WiFi op een Autonoom access point Configuration-voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u Wired Equivalent Privacy (EVN) kunt gebruiken en configureren op een Cisco Autonomous Access Point (AP).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat u een administratieve verbinding met de WLAN-apparaten kunt maken en dat de apparaten normaal in een niet-versleutelde omgeving werken. Om een standaard 40-bits EFN te configureren moet u twee of meer radio-eenheden hebben die met elkaar communiceren.

Gebruikte componenten

De informatie in dit document is gebaseerd op een 1140 AP die Cisco IOS® release 15.2JB runt.

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

Het encryptie-algoritme is ingebouwd in de 802.11 (Wi-Fi) standaard. gebruiken de stream-algoritme RC4 voor vertrouwelijkheid en de Cyclic Redundancy Check-32 (CRC-32) checksum voor integriteit.

Standaard 64-bits EFN gebruikt een 40-bits sleutel (ook bekend als de code-40), die aaneengezet is met een initialiseringsvector met 24 bits (IV) om de RC4-toets te vormen. Een 64-bits EFN-toets wordt gewoonlijk ingevoerd als een string van 10 hexadecimale (basis 16) tekens (nul tot en met negen en A-F). Elk teken vertegenwoordigt vier bits, en tien cijfers van vier bits elk 40 bits; als u de 24-bits IV toevoegt, produceert het de volledige 64-bits-sleutel.

Een 128-bits sleutel van EFG wordt gewoonlijk ingevoerd als een reeks van 26 hexadecimale tekens. 26 cijfers van vier bits elk gelijk aan 104 bits; als u de 24-bits IV toevoegt, produceert het de volledige 128-bits sleutel van het 128-bits-gebruik. De meeste apparaten staan de gebruiker toe de toets als 13 ASCII tekens in te voeren.

Verificatiemethoden

Er kunnen twee methoden voor echtheidscontrole worden gebruikt met behulp van de volgende formule: Open systeemverificatie en gedeelde sleutelverificatie.

Met Open System-verificatie hoeft de WLAN-client geen aanmeldingsgegevens aan AP te leveren voor verificatie. Elke client kan authenticeren met AP en dan proberen te associëren. In feite vindt er geen authenticatie plaats. Daarna kunnen de sleutels van de EVN worden gebruikt om gegevensframes te versleutelen. Op dit punt moet de cliënt de juiste sleutels hebben.

Met Shared Key Verificatie wordt de de sleutel van EFN gebruikt voor authenticatie in een viervoudige, uitdaging-antwoord handdruk:

1. De cliënt stuurt een verificatieaanvraag naar de AP.
2. Het AP antwoordt met een duidelijke uitdaging.
3. De client versleutelt de uitdaging-tekst met de geconfigureerde EFN-toets en reageert met een andere verificatieaanvraag.
4. AP decrypteert de reactie. Als het antwoord overeenkomt met de uitdaging-tekst, stuurt het AP een positief antwoord.

Na de authenticatie en associatie wordt de pre-gedeelde de sleutel van de EVN ook gebruikt om de gegevensframes met RC4 te versleutelen.

Op het eerste gezicht lijkt het alsof Shared Key Verificatie veiliger is dan Open System Verificatie, omdat de laatste geen echte authenticatie biedt. Het omgekeerde is echter waar. Het is mogelijk om de keystream af te leiden die voor de handdruk wordt gebruikt als u de uitdagingsframes in Shared Key Verificatie opneemt. Daarom is het raadzaam Open System-verificatie te gebruiken voor de authenticatie van het EFN in plaats van de gedeelde toetstichting.

TKIP (Temporal Key Integrity Protocol) werd gecreëerd om deze problemen met EFG aan te pakken. Gelijkaardig aan NUL gebruikt TKIP RC4-encryptie. TKIP verbetert echter EFG met de toevoeging van maatregelen zoals hashing per pakket, Berichtintegriteitscontrole (MIC) en Broadcast-sleutelrotatie om bekende kwetsbaarheden van EVN aan te pakken. TKIP gebruikt het

RC4 stream-algoritme met 128-bits coderingssleutels en 64-bits coderingssleutels.

Configureren

Deze sectie verschaft de GUI- en CLI-configuraties voor EFN.

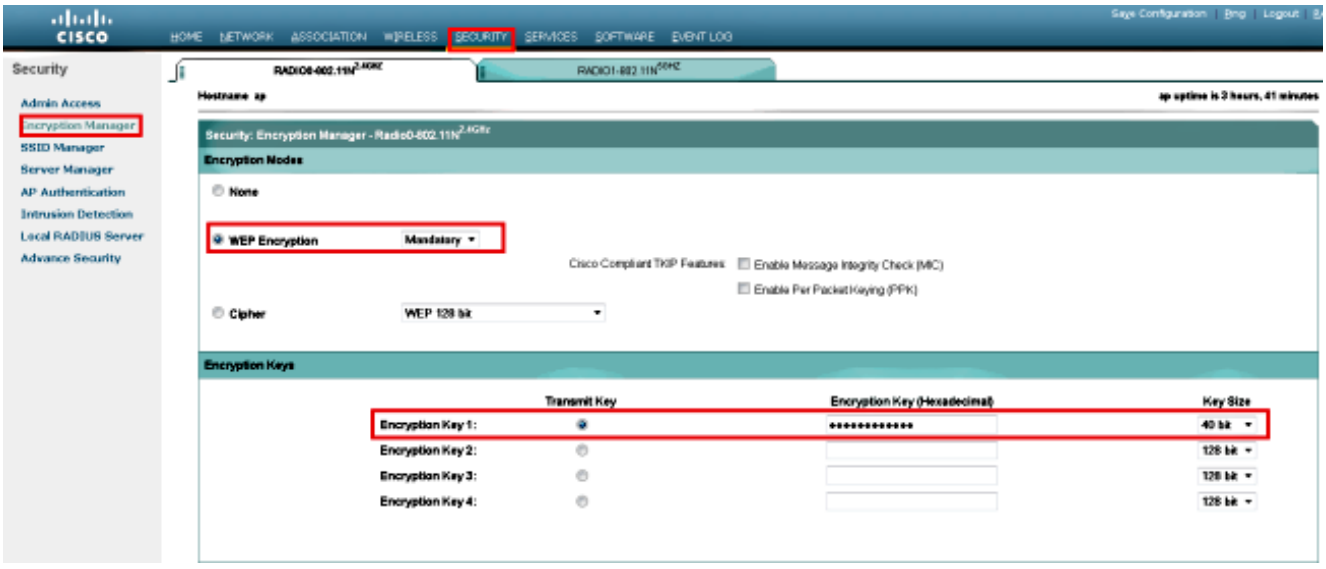
GUI-configuratie

Voltooi deze stappen om EFN met de GUI te configureren.

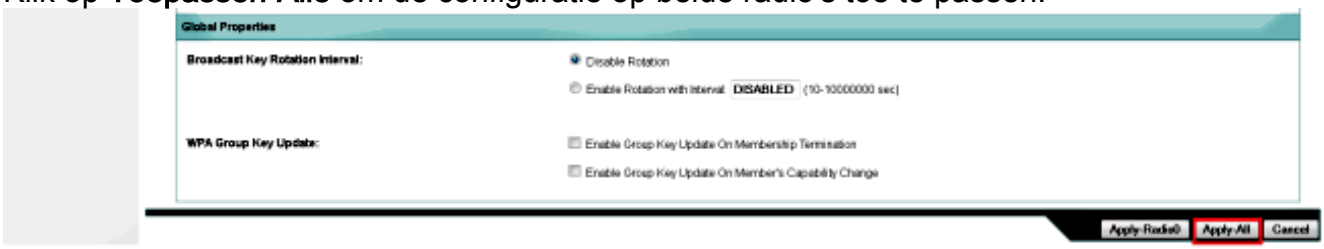
1. Sluit aan op de AP door de GUI.
2. Kies in het menu Beveiliging aan de linkerkant van het venster de optie **Encryption Manager** voor de radio-interface waaraan u de statische sleutels van de EVN wilt configureren.
3. Klik onder Encryption Modes op **EFN Encryption** en selecteer **Mandatory** van het vervolgkeuzemenu voor de client.

   De encryptie-methoden die door station worden gebruikt zijn:
   Standaard (geen encryptie) - vereist dat klanten met de AP communiceren zonder gegevensencryptie. Deze instelling wordt niet aanbevolen.**Optioneel** - Hiermee kunnen klanten met of zonder gegevensencryptie communiceren met de AP. Meestal gebruikt u deze optie wanneer u clientapparaten hebt die geen verbinding met een netwerk kunnen maken zoals niet-Cisco-clients in een 128-bits EFN-omgeving.**Verplicht (Full Encryption)** - vereist dat klanten gegevensencryptie gebruiken wanneer zij met AP communiceren. Clients die geen gegevensencryptie gebruiken, mogen niet communiceren. Deze optie wordt aanbevolen als u de beveiliging van uw WLAN wilt maximaliseren.
4. Selecteer onder Encryption Keys de radioknop **Transmit Key** en voer de 10-cijferige hexadecimale toets in. Zorg ervoor dat de Key Size is ingesteld op **40 bit**.

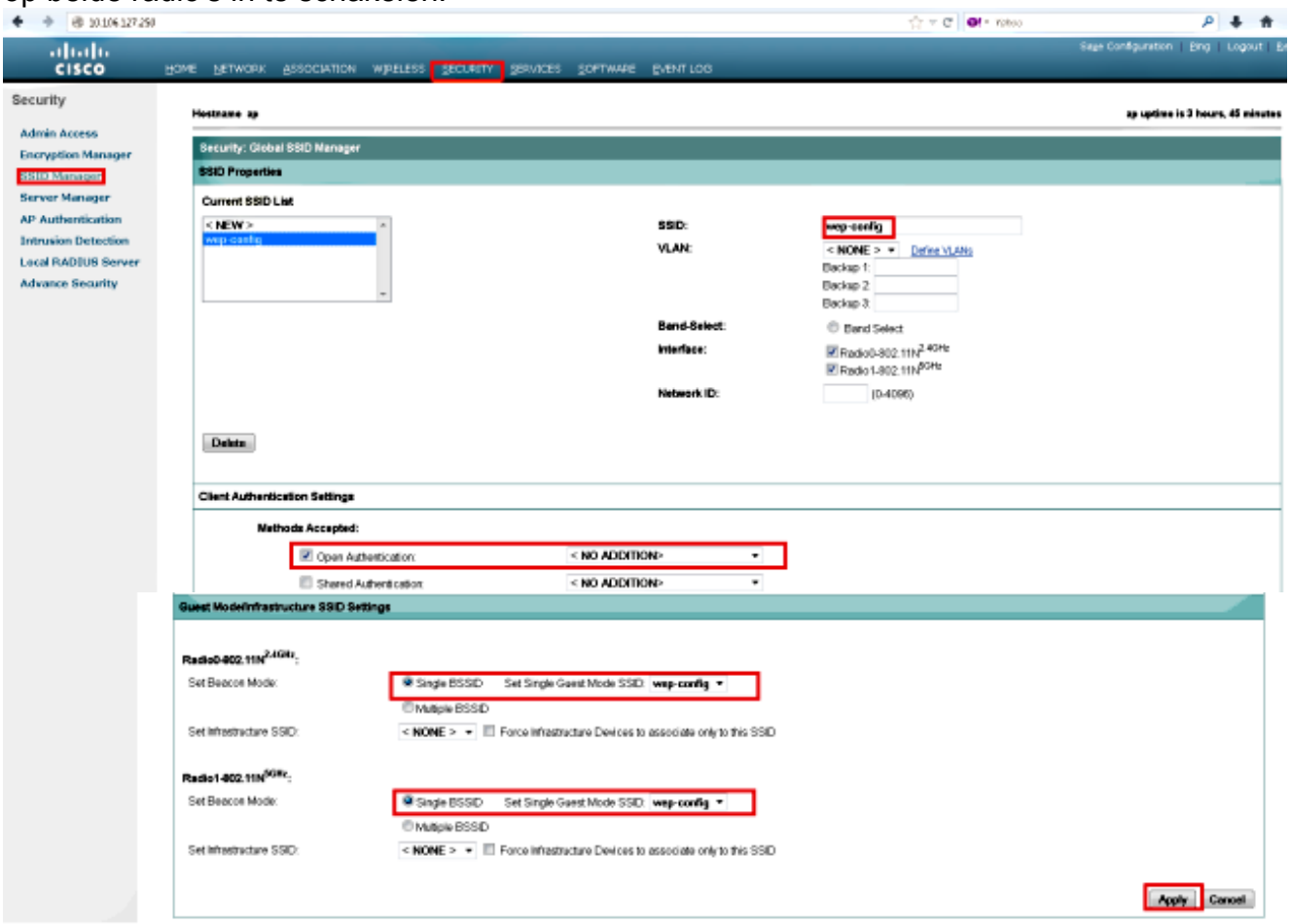
   Voer 10 hexadecimale cijfers in voor 40-bits EFN-toetsen of 26 hexadecimale cijfers voor 128-bits EFN-toetsen. De toetsen kunnen worden gebruikt door een combinatie van deze cijfers:
   0 tot 9a tot fA tot
   F



5. Klik op **Toepassen-Alle** om de configuratie op beide radio's toe te passen.



6. Maak een Service Set Identifier (SSID) met **Open Verificatie** en klik op **Toepassen** om deze op beide radio's in te schakelen.



7. Navigeren in naar het netwerk en de radio's inschakelen voor **2,4 GHz** en **5 GHz** om ze draaiend te houden.

CLI-configuratie

Gebruik deze sectie om de vorm van een NUL te geven aan de CLI.

```
ap#show run
Building configuration...

Current configuration : 1794 bytes
!
!
```

```
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
 dot11 ssid wep-config
 authentication open
 guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
```

```
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Verifiëren

Typ deze opdracht om te bevestigen dat de configuratie goed werkt:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

Problemen oplossen

Deze sectie bevat troubleshooting-informatie voor uw configuratie.

> **Opmerking:** Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Deze **debug** opdrachten zijn handig om de configuratie problemen op te lossen:

- **debug dot11 gebeurtenissen** - hiermee kan het debug in alle dot1x gebeurtenissen worden

ingeschakeld.

- **debug-pakketten van dot11** - hiermee kan de debug in alle dot1x-pakketten worden ingeschakeld.

Hier is een voorbeeld van het logboek dat toont wanneer de client succesvol aan WLAN associeert:

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

Wanneer de client de verkeerde toets invoert, wordt deze fout weergegeven:

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

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.