# Utilizzo del server SMTP in modalità sicura

In questa guida forniremo alcune indicazioni sull'ottimizzazione del server SMTP di IceWarp e sul suo impiego in modalità sicura, in modo da ridurre al minimo le possibilità di intrusione e di utilizzo non autorizzato del servizio.
Le impostazioni di seguito descritte rappresentano una situazione ideale di utilizzo del Server SMTP che potrebbe non essere sempre desiderabile per via di necessità o particolarità specifiche dell'installazione. Si invitano pertanto gli amministratori a valutare le proposte avanzate in questa guida per discernere quelle opportune da quelle non opportune nel loro caso.

## Parametri del Servizio

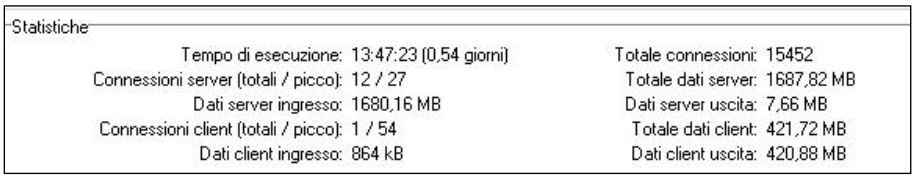
Nella sezione Servizi è possibile controllare l'esecuzione del modulo SMTP variandone alcuni parametri. Nello specifico nella scheda altro è possibile indicare

- *Cache dei thread del server*

  Ogni qualvolta una nuova connessione viene stabilita un thread viene assegnato al suo flusso esecutivo. Per migliorare le prestazioni del sistema, alla chiusura della connessione questi thread vengono immagazzinati in una cache in modo da poter essere riutilizzati e quindi evitando che il server ne debba creare di nuovi.
  La dimensione di default della cache è di 40 thread, si raccomanda di non modificarla a meno che ciò non sia richiesto per motivi particolari.

- *Numero massimo di connessioni entranti*

  Corrisponde al numero massimo di connessioni SMTP Server che possono essere stabilite simultaneamente. Questo limite va dimensionato dopo aver consultato le statistiche del servizio e nello specifico prestando attenzione al picco delle connessioni server.




  Nei casi di picchi contenuti è consigliato mantenere il valore di default (256).
  Unitamente a questa impostazione è opportuno tenere in considerazione il backlog (variabile API *c_system_adv_protocols_backlog*) che corrisponde al numero massimo di

connessioni che possono essere accettate e servite poi in un secondo momento. Il valore consigliato per questa seconda variabile è 5000.

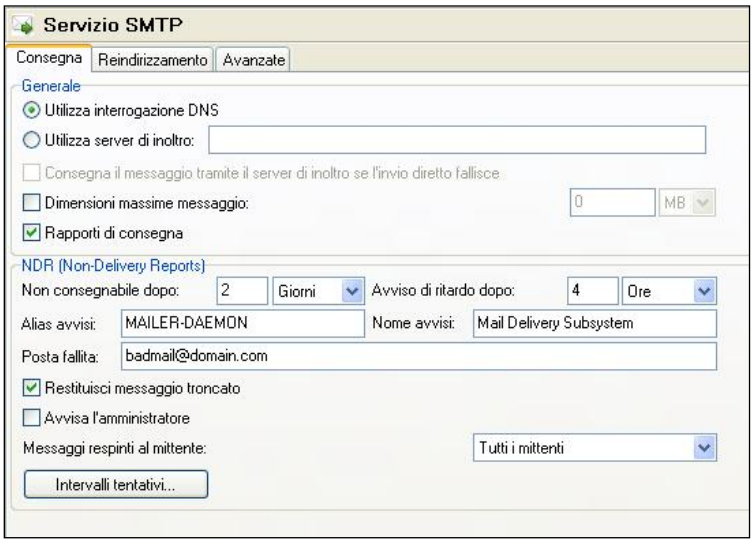
- *Numero massimo di connessioni uscenti*

  Corrisponde al numero massimo di connessioni SMTP Client che possono essere stabilite. Anche per dimensionare questa variabile è necessario tenere conto delle statistiche del servizio e, più precisamente, del valore di picco delle connessioni client. Anche in questo caso il valore di default è 256.

## Servizio SMTP

Nella sezione [Posta > Servizio SMTP] vi è la possibilità di gestire ulteriori parametri riguardanti il funzionamento del servizio.

- *Consegna*




In questa scheda è possibile impostare il sistema affinché faccia costantemente inoltro su di un altro server anziché interrogare i DNS per individuare la posizione dei destinatari remoti, oppure fare in modo che l'inoltro avvenga solo nei casi di mancato successo della consegna diretta.
E' altresì possibile imporre un limite massimo delle dimensioni del messaggio o modificare le tempistiche con le quali viene inviato l'avviso di ritardo di consegna di un messaggio e/o la notifica di mancata consegna.
Al di là di queste impostazioni, che possono essere più o meno desiderabili a seconda dello specifico server e delle preferenze degli amministratori, è sempre consigliato indicare un account adibito alla consegna della *Posta fallita*, evitando così che i rapporti di mancata consegna di messaggi il cui mittente non può essere accertato vadano persi.

- *Reindirizzamento*

Questa funzionalità permette di definire delle regole di reindirizzamento dei messaggi basate sull'indirizzo del destinatario. E' bene non abusare di questa funzionalità e definire nuove regole solo quando effettivamente indispensabile, onde evitare di ottenere comportamenti inattesi e difficilmente deducibili.
Potrebbe ad esempio risultare utile avvalersi del reindirizzamento qualora uno specifico server sul quale risiede il dominio di un destinatario dovesse sistematicamente rifiutare le sessioni stabilite dal server IceWarp. Potremmo allora definire una regola che, solo per i destinatari di quel dominio, imponga l'utilizzo di un server di inoltro.

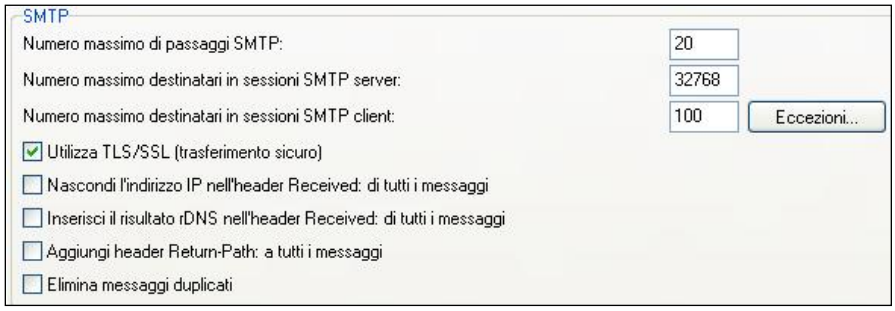
La regola sarebbe del seguente tipo

*Origine*: dominio.com
*Destinazione*: %%alias%%@%%domain%%
*Nome host*: IP server di inoltro

Le variabili *%%alias%%* e *%%domain%%* permettono di lasciare il destinatario esattamente invariato.

- *Avanzate*

In questa sezione i parametri maggiormente utili ai fini di un utilizzo razionale del Server sono quelli indicati nell'apposita sezione SMTP.

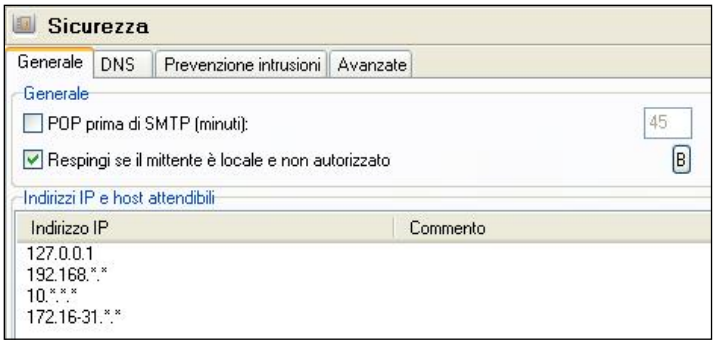



Il *numero massimo di passaggi SMTP* impedisce che si inneschi un loop di sessione in cui un messaggio viene inoltrato da un server all'altro senza mai giungere ad un punto di consegna. Assegnando un valore a questa funzionalità i passaggi effettuati dal messaggio vengono invece contati e al superamento del limite impostato il messaggio viene respinto. Il valore default di 20 è, nella norma, ragionevole nell'individuazione dei relay loop e non troppo restrittivo.
Il *numero massimo di destinatari in sessione SMTP server* e *client* sono invece impostazioni che devono essere date in base a scelte di amministrazione. Si tenga presente che il limite di destinatari in sessione server escluderà automaticamente dall'invio tutti i destinatari che eccedono il limite impostato, mentre il limite in sessione client si tradurrà nella divisione automatica in più sessioni, **portando comunque a termine** l'invio verso tutti i destinatari.

## Sicurezza

La sezione [Posta > Sicurezza] contiene funzionalità cruciali che se impostate opportunamente consentono l'accesso al servizio SMTP solo agli utenti ai quali ciò deve essere permesso.

- *Generale*



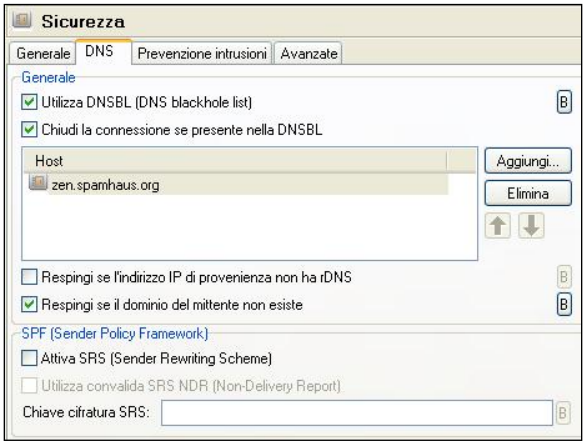

In questa scheda è sempre consigliata l'attivazione della funzionalità *Respingi se il mittente è locale e non autorizzato*. In questo modo quando quando in sessione il mittente dichiara di essere locale gli viene impedito di proseguire a meno che non abbia conseguito opportuna autorizzazione in una delle tre modalità:

- POP prima di SMTP
- IP attendibile
- Autenticazione SMTP

Le prime due modalità di autorizzazione sono attivabili proprio in questa scheda. Mentre è generalmente sconsigliato avvalersi della prima (v. guida "Autenticazione SMTP e relay" per maggiori informazioni), per quanto riguarda la lista di IP è invece consigliato definire i pochi indirizzi statici i cui utilizzatori sono conosciuti e, come dice la descrizione stessa, attendibili (generalmente la rete dalla quale si amministra il server, oltre agli IP assegnati al server stesso).
E' sempre consigliato, ove possibile, imporre/istruire l'utenza ad avvalersi dell'autenticazione SMTP come modalità di autorizzazione della sessione perché essa rimane il metodo più efficace per "chiudere fuori dalla porta" gli ospiti indesiderati a patto che le credenziali degli account siano robuste (v. guida "Messa in sicurezza di un server violato"). Per fare in modo che venga sempre effettuata autenticazione i client devono essere opportunamente impostati. Anche il WebClient ovviamente supporta questa funzionalità.


- *DNS*

  In questa scheda possono essere attivate alcune funzionalità che permettono di interrompere quelle sessioni per le quali i dettagli di chi stabilisce la connessione fanno pensare ad un probabile spammer.

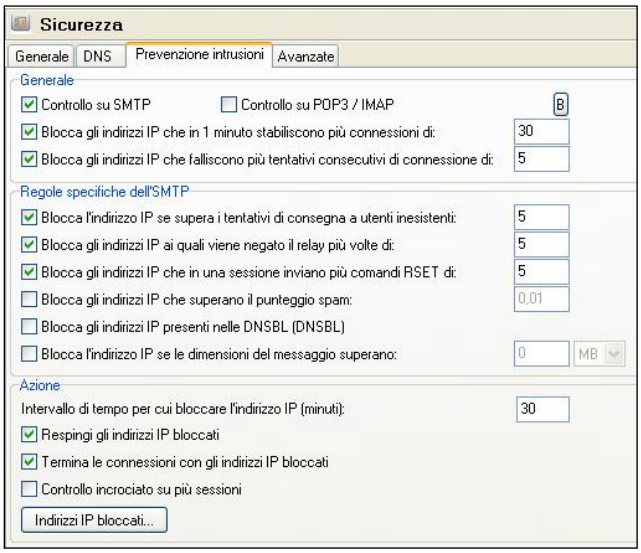



  E' consigliata l'attivazione della DNSBL e della funzionalità *Chiudi la connessione se presente nella DNSBL* (che chiude tutte le connessioni stabilite dagli IP individuati nelle blackhole list). E' attualmente consigliata l'adozione della lista zen.spamhaus.org che permette di ottenere con una singola interrogazione un responso da tutte le liste mantenute da *Spamhaus Project*, rappresentando pertanto un efficientissimo strumento di lotta allo spam.
  E' opportuno verificare, di tanto in tanto, che la lista che è stata adottata sia sempre raggiungibile e funzionante. Una semplice verifica che può essere effettuata consiste nell'effettuare un'interrogazione DNS la cui richiesta sia 2.0.0.127 seguita dall'indirizzo della lista utilizzata (es: 2.0.0.127.zen.spamhaus.org). Se la lista è funzionante, richiedendo il record A si otterrà risultato (127.0.0.2).

E' altresì raccomandato l'utilizzo della funzionalità *Respingi se il dominio del mittente non esiste* che fa una verifica DNS della presenza di un record A per il dominio che viene dichiarato come mittente e, in caso di inesistenza, respinge la sessione.

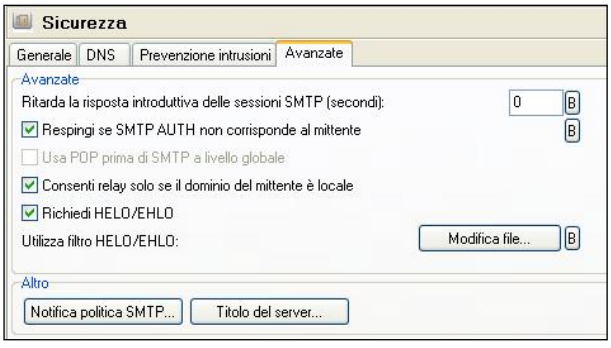
- *Prevenzione intrusioni*

  Questa utile funzionalità permette di bloccare, per un periodo di tempo a scelta, tutti quegli IP che mantengono un comportamento tipico dei sistemi volti ad individuare credenziali di accesso da sfruttare per l'invio di spam.
  Si faccia riferimento all'immagine mostrata sotto per una configurazione generalmente opportuna.




  Si sconsiglia di bloccare gli IP per un periodo successivo ai 30 minuti, considerando che essi potrebbero essere stati assegnati dinamicamente e pertanto essere associati al sistema malevolo solo per breve tempo.
  Se vi è qualche IP statico che deve essere autorizzato a mantenere comportamenti non conformi alle regole definite è possibile indicarlo nell'apposito bypass (B).

- Avanzate



In questa sezione è consigliata l'attivazione della funzionalità *Respingi se SMTP AUTH non corrisponde al mittente*, impedendo così ad un utente di autenticarsi con delle credenziali e successivamente dichiarare che il mittente sia qualcun altro. Questa funzionalità, unita all'autenticazione, lega a doppio filo ciascuna sessione SMTP ad uno specifico utente, rendendo anche più semplice la consultazione dei log.

Affinché un utente possa effettuare relay, ovvero inoltrare un messaggio su di un altro server delegando ad esso la consegna, è necessario che abbia ottenuto autorizzazione per mezzo di uno dei tre metodi precedentemente citati. Se l'autorizzazione è stata ottenuta a mezzo di IP attendibile o di POP prima di SMTP è possibile che il mittente che voglia fare relay sia esterno al server in questione. Per questo motivo è presente la funzionalità *Consenti relay solo se il dominio è locale* che esclude questa possibilità. Attivando questa funzionalità, in aggiunta alla configurazione finora proposta, si avrà la certezza che qualunque messaggio in uscita dal server sia stato generato da un mittente locale, che ha dimostrato di appartenere al server stesso fornendo le proprie credenziali.

Per concludere consigliamo l'attivazione della funzionalità *Richiedi HELO/EHLO* che impone che ciascuna sessione debba incominciare con uno dei due comandi di introduzione, così come richiesto da RFC. Questa richiesta, apparentemente superflua, permette di individuare i mittenti cosiddetti “RFC ignorant” che coincidono nella maggior parte dei casi con sistemi di invio massivo di posta indesiderata.