Progetto m146

Samuel, Aramis

February 9, 2018

Schema visio

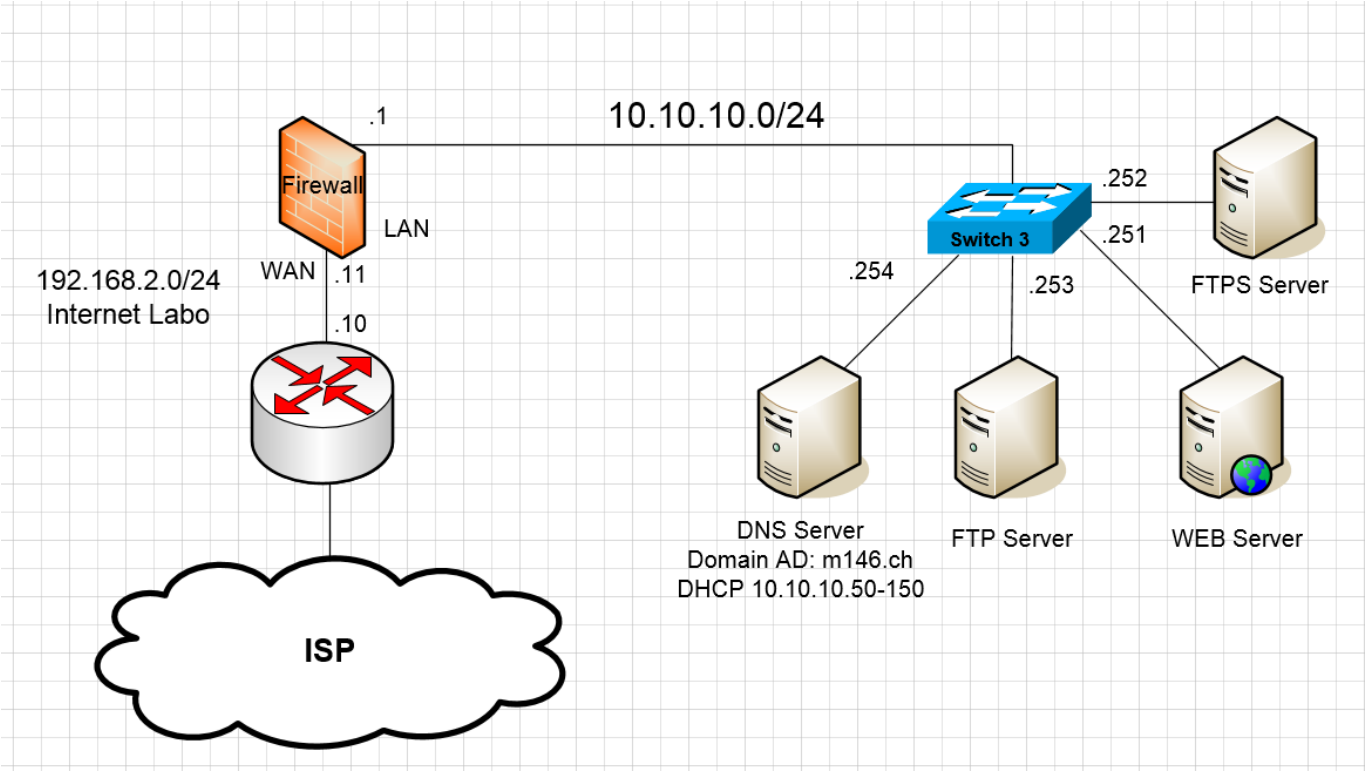

Figure 1: Network

Ambiente di sviluppo

Per poter lavorare da casa ho dovuto simulare la rete interna del firewall.

Per fare ciò ho creato una rete `NAT` in `virtualbox`.

Con il seguente comando da terminale si può creare una rete NAT con la rete `10.10.10.0/24`.

```
1 VBoxManage natnetwork add --netname m146 --network "10.10.10.0/24" --enable
```

Router

Il router è stato configurato cambiando le seguenti informazioni

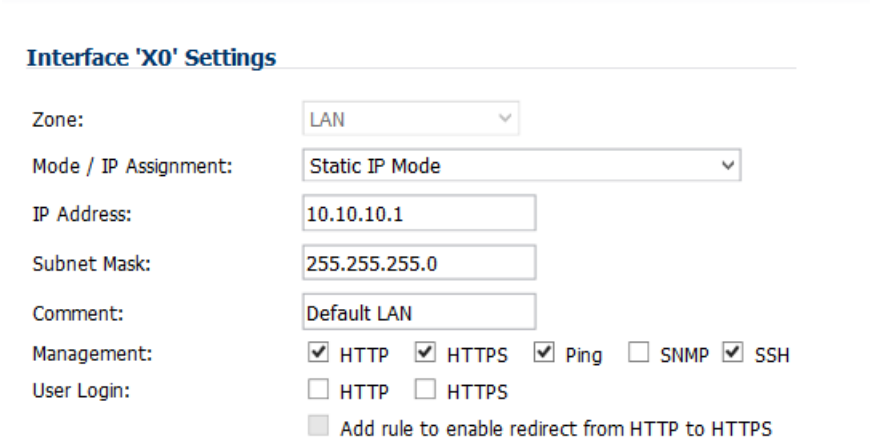

Figure 2: LAN

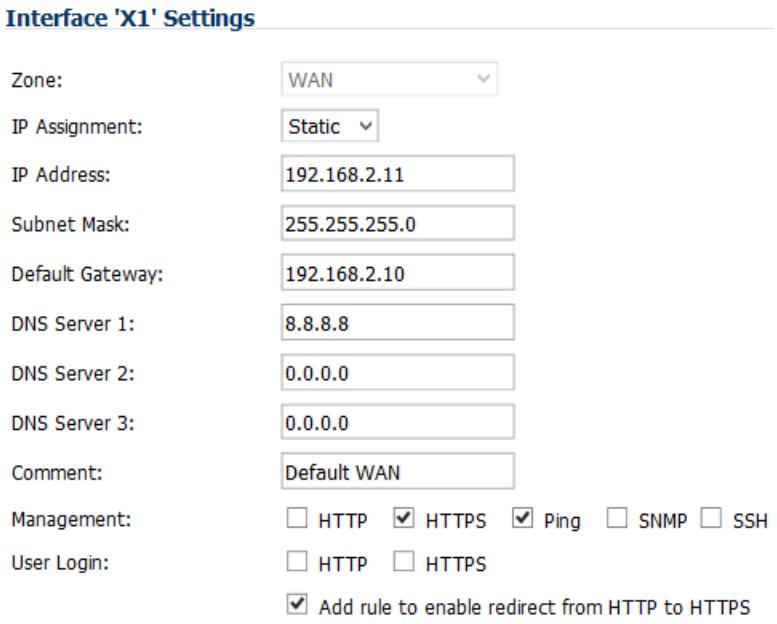

Figure 3: WAN

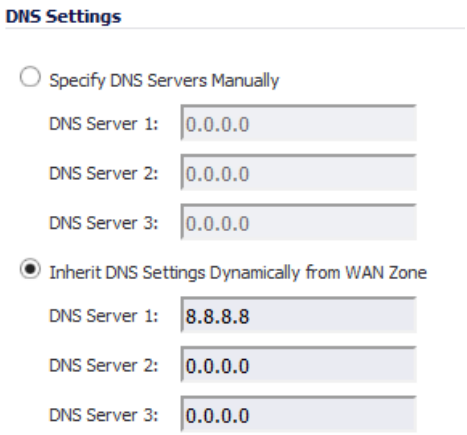

Figure 4: DNS

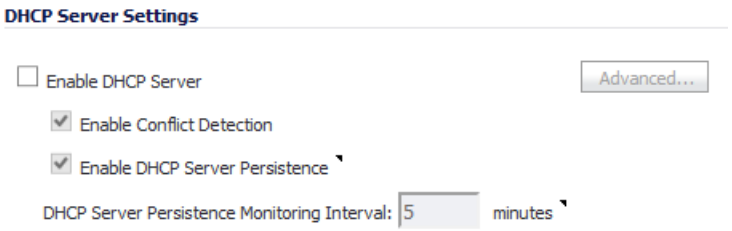

Figure 5: DHCP

Macchine virtuali

Tutte le operazioni sono state effettuate su delle macchine virtuali con installato la distro Linux `Alpine`.

DNS e DHCP

Info VM:
- IP 10.10.10.254
- GATEWAY 10.10.10.1
- DNS 10.10.10.254

Per configurare il server dns ho utilizzato `dhcpd`.

Per installare `dhcpd` si utilizza il seguente comando.

```
1 apk add acf-dhcp
```

Per configurarlo bisogna creare il file `dhcpd.conf` nella directory `/etc/dhcp/`.

In seguito il file di configurazione che ho fatto per il server dhcp.

```
1 # Configurazione standard
2 default-lease-time 302400;
```

```
max-lease-time 604800;
ddns-update-style none;
log-facility local7;
authoritative;

subnet 10.10.10.0 netmask 255.255.255.0
{
   range "10.10.10.50 10.2.0.200";
   option domain-name-servers 10.10.10.254;
   option routers 10.10.10.1;
   option domain-name "m146.ch";
}
```

Infine i seguenti comandi per far partire il servizio dhcp e per farlo partire a boot-time.

```
rc-service dhcpd start
rc-update add dhcpd
```

Per il server dns ho utilizzato `unbound`.

Per installarlo si utilizza il comando

```
apk add unbound
```

Per configuarlo si deve modificare il file `/etc/unbound/unbound.conf`.

```
server:
        verbosity: 1
## Specify the interface address to listen on:
        interface: 10.10.10.254
## To listen on all interfaces use:
#       interface: 0.0.0.0
        do-ip4: yes
        do-ip6: yes
        do-udp: yes
        do-tcp: yes
        do-daemonize: yes
        access-control: 0.0.0.0/0 allow
## Other access control examples
#access-control: 192.168.1.0/24 action
## 'action' should be replaced by any one of:
#deny (drop message)
#refuse (sends  a  DNS  rcode REFUSED error message back)
#allow (recursive ok)
#allow_snoop (recursive and nonrecursive ok).
## Minimum lifetime of cache entries in seconds.  Default is 0.
#cache-min-ttl: 60
## Maximum lifetime of cached entries. Default is 86400 seconds (1  day).
#cache-max-ttl: 172800
## enable to not answer id.server and hostname.bind queries.
```

```
        hide-identity: yes
## enable to not answer version.server and version.bind queries.
        hide-version: yes
## default is to use syslog, which will log to /var/log/messages.
use-syslog: yes
## to log elsewhere, set 'use-syslog' to 'no' and set the log file location below:
#logfile: /var/log/unbound
python:
remote-control:
        control-enable: no
## Note for forward zones, the destination servers must be able to handle
   recursion to other DNS server
## Forward all *.example.com queries to the server at 192.168.1.1
#forward-zone:
#        name: "example.com"
#        forward-addr: 192.168.1.1
## Forward all other queries to the Verizon DNS servers
forward-zone:
        name: "."
## Level3 Verizon
        forward-addr: 9.9.9.9
        forward-addr: 9.9.9.9
```

Dopodichè farlo partire e fare in modo che si avvii a boot-time tramite i seguenti comandi.

```
/etc/init.d/unbound start
rc-update add unbound
```

WebServer

Info VM:
- IP 10.10.10.251
- GATEWAY 10.10.10.1
- DNS 10.10.10.254

Il webserver installato si chiama `lighttpd`, che è molto sicuro, performante e semplice.

Per installarlo basterà eseguire il seguente comando.

```
apk add lighttpd
```

Rispettivamente, per avviarlo, fermarlo o riavviarlo si possono utilizzare i seguenti comandi

```
rc-service lighttpd start
rc-service lighttpd stop
rc-service lighttpd restart
```

Infine per impostarlo a runlevel, cioè che si avvii automaticamente all'accensione del server, si utilizza il seguente comando.

```
rc-update add lighttpd default
```

Se si vogliono configurare dei parametri si deve modificare il file di configurazione al seguente percorso.

```
/etc/lighttpd/lighttpd.conf
```

Mentre il percorso di default per l'htdocs si trova al seguente percorso.

```
/var/www/localhost/htdocs/
```

FTP

Info VM:
- IP 10.10.10.253
- GATEWAY 10.10.10.1
- DNS 10.10.10.254

Il servizio FTP è stato creato tramite `vsftpd` (Very Secure ftp Daemon), che è possibile installare su `Alpine` tramite il seguente comando

```
apk add vsftpd
```

Il servizio sarà immediatamente utilizzabile, con gli accessi anonimi abilitati di base. Se vogliamo possiamo creare una serie di utenti e home directories alle quali gli utenti possono accedere, ma per il momento non è stato configurato

La directory a cui il servizio FTP va a riferirsi come base è configurabile nel file `/etc/passwd:`, alla riga contenente

```
ftp:x:116:116:vsftpd daemon:<path directory>:/bin/false
```

Il servizio sarà gestibile tramite i seguenti comandi

```
rc-service vsftpd start
rc-service vsftpd stop
rc-service vsftpd restart
```

Come menzionato sopra, per far partire il servizio all'avvio della macchina, si utilizza il seguente comando

```
rc-update add vsftpd
```

FTPS

Info VM:
- IP 10.10.10.2
- GATEWAY 10.10.10.1
- DNS 10.10.10.254

Il procedimento per l'installazione di questo servizio è lo stesso di quello FTP. L'unica differenza è l'utilizzo dei certificati SSL/TLS per maggiore sicurezza.

La prima cosa da fare, dopo aver installato il servizio, è creare il certificato che andremo ad utilizzare, tramite il comando, che andrà a creare sia il certificato che la chiave in un unico file

```
openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout
   /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

Dopo averlo creato, dovremo andare a notificare vsftpd che deve utilizzare il certificato, cosa che possiamo fare modificando il file `/etc/vsftpd/vsftpd.conf`, al quale aggiungeremo/decommenteremo le seguenti righe

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem   # Certificato
rsa_private_key_file=/etc/ssl/private/vsftpd.pem # Chiave
ssl_enable=YES # Abilitiamo l'uso di SLL

ssl_tlsv1=YES # Abilitiamo l'uso di TLS
ssl_sslv2=NO # Disabilitiamo le alternative
ssl_sslv3=NO #
```

Infine dobbiamo riavviare il servizio tramite il comando citato nella sezione precedente.

Firewall

Test

Test Case	TC-001
Nome	Webserver
Descrizione	Testa il corretto funzionamento del webserver, se risponde alle richieste
Prerequisiti	
Procedura	In una `bash`, utilizzare il comando `wget 10.10.10.251`
Risultati attesi	Il file index.html viene salvato nella directory attuale

Test Case	TC-002
Nome	DHCP
Descrizione	Testa il corretto funzionamento server dhcp
Prerequisiti	
Procedura	Collegare una macchina virtuale alla rete virtuale NAT. In seguito utilizzare il comando `ifconfig` e
Risultati attesi	controllare che la interfaccia abbia unindirizzo IP compreso tra `10.10.10.50` e `10.10.10.200`

Test Case	TC-003
Nome	FTP
Descrizione	Testa il corretto funzionamento server FTP
Prerequisiti	
Procedura	Accedere tramite un client ftp al server
Risultati attesi	Accesso al server FTP ottenuto, e possibilità di scaricare e caricare file da esso

Test Case	TC-003
Nome	FTPS
Descrizione	Testa il corretto funzionamento server FTPS
Prerequisiti	
Procedura	Accedere tramite un client ftp al server
Risultati attesi	Accesso al server FTP ottenuto, con la dovuta richiesta di conferma del certificato, e possibilità di scaricare e caricare file da esso.

FTP

Dopo aver installato il server FTP, ci basterà cercre di collegarci con un client FTP (nel mio caso winSCP), e verificare che il collegamento vada a buon fine

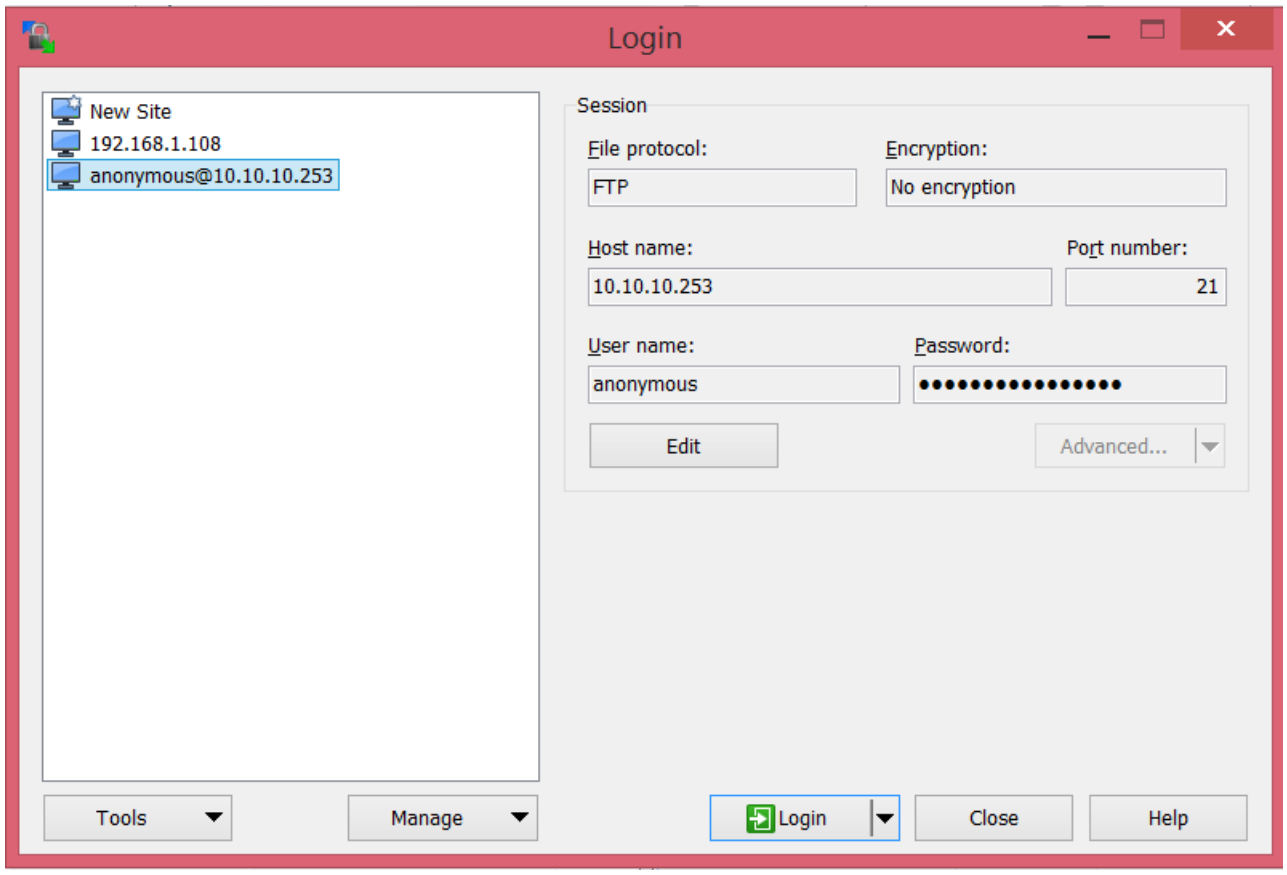

Figure 6: FTP

FTPS

Come per il servizio FTP, bisognerà collegarsi al server tramite client, utilizzando però SSL/TLS

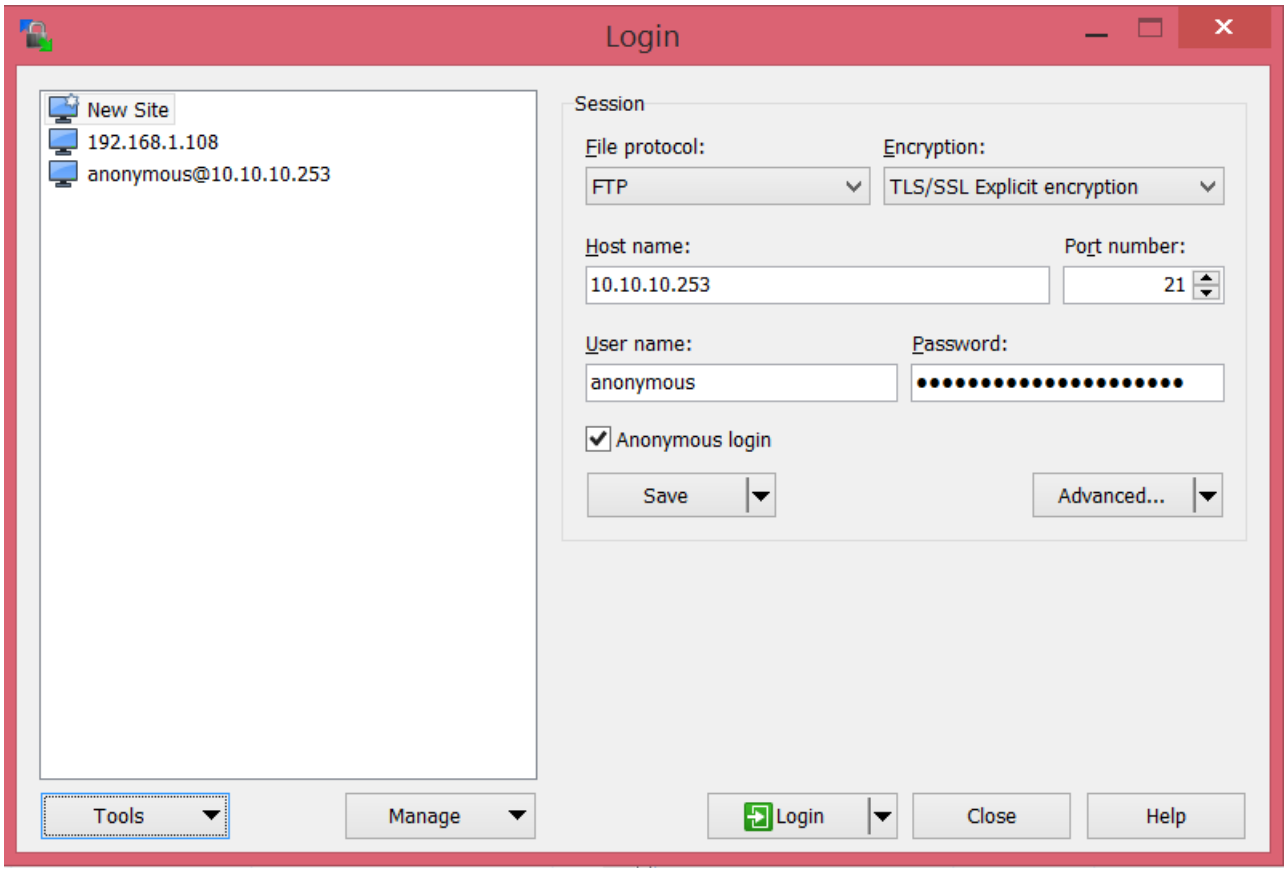

Figure 7: FTPS

Se il collegamento va a buon fine dovrebbe mostrere i certificati SSL/TLS trovati nel server, e chiedere di accettarli. Non essendo riuscito ad effettuare la connessione non posso verificare questo punto.

WEB

DNS

DHCP