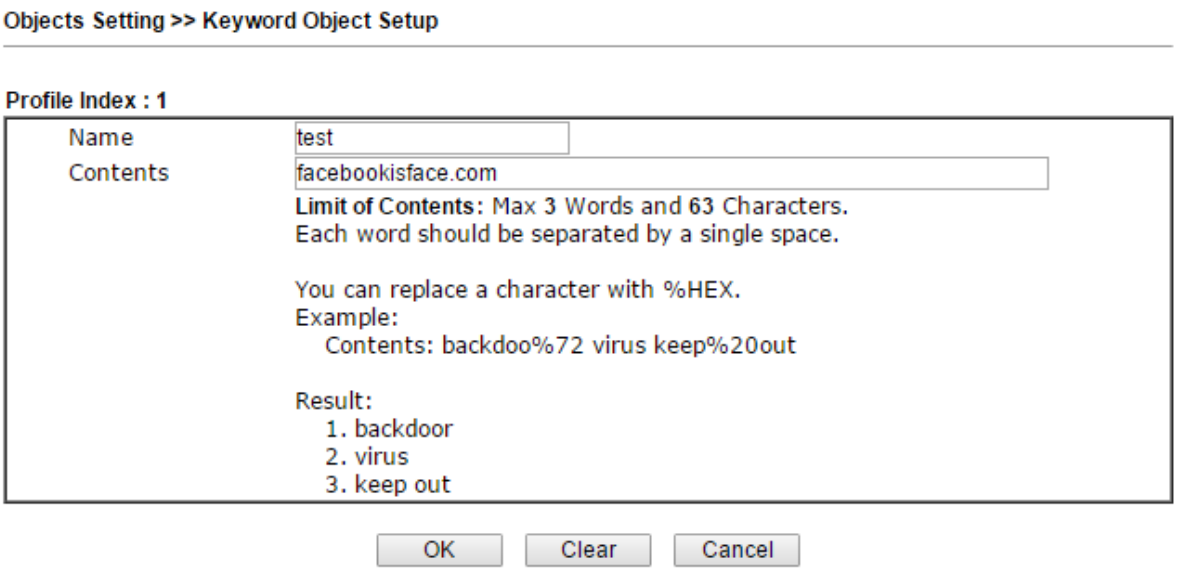
LAN İSTEMCİLERİ TARAFINDAN HANGİ WEB SİTELERİNİN ZİYARET EDİLDİĞİNİ ÖĞRENİN

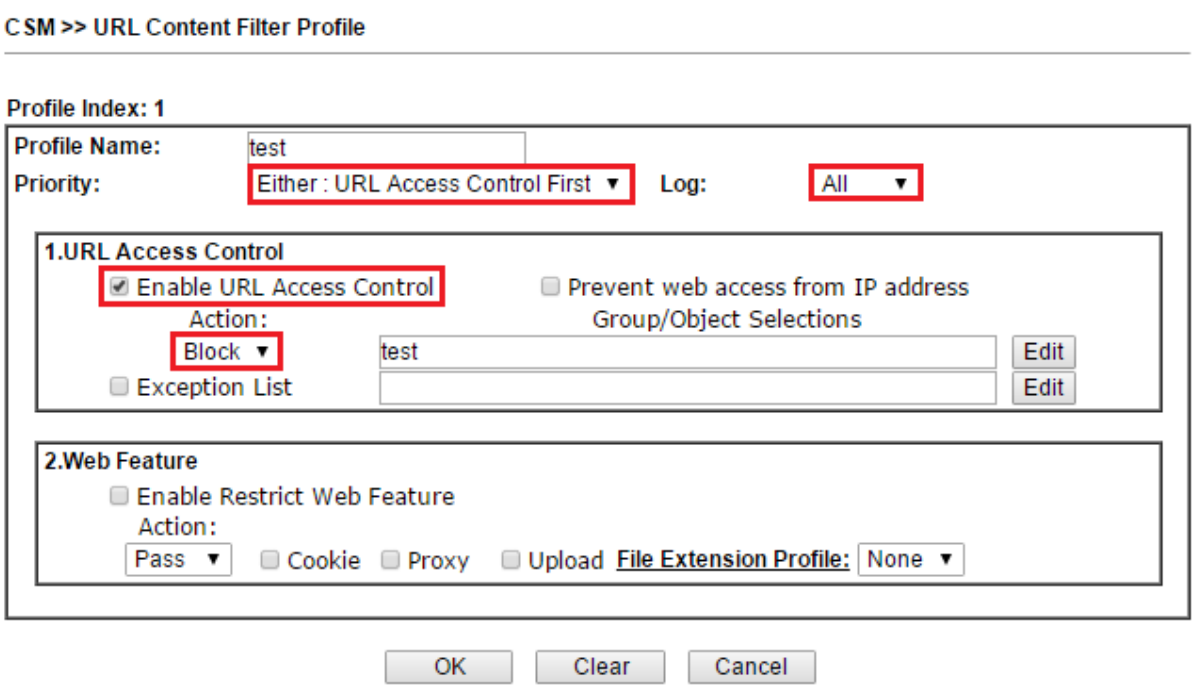
Syslog özelliği, kullanıcıların Vigor Router'ı izlemesini veya hata ayıklamasını sağlar. Ayrıca, LAN istemcilerinin tarama geçmişlerini izlemek için Syslog kullanabiliriz. Erişilen URL Logunu yazdırmak istediğimizden, URL Filtresi özelliğini ve DNS Filtresi özelliğini etkinleştirmemiz gerekir; ancak, hiçbir web sitesinin engellenmemesi için boş bir URL filtresi ve DNS filtresi kullanabiliriz. Bu makale, LAN istemcileri tarafından erişilen web sitelerinin nasıl kaydedileceğini ve Syslog'un bir USB sürücüsüne nasıl kaydedileceğini gösterecektir.

Bir URL Filtresi Oluşturun ve Bir Firewall Kuralı'na Uygulayın

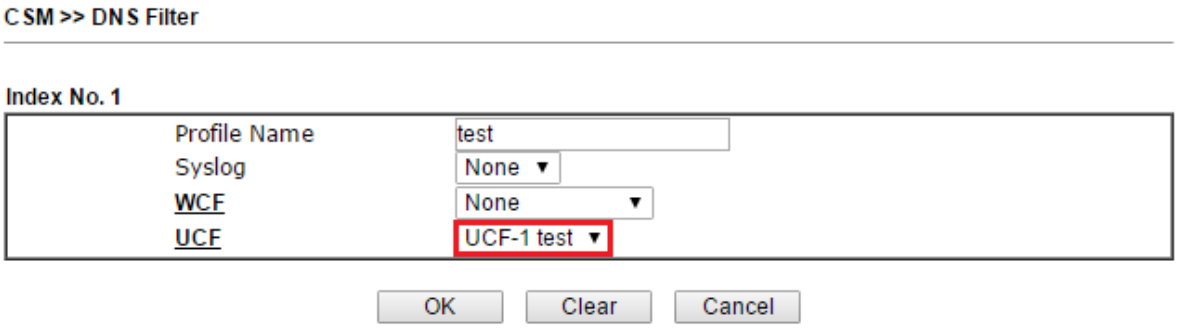
1. **Objects Setting >> Keyword Object'e** gidin. Bir index numarasına tıklayın.
   a. **Name** girin.
   b. Contents'e bazı boş içerikler girin.
   c. Kaydetmek için **OK'a** tıklayın.



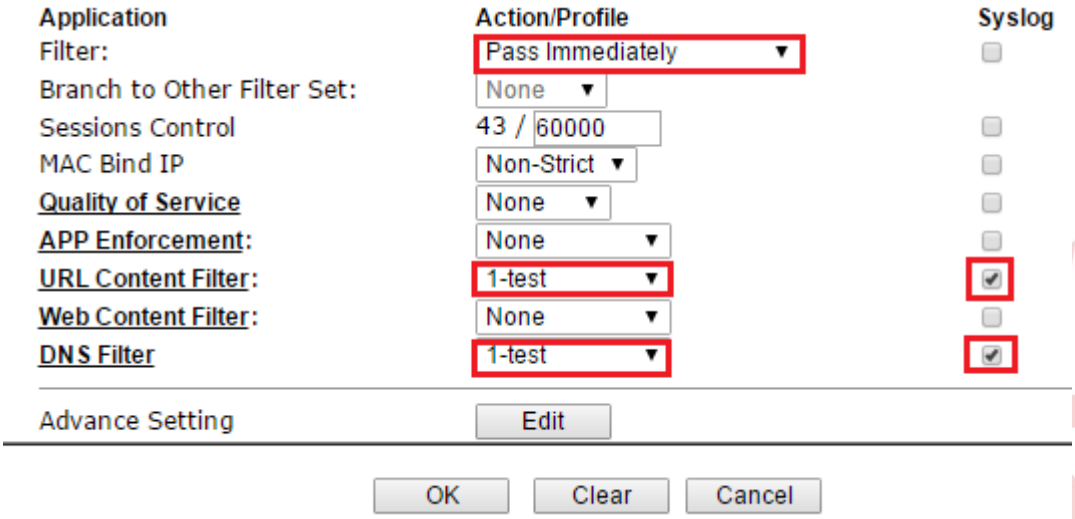
2. **CSM >> URL Content Filter Profile'da** bir URL Content Filter profili oluşturun, Profil numarasına tıklayın.
   a. **Profile name** girin.
   b. **Prioriy** için **"Either: URL Access Control First"** seçin.
   c. "All" olarak logu seçin, böylece iletilen veya engellenen tüm URL'lerin kaydedilmesi gerekir.
   d. "Enable **URL Access Control" u** etkinleştirin.
   e. **URL Access Control Action** için "Block" seçin.
   f. **Edit'e** tıklayın ve 1.adımda oluşturulan Keyword Object'i seçin.
   g. Kaydetmek için **OK'a** tıklayın.



3. **CSM >> DNS Filter'a** gidin. DNS Filter Profile Table'da bir profil numarasına tıklayın.
   a. **Profile Name** girin.
   b. 2.adımda oluşturulan URL Content Filter Profile'ı **UCF (URL Content Filter)** için seçin.
   c. Kaydetmek için **OK'a** tıklayın.

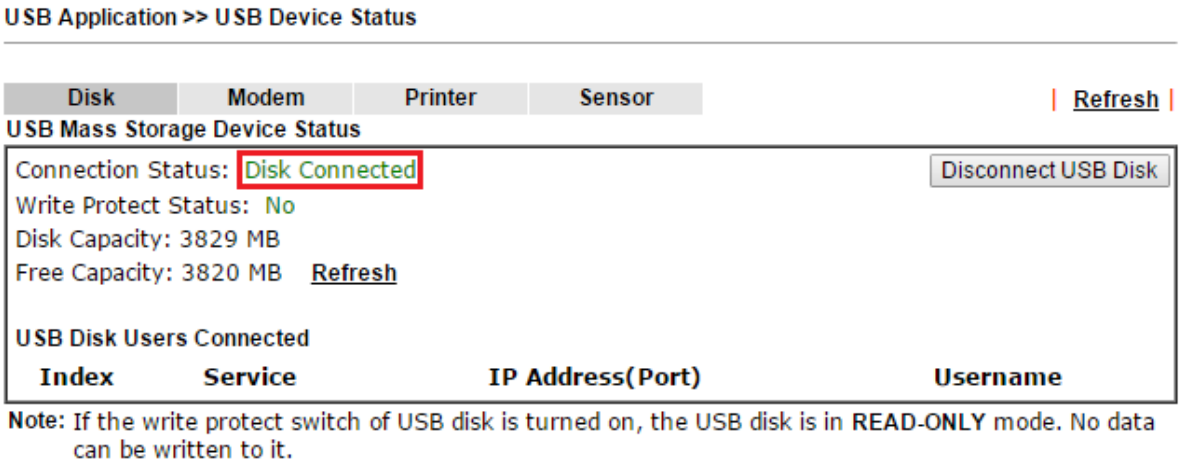


4. URL Content Filter ve DNS Filter'i Firewall kuralına uygulayın ve Syslog'u etkinleştirmeyi unutmayın. **Firewall >> Filter Setup >> Set 2 (Default Data Filter) 'a** gidin. Filter Rule numarasına tıklayın.
   a. Filter Rule için Enable'ı seçin.
   b. Source IP, destination IP ve service type'ı "Any" olarak bırakın.
   c. **Filter'ı** "Pass Immediately" olarak seçin.
   d. **URL Content Filter** için 2.adımda oluşturulan profili seçin ve Syslog'u işaretleyin.
   e. **DNS Filter** için 3.adımda oluşturulan profili seçin ve Syslog'u işaretleyin.
   f. Kaydetmek için **OK'a** tıklayın.

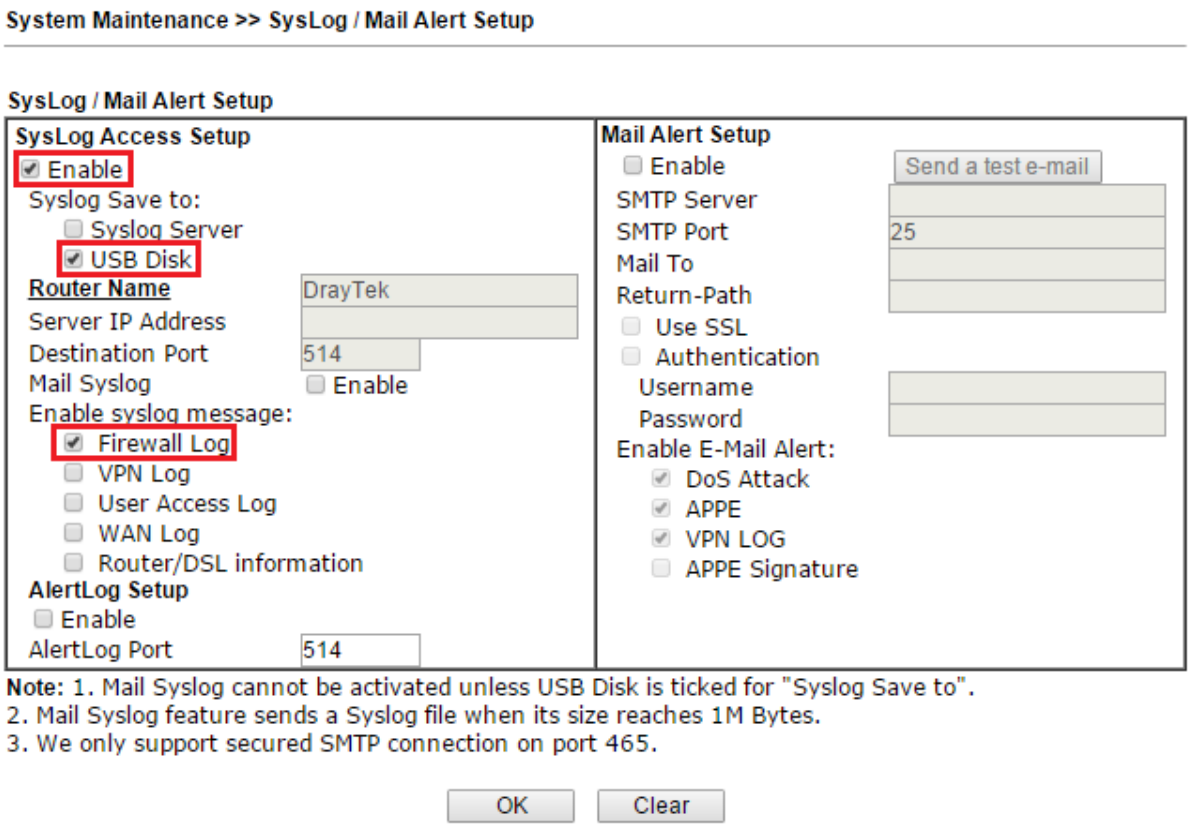


Bir USB Sürücüsüyle Syslog'u Kaydetme

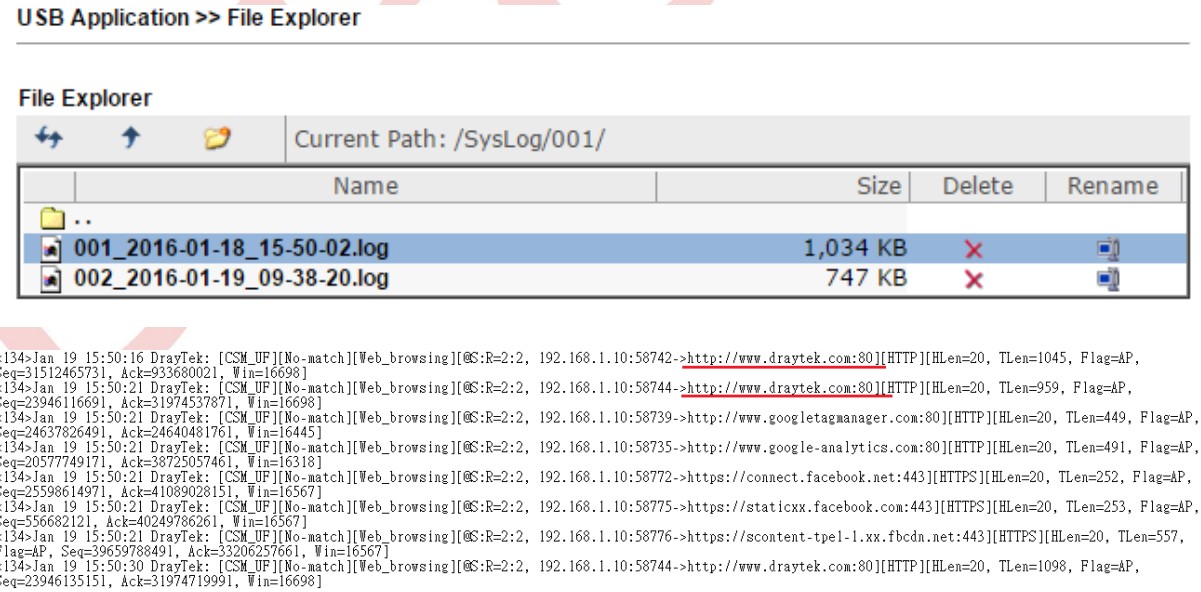
5. Bir takın ve Bağlantı Durumunun " Disk connected" gösterip göstermediğini kontrol etmek için **USB Application >> USB Device Status'e** gidin .



6. Syslog'u USB sürücüye kaydetmek için, **System Maintenance >> SysLog / Mail Alert Setup** sayfasına gidin.
   a. **Syslog Access'i** etkinleştirin.
   b. Logların aygıta kaydedileceğinden emin olmak için **USB Disk'i** etkinleştirin.
   c. Yalnızca Firewall Log'u etkinleştirin.
   d. Kaydetmek için **OK'a** tıklayın.



1. Yukarıdaki ayarlar tamamlandığında, USB cihazındaki yeni bir “SysLog” klasörüne kaydedilen logları kontrol etmek için **USB Application >> File Explorer’a** gidin. Web siteleri geçmişi, ağ yöneticilerinin net bir şekilde kontrol edebileceği gibi birer birer kaydedilir.



<134>Jan 19 15:50:16 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58742->http://www.draytek.com:80][HTTP][HLen=20, TLen=1045, Flag=AP, Seq=31512465731, Ack=933680021, Win=16698]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58744->http://www.draytek.com:80][HTTP][HLen=20, TLen=959, Flag=AP, Seq=23946116691, Ack=31974537871, Win=16698]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58739->http://www.googletagmanager.com:80][HTTP][HLen=20, TLen=449, Flag=AP, Seq=24637826491, Ack=24640481761, Win=16445]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58735->http://www.google-analytics.com:80][HTTP][HLen=20, TLen=491, Flag=AP, Seq=20577749171, Ack=38725057461, Win=16318]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58772->https://connect.facebook.net:443][HTTPS][HLen=20, TLen=252, Flag=AP, Seq=25598614971, Ack=41089028151, Win=16567]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58775->https://staticxx.facebook.com:443][HTTPS][HLen=20, TLen=253, Flag=AP, Seq=556682121, Ack=40249786261, Win=16567]
<134>Jan 19 15:50:21 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58776->https://scontent-tpe1-1.xx.fbcdn.net:443][HTTPS][HLen=20, TLen=557, Flag=AP, Seq=39659788491, Ack=33206257661, Win=16567]
<134>Jan 19 15:50:30 DrayTek: [CSM_UF][No-match][Web_browsing][@S:R=2:2, 192.168.1.10:58744->http://www.draytek.com:80][HTTP][HLen=20, TLen=1098, Flag=AP, Seq=23946135151, Ack=31974719991, Win=16698]