r t Anno 2009_Numero 107

rapporti tecnici INGV

Rete informatica INGV Roma

107

Istituto Nazionale di Geofisica e Vulcanologia

Anno 2009_Numero 107

rapporti tecnici INGV

RETE INFORMATICA INGV ROMA

Massimiliano Rossi, Emanuele Sammali, Manuela Sbarra, Gianpaolo Sensale, Diego Sorrentino, Francesco Zanolin, Lucio Badiali, Francesca Caprara, Pierluigi Cau, Pietro Ficeli, Melissa Mendicino

INGV (Istituto Nazionale di Geofisica e Vulcanologia, Centro Nazionale Terremoti - Servizi Informatici e Reti)

107

Indice

1. Analisi del progetto

1.1 Obiettivi

Durante il passaggio alla nuova connettività SPC[1], la rete informatica della sede INGV di Roma è stata oggetto di numerose valutazioni per rilevarne i punti deboli e poter realizzare, contestualmente alla migrazione, una nuova infrastruttura più performante, sicura e flessibile.
L'attuale struttura di rete impone molte limitazioni ai normali utenti, ai ricercatori con particolari esigenze e al servizio di sorveglianza sismica.
La chiusura indiscriminata di servizi offerti all'esterno della sede e l'utilizzo di proxy[2] per la navigazione sono i problemi maggiormente sentiti da utenti e ricercatori, mentre l'eccessiva suddivisione della rete esterna crea spesso disagi ai servizi di sorveglianza sismica, specie in fase di attivazione di server per lo scambio dati che in fase di ripristino del servizio a seguito di failure o aggiornamenti.
A causa della rigida struttura di rete spesso si deve ricorrere a complessi stratagemmi per permettere la comunicazione tra server su reti differenti, introducendo lentezza nella propagazione delle informazioni, utilizzo di risorse non necessarie (risorse intese come server, indirizzi pubblici, alimentazione, impianti di raffreddamento, spazio in sala macchine, tempo dedicato alla manutenzione e aggiornamento) numerosi punti di rottura (failure points) e difficoltà nel tracciare le connessioni.
La rete che si intende realizzare si propone come soluzione alle problematiche esistenti.

2. Progettazione

2.1 Vincoli

Al momento della riprogettazione della rete sono stati imposti i seguenti vincoli:

- La rete interna (MZ, rete Militarizzata) non deve, in nessun modo, essere visibile dall'esterno;
- Se un servizio in MZ deve essere raggiungibile dall'esterno, questo servizio sarà mappato sui sistemi di sicurezza perimetrale;
- Gli utenti della MZ devono poter utilizzare qualsiasi servizio offerto sulla BigInternet, purché l'utilizzo non sia causa di possibili problemi legali per l'Ente;
- Gli utenti devono poter navigare il World Wide Web con le impostazioni di default del browser;
- Gli utenti delle sedi INGV esterne ma dipendenti da Roma devono poter accedere in MZ su canale dedicato e cifrato e godere degli stessi diritti e doveri dei dipendenti della sede centrale;
- Ogni utente può consultare la propria casella di posta esterna, in IMAP[3] e POP3[4];
- L'unico server autorizzato ad inviare posta all'esterno della Sede è il mail-server istituzionale, posto in rete esterna (DMZ, rete Demilitarizzata);
- I server della DMZ devono poter utilizzare qualsiasi servizio offerto sulla BigInternet, purché l'utilizzo non sia causa di possibili problemi legali per l'Ente;
- Gli amministratori di server in DMZ possono scegliere i livello di sicurezza da applicare alla macchina:
  - **OpenServer**
    tutta la sicurezza della macchina è demandata al suo amministratore;

[1] Il **SPC** (Sistema Pubblico di Connettività) rappresenta la nuova infrastruttura di rete della *Pubblica Amministrazione* a cui potranno connettersi, oltre alle Pubbliche Amministrazioni Centrali, anche quelle locali.
L'infrastruttura del SPC è la naturale evoluzione della **RUPA** (Rete Unitaria della Pubblica Amministrazione), a cui si sta progressivamente sostituendo.
Vedi http://www.cnipa.gov.it/site/_files/5.SPC,Architettura%20SPC,Q,3.0.pdf.
[2] Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client.
[3] L'*Internet Message Access Protocol*, a volte anche chiamato *Interactive Mail Access Protocol*, è un protocollo di comunicazione per la ricezione di e-mail
[4] Il *Post Office Protocol* è un protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente su di un host per scaricare le e-mail del relativo account

o **ClosedServer**
la macchina risulta raggiungibile solo dalla MZ e DMZ ma risulta invisibile all'esterno;
o **Ibrido**
ogni amministratore richiede quali servizi aprire, world-wide o point-to-point.

I servizi più comunemente richiesti sono attivi di default per rendere la macchina operativa già al momento della sua installazione;

- Aggregazione di servizi per tipologia e utilizzo di risorse;
- Lo scambio dati tra diverse sedi INGV deve avvenire su canale dedicato e cifrato;
- L'acquisizione dati per il servizio di Sorveglianza Sismica deve avere un canale di comunicazione dedicato, separato dal resto dell'utenza;
- Riduzione delle risorse coinvolte nello scambio dati;
- Continuità dei servizi di rete, sorveglianza sismica e scambio dati durante la migrazione.

2.2 Progettazione dei lavori

La necessità di soddisfare i vincoli e adeguare la struttura di rete al nuovo tipo di connettività impone una completa ristrutturazione dell'intera infrastruttura informatica, non totalmente realizzabile sull'attuale struttura in quanto è necessario mantenere la continuità del servizio.
Per poter procedere quindi sarà necessario realizzare una rete parallela a quella attuale, che condivida lo spazio utenti interno mentre si realizzerà ex novo tutta la parte dai sistemi di sicurezza perimetrali fino alla BigInternet.

2.3 Risorse a disposizione

2.3.1 Connettività

Secondo il contratto SPC, l'Ente verrà fornito di diverse connettività ognuna di esse ridondata, sia come apparati fisici che come linee di comunicazione.
Gli apparati sono stati configurati in modalità VRRP[5], per convenzione utilizzando sempre gli ultimi tre indirizzi IP della classe in cui risiedono.
Le connettività saranno:
Linea a 60Mbps
completamente dedicata agli utenti (*zona Web*);
Linea a 20Mbps
dedicata al servizio di sorveglianza sismica (*zona Research*);
Linea a 10Mbps
dedicata allo scambio dati tra gli afferenti al contratto SPC (*zona Infranet*). Si propone come linea di backup in caso di totale failure della BigInternet;
Linea a 10Mbps
Virtual Private Network dedicata agli utenti delle sedi INGV (*VPN C*);
Linea a 10Mbps
Virtual Private Network dedicata allo scambio dati e al servizio di sorveglianza sismica tra sedi INGV (*VPN B*).

2.3.2 Indirizzamento

La sede romana ha ottenuto, da contratto, un indirizzamento diverso per ogni tipo di connettività sulla BigInternet acquistata:

Zona Web
rete 85.18.36.48, netmask 255.255.255.248;
Zone Research
rete 89.97.133.144, netmask 255.255.255.240;

[5] Il *Virtual Router Redundancy Protocol* è un metodo comunemente utilizzato per evitare interruzioni di rete durante il trasferimento di dati importanti. Il VRRP crea un collegamento virtuale tra i router all'interno di una stessa rete e legami con essi. Se il primo router usato per trasmettere i dati non riesce per qualsiasi motivo, un altro router rileva automaticamente il trasferimento.

Zona Infranet
rete 89.97.125.17, netmask 255.255.255.240;
A queste si aggiunge una intera classe C dedicata ai nostri server esposti:
Zona Ext-Ingv
rete 93.63.40.0, netmask 255.255.255.0

2.3.3 Hardware necessario

Per poter soddisfare alcune richieste è stato deciso di configurare più servizi su di una unica macchina, adeguatamente potenziata per poter sopportare il carico di lavoro.
Si è deciso, quindi, di raggruppare all'interno del sistema di sicurezza sia il DNS[6] secondario che il servizio Proxy nascondendolo, così da renderne l'utilizzo completamente trasparente agli utenti.
Per poter gestire adeguatamente le diverse reti separando il loro traffico è necessario che la macchina disponga di un adeguato numero di schede di rete.
Dalle precedenti specifiche si evince la delicatezza di questa macchina che dovrà quindi essere necessariamente ridondata poiché, in caso di failure, senza di essa si fermerebbe completamente qualsiasi forma di comunicazione con la BigInternet.

2.4 Schema di rete

A seguito di tutti i lavori di migrazione e ammodernamento, la struttura di rete dovrà essere consistente con quella mostrata in figura 1.

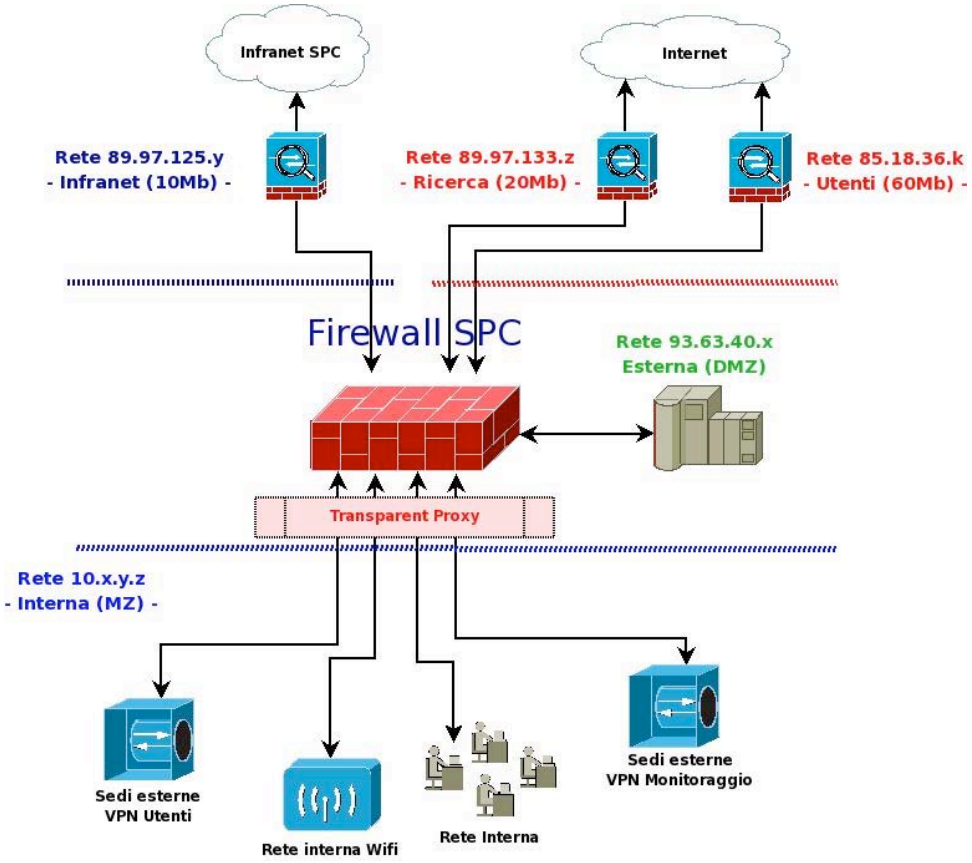

Figura 1. Nuova struttura della rete romana.

[6] *Domain Name System* è un servizio utilizzato per la risoluzione di nomi di host in indirizzi IP e viceversa. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS.

3. Realizzazione

3.1 Scelte tecnologiche

Per la realizzazione del nuovo sistema si è deciso di realizzare una soluzione utilizzando completamente *software libero* in quanto permette una elevata sicurezza e una totale personalizzazione del sistema:
GNU/Linux Debian 4.0
è una distribuzione GNU/Linux largamente usata e sviluppata attraverso la collaborazione di volontari da ogni parte del mondo[7];
IPTables
sofisticato software per l'intercettazione e manipolazione dei pacchetti in transito;
Bind
il più famoso ed utilizzato server DNS sulla BigInternet;
Squid
popolare software libero con funzionalità di proxy e web cache.

3.2 Configurazione GNU/Linux Debian

La distribuzione è stata installata seguendo la procedura di NetInstall, nella sua versione basilare, così da avere immediatamente tutti i pacchetti già all'ultima versione disponibile.
Sono stati, successivamente, installati i servizi SSH, per la gestione della macchina da remoto, Proxy e NameServer, non inclusi nella versione base.

3.2.1 Sicurezza del sistema
La macchina è stata immediatamente scollegata e si è provveduto alla sua messa in sicurezza seguendo l'Hardening HowTo[8] pubblicato direttamente sul sito uffiale della distribuzione.
E' stato inoltre disabilitato il supporto per il nuovo protocollo IPv6, in quanto non ancora utilizzato.

3.2.2 Configurazione della rete
La macchina è stata abilitata al forwarding dei pacchetti attraverso le differenti reti, altrimenti non sarebbe stato possibile utilizzare il sistema come un router.
Sono stati attivati i filtri di Reverse-path per prevenire attacchi di spoofing. In un usuale sistema GNU/Linux le interfacce di rete sono identificate con nomi del tipo *eth***x**, dove **x** è il numero progressivo della scheda di rete.
Per semplificare l'individuazione di problemi ogni scheda è stata rinominata a seconda della rete a cui afferisce:
int-ingv
rete interna MZ,
ext-ingv
rete esterna DMZ,
web
connettività dedicata agli utenti,
research
connettività dedicata alla sala sismica,
infranet
connettività dedicata alla comunicazione con gli altri Enti afferenti a SPC,
heart
sistema di failover.

Data la crescita di reti attualmente presenti, si è deciso di installare nel sistema ulteriori interfacce di rete che potrebbero essere utilizzate per evoluzioni future.

[7] http://www.debian.org
http://it.wikipedia.org/wiki/Debian
[8] http://www.debian.org/doc/manuals/securing-debian-howto/

3.2.3 Configurazione del FailOver

Per poter ottenere un servizio affidabile si è deciso di avere due sistemi completamente uguali e sincronizzati in modalità FailOver, uno attivo l'altro passivo sempre pronto ad entrare in funzione appena la macchina attiva subisce un guasto.
Il servizio è stato configurato per controllare ad intervalli regolari se la macchina attiva è funzionante. Sono stati attivati i controlli sia su cavo seriale che su scheda di rete (*interfaccia heart*).
Quando uno dei due controlli non va a buon fine la macchina attiva passa in modalità passiva e quella passiva prende il controllo.
All'avvio del servizio, il sistema di failover elegge, secondo direttive, la macchina attiva ed esegue uno script sulla macchina passiva così da disattivare tutte le interfacce di rete, tranne quella di *heartbeat*.
Quando la macchina attiva subisce un failure, il sistema di failover esegue lo stesso script e ne disattiva tutte le schede di rete (tranne la *heartbeat*). Nel frattempo il sistema di failover presente sulla macchina passiva viene informato del problema e configura il server in modalità attiva.

3.3 Configurazione IPTables

Il precedente sistema di firewalling è stato completamente riscritto, strutturando in maniera gerarchica le regole di filtraggio, abilitando l'esposizione di servizi interni su reti esterne e sfruttando le potenzialità delle "connessioni stabilite" (vedi capitolo 4).

3.4 Configurazione Bind

Data la crescente struttura di rete, interna ed esterna, abbiamo deciso di nominare diversamente ogni zona di rete con un diverso nome di dominio, seguendo lo standard adottato per i nomi delle interfacce di rete.
Sono state quindi attivate le nuove seguenti zone:

- ext-ingv.rm.ingv.it
- web.rm.ingv.it
- research.rm.ingv.it
- infranet.rm.ingv.it

Ogni macchina contenuta nelle suddette zone avrà poi, a seconda del servizio offerto, un alias[9] nelle principali zone di dominio di secondo o terzo livello, ingv.it o rm.ingv.it rispettivamente.
Il servizio di Name Server su questo server è primario per le seguenti zone:

- web.rm.ingv.it
- research.rm.ingv.it
- infranet.rm.ingv.it

mentre è secondario per le zone:

- ingv.it
- rm.ingv.it
- ext-ingv.rm.ingv.it

La macchina è stata aperta per la sincronia esclusivamente per gli altri Name Server autorizzati.

3.5 Configurazione Squid

La configurazione del server Proxy è stata riprogettata per permetterne l'utilizzo senza richiedere alcuna configurazione manuale da parte degli utenti all'interno del loro browser (vedi Figura 2).

[9] *CNAME*, permette di collegare un nome DNS ad un altro. La risoluzione continuerà con il nuovo nome indicato dal record CNAME. Questa funzione è molto utile quando, ad esempio, sullo stesso server sono disponibili più servizi

Il servizio di Proxy è stato configurato per accettare connessioni esclusivamente sulla porta 3128, universalmente riconosciuta.

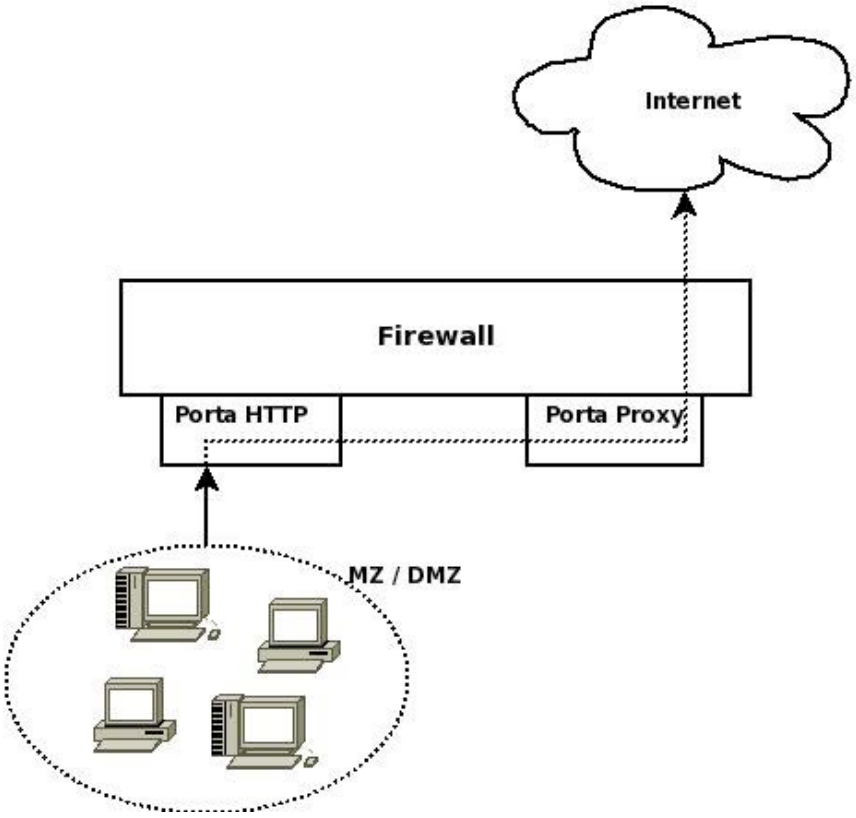

Figura 2. Configurazione del Transparent Proxy.

Il servizio che attualmente si è deciso di far passare attraverso Proxy è il servizio HTTP[10], sulla porta 80, e l'HTTP del server Tomcat[11], sulla porta 8080.
Per poter, quindi, far passare il traffico attraverso il server attivo è stata attivata una regola di reinstradamento dei pacchetti in ingresso al firewall sulle porte dei servizi da *proxare* verso quella del servizio.
Esternamente ogni utente viene identificato con l'IP esterno della zona dedicata agli utenti, assegnato al firewall.
I servizi HTTPS e HTTPS-Tomcat non sono stati rediretti in quanto il server Proxy in uso, per questo tipo di connessioni, entra in modalità passiva non filtrando né cachando i dati, rendendo vana l'operazione e appesantendo inutilmente il carico di lavoro della macchina.

3.6 Sicurezza del sistema

Sul server è stato attivato il servizio SSH per l'amministrazione del server da remoto.
L'accesso alla macchina è consentito solo da console e tramite scambio di chiavi SSH.
L'utente ROOT non può loggarsi direttamente da remoto, si deve accedere alla macchina come utente ed effettuare la "scalata dei permessi".
L'unico utente autorizzato ad accedere via SSH come ROOT è l'utente RESTARTER, a cui è concesso esclusivamente l'accesso da un server e per poter eseguire un riavvio del servizio di Name Server.

[10] L'*Hyper Text Transfer Protocol* (protocollo di trasferimento di un ipertesto), usato come principale sistema per la trasmissione di informazioni sul web. Le specifiche del protocollo sono gestite dal **World Wide Web Consortium**.
[11] *Apache Tomcat* (o semplicemente Tomcat) è un web container open source sviluppato dalla **Apache Software Foundation**. Implementa le specifiche *JSP* e *Servlet* di **Sun Microsystems**, fornendo quindi una piattaforma per l'esecuzione di applicazioni Web sviluppate nel linguaggio *Java*. La sua distribuzione standard include anche le funzionalità di web server tradizionale, che corrispondono al prodotto *Apache*.

Sfruttando il PAM[12] si è ristretto l'accesso come ROOT ai membri di un gruppo particolare.

4. Firewall

In Informatica, nell'ambito delle reti di computer, un firewall[13] è un componente passivo di difesa perimetrale (hardware o software) che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.
Usualmente la rete viene divisa in due sottoreti:
una, detta esterna, comprende l'intera Internet mentre l'altra interna, detta LAN[14], comprende una sezione più o meno grande di un insieme di computer locali.
In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall.
Grazie alla sua posizione strategica, il firewall risulta il posto migliore ove imporre delle logiche di traffico per i pacchetti in transito e/o eseguire un monitoraggio di tali pacchetti. La sua funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza.

4.1 Caratteristiche IPTables

Il nuovo sistema di protezione perimetrale include, tra le svariate feature, la possibilità di:

- definire dei blocchi di regole, chiamati **CATENE**, in cui si possono instradare i pacchetti filtrandoli in base al loro contenuto;
- definire una connessione **STABILITA**, che crea un canale di comunicazione tra 2 macchine che permette ai pacchetti appartenenti a tale connessione di transitare direttamente senza dover attraversare tutte le regole;
- aprire nuove porte di comunicazione purché appartenenti a una connessione preesistente (connessione **RELATIVA**);
- gestire in maniera ottimale il **LOG** prodotto;
- rifiutare le connessioni.
-

Queste sono principalmente le funzionalità sfruttate che verranno di seguito analizzate.

4.2 Definizione di catene custom

Avendo la possibilità di definire delle catene personalizzate si può redirigere un pacchetto in base sia al servizio che si vuole utilizzare che alle macchine che si desidera raggiungere.
In INGV si è deciso di percorrere entrambe le strade.
Sono state create diverse catene a seconda dei servizi più offerti, quali Server Web, standard e sicuro, Server FTP , Server Tomcat, standard e sicuro, e così via...
Istruendo la catena principale di IPTables che si occupa di far transitare pacchetti (catena **FORWARD**) a filtrare in base al servizio richiesto e inserendo in ogni catena l'elenco di macchine che offrono tale servizio (o necessitano del servizio) è stato possibile ridurre sensibilmente la richiesta computazionale e aumentare la responsività del sistema (vedi Figura 3).
In aggiunta sono state attivate regole di filtraggio più stringenti in base al servizio da raggiungere (non tra i precedentemente menzionati) e il server che lo espone, abilitando quando richiesto solo connessioni punto-punto.

---

[12] *Pluggable Authentication Modules* è un meccanismo per integrare più schemi di autenticazione a basso livello in un'unica API ad alto livello, permettendo a programmi che necessitino di una forma di autenticazione, di essere scritti indipendentemente dallo schema di autenticazione sottostante utilizzato.
[13] termine inglese dal significato originario di parete refrattaria, muro tagliafuoco; in italiano anche parafuoco o parafiamma.
[14] *Local Area Network.*

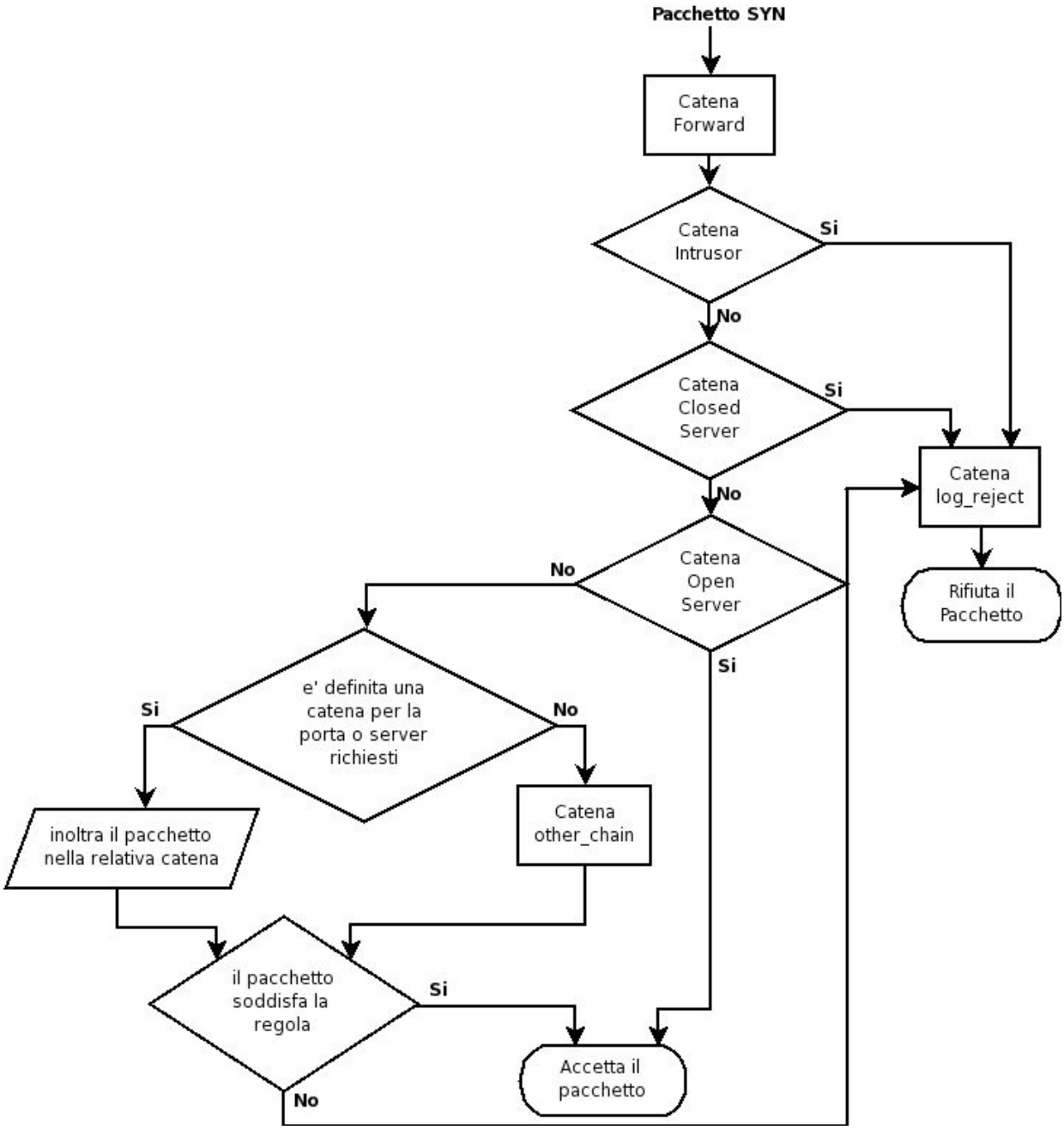

Figura 3. Percorso pacchetto SYN.

4.3 Connessioni stabilite

Il concetto di connessione stabilita ha permesso di aumentare le performance del firewall semplicemente obbligando il sistema ad accettare incondizionatamente tutti i pacchetti validi relativi ad una connessione già instaurata (vedi Figura 4).
Inserendo questa istruzione all'inizio della catena di **FORWARD** (la catena che si occupa di far transitare i pacchetti) i pacchetti successivi al primo non passano più attraverso le catene personalizzate ma vengono instradati direttamente riducendo la richiesta computazionale.

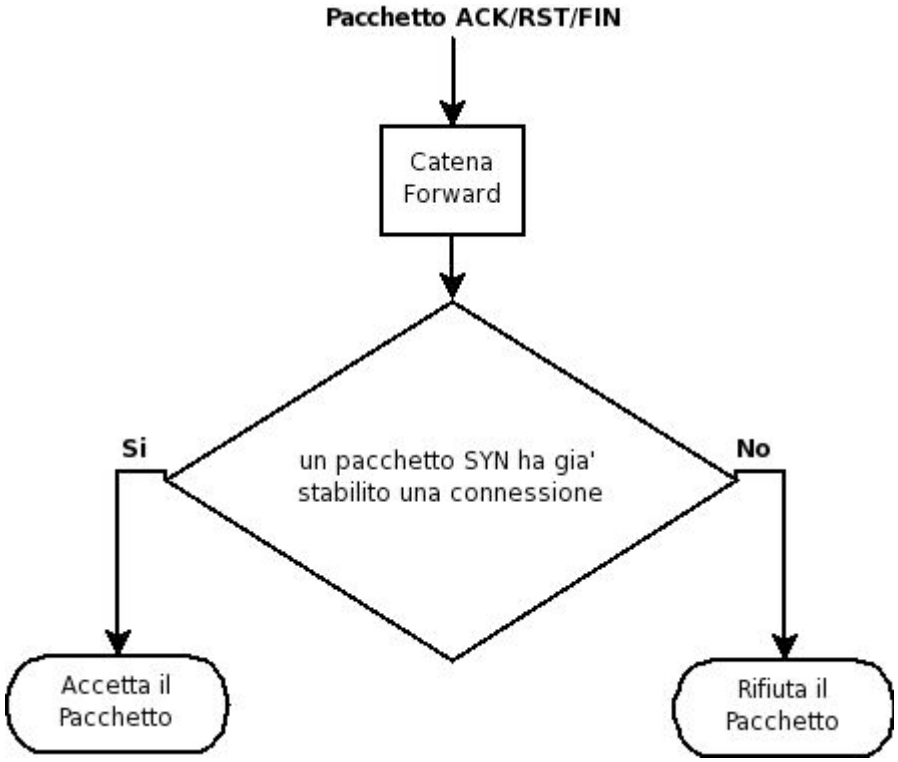

Figura 4. Percorso pacchetto di una connessione STABILITA.

4.4 Apertura nuove porte di comunicazione

Agganciando alla funzionalità di connessione stabilita quella di relazione a una connessione preesistente è possibile istruire il sistema per fargli accettare le nuove connessioni derivanti da quella originale, solitamente reindirizzate al di sotto delle porte privilegiate (porte 1-1024).
Questa funzionalità si è rivelata molto importante in quanto permette di chiudere senza alcun problema tutte le porte sapendo che in caso di necessità il sistema si auto-regolamenta, aprendo solo le porte strettamente necessarie per lo scambio di informazioni che poi verranno richiuse al termine della comunicazione.

4.5 Gestione dei LOG

Nel nuovo sistema è possibile abilitare la funzione di LOG sia per ogni catena personalizzata che per ogni servizio o macchina (vedi paragrafo 4.2) generando solo una riga per ogni connessione (relativa al pacchetto *SYN* - vedi figura 5) alleggerendo sia il lavoro dell'amministratore di rete che dovrà solo controllare che quell'unica riga non sia stata inoltrata nella catena di scarto, sia il lavoro della macchina che non deve più scrivere grosse moli di dati su disco, dispositivo incredibilmente lento rispetto ai tempi computazionali del resto della macchina. x
Usando le syslog facilities, oltretutto, i log del firewall sono stati rediretti su un file diverso da quello di sistema, così da avere un log file dedicato e pulito.

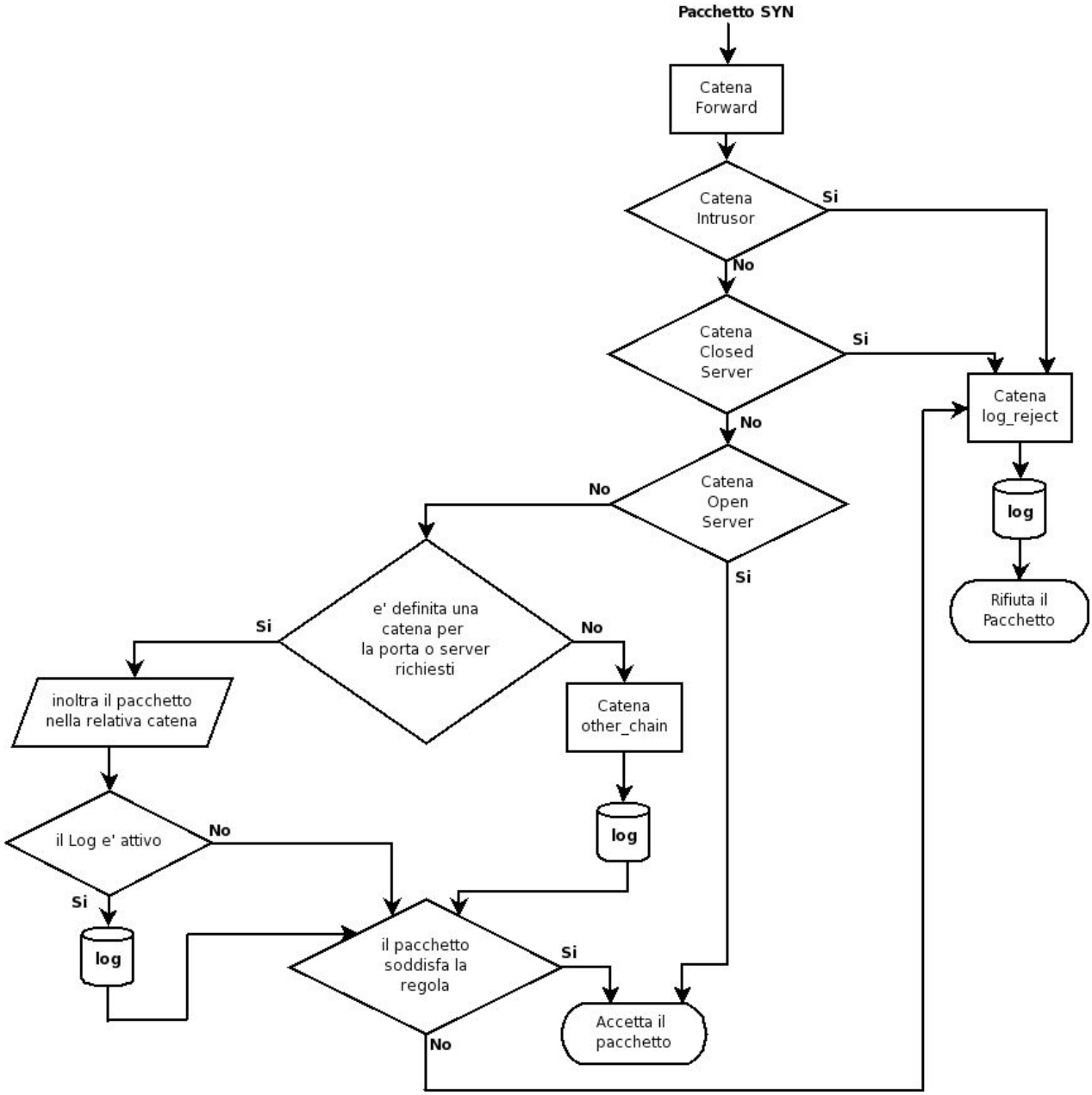

Figura 5. Sistema di tracciamento delle connessioni.

4.6 Rifiuto delle connessioni

Vi sono diversi motivi per cui risulta necessario dover rifiutare una connessione, in INGV abbiamo preso in considerazione solo i seguenti motivi:

- la macchina richiesta non espone il servizio richiesto;
- un particolare servizio non viene reso disponibile agli utenti in quanto tende ad appesantire considerevolmente il traffico sulla rete, rallentandone le prestazioni.
- un particolare IP sta tentando una scansione della rete pubblica e viene *blacklistato*.

Nei primi due casi il nuovo firewall è istruito per rispondere con un pacchetto tipo ICMP contraffatto che indica la macchina richiesta è irraggiungibile, facendo così cadere immediatamente la connessione.

Anche nel terzo caso viene restituito un pacchetto ICMP[15] contraffatto indicando che la rete richiesta non è raggiungibile, sperando di ingannare l'attaccante e farlo desistere dal suo attacco.
I vecchi sistemi, invece, preferivano sfruttare la funzione di **DROP** del pacchetto malizioso non inoltrando la richiesta al destinatario ma mantenendo la connessione "appesa" e gravando sulle prestazioni della macchina.

4.7 Gestione Firewall

4.7.1 Versioning
Per mantenere correttamente il versioning del sistema di protezione si è deciso di sfruttare le potenzialità del CVS[16], appoggiandosi al server di sviluppo già attivo in Sede.
E' stato creato un nuovo progetto, chiamato *ingv_fw*, e un account per ogni utente che ha necessità di lavorare sul progetto. Da questo momento ognuno può lavorare indipendentemente sulla propria macchina e apportare tutte le modifiche necessarie senza intaccare la copia ufficiale sul server finché non è pronto a salvare tutti cambiamenti apportati.
Il sistema CVS obbliga l'utente in procinto di aggiornare il file sul server ad inserire un commento sulle operazioni svolte e il sistema automaticamente memorizza tutte le informazioni necessarie per rintracciare l'utente che ha apportato modifiche, quando ha aggiornato il file e cosa ha modificato, mostrando sia le modifiche al file che i commenti ad esse relativi; ovviamente si preoccupa di mantenere un corretto versioning di ogni file.
A seguito dell'aggiornamento il sistema, su richiesta, avverte via mail gli altri membri del progetto che il file è stato modificato, così ognuno dalla propria postazione può aggiornare il progetto salvato sulla propria macchina.
Da notare che, a seguito di ogni modifica, i 2 firewall (attivo e backup) non sono ancora aggiornati.

4.7.2 Riavvio
Il sistema realizzato si presenta corredato da uno script (*restart_fw*) che si occupa di:
- Salvare l'attuale configurazione del file delle regole (operazione di per se superflua ma che permette di ritornare velocemente ad una versione precedente del firewall in caso di problemi);
- Salvare le statistiche del traffico di rete avvenuto tra il precedente e l'attuale riavvio del firewall;
- Aggiornare la copia in locale sul server via CVS;
- Aggiornare la copia sul server di backup (senza richiedere alcuna password grazie allo scambio di chiavi SSH);
- Riavviare il sistema di firewalling (viene richiesta la password di root ma non si da all'utente alcuna shell in quanto l'operazione viene svolta automaticamente dallo script).

5. Annotazioni tecniche

5.1 Repository dei sorgenti
L'ultima versione della configurazione del server è reperibile sul server di sviluppo dell'Ente.
Segue la procedura per il download:

```
$ export CVS_RSH=ssh
$ export CVSROOT=:ext:guest@cvs.rm.ingv.it:/reps
$ cvs checkout ingv_fw
```

[15] *Internet Control Message Protocol* è un protocollo di servizio che si preoccupa di trasmettere informazioni riguardanti malfunzionamenti, informazioni di controllo o messaggi tra i vari componenti di una rete di calcolatori.
[16] Il *Concurrent Versioning System*, implementa un sistema di controllo versione: mantiene al corrente di tutto il lavoro e di tutti i cambiamenti in un insieme di file, tipicamente è l'implementazione di un software in via di sviluppo, in progetto, e permette a molti sviluppatori (potenzialmente distanti) di collaborare.

Coordinamento editoriale e impaginazione
Centro Editoriale Nazionale | INGV

Progetto grafico e redazionale
Laboratorio Grafica e Immagini | INGV Roma

Via di Vigna Murata, 605
00143 Roma
Tel. +39 06518601 Fax +39 065041181

http://www.ingv.it

Istituto Nazionale di Geofisica e Vulcanologia