SEGRETARIATO GENERALE della GIUSTIZIA AMMINISTRATIVA

Servizio Centrale per l'Informatica e le Tecnologie di Comunicazione

Ufficio Sistemi e Processi

Capitolato tecnico

Strumenti McAfee: licenze, servizi di manutenzione e supporto specialistico

Sommario

1.SITUAZIONE ATTUALE

Questa Amministrazione utilizza apparati e sistemi di sicurezza prodotti dalla società Mcafee a partire dal 2009. Le tecnologie McAfee, integrate nei sistemi della G.A., sono state implementate sia a livello centralizzato, mediante l'uso di sistemi di prevenzione delle intrusioni e filtraggio del traffico web, sia a livello periferico con la diffusione di strumenti di antivirus e antimalware.

In modo particolare, i prodotti oggi in possesso dell'Amministrazione sono di seguito elencati:

1) **Suite protezione end point**
   - Console centralizzata ePO, per la gestione della suite di sicurezza del parco macchine
   - Modulo Antivirus
   - Host intrusion prevention
   - MOVE, antivirus ottimizzazione per le macchine virtuali
2) **Protezione navigazione web**
   - Webgateway implementato come proxy (su macchina virtuale) per il filtraggio delle URL e la protezione antimalware durante la navigazione web delle postazioni di lavoro.
3) **Network Intrusion Protection System**
   - Network Manager, per la gestione centralizzata del sistema di Intrusion Prevention
   - Sensori di rete per il rilevamento di attacchi di rete e sistemi antibotnet.
4) **Firewall Enterprise**
   - Protezione perimetrale e la segmentazione di rete.
5) **Vulnerability Manager**
   - Appliance per la verifica e la reportistica automatica delle vulnerabilità dei sistemi target.

Per quanto riguarda le componenti per la protezione end-point installate presso il Consiglio di Stato, si specificano alcuni dettagli di alcune funzionalità core per ciascuna componente:

- **ePolicy Orchestrator 5.1**: Console di Management centralizzata in grado di gestire la suite dei prodotti McAfee e che consente un controllo della conformità delle politiche di sicurezza e la protezione dei nodi dell'intera infrastruttura;
- **Virus Scan Enterprise 8.8**: è un'applicazione che, tramite una tecnologia antivirus avanzata, consente di proteggere i server e le workstation dalle minacce più comuni derivanti da e-mail, connessioni web, accesso ai siti FTP, ecc. Essa integra anche il modulo software aggiuntivo (AntiSpyware Enterprise) che consente di identificare spyware e programmi potenzialmente dannosi con la stessa tecnologia di scansione dell'applicazione antivirus.

- **Database**: consiste nello storage centrale utilizzato dall'applicazione ePolicy Orchestrator per memorizzare tutti i dati generati ed utilizzati;
- **ePolicy Orchestrator Agent**: è un modulo software che consente lo scambio di informazioni tra il sistema gestito e l'ePolicy Orchestrator Server. L'agent è il mezzo con cui ogni nodo prende gli aggiornamenti, le politiche ed i task implementati sul server.
- **Host Intrusion Prevention System**: con questa applicazione viene garantita la protezione dell'infrastruttura informatica dalle minacce complesse di sicurezza, mediante un livello di protezione basato su firme ed incorpora, inoltre, uno statefull firewall. Questo componente software ha pertanto il compito di proteggere l'Amministrazione dalle minacce note, inclusi gli attacchi zero-day. Gli aggiornamenti automatici delle firme consentono anche di bloccare l'esecuzione delle minacce emergenti compresi gli attacchi di buffer overflow;
- **McAfee Management for Optimized Virtual Environments (MOVE)**: è una soluzione ottimizzata per la protezione antivirus avanzata nei desktop e nei server virtualizzati, installata sui sistemi dell'Amministrazione. Essa, utilizzabile con tutti i principali hypervisor, permette di non avere agent installati sui sistemi virtuali utilizzando VMware NSX e VMware vCloud Networking and Security.

Di seguito, in figura 1, lo schema dell'architettura di front-end dell'Amministrazione:

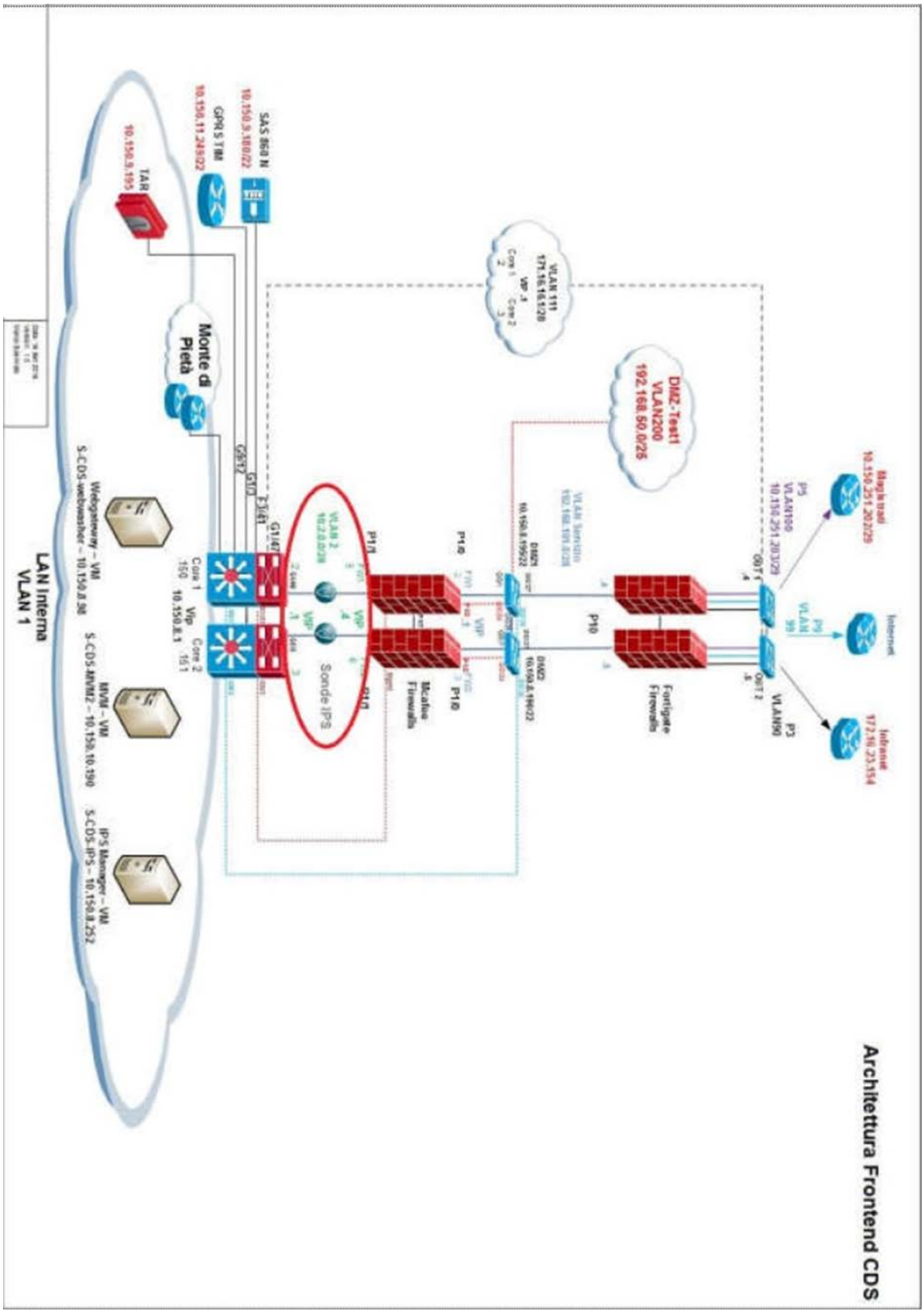

Figura 1. Architettura di front-end del Consiglio di Stato.

2. OGGETTO DELLA FORNITURA

Con la finalità di salvaguardare l'investimento tecnologico effettuato negli ultimi anni e dovendo assicurare il necessario aggiornamento e supporto tecnologico dei sistemi di sicurezza in uso, si rende indispensabile effettuare un'acquisizione che assicuri:

1. il rinnovo delle licenze software e canoni di manutenzione per gli apparati McAfee già in uso;
2. il potenziamento del livello di sicurezza/protezione sui sistemi dell'Amministrazione con l'acquisto del sistema SIEM;
3. la possibilità di un maggiore controllo e monitoraggio degli accessi con lo strumento ATD;
4. un servizio di supporto specialistico a consumo per 35 giorni uomo.

Per raggiungere gli obiettivi di potenziamento del livello di sicurezza e di monitoraggio degli accessi, si deve precedere all'acquisto di due nuove soluzioni McAfee, integrate nella piattaforma esistente e in uso presso l'Amministrazione.

In particolare il sistema ***SIEM,*** Security Information and Event Management, consente di associare, in un unico strumento, eventi particolari, minacce e rischi, per fornire un sistema di intelligence finalizzato ad assicurare risposte rapide in caso di necessità, una ininterrotta gestione dei log e una reportistica di ausilio. La soluzione deve essere scalabile, modulare e avere le caratteristiche di appliance; deve inoltre consentire la correlazione, la valutazione e la definizione di priorità su eventi di sicurezza rilevabili sia da sistemi di terze parti che da quelle McAfee.

Lo strumento di ***ATD*** di McAfee, Threat Intelligence Exchange, deve garantire la possibilità che in un unico sistema, tutti i prodotti di sicurezza presenti sui sistemi, lavorino in modo coordinato, individuino collettivamente le minacce, le mettano a fattor comune e agiscano come una difesa unificata dando resilienza alla protezione e immunità contro le infezioni da qualunque vettore di attacco arrivino. Tale strumento deve assicurare una migliore prevenzione delle minacce, riducendo significativamente i tempi tra l'individuazione del problema e la soluzione, e portando questi da alcuni giorni attuali a pochi millisecondi, quindi con una capacità di intervento quasi in modalità realtime.

Nella seguente tabella si forniscono gli elementi di dettaglio della fornitura con indicazione del codice prodotto su Mercato elettronico:

SKU	Product	Material Category	Nodes
IYVM35KADM	MFE Network Sec 3050 Sensor 1Yr GL+RMA	Support	1
IMTYCM-AD	MFE Network Sec Starter Mngr 1Yr GL	Support	1
IYVF35KADM	MFE Network Sec 3050 Sensor FO 1YrGL+RMA	Support	1
WAMYCM-AA	MFE Web Anti-Malware 1Yr GL	Support	2200
CEEYFM-AA	MFE Complete EP Protect Ent 1Yr GL [P+]	Support	2200
WSGYCM-AA	MFE Web Security 1Yr GL	Support	2200
MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrGL	Support	50
MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrGL	Support	70
FSWYCM-AA	MFE Vulnerability Mngr EN SW 1YrGL	Support	500
VYV3100ADM	MFE VulnrbiltyMgr MVM3100Appl 1Yr GL+NBD	Support	2
RBX850CG1	MFE NetSec XFPGbic 850nm 8K/6050 1Yr RMA	Support	2
TIECDE-AA	MFE Threat Intel Exchange P:1 GL [P+]	Perpetual License	2200
ATD-3000	MFE Adv Threat Def 3000 Standard HW	Appliance	1
ATD3000NBD	MFE Adv Threat Def 3000 Stand 1yrNBD	Support	1
MD-CONSULT-DY-Z1	Sol Svcs Custom Consult Daily (SEUR)	Consulting	35
ETM-4600-ELM	MFE Ent Sec Mgr, ELMand EvtRec 4600 Appl	Appliance	1
ETM4600ELMNBD	MFE Ent Sec Mgr Log Mgr 4600 1YrGL+NBD	Support	1
FE4016SWNE-X-XX12-R	Sidewinder S4016 Appliance Ext Warranty NBD 1 Yr	Support	2
PRSNN-X-CP12-R	Network Security Premium Support	Support	2
DSM-2600	MFE DB Event Monitor for SIEM 2600 Appl	Appliance	1
DSM2600NBD	MFE DB EvntMonitorforSIEM26001Yr GL+NBD	Support	1

Devono ritenersi comprese nel costo della fornitura le licenze d'uso dei prodotti e il relativo servizio di manutenzione. Il servizio di manutenzione delle licenze software dovrà comprendere tutte quelle attività necessarie per mantenere continuamente aggiornati i prodotti con le versioni rilasciate dalla casi produttrici.

Il fornitore dovrà mettere a disposizione dell'amministrazione un numero unico per la ricezione delle chiamate.

3. VERIFICHE DI CONFORMITÀ

A seguito di comunicazione da parte del Fornitore, e comunque entro e non oltre 60 giorni dalla data di stipula del contratto, l'Amministrazione procederà alla verifica di conformità della fornitura, che si concluderà con la redazione di apposito certificato di conformità.

Le operazioni di verifica di conformità si svolgeranno in due fasi:

- Fase 1: verifica inventariale
- Fase 2: verifica funzionale.

Durante la verifica inventariale, il Fornitore dovrà presentare ogni documentazione necessaria ad attestare l'effettiva consistenza della fornitura, sia in termini di licenze che di manutenzione.

La documentazione, che dovrà comprendere i codici dei prodotti forniti dalle case produttrici, sarà sottoposta ad approvazione da parte dell'Amministrazione.

Durante la verifica funzionale l'Amministrazione si riserva la facoltà di effettuare ulteriori motivate verifiche che ritenga opportuno, mirate ad accertare l'effettiva consistenza delle licenze software dei prodotti. In tal caso sarà possibile concordare un nuovo piano per terminare la verifica di conformità complessiva.

Il Fornitore deve garantire tutta l'assistenza necessaria e mettere a disposizione dell'Amministrazione tutte le apparecchiature e i mezzi essenziali per l'effettuazione delle verifiche.

4.RESPONSABILE DEL SERVIZIO

Al fine di consentire una ordinata e regolare esecuzione contrattuale, all'atto della stipula del contratto di fornitura il fornitore dovrà indicare un responsabile del servizio, eventualmente coincidente con il soggetto firmatario del contratto, che funga da interfaccia con l'Amministrazione per le comunicazioni relative ad aspetti logistici ed amministrativi, e più in generale che possa rappresentare il Fornitore.

Le comunicazioni, gli eventuali disservizi e/o inadempienze, comunicate al responsabile del servizio si intendono come direttamente presentate al Fornitore.

5. LIVELLI DI SERVIZIO E PENALI

L'impresa è obbligata in caso di malfunzionamento dei sistemi di sicurezza forniti, vale a dire in caso di qualsiasi anomalia funzionale che, anche indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza, a ripristinare la piena funzionalità del sistema.

Tale servizio di ripristino deve essere garantito tutti i giorni, compresi i festivi dalle ore 8.00 alle ore 19.00, per qualunque tipo di problema, con i seguenti livelli di servizio:

Livello di servizio	Caso di applicazione
SLA.1	Presa in carico del problema entro 2 ore dalla chiamata.
SLA.2	Intervento in loco entro 4 ore dalla chiamata

Il mancato rispetto dei termini previsti per gli SLA comporterà l'applicazione delle seguenti penalità.

Codice Penale	Livello di servizio	Penale
PE.1	SLA.1	Prevedere una penale pari al 0,15 per mille dell'importo netto contrattuale per ogni ora solare di ritardo.
PE.2	SLA.2	Prevedere una penale pari al 0,10 per mille dell'importo netto contrattuale per ogni ora solare di ritardo.