PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT
LOTTO 3

CITTA' METROPOLITANA DI MESSINA

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	14/12/2023

Indice

1. INTRODUZIONE 3
1.1 Premessa 3
1.2 Scopo 3
1.3 Riferimenti 3
1.4 Acronimi e glossario 4
2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO 4
2.1 Categorizzazione degli interventi 5
3. PROGETTO DI ATTUAZIONE 5
4. PRODOTTI OFFERTI 7
4.6 NGFW 8
4.6.1 Brand 1 – Fortinet 8
4.7 Servizio di supporto specialistico 10
5 PIANO DI LAVORO 11
5.1 Specifiche di Progetto 11
5.2 Piano delle attività 11
5.3 Piano di presa in carico 11
5.4 Specifiche di collaudo 12
6 Prestazioni Subappalto 12

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 Città Metropolitana di Messina, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: Piano dei Fabbis Città Metropolitana di Messina).

1. La Città metropolitana, quale ente di area vasta, oltre che delle funzioni attribuite dall'articolo 27 ai liberi Consorzi comunali, è titolare delle seguenti funzioni proprie:
a. adozione ed aggiornamento annuale di un piano strategico triennale del territorio metropolitano, che costituisce atto di indirizzo per l'ente e per l'esercizio delle funzioni dei comuni e delle unioni di comuni compresi nel predetto territorio, anche in relazione all'esercizio di funzioni ulteriori eventualmente delegate o assegnate dalla Regione;
b. pianificazione territoriale generale ed urbanistica che, nel fissare vincoli e obiettivi all'attività dei comuni compresi nel territorio metropolitano, individua in ogni caso le aree da destinare all'edilizia residenziale pubblica, convenzionata ed agevolata nonché le strutture di comunicazione, le reti di servizi e le infrastrutture e ne valuta la loro sostenibilità ambientale, ecologica ed energetica nel contesto metropolitano;
c. strutturazione di sistemi coordinati di gestione dei servizi pubblici locali del territorio metropolitano, già di competenza comunale;
d. mobilità e viabilità nel territorio metropolitano, assicurando la compatibilità e la coerenza della pianificazione urbanistica dei singoli comuni nell'ambito metropolitano e garantendo in ogni caso l'intermodalità dei trasporti nonché l'ottimizzazione dei collegamenti delle aree portuali ed aeroportuali con le infrastrutture autostradali;
e. promozione e coordinamento dello sviluppo economico e sociale nel territorio metropolitano, anche assicurando sostegno e supporto alle attività economiche e di ricerca innovative e coerenti con la vocazione della Città metropolitana, come delineata nel piano strategico del territorio di cui alla lettera a);
f. sostegno e sviluppo dei Consorzi universitari presenti nel territorio nonché degli enti culturali già sostenuti dalle ex province regionali;
g. partecipazione diretta alla programmazione, assegnazione e gestione di interventi finanziati con fondi europei, destinati alla Città metropolitana.

Con questo progetto il Comune di Messina intende innalzare significativamente il livello di cybersecurity dell'Azienda mediante l'acquisizione di prodotti per la sicurezza perimetrale e la protezione degli endpoint oltre all'erogazione di servizi connessi.
Gli interventi previsti riguardano:

- La fornitura in opera di Next Generation Firewall Fortinet di fascia 1;

Mediante la loro opportuna configurazione, l'Azienda Sanitaria avrà la possibilità di aumentare la protezione dalle minacce informatiche più comuni (malware) e ottenere una maggiore protezione verso le minacce informatiche più avanzate (advanced persistent threat, minacce zero day, …).
L'Amministazione, inoltre, fruirà del Servizio di Supporto Specialistico in ambito di cyber security, che sarà utilizzato per attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione.

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.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni - Piano dei Fabbis Città Metropolitana di Messina
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
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
SPC	Sistema Pubblico di Connettività

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.

Nel Piano Operativo dovrà inoltre essere indicato il modello organizzativo impiegato per l'esecuzione delle attività ed in particolare le persone di riferimento che saranno coinvolte nel processo, che comprendono almeno:

- il "*Responsabile dell'Amministrazione*" (già identificato nel "*Piano dei Fabbisogni*");
- il "*Responsabile del Fornitore*" (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale).

- **Responsabile del Fornitore**

Nome Cognome: *Emilio Minniti*
telefono/cellulare: *366.6320811*
e-mail: *emilio.minniti@maticmind.it*

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

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

Nome Cognome: *Mario Alberto Maugeri*
telefono/cellulare: *334.6537106*
e-mail: *marioalberto.maugeri@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
	□ 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

Nel "Piano Operativo" il Fornitore dovrà riportare, a titolo esemplificativo e non esaustivo, almeno i seguenti aspetti, in coerenza con quanto espresso dall'Amministrazione nel suo "Piano dei fabbisogni":

• l'importo contrattuale complessivo e per ciascuna voce oggetto di quotazione economica, con 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

Tipologia Prodotto	Codice Articolo	Descrizione Articolo	Produttore	Quantità	Prezzo Totale
Fornitura	NGFW-F1-FN	NGFW - Fascia 1	FORTINET	1	€ 1.211,18
Servizi	SP-STA	Servizio di supporto specialistico - Security Principal - fascia standard		94	€ 29.140,00
Servizi	SSAR-STA	Servizio di supporto specialistico - Senior Security Architect - fascia standard		107	€ 28.890,00
Servizi	SST-STA	Servizio di supporto specialistico - Senior Security Tester - fascia standard		101	€ 25.573,00
Servizi	JSAN-STA	Servizio di supporto specialistico - Junior Security Analyst - fascia standard		127	€ 28.892,50
Importo Complessivo					€ 115.706,68

• la durata del Contratto Esecutivo è 24

• In riferimento alle informazioni tecniche oggetto della fornitura, riferirsi ai capitoli successivi.

Relativamente a:

- configurazioni previste per gli apparati HW e SW forniti
- schemi logici dell'architettura di rete
- schemi di indirizzamento, policy di sicurezza ed ogni altra informazione di configurazione necessaria per l'introduzione dei nuovi apparati, stabiliti in accordo all'Amministrazione Contraente conformemente a quanto già implementato
- tempi di consegna di fornitura e relativa documentazione
- regole di nomenclatura individuate per i vari elementi, che dovranno in ogni caso essere conformi a quanto già eventualmente realizzato dall'Amministrazione Contraente e con quest'ultima condivise

riferirsi ai capitoli successivi.

- ogni altra informazione utile a consentire alle Amministrazioni rientranti nel perimetro di sicurezza cibernetica la redazione della comunicazione da trasmettere al CVCN o ai CV;

- indicazione dei prerequisiti necessari all'installazione degli elementi di fornitura e delle necessarie attività in carico all'Amministrazione Contraente

- indicazione delle verifiche funzionali da effettuare, descrivendo i casi di test identificati ed i risultati attesi e delle modalità di effettuazione di tali verifiche

- il cronoprogramma, riportante i tempi previsti per l'esecuzione delle attività e dei servizi richiesti in accordo con l'Amministrazione Contraente, è riportato al paragrafo di riferimento.

- l'indicazione del/i luogo/ghi e delle sedi di esecuzione dei servizi

INDIRIZZO	NUM. CIV.	COMUNE	CAP	Referente	Recapito telefonico	Mail
Corso Cavour	87	Messina	98122	Roberto Caracciolo	339.6988455	roberto2@cittametropolitana.me.it

- l'impegno in giorni persona dei singoli profili professionali coinvolti, previsto per l'erogazione di ciascun servizio di fornitura

Servizio	Figura professionale	Giornate
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	Security Principal	94
	Senior Security Architect	107
	Senior Security Tester	101
	Junior Security Analyst	127

- i CV delle risorse professionali da impiegare con le relative certificazioni

- le informazioni relative alla categorizzazione degli interventi e utili all'Amministrazione ai fini del calcolo degli indicatori di digitalizzazione, così come indicati dall'Amministrazione stessa in fase di Piano dei Fabbisogni.

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

4. PRODOTTI OFFERTI

Next Generation Firewall							
BRAND	**DENOMINAZIONE BRAND**	**FASCIA 1 (cfr. definizione CT Speciale)**					
BRAND 1	*Fortinet*	*Modello:* ***FGT-60F*** *Codice Prodotto* ***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)*					

Network Generation Firewall

4.6.1 Brand 1 – Fortinet

Fortinet FG-60F-BDL-950-12

L'apparato proposto come dispositivo per la sicurezza di fascia base è il FortiGate 60F, che offre una eccellente soluzione di sicurezza di fascia base, in un formato compatto desktop e fanless. Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi di fascia base.

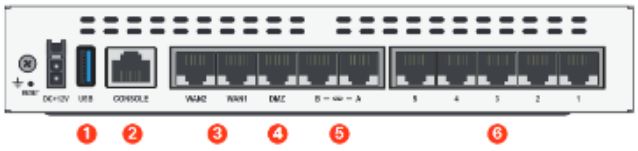
Requisiti minimi per i dispositivi di sicurezza di fascia base:

- Funzionalità Firewall
- Funzionalità Antivirus
- Funzionalità di Application Control
- Funzionalità di Intrusion Prevention System (IPS)
- VPN IPSec
- Funzionalità web/url filtering
- Almeno 6 interfacce 1000Base-T
- IPS throughput almeno pari a 300 Mbps
- Firewall throughput almeno pari a 1,5 Gbps
- VPN throughput almeno pari a 300 Mbps
- Almeno 400.000 sessioni contemporanee
- Almeno 20.000 nuove sessioni al secondo

Caratteristiche migliorative per i dispositivi di sicurezza di fascia base:

- Funzionalità Antispam
- Meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service
- Almeno 2 ulteriori interfacce 1000Base-T
- Funzionalità di TLS o SSL Inspection
- Supporto per configurazioni High Availability
- Funzionalità VPN TLS o SSL
- Supporto IPv6
- Miglioramento di almeno il 30% delle prestazioni minime previste per l'Intrusion Prevention throughput (390 Mbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per Firewall throughput (1,95 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per VPN throughput (390 Mbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di sessioni contemporanee (520.000)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di nuove sessioni al secondo (26.000)

Il Fortigate 60F è un appliance di fascia base, con form-factor di tipo desktop, che soddisfa i requisiti sia minimi che migliorativi di gara.



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

Hardware Features

Questo dispositivo è dotato di 8 interfacce 1000 base-T, 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 60F dispone del sistema operativo FortiOS comune a tutte le piattaforme di firewall Fortinet. Il sistema operativo FortiOS 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 3000 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.

Il livello di subscription fornito garantisce l'accesso anche alle seguenti funzionalità:

- Funzionalità native 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
  - Quality of Service (QoS) e Traffic Shaping
  - Data leak prevention (DLP)
  - Controller integrato per FortiSwitch e FortiAP
- 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 1000Base-T	8
Porte Console (RJ45)	1
Porte USB	1
Performance di Sistema	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10 / 10 / 6 Gbps
Latenza Firewall (64 byte UDP packets)	3.3 µs
Firewall Throughput (Pacchetti per Secondo)	9 Mpps
Sessioni Concorrenti (TCP)	700,000
Nuove Sessioni/Secondo (TCP)	35,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte)	6.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
IPS Throughput (Enterprise Traffic Mix)	1.4 Gbps
SSL-VPN Throughput	900 Mbps
SSL Inspection Throughput (IPS, HTTP)	630 Mbps
Application Control Throughput (HTTP 64K)	1.8 Gbps
Virtual Domains (Default / Maximum)	10/10
Numero Massimo di FortiSwitches Supportati	16
Numero Massimo di FortiAPs (Totali / Tunnel Mode)	64 / 32
Numero Massimo di FortiTokens	500
Configurazioni di High Availability	Active/Active, Active/Passive, Clustering
Dimensioni	
Altezza x Larghezza x Lunghezza (mm)	38.5 x 216 x 160
Peso	1.01 kg
Form Factor	Desktop

Riferimenti documentali pubblici:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf

4.7 SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio si 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

In aggiunta:

a. adozione ed aggiornamento annuale di un piano strategico triennale del territorio metropolitano, che costituisce atto di indirizzo per l'ente e per l'esercizio delle funzioni dei comuni e delle unioni di comuni compresi nel predetto territorio, anche in relazione all'esercizio di funzioni ulteriori eventualmente delegate o assegnate dalla Regione;
b. pianificazione territoriale generale ed urbanistica che, nel fissare vincoli e obiettivi all'attività dei comuni compresi nel territorio metropolitano, individua in ogni caso le aree da destinare all'edilizia residenziale pubblica, convenzionata ed agevolata nonché le strutture di comunicazione, le reti di servizi e le infrastrutture e ne valuta la loro sostenibilità ambientale, ecologica ed energetica nel contesto metropolitano;
c. strutturazione di sistemi coordinati di gestione dei servizi pubblici locali del territorio metropolitano, già di competenza comunale;
d. mobilità e viabilità nel territorio metropolitano, assicurando la compatibilità e la coerenza della pianificazione urbanistica dei singoli comuni nell'ambito metropolitano e garantendo in ogni caso l'intermodalità dei trasporti nonché l'ottimizzazione dei collegamenti delle aree portuali ed aeroportuali con le infrastrutture autostradali;
e. promozione e coordinamento dello sviluppo economico e sociale nel territorio metropolitano, anche assicurando sostegno e supporto alle attività economiche e di ricerca innovative e coerenti con la vocazione della Città metropolitana, come delineata nel piano strategico del territorio di cui alla lettera a);
f. sostegno e sviluppo dei Consorzi universitari presenti nel territorio nonché degli enti culturali già sostenuti dalle ex province regionali;
g. partecipazione diretta alla programmazione, assegnazione e gestione di interventi finanziati con fondi europei, destinati alla Città metropolitana.

Per l'effettuazione del complesso di attività previste per il supporto specialistico il Fornitore dovrà prevedere le figure professionali riportate nel seguito. Si precisa che, fatto salvo il possesso del diploma di scuola media superiore, i requisiti accademici richiesti per ogni figura (titoli di studio) possono essere utilmente soddisfatti attraverso il possesso di una cultura equivalente, maturata attraverso lo svolgimento di esperienze lavorativo-professionali, pari a:

d) □ **5 (cinque) anni aggiuntivi nel settore ICT** nel caso di laurea specialistica

e) □ **3 (tre) anni aggiuntivi nel settore ICT** nel caso di laurea triennale.

5 PIANO DI LAVORO

5.1 SPECIFICHE DI PROGETTO

- indicazione dei prerequisiti necessari all'installazione degli elementi di fornitura e delle necessarie attività in carico all'Amministrazione Contraente

- configurazioni previste;

Device (Vendor)	Configuration	Note	External Reference
FortiGate	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	SDWAN	
		FSSO	

- I tempi di consegna della fornitura e relativa documentazione indicati dal vendor sono stimati in 60 giorni lavorativi.

- 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.

5.2 PIANO DELLE ATTIVITÀ

Come concordato con l'Amministrazione contraente, la produzione del cronoprogramma (GANTT), 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.

5.3 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:

• 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.
• 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.
• 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.

• 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.
• 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.
• 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.
• Conduzione del servizio IT: la conduzione del servizio avverrà effettuando monitoraggi sulle performance per valutare l'efficacia dell'implementazione, identificando eventuali aree di miglioramento.
• Rapporti periodici: verranno forniti report periodici all'Amministrazione sulle prestazioni del servizio, sull'avanzamento delle attività e linee guida per garantire una comunicazione continua e trasparente

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.

5.4 Specifiche di collaudo

Il piano dei test previsto per i Firewall sarà composto dai seguenti punti:

1. Verifica delle policy applicate
2. Test di funzionamento della MPLS
3. Test HA
4. Report dei risultati: infine, si creerà un report dei risultati dei test, che include un riassunto delle attività, degli obiettivi e dei test case utilizzati. Il report potrà contenere anche eventuali raccomandazioni per migliorare il Firewall o per futuri test.

6 Prestazioni Subappalto

Nell’ambito dell’Accordo Quadro Cybersecurity 2 per le prestazioni erogate in subappalto è previsto quanto segue:

- Quota massima del subappalto: 50%
- Servizi per i quali è prevista la prestazione in subappalto:
  - Supporto Specialistico.

Nella tabella sottostante è necessario riportare la quota, le prestazioni e il nome delle aziende che erogheranno i servizi in subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

Servizi	Quota subappalto	Azienda del RTI che eroga il servizio	Nome dell’azienda che eroga la prestazione in subappalto
Supporto Specialistico	47%	Maticmind S.p.A.	Laser Service s.r.l.