**ALLEGATO 16**

**MODELLO DI DICHIARAZIONE TECNICA**

**GARA A PROCEDURA APERTA PER L’AFFIDAMENTO DI UN ACCORDO QUADRO AVENTE AD OGGETTO LA FORNITURA DI SERVIZI DI CONNETTIVITA’ DELLA RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE (S-RIPA)**

**LOTTO UNICO**

**ID SIGEF 2834**

CLASSIFICAZIONE CONSIP: AMBITO PUBBLICO

Sommario

[Premessa e istruzioni per la compilazione 3](#_Toc222486681)

[SEZIONE 1 – Servizio di Next Generation Firewall – Prodotto/i Offerto/i 4](#_Toc222486682)

[SEZIONE 2 – Fac-simile Dichiarazioni dei requisiti minimi e/o migliorativi offerti 4](#_Toc222486683)

**Premessa e istruzioni per la compilazione**

Il presente documento è così suddiviso:

1. **SEZIONE 1:** riporta il dettaglio del/dei prodotto/i offerto/i dal concorrente, per il Next Generation Firewall, con le informazioni circa la marca, il modello e il codice identificativo univoco.
2. **SEZIONE 2:** riporta i fac-simile relativi alle dichiarazioni dei requisiti minimi e/o migliorativi offerti.

Il Concorrente deve produrre, contestualmente al presente documento, idonea “Documentazione di Comprova”, di cui al par. 3.1 del Capitolato Tecnico, atta a verificare, così come indicato al par. 21 del Capitolato d’oneri, per ciascun requisito minimo e/o migliorativo dichiarato, il possesso dello stesso. A tale scopo è richiesto che le tabelle 2 e 3 della sezione 2 vengano compilate inserendo il nome del documento e il puntamento nel quale rinvenire il possesso del requisito specifico.

**SEZIONE 1 – Servizio di Next Generation Firewall – Prodotto/i Offerto/i**

Nella seguente tabella sono riportate le informazioni richieste per il prodotto/i offerto/i. Laddove per una stessa fascia fossero offerti più prodotti (ad esempio, marca diversa oppure marca identica ma modelli diversi) si chiede di compilare un’apposita riga per ciascuno di essi.

|  |  |  |  |
| --- | --- | --- | --- |
| Servizio | Marca | Modello | Codice identificativo univoco |
| **NGFW – Fascia 1** |  |  |  |
| **NGFW – Fascia 2** |  |  |  |
| **NGFW – Fascia 3** |  |  |  |

Tabella 1 - Servizio di Next Generation Firewall – Prodotto/i Offerto/i

**SEZIONE 2 – Fac-simile Dichiarazioni dei requisiti minimi e/o migliorativi offerti**

Nelle seguenti tabelle sono riportati i requisiti minimi e migliorativi del servizio NGFW. Nel caso in cui, per le singole Fasce del NGFW, venga offerto un prodotto differente, le seguenti dichiarazioni sono da estendersi e ripetersi per ciascun prodotto di ciascuna Fascia.

**Dichiarazione per i requisiti funzionali minimi**:

| Requisiti Funzionali Minimi | |
| --- | --- |
| NGFW - Fascia *<indicare la/le fascia/e a cui la dichiarazione si riferisce>* | |
| Throughput della Fascia | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità di network firewall (stateful inspection, policy enforcement, packet filtering, DNAT e SNAT, VPN IPSEC client to site e site to site, VPN TLS) | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Meccanismi di Intrusion Prevention System (IPS) avanzato, dotati di funzionalità di rilevamento, blocco e tracciamento delle minacce informatiche, attraverso l'adozione di meccanismi di ispezione dei malware basati su firme, rilevamento di anomalie (inclusa l'individuazione di anomalie nei protocolli di rete IP), analisi euristica e comportamentale, con la possibilità di definire firme personalizzate per contrastare attacchi non ancora censiti. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| WEB/URL Filtering statico e dinamico, con possibilità di controllare le statistiche sulla navigazione, di bloccare l'accesso a particolari siti e creare anche categorie personalizzate. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità anti-malware, sia su base firma che su base comportamentale. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità di anti-spam. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità di anti-botnet. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità di sandboxing integrata o su infrastruttura remota del Produttore, ubicata in UE. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Deep packet inspection per scansionare l'intero payload dei pacchetti. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| TLS/SSL inspection per l’ispezione del traffico cifrato. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| SSH inspection. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Controllo delle applicazioni con blocco dell’esecuzione in funzione della configurazione impostata dall’Amministratore di Sistema. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| QoS band-width management con la possibilità di impostare una larghezza di banda minima garantita e un limite massimo di larghezza di banda per il traffico insieme ad un valore di priorità. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Trasmissione di eventi e log al SIEM o XDR afferente al servizio trasversale SOC o ad altro strumento di raccolta log, ove disponibile, dell’Amministrazione. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Funzionalità di accesso selettivo alle applicazioni con modello Zero Trust basata su identificazione dei dispositivi client e autenticazione degli utenti. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Analisi del traffico su base geolocalizzazione degli IP e possibilità di filtraggio/blocco. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |
| Capacità di gestione del traffico dati da più reti LAN, fisiche e/o virtuali (VLAN) della sede dell’Amministrazione. | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* |

Tabella 2 - Requisiti Funzionali Minimi NGFW

**Dichiarazione per i requisiti funzionali migliorativi**

|  | Requisiti Funzionali Migliorativi | | |
| --- | --- | --- | --- |
| N° Criterio | NGFW - Fascia *<indicare la/le fascia/e a cui la dichiarazione si riferisce>* | | |
| n° 18 | Possibilità di importare/esportare feed IOC proprietari o di terze parti qualificate, quali MISP ACN e CERT-AgID, tramite protocolli standard (STIX/TAXII). | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 19 | Funzionalità di DNS Filter (filtraggio su base categorizzazione dei domini e reputazione) per proteggere i client dall’accesso a domini compromessi. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 20 | Disponibilità di usufruire di un database dinamico di mappatura IP/porta/protocollo dei servizi cloud, aggiornato direttamente dal vendor, che può essere utilizzato sia in ambito policy che in ambito routing. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 21 | **Interconnessione con Public Cloud e gestione di ambienti ibridi**  Supportare **almeno tre** tra le seguenti tecnologie: AWS, Azure, Oracle, Google. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 22 | **Integrazione con ambienti SDN**  Supportare **almeno due** tra le seguenti tecnologie: Open stack, Cisco ACI, vmware NSX/ESXi, Kubernetes. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 23 | Funzionalità di gestione della sicurezza per i dispositivi IOT, garantendo almeno la scansione dei dispositivi, il controllo delle vulnerabilità e malware e l’aggiornamento delle policy di sicurezza. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 24 | Funzionalità di DNS Proxy. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |
| n° 25 | Possibilità di integrazione con soluzioni di terze parti, anche non previste nativamente, attraverso utilizzo di protocolli standard e/o API documentate. | *SI / NO* | *<inserire il nome del documento allegato e il puntamento nel quale rinvenire il possesso del requisito>* | |

Tabella 3 - Requisiti Funzionali Migliorativi NGFW

Firma

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(firmato digitalmente)