SHARKMAIL by 2000net

La 2000net ha investito molte risorse per combattere il fenomeno dello “spam” e oggi è pronta a fornire una soluzione ad elevato livello tecnologico indirizzato al settore Business in grado di eliminare più **del 98% della posta indesiderata**.

Questa soluzione si chiama : **“SHARKMAIL” .**

Caratteristiche generali

Sharkmail è una piattaforma costituita da una parte Hardware ed una parte software.
Per le aziende che dispongono già di un server fornito da 2000net con funzioni di reverse proxy l’hardware viene recuperato ed eventualmente solo espanso.

Il software è composto da due parti: la parte di amministrazione e la parte di utente finale.
La parte di amministrazione consente di impostare la macchina al fine di configurarla correttamente in rete e abbia le impostazioni esatte per gli aggiornamenti. Questa parte, normalmente, viene gestita direttamente via remoto da 2000net.
La parte end-user consente di personalizzare il filtro antispam in maniera specifica per ciascun utente, nonché di istruire il motore antispam e di recuperare eventuali email indesiderate.

Caratteristiche principali

- Max Connection Block
- Tarpitting
- IPThrottle
- SPF (Sender Policy Framework)
- RBL (Realtime Block Lists)
- Greylist
- Aderenza al protocollo
- Controllo DNS
- Controllo Whitelist
- Controllo Blacklist
- Auto whitelist
- Integrazione con ActiveDirectory Microsoft 2003 srv
- Esistenza delle caselle di posta
- Scansione antivirus
- Scansione contenuto
- Scansione antispam
- Scansione dell’immagine
- Analisi Bayesiana
- Log e statistiche

Più 98% dello spam viene eliminato

Tutta le tecnologia è lato server questo significa che il PC client e i server di posta aziendali non devono installare alcun software aggiuntivo. Tale aspetto è di fondamentale importanza in quanto il prodotto non è invasivo,e la vostra rete non potrà subire disservizi, rallentamenti improvvisi o addirittura crash dei server.

Dettagli tecnici

La soluzione è basata su un sistema operativo sicuro e robusto, il firewall antispam riceve le e-mail per conto del server di posta elettronica isolandolo da una connessione internet diretta.

I controlli sulle e-mail in ingresso vengono effettuati su vari livelli:

ANALISI IP

I programmi usati per spedire spam possono inviare una grande quantità di messaggi verso un server,questo può causare rallentamenti, blocchi sul servizio e sprechi di risorse.
Per proteggere le infrastrutture da questo tipo di attacco, il firewall 2000net utilizza le seguenti tecniche:

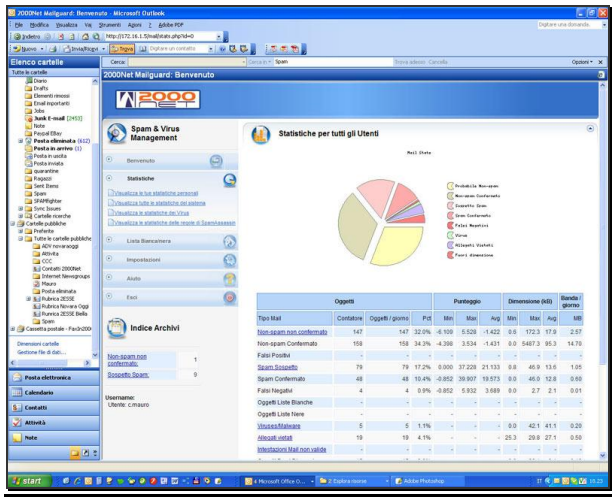
Max Connection Block
Enumera le connessioni provenienti da un particolare indirizzo IP e li blocca quando superano una certa soglia,impostata per default a 3 connessioni contemporanee da un medesimo ip.

Tarpitting
Visto che il protocollo SMTP (posta elettronica) permette di inviare la stessa e-mail a un numero elevato di destinatari,il firewall 2000net per ogni destinatario aggiunto alla e-mail,implementa un ritardo di ricezione esponenziale con una riserva di 5 e-mail.
Ciò significa che se lo spammer tenta di inviare un messaggio a 100 indirizzi e-mail, dal primo indirizzo inserito al quinto ,il server invierà una conferma immediata,al sesto indirizzo verrà data una conferma dopo 2 secondi, al settimo dopo 4, all'ottavo dopo 8 e successivi 16,32,64,128.

IPThrottle
Il firewall 2000Net enumera i messaggi provenienti da un particolare indirizzo IP e li blocca quando superano una certa soglia.
E' possibile aggiungere un particolare dominio con cui si scambiano molte e-mail, a una lista di indirizzi che vengono sempre accettati.
Per default un singolo server non può inviare più di 10 e-mail in un minuto.

SPF (Sender Policy Framework)
La specifica Sender Policy Framework consente di controllare se un determinato mittente e-mail sia stato falsificato o meno.
Molti "spammer" odierni utilizzano indirizzi e-mail falsificati.

Il protocollo SPF è uno sforzo comune che sta rapidamente guadagnando terreno. SPF richiede che l'azienda del mittente abbia pubblicato il suo server di posta in un record SPF. Ad esempio, se una mail è inviata da xyz@CompanyABC.com, la società "companyABC.com" deve pubblicare un record SPF affinché il protocollo possa determinare se l'e-mail sia stata davvero inviata dalla rete di "companyABC.com" o se sia stata falsificata.
Se l'azienda CompanyABC.com non pubblica alcun record SPF, il risultato del protocollo SPF sarà "sconosciuto".
Il firewall 2000Net è pronto e attivo per quanto riguarda SPF,per cui è in grado di comunicare ed approvare le e-mail spedite da domini SPF compliance.



SHARKMAIL *ha la possibilità di accettare email dall'esterno tramite autenticazione smtp. Questo permette agli utenti mobili di inviare e-mail in conformità a SPF. Inoltre il servizio smtp del firewall supporta le comunicazioni cifrate.*

RBL (Realtime Block Lists)
Il firewall utilizza alcune liste RBL.
Le RBL sono liste fornite da siti specializzati che identificano e pubblicano gli indirizzi ip degli spammer e dei server di posta configurati impropriamente.
Se il server riceve una e-mail da un ip presente in queste liste,assegna una probabilità maggiore alla e-mail che questa sia spam.
Il server non scarta immediatamente l'e-mail ma la passa ai controlli successivi.

Greylist (Opzionale)
Il sistema di greylist consente di tenere traccia di tutte le "triple" (destinatario, mittente, ip di provenienza) delle mail arrivate.
La prima volta che si presenta questa "tripla" la mail viene rifiutata con un errore temporaneo, al successivo tentativo la tripla sarà già nel database e la mail verrà accettata.
Solo i server conformi agli standard smtp sono in grado di ritentare l'invio di un messaggio rifiutato,mentre i programmi che solitamente gli "spammer" utilizzano,non sono in grado di farlo.
Di default questa funzione è disabilitata perché introduce un ritardo nella ricezione delle e-mail, dovuta al secondo tentativo di invio,ma se abilitata permette di ridurre in modo significativo lo spam.

ANALISI DEL MITTENTE

Dopo aver controllato la connessione, il firewall analizza l' indirizzo del mittente e del destinatario.

Aderenza al protocollo
Prima di convalidare un mittente il firewall controlla che il mittente sia specificato propriamente (Conforme RFC 821) e impedisce che mittenti non conformi agli standard inviino e-mail.

Controllo DNS
Per evitare che il mittente utilizzi un indirizzo falso, il firewall richiede che il dominio del mittente esista, sia valido e registrato in un dns.

Controllo Whitelist
Il firewall permette di definire una lista degli indirizzi e-mail e di domini fidati.
Le e-mail ricevute che hanno una corrispondenza in queste liste, non verranno mai considerate spam dai successivi controlli.

Controllo blacklist
Il firewall permette di definire una lista degli indirizzi e-mail e di domini non fidati.
Le email ricevute che hanno una corrispondenza in queste liste, verranno sempre considerate spam dai successivi controlli.

Auto whitelist
Il firewall ha un sistema di auto-apprendimento che permette di definire delle Whitelist automatiche.
Se un mittente invia alcune e-mail lecite, e poi ne invia una che il server rileva come spam, il server terrà conto di questo e in base al numero di e-mail lecite e alla probabilità che l'e-mail ricevuta sia veramente spam, prenderà una decisione in merito.
Se il mittente continuerà ad inviare e-mail che il server rileverà come spam, allora le probabilità che il filtro si stia sbagliando scenderanno (il mittente potrebbe per esempio avere il proprio personal computer infetto da un virus), e l'e-mail verrà contrassegnata come spam.

ANALISI DEL DESTINATARIO

Molti "spammer" attaccano un infrastruttura setacciando la rete in cerca di indirizzi e-mail. Il firewall permette di verificare la validità del destinatario in vari modi.

Aderenza al protocollo

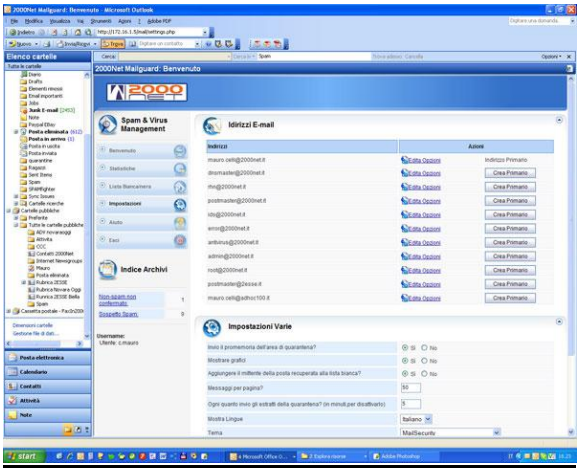
Prima di accettare una e-mail ,il firewall controlla che il destinatario sia specificato propriamente (Conforme RFC 821) e impedisce che e-mail con destinatario non conforme agli standard vengano processate.

Esistenza delle caselle di posta

Il firewall rifiuta immediatamente i messaggi con destinatario inesistente,impedendo che vengano processate e-mail illegittime con spreco di risorse e generazione di elevati bounce (messaggi di notifica).

Integrazione con mailserver basati su ActiveDirectory Windows 2003/ 2008 /2013 .

E' possibile integrare il firewall in un sistema ActiveDirectory (es. Microsoft Exchange Server 2003, 2007 e 2010) in modo che le caselle siano sincronizzate col dominio, oppure specificarle manualmente. Questa funzione consente di risparmiare notevoli perdite di tempo nel replicare le caselle nel software di antispam e di introdurre le doppie autenticazioni in fase di gestione degli utenti.



ANALISI DEL CONTENUTO

Scansione antivirus

La scansione basilare per la posta elettronica è la scansione antivirus.
Il firewall utilizza due livelli di scansione e espande automaticamente i file compressi.
La scansione antivirus ha la precedenza rispetto a tutte le altre tecniche di scansione ed è applicata anche quando il messaggio è accettato dai manager di connessione. Anche le e-mail provenienti da indirizzi IP, domini o caselle considerati fidati verranno scansionati e bloccati se viene riconosciuto un virus.
Inoltre il firewall blocca i messaggi che hanno allegati con estensioni pericolose (exe, com, etc.) e li deposita in un'area di quarantena specifica (Area Banned-File).

Scansione contenuto

L'e-mail viene controllata da un filtro che ne verifica l'integrità e la conformità alle specifiche per quanto riguarda l'intestazione. Se l'e-mail non supera questo controllo,viene depositata in un'area di quarantena specifica (Area Bad-Header).

Scansione antispam

Il firewall scansiona l'email con oltre 1700 controlli.
Questi controlli cercano di identificare le e-mail di spam,in particolare per ogni controllo che l'e-mail non passa,viene assegnato un punteggio crescente.
Quando il punteggio raggiunge un certo livello,l'e-mail viene rilevata come spam.
La lista dei controlli,viene aggiornata giornalmente.

Analisi dell'immagine
Al giorno d'oggi lo spam attraverso immagini rappresenta il 30% circa del traffico di spam su internet.
Il firewall utilizza delle tecniche mirate di analisi che bloccano varie tipologie d'immagini.

- *Riconoscimento ottico d'immagini (OCR)*
  Introdurre testo in immagini è una pratica comune per evitare i controlli di testo.
  Gli algoritmi di OCR permettono di scansionare le immagini in cerca di testo.
  Il firewall passa l'immagine in due motori OCR differenti in modo da avere una maggiore affidabilità.

- *Elaborazione d'immagine*
  Per mitigare gli effetti della scansione OCR gli spammer utilizzano tecniche di frammentazione, ombreggio e manipolazione del colore. Il firewall utilizza dei processi poco onerosi per normalizzare l'immagine prima della scansione OCR.

- *Analisi di GIF animati*
  Il firewall inoltre utilizza degli algoritmi per analizzare delle immagini GIF animate sospette.

Analisi Bayesiana
L'analisi Bayesiana è un algoritmo che crea un profilo delle parole utilizzate normalmente sia nelle e-mail di spam sia in quelle legittime generalmente spedite e ricevute da un'organizzazione o utente.
Per determinare se un messaggio è legittimo l'algoritmo confronta il contenuto del massaggio con il materiale raccolto.
Il controllo si attiva solo dopo che l'organizzazione ha ricevuto almeno 200 e-mail di spam.
Questo controllo è l'unico che richiede una interazione con l'utente, in particolare quando l'utente riceve una e-mail che è sfuggita al filtro, potrà spostarla in una cartella specifica in modo che il filtro possa imparare il proprio errore e porvi rimedio per le successive e-mail.

Gestione
Il firewall dispone di una interfaccia web utilizzabile direttamente dall'utente,o gestita dall'amministratore.
Tramite questa interfaccia,si potrà:

- Vedere e gestire le varie aree di quarantena delle e-mail
- Far consegnare le e-mail erroneamente considerate spam
- Istruire il firewall confermando le e-mail di spam o le e-mail lecite
- Impostare blacklist e whitelist

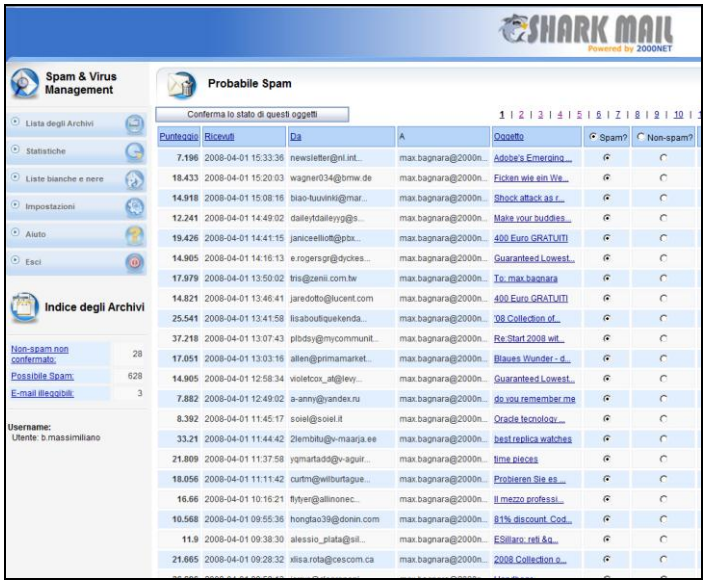
E' possibile inoltre chiedere al firewall di inviare agli utenti un riepilogo delle e-mail in quarantena quando queste superano un determinato numero.

E' anche possibile chiedere al firewall di inviare agli utenti a cadenze regolari una e-mail
contenente il riepilogo delle e-mail di spam, con la possibilità di confermarle (e quindi istruire i filtri bayesiani) o di recapitarle tramite un click su un link.

Log e statistiche
Il sistema è grado di produrre svariati log e statistiche in base numerosi situazioni.

Ciò consente di analizzare l'intero sistema e valutare determinati eventi.

L'operatore può intervenire autonomamente attraverso una semplice interfaccia WEB che gli da la possibilità di:



Impostazione del livello di sensibilità del filtro

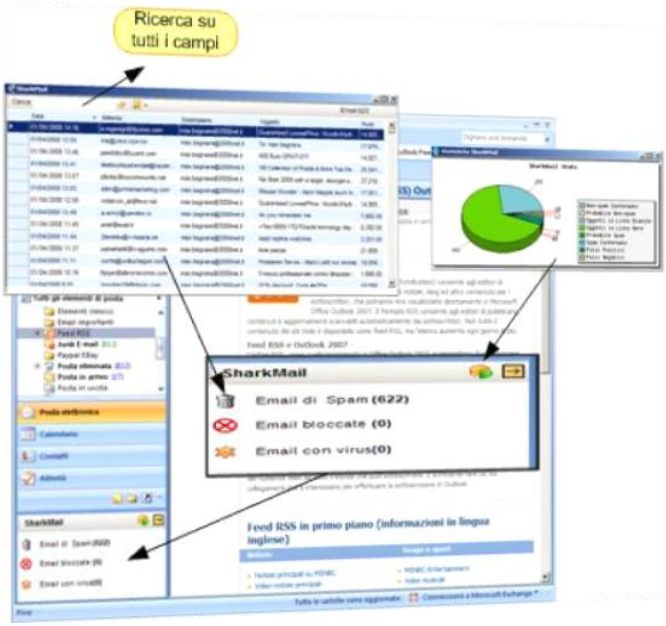
Impostazione delle liste bianche e liste nere

Contribuire all'apprendimento del sistema, classificando le email indesiderate

Accedere alle email in quarantena

Varie statistiche

[Connettore per outlook 2003/2007/2010]



L'accesso al database spam, oltre che avvenire attraverso l'apposita interfaccia WEB può anche essere effettuato con un plug-in sviluppato per Outlook 2003/2007/2010.

Questa modalità risulta è estremamente comoda e versatile per la gestione di tutte le email indesiderate.