Captive-portal: accesso autenticato alla rete geografica

L'esperienza dell'Università Politecnica delle Marche

Daniele Ripanti (d.ripanti@univpm.it)

WS_GARR, 18 Giugno 2009

Agenda:

Autenticazione degli utenti

Il sistema implementato

Pro e contro della soluzione

Demo

Obiettivo del progetto

Implementazione di un sistema di autenticazione per l'accesso degli utenti dell'Ateneo alla rete geografica con l'obiettivo di adeguare l'infrastruttura ai requisiti imposti dalla normativa.

I requisiti della soluzione:

- Contenimento dei costi di implementazione;
- Interventi ridotti nelle configurazioni delle reti interne delle strutture e dei singoli desktop utente;
- Tempi di implementazione ridotti e complessità tecnologica degli interventi "accettabile";
- Mantenimento dei servizi da sempre garantiti;
- Affidabilità della soluzione;
- Facilità di utilizzo.

Soluzione utilizzata

- Un captive-portal è un gateway che abilita il traffico di rete delle postazioni utente in seguito ad una procedura di login mediante interfaccia web;
- L'utente che accede alla rete mediante un browser e non ha effettuato l'autenticazione, viene indirizzato "in automatico" ad una pagina web di login;
- In seguito alla validazione delle credenziali, la postazione viene attivata dal gateway e l'utente può "navigare".

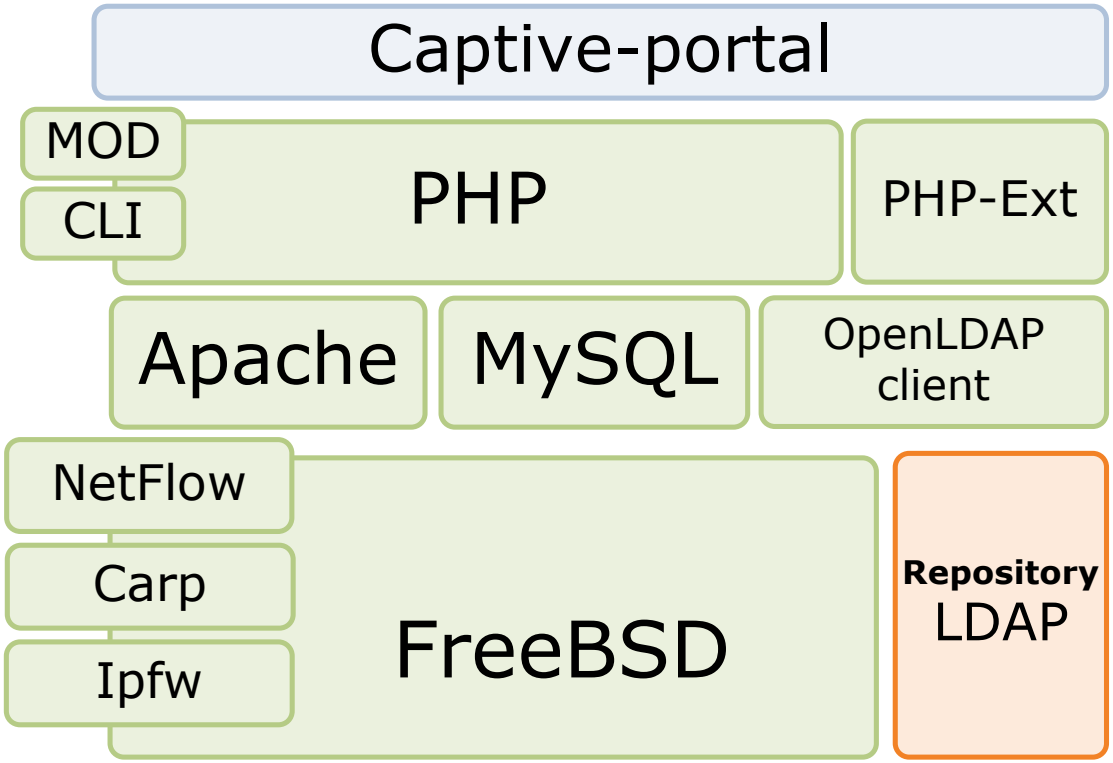
Ambito di applicazione nel nostro Ateneo

Il captive-portal viene utilizzato per l'autenticazione nelle connessioni:

- **Wired:**
  - Desktop utenti **-** personale dei dipartimenti, centri, etc.;
  - Biblioteche **-** accessi alla rete con postazioni presenti nei locali;
  - Internet point - chioschi per la distribuzione di servizi di rete installati negli spazi assegnati agli studenti e punti di accesso alle strutture (ingressi, etc.);
  - Laboratori informatici.
- **Wireless:**
  - Personale dei dipartimenti;
  - Eventi: convegni, workshop, etc.

Software e componenti

Il captive-portal è stato sviluppato dal nostro Ateneo e utilizza le seguenti tecnologie open source:

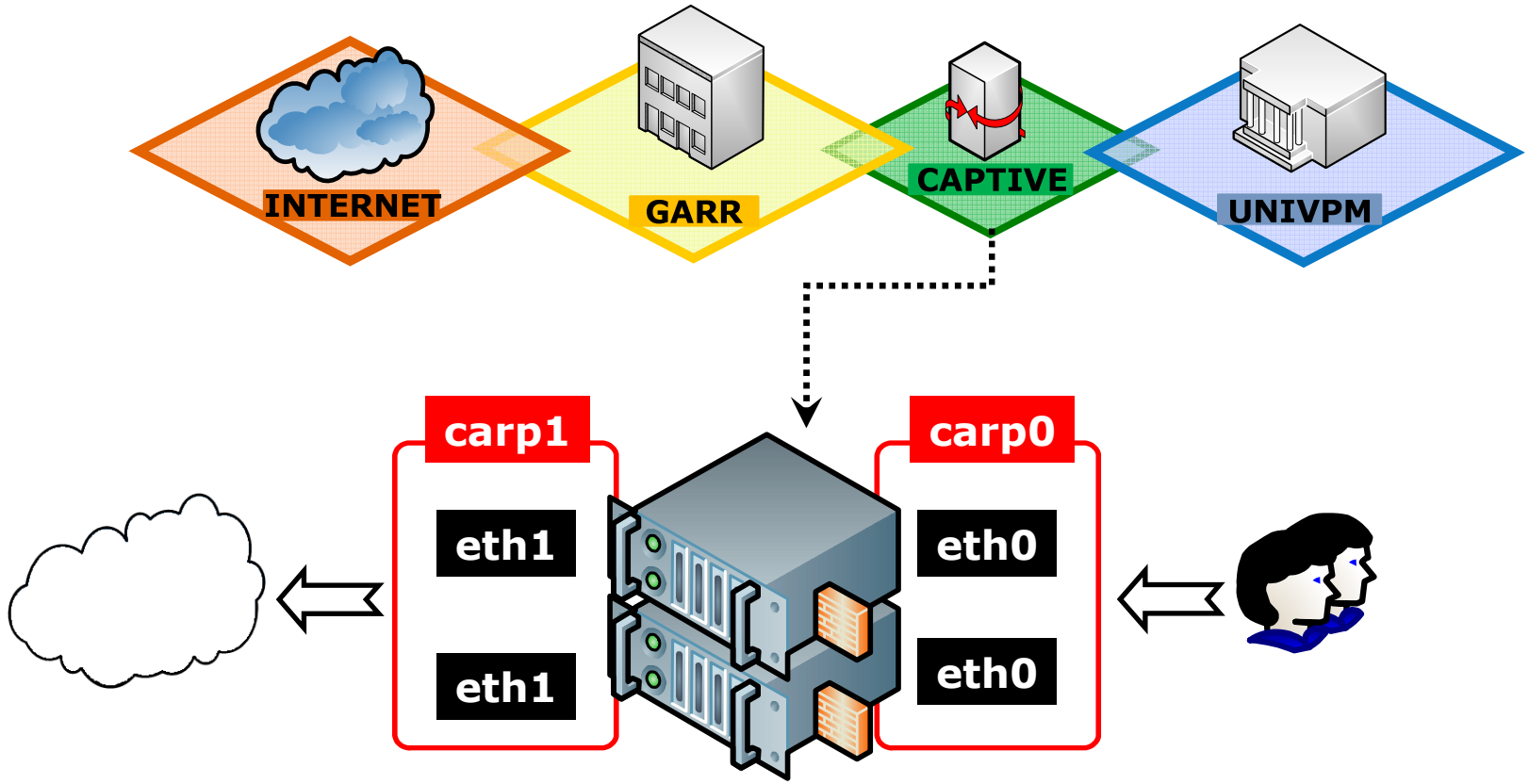


Attivazione del sistema

L'implementazione e la diffusione hanno comportato:

- L'installazione di un sistema HA con funzioni di routing del traffico di rete della rete UNIVPM;
- La configurazione del sistema di monitoraggio/registrazione delle connessioni;
- La definizione delle regole di firewall e in generale delle policy di accesso ad Internet (tabelle di utenti, porte, banda, etc.);
- Il censimento dei server presenti nella rete di Ateneo;
- La realizzazione dell'applicazione e il test;
- La definizione di ruoli e procedure per l'aggiornamento del repository di utenti;
- L'assistenza iniziale all'utenza attraverso documenti informativi, mail e help desk.

Schema della rete



Tempi di sviluppo e diffusione

- **GIUGNO 2008**

  Realizzazione dell'applicazione e sperimentazione CARP

- **LUGLIO 2008**

  Attivazione del sistema presso la Facoltà di Medicina

- **SETTEMBRE 2008**

  Attivazione presso la Facoltà di Economia

- **DICEMBRE 2008**

  Acquisizione delle attrezzature hardware

- **MARZO 2009**

  Attivazione del sistema di autenticazione in Ateneo

Applicazione: supporto “multi-firewall”

- Il captive-portal supporta i firewall Unix
  - IPFW
  - PF
  - IPTABLES
- L’amministratore può definire il firewall in uso attraverso il file di configurazione dell’applicazione e integrare facilmente le policy già esistenti;
- Il supporto dei 3 firewall elencati ha permesso la diffusione della soluzione nelle strutture dove sono presenti firewall/NAT server amministrati da personale interno.

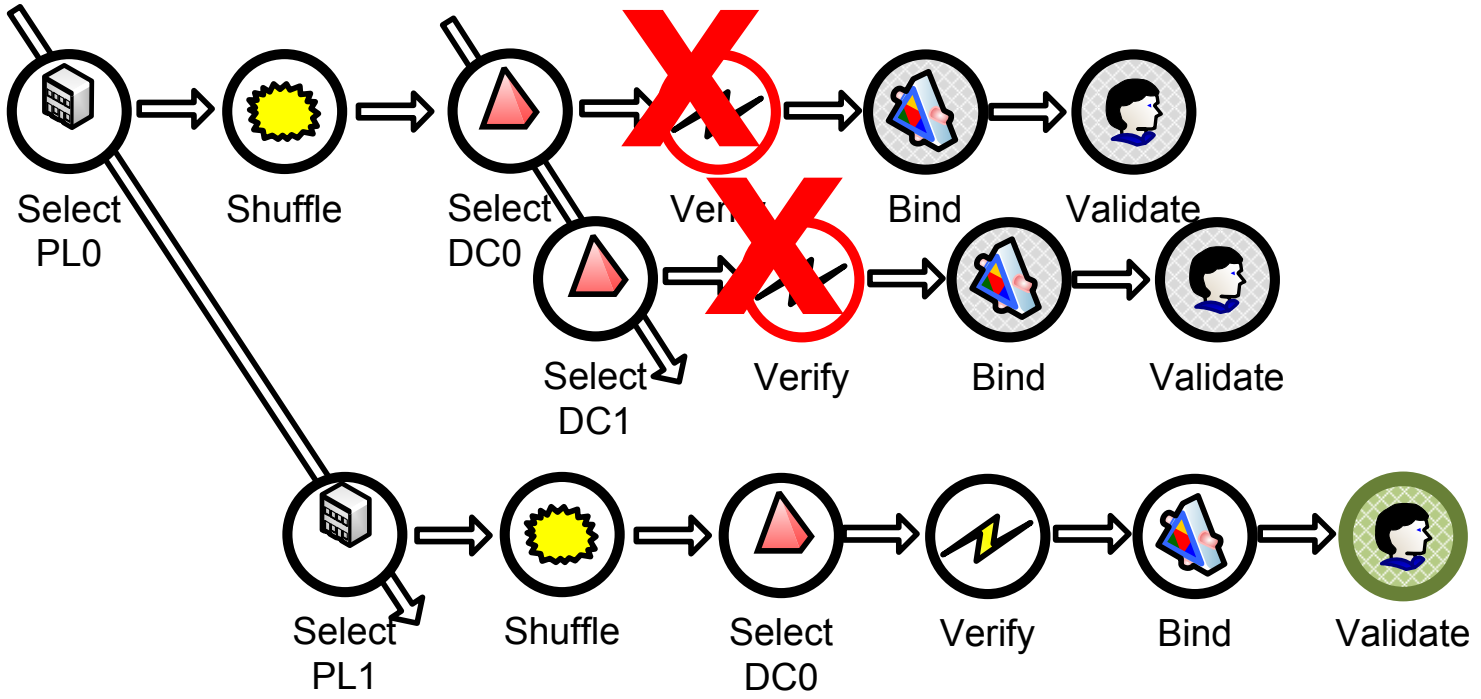
Applicazione: supporto “multilingua”

- Il captive-portal è “localizzato” in ITALIANO, INGLESE, FRANCESE, TEDESCO, SPAGNOLO, ALBANESE, CINESE e permette l’integrazione di altre lingue attraverso i file-dizionari;
- Il dizionario caricato per default è basato sulla lingua del browser che accede alla homepage dell’applicazione. L’utente può impostare la lingua e mantenere il dizionario richiesto per tutta la sessione di lavoro;
- Il supporto multilingua è stato implementato per garantire un facile utilizzo anche da parte del personale interno, studenti stranieri (es: Erasmus), ospiti delle strutture e partecipanti a convegni;
- I dizionari sono stati realizzati e aggiornati in collaborazione con il Centro Linguistico e il personale della Biblioteca.

Applicazione: accesso a LDAP e DBMS

- Il repository principale degli utenti è accessibile mediante LDAP;
- Il contenitore è basato su una infrastruttura MS Active Directory con diversi Domain Controller;
- Il captive-portal verifica le credenziali interrogando un DC disponibile dell'infrastruttura.
  La selezione avviene:
  - in base alla gerarchia di plessi in "ordine di vicinanza";
  - poi mediante creazione di una lista di DC del plesso "in uso" ordinata in modo casuale ad ogni verifica effettuata.
- Le credenziali per l'accesso alla rete sono le stesse usate in altre applicazioni (es: risorse elettroniche, servizi amministrativi –> cartellini, piani di studio…..).

Applicazione: algoritmo di selezione del server LDAP



Applicazione: rinnovi delle connessioni

- La connessione è garantita da un sistema di rinnovo automatico basato sulla validazione del token assegnato dal server al momento dell'attivazione dell'accesso;
- Il rinnovo viene effettuato mediante codice AJAX integrato nella pagina web e messaggi XML di risposta del server;
- Il server esegue periodicamente una pulizia automatica delle connessioni che non sono state rinnovate dal client dopo un numero di volte stabilito;
- Numero di rinnovi mancati, frequenza di verifica e rinnovo del token sono parametri di configurazione modificabili dall'amministratore di sistema e possono tenere conto di diversi scenari (es: numero di connessioni simultanee, prestazioni del sistema etc.).

Applicazione: controllo accessi

E' possibile definire:

- BLACKLIST di utenti

  Il repository LDAP è organizzato per FACOLTA'->TIPO UTENTE.

  L'applicazione web consulta un elenco degli utenti che non possono autenticarsi nonostante la validità delle credenziali.

  La blacklist permette di disattivare l'accesso ad Internet e conservare altri servizi (es: logon alla rete interna, servizi web locali etc.);

- BLACKLIST di IP

  E' possibile disabilitare l'attivazione di indirizzi IP;

- RETI "accreditate"

  L'applicazione autorizza login solo dalle reti definite "valide".

Applicazione: validazione XHTML e browser supportati

- L'applicazione produce codice XHTML validato;
- Attualmente sono state effettuate verifiche e test con i browser:
  - MS Internet Explorer 6.x, 7.x, 8.x
  - Mozilla Firefox 2.x, 3.x
  - Google Chrome
  - Safari 2.x
- Il supporto Javascript deve essere attivo per garantire il corretto funzionamento del codice AJAX impiegato per i rinnovi automatici delle connessioni;
- Gli utenti Unix (senza X e un browser) possono usare uno script shell (#!/bin/sh) per attivare e rinnovare la connessione di rete.

Sistema principale: CARP overview (1)

- Il sistema principale è basato su 2 server UNIX con il supporto CARP;
- CARP è l'acronimo di Common Address Redundancy Protocol;
- Implementa un meccanismo di failover per la configurazione di sistemi in alta affidabilità;
- E' utilizzabile per la realizzazione di router ma può essere impiegato anche per rendere ridondanti altri servizi di rete (es: web server, etc.);
- Supporta IPv4 e IPv6, è open source, libero da brevetti e licenze;
- I sistemi basati su CARP possono essere "asimmetrici" e a bilanciamento del carico;

Sistema principale: CARP overview (2)

- E' un protocollo di rete implementato dagli sviluppatori di OpenBSD ed è stato distribuito con il sistema operativo a partire dalla release 3.5 (Maggio 2004);
- Il protocollo è stato integrato successivamente in FreeBSD, NetBSD e Linux;
- Cisco ha sviluppato HSRP (Host Standby Redundancy Protocol) e l'IETF il VRRP (Virtual Router Redundancy Protocol). CARP introduce la funzionalità di crittografia degli "avvisi" mediante SHA1 HMAC;
- Il numero di protocollo ip assegnato dal team di OpenBSD è il 112, lo stesso di VRRP. IANA non lo ha mai registrato per mancanza di specifiche "formali";

Sistema principale: CARP overview (3)

- Nello scenario "cluster asimmetrico", il protocollo prevede:
  - L'elezione di un server MASTER che invia regolarmente un messaggio multicast di "presenza";
  - Un gruppo di server SLAVE che rimangono in ascolto degli avvisi inviati dal MASTER;
  - Nel caso di fault del MASTER e la conseguenze mancanza di invio di segnalazioni, il gruppo di server SLAVE iniziano l'invio di messaggi per la richiesta di elezione a server MASTER;
  - Il server SLAVE "più veloce" diventa il nuovo MASTER. La velocità è basata sulla frequenza delle segnalazioni che può essere configurata dall'amministratore;

Sistema principale: CARP overview (4)

- E' definito il "group of redundancy" come l'insieme di server che partecipano al cluster CARP;

- Ogni server del cluster CARP ha:
  - Un ip "unico" per ogni interfaccia fisica;
  - Il mac address assegnato dal vendor della scheda;
  - Uno o più ip "condivisi" per gruppi/interfaccia;
  - Un mac address "virtuale" condiviso;

Sistema principale: elezione del server MASTER CARP

ADVBASE (default 1)

ADVSKEW (default 0)

HOST A

- ADVBASE = 1
- ADVSKEW = 0
- Contatore 1 + 0/255 = **1**

HOST B

- ADVBASE = 1
- ADVSKEW = 100
- Contatore 1 + 100/255 = **1,39**

Attraverso la definizione del valore più **basso** si può decidere una elezione "forzata" del server MASTER.

CARP: struttura dell'avviso (1)

ip_carp.h

```
/*
 * The CARP header layout is as follows:
 *     0                   1                   2                   3
 *     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |Version| Type  | VirtualHostID |    AdvSkew    |    Auth Len   |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |   Reserved    |     AdvBase   |          Checksum             |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                            Counter (1)                        |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                            Counter (2)                        |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                          SHA-1 HMAC (1)                       |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                          SHA-1 HMAC (2)                       |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                          SHA-1 HMAC (3)                       |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                          SHA-1 HMAC (4)                       |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 *    |                          SHA-1 HMAC (5)                       |
 *    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 */
```

CARP: struttura dell'avviso (2)

- **Version -** Versione del protocollo CARP
- **Type -** Tipo di CARP_ADVERTISEMENT (settato a 0x01)
- **VirtualHostID -** ID del gruppo
- **ADVSkew -** Ritardo di invio dei pacchetti ADV
- **AuthLen -** Lunghezza dell'autenticazione
- **Reserved -** Utilizzi futuri
- **ADVBase -** Frequenza di invio dei pacchetti
- **Checksum -** Controllo di integrità del pacchetto
- **Counter 1 e 2 -** Contatori
- **SHA1-MAC -** 20 bytes contenente la password dei 36 totali

CARP: riferimenti

Alcuni riferimenti utili:

- **Wikipedia**
  http://en.wikipedia.org/wiki/Common_Address_Redundancy_Protocol
- **Documentazione FreeBSD**
  http://www.freebsd.org/doc/en/books/handbook/carp.html
- **Manpage OpenBSD**
  http://www.openbsd.org/cgi-bin/man.cgi?query=carp&sektion=4
- **Un esempio di configurazione**
  http://www.countersiege.com/doc/pfsync-carp/

Sistema principale: Netflow overview (1)

- Il sistema principale implementa il sistema NetFlow;
- NetFlow è un sistema per il monitoraggio del traffico di rete;
- Si basa sulla registrazione di "flussi" di dati;
- Un flusso di dati è definito come l'insieme di pacchetti che passano per un dispositivo e che hanno i seguenti campi uguali:
  - Indirizzo IP sorgente
  - Porta sorgente
  - Indirizzo IP destinazione
  - Porta destinazione
  - Tipo di protocollo
  - Tipo di servizio
  - Interfaccia di passaggio

Sistema principale: NetFlow overview (2)

- I flow sono mantenuti nella cache del "device-netflow" e sono registrati:
  - Quando una "trasmissione" risulta conclusa;
  - Quando si supera un determinato periodo di tempo di trasmissione (def: 30 minuti);
  - Quando la connessione risulta inattiva per un periodo di tempo stabilito (def: 15 secondi);
  - I flow contengono:
    - Timestamp di inizio e fine del flow
    - Ip sorgente e destinazione
    - Porta sorgente e destinazione
    - Pacchetti e bytes contenuti nel flow
    - Ip protocol / Tipo di servizio
    - Tutti i flags TCP del flow registrato

Sistema principale: NetFlow (3)

- Il traffico di rete viene conservato attraverso pacchetti che implementano il protocollo NETFLOW (softflowd e flow-tools);
- L'archiviazione è organizzata per "giorno" e flow di 5 minuti ciascuno;
- Tutti i log sono archiviati in un NAS "dedicato" e supporti esterni;
- L'Ateneo registra circa **1GB** di log in formato netflow.

NETFLOW: riferimenti

Alcuni riferimenti utili:

- **Wikipedia**
  http://en.wikipedia.org/wiki/Netflow
- **GARR**
  http://www.garr.it/documenti/GARR-03-001.pdf
- **Documentazione Cisco**
  http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- **Softflowd**
  http://www.mindrot.org/projects/softflowd/
- **Flow-tools**
  http://www.splintered.net/sw/flow-tools/

Sistema principale: CAPTIVE-LOG

- Il captive-portal ha un suo log file e contiene:
  - le autenticazioni (valide e non) degli utenti;
  - i rinnovi automatici;
  - Registrazioni relative a connessioni chiuse dal “cleaner” di sistema;
- Il log contiene il messaggio che descrive l’operazione effettuata ma anche la codifica dello stato;
- L’Ateneo registra circa **13MB** di log al giorno, archiviati e duplicati nel NAS dedicato.

Sistema principale: aggiornamenti del codice

- Gli amministratori di rete che mantengono in autonomia server NAT e Firewall interni nelle strutture di appartenenza, hanno accesso ad un server subversion per il download degli aggiornamenti del codice;
- Il file di configurazione contiene informazioni sulle revisioni e viene distribuito in modo da garantire eventuali schedulazioni degli aggiornamenti;
- Il mantenimento dell'applicazione è assicurato dal Centro Informatico;
- E' in corso una attività di riordino dell'infrastruttura di rete diretta al contenimento del numero di nat/firewall server installati presso strutture periferiche.

Diffusione: PRO (1)

- **Semplicità di utilizzo**. L'utente accede alla rete attraverso una pagina web e mediante login con le credenziali che utilizza abitualmente per altri servizi;
- **Connessione "automatica"**. Le postazioni degli utenti accedono al ad Internet dopo il forward della connessione web al "server locale". L'utente non deve ricordarsi l'indirizzo web del captive-portal, registrarlo nel bookmark, etc.;
- **Nessuna installazione di software "client-side"**. Tutti i sistemi operativi degli utenti integrano un browser web. Non è necessario pianificare l'installazione di pacchetti nei computer distribuiti.

Diffusione: PRO (2)

- **Costi contenuti**. Esistono numerose soluzioni open source. La realizzazione di una applicazione web ad-hoc ha richiesto risorse e tempi di sviluppo non “significativi”. La distribuzione ha richiesto pochi interventi centralizzati;
- **Adattabilità**. La soluzione può essere impiegata in diversi scenari;
- **Personalizzazione del codice**. L’applicazione ha incluso funzionalità specifiche per le nostre esigenze (es: supporto IPFW, dizionari, AD etc.);
- **Facilità di mantenimento della soluzione**. Si possono usare in alternativa distribuzioni di Linux/BSD (es: Zeroshell, Pfsense, M0n0wall). Unix e i pacchetti installati (es: Apache) sono strumenti utilizzati anche in altri servizi di Ateneo;

Diffusione: PRO (3)

- **Gestione delle utenze esterne.** La soluzione che abbiamo implementato integra pannelli di amministrazione dei "chioschi". L'operatore, in seguito alla registrazione di un documento, può attivare una postazione senza inserire credenziali di accesso (gli utenti "esterni" non hanno account istituzionali e non si effettuano registrazioni di schede "temporanee");

- **Utilizzo del repository utente**. L'applicazione utilizza l'infrastruttura AD presente in Ateneo mediante un algoritmo di selezione "affidabile" del Domain controller. Il sistema tiene conto della struttura di server organizzati per plessi in modo da garantire la distribuzione del carico delle query di verifica delle credenziali.

Diffusione: CONTRO (1)

- **Sicurezza**.

  Tecnologie captive-portal possono essere soggette a “sniffing” degli ip attivi.

  L’applicazione sviluppata integra il meccanismo dei rinnovi periodici mediante scambio di un token assegnato dal server al momento della prima autenticazione. Credenziali e token sono distribuiti mediante connessione https. Solo il client “autorizzato” può rinnovare e mantenere attiva la connessione. La frequenza dei rinnovi è decisa dall’amministratore del server;

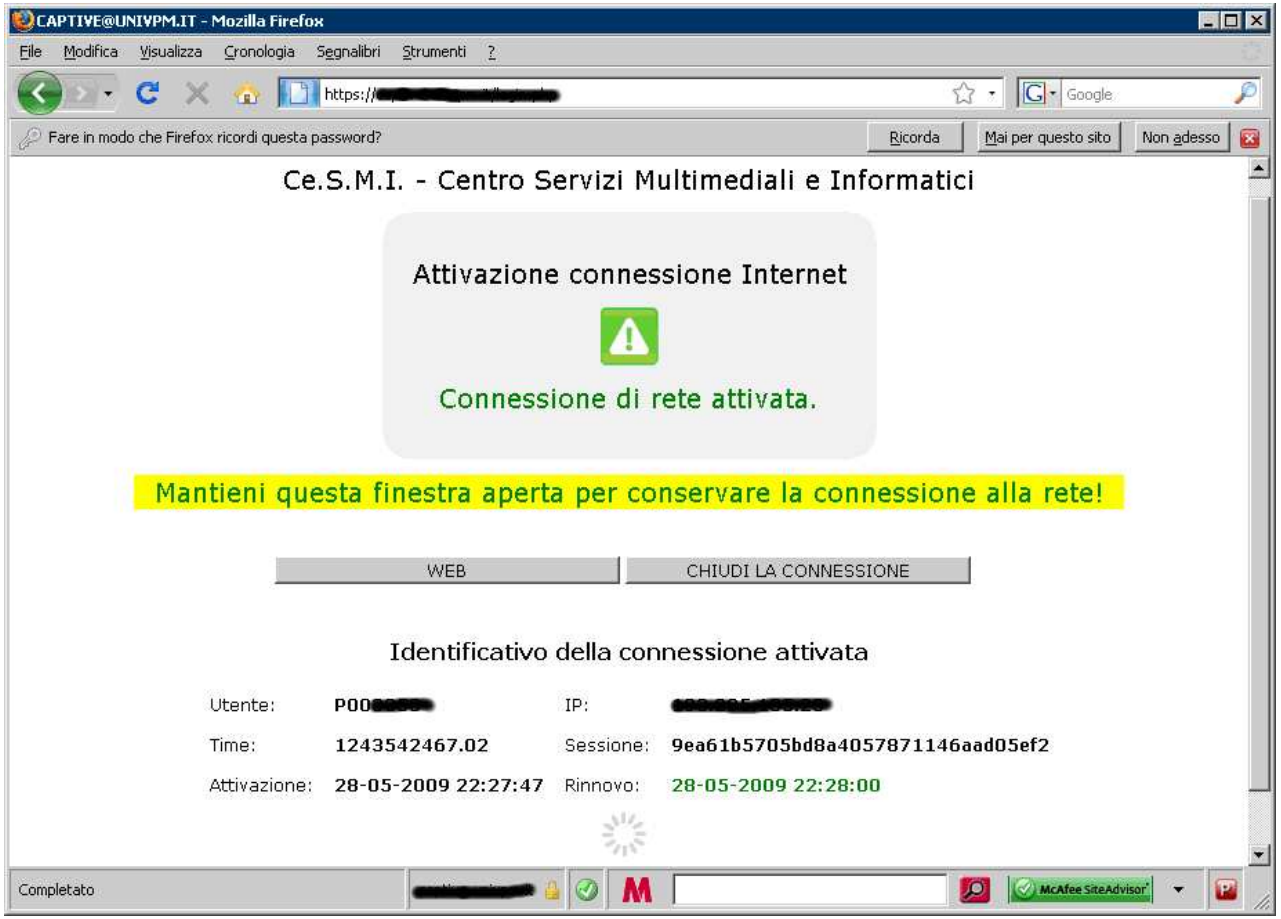
- **Amministrazione**. Rimane da sviluppare una interfaccia per semplificare la configurazione, l’amministrazione delle connessioni attive (es: cancellazione forzata di una connessione, avvio forzato del cleaner, consultazione log…), etc.;

Diffusione: CONTRO (2)

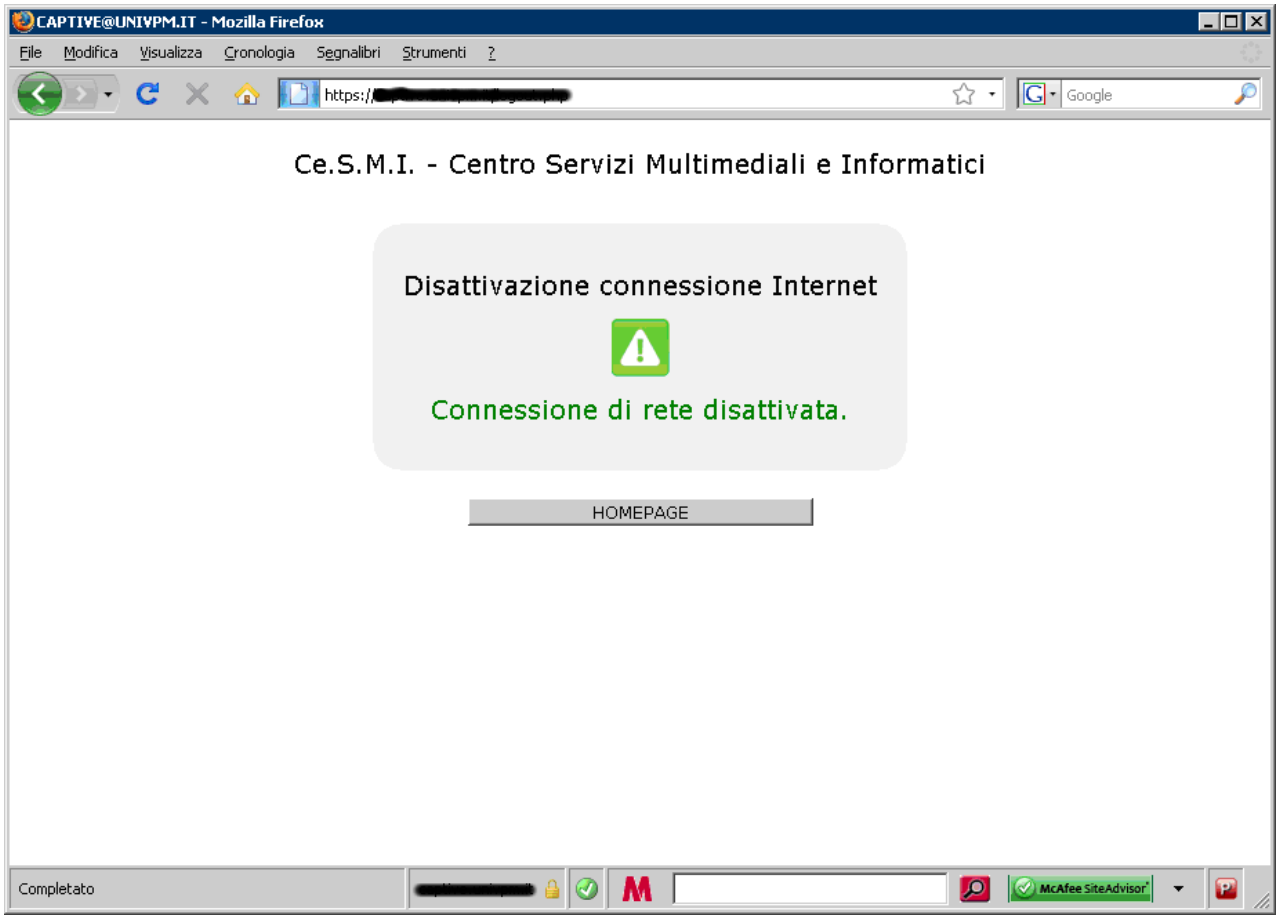
- **NAT**. Con l'attivazione del sistema è stata necessaria una riorganizzazione (ancora in corso) della rete per ridurre i NAT presenti in Ateneo e la conseguente duplicazione delle installazioni dell'applicazione.
- **Privacy**. E' stata necessaria una attività di informazione del personale sulle motivazioni dell'attivazione del sistema di autenticazione, sull'utilizzo e sulle forme di archiviazione dei logfile;
- **Forward delle connessioni**. I servizi basati su protocolli diversi dall'http richiedono una autenticazione preventiva da parte dell'utente;
- **Browser di alcuni device**. Non tutti i device (es: pda e smartphone) integrano browser con supporto HTTPS e tabs.

L’interfaccia di login del captive-portal

Pagina di attivazione della connessione di rete



Disattivazione del collegamento



Altri “stati”

Attivazione connessione Internet

Autenticazione fallita.

I dati inseriti non sono corretti oppure non completi.

Attivazione connessione Internet

Database non disponibile.

Nessun server disponibile.

Utente presente nella blacklist. Accesso negato.

Errore nell'attivazione della postazione.

Indirizzo IP della postazione non autorizzato.

Captive-portal log file

 # tail –f captive.log

2009-01-24 13:34:33|IPDISABLE|P00****|192.168.10.1|*|Connessione di rete disattivata.|1232780157.56|1260ccdcb749dfcbe5cfe3400fda4d23

2009-01-24 13:36:08|IPENABLE|P00****|192.168.10.2|1|Connessione di rete attivata|1232790444.63|43977e4611fb47189e2a7cf901b486e4

2009-01-24 13:41:18|RENEW|P000****|192.168.10.2|*|Rinnovo della connessione.|1232790444.63|43977e4611fb47189e2a7cf901b486e4

2009-01-24 13:39:03|IDLEDCL|P00****|192.168.10.5|*|Pulizia delle connessioni zombie.|1232799985|92b9e60b7bf0dcdfabd39fcb24706c03

Data/Ora | Codice stato | Username | IP | Stato check_user | Messaggio | Timestamp | ID connessione

CARP: configurazione del kernel

- La configurazione di un sistema FreeBSD deve essere preceduta dall'inclusione del supporto per:
  - CARP
  - FIREWALL

  nel kernel (GENERIC)

  attraverso l'interfaccia
  - **device carp**

  e nel caso di utilizzo di IPFW
  - **options IPFIREWALL**
  - **options IPFIREWALL_DEFAULT_TO_ACCEPT**
  - **options IPFIREWALL_VERBOSE**

CARP: configurazione parametri via sysctl

- Con **sysctl** si può configurare il modo di funzionamento del cluster CARP già avviato e mediante l'inserimento delle coppie **parametro=valore** in **/etc/sysctl.conf** si può conservare l'impostazione ad ogni avvio di sistema;
- I parametri che abbiamo configurato:

```
# sysctl -w net.inet.carp.allow=1
```

Attiva il funzionamento di CARP attraverso l'abilitazione del sistema a ricevere pacchetti (def: 1)

```
# sysctl –w net.inet.carp.preempt=1
```

Disattiva tutte le interfacce di un sistema se una va in errore (def: 0)

```
# sysctl –w net.inet.carp.log=0
```

Attiva il sistema di log - 0: disattivato, 1: registra info pacchetti CARP non validi; >1: registra messaggi cambio stato master/slave (def: 1)

CARP: configurazione interfacce di rete (1)

- **/etc/rc.conf**

  ifconfig_xl0="inet 192.168.1.2 netmask 255.255.255.0"

  ifconfig_xl1="inet 192.168.2.2 netmask 255.255.255.0"

  cloned_interfaces="carp0 carp1"

  ifconfig_carp0="vhid 1 advskew 2 pass passwd1 192.168.1.1/24"

  ifconfig_carp1="vhid 2 advskew 2 pass passwd2 192.168.2.1/24"

- Da linea di comando

```
# ifconfig carp0 create
# ifconfig carp0 vhid 1 advskew 2 pass passwd1
   192.168.1.1/24
# ifconfig carp1 create
# ifconfig carp1 vhid 2 advskew 2 pass passwd2
   192.168.2.1/24
```

CARP: configurazione interfacce di rete (2)

HOST A

```
[root@captive  ~]# ifconfig -a
eth0:   ether 00:1f:29:ea:6b:92
        inet 192.168.1.2 netmask 0xffffff00
        broadcast 192.168.1.255
        status: active
eth1:   ether 00:1f:29:ea:6b:90
        inet 192.168.2.2 netmask 0xffffff00
        broadcast 192.168.2.255
        status: active

carp0:  flags=49<UP,LOOPBACK,RUNNING>
        inet 192.168.1.1 netmask 0xffffff00
        carp: MASTER vhid 1 advbase 1 advskew 2
carp1:  flags=49<UP,LOOPBACK,RUNNING>
        inet 192.168.2.1 netmask 0xffffff00
        carp: MASTER vhid 2 advbase 1 advskew 2
```

CARP: configurazione interfacce di rete (3)

Comandi per la configurazione:

```
# ifconfig carp0 create

# ifconfig carp0          \\
      vhid 1               \\
      pass passwd1         \\
      carpdev xl0          \\
      advbase 1            \\
      advskew 100          \\
      192.168.1.1/24

# ifconfig carp0 down
```

CARP: configurazione interfacce di rete (4)

I parametri utili per le interfacce carp:

- **VHID -** Virtual HOST ID rappresenta l'identificativo del gruppo di interfacce ridondanti dei sistemi che partecipano al cluster (*valori da 1 a 255*);
- **PASS –** Comunicata tra i vari host dello stesso gruppo per garantire l'appartenenza;
- **CARPDEV -** Interfaccia fisica da associare all'interfaccia carp. Determinata in automatico, se non specificata, dal sistema in base all'appartenenza delle interfacce fisiche/carp alle subnet;
- **ADVBASE –** [adv. base] - Frequenza in secondi degli avvisi al gruppo di interfacce - (*valori da 1 a 255 – default 1*);
- **ADVSKEW –** [adv. skew] - Altera il valore ADVBASE permettendo la definizione "forzata" di un master (*valore di default 0/255 secondi*).

CARP: avvisi del MASTER

HOST "SLAVE"

 # tcpdump –i carp0

```
listening on carp0, link-type NULL (BSD loopback), capture size 96
   bytes
11:17:48.477043 IP 192.168.1.2 > VRRP.MCAST.NET: VRRPv2,
   Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
11:17:49.478126 IP 192.168.1.2 > VRRP.MCAST.NET: VRRPv2,
   Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
11:17:50.479029 IP 192.168.1.2 > VRRP.MCAST.NET: VRRPv2,
   Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
11:17:51.479939 IP 192.168.1.2 > VRRP.MCAST.NET: VRRPv2,
   Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
11:17:52.480905 IP 192.168.1.2 > VRRP.MCAST.NET: VRRPv2,
   Advertisement, vrid 1, prio 0, authtype none, intvl 1s, length 36
```

NetFlow: implementazione (1)

- I pacchetti utilizzati:
  - **/usr/ports/net-mgmt/flow-tools**
    Raccolta di tools. Il pacchetto contiene "flow-capture" utile per la cattura del traffico e l'invio dei flow al "collector", "flowdumper" per la consultazione dei dati registrati, flow-fanout per la duplicazione delle registrazioni e altre utility per la creazione di report, statistiche e accesso ai dati.
  - **/usr/ports/net-mgmt/softflowd**
    Pacchetto per la gestione dei flussi. Registra i flow ricevuti organizzandoli in file.

NetFlow: implementazione (2)

```
/usr/local/bin/flow-capture
   -p /var/run/flow-capture/flow-capture.pid   -n 287
   -N -1
   -w /log/netflow/
   -S 30
   127.0.0.1/127.0.0.1/12345
```

[Opzioni] *pidfile, numero di registrazioni giornaliere (5 min.), struttura directory YYYY-MM-DD, workdir, frequenza registrazione statistiche sui flow, directory di log, ip di ascolto/ip exporter/porta*

```
/usr/local/sbin/softflowd
   -i bge0
   -n 127.0.0.1:12345
```

[Opzioni] *interfaccia, ip/porta del collector*

Apache: configurazione della pagina di default

Il captive-portal deve presentare la pagina di login in automatico al primo accesso alla rete da una postazione non ancora abilitata.

APACHE

/usr/local/etc/apache/httpd.conf

e/o

/usr/local/etc/apache/extra/http-ssl.conf

```
ErrorDocument 404 http://[ip o dominio]/index.php
ErrorDocument 404 http://[ip o dominio]/index.php
```

IPFIREWALL

```
ipfw add pass ip from "table(2)“ to any
ipfw add pass ip from any to "table(2)“
ipfw add fwd 192.168.1.254,80 tcp from 192.168.1.0/24 to any 80
ipfw add fwd 192.168.2.254,80 tcp from 192.168.2.0/24 to any 80
```

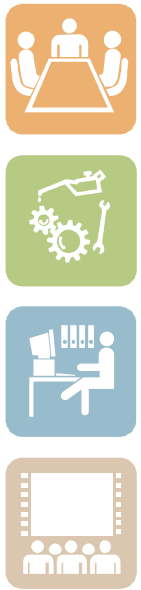
Autenticazione degli utenti nell'infrastruttura LDAP (Ms AD)

Accesso mediante LDAPS:

```
/usr/local/etc/openldap/ldap.conf
TLS_CACERT      /etc/ssl/certs/univpm-ad.pem
TLS_CACERTDIR   /etc/ssl/certs
```

Funzioni per la verifica delle credenziali

```
// Connessione al server dopo la selezione
@ldap_connect("ldaps://" . $server[$i], $ldap_port);
// Bind dell'utente
@ldap_bind($connesso[1], $rdn, $password);
// Ricerca "scheda"
@ldap_search($connesso[1], AD_LDAP, $filtro_ldap, $attributi);
// Estrazione dati dalla scheda
@ldap_get_entries($connesso[1], $ricerca);
```



Grazie per l’attenzione