SISTEMA SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

N. 412 **del** 29/03/2024

OGGETTO: Adesione all'Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi - Lotto 3 Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi - Lotto PAL Centro Sud" (Cig madre 88980918FA) - ID 2367" con il Fornitore RTI TELECOM ITALIA S.p.A., per l'affidamento di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt, servizi di supporto specialistico e servizio di manutenzione, per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 599.815,52 Iva esclusa (€ 731.774,93 Iva inclusa) per 24 mesi, dal 01/05/2024 fino al 30/04/2026.

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO PATRIMONIALE - UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE

Centro di Costo: BD07 L'Estensore:Dott.ssa SERENA SBRIGLIO Il presente Atto non contiene dati sensibili

Il Dirigente e/o il Responsabile del procedimento, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attestano che l'atto è legittimo nella forma e nella sostanza.

Il Responsabile del Procedimento	UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE	DIPARTIMENTO TECNICO PATRIMONIALE
Dott. MASSIMILIANO COLTELLACCI	Dott. MASSIMILIANO COLTELLACCI	Ing. PAOLA BRAZZODURO
Firmatario: MASSIMILIANO COLTELLACCI Data: 14/03/2024 11:45:51 CET	Firmatario: MASSIMILIANO COLTELLACCI Data: 14/03/2024 11:46:27 CET	Firmatario: PAOLA BRAZZODURO Data: 14/03/2024 14:14:36 CET

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso comporta uno scostamento sfavorevole rispetto al budget economico assegnato come di seguito dettagliato per singolo conto:

Costo previsto	Eserciz.	CE/CP	Numero conto	Descrizione conto	Addetto al controllo	Scostamento
€288.995,34	2024	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	Si
€431.278,82	2024	CP	101020997	Hardware e Attrezzature EDP	Dott. Massimiliano Coltellacci	No
€8.625,58	2025	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No
€2.875,19	2026	CE	502020106	Servizi di Assistenza Informatica	Dott. Massimiliano Coltellacci	No

Il Funzionario addetto al controllo di budget

Dott. MASSIMILIANO COLTELLACCI

Firmatario: MASSIMILIANO COLTELLACCI
Data: 14/03/2024 11:47:38 CET

Il Dirigente della UOC Pianificazione Strategica, Programmazione e Controllo di Gestione con la sottoscrizione del presente atto attesta la coerenza della dichiarazione riferita alla spesa, di cui al presente provvedimento del "funzionario addetto al controllo del budget", rispetto alla delibera n. 176 del 13/02/2024

Firmatario: MIRELLA PERACCHI
Data: 21/03/2024 14:11:30 CET

Il Dirigente della UOC Bilancio e Contabilità con la sottoscrizione del presente atto attesta la non copertura economico/finanziaria dei fondi finalizzati e quindi la spesa pari a € 431,278.82 iva compresa graverà interamente, ai sensi del D.Lgs.118/2011, sul FSR 2024.

Firmatario: STEFANIA DI CARLO
Data: 25/03/2024 13:19:15 CET

Parere del Direttore Amministrativo Dr.ssa Roberta Volpini

Favorevole

Firmatario: ROBERTA VOLPINI
Data: 27/03/2024 10:37:33 CET

(con motivazioni allegate al presente atto)
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 28/03/2024 15:56:52 CET

(con motivazioni allegate al presente atto)
Non favorevole

Il presente provvedimento si compone di n.38 pagine di cui n. 31 pagine di allegati

Il Commissario Straordinario
Dr. Giuseppe Quintavalle

Firmatario: GIUSEPPE QUINTAVALLE
Data: 29/03/2024 12:53:19 CET

REGIONE LAZIO

IL DIRETTORE SOSTITUTO DELLA U.O.C. SISTEMI E TECNOLOGIE INFORMATICHE E DI COMUNICAZIONE

VISTA la deliberazione del Commissario Straordinario n. 1 del 1° gennaio 2016, con la quale si è provveduto a prendere atto dell'avvenuta istituzione dell'Azienda Sanitaria Locale Roma 1 a far data dal 1° gennaio 2016, come previsto dalla legge regionale n. 17 del 31.12.2015 e dal DCA n. 606 del 30.12.2015;

VISTO il Decreto del Presidente della Regione Lazio T00013 del 5 aprile 2023 con il quale è stato nominato Commissario Straordinario dell'Azienda Sanitaria Locale Roma 1, il dott. Giuseppe Quintavalle;

VISTO l'Atto di Autonomia Aziendale, approvato con deliberazione n. 1153 del 17/12/2019, recepito con DCA U00020 del 27/01/2020, pubblicato sul BURL del 30/01/2020 n. 9 con il quale, tra l'altro, è stato istituito il Dipartimento Tecnico Patrimoniale di cui fa parte la U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione;

RICHIAMATA la Deliberazione n. 179 del 27/02/2020, avente ad oggetto "Atto aziendale dell'ASL Roma 1, approvato con Deliberazione n. 1153 del 17/12/2019 – Presa d'atto dell'esito positivo del procedimento di verifica regionale – Attuazione del nuovo modello organizzativo" la quale prevede l'attivazione del sopra citato Dipartimento e delle UU.OO.CC. nello stesso ricomprese;

VISTA la Delibera n. 347 del 08/07/2022 avente ad oggetto "*Sistema aziendale di deleghe e conseguente individuazione delle competenze nell'adozione degli atti amministrativi*" con la quale, tra l'altro, sono state individuate le competenze nell'adozione degli atti amministrativi

VISTO il D.LGS. 36 del 31 marzo 2023 "Codice dei contratti pubblici" nel quale è previsto, all'art. 226 comma 2, che a decorrere dalla data in cui il codice acquista efficacia ai sensi dell'articolo 229, comma 2, le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi ai procedimenti in corso e che per procedimenti in corso, rientrano, tra gli altri, le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia;

PREMESSO che con Delibera n. 908 del 25/10/2023 l'azienda ASL Roma 1 ha approvato il Documento Unico di Programma triennale degli acquisti di beni e servizi (anni 2024 - 2026) ed il Programma triennale dei lavori (anni 2024 - 2026) dell'azienda medesima, ai sensi e per gli effetti dell'art. 37 del D.Lgs. 36/2023;

che con DGR n. 958 del 22.12.2023, la Regione Lazio ha adottato il Piano biennale 2024-2025 degli acquisti di beni e servizi ai sensi degli articoli 498-bis e 498-ter del Regolamento Regionale n. 1/2002 e s.m.i.;

che l'Azienda Sanitaria Locale Roma 1 ha dimostrato sensibilità sul tema CyberSecurity ovvero la volontà di fornire servizi online con un'adeguata sicurezza del dato;

che per migliorare la sicurezza e la gestione della propria infrastruttura, soprattutto nell'ambito delle connettività infra-sito, l'Asl intende realizzare un'architettura basata su SDWAN, che offra sicurezza di nuova generazione e funzionalità di rete per migliorare l'efficienza della WAN senza

compromettere la sicurezza, garantendo lo stesso livello di funzionalità fornito dai fornitori di SD-WAN pure-play, supportando tutti i casi d'uso comuni, con sicurezza avanzata integrata in un'unica offerta;

che nell'ambito del progetto saranno dunque analizzate sedi coinvolte nella infrastruttura SDWAN con i rispettivi servizi e la loro tipologia, il numero di utenti stimato e di porte ethernet presenti in ogni sede, la larghezza di banda disponibile per dimensionare un'infrastruttura adeguata a gestire correttamente la rete in ogni presidio;

che per ogni sede sarà prevista l'alta affidabilità, quindi, sarà ridondato l'apparato indicato e verrà creato un cluster;

CONSIDERATO che tutti i servizi esposti all'interno della rete sono ospitati in gran parte presso il CED del Presidio Ospedaliero Santo Spirito in Sassia ove si continuerà ad applicare la logica di breakout verso internet dove il cliente dispone di un'installazione in esercizio di un cluster FortiGate su apparati 1800F;

che una eventuale seconda connessione internet futura su ogni presidio coinvolto nella rete SD-WAN potrà abilitare successivamente il breakout locale verso internet dei servizi da raggiungere senza utilizzare la rete internet dell'HUB e che l'architettura SDWAN realizzata sarà di tipo Hub e Spoke su tecnologia Fortinet in cui la sede del presidio ospedaliero Santo Spirito costituirà l'Hub e gli altri punti individuati gli spoke;

TENUTO CONTO che la vigente normativa in materia di acquisizione beni e servizi, come da ultimo modificata dalla legge 28 dicembre 2015, n. 208, prevede l'obbligo per gli Enti del SSN:

- di approvvigionarsi utilizzando le convenzioni stipulate dalle centrali regionali di riferimento ovvero, qualora non siano operative convenzioni regionali, le convenzioni-quadro stipulate da Consip S.p.A.; (art. 1, comma 449, l. 296/2006; art. 1 comma 548, l. 208/2015);

ATTESTATO che sul portale Acquistinretepa.it è presente l'Accordo Quadro avente ad oggetto l'affidamento di "Cybersecurity 2 - prodotti e servizi connessi - Lotto 3 Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – Lotto PAL Centro Sud" (Cig madre 88980918FA) – ID 2367", attivo dal 22/02/2023;

che l'Azienda intende avvalersi del predetto accordo quadro Consip e che pertanto ha presentato il proprio piano dei fabbisogni;

che l'aggiudicatario RTI TELECOM ITALIA S.p.A. ha prodotto il Piano Operativo allegato alla presente (ALL. 1);

che l'Azienda provvederà pertanto, in conformità con quanto prescritto dall'accordo quadro a stipulare con l'Operatore Economico aggiudicatario un contratto esecutivo per la durata di mesi 24 (dal 01/05/2024 fino al 30/04/2026) e per un importo complessivo di € 599.815,52 Iva esclusa pari ad € 731.774,93 Iva inclusa, in conformità al piano operativo allegato;

DATO ATTO che, come previsto dalla normativa sulla tracciabilità dei flussi finanziari, di cui alla legge n. 136/2010, si ottempererà alla generazione del CIG

derivato sulla piattaforma acquistinretepa col perfezionamento dell'ordine definitivo;

che il costo complessivo derivante dal presente provvedimento, pari ad € 599.815,52 Iva esclusa pari ad € 731.774,93 Iva inclusa, verrà imputata cosi come di seguito dettagliato:

- € 288.995,34 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2024
- € 8.624,58 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2025
- € 2.875,19 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2026
- € 431.278,82 iva inclusa - C.P 101020997 "Hardware e Attrezzature EDP" – Bilancio 2024

che si rinvia a successiva determinazione della struttura, l'imputazione e la liquidazione delle spese dovute per la corresponsione degli incentivi per Funzioni tecniche relativi alla presente procedura, ai sensi dell'art. 113 del D.lgs. n. 50/2016 approvato con Delibera n. 13 del 19/04/2022, ad esito dell'acquisizione della relazione del RUP sulla gestione della medesima procedura di gara;

che, pertanto, per il CE 50.20.20.106 l'anno 2024 presenta la seguente situazione economica:

Budget assegnato		€ 17.479.206,00
Budget già impegnato		€ 19.048.867,40
Importo impegnato con il presente atto		€ 288.995,34
Scostamento	-	€ 1.858.656,74

RITENUTO che con riferimento allo scostamento negativo, si precisa che lo stesso deriva dalla contabilizzazione di contratti avviati, la cui spesa per l'anno in corso, a fronte del budget definitivo assegnato ai CCS con deliberazione n. 176 del 13/02/2024, non può essere ridotta;

che il risparmio di spesa per la suindicata copertura si avrà sul nuovo assetto software cartella clinica e order entry relativo alla delibera n. 368 del 24/03/2023;

ATTESO che il Responsabile del Procedimento è il Dott. Massimiliano Coltellacci, Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione, cui compete la verifica e l'accertamento della regolarità e qualità della fornitura resa, anche ai fini della liquidazione;

che si ritiene opportuno nominare, ai sensi e per gli effetti dell'art. 101 del d.lgs. n. 50/2016, quale DEC per la procedura in oggetto, il Sig. Stefano Scaramuzzino e quale Assistente Dec la D.ssa Michela Mazzotta afferenti alla U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione;

ATTESTATO che il presente provvedimento a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge n. 241/1990 e successive modifiche ed integrazioni;

PROPONE

Per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi - Lotto 3 Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – Lotto PAL Centro Sud" (Cig madre 88980918FA) – ID 2367" con il Fornitore RTI TELECOM ITALIA S.p.A., per l'affidamento di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt, servizi di supporto specialistico e servizio di manutenzione, per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 599.815,52 Iva esclusa (€ 731.774,93 Iva inclusa) per per 24 mesi, dal 01/05/2024 fino al 30/04/2026.;

di dare atto che la spesa di € 731.774,93 iva inclusa, derivante dal presente provvedimento verrà imputato cosi come di seguito dettagliato:

- € 288.995,34 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2024
- € 8.624,58 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2025
- € 2.875,19 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2026
- € 431.278,82 iva inclusa - C.P 101020997 "Hardware e Attrezzature EDP" – Bilancio 2024

di nominare, ai sensi e per gli effetti dell'art. 101 del d.lgs. 50/2016, quale DEC per la procedura in oggetto, il Sig. Stefano Scaramuzzino e quale Assistente Dec la D.ssa Michela Mazzotta afferenti alla U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione;

di incaricare il Dirigente proponente, ad avvenuta adozione della presente delibera, di predisporre tutti gli atti conseguenti e necessari per dare avvio al contenuto di cui al presente provvedimento, ivi comprese le relative notifiche e/o comunicazioni all'Operatore Economico interessato;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile del procedimento	Il Direttore Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione	Il Direttore Dipartimento Tecnico Patrimoniale
Dott. Massimiliano Coltellacci	Dott. Massimiliano Coltellacci	Ing. Paola Brazzoduro

IL COMMISSARIO STRAORDINARIO

IN VIRTÚ dei poteri previsti:

- dall'art. 3 del D. Lgs 502/1992 e ss.mm.ii;
- dall'art. 8 della L.R. n. 18/1994 e ss.mm.ii;

nonché delle funzioni e dei poteri conferitigli con Decreto del Presidente della Regione Lazio n. T00013 del 5 aprile 2023;

Letta la proposta di delibera sopra riportata presentata dal Dirigente Responsabile dell'Unità in frontespizio indicata;

PRESO ATTO che il Direttore della Struttura proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge 241/1990 e successive modifiche ed integrazioni;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario riportati in frontespizio;

DELIBERA

di adottare la proposta di deliberazione avente per oggetto "*Adesione all'Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi - Lotto 3 Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – Lotto PAL Centro Sud" (Cig madre 88980918FA) – ID 2367" con il Fornitore RTI TELECOM ITALIA S.p.A., per l'affidamento di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt, servizi di supporto specialistico e servizio di manutenzione, per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 599.815,52 Iva esclusa (€ 731.774,93 Iva inclusa) per 24 mesi, dal 01/05/2024 fino al 30/04/2026.*" e conseguentemente, per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi - Lotto 3 Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – Lotto PAL Centro Sud" (Cig madre 88980918FA) – ID 2367" con il Fornitore RTI TELECOM ITALIA S.p.A., per l'affidamento di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt, servizi di supporto specialistico e servizio di manutenzione, per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 599.815,52 Iva esclusa (€ 731.774,93 Iva inclusa) per per 24 mesi, dal 01/05/2024 fino al 30/04/2026.;

di dare atto che la spesa di € 731.774,93 iva inclusa, derivante dal presente provvedimento verrà imputato cosi come di seguito dettagliato:

- € 288.995,34 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2024
- € 8.624,58 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2025
- € 2.875,19 iva inclusa - C.E 502020106 "Servizi di Assistenza Informatica" – Bilancio 2026
- € 431.278,82 iva inclusa - C.P 101020997 "Hardware e Attrezzature EDP" – Bilancio 2024

di nominare, ai sensi e per gli effetti dell'art. 101 del d.lgs. 50/2016, quale DEC per la procedura in oggetto, il Sig. Stefano Scaramuzzino e quale Assistente Dec la D.ssa Michela Mazzotta afferenti alla U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione;

di incaricare il Dirigente proponente, ad avvenuta adozione della presente delibera, di predisporre tutti gli atti conseguenti e necessari per dare avvio al contenuto di cui al presente provvedimento, ivi comprese le relative notifiche e/o comunicazioni all'Operatore Economico interessato;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile della struttura proponente provvederà all'attuazione della presente deliberazione curandone altresì la relativa trasmissione agli uffici/organi rispettivamente interessati.

Il COMMISSARIO STRAORDINARIO
Dr. Giuseppe Quintavalle
FIRMATO DIGITALMENTE

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

AQ CONSIP 2367 – LOTTO 3

ASL ROMA1

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	22/02/2024

Indice

1.INTRODUZIONE

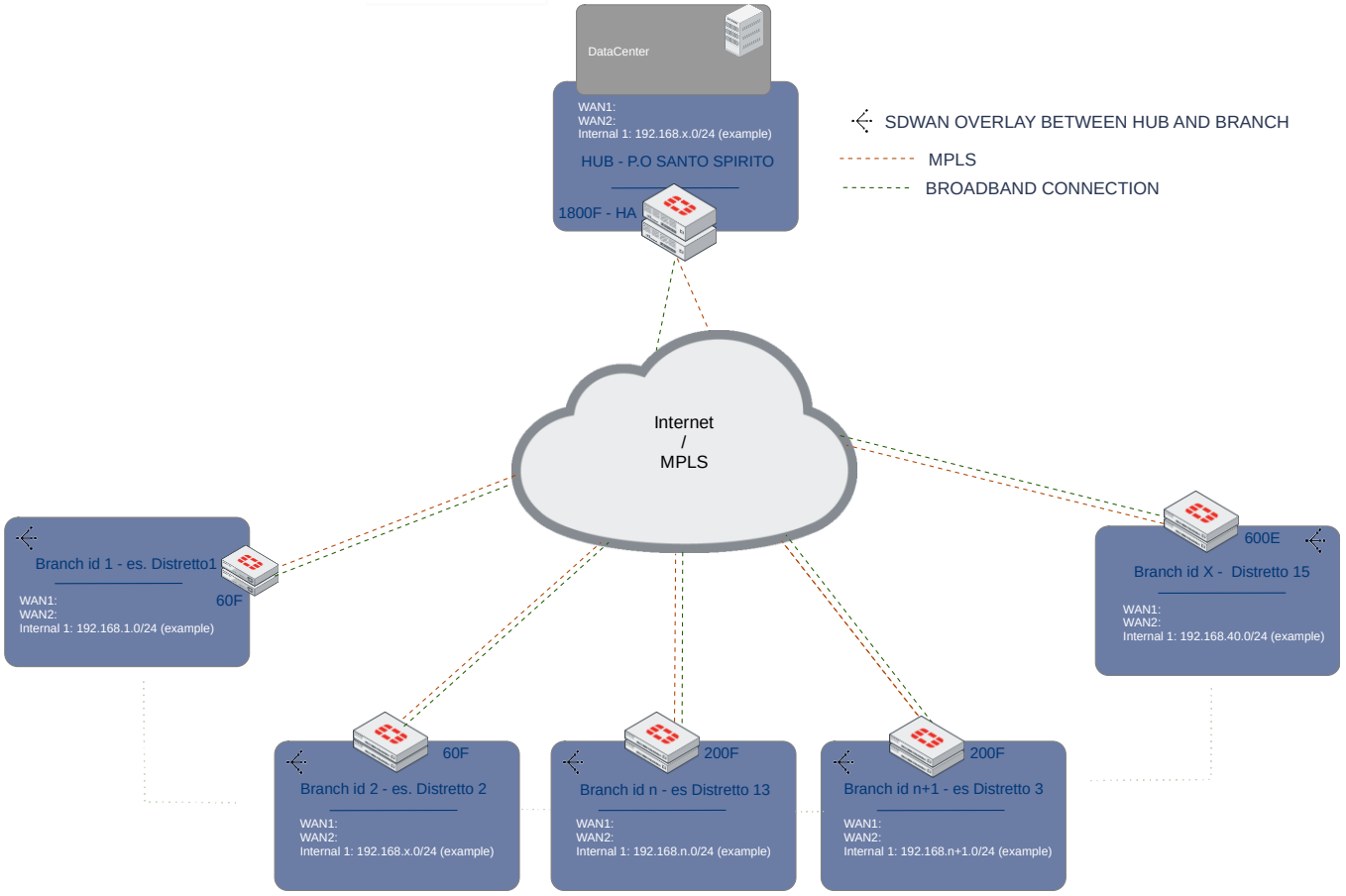
1.1 PREMESSA

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 **AZIENDA SANITARIA LOCALE ROMA 1**, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni allegato all'ODA 7636321 (Richiesta piano operativo).

> La mission aziendale dell'amministrazione contraente in ambito sanitario; l'amministrazione contraente ha dimostrato sensibilità sui temi CyberSecurity, temi sui quali è indispensabile un'accelerazione. Fornire servizi online a cittadini, imprese e professionisti ha infatti come prerequisito quello di una adeguata sicurezza del dato.

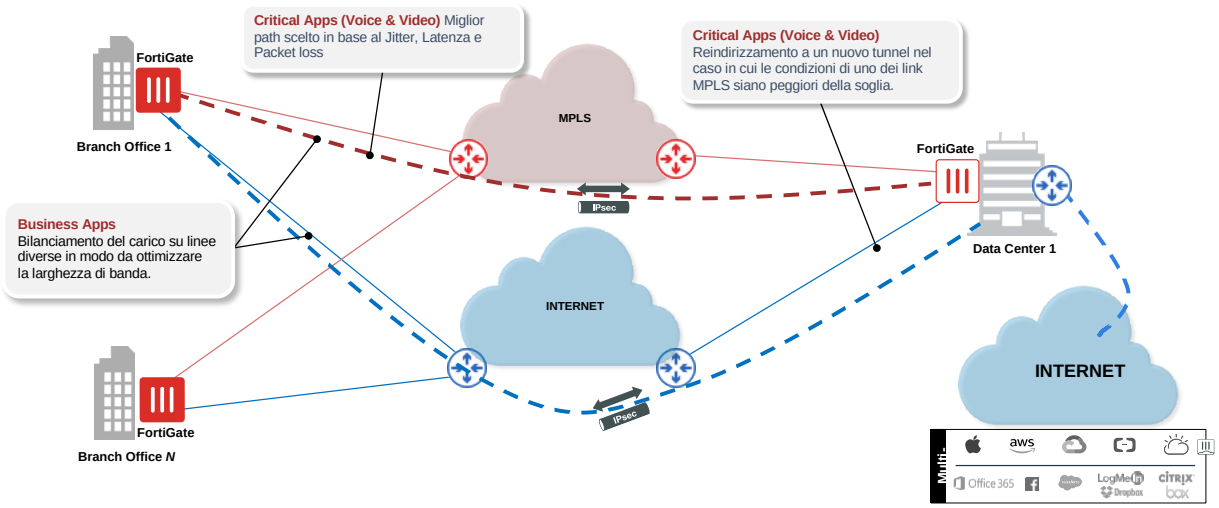
Per migliorare la sicurezza e la gestione della propria infrastruttura, soprattutto nell'ambito delle connettività infra-sito, l'amministrazione contraente intende realizzare un'architettura basata su SDWAN, che offra sicurezza di nuova generazione e funzionalità di rete per migliorare l'efficienza della WAN senza compromettere la sicurezza, garantendo lo stesso livello di funzionalità fornito dai fornitori di SD-WAN pure-play, supportando tutti i casi d'uso comuni, con sicurezza avanzata integrata in un'unica offerta.

Nell'ambito del progetto saranno dunque analizzate sedi coinvolte nella infrastruttura SDWAN con i rispettivi servizi e la loro tipologia, il numero di utenti stimato e di porte ethernet presenti in ogni sede, la larghezza di banda disponibile per dimensionare un'infrastruttura adeguata a gestire correttamente la rete in ogni presidio.
Per ogni sede sarà prevista l'alta affidabilità, quindi, sarà ridondato l'apparato indicato e verrà creato un cluster.
Tutti i servizi esposti all'interno della rete sono ospitati in gran parte presso il CED del presidio ospedaliero Santo Spirito ove si continuerà ad applicare la logica di breakout verso internet dove il cliente dispone di un'installazione in esercizio di un cluster FortiGate su apparati 1800F. Una eventuale seconda connessione internet futura su ogni presidio coinvolto nella rete SD-WAN potrà abilitare successivamente il breakout locale verso internet dei servizi da raggiungere senza utilizzare la rete internet dell'HUB.
L'architettura SDWAN realizzata sarà di tipo Hub e Spoke su tecnologia Fortinet in cui la sede del presidio ospedaliero Santo Spirito costituirà l'Hub e gli altri punti individuati gli spoke.
Di seguito l'High Level Design dell'architettura oggetto della presente proposta, rappresentato in uno schema di rete contenente sedi esemplificative che saranno arricchite dall'infrastruttura SDWAN:



Il potenziale che ne deriva sfruttando la soluzione tecnologica di SD-WAN di Fortinet in termini di utilizzo di tutti gli overlay intra-sito, privilegiando la qualità delle connessioni dei servizi critici al business, è rappresentato nella figura seguente, sintetizzata nella sede HUB del ASL-RM1 e 1-n sedi periferiche:

SD-WAN “ASL-RM1”



In maggior dettaglio nella tabella seguenti si riportano le sedi interessate dal progetto:

numero sede	SEDE (e/o via)
1	Via Garigliano
2	Via Tagliamento
3	Via Luzzatti
4	Via Lampedusa
5	Via Dei Frentani
6	Via Monte Rocchetta
7	Boncompagni
8	Clauzetto
9	LTV
10	TDQ
11	Castellani
12	Sabrata
13	Plinio
14	SZP
15	Presidio Via Cassia 721
16	Via Nomentana 2B
17	Via Tanaro
18	Boccea 271
19	Angelico
20	Largo Rovani 5
21	Ex Officine
22	Dina Galli3
23	Jacobini
24	Gasparri
25	Cassia 472
26	Via Canova
27	Via Tripoli
28	De Sanctis
29	Farnesina
30	Via Carducci
31	Silveri
31	Di Giorgio
33	Sala Puccinotti (c/o San Giovanni in Laterano)
34	Tornabuoni
35	Montesanto
36	Via Palestro
37	Baccini
38	MonteTomatico
39	Tenente Eula
40	Ventura
41	Anguillarese
42	Catone
43	Angelo EMO
44	Lablache 4

45	Riari
46	Cesano
47	Castel Di Giudo
48	Nomentana 338
49	Fornovo
50	Via Dina Galli 8
51	Via Piatti 19
52	Via dei Latini
53	Cassia 5
54	Igino Papa
55	Via della Lungara (Regina Coeli)
56	Lablache 36
57	Pasquariello
58	Cappellari
59	Montesacro
60	Casal Piombino
61	Forte Antenne
62	Innocenzo Iv
63	Aurelia 257
64	Barellai
65	Largo Lumiere
66	Montecatini 8
67	Quarrata 15
68	Borromeo
69	Montecitorio
70	Farulli
71	Olimpionici
72	Vittor Pisani
73	Dataria 96
74	Baccina 81
75	Bramante 6
76	Prima Porta
77	Oslavia
78	Quarrata 7 int.1
79	Turchia
80	Galline Bianche
81	Quarrata 7 int.2
82	Data Center PSN

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 - allegato all'ODA 7636321
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)**

[redacted]

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**

[redacted]

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**

[redacted]

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
X Servizi	X 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
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)
	X 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
X Sicurezza Informatica	□ Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	X 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

• la durata del Contratto Esecutivo

• informazione tecniche quali:

- informazioni riguardanti l'Hardware di ogni apparato. Per ogni tipologia di apparato indicare, il codice prodotto e la descrizione di ogni elemento costituente;

- informazioni riguardanti il Software di ogni apparato. Per ogni tipologia di apparato riportare, la release software configurata e l'elenco di tutte le patch correttive installate

- configurazioni previste;

- 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

- schemi logici dell'architettura

- 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
- 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

- l'elenco di eventuali deliverable di fornitura

- il cronoprogramma, riportante i tempi previsti per l'esecuzione delle attività e dei servizi richiesti in accordo con l'Amministrazione Contraente, evidenziando anche le tempistiche legate a eventuali attività propedeutiche a carico dell'Amministrazione. I tempi che saranno concordati, una volta approvati, dovranno essere rispettati pena l'applicazione delle penali, riportate nel Capitolato Tecnico- Parte Speciale capitolo 6. Si precisa che è facoltà dell'Amministrazione concordare con il Fornitore la possibilità di effettuare rilasci successivi in caso di forniture di particolare complessità, o in base a esigenze manifestate dall'Amministrazione

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

  inserire per ciascuna sede dell'Amministrazione indirizzo della sede e nominativo e contatti (cellulare e mail) del Referente tecnico della sede;

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

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

- le prestazioni che si intende subappaltare, nel rispetto delle previsioni dell'Accordo Quadro e di quanto indicato nel Piano dei fabbisogni;

- 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

BRAND	DENOMINAZIONE BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
NGFW	Fortinet	2	NGFW-F2-FN	FG-200F-BDL-C	6
NGFW	Fortinet	1	NGFW-F1-FN	FG-60F-BDL-C	100
NGFW	Fortinet	3	NGFW-F3-FN	FG-600E-BDL-C	2
NGFW	Fortinet	5	NGFW-F5-FN	FG-2600F-BDL-C	2
NAC	Fortinet	4	NAC-F4-FN	FNC-CA-700C-BDL-C1	1

4.1 NAC - FORTINAC

La soluzione FortiNAC di Fortinet si integra con numerosi dispositivi sia all'interno dell'**ecosistema Fortinet** (Security Fabric) sia all'interno di un panorama molto ampio di **soluzioni di sicurezza di terze parti**: a questo riguardo è bene precisare che le soluzioni di terze parti documentate non esauriscono il perimetro di integrabilità in quanto il **FortiNAC ha dei meccanismi di integrazione basati su protocolli standard** che permettono di estendere visibilità e il controllo degli accessi a qualsiasi soluzione di network-security sia presente presso le Amministrazioni.
Per quanto riguarda **l'ecosistema Fortinet**, una delle principali integrazioni avviene con il **NGFW FortiGate** di Fortinet ed in particolare riguarda **due aspetti che ne evidenziano la bidirezionalità** dell'interazione:

- **Fortinet Single Sign On (FSSO) per applicazione dinamica delle policy basate su autenticazione**: Il FortiNAC in questo caso, dopo aver autenticato l'utente e aver fatto eventuali controlli posturali, può agire da collector agent ed informare in real-time il NGFW attraverso un meccanismo proprietario basato su tag: in questo modo eventi di logon/logoff oppure di cambio di stato posturale del dispositivo endpoint fanno cambiare dinamicamente le policy di autorizzazione e quindi l'associazione dell'endpoint e dell'utente a gruppi di FSSO diversi a cui sono associati criteri e ruoli di sicurezza diversi. Per l'utente tutti questi passaggi sono trasparenti e in questo modo è possibile gestire l'accesso alla rete realizzando quella che si chiama "**Intent Base Segmentation**" cioè la possibilità avere un controllo granulare degli accessi ma allo stesso tempo un continuo assessment di sicurezza delle PdL e della profilazione degli utenti.
- **Il secondo aspetto** riguarda la possibilità del FortiNAC **di automatizzare delle azioni di isolamento o contenimento/remediation** in seguito ad informazioni che vengono fornite dal NGFW di Fortinet: ad esempio, in seguito ad una segnalazione di sicurezza del NGFW (es. rilevazione botnet) è possibile istruire il NAC per isolare la PdL e fornirgli un captive portal in cui si spiega all'utente che è avvenuto un incidente di sicurezza ed è necessario chiamare l'helpdesk per un'attività di bonifica. Questo è un esempio di framework **ATR (Automated Threat Response)**, tutti i prodotti Fortinet supportano questo framework quindi si possono integrare con il FortiNAC.

L'integrazione con il **NGFW Palo Alto** è di **tipo bidirezionale** e può essere sintetizzata con i seguenti aspetti di comunicazione:

- Attraverso l'utilizzo di **API XML** il **FortiNAC** dialoga con il **NGFW di Palo Alto** per gestire gli utenti con politiche di Single Sign On per l'implementazione dinamica di policy di sicurezza basate su autenticazione.
- Tramite l'inoltro di log **dal NGFW di Palo Alto al FortiNAC** è possibile inviare notifiche o intraprendere azioni di contenimento sull'host associato, come disabilitare l'host (isolamento) o contrassegnarlo come a rischio.

L'integrazione con il **NGFW Checkpoint è di tipo bidirezionale** e può essere sintetizzata con i seguenti aspetti di comunicazione:

- Attraverso l'Integrazione **SSO** il **FortiNAC** consente di inviare Radius Accounting verso dispositivi di terze parti (**NGFW Checkpoint**) contenenti dati quali: ip address e username, che consentono di gestire in modo dinamico le autenticazioni sui suddetti dispositivi. L'integrazione con la

funzionalità di Checkpoint Identity Awarness consente di sfruttare il meccanismo di **radius accounting** per creare delle politiche dinamiche basate sull'autenticazione effettuata sul FortiNAC ed inviata tramite Radius ai dispositivi Checkpoint.

- Tramite l'inoltro di log **dal NGFW di Checkpoint al FortiNAC** è possibile **inviare notifiche** o intraprendere **azioni di contenimento** sull'host associato, come disabilitare l'host (isolamento) o contrassegnarlo come a rischio.

Per quanto riguarda **l'integrazione della soluzione FortiNAC con prodotti di terze parti** e in particolare con soluzioni di sicurezza, l'integrazione segue il concetto già espresso del framework **ATR (Automated Threat Response)** che è **nativo per i prodotti Fortinet** e nativo per alcune terze parti (es. **Palo Alto, FireEye**) ma può essere comunque sfruttato per qualsiasi sistema di terze parti che supporti il protocollo standard *syslog*. La differenza di avere il supporto nativo risiede nel fatto che all'interno del FortiNAC sono già presenti i *parser* relativi alla tecnologia da integrare, questo non esclude la possibilità di effettuare manualmente il *parser* dei log di soluzioni di terze parti anche non documentate.
Il sistema ATR serve a correlare le informazioni di sicurezza che provengono dai prodotti che si vuole integrare, tali informazioni vengono normalizzate e utilizzate per intraprendere azioni di isolamento, limitazione o blocco degli endpoint compromessi per ridurre il tempo di contenimento di una minaccia. È quindi possibile decidere se intraprendere un'azione automatica oppure mandare esclusivamente un allarme per intraprendere una indagine manuale.
Le tecnologie integrabili **con il FortiNAC** possono essere classificate in **gruppi di categorie merceologiche**, per ognuna delle quali si fornisce di seguito un elenco con una breve descrizione relativa all'integrazione. **Tali tecnologie sono state validate reciprocamente in test di laboratorio sia da Fortinet sia dal vendor della tecnologia integrata.**

- **Network Infrastructure:** Integrazione di controllo degli accessi su rete cablata e Wireless, con possibilità di isolamento, limitazioni e blocco dell'accesso: **Adtran, Aerohive, AlaxalA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC,Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel,Juniper, NEC, Riverbed/Xirrus, and SonicWall.**
- **Security Infrastructure:** In questo caso è possibile sfruttare l'integrazione per analizzare e correlare eventi di sicurezza, fornendo un'azione di contenimento in seguito ad allarmi di sicurezza: **Fortinet, Palo Alto, CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper, Qualys, Sonicwall, Tenable.**
- **Authentication and Directory Services**: Integrazione necessaria per utilizzare database esterni di utenti per finalità di autenticazione e Single Sign On: **RADIUS-Cisco ACS, Free RADIUS, Microsoft IAS, LDAP-Google SSO, Microsoft Active Directory, Open LDAP**.
- **Sistemi operativi:** In questo caso l'integrazione riguarda il riconoscimento ed eventuali azioni di controllo posturale, ad esempio la possibilità di impedire l'accesso in rete a sistemi operativi deprecati o fuori supporto, oppure in modo più granulare impedire l'accesso in rete se non si ha una particolare patch/service pack: **Android, Apple MAC OSX and iOS, Linux, Microsoft Windows**
- **Endpoint Security Applications (software antivirus):** L'integrazione permette di **riconoscere i software antivirus** per il controllo posturale delle PdL e di **verificarne l'aggiornamento dei database di sicurezza** (es. firme antivirus) prima dell'accesso in rete: ad esempio è possibile impedire l'accesso in rete se una PdL non ha software antivirus a bordo, oppure se non aggiorna le firme da un periodo temporale definibile dall'amministratore del FortiNAC: **Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm**.
- **MDM (Mobile Device Management):** L'integrazione con i prodotti di gestione dei dispositivi mobili è fondamentale per **accelerare il processo di registrazione** dei dispositivi aziendali e distinguerli facilmente da dispositivi mobili personali, **diversificandone le politiche di accesso; AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF.**

Le metodologie di integrazione e la varietà di azioni e servizi che possono essere erogati possono variare di caso in caso, e vengono descritte nelle relative documentazioni e white paper.

Per **ulteriori integrazioni con terze parti,** la soluzione FortiNAC comprende un **completo set di REST API** che consente di gestire il FortiNAC da un orchestratore esterno in modo da poter **creare/modificare** configurazioni, **importare/esportare dati, gestire la profilazione degli amministratori, gestire i log** e numerose altre funzionalità per il corretto inquadramento del prodotto all'interno di un processo di automazione con terze parti. La libreria API è pubblica e può essere consultata al link:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9aace04f-688f-11ea-9384-00505692583a/FortiNAC_REST_Schema_pdf.pdf

4.2 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.

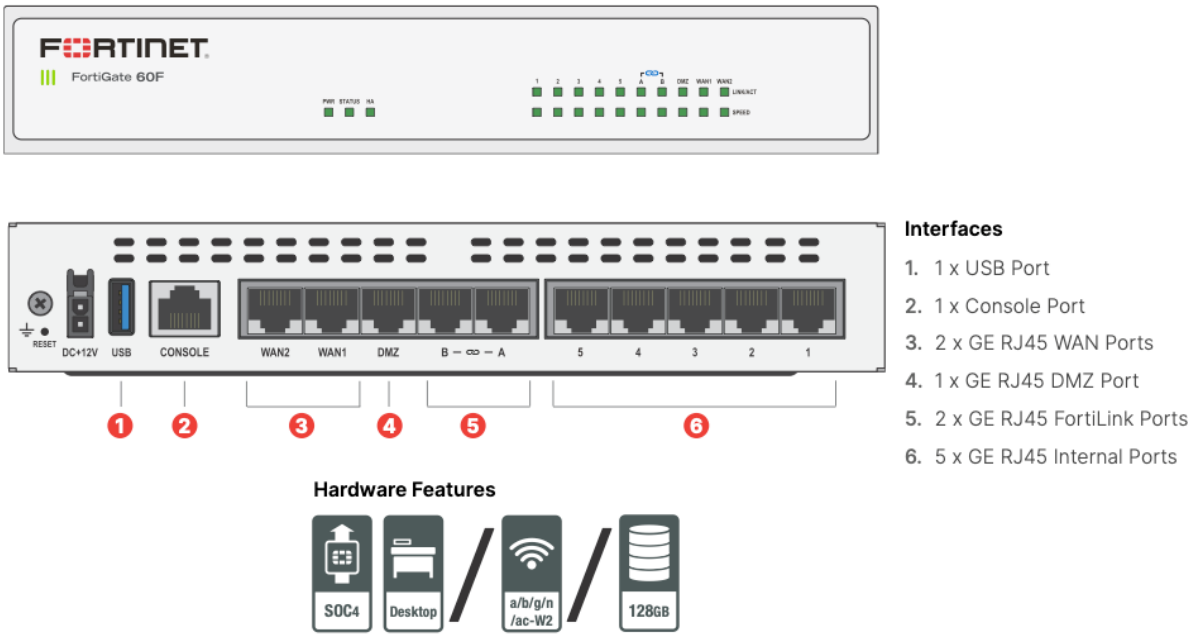
Gli apparati fisici installati on-premise presso la sede dell'Amministrazione contraente, permettono la visibilità completa del traffico attraverso la gestione di indirizzi IP, utenti e dispositivi con la possibilità di creare policy di sicurezza con una combinazione di questi fattori.

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.

Brand 1 – Fortinet – Apparato di Fascia 1

All'interno di questa fascia viene proposto il modello FortiGate-60F, di seguito sono riportate le caratteristiche tecniche dell'apparato.

FortiGate-60F:



Front-Back FortiGate-60F

Di seguito si riportano le caratteristiche tecniche principali dell'apparato; per ulteriori informazioni si può far riferimento al datasheet del FortiGate-60F (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf).

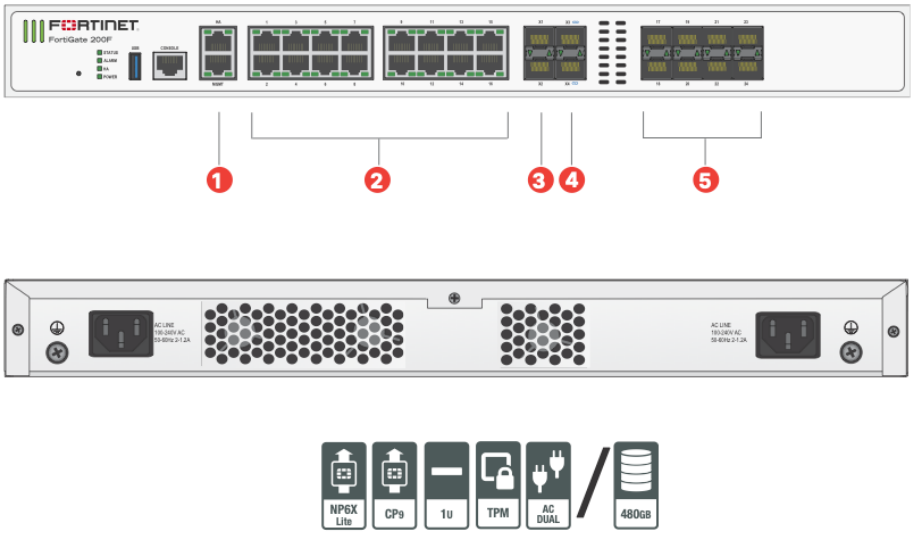
	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1.4 Gbps			
NGFW Throughput [2, 4]	1 Gbps			
Threat Protection Throughput [2, 5]	700 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps			
Firewall Latency (64 byte UDP packets)	3.3 µs			
Firewall Throughput (Packets Per Second)	9 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	900 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps			
CAPWAP Throughput (HTTP 64K)	8 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	24			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3			
Height x Width x Length (mm)	38.5 × 216 × 160 mm			
Weight	2.23 lbs (1.01 kg)			
Form Factor	Desktop			
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Caratteristiche tecniche FG-60F

Brand 1 – Fortinet – Apparato di Fascia 2

All'interno di questa fascia viene proposto il modello FortiGate-200F, di seguito sono riportate le caratteristiche tecniche dell'apparato.

FortiGate-200F:



Interfaces

1. 2 x GE RJ45 HA/ MGMT Ports
2. 16 x GE RJ45 Ports
3. 2 × 10 GE SFP+ Slots
4. 2 × 10 GE SFP+ FortiLink Slots
5. 8 x GE SFP Slots

Front-Back FortiGate-200F

Di seguito si riportano le caratteristiche tecniche principali dell'apparato; per ulteriori informazioni si può far riferimento al datasheet del FortiGate-200F (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-200f-series.pdf).

	FORTIGATE 200F	FORTIGATE 201F
Interfaces and Modules		
GE RJ45 Ports	16	
GE RJ45 Management / HA	1 / 1	
GE SFP Slots	8	
10 GE SFP+ FortiLink Slots (default)	2	
10 GE SFP+ Slots	2	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Trusted Platform Module (TPM)	Yes	
Bluetooth Low Energy (BLE)	Yes	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	5 Gbps	
NGFW Throughput [2, 4]	3.5 Gbps	
Threat Protection Throughput [2, 5]	3 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	27 / 27 / 11 Gbps	
Firewall Latency (64 byte, UDP)	4.78 µs	
Firewall Throughput (Packet per Second)	16.5 Mpps	
Concurrent Sessions (TCP)	3 Million	
New Sessions/Second (TCP)	280 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	13 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput	2 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	3500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300 000	
Application Control Throughput (HTTP 64K) [2]	13 Gbps	
CAPWAP Throughput (HTTP 64K)	20 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel)	256 / 128	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

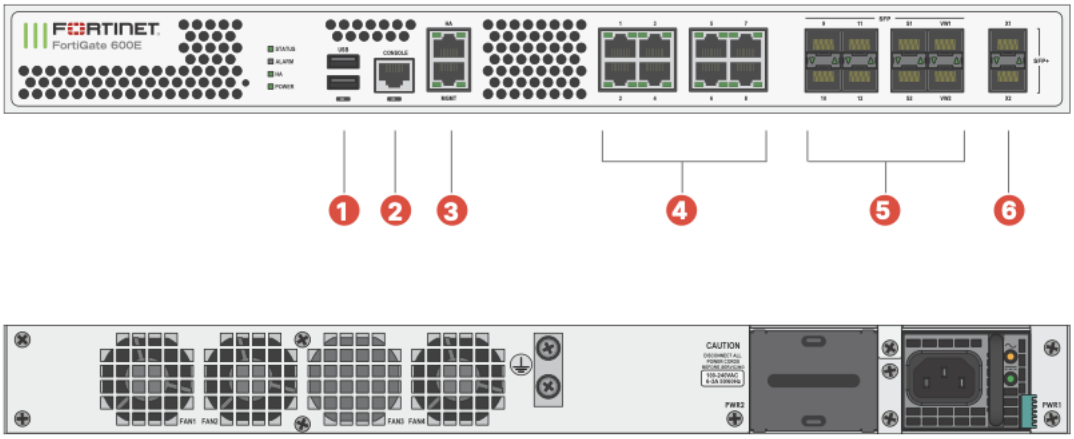
	FORTIGATE 200F	FORTIGATE 201F
Dimensions and Power		
Height x Width x Length (inches)	1.73 × 17.01 × 13.47	
Height x Width x Length (mm)	44 × 432 × 342	
Weight	9.92 lbs (4.5 kg)	10.14 lbs (4.6 kg)
Form Factor (supports EIA/non-EIA standards)	Ear Mount, 1 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	101.92 W / 118.90 W	104.52 W / 121.94 W
Current (Maximum)	100V / 2A, 240V / 1.2A	
Heat Dissipation	405.70 BTU/h	436.98 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	20%–90% non-condensing	
Noise Level	49.9 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certification	USGv6/IPv6	

Caratteristiche tecniche FG-200F

Brand 1 – Fortinet – Apparato di Fascia 3

All'interno di questa fascia viene proposto il modello FortiGate-600E, di seguito sono riportate le caratteristiche tecniche dell'apparato.

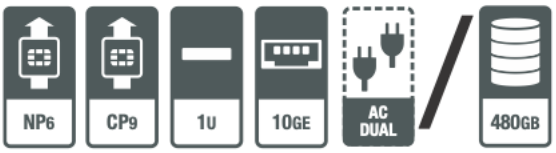
FortiGate-600E:



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



Front-Back FortiGate-600E

Di seguito si riportano le caratteristiche tecniche principali dell'apparato; per ulteriori informazioni si può far riferimento al datasheet del FortiGate-600E (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf).

	FG-600E	FG-601E
Interfaces and Modules		
Hardware Accelerated 10 GE SFP+ Slots	2	
Hardware Accelerated GE RJ45 Interfaces	8	
Hardware Accelerated GE SFP Slots	8	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Onboard Storage	0	2× 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	10 Gbps	
NGFW Throughput [2, 4]	9.5 Gbps	
Threat Protection Throughput [2, 5]	7 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps	
Firewall Latency (64 byte, UDP)	1.54 µs	
Firewall Throughput (Packet per Second)	40.5 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	450 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput	7 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10 000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	5500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800 000	
Application Control Throughput (HTTP 64K) [2]	15 Gbps	
CAPWAP Throughput (HTTP 64K)	18 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	96	
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-600E	FG-601E
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	16.1 lbs (7.3 kg)	16.6 lbs (7.5 kg)
Form Factor	Rack Mount, 1 RU	
Power Source	100–240V, 50/60 Hz	
Power Consumption (Average / Maximum)	129 W / 244 W	
Current (Maximum)	6A@100V	
Heat Dissipation	832 BTU/h	
Redundant Power Supplies (Hot Swappable)	Optional	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	10%–90% non-condensing	
Noise Level	59 dBA	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 9843 ft (3000 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

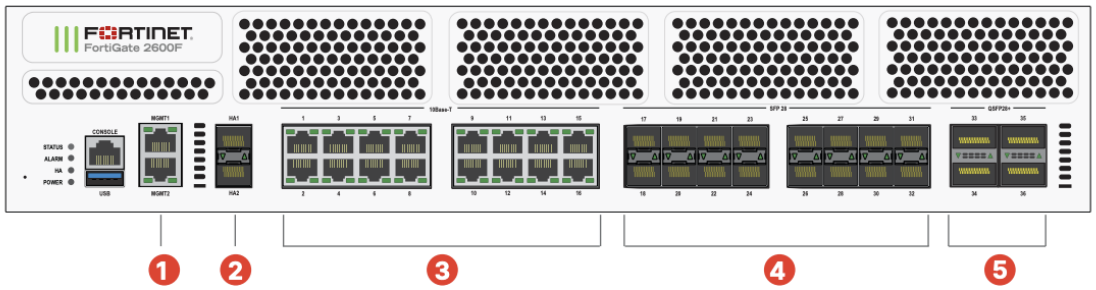
Caratteristiche tecniche FG-600E

Brand 1 – Fortinet – Apparato di Fascia 5

All'interno di questa fascia viene proposto il modello FortiGate-2600F, di seguito sono riportate le caratteristiche tecniche dell'apparato.

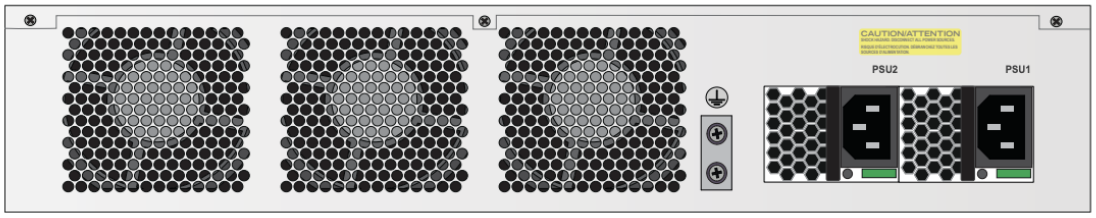
FortiGate-2600F:

FortiGate 2600F Series

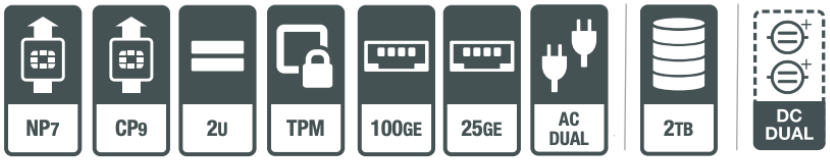


Interfaces

1. 2 x GE RJ45 MGMT Ports
2. 2 × 10 GE SFP+ / GE SFP HA Slots
3. 16 × 10 GE / GE RJ45 Ports
4. 16 × 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
5. 4 × 100 GE QSFP28 / 40 GE QSFP+ Slots



Hardware Features



Di seguito si riportano le caratteristiche tecniche principali dell'apparato; per ulteriori informazioni si può far riferimento al datasheet del FortiGate-2600F (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-2600f-series.pdf).

Specifications

	FG-2600F/-DC	FG-2601F/-DC
Interfaces and Modules		
Hardware Accelerated 10 GE / GE RJ45 Ports	16	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	16	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	4	
Hardware Accelerated 10 GE SFP+ / GE SFP HA Slots	2	
GE RJ45 Management Ports	2	
USB 3.0 Port	1	
Console RJ45 Port	1	
Onboard Storage	0	2× 1 TB NVMe SSD
Trusted Platform Module (TPM)	Yes	
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	31 Gbps	
NGFW Throughput [2, 4]	27 Gbps	
Threat Protection Throughput [2, 5]	25 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	198 / 196 / 140 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	198 / 196 / 140 Gbps	
Firewall Latency (64 byte, UDP)	3.41 µs	
Firewall Throughput (Packet per Second)	210 Mpps	
Concurrent Sessions (TCP)	24 Million / 40 Million*	
New Sessions/Second (TCP)	1 Million / 2 Million*	
Firewall Policies	100 000	
IPsec VPN Throughput (512 byte)[1]	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20 000	
Client-to-Gateway IPsec VPN Tunnels	100 000	
SSL-VPN Throughput	16 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	
SSL Inspection Throughput (IPS, avg HTTPS)[3]	20 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS)[3]	16 000	
SSL Inspection Concurrent Session (IPS, avg HTTPS)[3]	2.7 Million	
Application Control Throughput (HTTP 64K)[2]	64 Gbps	
CAPWAP Throughput (HTTP 64K)	62.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	196	
Maximum Number of FortiAPs (Total /Tunnel)	4096 / 2048	
Maximum Number of FortiTokens	20 000	
Maximum Number of Registered FortiClients	20 000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-2600F/-DC	FG-2601F/-DC
Dimensions and Power		
Height x Width x Length (inches)	3.5 × 17.25 × 21.1	
Height x Width x Length (mm)	88.4 × 438 × 536	
Weight	30.6 lbs (13.9 kg)	30.9 lbs (14.0 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU	
AC Power Supply	100–240VAC, 47/63 Hz	
Power Consumption (Average / Maximum)	416 W / 510 W	420.3 W / 513.7 W
Current (Maximum)	6A	
Heat Dissipation	1740 BTU/h	1754 BTU/h
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 90% non-condensing	
Noise Level	71.72 dBA	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

* Requires Hyperscale Firewall License

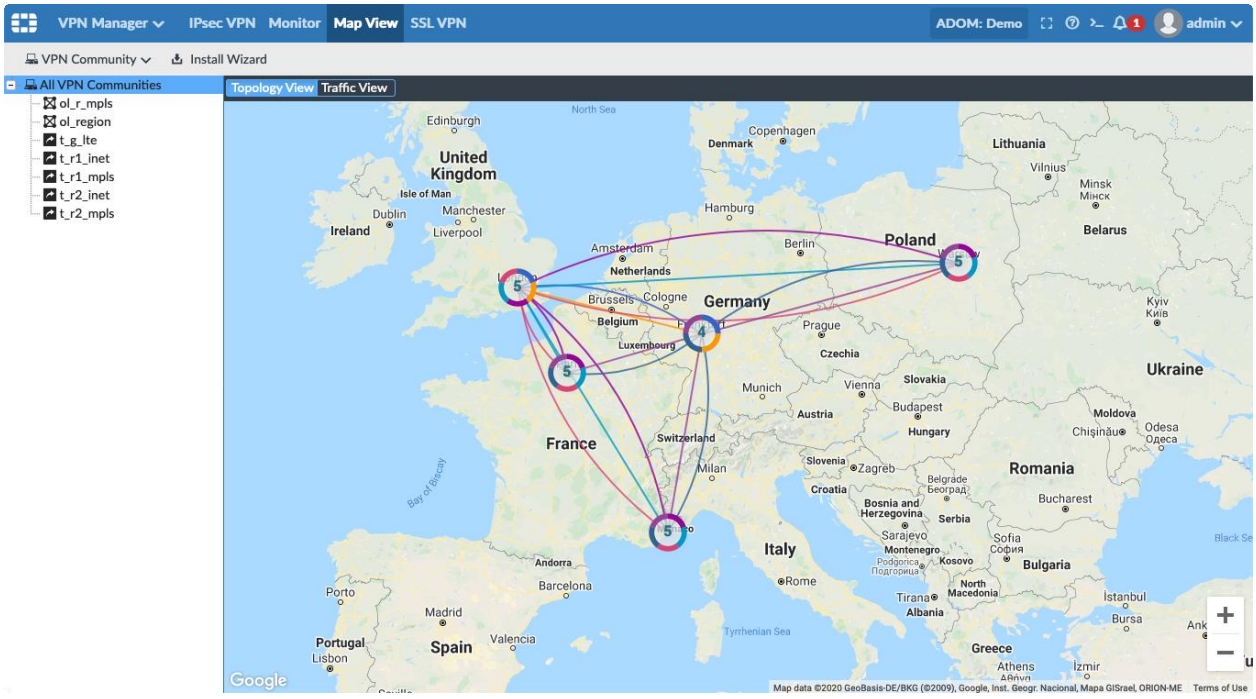
4.3 FORTIMANAGER

Il sistema di gestione centralizzata FortiManager consente di avere una singola console di management per tutta la configurazione dei sistemi FortiGate, sia SD-WAN che VPN, interfacce, policy di sicurezza, licenze, firmware ed anche LAN e WiFi.
L'ambito di fornitura prevede FortiManager per 10 device/cluster/vdom (sufficiente per il perimetro di progetto costituito di 6 sedi). Tale FortiManager sarà fornita in modalità Virtual Machine, installabile sulle più comuni piattaforme di virtualizzazione (Vmware, Hyper-V, KVM etc) che dovrà essere messa a disposizione dall'Amministrazione contraente.
Le caratteristiche principali della FortiManager sono le seguenti:

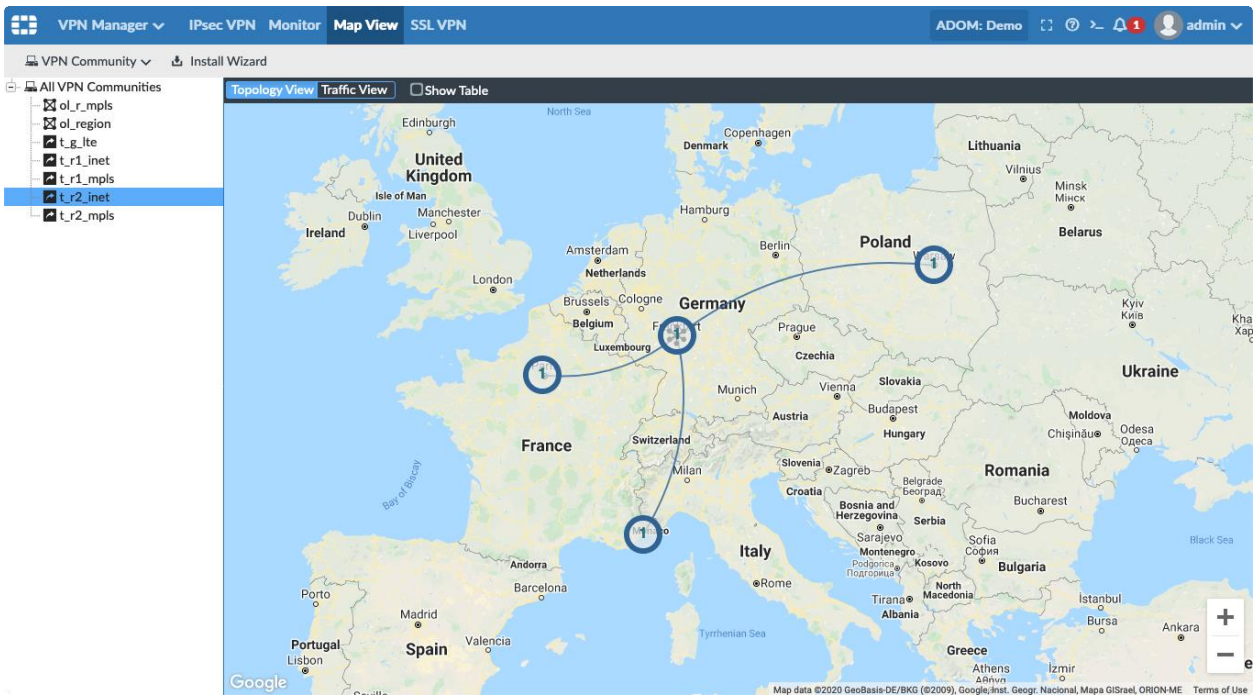
- Centralized device management: Una singola console raggiungibile in GUI via https che consente di gestire apparati FortiGate, FortiSwitches, FortiAPs e fornire funzionalità di update manager centralizzato per tutti gli apparati gestiti.
- Centralized policies and configuration management: Editor per la gestione facile e veloce di Policies Firewall, oggetti e template di configurazione completamente costruito in HTML5 con funzionalità drag&drop ed editor delle policies senza necessità di editare ogni signola policy per la modifica. È possibile definire dei template di configurazione di ogni componente di configurazione del device e associare questo template ad un device o ad un gruppo di device: agendo sulla modifica del template è quindi possibile cambiare la configurazione in maniera massiva su più device con un semplice click.
- Le policy FW sono raggruppate in policy Package associati ad un apparato o ad un gruppo di apparati: è possibile modificare ogni singola policy, attivarla/disattivarla, eliminarla. È anche possibile verificare lo storico delle modifiche effettuate all'interno di ciascun policy package. All'interno di ogni policy firewall è possibile configurare regole di traffico fino a Livello 7, associare security profile di web/video filtering, application control, IPS, DNS Filter, Antivirus, WAF nonchè abilitare o disalitare la Deep Packet Inspection (DPI).
- Capacità evolute di tracciamento delle revisioni, auditing delle attività effettuate dagli amministratori.
- Gestione dei Workflows per una migliore implementazione dell'utilizzo multiutenza.
- Gestione Centralizzata delle configurazioni e del monitoraggio di SD-WAN e VPN.
- Automazione: Gestione di templates and scripts per il provisioning di nuovi device o modifica degli esistenti. API JSON o XML per l'interazione con sistemi di automazione ed orchestratori di terze parti.
- Multitenancy e RBAC per una precisa definizione dei ruoli degli amministratori e del loro perimetro di gestione.
- Software upgrades e security updates centralizzati per i device gestiti.

Sotto Device Manager è possibile visualizzare la lista di tutti gli apparati gestiti, il loro hostname, la tipologia di apparato, la release SW e i template/policy di configurazione attualmente in uso.
È possibile creare degli shaping profile per definire delle classi di servizio su base applicazione/flusso di traffico L3-L4 con una banda minima garantita piuttosto che una banda massima (shaping). È inoltre possibile definire delle priorità di scheduling del traffico nonchè definire delle politiche di Drop in caso di congestione con meccanismi di weighted random early detection (Wred). Gli shaping profile possono poi essere associati a qualsiasi interfaccia Overlay/Underlay per intercettare le varie tipologie di traffico. È poi possibile monitorare il traffico associato ad ogni classe di servizio verificando la banda di ciascuna classe di servizio e il traffico droppato da eventuali shaping associati.

SD-WAN Monitor - Map View



VPN Manager- Map View (All VPN Communities)



VPN Manager- Map View (Specific VPN Communities)

4.4 SOLUZIONE SD-WAN

La soluzione Secure SD-WAN di Fortinet integrata nel sistema operativo FortiGate FortiOS del NGFW oggetto di fornitura, offre sicurezza di nuova generazione e funzionalità di rete per migliorare l'efficienza della WAN senza compromettere la sicurezza, garantisce lo stesso livello di funzionalità fornito dai fornitori di SD-WAN pure-play, supportando tutti i casi d'uso comuni, con sicurezza avanzata integrata in un'unica offerta. La soluzione è supportata da test indipendenti per offrire un'esperienza di qualità eccellente per voce e video, un elevato throughput VPN e il miglior rapporto prezzo/prestazioni. In Fortinet, la funzionalità SD-WAN è stata sviluppata internamente in modo organico ed è una caratteristica di ogni modello FortiGate. I processori di sicurezza appositamente progettati (SoC e ASIC) e l'intelligence sulle minacce informatiche di FortiGuard Labs garantiscono ulteriormente che la sicurezza sia parte integrante della soluzione SD-WAN di Fortinet.
Le funzionalità SD-WAN sono integrate all'interno del sistema operativo FortiGate FortiOS, i processi decisionali, di scelta del percorso e di rilevamento dell'integrità del percorso sono locali e distribuiti su ogni singolo dispositivo perimetrale WAN. Le configurazioni delle logiche SD-WAN, delle politiche di selezione del percorso, delle policy di sicurezza e della componente Overlay sono generalmente centralizzate. Ogni elemento periferico della soluzione SD-WAN è completamente autonomo e un'architettura SD-WAN distribuita continuerà a funzionare con o senza connettività all'infrastruttura di controllo/gestione centrale. Poiché ogni elemento periferico è responsabile del proprio processo decisionale e del monitoraggio end-to-end, la soluzione diventa veramente altamente scalabile. Fortinet SD-WAN sfrutta i molti anni di esperienza nel networking e nella sicurezza, inclusa la capacità di rilevamento delle applicazioni di livello 7, funzionalità di rete ottimizzate per hardware e software.
Tutti gli elementi di una soluzione Fortinet SD-WAN possono essere gestiti tramite GUI locale, CLI o tramite un'API JSON rest consentendo l'integrazione in sistemi di orchestrazione esterni. SD-WAN funziona instradando le applicazioni sulla connessione WAN più efficiente in qualsiasi momento, per garantire prestazioni applicative ottimali. È possibile identificare un'ampia gamma di applicazioni e applicare policy di routing a un livello molto granulare utilizzando un database di controllo delle applicazioni con firme che ad oggi permettono il riconoscimento di oltre 4.000 applicazioni con firme aggiunte e aggiornate regolarmente dal servizio di intelligence sulle minacce di FortiGuard Labs. FortiOS utilizza anche un Internet Service DB locale su ciasun FortiGate e costantemente aggiornato dai Fortiguards Labs contenente una combinazione di IP e porte TCP dei principali servizi Internet che permette di identificare e classificare le applicazioni (anche il traffico di applicazioni cloud crittografate) fin dal primo pacchetto.
Specificando i criteri di qualità da soddisfare per ciascuna applicazione, insieme alla definizione di SLA rigorosi basati su una combinazione di metriche di jitter, perdita di pacchetti e latenza, il FortiGate seleziona il collegamento corrispondente in base alle regole SD-WAN applicate. È possibile implementare diverse regole, dando priorità alle prestazioni del collegamento, alla larghezza di banda o al bilanciamento del carico rispetto ai collegamenti disponibili.
Le funzionalità di implementazione semplificate di Fortinet Secure SD-WAN consentono alle aziende di spedire appliance FortiGate NGFW configurate in fabbrica a ogni sito remoto. Il provisioning zero touch è un fattore chiave per le piccole, medie e grandi imprese con più filiali. Una volta collegato, FortiGate si connette automaticamente al servizio FortiDeploy in

FortiCloud. In pochi secondi, FortiDeploy autentica il dispositivo remoto e lo connette a un sistema centrale FortiManager fornendo Provisioning Zero Touch in modo semplice.
L'architettura della soluzione Fortinet Secure SD-WAN è composta dai seguenti elementi:

- Edge Devices: i FortiGate implementati presso le sedi dei clienti che implementano le funzionalità di SD-WAN e di Next Generation Firewall. Sono responsabili dello startup degli overlay (tunnel IPSec tra le sedi secondarie e le sedi principali e tunnel tra le varie sedi on demand in caso di comunicazione sede a sede).
- Gestione Centralizzata: il FortiManager è l'elemento responsabile di gestire centralmente i vari FortiGate implementando la configurazione (Overlay, Underlay, SD-WAN policy, Security Policy, Zero Touch Provisioning...) sui vari FortiGate. L'elemento è multi tenant, è quindi in grado di gestire più clienti contemporaneamente garantendo la separazione delle configurazioni tra essi.
- Log & Reports Centralizzato: il FortiAnalyzer è l'elemento responsabile di raccogliere centralmente i log generati dai vari FortiGate e di fornire informazioni circa il traffico gestito e genera reports che riassumono gli aspetti salienti.

La soluzione Fortinet ha anche la capacità di estendere l'ecosistema Software Defined a LAN e servizi Wi-Fi collegati localmente per fornire Secure SD-Branch. Questi servizi sono integrati nella piattaforma FortiGate e il FortiManager è l'unico pannello di configurazione e la piattaforma Zero Touch sia per Secure SD-WAN che per Secure SD-Branch.

4.5 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:

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

Per l'effettuazione del complesso di attività previste per il supporto specialistico il Fornitore prevedrà figure professionali Senior Security Architect, Senior Security Analyst, Junior Security Analyst, Senior Security Tester e Security Principal.

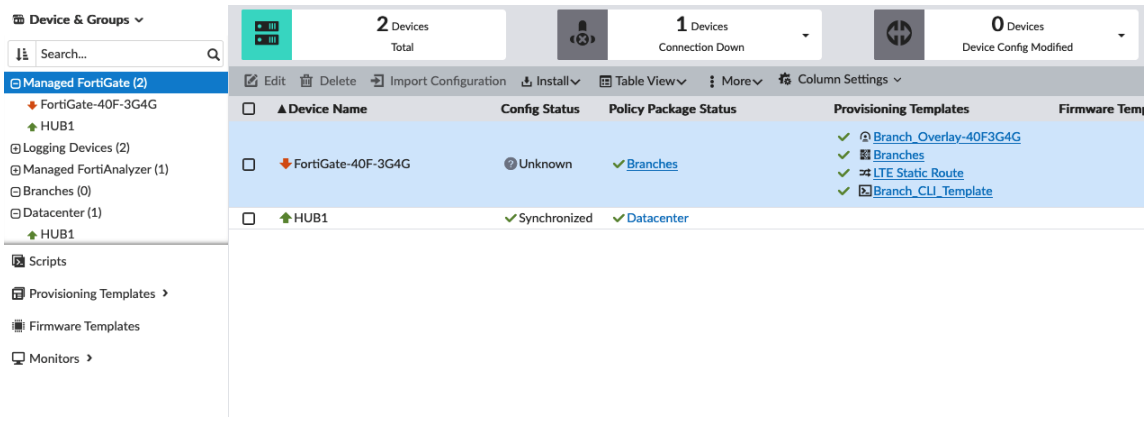
Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Junior Security Analist – Fascia standard	JSAN-STA	JR_SEC_AN_STD	240
Senior Security Analist – Fascia standard	SSAN-STA	SR_SEC_AN_STD	226
Junior Security Analist – Fascia Straordinaria	JSAN-STR	JR_SEC_AN_STR	200
Senior Security Analist – Fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	180

Attraverso i servizi specialistici si implementerà la soluzione basata su SDWAN presso il datacenter (HUB) e le sedi remote (SPOKE) dell'ASL-RM1. Si effettueranno verifiche della configurazione AS-IS sul FortiGate 1800F identificando i punti di miglioria e advanced fine-tuning secondo le esigenze specifiche del cliente, nell'ottica di evolverne il ruolo ad HUB dell'infrastruttura SDWAN che si andrà a realizzare.
Il deployment della soluzione avverrà secondo i seguenti passi e configurazioni:

- Progettazione di High Level Design
- Progettazione di Low Level Design, definizione della strategia di migrazione, procedure di rollback e schemi di collaudo
- Tuning delle configurazioni su cluster FortiGate 1800 della sede HUB al fine di implementare il ruolo di hub nella configurazione hub-spoke
- Definizione delle zone sdwan e delle strategie di steering del traffico sull'HUB (application, business critical, ottimizzazione delle connettività disponibili).
- Definizione dell'AS BGP per lo steering dinamico del traffico HUB-SPOKE
- Installazione, configurazione e tuning del FortiManager, soluzione di management centralizzata. Saranno definiti gli oggetti e le relative normalizzazioni, template di Provisioning e Policy Package per la configurazione automatizzata

delle sedi remote (spoke). La figura seguente riporta uno screen esemplificativo della soluzione.



- Setup degli overlay ridondati sui vari branch (o spoke, sedi remote) per la connessione datacenter (HUB) e le connettività internet sia attraverso l'hub e attraverso le connessioni di backup delle singole sedi. Saranno quindi configurati i tunnel IPSEC e il routing dinamico sull'AS BGP e le policy che consentiranno le interconnessioni intra-sede/internet richieste dall'IT del cliente.
- Attività di analisi per identificazione e tuning delle policy di sicurezza attuabili attraverso Security Profile nel contesto del cliente
- Attività di supporto di secondo e terzo livello durante il deploy della soluzione. Il cliente potrà richiedere supporto di secondo livello per le attività di:
    - FortiGate Health Check: revisione del corretto funzionamento delle funzionalità degli apparati e improvement delle performance
    - Configuration Verification: Verifica delle configurazioni e tuning delle soluzioni in modo che siano implementate in modo ottimale per soddisfare le esigenze del cliente.
    - Security Advisoring: verrà fornita, mensilmente e allegata ai report di servizio, la lista dei nuovi CVE e dei CVE aggiornati relativi ai prodotti di interesse.
    - Aggiornamenti delle release per Bug Fixing e Security Patching: le release saranno identificate dal tag Mature del Vendor
    - Implementazione delle modifiche alle configurazioni (es su perimetro Policy, Security Profile, VPN)
    - Reattività alle problematiche segnalate dal cliente o dagli eventi triggerati dal sistema di monitoraggio
    - Network Design & Implementation
    - Platform Integration: ottimizzazione delle integrazioni delle soluzioni Fortinet all'interno della rete del Cliente
    - Design and Configuration Review: Revisione delle configurazioni e delle documentazioni di progetto
    - Design and Configuration Validation: Implementare piani di test specifici per il cliente concentrandosi sulla verifica dello stato finale incentrato sull'impatto sul business.
    - Firewall Migration and Replacement Project: supporto ai progetti di migrazione "production-to-production" per migrazioni da soluzioni custom o di vendor terze parti
    - Software Upgrade and Platform Migration Project: Aggiornamenti del software a Major Realease dall'impatto rilevante, Feature Release o hardware migration/replacement
    - Technical Design Authority and Implementation: guida alla progettazione ed implementazione garantendo che eventuali problemi che possano sorgere vengano tracciati e risolti.

  Il team di supporto è costituito dal team di Network Operation (NSE4) e in terzo livello dai Network Security Architect (NSE7). Questi ultimi hanno il compito di sovraintendere all'intera organizzazione di servizio dal punto di vista tecnologico, proponendo interventi, migliorie o soluzioni tecnologiche di nuova generazione.

Le attività necessarie per l'implementazione del FortiNAC nel contesto del cliente saranno:

- Information Gathering sull'infrastruttura di rete/IT del cliente per l'implementazione del FortiNAC
    - Wireless Network
    - Wired Network
    - Directory Services
    - Radius Services
- Discussione ed Analisi dei Posture Requirements
    - Accesso personale VIP
    - Accesso personale tecnico
    - Accesso personale generico
    - Accesso personale consulenti esterni
    - Accesso ospiti (SelfRegistration, Sponsorship, Guest Management)
    - Accesso dispositivi unmanned (Stampanti, Telefoni VoIP, Conference, dispositivi IOT)
- Definizione Delivery Layout (requisiti di progetto)

- Installazione, configurazione e licensing n° 1 appliance FortiNAC
- Onboarding apparati di rete nel FortiNAC Inventory
- Configurazione Visibility del FortiNAC: questa fase consente di ridurre i rischi di sicurezza associati ai dispositivi non protetti che accedono alla rete offrendo visibilità totale su endpoint, utenti, dispositivi affidabili o non attendibili.
- Verifiche dei risultati ottenuti durante la fase di Visibility per l'identificazione dei rogue devices e caratterizzazione dei device che sono stati oggetto di discovery
- Configurazione Users/Groups/Guests/Captive Portal
- Persistent Agent Deployment
- Modellizzazione degli endpoint in FortiNAC; questa fase ha l'obiettivo di strutturare dei criteri sul FortiNAC che caratterizzino le tipologie di device noti con la finalità di applicarvi automaticamente criteri di accesso alla rete.
- Creazione e tuning delle Policy per la definizione e la registrazione dei device autorizzati ad accedere alla rete ministeriale segregando quelli non autorizzati
- Controllo dei device non compliant (per device con agent) e relativa segregazione in VLAN dedicate. Tale funzionalità è disponibile per sistemi operativi Windows/Linux/Mac e device mobile Android, sono esclusi i device iOS)
- Redazione Documentazione

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.

4.6 SERVIZIO DI MANUTENZIONE

Il servizio di manutenzione è opzionale (sebbene oggetto di quotazione) e quindi dovrà essere prestato, a pagamento, dall'Aggiudicatario soltanto se espressamente richiesto dall'Amministrazione.
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.
Sarà facoltà dell'Amministrazione Contraente richiedere a pagamento il servizio manutenzione in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*),
Il servizio di manutenzione è offerto per annualità, quindi per 12 mesi o massimo 24 mesi.
In accordo con l'Amministrazione, di predisporre 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). Tale possibilità dovrà essere riportata nel "*Piano Operativo*".

In fase di offerta economica al concorrente sarà richiesto di esprimere due valori percentuali in base al profilo di qualità richiesto per i servizi erogati, *Low Profile* (*Business Day*) o *High Profile* (*H24*). Ogni valore espresso rappresenta la percentuale del prezzo di fornitura degli elementi offerti in Accordo Quadro relativa al canone di manutenzione annuale (ad esempio: se il prezzo dell'elemento di fornitura "X" offerto dal concorrente è pari a 10€ e la percentuale relativa alla manutenzione per il profilo *Low Profile* offerta dal concorrente è pari al 10% il corrispondente canone annuale della manutenzione con profilo *Low Profile* dell'elemento di fornitura "X" è pari a 10€ x 10% = 1€).
Le attività di manutenzione potranno essere richieste dalle Amministrazioni Contraenti sui 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.

5.1 PIANO DI LAVORO

In seguito, si descrivono le WBS alto livello di progetto e la relativa pianificazione in termini di settimane dalle attività di presa in carico.

1. Approvvigionamento e consegna materiali hardware e software

Durante le settimane di attesa per la fornitura da parte del Vendor i servizi specialistici potranno avviare le attività di:

2. Interviste Raccolta requisiti e definizione e condivisione progetto HLD
3. Definizione e condivisione Progetto HLD
4. Sopralluoghi su tutte le sedi per definizione requisiti progetto LLD
5. Definizione e condivisione progetto LLD

A fornitura avvenuta si procederà al:

6. Installazione iniziale degli apparati in HA
7. Installazione del FortiManager
8. Configurazione del FortiManager: Definizione SDWAN Overlay e Branch Templates
9. Verifica configurazioni cluster 1800F per attuazione ruolo HUB
10. Configurazione HUB
11. Installazione Sede Remota Pilota
12. Supporto post migrazione sede pilota
13. Installazioni totalità sedi remota
14. Collaudo

Per la componente FortiNAC

15. Installazione, configurazione e licensing n° 1 appliance FortiNAC
16. Onboarding apparati di rete nel FortiNAC Inventory
17. Configurazione Visibility del FortiNAC:
18. Configurazione Users/Groups/Guests/Captive Portal
19. Creazione e tuning delle Policy
20. Collaudo

5.2 CRONOPROGRAMMA

Cronoprogramma		Month 1				Month 2				Month 3				Month 4				Month 5			
		Weeks																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Start del cliente Engineering	Approvvigionamento e consegna materiali hardware e software																				
	Interviste Raccolta requisiti e definizione e condivisione progetto HLD																				
Delivery SDWAN	Sopralluoghi tutte le sedi per definizione requisiti progetto LLD																				
	Definizione e condivisione progetto LLD																				
	Installazioni iniziali degli apparati																				
	Installazione del FortiManager																				
	Verifica configurazioni cluster 1800F per attuazione ruolo HUB Configurazione HUB																				
	Configurazione HUB Tuning Security Inspection profile																				
	Definizione Template SDWAN Overlay e Branch Templates Configurazione SDWAN sede HUB																				
	Installazione Sede Remota Pilota																				
	Supporto post attuazione sede pilota																				
	Installazioni totalità sede remota																				
	Collaudo																				
Delivery FortiNAC	Installazione, configurazione e licensing n° 1 appliance FortiNAC																				
	Onboarding apparati di rete nel FortiNAC Inventory																				
	Configurazione Visibility del FortiNAC:																				
	Configurazione Users/Groups/Guests/Captive Portal																				
	Creazione e tuning delle Policy																				
	Collaudo																				

5.3 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.

L'avvio delle attività di presa in carico avverranno durante il periodo meglio specificato nel piano di lavoro come "Intervista raccolta requisiti" per consentire al fornitore di avviare le attività di progettazione HLD. Si condivideranno inoltre i riferimenti necessari per avviare le attività di sopralluogo delle sedi e/o locali tecnici per la definizione di quanto necessario alla progettazione di dettaglio "LLD".

L'attività 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.

Se previsto e/o richiesto dall'amministrazione contraente saranno altresì forniti i dettagli necessari (es. tools IT Management) alla corretta implementazione dei processi di Incident, Change e Deploy Management richiesta per l'espletamento dei servizi descritti nei successivi paragrafi.

Si noti che qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del piano di presa in carico.

Durante le attività di Presa in carico si dovrà garantire:

- 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

5.4.1 PIANO DEI TEST

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 5.1

HQ HUB DEVICE

Test 1

Obiettivo	Funzionamento dei servizi interni e fruizione dai singoli segmenti L3		
Dati di Input	Piano di indirizzamento dei server interni		
Modalità di esecuzione	Network Tools / Browser		
Risultati attesi	Raggiungibilità		
Risultati Ottenuti	**Completa raggiungibilità dei servizi interni - ESITO OK**	**Firma**	

Test 2

Obiettivo	Fruizione securizzata dei servizi Internet		
Dati di Input	Navigazione Internet – Navigazione Internet di destinazione malevole		
Modalità di esecuzione	Navigazione via browser		
Risultati attesi	Navigazione Internet attraverso connettività WAN in configurazione SDWAN Blocco delle destinazioni malevole e/o non desiderate dalle policy aziendali		
Risultati Ottenuti	**Fruizioni dei contenuti Internet utilizzando tutte le connettività internet in maniera trasparente – blocco di siti malevoli – ESITO OK**	**Firma**	

Test 3

Obiettivo	Raggiungibilità delle sedi remote attraverso SDWAN		
Dati di Input	Piano di indirizzamento delle sedi remote – Simulazione di fail di link ridondanti e steering del traffico intrasito		
Modalità di esecuzione	Network Tools / Browser		
Risultati attesi	Raggiungibilità delle sedi remote		
Risultati Ottenuti	**ESITO OK**	**Firma**	

BO SPOKE DEVICE

Verifica della fruibilità dei servizi previsti.

Test 1

Obiettivo	Funzionamento dei servizi interni e fruizione dai singoli segmenti L3		
Dati di Input	Piano di indirizzamento dei server interni		
Modalità di esecuzione	Network Tools / Browser		
Risultati attesi	Raggiungibilità		
Risultati Ottenuti	**Completa raggiungibilità dei servizi interni - ESITO OK**	**Firma**	

Test 2

Obiettivo	Fruizione securizzata dei servizi Internet (internet breakout se presente)
Dati di Input	Navigazione Internet – Navigazione Internet di destinazione malevole

Modalità di esecuzione	Navigazione via browser		
Risultati attesi	Navigazione Internet attraverso connettività WAN in configurazione SDWAN Blocco delle destinazioni malevole e/o non desiderate dalle policy aziendali		
Risultati Ottenuti	**Fruizioni dei contenuti Internet utilizzando tutte le connettività internet in maniera trasparente – blocco di siti malevoli – ESITO OK**	**Firma**	

Test 3

Obiettivo	Raggiungibilità della sede HQ attraverso SDWAN		
Dati di Input	Piano di indirizzamento della sede HQ		
Modalità di esecuzione	Network Tools / Browser		
Risultati attesi	Raggiungibilità dei servizi su sede principale (HQ)		
Risultati Ottenuti	**ESITO OK**	**Firma**	

GESTIONE CENTRALIZZATA

Verifica della fruibilità dei servizi previsti.

Test 1

Obiettivo	Gestione dei devices e provisioning attraverso FortiManager		
Dati di Input	Network Parameters BO Site		
Modalità di esecuzione	Console FortiManager		
Risultati attesi	Configurazione del FortiGate della sede Remota		
Risultati Ottenuti	**Configurazione terminata con successo della sede remota ed esecuzione dei test al 4.2 – ESITO OK**	**Firma**	

VPN

Verifica della fruibilità dei servizi previsti.

Test 1

Obiettivo	Connessione ad eventuali VPN IPSEC esterne se previste e via FortiClient		
Dati di Input	Utenza/Password dell'utente campione – Piano indirizzamento IPSEC esterne		
Modalità di esecuzione	Laptop		
Risultati attesi	Connessione ai servizi via VPN		
Risultati Ottenuti	**Connessione avvenuta – Raggiungibilità servizi interni - ESITO OK**	**Firma**	

6 TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

Descrizione	Codice Articolo	Qta'	Durata	Listino CS2	Totale
NGFW Fascia 1	CS2L3-NGFW-F1_TELSY	100		1.211,18 €	121.118,00 €
NGFW Fascia 2	CS2L3-NGFW-F2_TELSY	6		6.672,19 €	40.033,14 €
NGFW Fascia 3	CS2L3-NGFW-F3_TELSY	2		12.502,60 €	25.005,20 €
NGFW Fascia 5	CS2L3-NGFW-F5_TELSY	2		50.386,49 €	100.772,98 €
NAC Fascia 4	CS2L3-NAC-F4_TELSY	1		66.577,91 €	66.577,91 €
Manutenzione profilo HP - NGFW - fascia 1 Fortinet	CS2L3-MANHP-NGFW-F1_TELSY	100	24	48,45 €	4.844,72 €
Manutenzione 24 mesi NGFW fascia 2 profilo HP	CS2L3-MANHP-NGFW-F2_TELSY	6	24	266,89 €	1.601,33 €
Manutenzione 24 mesi NGFW fascia 3 profilo HP	CS2L3-MANHP-NGFW-F3_TELSY	2	24	500,10 €	1.000,21 €
Manutenzione 24 mesi NGFW fascia 5 profilo HP	CS2L3-MANHP-NGFW-F5_TELSY	2	24	2.015,46 €	4.030,92 €
Manutenzione 24 mesi NAC Fascia 4 profilo HP	CS2L3-MANHP-NAC-F4_TELSY	1	24	2.663,12 €	2.663,12 €
Senior Security Analyst fascia standard	CS2L3-SSAN-STA	226		271,00 €	61.246,00 €
Senior Security Analyst fascia straordinaria	CS2L3-SSAN-STR	180		325,20 €	58.536,00 €
Junior Security Analyst fascia standard	CS2L3-JSAN-STA	240		227,50 €	54.600,00 €
Junior Security Analyst fascia straordinaria	CS2L3-JSAN-STR	200		288,93 €	57.786,00 €
					599.815,52 €

7 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:
  - Formazione;
  - Hardening;
  - 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 (gruppo TIM)
Supporto Specialistico	**0%**	**TIM SpA**	**TELSY**