ISE-configuratievoorbeeld met statische omleiding voor geïsoleerde gastennetwerken

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco Identity Services Engine (ISE) kunt configureren met statische omleiding voor geïsoleerde gastennetwerken om de redundantie te behouden. Het beschrijft ook hoe te om de beleidsknooppunt te vormen zodat de cliënten niet met een onverifieerbare certificaatwaarschuwing worden veroorzaakt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE Central Web Verification (CWA) en alle bijbehorende componenten
- Browser verificatie van de geldigheid van het certificaat
- Cisco ISE-software Versie 1.2.0.899 of hoger
- Cisco draadloze LAN-controller (WLC) versie 7.2.10.0 of hoger (versie 7.4.10.0 of hoger heeft de voorkeur)

Opmerking: CWA wordt beschreven in het artikel [Central Web Authentication on the WLC and ISE Configuration Voorbeeld](#) Cisco.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE-software Versie 1.2.0.899
- Cisco Virtual WLC (vWLC) versie 7.4.110.0
- Cisco adaptieve security applicatie (ASA)) versie 8.2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

In veel Bring Your Own Device (BYOD) omgevingen is het gastennetwerk volledig geïsoleerd van het interne netwerk in een de-Militarised Zone (DMZ). Vaak biedt de DHCP in de gast-DMZ openbare DNS-servers (Domain Name System) aan de gastgebruikers omdat de enige dienst die wordt aangeboden is internettoegang.

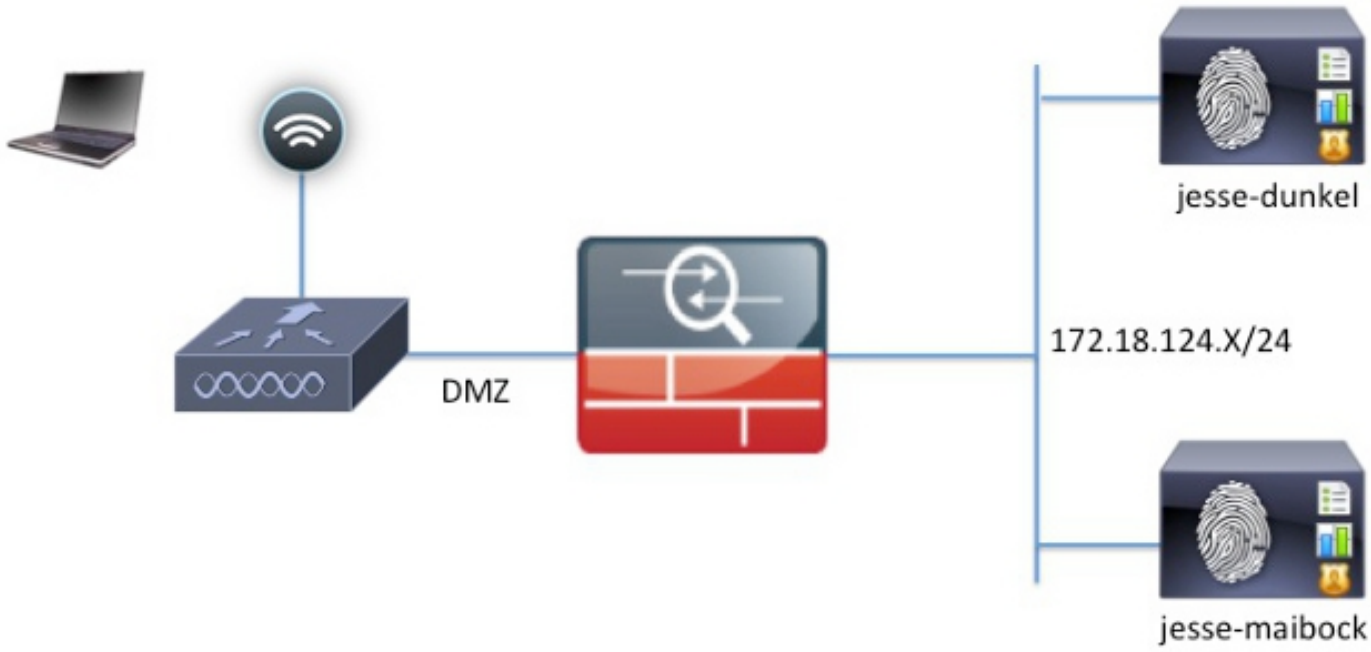
Dit maakt gastomleiding op de ISE moeilijk voorafgaand aan versie 1.2 omdat de ISE clients omleidt naar de Fully Qualified Domain Name (FQDN) voor webverificatie. Met ISE-versies 1.2 en hoger kunnen beheerders gastgebruikers echter doorsturen naar een statisch IP-adres of hostnaam.

Configureren

Netwerkdiagram

Dit is een logisch diagram.

> Opmerking: fysiek is er een draadloze controller in het interne netwerk, de access points (AP's) bevinden zich op het interne netwerk en de Service Set Identification (SSID) is verankerd aan de DMZ-controller. Raadpleeg de documentatie bij Cisco WLC's voor meer informatie.



Configuratie

De configuratie op de WLC blijft onveranderd ten opzichte van een normale CWA configuratie. De SSID is zo geconfigureerd dat MAC-filtering met RADIUS-verificatie mogelijk is en de RADIUS-accounting naar twee of meer ISE-beleidsknooppunten.

Dit document richt zich op de ISE-configuratie.

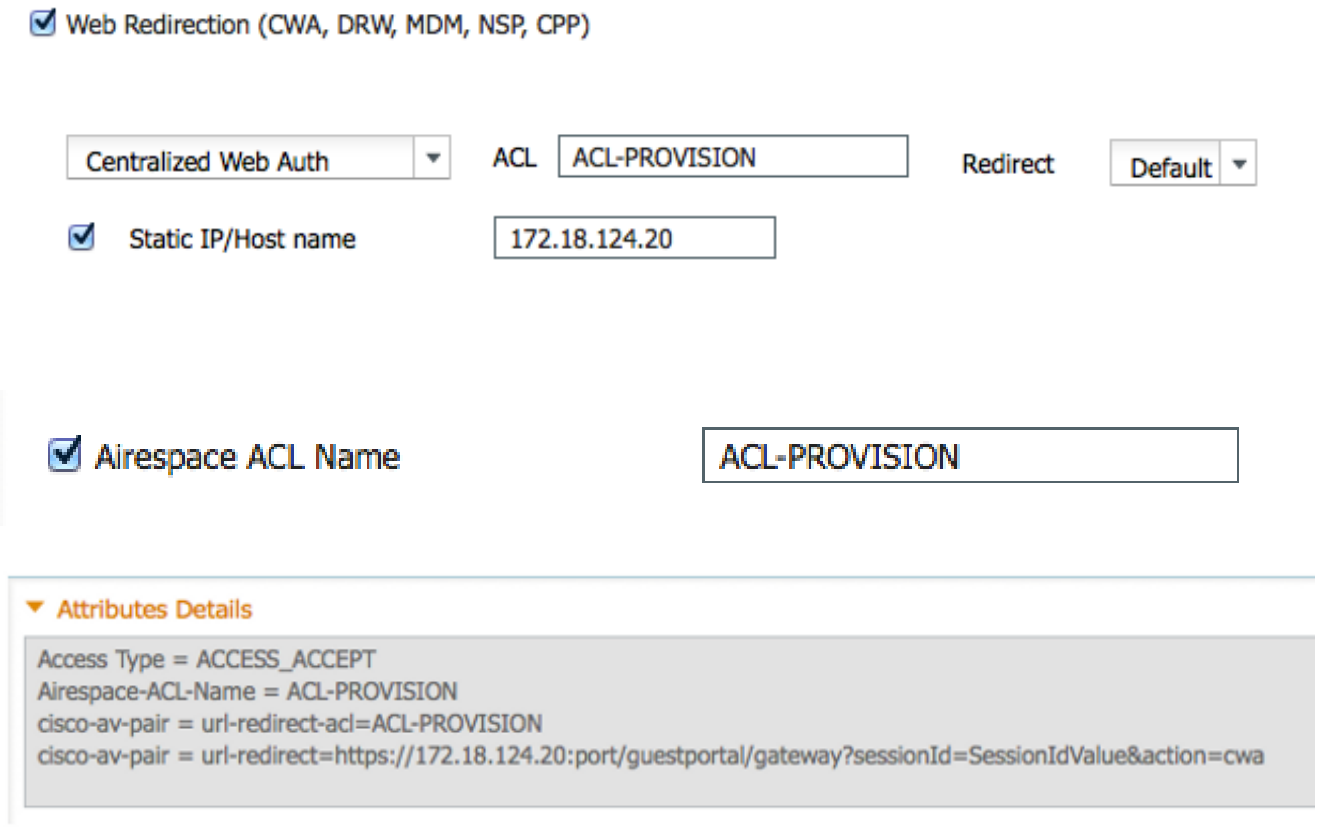
> Opmerking: in dit voorbeeld zijn de beleidsknooppunten jesse-dunkel (172.18.124.20) en jesse-maibock (172.18.124.21).

De CWA-stroom begint wanneer de WLC een RADIUS MAC-verificatie-omzeiling (MAB) verstuurt naar de ISE. De ISE reageert met een doorverwijzing URL naar de controller om HTTP-verkeer naar de ISE te leiden. Het is belangrijk dat het RADIUS- en HTTP-verkeer naar hetzelfde Policy Services Node (PSN) gaat omdat de sessie op één PSN wordt onderhouden. Dit wordt normaal uitgevoerd met één regel, en de PSN voegt zijn eigen hostname in de CWA URL in. Met een statische omleiding moet u echter voor elke PSN een regel maken om er zeker van te zijn dat de RADIUS en HTTP verkeer naar hetzelfde PSN worden verzonden.

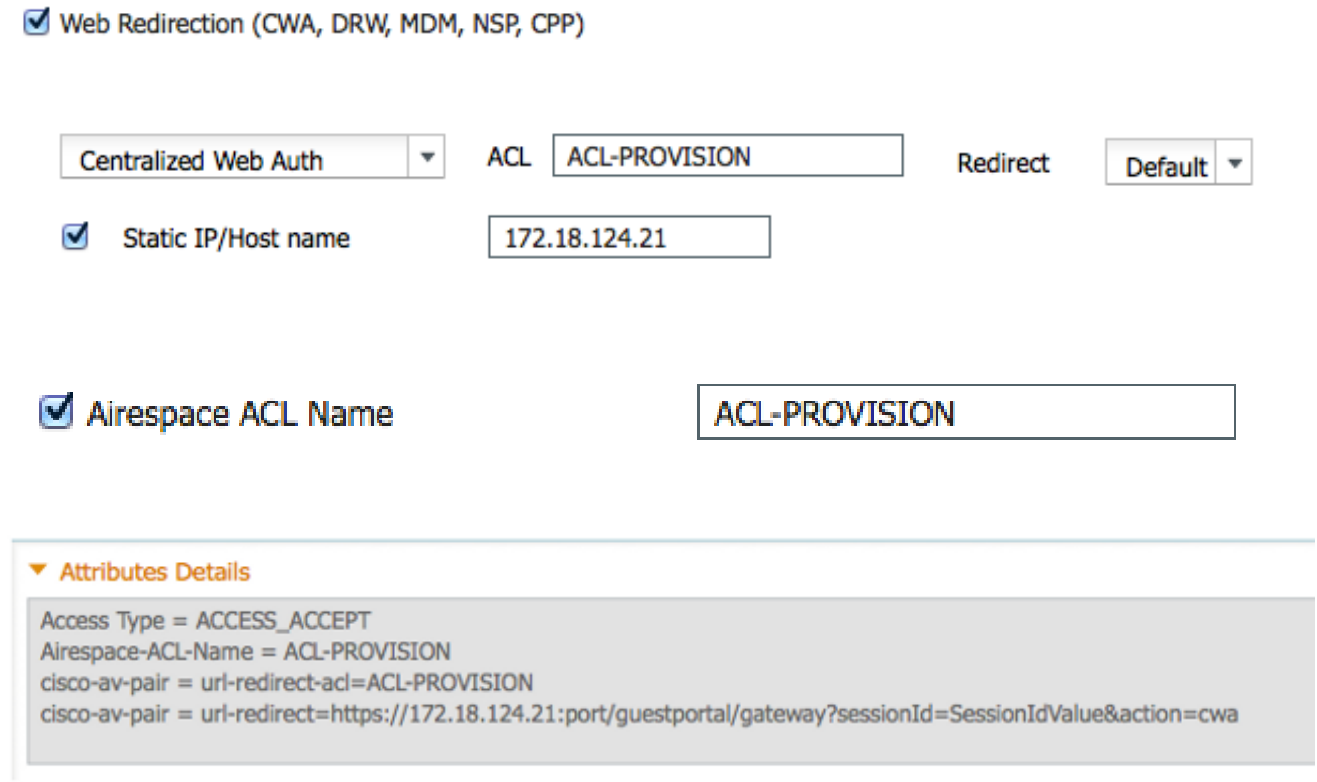
Voltooi de volgende stappen om de ISE te configureren:

1. Stel twee regels in om de client naar het PSN IP-adres te leiden. Navigeer naar Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen.

   Deze afbeeldingen tonen de informatie voor profielnaam DunkelGuestWireless:



Deze afbeeldingen tonen de informatie voor de profielnaam MaibockGuestWireless:



Opmerking: de ACL-bepaling is een lokale toegangscontrolelijst (ACL) die op de WLC is geconfigureerd om de client in staat te stellen bij verificatie te communiceren met

---

ISE. Raadpleeg het artikel in WLC en ISE Configuration Voorbeeld van Cisco voor meer informatie over de Central Web Verification.

2. Configureer het autorisatiebeleid zodat dit overeenkomt met het kenmerk Netwerktoegang:ISE-hostnaam en geef het juiste autorisatieprofiel op:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then MaibockGuestWireless
✓	Default	if no matches, then DenyAccess	

Nu de client wordt omgeleid naar een IP-adres, ontvangen gebruikers certificaatwaarschuwingen omdat de URL niet overeenkomt met de informatie in het certificaat. De FQDN in het certificaat is bijvoorbeeld jesse-dunkel.rtpaaa.local, maar de URL is 172.18.124.20. Hier is een voorbeeldcertificaat dat de browser toestaat om het certificaat met het IP-adres te valideren:

Issuer

* Friendly Name	jesse-dunkel.rtpaaa.local,jesse-dunkel.rtpaaa.local,172.18.124.20,172.18.124.20#RTPAAA-
Description	
Subject	CN=jesse-dunkel.rtpaaa.local
Subject Alternative Name (SAN)	DNS Name: jesse-dunkel.rtpaaa.local DNS Name: 172.18.124.20 IP Address: 172.18.124.20
Issuer	DC=local,DC=rtpaaa,CN=RTPAAA-Sub-CA1
Valid From	Thu, 19 Dec 2013 14:00:39 EST
Valid To (Expiration)	Sun, 20 Jul 2014 13:54:58 EDT
Serial Number	37 80 74 E7 00 00 00 00 00 14
Signature Algorithm	SHA1WithRSAEncryption
Key Length	2048

Protocol

- ☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling
- ☑ HTTPS: Use certificate to authenticate the ISE Web Portals

Met behulp van Subjecteer Alternative Name (SAN) vermeldingen, kan de browser de URL met het IP-adres 172.18.124.20 valideren. Er moeten drie SAN-vermeldingen worden gemaakt om de verschillende onverenigbaarheden van de client aan te pakken.

3. Maak een SAN-vermelding voor de DNS-naam en zorg ervoor dat deze overeenkomt met de CN=-vermelding in het veld Onderwerp.

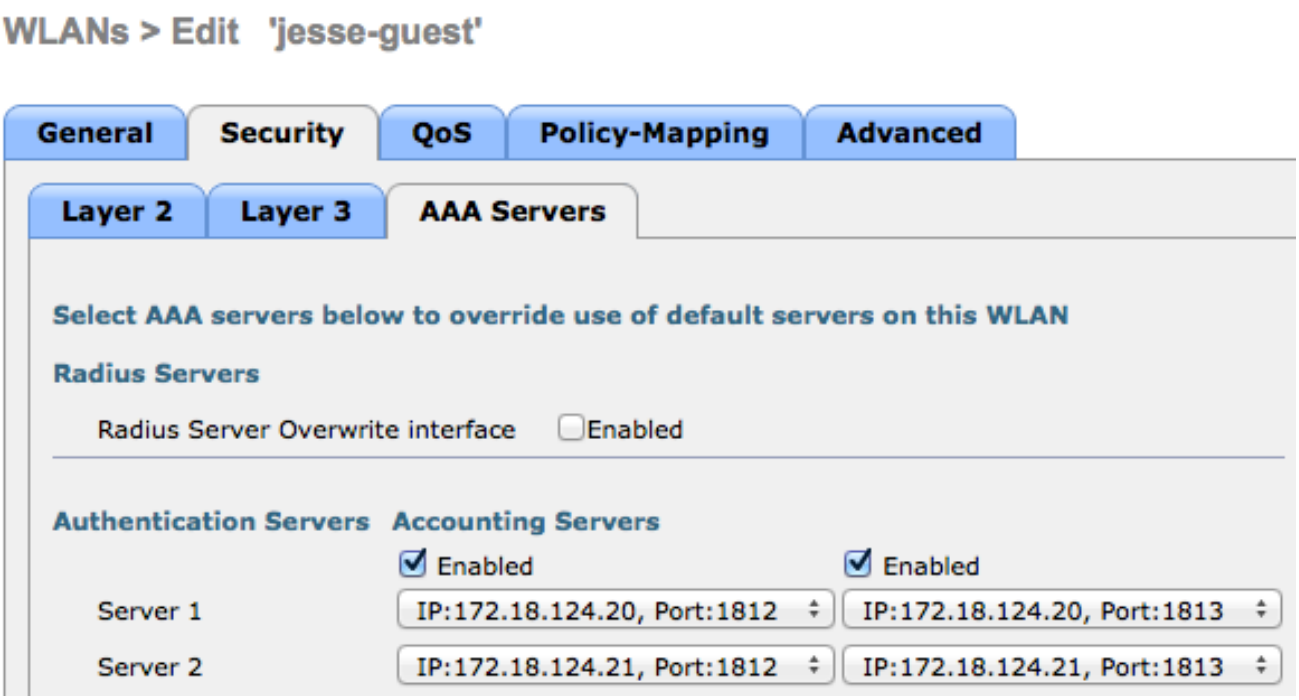
4. Maak twee vermeldingen om clients in staat te stellen het IP-adres te valideren; dit geldt voor zowel de DNS-naam van het IP-adres als het IP-adres dat in het IP-adreskenmerk wordt weergegeven. Sommige clients verwijzen alleen naar de DNS-naam. Anderen accepteren geen IP-adres in het attribuut DNS Name, maar verwijzen in plaats daarvan naar het attribuut IP Address.

N.B.: Raadpleeg de Hardware Installatiehandleiding voor Cisco Identity Services Engine, release 1.2, voor meer informatie over het genereren van certificaten.

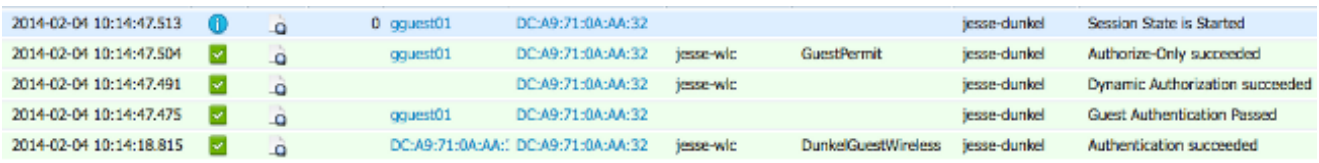
Verifiëren

Voltooi deze stappen om te bevestigen dat uw configuratie correct werkt:

1. Om te verifiëren dat beide regels functioneel zijn, stelt u handmatig de volgorde in van de ISE-PSN's die op het WLAN zijn geconfigureerd:



2. Log in op de gast-SSID, navigeer naar Bediening > Verificaties in de ISE en controleer of de juiste autorisatieregels zijn getroffen:

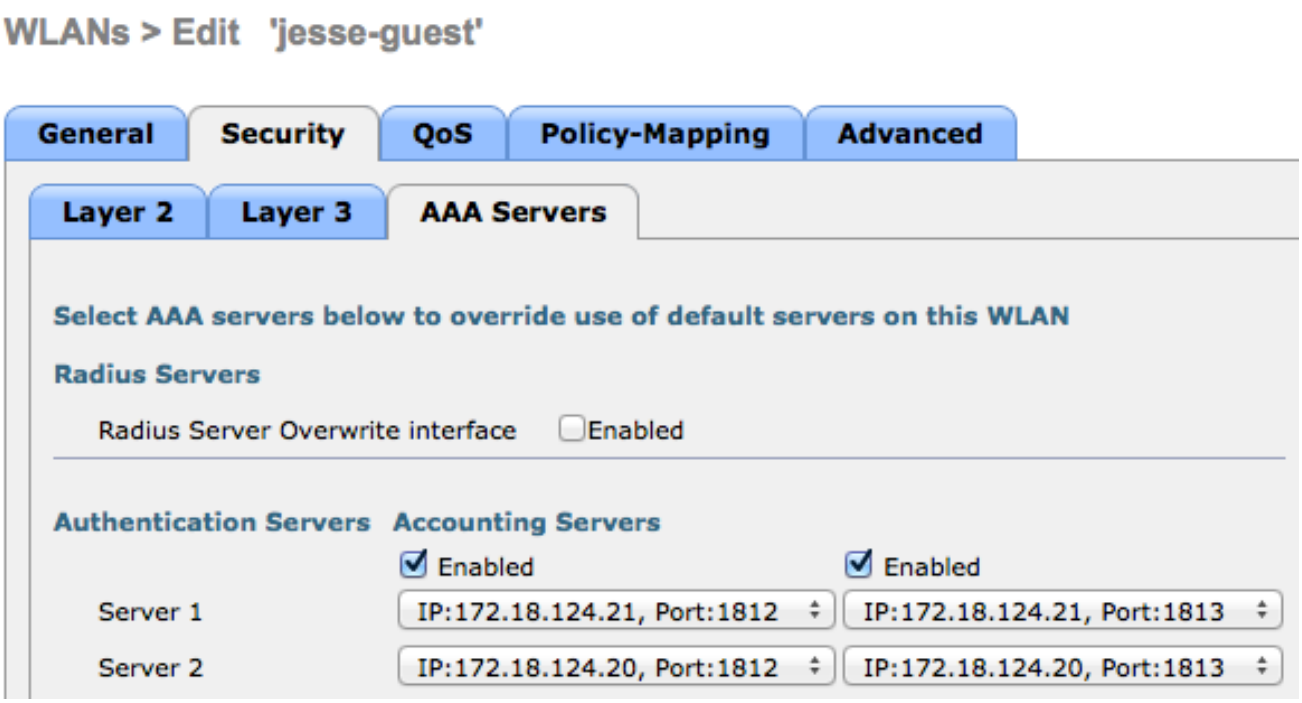


De eerste MAB-authenticatie wordt gegeven aan het DunkelGuestWireless autorisatieprofiel. Dit is de regel die specifiek omleidt naar jesse-dunkel, dat is het eerste ISE-knooppunt.

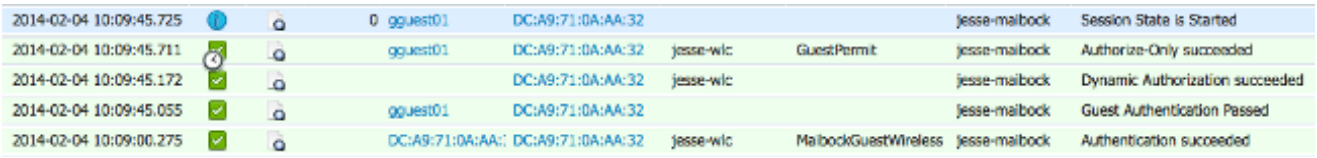
Nadat de gebruiker guest01 inlogt, wordt de juiste definitieve toestemming van GuestPermit gegeven.

3. Om de verificatiesessies van de WLC te wissen, koppelt u het clientapparaat los van het draadloze netwerk, navigeert u naar Monitor > Clients op de WLC en verwijdert u de sessie uit de uitvoer. De WLC houdt de inactieve sessie standaard vijf minuten, dus om een geldige test uit te voeren, moet je opnieuw beginnen.

4. Keer de volgorde van de ISE-PSN's onder de gast WLAN-configuratie om:



5. Log in op de gast-SSID, navigeer naar Bediening > Verificaties in de ISE en controleer of de juiste autorisatieregels zijn getroffen:



Bij de tweede poging wordt het MaibockGuestWireless-autorisatieprofiel correct ingedrukt voor de eerste MAB-verificatie. Gelijkaardig aan de eerste poging tot jesse-dunkel (Stap 2), de authentificatie aan jesse-maibock raakt correct de GuestPermit voor de definitieve vergunning. Omdat er geen PSN-specifieke informatie in het GuestPermit-autorisatieprofiel staat, kan één regel worden gebruikt voor de verificatie van elke PSN.

Problemen oplossen

Het venster Verificatiedetails is een krachtige weergave die elke stap van het verificatie-/autorisatieproces weergeeft. Om toegang te krijgen, navigeer je naar Operations > Authentications en klik je op het vergrootglaspictogram onder de kolom Details. Gebruik dit

venster om te verifiëren dat de voorwaarden van de authenticatie/autorisatieregel correct worden geconfigureerd.

In dit geval is het veld Policy Server het primaire aandachtsgebied. Dit veld bevat de hostnaam van de ISE-PSN waarmee de verificatie wordt uitgevoerd:

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

Vergelijk het item Policy Server met de regelvoorwaarde en controleer of de twee overeenkomende items (deze waarde is hoofdlettergevoelig):

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

Opmerking: het is belangrijk om te onthouden dat u de verbinding met de SSID moet verbreken en de client-ingang van de WLC tussen tests moet wissen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.