Zeroshell come Captive Portal per l'accesso ad IDEM

Fulvio Ricciardi

INFN Lecce

IDEM DAY - Bologna 10 Novembre 2011

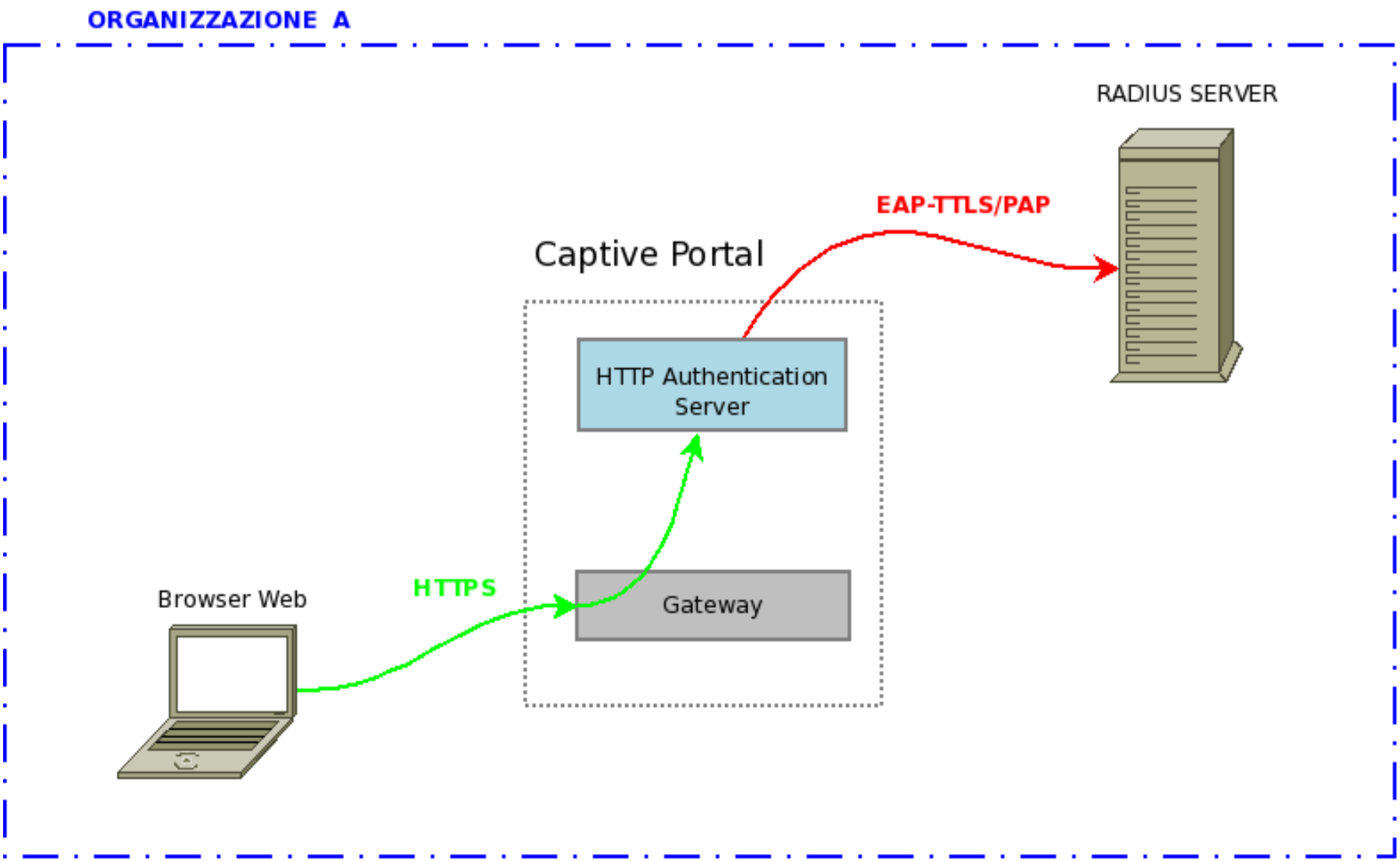
Gli argomenti trattati

- Proteggere la rete tramite Captive Portal
  - Vantaggi e svantaggi
  - L'accesso federato
  - I nemici del Captive Portal
- Cosa è Zeroshell?
- Il Captive Portal di Zeroshell
  - Configurazione e funzionalità
  - Configurazione come Shibboleth SP

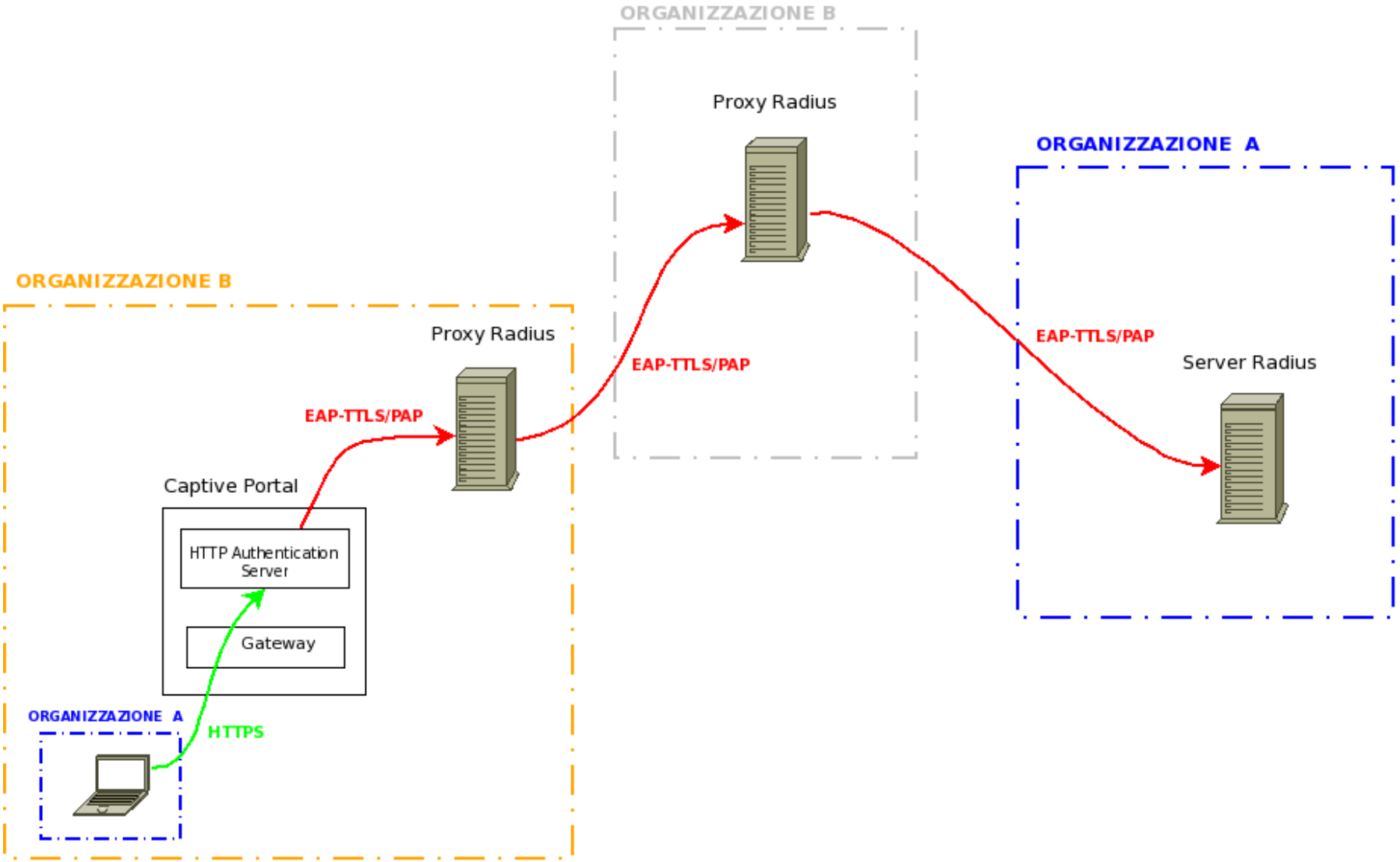
Definizione di Captive Portal

- E’ un gateway di livello 2 o 3 che unisce due segmenti di rete
  - I client che si associano al primo segmento ottengono subito connettività IP, ma non possono comunicare con il secondo segmento se non si autenticano
  - Le richieste http/https dei client non autenticati vengono redirette verso un portale di autenticazione in cui l’utente deve dimostrare la propria identità

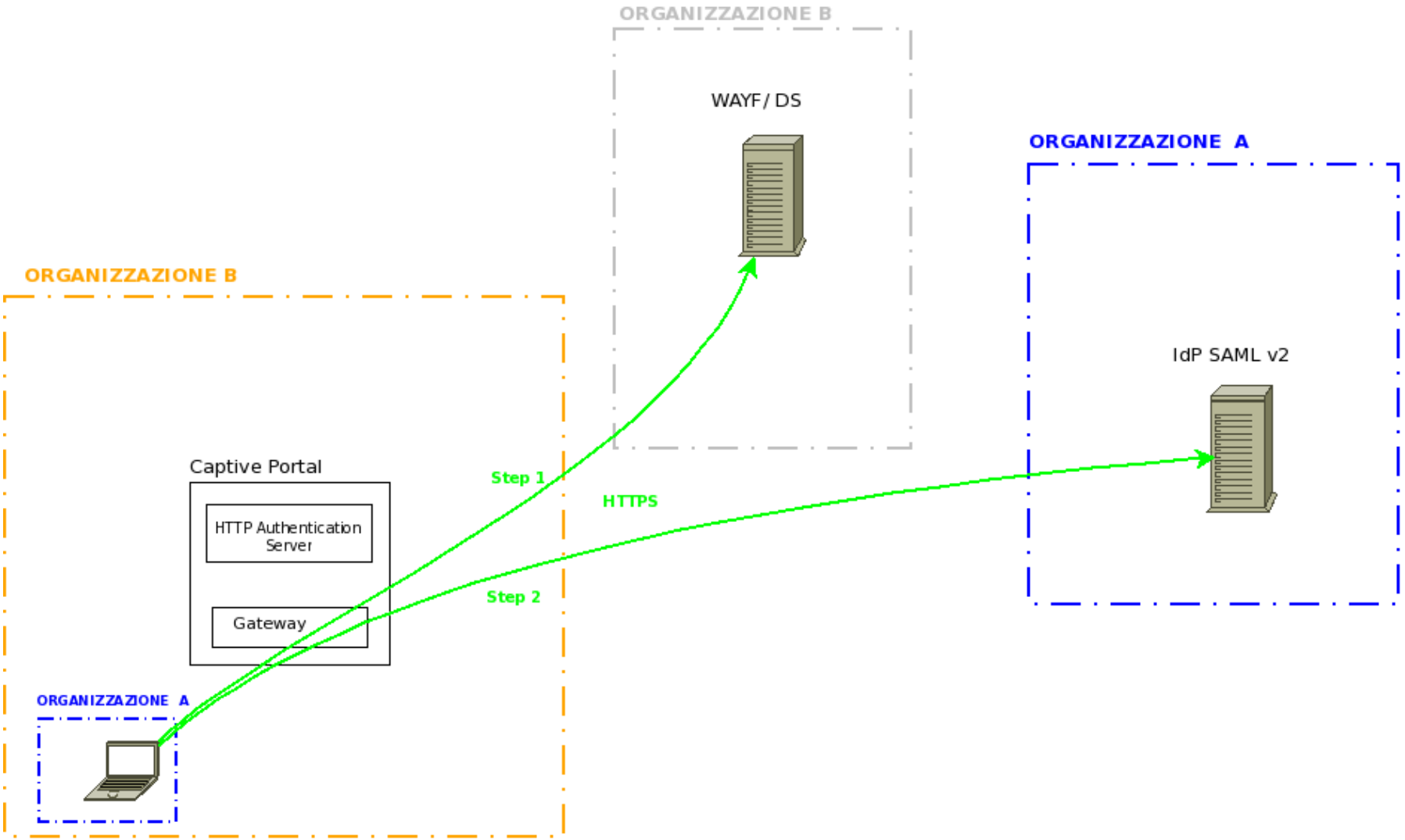
Captive Portal Standalone



Captive Portal Federato tramite Proxy Radius (bassa sicurezza)



Captive Portal Federato SAML v2 (Autenticazione End-to-End)

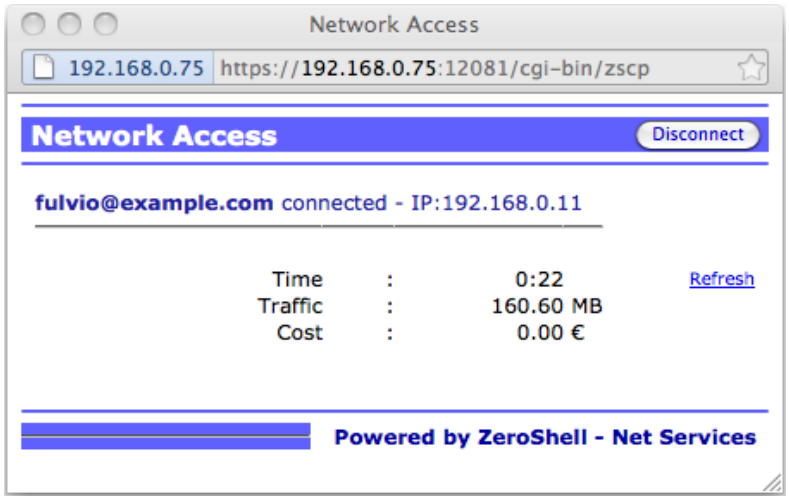


I nemici del Captive Portal

- MAC e IP spoofing nel tentativo di ottenere l'accesso fraudolento alla rete al posto di un utente autenticato
- DoS causati da client non ancora autenticati che utilizzano le porte 80 e 443 in maniera impropria per superare il firewall (es. Skype e altri P2P)
- DoS causati da client non ancora autenticati che tentano gli update del Sistema Operativo o delle signature dell'antivirus via HTTP
  - Nel caso di federazione SAML il DoS diventa un DDoS verso il WAYF

Finestra Network Access e il segreto condiviso

- Per rendere inefficace il MAC e IP spoofing è necessario che Client e Captive Portal condividano un segreto: ***Authenticator***



- L'Authenticator ha una durata limitata (1 minuto o più)
- La finestra Popup si preoccupa di rinnovare l'Authenticator prima che scada
- Se l'Authenticator scade il Captive Portal disconnette l'utente

Come è custodito e rinnovato l'Authenticator

- Il campo ***Authenticator*** contenuto nel codice HTML della finestra Popup è il segreto condiviso tra il Client e Captive Portal:

```
<input type=hidden name=Authenticator
value="U2FsdGVkX1HYuOsP4UNR1R8gPP1dtfJs8dULujxPrLw86Ok/
9KW1jjK1oIjs2sX e6vxU3sLujFos/kOaJf2mQ==">
```

- Il Captive Portal genera e successivamente rinnova l'Authenticator con il seguente codice bash:

```
echo -e "$USER@$REALM\n$IP\n$TIMESTAMP\n$TYPE" |
openssl aes-256-cbc -e -a -k "$SECRET"
```

- *La finestra Popup manda periodicamente l'Authenticator al Captive Portal per il rinnovo. L'Authenticator rinnovato non è mai uguale al precedente poiché il TIMESTAMP cambia.*

Limitare problemi di Denial of Service

- Per le connessioni sulle porte 80 e 443 TCP che **non contengano richieste HTTP/ HTTPS** l'unica limitazione possibile è a livello di Kernel (Netfilter in Linux):

```
Chain CapPortHTTPS (1 references)
target     prot opt source               destination
ACCEPT     all  --  192.168.0.101        0.0.0.0/0           MAC 12:2D:31:A0:66:B1
REDIRECT   tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02 limit:
avg 50/min burst 10 mode srcip redir ports 12081
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
REDIRECT   tcp  --  0.0.0.0/0            0.0.0.0/0           redir ports 12081
```

- Per le connessioni sulle porte 80 e 443 TCP che **contengano richieste HTTP/HTTPS** come le richieste di update del Sistema Operativo e dell'Antivirus si può agire a livello applicativo nel web server:

```
RewriteCond %{REQUEST_URI} !/msdownload/update
RewriteCond %{REQUEST_URI} !/windowsupdate/
RewriteCond %{REQUEST_URI} !/ubuntu/dists/
RewriteCond %{REQUEST_URI} !/daily-.*.cdiff
RewriteRule ^.*$ https://%{SERVER_ADDR}:12081/cgi-bin/zscp?
Section=CPAuth&Action=Show&ZSCPRedirect=%{SERVER_NAME}:::https://%{SERVER_NAME}%
{REQUEST_URI}?${filter:%{QUERY_STRING}} [L]
```

Confronto tra Captive Portal con autenticazione SAML e 802.1x

- Il Captive Portal non ha bisogno di nessuna configurazione lato client
- I supplicant 802.1x sono complicati da configurare e inadatti per l'utente occasionale
- In ambienti federati mediante 802.1x l'autenticazione più utilizzata è EAP-TTLS con PAP, ma il supplicant nativo di Windows non supporta EAP-TTLS
- 802.1x offre supporto per lo scambio di chiavi di cifratura che possono essere usate per criptare il Layer 2 come nel caso di WPA/WPA2 Enterprise

Cosa è Zeroshell?

- E' una distribuzione Linux che fornisce i principali servizi di rete
- Configurabile via web
  - Il nome Zero-Shell (Senza-Shell) significa che la configurazione dovrebbe avvenire esclusivamente via Web. L'accesso alla shell è comunque possibile
- I siti web sono:
  - http://www.zeroshell.net/ (Italiano)
  - http://www.zeroshell.net/eng/ (Inglese)

I principali servizi offerti da Zeroshell

- Routing e Bridging con supporto delle VLAN 802.1q
- Firewall con supporto per i filtri Layer 7
- Traffic Shaping e QoS assegnando banda massima, banda garantita e priorità in base alla tipologia di traffico
- Load Balancing e Failover dei collegamenti WAN
- VPN site-to-site con OpenVPN (TAP)
- VPN gateway per accessi Host-to-LAN (OpenVPN e IPSec/L2TP)
- Captive Portal con backend di autenticazione Kerberos 5, RADIUS, certificati X.509 e SAML v2 mediante Shibboleth
- Proxy HTTP trasparente con scansione antivirus delle pagine web
- Server LDAP, Kerberos 5, RADIUS con accounting, DNS e DHCP
- Access Point Wi-Fi con supporto per Multiple SSID

Scelta del download più appropriato

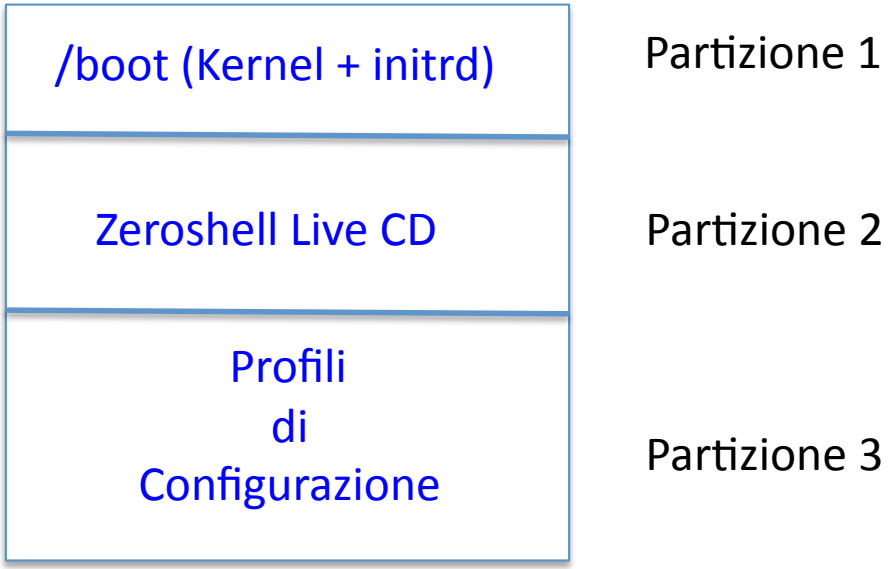
http://www.zeroshell.net/download/

- ***ZeroShell-1.0.beta16.iso*** (Live CD)
- ***ZeroShell-1.0.beta16-CompactFlash-IDE-USB-SATA-1GB.img.gz*** (immagine generica da installare su HD o Flash USB)
  - *gunzip –c ZeroShell-1.0.beta16-CompactFlash-IDE-USB-SATA-1GB.img.gz > /dev/sdx*
  - Physdiskwrite da Windows
- ***ZeroShell-1.0.beta16-ALIX-CompactFlash-1GB.img.gz*** (Immagine per dispositivi embedded come Alix o Soekris che utilizzano la porta seriale)
- ***ZeroShell-1.0.beta16-VMWARE.zip*** (Macchina Virtuale VMWare)

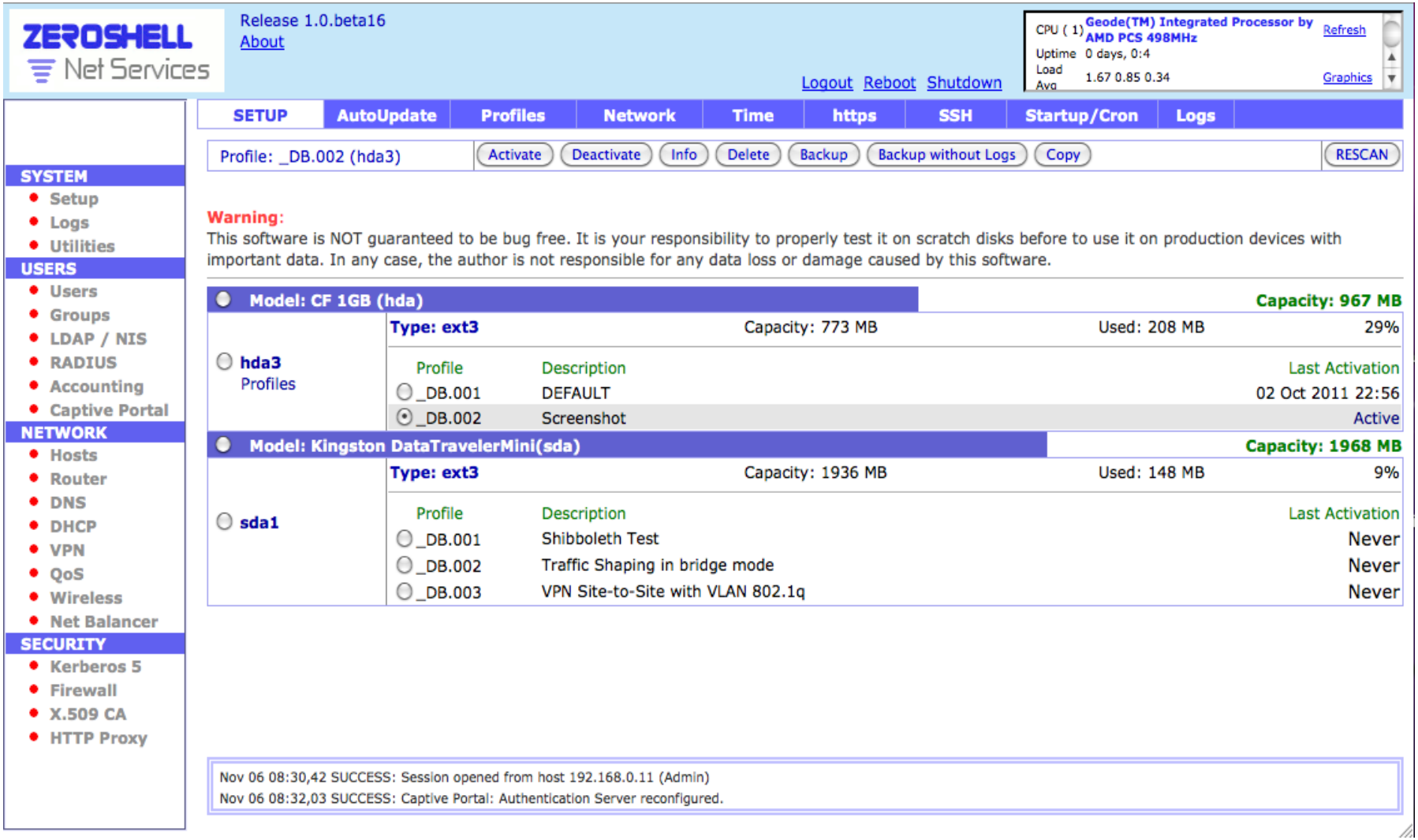
Read-Only e No-Devel per una maggiore sicurezza

- La partizione contenente Zeroshell è sempre una ISO9660
- Vengono rimossi gli header delle librerie e i tool di sviluppo
- Esistono distribuzioni non ufficiali in Read-Write e con i compilatori

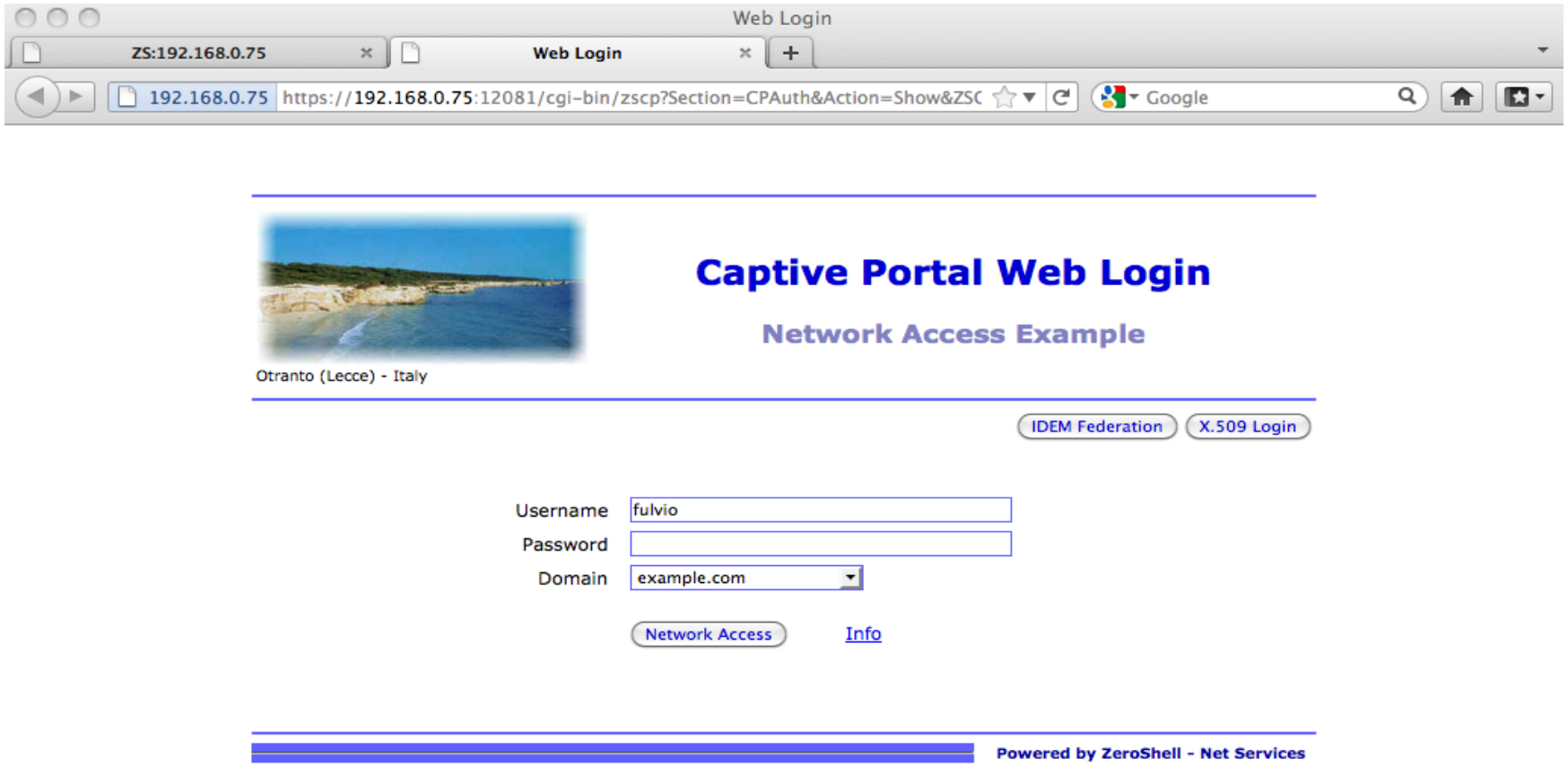
Installazione su Hard Disk o Flash USB



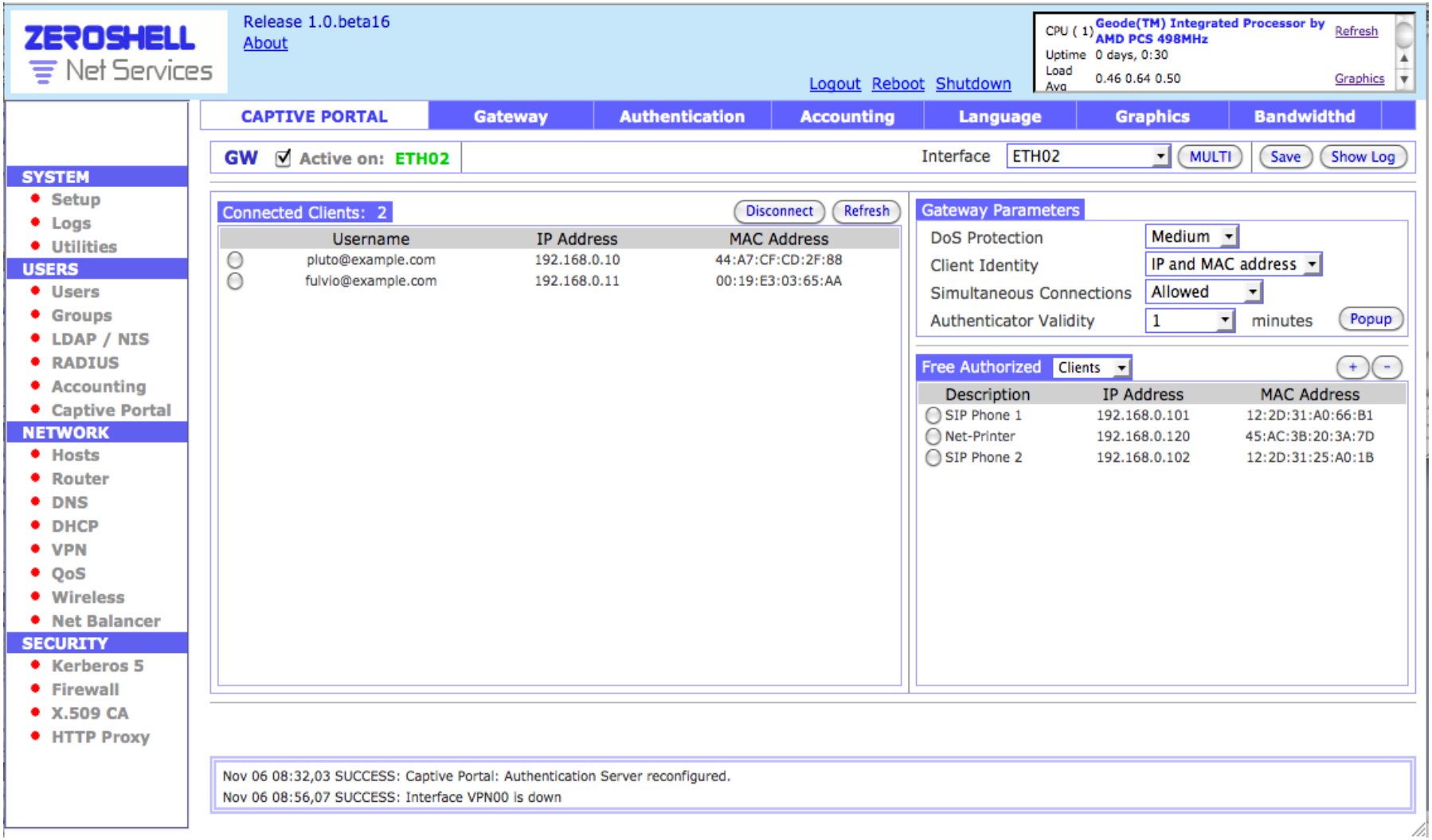
Gestione dei Profili di Configurazione



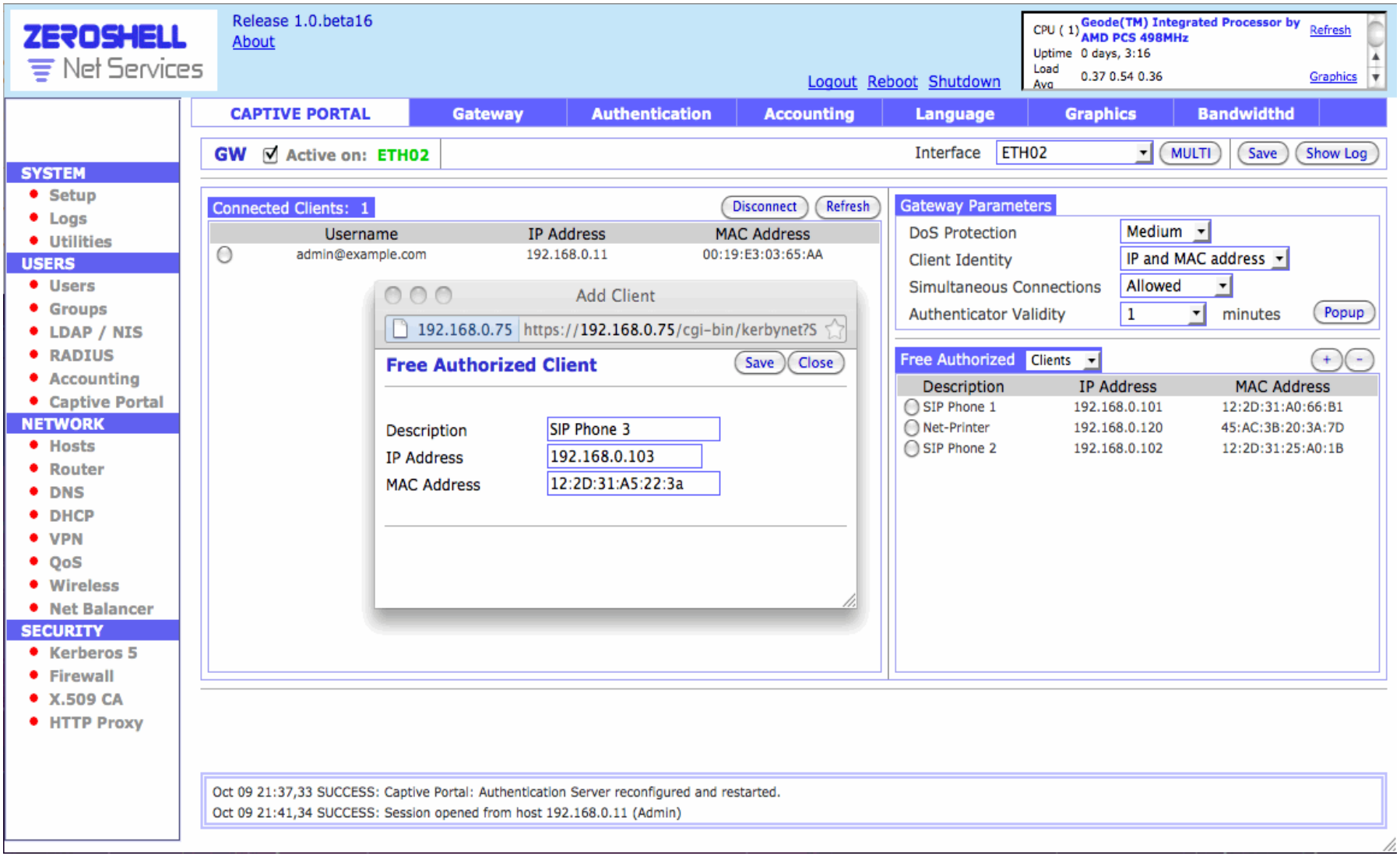
Web Login Page



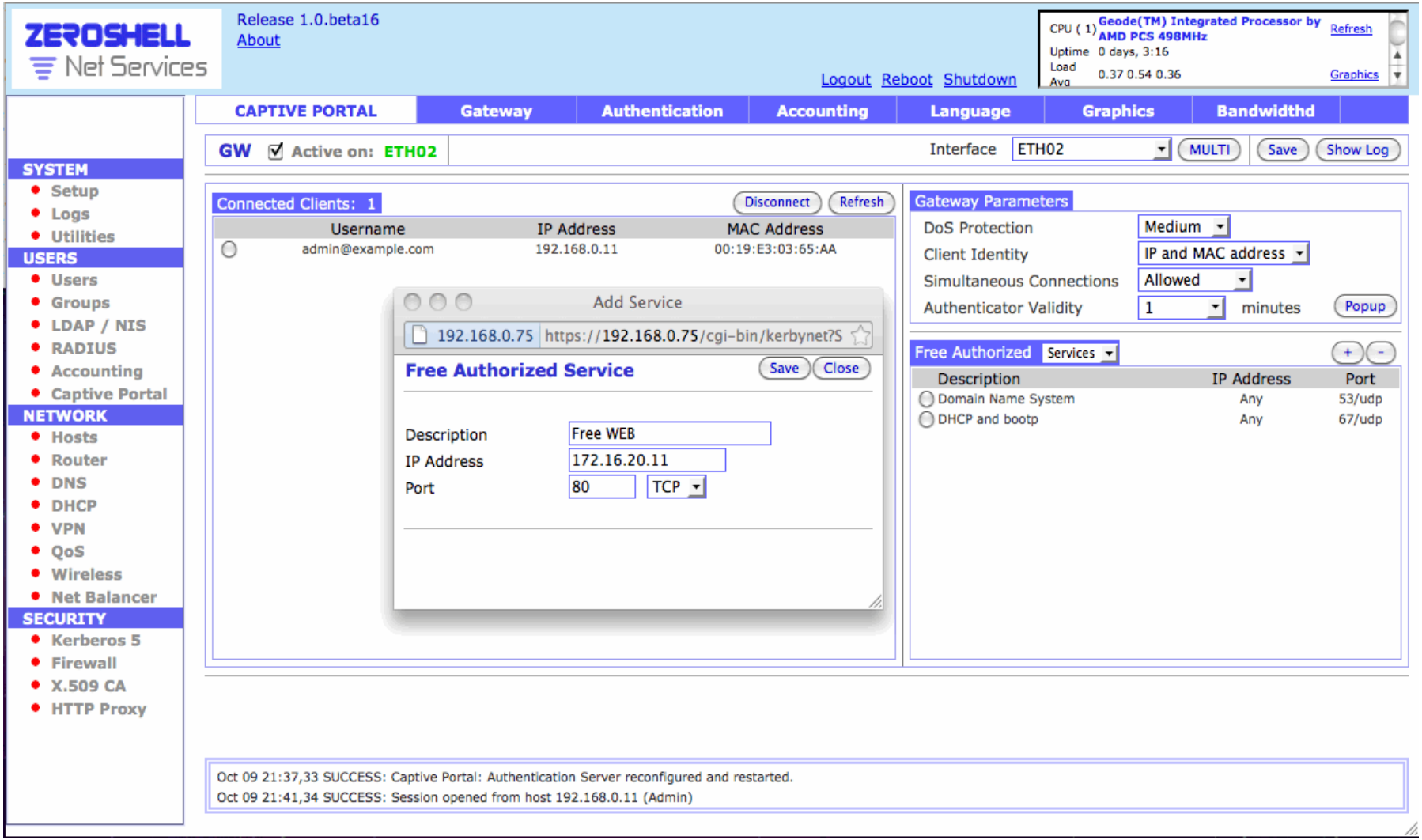
Captive Portal Gateway Configuration



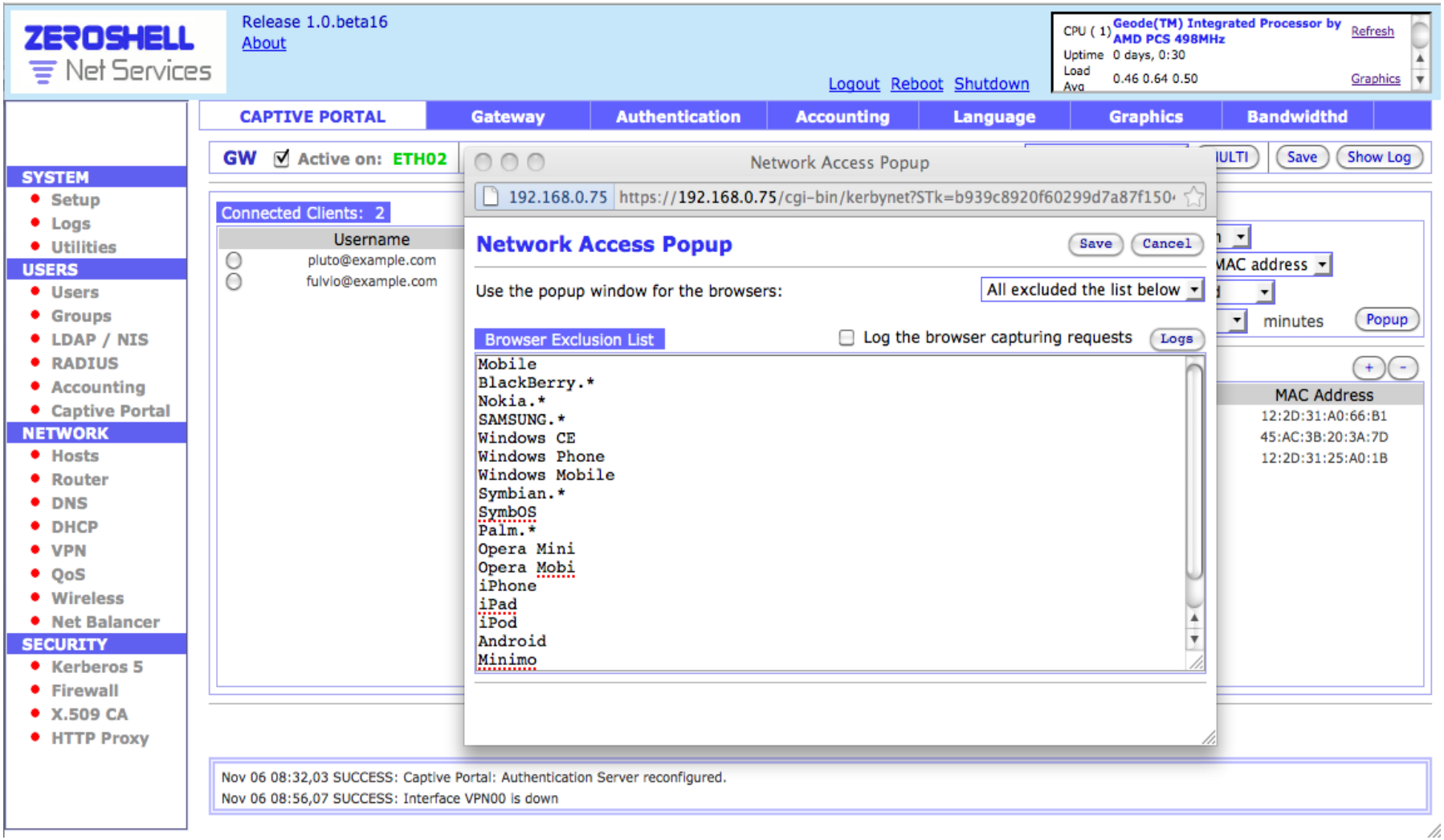
Free Authorized Clients



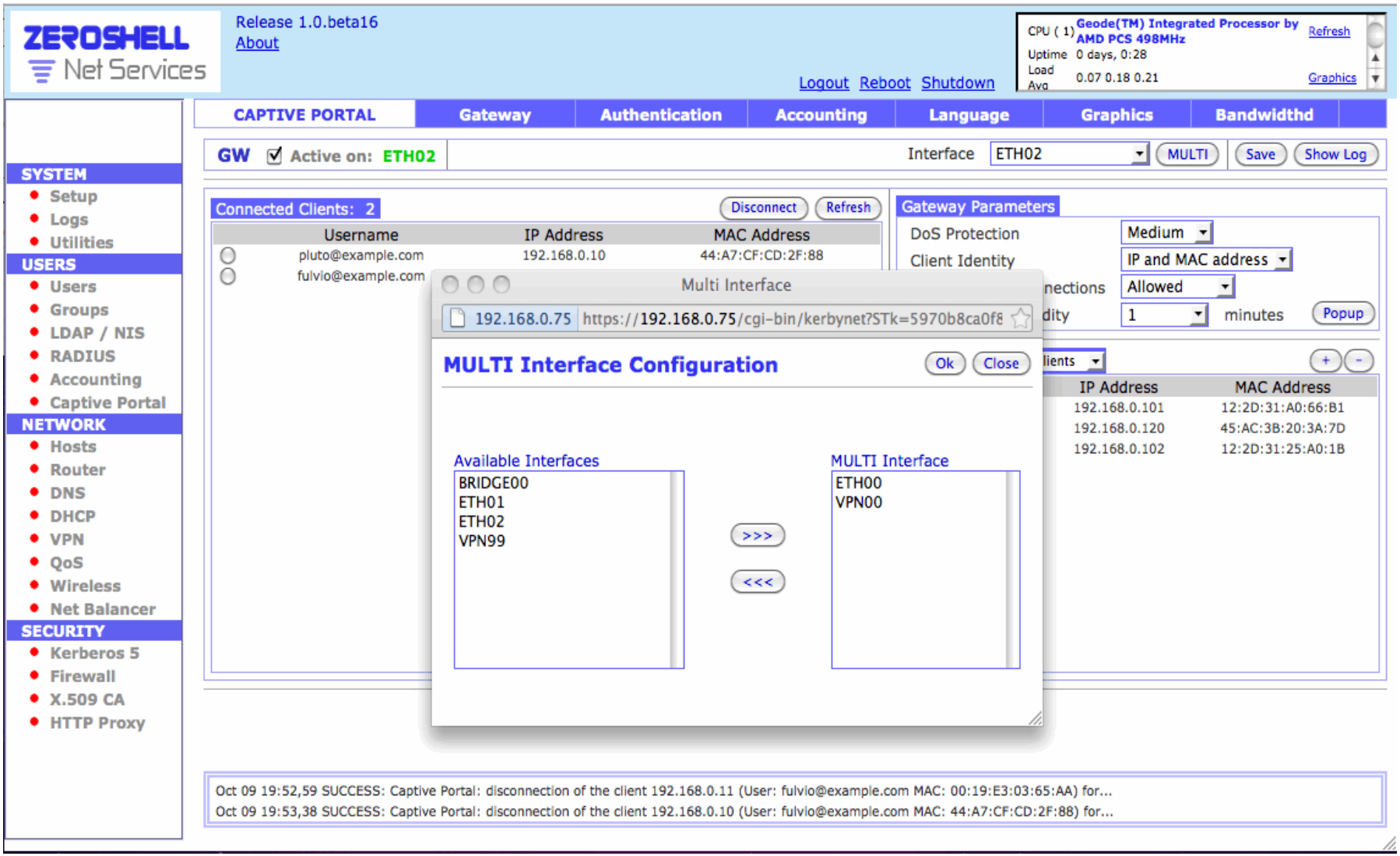
Free Authorized Services



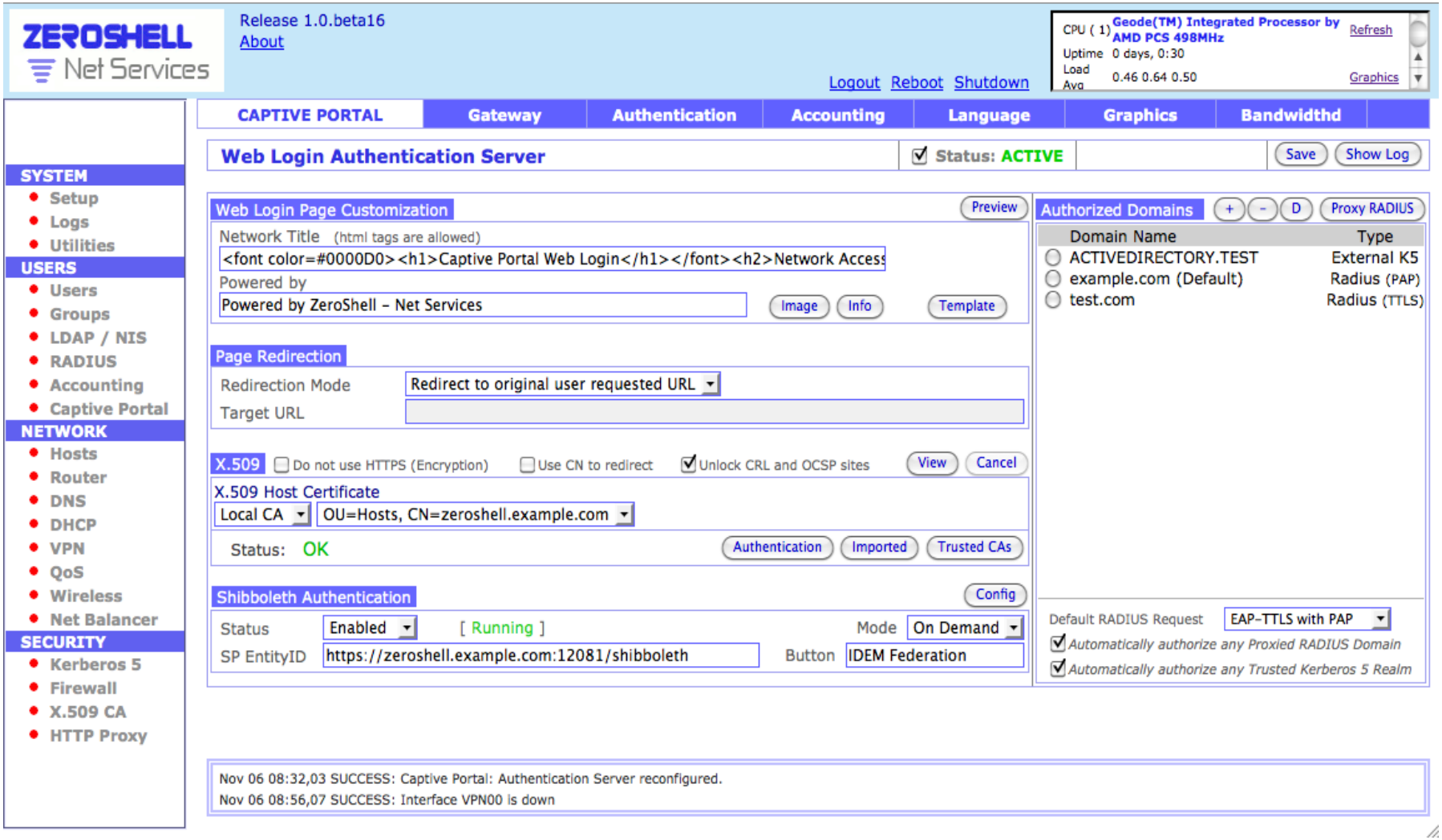
Network Access Popup for Mobile Devices



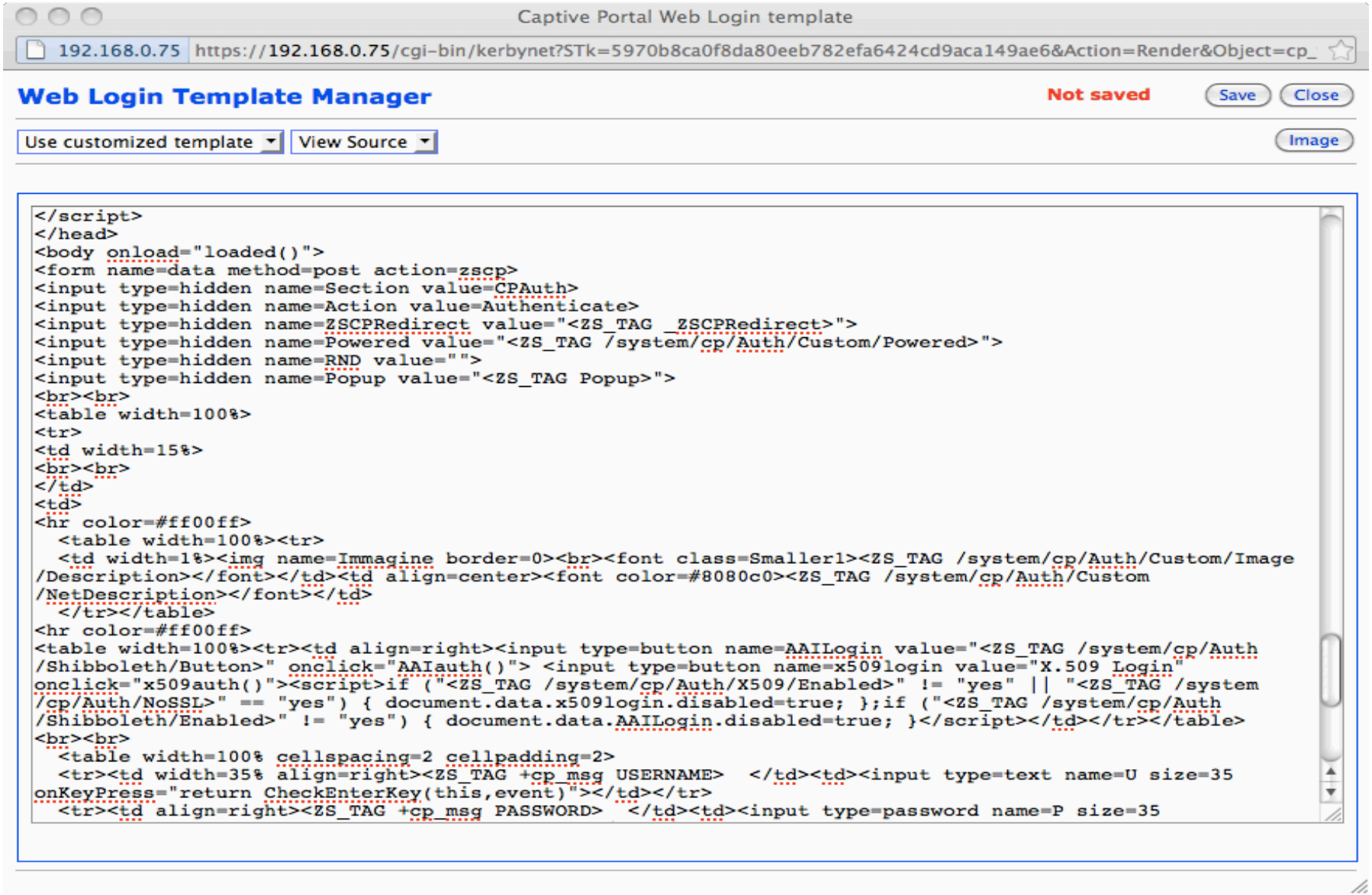
Multi Network Interface Configuration (Routing/Bridging)



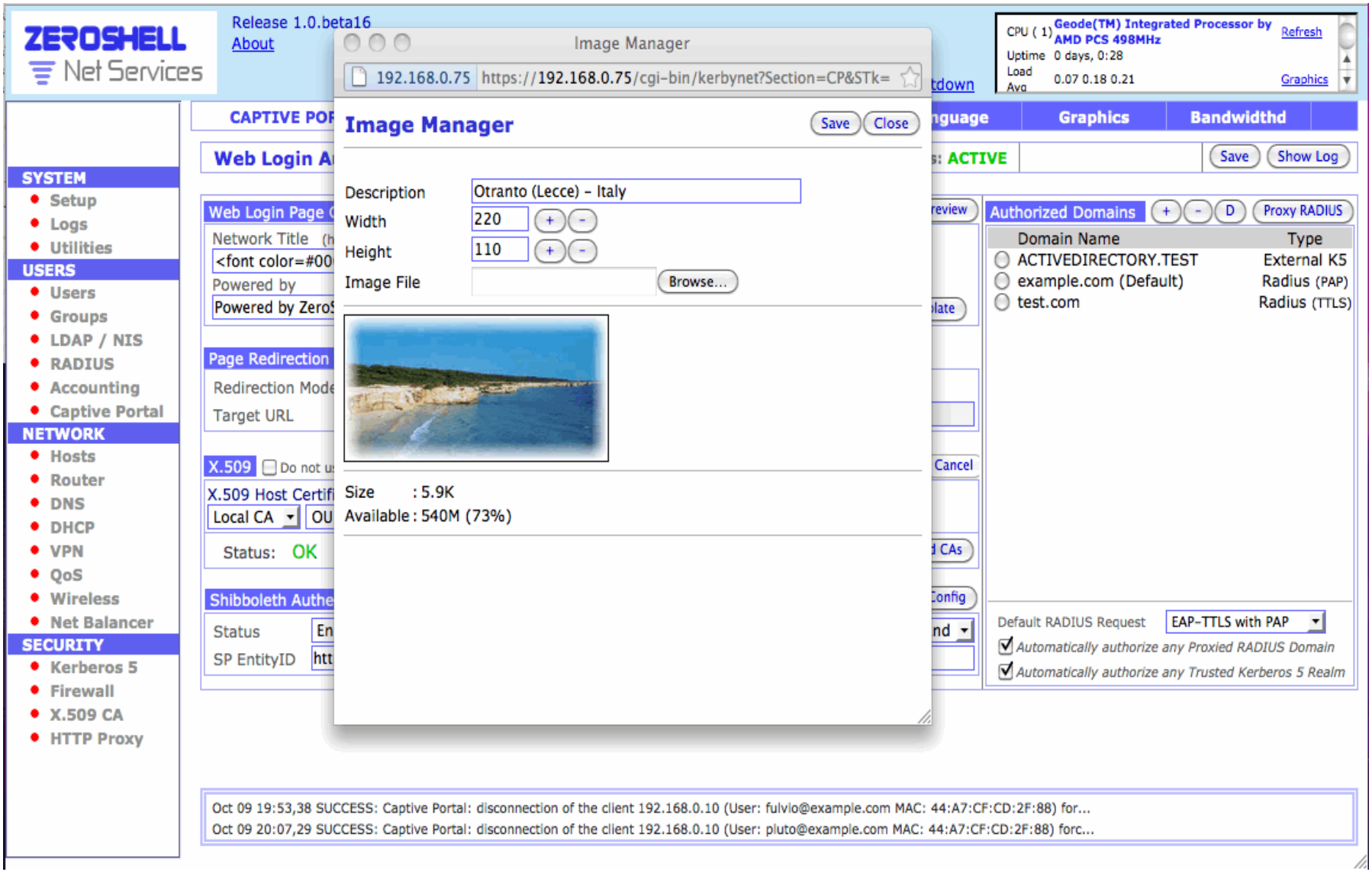
Captive Portal Authentication Configuration



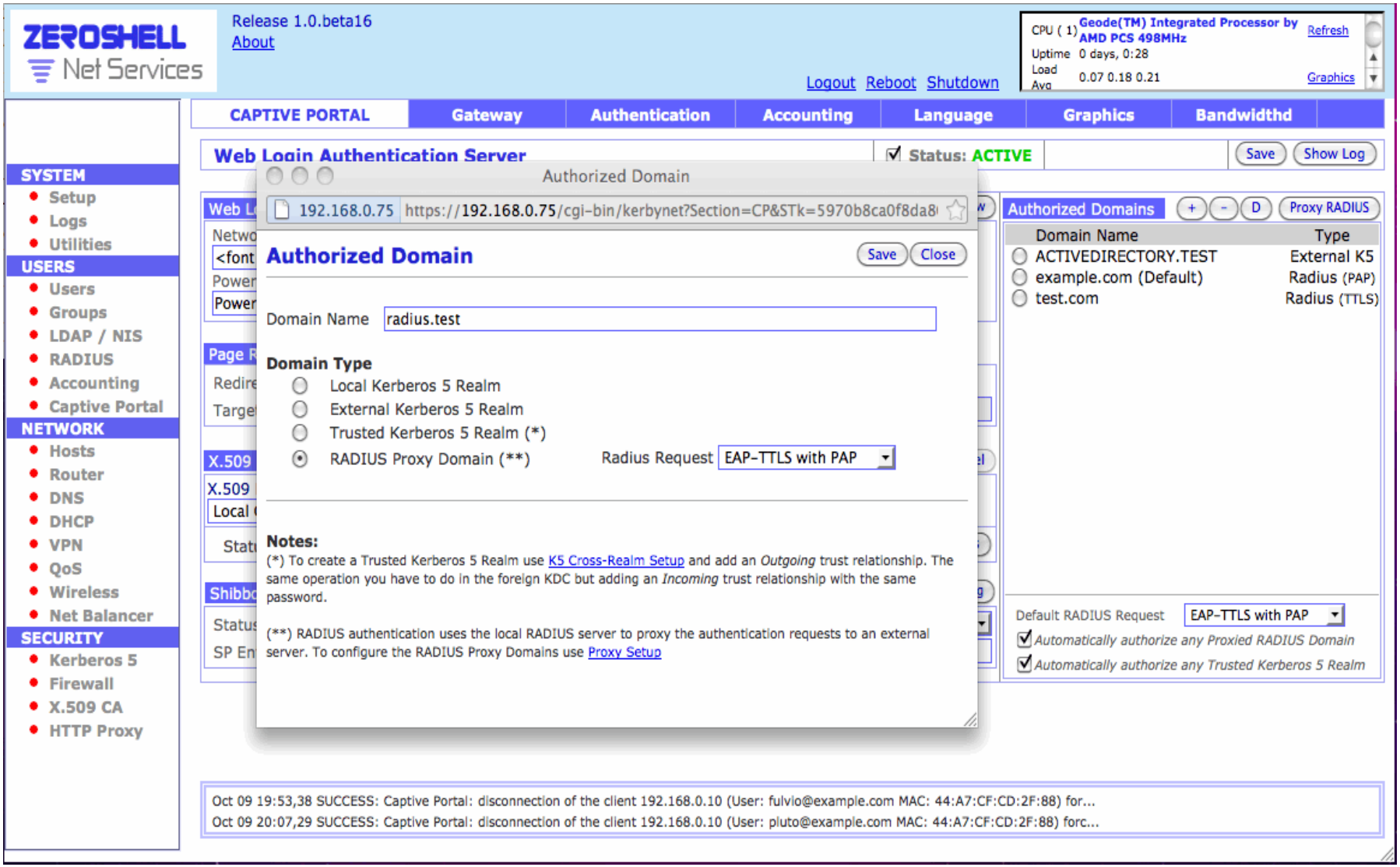
Captive Portal Template Manager



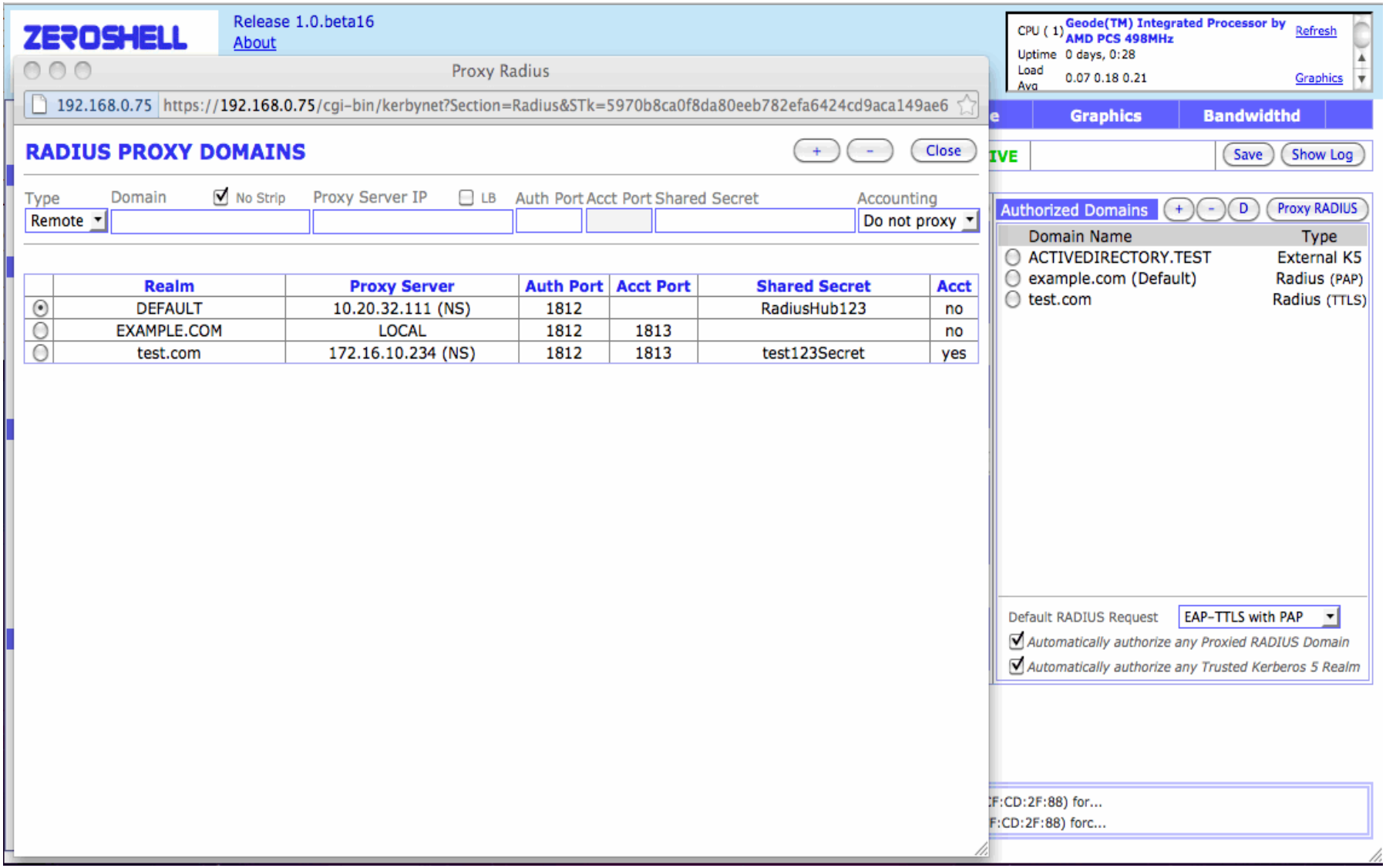
Captive Portal Image Manager



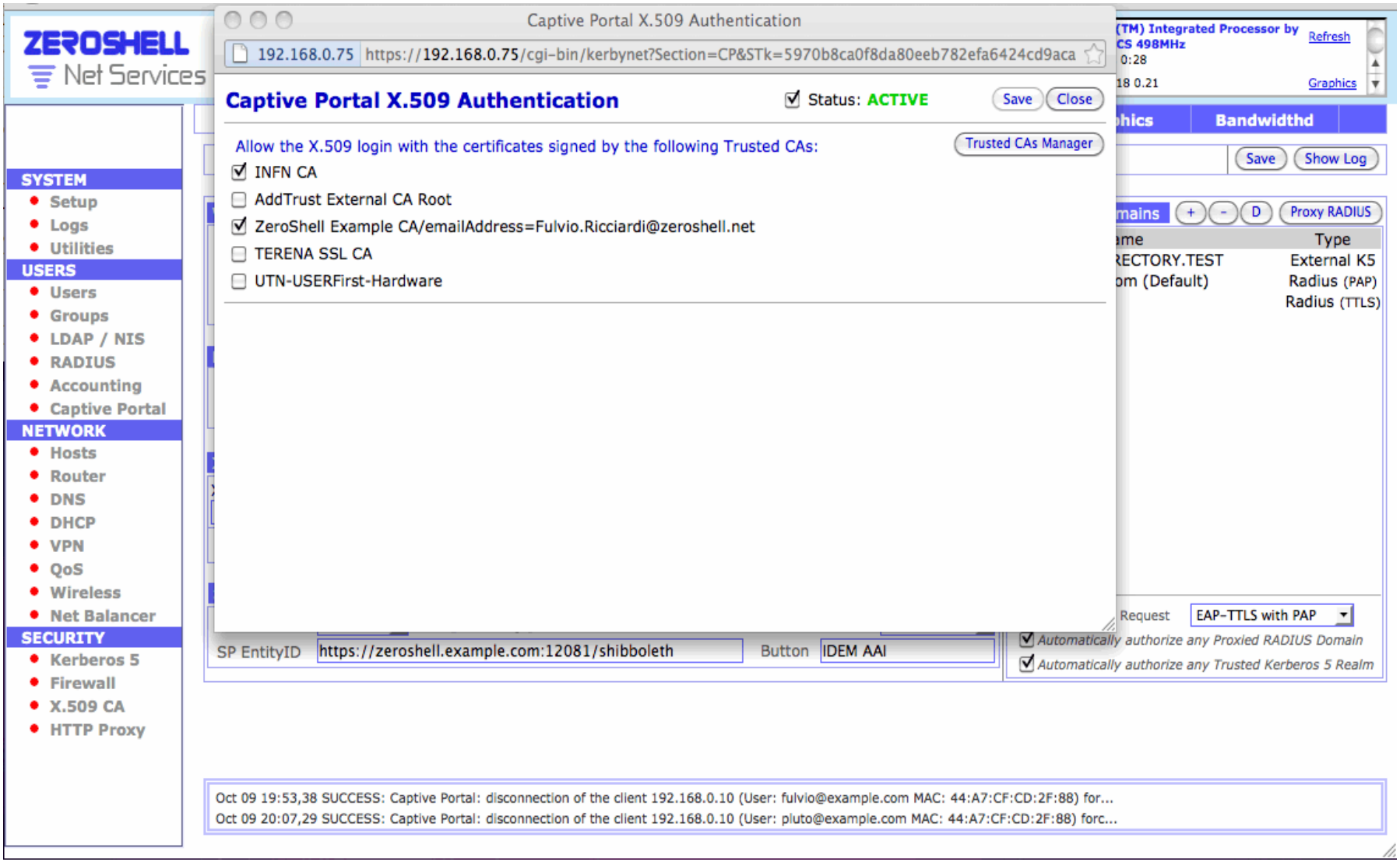
Configure Authorized Kerberos5/RADIUS Domains



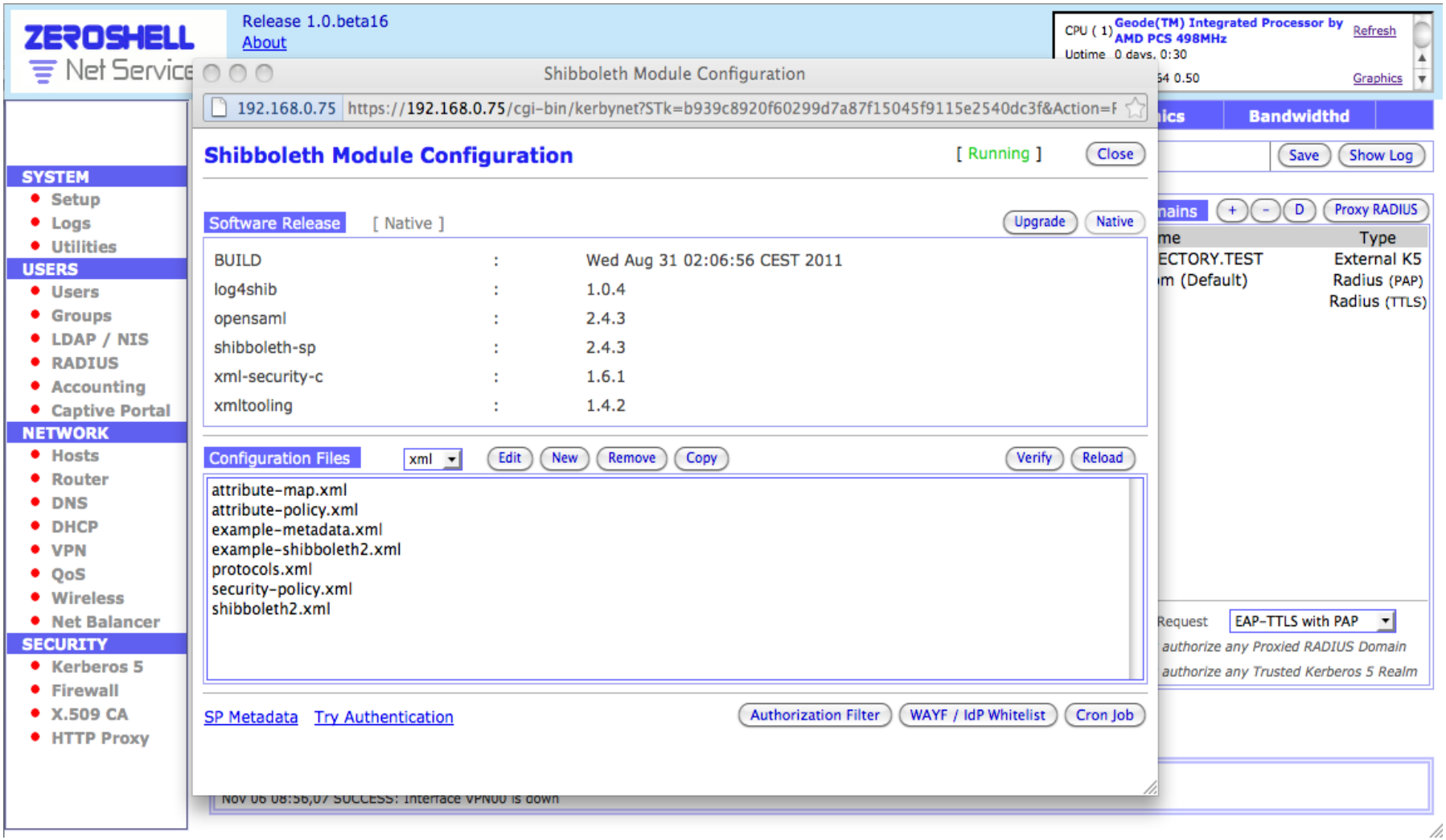
Proxy Radius



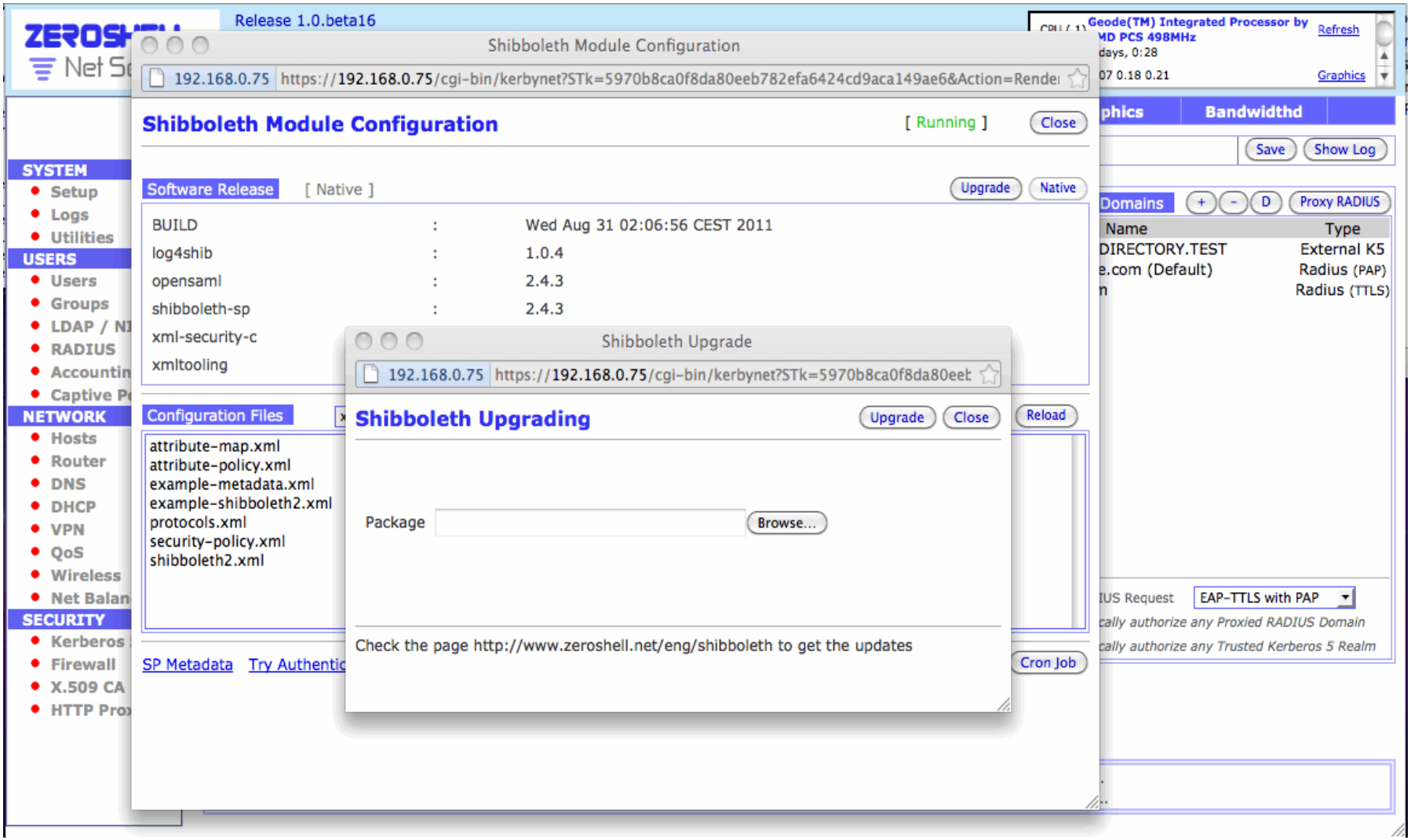
X.509 Certificate Authentication



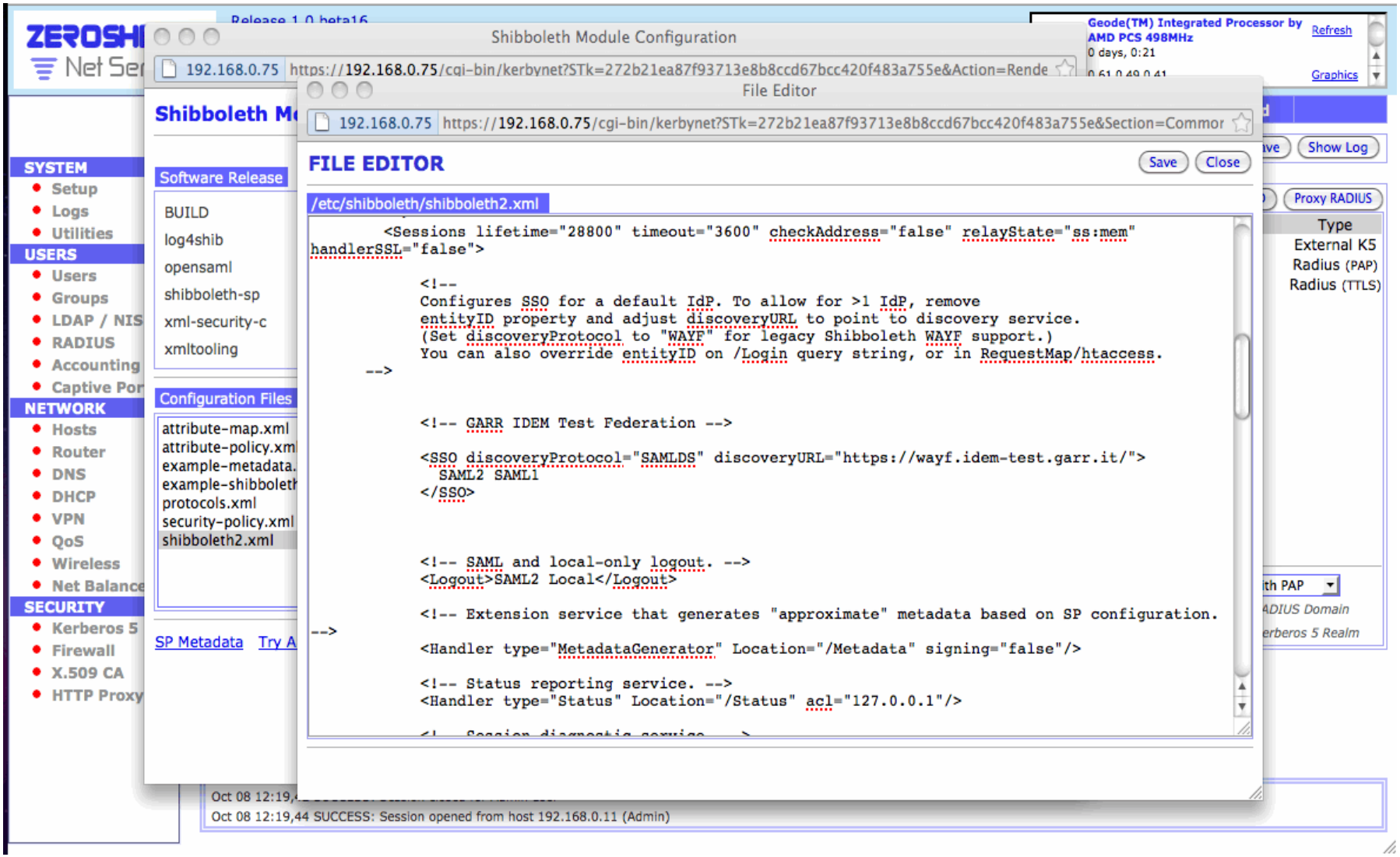
Shibboleth Configuration



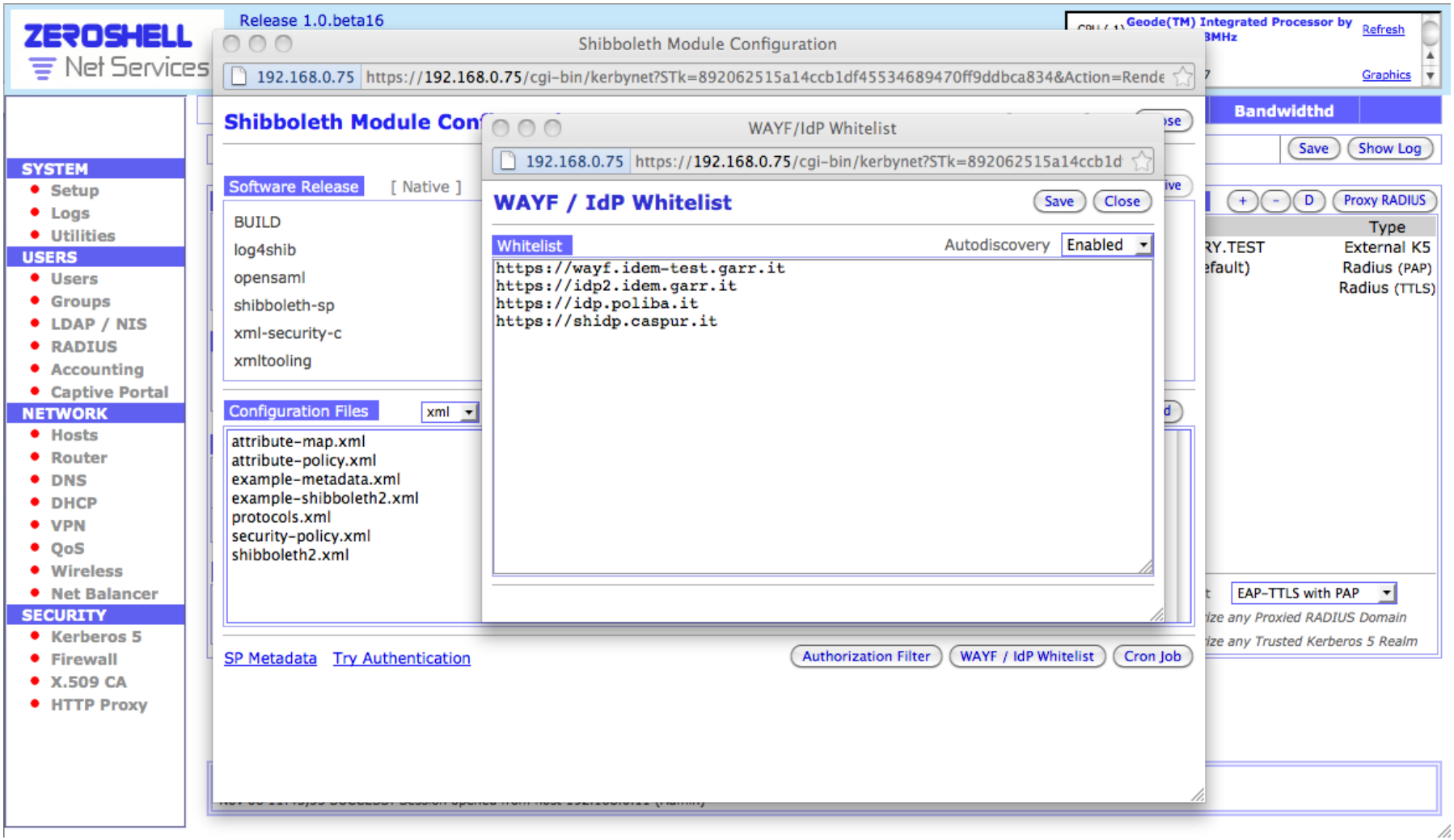
Shibboleth Upgrading



Configuring Shibboleth by File Editor



Identity Provider e WAYF Auto-Discovery

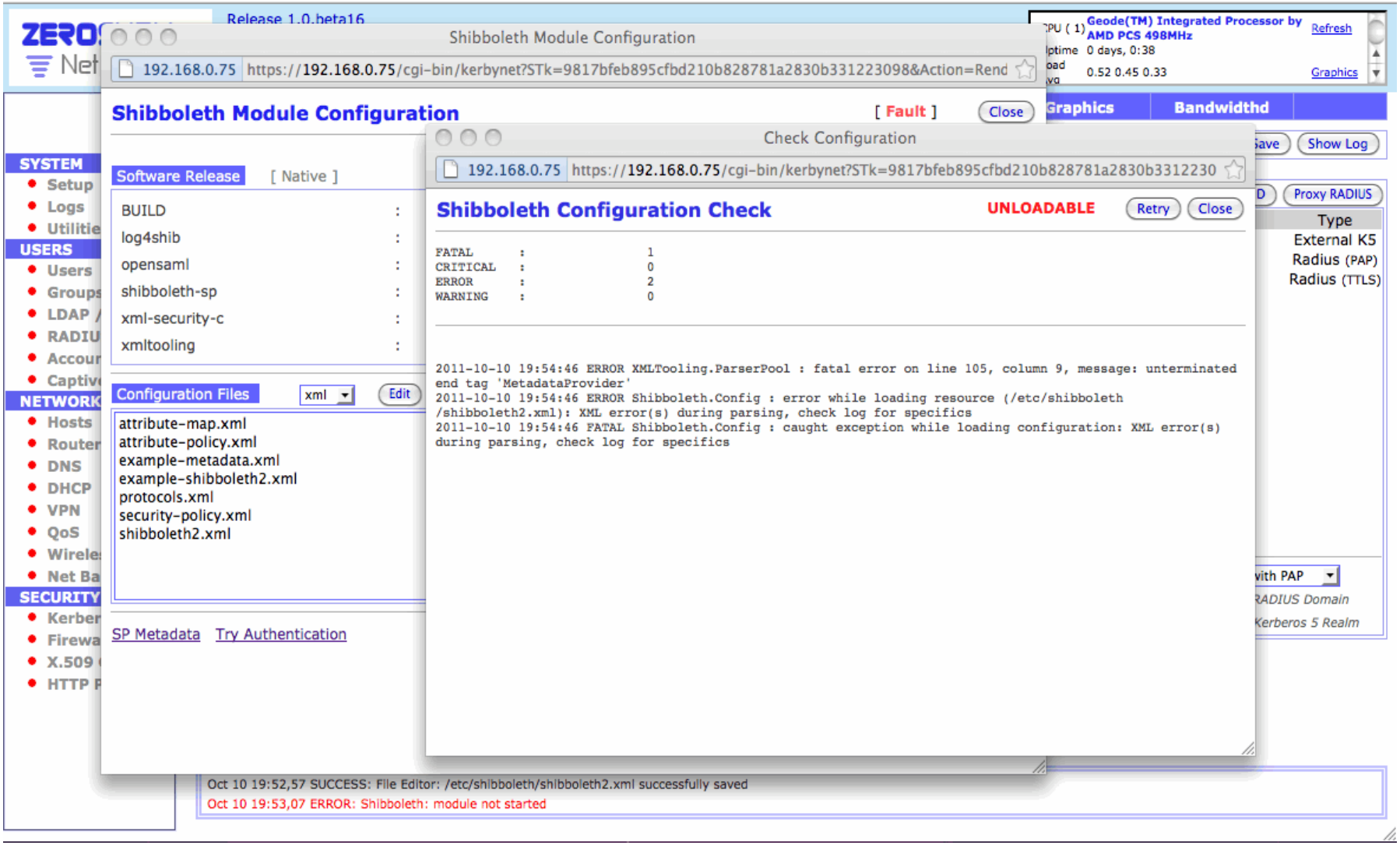


Auto-Discovery: nessun man in the middle

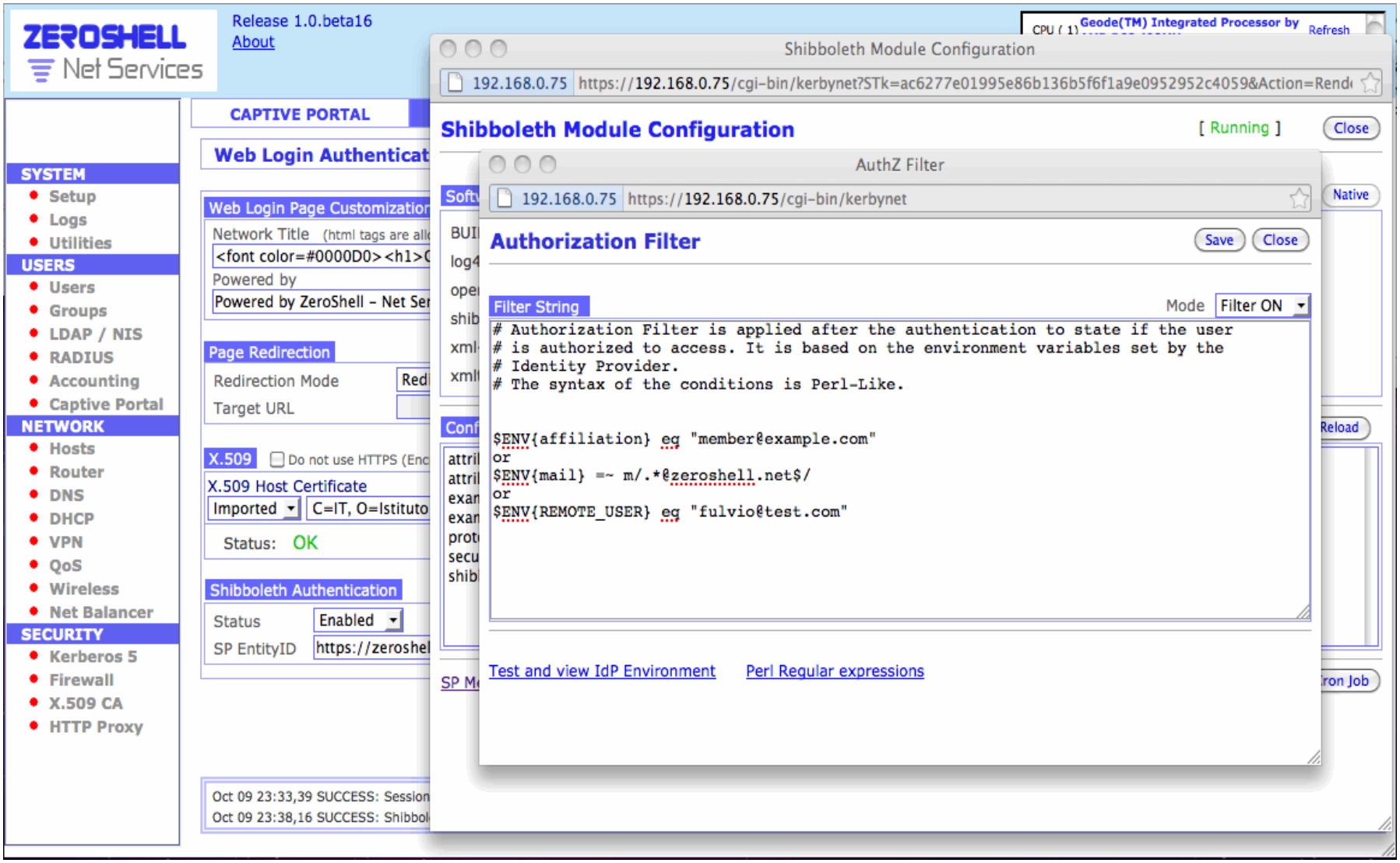
```
diff -r -u shibboleth-2.4.3/shibsp/handler/impl/SAMLDSSessionInitiator.cpp shibboleth-2.4.3-zs/shibsp/handler/impl/SAMLDSSessionInitiator.cpp
--- shibboleth-2.4.3/shibsp/handler/impl/SAMLDSSessionInitiator.cpp 2011-06-28 02:39:27.000000000 +0200
+++ shibboleth-2.4.3-zs/shibsp/handler/impl/SAMLDSSessionInitiator.cpp     2011-10-16 11:26:08.000000000 +0200
@@ -282,6 +282,16 @@
         req = req + "&returnIDParam=" + m_returnParam;
     if (isPassive)
         req += "&isPassive=true";
+    //
+    // Patch by Fulvio.Ricciardi(at)zeroshell.net for IdP AutoDiscovery in Zeroshell Captive Portal
+    //
+    char cmd[150];
+    strcpy(cmd,"/root/kerbynet.cgi/scripts/idpDiscovery SAMLDS ");
+    strncat(cmd,req.c_str(),100);
+    system(cmd);
+    //
+    // End of the patch
+    //

     return make_pair(true, request.sendRedirect(req.c_str()));
 }
```

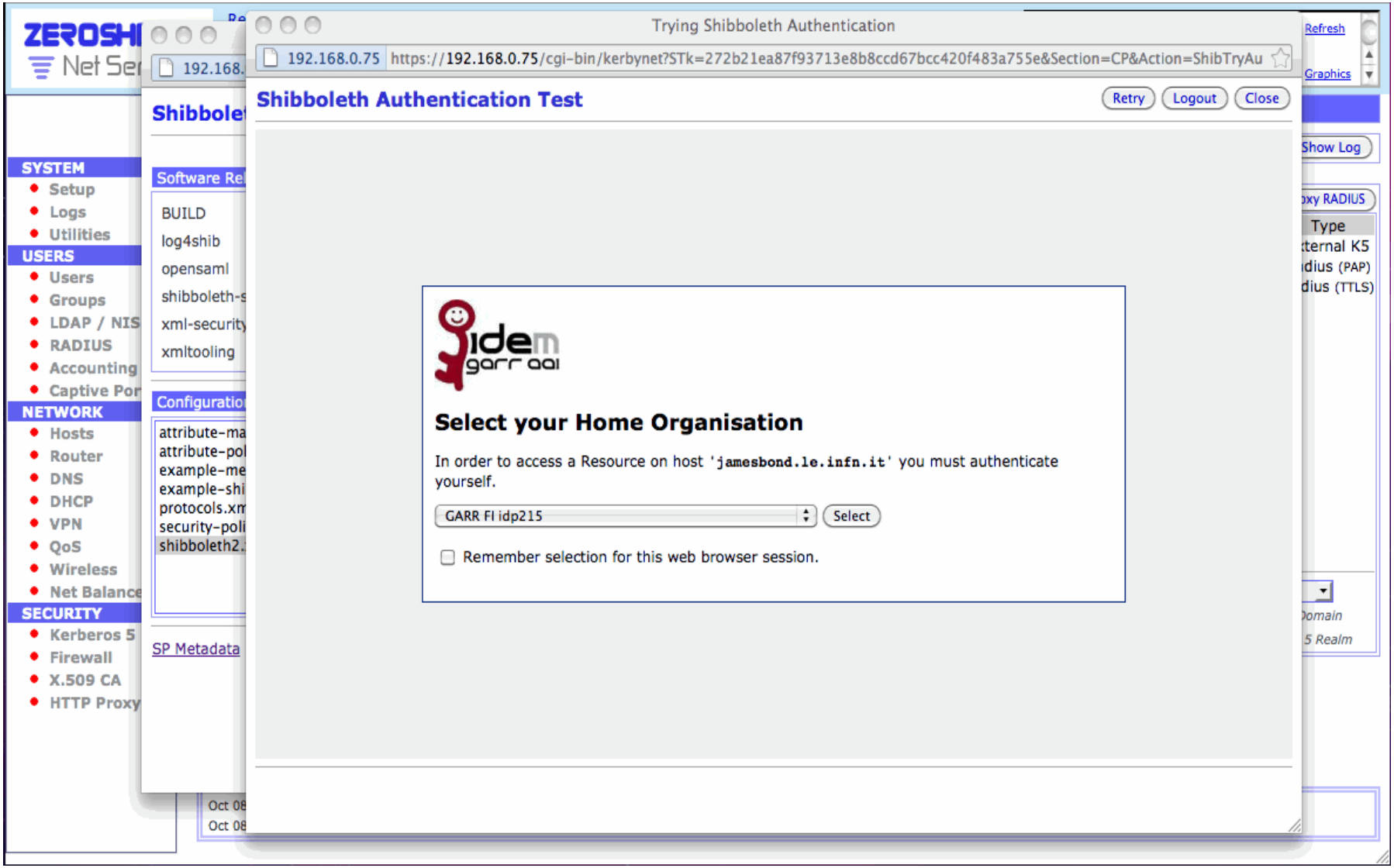
Checking the Shibboleth Configuration



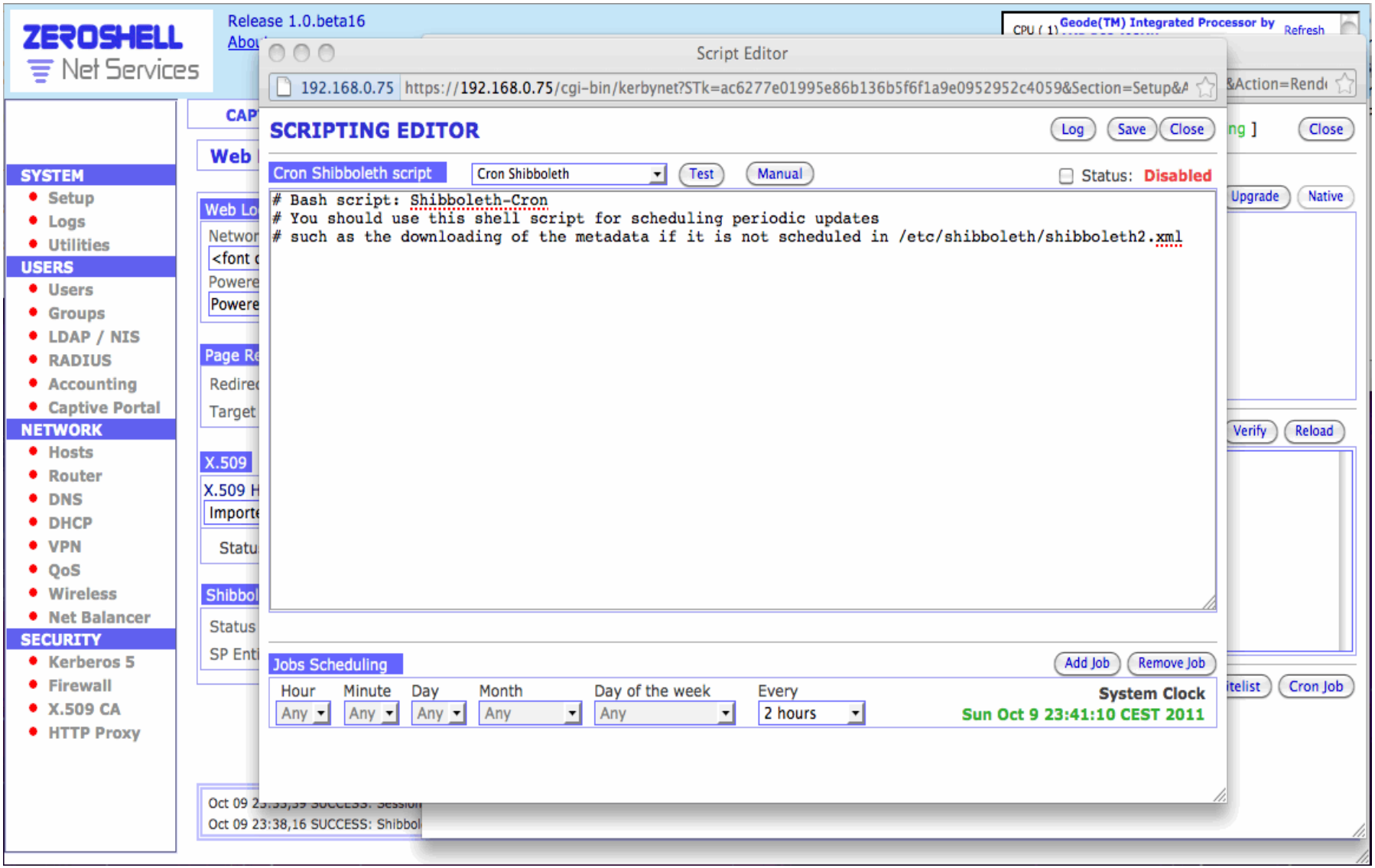
Perl Authorization Filters



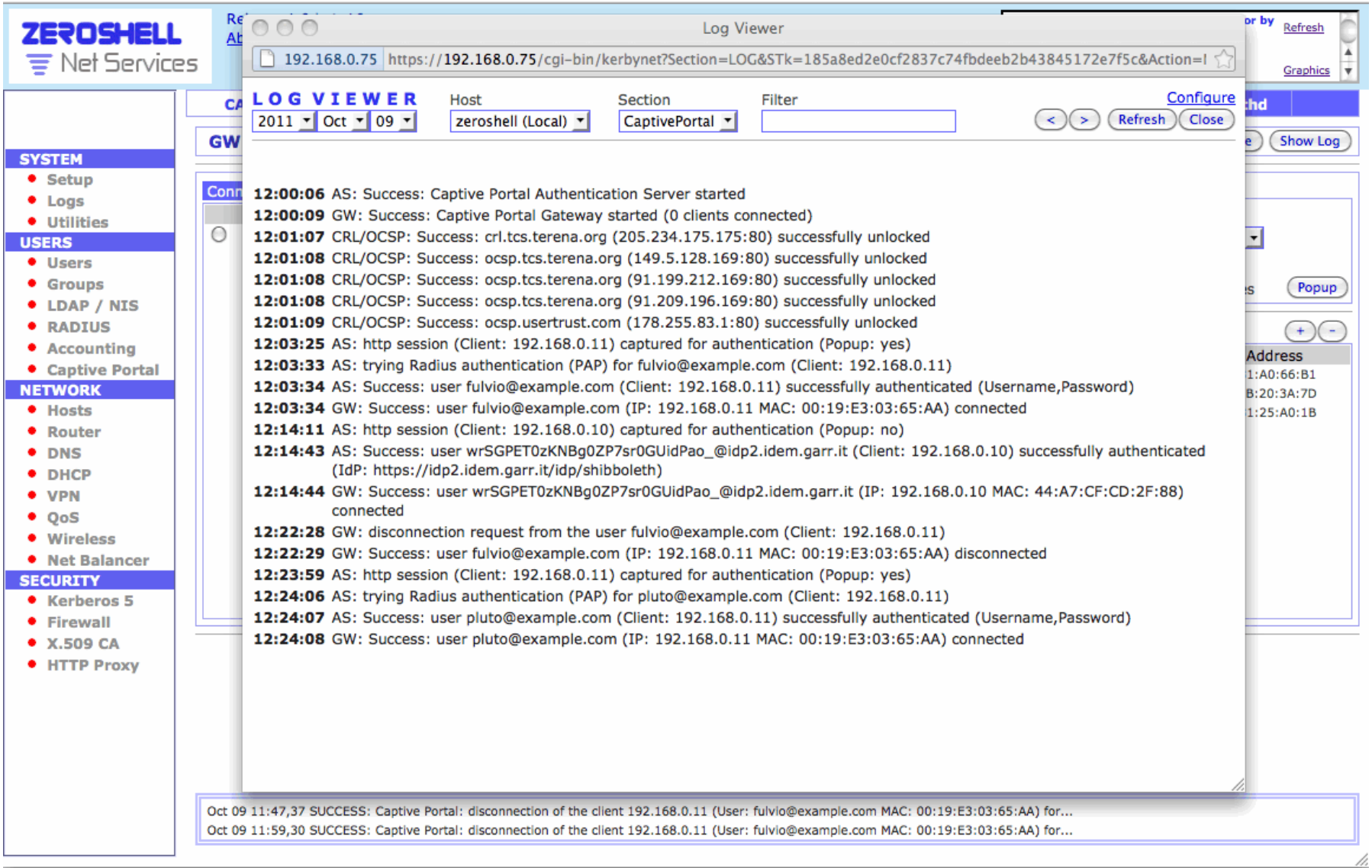
Try Authentication



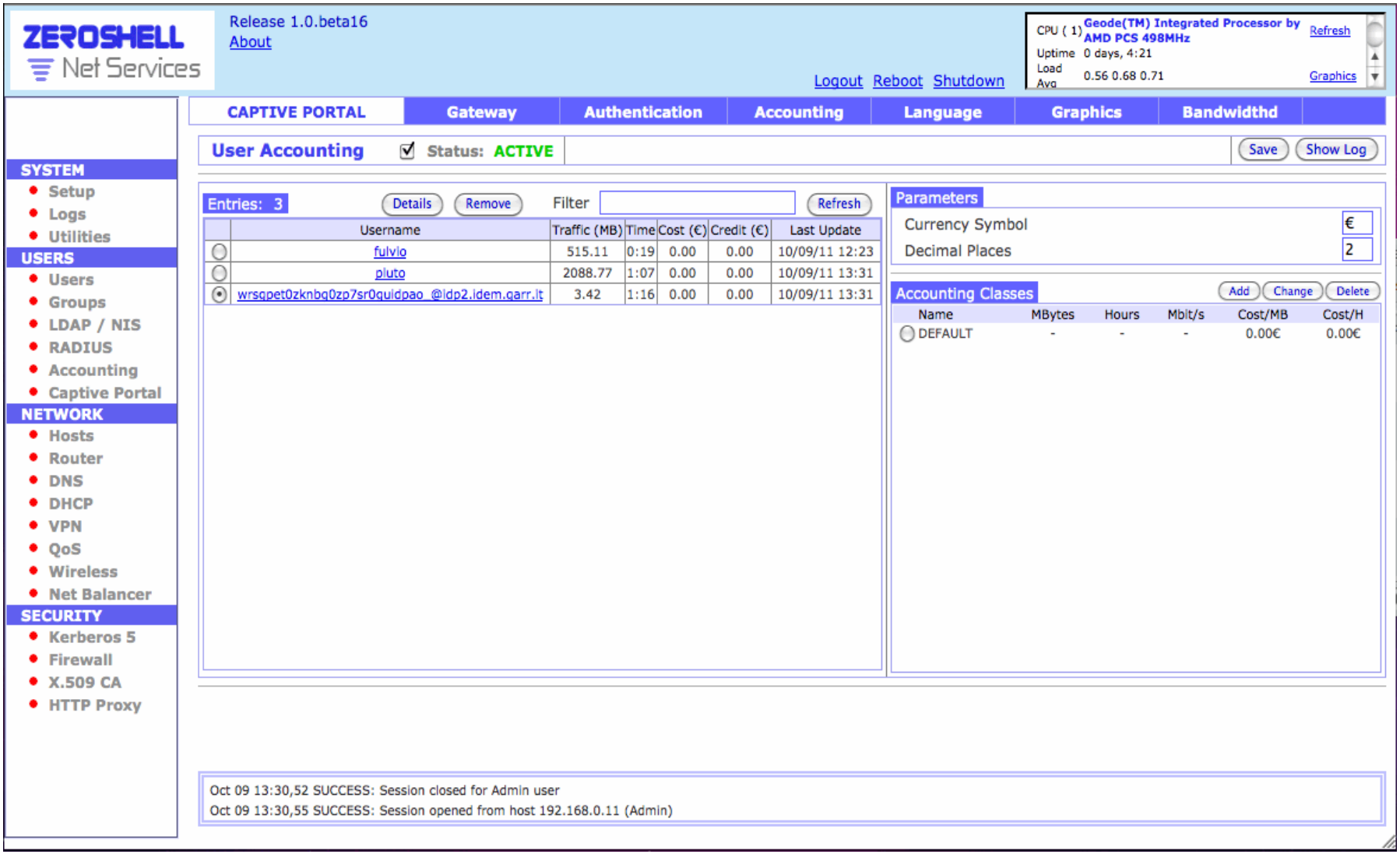
Cron Job


ZEROSHELL
Net Services
Release 1.0.beta16
Script Editor
192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?STk=ac6277e01995e86b136b5f6f1a9e0952952c4059&Section=Setup&A
SCRIPTING EDITOR
Log
Save
Close
Cron Shibboleth script
Cron Shibboleth
Test
Manual
Status: Disabled
Bash script: Shibboleth-Cron
You should use this shell script for scheduling periodic updates
such as the downloading of the metadata if it is not scheduled in /etc/shibboleth/shibboleth2.xml
Jobs Scheduling
Add Job
Remove Job
Hour
Minute
Day
Month
Day of the week
Every
Any
Any
Any
Any
Any
2 hours
System Clock
Sun Oct 9 23:41:10 CEST 2011
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Accounting
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
Wireless
Net Balancer
SECURITY
Kerberos 5
Firewall
X.509 CA
HTTP Proxy
Upgrade
Native
Verify
Reload
Cron Job
Oct 09 23:38,16 SUCCESS: Shibbol

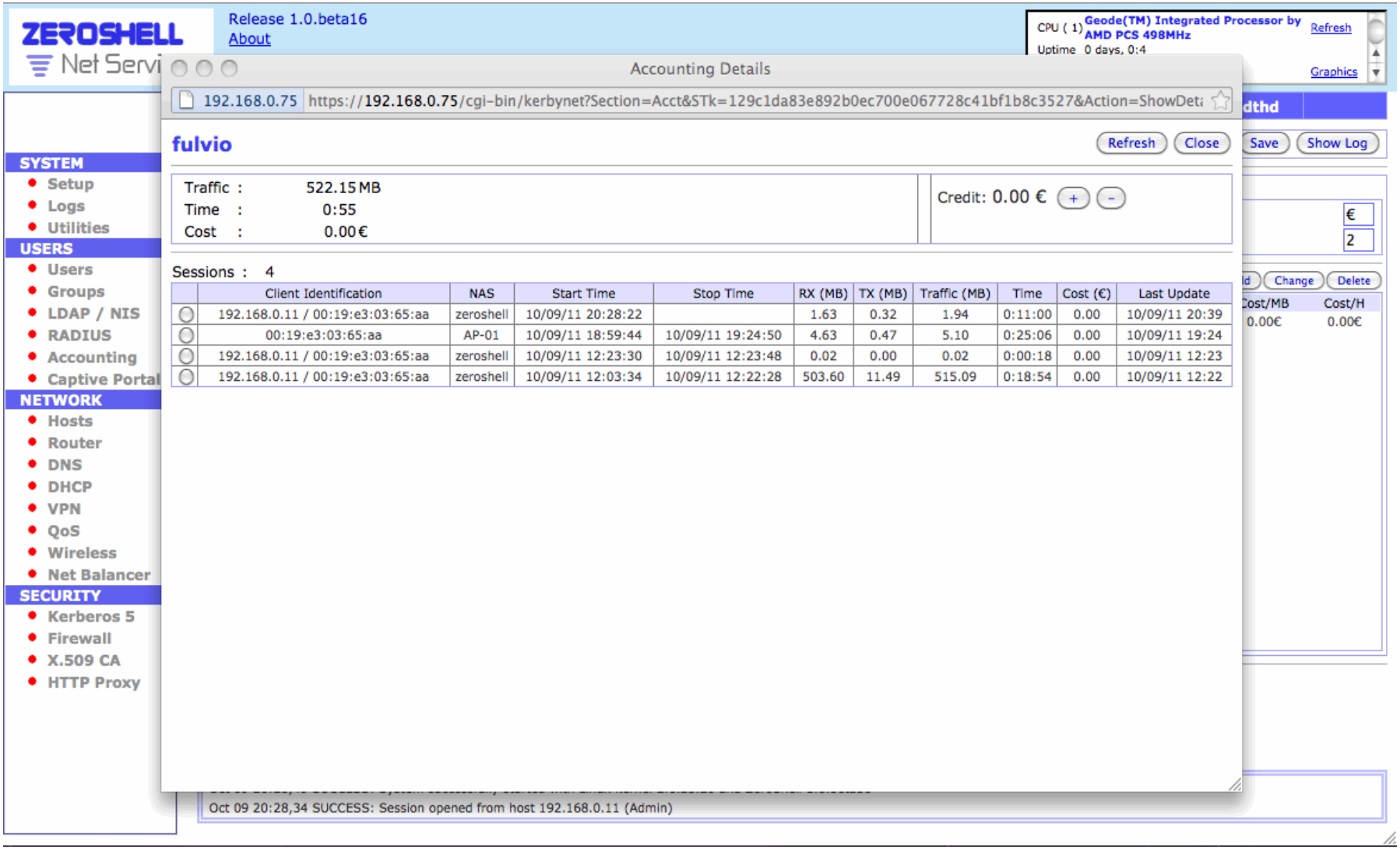
Log Viewer


ZEROSHELL
Net Services
SYSTEM
Setup
Logs
Utilities
USERS
Users
Groups
LDAP / NIS
RADIUS
Accounting
Captive Portal
NETWORK
Hosts
Router
DNS
DHCP
VPN
QoS
Wireless
Net Balancer
SECURITY
Kerberos 5
Firewall
X.509 CA
HTTP Proxy
Log Viewer
192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?Section=LOG&STk=185a8ed2e0cf2837c74fbdeeb2b43845172e7f5c&Action=l
LOG VIEWER
Host
zeroshell (Local)
Section
CaptivePortal
Filter
Configure
2011 Oct 09
Refresh
Close
12:00:06 AS: Success: Captive Portal Authentication Server started
12:00:09 GW: Success: Captive Portal Gateway started (0 clients connected)
12:01:07 CRL/OCSP: Success: crl.tcs.terena.org (205.234.175.175:80) successfully unlocked
12:01:08 CRL/OCSP: Success: ocsp.tcs.terena.org (149.5.128.169:80) successfully unlocked
12:01:08 CRL/OCSP: Success: ocsp.tcs.terena.org (91.199.212.169:80) successfully unlocked
12:01:08 CRL/OCSP: Success: ocsp.tcs.terena.org (91.209.196.169:80) successfully unlocked
12:01:09 CRL/OCSP: Success: ocsp.usertrust.com (178.255.83.1:80) successfully unlocked
12:03:25 AS: http session (Client: 192.168.0.11) captured for authentication (Popup: yes)
12:03:33 AS: trying Radius authentication (PAP) for fulvio@example.com (Client: 192.168.0.11)
12:03:34 AS: Success: user fulvio@example.com (Client: 192.168.0.11) successfully authenticated (Username,Password)
12:03:34 GW: Success: user fulvio@example.com (IP: 192.168.0.11 MAC: 00:19:E3:03:65:AA) connected
12:14:11 AS: http session (Client: 192.168.0.10) captured for authentication (Popup: no)
12:14:43 AS: Success: user wrSGPET0zKNBg0ZP7sr0GUidPao_@idp2.idem.garr.it (Client: 192.168.0.10) successfully authenticated (IdP: https://idp2.idem.garr.it/idp/shibboleth)
12:14:44 GW: Success: user wrSGPET0zKNBg0ZP7sr0GUidPao_@idp2.idem.garr.it (IP: 192.168.0.10 MAC: 44:A7:CF:CD:2F:88) connected
12:22:28 GW: disconnection request from the user fulvio@example.com (Client: 192.168.0.11)
12:22:29 GW: Success: user fulvio@example.com (IP: 192.168.0.11 MAC: 00:19:E3:03:65:AA) disconnected
12:23:59 AS: http session (Client: 192.168.0.11) captured for authentication (Popup: yes)
12:24:06 AS: trying Radius authentication (PAP) for pluto@example.com (Client: 192.168.0.11)
12:24:07 AS: Success: user pluto@example.com (Client: 192.168.0.11) successfully authenticated (Username,Password)
12:24:08 GW: Success: user pluto@example.com (IP: 192.168.0.11 MAC: 00:19:E3:03:65:AA) connected
Refresh
Graphics
Show Log
Popup
Address
Oct 09 11:47,37 SUCCESS: Captive Portal: disconnection of the client 192.168.0.11 (User: fulvio@example.com MAC: 00:19:E3:03:65:AA) for...
Oct 09 11:59,30 SUCCESS: Captive Portal: disconnection of the client 192.168.0.11 (User: fulvio@example.com MAC: 00:19:E3:03:65:AA) for...

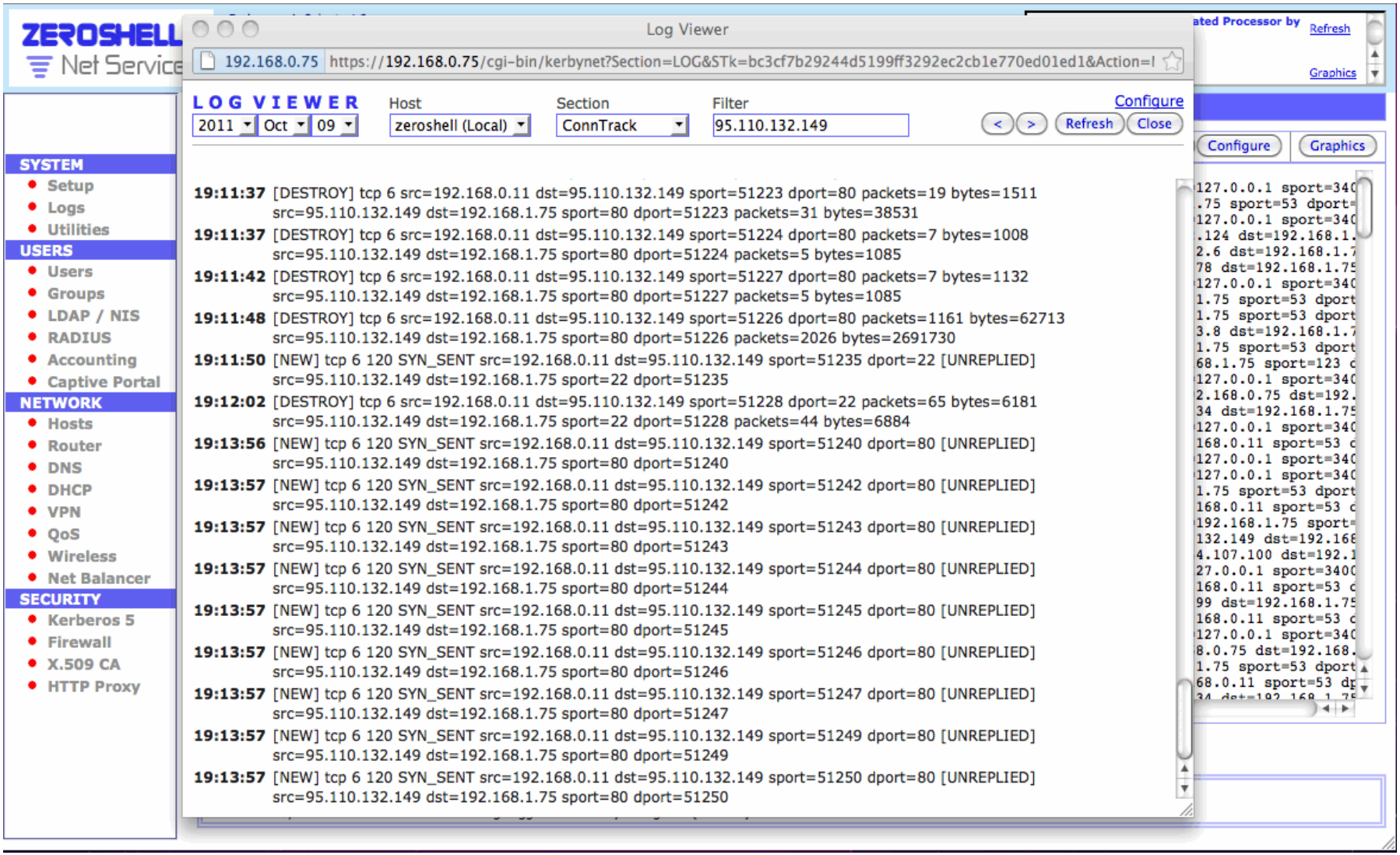
Radius Accounting



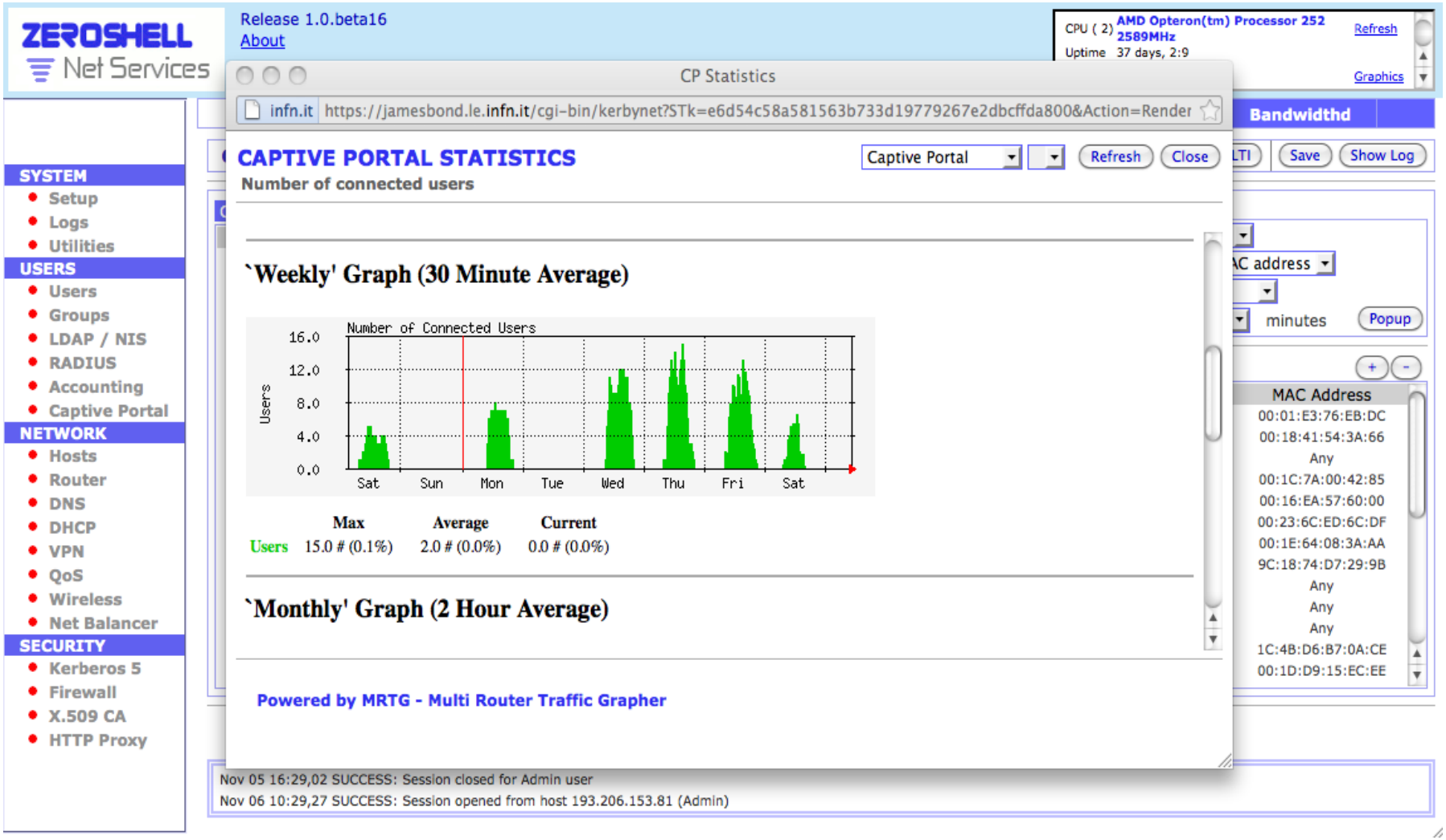
Radius Accounting Details



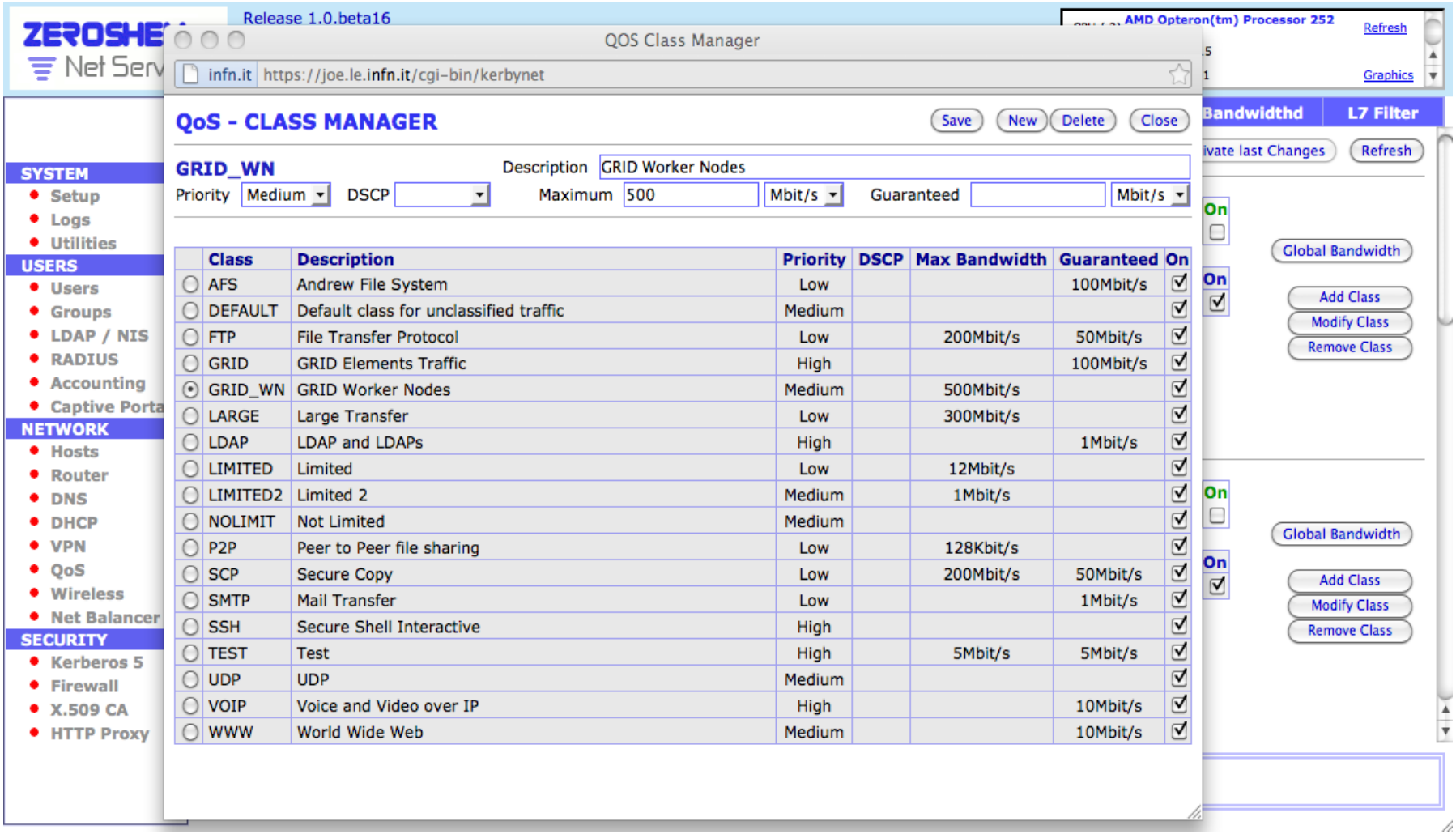
Connection Tracking



Captive Portal Statistics



Traffic Shaping e QoS



Classificazione del traffico in classi di QoS