Abilitare un Captive Portal sulla rete wireless Cisco

Abilitazione di Captive Portal sulla rete wireless Cisco

In un ambiente aziendale sempre più mobile e collaborativo, sempre più organizzazioni stanno aprendo i propri ambienti di rete per la condivisione controllata delle risorse con partner aziendali, clienti e altri ospiti. Le aziende sono alla ricerca di metodi migliori per:

·Accesso wireless sicuro a Internet per i clienti
· Accesso limitato alle risorse di rete aziendali per i partner aziendali
· Rapida autenticazione e connettività per i dipendenti che utilizzano i dispositivi mobili personali

Un access point wireless (AP) Cisco per piccole imprese, ad esempio WAP321 o WAP561, può essere facilmente integrato nella rete cablata esistente per fornire una connettività wireless con velocità e sicurezza paragonabili a una tipica connessione cablata.

La funzionalità Cisco Captive Portal offre un modo pratico, sicuro ed economico per offrire l'accesso wireless ai client e agli altri visitatori, mantenendo la sicurezza della rete interna. Una rete guest può servire per molti importanti scopi aziendali, tra cui la semplificazione delle attività con i partner, l'aumento della soddisfazione dei clienti e l'aumento della produttività dei dipendenti.

Captive Portal può fornire le seguenti funzionalità di base:

·Pagina di login guest personalizzata con logo aziendali
· Possibilità di creare più istanze del portale vincolato
· Opzioni di autenticazione multiple
· Possibilità di assegnare diritti e ruoli diversi
· Possibilità di assegnare larghezza di banda (a monte e a valle)

Come configurare Captive Portal?

Captive Portal può essere configurato tramite l'interfaccia grafica del dispositivo, per una configurazione rapida e di base, il cliente può utilizzare la procedura guidata per abilitare la funzione, vedere i passaggi seguenti:

Utilizzo dell'Installazione guidata

Eseguire l'installazione guidata dal dashboard principale della GUI del dispositivo.

Seguire le schermate della procedura guidata.

Abilitare l'accesso Guest (Captive Portal).

Assegnare un nome alla rete guest, ad esempio "Società - Guest".

Selezionare un tipo di protezione.

Se si desidera visualizzare una pagina Web specifica dopo che gli utenti hanno accettato le

condizioni per l'utilizzo del servizio dalla pagina iniziale, digitare l'URL e quindi l'URL che si desidera visualizzare sarà il sito Web della società.

Selezionare Successivo per passare alla pagina successiva.

Ora l'installazione di Captive Portal è completata, il cliente è in grado di connettersi alla rete guest e ottenere la pagina di benvenuto.

Per una configurazione e personalizzazione avanzate del portale, accedere all'interfaccia grafica del dispositivo dal menu Captive Portal.

Selezionare Configurazione istanza. Verrà creato un nome di istanza denominato "wiz-cp-inst1". È possibile scegliere questo nome o creare un nuovo nome per la configurazione dell'istanza e quindi salvare. Se si sceglie "wiz-cp-inst1", viene visualizzata la pagina Configurazione istanza.

Si noterà che l'installazione guidata associa automaticamente il nome dell'istanza del portale vincolato "**wiz-cp-inst1**" al SSID guest creato durante l'installazione guidata.

Se l'istanza è stata creata utilizzando la GUI, è necessario associarla alla rete guest creata. Dal menu a discesa selezionare il nome dell'istanza "Guest" o l'istanza creata dalla procedura guidata "**wiz-cp-inst1**".

Dal menu selezionare Configurazione portale Web per configurare la pagina di benvenuto del guest, scegliere il nome dell'istanza dal menu a discesa.

Selezionare il metodo di autenticazione per Captive Portal da utilizzare per verificare i client:

·Guest: l'utente non deve essere autenticato da un database.
· Locale: il dispositivo WAP utilizza un database locale per gli utenti autenticati.
· RADIUS: il dispositivo WAP utilizza un database su un server RADIUS remoto per autenticare gli utenti.

Se si sceglie il metodo di verifica "Locale", è necessario creare utenti locali.

Dal menu scegliere Locale.

Immettere il parametro use (nome dell'utente) e scegliere i parametri per il profilo utente.

Personalizzazione della pagina del portale Web, è possibile caricare il logo della propria società e le immagini grafiche in un massimo di 3 file, uno per lo sfondo della pagina (predefinito: cisco-bkg) al secondo per il logo della società (predefinito: cisco-log) e il terzo per la schermata di accesso (predefinito: log-key).

** Notare che le dimensioni di questo file devono essere di 5 KB.

Èora possibile personalizzare la pagina del portale Web, ad esempio aggiungere criteri di utilizzo accettazione, titolo e nome della finestra e così via...

Pagina personalizzata con il metodo di verifica Guest, questo significa che non è necessario eseguire l'autenticazione, l'utente dovrà solo accettare le condizioni del servizio e selezionare il pulsante Connetti, immettendo il nome utente è facoltativo.

Pagina personalizzata con il metodo di verifica impostato su Locale significa che l'utente deve immettere un nome utente e una password per l'autenticazione, quindi l'utente dovrà accettare le condizioni per l'utilizzo del servizio e selezionare il pulsante Connetti.

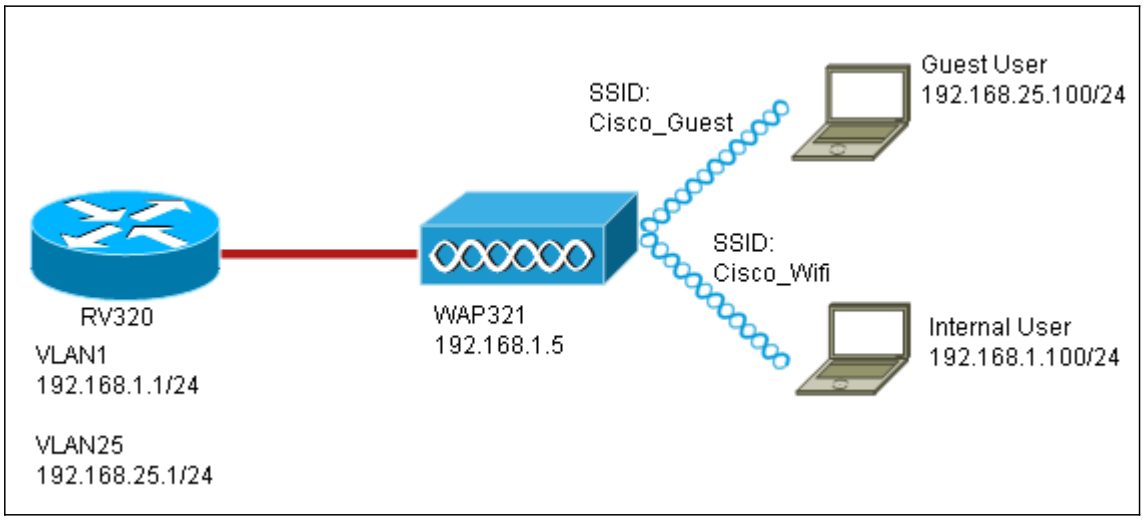
Captive Portal in un ambiente multi VLAN

In alcuni casi una rete ha bisogno di più VLAN per scopi diversi, per servire diversi gruppi di

utenti. Un esempio comune è rappresentato dalla creazione di una rete separata per gli utenti guest per impedire agli utenti non autorizzati di accedere alle risorse della rete aziendale. A volte sono presenti più reti wireless che devono essere disponibili a utenti diversi per lo stesso motivo. I modelli WAP321 e WAP561 possono soddisfare queste esigenze utilizzando Captive Portal, ma richiedono una configurazione aggiuntiva della rete. In questa sezione verrà esaminata la configurazione.

Introduzione - Configurazione esistente

in questo documento si presume che sia già presente una configurazione di rete. Nell'esempio vengono mostrate due reti, la rete principale e la rete guest. La configurazione per la creazione e la gestione degli indirizzi DHCP in ogni rete è già stata configurata. WAP321 è già stato configurato per trasmettere un SSID diverso per ogni rete. L'impostazione corrente sarà simile alla seguente:

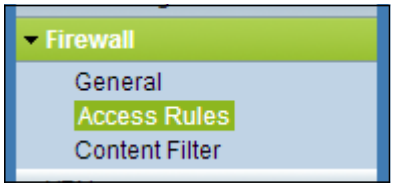


Al termine della configurazione, il routing tra VLAN verrà abilitato sulla rete in modo che tutti i client wireless possano accedere al Captive Portal, abilitando la connettività di rete.

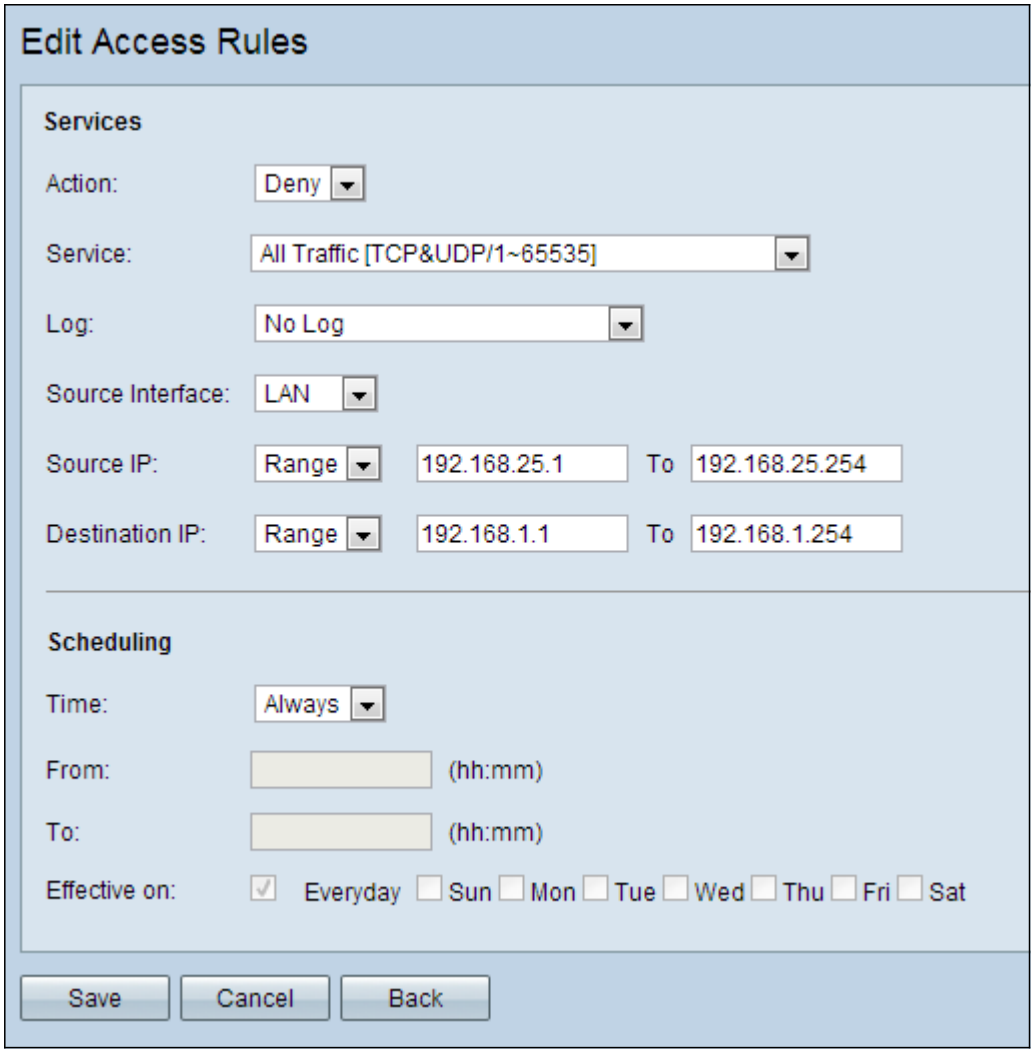
Configurazione

Innanzitutto, abilitare il routing tra VLAN sul router principale, in questo caso una RV320. Per configurarlo, andare a Gestione porte > Appartenenza VLAN per abilitare il routing tra VLAN. Controllare le VLAN 1 e 25 sulla sinistra della pagina e fare clic su Edit (Modifica). Nella colonna InterVLAN Routing, fare clic sulla casella a discesa per ciascuna rete e selezionare Enabled. Salvare le impostazioni.

Ora tutti gli utenti devono essere in grado di accedere al portale captive, ma possono anche accedere a qualsiasi risorsa sulla VLAN principale o sulla VLAN guest. Per limitare l'accesso, configurare una regola di controllo dell'accesso sulla RV320. Per configurare questa restrizione, scegliere Firewall > Regole di accesso.



Nella parte inferiore della pagina fare clic su Aggiungi. Si desidera aggiungere un totale di 2 regole di accesso per lo scenario. Configurare innanzitutto la regola che nega l'accesso dalla subnet guest 192.168.25.x/24 alla subnet interna 192.168.1.x/24, come mostrato a destra.



Fare clic su Salva nella parte inferiore della pagina, quindi su Indietro. Aggiungere ora un'altra regola, questa volta impostando l'azione come "Consenti" e l'IP di destinazione come "Singolo". Configurare la regola in modo da consentire l'accesso dalla subnet 192.168.25.x/24 a 192.168.1.5, attualmente configurata come IP statico WAP321. Questa regola verrà inserita prima della regola di negazione appena creata, consentendo il traffico a 192.168.1.5 dalla rete guest e da nessun'altra parte della rete principale.

Al termine, la pagina delle regole di accesso dovrebbe avere questo aspetto.

Per configurare Captive Portal in questa configurazione, è sufficiente seguire i passaggi della prima sezione per ogni rete necessaria per configurare il Captive Portal.

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco