Teknisk information om Mailfilter-ng

- **Hur loggar administratörer & användare in i Halon för att konfigurera/ändra inställningar?**

  All inloggning sker likt gamla Mailfilter via SWAMID / SSO. Webb-adressen till Halons kontrollpanel är https://kontrollpanelen.sunet.se (samt https://halon-eu.sunet.se för testmiljön)

- ### Vad heter de nya MX:arna som Mailfilter-ng tillhandahåller, och vilka nät behöver man öppna för?

  De nya MX-servrarna ligger i samma "nät-block" som gamla Mailfilter, dvs. `192.36.171.200/29` samt `89.45.235.0/28` , detta för att migreringen ska kunna ske utan extra brandväggsändringar. De ny MX:arna heter: `mailfilter-ng-1.sunet.se` , `mailfilter-ng-2.sunet.se` , `mailfilter-ng-3.sunet.se` samt `mailfilter-ng-4.sunet.se`

- ### Hur skapar jag användare i Mailfilter-ng?

  Användare kan skapas automatiskt i och med att de får ett epost-meddelande (men då förutsatt att man slagit på att auto-skapa användare under domän-inställningar)
  En användare autoskapas också när denne loggar på webbgränssnittet, samt att primär epost-adress automatiskt läggs till som ett alias (förutsatt att eppn är skiljt från mail-attributet). Det går även att skapa användare manuellt via GUI eller API (se https://github.com/SUNET/Mailfilter-ng-APIs), om man behöver göra per-användarinställningar i förväg.

- ### Kan man migrera sina inställningar från Canit till Halon?

  Nej, Canit och Halon är helt olika system, och regler och inställningar är inte i ett kompatibelt format för att läsas över. Däremot är principen för hur systems inställningar & funktioner väldigt snarlika, så man kan ställa in liknade inställningar per domän och/eller användare.

- ### "Recipient Verification", varför behöver vi som kund ha det påslaget?

  Utan "recipient verification" kommer Mailfilter-ng skicka vidare all epost in till er, även epost för ej existerande mottagare/epost-brevlådor, vilket kommer leda till sk backscatter
  Det leder ofta till att er domän får dåligt ryckte (när det gäller felkonfigurerade epost-servrar), nått som är onödigt att dra på sig, förutom alla extra resurser som går åt på att behandla de felaktiga epost:en som generellt bara är skräp.

  KUA har tagit fram en enkel HOWTO för att aktivera recipient verification i Microsoft Exchange, den finns omskriven här: https://forum.sunet.se/content/perma?id=3987 men är inte Exchange nästkommande "hop" från Mailfilter-ng, finns även konfigurations-alternativet: *Domain Recipient filtering Alternative recipient lookup* där alternativ SMTP-pratande server kan anges för att slå upp epost-adresser för domänen.

  SU har också skrivit en HOWTO för Postfix som finns här: https://forum.sunet.se/content/perma?id=4127

- **Finns motsvarigheten till Custom-rules i Mailfilter-ng?**

  Ja & Nej. Då Halon inte arbetar på samma sätt som Canit så Custom-rules finns inte på samma sätt.
  Vissa innehålls-matchningsfunktion finns dock, men det är inte fullt lika flexibelt som tidigare

- **Kan man (likt i CanIt) tagga viss SA spam score (5.1 - 11) , och sätta ett "tak" på SA spam score (11+) då epost ska rejectas (eller kastas)?**

  Korta svaret är Nej. Det längre är att Halon i dagsläget endast supporterar antingen "reject" eller "tag". Man kan justera tröskel-nivån för SA-spam score för den "action" man valt att sätta. Tanken är att ni inte ska behöva hantera det på detaljnivå, så som det behövs tidigare för att CanIt skulle fungera någorlunda önskvärt.

- **Hur bra fungerar Halon/CYRENs antispam jämfört med CanIt**

  CYRENs IP-reputation & RPD (Reoccuring Pattern Detection) fungerar väldigt bra utan att man behöver gå in och "tweaka" några regel-inställningar. Deras IP-reputation skydd är en kombination av traditionell IP-blacklist och Greylisting. Om det är ett helt okänd avsändare/IP så kommer den att tempfail:as som vanlig Greylisting fungerar. Man kan snabba upp processen att få sina IP-adresser godkända genom att rapportera in dem via: http://www.cyren.com/security-center/cyren-ip-reputation-report

  Det går även att undata dem från IP-reputation (*Black-/whitelist Exclude from IP reputation*) och/eller RPD (*Black-/whitelist Whitelist*) per domän.

- **Kan användaren själv ändra sina inställningar för antispam och antivirus?**

  Ja, precis som i CanIt, kan användare logga in i samma GUI som en admin, dock har de bara tillgång till en begränsad mängd inställningar

- **Kan man stänga av Antivirus och/eller Antispam för specifik mottagare?**

  Ja, en administratör kan avaktivera dessa funktioner per mottagare (per e-postadress).

- **Finns karantän-funktion, och hur fungerar den?**

  Ja, karantän finns, men man måste slå på det under fliken **Inbound protection** "***Spam action***". E-post som hamnar i karantän ligger kvar 2 veckor innan de raderas (tidensperioden kan inte modifieras).

- **Vi får legetim epost klassifierad som spam, varför då?**

  Ja, det händer (mer eller mindre) i alla spamfilter tyvärr, CYREN har skrivit en artikel om det här: https://www.cyren.com/fp-reasons-explained

- **Finns det utgående scanning också?**

  Ja, det sätt per domän. Just nu går den via samma servrar som inkommande MX, dock måste utgående skickas via port `587` (`submission`) .

- **Finns utgående Ratelimit?**

  Ja, den kan sättas per domän och kan även justeras per avsändare (epost-adress). Den är dessutom mer granulär i nya Mailfilter-ng, det går att konfigurera för all epost, per "bulk" (massutskicks)klassifierad epost och per e-post som klassas som Spam av filtret. Det gör att ett kapat användarkonto troligtvis kan fortsätta att arbeta och skicka utåtgående epost och att e-post spam:en stoppas av ratelimitingen.

  Att överträda ratelimit innebär dock inte permanent blockering i 3 dygn som tidigare i CanIt, istället är Halons ratelimiting baserad på regeln X antal epost / Y tidsenheter, där default är 1000 (epost) / 86400 (24 timmar). Övertrasseras gränsen blir överskjutande epost blockerade upp till ett dygn, när ratelimit-räknaren återställs.

- **Hur länge finns Canit kvar?**

  Tanken är att Mailfilter-ng (Halon) skall ha tagit över samtliga organisationer under första halvan av 2021.
  Den gamla Canit-installationen kommer finnas kvar så länge som behov finns, dock endast för att kunna titta på gammal konfiguration och söka i de äldre loggarna.

- **Kan man flytta en domän/underdomän i taget?**

  Ja det fungerar utmärkt. En domäns mailrouting sköts via MX-pekare så det styr ni över själva.
  Lämpligt att börja med en lite domän så man ser att allt fungerar innan man styr över hela organistationen.

- **IPv6, SPF, DKIM och DMARC**

  Ja, Halon-MTA har IPv6 och har stöd för verifiering av SPF, DKIM samt DMARC.
  Halon kan även DKIM-signera utgående epost (en per-domän inställning). Dock måste du generera din selector public/private key själv (görs enklast via opendkim-genkey från opendkim-milter paketet (som är OSS))

- **Maximal storlek på mail?**

  Nuvarande maxstorlek är 40MB (som i CanIt) och det styrs centralt. Det kan mao alltså inte ändras av den lokala organisationen.

- **Finns URL-filtrering (som CanIts URLproxy)?**

  Halon har en extra URL-filtreringsfunktion, men den ingår inte i standardutförandet.
  URL-filtrering "TOCP" (Time of Click Protection) köpas till (en sk. "premium"-tjänst som kostar per användare (inte epost-adresser), hör av er för pris. Mer information här Halon Time-of-Click Protection.pdf

  Vi har nu byggt en egen förenklad "URL-protection" funktion, den är dock inte aktiverad per default, så den behöver konfigureras av kunden själv.

- **Vad är skillnaden på Halons TOC (click protection) och en inbyggda URL-protection (URLproxy) ?**

  Halons TOC (Click Protection) kostar lite extra pengar. Den skriver om ***samtliga URLer*** som den hittar i epost URLerna scannas först när en användare öppnar den. Då scannas URLen av en mängd olika motorer, främst Sophos motor (därav den extra kostnaden som tillkommer).

  URL-protection (URL proxy) skriver endast om URLer om epost-meddelande blev klassat som spam/suspicious, om domänen är helt okänd ("NewlySeen"), samt om URLen finns med i URL-blocklistan. Övriga URLer kommer den inte skriva om.

- **Finns API-access ?**

  Ja, det nås via kontrollpanelen (prod) / halon-eu (devops/test) via port 8443 .
  Vi har lagt upp API-dokumentationen här: https://github.com/SUNET/Mailfilter-ng-APIs , vi behöver däremot skapa en API-användare (användare@realm) samt generera ett lösenord och skicka över uppgifterna till er.

- **Vad kostar det?**

  Kostnaden är oförändrat, dvs. priset är den samma som tidigare, se separat dokument.

- **Vem ska man prata med?**

  Avtalsfrågor: tomas@sunet.se
  Felanmälan: noc@sunet.se
  Frågor & fundering kan även postas på maillistan: mailfilter-ng@lists.sunet.se