Zeroshell: VPN Lan-to-Lan

Il sistema operativo multifunzionale

creato da Fulvio.Ricciardi@zeroshell.net

www.zeroshell.net

Assicurare la comunicazione fra due sedi

(Autore: cristiancolombini@libero.it)

Assicurare la comunicazione fra due sedi**:**

Questa breve guida pratica ci consentirà di attivare un Tunnel VPN fra due sedi collegate ad internet. Questo tipo di comunicazione garantisce sicurezza nello scambio di informazioni fra le due sedi. Sarà poi possibile scrivere le politiche di comunicazione fra le due sedi.

Ecco di seguito i passi da seguire :

Schema logico della soluzione
Preparazione dei firewall
Preparazione del certificato
Creazione del tunnel vpn
Filtri di sicurezza sul tunnel

Schema logico della soluzione:

Prima di cominciare è opportuno avere le idee chiare su ciò che si sta per fare:
avendo due sedi (SiteA e SiteB) connesse ad internet con ip pubblici statici è possibile creare una relazione (tunnel vpn) di comunicazione fra i loro due rispettivi firewall in modo che si possa garantire uno scambio di dati sicuro.

L'esempio che andrò ad implementare è stato eseguito in laboratorio; solo per questo motivo gli ip pubblici sulle interfacce esterne dei firewall appartengono alla stessa sottorete. Nella realtà si avranno ip di reti pubbliche diverse che comunque si troveranno sulla rete pubblica grazie ai rispettivi router. Questi router dovranno essere privi di nat dinamico per permettere al mondo esterno di raggiungere l'ip pubblico sulla interfaccia di rete esterna del firewall.

Nell'immagine seguente vediamo gli indirizzamenti delle reti private:

SiteA:

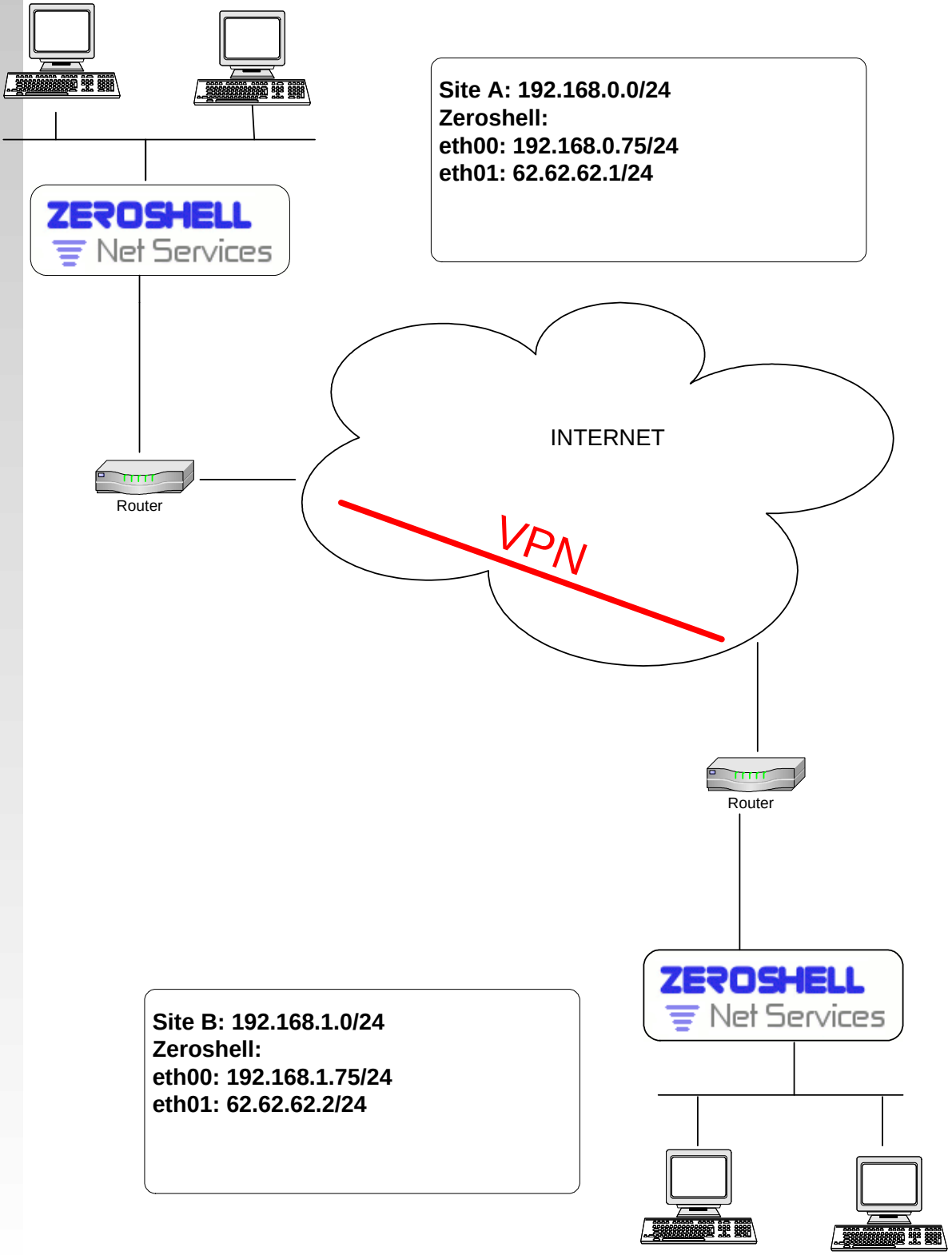
rete privata: 192.168.0.0/24
ip pubblico del firewall: 62.62.62.1

SiteB:

rete privata: 192.168.1.0/24
ip pubblico del firewall: 62.62.62.2

VPN con Zeroshell

Lunedì 19 Febbraio 2007



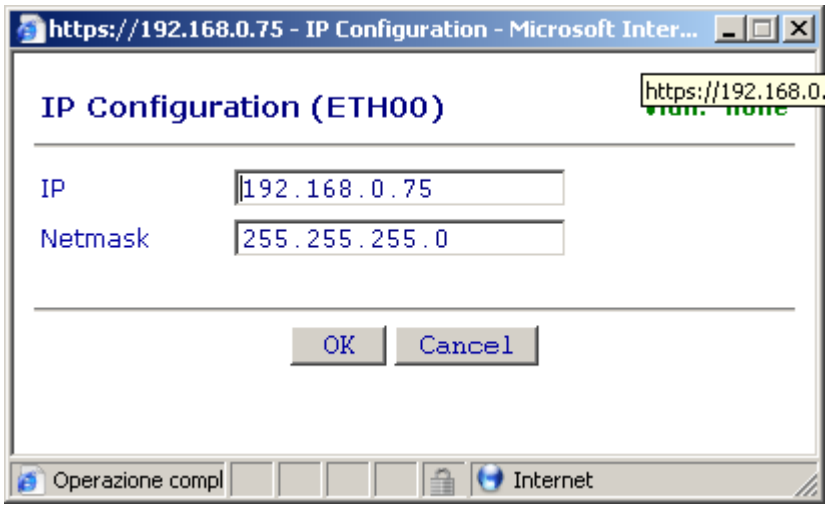
Il tunnel VPN rappresentato col colore rosso connette le interfacce esterne dei 2 rispettivi firewall, in modo esclusivo e un tramite certificato.
Una volta stabilita la relazione sicura fra i due firewall, potremo stabilire cosa realmente dovrà passare in questo Tunnel.

Preparazione dei firewall

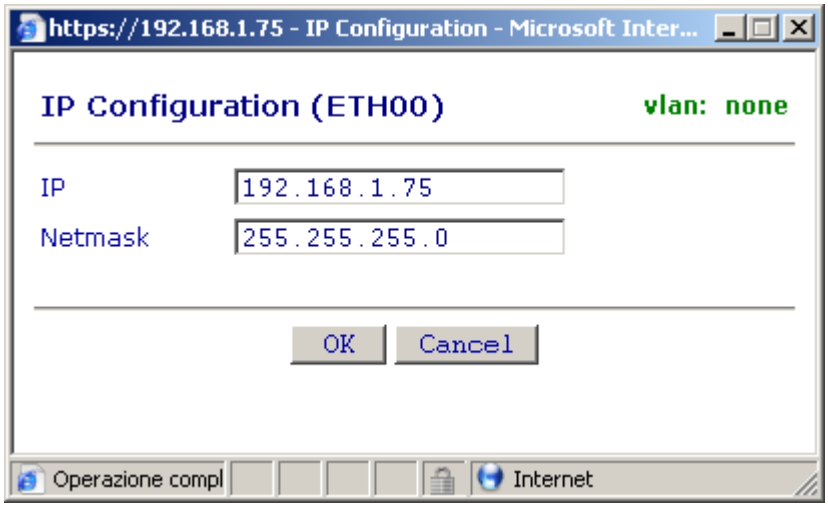
Facendo riferimento alla guida “Proteggere una piccola rete con stile” già presente fra la documentazione nel sito ufficiale www.zeroshell.net, è facile preparare la configurazione base dei due firewall:

1 – primo accesso al firewall
2 – impostazione dell’indirizzo ip sulla scheda di rete interna:

SiteA:

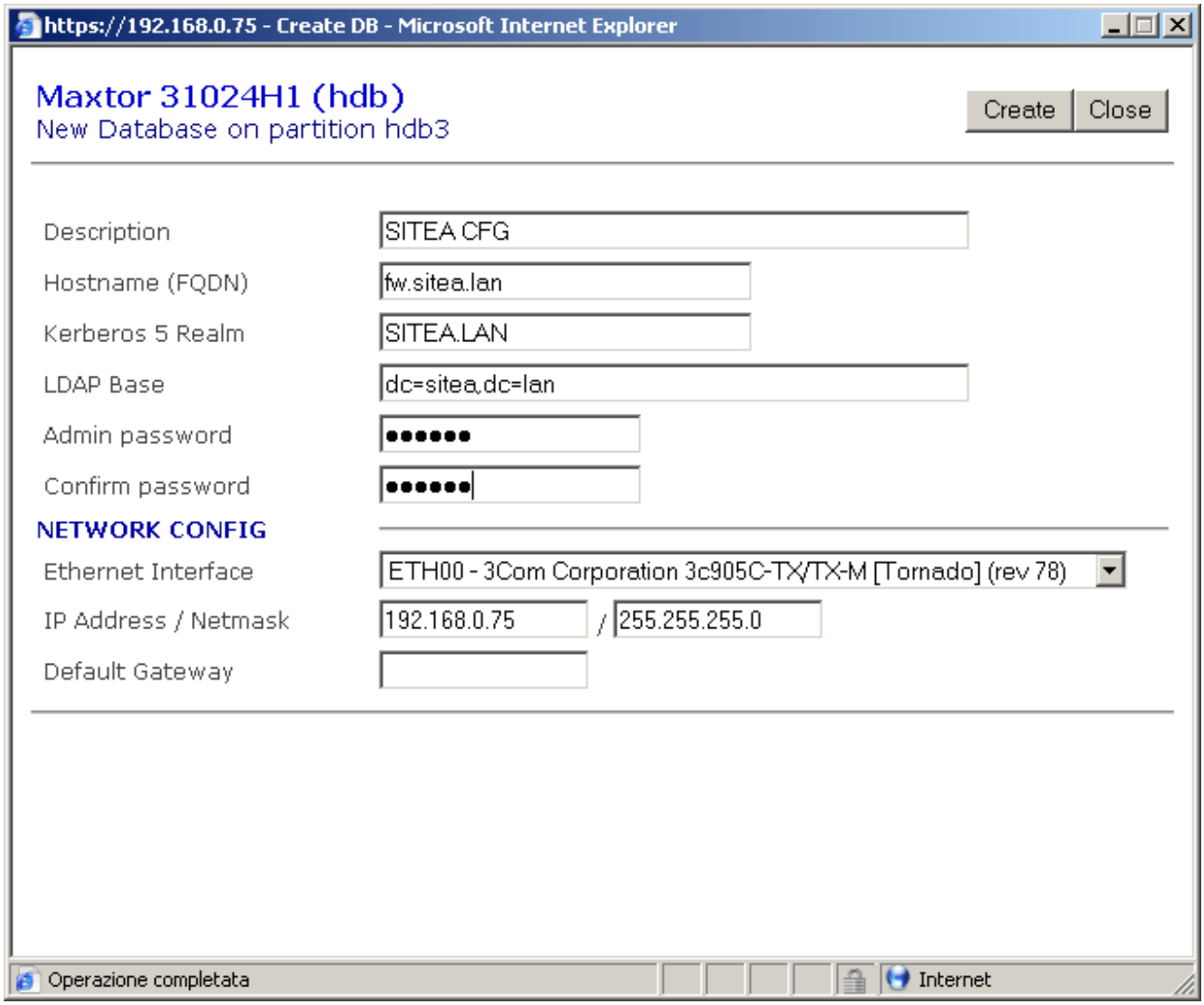


SiteB:

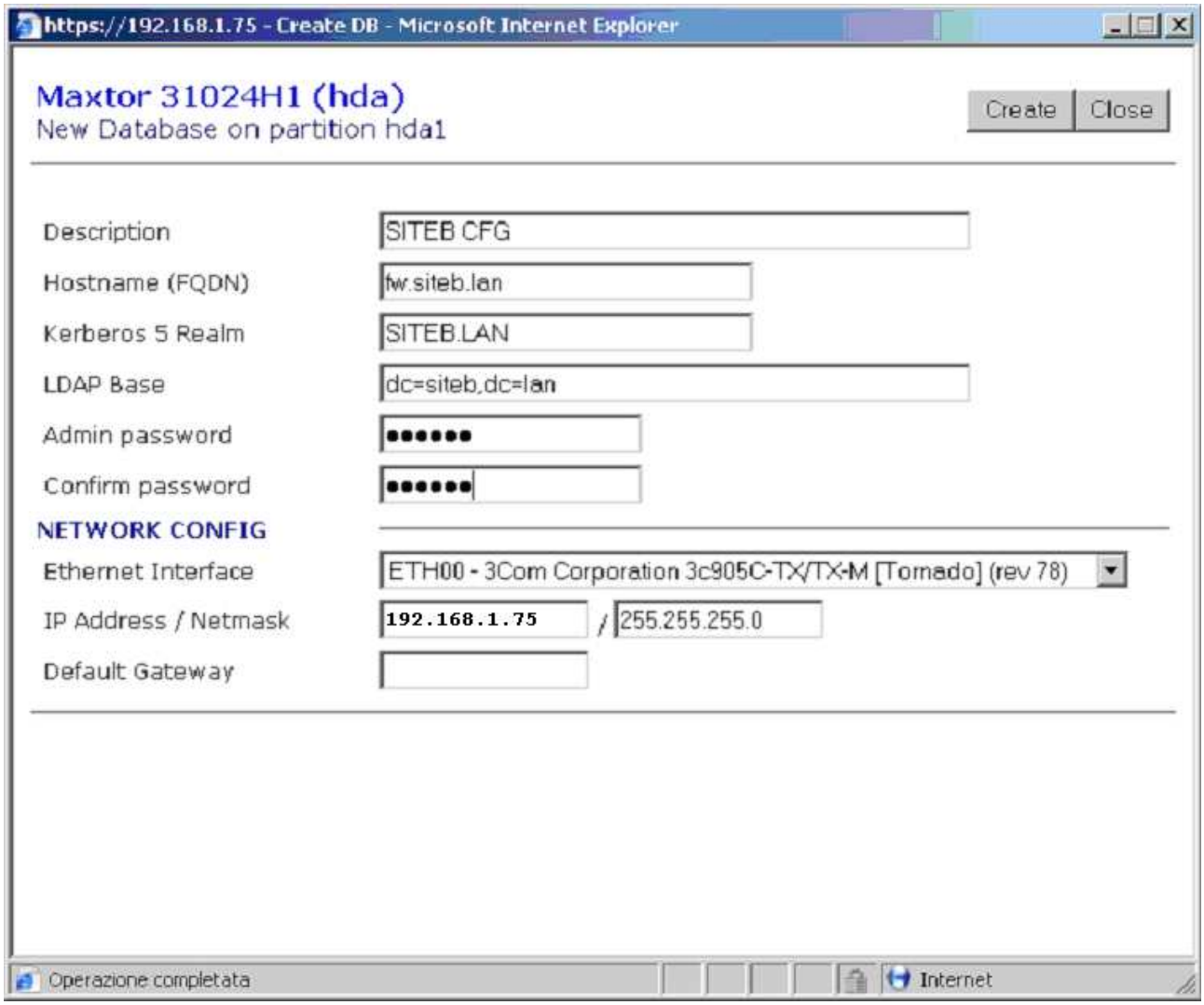


3 – Creare un databse di configurazione:

SiteA:

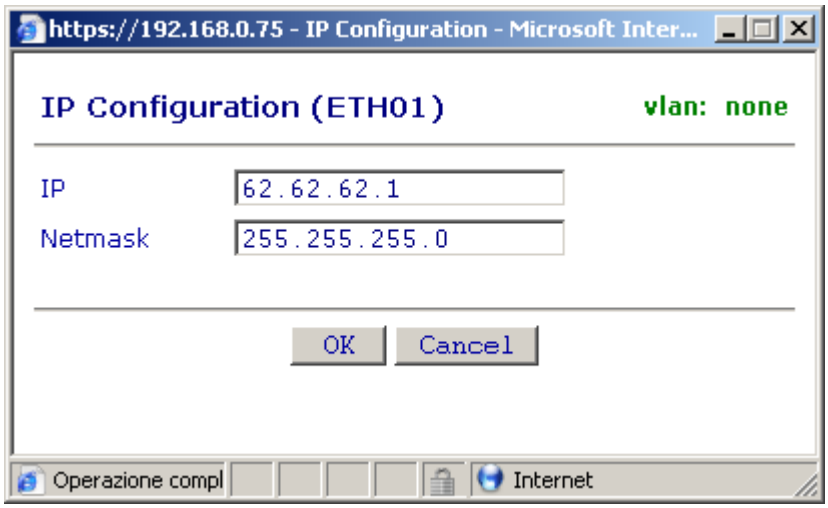

https://192.168.0.75 - Create DB - Microsoft Internet Explorer
Maxtor 31024H1 (hdb)
New Database on partition hdb3
Create
Close
Description
SITEA CFG
Hostname (FQDN)
fw.sitea.lan
Kerberos 5 Realm
SITEA.LAN
LDAP Base
dc=sitea,dc=lan
Admin password
Confirm password
NETWORK CONFIG
Ethernet Interface
ETH00 - 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 78)
IP Address / Netmask
192.168.0.75
/
255.255.255.0
Default Gateway
Operazione completata
Internet

SiteB:

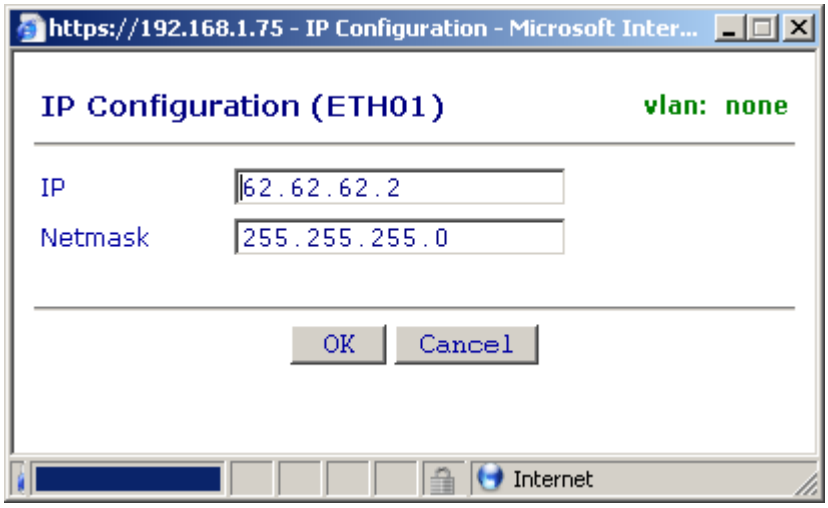


4 – Attivare su entrambi i firewall i databases ed attendere il riavvio dei sistemi
5 – Impostare gli indirizzi ip sulle schede di rete esterne:

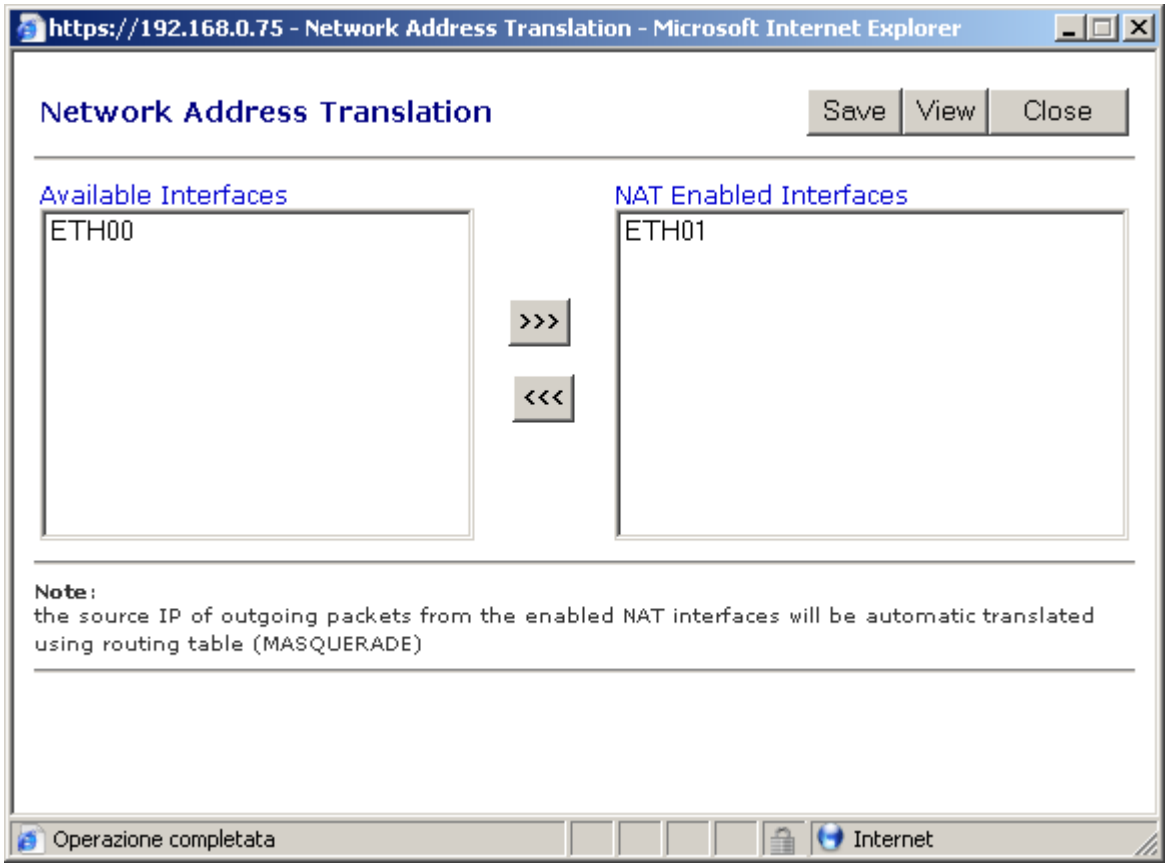
SiteA:



SiteB:



6 – Nel Router, alla voce NAT spostiamo la ETH01 in modo che vada a mascherare la nostra rete sulla ETH00 (per entrambi i firewall) :



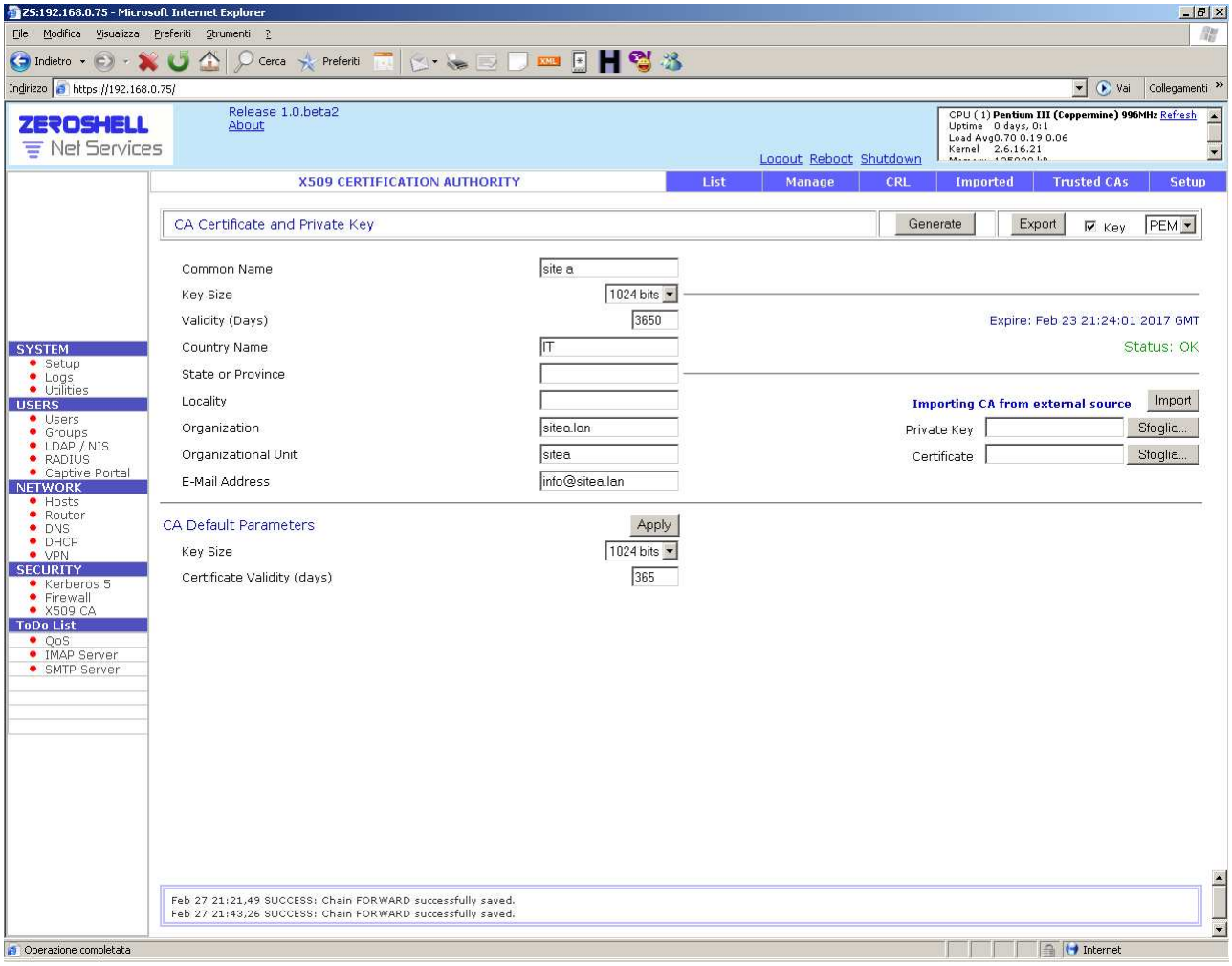
A questo punto siamo pronti per lavorare alla creazione del tunnel.

Preparazione del certificato

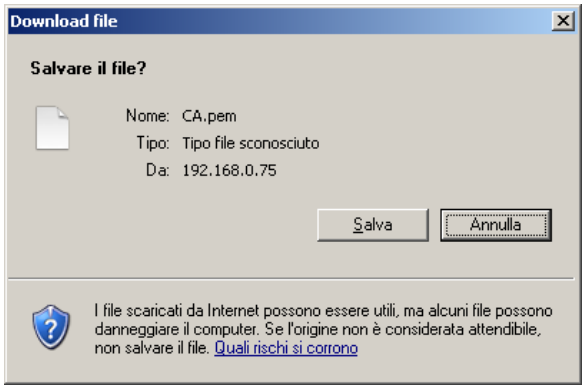
Per poter relazionare i due firewall sul un tunnel VPN, questi dovranno possedere lo stesso certifcato.
Per questo motivo dovremo crearne uno su uno dei due firewall ed importarlo sull'altro:

Creare il certificato:

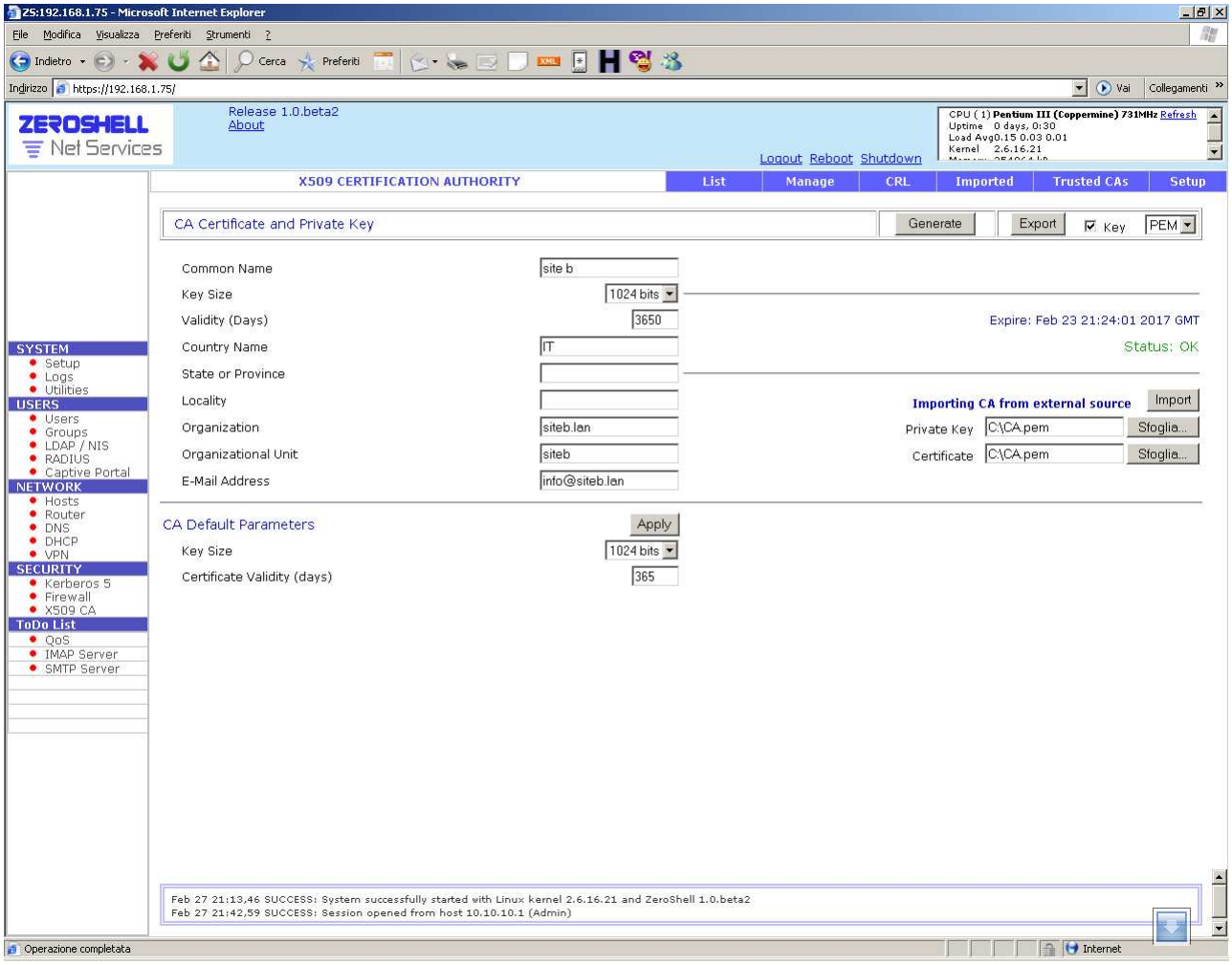
Nel menu "X509 CA", portarsi alla voce "SETUP":



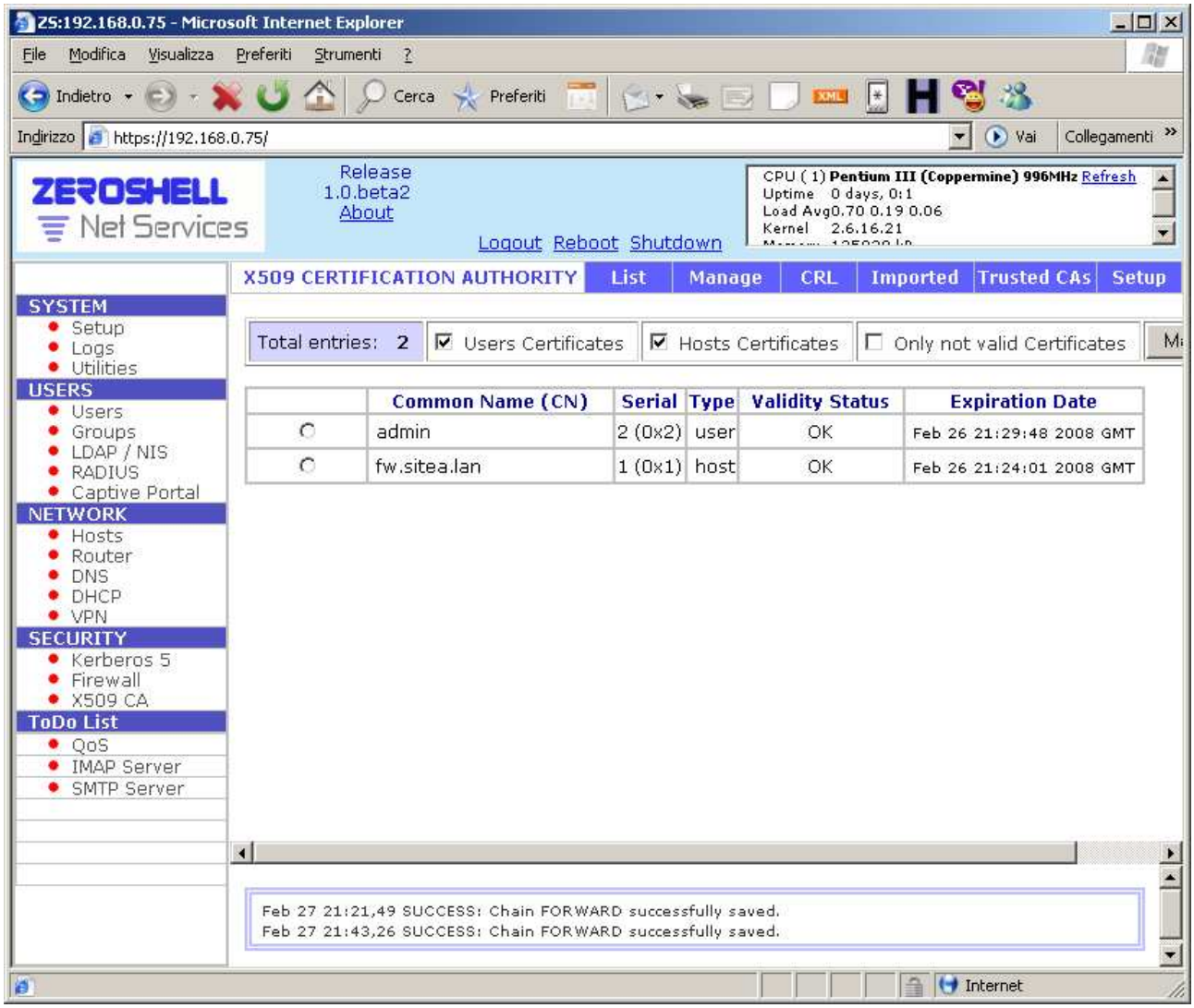
Compilare i campi e cliccando su "GENERATE" procedere con la creazione del certificato.
Fatto ciò, siamo pronti ad esportarlo in un file tramite il bottone "EXPORT":



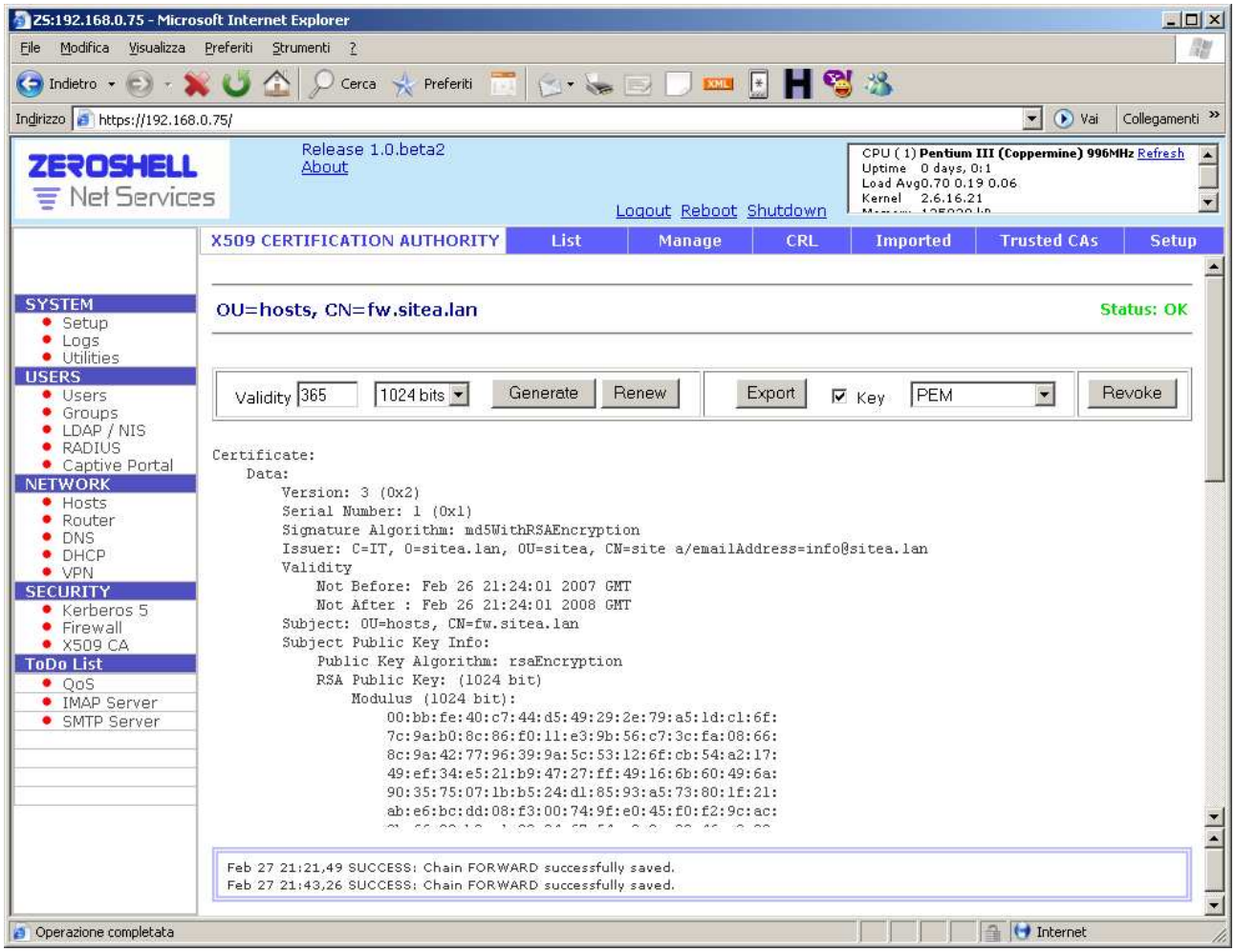
Questo file dovrà esssere importato nello stesso menu “X509 CA”dell’altro firewall alla voce “SETUP”:



Tramite i due bottoni “Sfoglia” selezionare il certifcato e poi cliccare su “Import”.
Fatto ciò, su entrambi i firewall nel menu “X509 CA”, portarsi alla voce “List”, verificare che le voci realtive al “Validity Status” siano OK.



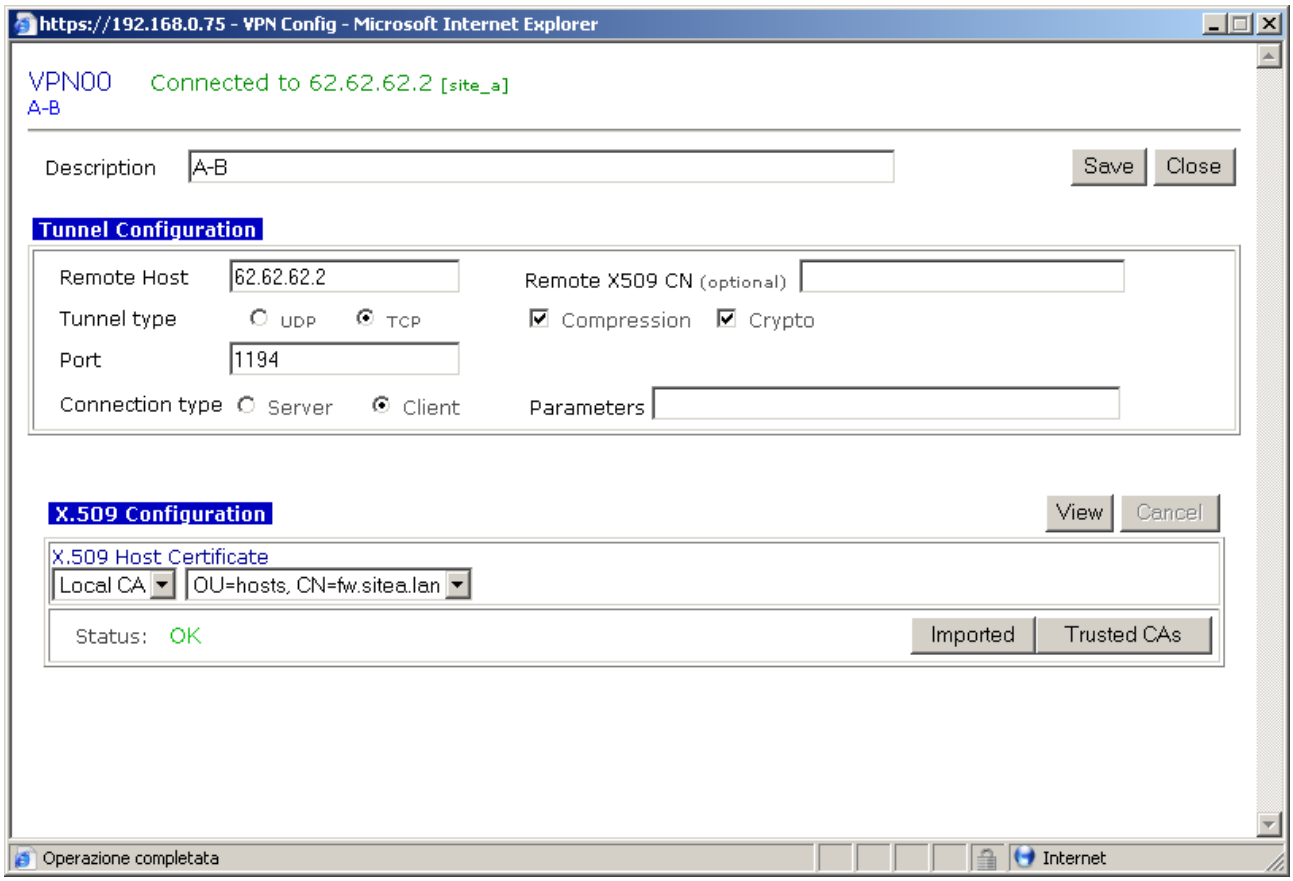
In caso contrario entrare in “manage” dopo aver selezionato l’host o lo user tramite bottone radio, revocare e rigenerare il certificato con i bottoni “Revoke” e “Regenerate”.


ZS:192.168.0.75 - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo https://192.168.0.75/
Vai Collegamenti
ZEROSHELL
Net Services
Release 1.0.beta2
About
Logout Reboot Shutdown
CPU (1) Pentium III (Coppermine) 996MHz Refresh
Uptime 0 days, 0:1
Load Avg0.70 0.19 0.06
Kernel 2.6.16.21
X509 CERTIFICATION AUTHORITY
List
Manage
CRL
Imported
Trusted CAs
Setup
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
SECURITY
Kerberos 5
Firewall
X509 CA
ToDo List
QoS
IMAP Server
SMTP Server
OU=hosts, CN=fw.sitea.lan
Status: OK
Validity 365
1024 bits
Generate
Renew
Export
Key
PEM
Revoke
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=IT, O=sitea.lan, OU=sitea, CN=site a/emailAddress=info@sitea.lan
Validity
Not Before: Feb 26 21:24:01 2007 GMT
Not After : Feb 26 21:24:01 2008 GMT
Subject: OU=hosts, CN=fw.sitea.lan
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:bb:fe:40:c7:44:d5:49:29:2e:79:a5:1d:c1:6f:
7c:9a:b0:8c:86:f0:11:e3:9b:56:c7:3c:fa:08:66:
8c:9a:42:77:96:39:9a:5c:53:12:6f:cb:54:a2:17:
49:ef:34:e5:21:b9:47:27:ff:49:16:6b:60:49:6a:
90:35:75:07:1b:b5:24:d1:85:93:a5:73:80:1f:21:
ab:e6:bc:dd:08:f3:00:74:9f:e0:45:f0:f2:9c:ac:
Feb 27 21:21,49 SUCCESS: Chain FORWARD successfully saved.
Feb 27 21:43,26 SUCCESS: Chain FORWARD successfully saved.
Operazione completata
Internet

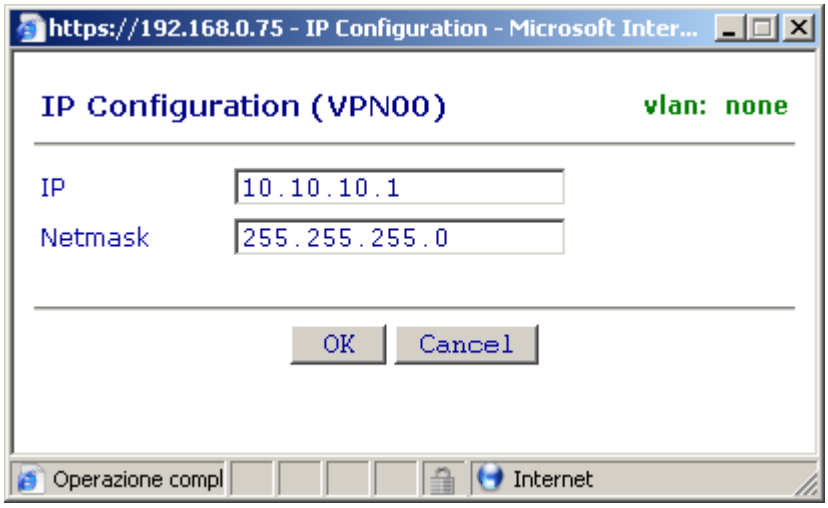
Creazione del tunnel vpn

Bene, ora possiamo fare in modo che logicamente i due firewall possano comunicare.
Sul Firewall del SiteA, portarsi nel menu SETUP alla voce NETWORK, cliccare sul bottone MAKE VPN:

SiteA:
Compilare i campi come segue, indicando una breve descrizione (A-B), l'host remoto al quale chiedere la comunicazione sicura (62.62.62.2 che è l'ip della rete pubblica del firewall di SiteB), il tipo di tunnel (TCP), se vogliamo possiamo modficare la porta standard (1194.. io lascio questa), la connection type dovrà essere da un lato client e dall'altro server (cleint), scelgo poi il Certificato locale di fw.sitea.lan (Local CA …) .

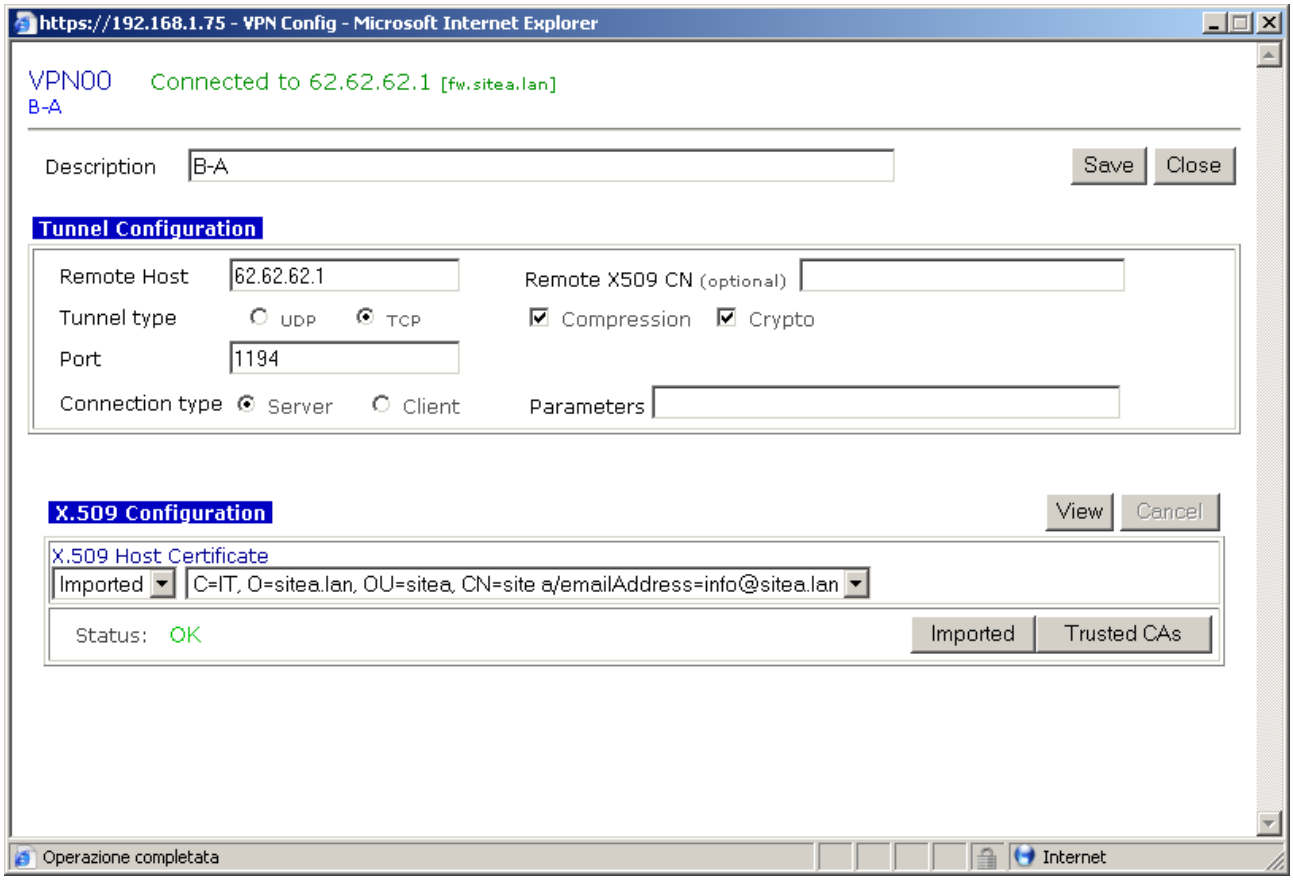


Una volta premuto il tasto Save, Open VPN si reinizzializza e vedremo la voce VPN00 fra le nostre schede di rete.
Selezionando il radio alla sinistra di VPN00, clicchiamo su ADD IP:

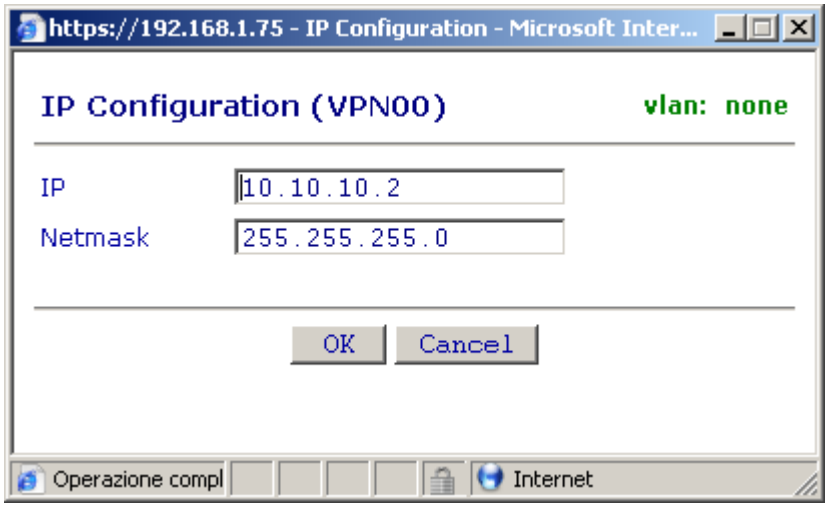


Qui dobbiamo inserire un ip di una rete non presente nelle nostre sedi; questa servirà esclusivamente ai due firewall per trasportare i pacchetti da una sede all'altra sul tunnel VPN. Io ho impostato il 10.10.10.1 in SiteA ed il 10.10.10.2 in SiteB.

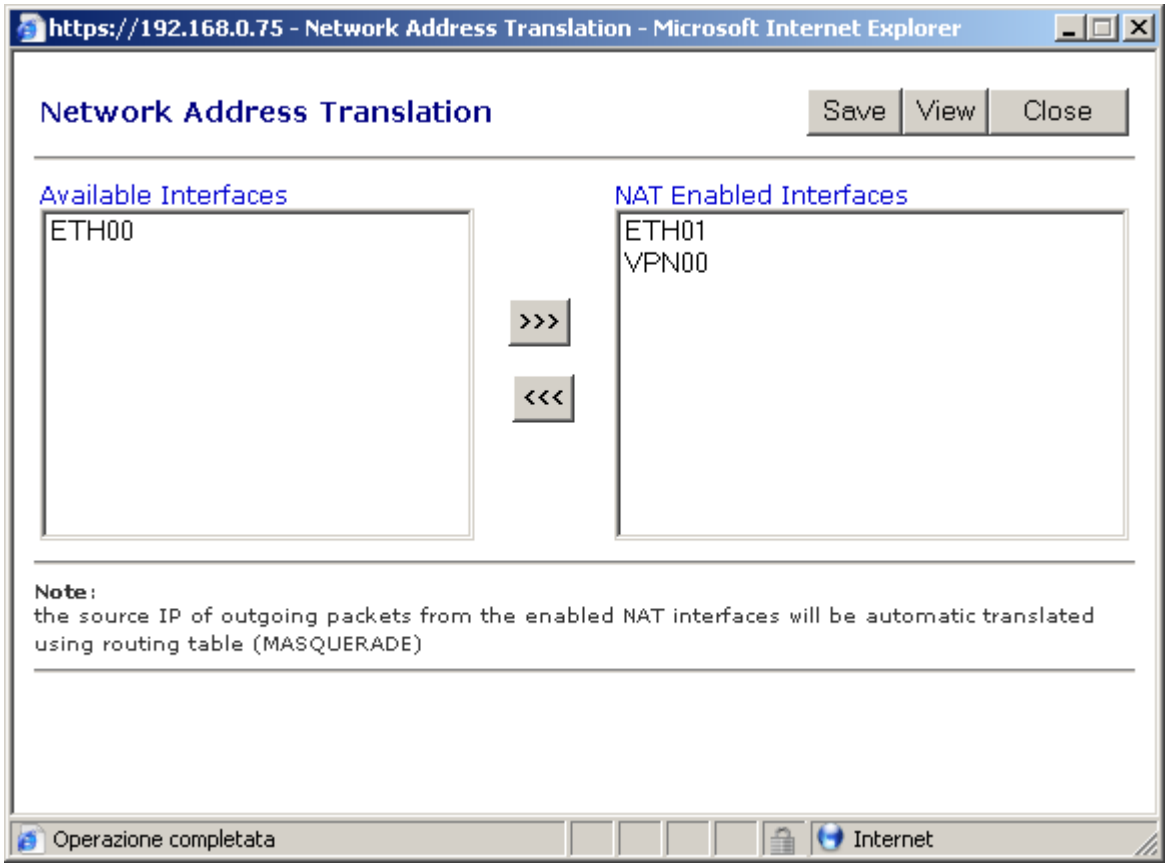
SiteB:
lo stesso lavoro svolto sul SiteA va fatto sul SiteB con alcuni accorgimenti:
Compilare i campi come segue, indicando una breve descrizione (B-A), l'host remoto al quale chiedere la comunicazione sicura (62.62.62.1 che è l'ip della rete pubblica del firewall di SiteA), il tipo di tunnel (TCP), se vogliamo possiamo modficare la porta standard (1194.. io lascio questa), la connection type dovrà essere da un lato client e dall'altro server (server), scelgo poi il Certificato importato di sitea.lan (imported …) .



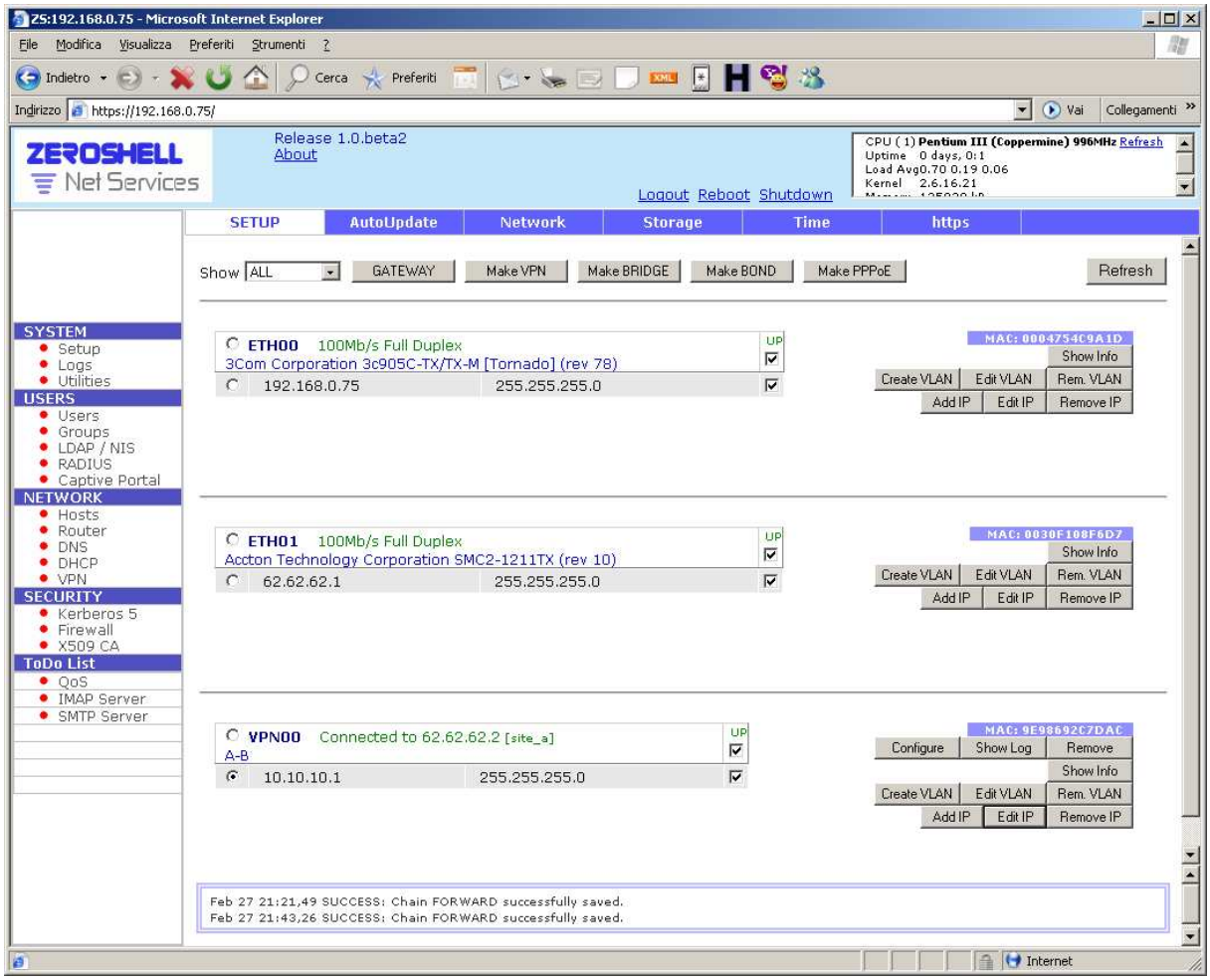
Una volta premuto il tasto Save, Open VPN si reinizzializza e vedremo la voce VPN00 fra le nostre schede di rete.
Selezionando il radio alla sinistra di VPN00, clicchiamo su ADD IP:



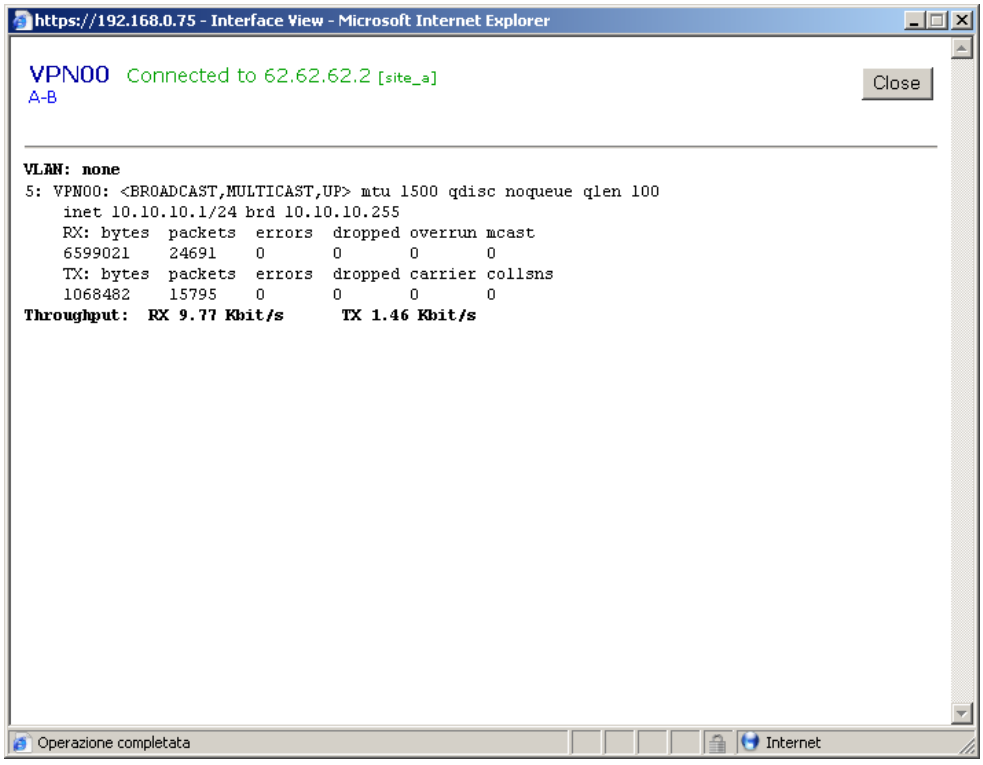
Verifichiamo che in ROUTER , alla voce NAT la situazione sia la seguente per entrambi i firewall:



Dovremmo a questo punto avere il tunnel attivo e funzionante:



Con un click su “Show Info” della VPN00 vediamo il traffico che passa sul tunnel se per esempio lanciamo un ping verso la sede remota:

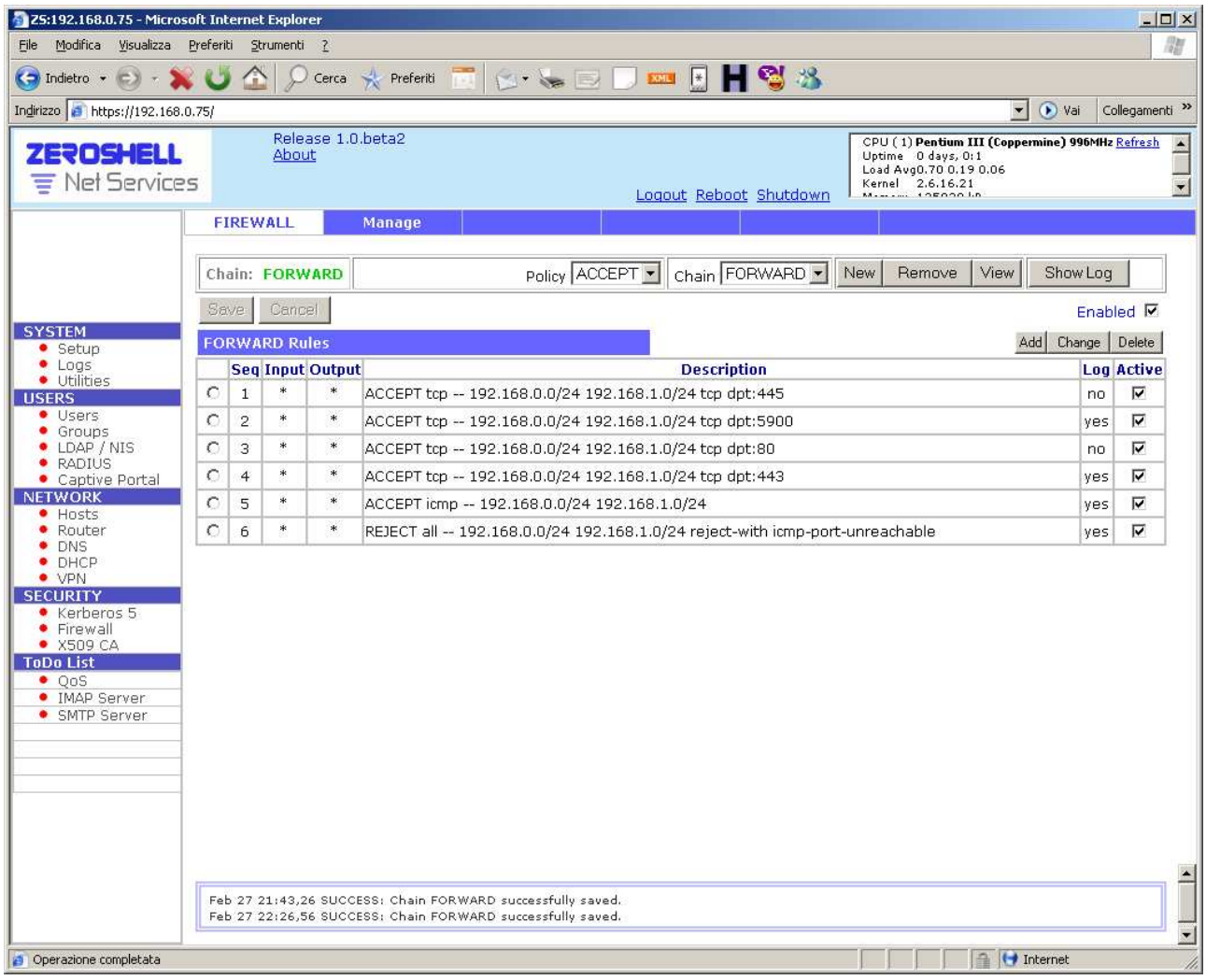


Filtri di sicurezza sul tunnel

A questo punto qualsiasi comunicazione può passare da una sede all'altra. Per motivi sempre legati alla sicurezza possiamo stabilire per esempio che dal SiteA al SiteB passino solo determinati tipi di richieste, per esempio:

il ping per verificare lo stato della connessione (ICMP)
accesso ad alcune cartelle condivise di windows (tcp 445)
assistenza remota con Tight VNC (tcp 5900)
consultazione di un server web (TCP 80 e TCP 443)

Ecco come nel menu FIREWALL dobbiamo intervenire:



	Seq	Input	Output	Description	Log	Active
○	1	*	*	ACCEPT tcp -- 192.168.0.0/24 192.168.1.0/24 tcp dpt:445	no	☑
○	2	*	*	ACCEPT tcp -- 192.168.0.0/24 192.168.1.0/24 tcp dpt:5900	yes	☑
○	3	*	*	ACCEPT tcp -- 192.168.0.0/24 192.168.1.0/24 tcp dpt:80	no	☑
○	4	*	*	ACCEPT tcp -- 192.168.0.0/24 192.168.1.0/24 tcp dpt:443	yes	☑
○	5	*	*	ACCEPT icmp -- 192.168.0.0/24 192.168.1.0/24	yes	☑
○	6	*	*	REJECT all -- 192.168.0.0/24 192.168.1.0/24 reject-with icmp-port-unreachable	yes	☑

Come si vede ho creato delle regole che vengono lette dall'alto verso il basso. In fondo ho messo la regola che blocca qualsiasi tipo di comunicazione dalla rete 192.168.0.0/24 alla 192.168.1.0/24. Tutto quello che sta sopra sono le richieste che invece dovranno passare. Teniamo presente che se dobbiamo gestire il firewall remoto, è opportuno che la porta tcp 443 debba essere aperta come nella mia quarta regola per esempio.

E' bene intervenire su entrambi i firewall e scrivere regole che vadano a tutelare le sedi in base alle necessità.