HOWTO: Use ZeroShell as a Radius server for Identity Based Networking Services (IBNS)

By Marco Battaglia CCNA – Cisco Firewall Specialist – Cisco VPN Specialist

ZeroShell can be obtained from:
http://www.zeroshell.net
Questo documento è stato redatto utilizzando ZeroShell version 1.0 beta 7 e un Cisco Catalyst 2950 switch (a seconda della versione dell'IOS) supportano i Radius server per user authentication.
E' possible utilizzare il Radius server per automatizzare i processi di assegnazione alle VLAN degli utenti in base allo username e password utlizzati.
Le parti interessate da configurare sono:

- Zeroshell: per la parte Radium e creazione utenti.
- Cisco IOS: implementazione dot1x.
- NIC: impostazioni specifiche sulla scheda di rete.

In questo scenario l'esigenza era quella di assegnare ad ogni utente una VLAN di appartenenza a seconda dell'ambito di lavoro (Amministrazione, commerciali…) senza la necessità di dover muovere le plug sullo switch o entrare nella configurazione dello stesso per fare a mano la configurazione.

Quella che segue è una configurazione di base da prendere come esempio per poter abilitare l'autenticazione dot1x. (Ovviamente poi a seconda delle esigenze sono necessarie delle customizzazioni della configurazione).
Configurazione (per questo test è stato utilizzato uno switch Cisco Catalyst 2950 con IOS 12.1(22)EA4:

```
(config)aaa new-model
(config)aaa authentication dot1x default group radius local
(config)aaa authorization network default group radius local
(config)radius-server host ZeroshellIP auth-port 1812 acct-port 1813 key cisco
(config)dot1x system-auth-control
(config-if)interface FastEthernet0/2
(config-if)switchport mode access
(config-if)speed 100
(config-if)duplex full
(config-if)dot1x port-control auto
(config-if)dot1x max-req 10
(config-if)dot1x reauthentication
```

Ovviamente è necessario creare le VLAN che vi occorrono:

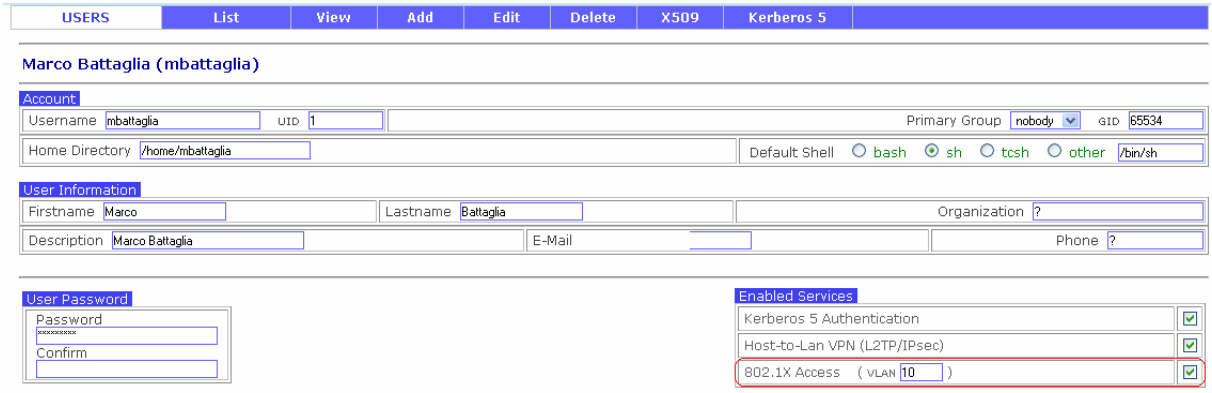
```
sw1prova#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

(vlan)#vlan 30 name dot1xtest3
VLAN 30 added:
    Name: dot1xtest3
```

Per Zeroshell ip ovviamente si intende l'ip del vostro server Zeroshell.

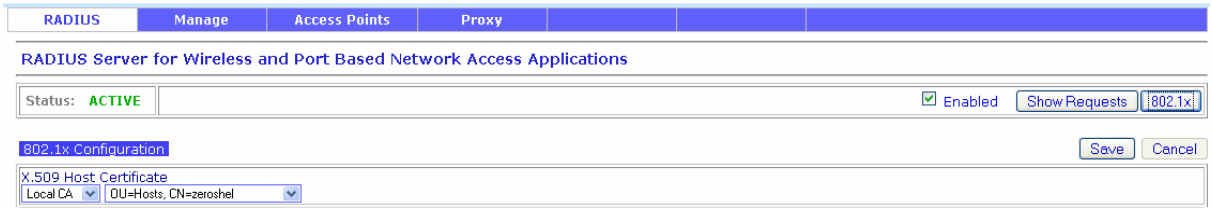
Ovviamente è necessario configurare Zeroshell per puntare al vostro database e non utilizzando quello di esempio pre-installato in Zeroshell.

Configurazione:
Per configurare Zeroshell per rispondere alle vostre richieste radius, come prima cosa bisogna aggiungere un utente:

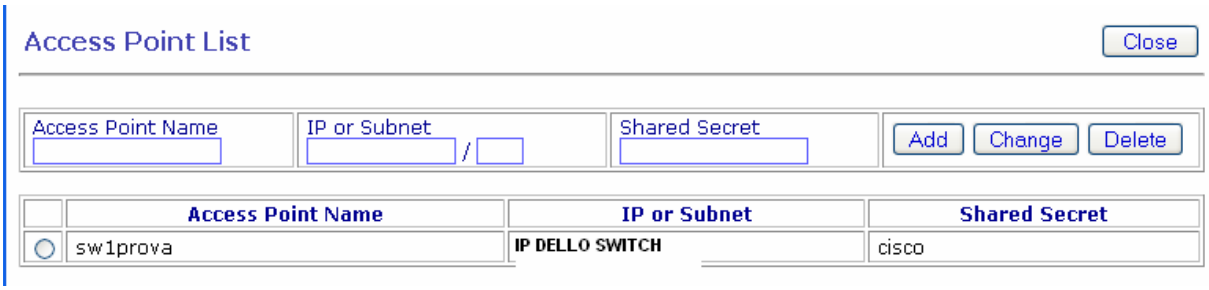


Come potete vedere ho già in questa fase inserito in che VLAN l'utente dovrà finire una volta inserite le credenziali corrette.

A questo punto bisogna abilitare il server Radius di Zeroshell:



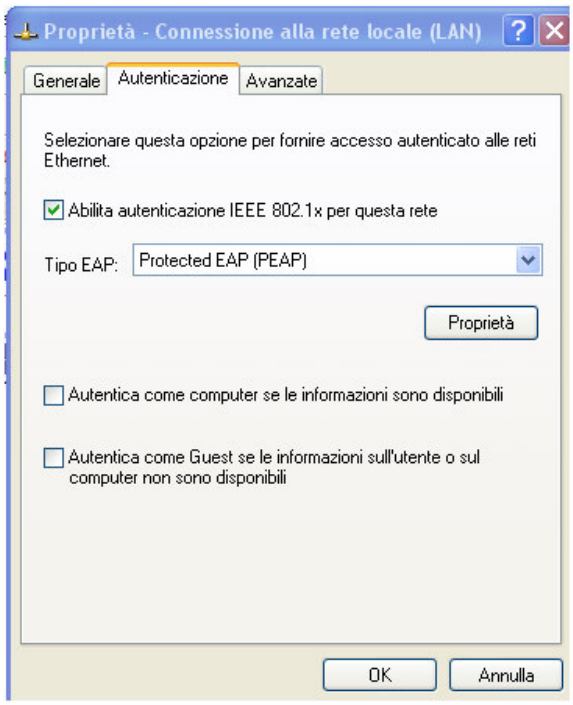
Adesso cliccando sul tasto Access Points Dobbiamo indicare l'ip e la shared key che permette la comunicazione tra lo switch ed il server radius:

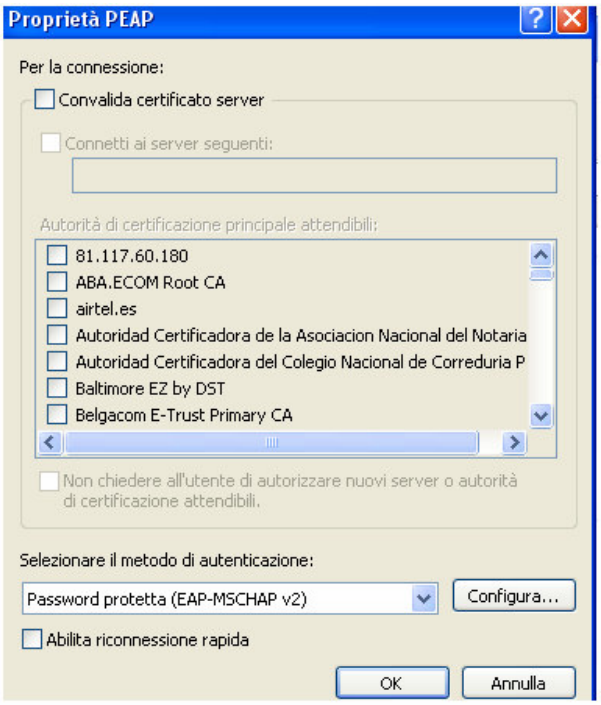


I dati necessari sono come potete notare:
- Nome dello switch
- Indirizzo ip e subnet
- La shared secret che avete inserito prima nello switch alla riga:

```
(config)radius-server host ZeroshellIP auth-port 1812 acct-port 1813 key cisco
```

Ora non resta che configurare la scheda di rete (in questo esempio il client è winxp SP2, e viene configurate mediante Protected EAP) in questo modo:



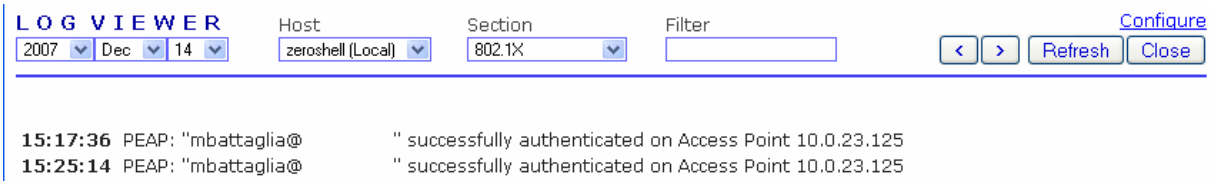


A questo punto non vi resta che collegare il cavo di rete e se tutto è configurato correttamente vi verrà proposta una schermata di autenticazione (si apre un pop-up sopra la scheda di rete in basso a dx).
Per verificare il corretto funzionamento:

Sullo switch date uno show vlan e vedrete che la porta su cui siete connessi entrerà a far parte della VLAN assegnata prima.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                                Fa0/9, Fa0/10, Fa0/11,Fa0/12
10   testdot1x                        active    Fa0/2
```

E nei log del dot1x dovreste vedere questo:



Questo vuole solo essere una guida indicativa, ovviamente sono possibili “infinite” combinazioni di configurazioni e tuning sull’apparato.