Radius-Server mit 802.1x- und MAC-Authentication im WLAN einrichten

Inhaltsverzeichnis

Dieser Beitrag konzentriert sich auf den Bereich WLAN.

Folgende Sachen sind an diesem Wiki Beitrag noch zu überarbeiten:

1. Konsolidierung mit dem Netzwerk Beitrag, bspw. das Anlegen eines Radius Profils und von Radius Usern in einen eigenen Beitrag auslagern und dann von hier darauf verweisen
2. Prüfen, ob es möglich ist verschiedene Radius Profile zu erstellen, so dass MAC-Adressen-Radius-User nicht für die Auth an einem 802.1x WPA2-/3-Enterprise Wifi verwendet werden können
3. Gebt gern Feedback unten in der Kommentarfunktion. Was fehlt euch, was ist unverständlich beschrieben, etc.?

Was wollen wir?

Radius in der Unifi Network Application (Controller) konfigurieren, damit wir dies als Basis für 802.1x oder MAC-Authentication verwenden können.

Warum wollen wir das?

Wir wollen, dass sich Geräte per 802.1x (User/Passwort) oder mit ihren MAC-Adressen authentifizieren, um diese dynamisch in unterschiedliche VLANs zu führen. Dies erspart uns die Erstellung diverser SSIDs (bspw. eine SSID pro VLAN) und reduziert somit die Kanalauslastung. Nach der Einrichtung verbinden sich Endgeräte, die normalerweise in unterschiedlichen VLANs und somit SSIDs (Management, IoT, Security, etc) liegen würden, mit max. 3 SSIDs, bspw.:

- SSID1: WPA-3-Enterprise (PMF required, Fast Roaming enabled): Hier verbinden sich aktuelle Highend-Geräte, wie bspw. Smartphones, Notebooks oder Tablets
- SSID2: WPA2/WPA3 (PMF optional): Hier verbinden sich alle anderen persönlichen Geräte, wie bspw. IoT, Sonos, Security Things, whatever
- SSID3: WPA2/WPA3 (PMF optional): Hier verbinden sich Gäste

Was ist 802.1x Authentication?

Bei 802.1x erstellt man pro User einen Account mit Passwort und VLAN Zuweisung. Dieser Account kann von mehreren Endgeräten gleichzeitig genutzt werden. Voraussetzung ist, dass das OS des Endgerätes diese Art der Authentifizierung unterstützt.

Unifi stellt dafür zwei Sicherheitsprotokolle bereit:

1. WPA-Enterprise
2. WPA3-Enterprise

Was ist MAC-Authentication?

Auf Basis der MAC-Adresse entscheidet der Radius Server, ob sich ein Gerät mit dem WLAN verbinden darf. Ist die MAC-Adresse nicht bekannt, wird der Verbindungsaufbau abgelehnt. Dieses Konzept ist erstmal losgelöst von 802.1x und ist als Ergänzung zu betrachten.

Und wie geht das genau?

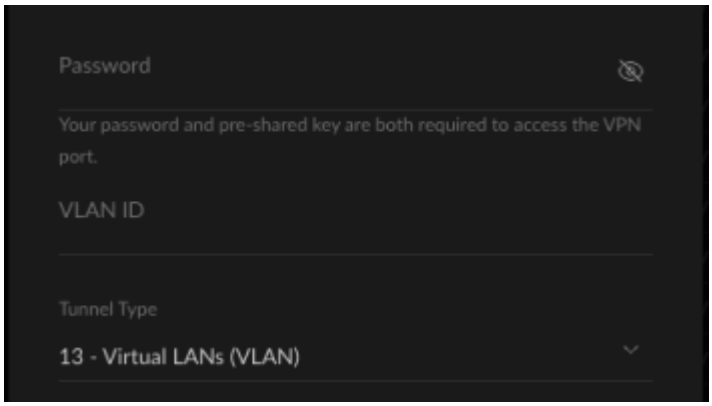
1 Radius Profil anlegen

Menü (v6.5.55): "Settings - Advanced Features - Radius" -> Einstellungen des Default Profiles wie folgt anpassen:

Wenn sich meine Endgeräte mit Wifi-Schnittstelle am WLAN per Radius authentifizieren sollen, ist die Einstellung "Enable Wireless" im "Default" Radius Profil zu aktivieren. Wenn dieses Profil zusätzlich auch für Wired (verkabelte) Ethernet Endgeräte verwendet werden soll, ist zusätzlich die Option "Enable Wired" zu aktivieren, mehr dazu: >>> hier klicken <<<

2 Radius User anlegen

Menü (v6.5.55): "Settings - Advanced Features - Radius" -> "Default Profile - Radius Users" auswählen und Schaltfläche "Create New Radius User" betätigen:



Unabhängig von 802.1x oder MAC-Authentication sind "VLAN ID", "Tunnel Type" und "Tunnel Medium Type" immer wie folgt zu konfigurieren:

- VLAN ID: <vlan_id>
- Tunnel Type: 13 - Virtual LANs (VLAN)
- Tunnel Medium Type: 6 - 802 (includes all 802 media plus Ethernet "canonical format")

Bei der VLAN ID tragt ihr einfach die ID eures VLANs ein, wie der Name schon sagt. Soll das entsprechende Gerät bzw. der User in das Default LAN lasst ihr das Feld einfach leer.

Nun kommt der unterscheidende Teil: "Username" und "Password"

2.1 802.1x-Authentication User anlegen

- Username: <username>
- Password: <password>
- "VLAN ID", "Tunnel Type" und "Tunnel Medium Type" eingeben (siehe vorangegangenes Kapitel)

2.2 MAC-Authentication User anlegen

Hier wird kein herkömmlicher User mit Passwort angelegt, sondern die MAC-Adresse eures Gerätes als "User" und "Password" eingegeben.

Es empfiehlt sich folgendes Format zu verwenden:

In dieser Schreibweise werden die MAC-Adressen auch in der Network Application unter "Client Devices" angezeigt. So können die MAC-Adressen von dort einfach kopiert werden. Aber Achtung, eine MAC-Adresse kann erst kopiert werden, wenn sich das dazugehörige Gerät einmal anmelden durfte. Wenn man die MAC-Adresse nicht kennt bzw. nicht ermitteln kann, könnte man das Gerät bspw. am Gäste-WLAN anmelden. Anschließend den User anlegen und dann das Gerät an der richtigen SSID anmelden.

- Username: <mac-address>
- Password: <mac-address>
- "VLAN ID", "Tunnel Type" und "Tunnel Medium Type" eingeben (siehe vorangegangenes Kapitel)

3 WLAN einrichten

Wir bleiben bei den drei Beispiel-SSIDs aus dem Kapitel "Warum wollen wir das?" Alle Menüpunkte, die nachfolgend nicht aufgeführt werden, befinden sich in den Default-Einstellungen. Ihr könnt die natürlich eurer Erfahrung nach nach beliebig anpassen.

3.1 SSID mit 802.1x anlegen

Hier verbinden sich unsere High-Endgeräte. Dementsprechend empfiehlt sich folgende Konfiguration:

- Enable: Enabled
- Name: <Name der SSID>
- Network: <Hauptnetzwerk> (Wenn ich ehrlich bin, bin ich mir unsicher, was hier zu konfigurieren ist, bzw. welche Auswirkungen das überhaupt hat, da man am Radius User das VLAN konfiguriert.)

Advanced:

- WiFi Band: 5GHz
- BSS Transition: Enabled
- Enable Fast Roaming: Enabled

Security:

- Security Protocol: WPA-2 Enterprise oder WPA-3 Enterprise (Wenn ihr aktuelle Endgeräte mit aktuellem OS habt, solltet ihr euer Glück mit WPA-3 Enterprise probieren)
- PMF: Required (bei WPA-3 Enterprise) oder Optional (bei WPA-2 Enterprise)

Es gibt Geräte, die mit PMF (Protected Management Frames) gar nicht zu recht kommen. Die gehören dann auf jeden Fall nicht in diese SSID.

3.2 SSID mit Radius MAC-Authentication anlegen

Hier verbinden sich all unsere anderen persönlichen Endgeräte (IoT, Sonos, Security Things, whatever). Dementsprechend empfiehlt sich folgende Konfiguration:

- Enable: Enabled
- Name: <Name der SSID>
- Password: <Password>
- Network: <Hauptnetzwerk> (Wenn ich ehrlich bin, bin ich mir unsicher, was hier zu konfigurieren ist, bzw. welche Auswirkungen das überhaupt hat, da man am Radius User das VLAN konfiguriert.)

Advanced:

- WiFi Band: 2.4GHz und 5GHz
- BSS Transition: Enabled
- Enable Fast Roaming: Enabled

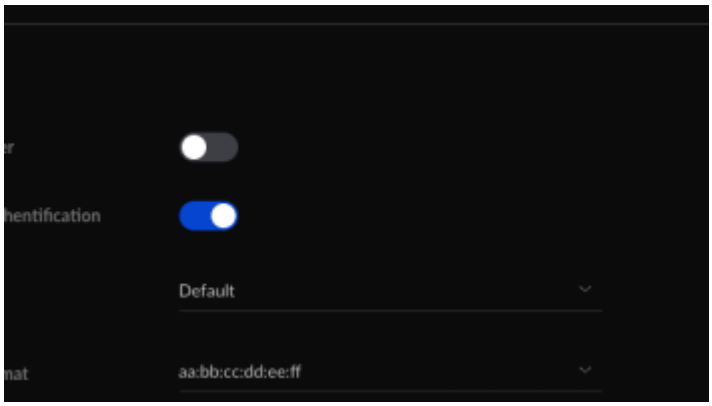
Security:

- Security Protocol: WPA-2/WPA-3
- PMF: Optional

Es gibt Geräte, die mit PMF (Protected Management Frames) gar nicht zu recht kommen. Die gehören dann auf jeden Fall nicht in diese SSID.

MAC Authorization:

Hier ist folgende Konfiguration vorzunehmen. Diese Schreibweise von MAC-Adressen empfiehlt sich, da es die Schreibweise in der Network Application ist, siehe auch Kapitel "MAC-Authentication User anlegen":



4 Tips und Tricks

-> erstmal nur ein Sammler, wird später ausformuliert…

1. Ein Gerät im IoT VLAN verlangt, die Inbetriebnahme mit einem Gerät im selben WLAN, welches sich aber in einem anderen VLAN/WLAN befindet

5 Upvote des Feature Requests im offiziellen Ubiquiti Forum

Wenn euch Radius, 802.1x, MAC Authentication und Co gefällt, lasst gerne ein Upvote bei folgendem Feature Request da und diskutiert mit, was euch fehlt:

https://community.ui.com/questions/Radius-Users-and-Radius-Profile-improvement-suggestions/41760fec-f6b0-4d09-ae12-bffa14a6a664

Disclaimer:

Alle Anleitungen/Tutorials sind nach bestem Wissen und Gewissen verfasst, gehen immer von den definierten Software/Firmware-Versionen aus und sind auf das englische GUI ausgelegt.

Es gibt keine Garantie auf Erfolg. Im Falle eines Misserfolges hilft aber die Community hier sicherlich weiter.

Keiner der Autoren oder der Betreiber des Forums ist für die aus der Nutzung resultierenden Probleme/Herausforderungen verantwortlich.

Jegliche hier beschriebenen Schritte erfolgen ausnahmslos in eigener Verantwortung des Durchführenden.

Eltern haften für ihre Kinder.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!