



macOS'TAN VIGOR ROUTER'A SSL VPN

Bu makale Vigor Router'ın internet istemcileri, özellikle macOS'un bir SSL VPN tüneli tarafından yerel ağa erişmesine izin vermek için SSL VPN ağ geçidi olarak nasıl ayarlanacağını göstermektedir. Makalede router için gereken yapılandırmanın yanı sıra DrayTek tarafından sağlanan ücretsiz VPN istemci uygulaması olan Smart VPN'i kullanarak bir mac'tan SSL VPN bağlantısının nasıl başlatılacağını gösteriyoruz.

Vigor Router Üzerinde Kurulum

DrayOS

- 1. Routerın internet bağlı olduğundan ve internetteki VPN istemcilerinin erişebilmesi için prtak bir WAN IP adresine sahip olduğundan emin olun.
- 2. VPN and Remote Access >> Remote Access Control sayfasında "SSL VPN Service" nin etkin olduğundan emin olun.

Remote Access Control Setup		
V	Enable PPTP VPN Service	
	Enable IPSec VPN Service	•
	Enable L2TP VPN Service	
	Enable SSL VPN Service	

- 3. SSL VPN istemcisi için kullanıcı profili oluşturun. **VPN and Remote Access** >> **Remote Dial-in User** sayfasına gidin. Aşağıdaki adımları takip ederek bir profil oluşturun.
 - Allowed Dial-In Type için "SSL Tunnel" işaretleyin.

VPN and Remote Access >> Remote Access Control Setup

- Username ve Password girin.
- Profili kaydetmek için OK'a tıklayın.

VPN and Remote Access >> Remote Dial-in User

Index No. 5	
User account and Authentication Enable this account Idle Timeout 0 second(s)	Username SSLuser Password(Max 19 char) ······· Enable Mobile One-Time Passwords(mOTP)
Allowed Dial-In Type PPTP IPsec Tunnel L2TP with IPsec Policy None SSL Tunnel Specify Remote Node	PIN Code Secret IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509)
Remote Client IP Or Peer ID Netbios Naming Packet Multicast via VPN Pass Block (for some IGMP,IP-Camera,DHCP Relayetc.)	None ↓ IPsec Security Method ✓ ✓ Medium(AH) High(ESP) ✓ Josef 3DES Local ID (optional)
Subnet LAN 1 Assign Static IP Address 0.0.0.0	





Linux

- 1. Routerın internet bağlı olduğundan ve internetteki VPN istemcilerinin erişebilmesi için prtak bir WAN IP adresine sahip olduğundan emin olun.
- 2. VPN and Remote Access >> Remote Access Control sayfasında "SSL VPN Service" nin etkin olduğundan emin olun.

VPN and Remote Access >> Remote Access Control	
Remole Access Control	
Enable PPTP VPN Service	
Enable L2TP VPN Service	
Enable SSL Tunnel Service (While SSL VPN Port is equal to HTTPS Management Port, please ensure HTTPS Allow is set as Enable via System Maintenance >>Access Control.) Enable OpenVPN Service (OpenVPN will create interface tun0(udp) & tun1(tcp) automatically when service is enabled.)	/
C Enable IPsec Service	
IPsec Remote Dial-In Service : None L2TP over IPsec DHCP over IPsec	

3. SSL VPN ile HTTPS portları aynı ise **System Maintenance** >> **Access Control**'de HTTPS Allow'un etkinleştirildiğinden emin olun.

Access Control			
✓ Internet Access Contr	01		
Web Allow :	🔘 Enable 🛞 Di	sable	
Teinet Allow :	🔘 Enable 🛞 Di	sable	
SSH Allow :	💮 Enable 💿 Di	sable	
HTTPS Allow :	🛞 Enable 🔘 Di	sable	
FTP Allow :	🔘 Enable 🛞 Di	sable	
Server Certificate	Default	×	

- 4. SSL VPN istemcileri için kullanıcı profili oluşturun. User Management >> User Profile 'a gidin ve Add'e tıklayın.
 - **Enable**'i işaretleyin.
 - Username ve Password girin
 - PPTP/L2TP SSL Server'da **SSL Tunnel** için "Enable" seçeneğini seçin.
 - Profili kaydetmek için **Apply**'a tıklayın.





			Use	er Profile			X	T
Us	er Pr	ofile						
٩	Add	×		Username : Enable	dray			
		Ena		Password :	••••	Strength : Weak		
1		true		System User :	true 👻			
2	v	true		Painting Laurely	Adapta	1		
3	хр	true		Privilege Level :	Admin			
4	b	true						
5		true		Idle Timeout(sec) :	300]		
6		true		DHCP from	lan1 v			
7	t	true					=	
8		true		Static IP Address :	(9	Optional)		
9	nl	true		^				
10		true		~				
11		true						
12		true		PPTP Dial-in :	🔵 Enable 💿 Disable			
13		true		L2TP Dial-in :	🔵 Enable 📀 Disable			
			1	SSL Tunnel :	💿 Enable 🔵 Disable			
			11	Use mOTP :	🔵 Enable 💿 Disable			
				Remote IP/Host Name	ə :	(Optional)		
				^				
				^			-	
			14					

macOS'ta VPN Kurulumu

1. Mac SmartVPN'i başlatın. Ayarlar simgesine tıklayın ve Certificate Verify Level için "Basic" seçeneğini seçin.

		Smart VPN		
	Certificate verify level :	Basic		
		Cancel	ОК	
	User Na	me: Required		
		Authentication	Settings	
		Connect		
+			Advanced	
	Dr	ay Tek	Restore Apply	
-		_	_	





- 2. VPN profili oluşturmak için '+'ya tıklayın.
 - Profil adı verin.
 - Server'da Vigor Router'ın IP ya da domain adını girin.
 - Varsayılan olarak 443 olan SSL VPN portunu yazın.
 - Username yazın.
 - Authentication Settings'e tıklayın.

	-	Smart VPN
	Create a new Smart V	/PN profile:
	Profile:	SSLVPN
	Server:	Draytek.sslvpn.com
	Port:	443
	User name:	dray
		Authentication Settings
+ - 0		Advanced
	Ľ	DrayTek Restore Apply

3. User Authentication için "Password" u seçin ve şifreyi yazın. Ardından OK'a tıklayın.

User Authentication: O Password: ••••
mote Generate Secret
PIN:
 Cancel Create
 Advanced
 DrayTek Restore Apply





4. Connect'e tıklayın ve gerekli bilgilere erişime izin verin.

	Smart	VPN
SSLVPN	Profile: Server: Port: User Name:	SSLVPN Draytek.sslvpn.com 443 dray Authentication Settings Connect
+		Advanced
	Dray	Tek Restore Apply







5. VPN'den sonra bunun gibi bağlantı istatistiklerini görebiliriz.

G SSLVPN	Profile	COLVON	
	Profile.	SSLVPN	
	Server:	Draytek.sslvpn.co	m
	Port:	443	
	User Name:	dray	
		Authentication S	ettings
		Disconnect	
	IP Address:	192.168.22.12	
	Connection time:	0:01:08	
	Sent:	2 KB/35	
	Received:	807 bytes/22	
+			Advanced
		-T.1	Destare Apply

