ALLEGATO TECNICO

1. Premessa

La fornitura consiste in tutto quanto necessario ad attivare la tecnologia CheckPoint SandBlast all'interno della rete del Comune di Reggio Emilia.
L'ente ritiene infatti prioritario attivare un sistema che permetta di prevenire l'ingresso di ramsomware (vedi CryptoLocker, Wannacry, Petya) che potrebbero rendere inaccessibili tutti i documenti dell'ente e/o provocare il furto di dati personali o riservati. Questi malware entrano generalmente attraverso le mail (come allegati o link su cui l'utente viene invitato a cliccare). Questi malware spesso non vengono intercettati dagli antivirus poiché utilizzano sempre nuove "firme" che vengono intercettate dagli strumenti tradizionali (antivirus, antispam) solo dopo un certo lasso di tempo dall'entrata in circolazione del malware, esponendo così la rete ad attacchi. La tecnologia SandBlast, che puo' operare sia a livello di difesa perimetrale che come agente installato sui singoli end-point, non utilizza i sistemi usati classicamente da antivirus / antispam ("firme", tipologia/formato della mail, classificazione del mittente) ma simula l'esecuzione dei contenuti "pericolosi" in un ambiente isolato in modo da verificare se sono nocivi. SandBalst lavora inoltre sia sugli allegati delle mail (ad esempio documenti di Office che contengono macro che mandano in esecuzione malware) che su oggetti scaricati inavvertitamente dall'utente quando cerca di entrare nel link indicato nel testo della mail (es: javacript).
Per far ciò si utilizza un'appliance hardware installata presso la sala server dell'ente e componenti software installati sui due gateway del firewall. I componenti sw intercettano l'allegato e/o il modulo scaricato da internet e, prima di renderlo disponibile all'utente, lo passano all'appliance che tenta di eseguirlo su un insieme di macchine virtuali rappresentative del parco pc (ad esempio con diverse versioni dei principali sistema operativi, di Office/Libreoffice, jvm, vari plug-in, ecc). In questo modo il sistema verifica se si tentano di fare operazioni "non lecite" che generalmente indicano la presenza di un malware.

L'ente sta utilizzando gia il firewall CheckPoint e ha deciso di attivare questa ulteriore difesa nella modalità perimetrale ed on premise poiché si integra e completa il sistema già in uso. In questo modo possono essere utilizzati i due nodi del firewall per installare il nuovo software, evitando di avere punti che, in caso di malfunzionamenti, provochino interruzione di servizi. Inoltre dal punto di vista della gestione si utilizzano gli stessi strumenti che i sistemisti del Servizio Gestione e Sviluppo delle Tecnologie già conoscono per amministrare il firewall CheckPoint.

2. Descrizione situazione iniziale

L'ente ha installato un'architettura Firewall Check Point composta da:

- N.1 Virtual Appliance Security Management Server Check Point installata sull'infrastruttura VMWARE dell'ente con supporto per *2 gateway e* comprensiva delle *seguenti blade di management*:
  - Network Policy Management
  - Endpoint Policy Management
  - Logging & Status
  - Monitoring
  - User Directory
  - SmartReporter
  - SmartEvent

- N.2 Gateway Check Point con bundle Next Generation Threat Prevention, NGTP, su piattaforma Open Certified Server con licenza 8 core. Sono incluse i seguenti moduli/blade
  - Firewall
  - VPN
  - Advanced Networking & Clustering
  - Identity Awareness
  - Application Control (*)
  - URL Filtering (*)
  - Anti-Virus (*)
  - Intrusion Prevention System (*)
  - Antibot (*)
  - Antispam (*)

  (*) Per le Service Blade indicate il servizio è licenziato fino al 18/3/2019

  I due Gateway sono installati su una coppia di Server HP DL360p Gen9, presenti nell'hardware compatibility list di CheckPoint, ognuno con le seguenti caratteristiche:
    - Processore Intel E5-2630V3 con 8 core
    - Memoria, 16GB
    - Dischi, 3 x 300GB 12G SAS in configurazione Raid 1 + spare
    - Network Interface, 8 porte Gigabit Ethernet 1000 Base Tx
    - Alimentazione singolo 500W

- Supporto hardware/software di tipo Collaborative Enterprise Standard Edition comprensivo del rinnovo dei servizi a canone attivo fino al 18/3/2019.

L'elenco del software/servizi CheckPoint attivi fino al 18/3/2019 è riportato nella seguente tabella

CODICE	DESCRIZIONE	Q.TÀ'
CPSG-P807	Check Point Open Server Gateway Licence for 8 Core, 7 blades	1
CPSG-P807-HA	Check Point Open Server Gateway Licence for 8 Core, 7 blades for HA	1
CPSM-P205	Check Point Security Management for 2 gateways and 5 blades	1
CPSB-EVS-C200	Check Point Smart Event and Reporting blades	1
CPSB-NGTP-L-3Y	Service Bundle servizi Next Generation Threat Prevention 3 years	1
CPSB-NGTP-L-3Y-HA	Service Bundle servizi Next Generation Threat Prevention 3 years for HA	1
Renewal MOB 50 user 3 years	Renewal MOB 50 user 3 years	1
Renewal MOB 50 user 3 years	Renewal MOB 50 user 3 years	1
CPCES-CO-STANDARD 3Y	Collaborative Enterprise Support Standard Edition 3 year	1

3. Descrizione della fornitura

La fornitura consiste in:

1. Appliance SandBlast TE250X con licenza NGTX installata presso la sala server dell'ente
2. Upgrade del software dei due Gateway Check Point con bundle NGTP, su piattaforma Open Certified Server con licenza 8 core al package NGTX.
3. Licenziamento di tutte le blade previste sia sull'appliance che sui due gateway fino 31/3/2020
4. Supporto hardware/software di tipo Collaborative Enterprise Standard Edition per tutta la soluzione CheckPoint (2 Gateway NGTX, Virtual Appliance Security Management Server, Appliance TE250X) fino al 31/3/2020
5. Attività di installazione e configurazione della soluzione da effettuarsi PREFERIBILMENTE on site ed in collaborazione con il personale del Servizio Gestione e Sviluppo Tecnologie dell'ente

Fare riferimento alla tabella sotto per l'elenco dei codici CheckPoint

Cod. CheckPoint	Descrizione	Fino al
CPAP-SBTE250X-8VM	TE Appliance TE250X	
CPEBP-NGTX	Blades NGTX per 2 gateways CPSG-P807	31-03-2020
CPCES-CO-STANDARD	Manutenzione Collaborative Standard fino al 31-03-2020 per TE250X	31-03-2020

CPCES-CO-STANDARD	Manutenzione Collaborative Standard (base installata) fino al 31-03-2020	31-03-2020

L'account ID del Comune di Reggio Emilia è **5962797**

4. Condizioni di fornitura

Fornitura ed inizio delle attività di installazione: entro 30 giorni solari dall'ordine
Collaudo: il collaudo con esito positivo e sottoscritto fra le parti, deve essere effettuato entro 2 mesi dall'inizio attività

IL DIRIGENTE
(Dott.ssa Lorenza Benedetti)

BENEDETTI LORENZA
Firmato digitalmente da BENEDETTI LORENZA
Data: 2017.12.18 09:00:54 +01'00'