Allegato A

Fornitura di apparati Firewall di tipologia Next-Generation per il potenziamento dell'infrastruttura di rete dell'Unione delle Terre d'Argine

Relazione tecnica

I tecnici del Settore Sistema Informativo Associato (S.I.A.) Area Reti e sistemi dell'Unione delle Terre d'Argine, considerati gli apparati presenti attualmente in ambiente di Produzione nell'infrastruttura di rete, intendono procedere all'acquisto di n. 2 (due) nuovi dispositivi Firewall di tipologia Next-Generation Security della marca *Palo Alto Networks*, per le seguenti motivazioni:

- consentire l'interoperabilità effettiva, concreta e completa tra i due Firewall che si intendono acquistare e il Firewall di Palo Alto Networks già presente ed installato presso il Comune di Novi di Modena: tale interoperabilità, per tutte le funzioni degli apparati, si realizza solo tra apparati della stessa marca;
- realizzare economie di gestione utilizzando una sola tecnologia;
- sincronizzare le Policy, importare quelle già esistenti e creare template a livello di oggetti, regole, device etc riutilizzandole con la nuova infrastruttura;
- mantenere ed utilizzare tutte le conoscenze già acquisite dal personale tecnico del S.I.A. per quanto concerne configurazione, aggiornamenti software, diagnostica e risoluzione dei problemi su Firewall Palo Alto Networks;
- installare la stessa versione del software PAN-OS su tutte le appliance, fisiche e virtuali di Palo Alto Networks: le stesse policy applicate ai firewall più piccoli possono essere esportate ed importate su modelli più performanti e/o virtuali;
- esportare e importare la configurazione da un dispositivo Palo Alto Networks ad un altro, mantenerla as-is o modificarla ed adattarla in caso di esigenze differenti, in caso di fail/necessità di replacement/migrazione o ripristino: tale gestione delle configurazioni offre la possibilità di ripristinare le funzionalità di un apparato in seguito ad un evento avverso tra le sedi di Novi di Modena e di Carpi consentendo le connessioni alla rete attraverso il firewall del sito remoto semplicemente importando ed eventualmente modificando la configurazione del firewall del sito down;

- avere un'unica appliance fisica evitando così l'utilizzo di macchine virtuali per la gestione dei firewall che in caso di problemi ai server VMware renderebbero il firewall ingestibile;
- avere la possibilità di deviare il traffico di rete per vie alternative (Policy Based Routing) utilizzando l'applicazione come criterio: ad esempio, deviare un'applicazione specifica verso una diversa Linea Adsl rispetto alla connessione Internet principale (default gateway);
- avere allo stesso tempo il supporto di diverse modalità di funzionamento delle interfacce: L3, L2, Bridge, TAP, sulla stessa istanza di firewall fisica o istanza virtuale sulla stessa macchina fisica;
- avere la possibilità di riconoscere l'applicazione, il contenuto (minacce) e l'utente in un unico passaggio, senza buffering del traffico di rete;
- avere la capacità di permettere, bloccare e controllare in maniera flessibile i file type che vengono trasportati tramite diverse applicazioni di rete, come specificato nell'esempio seguente:

- utilizzare un firewall in cui l'ingegnerizzazione hardware e software preveda una distinzione tra la componente di firewalling/enforcement e quella di gestione, in modo tale che problematiche su quest'ultima non siano bloccanti per l'analisi del traffico. Questa distinzione prevede hardware dedicato al contesto di gestione, quale: CPU, Storage, RAM, schede di rete e hardware dedicato al contesto di firewall quale: CPU , FPGA, RAM e Schede di rete.

Carpi, 10/12/2015

Settore S.I.A.
Sistema Informativo Associato