PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT

LOTTO 2

PROVINCIA DI BRESCIA

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	06/03/2024
2.0	Seconda emissione	27/03/2024

Indice

1. INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt per la Pubblica Amministrazione PROVINCIA DI BRESCIA, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: PIANO+DEI+FABBISOGNI+Provincia di Brescia-v1.00.pdf).

La Provincia di Brescia da un po' di tempo ha iniziato un percorso di miglioramento in ambito cybersecurity e di messa in sicurezza delle proprie infrastrutture. In questo contesto necessita di installare un sistema Next Generation Firewall (NGFW) per il controllo dell'infrastruttura aziendale con apparati che consentano l'ispezione dei pacchetti di rete a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware, capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione e l'attivazione di policies di navigazione web con logiche basate sulle utenze di gruppo integrate con l'Active Directory di Microsoft. I nuovi NGFW verranno utilizzati con il fine di garantire una migliore sicurezza informatica interna (c.d. back-end) e per segmentare meglio l'infrastruttura di rete creando opportuni "isolamenti". Si richiede altresì un supporto specialistico di Personale specializzato in ambito cyber security con l'obiettivo di supportare codesto Ente in varie attività inerenti sia la fornitura sia, in maniera più generale, la propria infrastruttura di sicurezza informatica per le seguenti attività: la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire una migliore sicurezza complessiva; l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare per garantire una migliore sicurezza complessiva; il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica.
Le tempistiche previste per l'attivazione del progetto (fase di collaudo) sono il 31.12.2024 e si prevede una durata contrattuale di 24 mesi.

1.2 SCOPO

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni - PIANO+DEI+FABBISOGNI+Provincia di Brescia-v1.00
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale

Identificativo
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

1.4 ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa

2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- ✓ **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

  Nome Cognome: Massimiliano Materazzi
  e-mail: massimiliano.materazzi@telecomitalia.it

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

- ✓ **Responsabile del Fornitore**

  De Girolamo Angelina
  Tel. ***+393357533522***
  e-mail: ***angelina.degirolamo@telecomitalia.it***

  Flavia Finamore
  *Tel.:****+39335750880***
  e-mail: ***Flavia.finamore@maticmind.it***

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo

- ✓ **Referente Tecnico per l'erogazione dei servizi**

  Nome Cognome: Carlo Omini
  e-mail: carlo.omini@telecomitalia.it

Renato Barbero
*telefono/cellulare:**3358068530***
*e-mail:**renato.barbero@maticmind.it***

che dovranno garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

2.1 CATEGORIZZAZIONE DEGLI INTERVENTI

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

Ambito (layer)	Obiettivi Piano Triennale
□ Servizi	□ Servizi al cittadino
	□ Servizi a imprese e professionisti
	x Servizi interni alla propria PA
	□ Servizi verso altre PA
□ Dati	□ Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	□ Aumentare la qualità dei dati e dei metadati
	□ Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
□ Piattaforme	□ Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	□ Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	□ Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
□ Infrastrutture	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	□ Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
□ Interoperabilità	□ Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	□ Adottare API conformi al Modello di Interoperabilità
□ Sicurezza Informatica	□ Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA

	□ Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3. PROGETTO DI ATTUAZIONE

Il progetto di attuazione prevede la fornitura di quanto indicato nella tabella seguente, in cui viene indicato l'importo contrattuale complessivo; in ciascuna voce oggetto di quotazione economica si indicano il dettaglio dei prodotti e dei servizi oggetto del contratto esecutivo, anche in base alle indicazioni riportate nei rispettivi paragrafi relativi ai prodotti e ai servizi previsti.

CODICE IN CONVENZIONE

Si allega nota di CONSIP in cui, in data 05/03/2024 è stato effettuato un cambio del codice (e del relativo prodotto) in convenzione utilizzato nel presente documento.

acquistinretepa

Cybersecurity – prodotti e servizi connessi 2 – ID 2367
Tutti i lotti

*ultimo aggiornamento al 05_03_2024

Next Generation Firewall (NGFW)

Marca	Fascia 1		Fascia 2		Fascia 3		Fascia 4		Fascia 5		Fascia 6	
	Modello	Codice articolo produttore	Modello	Codice articolo produttore	Modello	Codice articolo produttore	Modello	Codice articolo produttore	Modello	Codice articolo produttore	Modello	Codice articolo produttore
Fortinet	FGT-60F	FG-60F-BDL-C (include 1xFG-60F-BDL-950-12 + 1xFMG-VM-10-UG + 1xFC- 10-0060F-950-02-12+ 2xFC1-10-M3004-248-02- 12)	FGT-200F	FG-200F-BDL-C (include 1xFG-200F- BDL-950-12 + 1xFMG-VM-10-UG + 1xFC-10- F200F-950-02-12 + 2xFC1-10-M3004-248- 02-12)	FGT-400F	FG-400F-BDL-C (include 1x FG-400F-BDL-950-12 + 1xFMG-VM-10-UG + 1x FC-10-0400F-950-02-12 +2xFC1-10-M3004-248-02-12)	FGT-1100E	FG-1100E-BDL-C (include 1xFG-1100E- BDL-950-12 + 1xFMG- VM-10-UG + 1xFC-10-FI 1HE-950-02-12 + 2xFC1-10-M3004-248- 02-12)	FGT-2600F	FG-2600F-BDL-C (include 1x FG-2600F- BDL-950-12 + 1xFMG- VM-10-UG + 1xFC-10-F26HF-950-02-12 + 2xFC1-10-M3004-248- 02-12)	FGT-3000F	FG-3000F-BDL-C (include 1xFG-3000F-BDL-950-12 + 1xFMG-VM-10-UG + 1x FC-10-F3K0F-950-02-12 +2xFC1-10-M3004-248-02-12)
Cisco	CISCO-PR1010- F1C	CISCO-FPR1010-FIC: 1xFPR1010-NGFW-K9 + 1xL-FPR1010T-TMC= (24 mesi) + 1xSF-FMC-KVM- 10-K9	CISCO-FPR2110-F2C	CISCO-FPR2110-F2C: 1xFPR2110-NGFW-K9 + 1xL-FPR2110T-TMC= (24 mesi) + 1xSF-FMC- KVM-10-K9	CISCO-FPR2130-F3C	CISCO-FPR2130- F3C: 1xFPR2130- NGFW-K9 + 1xL-FPR2130T-TMC= (24 mesi) + 1xSF-FMC- KVM-10-K9	CISCO-FPR2140-F4C	CISCO-FPR2140-F4C: 1xFPR2140-NGFW-K9 + 1xFPR2K-NM-8X10G + 1xL-FPR2140T- TMC= (24 mesi) + 1xSF-FMC-KVM-10-K9	CISCO-FPR4115-F5C	CISCO-FPR4115-F5C: 1xFPR4115-NGFW-K9 + 2xFPR4K-NM-8X1G- F+ 1xL-FPR4115T- TMC= (24 mesi) + 1xSF-FMC-KVM-10- K9	CISCO-FPR9300-F6C	CISCO-FPR9300-F6C: 1xFPR-CH-9300-AC + 1xFPR9K-SUP + 1 x FPR9K-SM-40= + 1xFPR9K-NM-4X40G + 1xFPR9K-NM-2X100G + 1xL-FPR9K-40T-TMC= (24 mesi) + 1xSF-FMC-KVM-10-K9
Palo Alto	PAN-PA-440-CONSIP-BUN-F1	PAN-PA-440, PAN-PWR-CORD EU, PAN-PRA-25, sottoscrizione PAN-PA- 440-BND-CORESEC per 24 mesi, comprensivo di manutenzione PAN-SVC-BKLN-440+ PAN-SVC- BKLN-PRA-25	PAN-PA-1410- CONSIP-BUN-F2	PAN-PA-1410, PAN-PWR-CORD-EU, PAN-PRA-25, sottoscrizioni PAN-PA-1410-TP, PAN-PA-1410-ADVURL, PAN-PA-1410-WF per 24 mesi, comprensivo di manutenzione PAN-SVC-BKLN-1410+PAN-SVC-BKLN-PRA-25	PAN-PA-3420- CONSIP-BUN-F3	PAN-PA-3420, PAN-PWR-CORD-EU, PAN-PRA-25, sottoscrizioni PAN-PA-3420-TP, PAN-PA-3420-ADVURL, PAN-PA-3420-WF per 24 mesi, comprensivo di manutenzione PAN-SVC-BKLN-3420+PAN-SVC-BKLN-PRA-25	PAN-PA-3430- CONSIP-BUN-F4	PAN-PA-3430, PAN-PWR-CORD-EU, PAN-PRA-25, sottoscrizioni PAN-PA-3430-TP, PAN-PA-3430- DVURL, PAN-PA-3430-WF per 24 mesi, comprensivo di manutenzione PAN-SVC-BKLN-3430+PAN-SVC-BKLN-PRA-25	PAN-PA-5250- CONSIP-BUN-F5	PAN-PA-5250- CONSIP-BUN-F5 (include PAN-PA-5250- AC, PAN-PWR-CORD- EU, PAN-PRA-25 sottoscrizioni PAN-PA-5250-TP, PAN-PA- 5250-ADVURL, PAN-PA-5250-WF per 24 mesi e comprensivo di manutenzione PAN- SVC-BKLN-5250 + PAN-SVC-BKLN-PRA-25)	PAN-PA-5260-CONSIP-BUN-F6	PAN-PA-5260-CONSIP-BUN-F6 (include PAN-PA-5260-AC, PAN-PWR-CORD-EU. PAN-PRA-25 sottoscrizioni PAN-PA-5260-TP. PAN-PA-5260-ADVURL. PAN-PA-5260-WF per 24 mesi. Comprensivo di manutenzione PAN-SVC-BKLN-5260 + PAN-SVC-BKLN-PRA-25)
Forcepoint	N120-C-F1	N120-C-F1 comprensivo di (N120, FPURL1X, FPAMD1X, SMCX)	N2101-C-F2	N2101-C-F2 comprensivo di (N2101 + 2x MOGF4, FPURL8X, FPAMD8X, SMCX)	N2101-C-F3	N2101-C-F3 comprensivo di (N2101 + MOE10F4, FPURL8X, FPAMD6X, SMCX)	N3401-C-F4	N3401-C-F4 comprensivo di (N3401 + MOD10F4+ 2x MODG8, FPURL10X, FPAMD7X, SMCX)	N3405-C-F5	N3405-C-F5 comprensivo di (N3405 + MOD10F8 + 2x MODG8, FPURL11X, FPAMD8X, SMCX)	N3410-C-F6	N3410-C-F6 comprensivo di (N3410 + MOD100F2 + MOD40F2 + MOD10F8, FPURL12X, FPAMD9X, SMCX)

Tipologia Prodotto	Codice Articolo	Descrizione Articolo	Produttore	Quantità	Prezzo Totale
Fornitura	FG-400F-BDL-C	FG-400F-BDL-C (include lx FG-400F- BDL-950-12 + 1xFMG- VM-10-UG + lx FC-10-F6H0E-950-02-12 + 2xFC1-10-M3004- 248-02-12)	FORTINET	2	€ 25.005,20
Servizi	SSAR-STA	Servizio di supporto specialistico - Senior Security Architect - fascia standard	MATICMIND	7	€ 1.890,00
Manutenzione 24 mesi		Manutenzione HP Fortinet in fornitura 24 mesi (24x7x4)	MATICMIND	1	€ 2.000,40

Importo Complessivo	€ 28.895,60

La durata del Contratto Esecutivo è 24 mesi
Relativamente all'hardware previsto in fornitura, si tratta di due appliance Fortinet le cui caratteristiche specifiche e funzionale sono descritte nel capitolo dedicato.
La configurazione prevista per la soluzione proposta è basata su un cluster in alta affidabilità (active/passive).
Relativamente alle regole di nomenclatura degli elementi proposti, queste saranno concordati con il cliente e comunque conformi a quanto già eventualmente realizzato dall'Amministrazione Contraente.

I prerequisiti per la realizzazione della soluzione sono dettagliati nel capitolo specifico.
I luoghi di esecuzione dei servizi sono i seguenti:

INDIRIZZO	COMUNE	CAP	Referente	Recapito telefonico	Mail
Via Milano 13	Brescia	25100	Stefano Franceschini	+390303748516	sfranceschini@provincia.brescia.it

I prodotti e i servizi proposti, in relazione alle esigenze espresse dall'Amministrazione nel Piano dei Fabbisogni si compongono degli elementi descritti in dettaglio nei capitoli successivi.

4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
BRAND 2	*FORTINET*	3	FG-400F-BDL-C	FG-400F-BDL-C (include 1x FG-400F- BDL-950-12 + 1xFMG- VM-10-UG + 1x FC-10-F6H0E-950-02-12 + 2xFC1-10-M3004- 248-02-12)	2

La fornitura è costituita da due elementi:

- FortiGate FG-400F
- FortiManager come Virtual Machine

Le licenze previste e il supporto sono le seguenti:

Componente	Servizio	Durata	Codice che lo include
FortiGate FG-400F	FortiCare Premium (supporto hardware)	12 mesi (primo anno)	FG-400F-BDL-950-12

FortiGate FG-400F	FortiCare Premium (supporto hardware)	12 mesi (secondo anno)	FC-10-F6H0E-950-02-12
FortiGate FG-400F	Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service)	12 mesi (primo anno)	FG-400F-BDL-950-12
FortiGate FG-400F	Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service)	12 mesi (secondo anno)	FC-10-F6H0E-950-02-12

5. PRODOTTI DELLA FORNITURA

Nel seguente paragrafo è riportata la descrizione tecnica dei prodotti forniti.

5.1 NEXT GENERATION FIREWALL

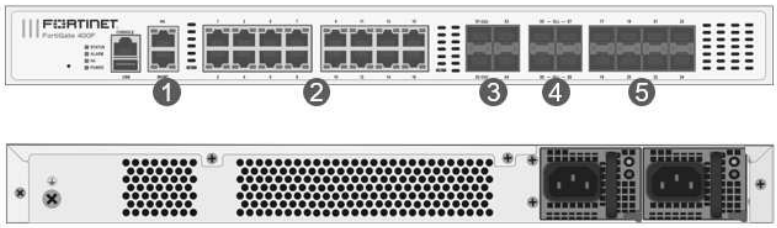
L'apparato proposto come dispositivo NGFW di fascia 3 è il FortiGate 400F, un'appliance di fascia mid-range che fornisce una soluzione di firewall di nuova generazione (NGFW) che permette di erogare servizi di sicurezza ad alte prestazioni grazie all'utilizzo di ASIC dedicati per l'analisi del traffico e dei contenuti.
Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi di fascia alta.
Requisiti dimensionali minimi per i Next Generation Firewall di fascia 3:

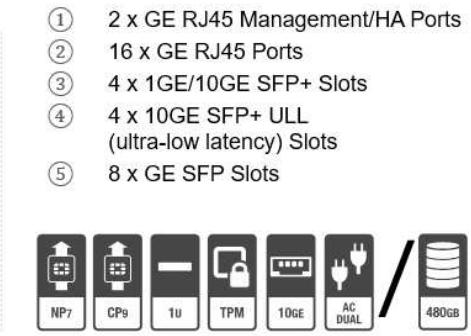
- Throughput NGFW [Gbps]: almeno 4
- Numero di sessioni TCP contemporanee: almeno 1.500.000
- Numero di nuove sessioni TCP/secondo: almeno 20.000
- Porte 1000Base-T: almeno 8
- Porte 10 GE SFP+: almeno 2

Requisiti dimensionali migliorativi per i Next Generation Firewall di fascia 2:

- Throughput NGFW [Gbps]: valore compreso tra 4 e 5,2
- Porte 1000Base-T: almeno 10
- Porte 1 GE SFP: almeno 4

Il Fortigate 400F è un'appliance di fascia alta che soddisfa i suddetti requisiti, sia minimi che migliorativi.





Questo dispositivo è dotato di 16 interfacce 1000 base-T, 2 interfacce 1000 base T dedicate al management/HA, 8 slot SFP (corredati da 2 transceiver 1000base-SX) e di 8 interfacce 10Gbps SFP+ di cui 4 a bassa latenza. Il sistema viene offerto completo di subscription Fortiguard UTP (Unified Threat Protection) per i servizi di Application Control, IPS, AV (AntiMalware Protection), Web Filtering ed Antispam.
Il FortiGate 400F dispone del sistema operativo FortiOS comune a tutte le piattaforme di firewall Fortinet. Il sistema operativo FortiOS, ha a disposizione un ricco set di funzionalità di sicurezza basate su AI/ML che fornisce all'utente un elevato numero di funzionalità aggiuntive incluse nell'offerta senza necessità di ulteriori subscription. In particolare all'interno del pacchetto base sono presenti tutte le funzionalità necessarie all'implementazione semplice e sicura di architetture SD-WAN. L'implementazione Secure SD-WAN del FortiOS garantisce un controllo intelligente dei percorsi su rete WAN, con o senza overlay IP-SEC, utilizzando più di 4000 applicazioni o utenti/gruppi per gestire le metriche di qualità della rete ed implementando politiche di routing e bandwidth management con l'utilizzo delle funzionalità di Quality of Service e Traffic Shaping.
Integrato nelle funzionalità del sistema operativo FortiOS, il servizio Universal ZTNA controlla, verifica e facilita automaticamente l'accesso degli utenti alle applicazioni riducendo le minacce laterali e fornendo l'accesso solo agli utenti convalidati. Mediante la protezione fornita della funzionalità di ispezione SSL l'apparato può fornire sicurezza all'edge di rete senza alcun impatto prestazione.
Il livello di subscription fornito garantisce l'accesso anche alle seguenti funzionalità:

- Funzionalità FortiOS
  - SSL Inspection
  - SD-WAN
  - Routing e NAT con supporto per la Traffic Redirection con ICAP (Internet Content Adaptation Protocol)
  - L2 Switching (con supporto VXLAN e EMAC)
  - Explicit proxy (funzionalità Secure Web Gateway)
  - Quality of Service (QoS) e Traffic Shaping
  - Data leak prevention (DLP)
  - Controller integrato per FortiSwitch e FortiWiFi
- FortiCare; include Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB
- Estensione del servizio AV - Advanced Malware Protection (AMP)
  - Mobile Malware Security; per proteggere i client dalle minacce destinate a device mobili. La subscription include le funzionalita' di mobile application control e protezione antimalware per piattaforme Apple IOS ed Android
  - Botnet
  - Content Disarm and Reconstruction (CDR); per rimuovere gli allegati malevoli e sostituirli con un file "disarmato"
  - Virus Outbreak Protection; servizio di verifica delle firme antivirus in tempo reale.
- DNS Filtering: il servizio permette di filtrare direttamente le query DNS per evitare traffico http verso domini compromessi
- **FortiSandbox Cloud Service; servizio che permette di massimizzare la protezione dalle minacce 0-day e identificare un attacco sulla base di tecniche di analisi avanzata e**

sandboxing. Il servizio, richiesto in gara è già disponibile nel bundle dei servizi e non è soggesto a costi aggiuntivi

La tabella seguente fornisce un dettaglio delle specifiche tecniche e prestazionali della macchina:

Specifiche hardware	
Interfacce GE RJ45	18 (+2 MGT/HA)
GE SFP Slots	8
Interfacce 10GE SFP+	8 (di cui 4 Ultra low latency)
Porte Console (RJ45)	1
Porte USB	2
Performance di Sistema	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	79,5 / 78,5 / 70 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79,5 / 78,5 / 70 Gbps
Latenza Firewall (64 byte UDP packets)	4,19 µs / 2,5 µs (ULL)
Firewall Throughput (Pacchetti per Secondo)	105 Mpps
IPS Throughput (Enterprise Traffic Mix)	12 Gbps
Sessioni Concorrenti (TCP)	8 Million
Nuove Sessioni/Secondo (TCP)	500.000
Firewall Policies	10.000
IPsec VPN Throughput (512 byte)	55 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2.000
Client-to-Gateway IPsec VPN Tunnels	50.000
SSL-VPN Throughput	3,6 Gbps
Utenti concorrenti SSL-VPN (Massimo raccomandato, tunnel mode)	5.000
SSL Inspection Throughput (IPS, HTTP)	8 Gbps
Application Control Throughput (HTTP 64K)	28 Gbps
Virtual Domains (Default / Maximum)	10/10
Numero Massimo di FortiSwitches Supportati	72
Numero Massimo di FortiAPs (Totali / Tunnel Mode)	512/256
Numero Massimo di FortiTokens	5000
Configurazioni di High Availability	Active/Active, Active/Passive, Clustering
Dimensioni	
Altezza x Larghezza x Lunghezza (mm)	44,45 x 432 x 380
Peso	6,4 kg
Form Factor	1 RU

Riferimenti documentali pubblici:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf

6. PREREQUISITI DEI PRODOTTI

Prerequisiti tecnologici

Eventuali attività propedeutiche e/o correttive su endpoint e oggetti di rete dell'infrastruttura dell'azienda contraente potranno essere indicati e suggeriti in fase di analisi ma sono da intendersi completamente a carico dell'amministrazione contraente, salvo quelle esplicitamente definite nella lista di attività sottostante:

Device (Vendor)	Configuration	Note
Fortinet	Basic Setup	Verifica disponibilità spazio nei rack per i nuovi firewall
		Verifica disponibilità elettrica nei rack
		Verifica disponibilità porte negli switch
		Disponibilità mappa di rete e indirizzamento IP
		Routing Info

Si precisa che tutte le eventuali attività propedeutiche all'installazione degli apparati sono a carico dell'Amministrazione Contraente (predisposizione delle linee di alimentazione, linee dati, rack, supporti etc…).

7.SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa.

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	

Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	**7**
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Junior Security Analyst: in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

Security Principal: in possesso della certificazione ISACA CISM (Certified Information Security Manager)

Senior Security Architect: in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional)

Senior Security Analyst: in possesso di almeno una delle seguenti certificazioni:
EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst

Le attività che l'Amministrazione intende svolgere attraverso il servizio di supporto specialistico consistono in:

- Configurazione degli apparati secondo progetto condiviso con il Cliente e "Best-Practice" Fortinet

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze del cliente e comunque in funzione della fornitura prodotti richiesta tramite questo piano. Qualsiasi altra necessità sarà valutata di volta in volta in accordo con il cliente.

10. SERVZIO DI MANUTENZIONE

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site.
L'Amministrazione Contraente ha richiesto a pagamento il servizio di manutenzione in base al profilo di qualità per i servizi erogati: High Profile (H24).

Il servizio di manutenzione è offerto per annualità, quindi per 24 mesi.
In accordo con l'Amministrazione, si predisporrà un accesso remoto sicuro utilizzando account VPN personali configurati e abilitati opportunamente, con tracciatura degli accessi per eventuali successivi audit, accessi che comunque dovranno essere limitati al tempo strettamente necessario all'esecuzione dell'attività, ad esempio mediante utenze token create all'occorrenza a supporto delle stesse (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione).
Le attività di manutenzione sono previste per i soli elementi di fornitura acquistati nell'ambito del presente AQ.
Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
- intervento presso la sede/luogo interessato
- ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati o verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

11 PIANO DI LAVORO

Nela seguente tabella vengono sintetizzate le configurazioni previste:

Vendor	Device	Configuration	Note	External Reference
Fortinet	FG-400F-BDL-C	Basic Setup	Software Upgrade	
			Interfacce di Rete	
			Routing Info	
			High Availability	
			Licensing	
			MGMT VPN	
		NGFW Setup	Firewall	
			AntiVirus	
			Application Control	
			IPS	
			VPN IPSec	
			Web/URL Filtering	
		Advanced Configuration Backend	Creazione Virtual System BACK-END	
			Configurazione topologia (routing e interfacce)	
			Creazione regole di backend per network e Zone	
			Tuning profili NGFW per traffico back end (IPD antivirus antimalware application control) in modalità monitoring	

			Messa in produzione	
			Tuning profili ngwf (modalità prevent)	
			Hardening regole	
		Advanced configuration Front End	Creazione Virtual System Front-End	
			Configurazione topologia (routing e interfacce del PA 850 in produzione)	
			import regole da PA850	
			verifica profili NGFW per traffico back end (IPS antivirus antimalware application control) in modalità monitoring	
			Messa in produzione (dismissione del PA850)	
			Tuning profili ngwf (modalità prevent)	
			Hardening regole	

Per quanto concerne le regole di nomenclatura, verrà data continuità alle regole in essere, ulteriori nuove regole di nomenclatura verranno concordate con l'amministrazione Contraente ed inserite nel relativo documento progettuale di High Level Design.

11.1 GANTT

Come concordato con l'Amministrazione contraente, la produzione del cronoprogramma, riportante i tempi previsti per l'esecuzione delle attività e dei servizi richiesti, viene temporaneamente rimandata. Al momento del rilascio del cronoprogramma, il presente Piano Operativo sarà oggetto di aggiornamento.
Il cronoprogramma sarò rilasciato al termine della prima fase dell'attività sistemistica ovvero analisi dell'infrastruttura ,definizione dei desiderata e creazione del progetto esecutivo (HLD) concordato.

11.2 PIANO DI PRESA IN CARICO

Di seguito si riportano le principali attività:

- predisposizione e configurazione dei servizi proposti;
- creazione dell'account del referente dell'Amministrazione per l'accesso al Portale della Fornitura e configurazione dell'Area Privata;
- acquisizione di Know-How relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione;
- acquisizione degli standard, modalità operative, linee guida e metodologie in uso presso l'Amministrazione, ove presenti.

Entro 5 giorni dalla stipula del Contratto esecutivo verrà svolta la prima riunione di lavoro con il referente tecnico del Fornitore ed i referenti tecnici dell'Amministrazione.
A seguito di tale riunione la presa in carico prevederà:

- rilevazione delle configurazioni in essere sui vari sistemi
- esame della documentazione esistente (es. elenco degli asset informatici, catalogo dei sistemi e delle applicazioni, etc.) con assistenza di personale esperto
- affiancamento condotta con l'eventuale fornitore uscente.

Durante l'attività di Presa in carico si garantirà:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal RTI e dall'Amministrazione.

L'avvio del progetto prevedrà le seguenti fasi:

1. Identificare il team di progetto: Verrà designato un team di progetto che lavorerà sulla presa in carico del servizio IT e verrà definito un responsabile del progetto.
2. Definizione del piano di attuazione: sarà creato un piano di attuazione che includa un calendario per l'implementazione del servizio IT e delle attività di acquisizione di conoscenze, standard e linee guida.

3. Acquisizione di informazioni sull'organizzazione: verranno raccolte le informazioni sul contesto organizzativo, tecnologico e funzionale dell'Amministrazione attraverso la revisione della documentazione disponibile, interviste con i rappresentanti dell'Amministrazione, e visite sul campo.
4. Acquisizione di standard e metodologie: Rivedere gli standard, le modalità operative, le linee guida e le metodologie in uso presso l'Amministrazione per integrare le migliori pratiche in uso e conformarsi ai requisiti dell'Amministrazione
5. Questa fase sarà completata al termine della messa in esercizio del servizio.
6. Formazione del personale: il personale coinvolto nella presa in carico del servizio sarà formato “on the job” in modo da assicurare la conoscenza dei processi dell'organizzazione e dei protocolli standard.
7. Test del servizio: il servizio sarà testato con i rappresentanti dell'Amministrazione per valutare l'efficacia dell'implementazione e identificare eventuali problemi o aree di miglioramento.

11.3 SPECIFICHE DI COLLAUDO

Le schede di collaudo dei servizi/forniture previste saranno concordate con l’Amministrazione.
Il piano dei test previsto per il firewall sarà composto dai seguenti punti:

- Verifica accesso alla console di management del firewall in modalità Operator e Admin
- Verifica della corretta erogazione dei servizi interni da una postazione client interna all’infrastruttura
- Verifica della corretta erogazione dei servizi interni Pubblicati da una postazione Esterna all’infrastruttura
- Verifica della corretta erogazione dei servizi interni da parte di un client connesso all’infrastruttura tramite client Fortinet
- Verifica della corretta erogazione dei servizi Internet da una postazione client interna all’infrastruttura
- Verifica del sistema di logging e di tracciamento delle connettività degli utenti
- Verifica della connettività di accesso remoto tramite il client Fortinet
- Test di fail-over del firewall primario e di ripristino da fault
- Verifica corretta procedura di backup e salvataggio della configurazione
- Verifica di ripristino della configurazione da backup

In fase di completamento della fase progettuale e del Low Level Design verranno definite tutte verifiche funzionali che verranno effettuate in fase di collaudo .
Tale documento verrà rivisto e aggiornato al termine della messa in produzione della soluzione e prima del collaudo.

A corredo della fornitura verranno, prodotti e rilasciati i seguenti deliverable:

- Documentazione di Progetto con “High-Level” e “Low-Level” Design;
- “Test-List” per collaudo e rilascio finale della piattaforma Fortinet;
- Procedura di Backup and Restore.

12. TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

Codice Articolo Convenzione	Quantità	Durata	Prezzo Totale
CS2L2-NGFW-F3-FN	2		25005,20

CS2L2-MANHP-NGFW-F3-FN	2	24	2000,40
CS2L2-SSAR-STA	7		1890,00

13. PRESTAZIONE DI SUBAPPALTO

Essendo i servizi erogati da azienda facente parte di RTI, non si prevede l'impiego del subappalto.