Policy del servizio Antispam ed Antivirus

Tutte le caselle email ospitate sui nostri server **sono protette da più livelli di Antispam ed Antivirus** sia per le email in arrivo che per quelle in uscita. I nostri sistemi di analisi sono basati su Spamassassin, ClamAV ed un software commerciale in grado di intercettare i nuovi trend di Spam in tempo reale.

Il primo strato di protezione è a livello di connessione SMTP.

Tutti i server remoti che si connettono ai nostri MX devono avere i seguenti requisiti:

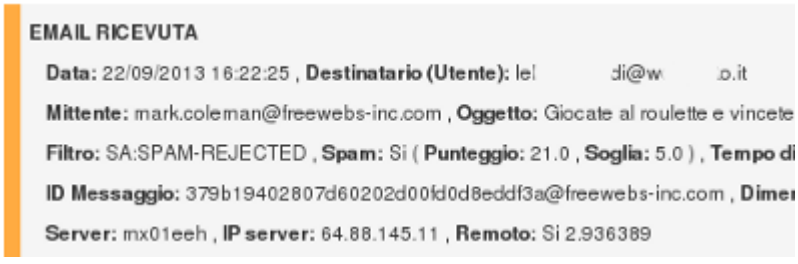
- Un reverse DNS qualificato (di tipo FQDN) e valido
- Non essere presenti nelle DNSBL zen.spamhaus.org
- Presentarsi con un HELO FQDN valido

Se il vostro server o la sua configurazione non rispetta queste best-practices difficilmente sarete in grado di consegnare le vostre email in giro per la rete.

Filtri ANTISPAM: Vengono applicate delle penalizzazioni legate al contenuto delle email ed alla presenza dell'IP mittente in varie DNSBL meno rilevanti. Se le penalizzazioni sono inferiori ad un certo punteggio **l'email viene messa in quarantena** nella cartella "Spam" della mailbox dell'utente (consultabile da Webmail o IMAP), se le penalizzazioni sono molte l'email viene respinta con un errore 500 a livello di dialogo SMTP. Il mittente dell'email potra così ricevere una notifica di mancata consegna e prendere i provvedimenti del caso.

Scansione ANTIVIRUS: Viene inoltre applicata una scansione Antivirus, Antimalware ed Antiphishing. In questo caso l'email viene accettata ma scartata silenziosamente in quanto il mittente di queste email è quasi sempre inesistente per cui inviare una notifica non ha senso. Questo comportamente potrebbe subire variazioni nel tempo.

Lo strumento di analisi dei log in tempo reale, ETLive, permette di verificare se il filtro Antispam o Antivirus ha bloccato un messaggio a casua di un falso positivo.



Le **Whitelist**, attivabili dalla webmail o dal pannello di controllo, agiscono solo a livello di analisi del contenuto della email "ANTISPAM". Se l'email arriva da un IP in blacklist, da un server non correttamente configurato o contiene un virus questa verrà respinta in ogni caso.

Le **Blacklist** sono anch'esse gestibili dall'utente tramite webmail e causano il respingimento del messaggio al mittente con un errore SMTP di tipo 500.

Le whitelist e blacklist inserite dagli utenti hanno lo scopo di sanere una situazione problematica in maniera temporanea. Il nostro sistema è in grado di apprendere, sulla base delle segnalazioni degli utenti, eventuali problematiche di falsi positivi/negativi e di adattare i propri filtri in tal senso. In virtù di questo fatto le personalizzazioni degli utenti posso essere automaticamente rimosse dopo alcuni mesi.

Gli indirizzi email dei mittenti delle email devono essere indirizzi internet validi, non è possibile accettare email da mittente ai quali non è possibile inviare una risposta (ad esempio domini senza una corretta configurazione DNS o domini invalidi o inesistenti). Se il dominio mittente utilizzate SPF o DKIM le impostazioni devono essere corrette.

Le liste DNSBL possono variare nel tempo in funzione di fattore tecnici, eventuali variazioni verranno, per quanto possibile ed opportuno, segnalate su queste pagine successivamente alla loro applicazione. In questi casi i nostri server, quando ricevono una connessione da un IP in blacklist, restituiscono un **errore "permanente" 5.x.x**, in questo caso il server remoto non ritenterà la connessione e genererà subito un bounce (messaggio di errore) al mittente.

Tranne l'analisi antispam i filtri sopra indicati non sono personalizzabili dall'utente e sono legati a regole comuni e di buon senso che tutti gli amministratori di server email devono seguire. Inoltre, essendo il blocco a livello di IP/DNS o prime fasi del dialogo SMTP, non sono presenti nei log dei nostri sistemi gli indirizzi email dei mittenti bloccati ma solo gli indirizzi IP dei server mittenti. In ogni caso, a seguito di un blocco per uno dei motivi sopra riportati, al server mittente o al mittente stesso (ovvero l'indirizzo email specificato nell'header "**Return-Path**") torna sempre indietro un messaggio di errore, per cui nessuna email può andare persa.

In ogni caso il nostro supporto tecnico è a disposizione dei clienti/mittenti per valutare casi di falsi positivi e risolversi.

E' presente inoltre un sistema di **Antispam ed Antivirus anche sui nostri server SMTP**, questo per evitare che la compromissione di un account email possa portare all'invio di spam dai nostri server e penalizzare la reputazione dei nostri IP oltre che alla consegna delle email degli utenti. Tramite ETLive è possibile verificare se un account o un messaggio è stato bloccato per questi motivi.

Policy del servizio SMTP Autenticato

Euroweb al fine di garantire un elevato livello di deliverability delle email inviate dai propri server SMTP ha predisposto delle **policy di utilizzo a tutela di tutti i nostri clienti ed utenti**. Tali policy sono necessarie per prevenire eventuali inserimenti in blacklist dei nostri sistemi SMTP, per evitare eventuali invii massimi di email da parte di botnet che potrebbero essere entrate in possesso in maniera fraudolenta della password di un utente o per evitare eventuali abusi da parte degli utenti del servizio stesso.

Le policy prevedono il blocco dell'account SMTP (solo invio mediante SMTP, tutte le altre funzionalità, compresa la consultazione delle email, non vengono bloccate) se viene riscontrata un'attività anomala di connessione al server o invio di email. Per attività anomala si intende un numero elevato di autenticazioni SMTP nel giro di pochi minuti, autenticazioni contemporanee da più indirizzi IP distinti fra di loro o invio di messaggi contenente Spam/Sospetto Spam.

In ogni caso **il blocco è stato studiato per non entrare mai in funzione durante la normale attività di invio email** da parte dell'utente mediante i classici strumenti di consultazione ed invio delle email (Outlook, Thunderbird, iPhone, Webmail, altri client email). Può invece scattare il blocco se l'account è inserito in sistemi automatizzati di invio di email (quali ad esempio Sendblaster o altri software di invio massimo di email) o se si eseguono invii massivi di email dal proprio client email o da webmail.

L'SMTP Autenticato fornito con il servizio di email hosting è da utilizzare rispettando i seguenti limiti:

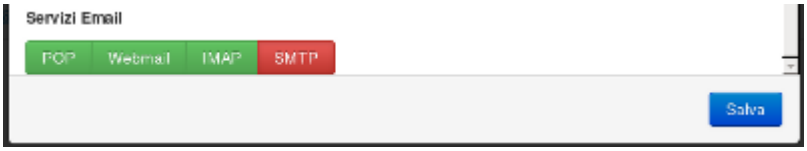
- l'utilizzo è consentito da parte di client email dell'utente (MS Outlook, Thunderbird, Apple Mail, dispositivi mobili, Webmail, altro) per l'invio di **email interpersonali**
- non è consentito l'utilizzo da parte di sistemi di invio automatizzato di mailing list, newsletter, dem (siamo essi lato client o lato server)
- la dimensione massima degli allegati che è possibile inviare è 25MB (tenendo conto che molte caselle email remote non accettano allegati così grandi)
- il numero massimo di destinatari (recipients) per ogni singolo invio è 50
- il numero massimo di autenticazioni eseguibili all'interno di 30 minuti è di 100-150 (varia in base a diversi fattori)
- il numero massimo di differenti indirizzi IP dal quale un utente può eseguire autenticazioni all'interno di 30 minuti è di 5
- ogni altro tipo di abuso, ritenuto tale per via del fatto che posa pregiudicare l'operatività degli altri utenti, prevede il blocco temporaneo dell'account SMTP

A partire dai limiti sopra impostati è stabilito un numero, indicativo, massimo di email inviabili per singolo account SMTP pari a circa 1000/1500 email / ora. Più che sufficienti per tutte le tipologie di utenti.

Nel caso di superamento dei limiti di invio o in presenza di un abuso del servizio l'account utilizzato per l'invio verrà in maniera automatica intercettato dal sistema e bloccato (solo a livello di servizio SMTP).

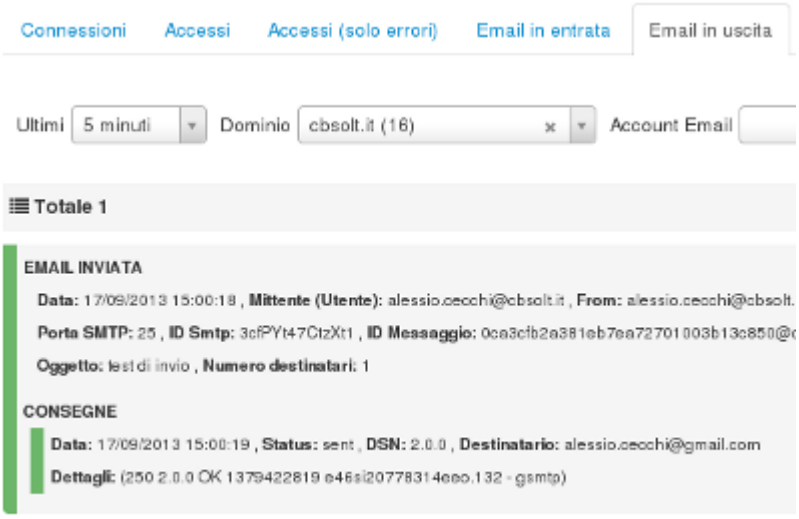
L'account andato in "blocco" può essere sbloccato (o verificato se sia bloccato), in autonomia, dal pannello di controllo dal cliente titolare del dominio su Euroweb andando in

Domini -> Email -> Modifica Account Email (selezionare l'account bloccato) -> scorrere fino a "Servizi Email" e cliccare sulla voce SMTP che passerà da rossa a verde



Se a seguito dello sblocco dovesse ripresentarsi un nuovo invio di spam sullo stesso utente l'account verrà bloccato dai nostri operatori e rimarrà bloccato fino a quando non avremo ricevuto un riscontro di interruzione dell'abuso da parte dell'utente titolare dell'account email con conferma della risoluzione del problema che causava l'invio delle email di spam (in genere PC infetto da Virus che ruba le password della casella email).

Tramite lo strumenti **ETLive -> Archivio Log Mail Inviate**, disponibile nel pannello di controllo, è possibile avere un dettaglio delle email inviate dall'account che è stato sottoposto al blocco. Questo può aiutare a diagnosticare le cause del blocco.



Il servizio SMTP analizza inoltre le email per individuare la presenza di Virus o Spam, nel caso in cui questi messaggi contenessero materiale dannoso per gli utenti destinatari o per la reputazione dei server di Euroweb l'invio non viene permesso.