

Progetto m146

Samuel, Aramis

March 9, 2018

Schema visio

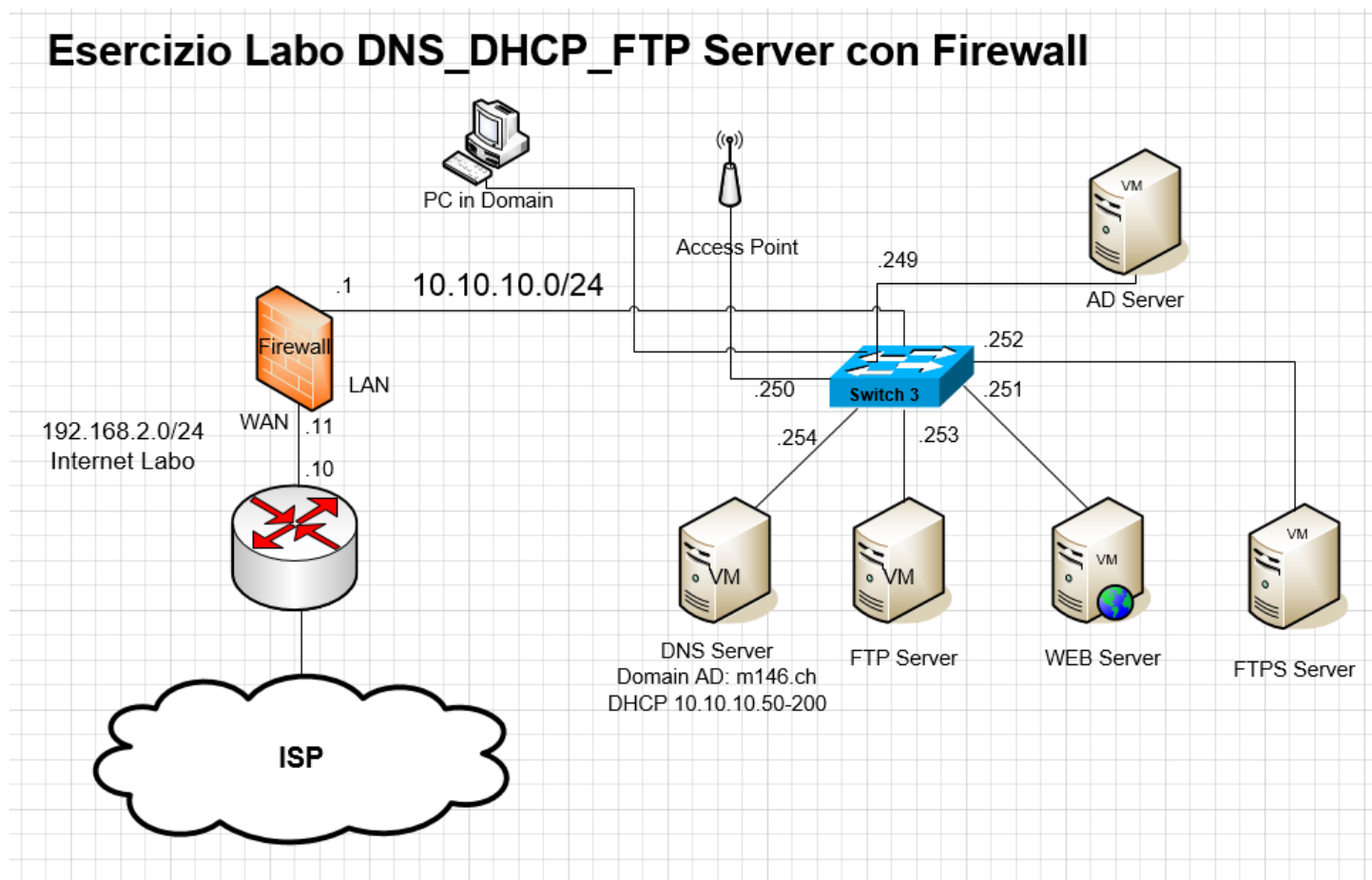


Figure 1: Network

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

Interface 'X0' Settings

Zone:	LAN
Mode / IP Assignment:	Static IP Mode
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0
Comment:	Default LAN
Management:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS

Figure 2: LAN

Interface 'X1' Settings

Zone:	WAN
IP Assignment:	Static
IP Address:	192.168.2.11
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.2.10
DNS Server 1:	8.8.8.8
DNS Server 2:	0.0.0.0
DNS Server 3:	0.0.0.0
Comment:	Default WAN
Management:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input checked="" type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS

Figure 3: WAN

DNS Settings

☐ Specify DNS Servers Manually

DNS Server 1:

DNS Server 2:

DNS Server 3:

☒ Inherit DNS Settings Dynamically from WAN Zone

DNS Server 1:

DNS Server 2:

DNS Server 3:

Figure 4: DNS

DHCP Server Settings

☐ Enable DHCP Server Advanced...

☒ Enable Conflict Detection

☒ Enable DHCP Server Persistence

DHCP Server Persistence Monitoring Interval: minutes

Figure 5: DHCP

Access Point

L'access point è stato configurato cambiando le seguenti informazioni

Nome utente: **admin** Password: **admin**

Local IP Address: . . .

Subnet Mask:

DHCP Server: ☐ Enable ☒ Disable


Figure 6: Rete Interna wireless

Wireless Network Mode: Mixed

Wireless Network Name (SSID): Gruppo1

Wireless Channel: 13 - 2.472GHz

Wireless SSID Broadcast: ☒ **Enable** ☐ **Disable**



Status : SES Inactive

Reset Security

Figure 7: Sezione wireless

Security Mode: WPA2 Personal

WPA Algorithms: TKIP+AES

WPA Shared Key: Password&1

Group Key Renewal: 3600 seconds

Figure 8: Sezione sicurezza wireless

Macchine virtuali

Tutte le operazioni sono state effettuate su delle macchine virtuali con installato la distro Linux **Alpine**, eccetto per il server contenente l'active directory, il quale è installato con Windows.

Active Directory

Info VM:

- IP 10.10.10.249
- GATEWAY 10.10.10.1
- DNS 10.10.10.254

Su questo server Windows sono state aggiunte le funzionalità di Active Directory, per gestire gli utenti, e DNS, per poter reindirizzare i client sul server DNS esterno. Questo è possibile semplicemente dando al server Windows il nostro server Linux come DNS, così che quando un client fa una richiesta a Windows, se non dovesse riuscire a tradurre l'indirizzo lo manda al DNS Linux.

Bisogna però ricordarsi di cambiare l'opzione `dynamic updates` su `Nonsecure and secure`, per permettere la comunicazione con Linux.

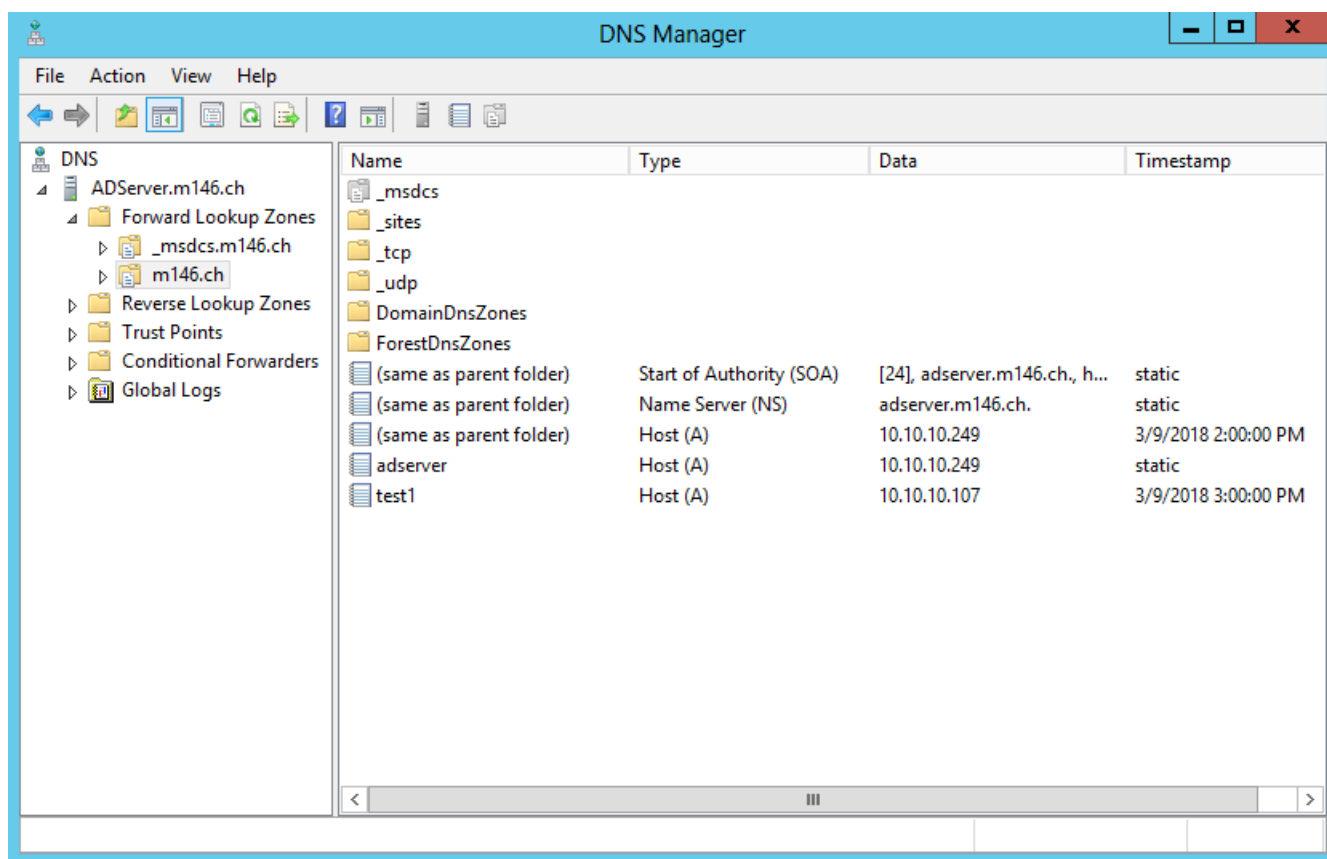


Figure 9: DNS

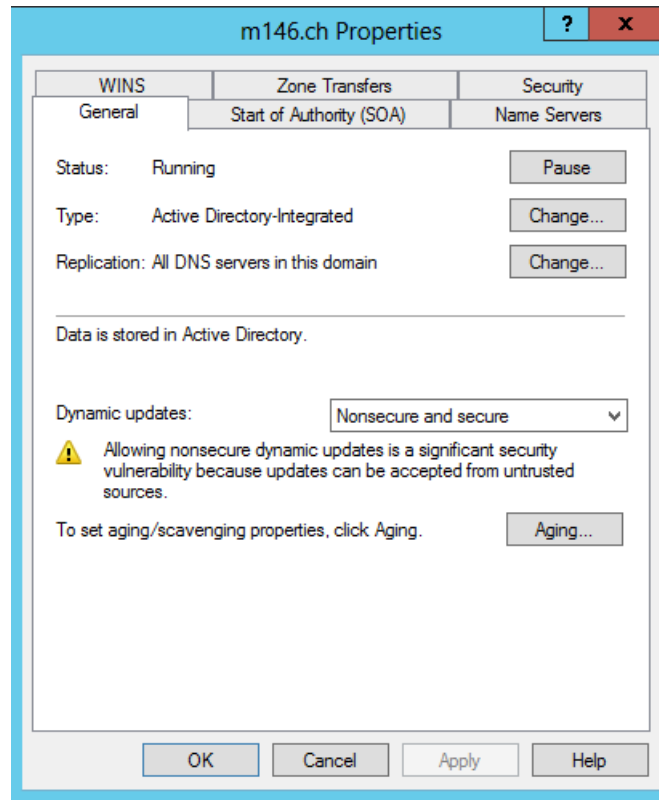


Figure 10: DNS

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 `dhcpcd`.

Per installare `dhcpcd` si utilizza il seguente comando.

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

Per configurarlo bisogna creare il file `dhcpcd.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;
3 max-lease-time 604800;
4 ddns-update-style none;
5 log-facility local7;
6 authoritative;
7
8 subnet 10.10.10.0 netmask 255.255.255.0
9 {
10     range "10.10.10.50 10.2.0.200";
11     option domain-name-servers 10.10.10.254;
12     option routers 10.10.10.249;
```

```
13 option domain-name "m146.ch";
14 }
```

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

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

Per il server dns ho utilizzato unbound.

Per installarlo si utilizza il comando

```
1 apk add unbound
```

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

```
1 server:
2     verbosity: 1
3 # Interfaccia su cui ascolta
4     interface: 10.10.10.254
5     do-ip4: yes
6     do-ip6: yes
7     do-udp: yes
8     do-tcp: yes
9     do-daemonize: yes
10 # Accetta richieste da chiunque
11     access-control: 0.0.0.0/0 allow
12     local-data: "web-intranet 10800 IN A 10.10.10.251"
13     local-data: "web-extranet 10800 IN A 10.10.10.12"
14     local-data: "ftp_intranet 10800 IN A 10.10.10.253"
15     local-data: "ftp_intranet 10800 IN A 10.10.10.252"
16     local-data: "ftp_extranet 10800 IN A 10.10.10.11"
17     local-data: "m146.ch 10800 IN A 10.10.10.249"
18     hide-identity: yes
19     hide-version: yes
20 use-syslog: yes
21 python:
22 remote-control:
23     control-enable: no
24 forward-zone:
25     name: "."
26 # Forwarding verso 9.9.9.9 e 8.8.8.8
27     forward-addr: 9.9.9.9
28     forward-addr: 8.8.8.8
```

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

```
1 /etc/init.d/unbound start
2 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.

```
1 apk add lighttpd
```

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

```
1 rc-service lighttpd start
2 rc-service lighttpd stop
3 rc-service lighttpd restart
```

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

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

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

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

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

```
1 /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

```
1 apk add vsftpd
```

Il servizio sarà immediatamente utilizzabile, con gli accessi anonimi abilitati di base. Se non lo fossero, si deve modificare la seguente riga nel file `/etc/vsftpd/vsftpd.conf`.

```
1 anonymous_enable=YES
```

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

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

Il servizio sarà gestibile tramite i seguenti comandi


```
1 rc-service vsftpd start
2 rc-service vsftpd stop
3 rc-service vsftpd restart
```

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

```
1 rc-update add vsftpd
```

FTPS

Info VM:

- IP 10.10.10.252 - 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 creerà sia il certificato che la chiave in un unico file

```
1 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

```
1 ssl_enable=YES      # Turn ON SSL
2 anonymous_enable=YES
3 allow_anon_ssl=YES
4 force_local_data_ssl=YES  # Use encryption for data
5 force_local_logins_ssl=YES # Use encryption for authentication
6
7 rsa_cert_file=/etc/ssl/private/vsftpd.pem  # Certificato
8 rsa_private_key_file=/etc/ssl/private/vsftpd.pem # Chiave
9
10 ssl_tlsv1=YES # Abilitiamo l'uso di TLS
11 ssl_sslv2=NO # Disabilitiamo le alternative
12 ssl_sslv3=NO #
```

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

Firewall

Test

Test Case	TC-001
Nome	Webserver

Test Case	TC-001
Descrizione	Testa il corretto funzionamento del webserver, se risponde alle richieste
Prerequisiti	
Procedura	In una <code>bash</code> , utilizzare il comando <code>wget 10.10.10.251</code>
Risultati attesi	Il file <code>index.html</code> viene salvato nella directory attuale
<hr/>	
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 <code>ifconfig</code> e
Risultati attesi	controllare che la interfaccia abbia un indirizzo 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.

Active Directory

FTP

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

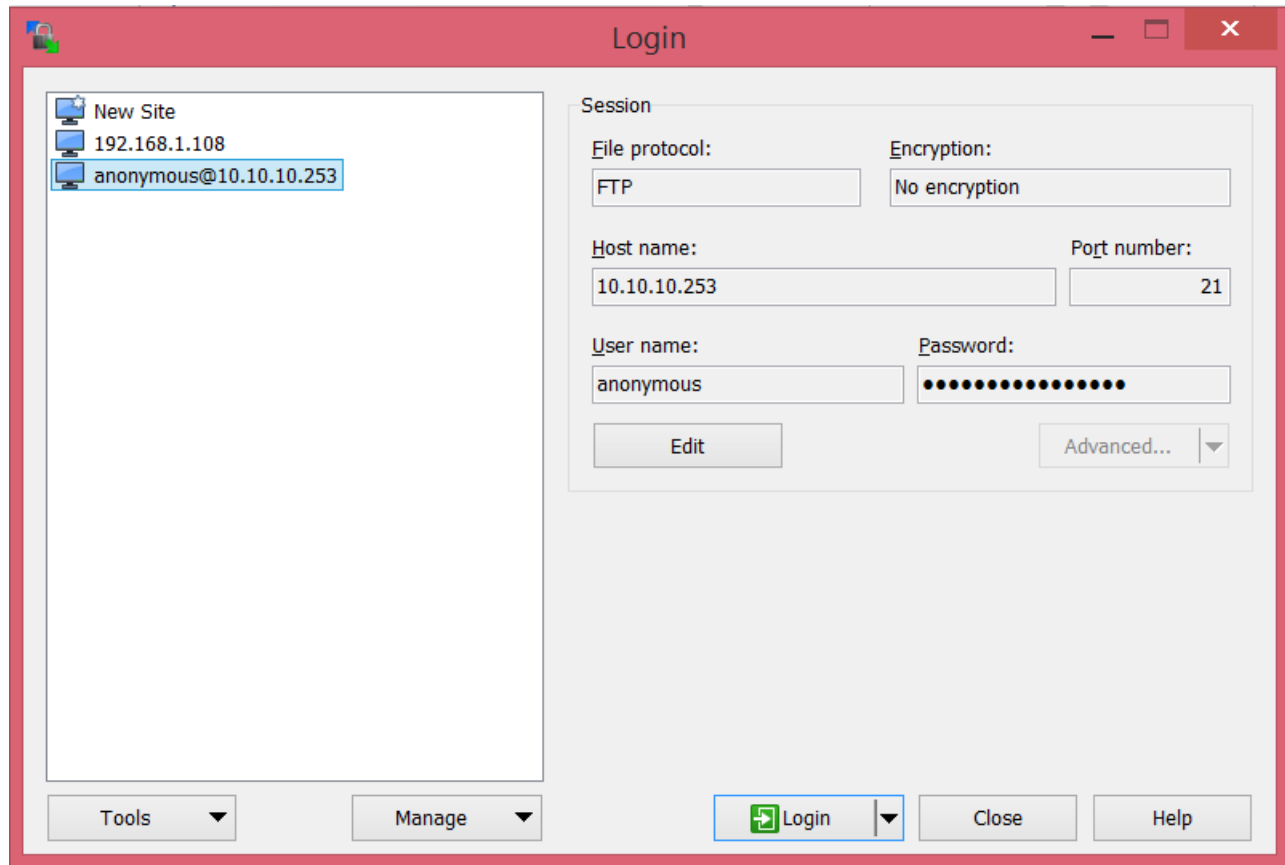


Figure 11: FTP

FTPS

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

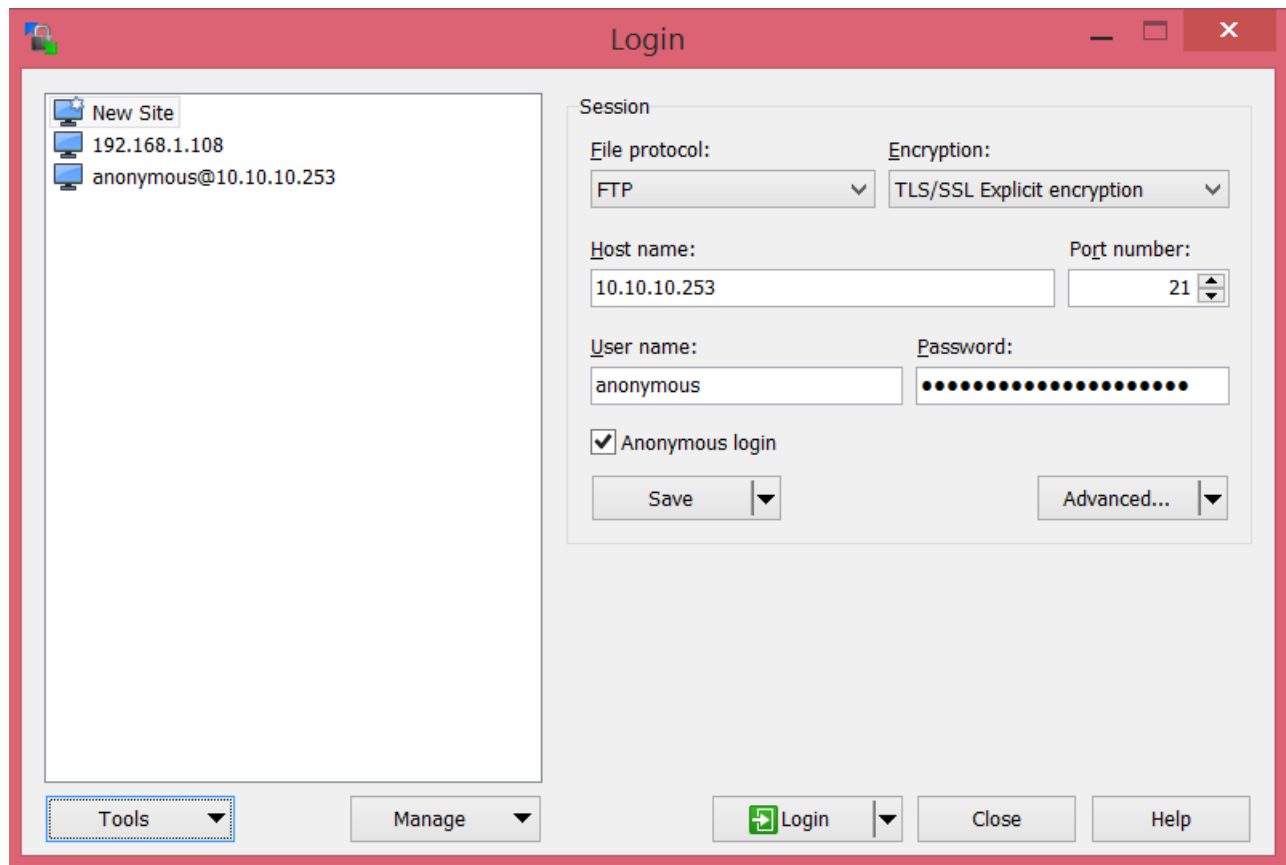


Figure 12: FTPS

Se il collegamento va a buon fine dovrebbe mostrare i certificati SSL/TLS trovati nel server, e chiedere di accettarli.

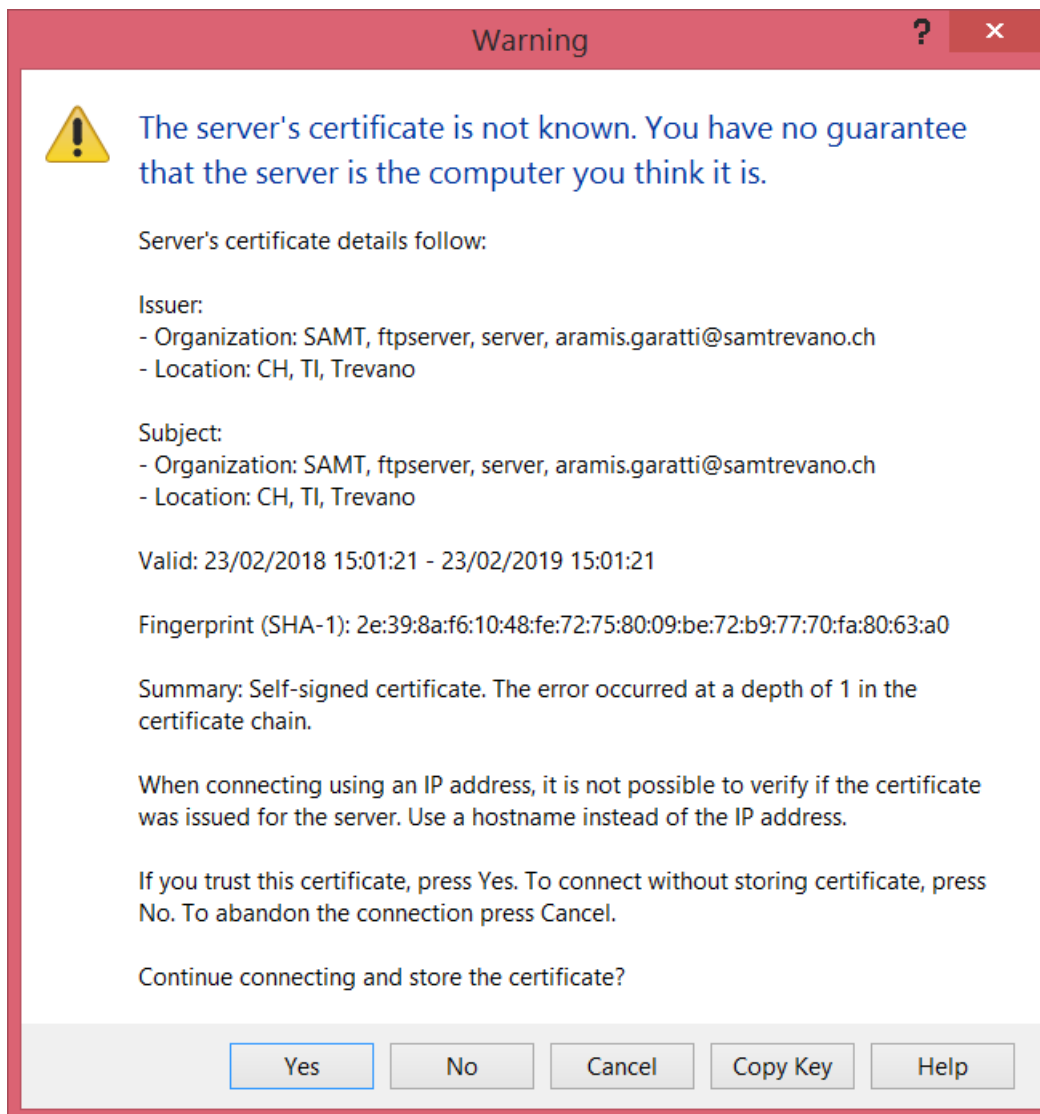


Figure 13: FTPS

WEB

<<<<<<< Updated upstream Comando

```
1 wget web-intranet
```

Risultato

```
1 Connecting to web-intranet (10.10.10.251:80)
2 index.html          100% |***|    36   0:00:00 ETA
```

DNS

Comando

```
1 dig @10.10.10.254 web-intranet
```

Risultato

```
1 ; <<>> DiG 9.9.7-P3 <<>> @10.10.10.254 web-intranet
2 ; (1 server found)
3 ;; global options: +cmd
4 ;; Got answer:
5 ;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 5865
6 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
7
8 ;; OPT PSEUDOSECTION:
9 ; EDNS: version: 0, flags;; udp: 4096
10 ;; QUESTION SECTION:
11 ;web-intranet.                IN      A
12
13 ;; ANSWER SECTION:
14 web-intranet.                10800   IN      A      10.10.10.251
15
16 ;; Query time: 63 msec
17 ;; SERVER: 10.10.10.254#53(10.10.10.254)
18 ;; WHEN: Fri Mar 09 16:03:44 CET 2018
19 ;; MSG SIZE rcvd: 57
```

DHCP

Risultato

```
en7: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500          options
      ether 00:24:9b:23:e9:4a                inet6 fe80::146a:b5c6:f53c:d5e%en7 prefixlen
64 secured scopeid 0x10                      inet 10.10.10.102 netmask 0xffffffff broadcast 10.10.10.255
      nd6 options=201<PERFORMNUD,DAD>        media: autoselect (100baseTX <full-duplex>)
active
```