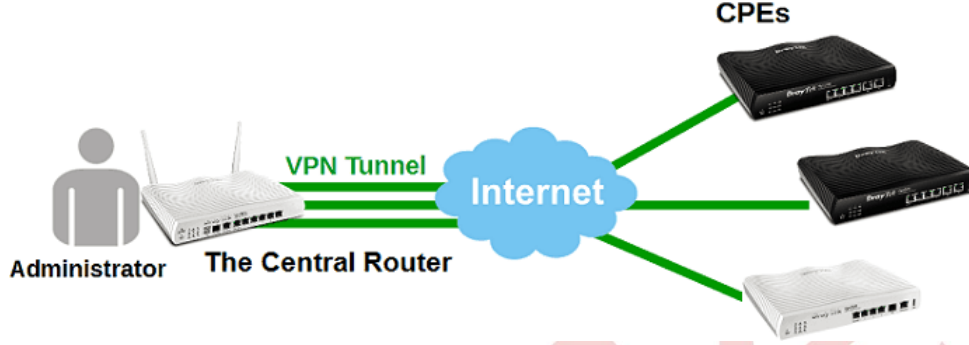


CENTRAL VPN MANAGEMENT (CVM) KULLANIMI

Merkezi VPN Yönetimi (CVM), birden fazla şube routerını VPN tünelleriyle merkezi bir routera bağlama özelliğidir ve Merkezi Yönlendiricideki Ağ Yöneticisinin 1. şubeye erişmesine izin verir. Tek bir tıklamayla VPN bağlantılarını kurma, 2. şube yedekleme ve geri yükleme, 3. şube Routerları için ürün yazılımı yükseltme gibi işlevleri sağlamaktadır.



DrayOS

CVM'nin çalışması için hem Merkezi Router'da (VPN sunucusu) hem de şube routerlarında (VPN İstemcileri) yapılandırmalar gerekir. DrayOS Router için merkezi bir router, 8'e kadar şube routerını yönetebilir.

<https://youtu.be/HNgrZXhk-yo> linkinden detaylarına bakabilirsiniz.

Merkezi Router Yapılandırma

1. **Central VPN Management >> General Setup** sayfasına gidin. General Settings sekmesinde,
 - a. **CVM SSL Port'u** etkinleştirin ve port numarası girin.
 - b. Remote Routera bağlanmak için **WAN interface/ IP** adresi girin.
 - c. ACS sunucusunun **URL'sini** yazın. Şube routerı yapılandırması için buna ihtiyacımız olacak.
 - d. (Not: https ve http içeren URL'ler sırasıyla CVM SSL Port ve CVM Port içindir.)
 - e. **Username** ve **Password** girin.

CVM >> General Setup

General Settings	IPsec VPN Settings
a.	<input checked="" type="checkbox"/> CVM SSL Port: 8443
	<input type="checkbox"/> CVM Port: 8000
b.	WAN IP for Remote Connection: WAN1 / 36.226.157.194
	Copy the following URL to paste onto Remote devices' ACS Server URL field
	"http://36.226.157.194:8000/ACSServer/services/ACSServlet"
c.	"https://36.226.157.194:8443/ACSServer/services/ACSServlet"
d.	Username: cvm
	Password:
	Polling Interval: 600 Seconds
	Note:
	1. To enable the CVM feature, one of the Port MUST be Enabled !
	2. If you choose to use CVM Port, the data between CVM Server & CPE Client will be transferred in plaintext, and could be revealed to ISP.

OK

2. IPsec sekmesine gidin. LAN-to-LAN VPN bağlantısı kurmak için **Local Subnet**'i seçin. Kaydetmek için **OK**'a tıklayın .

CVM >> General Setup

General Settings	IPsec VPN Settings
IPsec Mode:	Aggressive mode ▼
Security Method:	ESP ▼
Encryption Type:	AES ▼
Local Subnet:	LAN1 ▼
	192.168.92.2 / 255.255.255.0

OK

3. **System Maintenance >> Management** sayfasına gidin.CVM Port'un aktif olduğundan emin olun.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
Router Name	
<input checked="" type="checkbox"/> Default:Disable Auto-Logout	
Internet Access Control	Management Port Setup
<input checked="" type="checkbox"/> Allow management from the Internet	<input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports
Domain name allowed	Telnet Port 23 (Default: 23)
<input type="checkbox"/> FTP Server	HTTP Port 80 (Default: 80)
<input checked="" type="checkbox"/> HTTP Server	HTTPS Port 443 (Default: 443)
<input checked="" type="checkbox"/> HTTPS Server	FTP Port 21 (Default: 21)
<input checked="" type="checkbox"/> Telnet Server	TR069 Port 8069 (Default: 8069)
<input checked="" type="checkbox"/> TR069 Server	SSH Port 22 (Default: 22)
<input checked="" type="checkbox"/> SSH Server	
<input type="checkbox"/> Disable PING from the Internet	CVM Access Control
LAN Access Control	<input type="checkbox"/> CVM Port 8000 (Default: 8000)
	<input checked="" type="checkbox"/> CVM SSL Port 8443 (Default: 8443)

Şube Router (CPE) Yapılandırması

1. **System Maintenance >> TR-069** sayfasına gidin.
 - a. **Internet**'de ACS Server'ı seçin.
 - b. Merkezi routerdan kopyalanan ACS sunucusunun **URL**'sini girin .
 - c. Merkezi routerın CVM ayarlarında olduğu gibi **Username** ve **Password** girin.
 - d. **CPE Client**'ı etkinleştirin.
 - e. **Periodic Inform Settings** etkinleştirin.
 - f. Kaydetmek için **OK**'a tıklayın.

System Maintenance >> TR-069 Setting

ACS and CPE Settings

a. ACS Server On

ACS Server

b. URL

c. Username
Password

d. CPE Client Enable Disable

URL

Port

Username

Password

Periodic Inform Settings

e. Disable Enable

Interval Time second(s)

STUN Settings

Disable Enable

Server Address

Server Port

Minimum Keep Alive Period second(s)

Maximum Keep Alive Period second(s)

f.

System Maintenance >> Management sayfasına gidin. **Allow management from the Internet**'i işaretleyin ve **TR069 Server**'in işaretli olduğundan emin olun.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
Router Name <input type="text"/>	
<input checked="" type="checkbox"/> Default: Disable Auto-Logout	
Internet Access Control	
<input checked="" type="checkbox"/> Allow management from the Internet	
Domain name allowed <input type="text"/>	
<input type="checkbox"/> FTP Server	
<input checked="" type="checkbox"/> HTTP Server	
<input checked="" type="checkbox"/> HTTPS Server	
<input checked="" type="checkbox"/> Telnet Server	
<input checked="" type="checkbox"/> TR069 Server	
<input checked="" type="checkbox"/> SSH Server	
<input type="checkbox"/> Disable PING from the Internet	
Management Port Setup	
<input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports	
Telnet Port	<input type="text" value="23"/> (Default: 23)
HTTP Port	<input type="text" value="80"/> (Default: 80)
HTTPS Port	<input type="text" value="443"/> (Default: 443)
FTP Port	<input type="text" value="21"/> (Default: 21)
TR069 Port	<input type="text" value="8069"/> (Default: 8069)
SSH Port	<input type="text" value="22"/> (Default: 22)
CVM Access Control	
<input type="checkbox"/> CVM Port	<input type="text" value="8000"/> (Default: 8000)

Yukarıdaki konfigürasyondan sonra, şube raouterı Merkezi Router'a kaydolur ve Merkezi Router'ın Unmanaged Device List'inde görüldüğünü görmeliyiz.

Managed Device List'ini Düzenleme


Artık Merkezi Router, şube raouterını **Central VPN Management >> CPE Management >> Managed Devices List**'de görebilirsiniz. Routerı Managed Device List'e eklemek için,

- Unmanaged Devices List'den cihazı seçin.
- Description Adı** ve **Location** girin.
- Managed Devices List'e taşımak için **OK**'a tıklayın.

CVM >> CPE Management >> Managed Devices List

Managed Devices List CPE Maintenance Google Map Refresh

Managed Devices List



Chicago of...
192.168.1.11

Edit Delete

Unmanaged Devices List

	IP Address	Mac Address	Device Model	Description Name	Location
<input checked="" type="checkbox"/>	192.168.1.14	00:1D:AA:83:DC:B4	Vigor2912	LA office	Los Angeles
<input type="checkbox"/>	172.16.2.198	00:1D:AA:B3:85:B8	Vigor2925FVn		
<input type="checkbox"/>	192.168.1.12	00:50:7F:7B:83:18	Vigor3900		


Add

Bundan sonra router, adı ve IP adresiyle birlikte Managed Devices List'te görünecektir. Detaylı bilgileri kontrol etmek için üzerine çift tıklayın.

CVM >> CPE Management >> Managed Devices List

Managed Devices List CPE Maintenance Google Map Refresh

Managed Devices List



Chicago of...
192.168.1.11

LA office
192.168.1.14

NYC office
172.16.2.198

Houston of...
192.168.1.12

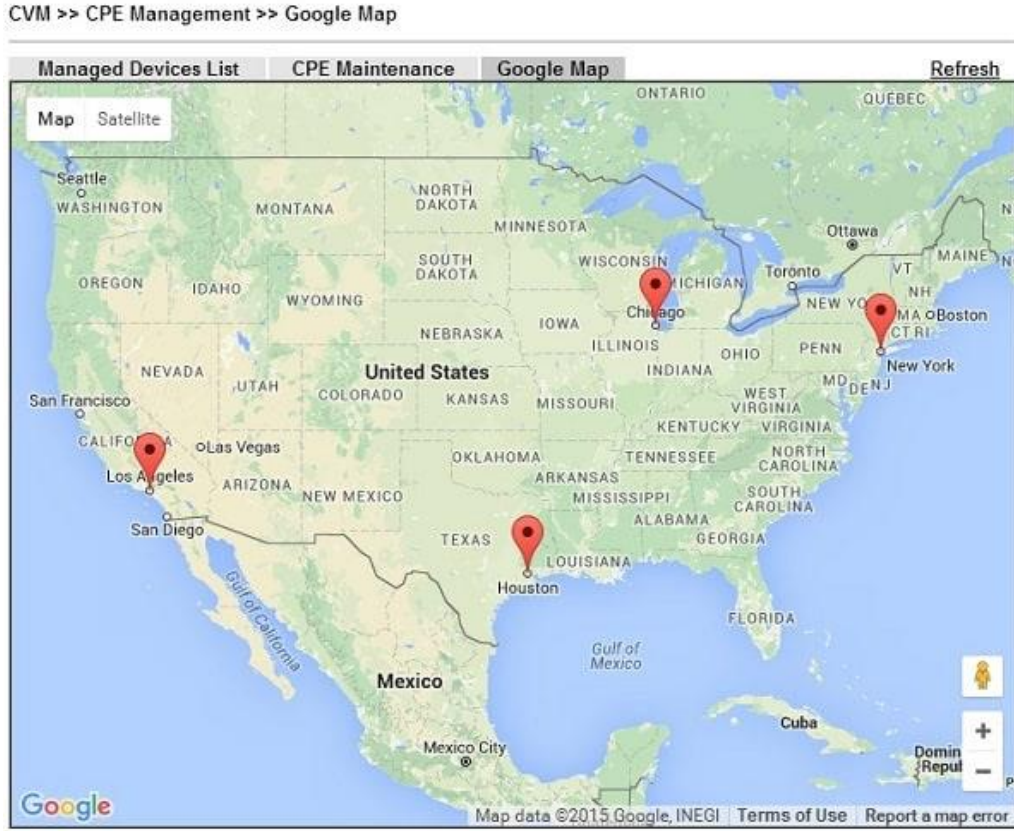
Edit Delete

Unmanaged Devices List

	IP Address	Mac Address	Device Model	Description Name	Location
--	------------	-------------	--------------	------------------	----------

Add

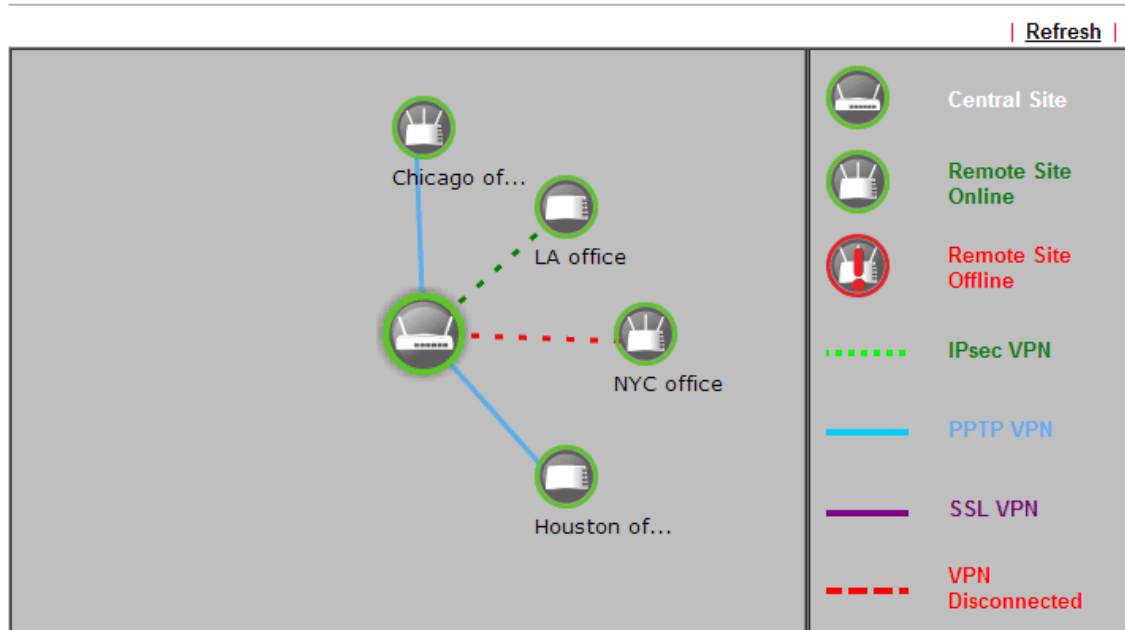
Tam adresi girdiyse, konumunu Google Map sekmesinden kontrol edebilirsiniz.



VPN Bağlantıları Kurmak

1. VPN bağlantısı kurmak için: **Central VPN Management >> VPN Management** sayfasına gidin. VPN Management sayfası, Managed Device List'te tüm cihazları ve bağlantı durumlarını gösterir.

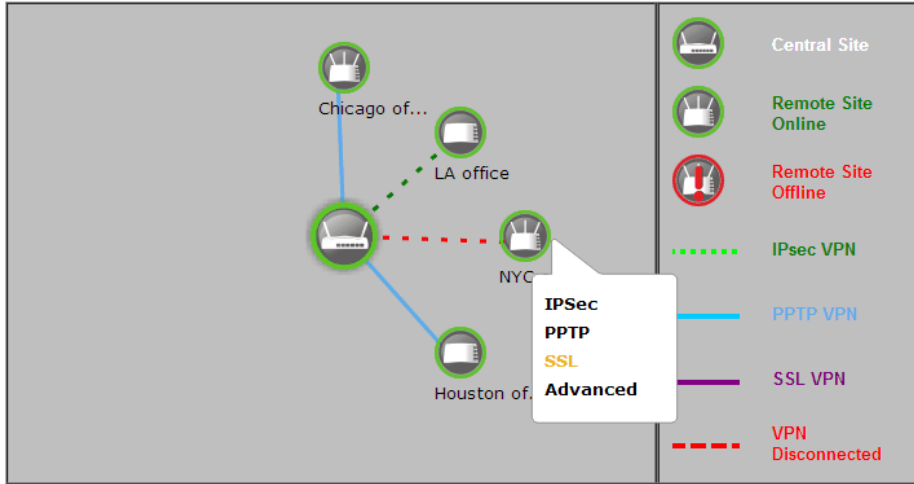
CVM >> VPN Management



Note: CVM SSL LAN-to-LAN dial-up might fail with the CPE of old version firmware. Please update the remote CPE to the latest version.

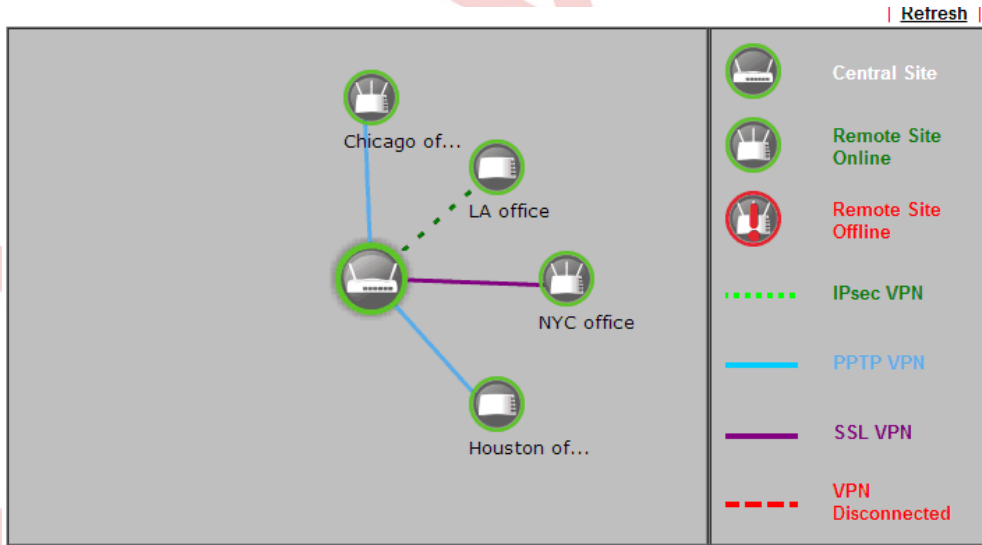
- VPN türü seçeneklerini göstermek için bir cihaza tıklayın, ardından VPN bağlantısını kurmak için seçeneklerden birine tıklayın. PPTP, IPsec ve SSL’de sistem otomatik olarak bir kullanıcı adı ve şifre verecektir; ancak, Yönetici “Advanced” i seçerek şifreleme yöntemlerini değiştirebilir.

CVM >> VPN Management



Note: CVM SSL LAN-to-LAN dial-up might fail with the CPE of old version firmware. Please update the remote CPE to the latest version.

- Birkaç saniye bekleyin ve sayfayı yenileyin, VPN bağlantısının açık olduğunu ve bağlantı bilgilerinin aşağıda CPE VPN Connection List ‘inde olduğunu göreceğiz.



Note: CVM SSL LAN-to-LAN dial-up might fail with the CPE of old version firmware. Please update the remote CPE to the latest version.

CPE VPN Connection List

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time
1 (cvm_83DCB4)	IPsec Tunnel AES-SHA1 Auth	111.231.100.132 via WAN2	192.168.29.1/24	0	0	1	3	0:23:24
2 (cvm_B385B8)	SSL Tunnel	111.231.100.132 via WAN-2	192.168.1.1/24	122	11	1	3	0:23:27
3 (cvm_84B47C)	PPTP/MPPE	111.231.144.110 via WAN2	192.168.200.1/24	0	0	135	21	0:23:22
4 (cvm_7B8318)	PPTP/MPPE	111.231.100.132 via WAN2	192.168.2.1/24	0	0	0	0	0:22:49

4. Bundan sonra, hem şube routerı hem de merkezi router, **VPN and Remote Access >> LAN to LAN** sayfasında LAN-to-LAN profili oluşturacak. **Network** Yöneticisi, orada VPN türünü de değiştirebilir ve ayarlar LAN-to-LAN profiline otomatik olarak uygulanır.

VPN and Remote Access >> LAN to LAN



LAN-to-LAN Profiles:

| [Set to Factory Default](#) |

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	cvm_83DCB4	<input checked="" type="checkbox"/>	Online	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	cvm_B385B8	<input checked="" type="checkbox"/>	Online	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	cvm_84B47C	<input checked="" type="checkbox"/>	Online	<u>19.</u>	???	<input type="checkbox"/>	---
<u>4.</u>	cvm_7B8318	<input checked="" type="checkbox"/>	Online	<u>20.</u>	???	<input type="checkbox"/>	---
<u>5.</u>	???	<input type="checkbox"/>	---	<u>21.</u>	???	<input type="checkbox"/>	---

Şube Router (CPE) Bakımı

Ağ Yöneticisi şube routerının yapılandırmasını günde bir kez yedeklemesini istiyorsa, merkezi routerdan CVM ile yapılabilir.

- Konfigürasyon yedeği için bir schedule oluşturun: **Application >> Schedule** sayfasına gidin Schedule eklemek için bir index numarasına tıklayın.
 - Enable Schedule Setup**'ı etkinleştirin.
 - Konfigürasyon yedeği için **Start Date** ve **Start Time** seçin.
 - Duration Time** için 5 dakika girin. (NOT: Daha uzun süre, şube routerının merkezi routerla olan bağlantıyı kaybetmesi durumunda routera daha fazla yeniden deneme süresi sağlar.)
 - Yapılandırma yedeklemesinin ne sıklıkla olacağını How Often'da seçin.

Applications >> Schedule

Index No. 1

a. Enable Schedule Setup

b. Start Date (yyyy-mm-dd) 2014 - 10 - 1

Start Time (hh:mm) 12 : 30

c. Duration Time (hh:mm) 0 : 5

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

Once

d. Weekdays



Sun Mon Tue Wed Thu Fri Sat

e.

- Central VPN Management >> CPE Management >> CPE Maintenance** sayfasına gidin, routera bağlı bir USB disk olduğundan emin olun.

CVM >> CPE Management >> CPE Maintenance

Managed Devices List | CPE Maintenance | Google Map | Refresh

USB Disk :  Disk Usage : 384MB / 1525MB 

| Set to Factory Default |

Index	Profile Name	Device Name	Action	File/Path	Schedule
1.					0 0 Now
2.					0 0 Now
3.					0 0 Now
4.					0 0 Now
5.					0 0 Now
6.					0 0 Now
7.					0 0 Now
8.					0 0 Now

<< 1-8 | 9-16 >>

Note: To enable the schedulings, an USB storage **MUST** be plugged onto router.

3. Bir CPE Bakım profili ekleyin: CPE Maintenance sayfasında, yeni bir profil eklemek için bir index numarasına tıklayın.
 - a. Profil adı girin.
 - b. **Enable**'ı işaretleyin.
 - c. **Device Name** için şube routerının **MAC Adresini** seçin.
 - d. Action Type için **Config Backup** seçin.
 - e. **Schedule profile**'a index girin.
 - f. Kaydetmek için **OK**'a tıklayın.

Central VPN Management >> CPE Management >> Maintenance Profile

Profile Name:

Enable

Device Name:

Router Name: NYC office

Router Model: Vigor2925FVn

Action Type:

File Name:

Index in **Schedule**:

Note: Action and Idle Timeout settings will be ignored.

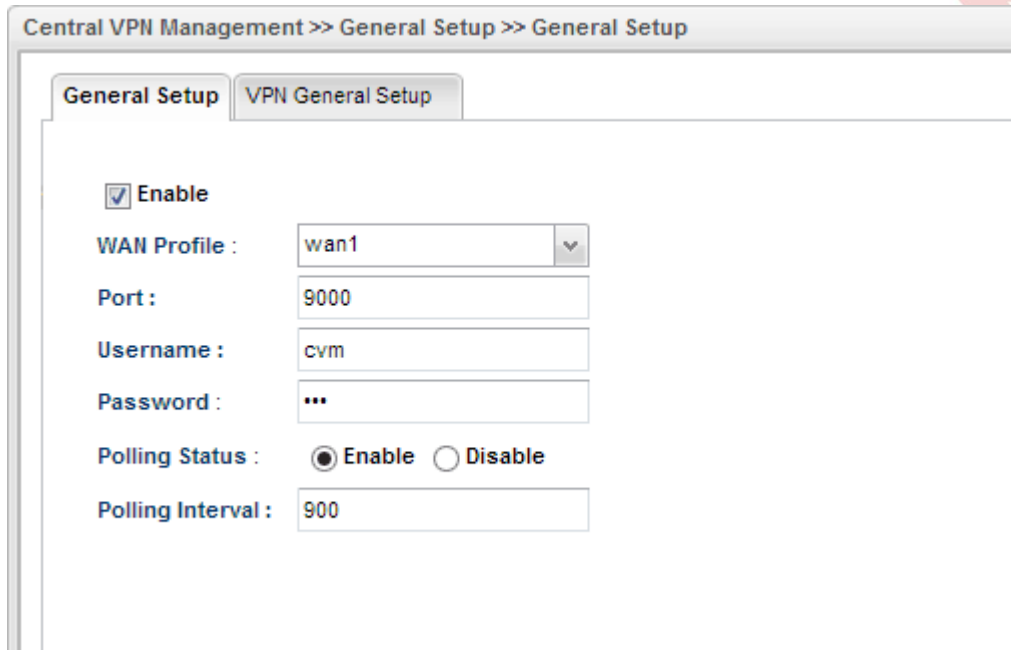
OK Clear Cancel

4. Yapılandırma yedeklemesinden sonra, yapılandırma dosyalarının başarılı bir şekilde kaydedilip kaydedilmediğini kontrol etmek için **USB Application >> File Explorer** sayfasına gidin .

Linux

CVM'nin çalışması için hem Merkezi Router'da (VPN sunucusu) hem de şube routerlarında (VPN İstemcileri) yapılandırmalar gerekir. Merkezi Router olarak Vigor2960, 12 routerı yönetebilir; Vigor3900, 16'ya kadar routerı yönetebilir.

1. **Central VPN Management >> General Setup >> General Setup** sayfasına gidin.
 - a. **Enable**'ı işaretleyin.
 - b. Remote routera bağlantısı için **WAN interface** seçin.
 - c. 0~65535 arasında **port number** girin. Örnekte 9000 kullanıyoruz.
 - d. **Username** ve **Password** girin. Şube router ayarlarında aynı kullanıcı adına ve şifreye ihtiyacımız olacak
 - e. **Apply**'a tıklayın.



Central VPN Management >> General Setup >> General Setup

General Setup | VPN General Setup

Enable

WAN Profile : wan1

Port : 9000

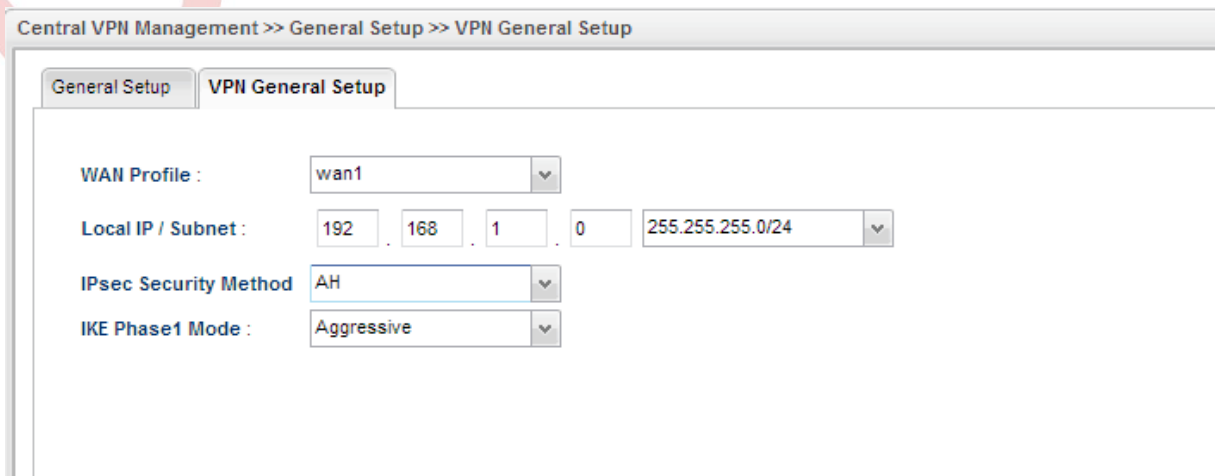
Username : cvm

Password : ***

Polling Status : Enable Disable

Polling Interval : 900

2. **Central VPN Management >> General Setup >> VPN General Setup** sayfasına gidin.
 - a. **WAN Profile** için wan1'i seçin.
 - b. Remote routera bağlantısı için **Local IP** ve **Subnet** girin.
 - c. **Apply**'a tıklayın.



Central VPN Management >> General Setup >> VPN General Setup

General Setup | VPN General Setup

WAN Profile : wan1

Local IP / Subnet : 192 . 168 . 1 . 0 255.255.255.0/24

IPsec Security Method : AH

IKE Phase1 Mode : Aggressive

3. "Web Allow," "Telnet Allow," "SSH Allow," and "HTTPS Allow" etkinleştirmek için **System Maintenance >> Access Control** sayfasına gidin.

System Maintenance >> Access Control >> Access Control

Access Control | Fail to Ban | Access Barrier

Customized Login Image : Enable Disable

Enforce HTTPS Management : Enable Disable

Internet Access Control

Apply to WAN Interface : wan1, wan2, wan3... X

Web Allow : Enable Disable

Telnet Allow : Enable Disable

SSH Allow : Enable Disable

HTTPS Allow : Enable Disable

SSL Proxy Allow : Enable Disable

FTP Allow : Enable Disable

SAMBA Allow : Enable Disable

TR069 Allow : Enable Disable

Access List : Enable Disable

4. Şube routerını merkezi routera kayıt olacak şekilde yapılandırma (Lütfen bu makalenin DrayOS bölümüne bakın)

Şube Router (CPE) Yönetimi

5. **Central VPN Management >> CPE Management**'a gidin. Şube routerının görülmesi, yukarıdaki tüm ayarların doğru olduğu anlamına gelir. Routerı seçin ve **Edit**'e tıklayın.

Central VPN Management >> CPE Management >> CPE Maintenance

CPE Maintenance | VPN Management | Map

Managed Devices Status

Edit | Detail | Delete | Refresh | Recycle Bin | Total number of devices: : 1

DrayTek_00507F_...

Maintenance

Add | Edit | Delete | Refresh | File Explorer

Profile	Device	Name	Action	Schedule	Weekdays	Filename	Status
---------	--------	------	--------	----------	----------	----------	--------

6. Şube router ile ilgili ayrıntılı bilgileri, iletişim kutusu içinde adı ve konumu gibi görünen iletişim kutusuna girebiliriz.

Edit Device

Model Name : Vigor3200

Device Name : DrayTek_00507F_Vigor_00507F741171

Name : Vigor3200

Manufacturer : DrayTek

OUI : 00507F

Product Class : Vigor

Mac Address : 00507F741171

Location : Germany

Latlng : 51.165691,10.451526

IP : 118.160.97.218

Port : 8069

URI : /cwm/CRN.html

Description : DrayTek Vigor Router

Hardware Version : 142

Software Version : 3.6.3

Modem Firmware Version : No DSL

Apply Cancel

7. VPN ağı kurmak için **Central VPN Management** >> **CPE Management** >> **VPN Management**'a gidin.
 - a. Bir şube routeri seçin.
 - b. VPN tipini tıklayın, burada PPTP kullanıyoruz.
 - c. VPN tüneli oluşturmak istendiğinde **OK'a** tıklayın .

Central VPN Management >> CPE Management >> VPN Management

CPE Maintenance VPN Management Map

PPTP IPsec Advanced Refresh

Keep VPN Settings

Add Delete Refresh

Profile	Device	Name
No items to show.		

Confirm

Are you sure establishing a PPTP tunnel with DrayTek_00507F_Vigor_00507F741171?

OK Cancel

8. Birkaç saniye bekleyin, VPN bağlantısı kurulduğunu görelim.

Central VPN Management >> CPE Management >> VPN Management

CPE Maintenance VPN Management Map

PPTP PPTP IPsec IPsec Advanced Refresh

Vigor3200

Keep VPN Settings

Add Delete Refresh

Profile	Device	Name
No items to show.		

Connected Devices Refresh

VPN	Type	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect	
1	CVM_7A02E8	PPTP/MPPE	117.170.77.71	192.168.40.0/24	00:02:48	2	0	Disconnect

Şube Router (CPE) Bakımı

1. CVM ile, yedekleme ve geri yükleme yapılandırılmaları gibi merkezi routerdan, router bakımı da yapabiliriz. Şube Router Bakımı yapmak için **Central VPN Management >> CPE Management >> CPE Maintenance**'a gidin, şube routerına tıklayın ve **Add**'e tıklayın .
2. Profil adı yazın, şube routerını seçin, **Action** seçin (burada Configuration Backup'ı seçiyoruz), **Schedule**'da action zamanını ayarlayın (burada Şimdi kullanıyoruz) ve **Filename** adını yazın .

Maintenance

Profile : Vigor3200

Device : DrayTek_00507F_Vigor_0

Name : Vigor3200(117.170.77.71)

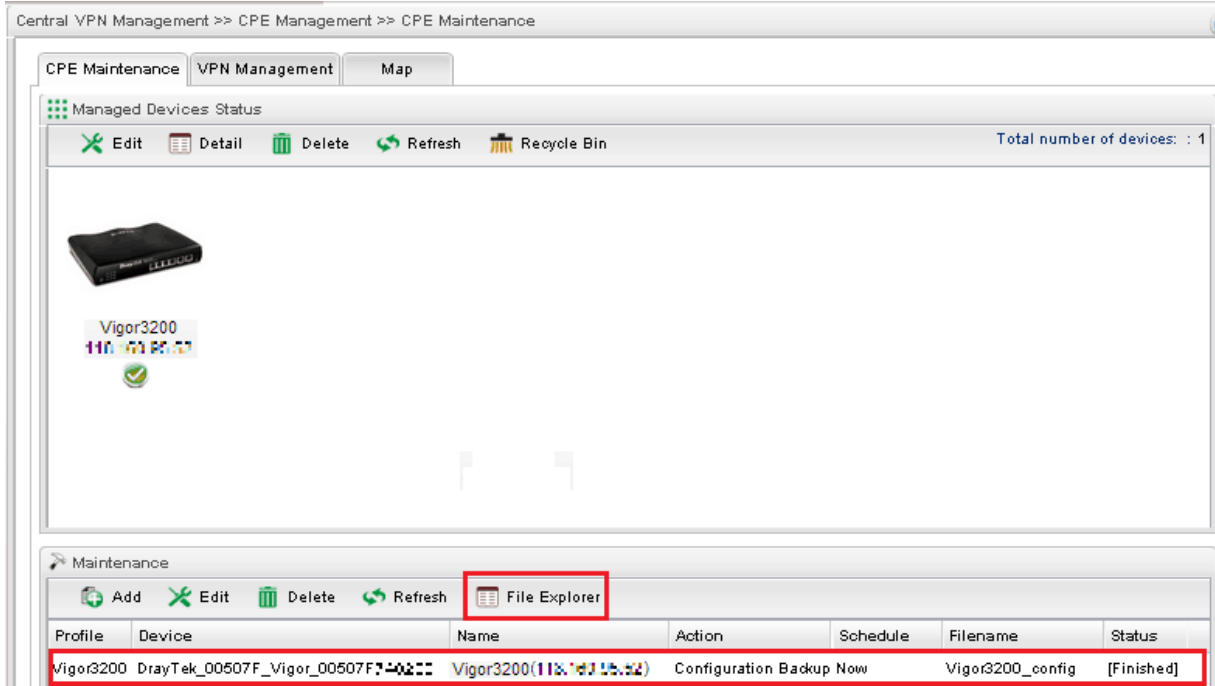
Action : Configuration Backup

Schedule : Now

Filename : Vigor3200_config

Apply Cancel

3. Birkaç saniye bekleyin ve sayfayı yenileyin. Status [Son], yapılandırmanın routera başarıyla kaydedildiğini gösterir. Merkezi routerda yaklaşık 800 Mbyte depolama alanı olacaktır.



1. Konfigürasyonu File Explorer ile bilgisayarlarımıza da indirebiliriz. Dosya adını seçin ve Download'ı tıklayın.

