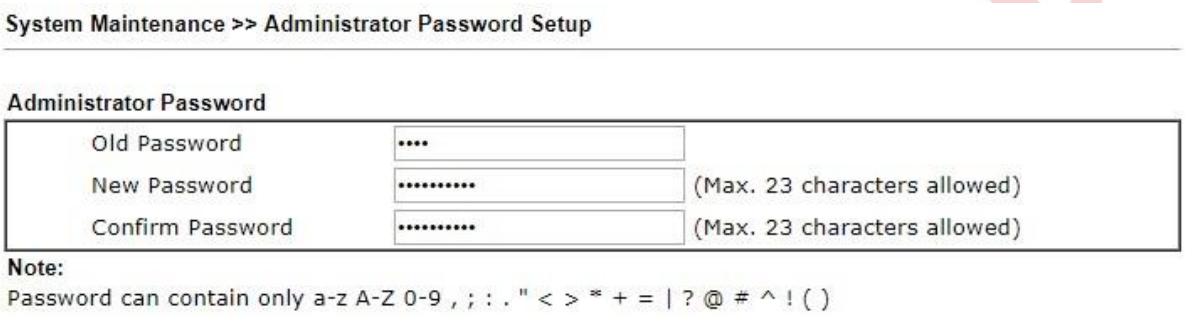
Ağ Güvenliğini Artırma Yolları

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**

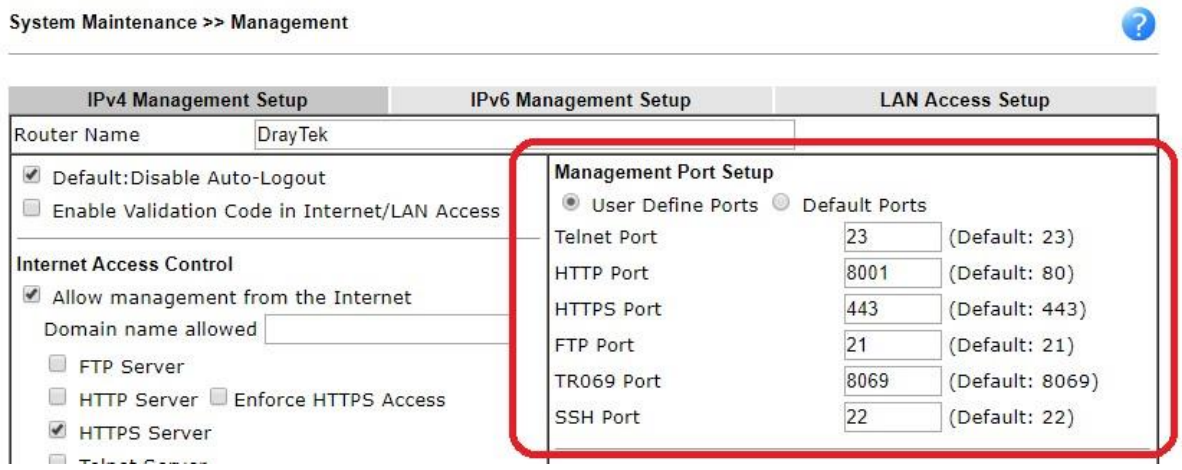
Varsayılan yönetici şifresini değiştirin

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.

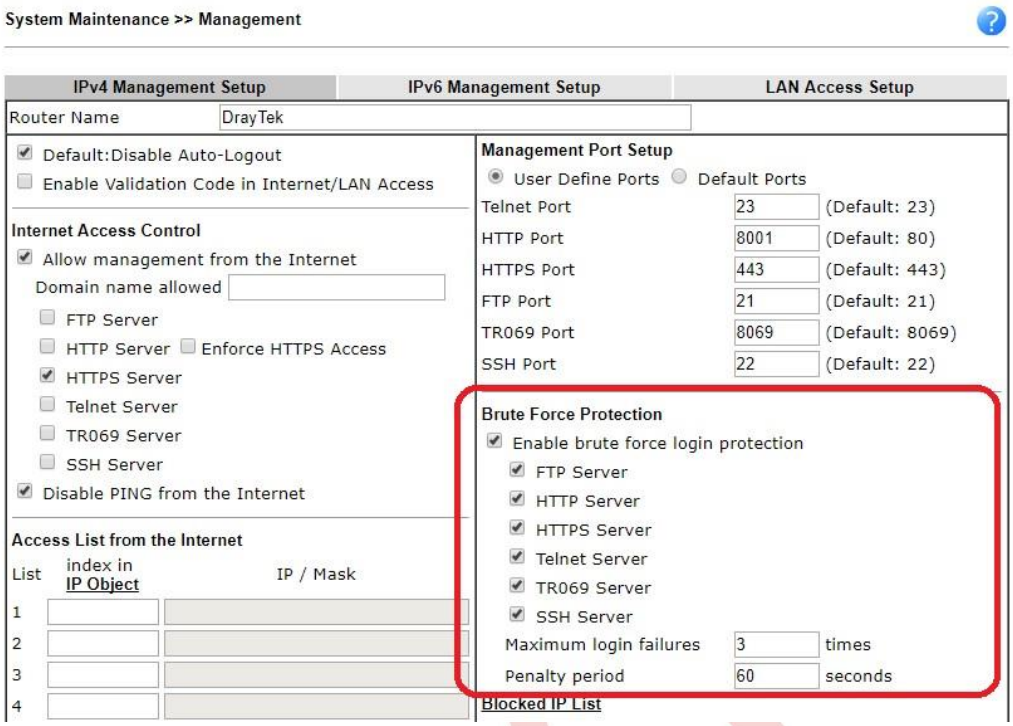


Yönetim portunu değiştirin Varsayılan olarak, VigorRouter, web arayüzü, komut satırı arayüzü ve diğer hizmetler için iyi bilinen portları kullanır.

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.

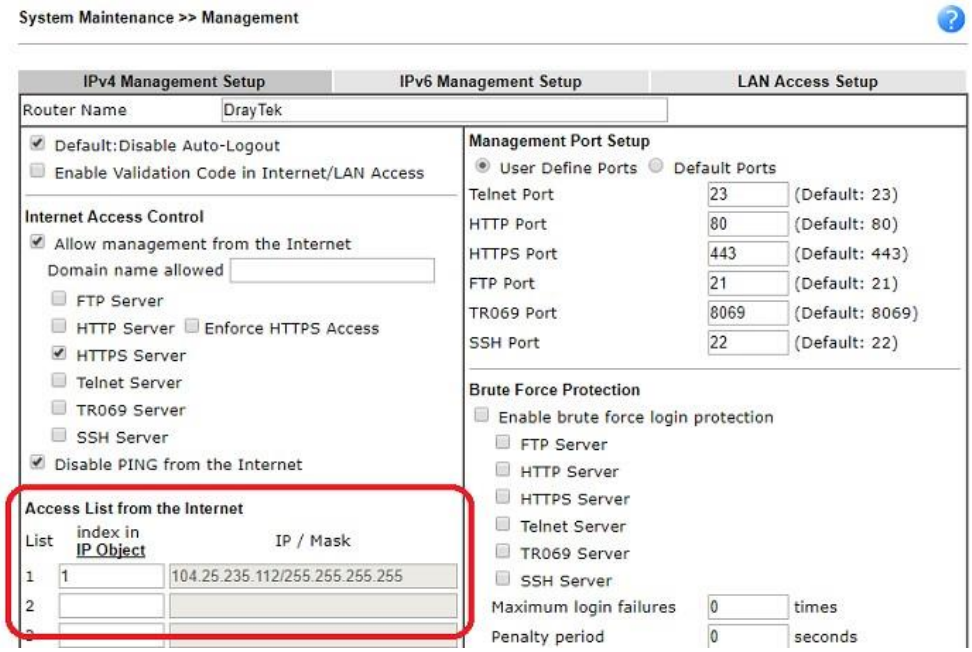


Brute Force Korumasını Etkinleştir Oturum açma sayfasına giriş yaptıktan sonra, giriş şifresi olmasa bile, saldırgan zaman geçse de doğru giriş şifresi bulunana kadar her olası şifreyi deneyebilir. Brute Force Protection'ı etkinleştirmek, VigorRouter'ın giriş yaparken çok fazla başarısız olan IP adresini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



Yönetim Erişimi için Erişim Listesi'ni Ayarlama

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



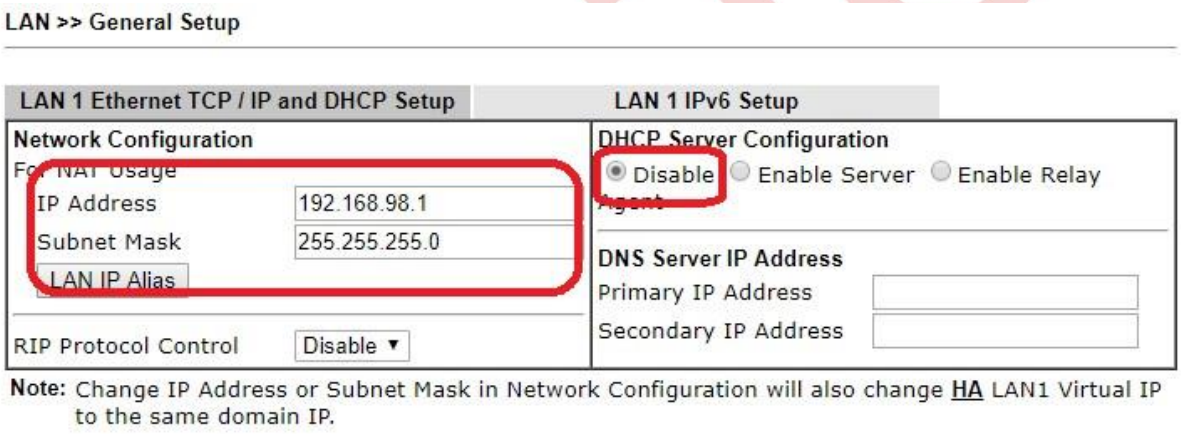
Local Network Güvenliği

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.

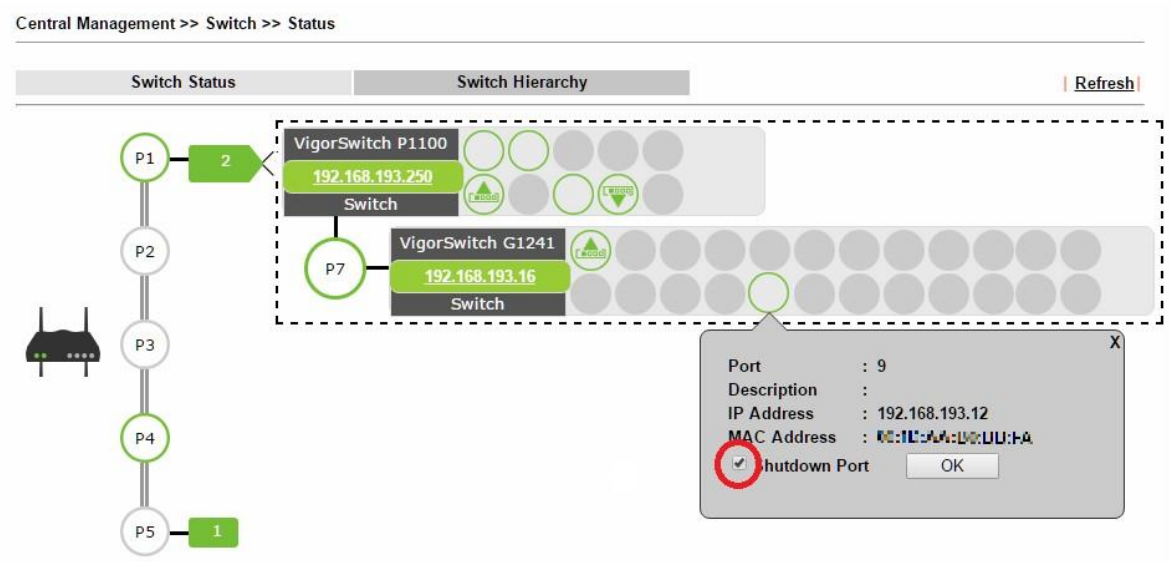
DHCP Sunucusunu Devre Dışı Bırakın ve LAN IP'sini Değiştirin

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.



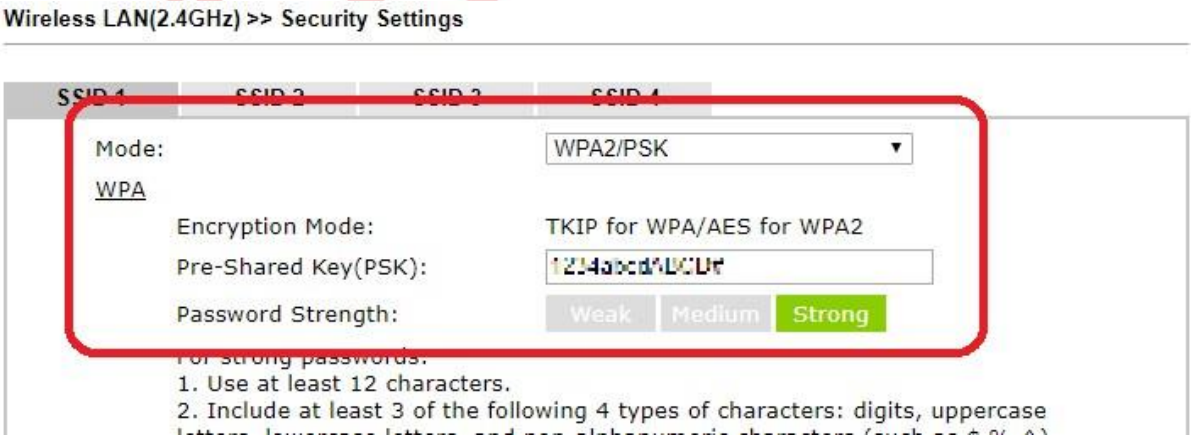
Switch'ler de Kullanılmayan Portları Kapatın

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.



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 uyguladığınızdan emin olun. WEP, WPA ve WPA2 arasında, WPA2 en güçlü güvenlik protokolüdür ve kullanmanızı öneririz.



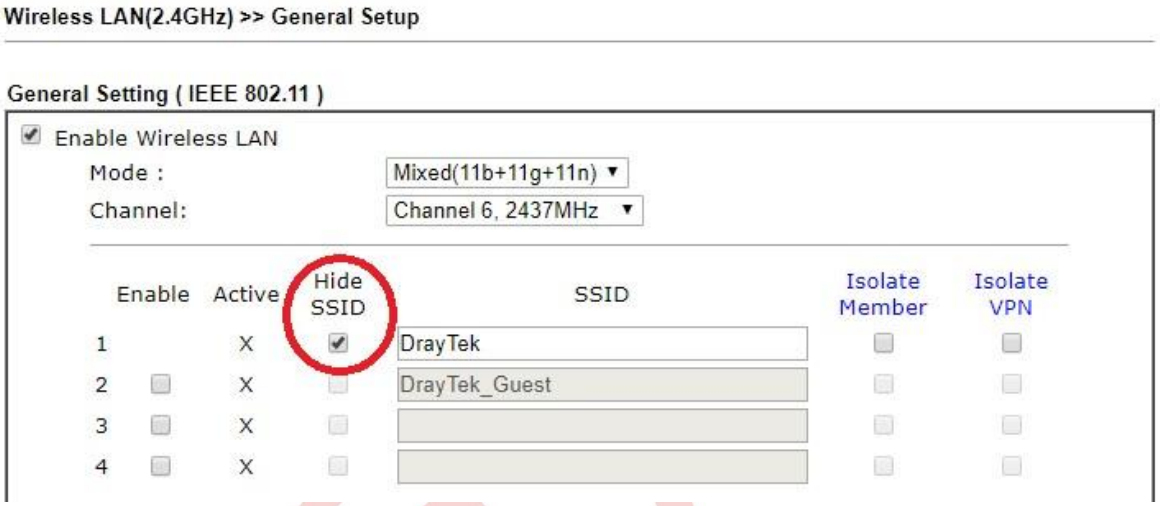
802.1X kimlik doğrulamasını kullanın (WPA2-Enterprise)

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'ı 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.

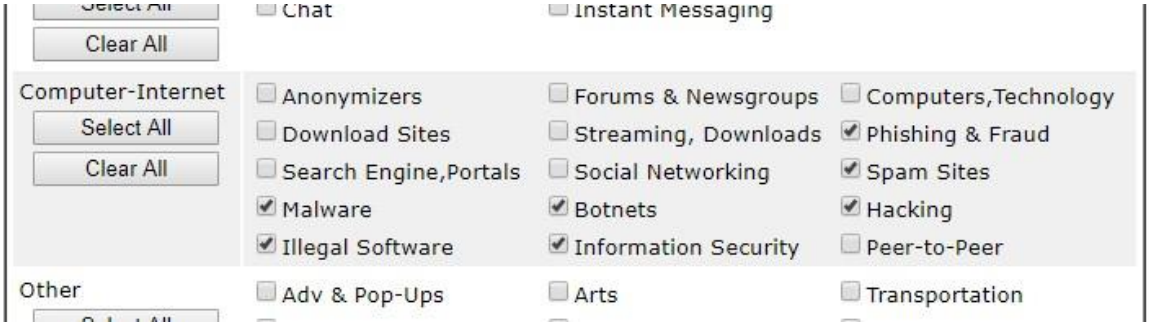


İnternet Erişim Güvenliği IP Filtresi Uygula

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 engellemenizi sağlayan harika bir çözümdür.



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.