



Capitolato Tecnico Servizi di manutenzione degli apparati di rete e sicurezza

CIG 93115283FD

Servizio Information Technology



INDICE

INTRODUZIONE	3
1.1 PREMESA	3
1.2 DEFINIZIONI E ACRONIMI	3
2. DESCRIZIONE DEL CONTESTO	4
2.1 INFRASTRUTTURA DI RETE DELLA SEDE DI ROMA	4
2.2 INFRASTRUTTURA DI RETE DELLE SEDI PERIFERICHE.....	5
3. COPERTURA DEGLI ATTUALI CONTRATTI DI MANUTENZIONE	6
4. SERVIZI DELLA FORNITURA	7
5. REQUISITI PER IL FORNITORE	7
5.1 CERTIFICAZIONI AZIENDALI.....	8
5.2 PERSONALE TECNICO	8
6. PENALI	8
7. SUPPORTO SPECIALISTICO	8
8. MODALITÀ DI PAGAMENTO	11

Introduzione

1.1 PREMESSA

La Fondazione Enasarco ha esigenza di rinnovare i servizi di manutenzione e supporto degli apparati di rete che costituiscono la LAN di palazzo: sede centrale di Roma e di tutte le sedi periferiche dislocate sul territorio nazionale.

A tal scopo indice la presente gara d'appalto al fine di raggiungere i seguenti obiettivi:

- Rinnovare la manutenzione dei dispositivi di rete Cisco Systems presenti esclusivamente presso la sede di Roma;
- Rinnovare la manutenzione dei dispositivi di sicurezza Checkpoint presenti in tutte le sedi della Fondazione valutando anche un possibile totale o parziale rinnovo dell'hardware (trade-in) degli stessi
- Attivare un contratto di supporto specialistico e manutenzione Hardware/Software della durata di 3 anni

Il dettaglio della soluzione richiesta è riportato nei successivi capitoli di questo documento.

1.2 DEFINIZIONI E ACRONIMI

Nel corpo del Capitolato Tecnico con il termine:

"LAN": Local area network;

"VoIP": voice over IP;

"Concorrente": impresa che concorre alla presente gara, ovvero potenziale Fornitore;

"NBD": Next Business Day;

"SLA": Service Layer Agreement;

"SPOF": Single Point of Failure;

"VLAN": Virtual Local Area Network (ID)

"NAC": Network Access Control

"AP": Access Point

"SW": Switch

"SIA": Sistema Informatico Aziendale

"AD": Active Directory

"EP": Endpoint

"WLC": Wireless Lan Controller

"ISE": Identity Service Engine

"SFP": Small Form-Factor Pluggable Transceiver

"POE": Power of Ethernet

"MAB": Mac Authentication Bypass

"RMA": Product Return & Replacement

2. Descrizione del contesto

2.1 INFRASTRUTTURA DI RETE DELLA SEDE DI ROMA

L'attuale infrastruttura di rete oggetto della presente fornitura, localizzata nella sede di Roma, è costituita da:

- n.2 Switch Cisco 6509E
- n.2 Switch Cisco 3850
- n.2 Firewall Cisco ASA5525
- n.2 Server Cisco UCS
- n.2 Firewall Checkpoint 5800

Di seguito forniamo il dettaglio degli apparati:

Modello	Product ID	Model	Numero di serie
Cisco Catalyst 6509	WS-C6509-E	C6800-32P10G WS-X6724-SFP VS-SUP2T-10G WS-X6704-10GE WS-X6748-GE-TX	JAE23160B6A SAL11487W35 JAE23150C54 SAL13410HLA SAL11477NNT
Cisco Catalyst 6509	WS-C6509-E	C6800-32P10G WS-X6724-SFP VS-SUP2T-10G WS-X6704-10GE WS-X6748-GE-TX	JAE23160B7X SAL1148825L JAE23150C6E SAL13410K9U SAL11466R3N
Cisco ASA 5525	ASA5525	ASA 5525-X with SW, 8 GE Data, 1 GE Mgmt, AC	FCH1917J9LG
Cisco ASA 5525	ASA5525	ASA 5525-X with SW, 8 GE Data, 1 GE Mgmt, AC	FCH1917JBGA
Cisco 3850	WS-C3850-24S-E	Cisco Catalyst 3850-24S-E Switch	FCW2313GHCK
Cisco 3850	WS-C3850-24S-E	Cisco Catalyst 3850-24S-E Switch	FOC2313X08E

Modello	Product ID	UUID	Numero di serie
Cisco UCS C220 M3S	UCSC-C220-M3S	3AB3BC7A-AD17-4710-895D-540C2DD6BB3F	FCH1906V10X
Cisco UCS C220 M3S	UCSC-C220-M3S	22A5822A-207F-492A-9A36-C1C64346D088	FCH1906V10U

Modello	Product ID	Licenze	Numero di serie
Checkpoint 5800 Appliance	PL-30-00	Firewall, Ipsec VPN, IPS, Application Control, URL Filtering, Content Awareness, Anti-Virus, Anti-Bot, Threat Emulation Cloud, Threat Extraction, Anti-Spam, Email Security, Mobile Access	1840BA0122
Checkpoint 5800 Appliance	PL-30-00	Firewall, Ipsec VPN, IPS, Application Control, URL Filtering, Content Awareness, Anti-Virus, Anti-Bot, Threat Emulation Cloud, Threat Extraction, Anti-Spam, Email Security, Mobile Access	1840BA0091

2.2 INFRASTRUTTURA DI RETE DELLE SEDI PERIFERICHE

L'attuale infrastruttura di rete oggetto della presente fornitura, localizzata presso le 19 sedi periferiche è costituita da:

- n. 1 Firewall Checkpoint 1550 (per ogni sede)

Di seguito forniamo il dettaglio degli apparati:

Modello	Product ID	Licenze	Numero di serie
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:40:E8
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:43:12
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:88
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:DC
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:43:02
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:1°
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:54
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:44:C0
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:44:6E
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:41:00
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:44:F0
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:42:F0
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:40:2E
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:44:52
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:18

Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:43:2E
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:42:F0
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:C6
Checkpoint 1550 Appliance	Appliance 1550	Firewall, Application Control, Identity Awareness, Advanced Networking, IPS, IPSEC VPN	00:1C:7F:97:45:B4

3. Copertura degli attuali contratti di manutenzione

Qualora per gli apparati oggetto della presente gara d'appalto, non sia più possibile attivare un regolare contratto di manutenzione con il Vendor, come ad esempio per i Cisco UCS, è richiesto al fornitore di predisporre il quantitativo di scorte necessarie al fine di erogare i servizi di manutenzione richiesti.

4. Servizi della fornitura

Il Fornitore dovrà formulare l'offerta economica per il rinnovo totale dei contratti di manutenzione in essere per le tecnologie Cisco e Checkpoint.

I nuovi contratti di manutenzione dovranno scadere il 31/12/2025.

Rinnovo del contratto di manutenzione Cisco e Checkpoint

È richiesta la manutenzione dell'intero parco macchine oggetto della presente gara con copertura 8x5xNBD (8:30–17:30) con ripristino Next Business Day ed apertura dell'intervento entro e non oltre le 2 ore dalla segnalazione dell'anomalia. Il contratto di manutenzione dovrà avere validità fino al 31/12/2025.

Nella tabella seguente sono indicati i codici prodotto per il rinnovo della manutenzione Checkpoint:

SUPPORT				
Selected Support Level	Product	Product Type	Description	Qty
CPCES-CO-STANDARD-ADD	CPAP-SG5800-NGTX-HA	5000 Appliances	5800 Next Generation Threat Prevention and SandBlast (NGTX) Appliance for High Availability	1
CPCES-CO-STANDARD-ADD	CPAP-SG5800-NGTX	5000 Appliances	5800 Next Generation Threat Prevention and SandBlast (NGTX) Appliance	1
CPCES-CO-STANDARD-ADD	CPAC-4-10F-B	Attached Accessories	4 Port 10GBase-F SFP+ interface card.	2
CPCES-CO-STANDARD-ADD	CPAC-TR-10SR-B	Standalone Accessories	SFP+ transceiver for 10G fiber Ports - short range (10GBase-SR) compatible with CPAC-4-10F-B, CPAC-2-10F-B, CPAC-2-10F-SM525/5050/5	8
CPCES-CO-STANDARD	CPSM-NGSM5	Software Products	Next Generation Security Management Software for 5 gateways	1
SERVICE				
Service	Product	Product Type	Description	Qty
CPSB-NGFW-5800-3Y-HA	CPAP-SG5800-NGTX-HA	5000 Appliances	Next Generation Firewall Package subscription for 3 year for 5800 Appliance HA	1
CPSB-NGFW-5800-3Y	CPAP-SG5800-NGTX	5000 Appliances	Next Generation Firewall Package subscription for 3 year for 5800 Appliance	1

Item Type	SKU	Quantity
Support for Appliance Gateways	CPES-SS-PREMIUMPRO-1550-BUN-ADD	19
Annuity Blades	CPSB-NGFW-1550-BUN-2Y	19

5. Requisiti per il fornitore

In questo capitolo sono indicati i requisiti considerati obbligatori per poter partecipare alla gara d'appalto.

5.1 CERTIFICAZIONI AZIENDALI

- Certificazione aziendale ISO 9001:2008
- Certificazione aziendale Cisco GOLD
- Certificazione aziendale 4 Stars Checkpoint

5.2 PERSONALE TECNICO AZIENDALE

- Almeno 3 figure tecniche con certificazione Cisco CCIE di tipo Routing&Switching o Voice o Wifi in corso di validità
- Almeno 3 figure tecniche con certificazione Checkpoint CCSE in corso di validità

Struttura tecnica / divisione aziendale dedicata all'erogazione dei servizi del presente appalto:

- Almeno 1 persone con certificazioni ITIL Foundation
- Almeno 1 figura con ruolo di responsabilità all'interno della struttura dei servizi gestiti con certificazione ITIL Intermediate Service Operation.

6. Penali

Il mancato rispetto dei livelli di servizio e delle tempistiche di progetto indicate nella proposta tecnico-economica, comporterà l'applicazione di penali come di seguito indicato.

Accesso al servizio per supporto remoto specialistico	➤ da 0 a 2 ore	➤ 2 ore
Importo detratto	50€ ad ogni ora di superamento	100€ ad ogni ora di superamento

Ripristino con spare parts	➤ Superamento NBD
Importo detratto	500€ ad ogni giorno successivo allo SLA

7. Supporto specialistico

Nell'ambito della presente gara d'appalto è richiesto il servizio di supporto specialistico secondo quanto di seguito esposto.

Presenza in carico e documentazione

L'appaltatore è tenuto a prevedere una serie di attività da condurre da remoto e on site per acquisire la "conoscenza" necessaria all'erogazione del servizio di assistenza oggetto del presente bando.

Seguono elencate per punti alcune considerazioni utili a valutare correttamente l'impegno richiesto per la fase di startup e documentazione. Resta inteso che per tutti i punti sotto riportati il personale della stazione appaltante sarà disponibile a fornire le informazioni di volta in volta necessarie.

- Visita degli ambienti

- Definizione delle procedure di intervento (incident management, remote response, on site troubleshooting, spare part management, escalation...)
- Modalità di accesso ai locali
- Modalità di accesso agli apparati
- Istruzioni di troubleshooting per incident management

Configuration Management

È richiesto al fornitore di provvedere al salvataggio periodico delle configurazioni al fine di poter garantire l'eventuale sostituzione di apparati guasti a parità di funzionalità implementate

Incident Management

A seconda dei vari livelli di servizio minimi richiesti per ciascun elemento costituente l'infrastruttura il fornitore dovrà descrivere nella proposta tecnica il servizio di incident management che si impegna ad erogare secondo gli SLA opportuni. Il dettaglio di tecnologie, parti, argomenti oggetto del servizio richiesto è descritto nel capitolo "Perimetro" del presente capitolato tecnico.

Seguono alcune caratteristiche minime per il servizio richiesto:

- Single Point Of Contact erogato da tecnici qualificati
- Supporto di primo livello erogato da tecnici qualificati sulle tecnologie a perimetro
- Supporto di secondo livello erogato da tecnici specialisti su tecnologie e argomenti a perimetro
- Gestione escalation a vendor/terze parti
- Coordinamento di eventuali gruppi diversi (fornitore, cliente, vendor, terza parte) eventualmente coinvolti nella risoluzione dell'incident

Problem Management

Il fornitore è tenuto a descrivere la struttura preposta e le modalità di erogazione di un servizio di problem management richiesto all'interno del servizio. A titolo esemplificativo e non esaustivo si richiedono:

- In caso di incident ripetuti: analisi root cause, proposta soluzione, eventuale implementazione
- In caso di implementazione workaround: individuazione, proposta, eventuale implementazione di change volti a fornire una soluzione definitiva

Sono preferite soluzioni che prevedano chiare procedure dedicate e flow chart esplicativi del flusso di gestione.

Spare parts management

È compito del fornitore garantire la gestione della sostituzione parti. Il fornitore è tenuto a descrivere le modalità di erogazione del servizio che intende proporre.

Hardware maintenance

All'interno del servizio, per il periodo richiesto, per tutte le tecnologie/parti indicate il fornitore è tenuto a garantire l'hardware replacement.

Vendor Service

È compito del fornitore garantire:

- Gestione di eventuali anomalie sia esse di natura HW che SW ed accesso al servizio TAC erogato dal fornitore

- Hardware replacement
- Supporto per la gestione dei ticket aperti alla TAC del vendor
- Intervento on site da parte del vendor o del fornitore
- Supporto specialistico erogato da parte del fornitore

Il fornitore è tenuto a descrivere le modalità di erogazione del servizio che intende proporre.

On site troubleshooting

È richiesto l'intervento on site da parte di System Engineer qualificato nell'ambito tecnologico opportuno. L'obiettivo del personale del fornitore on site è il ripristino dell'operatività. Per questo vengono considerate preferenziali proposte in cui l'intervento on site venga garantito attraverso l'impiego di personale specialistico, qualificato già a conoscenza della realtà del cliente

Ticketing

È richiesto al fornitore un sistema di ticketing che consenta la gestione completa del servizio richiesto con particolare riferimento a incident management, problem management, spare parts management, hardware replacement, on site troubleshooting

Software Assurance

È richiesto al fornitore di garantire tramite vendor subscription la disponibilità di aggiornamenti software per bug fixing, minor/major release

SLA

PROCESSO	QUALIFICAZIONE	INTERVENTO	COPERTURA ORARIA
Accesso al servizio per supporto remoto specialistico ed eventuale escalation a vendor/terza parte	Max 2 ore	NBD	Lunedì-venerdì (festivi esclusi) 8:30-13:00, 14:00-17:30
Fornitura Spare Parts con intervento on site tecnico qualificato		NBD	Lunedì-venerdì (festivi esclusi) 8:30-13:00, 14:00-17:30

I tempi di intervento indicati in tabella non sono intesi da sommarsi l'uno all'altro.

Durante la qualifica è richiesto che il supporto specialistico identifichi quali azioni (tra ulteriori indagini/escalation, fornitura della parte di ricambio e intervento on site) sono necessarie per il ripristino dell'operatività.

Modalità di accesso al servizio

Il fornitore è tenuto a descrivere le modalità di accesso al servizio chiarendo eventuali differenze legate a tecnologie o fasce orarie.

Si richiede inoltre la descrizione delle best practices / standard/ tecnologie implementate per garantire riservatezza, accessibilità, sicurezza, disponibilità.

È considerato come requisito minimo l'accesso tramite mail, telefono, portale web.

8. Modalità di pagamento

Sono di seguito indicate le modalità di pagamento previste nelle varie fasi operative.

Fase Operativa	Pagamento di:
Attivazione del contratto di manutenzione Cisco e Checkpoint	80% del corrispettivo contrattuale
31/12/2022	5% del corrispettivo contrattuale
31/12/2023	5% del corrispettivo contrattuale
31/12/2024	5% del corrispettivo contrattuale
31/12/2025	5% del corrispettivo contrattuale

Per accettazione

(Data e firma digitale del Legale Rappresentante)