Mailing: servizi per le sedi

Alessandro Brunengo
per il gruppo mailing di CCR

Servizi in produzione

- supporto alias @infn.it
  - instradamento alias (implementato su infngw*.infn.it)
  - generazione automatizzata degli alias semplici
  - auto-selezione alias esteso e di indirizzo primario (https://mailing.infn.it)
- backup MX di sede
  - on demand (implementato su infngw*.infn.it)
- cattura e notifica per mail @inf.infn.it
  - solo per gli indirizzi del DG (implementato su mx*.infn.it)
- servizi per la PEC
  - gestione centralizzata acquisto ed attivazione caselle
  - backup caselle PEC (https://backpec.infn.it)
  - supporto generale per problemi relativi alla PEC

Richiesta di aiuto dal TIFPA

- A febbraio 2018 Unitn ha dismesso il servizio di supporto di ricezione e filtro antispam/antivirus che faceva per il TIFPA
  - con poco preavviso
- Difficolta' di man power e skill specifico insufficiente per sopperire rapidamente
- Il Tifpa ha chiesto il supporto del gruppo mailing
  - installazione e configurazione di un servizio ridondato di MX con filtri Antispam/Antivirus su server nazionali
  - inoltro al relay locale, che poi fa recapito nelle mailbox
- Il servizio e' stato implementato a marzo
  - operativo: finora non ci sono stati problemi

Configurazione

- Il servizio e' stato configurato utilizzando Sophos Pure Message
  - troppo tempo per aspettare Trend Micro
- Servizio configurato su due server sulla infrastruttura dei SSNN
  - coppia di server, uno al CNAF ed uno a Genova (mx*.infn.it)
- Caratteristiche:
  - server di frontiera in ricezione (MX per tifpa.infn.it)
  - filtri in fase di sessione SMTP (oltre allo standard postfix: IP blocker)
  - filtro antivirus: rimozione, subject tag, aggiunta di un extended header
  - filtro antispam: modifica del Subject
- MX utilizzati anche in uscita
  - l'outgoing locale invia agli MX
  - opportuni filtri in uscita: blocca lo spam ed avverte il mittente (locale)

Controllo sulla esistenza del destinatario

- Gestione del dominio tramite virtual mailbox e transport
- Unico aspetto particolare:
  - necessario non accettare la mail in caso di user inesistente
  - si deve evitare il backscattering (reject dopo RCPT TO)
- Quindi e' stato necessario trasferire l'elenco di indirizzi validi del TIFPA sugli MX nazionali
  - definita una interfaccia
  - il puppet server fa un accesso https autenticato in polling
  - il file reso disponibile contiene l'elenco degli indirizzi validi (inclusi indirizzi impersonali, mailing list, alias, etc…)
  - la gestione degli indirizzi validi resta sotto il controllo della sede

Evoluzione: estensione ad altri domini

Idea: configurare un sistema di ricezione, filtro e recapito

- estendibile ad altri domini in modo semplice e poco costoso
- scalabile orizzontalmente per supportare incremento di traffico
- flessibile nell'insieme di servizi da offrire

Funzionalita' minime

- software antivirus/antispam
- supporto di IP reputation e user unknown a livello di sessione SMTP
- filtri ed azioni differenziate per direzione di flusso
- quarantena accessibile all'utente
  - quindi sistema di autenticazione ed identificazione degli alias (LDAP)
  - esteso alla gestione della quarantena per le liste

Dettagli tecnici

- Il sistema implementato e' quasi adatto
  - la definizione degli indirizzi e del trasporto non cambia
- Il supporto alla quarantena richiede modifiche:
  - necessario appoggiarsi ad un LDAP per associare indirizzi, alias, eventuali indirizzi di liste, ad un utente
  - il server LDAP deve essere dedicato, per gestire le informazioni necessarie
  - l'autenticazine deve avvenire tramite AAI
- Gestione ottimizzata per alias che puntano all'esterno
  - questi possono essere inoltrati a destinazione direttamente dagli MX
- Modifica dell'interfaccia di definizione degli indirizzi
  - l'elenco deve associare un uid AAI ad ogni indirizzo
  - un elenco separato per alias esterni
  - comunque sempre a totale controllo della sede

Evoluzione, fase II

- Supporto per il delivery diretto verso le mailbox
  - e' necessaria una valutazione tecnica delle configurazioni necessarie
- Supporto per un servizio di outgoing autenticato
  - ridondato e scalabile orizzontalmente
  - autenticazione su AAI
  - eventuale autenticazione con certificato (anche di server)
  - supporto per SPF, DKIM, DMARC
- Servizio di outgoing non autenticato
  - dove e' impossibile configurare un sistema di invio autenticato
  - a supporto si sistemi di automazione o allarmistica
  - filtri sulle destinazioni ammesse (proteggere da spam o dos generato internamente)

Prossimi passi

- Definizione della soluzione AS/AV da adottare (vedi talk precedenti)
- Riconfigurazione del sistema di ricezione per il TIFPA
  - Compatibile con i requisiti definiti precedentemente
- Configurazione sistema embrionale di outgoing autenticato
  - Agganciato alla autenticazione AAI
  - Abilitato per tutte le utenze INFN
- Sara' opportuna una rivalutazione del man power necessario per i servizi di supporto alla posta elettronica