Ermöglichung eines Captive Portals für Ihr Cisco Wireless Network

Aktivierung des Captive Portals in Ihrem Cisco Wireless Network

In einer zunehmend mobilen und kollaborativen Geschäftsumgebung öffnen immer mehr Unternehmen ihre Netzwerkumgebungen für die kontrollierte gemeinsame Nutzung von Ressourcen mit Geschäftspartnern, Kunden und anderen Gästen. Unternehmen suchen nach besseren Möglichkeiten, um:

·Sicherer Wireless-Internetzugang für Besucher
· eingeschränkten Zugriff auf Unternehmensnetzwerkressourcen für Geschäftspartner
· Schnelle Authentifizierung und Konnektivität für Mitarbeiter, die dort private Mobilgeräte verwenden

Ein Cisco Small Business Wireless Access Point (AP), wie der WAP321 oder der WAP561, kann problemlos in das bestehende kabelgebundene Netzwerk integriert werden, um eine Wireless-Verbindung mit einer Geschwindigkeit und Sicherheit bereitzustellen, die mit einer typischen kabelgebundenen Verbindung vergleichbar ist.

Die Cisco Captive Portal-Funktion bietet eine komfortable, sichere und kosteneffiziente Möglichkeit, Clients und anderen Besuchern Wireless-Zugriff anzubieten und gleichzeitig die Sicherheit Ihres internen Netzwerks zu gewährleisten. Ein Gastnetzwerk kann vielen wichtigen Geschäftszwecken dienen, z. B. zur Optimierung der Geschäftsabläufe mit Partnern, zur Steigerung der Kundenzufriedenheit und zur Steigerung der Mitarbeiterproduktivität.

Captive Portal bietet folgende grundlegende Funktionen:

·Benutzerdefinierte Anmeldeseite für Gäste mit Firmenlogos
· Erstellung mehrerer Instanzen des Captive Portals
· Mehrere Authentifizierungsoptionen
· Möglichkeit zur Zuweisung unterschiedlicher Rechte und Rollen
· Möglichkeit zur Zuweisung von Bandbreite (Upstream und Downstream)

Wie wird Captive Portal eingerichtet?

Captive Portal kann über die Geräte-GUI eingerichtet werden. Kunden, die eine schnelle und einfache Einrichtung vornehmen, können den Einrichtungsassistenten verwenden, um die Funktion zu aktivieren. Weitere Informationen finden Sie in den folgenden Schritten:

Verwenden des Installationsassistenten

Führen Sie den Setup-Assistenten über das Haupt-Dashboard der Geräte-GUI aus.

Folgen Sie den Bildschirmen des Assistenten.

Gastzugriff aktivieren (Captive Portal).

Geben Sie Ihrem Gastnetzwerk einen Namen, z. B. "Mein Unternehmen - Gast".

Wählen Sie einen Sicherheitstyp aus.

Wenn Sie eine bestimmte Webseite haben, die Sie anzeigen möchten, nachdem die

Benutzer die Nutzungsbedingungen von der Willkommensseite akzeptiert haben, geben Sie die URL ein, und als Nächstes kann diese URL Ihre Website sein.

Wählen Sie Weiter aus, um zur nächsten Seite zu wechseln.

Nachdem Ihr Captive Portal fertig eingerichtet ist, kann Ihr Kunde jetzt eine Verbindung zu Ihrem Gastnetzwerk herstellen und die Willkommensseite erhalten.

Um das Portal vorab einzurichten und anzupassen, melden Sie sich bitte im Captive Portal-Menü in der Geräte-GUI an.

Wählen Sie Instanzkonfiguration aus. Sie werden feststellen, dass der Assistent einen Instanznamen mit dem Namen "wiz-cp-inst1" erstellt hat. Sie können diesen Namen auswählen oder einen neuen Namen für die Instanzkonfiguration erstellen und dann speichern. Wenn Sie "wiz-cp-inst1" auswählen, gelangen Sie auf dem Bildschirm zur Seite "Instance Configuration" (Instanzkonfiguration).

Sie werden feststellen, dass der Einrichtungsassistent der Gast-SSID, die Sie während des Einrichtungsassistenten erstellt haben, automatisch den Namen der Captive Portal-Instanz "wiz-cp-inst1" zuordnet.

Wenn Sie die Instanz über die GUI erstellt haben, müssen Sie nun eine Verbindung zum von Ihnen erstellten Gastnetzwerk herstellen.
Wählen Sie aus dem Dropdown-Menü den Instanznamen "Gast" oder die vom Assistenten "wiz-cp-inst1 erstellte Instanz aus.

Wählen Sie im Menü die Option Web Portal Configuration (Webportportportkonfiguration) aus, um Ihre Gastbegrüßungsseite zu konfigurieren, und wählen Sie den Instanznamen aus dem Dropdown-Menü aus.

Wählen Sie die Authentifizierungsmethode für Captive Portal aus, um Clients zu überprüfen:

·Guest (Gast): Der Benutzer muss nicht durch eine Datenbank authentifiziert werden.
· Local (Lokal): Das WAP-Gerät verwendet eine lokale Datenbank für authentifizierte Benutzer.
· RADIUS - Das WAP-Gerät verwendet eine Datenbank auf einem Remote-RADIUS-Server, um Benutzer zu authentifizieren.

Wenn Sie die Überprüfungsmethode "Locale" (Gebietsschema) auswählen, müssen Sie lokale Benutzer erstellen.

Wählen Sie aus dem Menü Lokal.

Geben Sie den Parameter use (Name des Benutzers) ein, und wählen Sie die Parameter für das Benutzerprofil aus.

Web Portal Page Customization, jetzt können Sie Ihr Firmenlogo und Ihre Grafiken hochladen. Sie können bis zu 3 grafische Dateien hochladen, eine für den Seitenhintergrund (Standard cisco-bkg) die zweite für das Firmenlogo (Standard, cisco-log) und eine dritte für

den Anmeldefenster (Standard, Logschlüssel).

** Bitte beachten Sie, dass die Dateigröße für diese Grafikdatei 5 KB betragen muss.

Jetzt können Sie Ihre Webseite anpassen, z. B. Acceptance Use Policy, Fenstertitel und -name usw.

Benutzerdefinierte Seite mit Überprüfungsmethode als "Gast", d. h., die Authentifizierung ist nicht erforderlich. Der Benutzer muss nur die Nutzungsbedingungen akzeptieren und die Schaltfläche "Verbinden" auswählen. Die Eingabe des Benutzernamens ist optional.

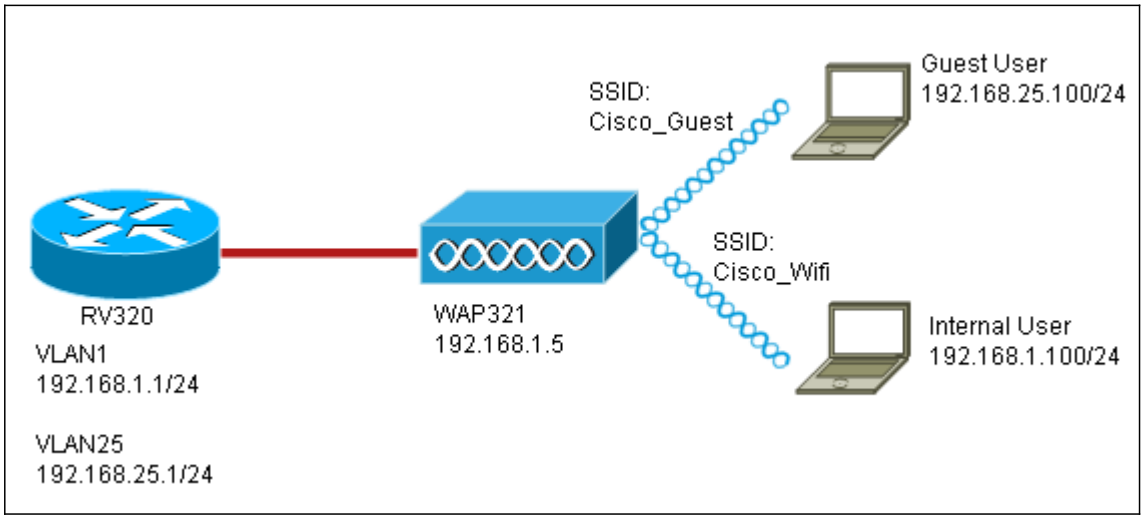
Benutzerdefinierte Seite mit Überprüfungsmethode "Lokal" bedeutet, dass der Benutzer zur Authentifizierung Benutzernamen und Kennwort eingeben muss. Anschließend muss der Benutzer die Nutzungsbedingungen akzeptieren und die Schaltfläche "Verbinden" auswählen.

Captive Portal in einer Multi-VLAN-Umgebung

In einigen Fällen sind für ein Netzwerk mehrere VLANs für verschiedene Zwecke erforderlich, die verschiedene Benutzergruppen bedienen. Ein häufiges Beispiel ist ein separates Netzwerk für Gastbenutzer, um nicht autorisierte Benutzer am Zugriff auf Ressourcen im Unternehmensnetzwerk zu hindern. Manchmal gibt es mehrere Wireless-Netzwerke, die verschiedenen Benutzern aus demselben Grund zur Verfügung stehen müssen. WAP321 und WAP561 können diese Anforderungen über das Captive Portal erfüllen, erfordern jedoch eine zusätzliche Konfiguration im Netzwerk. In diesem Abschnitt wird die Konfiguration erläutert.

Einführung - Vorhandene Konfiguration

In diesem Dokument wird davon ausgegangen, dass bereits eine Netzwerkkonfiguration vorhanden ist. In diesem Beispiel gibt es zwei Netzwerke: das Hauptnetzwerk und das Gastnetzwerk. Die Konfiguration zum Erstellen und Bereitstellen von DHCP-Adressen für jedes Netzwerk wurde bereits konfiguriert. Der WAP321 wurde bereits so konfiguriert, dass er für jedes Netzwerk eine andere SSID sendet. Die aktuelle Konfiguration sieht folgendermaßen aus:

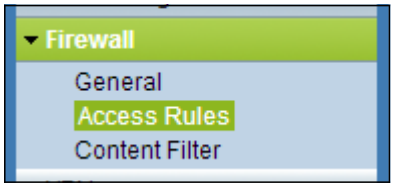


Nach Abschluss der Konfiguration wird Inter-VLAN-Routing im Netzwerk aktiviert, sodass alle Wireless-Clients auf das Captive Portal zugreifen können, um die Netzwerkverbindung zu ermöglichen.

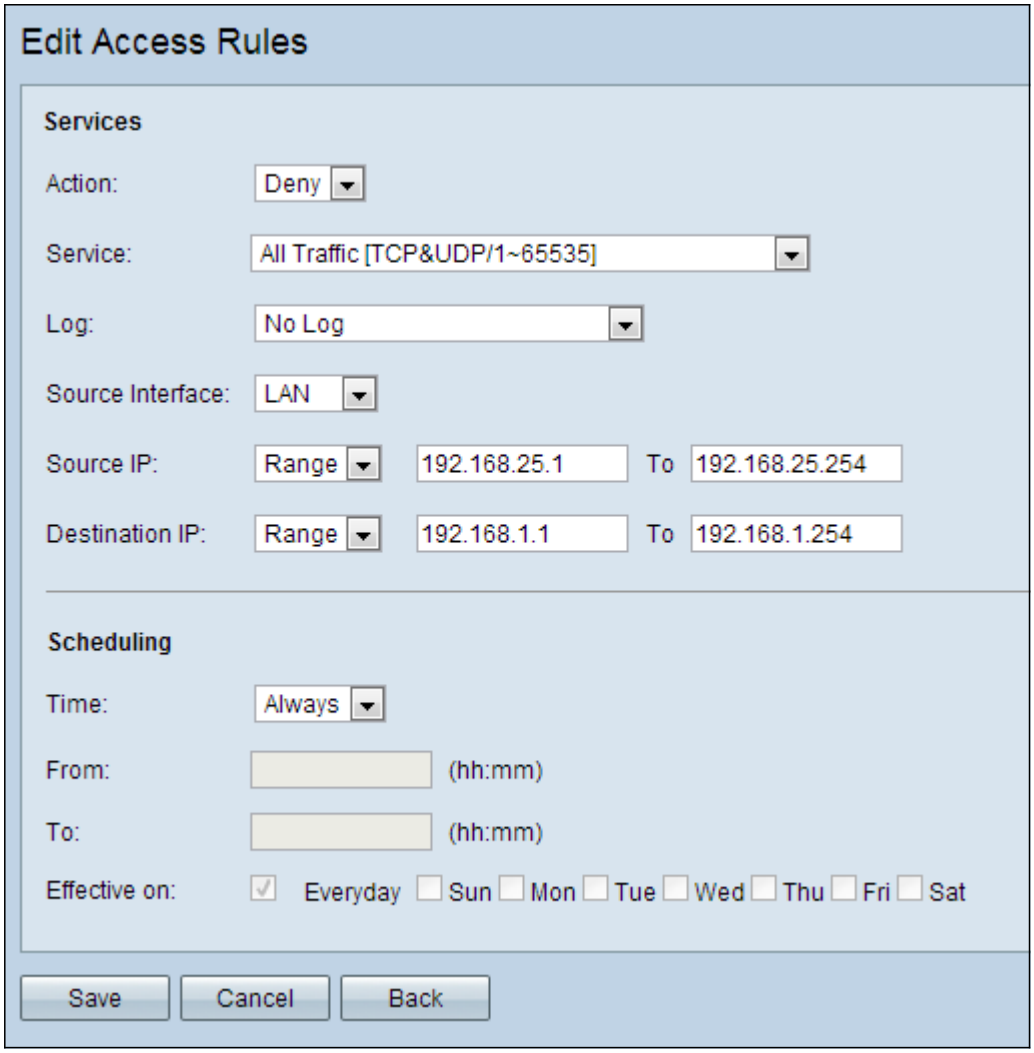
Konfiguration

Aktivieren Sie zunächst Inter-VLAN-Routing auf dem Core-Router, in diesem Fall RV320. Um dies zu konfigurieren, gehen Sie zu Port Management > VLAN Membership, um Inter-VLAN-Routing zu aktivieren. Aktivieren Sie links auf der Seite die Optionen VLAN 1 und 25, und klicken Sie auf Edit. Klicken Sie in der Spalte InterVLAN Routing (VLAN-übergreifendes Routing) auf das Dropdown-Feld, und wählen Sie Enabled (Aktiviert) aus. Speichern Sie die Einstellungen.

Jetzt sollten alle Benutzer auf das Captive Portal zugreifen können, aber sie können auch auf alle Ressourcen entweder im Haupt-VLAN oder im Gast-VLAN zugreifen. Konfigurieren Sie zur Zugriffsbeschränkung eine Zugriffskontrollregel für den RV320. Gehen Sie zu Firewall > Zugriffsregeln, um diese Einschränkung zu konfigurieren.



Klicken Sie unten auf der Seite auf Hinzufügen. Wir möchten insgesamt 2 Zugriffsregeln für unser Szenario hinzufügen. Konfigurieren Sie zunächst die Regel, die den Zugriff vom 192.168.25.x/24-Gast-Subnetz auf das interne Subnetz 192.168.1.x/24 verweigert, wie rechts dargestellt.



Klicken Sie unten auf der Seite auf Speichern, und klicken Sie anschließend auf Zurück. Fügen Sie nun eine andere Regel hinzu, legen Sie diesmal die Aktion auf "Zulassen" und die Ziel-IP auf "Single" fest. Konfigurieren Sie die Regel so, dass der Zugriff vom Subnetz 192.168.25.x/24 auf das Subnetz 192.168.1.5 zugelassen wird, das derzeit als statische WAP321 konfiguriert ist. Diese Regel wird vor der soeben erstellten Deny-Regel platziert, mit der der Datenverkehr aus dem Gastnetzwerk auf 192.168.1.5 und aus dem Hauptnetzwerk weitergeleitet wird.

Wenn Sie fertig sind, sollte die Seite mit den Zugriffsregeln wie folgt aussehen.

Um das Captive Portal in dieser Konfiguration zu konfigurieren, folgen Sie einfach den Schritten aus dem ersten Abschnitt für jedes Netzwerk, das Sie für das Captive Portal konfigurieren müssen.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.