Workshop

Soluzioni wireless BLS

© 2011 Copyright B.L.S. Consulting S.r.l.

Cosa chiedono le aziende?

Le aziende hanno tre esigenze:

1. Fornire un accesso sicuro alla rete aziendale sia mediante reti wired che mediante reti wireless

2. Fornire un accesso limitato ad Internet agli ospiti (clienti, fornitori, ecc.) senza la necessità di creare degli account, senza specifiche configurazioni ma limitato alla presenza in azienda

3. Fornire un accesso ai colleghi per potersi collegare in VPN alla propria sede/azienda

Cosa chiedono Comuni e scuole?

I Comuni e le scuole hanno tre esigenze:

1. Fornire un accesso gratuito ad Internet che implementi le normative vigenti in materia di wireless e privacy
2. Un sistema di identificazione che non richieda carico di lavoro all'ente e nel contempo mantenga la privacy dell'utilizzatore
3. L'accesso ad Internet deve essere limitato ai siti consoni filtrando eventuali accessi a siti fraudolenti, illegali, per adulti, ecc.

Cosa offre BLS per soddisfare queste esigenze?

Abbiamo sviluppato insieme ai nostri principali clienti un'appliance specifica per gestire le reti wireless, e flessibile per implementare le funzionalità richieste da aziende private, enti pubblici ed esercizi aperti al pubblico.

In particolare l'appliance fornisce:

- autenticazione certa dell'utente
- funzionalità di rete necessarie quali dns, dhcp, proxy, ecc.
- tenuta dei log secondo le normative vigenti
- statistiche di utilizzo

Quali sono i vantaggi?

L'appliance presenta numerosi vantaggi:

- facile da installare → costi ridotti di avviamento
- opensource → costo ridotto, affidabile, personalizzabile
- fisica, virtuale, service → si adatta alla struttura del cliente
- completa → implementa tutte le funzioni necessarie
- sicura → *volendo* implementa le specifiche militari di sicurezza
- sviluppata per l'Italia → implementa e si adegua alle normative

Caratteristiche tecniche: sbox4

Sfruttando l'esperienza delle nostre precedenti distribuzioni durante lo scorso anno abbiamo sviluppato la nuova infrastruttura, chiamata appunto sbox4.

L'appliance di gestione delle reti wireless si basa sulla sbox4.

Questa infrastruttura è evoluta da una distribuzione non standard ma estremamente sicura ad un sistema di gestione delle appliance basato su distribuzioni standard e con livelli di sicurezza ancora superiori.

La sbox4 sfrutta quindi i vantaggi delle distribuzioni standard mantenendo però inalterati i vantaggi delle precedenti versioni delle sbox, in particolare la facilità di configurazione dei servizi.

Caratteristiche tecniche: sbox4

Principali caratteristiche della sbox4:

Doppia politica di supporto

1. commerciale: basata su distribuzione RedHat ES, supporto e aggiornamento del sistema operativo garantito da RedHat a prezzi modici

2. modalità opensource: basata su distribuzione free CentOS, totalmente compatibile con RedHat ES e supportata dalla comunità Open

Caratteristiche tecniche: sbox4

Principali caratteristiche della sbox4:

Configurazione facilitata e automatica dei servizi: da pochi file di configurazione vengono automaticamente generati ed avviati tutti i servizi necessari.

Gestione via web: i file di configurazione sono facilmente gestibili via web, rispetto alle sbox precedenti l'interfaccia copre tutti i servizi ed è stata notevolmente semplificata.

Sicurezza: il sistema viene posto automaticamente in sicurezza all'avvio. Sono previsti tre livelli diversi di sicurezza in base all'utilizzo, quello più avanzato *paranoic* è compatibile e supera i test per le specifiche militari DSMIL e NSA

Caratteristiche tecniche: sbox4

Principali caratteristiche della sbox4:

Supporto ambienti virtuali VMware: la sbox4 è stata sviluppata per ambienti virtuali, anche se funziona perfettamente su appliance hardware.

Ciò significa che:

- si accorge automaticamente di girare in ambiente virtuale
- automaticamente avvia e configura i vmware tools
- è ottimizzata per garantire le massime prestazioni
- è configurata per sfruttare le caratteristiche di High Availability e Fault Tolerance di VMware

Architettura

L'appliance si basa su due principali sistemi:

Central Authentication Service (CAS)

E' il sistema di autenticazione Opensource più utilizzato, sviluppato originariamente dall'Università di Yale e poi passato in gestione ad una comunità specifica Jasig.

Authentication Gateway (NOCATCAS)

Progetto opensource originariamente sviluppato dalla comunità NoCat e attualmente gestito da BLS.

Central Authentication Service

Il CAS è un sistema di single sign-on che si basa su diversi sistemi di autenticazione quali database, LDAP, RADIUS, Active Directory.

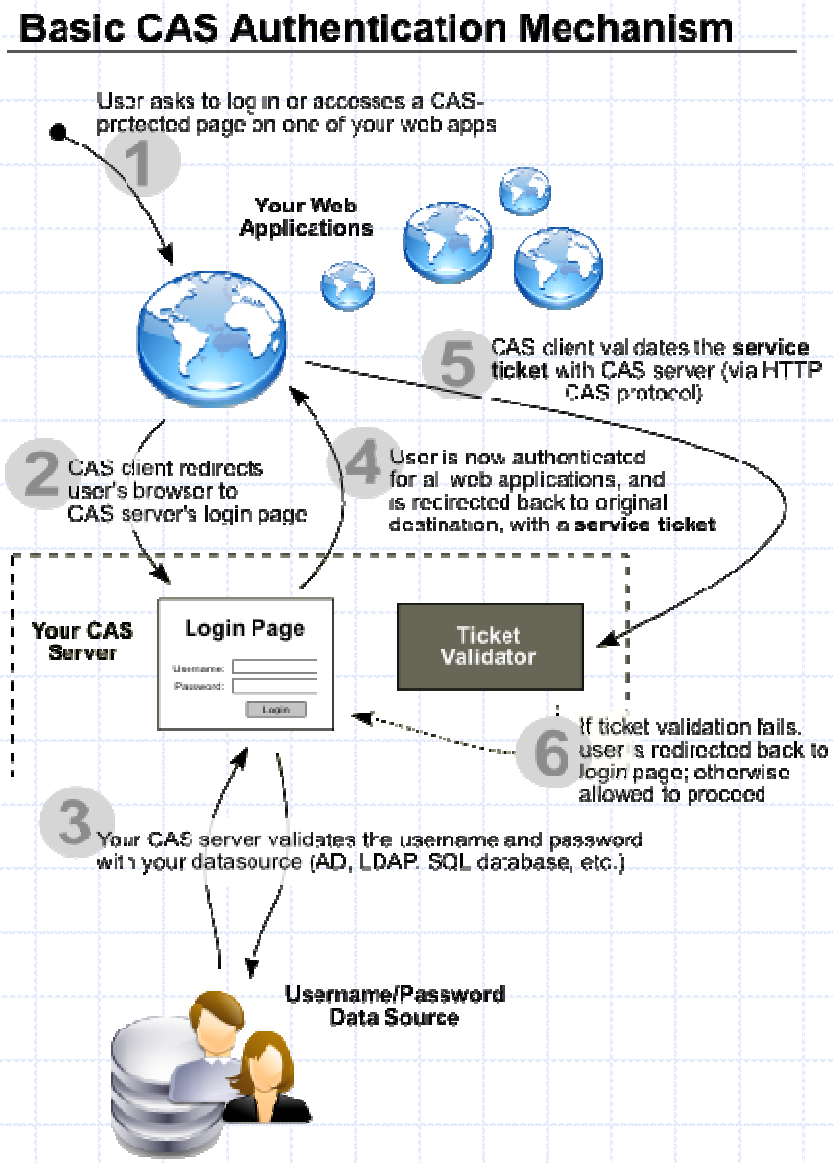
Molti servizi ed applicativi hanno implementato l'autenticazione con CAS (in gergo: CASifying application), tra questi: Zimbra Collaboration Suite, Microsoft SharePoint e altre numerose applicazioni basate su ASP .NET, Apache, TomCat, Joomla, Zope, OpenCms, Firefox (CAS BAR), ecc.

Si basa su protocolli standard HTTP/SSL.

Central Authentication Service

Fasi autenticazione

1. Accesso al servizio
2. Redirezione alla pagina di login
3. CAS autentica l'utente mediante uno dei possibili sistemi
4. Il client riceve un ticket dal CAS
5. Il ticket viene passato al servizio e viene validato da quest'ultimo mediante il ticket validator di CAS
6. Se il ticket non è valido l'utente viene rediretto nuovamente alla pagina di login



Central Authentication Service

Ha due principali difetti:

1. installazione complicata
2. ammette un solo sistema di autenticazione per volta

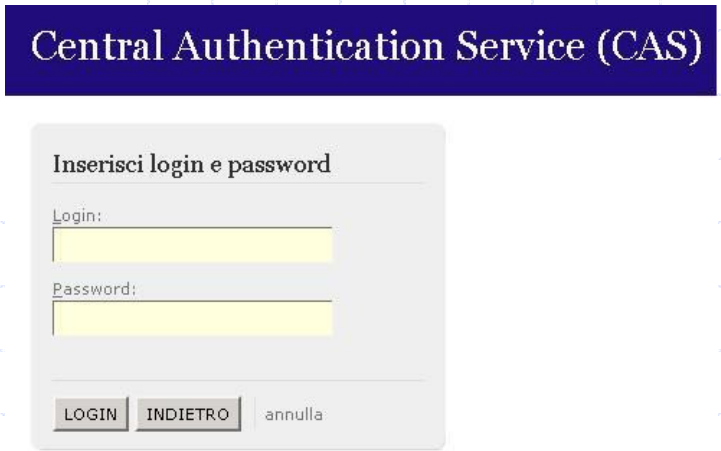
BLS ha risolto entrambi i problemi:

1. il CAS viene autoconfigurato dai sistemi della sbox4, riducendo l'installazione all'impostazione di alcuni semplici parametri (nome azienda, indirizzo email di riferimento, indirizzo ip del CAS server e poco altro) e al riavvio del servizio
2. abbiamo apportato delle consistenti modifiche rilasciate in Opensource per permettere l'attivazione di più sistemi di autenticazione in contemporanea

Central Authentication Service

A differenza del CAS standard, viene chiesto all'utente di selezionare il metodo di auteticazione.

Poi in base alla scelta fatta vengono richiesti i dati necessari per autenticare l'utente.



Central Authentication Service

BLS ha anche sviluppato tre sistemi aggiuntivi di autenticazione per il CAS:

1. mediante Carta Regionale dei Servizi (CRS)
2. mediante Digipass Vasco
3. mediante invio di password di accesso via SMS

Oltre a questi sistemi, sull'appliance, è già installato anche l'autenticazione mediante password su database MySQL.

E' possibile utilizzare il sistema di gestione degli utenti e il corrispondente database già presente sull'appliance o collegarsi ad un database esterno.

Authentication Gateway

Il sistema di authentication gateway NOCAT/NOCATCAS era un vecchio progetto Opensource ormai obsoleto e abbandonato.

Aveva però delle interessanti caratteristiche:

- si integrava con CAS
- si integrava con le funzionalità di rete di Linux, mentre la maggior parte dei sistemi equivalenti si basano su freeBSD o OpenBSD
- si integrava con i principali servizi comunemente utilizzati in ambiente Linux: SQUID come proxy, BIND DNS e DHCP

Non era però un progetto maturo e con le caratteristiche di affidabilità e sicurezza richieste dalle aziende.

Authentication Gateway

Visto che il progetto è stato poi abbandonato, e attualmente non è neanche più accessibile su Internet, BLS ha deciso di prenderlo in gestione.

Abbiamo quindi aggiornato e sistemato il software adeguandolo alle esigenze delle aziende e degli enti.

Adesso il software è sicuro, gira sotto le ultime distribuzioni di Linux e utilizza le ultime versioni di TomCat, Java e Perl.

Inoltre abbiamo apportato delle aggiunte per implementare la gestione dei log richiesta dalla normativa Italiana in materia di Privacy.

Come funziona?

1. l'utente accede alla rete wireless senza necessità di inserire alcuna password, chiave o certificato
2. il DHCP e il DNS si occupano di configurare automaticamente il client
3. l'utente ha già accesso ad Internet limitatamente ad alcuni semplici servizi, se però vuole navigare od utilizzare la posta elettronica o qualunque altro servizio complesso deve autenticarsi
4. l'utente deve quindi aprire un browser e verrà automaticamente ridiretto verso il CAS server che procederà con l'autenticazione mediante uno dei sistemi previsti
5. se l'autenticazione va a buon fine l'authentication gateway aprirà l'accesso verso Internet o verso altre reti
6. finché l'utente non si scollegherà volontariamente o non chiuderà una apposita finestra del browser continuerà ad avere accesso

Quali sono i vantaggi rispetto ad altri prodotti?

L'appliance ha moltissimi vantaggi rispetto ad altri prodotti simili:

- si basa su uno standard "de facto" per quanto riguarda l'autenticazione
- questo permette utilizzare il sistema di autenticazione anche per altri scopi quali l'accesso alla propria casella di posta elettronica, alla area riservata del sisto web, ai propri applicativi, ecc.
- implementare nuovi sistemi di autenticazione è estremamente semplice, se non sono già disponibili
- permette all'utente di autenticarsi una sola volta, al momento dell'accesso alla rete wireless e accedere poi, senza doversi nuovamente autenticare agli altri applicativi su cui ha diritti; vero single sign-on

Sviluppi futuri

Oltre a seguire le modifiche imposte dall'evoluzione normativa, abbiamo già in sviluppo:

1. App per autenticarsi su CAS da Apple iPhone e iPad, verrà rilasciata sul App store di Apple

2. App per autenticarsi su CAS da apparati che utilizzano Android quali cellulari e tablet pc, verrà rilasciata sul Market di Google Android

Altre funzioni

In aggiunta al sistema di autenticazione CAS e all'authentication gateway NOCATCAS l'appliance implementa diversi altri servizi necessari:

1. Servizi di networking DHCP, DNS e PROXY
2. Log server
3. Statistiche realtime e storiche

Servizi di networking

I servizi di networking sono necessari per garantire un accesso “agile” cioè senza la necessità di impostare parametri particolari sul client.

L’esperienza fatta sul campo ha permesso prendere in considerazioni tutte le possibili configurazioni degli apparati utilizzati per l’accesso, nel limite del possibile non sarà necessario modificare in alcun modo la configurazione di tali apparati.

Ciò riduce le richieste di supporto e facilita l’uso del sistema.

Log server

L'appliance implementa un log server basato su un prodotto commerciale e completato con nostri servizi.

Il sistema di log utilizzato garantisce:

- non modificabilità → infatti i log sono memorizzati in appositi database con hashing e timestamp periodici (ai nostri clienti forniamo il servizio di Time Stamp Authority o TSA)

- completezza → l'agent si collega al log server mediante protocolli che garantiscono la registrazione di tutti gli eventi/accessi, inoltre il server di log è in grado di reggere fino a 150.000 messaggi al secondo

- sicurezza → i log sono conservati in database crittografati, la comunicazione tra agent e server di log è crittografata

Statistiche storiche e realtime

Il sistema mantiene oltre ai log delle informazioni statistiche continuamente aggiornate su database.

Periodicamente le statistiche vengono esportate e visualizzate mediante una libreria basata su flash.

Le informazioni accessibili comprendono:

-utenti attualmente collegati (realtime)

-log degli accessi con data e ora di login e logout (storico)

-statistiche di accesso ad Internet (quasi realtime, aggiornato ogni minuto)

-statistiche storiche di accesso ad Internet (storico riepilogato per giorno)

Ringraziamenti

L'appliance è stata sviluppata con l'apporto di numerosi nostri clienti e collaboratori, in particolare ringraziamo:

Oscar Baracchi e Lorenza Ciprandi del Comune di Vigevano, per i suggerimenti, l'aiuto in fase di collaudo e lo sviluppo delle sistema di statistiche

Domande e risposte

GRAZIE!

Mauro Bruseghini: mbruse@bls.it