Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Ottobre 2009

Rapporto tecnico N.26

Infrastruttura Wireless presso le Strutture CNR Piemonte

Giancarlo Birello, Ivano Fucile, Valter Giovanetti

RAPPPORTO TECNICO CERIS-CNR
Anno 4, N° 26 del 12 ottobre 2009

Direttore Responsabile
Secondo Rolfo

Direzione e Redazione
Ceris-Cnr
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
http://www.ceris.cnr.it

Sede di Roma
Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano
Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione
Maria Zittino
m.zittino@ceris.cnr.it

Infrastruttura Wireless presso le Strutture CNR Piemonte

The Wireless infrastructure at Piedmont CNR network.

a cura dell'Ufficio IT Ceris-CNR

Giancarlo Birello, Ivano Fucile, Valter Giovanetti
(Ceris-Cnr)

Ceris-Cnr
Ufficio IT
Strada delle Cacce, 79
10100 Torino – Italy
Tel.: 011 3977303/388/512
Autore corrispondente: Giancarlo Birello, G.Birello@ceris.cnr.it

ABSTRACT:

The increasing popularity of laptop computer and the work on mobility requirement are the main reasons to deploy a wireless network infrastructure providing a secure internet connection for local and external users.

Wireless network has a lot of benefits but it is necessary take special care with security to prevent intrusions and illegal use of the network. Central administered wireless infrastructure is a good solution for security and it allows an easy maintenance of the access point configuration.

The Sonicwall Network Security Appliance NSA-5500 is the core of Piedmont CNR Network Infrastructure and its options regarding wireless LAN allow us to deploy a wireless infrastructure meeting all requirements.

The main features of our deployment are: multiple SSID announcement, 802.1x protocol support, captive portal authentication, radius and ldap integration, cross-authentication with local and national organizations.

KEYWORDS: wireless, internet, 802.1x, vlan, radius

JEL CLASSIFICATION: Y90 - OTHER

INDICE

INDICE DELLE FIGURE

1. INTRODUZIONE

La diffusione tra i nostri utenti di nuove apparecchiature, soprattutto computer portatili, dotati di serie di interfacce wireless, l'esigenza sempre maggiore di lavoro in mobilità e l'interscambio crescente tra strutture ed enti nel mondo scientifico sono le ragioni che ci hanno spinto a considerare un'implementazione distribuita e sicura di rete wireless all'interno delle strutture CNR afferenti all'Infrastruttura di rete CNR Piemonte. Inoltre distribuire centralmente tale servizio risolve anche eventuali buchi nella sicurezza della rete causati dall'uso di *access point* personali, in questo modo resi obsoleti, installati autonomamente nei vari uffici e normalmente impiegati senza adottare particolari precauzioni sui protocolli di autenticazione per l'accesso alla rete.

Un'unica infrastruttura wireless ha oltremodo il vantaggio di uniformità degli accessi per tutti gli utenti delle diverse strutture che, abbinato a una gestione centralizzata da parte nostra, evita alle strutture la necessità di sviluppare localmente competenze sugli aspetti tecnici e sistemistici degli accessi wireless.

Bisogna tener presente che l'accesso wireless è molto più soggetto ad abusi che l'accesso in rete tramite cavo quindi va posta particolare attenzione al tema sicurezza, adottando tutte le misure necessarie e i protocolli sicuri che ormai sono disponibili e maturi da tempo per questa tecnologia.

Visto lo scopo e per evitare parte dei rischi, l'accesso wireless è stato limitato ai soli utenti previamente autenticati, siano questi utenti locali o utenti di altre strutture ed enti con i quali esistano accordi di mutuo riconoscimento. In particolare sono state messe a disposizione tre reti: una per i soli utenti locali, una per gli utenti afferenti alla gerarchia Eduroam ed una per gli utenti di enti con i quali esistono particolari rapporti di cross-autenticazione. Ognuna di queste reti, in base al target dell'utenza, differisce dall'altra per tipologia di protocollo di autenticazione e servizi abilitati verso internet, come verrà descritto nel seguito del documento.

2. APPARATI

2.1 Network Security Appliance Sonicwall

L'Infrastruttura di rete CNR Piemonte si è dotata nel corso del 2008 di nuovi apparati di rete, un paio di firewall/router della Sonicwall in High Availability NSA-5500, migliorando così concretamente le prestazioni e la sicurezza dell'intera rete.

Tra i vari servizi che questi apparati permettono di gestire è molto interessante sicuramente il controllo e amministrazione della rete wireless. In modo centralizzato e decisamente semplice ed intuitivo, permettono la gestione diretta di più Access Point (AP), con tutte le caratteristiche di sicurezza richieste e riducendo al minimo l'impatto sui tempi di amministrazione delle risorse in gioco.

Tra le altre caratteristiche, nel nostro caso era particolarmente utile la possibilità di gestire SSID multipli per offrire all'utenza forme diverse di accesso alla rete wireless, in funzione della tipologia e dell'Ente di appartenenza dell'utente stesso. Inoltre il supporto della tecnologia 802.1x e l'autenticazione tramite server radius avrebbero permesso l'adesione a circuiti nazionali e internazionali di cross-autenticazione (es. Eduroam) che hanno come prerogativa l'accesso tramite tali tecnologie. Infine la disponibilità di un *captive portal* e le possibilità di personalizzazione erano i presupposti necessari a implementare un servizio specifico per la nostra utenza e per estendere la fruibilità del servizio ad altri enti potendo così indirettamente estendere la copertura wireless non solo presso le nostre strutture.

Per usufruire di tutte queste funzioni gli apparati Sonicwall richiedono che gli Access Point siano della Sonicwall. Essendo già in possesso di un paio di tali AP e riscontrando la loro validità funzionale oltre ad un costo relativamente contenuto rispetto alle caratteristiche offerte, questo requisito negativo ci è sembrato comunque ampiamente smorzato dai numerosi vantaggi tecnici e amministrativi che si hanno adottando tale soluzione.

Infine a livello di rete per gestire gli SSID multipli è richiesto il supporto delle VLAN. La nostra infrastruttura già utilizza ampiamente le VLAN per differenziare il traffico tra le varie strutture CNR e gli apparati a nostra disposizione erano sicuramente adeguati allo scopo, pertanto si è deciso implementare il servizio di accesso wireless sfruttando completamente le funzioni offerte dagli apparati Sonicwall NSA-5500.

2.2 Switch

Come premesso nel precedente paragrafo, sulla rete devono essere attivabili le VLAN, in particolare gli switch attivi sull'infrastruttura devono poterle gestire.

A livello di centro stella gli switch HP installati, al pari di quello presente presso il Ceris a Moncalieri, offrono il completo supporto delle VLAN, così come gli switch 3com presso l'edificio dell'Imamoter e dell'Istec. Non altrettanto si può dire per gli apparati presenti presso l'IVV, l'IRPI e l'edificio dei Servizi di Area, ma in tal caso, sfruttando la ricchezza di fibre ottiche tra il centro-stella e le suddette strutture, si può ovviare al problema dedicando un link in fibra alla rete degli Access Point.

Infine per estendere la rete wireless attraverso il link AemNet che collega il centro-stella alla sede del Ceris di Moncalieri, abbiamo richiesto la disponibilità di VLAN dedicate su tale link alla ditta fornitrice del servizio. La disponibilità di AemNet a tale configurazione ha così reso possibile l'implementazione del servizio wireless anche presso la struttura di Moncalieri, registrando la nuova configurazione anche nel contratto di rinnovo firmato quest'anno.

2.3 Server

I server coinvolti nel servizio di accesso wireless sono due: un server radius per l'autenticazione degli utenti ed un web server per il *captive portal*.

Il primo è stato implementato su piattaforma Linux (Ubuntu Server 8.04), sul quale però non era disponibile il pacchetto della versione di Freeradius con il supporto del protocollo 802.1x e pertanto è stato compilato da sorgente, in particolare è stata installata la versione “FreeRADIUS Version 2.0.5”. Tale server radius è stato quindi inserito all'interno di vari accordi di cross-autenticazione, i cui dettagli di configurazione verranno dati nel seguito, e in particolare: la gerarchia Eduroam attraverso il Garr, il CNR Amministrazione Centrale, l'Università di Torino, il Politecnico di Torino ed il CSP Piemonte. Infine per l'autenticazione dei nostri utenti locali è stato attivato l'accesso tramite protocollo Ldap al database degli utenti, che nello specifico è mantenuto in Active Directory in un dominio di Windows Server 2003R2.

Per il web server, essendo le pagine di personalizzazione del captive portal disponibili in linguaggio ASP, è stato utilizzato un server IIS su piattaforma Windows Server 2003R2. Il *captive portal* è stato personalizzato in modo da accedere per l'autenticazione al server radius su menzionato, sfruttando le pagine ASP di esempio disponibili della Sonicwall e che verranno illustrate in dettaglio nel seguito. Infine è stato necessario dotare il server web di un certificato SCS ottenuto tramite il Garr, poiché la pagina del *captive portal* è acceduta tramite protocollo crittografato HTTPS e l'utilizzo di tale certificato, la cui CA (Certification Authority) è inclusa nei principali browser, evita all'utente la comparsa di spiacevoli pop-up o messaggi sulla sicurezza.

3. INFRASTRUTTURA DI RETE

3.1 Requisiti

Necessarie per il corretto funzionamento degli Access Point e per la gestione degli SSID multipli sono le VLAN, in particolare è necessaria una VLAN dedicata per ogni SSID annunciato più un default *untagged*. Su quelle dedicate viaggerà il traffico generato dall'utente connesso al relativo SSID mentre su quella di default transiterà il traffico di gestione tra l'NSA (Network Security Appliance) e l'Access Point.

Si illustrano nel seguito le configurazioni specifiche degli apparati coinvolti nel servizio per la definizione delle VLAN, tenendo presente che nel nostro caso è stato previsto l'annuncio dei tre SSID che verranno esaminati in dettaglio nel paragrafo 4 e seguenti.

3.2 Configurazione NSA-5500

Sull'apparato Sonicwall, vista la disponibilità, viene dedicata un'interfaccia Giga ethernet (X7) agli apparati wireless e configurata per la gestione delle 3 VLAN relative con tag 210, 211 e 212 oltre al traffico *untagged*. Vengono previamente definite 3 nuove zone, oltre alla zona WLAN di default, a cui vengono assegnate le VLAN, in modo da poter trattare, con sistemi di autenticazione diversi, gli accessi alle tre reti wireless virtuali. I dettagli sulle zone WLAN-Ospiti, WLAN-Eduroam e WLAN-Staff sono riportati nel seguito nei paragrafi relativi ad ogni singolo SSID.

X7	WLAN	[redacted].10.1	255.255.255.0	Static	1000 Mbps full-duplex
X7:V210	WLAN-Ospiti	[redacted].210.1	255.255.255.0	Static	VLAN Sub-Interface
X7:V211	WLAN-Eduroam	[redacted].211.1	255.255.255.0	Static	VLAN Sub-Interface
X7:V212	WLAN-Staff	[redacted].212.1	255.255.255.0	Static	VLAN Sub-Interface

Figura 1: Definizione Zone NSA-5500 Sonicwall

Inoltre viene attivato il server Dhcp interno dell'apparto sulle VLAN 210, 211 e 212 con range da 2 a 222 (es. x.y.210.2 → x.y.210.222).

3.3 Configurazione switch

Switch HP centro-stella

Il centro-stella dell'Infrastruttura di rete CNR Piemonte è costituito da due switch HP connesi tra loro tramite un trunk al Gigabit. Entrambi gli switch gestisco l'intera suddivisione della rete in VLAN per differenziare il traffico delle varie strutture CNR presenti. Si è cercato di mantenere limitato ad un solo switch la gestione della nuova infrastruttura wireless per ovviamente limitare le complicazioni e l'appesantimento della gestione degli apparati.

In particolare sull'apparato interessato dalla nuova rete wireless sono state definite 4 nuove VLAN, oltre a quelle già esistenti: la 200 per il traffico untagged richiesto dagli AP e le 210, 211 e 212 per il traffico dei tre SSID annunciati.

Su tutti i link, sia verso l'NSA-5500 che verso le varie strutture CNR, indipendentemente se in rame o fibra ottica, è stato inviato il traffico untagged più quello delle 3 VLAN. Fa eccezione il link verso l'Imamoter/Istec in quanto si è utilizzata la stessa fibra già impiegata per il traffico standard e quindi è stato necessario marcare il traffico untagged dell'AP con una VLAN (200) che poi sul lato Imamoter/Istec viene scorporato e convertito nuovamente in untagged prima di inviarlo all'AP.

Nella configurazione dello switch, alla porta presente in (STATIC) viene inviato il traffico tagged della VLAN relativa mentre alla porta presente nell'ultima colonna viene inviato il traffico untagged. Le porte presenti nell'ultima colonna costituisco un dominio separato da tutte le altre porte dello switch. Nella figura sotto, ad esempio, alla porta A1 verrà inviato il traffico untagged generato dalle porte B6 e A2-A5,B8-B10 ed il traffico tagged delle VLAN 210, 211 e 212 generato dalla stessa serie di porte precedenti. In questo caso il traffico della porta B6 con tag 200 è convertito in untagged prima di inviarlo all'insieme di porte A1-A5, B8-B10.

200	vlan200	STATIC	(STATIC) B6 (GVRP) None	A1-A5,B8-B10
210	vlan210	STATIC	(STATIC) A1-A5,B6,B8-B10 (GVRP) None	None
211	vlan211	STATIC	(STATIC) A1-A5,B6,B8-B10 (GVRP) None	None
212	vlan212	STATIC	(STATIC) A1-A5,B6,B8-B10 (GVRP) None	None

Figura 2: Configurazione VLAN switch HP centro-stella

Switch HP Moncalieri

Lo switch principale della rete della Sede del Ceris di Moncalieri è un apparato HP uguale a quelli del centro-stello presso l'Ufficio IT e come tale gestibile e con ampio supporto delle VLAN.

Nella configurazione si è isolato completamente il traffico wireless dal resto del traffico di rete standard, dovendo utilizzare lo stesso apparato per entrambe le infrastrutture. In particolare dallo switch AemNet arriva, tramite una porta dedicata, il traffico wireless untagged ed il traffico tagged 210, 211 e 212 che viene smistato ai due Access Point al momento installati presso la Sede di Moncalieri. Per poter separare il traffico wireless dal resto si è comunque isolato il traffico untagged con una VLAN (200) a livello di switch come si può rilevare dalla figura seguente.

200	vlan200	STATIC	(STATIC) None (GVRP) None	B1-B3
210	vlan210	STATIC	(STATIC) B1-B3 (GVRP) None	None
211	vlan211	STATIC	(STATIC) B1-B3 (GVRP) None	None
212	vlan212	STATIC	(STATIC) B1-B3 (GVRP) None	None

Figura 3: Configurazione VLAN switch HP Moncalieri

Switch 3com Imamoter

Nel caso del traffico wireless per le Strutture Imamoter/Istec si è sfruttata la fibra ottica già operativa ed attestata su uno switch 3com differenziando il traffico untagged richiesto dagli Access Point tramite un'ulteriore VLAN (200) configurata sullo switch.

In particolare dalle figure si può vedere come sulla porta 25, link in fibra verso il centro-stella, oltre al traffico untagged normale, arriva traffico tagged 200, 210, 211 e 212 (nella figura di destra si è riportato solo il caso della VLAN 210, per la 211 e 212 è esattamente la stessa configurazione). L'Access Point è connesso sulla porta 1 tramite la

quale, oltre al traffico tagged, transiterà il traffico untagged ottenuto dalla conversione del traffico tagged 200 che proviene dalla porta 25.

Questa soluzione ha permesso risparmiare un apparato di rete, un convertitore fibra/rame, che invece si è reso necessario per quelle strutture non dotate di un apparato switch gestibile e in grado di controllare le VLAN.

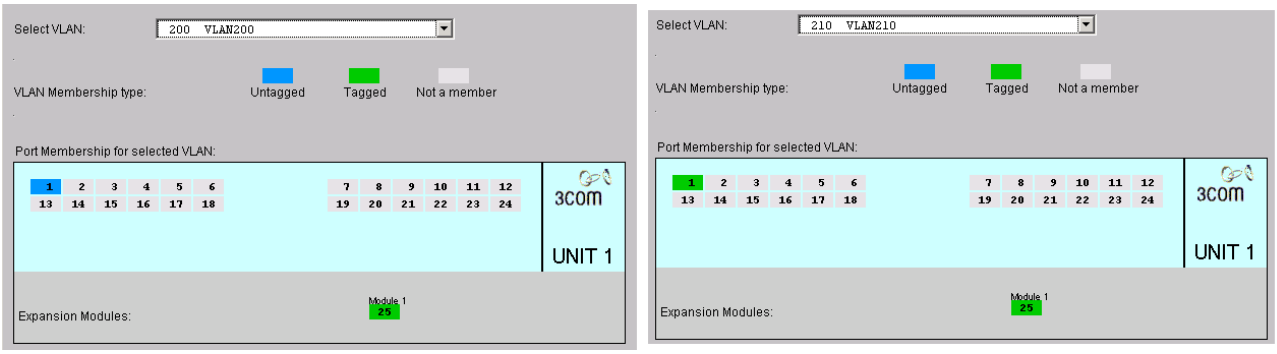

Figura 4: Configurazione VLAN switch 3Com Imamoter

Switch AEMNET

I link tra il centro-stella ed alcune strutture sono forniti da AemNet ed è a carico della ditta l'intera gestione, compresa quella degli apparati.

La disponibilità di AemNet a modificare la configurazione del link verso la Sede di Moncalieri ci ha permesso estendere anche a tale struttura l'infrastruttura wireless. In particolare abbiamo richiesto lo sdoppiamento del link, reso possibile dalla disponibilità di VLAN sull'anello in fibra, in modo da far transitare su un primo link il traffico untagged normale e su un secondo link il traffico untagged e quello delle VLAN 210, 211 e 212 richiesto dall'infrastruttura wireless.

3.4 Configurazione fibre

Non tutte le Strutture CNR disponevano di switch in grado di gestire le VLAN e quindi in tal caso si è sfruttata la ricchezza di fibre ottiche tra il centro-stella e la struttura per creare un link riservato al solo traffico dell'infrastruttura wireless.

Nello specifico le strutture interessate dal link in fibra dedicato sono state l'IVV, l'IRPI e la palazzina dei Servizi di Area. Lato centro-stella sullo switch erano già disponibili delle porte in fibra mentre lato struttura è stato necessario attestare la fibra su un convertitore fibra/rame per poter collegare l'Access Point. Si è comunque verificato che anche convertitori FastEthernet economici hanno assolto bene al compito mantenendo intatto il traffico untagged e tagged in transito.

3.5 *Configurazione Access Point*

Per quanto riguarda gli Access Point è stato praticamente nullo l'intervento di configurazione richiesto in quanto, una volta collegato il cavo di rete e acceso l'apparato, viene immediatamente riconosciuto dall'NSA-5500, che provvede ad aggiornargli il firmware con una versione compatibile col proprio sistema operativo e caricare la configurazione impostata a priori sul NSA-5500 e distribuita automaticamente a tutti gli Access Point Sonicwall ad essa connessi. In questa modalità l'unità centrale ha il controllo continuo e diretto degli Access Point e garantisce l'uniformità delle configurazioni mantenendo sincronizzati dinamicamente gli apparati con la configurazione impostata dall'amministratore sull'NSA-5500.

3.6 *Configurazione generale*

Volendo riassumere la configurazione della copertura wireless ad oggi attiva presso l'Infrastruttura di rete CNR Piemonte, che coinvolge due siti, l'Area di Ricerca di Mirafiori e la sede del Ceris a Moncalieri presso il Real Collegio, si riporta la figura seguente nella quale si può osservare la distribuzione dei 7 Access Point e le connessioni di base della rete wireless.

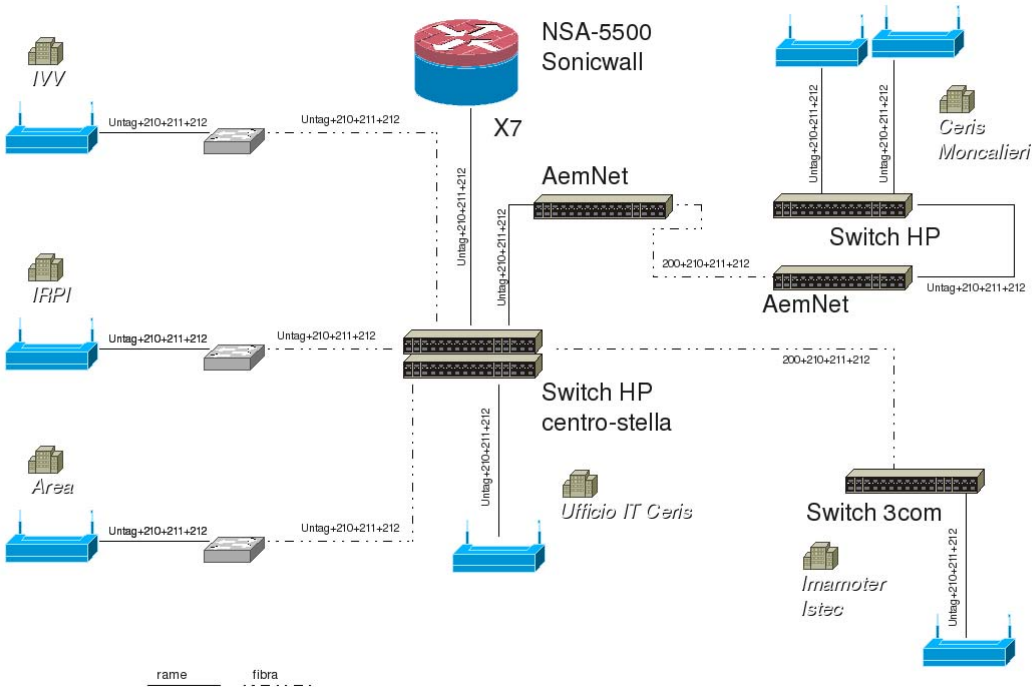

Figura 5: Infrastruttura wireless complessiva

4. SSID TOCNR-STAFF

Una prima rete wireless annunciata è quella TOCNR-Staff dedicata ai soli utenti dell'Infrastruttura di rete CNR Piemonte. Tramite questo accesso si accede all'intera rete locale ed ai servizi di rete come avviene per i PC connessi tramite cavo. Questa rete è pensata per tutti gli utenti dotati di computer portatile con dispositivo wireless e permette, senza la stesura di cavi o la disponibilità di prese di rete aggiuntive, potersi collegare alla rete locale per poter lavorare. In aggiunta può essere anche utilizzata da PC fisso con dispositivo wireless e può tornar utile nel caso di indisponibilità di prese evitando così la stesura ulteriore di cavi.

Per l'accesso a questa rete sono applicati gli standard più stretti sulla sicurezza, data la sensibilità del tipo di accesso, ed in particolare lo standard WPA2 tramite autenticazione su server radius 802.1x. Questo significa che le credenziali inserite dall'utente per potersi autenticare, che coincidono con le stesse usate per accedere alla rete ed ai vari servizi (es. N.Cognome / password), vengono inviate in formato crittografato attraverso la rete fino al server di autenticazione, in tal modo la possibilità di intrusione e rilevamento di questi dati sensibili è limitata al minimo.

Nei paragrafi successivi riportiamo le configurazioni specifiche per questo SSID che sono state implementate sui vari apparati in gioco.

4.1 Configurazione Sonicwall

Oltre alla configurazione di una VLAN dedicata a questo SSID, come riportato nel paragrafo 3.2 Configurazione NSA-5500, è stata creata una zona WLAN-Staff in modo tale da poterne definire le caratteristiche univocamente e distinte dalle altre reti annunciate. In particolare questa rete è stata considerata “Trust” e sono stati attivati i servizi di Gateway Antivirus, Anti-Spyware e Intrusion Prevention, come rilevabile dalla figura seguente:

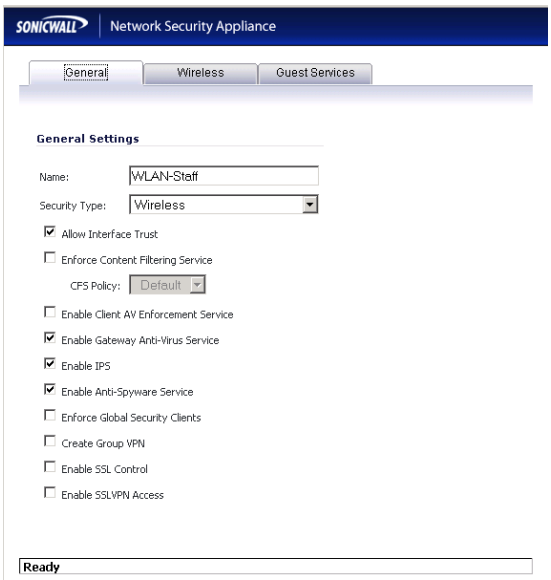

Figura 6: Dettaglio zona WLAN-Staff

È stato quindi creato un profilo a livello di Virtual Access Point per definirne i criteri di sicurezza, come indicato nella figura 7:

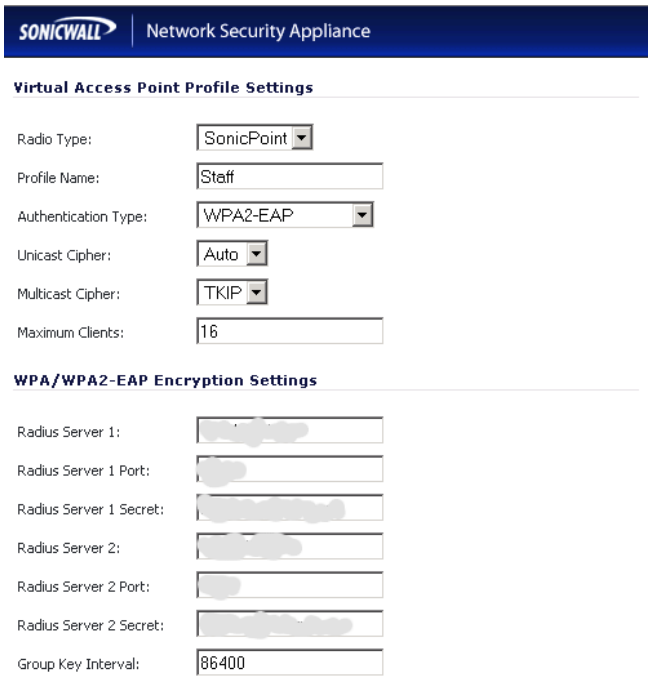

Figura 7: Dettaglio profilo TOCNR-Staff

Quindi tale profilo è stato assegnato al SSID TOCNR-Staff e incluso nel gruppo di SSID che in automatico vengono assegnati agli Access Point quando connessi all'apparato principale.

Infine sul firewall dell'NSA-5500 è stato aperto il traffico per tale rete verso la LAN, la DMZ e la WAN in modo analogo a quanto applicato ai computer connessi via cavo alla rete locale.

4.2 Configurazione freeradius

Il server radius per questa rete wireless deve effettuare l'autenticazione tramite 802.1x degli utenti accedendo al server Ldap che nel nostro caso è costituito da Active Directory in un dominio Windows Server 2003R2. In questo caso gli unici utenti autorizzati ad accedere sono i soli utenti presenti nel nostro database locale, senza attivare nessun altro accordo di cross-autenticazione.

Nel file *clients.conf* è stato inserito l'indirizzo IP ed il secret prestabilito nella

configurazione precedente per permettere al NSA-5500 di autenticare tramite questo server radius.

È stato attivato il supporto del server per il protocollo EAP e i vari sotto moduli necessari all'autenticazione WPA stabilita per l'accesso alla rete TOCNR-Staff, in particolare il modulo MS-Chapv2 necessario per la compatibilità con le piattaforme Windows e l'accesso a Active Directory per l'autenticazione.

Per l'autenticazione tramite server Ldap è stato modificato il file ldap nella directory modules come segue:

```
ldap {
    server = "xxxxxx.to.cnr.it"
    port = 3268
    identity = "CN=xxxxxxx,CN=xxxxxx,DC=to,DC=cnr,DC=it"
    password = "xxxxxx"
    basedn = "DC=to,DC=cnr,DC=it"
    filter = "(sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}})"
```

Infine nel file *users* si è introdotta una condizione che impone, nel caso di utente che tenta l'autenticazione per la rete TOCNR-Staff di limitare la ricerca ai soli utenti locali, cioè ai soli utenti raggiungibili via Ldap in Active Directory che è la sola forma di autenticazione locale impostata.

4.3 Configurazione client

Per i client Windows, in particolare Windows XP, occorre modificare leggermente la configurazione di default, impostando l'autenticazione WPA2 con crittografia TKIP, il tipo EAP selezionare “ Protected EAP (PEAP)” ed il metodo di autenticazione “EAP-MSCHAP v2”. Per una guida dettagliata si rimanda all'area Supporto sul sito dell'Infrastruttura di Rete CNR Piemonte, dove viene guidato l'utente passo a passo nella configurazione di un client Windows XP.

Per i client linux, nello specifico per un client Ubuntu Desktop, utilizzando Network Manager, si deve impostare la configurazione illustrata nella figura seguente:

Figura 8: Cliente Ubuntu WPA e WPA2

Si è anche verificata la possibilità di connessione tramite cellulare, dotato di connessione wireless e sistema Windows Mobile 6.0, ma è stato necessario scaricare ed installare un software aggiuntivo, ottenuto dal sito www.securew2.com, a cui si rimanda per ulteriori spiegazioni e informazioni su installazione e configurazione.

5. SSID EDUROAM

Questa rete è quella annunciata all'interno del circuito internazionale Eduroam. A questa rete, grazie all'inserimento del server radius nella gerarchia Eduroam, possono accedere tutti gli utenti che appartengo ad un'organizzazione inserita nel circuito e viceversa, qualsiasi nostro utente che si trovi presso un'altra organizzazione inserita nella gerarchia Eduroam potrà accedere alla rete wireless eduroam utilizzando le proprie credenziali locali, es. N.cognome@to.cnr.it e la propria password. Si evidenzia come lo user name da utilizzare, se si sta accedendo da un'altra organizzazione, è il solito N.Cognome seguito da un realm che identifica l'organizzazione di appartenenza, che nel caso dei nostri utenti è @to.cnr.it.

Per aderire alla gerarchia Eduroam è necessario rispettare alcuni standard di sicurezza e in particolare applicare l'autenticazione tramite 802.1x. Con questo protocollo si ha la sicurezza che le credenziali transitano in forma crittografata tra il computer dell'utente che accede alla rete wireless fino al suo server di autenticazione, evitando che nel mezzo possano essere intercettate e quindi utilizzate illegalmente.

La configurazione degli apparati è simile a quella impiegata per la rete TOCNR-Staff, con la differenza che l'accesso è permesso a tutti gli utenti, non solo quelli locali, e cambiano le regole sul firewall verso la LAN e le porte disponibili. Seguono le configurazioni nel dettaglio dei vari apparati.

5.1 Configurazioni Sonicwall

Oltre alla configurazione di una VLAN dedicata a questo SSID, come riportato nel paragrafo 3.2 Configurazione NSA-5500, è stata creata una zona WLAN-Eduroam in modo tale da poterne definire le caratteristiche univocamente e distinte dalle altre reti annunciate. In particolare questa rete, al contrario della precedente, non è stata considerata “Trust” e non sono stati attivati i servizi di Gateway Antivirus, Anti-Spyware e Intrusion Prevention, come rilevabile dalla figura seguente:

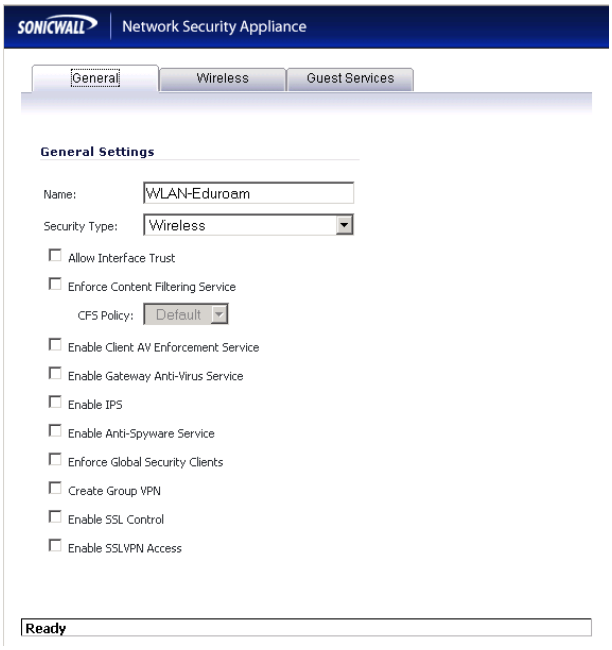

Figura 9: Dettaglio zona WLAN-Eduroam

È stato quindi creato un profilo a livello di Virtual Access Point per definirne i criteri di sicurezza, come indicato nella figura seguente:

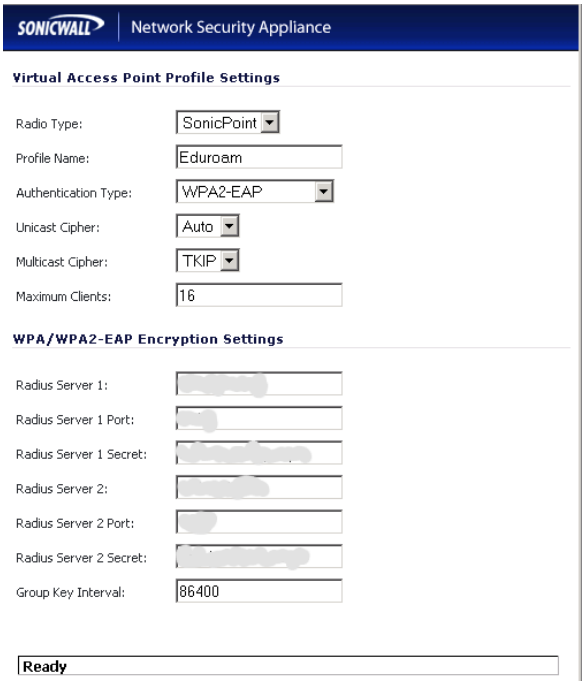

Figura 10: Dettaglio profilo Eduroam

Quindi tale profilo è stato assegnato al SSID eduroam e incluso nel gruppo di

SSID che in automatico vengono assegnati agli Access Point quando connessi all'apparato principale.

Infine sul firewall dell'NSA-5500 è stato aperto il traffico per tale rete verso la DMZ, eccettuato il traffico che già normalmente è interdetto dalla WAN verso la DMZ stessa, e verso la WAN limitata alle porte come richiesto dalle specifiche di Eduroam elencate nella figura seguente:

HTTP	TCP	80	80
HTTPS	TCP	443	443
IMAP3	TCP	220	220
IMAP4	TCP	143	143
POP3 (Retrieve E-Mail)	TCP	110	110
Terminal Services TCP	TCP	3389	3389
PPTP	TCP	1723	1723
SSH	TCP	22	22
ESP (IPSec)	IPSEC_ESP	1	1
FTP	TCP	21	21
IKE (Key Exchange)	UDP	500	500
IKE (Traversal)	UDP	4500	4500
Submission Port	TCP	587	587
IMAPS	TCP	993	993
POPS	TCP	995	995
OpenVPN	UDP	1194	1194
Cisco IPSec VPN over TCP	TCP	10000	10000
SMTPS	TCP	465	465

Figura 11: Traffico Eduroam permesso

5.2 *Configurazione freeradius*

Per il corretto funzionamento è necessario che il nostro server radius sia inserito nella gerarchia dei radius di Eduroam. Questo lo si è ottenuto attraverso il Garr, riferimento nazionale per la rete Eduroam, agganciando il nostro radius al radius nazionale del Garr inserito nella rete Eduroam. Nella configurazione del server si è inserito quindi nel file *clients.conf* i riferimenti (indirizzo IP e secret) del server radius Garr:

```
client 192.84.xxx.xxx/32 {
secret          = **********
shortname       = garredu
}
```

Nel file proxy.conf è stata poi inserita una direttiva DEFAULT in base alla quale, per un utente con realm non tra quelli conosciuti, viene reindirizzata l'autenticazione verso il radius del Garr che a sua volta provvederà a ricercare il server radius di appartenenza dell'utente che sta accedendo:

```
realm DEFAULT {
        type            = radius
        authhost        = 192.84.xxx.xxx:1812
        accthost        = 192.84.xxx.xxx:1813
        secret          = **********************
        nostrip
}
```

5.3 Configurazioni client

Essendo il protocollo di autenticazione lo stesso di quello utilizzato per la rete TOCNR-Staff si rimanda al paragrafo 4.3 per la trattazione sulla configurazione dei client.

Come già accennato, esiste la reversibilità di accesso su tale rete, quindi un utente locale che si trovi presso un ente che aderisce a Eduroam, potrà accedere alla rete wireless dell'ospitante tramite le proprie credenziali locali, col solo accorgimento dell'aggiunta del nostro realm (@to.cnr.it) al suo nome utente. In aggiunta, le regole della rete Eduroam consigliano che il SSID annunciato sia sempre lo stesso, cioè 'eduroam', in tal modo una volta configurato l'accesso per una località, al trovarsi in un altra organizzazione aderente a Eduroam, in automatico e comunque senza necessità di ripetere la configurazione, il nostro computer si aggancerà alla rete wireless tramite lo stesso SSID eduroam.

6. SSID TOCNR-OSPITI

Questa terza rete è stata impostata per permettere l'accesso a tutti coloro che appartengono ad organizzazioni con le quali esistano degli accordi di cross-autenticazione. Per poter racchiudere in un unico sistema tutte le tipologie di autenticazione che le varie organizzazioni con cui collaboriamo utilizzano, si è scelto di implementare l'autenticazione tramite captive portal.

La rete TOCNR-Ospiti è inizialmente aperta, cioè il client si connette alla rete wireless senza alcun tipo di autenticazione ma il traffico da e verso il computer è tutto bloccato fino a quanto l'utente, aprendo un browser, non si autentica con le proprie credenziali e solo dopo l'esito positivo dell'autenticazione è permesso il traffico.

Per questa rete si è sfruttata l'opzione offerta dal NSA-5500 di poter gestire il captive portal con pagine di autenticazione personalizzate, che nel nostro caso sono state caratterizzate per autenticare l'utente tramite lo stesso server radius utilizzato per i casi precedenti.

6.1 Configurazione Sonicwall

Oltre alla configurazione di una VLAN dedicata a questo SSID, come riportato nel paragrafo 3.2 Configurazione NSA-5500, è stata creata una zona WLAN-Ospiti in modo tale da poterne definire le caratteristiche univocamente e distinte dalle altre reti annunciate. In questo caso in particolare oltre alla configurazione simile a quella della rete eduroam si è anche configurata l'opzione relativa ai Guest Services per impostare l'autenticazione su tale rete tramite captive portal come nelle figure seguenti:

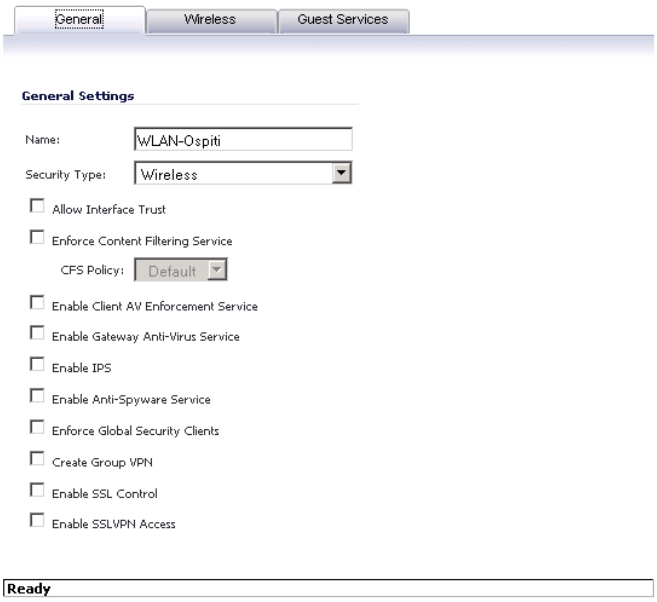

Figura 12: Dettaglio zona WLAN-Ospiti

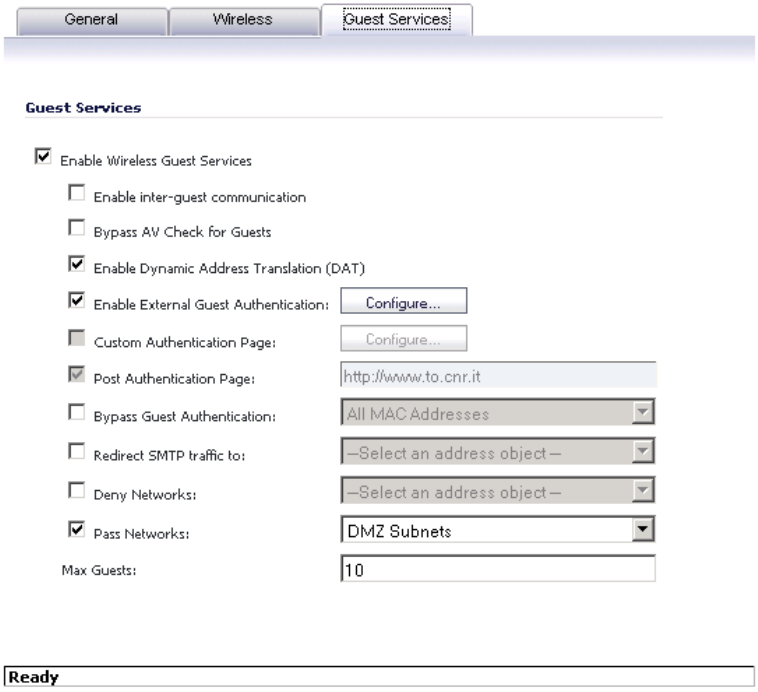

Figura 13: Configurazione Guest Services

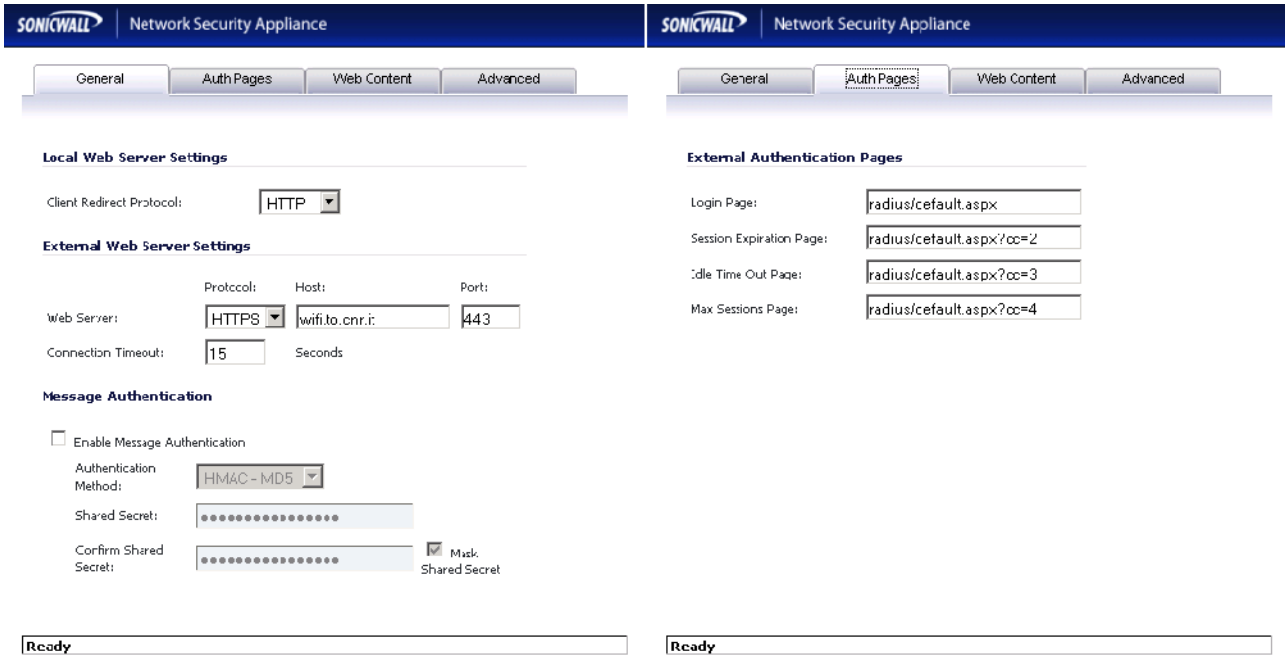

Figura 14: Configurazione Captive Portal

Inoltre sul firewall dell'NSA-5500 è stato aperto il traffico per tale rete verso la DMZ, eccettuato il traffico che già normalmente è interdetto dalla WAN verso la DMZ

stessa, e verso la WAN limitata alle porte come per la rete Eduroam (cfr. 5.1 Configurazione Sonicwall della rete eduroam).

Si è quindi attivato un sito sul server Web (IIS6.0 su Windows server 2003R2) in grado di gestire le pagine dinamiche ASPX, essendo in tale formato forniti gli script dalla Sonicwall per sviluppare il Captive portal in modo personalizzato. Nello specifico le pagine utilizzate sono quelle che come autenticazione accedono ad un server radius, la cui configurazione è fatta modificando il file dei parametri *myvars.aspx* che risulta così definito:

```
<script language="VB" runat="server">
'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event
is non-exclusive.
Dim logoutPopup as String = "1"
'Set the RADIUS server IP or Name
'Make sure the LHM Server is setup as client on the RADIUS Server
Dim myRadiusServer as String = "xxx.xxx.xxx.xxx"
'Set the RADIUS Port
Dim myRadiusPort as String = "1812"
'Set the RADIUS Secret
Dim myRadiusSecret as String = "**********"
'Set the default LHM Session Timeout (for when no attributes is retrieved)
Dim sessTimer as String = "3600"
'Set the default LHM Idle Timeout (for when no attributes is retrieved)
Dim idleTimer as String = "300"
'Set the secret for use with optional HMAC auth, as configured in the Extern
Guest Auth config on the SonicWALL
Dim strHmac as String = "**********"
'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"
'Set the logo image to use
Dim logo as String = "wificnrtortm.gif"
'----------------------End of Configurable Settings----------------------
</script>
```

Da questo file attingono le informazioni gli script di login e logout utilizzati dal Captive portal per dare l'accesso alla rete agli utenti che si autenticano.

Infine sul server web è stato installato un certificato rilasciato da SCS tramite il servizio di CA del Garr affinché gli utenti che accedono alla pagina di autenticazione, che è per ovvie ragione criptata tramite protocollo HTTPS, non debbano subire i fastidiosi messaggi di certificato non attendibile che invece sarebbero comparsi utilizzando un certificato emesso da una CA non presente nei principali browser.

6.2 Configurazione freeradius

Per questa rete l'accesso è previsto, oltre che per gli utenti locali ai quali comunque si consiglia l'accesso tramite la rete TOCNR-Staff, per tutti quegli utenti che appartengono a strutture ed enti con i quali esiste un rapporto di cross-autenticazione. In particolare sono stati finora stipulati accordi in tal senso con: CNR Sede centrale, Politecnico di Torino, Università di Torino e CSP Piemonte. Questi accordi si configurano sul server radius e risulta quindi:

nel file *clients.conf*

```
client 130.192.X.X/32 {
        secret          = **********
        shortname       = polito
}
client 130.192.X.X/32 {
        secret          = **********
        shortname       = unito
}
client 194.116.X.X/32 {
        secret          = **********
        shortname       = cspto
}
client 150.146.X.X/32 {
        secret          = **********
        shortname       = cnrsede
}
```

nel file *proxy.conf*

```
realm cnr.it {
        type            = radius
        authhost        = 150.146.x.x:1812
        accthost        = 150.146.x.x:1813
        secret          = *********
}
realm polito.it {
        type            = radius
        authhost        = 130.192.x.x:1645
        accthost        = 130.192.x.x:1646
        secret          = *********
        nostrip
}
realm studenti.polito.it {
        type            = radius
        authhost        = 130.192.x.x:1645
```

```
        accthost        = 130.192.x.x:1646
        secret          = *********
        nostrip
}
realm unito.it {
        type            = radius
        authhost        = 130.192.x.x:1645
        accthost        = 130.192.x.x:1646
        secret          = *********
        nostrip
}
realm studenti.unito.it {
        type            = radius
        authhost        = 130.192.x.x:1645
        accthost        = 130.192.x.x:1646
        secret          = *********
        nostrip
}
realm csp.it {
        type            = radius
        authhost        = 194.116.x.x:1812
        accthost        = 194.116.x.x:1813
        secret          = *********
        nostrip
}
```

Da quest'ultimo si possono desumere tutti i realm (evidenziati in grassetto) delle strutture con i quali i rispettivi utenti devo autenticarsi qualora vogliano accedere alla rete TOCNR-Ospiti annunciata dagli access point della nostra infrastruttura di rete.

6.3 Configurazione client

I client che vogliono accedere a questa rete non necessitano di configurazione alcuna, sarà sufficiente connettersi alla rete annunciata, di tipo open ma dalla quale non è possibile effettuare traffico verso alcun sito ad eccezione di quello di autenticazione, e quindi aprire il browser su una pagina web qualsiasi. A questo punto entra in gioco il captive portal che intercetta la richiesta e reindirizza il browser dell'utente sulla pagina di autenticazione che si presenta così:

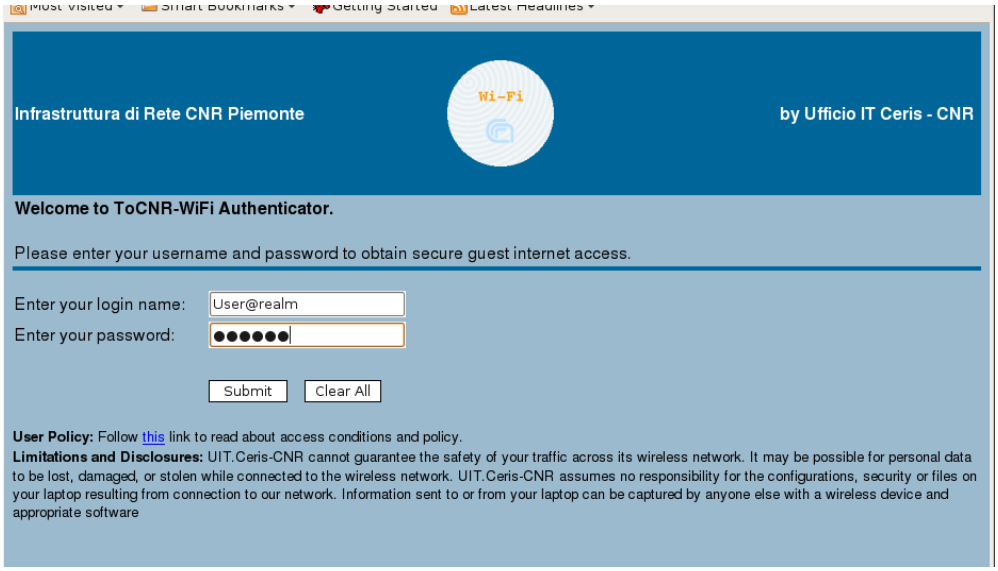

Figura 15: Pagina autenticazione Captive Portal

In questa pagina vanno inserite le credenziali con cui l'utente vuole autenticarsi, ponendo attenzione ad inserire anche il realm nel caso di utenti che non appartengono ai nostri utenti locali, e quindi dopo aver premuto Submit, se le credenziali sono valide, comparirà la seguente pagina (v. fig. 16) che annuncia il successo dell'autenticazione e la possibilità quindi di effettuare traffico verso internet, limitatamente a quello permesso per questa rete.

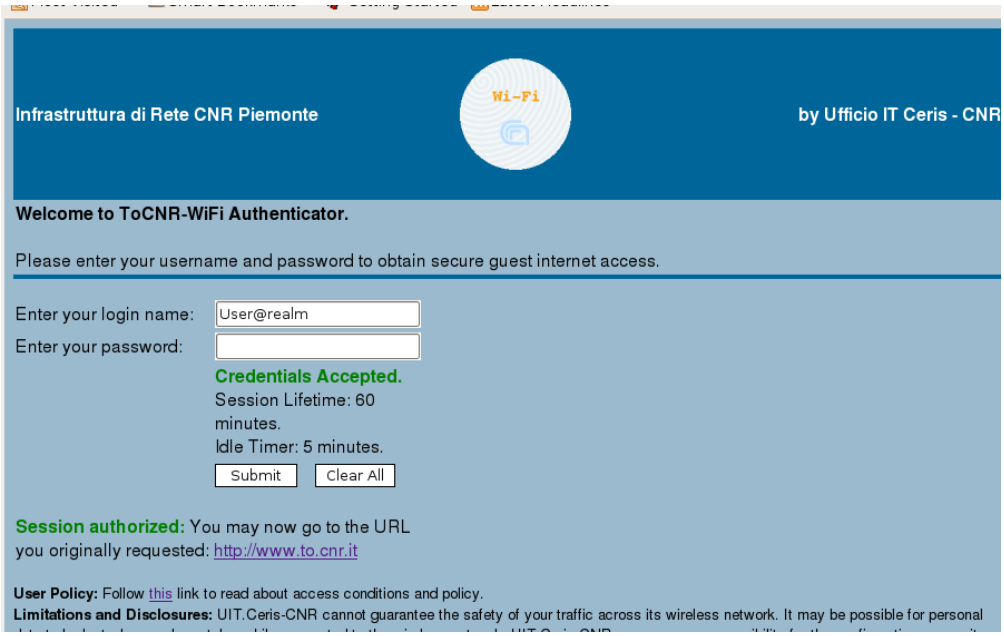

Figura 16: Pagina utente autenticato Captive Portal

Contemporaneamente comparirà anche il pop-up (v. fig. 17) tramite il quale, qualora l'utente lo desideri, può terminare la sua sessione prima del timeout, effettuando il logout dalla rete. In questo caso il popup si modificherà come nella figura 18.

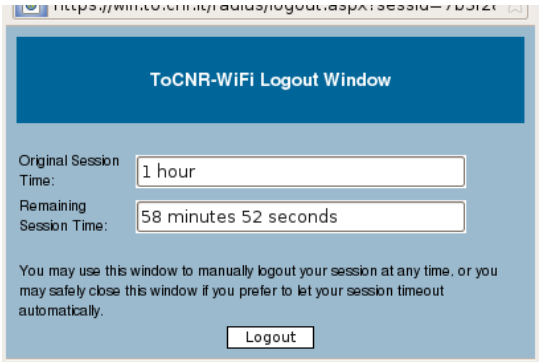

Figura 17: Popup durata sessione Captive Portal

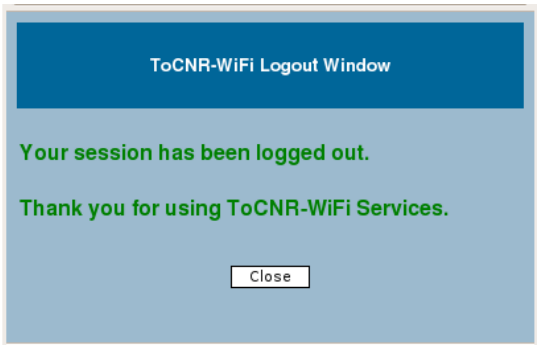

Figura 18: Popup termine sessione Captive Portal

È importante evidenziare nuovamente la reversibilità che gli accordi di cross-autenticazione offrono, cioè la possibilità per un nostro utente locale di poter accedere alle reti wireless delle strutture ed enti con le quali esitono gli accordi, interessante soprattutto tenendo conto delle coperture wireless che enti come il Politecnico di Torino o l'Università di Torino offrono.

7. CONCLUSIONI

Da quasi un anno dall'inizio della disponibilità della rete wireless, con il continuo ampliamento della copertura, l'ultimo access point installato qualche settimana fa, possiamo essere soddisfatti dei risultati tecnici ottenuti e del ritorno in termini di gradimento da parte degli utenti del servizio offerto.

Per gli aspetti tecnici ed informatici, la gestione tramite la NSA Sonicwall ha reso realmente semplice la gestione dei vari Access Point, la loro integrazione nell'infrastruttura di rete esistente e le operazioni necessarie all'ampliamento della copertura.

Anche gli utenti hanno gradito il servizio offerto, in alcuni casi andando oltre le previsioni di utilizzo, impiegandolo ad esempio per raggiungere in wireless computer in laboratori dove l'alternativa sarebbe stata quella di costosi e più che tutto devastanti lavori di cablaggio e posa di cavi. Un altro interessante impiego è stato durante un congresso ospitato presso il Ceris a Moncalieri che ha messo a prova la capacità di gestire in modo sicuro il rilascio di un paio di centinaia di credenziali e coordinato con la segreteria del congresso, per permettere l'accesso wireless ai partecipanti, mantenendo allo stesso tempo il livello di sicurezza richiesto da tale servizio. Non ultimo l'aspetto della reciprocità del servizio che ha reso possibile ai nostri utenti sfruttare gli accessi wireless offerti da alcune altre importanti strutture piemontesi dotate di copertura wireless particolarmente estesa e presso le quali sovente si trovano a seguito di numerose collaborazioni in essere.

Oltre a futuri ampliamenti della copertura anche presso quelle strutture non ancora servite, sicuramente uno dei prossimi obiettivi sarà quello di ampliare l'offerta d'accesso tramite autenticazione federata e nello specifico l'integrazione del servizio wireless con la Federazione IDEM del Garr, al cui progetto l'Infrastruttura di rete CNR Piemonte ha partecipato attivamente fino dai sui albori.