Utilizzo dei Server DNS e relative implicazioni

Una questione di fondamentale importanza è l'impostazione dei Server DNS. Da questi server dipende il buon esito di tutte le risoluzioni dei nomi di dominio che si rendono necessarie ai fini del funzionamento di IceWarp Server.
La risoluzione DNS è fondamentale per supportare, fra le altre, le seguenti operazioni:

- consegna della posta a destinatari remoti;
- applicazione delle politiche di sicurezza (DNSBL, respingi se il dominio del mittente non esiste, ecc.);
- analisi dei messaggi da parte dell'Antispam (più precisamente da parte delle funzionalità facenti capo alla componente fondamentale SpamAssassin).

L'obiettivo di questa guida è quello di fornire alcuni dettagli sulla configurazione dei DNS su IceWarp e alcune procedure per la verifica del loro funzionamento e della loro efficacia.

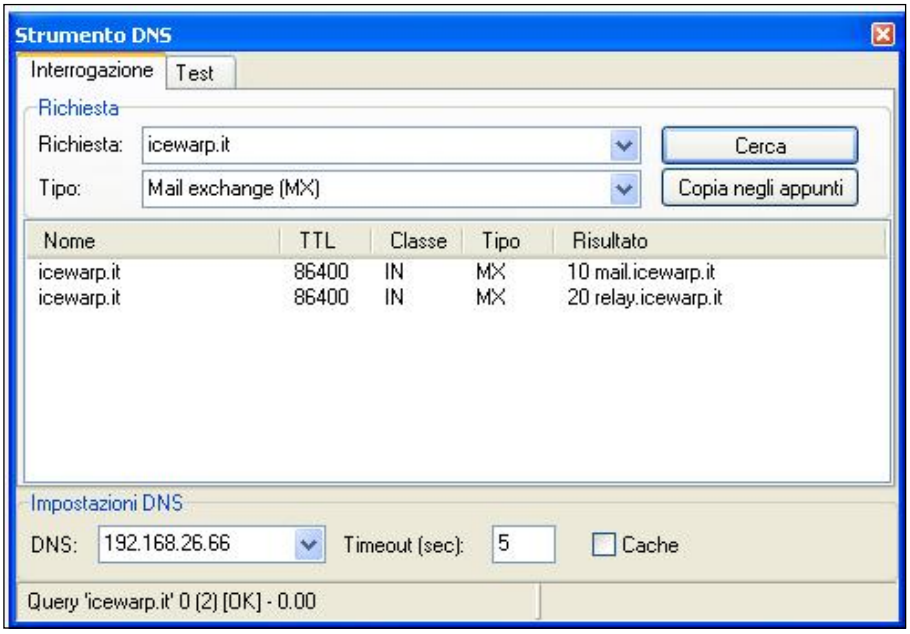
Impostazione Server DNS

La configurazione DNS si trova nella sezione [Sistema > Connessione > Generale]. Gli indirizzi dei Server DNS ai quali fare riferimento possono essere indicati nell'apposito campo, separandoli con un punto e virgola.
E' bene indicare due o più Server DNS i quali verranno interrogati in modalità round-robin (se l'interrogazione di uno di essi fallisce si passerà ad interrogare il successivo e così via). Per impostazione predefinita viene rilevato l'indirizzo configurato come Server DNS preferito nella scheda di rete del server, indirizzo che si può riassegnare anche premendo il tasto : posto a destra del campo indirizzi.
Particolarmente importanti sono le altre impostazioni della sezione. Il *timeout di interrogazione* stabilisce il tempo massimo da attendere prima di ritenere fallita un'interrogazione e passare al server successivo. La *cache di risoluzione* permette invece di memorizzare un determinato

numero di interrogazioni senza doverle effettuare ogni volta, aumentando di conseguenza le prestazioni del Server.
Un'impostazione ragionevole per questa opzione ricade nel range di valori tra 128 e 512. E' sconsigliato eccedere onde non impegnare troppa memoria di sistema e non immagazzinare troppe risoluzioni, tenendo anche conto del fatto che il loro esito potrebbe variare dopo un certo periodo di tempo.

Verificare il funzionamento dei Server DNS

Nella sezione di configurazione dei server DNS di IceWarp ci sono due utili strumenti per verificare rapidamente ed efficacemente il funzionamento dei server che si è scelto di utilizzare. Il pulsante “Test server DNS” permette di effettuare un'interrogazione di prova e restituisce un messaggio di successo o di errore in base all'esito della stessa mentre lo “Strumento DNS” consente la definizione e l'esecuzione di interrogazioni approfondite indicando la richiesta, il tipo di record che si vuole ottenere e fornendo una risposta corredata da TTL (tempo di esecuzione), classe e priorità.



Lo strumento permette di effettuare qualsiasi tipo di interrogazione sul server indicato, richiedendo tutti i record o un record specifico ed eventualmente mettendo in cache le interrogazioni già effettuate (che, se eseguite nuovamente, verranno prelevate direttamente dalla cache).

Dato l'elevato numero di risoluzioni DNS che il mail server deve effettuare durante le normali attività di invio e ricezione, l'importanza del loro esito e l'influenza sulle prestazioni del sistema, è fondamentale utilizzare server DNS affidabili e verificarne periodicamente lo stato di buon funzionamento.

Verificare il funzionamento di una DNSBL

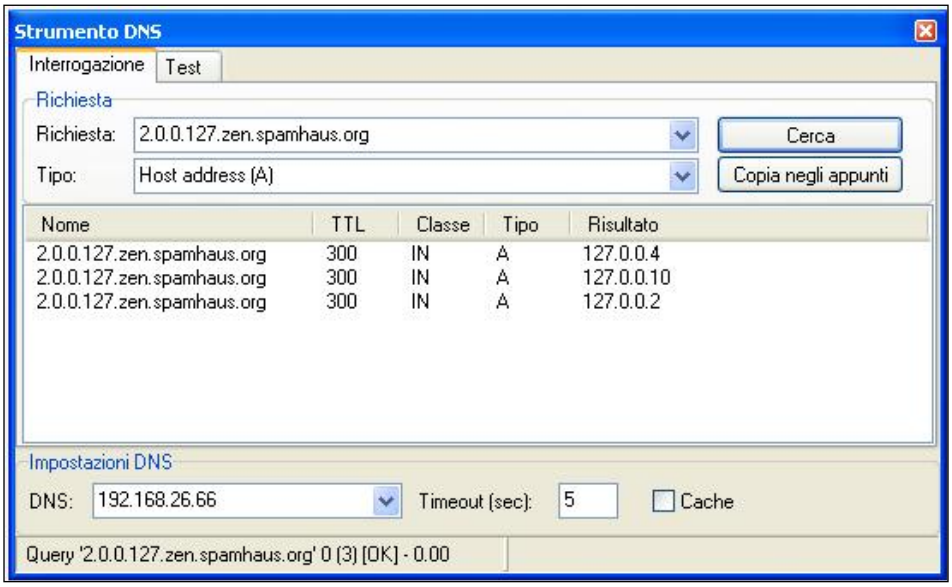
Le DNSBL (DNS Blackhole-lists) sono elenchi aggiornati di indirizzi IP associati a server o reti note per dare origine a un certo numero di comunicazioni spam o per non aiutare a fermarle (contribuendo quindi indirettamente alla loro diffusione). Sulle DNSBL si basano alcune funzionalità di Sicurezza (la possibilità di chiudere qualsiasi connessione proveniente da un indirizzo IP inserito in una di esse o il blocco dell'indirizzo IP per mezzo del sistema di Prevenzione intrusioni) nonché il sistema Realtime Blackhole lists (RBL) di SpamAssassin.
Tramite il già citato Strumento DNS è possibile verificare il funzionamento di una DNSBL con i server ai quali ci si appoggia. Infatti non tutti i server DNS permettono di interrogare tutte le DNSBL con successo. Ad esempio alcuni resolver gratuiti come *Google Public DNS* e *Level3* non sono adatti all'interrogazione delle liste mantenute da Spamhaus Project, che sono fra le più complete e affidabili attualmente in circolazione.
E' quindi opportuno, per quanto possibile, avvalersi dei propri server DNS (tipicamente quelli messi a disposizione dal proprio fornitore di connettività) ai fini della consultazione delle DNSBL.

La verifica dell'efficacia di un determinato server DNS nell'interrogazione di una specifica lista può essere effettuata abbastanza semplicemente. La maggior parte delle liste permette di effettuare un test di funzionamento con una richiesta di record A nella seguente forma:

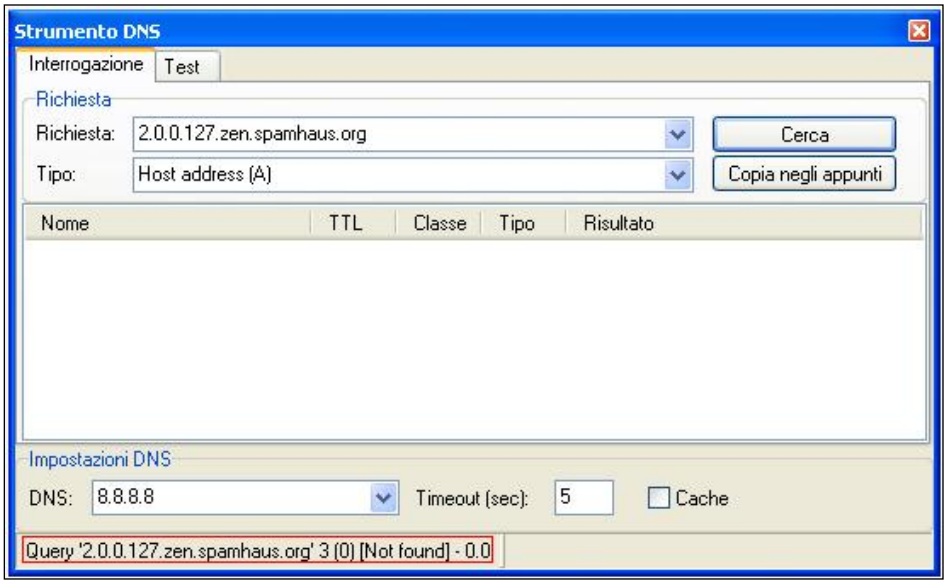
2.0.0.127.<nomelista>

Se l'interrogazione produce esito positivo, vengono di solito restituiti un certo numero di risultati nella forma *127.0.0.x* dove *x* corrisponde al codice di classificazione che viene assegnato dalla lista a ciascun elemento in essa inserito.

Si veda il seguente esempio:



La stessa interrogazione, nel momento in cui questa viene scritta, non sempre produce risultato se effettuata appoggiandosi ad un server DNS pubblico di Google:



Registrazione attività

La risoluzione DNS, come tutte le altre operazioni effettuate a partire da IceWarp Server, può essere registrata in un apposito log attivabile da [Sistema > Registrazione > Debug > Log DNS].
Il logging della risoluzione DNS può rivelarsi particolarmente utile per rilevare intoppi nel flusso comunicativo o altre problematiche causate da risoluzioni fallite o eccessivamente lunghe.
Le informazioni registrate sono dettagliate e facilmente interpretabili.
A titolo di esempio riportiamo il logging corrispondente all'invio di un messaggio ad un destinatario remoto (del dominio *icewarp.it*), effettuato da un client di posta elettronica avente indirizzo IP 1.2.3.4:

```
SYSTEM [1098] 16:27:13   4.3.2.1.combined.njabl.org.(A)-> res=1, responsecode=3, ancount=0 500 ms
SYSTEM [1098] 16:27:13   4.3.2.1.dnsbl.sorbs.net.(A)-> res=1, responsecode=3, ancount=0 344 ms
SYSTEM [1098] 16:27:14 * 4.3.2.1.zen.spamhaus.org.(A)-> res=1, responsecode=3, ancount=0 531 ms
SYSTEM [1098] 16:27:14   4.3.2.1.bl.spamcop.net.(TXT)-> res=1, responsecode=3, ancount=0 188 ms
SYSTEM [1098] 16:27:15 * 4.3.2.1.plus.bondedsender.org.(A)-> res=1, responsecode=3, ancount=0 1031 ms
SYSTEM [1098] 16:27:15   4.3.2.1.list.dnswl.org.(A)-> res=1, responsecode=3, ancount=0 375 ms
SYSTEM [0EC4] 16:27:15   icewarp.it(MX)-> res=1, responsecode=0, ancount=2 0 ms
SYSTEM [0EC4] 16:27:15   mail.icewarp.it(A)-> res=1, responsecode=0, ancount=1 0 ms
```

Sul sistema utilizzato per l'esempio era attivo l'Antispam con elaborazione estesa anche ai messaggi in uscita. Come si potrà notare, l'indirizzo IP di provenienza (rovesciato secondo la convenzione delle DNSBL, cioè con gli ottetti letti da destra verso sinistra: 1.2.3.4 -> 4.3.2.1) è stato confrontato con tutti i server RBL attivi (prime 4 righe) oltre ad altri due server legati a regole di SpamAssassin (righe 5 e 6). In tutti questi casi è stato ottenuto *responsecode* 3 (Not found), cioè l'indirizzo IP cercato non era presente nelle DNSBL/RBL interrogate.
Dopo questi controlli, effettuati durante la sessione SMTP Server di ricezione, il sistema ha provveduto a risolvere il nome del dominio di destinazione *icewarp.it* ottenendone il record MX il quale è stato a sua volta risolto ottenendo il record A corrispondente, ovvero l'indirizzo IP del server remoto, informazione che ha permesso infine di stabilire la sessione Client di consegna del messaggio.