UniFi Giriş Nöqtələri ilə RADIUS NPS Serverində istifadəçi adından asılı olaraq VLAN-ların avtomatik təyin edilməsi

Müasir dövrdə korporativ ofislər WiFi şəbəkəsinin təhlükəsizliyini artırmaq üçün WPA2 Enterprise texnologiyasından istifadə edirlər. Bu üsül, WiFi şəbəkəsinə vahid şifrə ilə yox, RADIUS Server vasitəsi ilə, WiFi-dan AD domain istifadəçi şifrəsini tələb edir. Belə ki WPA2 Enterprise bir çox üstünlüklər verir:

- WPA2 Enterprise texnoloqiyanın təyinatı və müsbət cəhətləri
- Daxili WiFi .şəbəkəsinin dizaynı
- Şəbəkə avadanlıqların konfiqurasiyası

- Giriş nöqtələri kontrollerin sazlanması
- NPS Serverin sazlanması

WPA2 Enterprise texnoloqiyanın təyinatı və müsbət cəhətləri

Müasir dövrdə korporativ ofislər WiFi şəbəkəsinin təhlükəsizliyini artırmaq üçün WPA2 Enterprise texnologiyasından istifadə edirlər. Bu üsül, WiFi şəbəkəsinə vahid şifrə ilə yox, RADIUS Server vasitəsi ilə, WiFi-dan AD domain istifadəçi şifrəsini tələb edir. Belə ki WPA2 Enterprise bir çox üstünlüklər verir:

Təhlükəsizlik: WPA2 Enterprise, WPA2 Personal ilə müqayisədə daha yüksək səviyyədə təhlükəsizlik təmin edir. O, daha təhlükəsiz identifikasiya metodundan (məsələn, 802.1X/EAP) istifadə edir ki, bu da istifadəçilərdən WPA2 Personal-da istifadə olunan əvvəlcədən paylaşılan açar (PSK) əvəzinə istifadəçi adı və parol və ya digər etimadnaməsi ilə autentifikasiya etməyi tələb edir.

İstifadəçi İdarəetmə: WPA2 Enterprise RADIUS (Remote Authentication Dial-In User Service) serveri vasitəsilə mərkəzləşdirilmiş istifadəçi idarəetməsinə imkan verir. Bu, şəbəkə inzibatçıların şəbəkəyə girişi idarə etmək və nəzarət etmək, o cümlədən istifadəçiləri və cihazları əlavə etmək və silmək üçün asanlaşdırır.

Audit və Giriş: WPA2 Enterprise daha yaxşı audit və qeyd imkanları təmin edir, şəbəkə administratorlarına şəbəkəyə girişi daha effektiv şəkildə izləməyə imkan verir. Bu təhlükəsizlik məqsədləri üçün vacib ola bilər.

Daxili WiFi .şəbəkəsinin dizaynı

Buna nail olmaq üçün iki üsül var:

1. Siz bunu daxili şəbəkədə müxtəlif çoxsaylı SSID yaratmaqla nail ola bilərsiniz. Bu zaman hər bir SSID müvafiq VLAN-a təyin olunmalıdır. Bu ən asan üsüldür, mənfi (şəxsən mənə görə) cəhəti odur ki, tələblərdən asılı olaraq, sizdə 10-12 SSID ola. Bu da, şəxsən mənə görə, istifadəçilərə çətinlik yaradacaq və onlar sizə daim “Mən hansı vayfaya qoşulmalıyam” sualla müraciət edəcəklər
2. Siz daxili şəbəkədə 1 dənə SSID yaradlrslz və ona qoşulan istifadəçidən asılı olaraq onu müvafiq VLAN-a təyin edirisniz. Texniki olaraq bu üsüla “dynamic VLAN assignment” deyilir. Bu cür siz yalnız bir SSID vasitəsi ilə tək NPS serverindən istifadə etməklə müxtəlif VLAN-ları idarə edə bilərsiniz. Bu təlimatda biz məhz bu metodu araşdıracağıq.

Şəbəkə avadanlıqların konfiqurasiyası

İlk oncə sizin svitçə qoşulu olan hır giriş nöqtələri (Access Point) sazlanmalıdır. Biz öz ofisinizdə Cisco Catalyst svitçlərdən istifadə etdiyindən burada məhz cisco svitç konfigurasiyasını təqdim edirik.

```
interface GigabitEthernet3/0/26
description UniFi_AP_UniFiAPName
switchport trunk encapsulation dot1q
switchport trunk native vlan 30
switchport trunk allowed vlan 25,26,30-32
switchport mode trunk
```

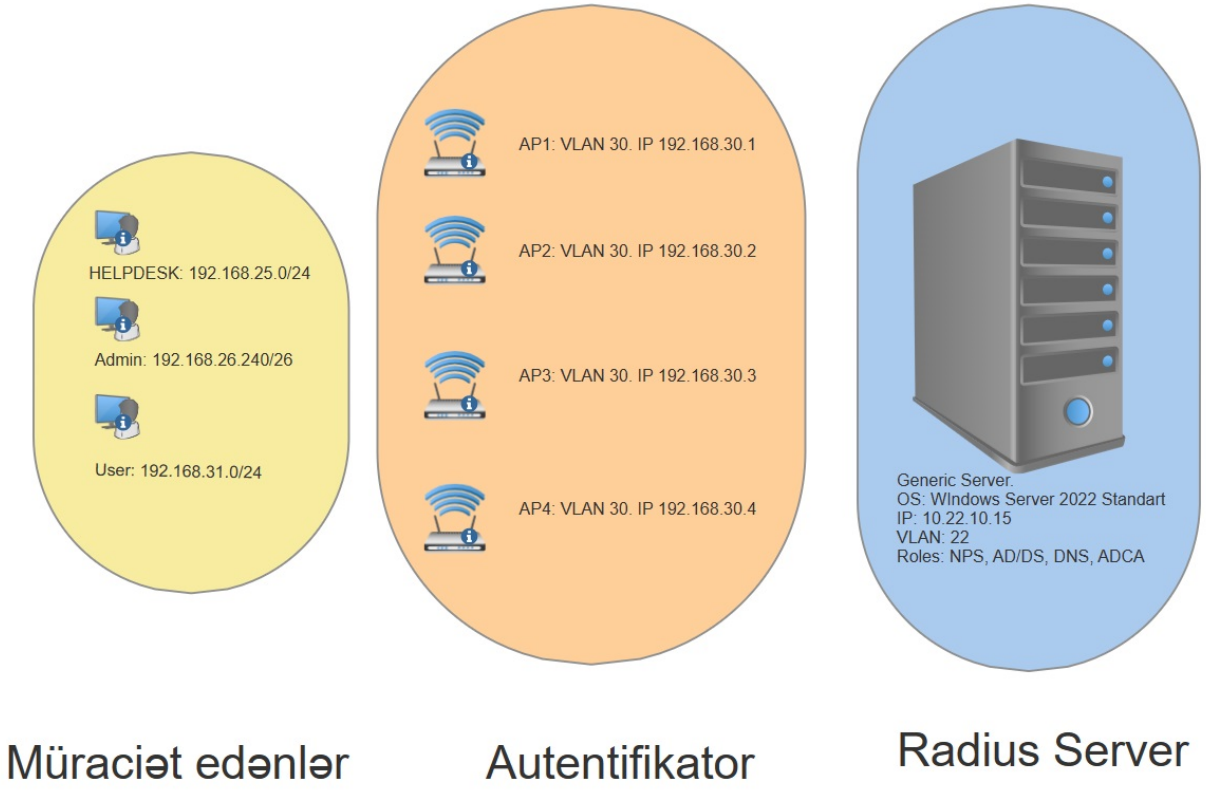
Burada VLAN-ların təyinatımı təqdim edirik

VLAN25 – Helpdesklər üçün nəzərə tutulub. Bu VLAN -da məhdudiyyətlər çövcuddur və IT infrastrukturunda yer alan bəzi server və şəbəkə avadanlıqlara giriş imkanları verir. Alacaqları IP ünvan: 192.168.25.0/24

VLAN26 – Adminlər üçün nəzərə tutulub. Bütün infrastruktura məhdudiyyətsiz giriş imkanı verir. Alacaqları IP ünvan: 192.168.26.240/26.

> Real dünyada bunu eləmək məsləhət deyil. İri dövlət qurumlarda, iri şirkətlərdə və strateji əhəmiyyətli obyektlərdə WıFİ vasitəsi ilə heç bir haıda server və şəbəkə avadanlırlara giriş olmamalıdır. Eləsəz, məncə, ən yaxşı halda işdən çıxarılacaqsımız. Bunu biz burda sədəcə test məqsədi ilə göstəririk.

VLAN31 – İstofadəçilər üçün nəzərdə tutulub və burada istoifadəçi səviyyəsində server infrastrukturuna icazələr mövcuddur. Misal üçün: 1C Server icazə verilən portlar – tcp/1540, tcp/1541 və tcp/1560-1591



Müraciət edənlər

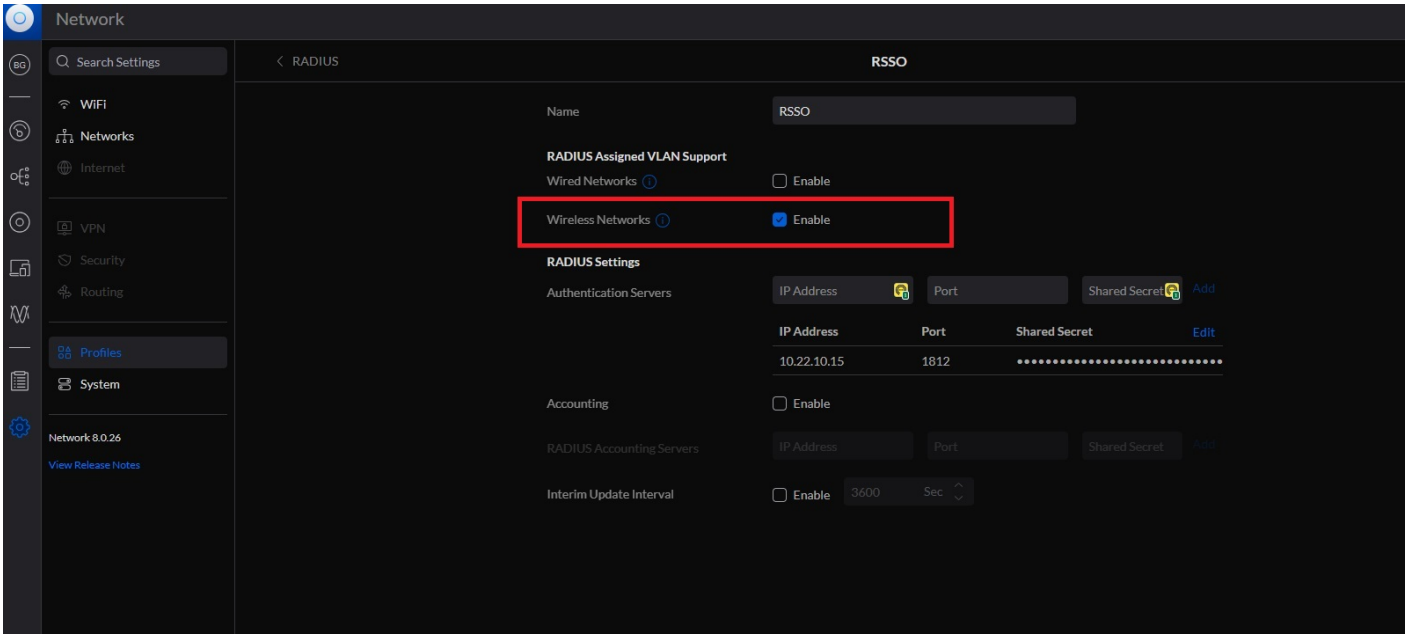
Autentifikator

Radius Server

Giriş nöqtələri kontrollerin sazlanması

Bizdə infrastrukturda Ubiquiti UniFi WiFI Controller istifadə olunduğundan, bütün işlər məhz bu softun üzərində aparılacaq. Amma onu demək lazimdır ki, digər giriş nöqtələri kontrollerlərdədə eyni (istər Cisco, Rukus, Huawei və s.) sazlamaları etmək mümkündür. Ən azından bu UniFi-da varsa, başqa giriş nöqtələri kontrollerlərdədə bu olmalıdır!

Konfiqurasiya zamanı, kontrollerə RADİUS serveri əlavə etdikdə **RADIUS Assigned VLAN Support** bölməsində **Wireless Networks** bölməsini aktivləşdirin.

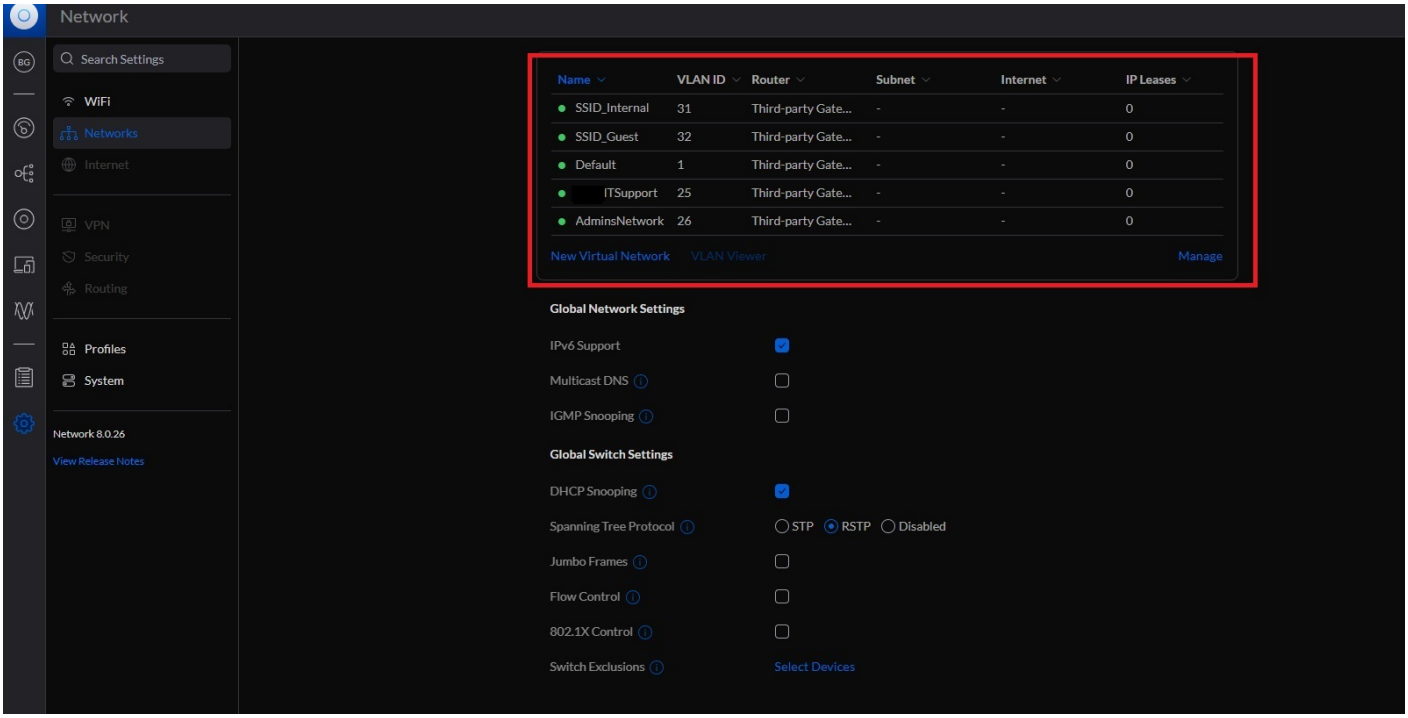


Əmin olun ki bütün lazımı VLAN-ları əlavə etmisiniz

Bizim konfiqurasiyada 4 ədəd VLAN istofadə olunur.

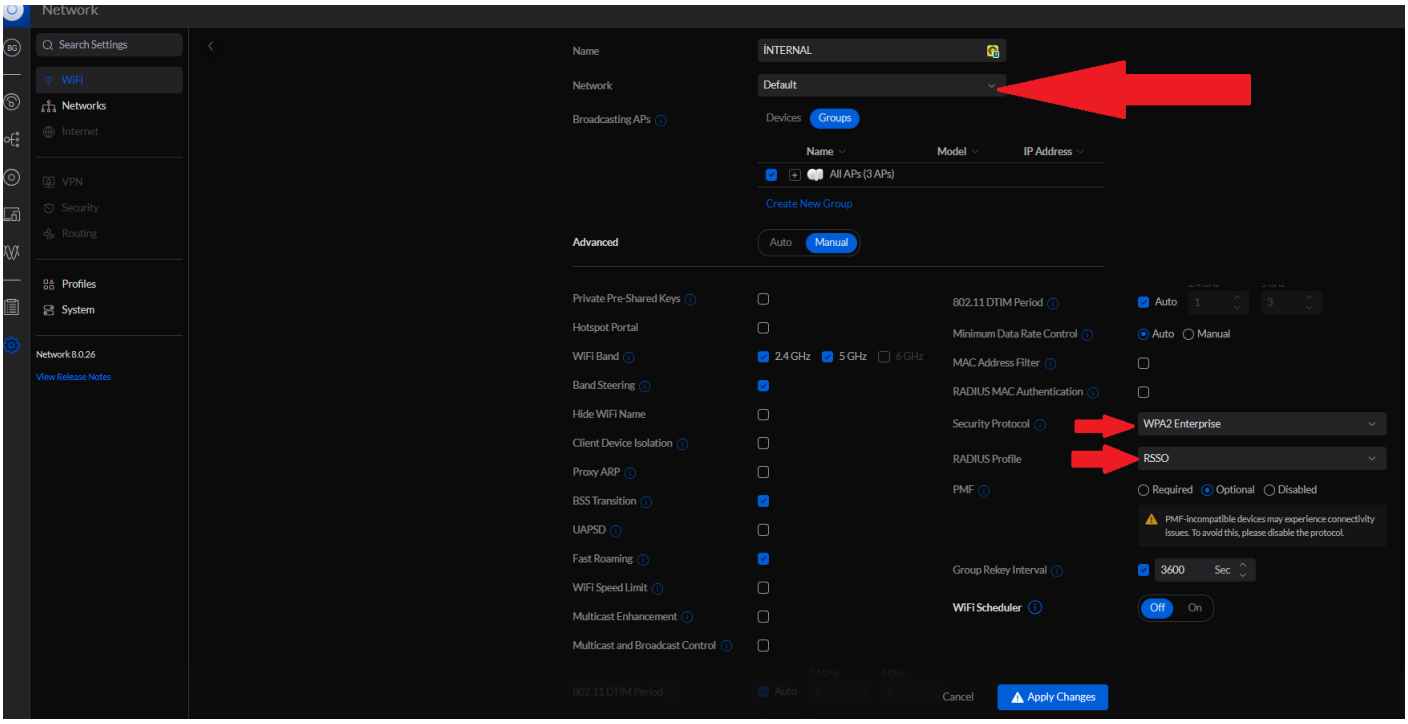
AD	VLAN ID	Təsvir

SSID_Internal	31	Sadə istofadəçilər üçün nəzərdə tutlub harda ki • server şəbəkəsinə məhdud icazələr mövcuddur • icazələr yalnız ancaq lazım olan tcp və udp protlar vasitəsi il verilib • Application Control aktivləşdirilib
SSID_Guest	32	Hamı üçün nəzərdə tutlan WiFI şəbəkə. Bu VLAN-dan daxili şəbəkəyə heç bir icazə mövcu deyildir.
IT_Support	25	Helpdesk-lər üçün nəzərdə tutlmuş WiFI şəbəkə hardan texniki qrup seçilmiş server və şəbəkə avadanlıqlarına giriş icazələri verilib
AdminNetwork	26	Əsas admin VLAN və burada bütün infrastruktur əlçatandır.



SSID əlavə edin, istədiyiniz kimi adlandırın və əsas məsələ əmin olun ki

- **Network** bölməsində **Defaulr Network** seçilib
- **Security Protocol** bölməsində **WPA2 Enterprise** seçilib
- **RADIUS Profile** bölməsində daha öncəki addımda yaratdığınız radius profaylı seçin. Bizim misalda bu **RSSO**-dur


Network
Search Settings
WiFi
Networks
Internet
VPN
Security
Routing
Profiles
System
Network 8.0.26
View Release Notes
Name
İNTERNAL
Network
Default
Broadcasting APs
Devices
Groups
Name
Model
IP Address
All APs (3 APs)
Create New Group
Advanced
Auto
Manual
Private Pre-Shared Keys
Hotspot Portal
WiFi Band
2.4 GHz
5 GHz
6 GHz
Band Steering
Hide WiFi Name
Client Device Isolation
Proxy ARP
BSS Transition
UAPSD
Fast Roaming
WiFi Speed Limit
Multicast Enhancement
Multicast and Broadcast Control
802.11 DTIM Period
Auto
Minimum Data Rate Control
Auto
Manual
MAC Address Filter
RADIUS MAC Authentication
Security Protocol
WPA2 Enterprise
RADIUS Profile
RSSO
PMF
Required
Optional
Disabled
PMF-incompatible devices may experience connectivity issues. To avoid this, please disable the protocol.
Group Rekey Interval
3600
Sec
WiFi Scheduler
Off
On
Cancel
Apply Changes

NPS Serverin sazlanması