulle tecnologie fornite.

2.3. Collaudo

La modalità di esecuzione delle varie attività di collaudo della fornitura avverranno sulla base di liste di riscontro (checklist) che indirizzano tutte le caratteristiche richieste del presente documento. Il piano di collaudo del sistema e le liste di riscontro dovranno essere presentati dal Fornitore e approvati dal Committente. La pianificazione del collaudo deve essere in accordo con il piano di installazione e di attivazione del sistema.
Il collaudo dovrà accertare che la soluzione sia stata regolarmente installata, sia regolarmente funzionante, sia perfettamente integrata con la struttura applicativa pre-esistente, soddisfi le esigenze previste e sia conforme alle indicazioni contenute nel presente capitolato tecnico.
Il Fornitore si impegna alla tempestiva eliminazione di tutti i difetti e/o vizi eventualmente riscontrati in sede di collaudo.
Tutto quanto necessario per l'effettuazione delle prove di collaudo (eventuali strumenti di misura, manodopera, ecc.) dovrà avvenire a cura, spese e responsabilità del Fornitore.
La soluzione si intenderà collaudata positivamente solo dopo l'eliminazione definitiva di ogni difetto e /o vizio eventualmente riscontrati in sede di collaudo e la firma dell'accettazione lavori da parte del Committente.
Nel caso di collaudo negativo per responsabilità del Fornitore, lo stesso è tenuto a propria cura e spese ad eliminare i vizi accertati entro il termine massimo di 15 giorni, ferma l'applicazione delle penali previste dal contratto fino al collaudo con esito positivo.
Eventuali inadempimenti e/o ritardi dovuti a causa di forza maggiore dovranno essere comunicati tempestivamente dal Fornitore al Committente.

2.4. Documentazione tecnica e manualistica

Il Fornitore deve rendere disponibile al Committente la seguente documentazione:

- Documentazione tecnica, relativa ad ogni componente della fornitura (installazione, configurazione, architettura funzionalità, ecc.);
- Disegno della soluzione implementata che riporti il posizionamento dei sistemi di protezione, le caratteristiche di funzionamento e le modalità di funzionamento dei software in relazione all'attuale rete locale del Committente;
- Verbali. Si prevede di documentare e riassumere gli aspetti trattati e le decisioni prese nel corso delle riunioni di avanzamento effettuate nell'ambito di progetto.

3. Oggetto della fornitura

Viene richiesta la fornitura di un sistema di sicurezza perimetrale mediante fornitura di hardware e software, a noleggio e in comodato d'uso gratuito per l'intera durata dei contratto, e dei servizi di installazione, configurazione, gestione, manutenzione e monitoraggio proattivo per un periodo di trenta mesi, a decorrere dall'1/01/2012.

3.1. Contesto del Committente e situazione attuale

A scopo informativo, si riportano le informazioni relative al contesto del Committente e alla soluzione attualmente in uso.

3.1.1 Contesto del Committente

La rete della Provincia di Como è così strutturata:

SEDE VIA BORGO VICO 148:
Connettività:

- n. 2 connettività internet, 8 megabit, con backup, ciascuna con un pool di 16 indirizzi pubblici (una ad uso generale ed una prevalentemente dedicata al sistema bibliotecario)
- connettività MPLS Telecom in fibra con le sedi di Via Volta, Via Sirtori e Via Borgo Vico 163.

LAN Provincia:
Utenti: circa 300
(Le sedi di Via Borgo Vico 163 e Via Sirtori dispongono solamente del collegamento con la sede centrale ed utilizzano la connettività internet in uscita da essa: gli utenti sono stati conteggiati nel numero sopraindicato).
È presente un router fornito da Lombardia Integrata per una connessione VPN dedicata per alcuni servizi erogati per conto di Regione Lombardia.
È presente inoltre una rete wireless che copre alcune sale di rappresentanza (la sala dove si svolge il Consiglio Provinciale e alcune sale attigue), attestata su una VLAN dedicata.
Si sta valutando la creazione un'altra VLAN da dedicare a sale che vengono concesse in uso a soggetti esterni.
Si sta studiando la realizzazione di un'altra rete wireless per una sala corsi.
Il server di posta (Exchange 2003) gestisce 410 caselle di posta.
Sono attivi collegamenti VPN con alcuni fornitori di software per la manutenzione remota dei loro software (sia site-to-site, sia client-to-site).
Vi è una DMZ.

SEDE VIA VOLTA:
Connettività:

- connettività internet, 8 megabit, con 16 IP pubblici
- connettività MPLS Telecom 8 megabit con la sede di Via Borgo Vico 148 (è in corso l'acquisizione del backup) e con i CPI (n. 5) (2Mb ciascuna)

Utenti: circa 120 (tra sede e CPI: gli utenti dei CPI escono su internet tramite la connettività della sede di Via Volta).
Vi è un'estensione della rete (in parte cablata ed in parte wireless) verso la confinante Prefettura che dovrà essere attestata sul firewall. Sarà utilizzata solo in casi particolari. Alla stessa bisogna garantire l'accesso internet, i servizi VPN, l'accesso ad alcuni server.
È presente un server di posta Lotus Domino (che si ha intenzione di dismettere nei prossimi mesi).
È presente un server Sharepoint e n. 2 server IIS.

In complesso, tra le varie sedi, sono presenti 3 domini Windows (2003), senza relazioni di trust: 1 in Via Borgo Vico 148, 1 in Via Volta ed 1 in Via Sirtori.

3.1.2 Situazione attuale

Si riporta di seguito l'elenco delle componenti tecnologiche che compongono la soluzione attualmente installata presso le sedi di Via Volta e di Via Borgo Vico 148.

Via Volta

Hardware/Software Firewall	Cluster Check Point realizzato con due moduli Check Point R71.30 a bordo di due appliance IP290 Management distribuita su piattaforma Check Point Provider-1 (Secure Platform R71.30)

Software Antispam	Erogato dal server di via Borgo Vico
Web/url filtering	IWSS 3.1 installato su proxy squid. Web filtering agganciato a websense di via Borgo Vico
Reverse Proxy	Soluzione di reverse proxy basata su tecnologia IIS
Proxy server	Squid con IWSS 3.1 integrato con websense su piattaforma hardware IBM 3250
Lac	Appliance proprietaria su piattaforma hardware IBM 3250

Via Borgo Vico

Hardware/Software Firewall	Cluster Check Point realizzato con due moduli Check Point R70.30 a bordo di due appliance IP290 Management distribuita su piattaforma Check Point Provider-1 (Secure Platform R70.30)
Software Antispam	Trend Micro IMSS/SPS Version: 7.1 per 400 caselle di posta, su piattaforma Vmware
Web/url filtering	Websense Web Security versione 7.5 per 300 utenti, su piattaforma Vmware
Proxy server	Squid con IWSS 3.1 integrato con websense, su piattaforma Vmware
LAC	Appliance proprietaria su piattaforma Vmware
Bilanciatori	N°2 Appliance proprietarie su hardware dedicato
Reverse Proxy	Soluzione di reverse proxy basata su tecnologia IIS

3.2. Tecnologie richieste

Si riporta elenco delle componenti tecnologiche hardware e software della soluzione richiesta, sia per la sede di Borgo Vico, sia per la sede di via Volta. L'hardware fornito dovrà essere tutto rackable e dovrà essere installato in rack 19" forniti dal Committente. Stante la comprovata efficacia sperimentata durante i precedenti contratti dell'attuale architettura, si richiede la fornitura di una soluzione che ricalchi lo schema logico di quella attualmente in uso.
Dettaglio delle componenti tecnologiche hardware e software della soluzione richiesta per la sede di Borgo Vico:

Software Firewall/IPS	Soluzione Firewall in cluster con management distribuita ed esterna all'Amministrazione
Software Antivirus	Soluzione Antivirus perimetrale con le

	caratteristiche di seguito riportate
Software Antispam	Soluzione Antispam perimetrale con le caratteristiche di seguito riportate
Proxy + Web/url filtering	Soluzione di Web Filtering perimetrale con le caratteristiche di seguito riportate
Reverse Proxy	Soluzione di reverse proxy con le caratteristiche di seguito riportate
Controllo accessi LAN	Soluzione di controllo degli accessi alla LAN con le caratteristiche di seguito riportate
Gestione connettività Internet	Soluzione di bilanciamento traffico IP con le caratteristiche di seguito riportate

Tabella 1. Sede di via Borgo Vico

Dettaglio delle componenti tecnologiche hardware e software della soluzione richiesta per la sede di Via Volta:

Software Firewall/IPS	Soluzione Firewall in cluster con management distribuita ed esterna all'Amministrazione
Software Antivirus	Soluzione Antivirus perimetrale con le caratteristiche di seguito riportate
Software Antispam	Soluzione Antispam perimetrale con le caratteristiche di seguito riportate
Proxy + Web/url filtering	Soluzione di Web Filtering perimetrale con le caratteristiche di seguito riportate
Controllo accessi LAN	Soluzione di controllo degli accessi alla LAN con le caratteristiche di seguito riportate

Tabella 2. Sede di Via Volta

Il fornitore garantirà l'installazione di un sistema che possa dirsi migliorativo dell'attuale sia in termini di hardware sia in termini di software, fornendo, tra l'altro, i software aggiornati all'ultima versione disponibile.

3.3. Caratteristiche del servizio

Si richiede al fornitore di fornire, gestire, monitorare e manutenere la soluzione, collaborando con il Committente nella progettazione e gestione delle politiche di sicurezza.
Si intendono a carico del fornitore tutte le attività (a titolo indicativo ma non esaustivo: configurazione, ottimizzazione, gestione, manutenzione, aggiornamento, troubleshooting) riguardanti qualsiasi aspetto connesso al servizio.
Il servizio dovrà essere erogato utilizzando apparati che si interfaccino con i sistemi già in uso presso la Provincia di Como attraverso interfacce conformi agli standard IEEE Ethernet/Fast-Ethernet/Gigabit-Ethernet.
Al fine di consentire una gestione efficace del servizio, tutti i dispositivi utilizzati dovranno consentire l'autenticazione tramite accesso logico da console e da remoto.
Inoltre, la soluzione proposta dovrà ridurre al minimo le componenti hardware da installare presso le due sedi del Committente pur garantendo l'alta affidabilità dei singoli servizi oggetto della fornitura, utilizzando ad esempio tecnologie di virtualizzazione.
Il Committente richiede comunque soluzioni tecnologiche dedicate per ogni tematica del progetto, ad eccezione delle tecnologie firewall, IPS e concentratore VPN che potranno essere gestite sul medesimo apparato. È quindi escluso l'impiego di soluzioni di tipo UTM (Unified Threat Management).
I prodotti relativi alle tecnologie di firewall, antivirus, antispam e URL filtering dovranno essere presenti nel "Quadrante Magico" di Gartner di riferimento; il Concorrente dovrà produrre la relativa documentazione.

3.4. Servizio di firewall

I sistemi firewall in cluster forniti dovranno avere un minimo di 8 interfacce per la sede di Via Borgo Vico e di 6 interfacce, espandibili a 8, per la sede di Via Volta, e dovranno inoltre garantire la resistenza al singolo guasto grazie ad un'architettura ridondata.
I firewall consentiranno di applicare regole di assenso o restrizione sui singoli servizi sia a livello di network sia a livello di singolo indirizzo IP.
I sistemi di firewalling su cui sarà basato il servizio dovranno supportare una politica di sicurezza di rete del tipo: "Nega qualsiasi servizio fatta eccezione per quelli esplicitamente permessi". In fase di installazione e messa in esercizio tutti i servizi dovranno essere temporaneamente bloccati e sarà possibile autorizzare i servizi necessari solo ad istallazione avvenuta e dopo aver effettuato una verifica della corretta operatività del firewall.
I firewall analizzeranno tutti i pacchetti prima che essi raggiungano il sistema operativo del gateway, inoltre verificheranno la compatibilità di ogni pacchetto con le politiche di sicurezza definite prima di processare i livelli alti della comunicazione.
Ognuno dei sistemi di Firewall sarà costituito da:

- una propria e dedicata stazione di management;
- una consolle di controllo;
- Server di log.

Ciascuna stazione di management, che costituisce il punto nevralgico per il controllo centralizzato di tutti i nodi che compongono l'architettura di security, dovrà essere esterna all'Ente, quindi non installata sui firewall, e accessibile attraverso una GUI dedicata (non basata su piattaforme browser) da più client contemporaneamente e con livelli di accesso alle risorse opportunamente delegabili secondo profili predefiniti. L'accesso via GUI alla management deve poter avvenire attraverso processi di autenticazione basati anche su certificati o su schemi a più fattori (ad esempio, One Time Password).
Inoltre, la soluzione richiesta deve prevedere sia che la stazione di management sia in architettura di alta affidabilità, sia, come servizio opzionale, che una stazione di management secondaria, possa essere attestata presso la sede del Committente; quest'ultima soluzione dovrà garantire continuità di servizio in caso di temporanea indisponibilità della stazione di management principale attestata presso il Fornitore.
La soluzione richiesta deve anche prevedere la possibilità di accentrare le due stazioni di management (quella che gestisce il cluster di firewall di via Borgo Vico e quella che gestisce il cluster di firewall di via Volta) su un'unica stazione di management, con le caratteristiche indicate al paragrafo precedente. Tale stazione unica di management dovrà comunque garantire la possibilità di poter creare e gestire le politiche di sicurezza distinte per ciascuno dei due cluster di firewall, con privilegi di amministrazione differenziati.
L'aspetto dell'interfaccia di management dovrà essere caratterizzato da una semplicità grafica che la renda facilmente utilizzabile anche da parte di personale meno esperto (ad es., presenza di funzionalità drag and drop, ricerca contestuale, cloning degli oggetti).
Il sistema deve integrare un servizio di raccolta log centralizzato, remoto rispetto ai firewall veri e propri che dovranno generare i log di tutte le connessioni ispezionate e trasmetterli criptati verso il rispettivo log server. Ogni management dovrà avere il proprio log server che potrà eventualmente coincidere con la stazione di management.
I log dovranno essere raccolti dal server in real time e dovranno essere archiviati in un database e non su file di testo. Dovrà essere possibile l'interrogazione tramite query personalizzabili.
Infine, attraverso la raccolta dei log e la loro elaborazione, si dovranno prevedere report sintetici, consultabili via web e disponibili con dati aggiornati con frequenza giornaliera, settimanale e mensile, relativi, a titolo di esempio, alle seguenti informazioni: statistiche generali sull'attività del Firewall, allarmi e attività di eventuali utenti in VPN, utilizzo della interfacce dei Firewall con ripartizione del traffico per i protocolli più comunemente usati (http, https, ftp, dns, smtp), eventi rilevati dai log, ecc.
La tecnologia utilizzata sarà del tipo stateful inspection che consente a differenza delle altre di esaminare i dati di tutti e sette i livelli della comunicazione e di confrontarne lo stato con quelli della precedente comunicazione, controllando indirizzo IP, numero della porta e altre

informazioni in modo tale da determinare se i pacchetti sono conformi alee regole definite nelle politiche di sicurezza
I sistemi di firewall devono riconoscere ed ispezionare più di 200 protocolli tra cui:

- VoIP (SIP, H.323, MGCP, e SCCP con il supporto del NAT);
- Instant Messaging (MSN, Yahoo, ICQ, GoogleTalk, e QQ);
- Peer-to-peer (Kazaa, Gnutella, BitTorrent, eMule, DirectConnect, Soulseek, Thunder e Winny);

e deve inoltre garantire i seguenti valori dichiarati:

- Firewall Throughput 1.5Gbps;
- VPN Throughput 1.0Gbps;
- Sessioni concorrenti 900.000;
- IPS Throughput 1.4Gbps;
- Numero VLAN supportate 1024;
- Supporto dell'accelerazione software dei pacchetti;
- Disponibilità dell'acceleratore del traffico VPN;
- Sistema Disk Based;
- Supporto dei protocolli di routing dinamici BGP, OSPF, RIPv1, RIPv2;
- Supporto di due connettività Internet distinte in modo da poter assicurare la continuità del traffico sia in ingresso che in uscita. Il firewall deve implementare la funzionalità di DNS proxy in modo da restituire la risoluzione del nome del servizio (ad esempio www, smtp, pop) con l'indirizzo IP annunciato sul link attivo.

Inoltre, la stazione di management deve poter gestire altre funzionalità aggiuntive di sicurezza, tra cui:

- Quality of Service
- Controllo delle applicazioni;
- Data Loss Prevention;
- User Access Identity (NAC software);
- Sistema di revisione delle politiche di sicurezza;
- Integrazione del database utenti con Microsoft Active Directory: le policy dovranno poter essere realizzate utilizzando gli oggetti presenti nelle AD del Committente.

Per aumentare il livello di protezione fornito dal servizio sarà possibile inoltre, nascondere con porte fittizie, le porte effettive di ascolto dei sistemi server protetti dai firewall, utilizzando appunto un sistema di PAT Management.
Il fornitore dovrà farsi carico dell'attività di User Management, ossia di garantire e manutenere le autorizzazioni ed il profilo di accesso al servizio erogato. Il fornitore provvederà ad evadere tutte le richieste di creazione, modifica e/o cancellazione degli account utente, di modifica delle password, di sblocco sessioni secondo le modalità concordate.

3.5. Servizio di Content Filtering

E' necessario monitorare la rete aziendale controllando tutti gli accessi IP delle workstation e bloccando tipologie di siti particolari.
Si vuole ottenere un'architettura ridondata in modo da avere una protezione sia dai siti ritenuti pericolosi sia dall'uso inappropriato del web quali pornografia, violazione del copyright, download di file, media streaming, ecc..
Inoltre, visto che in realtà di grandi dimensioni il 40% dell'utilizzo di Internet in ufficio risulta slegato dalle attività lavorative, per preservare la produttività individuale è necessario definire una serie di categorie "non navigabili".
Le politiche di navigazione verranno definite associando ai singoli settori e/o singoli utenti appartenenti alla Provincia di Como nonché singoli IP o classi di IP le relative categorie ritenute utili per lo svolgimento delle attività lavorative.
Il fornitore assegnatario dovrà garantire le seguenti caratteristiche del servizio di Content Filtering Management:

3.5.1. Gestione e controllo dell'accesso alle risorse Internet

Per la gestione ed il controllo degli accessi alle risorse Internet degli utenti è richiesto un servizio Web Filtering, che possa essere integrato con una tecnologia di proxy.
La soluzione richiesta, per la gestione ed il controllo della navigazione di 500 utenti, dovrà essere installata su un apparato, possibilmente in ambiente virtuale, integrandola con il proxy server.
La soluzione dovrà prevedere l'installazione di due server proxy web, uno presso la sede di via Borgo Vico 148 ed il secondo presso la sede di Via Volta. Entrambi i proxy dovranno essere integrati al sistema di web filtering della sede di Via Borgo Vico 148.
Sia il server di web filtering sia il server proxy dovranno essere integrati nella struttura Active Directory. Tutti i client delle sedi dovranno puntare ai proxy server per essere abilitati a navigare su Internet: l'integrazione del proxy con l'Active Directory consentirà una precisa identificazione degli utenti, anche nelle sedi remote. La procedura di autenticazione sarà trasparente se l'utente richiede l'accesso ad Internet da un PC membro del dominio, mentre sarà esplicita, mediante una apposita finestra di pop-up, se l'utente accede da un PC non membro di dominio (es. il PC di personale esterno)
A tutti gli utenti, locali o delle sedi remote, registrati sull'Active Directory della sede centrale, si dovranno applicare le policy di Web Filtering e dovrà essere garantita la reportistica in modo granulare fino a gestire un singolo utente di dominio o un gruppo di utenti dello stesso.
Con questa specifica integrazione, tutte le richieste rivolte al proxy dagli utenti della rete verranno processate dal web server il quale, applicando le policy definite, ne regolamenterà il traffico. Le policy potranno essere definite per

- Utente di dominio
- Indirizzo IP
- Network Range
- Gruppo di utenti di dominio

Tale architettura dovrà gestirà l'accesso ad Internet generato dai protocolli http, https ed ftp, oltre a tutti i protocolli che si possono incapsulare in questi, come, per es., MSN Messenger, AOL, Streaming ed altri, con l'eccezione di Skype attraverso il protocollo https.

Si deve infine prevedere:

- Una procedura per l'utilizzo di internet da parte degli utenti guest, non appartenenti al Dominio (il Committente ha alcune sale che concede in uso per convegni, venti, ecc.);
- una gestione centralizzata e semplificata dell'accesso ai servizi Internet tramite policy di Active Directory, concentrando i controlli in un unico punto (il proxy server) e bloccando qualsiasi altro accesso non autorizzato;
- applicazione granulare e differenziata per singolo utente delle policy di URL Filtering relative agli accessi ad Internet effettuati da tutti gli utenti che utilizzano server Terminal/Citrix;
- caching del traffico web con conseguente aumento delle prestazioni nell'accesso alle pagine più visitate (funzionalità erogata dal server proxy);

Tutti i dati relativi all'accesso ad Internet generati dal sistema di web filtering devono essere raccolti e memorizzati su un database, in modo da garantire un periodo di retention pari a circa 6 mesi.
Deve essere inoltre garantito un backup regolare dei log utilizzando l'infrastruttura di backup del Committente.
Il fornitore assegnatario dovrà erogare il servizio di Content Filtering Management per i seguenti sistemi operativi:
Windows 2000 Professional; Windows 2000 Server; Windows 2003 Server; Windows 2008 Server; Windows XP; Windows Vista; Windows Seven; Linux (kernel 2.2 o superiore); Mac OSX, MAC OS9; Unix (HP-UX, Sun Solaris, IBM AIX).

3.6. Servizio di protezione della posta elettronica da virus e spam

Il fornitore dovrà fornire e gestire un sistema centralizzato e ridondato per la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica. Il sistema proposto dovrà essere caratterizzato dai seguenti parametri:

- efficienza di scansione: 100% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione;
- efficienza nel riparare file o messaggi infetti: 100% dei virus per i quali esiste la possibilità di recupero;
- capacità di eseguire la scansione in tempo reale sui pacchetti IP;
- capacità di eseguire la scansione differita di interi file/documenti allegati;
- supporto;
- configurazioni antispamming che consentano il blocco di messaggi di posta elettronica che transitano per il gateway basati su black list e riconoscimento di porzioni del contenuto del messaggio di posta elettronica personalizzabili;
- supporto ai filtri di esclusione sul tipo di file trasferito in allegato (esempio: vbs, exe, pif, bat, etc.);
- controllo sulla presenza di codice dannoso sui file allegati ai messaggi di posta elettronica supportando almeno i seguenti formati di dati:
  - file con diverse estensioni (vbs, exe, pif, bat);
  - file in formati compressi (zip, gzip, tgzip, rar);
  - verifica sintattica e semantica sull'header dei messaggi;
- piena interoperabilità e/o trasparenza rispetto client e server;
- 2 secondi di ritardo massimo introdotto per l'analisi di ogni singolo messaggio (riferito a messaggi di circa 2 Mbyte);
- 1 secondo di ritardo medio introdotto per l'analisi di ogni singolo messaggio (riferito a messaggi di circa 200 Kbyte);
- supporto dei protocolli standard: SMTP, POP vers, 3 e vers. 4, IMAP vers. 4.

La soluzione proposta deve inoltre prevedere:

- elevate performance dei filtri RBL e del controllo sul carico degli IP sorgenti
- elevato dettaglio dei log del sistema
- architettura in alta affidabilità
- ampliamento dei controlli su filtri RBL, mediante l'interrogazione di ulteriori data base di black list, in aggiunta a quelli offerti dal produttore del sistema antivirus e antispam;
- maggiore granularità nelle politiche di protezione dell'accesso da parte di indirizzi IP ritenuti sospetti: deve infatti essere possibile stabilire, se necessario, il numero di connessioni contemporanee che un indirizzo IP può effettuare;
- possibilità di regolamentare la ricezione delle email applicando filtri di espressioni regolari associate in modo granulare agli indirizzi dei mittenti: per esempio, dovrà essere possibile scartare a priori tutte le email aventi un numero di caratteri superiore a "n" nell'indirizzo del mittente;
- attivazione di livelli di log sui file di testo con maggiori dettagli.

3.7. Servizio di protezione del traffico http e FTP da virus

Il fornitore assegnatario dovrà garantire le seguenti caratteristiche del servizio di protezione del traffico http e FTP da virus:

3.7.1. HTTPS - HTTP Gateway

Gestione di un sistema centralizzato e ridondato per la protezione da codice dannoso che può propagarsi per il tramite della navigazione WEB e per la protezione da attacchi informatici veicolati tramite il protocollo http; il fornitore assegnatario dovrà proporre un sistema caratterizzato dai seguenti parametri:

- efficienza di scansione: 99% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione;
- scansione in tempo reale sui pacchetti IP;

- supporto dei formati comprèssi (almeno zip, gzip, tgzip, rar);
- supporto ai filtri di esclusione sul tipo di file trasferito (esempio: vbs, exe, pif, bat,etc.);
- piena interoperabilità e/o trasparenza rispetto client e server;
- 2 secondi a Mbyte di ritardo massimo introdotto;
- supporto di protocolli standard: HTTP, HTTPS.

3.7.2. FTPS - FTP Gateway

Gestione di un sistema centralizzato e ridondato per la protezione da codice dannoso che può propagarsi per il tramite del trasferimento di file mediante FTP; il fornitore assegnatario dovrà proporre un sistema caratterizzato dai seguenti parametri:

- efficienza di scansione: 100% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e da! media di trasmissione;
- scansione in tempo reale sui pacchetti IP;
- supporto dei formati compressi (almeno zip, gzip, tgzip, rar);
- piena interoperabilità e/o trasparenza rispetto client e server;
- 2 secondi a Mbyte di ritardo massimo introdotto;
- supporto di protocolli standard: FTP, FTPS.

3.8. Servizio di Reverse Proxy

Gestione di un sistema centralizzato e ridondato di reverse proxy per la pubblicazione, via http/https, del servizio di posta elettronica MS Exchange tramite Outlook Web Access e di eventuali altre applicazioni web.
In particolare, il servizio Reverse Proxy dovrà prevedere la configurazione di un server, preferibilmente virtuale, attestato sulla DMZ del Committente in modo da permettere agli utenti remoti di utilizzare il servizio di posta elettronica tramite web mail e tramite il client Outlook senza pubblicare direttamente su Internet il mail server Exchange.
Sono inoltre comprese nel contratto tutte le attività relative alla pubblicazione di eventuali nuove applicazioni web e/o nuovi servizi.

3.9. Servizio di Retention della posta elettronica

È richiesto che il fornitore garantisca il servizio di retention della posta elettronica che deve prevedere la ricezione della posta elettronica a carico del fornitore in caso di temporanea irraggiungibilità dei server di posta del Committente (es. per interruzione del servizio di connettività o per fermo dei server).
In particolare, il fornitore dovrà predisporre presso la propria infrastruttura almeno due server di posta, in modo da mantenere i messaggi di posta in coda per un periodo massimo di 30 giorni, in attesa che vengano risolti gli inconvenienti che hanno portato alla mancata consegna degli stessi ai server interni.
Sono a carico del fornitore le eventuali modifiche o richieste di modifiche alle zone dns registrate dal Committente.

3.10. Servizio Intrusion Detection/Preventions System (IDS/IPS)

Il fornitore dovrà erogare un servizio consistente nell'implementazione e gestione di sistemi di rilevamento ed eventuale prevenzione delle intrusioni Intrusion Detection/Prevention System, che consenta di identificare positivamente tutte le sequenze di eventi, condotti da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o di una rete.
Il servizio di IDS/IPS Management dovrà avere le seguenti funzionalità:

- supporto dei protocolli IEEE Ethernet, Fast-Ethernet, Gigabit Ethernet e tutti i protocolli specificati nello standard TCP/IP.
- capacità di rilevazione degli attacchi garantendo la minore percentuale possibile di falsi positivi e falsi negativi.

- raccolta e conservazione tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili;
- raccolta di informazioni sugli eventi di attacco da una o più sorgenti di informazione tramite"sensori" posti sulla rete;
- analisi predeterminata degli eventi rilevati attraverso l'utilizzo di "signature analysis" che consentono di riconoscere le serie di pacchetti (o i dati contenuti in essi), selezionate preventivamente in fase di configurazione al fine di riconoscere un tipico pattern rappresentativo di un attacco;
- gestione del database delle "signature". Il fornitore dovrà aggiornare con periodicità almeno mensile (o più di frequente se richiesto dal Committente) le "signature" dei sistemi IDS/IPs per mezzo dei quali viene erogato il servizio; il fornitore dovrà inoltre provvedere alla creazione di nuove "signature" su richiesta dal Committente usando un linguaggio di programmazione open;
- 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;
- notifica al Committente di eventuali situazioni che necessitino di interventi/decisioni da parte del Committente stessa;
- console di management unica per la componente IDS e per quella IPS;
- architettura ridondata ed integrata negli apparati di sicurezza perimetrale.

Di seguito vengono indicati ulteriori dettagli tecnici della soluzione richiesta.
Tipologie di protezione implementate:

- attacchi malware;
- attacchi DoS e DDoS;
- vulnerabilità di server e applicazioni;
- protocol misuse;
- minacce interne;
- traffico generato da applicazioni non desiderate (incluse IM e P2P);
- Geo Protection: il traffico deve essere monitorato e controllato in base alla Nazione di origine o destinazione; deve essere possibile gestire delle esclusioni su tali controlli;
- Real Time Protection: la soluzione deve essere costantemente aggiornata e prevedere che molti suoi controlli siano applicati in modo pre-emptive, in modo da proteggere la rete prima che le vulnerabilità (soprattutto Microsoft) siano scoperte e gli exploits creati;

La soluzione dovrà essere integrata negli apparati di sicurezza perimetrale.

3.11. VPN Management

Il fornitore dovrà erogare un servizio di VPN Management consistente nella implementazione e nella gestione di reti virtuali private, basato su una tecnologia che disponga delle seguenti caratteristiche:

- **Data Origin Authentication:** verifica l'autenticità del mittente di ciascun datagramma IP;
- **Data integrity:** verifica che il contenuto di ciascun datagramma non sia stato modificato (deliberatamente o a causa di errori di linea) durante il transito tra sorgente e destinazione;
- **Data confidentiality:** nasconde il testo in chiaro contenuto in un messaggio, mediante l'impiego della crittografia;
- **Replay protection:** assicura che un hacker, intercettato un datagramma IP, non sia in grado,a posteriori, di rispedirlo a destinazione per qualche scopo illecito.

Il fornitore dovrà erogare il servizio di VPN Management secondo le seguenti modalità:

- **autonoma:** il fornitore dovrà provvedere alla realizzazione e gestione di entrambe le terminazioni dei tunnel che realizzano la VPN del Committente;
- **cooperativa**: il fornitore dovrà interagire con altri fornitori per la realizzazione e gestione dei tunnel che realizzano la VPN;

- **predefinita**: ai fini di semplificare la gestione cooperativa nei casi in cui differenze tecnologiche e gestionali tra fornitori diversi non garantiscano una completa interoperabilità è possibile che la scelta del fornitore sia dettata dall'amministrazione che eroga i servizi applicativi. Le altre amministrazioni per poter usufruire dei servizi su VPN IPSec richiedono il servizio di VPN Management allo stesso fornitore.

Sarà pertanto responsabilità del fornitore la progettazione e la fornitura del servizio.

3.11.1. Tipologia delle connessioni

Di seguito sono descritte le possibili modalità di connessione di riferimento per il servizio VPN IPSec che il fornitore dovrà implementare su richiesta del Committente.

Connessione gateway-to-gateway

In questa modalità operativa il servizio offerto dovrà operare creando un tunnel tra due gateway secondo i meccanismi "tunnel mode" descritti nella specifica pubblica RFC 2401. I dispositivi gateway possono essere di tipo hardware e specifici per tale servizio o di tipo software installato su una TdR dell'Ente. È facoltà dell'Ente richiedere dispositivi gateway di tipo hardware specifici per tale servizio. Il fornitore assegnatario sarà completamente responsabile dell'erogazione dei servizi in modalità autonoma o predefinita, mentre il servizio, erogato in modalità cooperativa, richiederà l'implementazione e gestione dell'estremità dei tunnel sotto il dominio amministrativo del fornitore, oltre a tutte le attività necessarie ad attivare il tunnel con fornitori terzi che gestiscono l'altra estremità. La modalità cooperativa richiederà che il fornitore impieghi sistemi interoperabili con terminazioni di tunnel diverse, gestite da fornitori terzi.

Il fornitore dovrà inoltre prevedere la possibilità di realizzare una collegamento VPN tra le sedi di Via Borgo Vico 148 e di Via Volta, in modo da garantire continuità di collegamento anche nel caso in cui la rete geografica basata su tecnologia MPLS non sia disponibile. Il fornitore dovrà fornire al gestore della connettività MPLS in uso tra le due sedi del Committente le informazioni tecniche necessarie ad apportare eventuali modifiche sui router MPLS al fine di realizzare quanto sopra esposto.

I sistemi di sicurezza perimetrale proposti devono prevedere almeno un VPN throughput di 1Gbps.

Connessione per l'accesso remoto (host esterno-gateway)

Il servizio dovrà operare creando un tunnel tra il nodo interessato ed un gateway della rete, secondo la modalità standard IPSec "tunnel mode" come descritta in RFC-2401.

Gli apparati forniti devono prevedere la gestione dell'accesso "sicuro" degli utenti remoti ai sistemi informatici del Committente, attestati sulla rete interna (es. server di posta, server gestionale, ecc.) che, per definizione, non dovrebbero mai essere visibili su Internet. Nessun accesso dall'esterno alla rete LAN interna dovrebbe essere consentito se non in modalità VPN.

In particolare, la gestione dell'accesso ai sistemi interni dell'Azienda da parte di utenti nomadi o clienti/partner/fornitori, mediante un'architettura VPN, potrà essere gestita installando sui PC remoti o su dispositivi palmari, che dovranno comunicare con la sede del Committente, un client VPN, che si occuperà sia di autenticare il singolo utente con il firewall, sia di cifrare il traffico di dati sulle dorsali Internet.

Nel caso in cui l'Amministrazione abbia la necessità di rendere il più flessibile possibile l'utilizzo, da parte di utenti esterni, di applicazioni e servizi attestati sulla propria rete, non vincolandolo all'impiego di uno specifico client installato sul PC remoto, gli apparati dovranno consentire di realizzare VPN senza l'utilizzo di alcun client software installato sui PC remoti: l'opzione Clientless VPN, infatti, è in grado di semplificare l'accesso alle risorse aziendali consentendo agli utenti remoti di accedere, in modalità web-based ed attraverso una VPN su SSL, alle applicazioni presenti all'interno della rete aziendale, anche non web-based, semplicemente utilizzando un browser e scaricando un plug-in dal gateway: la tecnologia utilizzata deve consentire, quindi, agli utenti remoti di utilizzare localmente le loro applicazioni client, creando, attraverso il protocollo web ed in modo trasparente, tunnel VPN per il traffico applicativo.

Gli utenti remoti, senza l'installazione e l'aggiornamento di alcun client, devono poter accedere in modo sicuro a tutte le applicazioni che supportano il protocollo IP (Internet Protocol), come se si trovassero all'interno della rete aziendale: devono essere supportati i protocolli TCP, UDP,

VoIP, ICMP e le applicazioni che utilizzano porte dinamiche, come l'FTP, mentre l'autenticazione deve poter avvenire tramite LDAP, X.509 Certificates, SecureID, Radius, Tacacs.
La soluzione deve garantire una elevata affidabilità, essere costituita da un'unica infrastruttura su cui sono installati sia i servizi di firewall sia quelli di clientless VPN e deve essere semplice da utilizzare: tutte le funzionalità di sicurezza perimetrale devono essere gestite attraverso un'unica console di management, che consenta di implementare sia le policy del firewall sia quelle relative alle VPN con gli utenti remoti.
Il fornitore dovrà fornire le caratteristiche relative al client e al gateway terminatori del tunnel. La parte client dovrà essere fornita almeno per le seguenti piattaforme: Windows-2000, Windows-XP, Windows Vista, Windows Seven, Linux (kernel 2.2 o superiore), Mac OSX.
Il sistema di sicurezza perimetrale proposto deve prevedere la fornitura di almeno 1.000 client VPN e la gestione di almeno 50 connessioni VPN SSL contemporanee.

3.12. Gestione della banda Internet

Il fornitore dovrà garantire un servizio di bandwidth management, gestibile centralmente, ridondato ed integrato sui moduli firewall. Si dovrà ottimizzare l'utilizzo della banda Internet in modo da garantire agli utenti, aziendali e remoti, la disponibilità di banda per le applicazioni maggiormente sensibili alla latenza (es. accesso ai servizi Terminal/Citrix, videoconferenza, ecc.).
La soluzione dovrà essere implementata in modo che il traffico di rete meno sensibile alla latenza, come e-mail, traffico Web, ecc. non interferisca con traffico più critico quale VPN, videoconferenza e VoiP, applicazioni pubblicate con servizi Terminal/Citrix.
La soluzione dovrà consentire la definizione, analogamente a quanto avviene per i moduli firewall, di politiche di controllo della banda basate su oggetti quali PC, le subnet o gruppi di essi, fornendo inoltre la possibilità di definire gli orari di validità delle stesse.
Deve essere infine prevista la possibilità di:

- limitare alcune tipologie di traffico a valori di banda da concordare in fase di analisi
- garantire ad alcune tipologie di traffico la quantità minima di banda necessaria per il loro corretto funzionamento.
- assegnare dinamicamente ad altro traffico la banda riservata ad alcuni servizi, quando questi non la utilizzino.

3.13. Gestione DMZ

Il fornitore dovrà garantire la gestione e manutenere l'area DMZ della rete del Committente, garantendo il funzionamento delle attuali apparecchiature e servizi installati. Il fornitore dovrà inoltre affiancare il personale del CED del Committente per la corretta configurazione di apparati e servizi dell'area DMZ.
Relativamente alla sede di Via Volta, il fornitore dovrà effettuare un'analisi dei servizi pubblici attualmente attivi, implementando, se del caso, una nuova DMZ. Tenuto conto delle caratteristiche tecniche delle applicazioni da pubblicare e dei requisiti di sicurezza necessari per la protezione dei dati, il fornitore dovrà eventualmente implementare anche un reverse proxy da attestare sulla DMZ della Sede di Via Volta.
Il fornitore dovrà altresì supportare il personale del CED del Committente nelle configurazioni di nuovi apparati e servizi.

3.14. Event & Log Monitoring Management

Il fornitore dovrà provvedere alla raccolta, verifica, correlazione, analisi e storicizzazione degli allarmi generati e delle informazioni raccolte nei file di log dalle piattaforme caratterizzanti la soluzione oggetto del presente bando. Il servizio dovrà permettere il monitoraggio del livello di sicurezza raggiunto all'interno dell'Ente ed avere le seguenti caratteristiche:

- Supporto alla sorveglianza ed alla gestione degli allarmi.
- offrire la possibilità di convogliare tutti gli eventi/allarmi generati dai firewall e dai sistemi IDS e IPS verso un unico punto di correlazione;

- offrire un'attività di monitoraggio proattivo, analisi e correlazione dei log generati dal firewall e dai sistemi IDS e IPS e relativi al traffico in transito tra le reti interne del Committente e le reti esterne (es. Internet), svolta H24x7, per la rilevazione di traffico potenzialmente anomalo: attraverso un'opportuna tecnologia di analisi, anche con la compartecipazione del Committente stesso, per mezzo di idonei strumenti per definire il traffico atteso, il sistema deve essere in grado di segnalare eventi non rilevati dai sistemi di sicurezza perimetrale come eventi anomali. In particolare, i sistemi di event management devono poter consentire di effettuare il monitoraggio e l'analisi del traffico interno al fine di rilevare in maniera proattiva problematiche e malfunzionamenti imputabili a errori di configurazione degli applicativi e dei sistemi operativi, presenza di comunicazioni generate da worm o virus, altro traffico che possa essere sintomo di problemi all'infrastruttura;
- raccogliere e correlare in real-time le informazioni raccolte e presentarle, a valle di una normalizzazione, tramite un'interfaccia grafica e/o mediante generazione di un report di sintesi secondo dei template definibili sulla base delle specifiche esigenze dipendenti dalle tecnologie degli elementi gestiti;
- configurare la notifica di eventi/allarmi a fronte del superamento di soglie prefissabili e/o al verificarsi di eventi critici che impattino sulla sicurezza dell'ambiente informatico del Committente;
- assegnare differenti priorità agli eventi/allarmi e fornire, per ogni notifica inviata al Committente, informazioni circa:
  - la sorgente dell'evento/allarme;
  - la tipologia dell'evento/allarme;
  - la descrizione dell'evento/allarme;
  - la severità dell'evento/allarme;
  - l'istante temporale in cui si è verificato l'evento/allarme;
  - gruppo di appartenenza dell'evento/allarme;
  - ulteriori informazioni descrittive dell'evento/allarme, della risorsa che lo ha generato e di eventuali azioni automatiche o predefinite eseguite o disponibili;
- offrire la possibilità di reinstradamento dei messaggi di allarme e degli eventi a sistemi esterni
- essere integrabile con:
  - sistemi di trouble ticketing;
  - tool di reporting;
  - prodotti di supporto alle attività di help desk.

Il Fornitore dovrà predisporre con cadenza semestrale un documento nel quale saranno riepilogate e commentate le seguenti informazioni:

- commento dei principali eventi rilevati dal firewall nel periodo;
- analisi dello stato del firewall nel periodo;
- descrizione delle principali attività sistemistiche svolte dal Fornitore presso la sede del Committente nel periodo;
- descrizione delle principali attività sistemistiche svolte dal Fornitore presso la propria sede nel periodo;
- descrizione degli interventi di Help Desk effettuati dal Fornitore nel periodo;
- descrizione delle modifiche di policy effettuate nel periodo;
- descrizione delle segnalazioni di eventi rilevate e notificate al Committente
- eventuali suggerimenti su modifiche e nuove implementazioni all'architettura ed alla configurazione del firewall, per accrescere ed ottimizzare l'efficacia del sistema di sicurezza perimetrale.

3.15. Network Address Translation Management

Il fornitore dovrà erogare un servizio di Network Address Translation (NAT) Management consistente nella progettazione, implementazione e gestione di regole di traduzione di indirizzi IP configurati all'interno dell'infrastruttura di rete dell'amministrazione. Il servizio proposto dovrà essere tale da consentire di:

- realizzare la configurazione del NAT in maniera indipendente dalle regole che gestiscono il traffico e dal database degli oggetti; in particolare, ciascuna regola di NAT deve poter contenere:
  - IP sorgente del pacchetto
  - IP sorgente traslato
  - IP destinazione del pacchetto
  - IP destinazione traslato
- nascondere i dettagli dell'indirizzamento utilizzato all'interno di una rete quando ci si connette da quella rete verso altre reti ritenute non fidate;
- convertire un pool di indirizzi IP utilizzati per la rete Intranet dell'amministrazione in un pool di indirizzi IP pubblici utilizzabili per l'accesso al SPC.

Dovrà articolare il servizio di NAT Management nelle seguenti fasi:

- analisi dei requisiti utente;
- analisi del piano di indirizzamento a cui vanno applicate le traduzioni di indirizzi;
- studio delle caratteristiche dei dispositivi che dovranno effettuare la traduzione degli indirizzi, limitatamente alle funzionalità a supporto del "natting";
- sintesi del piano di "natting";
- implementazione del piano di "natting", ove applicabile.

Il fornitore dovrà erogare il servizio di NAT Management assicurando le attività di progettazione, attivazione, manutenzione e gestione del piano di indirizzamento.

3.16. Controllo degli accessi alla rete Lan mediante il protocollo 802.1x

Il controllo degli accessi alla rete LAN, anche mediante il protocollo 802.1x, dovrà essere effettuato mediante uno o più apparati installati ed attivati almeno sulle sedi di Via Borgo Vico 148 e Via Volta, non dovrà richiedere l'installazione di alcun agent dedicato sui device da controllare (client, server, stampanti, access point, ecc.) e dovrà avere le seguenti funzionalità:

- consentire il controllo dell'accesso degli host alla rete permettendone l'isolamento e autenticando quelli abilitati tramite protocollo 802.1x;
- effettuare l'inventario degli host collegati alla rete e delle relative configurazioni hardware e software, servizi e processi attivi;
- fornire una rappresentazione dinamica ed automatica della topologia della rete e rilevare i dati relativi ai singoli switch.

La categorizzazione dei nuovi host rilevati dovrà avvenire in base ai seguenti criteri:

- esito dell'autenticazione mediante protocollo 802.1x;
- appartenenza dell'host ad opportuni gruppi Active Directory;
- appartenenza dell'utente ad opportuni gruppi Active Directory o a gruppi definiti localmente, scorrelati da Active Directory;
- accesso da punti rete specifici;
- accesso in determinati intervalli temporali;
- stato degli aggiornamenti di sistema e del software anti-virus;
- volume di traffico generato in precedenza dall'host;
- presenza sugli host di software non consentito.

Nel caso i criteri venissero soddisfatti, la soluzione proposta deve prevedere due tipologie di autorizzazione:

- accesso completo, che consentirà all'host di collegarsi a tempo indeterminato sulla rete o VLAN consentita in base alla sua categorizzazione;
- accesso per utenti temporanei, che consentirà all'host di collegarsi sulla rete o VLAN consentita in base alla sua categorizzazione, per un periodo di tempo predeterminato e previa autenticazione dell'utente.

Per ogni host che non soddisfi i criteri richiesti dovrà essere impedita qualsiasi forma di comunicazione con gli altri host facenti parte della rete cui questo si è collegato.
Sarà necessario poter spostare gli host, in base ai criteri soddisfatti, su diverse VLAN; sarà inoltre necessario che lo strumento di controllo accessi rilevi e blocchi preventivamente

qualsiasi host sconosciuto e che, a intervalli prestabiliti (configurabili dall'utente amministratore), effettui nuovamente l'autenticazione degli host.
La soluzione proposta dovrà tener traccia delle connessioni di nuovi host, dei cambi di indirizzi IP da parte di host già rilevati, delle associazioni di nuovi indirizzi IP ai vari host, della presenza di IP duplicati nella rete e delle variazioni dei servizi di rete attivi sui singoli host.
Per tutti gli eventi sopra elencati dovrà essere possibile fornire meccanismi di alerting, tramite e-mail o sms, oltre ad effettuare normale logging degli eventi stessi.
Dovrà essere fornita un'unica console di visualizzazione dei log generati dagli apparati installati presso le sedi del Committente.
Il sistema di logging dovrà anche registrare gli accessi (tramite autenticazione 802.1x o tramite le credenziali locali, in caso di utenti ospiti), i passaggi da online a offline (e vice versa) dei singoli host, il passaggio di un host dallo stato "accesso bloccato" a quello "accesso consentito" e i cambiamenti nel software installato sui singoli host. Deve essere inoltre previsto di spedire i suddetti log allo stesso sistema di raccolta log nel quale confluiscono quelli del firewall.
Per tutti gli host rilevati si dovranno raccogliere i dati relativi al software installato, al sistema operativo e alle caratteristiche hardware, analogamente, per ogni switch rilevato nella rete, dovranno essere forniti dati relativi allo stato delle porte e agli host che vi si collegano e si dovrà monitorare il traffico in ingresso e in uscita da ogni porta.
La gestione della soluzione proposta dovrà avere i seguenti requisiti:

- interfaccia web centralizzata per la gestione dei sistemi presenti in tutte le sedi del Committente;
- le policy definite per i singoli host rilevati da ciascun sistema potranno essere applicate a prescindere dalla LAN di accesso dell'host stesso, anche in sedi diverse;
- accesso protetto con autenticazione basata su più fattori (ad es., OTP) anche mobile;
- profili di accesso amministrativo diversi (amministrazione, visualizzazione, creazione utenti ospiti, ecc.);
- amministratori locali per la gestione degli accessi nelle singole sedi;
- amministratori globali per la gestione degli accessi di tutte le reti;
- interagire con il sistema di Active Directory per gestire gli utenti di dominio e poter effettuare ricerche nei log, anche in tempo reale;
- assegnazione automatica al gruppo Accesso Completo di tutte le macchine appartenenti al Dominio.

Dovrà essere possibile visualizzare gli inventari relativi ai singoli host, in modalità aggregata o riguardanti lo stato dei singoli host.
Tali dati dovranno essere visualizzati all'interno dell'interfaccia web e tramite esportazione in formato Excel o pdf.

3.17. Bilanciatore di connettività multiple

La soluzione proposta dovrà essere installata ed attivata sulla sede di via Borgo Vico 148 e dovrà essere in grado di:

- prevedere la distribuzione delle connessioni in uscita su diverse connettività tenendo conto della banda disponibile sulle stesse, della presenza o meno di guasti (fault tolerance) o seguendo delle politiche prefissate;
- gestire il traffico in ingresso proveniente da eventuali nuove connettività.

Il bilanciatore dovrà farsi carico del "connection tracking" ovvero, dovrà identificare le connessioni e i pacchetti relativi ad ogni singolo servizio gestito in modo da mantenere la coerenza nel routing di protocolli complessi come l'ftp, h.323, sip e similari, e dovrà inoltre, dove necessario, occuparsi del "NAT" delle connessioni stesse.
Onde evitare disservizi, la tecnologia proposta dovrà essere in grado di lavorare in modalità trasparente (bridge), almeno sulla connettività principale.
La configurazione del sistema e delle politiche prefissate dovrà essere gestibile attraverso un'interfaccia web adeguatamente protetta; le politiche di routing verso le varie connettività dovranno essere configurabili in base a tutti i campi che compongono le connessioni tcp/ip udp o icmp che attraversano il bilanciatore.

Inoltre, la soluzione proposta dovrà consentire l'applicazione anche di politiche di "Quality of service" al traffico prima che questo venga inoltrato alla connettività preselezionata.
L'interfaccia web dovrà consentire di visualizzare in tempo reale tutte le connessioni attive e le relative connettività utilizzate, in modo da avere una chiara visione, anche con l'ausilio di grafici, del corretto funzionamento dell'apparato stesso.

4. Gestione del servizio fornito

Sono richiesti i seguenti servizi di gestione dei sistemi descritti:

- Servizio di monitoring remoto delle componenti hardware e software;
- Servizio di monitoraggio proattivo e di correlazione degli eventi generati dai sistemi di sicurezza
- Servizio di notifica degli eventi rilevati che rappresentino delle effettive o potenziali anomalie, con verifica da parte del personale tecnico del fornitore per evitare quanto più possibile la segnalazione di falsi positivi
- Servizio di troubleshooting remoto;
- Servizio di change Management;
- Servizio di reporting sui servizi erogati.

L'erogazione dei servizi potrà avvenire da remoto; in tal caso il fornitore dovrà utilizzare una connessione di rete sicura e cifrata (Virtual Private Network) tra la propria sede e quella del Committente. Tale connessione sarà ad esclusivo onere del fornitore.
Per le caratteristiche tecniche dei servizi offerti, dovrà essere prodotto un documento completo illustrante nel dettaglio le modalità di erogazione per ognuno dei servizi offerti secondo il seguente schema:

- Descrizione del servizio;
- Copertura del servizio;
- Canali di comunicazione;
- Livelli di servizio (SLA).

4.1 Monitor remoto

Descrizione dei servizio

Il servizio ha l'obiettivo di monitorare il corretto funzionamento dei sistemi, dei servizi applicativi e della rete nell'ambito dei sistemi di sicurezza oggetto dei presente capitolato.
Il servizio deve prevedere le seguenti principali caratteristiche:

1. noleggio del prodotto software per il monitoraggio di apparati e servizi, del server necessario e del reltivo S.O.; tale sistema sarà attestato sulla LAN della sede di via Borgo Vico e si occuperà di raccogliere una serie di dati dai sistemi di sicurezza descritti nei paragrafi precedenti; il server potrà eventualmente essere un server virtualizzato messo a disposizione dal Committente (ciò dipenderà dal S.O. operativo richiesto);
2. possibilità per il personale tecnico del Committente di consultare via web le informazioni relative agli apparati monitorati, attraverso la visualizzazione di tutti i principali dati sull'utilizzo e sullo stato dei dispositivi monitorati, aggiornati ogni 30 secondi e presentati in forma grafica e tabellare;
3. 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;
4. backup delle configurazioni, sia in occasione della conclusione della prima installazione e successivamente ad ogni modifica sostanziale;
5. possibilità di implementare numerosi controlli (alcune centinaia) su apparati e servizi, quali, ad es., informazioni su utilizzo delle risorse (RAM, CPU, ecc.), traffico sulle interfacce, sovraccarichi, stato sei servizi, ecc.;

Il sistema deve inoltre prevedere le seguenti funzionalità:

- Network Discovery automatico
- Templates preconfigurati con un set raccomandato di sensori, per un numero vario di device
- Interfaccia altamente interattiva e customizzabile per una efficiente fruibilità

- Configurazione organizzata in modo gerarchico "ad albero"
- HTML-API che abilitano programmi esterni ad avere accesso alle informazioni del database del sistema di monitoraggio e di manipolare gli oggetti dello stesso database.
- La possibilità di utilizzare "Remote Probes" per provvedere ad un monitoraggio Multi-location e permettere di distribuire possibili sovraccarichi della CPU destinata al monitoraggio; le probe possono agire anche come semplici "packet sniffing" (ad es., deve essere possibile sganciare delle probe sulle sedi remote per analizzare il traffico fra sedi o il carico o il funzionamento di apparecchiature remote)
- Bandwith monitoring utilizzando SNMP, NetFlow e Packet Sniffing per una profonda analisi e a supporto di eventuali debugging
- Più tipi di sensori per un totale e completo monitoraggio si piccoli, medi e grandi network, ad es.:
  - SNMP (supports SNMP V1, V2c and V3)
  - WMI (Windows Management Instrumentation)
  - HTTP based services
  - Vari TCP e UDP based services come p.e.: PING, SMTP, POP3, FTP…
  - Sensori VMware per il monitoraggio di sistemi virtualizzati
  - SQL Servers
  - File Servers
  - Antivirus pattern monitor
  - Ecc.
- Vari triggers per ottenere l'alerting e la notifica via email, SMS, pager message, HTTP request;
- state-of-the-art, AJAX-based web interface, per la configurazione di device e sensori per una corretta gestione del monitoraggio
- web server integrato con supporto di SSL security, login multipli, user group
- Web Interface supportata da: Microsoft Internet Explorer, Firefox, Apple Safari e Google Chrome
- Funzionalità avanzate di "search"
- User Administation con "right management"
- Modalità diverse per pubblicare i dati, anche differenziate per i singoli utenti
- "Mappe" per il monitoraggio di informazioni aggregate, grafici e tabelle con layouts e sfondi customizzabili (es.: con la mappa del network)
- utenti con permission "read-only", abilitati e limitati su determinati gruppi di device o sensori
- messa in avidenza agli utenti delle segnalazioni generate dai sensori del sistema di monitoraggio tramite grafici e tabelle
- Integrazione su siti web esterni, con chiamate via HTTP.

I report di funzionamento devono:

- poter esser definiti per qualsiasi arco di tempo
- rilasciare complete informazioni su ogni sensore
- essere popolati da nuovi sensori e gruppi di sensori usando dei semplici tags
- essere facilmente customizzabili

Il controllo avverrà remotamente e le eventuali anomalie saranno segnalate secondo i Canali di comunicazione ed i Livelli di servizio descritti di seguito.

Copertura del servizio

La copertura del servizio sarà di sette giorni su sette, 24x24.

Canali di comunicazione

Le comunicazioni avverranno tramite: e-mail, telefono, sms, fax.

Livelli di servizio (SLA)

In caso di malfunzionamenti, la segnalazione dovrà essere effettuata entro *2 ore* dall'evento.

4.2. Monitor degli eventi rilevati

Il servizio di monitoraggio degli eventi rilevati dal sistema di monitoring, i cui requisiti sono descritti al paragrafo precedente, deve presentare le seguenti caratteristiche:

- nell'ambito dei sistemi di sicurezza oggetto dei presente capitolato, monitoraggio dei dispositivi e dei servizi erogati, verifica della raggiungibilità degli apparati, con l'evidenziazione dei tempi totali di effettivo utilizzo e di eventuale disservizio;
- generazione di alert a fronte del verificarsi di eventi definiti in fase di configurazione del servizio e possibilità di notificarli via mail anche al personale del Committente;
- monitoraggio proattivo dei dispositivi: gli apparati ed i servizi devono essere controllati remotamente dal personale tecnico del Fornitore che, in caso di guasto o malfunzionamento, deve intervenire tempestivamente da remoto per diagnosticare e segnalare il problema, notificandolo al cliente telefonicamente e/o via email;
- offrire la possibilità di reinstradamento dei messaggi di allarme e degli eventi a sistemi esterni
- essere integrabile con:
    - sistemi di trouble ticketing;
    - tool di reporting;
    - prodotti di supporto alle attività di help desk.

4.3. Troubleshooting

Descrizione del servizio

L'analisi e la relativa risoluzione delle diverse problematiche che si potrebbero presentare durante lo svolgimento del servizio di sicurezza in questione sono ovviamente un aspetto fondamentale della fornitura in oggetto.

Il servizio può derivare da una segnalazione del servizio di monitor remoto o da una richiesta diretta del Committente.

L'obiettivo deve essere quello di minimizzare i tempi di fermo, con l'utilizzo di processi standard per l'analisi e la gestione dei problemi e con l'uso di procedure idonee a tracciare e notificare i problemi riscontrati, al fine di garantire il rispetto dei livelli minimi di servizio. Il fornitore si impegna, senza oneri aggiuntivi per il Committente, a effettuare manutenzioni e aggiornamenti del sistema fornito nel caso in cui vengano modificate le infrastrutture in uso (server, apparati attivi, connettività, ecc.)

Copertura del servizio

La copertura del servizio sarà di sei giorni a settimana dal Lunedì a sabato dalle 08,00 alle 20,00.

Canali di comunicazione

Le comunicazioni avverranno tramite: e-mail, telefono, sms, fax.

Livelli di servizio (SLA)

I livelli di servizio richiesti per il servizio di troubleshooting sono:

- 60 minuti per la segnalazione del guasto se la segnalazione proviene dal sistema di monitor remoto;
- 2 ora 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 dei malfunzionamenti delle componenti software non dipendenti dal fornitore del servizio.

4.4. Change Management

Descrizione del servizio

Il servizio di Change Management copre qualsiasi necessità di modifica dei dati di configurazione e applicativi di un servizio nell'ambito di un sistema funzionante (ad es., creazione/modifica delle regole del firewall). Il servizio viene attivato solo su richiesta del Committente.

Il servizio richiesto deve prevedere anche la possibilità per il personale del Committente 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. Relativamente al servizio di

firewall, il servizio deve prevedere che per ciascuna modifica di configurazione, eventualmente realizzata autonomamente dal personale del Committente, il personale tecnico del fornitore provveda, in maniera proattiva, ad analizzare la coerenza della modifica apportata con la configurazione generale del sistema ed a inviare all'amministrazione una mail di notifica contenete un giudizio di conformità o meno.
Il servizio di Change Management deve prevedere una definizione granulare dei privilegi d'accesso ai sistemi da parte degli amministratori; ad es., devono poter essere create utenze per la sola visualizzazione dei log, altre utenze per la sola visualizzazione della configurazione, altre ancora per la sola modifica delle configurazioni, ecc.

Copertura del servizio

La copertura del servizio sarà di tipo *Business Time,* ossia di cinque giorni a settimana dal Lunedì a venerdì lavorativi dalle 08,00 alle 18,30.

Canali di comunicazione

Le comunicazioni avverranno tramite: e-mail, telefono, sms, fax.

Livelli di servizio (SLA)

I livelli di servizio richiesti per il servizio di change management sono: 1 ora per l'acquisizione della segnalazione della richiesta; 4 ore per la presa in carico e la realizzazione della modifica.

4.5. Reporting sui servizi erogati

Descrizione del servizio

Il servizio consiste nel rilascio di relazioni dettagliate sullo stato dei servizi erogati, sulle problematiche trattate e le relative soluzioni.

Copertura del servizio

l report verranno trasmessi al Committente con cadenza semestrale con possibilità di richiesta di report a seguito di eventi particolari.

Canali di comunicazione

I report verranno trasmessi via e-mail.

Livelli di servizio (SLA)

I report saranno trasmessi entro il bimestre successivo al periodo a cui il report si riferisce.

4.6. Manutenzione dei sistemi

4.6.1. Manutenzione correttiva

La manutenzione correttiva consiste sia nella riparazione dei guasti, blocco o altro inconveniente che dovesse verificarsi, sia 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 del sistema.
Il Fornitore sarà obbligato:

- in caso di malfunzionamento "bloccante" delle apparecchiature - intendendosi per malfunzionamento "bloccante" qualsiasi anomalia funzionale che provochi l'interruzione del servizio all'utenza -, ad intervenire entro 4 (quattro) ore lavorative dalla notifica del problema e a ripristinare, in loco, la piena funzionalità delle apparecchiature entro 8 (otto) ore lavorative dal ricevimento della notifica (a mezzo FAX o e-mail);
- in caso di malfunzionamento "non bloccante" delle apparecchiature - intendendosi per malfunzionamento "non bloccante" qualsiasi anomalia funzionale che provochi la non completa disponibilità del servizio all'utenza e, in ogni caso, ogni difformità del prodotto in esecuzione dalla relativa documentazione tecnica e manualistica d'uso -, ad intervenire entro 16 (sedici) ore lavorative dalla notifica del problema e a ripristinare, in loco, la piena funzionalità delle apparecchiature entro 24 (ventiquattro) ore lavorative dal ricevimento della notifica (a mezzo FAX o e-mail).

A tal proposito il Fornitore dovrà fornire un numero di telefono ed un indirizzo e-mail al quale indirizzare le richieste di assistenza.
Tale servizio dovrà essere garantito per tutta la durata del contratto, dalle 08:00 alle 20:00, esclusi domeniche e festivi.

A seguito del malfunzionamento e/o del fermo delle apparecchiature, qualora il ripristino della loro funzionalità non intervenga entro il termine precedentemente descritto, il Committente applicherà le penali disciplinate nel contratto, salvo in ogni caso il risarcimento al maggior danno. Le parti di ricambio - che dovranno essere identiche alle parti sostituite - verranno fornite dal Fornitore senza alcun onere aggiuntivo per l'Ente. Le parti sostituite verranno ritirate dal Fornitore stesso. La manutenzione dovrà essere estesa anche alle parti di ricambio.
Ove il ripristino del malfunzionamento e/o il fermo delle apparecchiature richieda tempi superiori a quelli precedentemente indicati ovvero comporti il trasferimento delle stesse in luogo diverso dai locali dell'Ente, il fornitore dovrà provvedere, a propria cura e spese e per l'intero periodo del ripristino, alla sostituzione delle apparecchiature stesse con altre aventi le medesime caratteristiche tecniche e funzionali, ferma restando l'applicazione delle penali disciplinate nel contratto, sino al momento della sostituzione delle apparecchiature. Per ogni intervento di manutenzione dovrà essere redatta da un incaricato dell'Ente ed uno del Fornitore un'apposita nota di ripristino, in formato cartaceo od elettronico, nella quale dovranno essere registrati l'ora della chiamata e quella dell'avvenuto ripristino, nonché le prestazioni effettuate.

4.6.2. Manutenzione preventiva

Il Fornitore si impegna a proporre e concordare con il Committente interventi (regolazioni, controlli, sostituzioni) finalizzati all'ottimizzazione ed l'aggiornamento della soluzione; tali interventi dovranno essere effettuati periodicamente al fine di consentire la perfetta funzionalità della soluzione e prevenirne i malfunzionamenti anche tramite servizi di assistenza tecnica preventivi miranti a ridurre i costi di gestione dei sistemi mediante l'eliminazione delle possibili fonti di problemi. Il Fornitore deve fornire update del software gratuiti e nel minor tempo possibile qualora fossero riscontrati dei bug software da parte del Committente.
il Fornitore deve inoltre verificare la disponibilità di aggiornamenti dei componenti software messi in produzione e - dopo aver informato l'Ente (all'indirizzo infoced@provincia.como.it) - installare tali aggiornamenti (minor e major release del software fornito) in maniera trasparente per il Committente. In caso di aggiornamenti che richiedano temporanee sospensioni dei servizi di sicurezza, l'installazione di tali aggiornamenti deve essere concordata con il CED del Committente e effettuata in modi e tempi che non richiedano l'interruzione dell'attività del Committente o che, comunque, riducano al minimo il disservizio.
Il servizio comprenderà altresì, a totale carico del Fornitore, l'effettuazione delle modifiche tecniche, consistenti nei miglioramenti e/o aggiornamenti (es. installazione patch o nuove release software), al fine di elevare il grado di affidabilità del sistema, di migliorare il funzionamento e di aumentare la sicurezza.
Sono inoltre compresi nella fornitura 15 giorni di servizi di personalizzazione e supporto specialistico, da fruire nell'arco di 30 mesi, per servizi quali:

- ottimizzazione delle configurazioni dei sistemi forniti;
- evoluzione dei prodotti installati e delle modalità di configurazione;
- test di funzionamento sistemistico e applicativo dei sistemi;
- miglioramento nel supporto delle tecnologie;

Il Fornitore deve fornire i seguenti canali per l'inoltro delle segnalazioni:

- email;
- telefono;
- sms
- fax.

Si richiede che le comunicazioni per finalità di manutenzione ordinaria possano essere effettuate da lunedì a venerdì, durante le ore lavorative (8.00 - 18.30).
Il servizio di manutenzione ordinaria deve poter essere erogato:

- attraverso assistenza telefonica;
- attraverso intervento on-site.

Per entrambi i tipi di manutenzione su indicati, l'Impresa dovrà utilizzare parti di ricambio di primaria qualità e nuove di fabbrica, ove esistenti prodotte dallo stesso costruttore del sottosistema.

4.7 Servizio di trouble ticketing

Per consentire all'Ente di monitorare il livello del servizio fornito e di controllare il rispetto degli SLA, nonché di analizzare le casistiche delle problematiche, si richiede che il fornitore adotti un sistema di trouble ticketing.
Per ogni richiesta, sia pervenuta dal Committente, sia generata dai sistemi di monitoring, deve essere aperto un ticket che dovrà essere numerato univocamente e progressivamente. All'apertura del ticket dovrà essere inviata una mail, contente tutte le informazioni relative all'apertura del ticket stesso ed il nominativo del tecnico che l'ha in carico, ad uno o più indirizzi mail che saranno comunicati dal Committente prima del collaudo. Al termine delle attività, dovrà essere inviata ai medesimi indirizzi una mail di chiusura del ticket con l'indicazione delle attività effettuate.

4.8. Altri servizi inclusi

L'Ente sta procedendo alla virtualizzazione della DMZ della sede di Via Borgo Vico 148.
Si intendono incluse nel servizio tutte le eventuali attività di riconfigurazione, modifica, ecc. che dovessero rendersi necessarie a seguito della realizzazione di tale progetto.

4.9. Centro Servizi Territoriale (CST) progetto SiscoTel

Il Committente si riserva di affidare, ai sensi dell'art. 57 comma 3 lett. B del D.Lgs. n. 163/06, un completamento di fornitura di servizi analoghi a quelli del presente capitolato per il costituendo Centro Servizi Territoriale (CST) del progetto SiscoTel. Il CST sarà realizzato nella sala server della sede di Via Borgo Vico 148.

5. Requisiti tecnici e professionali del Concorrente

Al fine di presentare offerta, il Concorrente dovrà dimostrare di disporre di un'adeguata struttura tecnica per fornire il servizio oggetto della gara, rispettando inoltre i seguenti requisiti:

- Iscrizione nel Registro delle Imprese della C.C.I.A.A. se l'impresa è italiana o straniera residente in Italia, ovvero nel corrispondente registro Professionale dello stato di appartenenza per le imprese non residenti in Italia (in caso di ATI, il suddetto requisito dovrà essere posseduto da tutte le imprese costituenti l'ATI);
- avere almeno 4 tecnici dipendenti in possesso di certificazioni sulla tecnologia firewall e almeno 2 tecnici dipendenti certificati su ciascuna delle altre tecnologie previste dal progetto (antivirus/antispam, url filtering); in caso le certificazioni fossero scadute da oltre 12 mesi, devono essere già in corso le procedure per il loro rinnovo;
- disporre di personale tecnico dipendente certificato sulle tecnologie VMware, Microsoft e Citrix;
- aver già installato e mantenuto, nel quinquennio antecedente la pubblicazione del bando, almeno 3 soluzioni con caratteristiche similari a quelle del presente bando;
- disporre di personale tecnico dipendente certificato sulle tecnologie utilizzate per l'erogazione dei servizi oggetto del bando che garantisca l'operatività 24 ore su 24 relativamente all'attività di monitoring remoto; il Concorrente dovrà produrre adeguata documentazione dalla quale risulti la regolarizzazione tra azienda e tecnici dell'attività sopra citata;
- disporre di un'infrastruttura di connettività gestita direttamente e multicarrier, totalmente ridondata;
- disporre di un'infrastruttura del Security Operation Center (SOC) attestata presso un data center di un primario operatore nazionale o internazionale;
- disporre di un'infrastruttura di disaster recovery attestata presso un secondo data center;
- che almeno uno dei due data center possa essere collegato alla rete MPLS in uso al Committente (il collegamento alla rete MPLS utilizzata dal Committente non è oggetto del presente bando);

6. Criteri di Valutazione

Le offerte verranno valutate secondo il criterio previsto dall'art. 83 del D.Lgs. n. 163/2006 e successive modificazioni ed integrazioni dell'offerta economicamente più vantaggiosa selezionata mediante l'assegnazione di un massimo di 40 punti per l'offerta economica e di un massimo di 60 punti per l'offerta tecnica, per un totale massimo di 100 punti.
La valutazione delle offerte tecniche sarà effettuata dalla commissione tecnica nominata dal Committente.

6.1 Punteggio offerta economica

All'offerta economica più bassa verranno assegnati 40 punti.
Alle altre offerte il punteggio verrà assegnato sulla base della seguente formula:

$$\frac{40 \times \text{offerta economica più bassa}}{\text{Prezzo offerta}}$$

6.2 Punteggio offerta tecnica

I 60 punti per l'offerta tecnica verranno così assegnati:

Qualità della documentazione prodotta — fino a 5 punti

Architettura tecnologica della soluzione proposta — fino a 10 punti
Così suddivisi:
- Utilizzo virtualizzazione (con particolare riferimento alla sua estensione) — fino a 5 punti
- Architettura ridondata (con particolare riferimento ai servizi Non in alta affidabilità) — fino a 5 punti

Soluzione tecnologica — fino a 20 punti
(verranno valutati gli elementi caratterizzanti l'offerta facendo riferimento a quanto previsto nei vari sottopunti dell'art. 3 del presente capitolato)

Piano di installazione, configurazione, rilascio e collaudo
(con particolare riferimento all'indicazione dei tempi di realizzazione, degli eventuali fermi e della loro estensione e durata) — fino a 10 punti

Gestione del servizio — fino a 10 punti
Così suddivisi:
- Monitor Remoto: migliorie rispetto alle coperture e agli SLA richiesti — fino a 1 punto
- Troubleshooting: migliorie rispetto alle coperture e agli SLA Richiesti — fino a 3 punti
- Change Management: migliorie rispetto alle coperture e agli SLA Richiesti — fino a 3 punti
- Manutenzione dei sistemi: migliorie rispetto alle coperture e agli SLA Richiesti — fino a 3 punti

Formazione
- Migliorie rispetto a quanto richiesto — fino a 5 punti

7. Modalità di presentazione dell'offerta tecnica

L'offerta tecnica dovrà essere costituita:

1) **Relazione tecnica**, composta al massimo da 25 pagine A4, con una numerazione progressiva ed univoca delle pagine, illustrante chiaramente il progetto presentato, che fornisca in particolare le seguenti informazioni:
   a) caratteristiche dettagliate della soluzione offerta e relative scelte tecnologiche;
   b) modalità di erogazione dei servizi;
   c) modalità di formazione degli operatori del CED;
   d) evetuali migliorie rispetto a quanto richiesto nel capitolato.
2) **Piano d'installazione della soluzione**, nel quale il Concorrente dovrà specificare i tempi di realizzazione e di messa in opera della soluzione. Il piano d'installazione dovrà specificare quali tempi di interruzione del servizio sono necessari al completamento dell'implementazione della soluzione stessa. Dovrà inoltre specificare ogni indicazioni necessaria al fine di determinare l'eventualità di possibili passi operativi da concordare con altri operatori (ad es., fornitore delle linee dati, fornitore del servizio di DNS) in modo da garantire il corretto rilascio delle soluzioni oggetto del presente capitolato. Poiché i servizi oggetto del bando sono a regime e rappresentano un alto grado di criticità, il Concorrente dovrà perciò presentare un piano che minimizzi le interruzioni di erogazione dei servizi, dichiarando la sua eventuale disponibilità ad operare in orari serali e/o festivi.
3) **Certificazioni e attestazioni**. Il Concorrente dovrà elencare e documentare tutte le certificazione tecniche richieste al precedente art. 5 del presente Capitolato.

Le relazioni dovranno essere redatte in lingua italiana ed essere sottoscritte in ogni loro pagina dalla persona o dalle persone abilitate ad impegnare legalmente la società concorrente. La relazione tecnica e ogni altra eventuale documentazione allegata, pena l'esclusione dell'offerta dalla gara, devono essere prive di qualsivoglia indicazione, riferimento, menzione (diretta o indiretta) delle condizioni economiche.
Tutta la documentazione dell'offerta tecnica dovrà essere fornitura anche su supporto informatico (CD).

8. Penalità

La mancata osservanza dei termini previsti al capitolo 4 una penale di € 100,00 (cento) per ogni ora di ritardo oltre i termini fissati.
Ove si verifichino inadempienze della ditta fornitrice nell'esecuzione delle prestazioni contrattuali, sarà applicata dall'Ente appaltante, in ragione della loro gravità, una penale rapportata all'importo delle prestazioni non eseguite o non esattamente eseguite, fino al massimo del 10% (dieci per cento) dell'importo contrattuale.
Nel caso di inadempienze gravi l'Ente stesso avrà facoltà di risolvere il contratto con tutte le conseguenze di legge e di capitolato che la risoluzione comporta, ivi compresa la facoltà di affidare la fornitura a terzi in danno dell'impresa.
In ognuna delle ipotesi sopra previste l'Ente non compenserà la fornitura non eseguita, salvo il diritto al risarcimento dei maggiori danni.

9. Cauzioni

9.1 Cauzione provvisoria

La cauzione provvisoria prestata a garanzia della valida partecipazione alla gara e della stipulazione del contratto è stabilita nella misura del 2% dell'importo a base d'asta e pertanto pari ad Euro 6.010,00 e potrà essere effettuata mediante versamento in contanti presso la Tesoreria Provinciale, ovvero tramite assegno circolare ovvero fideiussione bancaria o polizza assicurativa, rilasciata da impresa di assicurazioni debitamente autorizzata all'esercizio del ramo cauzioni.

Essa rimarrà vincolata fino alla stipulazione definitiva del contratto ed alla comunicazione di svincolo dell'Amministrazione Provinciale.
La fideiussione bancaria o la polizza assicurativa dovranno prevedere espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'esecuzione di cui all'art. 1957 comma 2) Codice Civile, nonché la sua operatività a semplice richiesta della stazione appaltante ed il versamento entro 15 giorni dalla richiesta.
La garanzia deve avere validità di 180 giorni dalla data di presentazione dell'offerta.
Ai sensi dell'art. 75 del D.Lgs. 163/2006 l'importo della garanzia prestata a titolo di cauzione provvisoria è ridotto del 50% per gli operatori economici ai quali venga rilasciata, da organismi accreditati, ai sensi delle norme europee della serie UNI CEI EN 45000 e della serie UNI CEI EN ISO/IEC 17000, la certificazione del sistema di qualità conforme alle norme europee della serie UNI CEI ISO 9000, ovvero la dichiarazione della presenza di elementi significativi e tra loro correlati di tale sistema. Per fruire di tale beneficio la ditta partecipante dovrà segnalare il possesso del requisito nelle forme previste dall'art. 75 comma 7) D.Lgs. 163/2006.
La fideiussione/polizza, nel caso di Associazione Temporanea di concorrenti, in particolare costituende, dovrà essere intestata segnatamente a tutte le imprese associate, partecipanti all'Associazione Temporanea a pena di esclusione dalla gara.
In ogni caso la cauzione provvisoria dovrà essere accompagnata da una dichiarazione – rilasciata da un fideiussore verso l'impresa concorrente – d'impegno a rilasciare la cauzione definitiva qualora l'offerente risultasse aggiudicatario – a pena di esclusione dalla gara –.

9.2 Cauzione definitiva

A garanzia degli obblighi assunti con l'appalto, la ditta appaltatrice dovrà prestare cauzione per un ammontare pari al 10% dell'importo netto contrattuale ai sensi dell'art. 113 D.Lgs. n. 163/06;
In caso di aggiudicazione con ribasso d'asta superiore al 10 per cento la garanzia fideiussoria è aumentata di tanti punti percentuali quanti sono quelli eccedenti il 10 per cento, ove il ribasso sia superiore al 20 per cento l'aumento è di due punti percentuali per ogni punto di ribasso superiore al 20 per cento.
Ai sensi dell'art. 75 del D.Lgs. 163/2006 l'importo della garanzia prestata a titolo di cauzione provvisoria è ridotto del 50% per gli operatori economici ai quali venga rilasciata, da organismi accreditati, ai sensi delle norme europee della serie UNI CEI EN 45000 e della serie UNI CEI EN ISO/IEC 17000, la certificazione del sistema di qualità conforme alle norme europee della serie UNI CEI ISO 9000, ovvero la dichiarazione della presenza di elementi significativi e tra loro correlati di tale sistema. Per fruire di tale beneficio la ditta partecipante dovrà segnalare il possesso del requisito nelle forme previste dall'art. 75 comma 7) D.Lgs. 163/2006.

10. Fatturazioni e pagamento

La fatturazione sarà trimestrale anticipata, pagamento a 30 (trenta) giorni e avrà inizio al dopo il collaudo, previa contestuale emissione delle relative fatture ed il saggio di interesse per ritardato pagamento sarà pari a quello fissato dall'art. 1284 C.C. e tale pagamento verrà effettuato a mezzo mandato diretto intestato all'impresa.
L'impresa è tenuta a notificare tempestivamente le variazioni che si verificassero nelle modalità di pagamento, in difetto di tale notificazione e anche se la variazione fosse pubblicata nei modi di legge, l'Amministrazione è esonerata da ogni responsabilità per i pagamenti eseguiti.

10.1. Sospensione dei Pagamenti

La Provincia di Como, al fine di garantirsi in modo efficace sulla puntuale osservanza delle clausole contrattuali, può sospendere, ferma l'applicazione delle eventuali penalità, il pagamento all'impresa cui sono state contestate inadempienze nell'esecuzione della fornitura.

10.2. Spese

Tutte le spese inerenti e conseguenti alla stipulazione del contratto, ivi comprese quelle fiscali, sono a carico del Fornitore.

11. Ulteriori Precisazioni

Tutte le norme e i termini indicati nel capitolato devono ritenersi essenziali e vincolanti, ove non espressamente specificato diversamente, ai fini dell'appalto; tuttavia le precisazioni tecniche contenute nel capitolato hanno carattere minimale, indicativo e non limitativo, poiché l'appaltatore si obbliga a fornire tutto quanto necessario per rendere la soluzione completa, efficiente, installata a regola d'arte e perfettamente funzionante.
L'appaltatore assume l'obbligo di agire in modo che il personale dipendente, incaricato di effettuare le prestazioni contrattuali, mantenga riservati i dati e le informazioni di cui venga in possesso, non li divulghi e non ne faccia oggetto di sfruttamento, rispettando rigorosamente le direttive della legge 196/2003 e successive modifiche ed integrazioni.
L'obbligo di cui al precedente comma non concerne i dati che siano o divengano di pubblico dominio o che già siano in possesso dell'impresa fornitrice, nonché, salva diversa indicazione in contratto, i concetti, le idee, le metodologie e le esperienze tecniche che vengono portati a sua conoscenza nel corso del contratto, o in esecuzione delle prestazioni contrattuali.
La stazione appaltante assume, altresì, l'obbligo di mantenere riservate le informazioni tecniche portate a sua conoscenza dall'impresa fornitrice, nello svolgimento del rapporto contrattuale, come informazioni riservate.
La Provincia si riserva la facoltà di richiedere la consegna della fornitura, con le riserve di legge, nelle more della formalizzazione del contratto.
La Provincia si riserva la facoltà di affidare a terzi la valutazione tecnica e/o la validazione dei prodotti e servizi forniti.

12. Problematiche e contenziosi (Dlvo163/2006)

Per quanto non previsto dal presente capitolato a completamento delle disposizioni in esso contenute, si applicano le norme di legge e di regolamento vigenti in materia.
In caso di controversie di qualsiasi natura, la competenza, in via esclusiva, spetterà al foro di COMO.