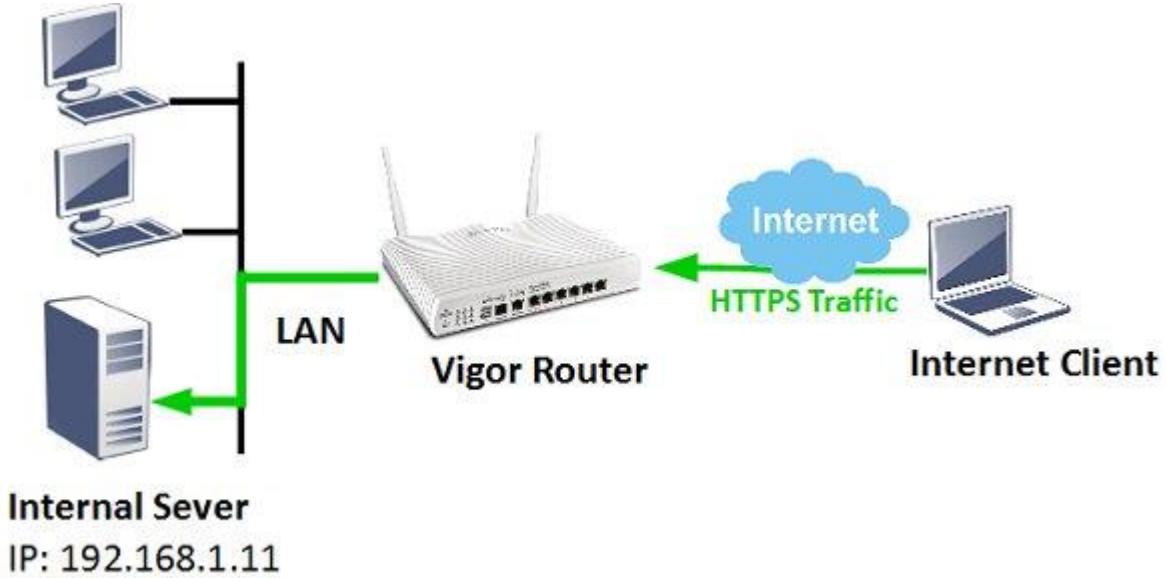


HTTPS İsteklerini Dahili Sunucuya Yönlendirme

VigorRouter, WAN'daki bağlantı isteklerini LAN üzerindeki dahili bir sunucuya yönlendirmek için Port Redirection ve Open Ports gibi NAT ayarları sağlar. Bununla birlikte, 443 numaralı TCP portunu kullanan HTTPS isteklerine gelince, yalnızca NAT kurulumuna değil, Router'ın HTTPS ve SSL VPN servis portunu da değiştirmemiz gerekir, çünkü bu işlevler varsayılan olarak 443 numaralı TCP portunu da dinler ve NAT ayarlarından daha yüksek önceliğe sahiptir. Bu makalede, HTTPS isteklerinin dahili bir sunucuya nasıl yönlendirileceği gösterilmektedir.



1. HTTPS yönetimi için portunu değiştirin: System Maintenance >> Management'e gidin, HTTP Portunu 443'ten başka bir numarayla değiştirin, sonra uygulamak için OK'a tıklayın.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
Router Name: DrayTek <input type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access 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 type="checkbox"/> SSH Server	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port: 23 (Default: 23) HTTP Port: 80 (Default: 80) HTTPS Port: 4433 (Default: 443) FTP Port: 21 (Default: 21) TR069 Port: 8069 (Default: 8069) SSH Port: 22 (Default: 22) Brute Force Protection <input type="checkbox"/> Enable brute force login protection <input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server

2. SSL VPN işlevi için portunu değiştirin: SSL VPN >> **General Setup**'a gidin, portunu 443'ten başka bir numarayla değiştirin, sonra uygulamak için OK'a tıklayın. (SSL VPN'i desteklemeyen modellerde, bu adımı atlayabilirsiniz.)

SSL VPN >> General Setup

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> WAN4
Port	4433 (Default: 443)			
Server Certificate	self-signed ▼			

Note:

1. The settings will act on all SSL applications.
2. Please go to **System Maintenance >> Self-Signed Certificate** to generate a new "self-signed" certificate.

OK Cancel

3. Şimdi Port Redirection için TCP portunu kullanabilirsiniz. NAT >> Port Redirection bölümüne gidin, uygun bir indexe tıklayın.

NAT >> Port Redirection

Port Redirection							Set to Factory Default
Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status	
1.		All				x	
2.		All				x	
3.		All				x	

4. Profili etkinleştirin ve profili aşağıdaki gibi yapılandırın, sonra uygulamak için OK'a tıklayın.

- Mode: Single
- Protocol: TCP
- Public Port: 443
- Private IP: Internal serverin IP adresi.
- Private Port: 443

NAT >> Port Redirection

Index No. 1

<input checked="" type="checkbox"/> Enable	
Mode	Single ▼
Service Name	HTTPS
Protocol	TCP ▼
WAN Interface	ALL ▼
Public Port	443
Private IP	192.168.1.11
Private Port	443

Şimdi, Router'in WAN arayüzüne gönderilen HTTPS istekleri olduğunda, dahili sunucuya yönlendirilecek.