Verhoog de Time-out voor webverificatie op de draadloze LAN-controller

Inhoud

Inleiding

Dit document bevat de stappen die vereist zijn voor de Web-auth Service Set Identifier (SSID) om een VPN-gebruiker toegang te geven zonder volledige verificatie en zonder een verbroken verbinding elke paar minuten. Om dit te bereiken, moet een gebruiker de Web-Verificatie (Web-auth) tijd op de Draadloze LAN controller (WLC) verhogen.

Voorwaarden

Vereisten

Cisco raadt aan dat u weet hoe u de WLC voor basisbediening en Web-auth moet configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco 5500 Series WLC-applicatie met firmware versie 8.0.10.0

> **Opmerking** De configuratie en de webauth verklaring in dit document zijn van toepassing op alle WLC-modellen en alle Cisco Unified Wireless Network-beeldversie 8.0.10.0 en hoger.

Achtergrondinformatie

In veel instellingen voor klantnetwerk zijn er instellingen die een groep zakelijke gebruikers of gasten VPN toegang tot bepaalde IP adressen toestaan zonder de vereiste om Web-auth-beveiliging door te geven. Deze gebruikers ontvangen een IP-adres en verbinden direct met VPN zonder de behoefte aan enige geloofsbrieven om via Web-auth veiligheid echt te worden gemaakt. Deze SSID kan in gebruik zijn door een andere reeks gebruikers die ook normale en volledige Web-auth doorlopen om toegang tot internet te krijgen. Dit scenario is mogelijk via een pre-authenticatie ACL op SSID dat gebruikersverbindingen naar VPN IP adressen toestaat alvorens zij

Verificatie doorgeven. Het probleem voor deze VPN-gebruikers is dat ze het IP-adres kiezen maar nooit de volledige Web-auth voltooien. Daarom wordt de Web-auth timeout timer geactiveerd en de client is gedeauthenticeerd:

```
*apfReceiveTask: Sep 03 12:01:55.694: 00:24:d7:cd:ac:30 172.30.0.118 WEBAUTH_REQD (8)
Web-Auth Policy timeout

*apfReceiveTask: Sep 03 12:01:55.694: 00:24:d7:cd:ac:30 172.30.0.118 WEBAUTH_REQD (8)
Pem timed out, Try to delete client in 10 secs.
```

De waarde van deze tijdelijke versie is 5 minuten en heeft een vaste waarde in WLC versies eerder dan 7.6. Deze korte tijd veroorzaakt dat het draadloze netwerk voor dit soort gebruikers bijna onbruikbaar wordt. De mogelijkheid om deze waarde te wijzigen wordt toegevoegd aan WLC versie 8.0 die gebruikers toegang tot VPN biedt via pre-auth ACL-toegestaan verkeer.

Configureren

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Voltooi deze stappen om de Web-auth timeout in de WLC te vergroten:

1. Maak een ACL die verkeer naar het VPN IP-adres toestaat.

2. Pas ACL als **Presence ACL (ACL) toe** op de configuratie van het draadloze LAN (WLAN) onder Layer 3 security.

3. Meld u aan via de CLI en voer het opdracht Web-auth timeout van het **beveiligings web-auth**

timeout in om de Web-auth timeout waarde te verhogen:

```
(WLC)>config wlan security web-auth timeout ?
<value> Configures Web authentication Timeout (300-14400 seconds).

(WLC)>config wlan security web-auth timeout 3600
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Web-auth sessie timeout waarde voor uw WLAN verschijnt als deze voorbeelduitvoer toont:

```
(WLC)>show wlan 10
Web Based Authentication..... Enabled
Web Authentication Timeout..... 3600
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Voer de opdracht **debug client <mac-adres>in** om de Web-auth timer te zien starten voor de gebruiker die verbinding maakt met VPN zonder verificatie.