

Zeroshell come Captive Portal per l'accesso ad IDEM

Fulvio Ricciardi
INFN Lecce

Gli argomenti trattati

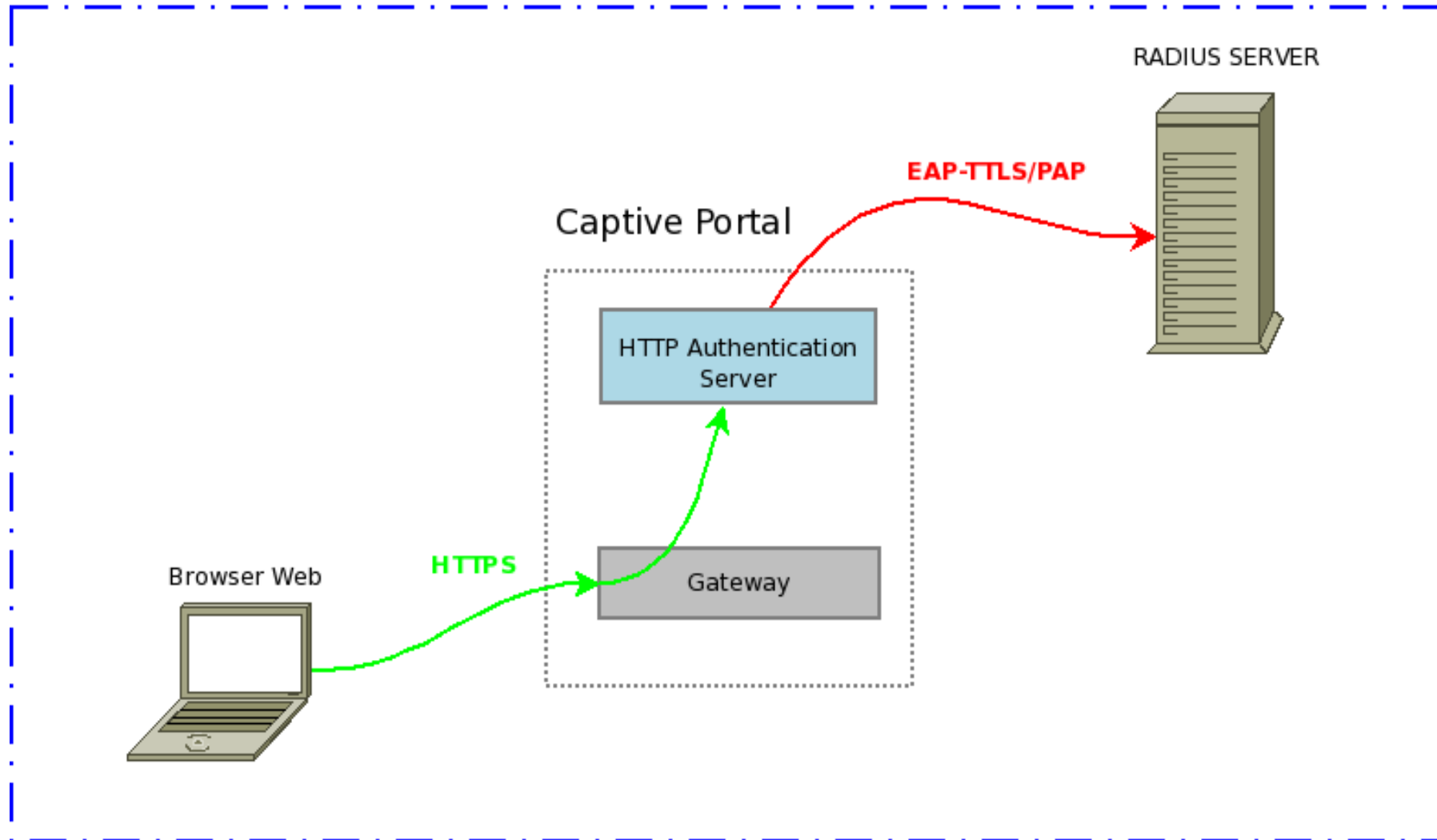
- Proteggere la rete tramite Captive Portal
 - Vantaggi e svantaggi
 - L'accesso federato
 - I nemici del Captive Portal
- Cosa è Zeroshell?
- Il Captive Portal di Zeroshell
 - Configurazione e funzionalità
 - Configurazione come Shibboleth SP

Definizione di Captive Portal

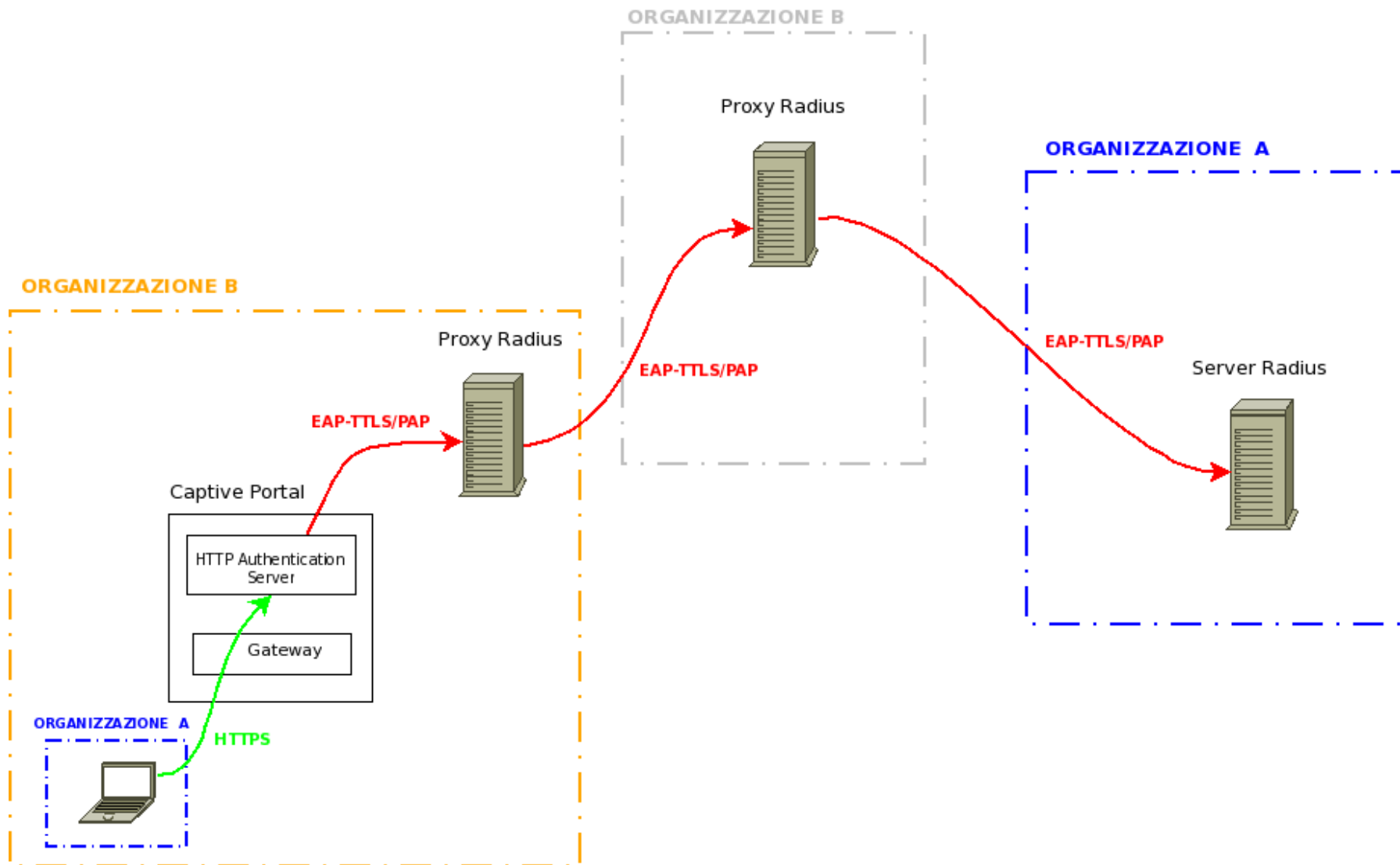
- E' un gateway di livello 2 o 3 che unisce due segmenti di rete
 - I client che si associano al primo segmento ottengono subito connettività IP, ma non possono comunicare con il secondo segmento se non si autenticano
 - Le richieste http/https dei client non autenticati vengono reindirizzate verso un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

Captive Portal Standalone

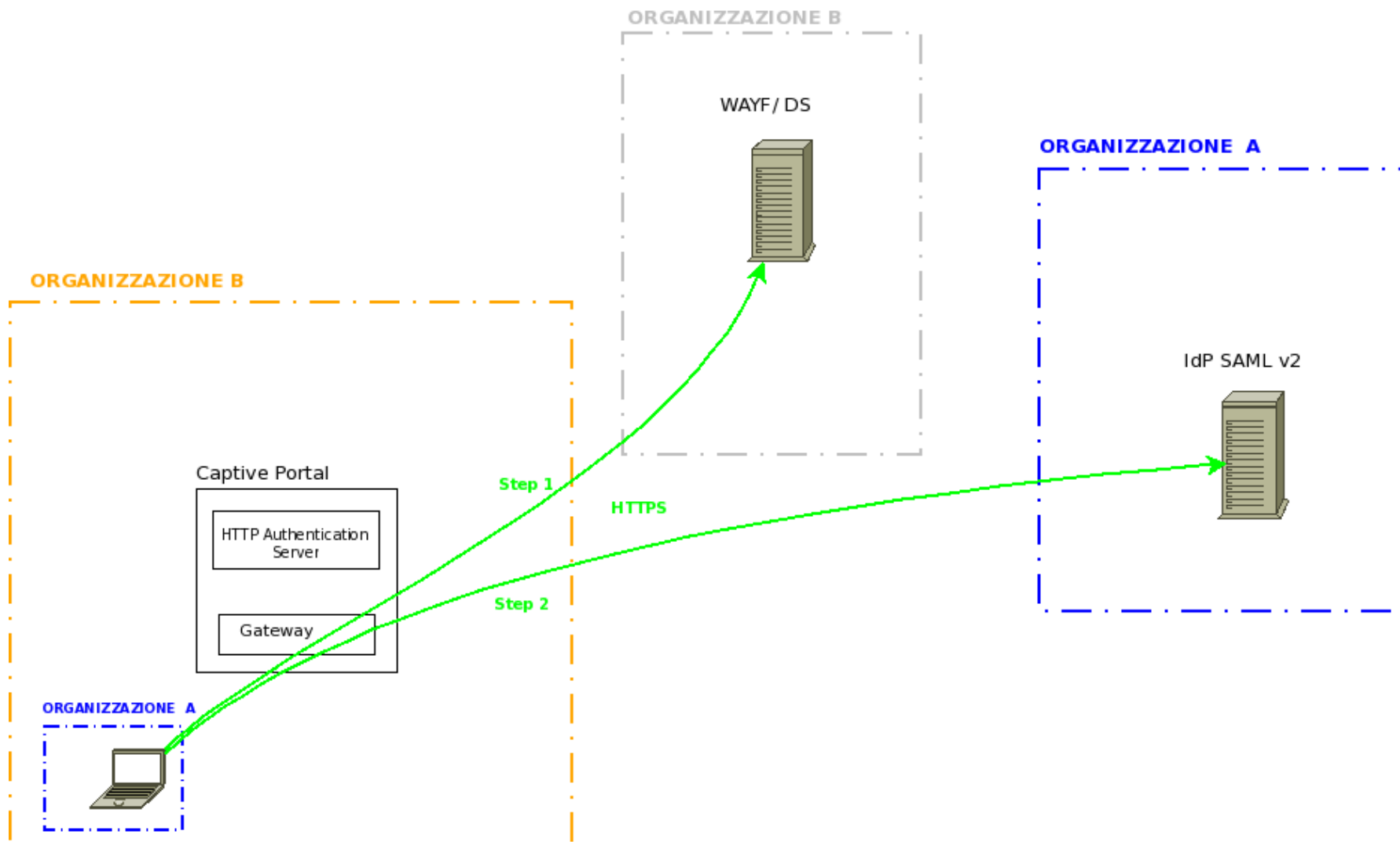
ORGANIZZAZIONE A



Captive Portal Federato tramite Proxy Radius (bassa sicurezza)



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

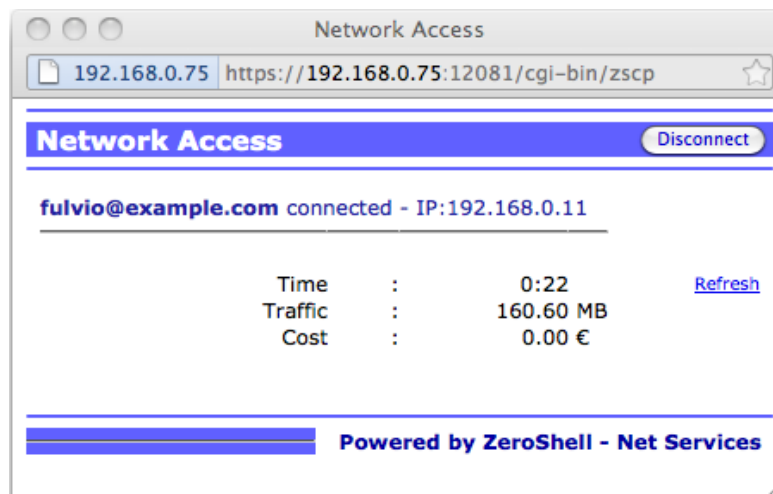


I nemici del Captive Portal

- 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           MAC 12:2D:31:A0:66:B1
ACCEPT     all  -- 192.168.0.101          0.0.0.0/0
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

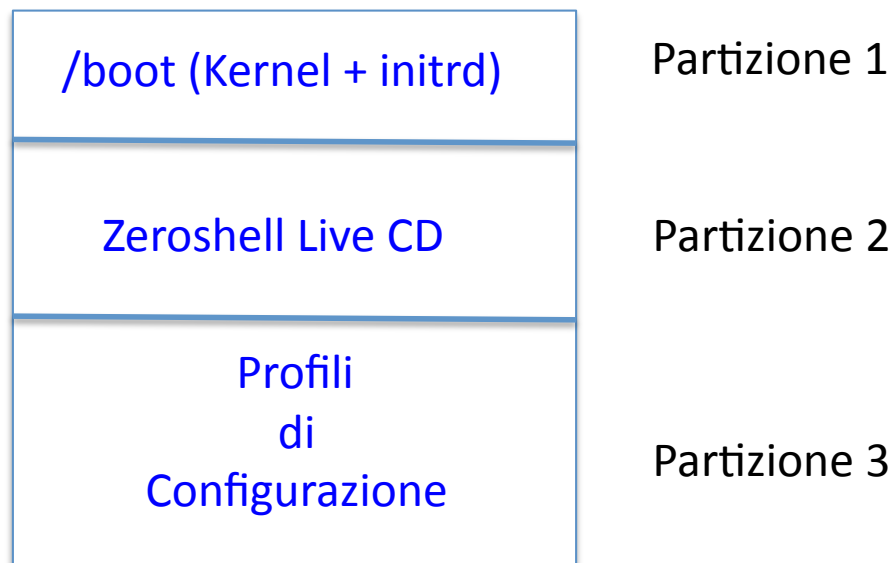
<http://www.zeroshell.net/download/>

- ***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



Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)

Uptime 0 days, 0:4

Load Avg 1.67 0.85 0.34 [Graphics](#)

[Logout](#)
[Reboot](#)
[Shutdown](#)

SETUP
AutoUpdate
Profiles
Network
Time
https
SSH
Startup/Cron
Logs

Profile: **_DB.002 (hda3)**

Activate
Deactivate
Info
Delete
Backup
Backup without Logs
Copy

RESCAN

Warning:
This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

Model: CF 1GB (hda)		Capacity: 967 MB
<input checked="" type="radio"/>	hda3	
Type: ext3		Capacity: 773 MB Used: 208 MB 29%
		Profile Description Last Activation
<input type="radio"/>	_DB.001	DEFAULT 02 Oct 2011 22:56
<input checked="" type="radio"/>	_DB.002	Screenshot Active

Model: Kingston DataTravelerMini(sda)		Capacity: 1968 MB
<input type="radio"/>	sda1	
Type: ext3		Capacity: 1936 MB Used: 148 MB 9%
		Profile Description Last Activation
<input type="radio"/>	_DB.001	Shibboleth Test Never
<input type="radio"/>	_DB.002	Traffic Shaping in bridge mode Never
<input type="radio"/>	_DB.003	VPN Site-to-Site with VLAN 802.1q Never

Nov 06 08:30,42 SUCCESS: Session opened from host 192.168.0.11 (Admin)

Nov 06 08:32,03 SUCCESS: Captive Portal: Authentication Server reconfigured.

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Accounting
- Captive Portal

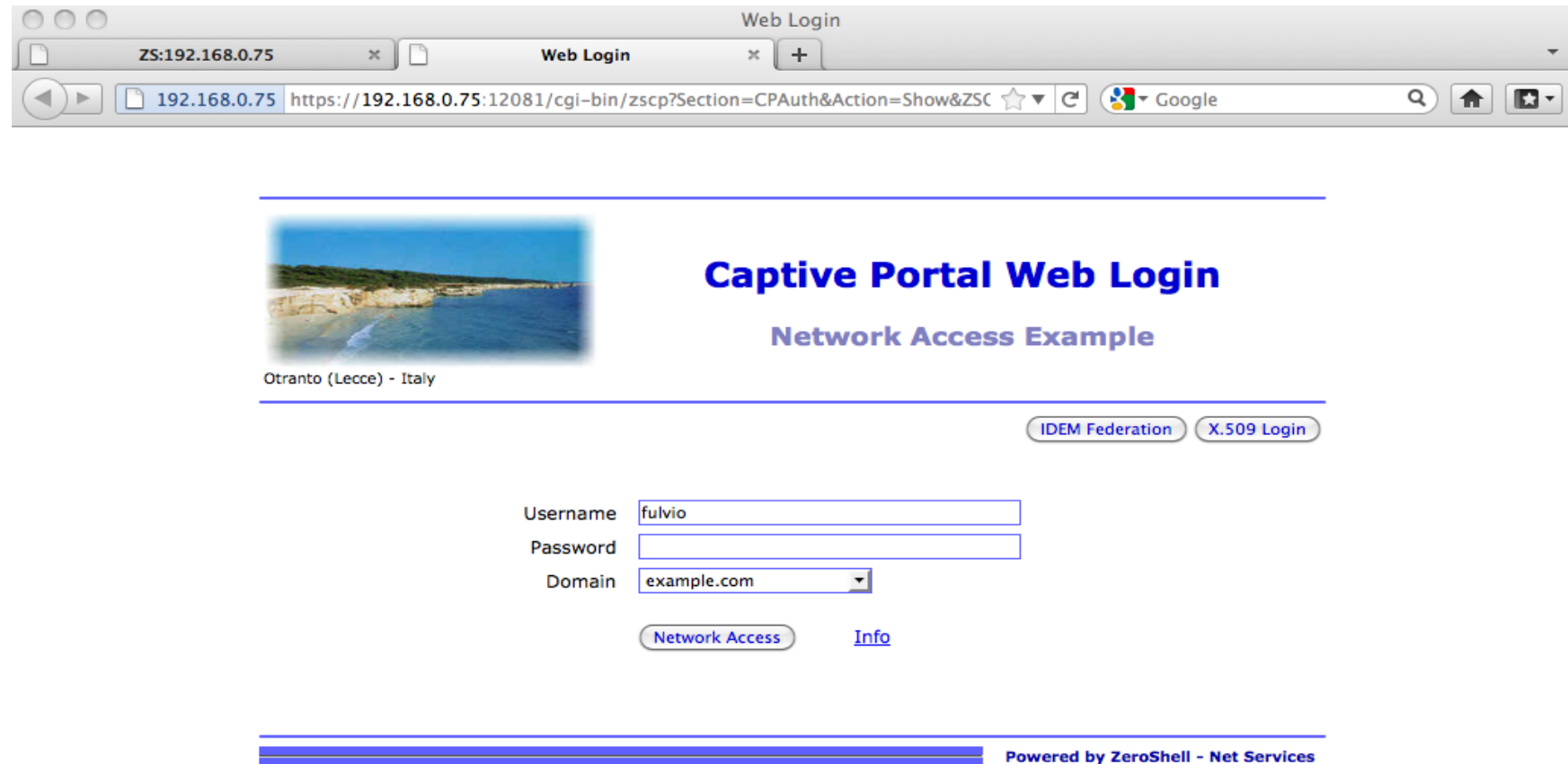
NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS
- Wireless
- Net Balancer

SECURITY

- Kerberos 5
- Firewall
- X.509 CA
- HTTP Proxy


Web Login Page



The screenshot shows a web browser window titled "Web Login". The address bar displays the URL: `https://192.168.0.75:12081/cgi-bin/zscp?Section=CPAuth&Action=Show&ZSC`. The page content includes:

- A horizontal blue line at the top.
- A photograph of a coastline with the caption "Otranto (Lecce) - Italy".
- The main heading: **Captive Portal Web Login**
- The subtitle: **Network Access Example**
- Two buttons: [IDEM Federation](#) and [X.509 Login](#).
- Form fields:
 - Username:
 - Password:
 - Domain: (with a dropdown arrow)
- Two buttons at the bottom: [Network Access](#) and [Info](#).
- A footer bar with the text: **Powered by ZeroShell - Net Services**.

Captive Portal Gateway Configuration



Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)

Uptime 0 days, 0:30

Load Avg 0.46 0.64 0.50 [Graphics](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL
Gateway
Authentication
Accounting
Language
Graphics
Bandwidth

GW Active on: **ETH02**
Interface: **ETH02** [MULTI](#) [Save](#) [Show Log](#)

Connected Clients: 2 [Disconnect](#) [Refresh](#)

Username	IP Address	MAC Address
<input type="radio"/> pluto@example.com	192.168.0.10	44:A7:CF:CD:2F:88
<input type="radio"/> fulvio@example.com	192.168.0.11	00:19:E3:03:65:AA

Gateway Parameters

DoS Protection: **Medium**

Client Identity: **IP and MAC address**

Simultaneous Connections: **Allowed**

Authenticator Validity: **1** minutes [Popup](#)


Free Authorized Clients [+](#) [-](#)

Description	IP Address	MAC Address
<input type="radio"/> SIP Phone 1	192.168.0.101	12:2D:31:A0:66:B1
<input type="radio"/> Net-Printer	192.168.0.120	45:AC:3B:20:3A:7D
<input type="radio"/> SIP Phone 2	192.168.0.102	12:2D:31:25:A0:1B

Nov 06 08:32,03 SUCCESS: Captive Portal: Authentication Server reconfigured.

Nov 06 08:56,07 SUCCESS: Interface VPN00 is down

Free Authorized Clients



Release 1.0.beta16
[About](#)

CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz [Refresh](#)

Uptime 0 days, 3:16

Load Avg 0.37 0.54 0.36 [Graphics](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL
Gateway
Authentication
Accounting
Language
Graphics
Bandwidth

GW Active on: ETH02
Interface: ETH02 MULTI Save Show Log

Connected Clients: 1 Disconnect Refresh

Username	IP Address	MAC Address
admin@example.com	192.168.0.11	00:19:E3:03:65:AA

Add Client

192.168.0.75 <https://192.168.0.75/cgi-bin/kerbynet?S>

Free Authorized Client Save Close

Description:

IP Address:

MAC Address:

Gateway Parameters

DoS Protection:

Client Identity:

Simultaneous Connections:

Authenticator Validity: minutes Popup


Free Authorized Clients + -

Description	IP Address	MAC Address
<input type="radio"/> SIP Phone 1	192.168.0.101	12:2D:31:A0:66:B1
<input type="radio"/> Net-Printer	192.168.0.120	45:AC:3B:20:3A:7D
<input type="radio"/> SIP Phone 2	192.168.0.102	12:2D:31:25:A0:1B

Oct 09 21:37,33 SUCCESS: Captive Portal: Authentication Server reconfigured and restarted.

Oct 09 21:41,34 SUCCESS: Session opened from host 192.168.0.11 (Admin)

Free Authorized Services



Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)

Uptime 0 days, 3:16

Load Avg 0.37 0.54 0.36 [Graphics](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL
Gateway
Authentication
Accounting
Language
Graphics
Bandwidth

GW Active on: **ETH02**
Interface: **ETH02** [MULTI](#) [Save](#) [Show Log](#)

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

Connected Clients: 1
[Disconnect](#) [Refresh](#)

Username	IP Address	MAC Address
admin@example.com	192.168.0.11	00:19:E3:03:65:AA

Add Service

192.168.0.75 <https://192.168.0.75/cgi-bin/kerbynet?S>

Free Authorized Service [Save](#) [Close](#)

Description:

IP Address:

Port:

Gateway Parameters

DoS Protection:

Client Identity:

Simultaneous Connections:

Authenticator Validity: minutes [Popup](#)

Free Authorized Services [+](#) [-](#)

Description	IP Address	Port
<input type="radio"/> Domain Name System	Any	53/udp
<input type="radio"/> DHCP and bootp	Any	67/udp

Oct 09 21:37,33 SUCCESS: Captive Portal: Authentication Server reconfigured and restarted.

Oct 09 21:41,34 SUCCESS: Session opened from host 192.168.0.11 (Admin)

Network Access Popup for Mobile Devices

The screenshot displays the Zeroshell web management interface. At the top left, the logo 'ZEROSHELL Net Services' is visible, along with the release version 'Release 1.0.beta16' and an 'About' link. On the top right, system statistics are shown: CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz, Uptime 0 days, 0:30, and Load Avg 0.46 0.64 0.50. A navigation bar includes links for Logout, Reboot, and Shutdown, and tabs for CAPTIVE PORTAL, Gateway, Authentication, Accounting, Language, Graphics, and Bandwidth. A left sidebar contains a menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The main content area shows the 'CAPTIVE PORTAL' configuration for gateway 'GW', which is active on interface 'ETH02'. It lists two connected clients: 'pluto@example.com' and 'fulvio@example.com'. A 'Network Access Popup' dialog box is open, titled 'Network Access Popup', with a URL 'https://192.168.0.75/cgi-bin/kerbynet?STk=b939c8920f60299d7a87f150'. The dialog contains a 'Browser Exclusion List' with the following items: Mobile, BlackBerry.*, Nokia.*, SAMSUNG.*, Windows CE, Windows Phone, Windows Mobile, Symbian.*, SymbOS, Palm.*, Opera Mini, Opera Mobi, iPhone, iPad, iPod, Android, and Minimo. There are 'Save' and 'Cancel' buttons, a checkbox for 'Log the browser capturing requests', and a 'Logs' button. The background interface also shows a 'MAC Address' table with entries: 12:2D:31:A0:66:B1, 45:AC:3B:20:3A:7D, and 12:2D:31:25:A0:1B. A status bar at the bottom shows system messages: 'Nov 06 08:32,03 SUCCESS: Captive Portal: Authentication Server reconfigured.' and 'Nov 06 08:56,07 SUCCESS: Interface VPN00 is down'.

Multi Network Interface Configuration (Routing/Bridging)

The screenshot displays the Zeroshell web interface for configuring a Captive Portal. The main interface is titled "ZEROSHELL Net Services" and shows system information like "Release 1.0.beta16" and "AMD PCS 498MHz". A navigation menu on the left includes sections for SYSTEM, USERS, NETWORK, and SECURITY. The main content area is divided into tabs: CAPTIVE PORTAL, Gateway, Authentication, Accounting, Language, Graphics, and Bandwidth. The "CAPTIVE PORTAL" tab is active, showing "GW" and "Active on: ETH02". A "Connected Clients" table lists two users: pluto@example.com (192.168.0.10) and fulvio@example.com (192.168.0.11). A "Gateway Parameters" section is visible with settings for DoS Protection (Medium), Client Identity (IP and MAC address), and Allowed connections (1 minutes). A "MULTI Interface Configuration" dialog box is open in the foreground, showing a list of "Available Interfaces" (BRIDGE00, ETH01, ETH02, VPN99) and a "MULTI Interface" list (ETH00, VPN00). The dialog has "Ok" and "Close" buttons. At the bottom, a log shows disconnection messages for clients 192.168.0.11 and 192.168.0.10.

ZEROSHELL Net Services
Release 1.0.beta16
About

CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz Refresh
Uptime 0 days, 0:28
Load Avg 0.07 0.18 0.21 Graphics

Logout Reboot Shutdown

CAPTIVE PORTAL Gateway Authentication Accounting Language Graphics Bandwidth

GW Active on: **ETH02** Interface: ETH02 MULTI Save Show Log

Connected Clients: 2 Disconnect Refresh

Username	IP Address	MAC Address
pluto@example.com	192.168.0.10	44:A7:CF:CD:2F:88
fulvio@example.com	192.168.0.11	00:19:E3:03:65:AA

Gateway Parameters


DoS Protection: Medium
Client Identity: IP and MAC address
Allowed connections: Allowed
Idle timeout: 1 minutes

MULTI Interface Configuration

Available Interfaces: BRIDGE00, ETH01, ETH02, VPN99
MULTI Interface: ETH00, VPN00

Oct 09 19:52,59 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 19:53,38 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: fulvio@example.com MAC: 44:A7:CF:CD:2F:88) for...

Captive Portal Authentication Configuration



Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)

Uptime 0 days, 0:30

Load Avg 0.46 0.64 0.50 [Graphics](#)

[Logout](#)
[Reboot](#)
[Shutdown](#)

CAPTIVE PORTAL
Gateway
Authentication
Accounting
Language
Graphics
Bandwidthd

Web Login Authentication Server

Status: ACTIVE

Web Login Page Customization

Network Title (html tags are allowed)

Powered by

Page Redirection

Redirection Mode:

Target URL:

X.509
 Do not use HTTPS (Encryption)
 Use CN to redirect
 Unlock CRL and OCSP sites

X.509 Host Certificate

Local CA:
 OU=Hosts, CN=zeroshell.example.com

Status: **OK**

Shibboleth Authentication

Status: [Running]
 Mode:

SP EntityID:
 Button:

Authorized Domains

Domain Name	Type
<input type="radio"/> ACTIVEDIRECTORY.TEST	External K5
<input type="radio"/> example.com (Default)	Radius (PAP)
<input type="radio"/> test.com	Radius (TTLS)

Default RADIUS Request:

Automatically authorize any Proxied RADIUS Domain

Automatically authorize any Trusted Kerberos S Realm

Nov 06 08:32,03 SUCCESS: Captive Portal: Authentication Server reconfigured.

Nov 06 08:56,07 SUCCESS: Interface VPN00 is down

Captive Portal Template Manager

Captive Portal Web Login template

192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?STk=5970b8ca0f8da80eeb782efa6424cd9aca149ae6&Action=Render&Object=cp_ ☆

Web Login Template Manager Not saved [Save](#) [Close](#)

[Use customized template](#) [View Source](#) [Image](#)

```
</script>
</head>
<body onload="loaded()">
<form name=data method=post action=zscrp>
<input type=hidden name=Section value=CPAuth>
<input type=hidden name=Action value=Authenticate>
<input type=hidden name=ZSCPRedirect value="<ZS_TAG _ZSCPRedirect">">
<input type=hidden name=Powered value="<ZS_TAG /system/cp/Auth/Custom/Powered">">
<input type=hidden name=RND value="">
<input type=hidden name=Popup value="<ZS_TAG Popup">">
<br><br>
<table width=100%>
<tr>
<td width=15%>
<br><br>
</td>
<td>
<hr color=#ff00ff>
<table width=100%><tr>
<td width=1%><img name=Imagine border=0><br><font class=Smaller1><ZS_TAG /system/cp/Auth/Custom/Image
/Description></font></td><td align=center><font color=#8080c0><ZS_TAG /system/cp/Auth/Custom
/NetDescription></font></td>
</tr></table>
<hr color=#ff00ff>
<table width=100%><tr><td align=right><input type=button name=AAILogin value="<ZS_TAG /system/cp/Auth
/Shibboleth/Button" onclick="AAIauth()"> <input type=button name=x509login value="X.509 Login"
onclick="x509auth()"><script>if ("<ZS_TAG /system/cp/Auth/X509/Enabled" != "yes" || "<ZS_TAG /system
/cp/Auth/NoSSL" == "yes") { document.data.x509login.disabled=true; };if ("<ZS_TAG /system/cp/Auth
/Shibboleth/Enabled" != "yes") { document.data.AAILogin.disabled=true; }</script></td></tr></table>
<br><br>
<table width=100% cellpadding=2 cellspacing=2>
<tr><td align=right><ZS_TAG +cp_msg USERNAME> </td><td><input type=text name=U size=35
onKeyPress="return CheckEnterKey(this,event)"></td></tr>
<tr><td align=right><ZS_TAG +cp_msg PASSWORD> </td><td><input type=password name=P size=35
```


Captive Portal Image Manager

The screenshot displays the Zeroshell Net Services web interface. On the left is a navigation menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The main content area shows the 'Image Manager' window for the 'Web Login Page'.

Image Manager Window:

- URL: `https://192.168.0.75/cgi-bin/kerbynet?Section=CP&STk=`
- Buttons: Save, Close
- Form fields:
 - Description: Otranto (Lecce) - Italy
 - Width: 220
 - Height: 110
 - Image File: Browse...
- Image preview: A landscape photo of a beach and sea.
- File info: Size: 5.9K, Available: 540M (73%)

Background Interface Elements:

- System status: CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz, Uptime: 0 days, 0:28, Load: 0.07 0.18 0.21.
- Authorized Domains table:

Domain Name	Type
<input type="radio"/> ACTIVEDIRECTORY.TEST	External K5
<input type="radio"/> example.com (Default)	Radius (PAP)
<input type="radio"/> test.com	Radius (TTLS)
- Default RADIUS Request: EAP-TTLS with PAP
- Checkboxes: Automatically authorize any Proxied RADIUS Domain, Automatically authorize any Trusted Kerberos 5 Realm
- Log messages at the bottom:

```
Oct 09 19:53,38 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: fulvio@example.com MAC: 44:A7:CF:CD:2F:88) for...
Oct 09 20:07,29 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: pluto@example.com MAC: 44:A7:CF:CD:2F:88) forc...
```

Configure Authorized Kerberos5/RADIUS Domains

ZEROSHELL Net Services

Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)
Uptime 0 days, 0:28
Load Avg 0.07 0.18 0.21 [Graphics](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL Gateway Authentication Accounting Language Graphics Bandwidth

Web Login Authentication Server Status: **ACTIVE** [Save](#) [Show Log](#)

Authorized Domain

Web L 192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?Section=CP&STk=5970b8ca0f8da8

Authorized Domain [Save](#) [Close](#)

Domain Name

Domain Type

Local Kerberos 5 Realm
 External Kerberos 5 Realm
 Trusted Kerberos 5 Realm (*)
 RADIUS Proxy Domain (**)

Radius Request

Notes:

(*) To create a Trusted Kerberos 5 Realm use [K5 Cross-Realm Setup](#) and add an *Outgoing* trust relationship. The same operation you have to do in the foreign KDC but adding an *Incoming* trust relationship with the same password.

(**) RADIUS authentication uses the local RADIUS server to proxy the authentication requests to an external server. To configure the RADIUS Proxy Domains use [Proxy Setup](#)

Authorized Domains [+](#) [-](#) [D](#) [Proxy RADIUS](#)

Domain Name	Type
<input type="radio"/> ACTIVEDIRECTORY.TEST	External K5
<input type="radio"/> example.com (Default)	Radius (PAP)
<input type="radio"/> test.com	Radius (TTLS)

Default RADIUS Request

Automatically authorize any Proxied RADIUS Domain
 Automatically authorize any Trusted Kerberos 5 Realm

Oct 09 19:53,38 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: fulvio@example.com MAC: 44:A7:CF:CD:2F:88) for...
Oct 09 20:07,29 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: pluto@example.com MAC: 44:A7:CF:CD:2F:88) forc...

Proxy Radius

ZEROSHELL Release 1.0.beta16 [About](#)

CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz [Refresh](#)
 Uptime 0 days, 0:28
 Load Avg 0.07 0.18 0.21 [Graphics](#)

192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?Section=Radius&STk=5970b8ca0f8da80eeb782efa6424cd9aca149ae6

RADIUS PROXY DOMAINS + - Close

Type Domain No Strip Proxy Server IP LB Auth Port Acct Port Shared Secret Accounting

Remote Do not proxy

	Realm	Proxy Server	Auth Port	Acct Port	Shared Secret	Acct
<input checked="" type="radio"/>	DEFAULT	10.20.32.111 (NS)	1812		RadiusHub123	no
<input type="radio"/>	EXAMPLE.COM	LOCAL	1812	1813		no
<input type="radio"/>	test.com	172.16.10.234 (NS)	1812	1813	test123Secret	yes

Authorized Domains + - D Proxy RADIUS

Domain Name	Type
<input type="radio"/> ACTIVEDIRECTORY.TEST	External K5
<input type="radio"/> example.com (Default)	Radius (PAP)
<input type="radio"/> test.com	Radius (TTLS)

Default RADIUS Request

Automatically authorize any Proxied RADIUS Domain
 Automatically authorize any Trusted Kerberos 5 Realm

F:CD:2F:88) for...
 F:CD:2F:88) forc...

X.509 Certificate Authentication

ZEROSHELL
Net Services

Captive Portal X.509 Authentication Status: **ACTIVE** Save Close

Allow the X.509 login with the certificates signed by the following Trusted CAs: Trusted CAs Manager

- INFN CA
- AddTrust External CA Root
- ZeroShell Example CA/emailAddress=Fulvio.Ricciardi@zeroshell.net
- TERENA SSL CA
- UTN-USERFirst-Hardware

SP EntityID Button

Request

- Automatically authorize any Proxied RADIUS Domain
- Automatically authorize any Trusted Kerberos 5 Realm

Oct 09 19:53,38 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: fulvio@example.com MAC: 44:A7:CF:CD:2F:88) for...

Oct 09 20:07,29 SUCCESS: Captive Portal: disconnection of the client 192.168.0.10 (User: pluto@example.com MAC: 44:A7:CF:CD:2F:88) forc...

Shibboleth Configuration

ZEROSHELL Release 1.0.beta16
Net Services About

CPU (1) Geode(TM) Integrated Processor by AMD PCS 498MHz Refresh
Uptime 0 days, 0:30
4 0.50 Graphics

192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?STk=b939c8920f60299d7a87f15045f9115e2540dc3f&Action=F

Shibboleth Module Configuration [Running] Close

Software Release [Native] Upgrade Native

BUILD	:	Wed Aug 31 02:06:56 CEST 2011
log4shib	:	1.0.4
opensaml	:	2.4.3
shibboleth-sp	:	2.4.3
xml-security-c	:	1.6.1
xmltooling	:	1.4.2

Configuration Files xml Edit New Remove Copy Verify Reload

- attribute-map.xml
- attribute-policy.xml
- example-metadata.xml
- example-shibboleth2.xml
- protocols.xml
- security-policy.xml
- shibboleth2.xml

SP Metadata Try Authentication Authorization Filter WAYF / IdP Whitelist Cron Job

Nov 06 08:56:07 SUCCESS: Interface VPN00 is down

Request EAP-TTLS with PAP
authorize any Proxied RADIUS Domain
authorize any Trusted Kerberos 5 Realm

Shibboleth Upgrading

The screenshot displays the ZeroShell web interface for Shibboleth Module Configuration. The main window is titled "Shibboleth Module Configuration" and shows the current software release as "1.0.beta16". The configuration is in a "Running" state. A "Shibboleth Upgrade" dialog box is open, prompting the user to select a package for upgrade. The dialog includes a "Package" input field with a "Browse..." button and a "Check the page http://www.zeroshell.net/eng/shibboleth to get the updates" message.

Shibboleth Module Configuration [Running] [Close]

Software Release [Native] [Upgrade] [Native]

BUILD	:	Wed Aug 31 02:06:56 CEST 2011
log4shib	:	1.0.4
opensaml	:	2.4.3
shibboleth-sp	:	2.4.3
xml-security-c	:	
xmlltooling	:	

Shibboleth Upgrading [Upgrade] [Close] [Reload]

Package [Browse...]

Check the page <http://www.zeroshell.net/eng/shibboleth> to get the updates

Configuration Files

- attribute-map.xml
- attribute-policy.xml
- example-metadata.xml
- example-shibboleth2.xml
- protocols.xml
- security-policy.xml
- shibboleth2.xml

[SP Metadata](#) [Try Authentication](#)

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Accounting
- Captive Portal

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS
- Wireless
- Net Balance

SECURITY

- Kerberos
- Firewall
- X.509 CA
- HTTP Proxy

Geode(TM) Integrated Processor by AMD PCS 498MHz

days, 0:28

07 0.18 0.21

Domains [+] [-] [D] [Proxy RADIUS]

Name	Type
DIRECTORY.TEST	External K5
e.com (Default)	Radius (PAP)
n	Radius (TTLS)

RADIUS Request: **EAP-TTLS with PAP**

locally authorize any Proxied RADIUS Domain

locally authorize any Trusted Kerberos 5 Realm

[Cron Job]

Configuring Shibboleth by File Editor

The screenshot displays the ZeroShell web interface for configuring the Shibboleth module. The main window is titled "Shibboleth Module Configuration" and shows a navigation menu on the left with categories like SYSTEM, USERS, NETWORK, and SECURITY. The "Configuration Files" section is active, listing files such as shibboleth2.xml. A "FILE EDITOR" window is open, showing the contents of /etc/shibboleth/shibboleth2.xml. The XML configuration includes session settings, SSO configuration for GARR IDEM Test Federation, and handler definitions for metadata generation and status reporting. A log message at the bottom indicates a successful session opening from host 192.168.0.11 (Admin).

```
<Sessions lifetime="28800" timeout="3600" checkAddress="false" relayState="ss:mem" handlerSSL="false">
  <!--
  Configures SSO for a default IdP. To allow for >1 IdP, remove
  entityID property and adjust discoveryURL to point to discovery service.
  (Set discoveryProtocol to "WAYF" for legacy Shibboleth WAYF support.)
  You can also override entityID on /Login query string, or in RequestMap/htaccess.
  -->

  <!-- GARR IDEM Test Federation -->
  <SSO discoveryProtocol="SAMLDS" discoveryURL="https://wayf.idem-test.garr.it/">
    SAML2 SAML1
  </SSO>

  <!-- SAML and local-only logout. -->
  <Logout>SAML2 Local</Logout>

  <!-- Extension service that generates "approximate" metadata based on SP configuration.
  -->
  <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>

  <!-- Status reporting service. -->
  <Handler type="Status" Location="/Status" acl="127.0.0.1"/>

  <!-- Session diagnostic service -->
```

Identity Provider e WAYF Auto-Discovery

The screenshot displays the Zeroshell Net Services web interface. On the left is a navigation menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The main content area is titled 'Shibboleth Module Configuration' and includes sections for 'Software Release' (listing log4shib, opensaml, shibboleth-sp, xml-security-c, xmltooling) and 'Configuration Files' (listing attribute-map.xml, attribute-policy.xml, example-metadata.xml, example-shibboleth2.xml, protocols.xml, security-policy.xml, shibboleth2.xml). A 'WAYF / IdP Whitelist' dialog box is open, showing a list of whitelisted URLs: https://wayf.idem-test.garr.it, https://idp2.idem.garr.it, https://idp.poliba.it, and https://shidp.caspur.it. The 'Autodiscovery' checkbox is checked. At the bottom of the dialog are buttons for 'Authorization Filter', 'WAYF / IdP Whitelist', and 'Cron Job'. The background interface also shows a 'Bandwidth' section with 'Save' and 'Show Log' buttons, and a 'Proxy RADIUS' section with a table of RADIUS servers.

	Type
RY.TEST	External K5
(default)	Radius (PAP)
	Radius (TTLS)

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

Shibboleth Module Configuration [Fault] [Close]

Check Configuration UNLOADABLE [Retry] [Close]

FATAL	:	1
CRITICAL	:	0
ERROR	:	2
WARNING	:	0

2011-10-10 19:54:46 ERROR XMLTooling.ParserPool : fatal error on line 105, column 9, message: unterminated end tag 'MetadataProvider'
2011-10-10 19:54:46 ERROR Shibboleth.Config : error while loading resource (/etc/shibboleth/shibboleth2.xml): XML error(s) during parsing, check log for specifics
2011-10-10 19:54:46 FATAL Shibboleth.Config : caught exception while loading configuration: XML error(s) during parsing, check log for specifics

Oct 10 19:52,57 SUCCESS: File Editor: /etc/shibboleth/shibboleth2.xml successfully saved
Oct 10 19:53,07 ERROR: Shibboleth: module not started

Perl Authorization Filters

The screenshot displays the ZeroShell Net Services web interface. The main navigation menu on the left includes sections for SYSTEM, USERS, NETWORK, and SECURITY. The main content area is titled 'Captive Portal' and contains several configuration panels. The 'Shibboleth Authentication' panel is active, showing the status as 'Enabled' and the SP EntityID as 'https://zeroshell...'. A modal window titled 'Shibboleth Module Configuration' is open, showing the 'AuthZ Filter' configuration. The 'Filter String' field contains the following Perl-like expressions:

```
# Authorization Filter is applied after the authentication to state if the user
# is authorized to access. It is based on the environment variables set by the
# Identity Provider.
# The syntax of the conditions is Perl-Like.

$ENV{affiliation} eq "member@example.com"
or
$ENV{mail} =~ m/.*@zeroshell.net$/
or
$ENV{REMOTE_USER} eq "fulvio@test.com"
```

Below the filter string, there are links for 'Test and view IdP Environment' and 'Perl Regular expressions'. The status of the filter is shown as 'Filter ON'.

Try Authentication

The screenshot shows a web browser window titled "Trying Shibboleth Authentication" with the URL `https://192.168.0.75/cgi-bin/kerbynet?STk=272b21ea87f93713e8b8ccd67bcc420f483a755e&Section=CP&Action=ShibTryAu`. The main content is a "Shibboleth Authentication Test" dialog box. The dialog box contains the IDem logo (a red stick figure with a smiley face) and the text "Select your Home Organisation". Below this, it states: "In order to access a Resource on host 'jamesbond.le.inf.n.it' you must authenticate yourself." There is a dropdown menu with "GARR FI idp215" selected and a "Select" button. A checkbox labeled "Remember selection for this web browser session." is also present. The background shows a ZeroShell Net Services menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balance), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The browser's address bar shows "192.168.0.75" and "192.168.0.75". The browser's title bar shows "Trying Shibboleth Authentication". The browser's status bar shows "Oct 08" and "Oct 08".

Cron Job

The screenshot displays the Zeroshell web interface. On the left is a navigation menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The main content area is titled 'SCRIPTING EDITOR' and shows a 'Cron Shibboleth script' with a status of 'Disabled'. The script content is as follows:

```
# 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
```

Below the script editor is a 'Jobs Scheduling' section with dropdown menus for Hour (Any), Minute (Any), Day (Any), Month (Any), Day of the week (Any), and Every (2 hours). A 'System Clock' shows the time as 'Sun Oct 9 23:41:10 CEST 2011'. At the bottom, a log entry reads: 'Oct 09 23:38,16 SUCCESS: Shibboleth'.

Log Viewer

ZEROSHELL
Net Services

Log Viewer
192.168.0.75 https://192.168.0.75/cgi-bin/kerbynet?Section=LOG&STk=185a8ed2e0cf2837c74fbdeeb2b43845172e7f5c&Action=I

LOG VIEWER Host: zeroshell (Local) Section: CaptivePortal Filter: [] Refresh Close

2011 Oct 09

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

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: ocspl.tcs.terena.org (149.5.128.169:80) successfully unlocked
12:01:08 CRL/OCSP: Success: ocspl.tcs.terena.org (91.199.212.169:80) successfully unlocked
12:01:08 CRL/OCSP: Success: ocspl.tcs.terena.org (91.209.196.169:80) successfully unlocked
12:01:09 CRL/OCSP: Success: ocspl.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

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



Release 1.0.beta16
[About](#)

CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)

Uptime 0 days, 4:21

Load Avg 0.56 0.68 0.71 [Graphics](#)

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL
Gateway
Authentication
Accounting
Language
Graphics
Bandwidthd

User Accounting **Status: ACTIVE**
[Save](#) [Show Log](#)

Entries: 3 [Details](#) [Remove](#) Filter [Refresh](#)

	Username	Traffic (MB)	Time	Cost (€)	Credit (€)	Last Update
<input type="radio"/>	fulvio	515.11	0:19	0.00	0.00	10/09/11 12:23
<input type="radio"/>	pluto	2088.77	1:07	0.00	0.00	10/09/11 13:31
<input checked="" type="radio"/>	wrsqpet0zknba0zp7sr0quidpao_@ldp2.ldem.qarr.it	3.42	1:16	0.00	0.00	10/09/11 13:31

Parameters

Currency Symbol

Decimal Places

Accounting Classes [Add](#) [Change](#) [Delete](#)

Name	MBytes	Hours	Mbit/s	Cost/MB	Cost/H
<input type="radio"/> DEFAULT	-	-	-	0.00€	0.00€

Oct 09 13:30,52 SUCCESS: Session closed for Admin user

Oct 09 13:30,55 SUCCESS: Session opened from host 192.168.0.11 (Admin)

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

Radius Accounting Details

ZEROSHELL Net Servi Release 1.0.beta16 [About](#) CPU (1) **Geode(TM) Integrated Processor by AMD PCS 498MHz** [Refresh](#)
Uptime 0 days, 0:4 [Graphics](#)

Accounting Details

192.168.0.75 <https://192.168.0.75/cgi-bin/kerbynet?Section=Acct&STk=129c1da83e892b0ec700e067728c41bf1b8c3527&Action=ShowDet>

fulvio [Refresh](#) [Close](#) [Save](#) [Show Log](#)

Traffic : 522.15 MB
Time : 0:55
Cost : 0.00 € Credit: 0.00 € [+](#) [-](#)

Sessions : 4

	Client Identification	NAS	Start Time	Stop Time	RX (MB)	TX (MB)	Traffic (MB)	Time	Cost (€)	Last Update
<input type="radio"/>	192.168.0.11 / 00:19:e3:03:65:aa	zershell	10/09/11 20:28:22		1.63	0.32	1.94	0:11:00	0.00	10/09/11 20:39
<input type="radio"/>	00:19:e3:03:65:aa	AP-01	10/09/11 18:59:44	10/09/11 19:24:50	4.63	0.47	5.10	0:25:06	0.00	10/09/11 19:24
<input type="radio"/>	192.168.0.11 / 00:19:e3:03:65:aa	zershell	10/09/11 12:23:30	10/09/11 12:23:48	0.02	0.00	0.02	0:00:18	0.00	10/09/11 12:23
<input type="radio"/>	192.168.0.11 / 00:19:e3:03:65:aa	zershell	10/09/11 12:03:34	10/09/11 12:22:28	503.60	11.49	515.09	0:18:54	0.00	10/09/11 12:22

Oct 09 20:28,34 SUCCESS: Session opened from host 192.168.0.11 (Admin)

Connection Tracking

The screenshot displays the Zeroshell Net Service interface. On the left is a navigation menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Accounting, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), and SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy). The main window is titled 'Log Viewer' and shows a list of connection tracking logs. The logs are filtered by Host 'zeroshell (Local)', Section 'ConnTrack', and Filter '95.110.132.149'. The logs show various TCP connections, including SYN_SENT and DESTROY events, with details on source/destination IP addresses, ports, packets, and bytes.

LOG VIEWER Host: zeroshell (Local) Section: ConnTrack Filter: 95.110.132.149

2011 Oct 09

19:11:37 [DESTROY] tcp 6 src=192.168.0.11 dst=95.110.132.149 sport=51223 dport=80 packets=19 bytes=1511 src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51223 packets=31 bytes=38531

19:11:37 [DESTROY] tcp 6 src=192.168.0.11 dst=95.110.132.149 sport=51224 dport=80 packets=7 bytes=1008 src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51224 packets=5 bytes=1085

19:11:42 [DESTROY] tcp 6 src=192.168.0.11 dst=95.110.132.149 sport=51227 dport=80 packets=7 bytes=1132 src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51227 packets=5 bytes=1085

19:11:48 [DESTROY] tcp 6 src=192.168.0.11 dst=95.110.132.149 sport=51226 dport=80 packets=1161 bytes=62713 src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51226 packets=2026 bytes=2691730

19:11:50 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51235 dport=22 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=22 dport=51235

19:12:02 [DESTROY] tcp 6 src=192.168.0.11 dst=95.110.132.149 sport=51228 dport=22 packets=65 bytes=6181 src=95.110.132.149 dst=192.168.1.75 sport=22 dport=51228 packets=44 bytes=6884

19:13:56 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51240 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51240

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51242 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51242

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51243 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51243

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51244 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51244

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51245 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51245

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51246 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51246

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51247 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51247

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51249 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51249

19:13:57 [NEW] tcp 6 120 SYN_SENT src=192.168.0.11 dst=95.110.132.149 sport=51250 dport=80 [UNREPLIED] src=95.110.132.149 dst=192.168.1.75 sport=80 dport=51250

Captive Portal Statistics

ZEROSHELL Net Services

Release 1.0.beta16
[About](#)

CPU (2) **AMD Opteron(tm) Processor 252** Refresh
2589MHz
Uptime 37 days, 2:9 Graphics

CP Statistics
infn.it https://jamesbond.le.infn.it/cgi-bin/kerbynet?STk=e6d54c58a581563b733d19779267e2dbcffda800&Action=Render

CAPTIVE PORTAL STATISTICS Captive Portal Refresh Close

Number of connected users

Weekly' Graph (30 Minute Average)

Day	Max	Average	Current
Sat	15.0 # (0.1%)	2.0 # (0.0%)	0.0 # (0.0%)
Sun			
Mon			
Tue			
Wed			
Thu			
Fri			
Sat			

Monthly' Graph (2 Hour Average)

Powered by MRTG - Multi Router Traffic Grapher

Nov 05 16:29,02 SUCCESS: Session closed for Admin user
Nov 06 10:29,27 SUCCESS: Session opened from host 193.206.153.81 (Admin)

Bandwidthd Save Show Log

MAC address

minutes Popup

MAC Address

- 00:01:E3:76:EB:DC
- 00:18:41:54:3A:66
- Any
- 00:1C:7A:00:42:85
- 00:16:EA:57:60:00
- 00:23:6C:ED:6C:DF
- 00:1E:64:08:3A:AA
- 9C:18:74:D7:29:9B
- Any
- Any
- Any
- 1C:4B:D6:B7:0A:CE
- 00:1D:D9:15:EC:EE

Traffic Shaping e QoS

Release 1.0.beta16

ZEROSHELL Net Services

QoS Class Manager

https://joe.le.infn.it/cgi-bin/kerbynet

QoS - CLASS MANAGER [Save] [New] [Delete] [Close]

GRID_WN Description: GRID Worker Nodes

Priority: Medium DSCP: [] Maximum: 500 Mbit/s Guaranteed: [] Mbit/s

Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed	On
<input type="radio"/> AFS	Andrew File System	Low			100Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> DEFAULT	Default class for unclassified traffic	Medium				<input checked="" type="checkbox"/>
<input type="radio"/> FTP	File Transfer Protocol	Low		200Mbit/s	50Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> GRID	GRID Elements Traffic	High			100Mbit/s	<input checked="" type="checkbox"/>
<input checked="" type="radio"/> GRID_WN	GRID Worker Nodes	Medium		500Mbit/s		<input checked="" type="checkbox"/>
<input type="radio"/> LARGE	Large Transfer	Low		300Mbit/s		<input checked="" type="checkbox"/>
<input type="radio"/> LDAP	LDAP and LDAPs	High			1Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> LIMITED	Limited	Low		12Mbit/s		<input checked="" type="checkbox"/>
<input type="radio"/> LIMITED2	Limited 2	Medium		1Mbit/s		<input checked="" type="checkbox"/>
<input type="radio"/> NOLIMIT	Not Limited	Medium				<input checked="" type="checkbox"/>
<input type="radio"/> P2P	Peer to Peer file sharing	Low		128Kbit/s		<input checked="" type="checkbox"/>
<input type="radio"/> SCP	Secure Copy	Low		200Mbit/s	50Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> SMTP	Mail Transfer	Low			1Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> SSH	Secure Shell Interactive	High				<input checked="" type="checkbox"/>
<input type="radio"/> TEST	Test	High		5Mbit/s	5Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> UDP	UDP	Medium				<input checked="" type="checkbox"/>
<input type="radio"/> VOIP	Voice and Video over IP	High			10Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/> WWW	World Wide Web	Medium			10Mbit/s	<input checked="" type="checkbox"/>

Bandwidthd L7 Filter

Global Bandwidth [On] [Add Class] [Modify Class] [Remove Class]

Global Bandwidth [On] [Add Class] [Modify Class] [Remove Class]

Classificazione del traffico in classi di QoS

QoS		Apply to	Sequence		
		Routed and Bridged Packets	64	+	-
				Confirm	Close
Packet Matching	Description	Value	Not		
	Input	<input type="text"/>	<input type="checkbox"/>		
	Output	<input type="text"/>	<input type="checkbox"/>		
	Source IP (*)	<input type="text"/>	<input type="checkbox"/>		
	Destination IP	<input type="text"/>	<input type="checkbox"/>		
	Fragments	[<input type="checkbox"/> match only second and further fragments]	<input type="checkbox"/>		
	Packet Length	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>		
	Source MAC	<input type="text"/>	<input type="checkbox"/>		
Protocol Matching <input type="checkbox"/> Not	Match all Layer 4 Protocols				
<input type="text" value="ALL"/>					
Connection State <input type="checkbox"/> Not	<input type="checkbox"/> NEW <input type="checkbox"/> ESTABLISHED <input type="checkbox"/> RELATED <input type="checkbox"/> INVALID <input type="checkbox"/> UNTRACKED				
IPTABLES Parameters	<input type="text"/>				Manual
Time Matching	From <input type="text"/> : <input type="text"/> to <input type="text"/> : <input type="text"/>		<input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun		
Layer 7 Filters	Protocol Description <input type="checkbox"/> Not				L7 Manager
	<input type="text" value="SIP - Session Initiation Protocol - Internet telephony - RFC 3261, 3265, etc."/>				
DiffServ	DSCP	<input type="text"/>			
Connection Limits	Parallel connections per IP <input type="text"/> more than <input type="text"/>		Traffic per connection <input type="text"/> more than <input type="text"/> MB		
TARGET CLASS	<input type="text" value="VOIP"/>	<input type="checkbox"/> LOG <input type="text"/>		/	<input type="text" value="Second"/> Burst <input type="text"/>

NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
 (**) TCP and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)