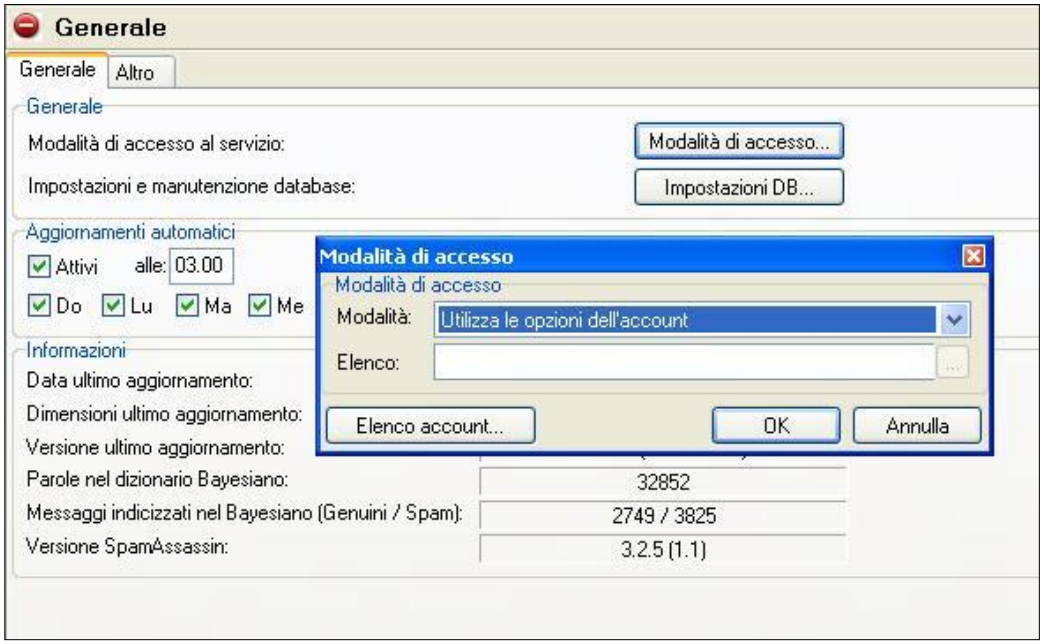
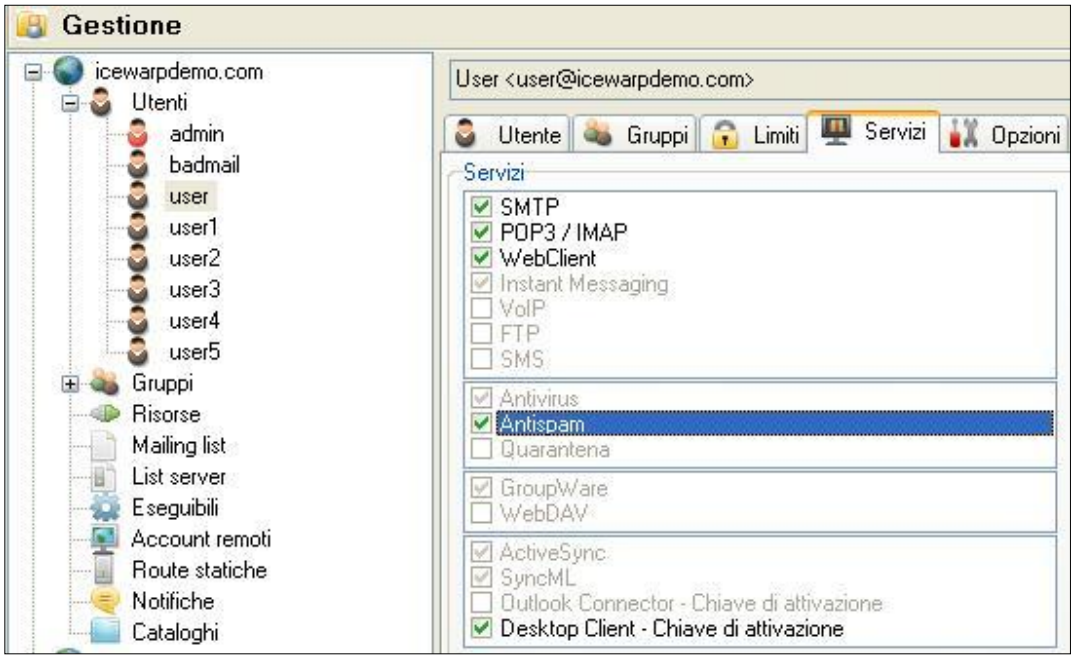
Antispam

IceWarp Server integra diverse tecnologie Anti-Spam altamente personalizzabili in modo che ciascun amministratore di sistema possa sfruttare le potenzialità offerte adattandole alle particolari caratteristiche della propria installazione e permettendo anche agli utenti una certa autonomia nella definizione di regole per l'identificazione di mittenti non genuini o indesiderati.
Prenderemo ora in esame tutte le impostazioni principali del modulo Antispam dando anche qualche consiglio su come configurarle, tuttavia occorre tenere presente che **non** esiste una configurazione universalmente corretta, data la diversità dei sistemi che si possono implementare e delle condizioni di utilizzo.

Generale

Per utilizzare l'Antispam è innanzitutto necessario stabilire una connessione dati con un database di appoggio, per il quale si consiglia di utilizzare la tecnologia MySQL.
E' necessario specificare una "**Modalità di accesso**" che definisce come le regole dell'Antispam vengono applicate agli utenti del sistema. Scegliendo "Tutti gli account" il servizio verrà imposto a tutti gli utenti locali, mentre scegliendo "Account in elenco" è possibile specificare quali utenti ne faranno uso.
E' altresì possibile demandare la scelta sull'utilizzo dell'Antispam ai domini o ai singoli account impostando "Utilizza le opzioni del dominio" o "Utilizza le opzioni dell'account".





Nella sezione “Altro” è possibile scegliere se processare i messaggi uscenti e come trattarli in caso vengano classificati SPAM.
E' anche possibile scegliere la “**Modalità antispam**” desiderata. Le tre opzioni sono Utente, Dominio, Sistema. La scelta condiziona il livello al quale vengono applicate le regole di Lista Nera e Lista Bianca. Se l'antispam è in modalità “Utente” tali regole saranno valide solo per l'utente che le definisce. Diversamente se la modalità scelta è “Dominio” o “Sistema” le regole create da un utente verranno applicate a tutti gli utenti dello stesso dominio o a tutti gli utenti locali.
Queste ultime due modalità, specialmente la modalità Sistema, sono da utilizzare con attenzione. Sono indicate nei casi in cui vi è una familiarità di qualche tipo tra gli utenti locali che li porta a poter collaborare nella lotta allo spam. Situazioni di questo tipo possono essere ad esempio un dominio aziendale utilizzato esclusivamente per fini di lavoro, o un sistema sul quale sono definiti più domini che fanno tutti capo ad uno stesso ente/azienda.
Per mezzo della “**Modalità utenti locali**” è invece possibile scegliere come trattare gli utenti locali che sono stati inseriti in quarantena, lista bianca o nera. Anche in questo caso è necessario tenere conto della tipologia di legame che vi è tra gli utenti locali. Se tutti gli utenti sono collaboratori di una stessa realtà e sono più o meno “conosciuti” è possibile procedere ignorando questi controlli.

Per quanto riguarda le “**Dimensioni massime dei messaggi da processare”** è bene tenere conto dell'aumento di dimensione che ha ultimamente subito lo spam. Un'impostazione attualmente adatta è 512 kB.

Azione

Le azioni che il filtro Antispam può intraprendere in base al punteggio assegnato ad un messaggio sono 3: QUARANTINE, SPAM e REJECT.
Per quanto riguarda i messaggi respinti si può scegliere se archiviarli in un determinato account o eliminarli. La seconda possibilità è sconsigliata, soprattutto dato che la distruzione e l'occultamento della corrispondenza da parte di persone diverse dal destinatario sono considerate reato dalla legislazione attualmente vigente.
Vi è anche la possibilità di modificare l'oggetto dei messaggi ritenuti spam per renderli immediatamente riconoscibili e, nel caso si desideri utilizzare una apposita cartella per tali messaggi, è possibile integrarla con una specifica cartella dell'account IMAP.

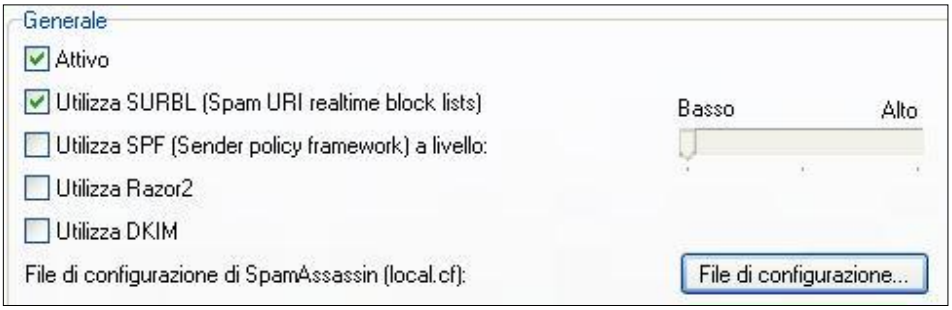
Quarantena

Anche per la quarantena è necessario definire una modalità di accesso così come descritto per l'Antispam ed è altresì possibile impostare l'invio di un "Challenge Response" ai mittenti dei messaggi messi in quarantena, ovvero di un messaggio atto a verificare che l'invio sia stato effettuato da un utente reale e non da un sistema automatizzato così da disporne la consegna al destinatario evitando la quarantena.
Affinché questa ultima modalità funzioni correttamente è necessario impostare opportunamente l'URL dei Rapporti Antispam in [Sistema > Servizi > SmartDiscover].

SpamAssassin

SpamAssassin è un progetto open source dedicato al contrasto dello spam. Questo software utilizza una serie di regole per determinare se un messaggio è spam o genuino.
SpamAssassin è molto efficace specialmente nell'individuazione di messaggi di "phishing" volti a ottenere le credenziali dei servizi finanziari degli utenti.
IceWarp Server utilizza le regole di SpamAssassin ma ha un proprio motore interno per processare i messaggi.
Le ulteriori tecnologie impiegate sono:

- SURBL (Spam URI Realtime block lists): sistema che individua gli URI legati allo spam nel corpo del messaggio invece che identificare i mittenti;
- SPF (Sender Policy Framework): gli amministratori di dominio hanno la possibilità di specificare un elenco di IP a partire dai quali proverranno i messaggi del loro dominio. SPF controlla questi elenchi (contenuti in un apposito record del DNS) per accertarsi che il mittente sia effettivamente chi egli dichiara di essere. Se il record del DNS non è pubblico il sistema può ritenere il messaggio non genuino ma non può esserne certo. Il punteggio da assegnare a tali messaggi è regolabile tramite il cursore mostrato nell'interfaccia (Basso: 0.1, Medio: 0.5, Alto: 5.0, impostazione rigida);
- Razor2: sistema di filtraggio distribuito e collaborativo;
- DKIM: si tratta di un metodo per associare un nome di dominio ad una mail per mezzo della crittografia a chiave pubblica e di una firma digitale. Se un messaggio proveniente da un dominio che ha un record "DNS DomainKey" non è firmato allora il punteggio spam totale viene incrementato.



Abilitando le funzioni di reportistica si può ottenere un report dettagliato che indica come i messaggi vengono processati da SpamAssassin.
La modalità consigliata è "Inserisci il rapporto negli header e/o nell'oggetto del messaggio originale" che comporta la ricezione del messaggio con gli header arricchiti dal rapporto.

RBL

E' altresì possibile interrogare le liste RBL (Realtime blackhole list) per identificare i messaggi recapitati da sistemi noti per essere fonte di spam.
E' opportuno limitare il numero di liste da interrogare per evitare di avere ripercussioni sulle prestazioni del server. Si tenga presente che ciascuna lista selezionata viene interrogata almeno una volta per qualsiasi messaggio in ingresso, appesantendo quindi l'elaborazione.

Antispam LIVE

Un'altra tecnologia che si può utilizzare nella lotta allo spam è IceWarp Anti Spam LIVE. Questo strumento si appoggia a un centro di rilevazione che monitorando grandi quantitativi di traffico Internet riesce a identificare nuove tipologie di attacchi spam, virus e phishing poco dopo la loro immissione sulla Rete.
Lo scopo di Antispam LIVE non è quello di dare un giudizio finale su di un messaggio quanto piuttosto di integrare il punteggio spam assegnato tramite le altre tecnologie. Per questo motivo Antispam LIVE entra in funzione solo quando il punteggio spam è inferiore a quello necessario per classificare un messaggio come spam (indicato nella sezione "Azione").
Se Antispam LIVE non rileva alcuna traccia di spam in un messaggio c'è anche la possibilità di decrementarne il punteggio totale del valore specificato nelle impostazioni.

Filtro Bayesiano

I filtri bayesiani affrontano lo spam dal punto di vista statistico affidandosi a un database di parole associate alle frequenze con le quali esse compaiono in messaggi spam e genuini.
E' sconsigliato fare uso di sistemi di apprendimento automatico del database bayesiano in quanto gran parte dello spam attualmente in circolazione ricorre a sotterfugi per ridurre l'efficacia dei sistemi che ne fanno uso. Questi trucchi spesso consistono nell'introduzione nel messaggio, anche in forma codificata, di parole di uso comune che possono quindi essere presenti in messaggi genuini. Così facendo se il messaggio viene classificato come spam anche per questi "termini genuini", viene aumentato il valore di occorrenza nei messaggi spam. Procedendo di volta in volta con questi sistemi di "avvelenamento" del dizionario si arriva a situazioni nelle quali il bayesiano non è più in grado di determinare efficacemente cosa è spam e cosa non lo è.
Un'utile funzionalità permette di ignorare determinate parole e quindi evitare di indicizzarle. In questo modo l'amministratore di sistema può inserire quei termini che ricorrono frequentemente nelle comunicazioni di quello specifico sistema e che potrebbero altrimenti essere considerati spam (nomi aziendali, prodotti, ecc).

Liste nera e bianca

La definizione di regole di lista nera e bianca, assieme alle impostazioni della Modalità Antispam (v. sezione "Generale"), permettono agli utenti del mailserver di contribuire alla lotta contro lo spam. Si tenga presente che se la quarantena è attiva, la lista nera e bianca verranno attivate di conseguenza.
Nel caso in cui l'antispam sia impostato a livello utente è comunque possibile definire, da console di amministrazione, delle regole che valgano per un intero dominio o per tutto il sistema. Nel primo caso va indicato come proprietario il nome del dominio senza aggiungere null'altro, nel secondo caso il campo dove si inserisce il proprietario va lasciato vuoto.

Nelle funzionalità di lista nera è anche possibile disporre l'eliminazione automatica dei messaggi provenienti da mittenti inseriti in lista nera. In merito a tale scelta si tenga sempre presente la considerazione precedentemente fatta a proposito dell'eliminazione di messaggi (v. sezione "Azione").
Per quanto riguarda la Lista bianca è anche possibile fare in modo di memorizzarvi automaticamente gli account che rientrano in particolari situazioni.
Una funzionalità che in situazioni di normalità è senz'altro utile attivare è quella che dispone la memorizzazione automatica dei **destinatari di e-mail attendibili**. Dopo aver scritto un messaggio a qualcuno è infatti naturale aspettarsi una risposta e l'aggiunta di tale destinatario ci assicura che la risposta non venga bloccata per un qualsivoglia motivo.

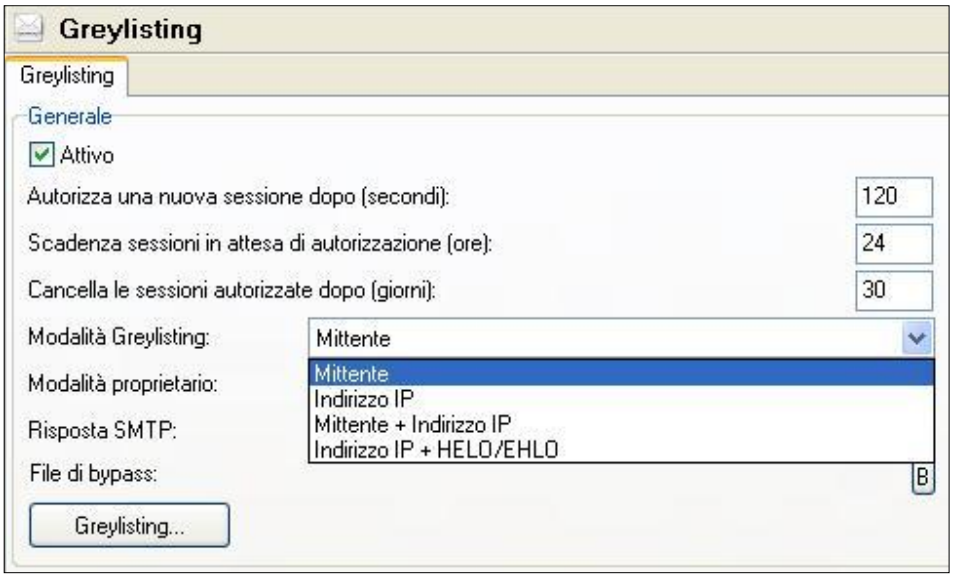
Greylisting

Il Greylisting consiste nel rimandare l'accettazione di una sessione per uno specifico periodo di tempo, basandosi sul fatto che molti sistemi di spamming tentano di effettuare un invio al server e, in caso la sessione non abbia immediatamente esito positivo, non vanno oltre.
Un sistema genuino, invece, osserva di solito le specifiche del protocollo SMTP, che prevedono che a fronte di un rifiuto momentaneo come quello opposto dal Greylisting, debbano essere effettuati ulteriori tentativi, riuscendo a consegnare il messaggio senza particolari disagi per gli utenti.
Tra le impostazioni di personalizzazione del Greylisting vi è la possibilità di stabilire il periodo di tempo per il quale le sessioni autorizzate verranno mantenute tali. E' ragionevole indicare un periodo di tempo abbastanza lungo (tipicamente 30 giorni) per non rendere la funzionalità troppo rigida. E' bene prestare attenzione anche alla **Modalità Greylisting** e alla **Modalità proprietario**.

La prima stabilisce quale informazione controllare per identificare il mittente con quattro possibilità:

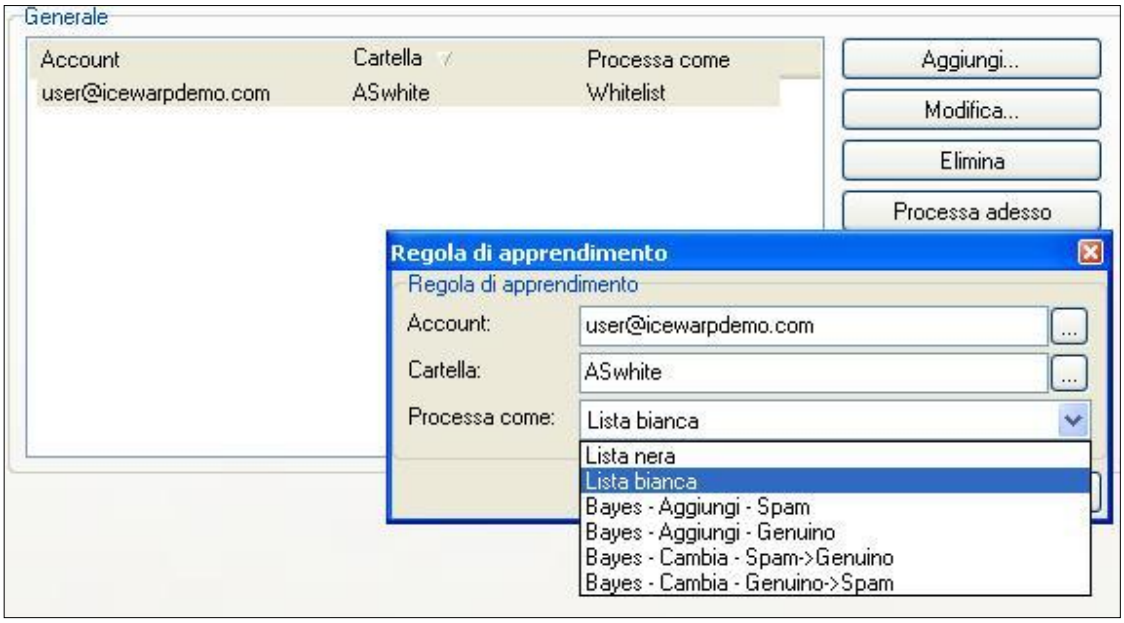
-*Mittente*: solo l'indirizzo email dichiarato in sessione;
-*Indirizzo IP*: solo l'indirizzo IP;
-*Mittente + IP*: entrambe le precedenti informazioni;
-*IP + HELO/EHLO*: l'indirizzo IP e il nome dichiarato in corrispondenza del comando HELO/EHLO in sessione SMTP.

La seconda impostazione invece stabilisce il proprietario della regola. A seconda che l'impostazione sia *E-mail* o *Dominio*, dopo aver superato il Greylisting un determinato account sarà autorizzato ad inizializzare nuove sessioni verso lo stesso destinatario indicato in precedenza o verso tutti i destinatari dello stesso dominio.



Regole di apprendimento

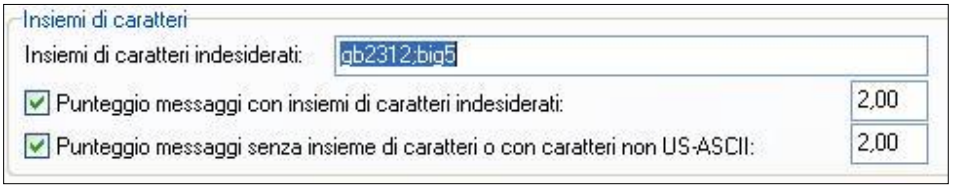
Le regole di apprendimento consentono una approfondita collaborazione da parte degli utenti nella definizione di liste nera e bianca e nell'istruire il sistema bayesiano indicizzando le parole contenute nei messaggi che lo stesso utente riconosce come spam o genuini.
Per sfruttare questa funzionalità è opportuno creare delle apposite cartelle dell'account che saranno poi associate alle diverse regole disponendone quindi l'applicazione ai messaggi presenti al loro interno.



Per le stesse considerazioni fatte nella sezione "Bayesiano" è **fortemente consigliato** evitare di implementare le regole che comportano l'apprendimento del suddetto sistema. Ci si può invece tranquillamente avvalere delle regole **Lista bianca** e **Lista nera** che risultano anche comode laddove un utente non accede o accede raramente alla webmail leggendo invece la posta esclusivamente tramite un client.
Si tenga presente che tutti i messaggi inseriti nelle cartelle associate alle regole di apprendimento vengono **cancellati** dopo che l'indicizzazione è stata portata a termine. Per questo motivo è opportuno copiare i messaggi che si desidera conservare anziché spostarli.

Varie

In questa sezione è possibile personalizzare i punteggi spam assegnati in corrispondenza di specifiche caratteristiche del messaggio. Questi valori non andrebbero mai modificati con leggerezza perché hanno un importante peso nel giudizio finale che l'antispam darà del messaggio (spam o genuino).
Si consiglia di disabilitare le prime due regole di **Contenuto** che assegnano punteggio ai messaggi con parti html e text differenti e a quelli con immagini esterne. Si tratta infatti di due caratteristiche che molti messaggi genuini hanno e che possono pertanto provocare falsi positivi.
La sezione **Insiemi di caratteri** consente invece di specificare i set di caratteri da ritenere indesiderati.



Per quanto riguarda la sezione **Mittente** sono definite tre assegnazioni di punteggio.
La prima si riferisce ai messaggi con dominio del mittente inesistente. E' inutile attivare questa assegnazione nel caso in cui sia stata attivata la funzionalità di respingimento dei messaggi provenienti da tali mittenti [Posta > Sicurezza > Generale > Respingi se il mittente è locale e non autorizzato].
La seconda assegnazione si riferisce invece ai messaggi per i quali l'hostname dichiarato in corrispondenza del comando HELO non si risolve sullo stesso IP dal quale il messaggio è stato consegnato. Potrebbe non essere desiderabile attivare questa assegnazione in quanto molti client dichiarano il nome della macchina o l'indirizzo locale, che chiaramente non corrisponde all'IP con cui è stata aperta la sessione, inviando tuttavia dei messaggi assolutamente genuini.
L'ultima assegnazione consiste invece nella verifica callback SMTP che si accerta che la sessione in corso provenga da un vero server SMTP. Per fare questo viene inizializzata una sessione parallela verso la porta 25 dell'indirizzo IP di provenienza. E' necessario tenere presente che la risposta alla verifica potrebbe tardare fino a 5 secondi e pertanto questa funzionalità potrebbe rallentare sensibilmente il server.