İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING 4](#_Toc330026388)

[TEMEL PARSING YAPISI 5](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 25.9.2012 | V1 | Zyxel Zywall USG 300 | Hüseyin Sevin |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | Zyxel Zywall USG 300 |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | ZyxelZywalLUSG\_300\_V1\_1\_1\_Web\_Recorder |
| İstek yapan Adı Soyadı | Hüseyin Sevin |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 25.09.2012 |
| İstek yapılan kurum adı | TCDD 7. Bölge Müdürlüğü Afyon |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | Syslog |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# 

# ÖRNEK PARSING

|  |  |
| --- | --- |
| Local7.Alert 10.3.5.111 Sep 25 10:56:12 2012 zywall-usg-300 src="10.3.4.34:2536" dst="93.184.220.20:80" msg="web1.kure.tv: Audio/Video Clips(cache hit)" note="WEB BLOCK:BLUECOAT" user="unknown" devID="0019cb9747d9" cat="Blocked Web Sites" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Sep 25 10:56:12 2012 |
| SOURCENAME | Local7.Alert |
| EVENTCATEGORY | Blocked Web Sites |
| EVENTTYPE |  |
| USERSID | unknown |
| LOGNAME | ZyxelZywalLUSG\_300\_V1\_1\_1\_Web\_Recorder |
| COMPUTERNAME | 10.3.5.111 |
| CUSTOMSTR1 | 0019cb9747d9 Device ID |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.3.4.34 Source IP |
| CUSTOMSTR4 | 93.184.220.20 Destination IP |
| CUSTOMSTR5 | Audio/Video Clips(cache hit) Kategori |
| CUSTOMSTR6 | web1.kure.tv URL |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 2536 Source Port |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 80 Destination Port |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |