# Modello Offerta Tecnica – Lotto 1 Border Firewall

**Procedura aperta sopra soglia comunitaria con il criterio dell’offerta economicamente più vantaggiosa sulla base del miglior rapporto qualità/prezzo per l’affidamento di un contratto di fornitura di una infrastruttura di networking. CIG 8296137CD1**

 **DICHIARAZIONE DI OFFERTA TECNICA AI SENSI DEL DISCIPLINARE DI GARA n. 7759770**

Il/la sottoscritto/a ................................................................................................................................................

nato/a il ............................................ a..........................................................................(prov)............................

residente a ........................................................................................................................(prov).........................

nella sua qualità di …………………………………………………………………………..…..……………..

**dell’impresa/società/altro soggetto** …………………………………………………………………….………. con sede legale in………….....................…………………via ……………….………………………………………………..

codice fiscale………………………….…………p..i…………….………………………….………………….

**DICHIARA**

* di aver preso visione degli atti di gara per l’affidamento in oggetto e di essere perfettamente a conoscenza dei loro contenuti, che costituiscono legge speciale della presente procedura, di averli compresi e di accettarli integralmente ed incondizionatamente;
* Che l’offerta ha validità non inferiore a 180 (centoottanta) giorni solari dal termine ultimo per il ricevimento delle offerte

**INFORMAZIONI**

La tabella n. 1 indica i requisiti minimi relativi ai prodotti richiesti e va compilata obbligatoriamente in tutte le sue parti.

La tabella n. 2 indica gli aspetti migliorativi oggetto di valutazione, rispetto ai criteri di valutazione del disciplinare di gara. L’operatore andrà a compilare interamente ogni riga, rispetto a quanto offerto.

È richiesto di allegare tutta la documentazione tecnica necessaria alla verifica della presenza e conformità del requisito tecnico o prestazionale che l’operatore economico intende offrire, indicando puntualmente il riferimento nella documentazione fornita (ad esempio nome del documento allegato, pagina, paragrafo); laddove la documentazione risultasse non presente o non chiaramente dettagliata, il requisito tecnico o prestazionale sarà considerato mancante. Si raccomanda la compilazione ordinata e puntuale.

|  |  |
| --- | --- |
| Tabella n. 1 Lotto 1 Border FirewallRequisiti minimi richiesti | Indicare in modo puntuale la documentazione tecnica di riferimento allegata sia cartacea che digitale (es. nome allegato, pagina, paragrafo ecc.. ecc..) utile alla verifica della presenza del requisito tecnico o prestazionale che l’operatore economico intende offrire (non sono ammessi link a URL). |
| * N. 2 Next-Generation Firewall in configurazione H.A. Active/Active, con le seguenti caratteristiche tecniche minime, riferite al singolo apparato:
 |  |
| * + L’appliance fornita deve essere sviluppata su hardware fisico dedicato alla soluzione (firewall hardware).
 |  |
| * + Funzionalità integrate di controllo applicativo L7 ISO/OSI. Le policy di sicurezza da implementare dovranno essere di tipo applicativo.
 |  |
| * + Architettura del Firewall basata sulla separazione tra Data plane dedicato al traffico e Management plane dedicato alla gestione della piattaforma.
 |  |
| * + Firewall Throughput 17/20 Gbps (http/app)[[1]](#footnote-1).
 |  |
| * + Threat Prevention Throughput 8/9 Gbps (http/app)[[2]](#footnote-2).
 |  |
| * + IPsec VPN Throughput 8 Gbps.
 |  |
| * + Funzionalità di SSL remote access VPN per almeno 500 utenti.
 |  |
| * + Sessioni massime 4.000.000.
 |  |
| * + Nuove sessioni per secondo 150.000.
 |  |
| * + 10 Virtual Systems: Funzionalità di creazione di instanze separate logicamente del firewall, con separazione del traffico tra le diverse istanze.
 |  |
| * + Funzionalità di segmentazione della rete basata su Zone e protezione delle zone.
 |  |
| * + Interfacce configurabili in modalità L2, L3 IPv4 e IPv6.Le 3 modalità possono essere configurate contemporaneamente, su interfacce distinte, all'interno dello stesso contesto virtuale.
 |  |
| * + Supporto ai protocolli di routing OSPFv2/3 (graceful restart mechanism), BGP (graceful restart mechanism), RIP e rotte statiche.
 |  |
| * + PPPoE e DHCP.
 |  |
| * + Multicat PIM-SM, PIM-SSM, IGMPv3.
 |  |
| * + Bidirectional Forwarding Detection (BFD).
 |  |
| * + IPv6 SLACC.
 |  |
| * + 4096 802.1Q VLAN tags per device/interfacce.
 |  |
| * + Funzionalità di QoS con traffic shaping basato su policy (priority, guaranteed, maximum) per applicazioni, per utenti, per tunnel, con classificazione DSCP.
 |  |
| * + 802.3ad LACP.
 |  |
| * + NAT (IPv4): static IP, dynamic IP, dynamic IP/port.
 |  |
| * + NAT64, NPTv6.
 |  |
| * + High Availability active/active e active/passive; Failure detection basata su path monitoring e interface monitoring.
 |  |
| * + Funzionalità di DoS protection per contrastare il flooding dovuto a nuove sessioni.
 |  |
| * + Antivirus, anti-spyware (command-and-control), and vulnerability protection.
 |  |
| * + Funzionalità di IDS/IPS;
 |  |
| * + Funzionalità di DoS protection per contrastare il flooding dovuto a nuove sessioni.
 |  |
| * + Export dei flussi di dati (Netflow, Sflow e/o IPFIX).
 |  |
| * + Disponibilità di una dashboard (Application Command Center) che mostri come sommario grafico e interattivo applicazioni, utenti, URL, minacce e contenuti che attraversano la rete.
 |  |
| * + Funzionalità di amministrazione completa delle funzionalità del firewall, tramite una interfaccia locale (integrata nel firewall) e tramite una console di management centralizzato.
 |  |
| * + Eventuali soluzioni/funzionalità cloud based dovranno essere qualificate da AGID per il cloud della pubblica amministrazione.
 |  |
| * + Occupazione di spazio massimo di 2 x 3 RU 19”.
 |  |
| * + Alimentatori ridondati.
 |  |
| * + N. 4 100/1000/10G Cu RJ45; N. 16 1G/10G SFP/SFP+; N. 4 40G QSFP+.
 |  |
| * N. 2 (N. 4 in totale per la coppia di FW) transceiver ottici QSFP+ 40Gb SR4 100m OM3, 12 strand MPO.
 |  |
| * Servizi di aggiornamento software (inteso per tutte le funzionalità e software richiesti e forniti, soggetti a licenze) – 24 mesi.
 |  |
| * Servizio di Manutenzione e Hardware Replacement 8x5xNBD – 24 mesi.
 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Tabella n. 2 Lotto 1 Border FirewallAspetti migliorativi | Punteggio previsto in caso di offerta | Indicare con una X i requisiti tecnici o prestazionali che l’operatore economico intende offrire | Indicare in modo puntuale la documentazione tecnica di riferimento allegata sia cartacea che digitale (es. nome allegato, pagina, paragrafo ecc.. ecc..) utile alla verifica della presenza del requisito tecnico o prestazionale che l’operatore economico intende offrire (non sono ammessi link a URL). |
| Giornata di formazione (6 ore/giornata) aggiuntiva, rispetto al minimo richiesto nel capitolato tecnico - 0,25 punti/giornata | 1 max |  |  |
| La soluzione proposta ha la completa separazione fisica e hardware tra le componenti "Data Plane" dedicate al traffico e le componenti "Control Plane" dedicate alla gestione | 2 |  |  |
| La soluzione proposta permette di configurare contemporaneamente e tutte le interfacce fisiche in modalità “trasparente” (da non confondere/assimilare alla modalità L2). In questa modalità il firewall si comporta come un elemento di Livello 1 ISO/OSI inoltrando le PDU dei vari protocolli di Livello 2, come le BPDU dello Spanning Tree o le PDU dell'LACP. L'implementazione della seguente modalità “trasparente” prevede che il firewall sia installato in modo trasparente su un segmento di rete, attraverso il binding di due interfacce del firewall insieme. La modalità “trasparente” connette logicamente le due interfacce, essendo interna al firewall e crea una topologia di rete che non prevede alcun routing o switching per le due interfacce collegate | 5 |  |  |
| La soluzione proposta integra nativamente una tecnologia di Single Pass Parallel Processing, in base alla quale le analisi dei pacchetti per il riconoscimento dell'applicazione, dell'utente e del contenuto applicativo avvengono contemporaneamente. La modalità di Single Pass Parallel Processing (SP3) fornisce maggiori performance rispetto ad approcci di tipo UTM: il pacchetto di rete viene esaminato in un singolo passaggio, riducendo molte funzioni ridondanti e l’overhead derivante da tali funzioni.Non è previsto l’utilizzo di engine e set di signature separati né di proxy che richiedono il download dei contenuti prima di effettuare l’analisi | 8 |  |  |
| La soluzione proposta integra nativamente un motore di SSL Decryption Broker: SSL Decryption è la capacità di vedere internamente il traffic SSL non appena attraversa il firewall. Il firewall inoltra il traffico decriptato alla security chain, per poi criptarlo quando lo riceve indietro dall'ultimo elemento della security chain. In questo modo si evita di effettuare decryption/encryption ad ogni passo. Tale funzionalità non deve essere limitata al solo traffico HTTPS, ma estese anche ad applicazioni come FTPS e SSH. Grazie a queste funzionalità, se i dati sono originati dall’interno della rete, è possibile trovare applicazioni e minacce nascoste nel traffico cifrato | 3 |  |  |
| La soluzione proposta integra nativamente funzionalità di DNS Security, per la protezione del traffico DNS. Le funzionalità di DNS Security applicano predictive analytics, machine learning ed automazione per bloccare gli attacchi che utilizzano il DNS. E’ possibile bloccare e prevenire l’utilizzo di domini malevoli, neutralizzare le minacce nascoste nel DNS tunneling ed identificare macchine compromesse che cercano di contattare domini legati a infrastrutture di Command & Control | 2 |  |  |
| La soluzione proposta integra nativamente funzionalità di User-ID, per la definizione di security policy basate su utenti e gruppi di utenti | 3 |  |  |
| La soluzione proposta integra nativamente funzionalità di ottimizzazione delle security policy (Policy Optimizer) per adeguare le policy attuali ai requisiti di controllo applicativo | 4 |  |  |
| Funzionalità di QoS con traffic shaping basato su policy (priority, guaranteed, maximum) per applicazioni, per utenti, per tunnel, con classificazione DSCP | 2 |  |  |
| La soluzione proposta implementa nativamente il concetto di Zero Trust a livello di configurazione di base. Zero Trust è una iniziativa strategica il cui obiettivo è la prevenzione di data breach attraverso l’eliminazione del concetto di trust per l’architettura di rete interna. Si basa sul principio “never trust, always verify,” a partire dalla configurazione di default | 4 |  |  |
| La soluzione proposta integra nativamente l'applicazione di best practice secondo IronSkillet (day one configuration template) e strumenti open-source disponibili nel repository Github del fornitore | 2 |  |  |
| La soluzione proposta si integra nativamente con strumenti di Threat Intelligence aggregation open-source per la creazione di External Dynamic List | 5 |  |  |
| La soluzione proposta si integra nativamente con strumenti di Threat Intelligence in Cloud qualificata da Agid, per la condivisione e la ricerca di indicatori di compromissione. Tale soluzione e la relativa licenza dovrà essere offerta e funzionante per minimo 24 mesi (36 in caso di estensione della garanzia), a partire dalla data di esito positivo del collaudo | 6 |  |  |
| La soluzione proposta si integra nativamente con strumenti di Malware Analysis in Cloud qualificati da Agid | 4 |  |  |
| La soluzione proposta ha nativamente la disponibilità di Open API per la gestione e la personalizzazione della configurazione | 2 |  |  |
| La soluzione proposta si integra nativamente con ambienti di virtualizzazione VMware NSX | 1 |  |  |
| Console di management centralizzato dei firewall che non richieda utilizzo l'istallazione/esecuzione di client e compatibile con il protocollo HTML5 | 1 |  |  |
| La soluzione proposta permette di esportare la configurazione dei firewall in funzione presso il CNR-IMAA (Paloalto Newtorks PA-3020) ed importarle direttamente senza la necessità di modifiche e/o interventi manuali, sui nuovi firewall forniti (escluse le configurazioni necessarie per l'H.A.). Tale funzionalità dovrà essere possibile sia tramite le interfacce di management integrate negli apparati, sia tramite la piattaforma di gestione centralizzata. L'operazione dovrà essere reversibile anche dalla nuova alla precedente soluzione, in caso di fault dei nuovi sistemi | 15 |  |  |
| La Console di management centralizzato è in gradi di gestire completamente (es. aggiornamento OS, modifiche complete alla configurazione, backup configurazioni) i firewall in funzione presso il CNR-IMAA (Paloalto Newtorks PA-3020 e PA-200) | 6 |  |  |
| Estensione della garanzia di ulteriori 12 mesi (36 mesi in totale), comprensiva dell’assistenza tecnica e manutenzione sia per le componenti hardware che software, rispetto al minimo richiesto nel capitolato tecnico (24 mesi). L’estensione dell’assistenza tecnica e manutenzione dovrà essere erogata direttamente dal costruttore/produttore della soluzione offerta e verificabile in sede di collaudo, ad eccezione dei componenti per i quali non è richiesto il vincolo di unicità del produttore | 4 |  |  |
|  | Totale 80 |  |  |

…………………………………., …..……………………..

[Luogo] [Data]

……………………………………

[Firma]

1. Il throughput del firewall è misurato con le funzionalità di controllo applicativo e logging abilitate (64 KB HTTP)  [↑](#footnote-ref-1)
2. Il Threat Prevention Throughput è misurato con controllo applicativo, IDS/IPS, antivirus, anti-spyware, sandbox, file blocking, e logging abilitati (64 KB HTTP) [↑](#footnote-ref-2)