INFN
Istituto Nazionale di Fisica Nucleare

Commissione Calcolo Reti

Analisi TM

Alessandro Brunengo
per il gruppo mailing di CCR

Trend Micro IMSVA/IMSS

La licenza software acquistata da Trend Micro include due prodotti che implementano un filtro per la posta elettronica

- InterScan Messaging Security Virtual Appliance (IMSVA)
  - una appliance software che integra tutti i servizi
  - distribuita come immagine ISO, installabile su VM o su ferro
  - consiste in una Centos 6 con installazione custom di postfix, openldap, PostgreSQL, che affiancano la suite software IMSS
- InterScan Messaging Security Suite (IMSS)
  - pacchetto software da installare e configurare su server preesistente (”alla Sophos PM”)
  - supporta installazione su Postfix e Sendmail
  - piu’ flessibile ma manca di alcune funzionalita’ rispetto a IMSVA

Requirements

- IMSVA 9.1 patch 2 (30/03/2018)
  - Supporto per installazione su ferro
  - Vmware: ESXi 5.0 upd 3, 5.5 upd.2, 6.0
  - Hyper-V: Windows Server 2008 R2 SP1, 2012, 2012 R2
    Hyper-V Server 2008 R2 SP1, 2012 R2

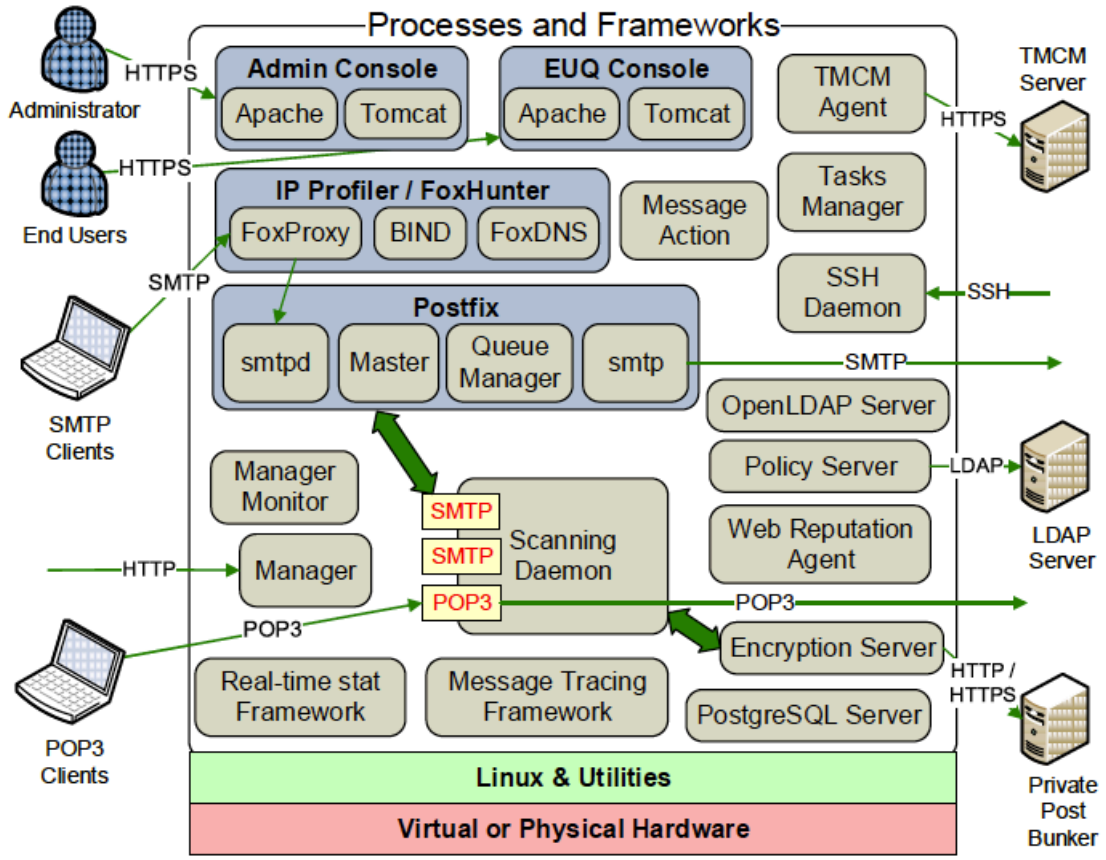
- IMSS 9.1 (29/09/2017)
  - RHEL 6.x, 7.x fino a 7.3

Requirements (cont.)

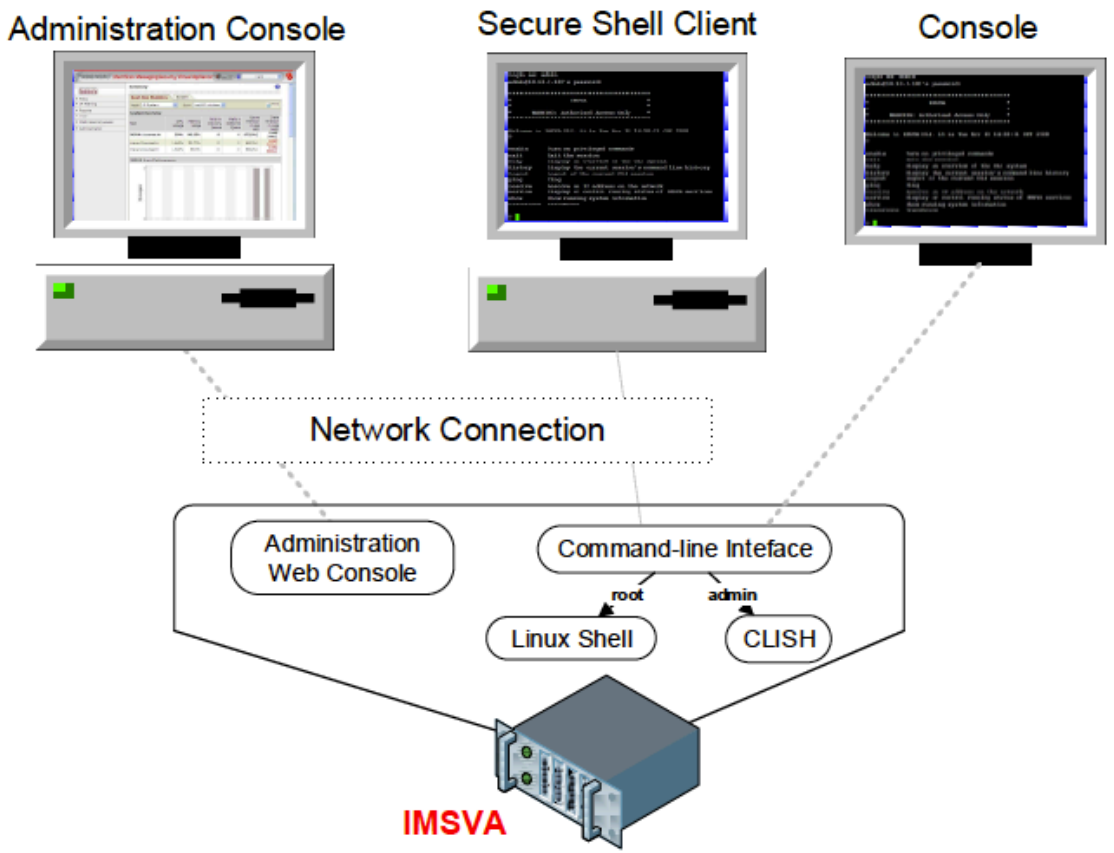
- IMSS/IMSVA: risorse consigliate:
  - CPU: 8 core Intel Xeon o equivalente, RAM: 8 GB, Disco: 250 GB

- Requirements sui server di appoggio
  - LDAP:
    - Microsoft Active Directory 2008 R2/2012/2012 R2
    - OpenLDAP 2.4.23
    - IBM Lotus Domino 8.0/8.5/9.0
    - Sun ONE LDAP 5.2 o superiore
  - Trend Micro Console Manager 5.5 sp1 patch 4 o 6.0 sp1 patch 3
  - TM Virtual Analizer 5.0, 5.5, 5.0

Architettura



Administration



Dove mettere il filtro

- Ci sono filtri che e' necessario applicare prima di eseguire la successiva analisi
  - IP reputation, che abbattono enormemente lo spam
  - esistenza del destinatario
- Va evitato il backscattering (filtri durante la sessioen SMTP)
- Questo requisito impone di installare il filtro sui relay di frontiera (MX)
- IMSVA (appliance) deve quindi sostituire gli MX attuali (o aggiungersi)
- IMSS puo' essere installato sugli MX in produzione, in sostituzione dell'attuale filtro utilizzato (Sophos PM o altro)

Sender filtering

- IP profiler, configurabile
  - analisi statistica su Spam, Virus, Directory Harvest Attack, Bounced Mail
  - intervalli temporali e soglie configurabili
  - azione configurabile in tipo (blocco permanente o temporaneo) e durata
- E-mail reputation
  - analisi standard (lo chiamano RBL+) su standard reputation database
  - analisi avanzata: aggiunge controllo su db che fanno analisi dinamica, tramite un valore di rating per gli spammer che fanno invii massicci ma occasionali
- SMTP traffic Throttling (solo IMSVA)
  - filtro basato su frequenza di connessioni e messaggi in intervalli di tempo
  - soglie e intervalli temporali configurabili
  - basati su IP o su indirizzo mittente
- Tutti questi filtri supportano white list e black list

Esistenza del destinatario

- IMSS/IMSVA non applicano direttamente tale filtro
- IMSVA agisce sulla configurazione del suo postfix
  - se si configura LDAP, la GUI configura il suo postfix per effettuare la verifica del destinatario via LDAP
    - per default sull'attributo mail, ma e' configurabile
  - modifiche manuali non sono supportate (e vengono sovrascritte)
- IMSS non opera in questo modo: la configurazione di LDAP non comporta modifiche sul postfix sottostante
  - e' possibile implementare policy preesistenti

Anti-virus scan options

- Advanced Threat Scan Engine (ATSE)
  - combinazione di scan basati su pattern e scan euristici
  - zero-day threats, embedded exploit code, parser evoluto per contenuti potenzialmente pericolosi
- Smart Protection Service
  - Servizio remoto di analisi per file e web site reputation up-to-date all'ultimo minuto
- Virtual Analyzer
  - Servizio remoto a cui inviare messaggi con attachment non identificati come Virus/Spam, ma con potenziali comportamenti malevoli (Deep Discovery Analyzer)

Policies

- Ogni messaggio viene sottoposto alla policy
- La policy e' un insieme di policy rules, che vengono applicate sequenzialmente
- Ogni policy rule e' definita da una route, un criterio di match, una action
  - la route e' coppia di indirizzi To-From, con supporto di wildcard, address group, LDAP user/group, ed eventuali exceptions
- Un messaggio viene sottoposto ad una sequenza di policy rules sulla base di indirizzo mittente e indirizzo destinatario
  - verranno applicate solo le regole per le quali la coppia From-To fa il match con la route della policy rule

Rule match conditions

- Sequenza di condizioni (tutte in AND o tutte in OR)
- indentificazione virus/malware (con selezione del tipo di file, e risultante sottoclassificazione)
- phishing, spam (con selezione del livello), graymail, web reputation
- criteri sugli attachment (file type, per estensione o identificazione, file name)
- dimensione del messaggio, numero di destinatari, received time
- criteri di match di keyword (con regexp) su selezionati header o nel body
- data loss prevention e regulatory compliance
- spoofing degli indirizzi locali (sulla base di un insieme di indirizzi IP configurabili)

Actions: tre operazioni

- Intercept (o no):
  - Delete: il messaggio viene rimosso dalla coda
  - Quarantine: il messaggio viene messo in quarantena
  - Hand-off (termina l'analisi e invia il messaggio per il delivery al server specificato)
    - il server puo' essere il postfix stesso (127.0.0.1:10026)
  - Cambia il destinatario
  - Do not intercept (prosegue l'analisi con le regole seguenti)
- Modify:
  - pre-configured actions per l'identificazione di un virus (clean attachment, delete attachment)
  - insert x-header
  - modifica subject o bosy
- Monitor
  - Invia una notifica (vedi oltre per le notifiche)
  - Aggiungi un indirizzo in BCC
  - Archivia in una area del server

Altre features

- Supporto SPF e DKIM
- Supporto DMARC (solo IMSVA)
- Supporto TLS
- Encryption per i mail in uscita (solo IMSVA)
- Time-of-click protection
  - riscrittura delle URL sospette per rimandare l'analisi della relativa web reputation al momento del click del ricevente

Notifiche

- Supporto per notifiche via mail in occasione di eventi
  - action nelle regole di scan
  - monitoraggio sul funzionamento delle diverse componenti
  - notifica di errori nella analisi dei messaggi
  - server resource limit (spazio disco)
- End User Quarantine digest
  - e' possibile abilitare inline actions, tramite link nel digest

Reportistica

- Supporto per invio di reportistica via mail
  - automatico schedulato (giornaliero, settimanale, mensile)
  - report on demand
  - formati html e csv
- Statistiche su tutti i contatori
  - mail totali, sender filter, virus, spam, …
  - classifica spammers virus per IP mittente, per indirizzo mittente, per indirizzo destinatario
  - statistiche su actions (deleted, quarantined, …)
- Mantenimento dello storico, con intervalli temporali configurabili

Quarantena

- Il software supporta l'utilizzo di quarantena
  - in funzione delle regole di policy
  - quarantena gestita in differenti aree
- Duplice accesso
  - amministrativo: completo
  - end user: solo le aree esplicitamente esportate, e non tutti i tipi di messaggio

End User Quarantine

- Autenticazione basata su
  - LDAP (include riconoscimento degli alias)
  - SMTP (poco utile: riconosce solo i messaggi a <username>@<domain>)
- La End User Quarantine supporta:
  - user action via interfaccia web
  - invio di digest messages (daily/weekly)
  - inline action nei messaggi di digest
  - configurazione di approved sender (white list per la quarantena)

Pool e TMCM

- IMSVA e IMSS supportano una configurazione di diversi server in pool
  - un server ha la funzione di master (parent)
  - gli altri server hanno ruolo di slave (children)
  - tutti i server del pool sono configurati come MX per i domini gestiti
- Solo il parent espone l'interfaccia di management
  - la configurazione viene propagata ai children automaticamente
- La quarantena e' distribuita
- IMSVA e IMSS supportano anche la configurazione centralizzata tramite Trend Micro Control Manager
  - il server TMCM gestisce centralmente tutte le configurazioni
  - i server cosi' gestiti non devono essere configurati in pool per ereditare la stessa configurazione
  - e' la soluzione suggerita per ambienti distribuiti geograficamente

Scalabilita’

- IMSS/IMSVA configurati in pool offrono una scalabilita’ orizzontale
  - l’aggiunta di server child permette di avere load balancing e failover per via del protocollo SMTP
  - la gestione distribuita della quarantena permette comunque un accesso centrale con carico ridistribuito
- IMSS/IMSVA configurati in pool permettono la separazione dei ruoli
  - per elevati carichi, e’ possibile configurare
    - un nodo parent con scanner, policy e EUQ disabled
    - un pool di children per scanner e policy (MX)
    - un pool di children per la gestione della EUQ

Update/Rollback

- IMSVA/IMSS supportano l'update automatico delle signature dai server Trend Micro ad intervalli configurabili (default: 15 minuti)
- IMSVA/IMSS supportano update di software
  - gli update sono manuali
  - e' supportato il rollback
  - ovviamente qualunque configurazione custom non standard non e' garantita operare attraverso un update

IMSVA: problemi

- Limiti sulla configurabilita' di postfix
  - routing semplice (solo transport): domain -> relay di destinazione
  - non c'e' supporto per virtual domain, virtual aliases, …
- Non e' supportata la configurazione manuale del postfix
- La versione attuale e' basata su una CentOS 6
  - kernel e pacchetti sofwtare non up-to-date
  - non e' supportato l'update dei pacchetti software
  - TLS utilizza protocolli di encription deprecati
  - la connessione criptata verso LDAP (per controllo recipient e per EUQ) non supporta certificati intermedi per la CA

IMSVA: problemi (cont.)

- Lo user database utilizzabile per la verifica del recipient e' solo LDAP
  - non supporta 389 directory server (solo AD, openldap, Lotus domino, Sun iPlanet)
- EUQ e LDAP
  - viene utilizzato un LDAP di cache locale
  - l'attributo da cui prendere l'elenco degli indirizzi associati ad una autenticazione e' sempre mail, anche se per lo user database si configura un attributo diverso
- Nelle prime prove fatte ci sono troppi falsi positivi
  - non e' disponibile il dettaglio delle singole regole che determinano il punteggio del filtro antispam
  - non si puo' intervenire sulle singole regole per modificare i punteggi

Considerazioni finali

- La soluzione IMSVA sembra poco flessibile per le nostre esigenze
- IMSS risolve quasi tutte le problematiche di IMSVA
  - server OS up to date
  - controllo sulla configurazione del postfix: alias e userdb, routing
  - sembra idoneo a sostituire Sophos PM
- L'attivita' non e' completa:
  - vanno esplorate le ampie configurabilita' delle policy rules
  - va fatta una analisi delle performance dei filtri

Note tecniche

- IMSVA e IMSS supportano configurazione in tre modalita':
  - GUI (scrive su local file e su db)
  - configuration files *.ini in /opt/trend/imss/ (hanno priorita' sul db)
  - database
- IMSS: e' possibile inibire la sovrascrittura di parametri di configurazione di postfix, definendo il parametro:

  detach_key_postfix=<colon-sep list of params>