PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE

AQ CONSIP 2367 – Lotto 3

Città Metropolitana di Messina

1. Indice

2. Revisioni

Revisione	Descrizione modifiche	Data
1.1	Prima emissione	28/06/2023

3. Introduzione

3.1. Premessa

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per la sicurezza perimetrale per la Città Metropolitana di Messina in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (allegato all'ordine n. **7174833**).

Con questo progetto il cliente Citta Metropolitana di Messina intende acquisire:

- N°2 New Generation Firewall con manutenzione Low Profile per 2 anni;
- Servizi di supporto specialistico fascia standard;

3.2. 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.

3.3. Riferimenti

- Piano dei Fabbisogni allegato all'ordine **7174833**
- 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

3.4. 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

4. 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)**, 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
  - **Massimiliano Materazzi, +393357384498, massimiliano.materazzi@telecomitalia.it**
- **Responsabile dell'Amministrazione**, già identificato nel "Piano dei Fabbisogni"
  - **Giacomo Lucà, 3356623778, g.luca@cittametropolitana.me.it**
- **Responsabile del Fornitore** (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale), che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo
  - **Rosario Villari, +393357356804, rosario.villari@telecomitalia.it**
- **Referente Tecnico per l'erogazione dei servizi**, che dovrà 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)
  - **Marco Leofrigio, +393316005563, marco.leofrigio@telecomitalia.it**

4.1. 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

X **Infrastrutture**	X 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

4.2. Progetto d'attuazione

La Città Metropolitana di Messina è l'ente pubblico territoriale che rappresenta la comunità autonoma individuata dal procedimento di aggregazione in libero consorzio di comuni. Attraverso questa istituzione la popolazione che la costituisce esercita democraticamente il proprio governo sul territorio nei confini risultanti dalla libera espressione delle autonomie, e si riconosce nelle proprie radici storiche, antropologiche, culturali ed ambientali che la identificano nel contesto della Regione siciliana, quale comunità particolare, distinta, ma non separata, integrata intorno al suo capoluogo. La Città metropolitana di Messina è un ente territoriale di area vasta, il cui territorio coincide con quello della preesistente Provincia. Istituita il 7 agosto 2015[1], è operativa dal 4 gennaio 2016 e comprende 108 Comuni.

Macro Requisiti ed Obiettivi che l'Amministrazione si propone con la fornitura

Ai fini delle evoluzioni del sistema informatico dell'Ente, è necessario un adeguamento delle dotazioni di sicurezza: si vuol procedere all'acquisizione di una coppia di firewall perimetrali, che garantisca un throughput dello stesso livello di quello attuale, completa dei servizi previsti per la messa in opera e per l'attivazione di servizi personalizzati di controllo.

Fra tali servizi, dovrà essere attivato e personalizzato un servizio di controllo e monitoraggio dei sistemi che gestiscono la Posta Elettronica e dei sistemi che gestiscono la raccolta dei log.

Le configurazioni del sistema di controllo, del Firewall e dei servizi annessi saranno tali da consentire l'interazione con le attuali regole del firewall di frontiera e dovranno essere in grado di gestire tutte le connessioni attualmente in uso presso la Città Metropolitana, oltre a quelle derivanti dall'utenza relativa ai nuovi progetti in Cloud.

5. Prodotti richiesti

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità
NGFW	Fortinet	3	NGFW-F3-FN	FG-600E-BDL-C	2

5.1. Prodotti della fornitura

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

5.1.1. Next Generation FireWall

Il servizio "Next Generation Firewall" oggetto della fornitura, fornito attraverso appliance FortiGate di Fortinet, garantisce servizi evoluti di sicurezza multi-minaccia attraverso l'adozione di un'unica piattaforma integrata che consente di contrastare efficacemente attacchi e minacce informatiche, grazie anche alla semplicità di gestione e alla flessibilità di inserimento in una vasta gamma di scenari di implementazione.

Gli apparati fisici installati on-premise presso la sede dell'Amministrazione contraente, permettono la visibilità completa del traffico attraverso la gestione di indirizzi IP, utenti e dispositivi con la possibilità di creare policy di sicurezza con una combinazione di questi fattori.

L'ispezione del livello applicativo (Application Control feature), permette una accurata identificazione delle applicazioni che generano traffico all'interno della rete senza comprometterne le performance. Una volta individuato il traffico applicativo, è possibile controllare le applicazioni, bloccare quelle indesiderate, limitare e garantire la relativa banda (Traffic Shaping feature), attivare i

profili di protezione antivirus/antimalware, IPS/IDS, DLP (Data Loss Prevention) e le altre verifiche di sicurezza dettagliate precedentemente.

5.1.2. Caratteristiche del servizio

Il servizio di NGFW dovrà essere erogato nella sede di Messina– referente: Roberto Caracciolo

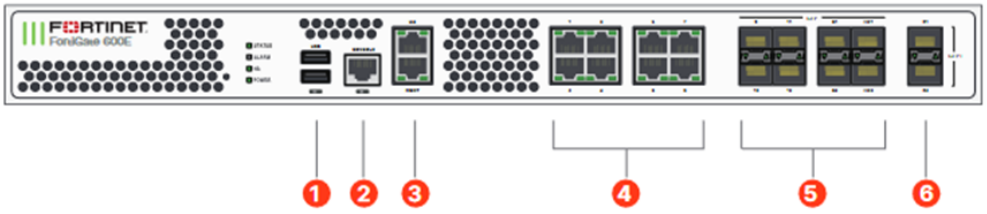
Nella sede\i indicata\e verranno forniti i seguenti apparati fisici, come indicato in tabella, secondo quanto richiesto nel Piano dei fabbisogni:

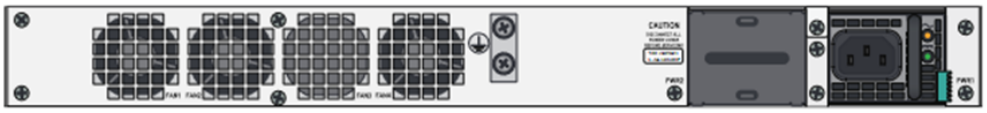
Next Generation FireWall				
Prodotto / Fascia	**Codice servizio**	**Brand**	**Codice fornitore**	**Quantità**
NGFW – Fascia 3	NGFW-F3-FN	Fortinet	FG-600E-BDL-C	2

5.1.3. Caratteristiche hardware \specifiche tecniche FortiGate

Hardware

FortiGate 600E Series

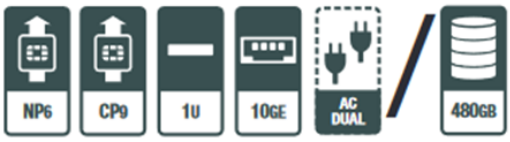




Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 8 x GE RJ45 Ports
5. 8 x GE SFP Slots
6. 2 × 10 GE SFP+ Slots

Hardware Features



5.2. 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 in seguito:

a) supporto per l'installazione, configurazione e messa in esercizio dei prodotti e delle licenze riportate in fornitura relative al NGFW compresa la ripresa delle policies dai sistemi esistenti Sonicwall

b) supporto consulenziale per analisi e valutazione del servizio di controllo e monitoraggio dei sistemi che gestiscono la Posta Elettronica.

c) supporto tecnico e sistemistico per la revisione dei sistemi che gestiscono la raccolta dei log

Di seguito si riporta quanto proposto, in aderenza a quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Senior Security Analyst – fascia standard	SSAN-STA	SR_SEC_AN_STD	45
Senior Security Architect – fascia standard	SSAR-STA	SR_SEC_ARCH_STD	50
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	50

6. La tabella di riassunto economico, riportata nel paragrafo

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) tenendo in considerazione che, data le attività specifiche del progetto e le competenze necessarie alla progettazione ed implementazione, la certificazione specifica necessaria rispetto a quanto previsto è la Network Security Professional (NSE 4) Fortinet.

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze dell'Amministrazione 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.

Nell'ambito del progetto proposto, attraverso i servizi specialistici e secondo quanto previsto dal successivo piano di lavoro, si provvederà alla sostituzione degli attuali apparati in possesso dalla PA contraente, in tecnologia con N nuovi apparati NGFW Fortigate.

6.1. Servizio 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.

In ottemperanza al quanto richiesto nel piano dei fabbisogni, per i prodotti forniti viene proposto il servizio di manutenzione per 24 mesi di tipo “High Profile” (H24).

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:
    1. intervento presso la sede e/o luogo interessato
    2. ripristino del servizio e/o funzionalità sui livelli preesistenti al guasto e/o anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati o verifica funzionale del sistema per assicurare l’eliminazione della causa del guasto.

In accordo con l’Ente verrà attivato un accesso remoto sicuro mediante account VPN configurati opportunamente, con tracciatura degli accessi per eventuali successivi audit.

Gli accessi saranno limitati al tempo strettamente necessario all’esecuzione delle specifiche attività.

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

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Durata (mesi)**
Manutenzione LP	MANLP-NGFW-F3	FORTINET	24

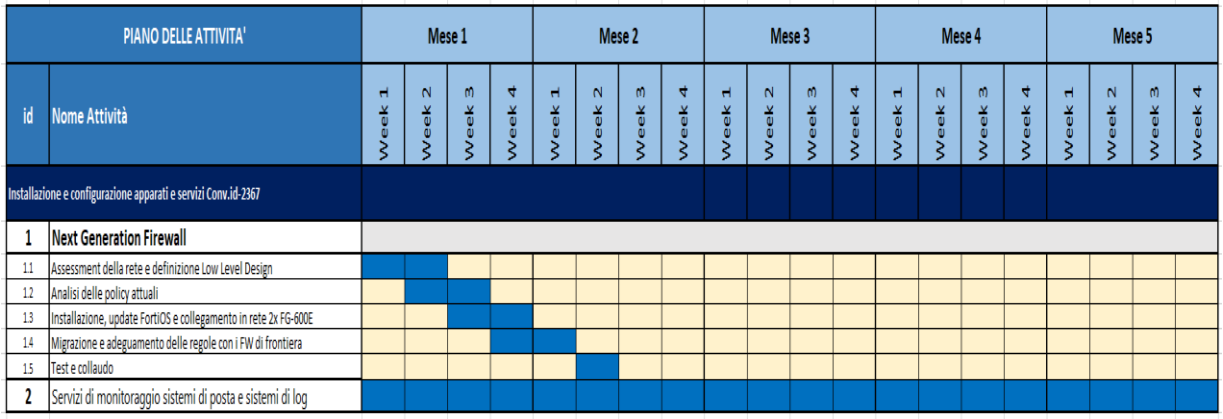
7. Piano di lavoro

Al fine di una corretta implementazione ed inizializzazione del servizio proposto, saranno necessarie le seguenti fasi operative:

Servizio NGFW

- Provisioning e delivery degli apparati
- Installazione apparati nelle apposite sedi della PA
- Supporto alle operazioni di configurazione degli apparati in HA ove richiesto ed alle altre operazioni richieste (quali definizione delle interfacce fisiche, dei PortChannel di interconnessione altri apparati e definizione delle interfacce logiche (VLAN), definizione static L3 routing , migrazione dell’as-is sugli apparati attuali delle regole di sicurezza dai firewall esistenti.
- Test da un segmento interno L3 di staging e collaudo
- GO LIVE

7.1. GANTT



7.2. Piano di presa in carico

L'attività di presa in carico del sistema consiste nell'acquisire tutte le informazioni che sono necessarie all'erogazione dei servizi e di quanto indicato nel sopra riportato piano di lavoro, con l'obiettivo di acquisire know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione oltre a standard, modalità operative, linee guida, ove presenti. Come specificato da piano dei fabbisogni l'amministrazione contraente fornirà l'accesso ai sistemi attuali dai quali estrarre la configurazione esistente degli apparati Sonicwall.

L'attività di assessment e di supporto consulenziale potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. schemi logici e di low level design dell'infrastruttura di rete, informative sulle connettività presenti, piani di indirizzamento etc) con assistenza di personale esperto e affiancamento condotta con eventuali ulteriori fornitori dell'amministrazione contraente.

Le attività saranno oggetto di verbali dettagliati nei quali verrà indicato il piano di attività eseguito e quello programmato, eventuali difformità che dovessero rendersi necessarie e/o richieste da nuove o diverse esigenze operative, nonché eventuali carenze o mancanza di aggiornamento rilevato nella documentazione disponibile.

Durante le attività di Presa in carico saranno garantite:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi ivi compresa la reperibilità e disponibilità dei 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 dai rappresentanti del RTI e dell'Amministrazione.

7.3. Specifiche di collaudo

Per ciascun elemento che compone le macroaree di progetto, verranno effettuate prove di esercibilità e test funzionali secondo il piano di seguito riportato. Le date di collaudo potranno essere definite in accordo al piano riportato al paragrafo precedente.

- Verifica funzionalità di base degli apparati
- Verifica funzionamento Alta affidabilità

- Monitoraggio funzionamento Policy

Per il servizio di NGF saranno eseguite le seguenti attività di verifica e test da affinare in sede del cliente.

Tipologia	Descrizione
Test Funzionale	Verifica che i dispositivi funzionino come previste siano in grado di eseguire le funzionalità base come la prevenzione dell'intrusione, la verifica delle autorizzazione agli accessi, delle politiche di sicurezza
Test di sicurezza	Verificare la capacità dei dispositivi di rilevare e prevenire possibili compromissioni e attacchi all'infrastruttura IT. Questi test possono includere simulazioni in ambiente controllato, test di identificazione e blocco di Virus e malware
Test di compatibilità	Questi tipi di test verificano la capacità dei dispositivi di funzionare correttamente con gli altri componenti dell'infrastruttura IT

8. Tabella riepilogativa dei servizi e relativi importi contrattuali

Codice articolo convenzione	Quantità	Durata (mesi)	Prezzo totale
CS2L3-NGFW-F3-FN	2		25.005,20€
CS2L3-MANLP-NGFW-F3-FN	2	12	875,18€
CS2L3-MANLP-NGFW-F3-FN	2	12	875,18€
CS2L3-SSAR-STA	50		13.500,00€
CS2L3-SSAN-STA	45		12.195,00€
CS2L3-SP-STA	50		15.500,00€
		TOTALE	**67.950,56€**

9. Prestazioni subappalto

Nell'ambito dell'Accordo Quadro Cybersecurity 2 le prestazioni erogate in subappalto nel presente piano operativo sono le seguenti:

- Supporto Specialistico;
- Manutenzione;