Een Capture Portal op uw Cisco Wireless Network inschakelen

Capture Portal voor uw Cisco Wireless Network

In een steeds mobieler, coöperatief zakenmilieu, maken meer organisaties hun netwerkomgevingen open voor gecontroleerd delen van middelen met partners, klanten en andere gasten. Bedrijven zoeken betere manieren om:

- Beveiligde draadloze internettoegang bieden aan bezoekende klanten
- Beperkte toegang tot bedrijfsnetwerkbronnen voor zakenpartners mogelijk maken
- Snelle verificatie en connectiviteit voor werknemers die daar persoonlijke mobiele apparaten gebruiken

Een Cisco Small Business Wireless Access Point (AP), zoals WAP321 of WAP561, kan eenvoudig in het bestaande bekabelde netwerk worden geïntegreerd om een draadloze connectiviteit met snelheid en beveiliging te bieden die een typische bekabelde verbinding regelt.

De optie Cisco Captive Portal biedt een handige, veilige, kosteneffectieve manier om draadloze toegang voor klanten en andere bezoekers te bieden terwijl de beveiliging van uw interne netwerk behouden blijft. Een gastnetwerk kan vele belangrijke bedrijfsdoeleinden dienen, waaronder het stroomlijnen van zaken met partners en het bieden van grotere klanttevredenheid en het verbeteren van werknemersproductiviteit.

Captive Portal kan de volgende basisfunctionaliteit bieden:

- Aangepaste gastenlogpagina met bedrijfslogo's
- Mogelijkheid om meerdere exemplaren van het portaal in gevangenschap te maken
- Meervoudige authenticatieopties
- Mogelijkheid om verschillende rechten en rollen toe te wijzen
- Mogelijk om bandbreedte toe te wijzen (stroomopwaarts en stroomafwaarts)

Captive Portal instellen

U kunt een portal voor interne instellingen opzetten via de GUI, want klanten kunnen de setup-wizard gebruiken om deze functie te activeren. Raadpleeg onderstaande stappen:

De wizard Instellen gebruiken

Start de setup-wizard vanuit het hoofddashboard van het apparaat GUI.

Volg de wizard.

Toegang tot wasprogramma inschakelen (Captive Portal).

Geef je gastnetwerk een naam, bijvoorbeeld "Mijn bedrijf-Gast".

Selecteer een beveiligingstype.

Als u een specifieke webpagina hebt die u wilt laten zien nadat gebruikers de

servicetermijnen van de welkomstpagina, het type in de URL en vervolgens, kan deze URL uw bedrijfswebsite zijn.

Selecteer Volgende om naar de volgende pagina te gaan.

Nu is uw setup-exemplaar van het Captive Portal voltooid. Uw klant kan zich nu aan uw gastnetwerk verbinden en de welkomstpagina verkrijgen.

Voor het vooraf instellen en aanpassen van het portal kunt u inloggen op de apparaatondersteuning en in het menu Captive Portal.

Selecteer Instance Configuration, u merkt dat de wizard een voorbeeldnaam heeft gemaakt die "wiz-cp-Against1" wordt genoemd. U kunt deze naam kiezen of een nieuwe naam maken voor uw Instantie-configuratie en vervolgens opslaan. Als u "wiz-cp-Against1" kiest, gaat het scherm u naar de Zie Instantie-pagina.

U merkt dat de wizard automatisch de naam **wiz-cp-Against1** aan de Guest SSID heeft gekoppeld aan de wizard die u tijdens de setup-wizard hebt gemaakt.

Als u de instantie hebt gemaakt met behulp van de GUI, moet u nu koppelen aan het netwerk dat u hebt gemaakt.
Selecteer in het uitrolmenu de Instance Name "Guest", of de instantie die is aangemaakt door de wizard "**wiz-cp-Against1**".

Selecteer in het menu de optie Web Portal Configuration om de gastwelkomstpagina te configureren, de naam van de instantie in het uitrolmenu.

Selecteer de authenticatiemethode die Captive Portal kan gebruiken om klanten te controleren:

- Guest — De gebruiker hoeft niet te zijn geauthentificeerd door een database.
- Lokaal — Het WAP-apparaat gebruikt een lokale database voor geauthenticeerde gebruikers.
- RADIUS - Het WAP-apparaat gebruikt een database op een externe RADIUS-server om gebruikers te authentiseren.

Als u verificatiemethode "Lokaal" kiest, moet u lokale gebruikers maken.

Kies in het menu Lokaal.

Voer de use parameter in (naam van de gebruiker) en kies de parameters voor het gebruikersprofiel.

Web portal Pagina met aanpassingen, nu hebt u de keuze om het bedrijfslogo en de afbeeldingen te uploaden die u kunt uploaden naar maximaal 3 grafische bestanden, één voor de pagina-achtergrond (standaard cisco-bkg) tweede voor het bedrijfslogo (standaard, cisco-log) en derde voor het inlogscherm (standaard, logtoets).

** Merk op dat de bestandsgrootte voor dit werkbestand 5 kB moet zijn.

U kunt nu uw webportal-pagina aanpassen, zoals Aanvaardbaarheidsbeleid, venstertitel en naam toevoegen, enzovoort..

Aangepaste pagina met verificatiemethode als Gast, dit betekent niet dat u de verificatie hoeft uit te voeren. De gebruiker hoeft alleen de servicebepalingen te aanvaarden en de knop Connect te selecteren. Het invoeren van de gebruikersnaam is optioneel.

Aangepaste pagina met verificatiemethode. Dit betekent dat de gebruiker een gebruikersnaam en wachtwoord moet invoeren om zich te authentiseren. De gebruiker moet de servicebepalingen accepteren en de knop Connect selecteren.

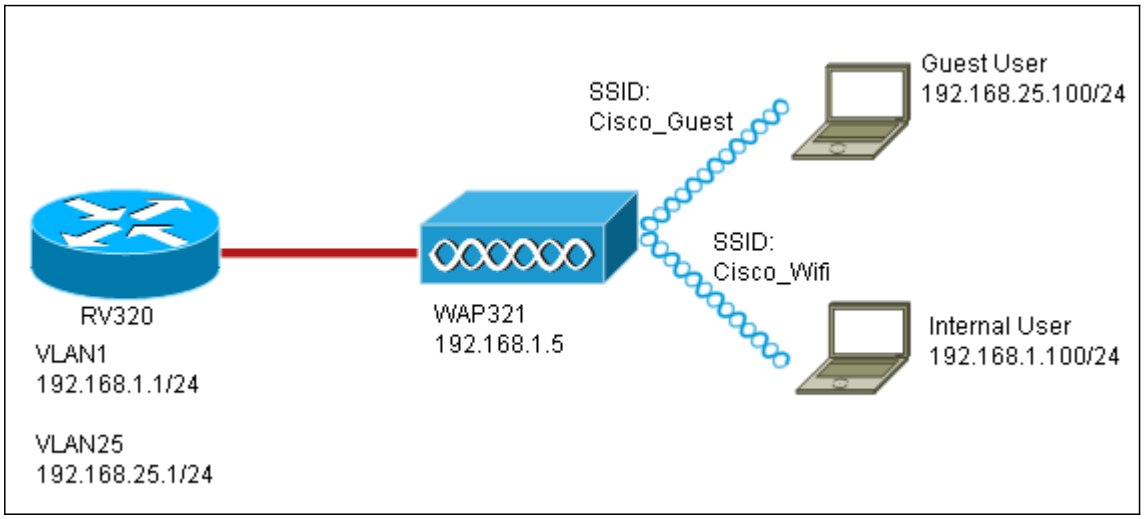
Captive Portal in een milieu van meerdere VLAN

In sommige gevallen heeft een netwerk van meerdere VLAN's voor verschillende doeleinden

nodig, die de verschillende groepen gebruikers van dienst zijn. Een veelvoorkomend voorbeeld is een afzonderlijk netwerk voor gebruikers in de Gast om te voorkomen dat onbevoegde gebruikers toegang hebben tot middelen op het bedrijfsnetwerk. Soms zijn er meerdere draadloze netwerken die om dezelfde reden beschikbaar moeten zijn voor verschillende gebruikers. WAP321 en WAP561 kunnen aan deze behoeften voldoen met behulp van het Captive Portal, maar hebben wel een beetje extra configuratie op het netwerk nodig. Deze sectie gaat over die configuratie.

Inro - bestaande configuratie

Dit document gaat ervan uit dat er al een netwerkconfiguratie is ingesteld. In dit voorbeeld, zijn er twee netwerken, het hoofdnetwerk en het gastnetwerk. De configuratie om DHCP-adressen van elk netwerk te maken en te gebruiken is al geconfigureerd. WAP321 is al geconfigureerd om een andere SSID voor elk netwerk uit te zenden. De huidige instellingen zien er zo uit:

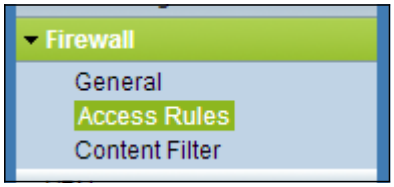


Wanneer de configuratie is voltooid, wordt de routing InterVLAN op het netwerk ingeschakeld zodat alle draadloze klanten toegang hebben tot het Captive Portal, waardoor netwerkconnectiviteit mogelijk wordt.

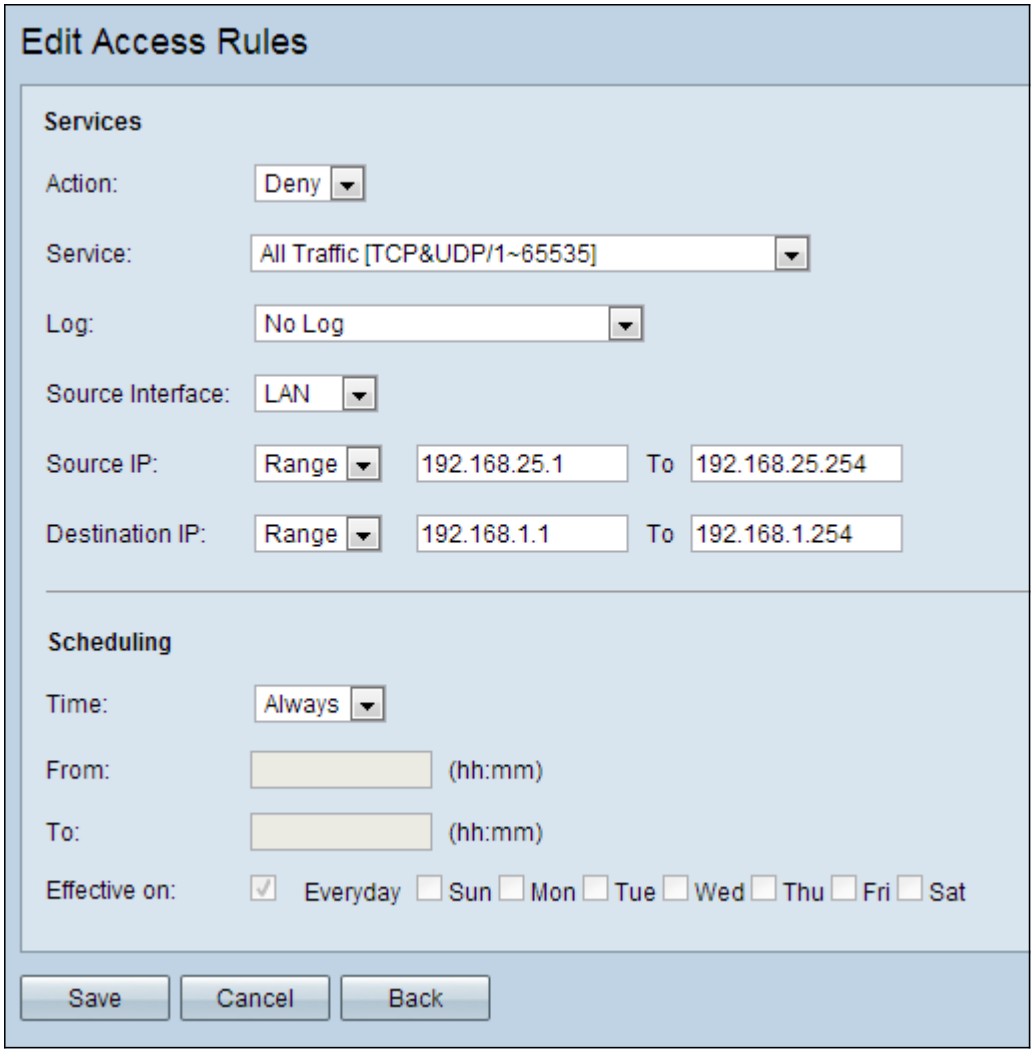
Configuratie

Stel eerst de routing tussen VLAN op de kernrouter in, in dit geval een RV320. Om dit te configureren gaat u naar Port Management > VLAN-lidmaatschap om routing tussen VLAN's mogelijk te maken. Controleer zowel VLAN 1 als VLAN 25 links op de pagina en klik op Bewerken. In de kolom InterVLAN-routing klikt u op in het uitrolvak voor elk en selecteert u Ingeschakeld. De instellingen opslaan.

Nu zouden alle gebruikers tot het gevangen portaal moeten kunnen toegang hebben, maar zij kunnen ook tot om het even welke middelen op of het belangrijkste VLAN of het Gast VLAN toegang hebben. Om de toegang te beperken, moet u een toegangscontroleregel op RV320 configureren. Ga naar Firewall > Toegangsregels om deze beperking te configureren.



Klik onder op de pagina Toevoegen. Wij willen voor ons scenario in totaal twee toegangsregels toevoegen. Ga eerst de regel aan die toegang van 192.168.25.x/24 gastvorm tot 192.168.1.x/24 interne Subnet ontzegt, zoals weergegeven aan de rechterkant.



Klik onder op de pagina Opslaan en klik vervolgens op Terug. Voeg nu een andere regel toe, deze tijd stelt de actie in als "Toestaan" en de bestemming IP als "Enkel." Configureer de regel om toegang toe te staan van 192.168.25.x/24 subster tot 192.168.1.5, wat momenteel is ingesteld om WAP321 statische IP te zijn. Deze regel zal worden geplaatst vóór de ontkenningsregel die we net hebben gemaakt, en die het verkeer vanaf het gastnetwerk naar 192.168.1.5 toestaat en nergens anders op het hoofdnetwerk.

Als u klaar bent, ziet de pagina met toegangsregels er zo uit.

Om in deze instelling een poort te configureren volgt u simpelweg de stappen uit de eerste sectie voor elk netwerk dat u nodig hebt om het portal te configureren.

Bekijk een video gerelateerd aan dit artikel...

Klik hier om andere Tech Talks uit Cisco te bekijken