

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.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text" value="test"/>
Contents	<input type="text" value="facebookisface.com"/>

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

2. **CSM >> URL Content Filter Profile'da** bir URL Content Filter profili oluşturun, Profil numarasına tıklayın.
 - a. **Profile name** girin.
 - b. **Prioriyi** 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.

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:	test	
Priority:	Either : URL Access Control First ▼	Log: All ▼
1.URL Access Control		
<input checked="" type="checkbox"/> Enable URL Access Control	<input type="checkbox"/> Prevent web access from IP address	
Action:	Group/Object Selections	
Block ▼	test	Edit
<input type="checkbox"/> Exception List		Edit
2.Web Feature		
<input type="checkbox"/> Enable Restrict Web Feature		
Action:	File Extension Profile: None ▼	
Pass ▼	<input type="checkbox"/> Cookie	<input type="checkbox"/> Proxy
	<input type="checkbox"/> Upload	

OK Clear Cancel

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.

CSM >> DNS Filter

Index No. 1

Profile Name	test
Syslog	None ▼
WCF	None ▼
UCF	UCF-1 test ▼

OK Clear Cancel

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.

Application	Action/Profile	Syslog
Filter:	Pass Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	<input type="checkbox"/>
Sessions Control	43 / 60000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
<u>Quality of Service</u>	None	<input type="checkbox"/>
<u>APP Enforcement:</u>	None	<input type="checkbox"/>
<u>URL Content Filter:</u>	1-test	<input checked="" type="checkbox"/>
<u>Web Content Filter:</u>	None	<input type="checkbox"/>
<u>DNS Filter</u>	1-test	<input checked="" type="checkbox"/>

Advance Setting

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 .

USB Application >> USB Device Status

Disk	Modem	Printer	Sensor	Refresh
USB Mass Storage Device Status				
Connection Status: Disk Connected				<input type="button" value="Disconnect USB Disk"/>
Write Protect Status: No				
Disk Capacity: 3829 MB				
Free Capacity: 3820 MB Refresh				
USB Disk Users Connected				
Index	Service	IP Address(Port)	Username	

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

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

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input type="checkbox"/> Syslog Server</p> <p><input checked="" type="checkbox"/> USB Disk</p> <p>Router Name <input type="text" value="DrayTek"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input type="checkbox"/> VPN Log</p> <p><input type="checkbox"/> User Access Log</p> <p><input type="checkbox"/> WAN Log</p> <p><input type="checkbox"/> Router/DSL information</p> <p>AlertLog Setup</p> <p><input type="checkbox"/> Enable</p> <p>AlertLog Port <input type="text" value="514"/></p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> APPE</p> <p><input checked="" type="checkbox"/> VPN LOG</p> <p><input type="checkbox"/> APPE Signature</p>
---	---

- Note:** 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
 3. We only support secured SMTP connection on port 465.

- 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.

USB Application >> File Explorer

File Explorer

Current Path: /SysLog/001/

Name	Size	Delete	Rename
..			
001_2016-01-18_15-50-02.log	1,034 KB	X	
002_2016-01-19_09-38-20.log	747 KB	X	

```
<134>Jan 19 15:50:16 DrayTek: [CSM_UF][No-match][Web_browsing][@G: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][@G: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][@G: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][@G: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][@G: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][@G: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][@G:R=2:2, 192.168.1.10:58776->https://scontent-tpel-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][@G: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]
```