Denominazione commerciale: **SECURE GUEST ACCESS**
Codice Articolo Fornitore: CaptivePortale@Smart
Unità di Misura: A corpo
Quantità Vendibile x unità di misura: 1
Lotto minimo per unità di misura: 1
Tempo di consegna (giorni): 60 gg
Disponibilità Minima Garantita: 1
Durata Garanzia : 36 mesi
Durata Assistenza Tecnica : 36 mesi
Descrizione: La piattaforma prevede l'attivazione del servizio LAN CONCERTO Secure Guest Access e comprende sia l'attivazione delle licenze del sistema presso il Cloud di TIM e sia l'attivazione del servizio di assistenza tecnica. Il servizio verrà erogato per n. 13 Access Point e verrà erogato su una unica sede .

DESCRIZIONE TECNICA

LAN CONCERTO Secure Guest Access è un sistema di autenticazione completo che si occupa di autenticare e di mantenere traccia degli utenti connessi al sistema, oltre ad abilitare l'erogazione di un insieme di servizi a valore aggiunto, la soluzione è una piattaforma completa ed aperta, orientata alle applicazioni geografiche con grandi numeri di utenti e dotata di connettori per interfacciarsi con altre reti, permettendo la realizzazione di una federazione di rete su scala municipale e di integrazione con Roaming Partner.

Funzionamento del sistema WiFi Secure Guest Access by MobiMESH

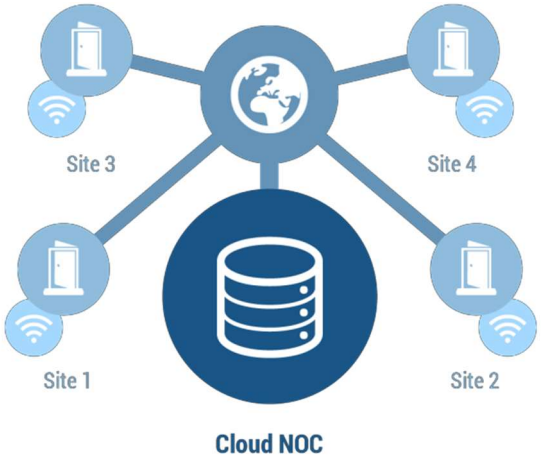
LAN CONCERTO si occupa di intercettare le connessioni alla rete da parte dell'utente, e, qualora esse siano effettuate da un utente non ancora autenticato, a dirottare l'utente stesso sulla pagina di autenticazione, dove è possibile fornire le proprie credenziali di accesso, che, se verificate positivamente, garantiranno all'utente di procedere con l'accesso alla rete.

Il Secure Guest Access si occupa quindi di:

- intercettare le connessioni degli utenti che accedono alla risorsa di rete;
- redirigere l'utente che cerca di navigare ad una pagina di benvenuto, definita nel seguito Welcome Page (WP), su cui si trovano un insieme di informazioni iniziali di benvenuto, ed i form necessari per registrarsi al servizio e per autenticarsi;
- permette l'auto-registrazione degli utenti, con associazione delle credenziali ad un numero di rete cellulare o con la possibilità di ottenerle tramite operatore;
- permette agli utenti in possesso di credenziali valide di accedere ad Internet secondo le modalità specificate dai ticket ad essi assegnati;
- permette la navigazione senza limiti sui siti compresi in una lista, definita Walled Garden, abilitabile e modificabile dal gestore di rete;
- permette al gestore di rete di determinare quali protocolli (TCP/IP) permettere prima e dopo l'autenticazione agli utenti registrati;
- permette al gestore di rete di determinare le tipologie di ticket, che definiscono la capacità degli utenti di accedere ad Internet, erogabili sulla rete; i ticket possono essere definiti imponendo vincoli al tempo di navigazione, sulle ripetizioni cadenzate (ad es: 1 ora al giorno), sulla quantità di traffico, ecc e permette all'utente di acquistare ticket tramite scratch card o tramite codice di gruppo.

Architettura

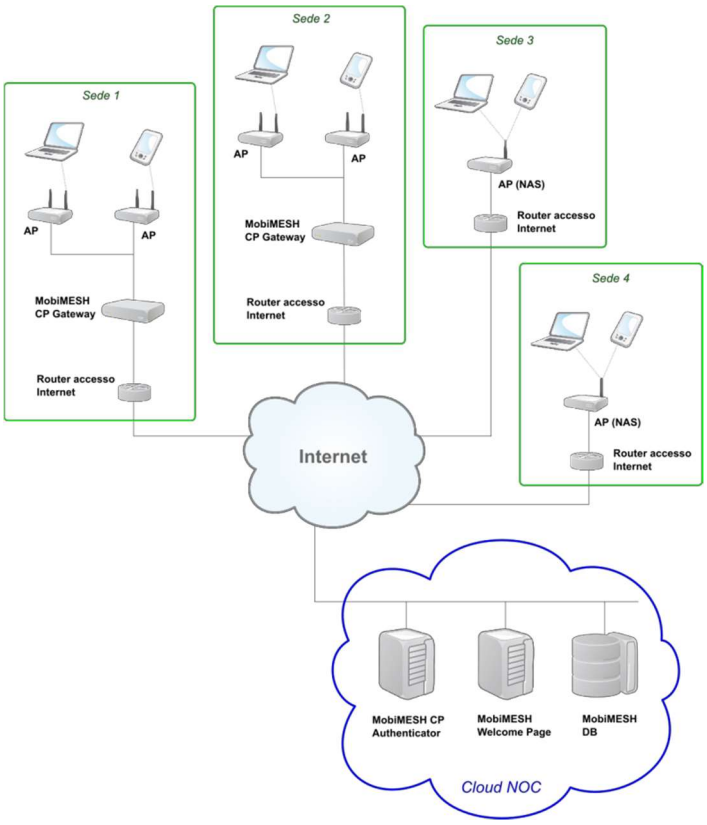
Le componenti di portale (Authenticator, DB utenti, Welcome Page) si trovano presso l'IDC TIM, in ambiente cloud ridondato e sicuro.



La componente a campo (NAS) può essere di due tipi:

- Access Point Cisco Meraki, Aruba Networks, Alcatel-Lucent: si tratta dei brand supportati dalla piattaforma ed inclusi nell'offerta LAN Concerto. Nel caso di questi brand l'Access Point stesso può fare da NAS, puntando al Cloud NOC per l'autenticazione;
- MobiMESH Gateway: per tutti gli Access Point ed in generale per tutte le tecnologie di accesso IP è possibile impiegare un MobiMESH Gateway, sotto forma di appliance o di software da installare su VM a campo, che si occupa delle funzionalità di NAS, disaccoppiando di fatto la componente di accesso da quella di autenticazione.
-

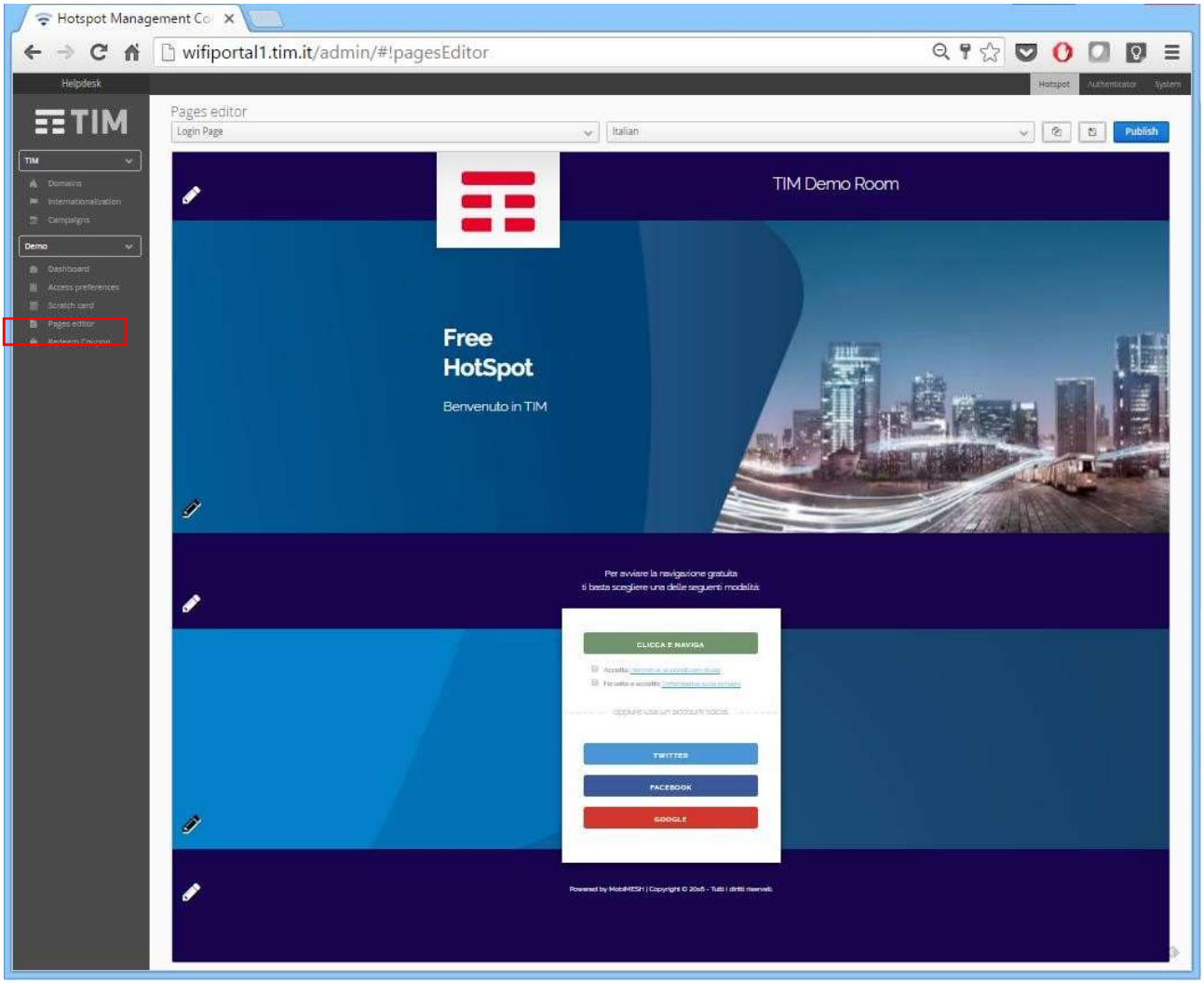
La configurazione tipica dell'architettura di rete è riportata nella figura che segue: un insieme di terminali a cui occorre garantire accesso pubblico ad Internet sono connessi ad una rete WLAN/LAN a valle della quale si colloca il Secure Guest Access.


Sede 1
AP
AP
MobiMESH
CP Gateway
Router accesso
Internet
Sede 2
AP
AP
MobiMESH
CP Gateway
Router accesso
Internet
Sede 3
AP (NAS)
Router accesso
Internet
Sede 4
AP (NAS)
Router accesso
Internet
Internet
MobiMESH CP
Authenticator
MobiMESH
Welcome Page
MobiMESH
DB
Cloud NOC

Welcome Page

La Welcome Page è la pagina che viene presentata all'utente che si collega alla rete, ed è impiegata per registrarsi o autenticarsi al servizio, per ottenere informazioni e puntatori utili, e per accedere ad Internet.

La Welcome Page può essere personalizzata direttamente dal Cliente attraverso una semplice interfaccia web che permette di modificare la grafica e i contenuti della pagina stessa.



Ciascuna sezione della Welcome Page può essere personalizzata inserendo immagini, testi, HTML, ecc nei punti opportuni, attraverso l'editor web punta e clicca.

La Welcome Page mostra inoltre i metodi di autenticazione e registrazione selezionati dall'utente (si veda a tal proposito la sezione relativa che segue).

La Welcome Page così generata è responsive, e si adatta automaticamente ai vari formati e dimensioni dei dispositivi.

La Welcome Page è una delle componenti dei Service Profile; infatti ciascun Service Profile prevede le modalità di autenticazione, le policy di accesso e la Welcome Page, e può essere applicato ad una singola location (sede cliente identificata univocamente, con connettività Internet dedicata o identificabile tramite VLAN/rete IP) o ad un insieme di location.

E’ quindi possibile fornire una Welcome Page differente per ciascuna sede Cliente, oppure per ciascun insieme di sedi Cliente; se l’insieme delle sedi Cliente associate ad una data Welcome Page è l’insieme totale delle sedi, tutte le sedi atterreranno sulla medesima Welcome Page.

Metodi di autenticazione

Il sistema Secure Guest Access prevede un vasto insieme di metodi di autenticazione, che possono essere selezionati ed impiegati dal Cliente e modificati in qualsiasi momento.

I metodi disponibili sono i seguenti:

- Classic Login: autenticazione tramite username e password, verificati sul database locale del sistema;
- Click&Surf: autenticazione 1-click, che prevede che l’utente effettui solamente un click sul bottone di accesso, prendendo visione dell’informativa sulla privacy e dei termini e condizioni. L’account sarà associato al MAC address del terminale impiegato;
- Mail&Surf: autenticazione tramite email, che prevede che l'utente fornisca l'indirizzo email, che viene verificato con un link inviato alla casella indicata. L'account sarà associato al MAC address del terminale impiegato;
- Scratch Card: autenticazione basata sull’inserimento di un numero di scratch card. Le scratch card sono generabili dall’apposito pannello (si veda il relativo paragrafo nel seguito) e sono consegnate al cliente, che, inserendo il numero, viene abilitato alla navigazione. Si noti che questo metodo di autenticazione può permettere l’identificazione univoca dell’utente che ha ricevuto la scratch card, se l’operatore che eroga la scratch card prende nota del numero di documento di identità dell’utente finale;
- **Group Code**: autenticazione basata su un codice di gruppo, utilizzabile da più utenti contemporaneamente. L'account è associato al MAC address del terminale, e non è possibile identificare univocamente l'utente a partire dal group code, in quanto condiviso tra più utenti;
- **Social Login Twitter**: autenticazione basata sull’account Twitter dell’utente. E’ possibile effettuare il Social Login con Twitter semplice (sola autenticazione) oppure effettuare la validazione in due passaggi, con l’SMS; in questo secondo caso, a valle dell’autenticazione dell’account viene effettuata una validazione tramite codice univoco inviato via SMS, permettendo in questo modo l’associazione di un numero di telefono cellulare all’account, così garantendo l’identificazione univoca dell’utente. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte;
- **Social Login Facebook**: autenticazione basata sull’account Facebook dell’utente. E’ possibile effettuare il Social Login con Facebook semplice (sola autenticazione) oppure effettuare la validazione in due passaggi, con l’SMS; in questo secondo caso, a valle dell’autenticazione dell’account viene effettuata una validazione tramite codice univoco inviato via SMS, permettendo in questo modo l’associazione di un numero di telefono cellulare all’account, così garantendo l’identificazione univoca dell’utente. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte;
- **Social Login Google**: autenticazione basata sull’account Google dell’utente. E’ possibile effettuare il Social Login con Google semplice (sola autenticazione) oppure effettuare la validazione in due passaggi, con l’SMS; in questo secondo caso, a valle dell’autenticazione dell’account viene effettuata una validazione tramite codice univoco inviato via SMS, permettendo in questo modo l’associazione di un numero di telefono cellulare all’account, così garantendo l’identificazione univoca dell’utente. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte;
- **Social Login Instagram**: autenticazione basata sull’account Instagram dell’utente. E’ possibile effettuare il Social Login con Instagram semplice (sola autenticazione) oppure effettuare la validazione in due passaggi, con l’SMS; in questo secondo caso, a valle dell’autenticazione dell’account viene effettuata una validazione tramite codice univoco inviato via SMS, permettendo in questo modo l’associazione di un numero di telefono cellulare all’account, così garantendo l’identificazione univoca dell’utente. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte;
- **Social Login LinkedIn**: autenticazione basata sull’account LinkedIn dell’utente. E’ possibile effettuare il Social Login con LinkedIn semplice (sola autenticazione) oppure effettuare la validazione in due passaggi, con l’SMS; in questo secondo caso, a valle dell’autenticazione dell’account viene effettuata una validazione tramite codice univoco inviato via SMS, permettendo in questo modo l’associazione di un numero di telefono cellulare all’account, così garantendo l’identificazione univoca dell’utente. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte;

- **OpenID:** autenticazione tramite account di terze parti interfacciate tramite protocollo OpenID Connect;
- **Roaming**: autenticazione tramite autenticatori terze parti (Roaming Partner, RADIUS esterni, ecc);
- **Autoregistrazione**: registrazione dell'utente tramite SMS e autenticazione con le credenziali inviate per SMS; questa modalità, grazie all'invio credenziali via SMS, garantisce l'associazione univoca dell'account al numero di telefono, e quindi l'identificazione. Il costo degli SMS non è incluso nella piattaforma, ma va corrisposto a parte.

È possibile raccogliere informazioni dall'utente nei metodi di registrazione locale, ottenendo quindi dati da associare al profilo; ad esempio è possibile associare al metodo Click&Surf la raccolta dell'indirizzo email per ottenere gli indirizzi email degli utenti, e così via.

I metodi possono essere abilitati indipendentemente l'uno dall'altro, e possono essere attivati e disattivati a piacere.

Si noti che per quanto riguarda i metodi con Social Login, le informazioni raccolte sono solo quelle base per l'autenticazione; qualora il Cliente richieda di ottenere ulteriori informazioni occorrerà modificare l'APP del Social Network a tale proposito, e verrà comunque richiesta autorizzazione da parte del Social Network all'utente finale.

Policy di navigazione

Il sistema Secure Guest Access prevede diversi meccanismi di gestione delle policy di navigazione per gli utenti autenticati. In particolare sono previste tre tipologie di meccanismo:

- **Static Limit**: impostazione di limiti fissi e statici per utente, senza nozione di stato. I limiti impostabili sono il session timeout, l'idle timeout, l'update interval, la banda per utente in uplink e in downlink. Si tratta del profilo più semplice, consigliato quando si impiega come NAS un Access Point;
- **Daily Limit**: impostazione di limiti semplici, con nozione di stato e ripetitività giornaliera. I limiti imponibili sono tempo, traffico, tempo e traffico, tempo o traffico, banda per utente in uplink e in downlink. E' inoltre possibile impostare il "throttled mode", che prevede che all'esaurirsi dei vincoli impostati si passi in modalità a banda ridotta fino al termine della giornata;
- **Ticket**: impostazione di limiti complessi, con più vincoli impostabili. I vincoli possono essere limiti fissi (che impostano massima banda in downlink e uplink, timeout di inattività, ID di profilo, ecc), limiti sui NAS di applicazione, sulla quantità di tempo di accesso, sul numero di login consentiti, sulla data di scadenza.

A ciascun dominio può essere associata una policy di default tra quelle sopra descritte, con i vincoli configurati; inoltre è possibile effettuare l'override della policy per utente.

Dashboard

Il sistema WiFi Secure Guest dispone di una Dashboard per ogni Service Profile, che visualizza i dati principali del sistema.

I grafici riportati nella dashboard sono:

Sessioni

- Numero di sessioni
- Numero medio di sessioni orarie
- Numero totale di account registrati
- Andamento dei login nel tempo

- Andamento delle contemporaneità nel tempo

Dispositivi

- Numero totale di dispositivi
- Numero medio di sessioni per dispositivo
- Numero medio di dispositivi per ora
- Confronto tra sessioni e dispositivi
- Analisi del numero di visite del dispositivo nel lasso di tempo

Traffico

- Traffico totale e distinzione Upload/Download
- Flusso di traffico nel tempo
- Medie di traffico per sessione e dispositivo

Durata

- Durata totale delle connessioni
- Durata media per sessione
- Durata media per dispositivo
- Andamento della durata delle connessioni nel tempo

Loyality

- Analisi nuovi utenti
- Ritorni dei nuovi utenti nei range temporali precedenti

Tutti i dati sono visualizzabili su intervalli di tempo definibili, e precisamente:

- Il giorno precedente;
- La settimana precedente;
- Il mese precedente;
- L'anno precedente.

Non sono incluse nella fornitura le seguenti componenti :

- Fornitura, configurazione e installazione AP;
- Configurazione rete LAN;
- SMS qualora si optasse per metodi di autenticazione che impiegano SMS;
- router di accesso Internet e connettività Internet;
- firewall e content filter e attività di configurazione e setup degli stessi;
- attività di configurazione portale/servizio ed evolutive;
- cablaggio strutturato e derivazione di alimentazione su tutti i siti;
- fornitura, posa e configurazione di armadi rack, UPS, switch altri elementi attivi o passivi non inclusi esplicitamente;
- parti di ricambio, ricambi di dispositivi, estensione di garanzia;
- interventi in campo al di fuori di quanto esplicitamente indicato;