Radius Macadressenkontrolle für WLAN über LDAPauth UCS (Univention) mit Fortinet Accesspoints

Du möchtest dich gerne für unsere Hilfe erkenntlich zeigen . Gerne. Wir bedanken uns bei dir für deine Spende!

Spenden

Hauseigenes Apt-Repo: https://apt.iteas.at

GITLAB Enterprise:

In diesem HowTo beschreibe ich wie man zusätzlich zur WLAN WPA2/3 Enterprise Auth. mit UCS (Univention) LDAP auch eine Macadressenkontrolle mit Radius umsetzen kann. Als Accesspoints verwenden wir hier FortiAP's. Das ganze hat den Vorteil das man mit Radius noch eine weiter Sicherheitsschicht einführt. Somit muss der Client am LDAP mit einem Computerkonto eingetragen sein. Ist er das nicht, ist trotz richtigen Authentifizierungsdaten kein Login am WLAN möglich.

Folgende OS Versionen wurden eingesetzt:
4.4-8 errata1019
FortiOS v7.0.1
ForitAP v7.0.1

Konfiguration

Voraussetzung ist hier das man sich bereits erfolgreich am WLAN mit WPA2/3 Enterprise anmelden kann, wenn man in einer ausgewählten LDAP-Gruppe des UCS-System Mitglied ist.

WLAN Fortinet

Um nun die MAC-Kontrolle für eine SSID zu aktivieren, geht man folgender Maßen for:

```
config wireless-controller vap
    edit "mywlanssid"
        set ssid "mywlanssid"
     +  set mac-username-delimiter colon
     +  set mac-password-delimiter colon
        set security wpa2-only-enterprise
        set pmf enable
```

```
     +  set radius-mac-auth enable
     +  set radius-mac-auth-server "UCS-Radius"
        set auth usergroup
        set local-bridging enable
        set usergroup "wifi-wlan"
        set schedule "always"
        set vlanid 44
    next
end
```

Essentiell sind die Zeilen mit dem „+“. Der Name des auth-server kann natürlich abweichen.

Konfiguration Univention UCS

Hierfür sind einige Dinge zu beachten. Zum einen muß die Funktion für die Macadressenkontrolle aktiviert werden:

```
usr set radius/mac/whitelisting=true
```

Weiters muss ein Filter im LDAP Modul von Radius verändert werden. Vorher legen wir noch kurz ein Backup der Dateien an:

```
cp  /etc/univention/templates/files/etc/freeradius/3.0/mods-available/ldap
/etc/univention/templates/files/etc/freeradius/3.0/mods-
available/ldap_backup_orig
cp  /etc/freeradius/3.0/mods-enabled/ldap /etc/freeradius/3.0/mods-
enabled/ldap_backup_orig
```

Nun die Änderungen durchführen:

```
nano /etc/univention/templates/files/etc/freeradius/3.0/mods-available/ldap

@!@
auth_type = configRegistry.get('freeradius/conf/auth-type/mschap', 'FALSE')
if auth_type and 'TRUE' == auth_type.upper() or 'YES' == auth_type.upper():
#else:
#       filter = 'Stripped-User-Name'
#print '\t\tfilter = "(uid=%%{%s:-%%{User-Name}})"' % filter
@!@
filter = "(|(uid=%{mschap:User-Name:-%{User-
Name}})(macAddress=%{mschap:User-Name:-%{User-Name}}))"
```

Nun noch die Änderungen in die Konfiguration übernehmen und den Radius neu starten. Danach den Radius neu starten:

```
ucr commit /etc/freeradius/3.0/mods-available/ldap && service freeradius
restart
```

Die Änderungen müssen natürlich auf allen Radiusservern im Netzwerk durchgeführt werden.

Zu guter letzt ist es noch wichtig für die Konten den Gerätetyp „Linux“ zu verwenden. Die WLANclients benötigen einen vollwertigen Computeraccount. Unter „Allgemein“ muss **Rechnername, MAC Adresse und IP** angegeben werden. Unter „Radius“ ein Hakerl bei **Netzwerkzugriff erlaubt** setzen.

Danach muss man unter „Erweiterte Einstellungen“ → Konto, das Gerätepasswort eintragen. Dies ist die MAC-Adresse des Gerätes in Großbuchstaben.
24-EF-BA-96-D2-03 → Falsch
24:ef:ba:96:d2:03 → Falsch
24:EF:BA:96:D2:03 → Richtig

Und schon ist die Macadressenkontrolle aktiv.

Clientfalle

Ändert man das Device/Gerätekontenpasswort in UCS auf die Macadrresse, muss dieses natürlich auch auf dem Client in der sssd.conf nachgetragen werden. Auch ein erneuter Export der Keytab ist erforderlich.

Radius Debug

Wichtig ist hier zu erwähnen das dies je nach Router/WLAN das man verwendet etwas anders sein kann. Um zu erfahren welches Passwort der Client nun wirklich mitsendet. Stoppt man Radius und startet ihn im Debugmode neu:

```
service freeradius stop
freeradius -X
```

Nun lässt man einen Client per WLAN verbinden. Sämtliche Anfragen und Logs sieht man nun live in dieser Ausgabe, auch welches Passwort vom Client mit gesendet wird.

UCS 4.4 kommt mit einer verbesserten Fehlersuche. Mit dem Kommandozeilentool `univention-radius-check-access` können Sie aktuelle Zugangsregeln für einen bestimmten Benutzer und/oder eine MAC-Adresse überprüfen. Sie rufen den Befehl als Benutzer root auf dem UCS-Server (in einem Terminalfenster oder auf der Konsole) auf. Die RADIUS-App protokolliert die Ereignisse und schreibt sie in die Logdatei `/var/log/univention/radius_ntlm_auth.log`. Wie ausführlich die Meldungen sind, legen Sie über die Univention-Configuration-Registry-Variable `freeradius/auth/helper/ntlm/debug` fest. Der FreeRADIUS-Server legt ebenfalls seine eigene Logdatei unter `/var/log/freeradius/radius.log` an.