Robustel Router’larda Siber Güvenlik İçin Alınabilecek Önlemler

Giriş

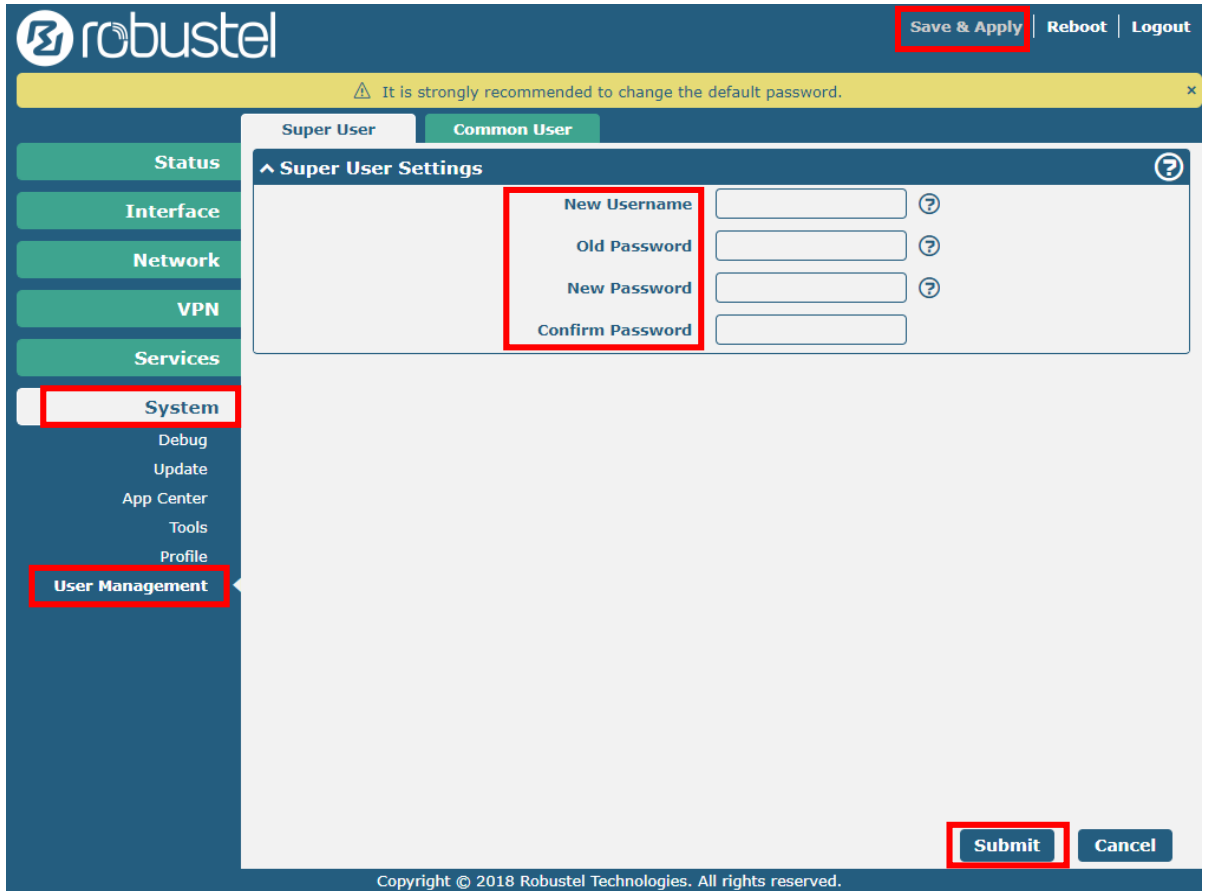
Son yıllarda IoT ve IIoT kapsamında, nesnelerin internete açılmaya başlamasıyla beraber siber saldırılar da hayli artış göstermeye başladı. Belirli bir IP adresinden başlayıp birçok IP adresini tarayarak, internete açık IP'lere ulaşım sağlamaya çalışan programlar yaygınlaşıyor.

Özellikle son dönemde siber korsanların yukarıda bahsedilen programlar vasıtasıyla, örneğin 5.26.149.1 – 5.26.149.254 aralığında, admin/12345, admin/admin ya da olabilecek default parametreleri kullanarak sıklıkla IP'lere ulaşmaya çalıştıklarını gözlemliyoruz. Bu aralıkta yer alan herhangi bir cihaza erişim sağlandığında, bu durum ciddi tehlikeleri beraberinde getiriyor.

Dolayısıyla, müşterilerimizin son dönemde hayli artış gösteren bu saldırılara yönelik siber güvenlik önlemi almalarında büyük fayda görüyoruz. Aksi takdirde routerları kullanan uygulamalarında ciddi güvenlik açıkları ortaya çıkabileceğinin ve önemli kayıplara neden olabileceğinin altını çizmek istiyoruz.

İyi haber, Robustel Router'ların güvenlik ayarlarının kolayca yapılandırarak bu risklerin en aza indirgenebilecek olması. Bu kılavuzumuzda, Robustel router'larda yapılabilecek bu basit siber güvenlik ayarlarını bulabilirsiniz.

1. Kullanıcı Adı / Şifre Değiştirme



System → User Management

New Username : Dilerseniz kullanıcı adını değiştirebilir, dilerseniz admin olarak da bırakabilirsiniz

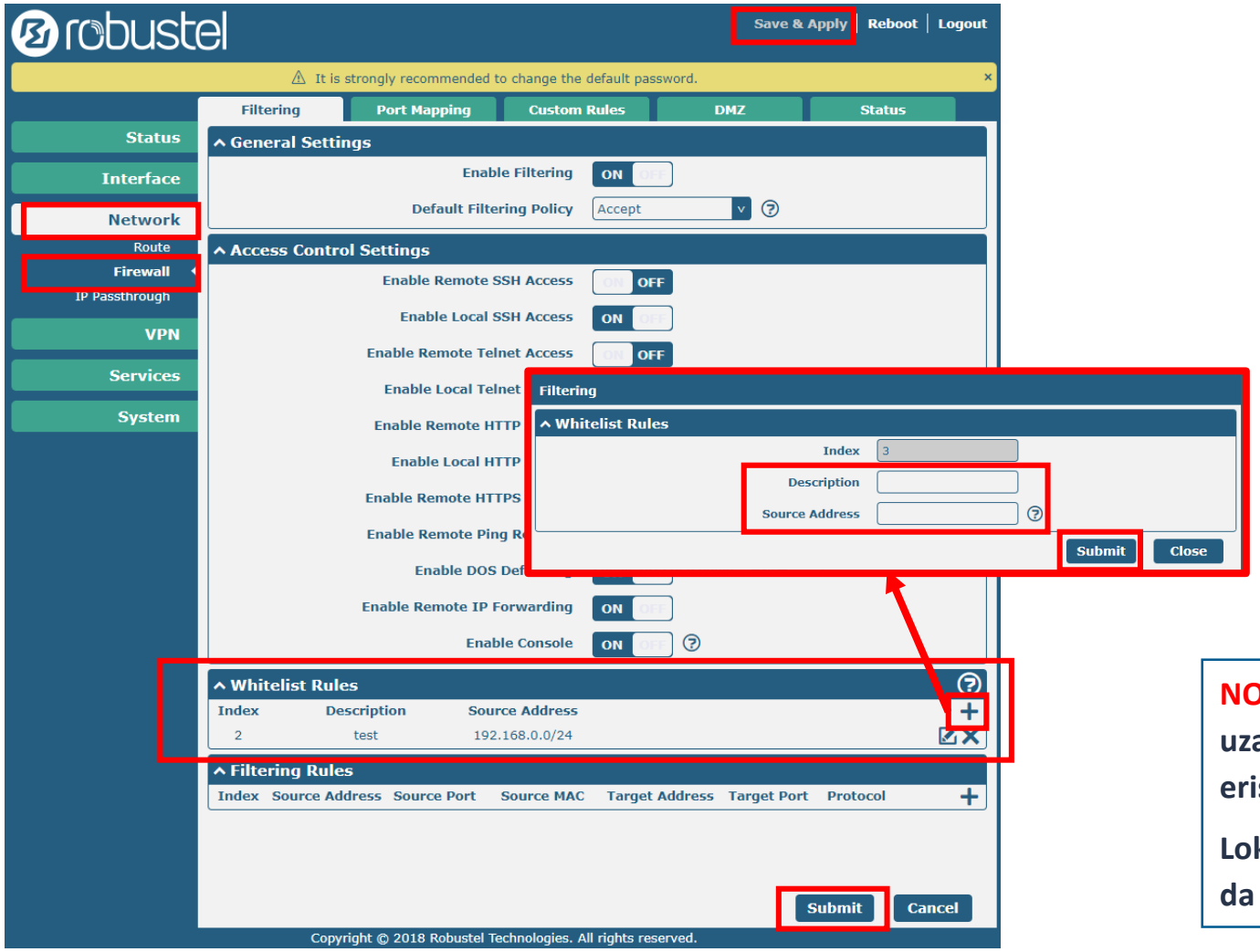
Old Password : Eski şifre buraya yazılır

New Password : Yeni şifre buraya yazılır

Confirm Password : Yeni şifre buraya tekrar tanımlanır

Ayarlar tamamlandıktan sonra kaydetmek için **Submit**, sonrasında da **Save & Apply** butonuna tıklanmalıdır.

2. Whitelist Tanımlama



Network → Firewall → Whitelist Rules

\+ ya tıkladıktan sonra, açılan ekranda;

Description : Kurala vereceğiniz isim

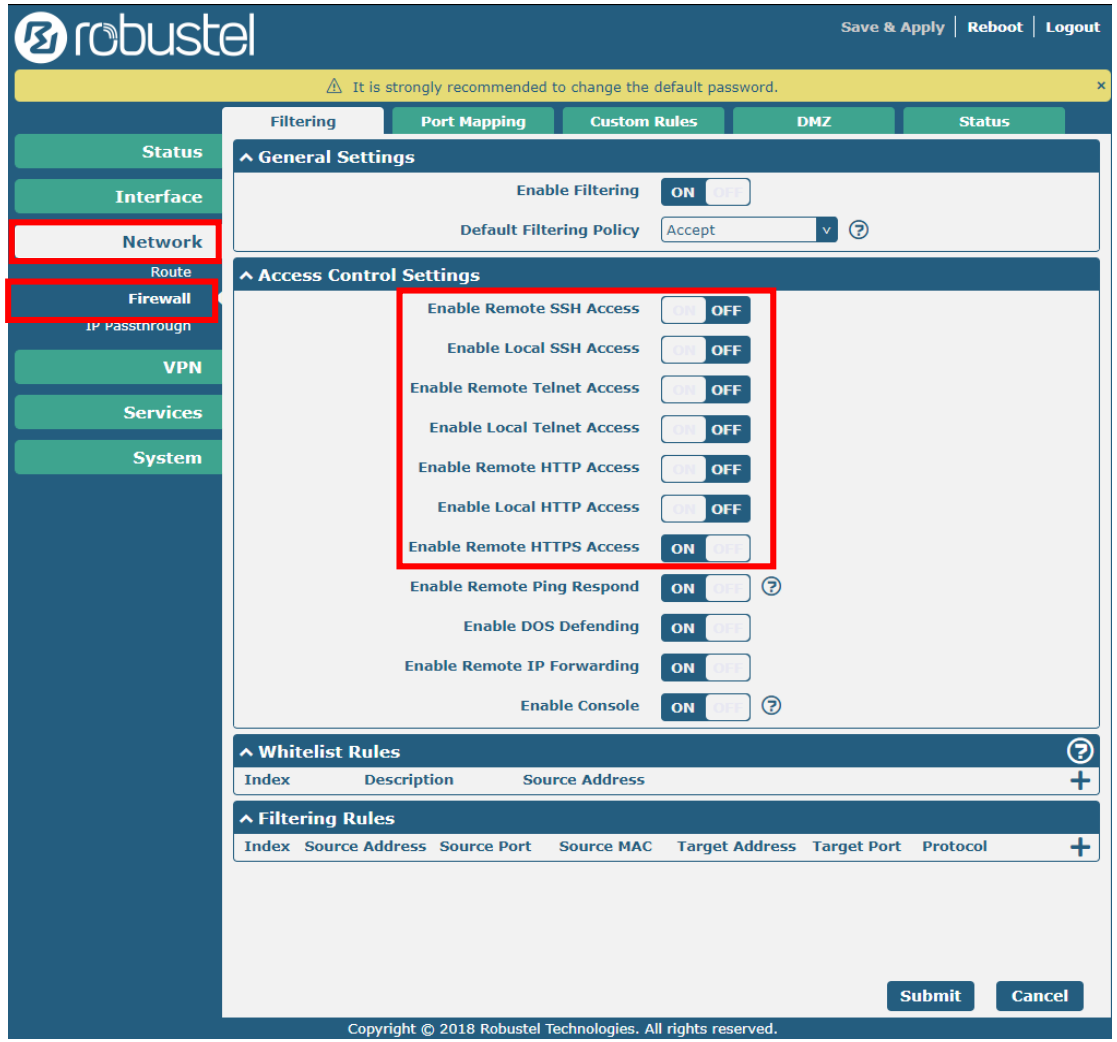
Source Adress : Cihaza bağlanabilecek IP adresi/ Subnetmask tanımı

***Örnek** : Sadece lokalden erişim istenirse, 192.168.0.0/24 gibi bir tanım yapılabilir (Tanım, Robustel'in lokal IP'sinin 192.168.0.1 olduğu düşünülerek verilmiştir)*

NOT : Kural olarak sadece Dış IP tanımı yapılırsa, cihaza uzaktan sadece o dış IP'den internete çıkan cihazlar erişebilir.

Lokal olarak da erişim sağlanması istenirse, bu tanımın da ayrıca yapılması gerekir.

3. Cihaza Erişim Yöntemlerini Azaltma

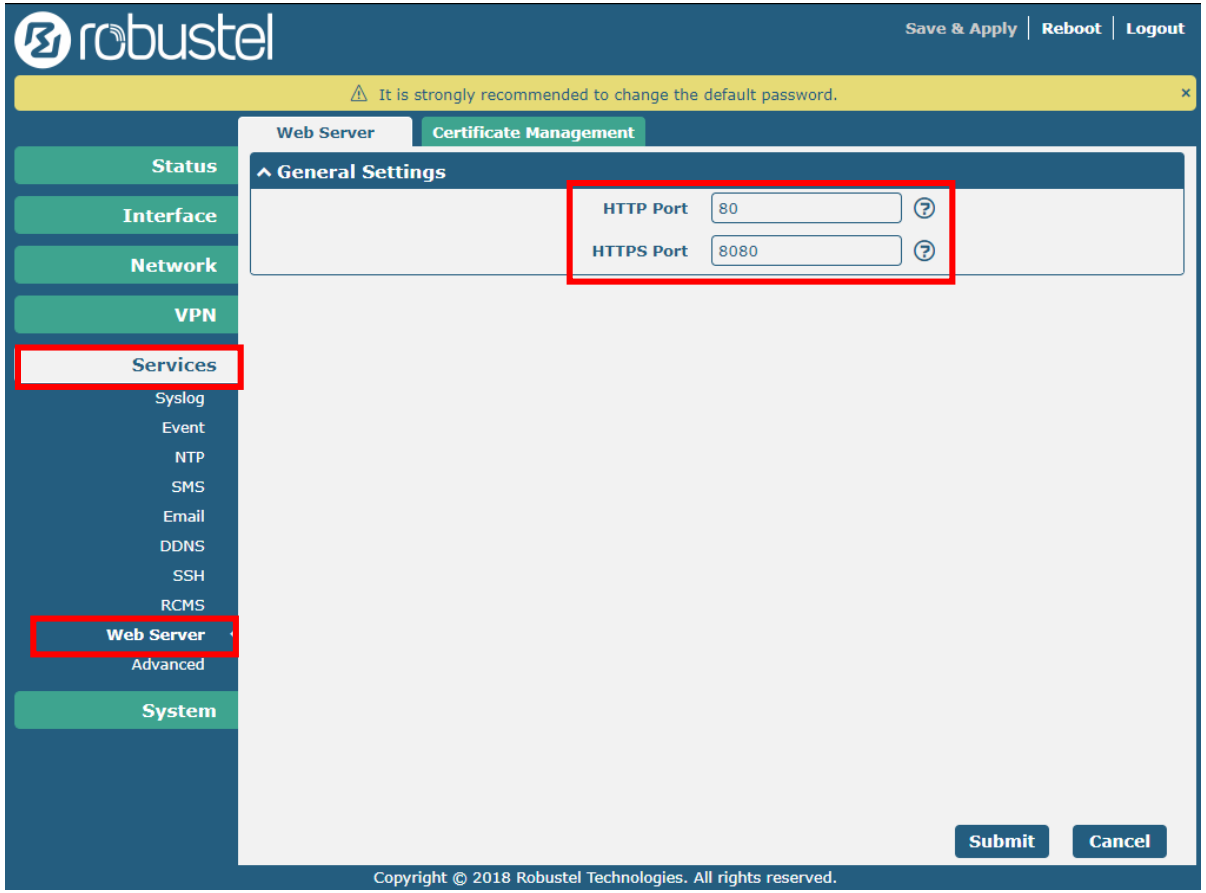


Network → Firewall → Access Control Settings

Cihaza erişim için kullanılabilecek yöntemler burada yer almaktadır.
Güvenliği artırmak için kullanılmayan erişim yöntemlerini daraltmak faydalı olacaktır.

SSH / Telnet / HTTP / HTTPS gibi ulaşım yöntemleri uzak erişim ya da lokal erişim için kısıtlanabilir.

4. HTTP / HTTPS Portlarını Değiştirme



Services → Web Server

Bir önceki sayfada, sadece uzaktan HTTPS erişimi açık bırakılmıştı.

Bu sekmeden de default olarak 443 olarak gelen HTTPS portu bir başka port numarası ile değiştirilebilir.

NOT : Bu ayar yapıldığı taktirde, cihazın web arayüzüne uzak erişim sağlamak için web tarayıcısına – https://dışIP:HTTPSport yazılmalıdır.
***Örnek** : https://5.26.149.155:8080*