
# MESSA IN SICUREZZA DI UNA RETE AZIENDALE

## Astaro - Sophos Network Security

Documentazione LPI

Documentazione LPI - Alessandro Campana - i4B SPAI Locarno 2010-2014

**INFORMAZIONI DEL DOCUMENTO**

Versione

Stampata il

Tempo a disposizione: 10 giorni (80 ore)

**INFORMAZIONI DI CONTATTO**

Clinica Luganese SA

Via Moncucco 10

6900 Lugano

Svizzera

Alessandro Campana

alessandro.campana@clinicaluganese.ch

_____

Alessandro Campana

LPI - Clinica Luganese SA

# Sommario

# 1. INTRODUZIONE

## 1.1 Situazione attuale

La azienda per cui lavoro, la Clinica Luganese SA, mi ha incaricato di creare una infrastruttura informatica comprendente un server fisico, un Firewall, uno Switch ed un terminale.
Più precisamente dovrò:

- Creare una azienda in VMware
- Garantire la sicurezza contro dei possibili attacchi esterni
- Avere una gestione della rete e degli accessi web
- Creare regole di navigazione per i vari utenti
- Instaurare una VPN con un ipotetico fornitore
- Mettere a disposizione per alcuni utenti un portale che permette la connessione verso l'interno

## 1.2 Strumenti e metodi

Gli strumenti fisici di cui sono in possesso sono:

- Un Firewall Astaro Gateway 220 versione 8.2
- Uno Switch Cisco da 4 porte
- Un server HP con 2 HD in RAID 0 da 128GB
- Un terminale con Windows 8 Pro

## 1.3 Astaro - Sophos Network Security

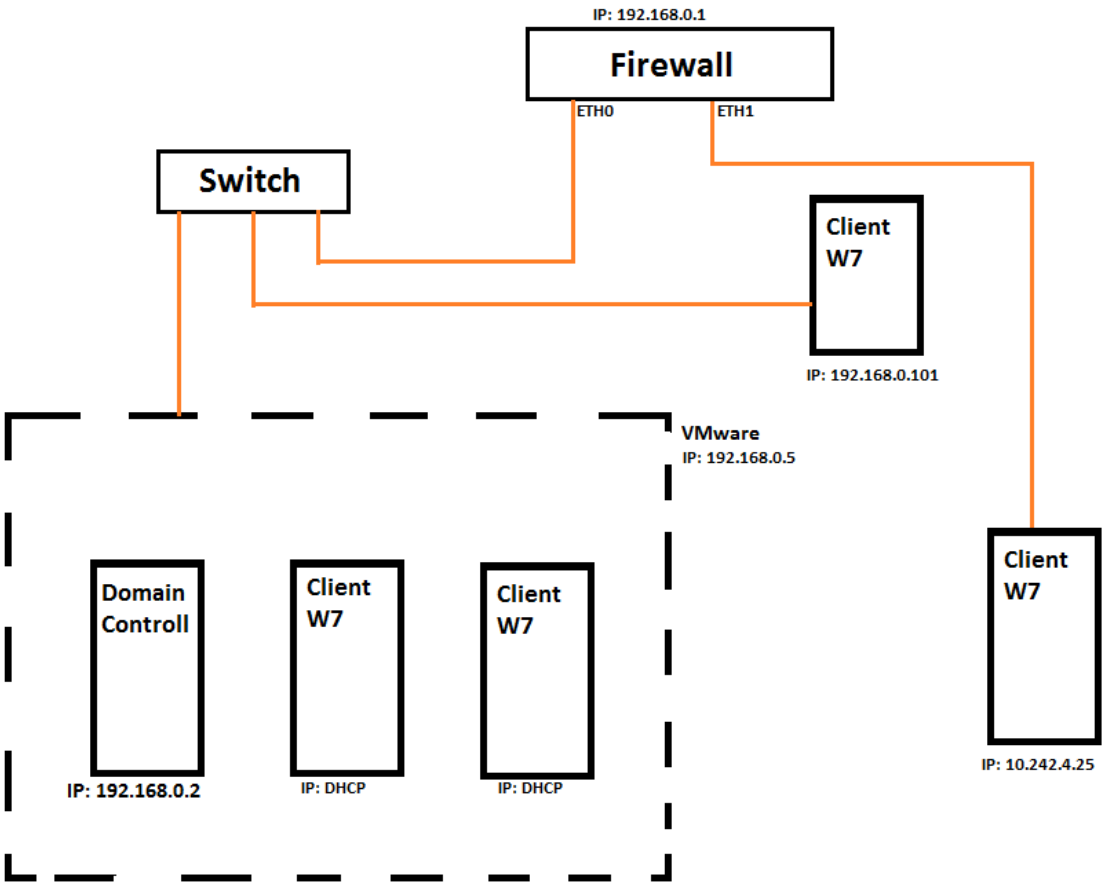
Astaro Gateway 220 è un potente sistema di difesa perimetrale. Contiene servizi per la gestione, la sicurezza, l'affidabilità ed il monitoring delle risorse di rete.

## 1.4 ESXI 5.1.0

VMware ESXI è un prodotto per la virtualizzazione molto utile in ambito sistemistico sia per l'efficienza che per la gestione. Con ESXI possiamo avere più server virtuali su di uno fisico, cosi da risparmiare spazio, consumi, ed avere una gestione più centralizzata dell'infrastruttura di rete.

## 1.5 Schema di rete

Di seguito è riportato lo schema di rete



## 1.6 Breve teoria sui vari argomenti trattati

**VPN:**
Una VPN (Virtual Private Network) è l'esenzione di una rete LAN utilizzando reti pubbliche
-Principali protocolli di Tunneling utilizzati:

- PPTP (Point to Point Tunneling Protocol): Autentificazione supportata CHAP / EAP
  - CHAP: La password è conosciuta sia dal client che dal server
  - EAP: Al posto della password, viene utilizzata una Smart Card
- L2TP: Versione migliorata di PPTP. Usata con IP Sec.

**IP sec:**
IP sec è un insieme di protocolli di autentificazione e cifratura.

- IKE: Protocollo per lo scambio delle chiavi per realizzare il flusso crittografato
- AH: Protocollo che fornisce la cifratura del flusso dei dati
- ESP: fornisce le strutture per l'autentificazione e la verifica della sicurezza del dato

IP Sec ha 2 modalità di funzionamento:

- Tunnel Mode: Connessione gateway-to-gateway, viene cifrato tutto il pacchetto IP e incapsulato in un nuovo. (solo il gateway deve avere il SW IP Sec)
- Transport Mode: Host-to-Host, viene cifrato solo il payload.

**SSL e TLS:**
Sono dei protocolli crittografici che permettono la comunicazione sicura.

**Routing**
il Routing è l'instradamento di un dato ricevuto, su di una porta o un interfaccia.

# 2. INSTALLAZIONE E CONFIGURAZIONE

## 2.1.1 Installazione ESXI 5.1.0

Dato il server privo di sistema operativo, procederemo con l'installazione di ESXI 5.1.0:

- Scarichiamo la ISO di ESXI 5.1.0. e la mettiamo su una pennetta USB
- Accendiamo il server e cliccando "F10" entriamo nel bios
- Andiamo nella categoria "Boot Order" e spostiamo "USB Device", come primario
- Riavviamo il server con l'USB inserita e scegliamo "Installazione ESXI GUI" (con interfaccia grafica)
- Attendiamo il caricamento dei file necessari e accettiamo i termini di condizione con "F11"
- Si aprirà una maschera dove ci verrà richiesto dove installare ESXI ( Nel mio caso userò una pennetta USB come disco di installazione del O.S.)
- Ci verrà richiesto se "Installare" o "aggiornare" ESXI. Noi scegliamo "Installare"
- Scegliamo il layout della tastiera "Swiss French"
- Scegliamo la Password per l'account "Root"
- Spostandoci in "Configure management network" e poi su "IP Configuration", gli daremo un IP fisso
- Ci chiederà un riavvio.
- Ora possiamo scaricare Vsphere per gestire il server da remoto.

## 2.1.2 Configurazione di ESXI

Finita l'installazione passiamo alla configurazione. Con l'ausilio di un computer, scarichiamo Vsphere Client, che ci servirà per amministrare il nostro server.
Aprendo Vsphere verrà richiesto l'IP del server (l'IP è quello che gli abbiamo assegnato in precedenza), l'username (Root) e la password (provola2).
Effettuiamo quindi la connessione al server ESXI.

## 2.2.1 Installazione di Windows server 2008 r2

Una volta connessi con Vsphere, clicchiamo con il tasto destro sul IP del server, e scegliamo "New Virtual Machine" .

- Scegliamo l'opzione "Custom"
- Scegliamo il nome della Virtual
- Scegliamo lo storage dove andremo a crearle
- Scegliamo il sistema operativo che andremo a installare e la relativa versione
- Scegliamo quanta CPU, memoria RAM e capacita del disco darli
- Finita questa procedura, avvieremo la Virtual e con "F2" entreremo nel BIOS, dove imposteremo come first boot il lettore CD.
- Precediamo quindi con la classica installazione di Windows server 2008 r2

### 2.2.2 Configurazione Windows server 2008 r2

Finita l'installazione del sistema operativo, precediamo con la configurazione del dominio.
Andiamo su "Aggiungi ruolo" e scegliamo l'opzione "Active Directory Domain Service".
Appena finisce di installarsi eseguiamo "CDpromo.exe" che ci permetterà di creare un nuovo dominio.
Procediamo con la creazione di 4 gruppi e 4 utenti dall'Active Directory.
Assegniamo quindi ogni un utente a un gruppo

## 2.3 Installazione di Windows 7 Professional

Clicchiamo con il tasto destro sul IP del server, e scegliamo "New Virtual Machine".

- Scegliamo l'opzione "Custom"
- Scegliamo il nome della Virtual
- Scegliamo lo storage dove andremo a crearle
- Scegliamo il Sistema operativo che andremo a installare e la relativa versione
- Scegliamo quanta CPU, memoria RAM e capacita del disco darli
- Finita questa procedura, avvieremo la virtual e con "F2" entreremo nel BIOS, dove imposteremo come first boot il lettore CD.
- Precediamo quindi con la classica installazione di Windows 7 Pro

## 2.4 Installazione di Astaro Security Gateway 220

Dato che il firewall Astaro ha già delle configurazioni, lo resettiamo. Per far ciò andiamo davanti al firewall e clicchiamo il tasto "Enter" e successivamente la "freccia in giù".
Sullo schermino LCD vedremo:
"Factory Reset?" nuovamente premeremo la "freccia in giù" e successivamente "Enter"
Attendiamo ora il suo riavvio.

## 2.5 Configurazione di base di Astaro Security Gateway 220

Utilizzando un pc con la scheda di rete impostata sulla "0" (192.168.0.X), potremo accedere alla WebAdmin page tramite browser digitando "http://192.168.0.1:4444".
Una volta collegati alla pagina ci verrà richiesta la configurazione di base:

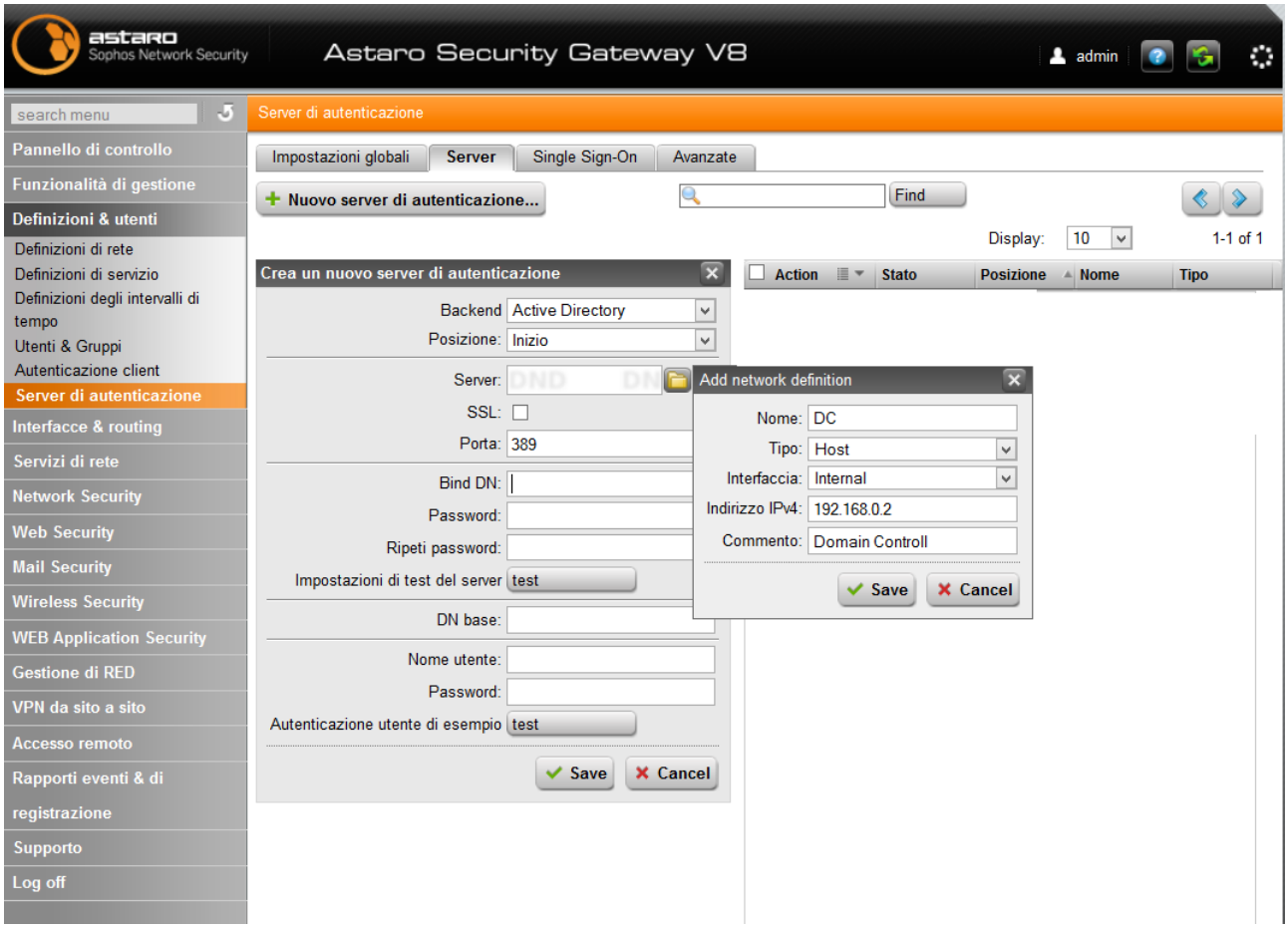
- Hostname
- Country
- Time
- Root Password

Una volta impostate le impostazioni di base, ci verrà richiesto se abbiamo un backup delle configurazioni per poter effettuare un restore. Nel nostro caso non le abbiamo, quindi procederemo cliccando su "Continue With This Wizard".

- Ci viene richiesta la licenza. Se non la possediamo avremo comunque 30 giorni di prova.
- Ci viene chiesto se abilitare il servizio DHCP sul Firewall, nel mio caso ho scelto di si.
- Ora ci viene chiesto l'interfaccia ETH0 che Uplink avrà (Ethernet standard)
- Firewall setting -> qui possiamo scegliere il traffico permesso (WEB, Terminal Services)
- Intrusion Prevention ->qui si può prevenire vari attacchi di rete su piattaforma Windows, Linux e OSx.
- Web Security -> qui scegliamo di controllare tutto il traffico di rete (anche HTTPS) e possiamo già bloccare diverse categorie di siti (Drugs, Pornografia, Social, ecc..)
- Finita la configurazione Wizard ci verrà mostrata una pagina comprendente tutte le configurazioni da noi scelte. Confermiamo con "Finish"

## 2.6 Configurazione Utenti AD in Astaro

Per poter gestire le regole di Webfiltering sui vari utenti o gruppi, bisognerà autentificare il firewall al DC. Per far ciò andiamo nel menu "Definizioni & utente" e successivamente "Server di autentificazione"




Qui inseriamo i parametri per la connessione con il Domain Control.
Bind DN: CN=Administrator, CN=Users, DC=bellnet, DC=local

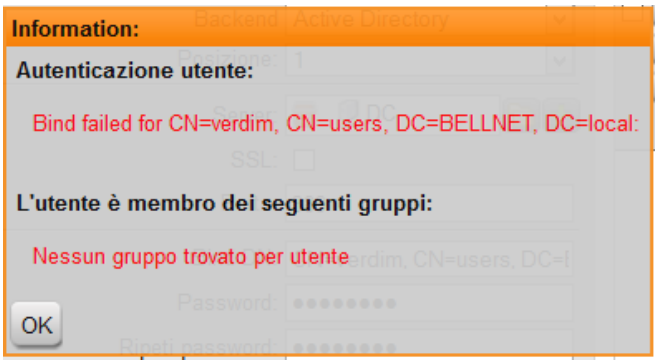
- CN= Qui inseriremo l'utente Administrator o un utente con tali permessi.
- CN= In questo secondo CN, dichiariamo la directory dove risiede l'utente nella AD
- DC= Qui inseriremo il nostro dominio
- DC= in questo secondo DC, inseriremo "local" dato che il dominio è locale.
- Attenzione! L'utente inserito in "CN=" deve avere i permessi di amministratore e, una volta scritta questa stringa, non si potrà spostare della directory "Users" della AD. A meno che aggiorniamo la stringa Bind DN con il nuovo percorso nel 2° CN.

DN base: DC=bellnet, DC=local

- DC= qui inseriamo il nostro dominio
- DC= in questo secondo DC, inseriremo "local dato che il dominio è locale.

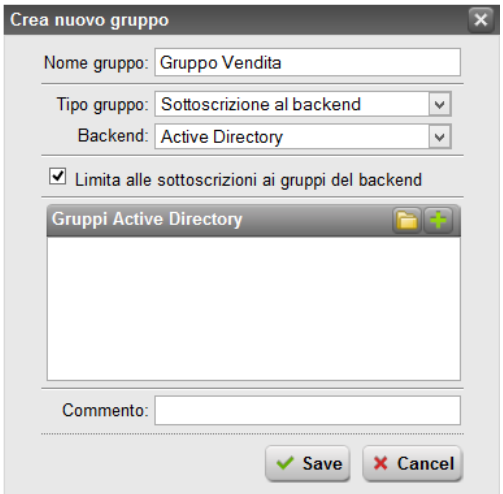
Una volta finito la configurazione dei campi, clicchiamo sul pulsante “Test” per testare se i parametri introdotti sono corretti.


Se ritorna questa messaggio, i parametri sono corretti, e l’utente è autorizzato a listare gli utenti e i gruppi della Active Directory.




In caso ritornasse questo messaggio, l’utente sekezionato nel “CN” non è autorizzato a listare i gruppi e gli utenti della Active Directory.

Ora il nostro Firewall si è autentificato alla AD. Possiamo quindi importare i gruppi dall’AD al Firewall, cosi da creare regole statiche che andranno applicate agli utenti appartenenti al gruppo. Per far ciò andiamo in “Definizioni & Utenti” e successivamente “Utenti e Gruppi”. Clicchiamo su “Gruppi” e quindi “Nuovo Gruppo”




Nome Gruppo: Inseriamo il nome del gruppo

Tipo di gruppo: Qui scegliamo se il gruppo sarà composto da membri statici oppure se verrà preso da un server di AD, EDirectory, Radius, LDAP,ecc.

Cliccando sull’icona delle cartelle, si aprirà una maschera con tutte le cartelle della AD. Sarà possibile selezionare il gruppo da noi desiderato e cliccare su salva per importare la configurazione del gruppo sul FW.

## 2.7 Configurazione autentificazione utenti

Ogni client che passa dal FW deve autentificarsi. Per evitare questo possiamo abilitare il "Single-Sign-On". Con il Single-Sign-On tutti gli utenti del dominio si autentificheranno automaticamente, senza dover conoscere nessuna password.

Per far ciò andiamo in "Definizioni & Utenti"-> "Server di Autentificazione"-> "Single-Sign-On"


Inseriremo il nome del dominio, l'utente Administrator e la password.
(Si può utilizzare un utente diverso da Amministratore, a patto che sia autorizzato ad aggiungere nuovi computer sul dominio)
Finiamo la procedura cliccando su "Salva".
In caso di riuscita, torna la scritta verde SSO Di AD salvato con successo.

È possibile che il FW non riesca a risolvere il nome del dominio. In questo caso ci torna un errore di comunicazione con il server AD in rosso.
Per risolvere questo problema andiamo in: "Servizi di rete"-> "DNS"-> "Richieste di routing"





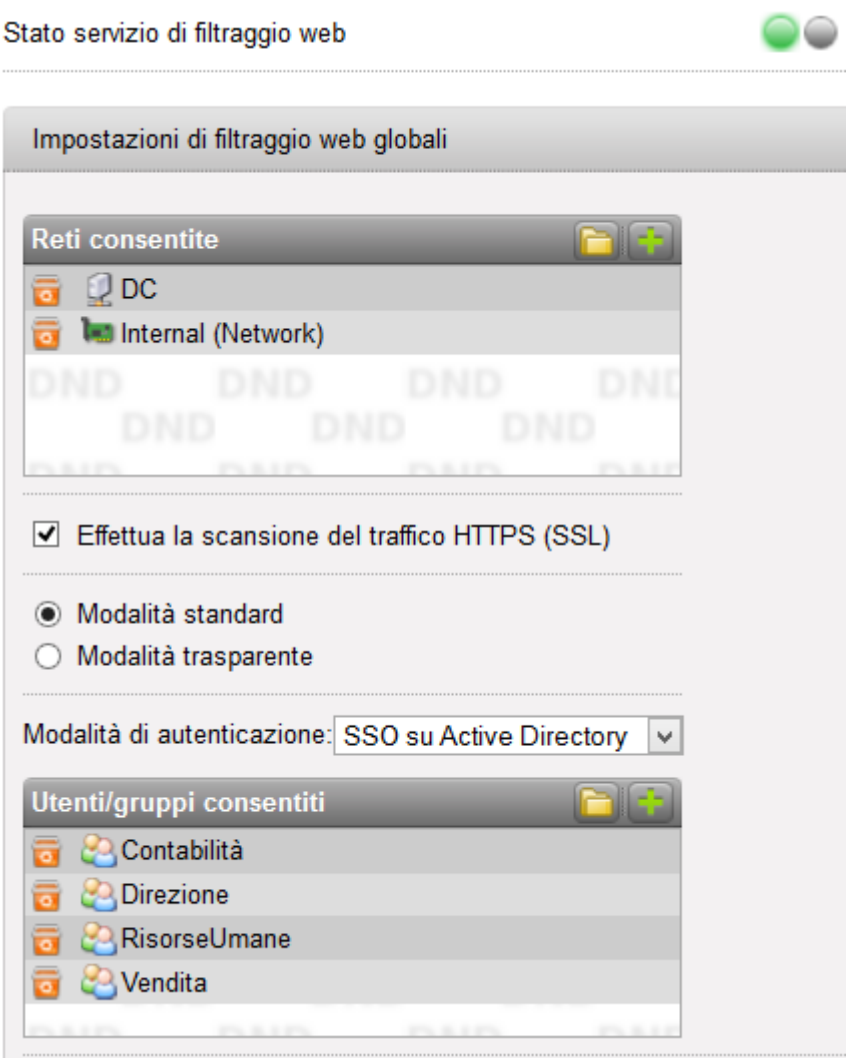
Creiamo quindi un nuovo percorso di richiesta DNS.


- Dominio: Nome del dominio
- Server Target: IP del Domain Control

## 2.8 Configurazione Filtraggio WEB

Passiamo ora alla configurazione del filtraggio del traffico web

Spostiamoci in: “Web Security”-> “Filtraggio Web”-> “Globale”




Abilitiamo il filtraggio WEB

Impostiamo le reti da sottoporre al filtraggio

Scegliamo di scansionare il traffico criptato (Https, SSL)

Scegliamo la modalità di autentificazione SSO (Sigle-Sign-On) che abbiamo prima creato, e importiamo tutti i gruppi.

Spostandoci nella pagina “Filtraggio URL” possiamo già creare delle regole di navigazione applicate a tutti coloro che passano dal FW.
Astaro ci da già delle categorie di siti che possiamo bloccare a priori.
ES: (Drugs, Criminal Activities, Games/Gambles, Weapons, ecc..)

## 2.9 Configurazione profili di filtraggio WEB

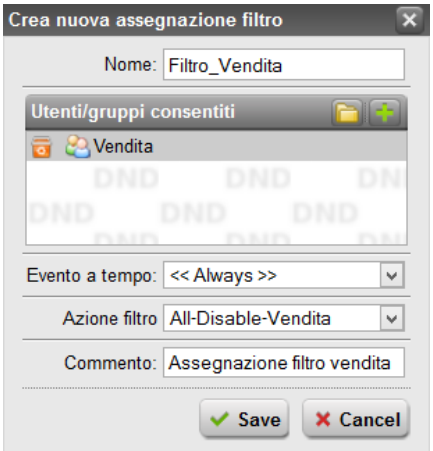
La configurazione dei profili di filtraggio web, permette di creare regole di navigazione specifiche per utenti/gruppi.
Spostiamoci in: "Web Security"-> "Profili di filtraggio WEB"-> "Profili Proxy"
Creiamo quindi un profilo Proxy:

- Nome: Nome del profilo Proxy
- Posizione: È possibile creare più profili e assegnare loro la posizione
- Reti di origine: Qui inseriremo le reti di origine che andranno al Proxy
- Assegnazione filtro: Qui inseriremo le assegnazione dei filtri che creeremo dopo
- Azione di fallback: Questa è l'opzione per un utente che non ha un assegnazione filtro, e gli viene assegnato un filtro generico.
- Modalità di funzionamento:
- Modalità di autentificazione: modalità di autentificazione al Proxy (nel nostro caso SSO su Active Directory)

Spostandoci in: "Web Security"-> "Profili di filtraggio WEB"-> "Azioni filtro" possiamo creare dei filtri di filtraggio web per i vari utenti/gruppi.
Creiamo quindi una nuova azione filtro:

- Nome: Nome del filtro
- Modalità: "Consenti per default"= di default è consentito tutto
  "Blocca per default"= Di default è tutto bloccato
- Blocca le seguenti categorie: Di seguito sono riportate le categorie dei siti WEB, ed è possibile bloccarle.
- Blocca questi URL/Siti: Inseriamo qui i siti da bloccare
- Consenti questi URL/Siti: inseriamo qui i siti consentiti sempre
- Esenzione file bloccate: Qui inseriamo le estenzioni file da bloccare (.exe, .vbs, .bat)
- Utilizza la scansione antivirus: Abilitare se si vuole utilizzare la scansione antivirus

Finita la configurazione del filtro, passiamo all'assegnazione del filtro a un utente/gruppo.
Spostiamoci in: "Web Security"-> "Profili di filtraggio WEB"-> "Assegnazione filtro"




Scegliamo il nome dell'assegnazione filtro

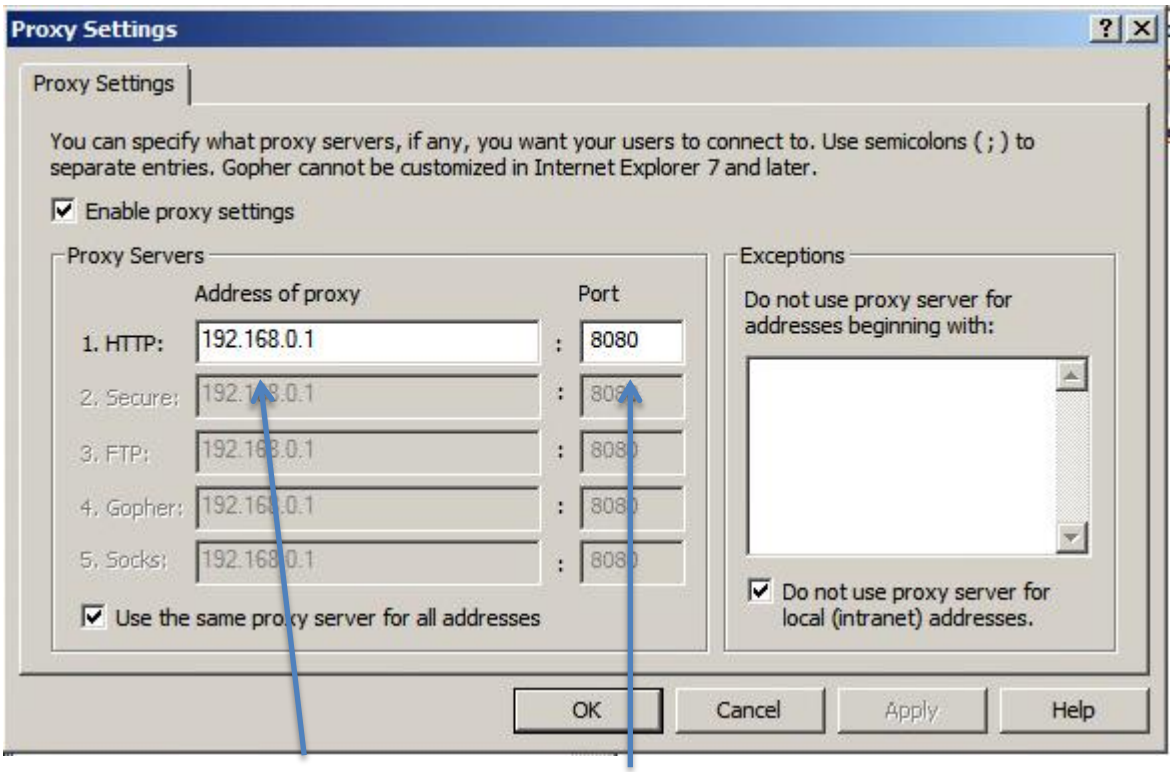
Scegliamo l'utente o il gruppo a cui assegnare il filtro

Scegliamo quando questa regola è attiva
Scegliamo quale filtro assegnarli
Aggiungiamo un commento (Non è obbligatorio)

## 3.0 Configurazione Proxy nei client Windows7 tramite GPO

Avendo 2 client possiamo settare i parametri di connessione al Proxy manualmente, ma dato che potrebbero aggiungersene altri, useremo un policy dal Domain Controll.
Per far ciò andiamo sul DC e apriamo "Goup Policy Management".

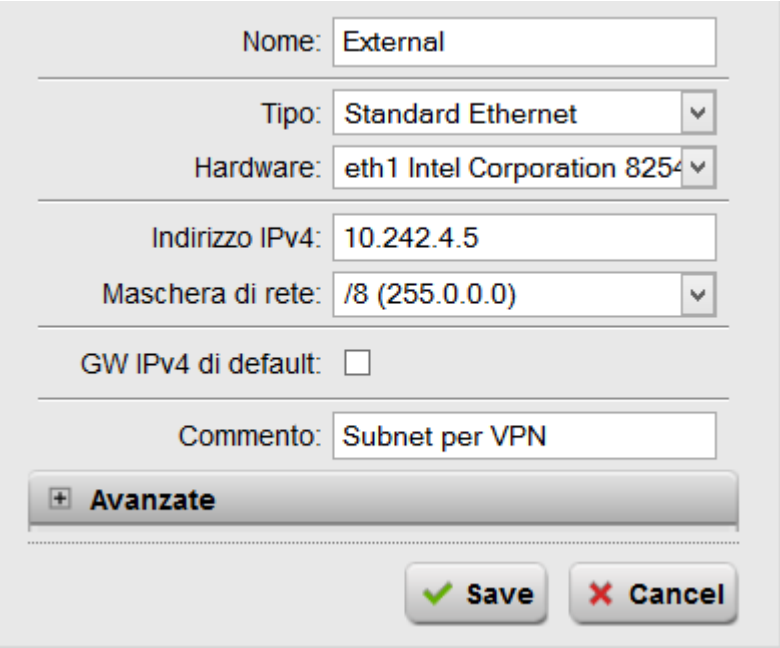
- Clicchiamo con il tasto destro sul nostro dominio (nel mio caso BELLNET.LOCAL) e scegliamo la prima opzione "Create a GPO in this Domain, and link it here".
- Ora andiamo a modificarla cliccandoci sopra con il tasto destro e poi "Edit"
- Navighiamo in "User Configuration" -> "Windows Settings" -> "Internet Explorer Maintenance" -> "Connection"
- Doppio click su "Proxy Setting"




- Andiamo a inserire l'ip del nostro Porxy e la porta.
- Spuntiamo la voce "use the same proxy server for all addresses" per far si che tutti i protocolli usino il proxy.

## 3.1 Configurazione VPN su Astaro

Per configurare una VPN, dato che non abbiamo una rete esterna, dobbiamo innanzitutto configurare un interfaccia del Firewall come subnet diversa dalla rete locale.
Andiamo in “Interfacce & routing” -> “Interfacce”
Clicchiamo su “Nuova interfaccia”



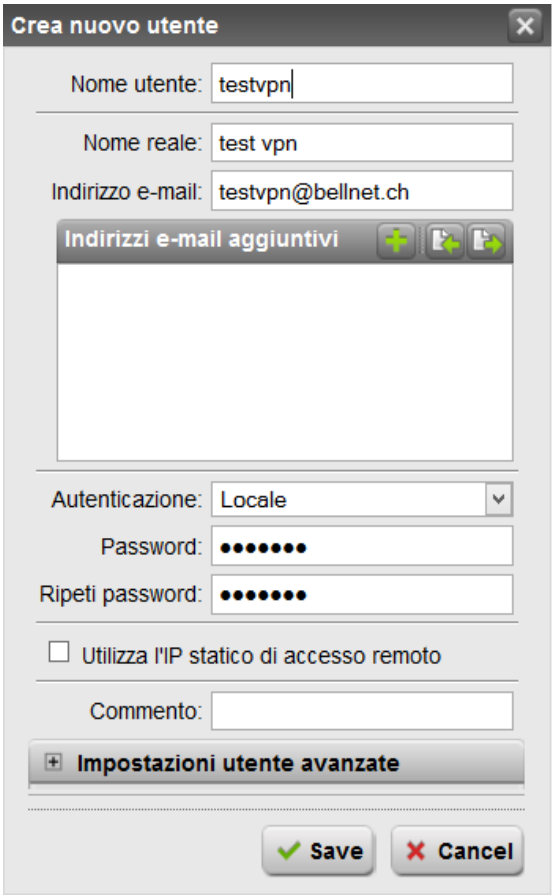

Scegliamo il nome del interfaccia

Scegliamo il tipo di collegamento
Scegliamo la porta sul FW

Diamo un IP all’interfaccia
e una maschera di rete
(Su un altra subnet)

Clicchiamo su “Save”

Passiamo ora alla creazione del utente per la connessione:
Andiamo in “Definizioni & Utenti”-> “Utenti & Gruppi”




Scegliamo il nome del utente

Scegliamo l’indirizzo email

Scegliamo come metodo di autentificazione “Locale”
Scegliamo la password

Salviamo il nuovo utente

Ora che abbiamo l'interfaccia dove si connetterà l'ipotetico fornitore e il relativo utente, andiamo a settare i paramenti per la connessione VPN Ipsec.
Spostiamoci in "Accesso Remoto" -> "Client VPN Cisco"

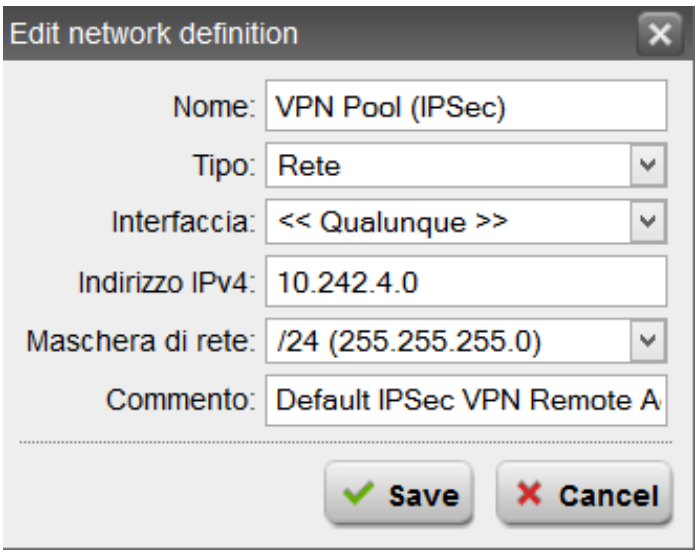

Scegliamo l'interfaccia dove ci si connetterà

Scegliamo il certificato del server

Creiamo un nuovo pool di indirizzi di rete cliccando sul "+" in verde.

Scegliamo le reti locali dove si vorrà far accedere la VPN

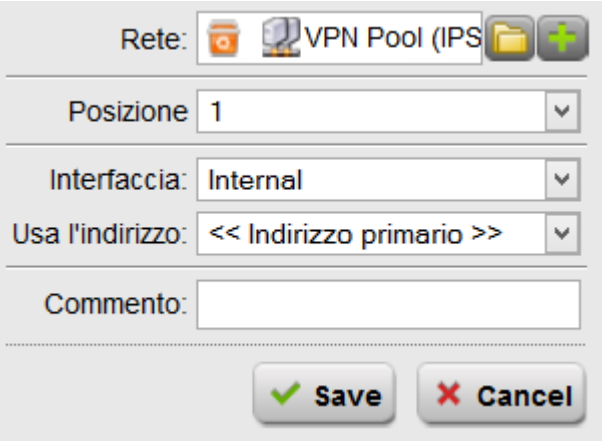
Scegliamo l'utente o il gruppo che saranno autorizzati alla connessione




-Scegliamo il nome
-Scegliamo "Rete"
-Scegliamo l'interfaccia
-Scegliamo l'indirizzo IP che verra assegnato all'utente che si connetterà
-Scegliamo la relativa maschera di rete

-Salviamo

Procediamo ora con la configurazione della NAT per far si che il PC remoto, possa comunicare con la LAN (DC, Client W7,ecc)
Andiamo in: "Network Security" -> "NAT" e quindi " Nuova regola di Mascheramento"




Scegliamo la rete della VPN

Scegliamo l'interfaccia a cui accedere

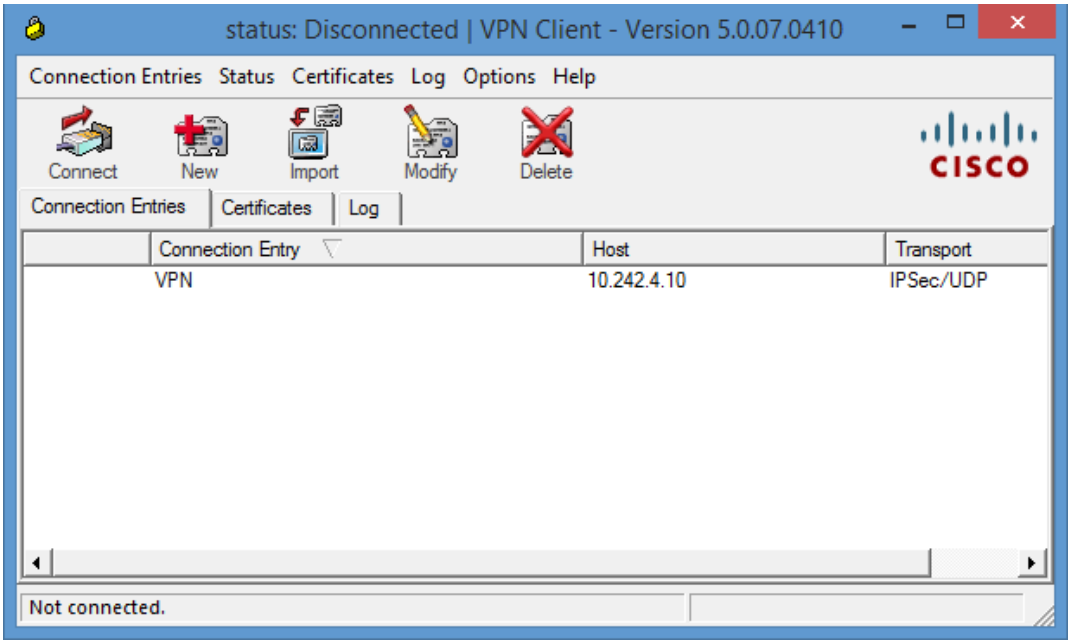
Salviamo

Prima di procedere con la configurazione del client VPN, dobbiamo scaricare il certificato a lui assegnatoli. Per far ciò andiamo in: "Accesso Remoto" -> "Gestione Certificati"

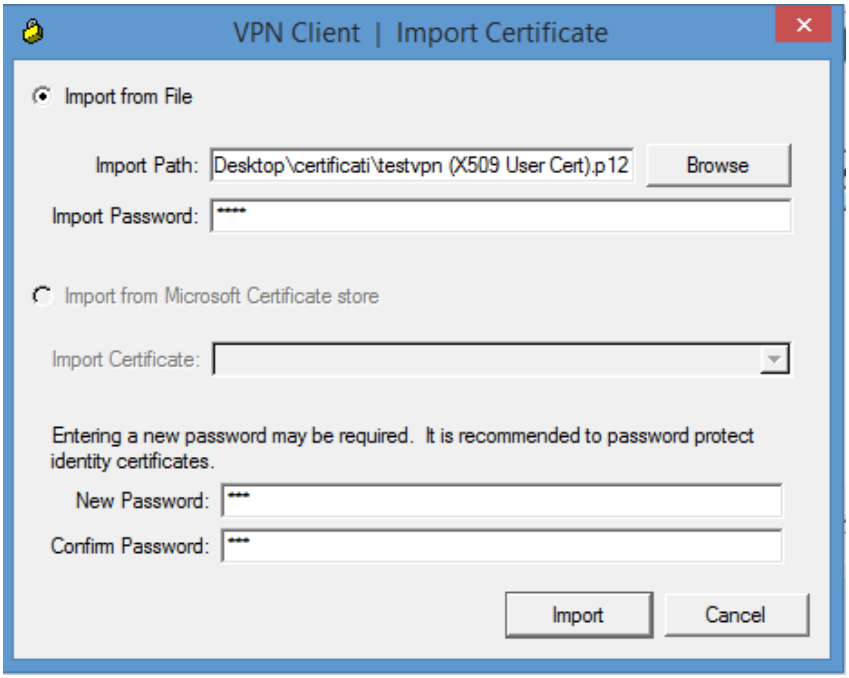

Cliccando su Download, si aprirà una maschera dove ci chiederà come esportare il certificato (PEM o PKCS#12). Noi scegliamo "PKCS#12" e scegliamo una password.

### 3.1.2 Configurazione VPN su client Windows 7

Per prima cosa andiamo su www.cisco.com e scarichiamo il client VPN.
Una volta scaricato ed installato, procediamo con la configurazione della VPN.



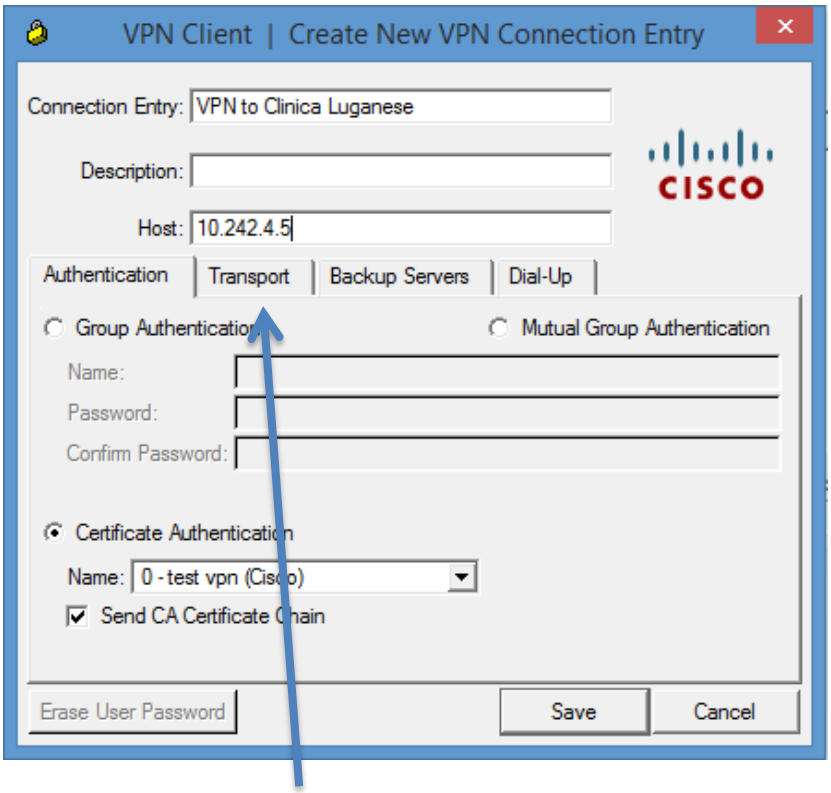

Cominciamo con l'importare il certificato scaricato in precedenza nel punto 3.9.
Andiamo in "Certificates" -> "Import.."




-Scegliamo il percorso del certificato
-Immettiamo la password del certificato

-Immettiamo la nuova password per il certificato

Ora cliccando su “New”, settiamo i parametri per la connessione VPN



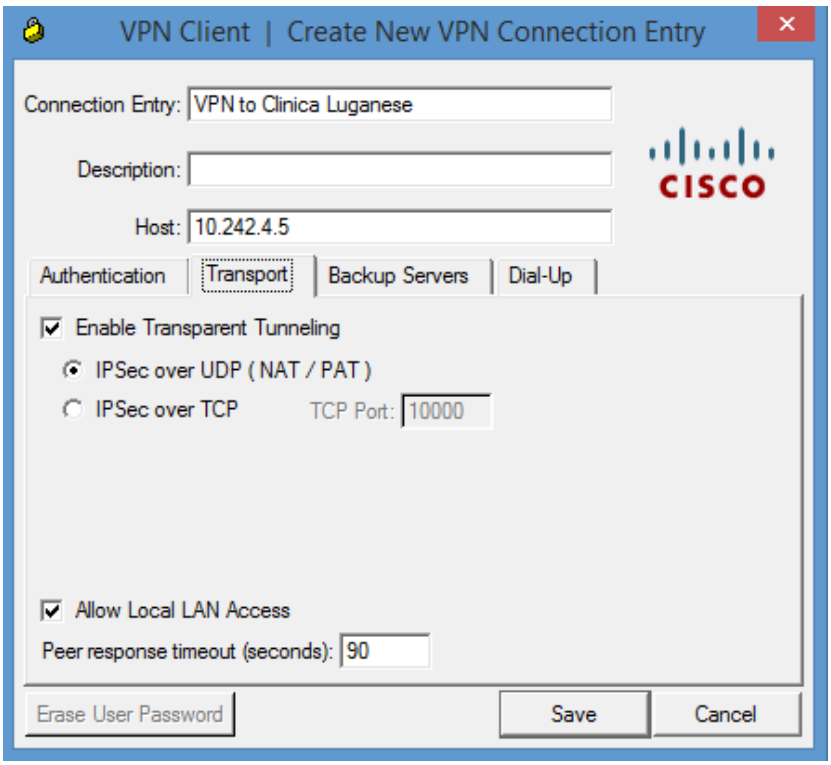

-Immettiamo il nome della VPN

-Immettiamo una descrizione

-Immettiamo l’indirizzo IP o Hostname della interfaccia esterna del FireWall

-Scegliamo come metodo di autentificazione “Certificate Authentication”

Spostiamoci in “transport”




Abilitiamo il “Trasparant Tunneling”

Abilitiamo “Local LAN Access”

Salviamo

## 3.2 Aggiornamento di  da UTM 8.1 a UTM 9.2

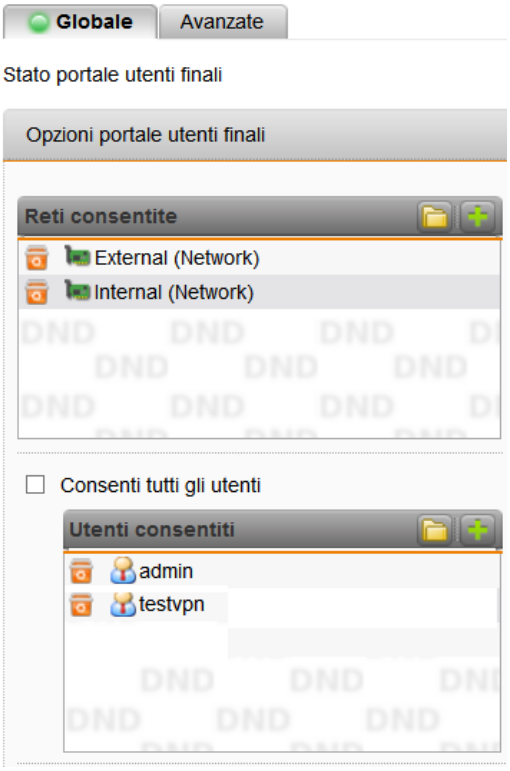
Arrivato quasi al termine del lavoro, mi accorgo che nella versione 8.2 non ce l'HTML 5.
Dato che l'ultima parte del lavoro è la creazione di un portale, aggiornerò la versione corrente alla 9.2. Per far ciò, andiamo sul sito di Astaro, e scarichiamo la ISO di Sophos UTM 9.2.
Masterizziamo quest'ultima su un CD.
Prima di aggiornare, faremo un backup delle impostazioni, cosi che sia possibile eseguire il restore una volta aggiornato.
Andiamo dunque in:
"Funzionalità di Gestione" -> "Backup e Ripristino" e clicchiamo su "Crea Backup ora"
Esportiamo questo Backup su una pennetta USB.
Ora, collegando un lettore CD esterno USB al Firewall, lo riavviamo. Al suo boot partirà da CD e chi chiederà di premere:

- Premi Enter -> Installare
- Premi F1 -> Help
- Premi F3 -> Troubleshooting

Finita l'installazione, ci chiederà di rimuovere il CD e riavviarlo.
Togliamo il CD, inseriamo la pennetta contenente il backup e riavviamo il Firewall.
Noteremo che tutte le impostazioni saranno come prima, dato che al suo primo avvio, Astaro cerca nelle periferiche un punto di restore.

## 3.3 Configurazione Portale Remote Desktop

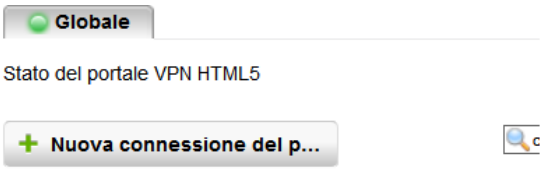
Con la versione UTM 9.2 di Sophos, possiamo creare il portale di accesso remoto per gli utenti. Andiamo innanzitutto su "Funzionalità di Gestione" -> "Portale Utenti"



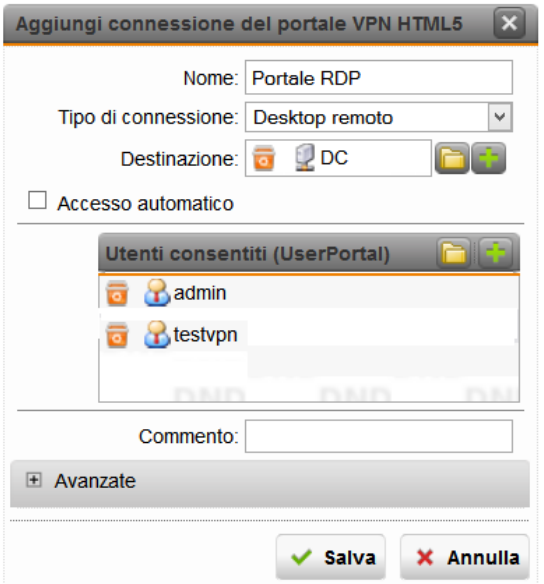

Scegliamo le reti di cui consentire la connessione al portale

Scegliamo gli utenti consentiti alla connessione del portale

Ora spostiamoci in "Accesso Remoto" -> "Portale VPN HTML5"




Clicchiamo su "Nuova connessione del portale"




Scegliamo il nome della connessione

Scegliamo il tipo di connessione (RD,http,HTTPS,...)

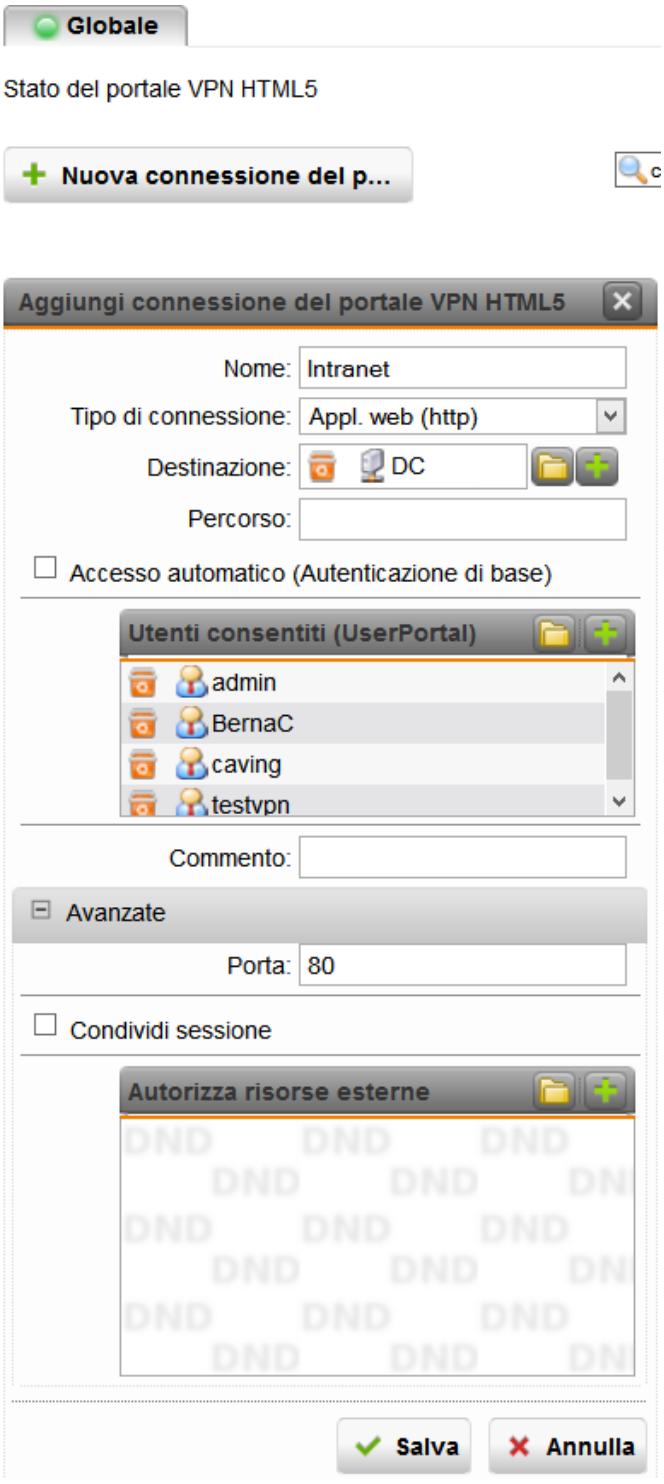
Scegliamo l'host a cui si farà l'RDP

Scegliamo gli utenti consentiti

Salviamo

## 3.4 Configurazione portale Web Intranet

Cominciamo con installare sul server (DC) il servizio Web Server IIS.
"Server Manager" -> "Add Roles" -> "Web Server IIS"
Ora collegandoci sulla pagina WebAdmin e andiamo in:
"Accesso Remoto" -> "Portale VPN HTML5" -> "Nuova connessione del Portale"




Scegliamo il nome
Scegliamo "Appl.Web HTTP" come tipo
Scegliamo il server con IIS

Scegliamo gli utenti che potranno connettersi

Scegliamo la porta di connessione del server IIS (80 di default)

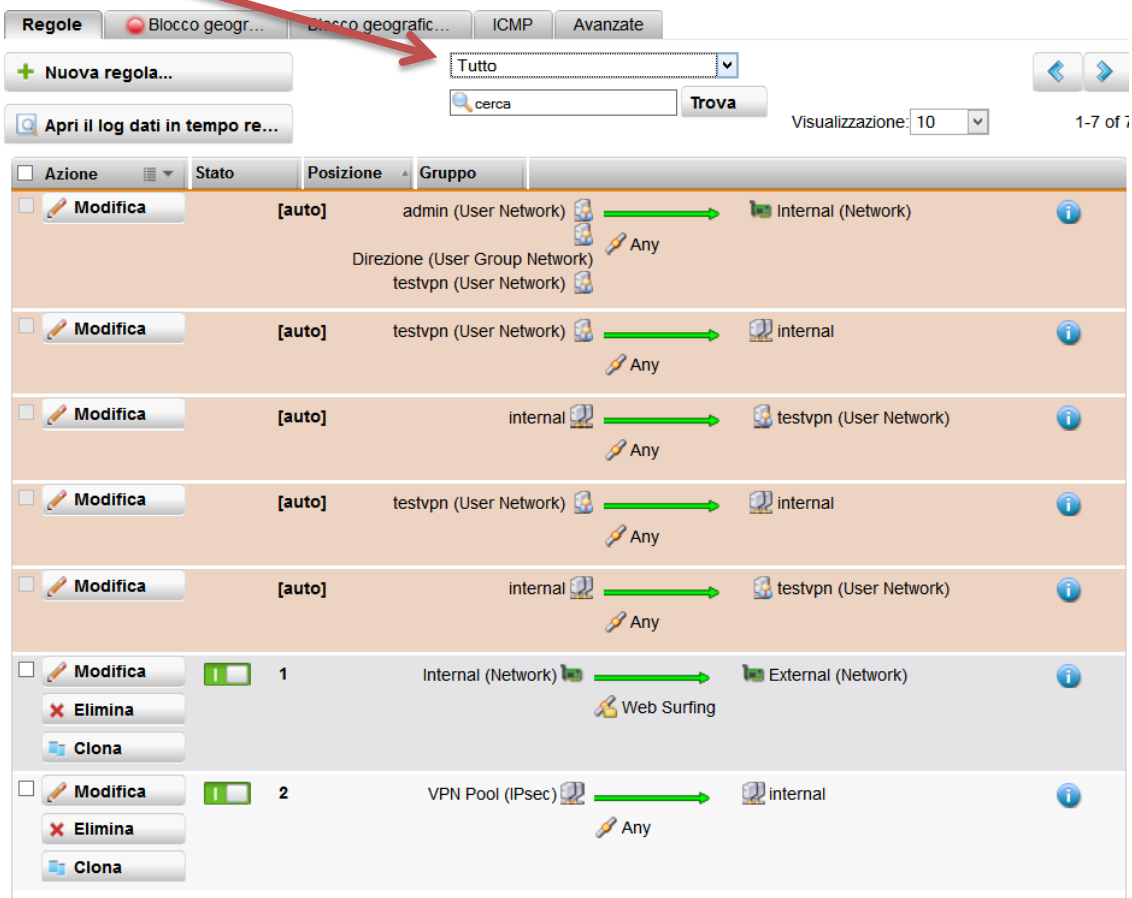
Salviamo

## 3.5 Configurazione regole Firewall

Andando in: -> “Network Protection” -> “Firewall” vediamo le regole del Firewall.
Delle regole vengono create automaticamente nella configurazione di un determinato servizio.


Ad esempio nell’ IP sec, quando si configura, ce da spuntare l’opzione:
“Regole Automatiche del Firewall”

Queste regole vengono create e abilitate automaticamente. Per vederle bisogna selezionare “tutto”.

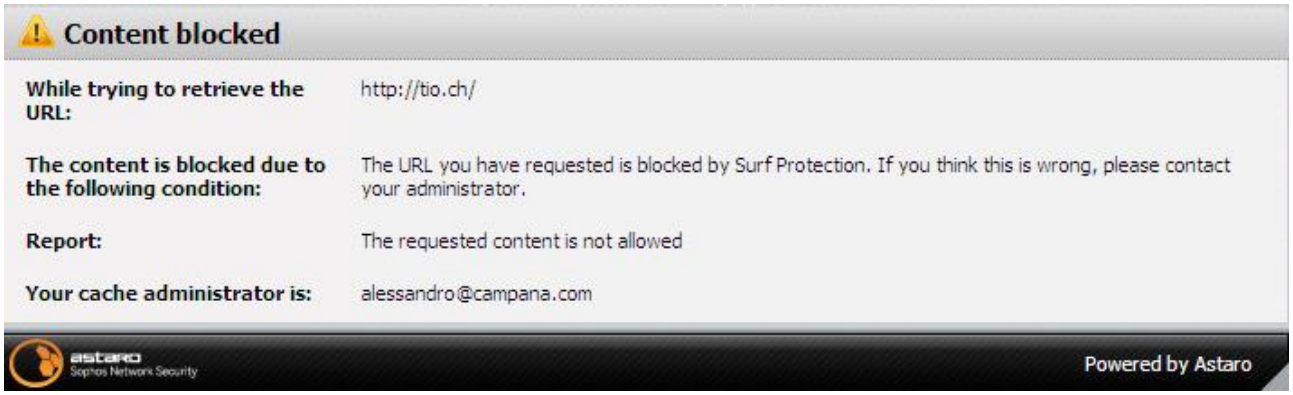


# 4. Test e prove sul funzionamento

## 4.1 Test sul funzionamento dei filtri di Webfiltering

Autentifichiamoci sul client Windows 7 (in LAN) con l'utente VergaP.
L'utente VergaP fa parte del gruppo Vendita.
Al gruppo vendita sono assegnati questi filtri:


Proviamo quindi a navigare su [www.tio.ch](http://www.tio.ch).

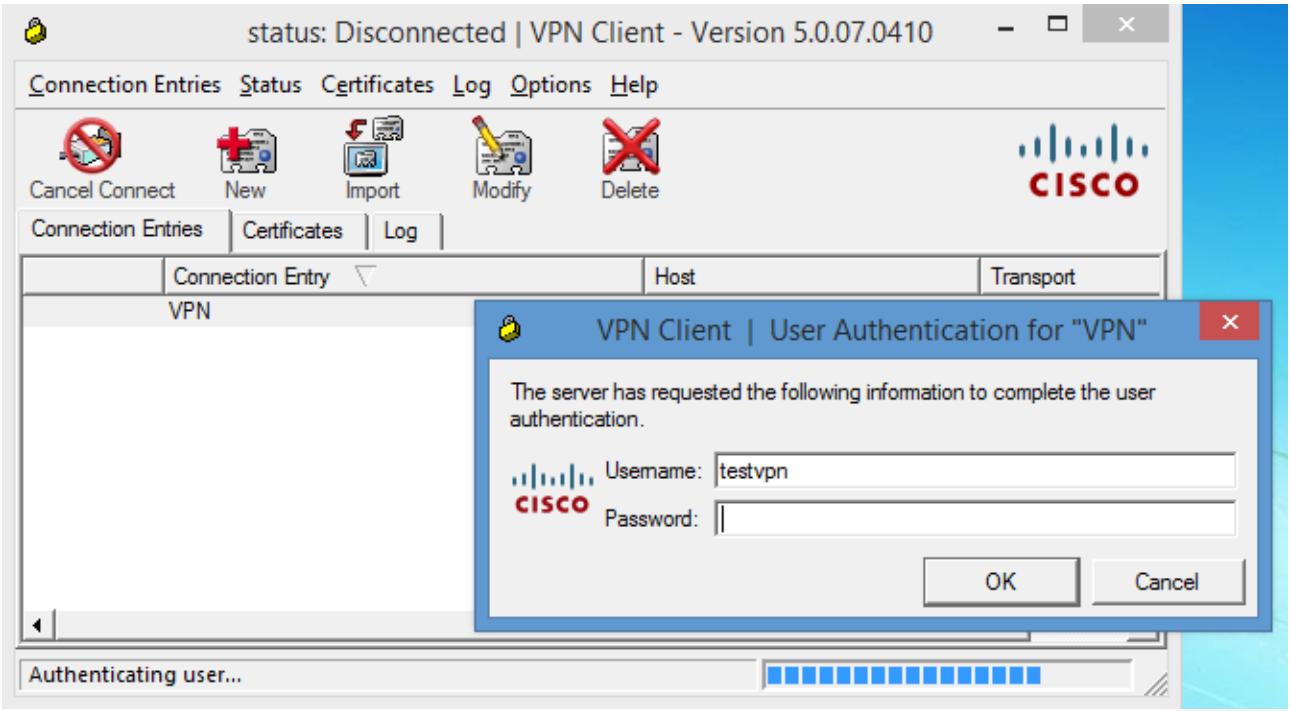



Il risultato è corretto. Tutti i siti sono stati bloccati, tranne quelli nella Whitelist.
Di conseguenza se ci connettiamo a [www.steg.ch](http://www.steg.ch) il Proxy ci lascerà navigare.

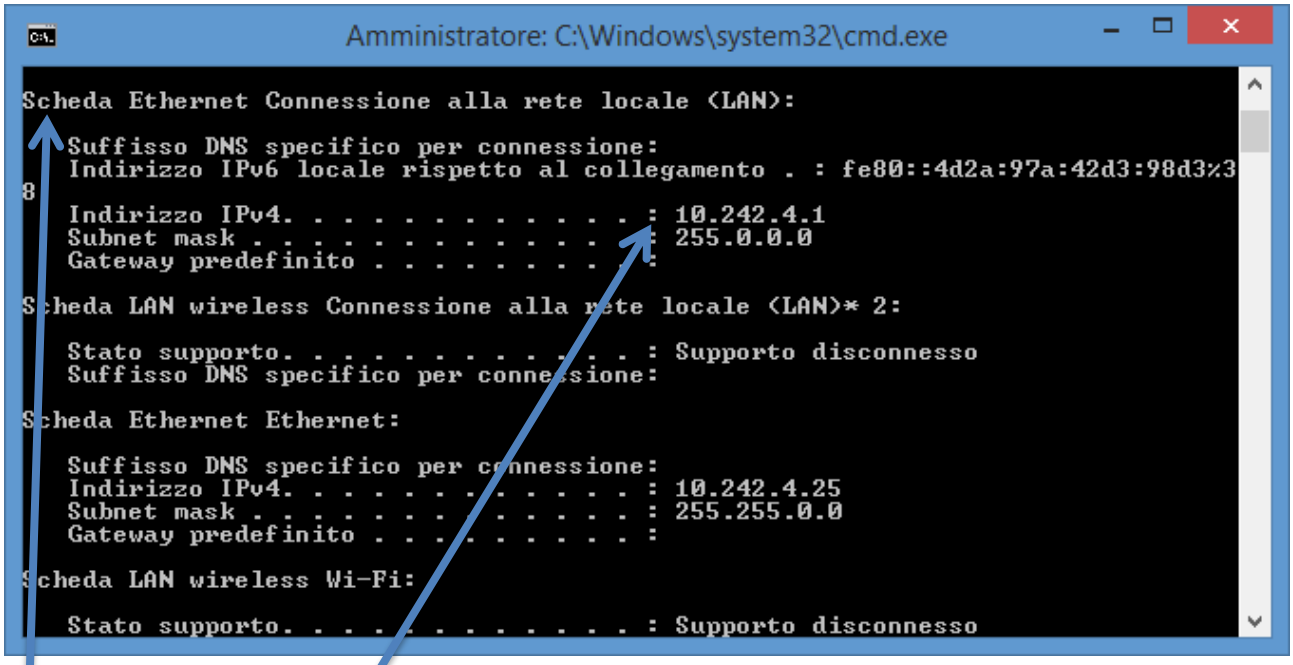

Torna questo errore perché non essendo collegato ad internet, non riuscirà a trovare l'Host.

## 4.2 Test sul funzionamento della VPN

Selezioniamo la VPN creata in precedenza e clicchiamo su “Connect”

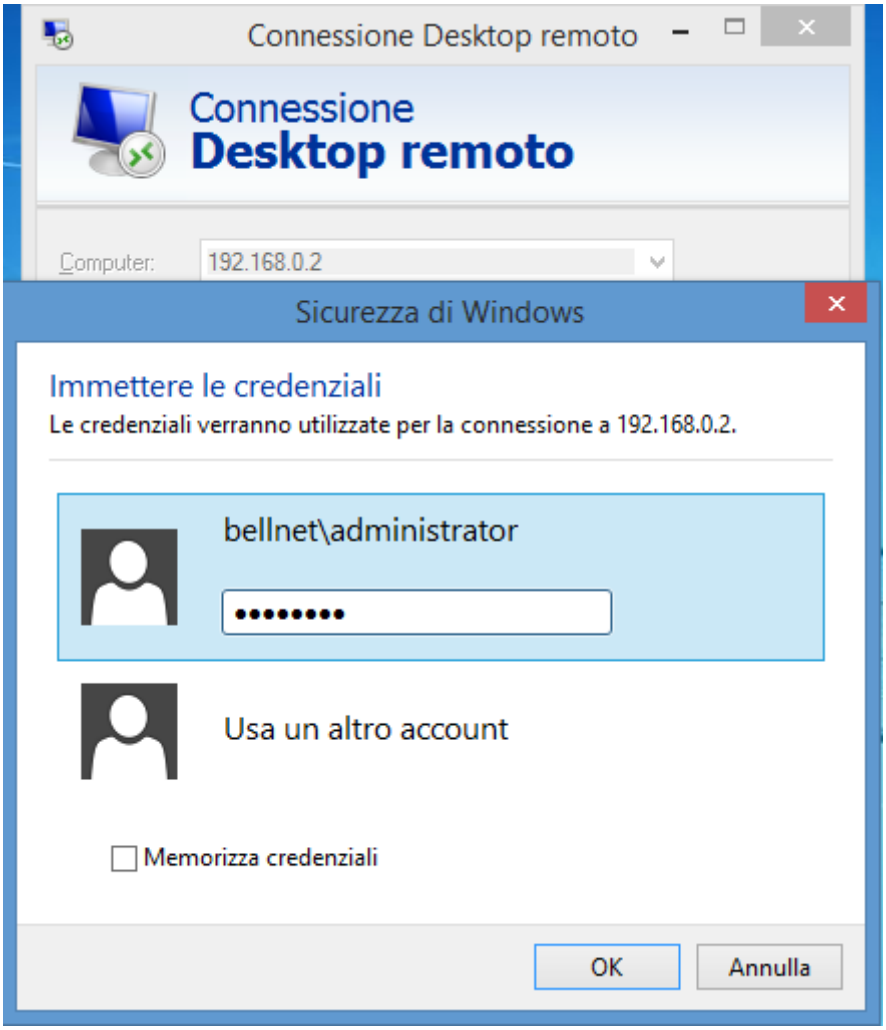



Verrà richiesta la password del utente “testvpn”. La immettiamo e clicchiamo “Ok”
Ora la maschera del client VPN si minimizzerà. Questo vuol dire che siamo connessi.
Apriamo il CMD e digitiamo “Ipconfig”

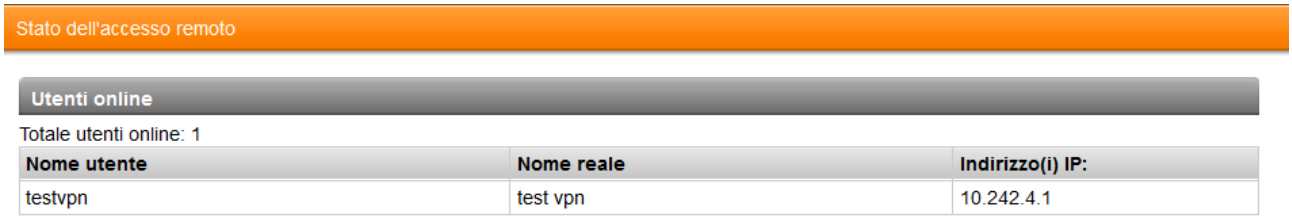



Come possiamo vedere, si creerà una nuova scheda ethernet virtuale, dove verrà assegnato l’IP dato dal “VPN Pool Ipsec”

Ora apriamo il “Remote desktop” (MSTSC.exe) e proviamo a collegarci al Domain Controll.



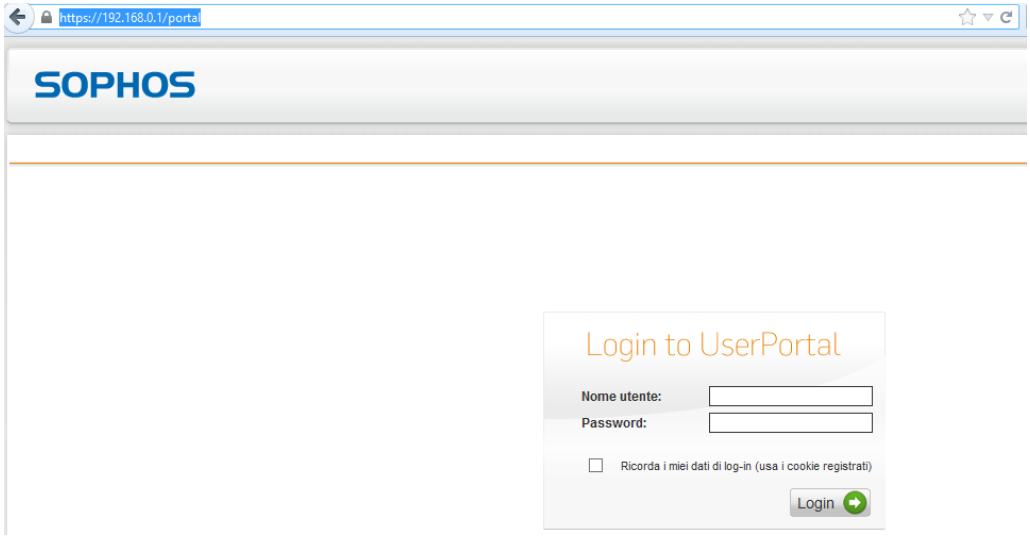

Andando sulla WebPage Admin del Firewall, nella sezione “Accesso Remoto”, possiamo vedere gli utenti connessi alla VPN.



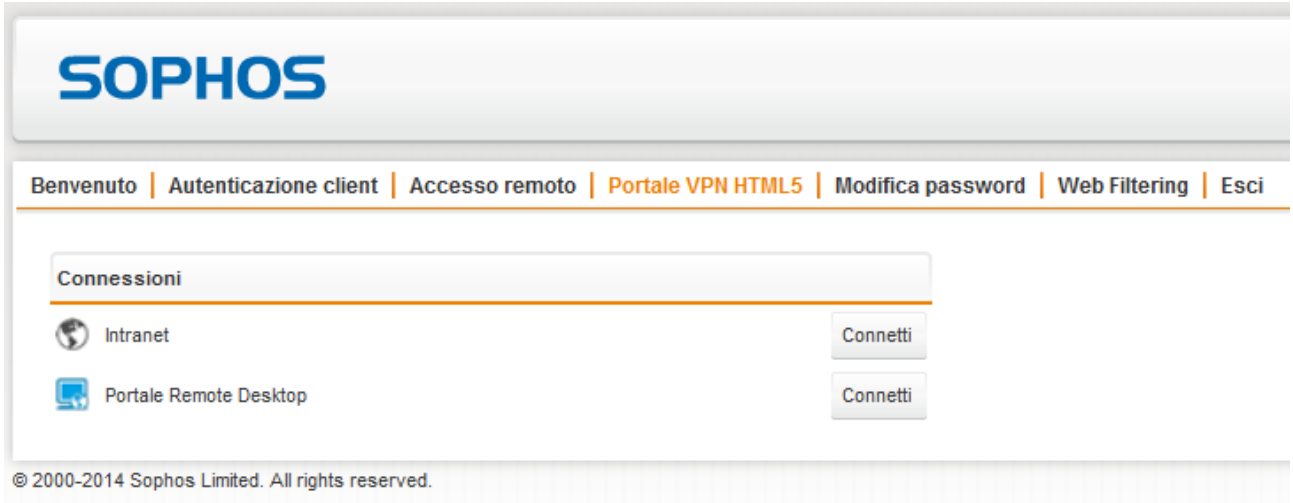

Possiamo confermare che la VPN funziona.

## 4.3 Test sul funzionamento del portale per il Remote Desktop

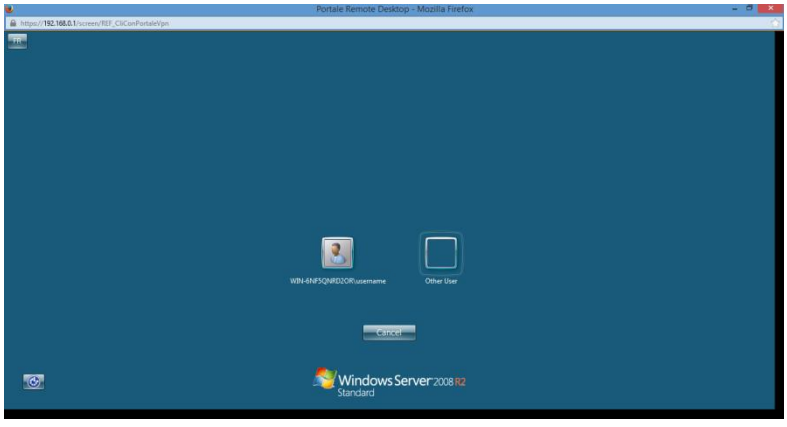
Con il terminale usato per la connessione VPN, apriamo il browser e digitiamo http://192.168.0.1/portal




Una volta autentificati con l'utente "testvpn", si aprirà questa maschera

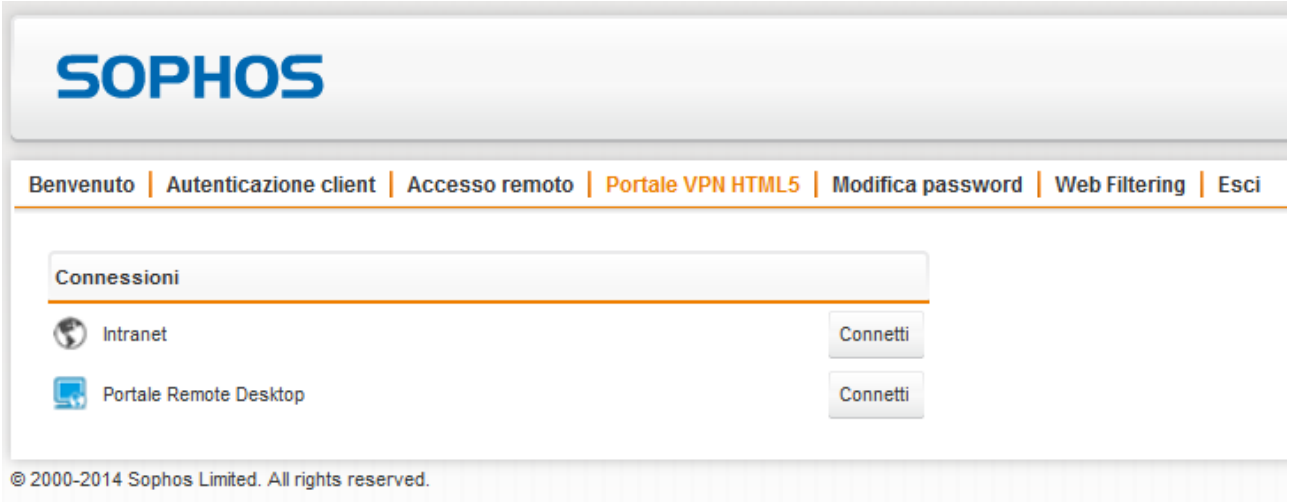



Spostandoci in "Portale VPN HTML5" vedremo , in connessioni, "Portale Remote Desktop"
Cliccando su connetti, si aprirà un'altra pagina con il computer remoto.

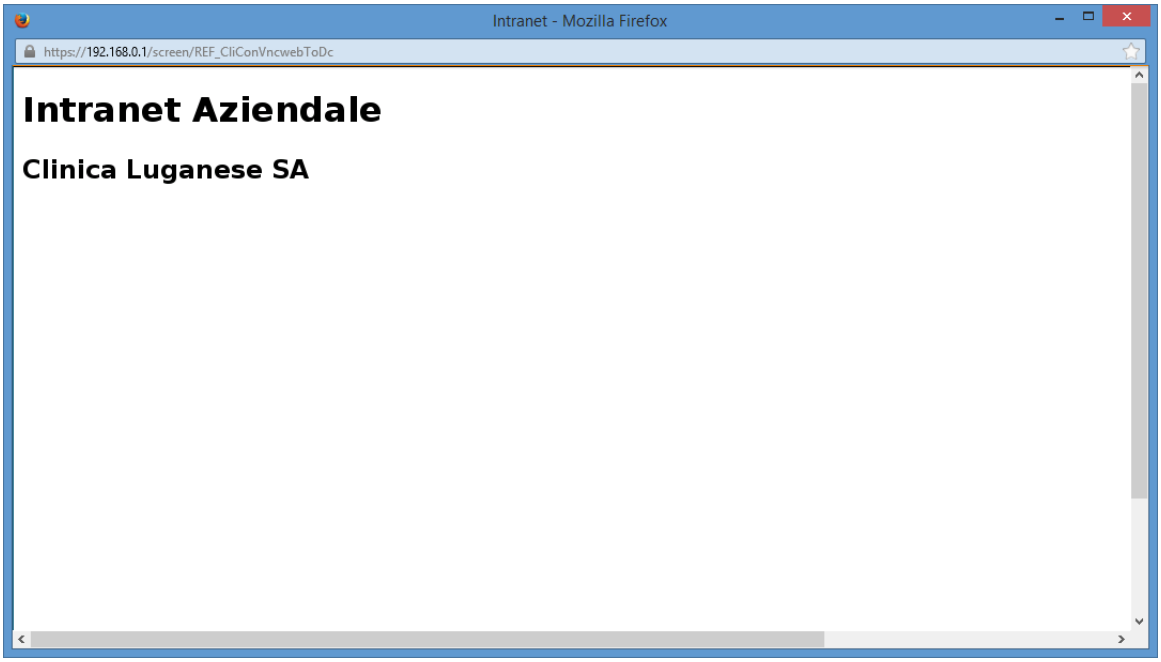


## 4.4 Test sul funzionamento del portale per Intranet

Come nel 4.3, ci colleghiamo all'indirizzo http://192.168.0.1/portal
Eseguiamo il login e ci spostiamo in "Portale VPN HTML5"




Cliccando su "Connetti" di "Intranet", si aprirà una nuova scheda con l'intranet remoto.



# 5. Conclusioni