Capitolato tecnico

PROCEDURA PER L'AFFIDAMENTO DELLA FORNITURA DI DISPOSITIVI E SERVIZI FINALIZZATI ALLA TRASFORMAZIONE DIGITALE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA MISSIONE 1 COMPONENTE 1, FINANZIATO DALL'UNIONE EUROPEA ALL'INTERNO DELL'INIZIATIVA NEXTGENERATIONEU - INVESTIMENTO 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI – Comuni Luglio 2022"

Revisione infrastruttura Network Security del Comune di Reggio Emilia

CPV 48730000-4

CUP J81C22001570006 - CIG A0078CD0F1 –

CUI F00145920351202200014

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Sommario

1 – Contesto di Riferimento

Il Comune di Reggio Emilia ha deciso di riallocare i propri sistemi server in un data center privato gestito da Lepida S.c.p.A.
A seguito di questa riconfigurazione si rende necessario riprogettare l'infrastruttura di rete per adattarsi alle nuove esigenze architetturali e gestire alti requisiti di sicurezza. Per realizzare questa riconfigurazione occorre sostituire l'attuale firewall on premise presente nel datacenter di Reggio Emilia, con una nuova infrastruttura di firewall virtuale da configurare nel datacenter del cloud Lepida.

Ad oggi sono presenti due appliance firewall Check Point installati in modalità "Open Server" aventi software GAIA R80.40; un server per la gestione centralizzata installato su VM avente soft-ware GAIA R81.10 ed una appliance Check Point dedicata al processo di sandboxing file avente software GAIA R81.10.
Ad oggi i firewall lavorano in cluster active-passive (HA) e gestiscono il ruolo di default gateway per le seguenti zone di rete:

- Link a ISP (Internet)
- Lepida Guest
- Guest
- SAP IREN
- Videosorveglianza
- VoIP
- Anagrafe
- PMV
- Internet-Point
- OCR
- Link a Provincia RE
- Wi-Fi dispositivi mobili
- Management AP
- Data store Lepida
- Timbratori scuole
- PC client
- DMZ Internet
- Server
- Management server

Le macro funzionalità attive sui sistemi firewall sono:

- Network ACL
- Web Filter e Web Application Control
- HTTPS Inspection
- IPS

- Anti-Virus perimetrale
- Anti-Bot
- Sandboxing per gli allegati ricevuti via mail e i download via web browser
- VPN StS
- VPN client

2 - Definizioni e acronimi

- Committente: Comune di Reggio Emilia;
- Esecutore: operatore economico affidatario;
- Gbps/s, Gb/s: Gigabit per secondo;
- Mbps/s, Mb/s: Megabit per secondo;
- CP: Check Point
- SGW: Security Gateway (Firewall)
- SMS: Security Management Server
- GAIA OS: Nome del sistema operativo Check Point Firewall
- Open Server: Macchina server prodotta da aziende non legate a Check Point il cui mo-dello è certificato per essere pienamente compatibile con GAIA OS
- VM: Virtual Machine;
- IPS: Intrusion Prevention System;
- MFA: Multi Factor Authentication;
- DCFW: Data Center Firewall;
- ISFW: Internal Segmentation Firewall;
- FWAaS: Firewall As A Service;

3 - Sedi destinazioni della fornitura

Le sedi interessate saranno:

Comune di Reggio Emilia – Piazza Scapinelli 2, 42121, Reggio Emilia

Lepida S.c.p.A. - Ferrara

4 – Oggetto della fornitura

La nuova infrastruttura di firewall, oggetto della presente fornitura, è così composta:

- Fornitura e configurazione degli apparati firewall per la sede del Comune di Reggio Emilia da dedicare alle zone di rete che verranno mantenute on-prem;
- Fornitura licenze per sistema di management su piattaforma VMware con funzionalità di policy server, log server e smart event.
- Fornitura e configurazione degli apparati firewall virtuali per il data-center in Lepida da dedicare alla protezione delle zone server, alla navigazione web, alla pubblicazione dei servizi su internet e all'accesso VPN StS / client;
- Fornitura e configurazione della soluzione per il controllo e la protezione dei PC portatili quando questi ultimi non saranno all'interno dei locali dell'ente (smart working);
- Redazione ed implementazione del progetto tecnico ed esecutivo di dettaglio per la soluzione architetturale.

Tutte le attività dovranno essere svolte in modalità training on-the job e al termine il personale dell'ente dovrà essere autonomo nella gestione quotidiana del firewall (attivazione di nuove regole, attivazione di nuove vlan/interfacce, gestione IPS, attivazione accessi VPN, ecc) e in grado di effettuare un filtro di primo livello in caso di problemi.

A. DESCRIZIONE DELLA FORNITURA

In questo paragrafo è descritta l'architettura che dovrà consentire il raggiungimento degli obiettivi generali di progetto. È importante sottolineare che l'architettura proposta costituisce una architettura di alto livello che dovrà quindi essere sviluppata e dettagliata dalla ditta affidataria in ciascuna delle componenti descritte e che dovrà tenere conto degli obiettivi e dei requisiti funzionali e tecnologici riportati nel presente documento. L'azienda esecutrice dovrà pertanto produrre il progetto tecnico di dettaglio e occuparsi dell'implementazione della soluzione proposta compatibilmente con i tempi e le modalità descritte all'interno del progetto esecutivo.
Ad oggi è presente un'unica istanza firewall rappresentata da un cluster di firewall hardware installati in modalità HA (active-passive). Il primo obiettivo della nuova architettura di rete consisterà nella divisione delle zone di rete in due istanze firewall; quest'ultime saranno rappresentate da un DCFW (Data Center Firewall) e da un ISFW (Internal Segmentation Firewall).
La tecnologia scelta dall'ente per questi due nuovi sistemi di network security è Check Point, questo è motivato da diversi elementi quali:

- La conoscenza ed esperienza maturata della soluzione da parte dei sistemisti interni al Servizio Tecnologie ed infrastrutture del Comune di Reggio Emilia,
- Il mantenimento delle attuali policy di sicurezza,
- La riduzione dei rischi derivati dalla migrazione alla nuova architettura,
- L'affidabilità dimostrata negli anni,
- Il riconoscimento di un alto valore da parte del mercato.

Le attuali zone di rete gestite dall'unico firewall on-prem verranno divise tra i due "layer" DCFW e ISFW con una proporzione indicativa di 60-40 (il 60% delle vlan verranno migrate sul DCFW e il resto verrà mantenuto sul FW on-prem).

Il collegamento tra i due siti sarà gestito tramite routing, per questo motivo sono state previste due interfacce dedicate (una per il DCFW ed una per il ISFW).

Il traffico ricevuto dal DCFW tramite la nuova interfaccia denominata "Link con CED Comune RE" dovrà essere autorizzato tramite una policy di tipo zone-based poiché tutte le connessioni saranno già state filtrate a priori sul ISFW.
Il traffico ricevuto dal ISFW tramite la nuova interfaccia denominata "Link con DC Lepida" dovrà essere autorizzato tramite una policy di tipo zone-based poiché tutte le connessioni saranno già state filtrate a priori sul DCFW.

È richiesto che ogni istanza firewall abbia un policy package dedicato.

Per poter garantire lo stesso livello di sicurezza in ufficio e in mobilità, la fornitura dovrà prevedere un sistema di FWAaS in cloud (SASE). Questa soluzione dovrà garantire le stesse funzionalità attivate sui sistemi DCFW. La tecnologia scelta per questa tematica è Check Point Harmony Connect Internet Access che dovrà essere licenziato per 120 utenti.

La descrizione dei requisiti tecnici per ogni macro soluzione è stata suddivisa nei seguenti sotto paragrafi:

- B.1 Requisiti tecnici relativi all'ambiente firewall
- B.2 Requisiti tecnici relativi al controllo della navigazione web in mobilità

B. CARATTERISTICHE FUNZIONALI RICHIESTE

B.1 Requisiti tecnici relativi all'ambiente firewall

La fornitura prevede n.2 istanze di Firewall: una destinata alla sede ove presente il CED del committente (Reggio Emilia) e la seconda al datacenter di Lepida (Ferrara).

L'istanza DCFW dovrà avere le seguenti caratteristiche:

- Check Point CloudGuard for Private Cloud Security (Vmware): 8 vCPU totali che saranno divise sui due nodi del cluster active-passive
- 16 GB RAM per ogni VM
- 100 GB disco virtuale per ogni VM
- Release software GAIA OS R81.10 o R81.20
- Bundle di funzionalità Check Point NGTX
- Supporto Check Point Collaborative Standard

L'istanza ISFW dovrà avere le seguenti caratteristiche:

- Due appliance modello SGW 3600
  - Due rack mount
- Release software GAIA OS R81.10 o R81.20
- Bundle di funzionalità Check Point NGFW
- Supporto Check Point Collaborative Standard

Il server per la gestione centralizzata dovrà avere le seguenti caratteristiche:

- Next Generation Security Management Software per 5 gateways con SmartEvent da installare su VM Vmware
- Release software GAIA OS R81.20 o successiva
- Supporto Check Point Collaborative Standard

La funzionalità relativa al processo di sandboxing (Threat Emulation) dovrà essere migrata dall'attuale appliance dedicata on-prem al servizio SaaS in cloud.

Per quanto riguarda le licenze VPN client (MOB) si utilizzeranno quelle ad oggi presenti, per le quali è richiesto il rinnovo del servizio Check Point.

B.2 Requisiti tecnici relativi al controllo della navigazione web in mobilità

La fornitura prevede l'attivazione del servizio di tipo Secure Access Service Edge (SASE) di Check Point chiamato Harmony Connect Internet Access che dovrà essere licenziato per 120 utenti. La soluzione dovrà gestire policy per gli utenti in mobilità (smart worker) relative a tutto il pacchetto di funzionalità NGTX. Il controllo del traffico da parte della soluzione SASE dovrà avvenire unicamente quando il PC si troverà fuori dagli uffici dell'ente, sarà quindi configurato il meccanismo denominato "on-net / off-net".

5 Fasi di realizzazione del progetto

La gestione del progetto dovrà essere eseguita nella seguente modalità:

1. Preparazione e consegna al committente del Low Level Design in cui si indicheranno tutte le informazioni dettagliate relative alle due istanze firewall quali: vlan id, nome interfacce fisiche, indirizzamenti IP;
2. Preparazione e consegna al committente di un GANTT che dovrà essere mantenuto aggiornato;
3. Installazione VM dedicate all'istanza firewall DCFW configurando unicamente la vlan di punto-punto con il CED del Comune di RE;
4. Preparazione nuovo policy set dedicato all'istanza firewall DCFW (il punto di partenza dovrà essere un clone del policy package installato sul precedente firewall);
5. Migrazione per step delle vlan interessate dal firewall che dovrà essere dismesso all'istanza DCFW;
6. Preparazione in laboratorio dei firewall dedicati all'istanza ISFW;
7. Preparazione nuovo policy set dedicato all'istanza firewall ISFW (il punto di partenza dovrà essere un clone del policy package installato sul precedente firewall);
8. Installazione firewall dedicati all'istanza ISFW in armadi dati CED;
9. Migrazione da attuali firewall open server HP a nuovi SGW 3600 Check Point;
10. Attivazione nuovo tenant Check Point Infinity per quanto riguarda la soluzione SASE Harmony Connect Internet Access;
11. Configurazione policy Harmony Connect Internet Access;
12. Installazione client Harmony Connect su una prima tranche di PC di test;
13. Fine tuning policy Harmony Connect Internet Access;
14. Installazione client Harmony Connect su una seconda tranche di PC;
15. Fine tuning policy Harmony Connect Internet Access;
16. Distribuzione client Harmony Connect sui PC restanti;
17. Revisione delle policy relative al Mobile Access e dismissione delle "Legacy Policy" per le "Unified Access Policy"
18. Preparazione e consegna al committente della documentazione di fine lavori;
19. Attivazione servizi di post vendita

6 Assistenza e durata servizio

Le licenze ed il supporto di assistenza da parte del Vendor Check Point per tutti gli articoli oggetto della fornitura dovranno avere una **durata di tre ann**i a decorrere dalla data del collaudo con esito positivo.

7 Tempi di realizzazione e collaudo

L'attuale sottoscrizione riguardante le licenze Check Point ha scadenza 31 Agosto 2023; nel caso in cui la nuova infrastruttura non venga attivata entro tale data, sarà cura dell'azienda fornitrice garantire la continuità del servizio.
Si richiede che l'infrastruttura descritta in questo capitolato venga installata, configurata e collaudata entro quattro mesi dalla data di stipula del contratto.
Il collaudo della fornitura potrà avvenire solo successivamente alla "verifica di conformità" indicata all'art. 6, lett. B del Capitolato d'oneri- Disciplinare.
Eventuali ritardi non saranno conteggiati per cause di forza maggiore. Dopo autorizzazione del Responsabile di Progetto dell'Ente, le attività potranno proseguire oltre tale termine.

IL DIRIGENTE
(Ing. Andrea Bertani)

ANDREA BERTANI
COMUNE DI REGGIO NELL'EMILIA
24.08.2023 16:28:11
GMT+01:00