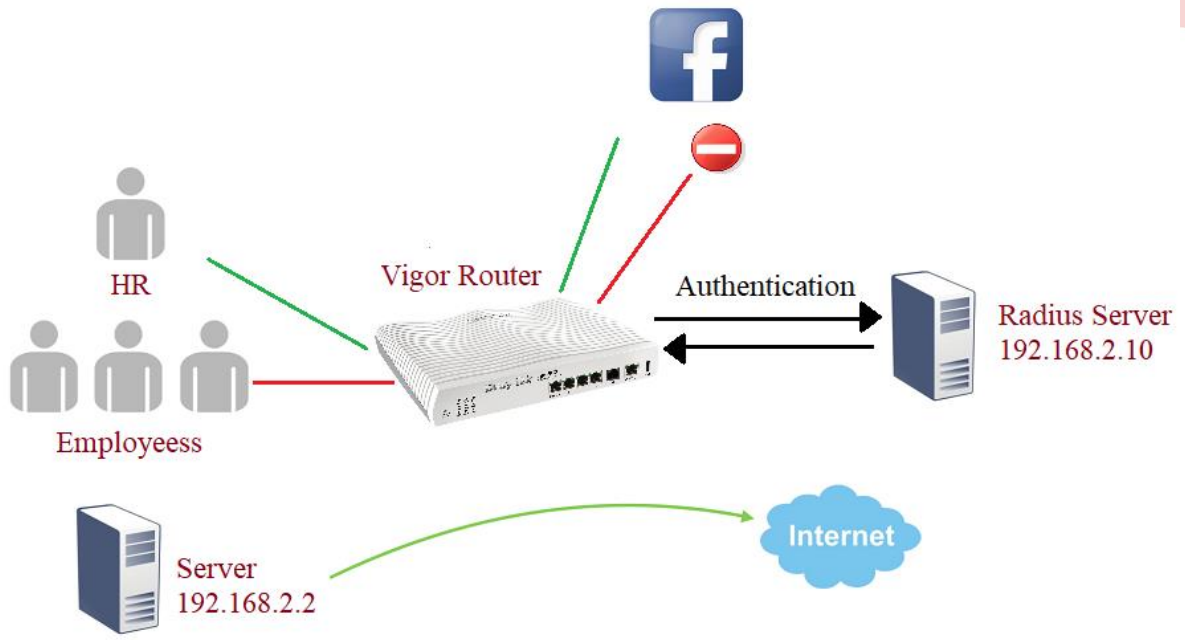


Kullanıcı Tabanlı Mod RADIUS ile nasıl kullanılır?

Bu yazıda, User Management'i RADIUS sunucusuyla nasıl kullanacağımızı göstereceğiz ve farklı kullanıcı hesapları için farklı politikalar belirleyeceğiz. Bu yapılandırmada, LAN istemcilerinin internet erişimi için kendi kullanıcı hesaplarıyla oturum açmaları gerekir. Yönetici farklı kullanıcı hesapları için farklı kurallar koyabilir. Örneğin, Facebook'u çalışanların çoğundan yasaklamak için bir kural oluşturabiliriz; Öte yandan, HR hesapları olan kullanıcılar internete herhangi bir sınırlama olmaksızın erişebilir.



Burada VigorAP Radius sunucusu olarak kullanılıyor.

RADIUS Sunucuda (VigorAP)

1. RADIUS Setting >> RADIUS sunucusundan RADIUS Server'i enable yapınız.
2. Kullanıcı Profili Oluştur:: Username ve password yazıp hesabı oluşturmak için Add butonuna tıklayınız.
3. Kimlik Doğrulama Kullanıcısı Ayarlama: Authentication Client , 802.1X kimlik doğrulama paketlerini VigorAP'ye gönderme iznine sahip ana bilgisayarlardır.Client IP ve Secret Key yazın ve ardından yeni bir istemci eklemek için Add butonuna tıklayınız.

RADIUS Setting >> RADIUS Server Configuration

 Enable RADIUS Server

Authentication Type

Radius EAP Type PEAP ▾

Users Profile (up to 96 users)

Username	Password	Confirm Password	Configure
HR	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Username		Select
1	employee		<input type="checkbox"/>
2	HR		<input type="checkbox"/>

Authentication Client (up to 16 clients)

Client IP	Secret Key	Confirm Secret Key	Configure
192.168.2.1	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Client IP		Select
1	192.168.2.1		<input type="checkbox"/>

VigorRouter'de;

1. User Management >> User Profile sayfasına gidin ve User based Mode'u enable yapın.

User Management >> General Setup

General Setup

Mode Selection:

- Rule-Based** is a management method based on IP address. Administrator may set different firewall rules to different IP address.
- User-Based** is a management method based on user profiles. Administrator may set different firewall rules to different user profiles.

Notice for User-Based mode:

- In User-Based mode, **Active Rules** in Firewall will be applied to all LAN clients, packets that matches the Active Rules will be blocked or pass immediately, no user authentication is required.
- Only **Inactive Rules** in Firewall can be set for individual user profile. In User-Based mode, packets that do not match Active Rules will need authentication, and the Inactive Rule applied to the specific user profile will then take effect.

2. Sunucu IP adresinden paketlerin geçmesine izin veren bir firewall filtresi ayarlayın: firewall >> Filter Setup'a gidin, Set 2'ye tıklayın, uygun bir kuralı tıklayın.

- Filtre Ruley'i etkinleştirmek için enable yapın.
- Bir Comments Girin.
- Yönü LAN / DMZ / RT / VPN -> WAN olarak ayarlayın.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

<input checked="" type="checkbox"/> Enable	Server	
Comments	None	None
Schedule Profile	None	None
	<input type="checkbox"/> Clear sessions when schedule is ON	
Direction	LAN/DMZ/RT/VPN -> WAN	Advanced
Source IP/Country	192.168.2.2	Edit
Destination IP/Country	Any	Edit
Service Type	Any	Edit
Fragments	Don't Care	
Application	Action/Profile	Syslog
Filter	Pass Immediately	<input type="checkbox"/>
Branch to Other Filter Set	None	<input type="checkbox"/>
Sessions Control	0 / 50000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	None	<input type="checkbox"/>
Advance Setting	Edit	

OK

Clear

Cancel

- Hedef IP'yi sunucu IP'si olarak ayarlamak için Edit'e tıklayın.

IP Address Edit

Address Type	Single Address
Start IP Address	192.168.2.2
End IP Address	0.0.0.0
Subnet Mask	255.255.255.254 / 31
Invert Selection	<input type="checkbox"/>
IP Group	None
IP Object	None
IPv6 Group	None
IPv6 Object	None
Country Object	None

OK

Close

- a. a) Address Type'dan Single Address'i seçin.
 - b) Start IP Address'i olarak Server IP'yi girin
 - c)Click'e tıkla ve kaydet.
- b. Pass Immediately olarak filtreyi seçin.
- c. Click'e tıklayıp kaydedin.

Not: Filter Rule'yi etkinleştirmek için Enable kontrolü yaparak bu kuralı Active Rule yaparsak, bu tüm paketin kuralla eşleşip eşleşmediğini kontrol edeceği anlamına gelir. Ancak bu IP yapılandırmasında yalnızca sunucunun IP adresinden gelen paketler geçecek, IP adresiyle eşleşmeyen diğer paketler kimlik doğrulamaya ihtiyaç duyacak ve karşılık gelen kullanıcı hesaplarına uygulanan firewall kuralı geçerli olacaktır.

4. Facebook'u engellemek için bir firewall kuralı ayarlayın: Firewall >> Filter Setup sayfasına gidin, Set 2 tıklayın ve ardından uygun bir kurala tıklayın.

- a. Comments'lere Girin.
- b. Filtre için Pass Immediately'i seçin.

Facebook engelleme ayarlarını yapmak için URL Content Filter, Web Content Filter ve DNS Filter filtre ayarlarına gidin. Daha fazla ayrıntı için "Bir Web Sitesini URL İçerik Filtresi ve DNS Filtresi ile Engelleme" ve "Sosyal Ağ Sitelerini Web İçeriği Filtresi ile Engelleme" konu başlıklarına bakınız.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

<input type="checkbox"/> Enable		
Comments	block_facebook	
Schedule Profile	None	None
	None	None
	<input type="checkbox"/> Clear sessions when schedule is ON	
Direction	LAN/DMZ/RT/VPN -> WAN	Advanced
Source IP/Country	Any	Edit
Destination IP/Country	Any	Edit
Service Type	Any	Edit
Fragments	Don't Care	
Application	Action/Profile	Syslog
Filter	Pass Immediately	<input type="checkbox"/>
Branch to Other Filter Set	None	
Sessions Control	0 / 50000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	1-block fb	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
DNS Filter	1-block fb	<input type="checkbox"/>
Advance Setting	Edit	

OK

Clear

Cancel

d.OK'a tıkla ve kuralı kaydet.

Not: Filtre Kuralını Etkinleřtirmek iin Check'i iřaretlemeyin, bu kuralı Inactive Rule yapar, bu nedenle belirli bir kullanıcı hesabına uygulayabileceğimiz bir policy olacaktır.

4. alıřanlar iin bir kullanıcı hesabı oluřturun: User Management >> User Profile sayfasına gidin, bir hesap eklemek iin uygun bir profili tıklayın.

a.Bu hesabı etkinleřtirin.

b.User Name'i Radius server username ile aynı girin.

c.Radius'u sein.

d.Önceki adımda oluřturulan facebook engelleme politikasını Policy olarak ayarlayın.

Profile Index 4

Common Settings

<input checked="" type="checkbox"/> Enable this account	
Username	HR (Only support A-Z a-z 0-9 - . @)
Password	Max: 24 characters
Confirm Password	
External Server Authentication	Radius

Login Settings

User Online Status : Block/ Unblock

Allow Authentication via	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Alert Tool <input checked="" type="checkbox"/> Telnet
Show Landing Page After Login	<input type="checkbox"/>
Idle Timeout	10 min. (0: Unlimited)
Auto Logout After	0 min. (0: Off)
Pop up Time-Tracking Window	<input checked="" type="checkbox"/>
Login Permission Schedule	None, None, None, None

Policy

Max. Login Devices	0 (0: Unlimited)
Firewall Policy	Default
The available options are the rules created in Firewall >> Filter Setup but NOT enabled.	
<input type="checkbox"/> Enable Time Quota	0 min. - 0 +
<input type="checkbox"/> Enable Data Quota	0 MB - 0 +
<input type="checkbox"/> Reset Quota Automatically To	Time Limit 0 min. Data Limit 0 MB
When	<input checked="" type="radio"/> Login Permission Schedule Ends <input type="radio"/> Schedule None Starts

Other Services

Allow this profile to be used by	<input type="checkbox"/> Internal RADIUS <input type="checkbox"/> Local 802.1X
Log	None

OK

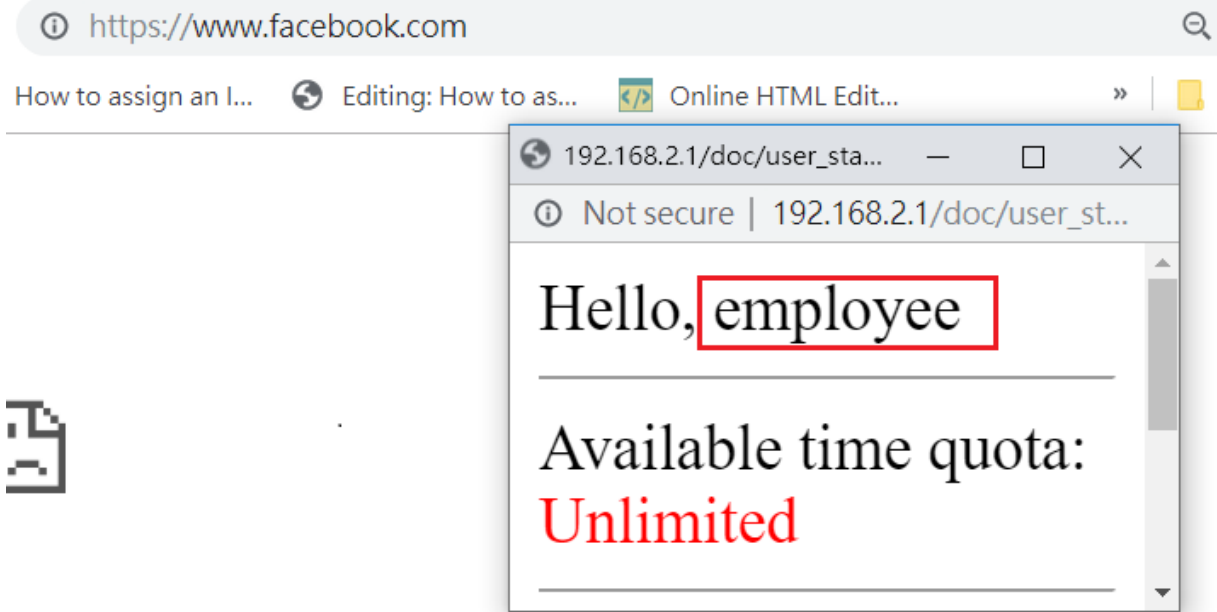
Refresh

Clear

Cancel

e.OK'a tıkla ve kaydet.

Son olarak ,LAN istemcileri internete erişmeye çalıştıklarında giriş yapmak zorunda kalacaklar.Çalışan hesabıyla giriş yaparlarsa , Facebook'a erişemezler.



This site can't be reached

The connection was reset.

Try:

HR hesabıyla giriş yaptığınızda ,Facebook sorunsuz çalışır.

