

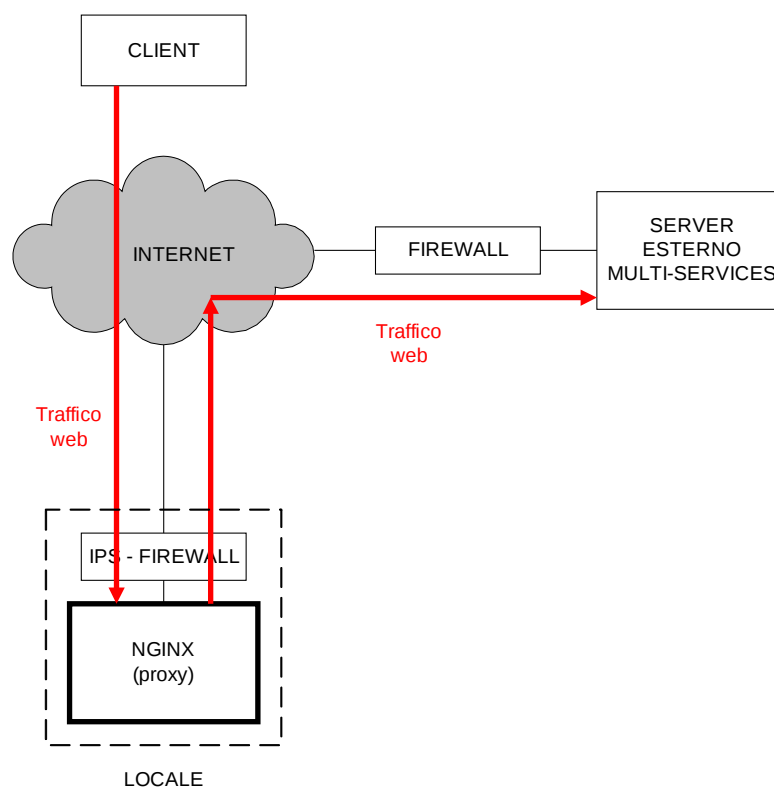
IL PIZZO DI INTERNET

Pierpaolo Palazzoli, Brescia, Italy
Fabio Mostarda, Brescia, Italy
Claudia Ghelfi, Brescia, Italy

Col termine “pizzo di internet” si fa riferimento ad un sistema che è in grado di proteggere “a distanza” i servizi internet. È la distanza la peculiarità che rende questo sistema innovativo, la possibilità di difendere anche i servizi non fisicamente inseriti nel contesto protetto.

Grazie all’implementazione di un proxy “Nginx”, protetto da un ips e un firewall, è possibile estendere il perimetro entro cui si garantisce la protezione.

Nello schema seguente è rappresentata la struttura logica del sistema:



La logica di implementazione del “pizzo di internet” percorre i seguenti passi:

1. si forza il DNS a convogliare verso il proxy Nginx tutto il traffico diretto verso il servizio internet posto sul server esterno;
2. il traffico intercettato viene filtrato da firewall e ips e ridirezionato, attraverso un indirizzo secondario, verso il server esterno;

3. il server esterno è preferibile sia configurato in modo tale da accettare solo le richieste provenienti dal proxy Nginx;

Il percorso intrapreso da una richiesta, quindi, viene spezzato in due tratte separate:

- o la prima si estende dal client all'Nginx
- o mentre la seconda è costituita dal link Nginx-Server esterno.

In questo modo solo il traffico autorizzato approda sul server esterno.

Allo stesso modo, le risposte del server esterno seguono l'analogo percorso, in direzione opposta, riattraversando Nginx.

NGINX

Si analizzano ora, in modo più approfondito, le potenzialità di Nginx .

Nginx (da pronunciarsi "engine x") è un server http, un reverse proxy nonché un proxy server IMAP/POP3. Può anche rivestire tutti questi ruoli contemporaneamente.

Nginx ha come punti di forza la stabilità, un ricco ventaglio di caratteristiche, una configurazione piuttosto semplice ed infine un basso consumo di risorse.

I principali ambiti applicativi di Nginx sono:

- o in sostituzione di Apache, con le seguenti caratteristiche:
 - abilità nel maneggiare numerosi connessioni contemporanee, file statici, index file e autoindexing,
 - rapido reverse proxying senza catching e semplice load-balancing,
 - supporto di server FastCGI remoti senza catching e semplice load-balancing,
 - architettura modulare. I filtri includono gzipping, byte ranges, chunked responses, XSLT, and SSI. Inclusioni SSI multiple in un'unica pagina possono essere processate in parallelo se sono gestite da server FastCGI o proxy.
 - supporta SSL e TLS SNI.

Nginx, come server http, offre inoltre:

- configurazione flessibile,
- riconfigurazione e upgrade online senza l'interruzione del servizio al cliente,
- controllo d'accesso basato sull'IP del client e autenticazione http base,
- possibilità di limitare la banda,
- possibilità di limitare il numero di connessioni simultanee o le richieste provenienti da un particolare indirizzo.
- o come server-proxy load-balancing,
- o come server proxy di posta, con le seguenti caratteristiche:
 - redirectione di IMAP/POP3 usando un server http esterno di autenticazione,
 - autenticazione usando un server http esterno di autenticazione e una connessione ridirezionata verso l'SMTP interno,
 - metodi di autenticazione:
 - POP3: USER/PASS, APOP, AUTH LOGIN PLAIN CRAM-MD5;
 - IMAP: LOGIN, AUTH LOGIN PLAIN CRAM-MD5;
 - SMTP: AUTH LOGIN PLAIN CRAM-MD5;
 - supporta SSL,
 - supporta STARTTLS e STLS.

O come un server con un semplice processo d'installazione, un file di configurazione pulito e pochi bugs.

Nginx è supportato dai seguenti sistemi operativi:

- FreeBSD 3.x, 4.x, 5.x, 6.x i386; FreeBSD 5.x, 6.x amd64;
- Linux 2.2, 2.4, 2.6 i386; Linux 2.6 amd64;
- Solaris 8 i386; Solaris 9 i386 and sun4u; Solaris 10 i386;
- MacOS X (10.4) PPC;

Può essere scaricato dal sito: <http://sysoev.ru/nginx/download.html> e richiede la presenza delle librerie pcre, openssl, zlib per la sua installazione.

APPLICAZIONE

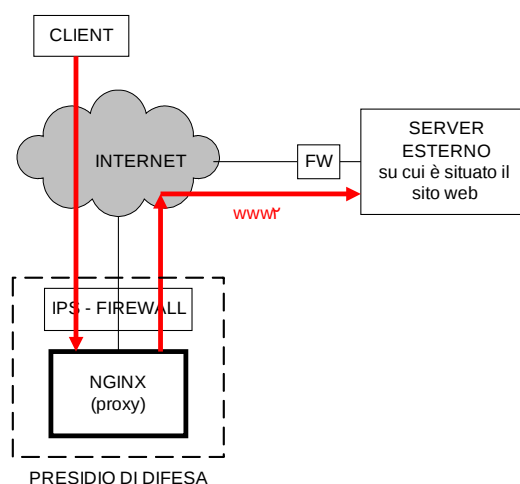
Nel caso specifico del “pizzo di internet“ Nginx è impiegato come reverse proxy. Forzare gli accessi ai servizi internet a passare attraverso Nginx, offre la possibilità di difendere questi servizi, senza la necessità di installare un sistema di protezione accanto al server che fornisce il servizio.

In base alla tipologia di servizio da salvaguardare nascono diverse applicazioni del “pizzo di internet“, a partire dalla tutela di una pubblicazione web, quale per esempio un sito internet, fino alla protezione di servizi di posta elettronica.

PROTEZIONE DI UNA PUBBLICAZIONE WEB

Si analizza in particolare il caso di un sito web. Nell'esempio si considera il sito fittizio www.ilpizzodinternet.it

Innanzitutto, per difendere una pubblicazione web a distanza, con un sistema di questo tipo, è necessario avere accesso ad alcune configurazioni, dettagliate nella sezione prerequisiti, così da dare vita alla struttura seguente:



Una volta che si è “preparato“ l'ambiente, è sufficiente configurare correttamente Nginx per ottenere il corretto instradamento del servizio e di conseguenza il suo passaggio entro il perimetro di protezione.

Il presidio costituito dal reverse proxy Nginx, dall'ips e dal firewall agisce come una sorta di portineria attraverso la quale è forzato a passare tutto il traffico entrante e uscente e che quindi ha la possibilità di controllarne l'autorizzazione.

A questa funzione base “del pizzo di internet“ poi possono esserne aggiunte altre, fornite dall'Nginx, come ad esempio il load-balancing.

Prerequisiti

Per implementare l'architettura in figura sono necessari i seguenti prerequisiti:

- o Il traffico diretto verso il sito web, deve essere ridirezionato verso il presidio di difesa, ovvero verso l'Nginx. Per realizzare ciò bisogna settare il file di configurazione dell'ambiente del particolare sito sul DNS aggiungendo il record:
www IN A “ip nginx“
- o A questo punto è indispensabile concludere la creazione del percorso che il traffico dovrà seguire, strutturando anche il tratto Nginx-Server esterno. Per questo link si usa un secondo record di comodo, quale per esempio www2.
Si configura quindi il DNS aggiungendo:
www2 IN A “ip server esterno“
- o Infine è consigliabile forzare il server esterno affinché accetti solo le richieste provenienti dall'Nginx, ad esempio configurando opportunamente il firewall.
Questa avvertenza accresce il grado di sicurezza dell'intero sistema.

Si osserva che l'indirizzo che appare al client è quello che lui stesso ha inserito, cioè non viene visualizzato l'ultimo indirizzo, quello di comodo.

In questo modo il client accede in maniera trasparente al servizio internet.

Configurazione di Nginx

Nginx deve essere configurato affinché canalizzi il traffico verso il server su cui è presente il sito. Il file di configurazione si trova in /etc/nginx/nginx.conf e deve essere simile al seguente. Il testo in grassetto è quello aggiunto per adempiere alle richieste del progetto, mentre il restante è generalmente già presente nel file di configurazione.

```
user www-data;  
worker_processes 1;  
  
error_log /var/log/nginx/error.log;  
pid /var/run/nginx.pid;  
  
events {  
    worker_connections 1024;  
}  
  
http {  
    include /etc/nginx/mime.types;  
    default_type application/octet-stream;
```

```
access_log /var/log/nginx/access.log;

server {
    listen 80;
    server_name www.ilpizzodinternet.it; #sito da proteggere
    location / {
        proxy_pass http://www2.ilpizzodinternet.it; #sito a cui reindirizzare il traffico
    }
}

sendfile on;
#tcp_nopush on;

#keepalive_timeout 0;
keepalive_timeout 65;
tcp_nodelay on;

gzip on;

include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
}
```

IMPLEMENTAZIONE ALTERNATIVA

Il “pizzo di internet“ può essere implementato anche con un sistema alternativo a Nginx, ovvero attraverso il mod_proxy di Apache.

Per attuare questo secondo metodo è sufficiente inserire nel file di configurazione di apache: httpd.conf il testo che segue:

```
<VirtualHost www.ilpizzodinternet.org>
    ServerAdmin admin@ilpizzodinternet.org
    ProxyPass / http://www2.ilpizzodinternet.org/
    ProxyPassReverse / http://www2.ilpizzodinternet.org/
    ServerAlias www.ilpizzodinternet.org www.ilpizzodinternet.net
    www.ilpizzodinternet.com
    ServerName www.ilpizzodinternet.org
    ErrorLog logs/www.ilpizzodinternet.org_error_log
    CustomLog logs/www.ilpizzodinternet.org_log combined
</VirtualHost>
```

