SCHEDA TECNICA - LOTTO 1
"FORNITURA E POSA IN OPERA DI 2 FIREWALL"

Caratteristiche tecniche per la piattaforma firewall. Architettura costituita da almeno 2 dispositivi in HA. La fornitura si intende comprensiva di installazione e configurazione di base. Gli apparati oggetto della fornitura devono essere necessariamente in produzione al momento dell'offerta con annessa dichiarazione da parte del fornitore a pena di esclusione.
Ogni dispositivo deve avere le seguenti caratteristiche minime a pena di esclusione:

- Statefull Inspection Firewall
- IPS – Intrusion Prevention System
- Application Firewall (Layer 7 Firewall)
- Web Application Firewall
- IPv6 full compliant
- Firewall throughput (1) - almeno 2Gbps
- Threat throughput (2) - almeno 1Gbps
- Nuove sessioni al secondo - almeno 10.000
- Sessioni concorrenti - almeno 200.000
- Interfacce:
  - Copper GbE Ports – almeno 4
  - Fiber 1GbE Ports – almeno 2
- High Availability:
  - Active-Active
  - Active-Passive with State Synchronization
  - Stateful failover
- Administration e System Management
  - Web GUI
  - Role-based access control
  - Command Line Interface (Serial, SSH, Telnet)
  - SNMP v2 e v3
- VPN:
  - IPSec – almeno 200 tunnel
  - SSL – almeno 200 utenti contemporanei
- Bandwidth Management
- Anti-Virus
- Anti-Spyware
- SSL inspection sia dai client verso Internet che viceversa.
- Virtual Systems – almeno 2
- Networking:
  - PBR – Policy Based Routing
  - Dynamic routing protocols:
    - RIP v1 e v2
    - OSPF
    - BGP
  - Multicast Forwarding Protocols
- Assistenza Next Business Day e aggiornamenti per almeno 3 anni.
- Architettura hardware dedicata.

- Risorse hardware distinte e dedicate per il piano di controllo ed il piano di inoltro per garantire la massima affidabilità.
- Disco per il mantenimento dei log e dello storico delle configurazioni – almeno 1
- Funzionalità di destination NAT e source NAT, con mappatura sia molti-a-uno che uno-a-uno.
- Controllo applicazioni sconosciute:
  - Mediante policy di firewalling specifiche
  - Mediante la creazione di signature custom
- Aggiornamenti del motore Anti-Virus e quelli delle applicazioni riconosciute devono essere almeno settimanali.
- Criterio di selezione delle regole di firewalling mediante categoria dell'URL per l'attivazione di controlli IPS, Anti-Virus e blocco file differenti per categorie di siti differenti.
- Applicazione di profili di Anti-Virus, Anti-Spyware, blocco dei file e IPS differenziati in base alla policy di firewalling e all'applicazione rilevata.
- Autenticazione degli utenti mediante server Kerberos, Active-Directory, LDAP e RADIUS.
- Autenticazione degli utenti via captive portal.
- Applicazione di profili di firewalling, IPS, Anti-Virus e QoS in base all'utente.
- Modalità trasparente passante (forwarding basato sull'interfaccia fisica di ingresso e non basato su MAC o su IP), layer3 e tap.
- Esportazione di log via syslog.
- Salvataggio di configurazioni in modo da poterle richiamare nel caso si renda necessario ristabilire velocemente un servizio interrotto a causa di una configurazione errata.

(1) Il firewall throughput deve essere calcolato con traffico IMIX e Application Identification abilitato per tutti i protocolli/applicativi.
(2) Il threat throughput deve essere calcolato con traffico IMIX e Application Identification, Anti Virus, Anti Spyware e IDP abilitati per tutti i protocolli/applicativi.

Per IMIX si intende traffico distribuito in maniera lineare da 64KByte a 1500KByte.

Costituiscono caratteristiche migliorative ma non essenziali:

- Maggiore firewall e threat throughput (bps) 5pt.
- Maggior numero di nuove sessioni al secondo (numero) 5pt.
- Maggior numero di sessioni concorrenti (numero) 7pt.
- Maggior numero di porte (numero) 15pt.
- Maggiore estensione di garanzia (tempo) 3pt.
- Sistema per l'analisi forense dei log integrato nella console del firewall (si o no) 15pt.
- Virtual Systems forniti (numero) 15pt.
- Analisi dei malware su sistemi cloud e successivo rilascio patch (si o no) 15pt.