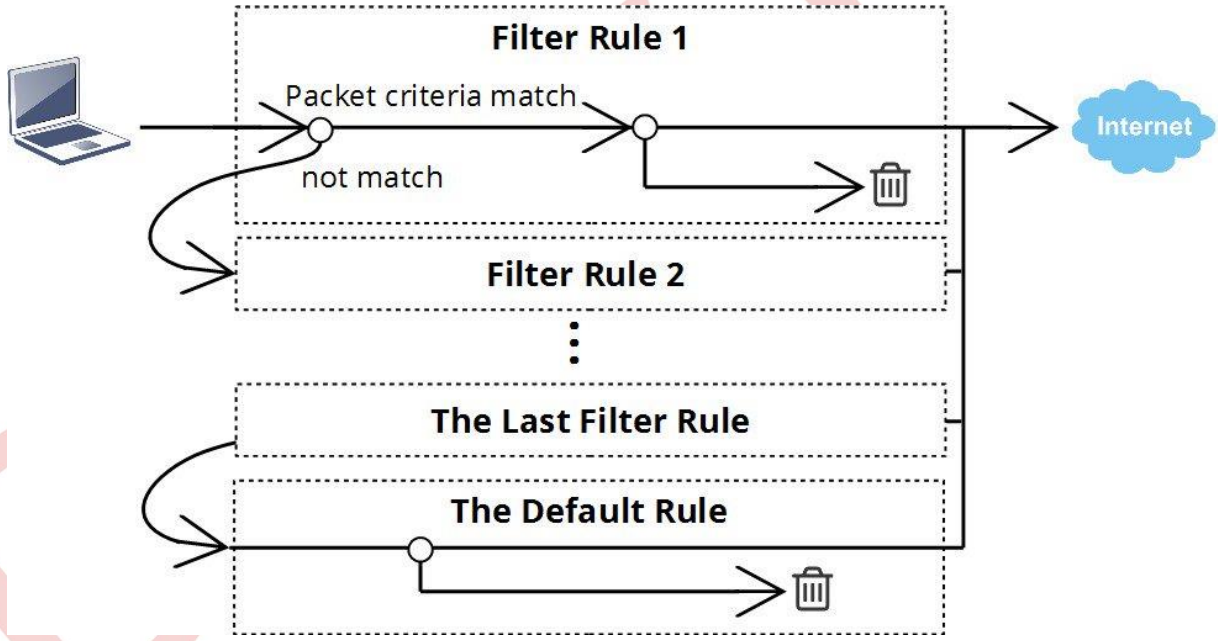
Güvenlik Duvarı İçerik Güvenliği Yönetimine Giriş)

Tüm VigorRouter, Network Administrator'un ağın gelen ve giden trafiğini kontrol etmesini, böylece ağ güvenliğini arttırmasını ve ağ kaynaklarının uygunsuz uygulamalara harcanmasını önlemesini sağlayan yerleşik firewall özelliklerine sahiptir. VigorRouter, kapsamlı bir firewall sunar IP-based policy, uygulamaların kullanımını kısıtlamak veya web sitelerine erişimi kısıtlamak amacıyla belirli bir kaynaktan veya belirli bir hedeften trafiğe erişimi, CSM'yi (içerik güvenliği yönetimi) ve DoS savunmasını da içerir.Bu makale size şebekeyi flooding saldırılarından korumak için DrayTek Firewall'un nasıl kullanılacağına dair genel bir bakış sunacaktır.

Vigor Router Firewall Kuralları

VigorRouter'da, her biri yönlendirme, kaynak IP adresi, hedef IP adresi, port numarası veya / ve protokol olabilen filtreleme koşullarına uyan paketlere uygulanacak olan 80'den fazla firewall kuralına sahip olabiliriz. Firewall kuralının sırası önemlidir, çünkü bir paket sadece bir kural izleyecektir. Bir paketin ölçütleriyle eşleşen birden fazla kural varsa, en küçük dizin numarasına sahip kural geçerli olacaktır.

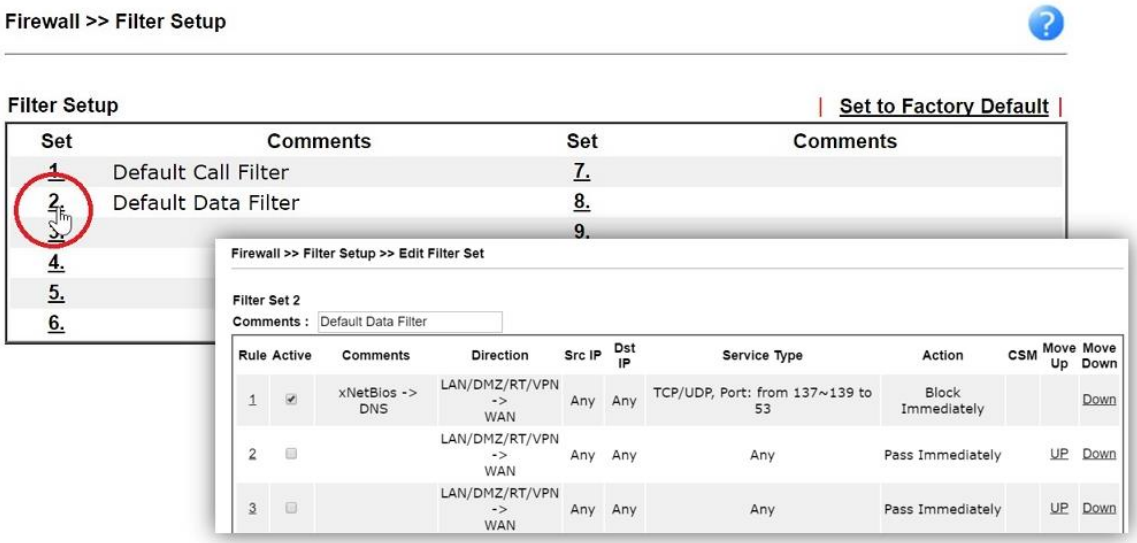
Paket, tüm filtre kurallarındaki kriterlerden herhangi biriyle eşleşmezse, fabrika varsayılan yapılandırmasında "pass" olan varsayılan yapılandırmayı izler. Default policy, Firewall>> General Setup >> "Default Rule" Sekmesinden değiştirilebilir.



Filtre Seti ve Filtre Kuralları

Firewall>> Filter Setup sayfasında, 12 Filter Sets göreceğiz ve her biri yedi filtre kuralı içeriyor. Varsayılan olarak, Filter Set 1 "Call Filtering" için kullanılır; bu, Filter Set 1'deki filtre kurallarının yalnızca internet bağlantısı kurulmadığında etkin olacağı ve yalnızca giden paketler için geçerli olacağı anlamına gelir; WAN bağlantısı çeviren trafiği kısıtlar. Filter Set 2, genel durumlar için geçerli olan varsayılan Data Filter'dir.

Genel bir filtre kuralı eklemek için, Firewall >> Filter Setup'a gidin, varsayılan Data Filter Set'ine girmek için Set 2'ye tıklayın. Filter set 2'de yedi filtre kuralı olduğunu göreceksiniz. Rule 1, giden NetBIOS trafiğini engellemek için önceden tanımlanmış bir kuraldır ve genellikle filtre yapılandırmasını Rule 2'den itibaren başlatırız.



Kural Yapılandırmasını Filtrele

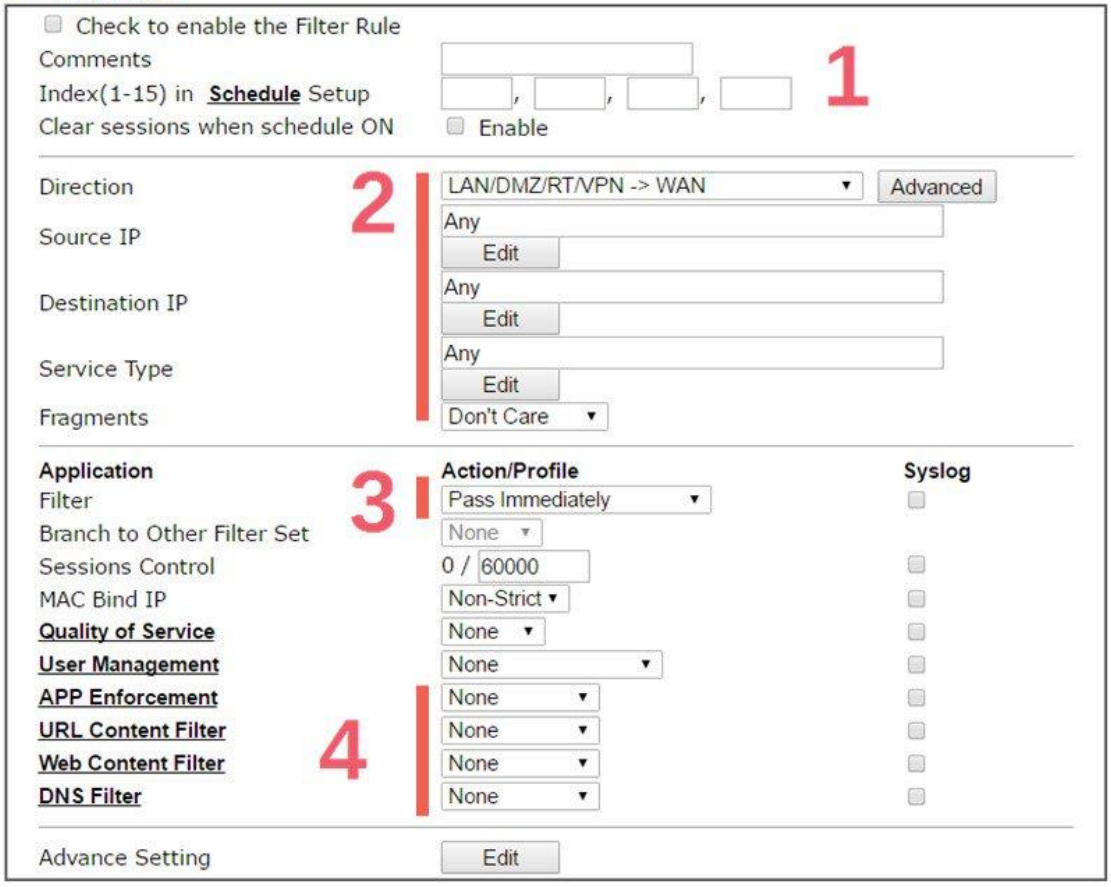
Dizin numarasına tıklayarak, kural yapılandırma sayfasına gireceğiz. Yapılandırma dört bölüme ayrılabilir. En üstte, tanımlama kuralı hakkında bazı yorumlar verebiliriz ve bu kuralı schedule profile ile bağlayabiliriz, böylece sadece belirli bir zamanda (isteğe bağlı olan) geçerli olur. İkinci kısım, filtreleme koşullarıdır. Hangi kuralın bu kurala uyması gerektiğini tanımlar. Burada bir veya daha fazla koşulu ayarlayabiliriz, onu "Any" olarak bırakmak, bu kuralı tüm paketler için geçerli kılar. Örneğin, belirli bir LAN hostu için bir policy belirlemek için Direction "LAN / DMZ / RT / VPN -> WAN" olmalı ve Source IP, bu LAN hostunun LAN IP adresi olmalıdır.

Üçüncü bölüm bu filtre kuralının Action'udur. "block" veya "pass" olabilir. "Block" seçilerek, router yukarıdaki kriterlere uyan tüm paketleri atar. "Pass", router bu paketleri kabul edecektir. Bununla birlikte, paketin içerik incelemesini yapmak için uygulama filtreleri uygulayabilir ve ardından verilerinde belirli bilgiler içeriyorsa paketi atmaya karar verebiliriz.

Son olarak, Content Security Management (CSM) profilleridir. Bunlar, Network Admininin LAN kullanıcılarının belirli web sitelerine erişimini kontrol etmesini veya belirli uygulamaların kullanımını kısıtlamasını sağlayan uygulama filtreleridir. Aşağıdaki paragraf aralarındaki farkı açıklayacaktır

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2



Filter Set 2'deki tüm filtre kurallarını kullandıktan sonra, sayfanın altında Next Data Filter Set'ini belirleyebilir, daha sonra seçilen Filter Set'inde daha fazla filtre kuralına sahip olabilirsiniz.

Filter Set 2

Comments : Default Data Filter

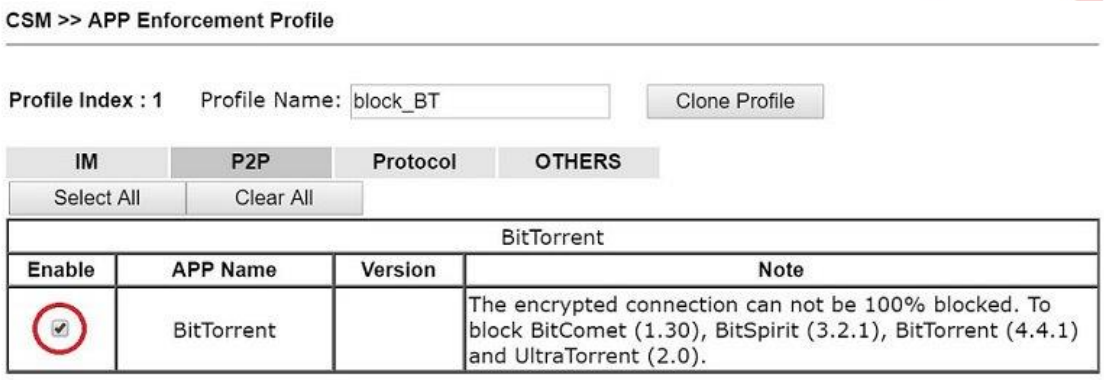
Rule	Active	Comments	Direction	Src IP	Dst IP	Service Type	Action	CSM	Move Up	Move Down
1	☑	xNetBios -> DNS	LAN/DMZ/RT/VPN -> WAN	Any	Any	TCP/UDP, Port: from 137~139 to 53	Block Immediately			Down
2	☑	Server	LAN/DMZ/RT/VPN -> WAN	192.168.1.254	Any	Any	Pass Immediately		UP	Down
3	☑	block_pokemon	LAN/DMZ/RT/VPN -> WAN	192.168.1.0/ 255.255.255.0	Any	Any	Pass Immediately	UCF-1	UP	Down
4	☑	Marketing	LAN/DMZ/RT/VPN -> WAN	192.168.1.20 ~ 192.168.1.24	Any	Any	Block Immediately		UP	Down
5	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
6	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	Down
7	☐		LAN/DMZ/RT/VPN -> WAN	Any	Any	Any	Pass Immediately		UP	

Filter Set 1 2 3 4 5 6 7 8 9 10 11 12 **Next Filter Set** Set#3

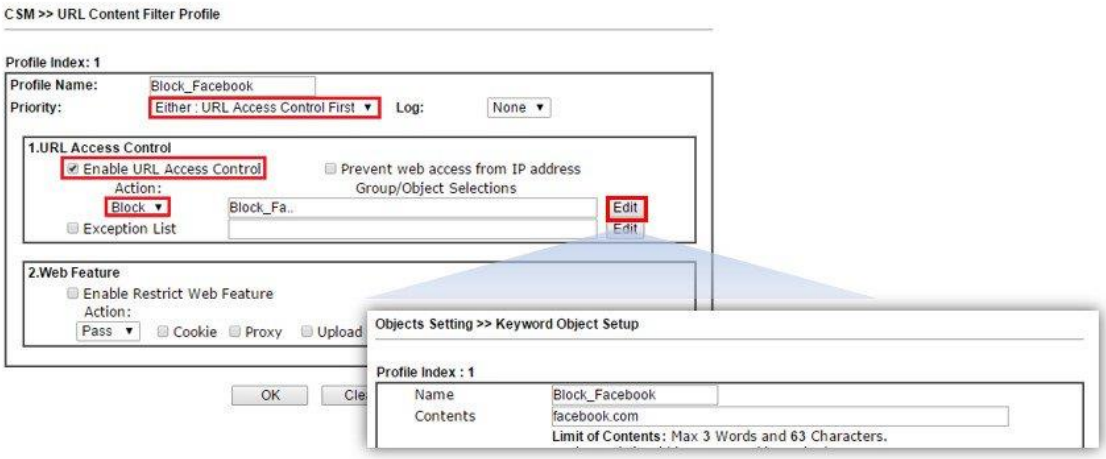
İçerik Güvenliği Yönetimi (CSM)

Bir filtre kuralı yapılandırmasının altında dört seçenek vardır: APP Enforcement, URL Content Filter, Web Content Filter ve DNS Filter. Bunların tamamına birden Content Security Management (CSM) denir.

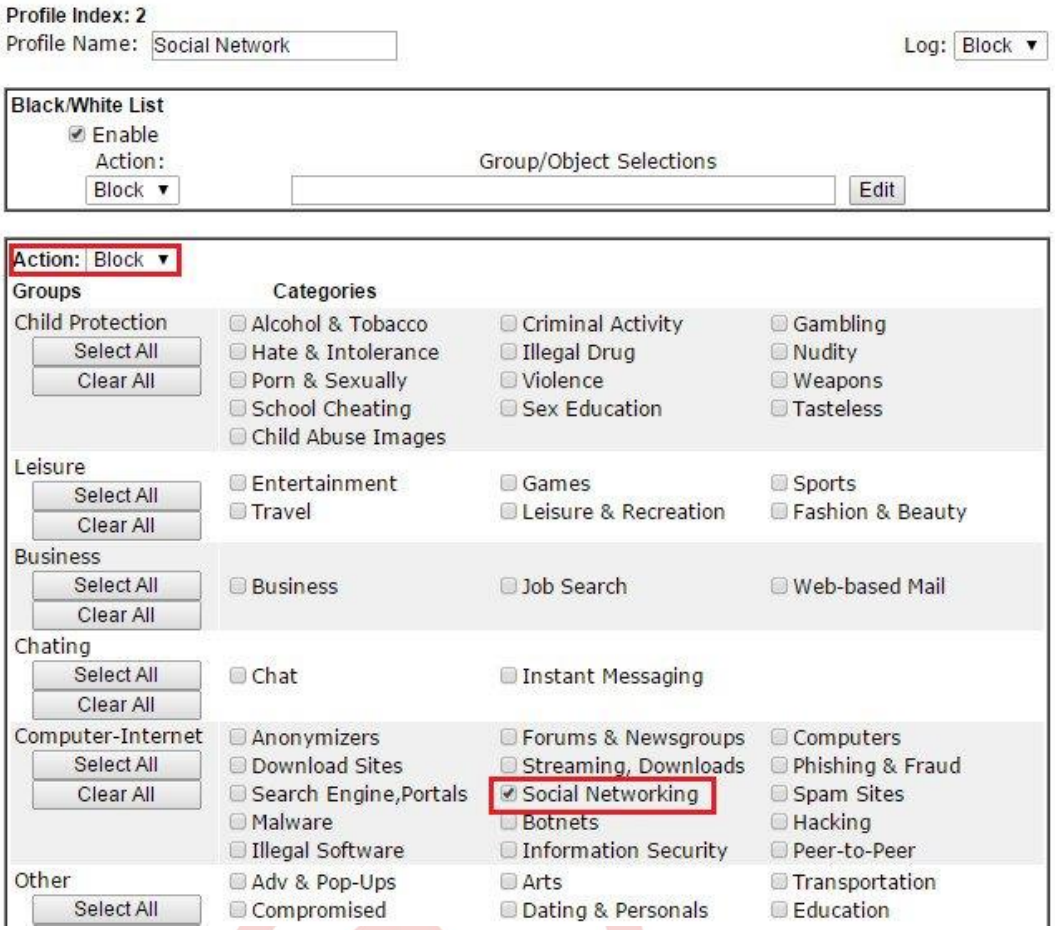
APP Enforcement, uygulamaların kullanımını kontrol etmek içindir. Tracing, paket kalıplarını izleyerek, LAN kullanıcılarının kullandığı uygulamaları tanıyabilir ve Network Administrator, belirli uygulamaların kullanımını engellemek için kurallar ayarlayabilir. Aşağıdaki örnek, BitTorrent kullanımını engelleyen bir profildir. Ayrıntılı talimatlar için Facebook App Enforcement bölümüne bakın.



URL Content Filter web sitelerini filtrelemek içindir. Router, HTTP paketlerindeki host adını kontrol ederek, LAN kullanıcılarının hangi siteye erişmeye çalıştığını öğrenebilir. URL Content Filter, belirli bir URL'ye erişimi engellemek için blacklist olarak kullanılabilir; veya izin verilen URL'lerin yalnızca bir kısmını geçirmek için white list olarak kullanılabilir. Aşağıdaki örnek, URL'nin "facebook.com" anahtar kelimesini içeren web sitelerine erişimi engelleyen bir profildir. Örnek için Blocking Windows Updates bölümüne bakın.



Web Content Filter ayrıca web sitelerini filtrelemek içindir, ancak URL anahtar kelimesine göre değil, web sitelerinin kategorisine göre. Bu lisans için gerekli bir hizmettir, çünkü CYREN'den gelen URL sınıflandırma servisini kullanıyoruz. Hizmet, Router'in, müşterinin hangi tür web sitesine erişmeye çalıştığını öğrenmesini sağlar ve Network Administrator, URL'lerinin her birini belirtmeden, belirli bir kategoriye giren tüm URL'lere erişimi kontrol eder. Aşağıdaki örnek, tüm sosyal ağ web sitelerini engelleyecek bir Web Content Filter profilidir. Ayrıntılı talimatlar için Sosyal Ağ Sitelerini Web İçerik Filtresi ile Engelleyin bölümüne bakın.



DNS Filter, HTTPS (şifreli) web sitelerinin de filtrelenmesini sağlamak için bir URL Content Filter ve Web Content Filter'in bir uzantısıdır. DNS Filter, Network Administrator'ün belirli anahtar kelimeler içeren DNS sorgularını engellemesini veya iletmesini ve böylece HTTPS web sitelerine erişimi kontrol etmesini sağlar. Firewall'da bir DNS Filter profili oluşturma ve uygulama hakkında Bir Web Sitesini URL İçerik Filtresi ve DNS Filtresi ile Engelleme bölümüne bakın.

DoS Savunma

VigorRouter ayrıca, sahte bağlantı talepleri tarafından tüketilen ağ kaynaklarını korumak için Denial of Service (DoS) Savunma sağlar. Network Administrator , **Firewall >> Defense Setup** sayfasından bunu etkinleştirebilir ve ayrıca her flooding politikasını ve eşiğini özelleştirebilir.