

## Ağ Güvenliğini Artırma Yolları

Bu makalede, yetkisiz kullanıcıların nasıl engelleneceği ve yerel ağın İnternet üzerindeki tehditlerden nasıl korunacağı da dahil olmak üzere, ağı güvende tutmak için VigorRouter'ınızda yapabileceğiniz bazı korumalar tanıtılmaktadır. **Router Güvenlik Koruması**

### Varsayılan yönetici şifresini değiştirin

Piyasadaki Router'lerin birçoğu, yönetim sayfası girişleri için aynı varsayılan şifreyi kullanır; Böylece, Router'inizin giriş şifresini tahmin etmek son derece kolaydır. Router'inizin giriş şifresini System Maintenance >> Administrator Password sayfasından değiştirdiğinizden ve ayrıca yeterince güçlü bir şifre kullandığınızdan emin olun.

#### System Maintenance >> Administrator Password Setup

##### Administrator Password

Old Password	****	
New Password	*****	(Max. 23 characters allowed)
Confirm Password	*****	(Max. 23 characters allowed)

##### Note:

Password can contain only a-z A-Z 0-9 , ; : . " < > \* + = | ? @ # ^ ! ( )

**Yönetim portunu değiştirin** Varsayılan olarak, VigorRouter, web arayüzü, komut satırı arayüzü ve diğer hizmetler için iyi bilinen portları kullanır.

Bu nedenle, LAN istemcileri, Router'in IP adresini öğrendikleri sürece Router'in yönetim sayfasına kolayca erişebilirler. Servis portunu değiştirmek, giriş sayfasına erişmeyi biraz zorlaştıracaktır, bunu System Maintenance >> Management sayfasında yapılandırabilirsiniz.

#### System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup
Router Name: DrayTek		
<input checked="" type="checkbox"/> Default: Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access		
<b>Internet Access Control</b> <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed:		
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server		
		<b>Management Port Setup</b> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports
		Telnet Port: 23 (Default: 23)
		HTTP Port: 8001 (Default: 80)
		HTTPS Port: 443 (Default: 443)
		FTP Port: 21 (Default: 21)
		TR069 Port: 8069 (Default: 8069)
		SSH Port: 22 (Default: 22)

**Brute Force Korumasını Etkinleştir** Oturum açma sayfasına giriş yaptıktan sonra, giriş şifresi olmasa bile, saldırgan zaman geçse de doğru giriş şifresi bulunana kadar her olası şifreyi deneyebilir. Brute Force Protection'ı etkinleştirmek, VigorRouter'ın giriş yaparken çok fazla başarısız olan IP adresini tanımlamasını ve bir ceza süresi boyunca giriş yapma girişimlerini engellemesini sağlar ve doğru şifreyi bulmak için gereken süreyi önemli ölçüde artıracaktır.

System Maintenance &gt;&gt; Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup															
Router Name: DrayTek																	
<input checked="" type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access																	
<b>Internet Access Control</b> <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed: <input type="text"/>																	
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet																	
<b>Access List from the Internet</b> <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td></td><td></td></tr> <tr><td>2</td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td></tr> </tbody> </table>			List	index in IP Object	IP / Mask	1			2			3			4		
List	index in IP Object	IP / Mask															
1																	
2																	
3																	
4																	
<b>Management Port Setup</b> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports																	
Telnet Port: 23 (Default: 23)																	
HTTP Port: 8001 (Default: 80)																	
HTTPS Port: 443 (Default: 443)																	
FTP Port: 21 (Default: 21)																	
TR069 Port: 8069 (Default: 8069)																	
SSH Port: 22 (Default: 22)																	
<b>Brute Force Protection</b> <input checked="" type="checkbox"/> Enable brute force login protection																	
<input checked="" 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																	
Maximum login failures: 3 times																	
Penalty period: 60 seconds																	
Blocked IP List																	

### Yönetim Erişimi için Erişim Listesi'ni Ayarlama

Router'ın seçilen bir IP address / subnet erişimini yalnızca erişim listesine ekleyerek sınırlayabilirsiniz. İnternet üzerinden yönetime izin verildiğinde, Access List şiddetle önerilir.

System Maintenance &gt;&gt; Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup												
Router Name: DrayTek														
<input checked="" type="checkbox"/> Default:Disable Auto-Logout <input type="checkbox"/> Enable Validation Code in Internet/LAN Access														
<b>Internet Access Control</b> <input checked="" type="checkbox"/> Allow management from the Internet Domain name allowed: <input type="text"/>														
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access <input checked="" type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet														
<b>Access List from the Internet</b> <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td>1</td><td>104.25.235.112/255.255.255.255</td></tr> <tr><td>2</td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td></tr> </tbody> </table>			List	index in IP Object	IP / Mask	1	1	104.25.235.112/255.255.255.255	2			3		
List	index in IP Object	IP / Mask												
1	1	104.25.235.112/255.255.255.255												
2														
3														
<b>Management Port Setup</b> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports														
Telnet Port: 23 (Default: 23)														
HTTP Port: 80 (Default: 80)														
HTTPS Port: 443 (Default: 443)														
FTP Port: 21 (Default: 21)														
TR069 Port: 8069 (Default: 8069)														
SSH Port: 22 (Default: 22)														
<b>Brute Force Protection</b> <input type="checkbox"/> Enable brute force login protection														
<input type="checkbox"/> FTP Server <input type="checkbox"/> HTTP Server <input type="checkbox"/> HTTPS Server <input type="checkbox"/> Telnet Server <input type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server														
Maximum login failures: 0 times														
Penalty period: 0 seconds														

### Local Network Güvenliği

**Konuklar için VLAN uygulamak** Local Network'de VLAN'ı ayarlamak, onlara internet bağlantısı sağlarken konuğu özel ağdan izole etmenize olanak tanır. Ayrıca, birden fazla subnet desteği, özel ağın ve konuk ağının farklı IP Subnet'lerinde olmasına ve ayrı DHCP ayarları veya Policy'lerine sahip olmasına izin verir.

Ağda VLAN özellikli bir Switch'iniz varsa, VigorRouter'da VLAN'ı ayarlamak için Tag-Based VLAN ile Multiple LAN Subnets kullanma kılavuzunu takip edebilirsiniz. VigorAP'ın multi-SSID'si de farklı VLAN'larla eşlenebilir, daha fazla bilgi için bkz. "Konuklar için Ayrı Bir Kablosuz Ağ Ekleme". VLAN özellikli bir switch veya AP yoksa, VigorRouter port-based VLAN da yapabilir, talimat için "Port LAN VLAN ile Birden Çok LAN Subnets Kullan"ı ziyaret edin.

### DHCP Sunucusunu Devre Dışı Bırakın ve LAN IP'sini Değiştirin

Bir cihazın Router ile iletişim kurması için Router ile aynı subnette bir IP adresi kullanması gerekir. DHCP işlevi etkinken, Router ağa bağlı cihaza otomatik olarak geçerli bir IP adresi atar. Yetkisiz hostların ağa erişmesini istemiyorsanız, DHCP sunucusunu devre dışı bırakabilir ve IP'yi yetkili hostlarda el ile yapılandırabilirsiniz. Ayrıca LAN IP aralığını da değiştirmek isteyebilirsiniz, bu nedenle yetkili olmayan hostların IP aralığını bulması daha zordur. IP ve DHCP ayarları LAN >> General Setup >> LAN1 Details Page'de yapılandırılabilir.

#### LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
<b>Network Configuration</b> For NAT Usage IP Address: 192.168.98.1 Subnet Mask: 255.255.255.0 LAN IP Alias RIP Protocol Control: Disable	<b>DHCP Server Configuration</b> Agent <input checked="" type="radio"/> Disable <input type="radio"/> Enable Server <input type="radio"/> Enable Relay DNS Server IP Address Primary IP Address Secondary IP Address

Note: Change IP Address or Subnet Mask in Network Configuration will also change **HA** LAN1 Virtual IP to the same domain IP.

### Switch'ler de Kullanılmayan Portları Kapatın

Açık bir Ethernet portu, sahte cihazların özel ağa erişimine neden olur; bu nedenle, kullanılmayan portları Switch yapılandırmasın da devre dışı bırakın. VigorSwitches ile birlikte SWM'yi (Merkezi Anahtar Yönetimi) destekleyen bir VigorRouter kullanıyorsanız, Switch'in port durumunu Router'ın yönetim sayfasından görüntüleyebilir ve kullanılmayan bir portu doğrudan kapatabilirsiniz.

Central Management >> Switch >> Status

Switch Status Switch Hierarchy Refresh

VigorSwitch P1100  
192.168.193.250  
Switch

VigorSwitch G1241  
192.168.193.16  
Switch

Port : 9  
Description :  
IP Address : 192.168.193.12  
MAC Address : 08:00:27:00:00:0A  
 Shutdown Port OK

### Kablosuz Ağ Güvenliği WPA2 güvenlik modunu kullanın

Kablosuz trafik yayın ile gönderildiği için yakınlardaki herhangi biri tarafından gizlice dinlenebilir; bu nedenle, trafiği şifrelemek ve yerel ağa erişimi kontrol etmek için güvenlik ayarları uyguladığımızdan emin olun. WEP, WPA ve WPA2 arasında, WPA2 en güçlü güvenlik protokolüdür ve kullanmanızı öneririz.

### Wireless LAN(2.4GHz) >> Security Settings

SSID 1 SSID 2 SSID 3 SSID 4

Mode: WPA2/PSK

WPA

Encryption Mode: TKIP for WPA/AES for WPA2

Pre-Shared Key(PSK): 1234abcd\*!@#%^

Password Strength: Weak Medium Strong

For strong passwords:  
1. Use at least 12 characters.  
2. Include at least 3 of the following 4 types of characters: digits, uppercase letters, lowercase letters, and non-alphabetic characters (such as #, %, &)

### 802.1X kimlik doğrulamasını kullanın (WPA2-Enterprise)

PSK (Pre-shared Key) kimlik doğrulaması, tek tek kullanıcıları yönetemez. Birisi yanlışlıkla veya kasıtlı olarak şifreyi açık ederse, Network Administrator'un Wi-Fi erişimini iptal etmesi için herkesin şifresini değiştirmesi gerekir. Wi-Fi erişimini daha verimli bir şekilde yönetmek için, her kullanıcının benzersiz bir kullanıcı adı ve şifre ile giriş yapmasını gerektiren 802.1X kimlik doğrulaması daha iyi bir seçenek olacaktır.

802.1X kimlik doğrulamasını dağıtmak için, kullanıcı veritabanını korumak ve kimlik bilgilerini doğrulamak için bir RADIUS sunucusuna ihtiyacınız olacaktır. Ağda bir RADIUS sunucunuz yoksa, sorun değil, hem VigorRouter hem de VigorAP yerleşik RADIUS sunucusunu destekler. “802.1X Kimlik Doğrulaması için Router’in Dahili RADIUS Sunucusunu Kullanma” ve Dahili kullanıcı veri tabanı ile 802.1X kimlik doğrulamasını uygulamak için “VigorAP’i RADIUS Sunucusu Olarak Kullanma” bölümüne bakın.

## SSID'yi Gizle

Router / AP'nin kablosuz ağ yayını yapmasını engellemek için Wireless LAN >> General Setup sayfasında “Hide SSID” yi işaretleyin, böylece yalnızca SSID'yi tanıyan kullanıcılar ağa erişebilir.

### Wireless LAN(2.4GHz) >> General Setup

#### General Setting ( IEEE 802.11 )

<input checked="" type="checkbox"/> Enable Wireless LAN						
Mode :		Mixed(11b+11g+11n) ▼				
Channel:		Channel 6, 2437MHz ▼				
Enable	Active	Hide SSID	SSID	Isolate Member	Isolate VPN	
<input type="checkbox"/>	X	<input checked="" type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	X	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	X	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	X	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	

## İnternet Erişim Güvenliği IP Filtresi Uygula

Hem giden hem de gelen trafiği yönetmek, LAN istemcilerinin güvenlik açığı bulunan hizmetleri kullanmasını engellemek için kurallar belirlemek veya local sunucuyu yalnızca belirli internet IP adresleriyle sınırlamak için VigorRouter’ın built-in Firewall özelliğini kullanabilirsiniz. Örnek için bkz.” Block FTP Service by Firewall”.

## Malware’e Erişimi Content Filter ile Engelleme

Local kullanıcının malware ile ilişkili web sitelerine erişmesini engellemek için URL Keyword Filter ayarlayın, bkz “ Bir Web Sitesini URL İçerik Filtresi ve DNS Filtresi ile Engelleme” . Web Content Filter ayrıca, Router’in malware web sitelerini otomatik olarak filtrelemesine yardımcı olan ve her URL’yi tanımlamadan hepsini engellemeyi sağlayan harika bir çözümdür.

<input type="checkbox"/> Select All	<input type="checkbox"/> Chat	<input type="checkbox"/> Instant Messaging
<input type="button" value="Clear All"/>		
<b>Computer-Internet</b>	<input type="checkbox"/> Anonymizers	<input type="checkbox"/> Forums & Newsgroups
<input type="button" value="Select All"/>	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Streaming, Downloads
<input type="button" value="Clear All"/>	<input type="checkbox"/> Search Engine,Portals	<input type="checkbox"/> Social Networking
	<input checked="" type="checkbox"/> Malware	<input checked="" type="checkbox"/> Botnets
	<input checked="" type="checkbox"/> Illegal Software	<input checked="" type="checkbox"/> Information Security
<b>Other</b>	<input type="checkbox"/> Adv & Pop-Ups	<input type="checkbox"/> Arts
		<input type="checkbox"/> Transportation
		<input type="checkbox"/> Computers,Technology
		<input checked="" type="checkbox"/> Phishing & Fraud
		<input checked="" type="checkbox"/> Spam Sites
		<input checked="" type="checkbox"/> Hacking
		<input type="checkbox"/> Peer-to-Peer

**Firmware’i Güncel Tutun**

Tüm güvenlik yamalarının (ve ayrıca yeni özelliklerin!) Eklendiğinden emin olmak için her zaman VigorRouter ve Vigor AP'nizdeki en yeni firmware sürümünü kullanın. En son sürümü “<https://www.draytek.com/support/latest-firmwares/>” adresinde bulabilirsiniz.

DrayTek