İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 08.11.2012 | Version 1.2.3 | Pfsense |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | PFSENSE |
| Versiyonu | 1.2.3 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | PFSENSE |
| İstek yapan Adı Soyadı | Hikmet Akdemir |
| Geliştirici Adı Soyadı |  |
| İstek tarihi | 08.11.2012 |
| İstek yapılan kurum adı | Boğaziçi Üniv. |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
|  | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2011-11-08 16:05:34 |
| SOURCENAME | Local01.Info |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME | Pfsense SysLog Recorder |
| COMPUTERNAME | 192.168.192.68 |
| CUSTOMSTR1 | tos 0x0 |
| CUSTOMSTR2 | S, cksum 0x5f4d (correct), 2348996315:2348996315(0) win 8192 <mss 1386,nop,wscale 2,nop,nop,sackOK> |
| CUSTOMSTR3 | 192.168.64.35 |
| CUSTOMSTR4 | 206.165.250.97 |
| CUSTOMSTR5 | ttl 127 |
| CUSTOMSTR6 | id 39014 |
| CUSTOMSTR7 | offset 0 |
| CUSTOMSTR8 | flags [DF] |
| CUSTOMSTR9 | proto TCP (6) |
| CUSTOMSTR10 | length 52 |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 11-08-2012 15:59:02 Local0.Info 192.168.192.68 Nov 8 16:05:34 pf: 005133 rule 80/0(match): pass in on em0: (tos 0x60, ttl 127, id 39014, offset 0, flags [DF], proto TCP (6), length 52) 192.168.64.35.49937 > 206.165.250.97.80: S, cksum 0x5f4d (correct), 2348996315:2348996315(0) win 8192 <mss 1386,nop,wscale 2,nop,nop,sackOK> |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | 2011-11-08 16:05:34 |
| SOURCENAME | Local01.Info |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME | Pfsense SysLog Recorder |
| COMPUTERNAME | 192.168.192.68 |
| CUSTOMSTR1 | tos 0x0 |
| CUSTOMSTR2 | S, cksum 0x5f4d (correct), 2348996315:2348996315(0) win 8192 <mss 1386,nop,wscale 2,nop,nop,sackOK> |
| CUSTOMSTR3 | 192.168.64.35 |
| CUSTOMSTR4 | 206.165.250.97 |
| CUSTOMSTR5 | ttl 127 |
| CUSTOMSTR6 | id 39014 |
| CUSTOMSTR7 | offset 0 |
| CUSTOMSTR8 | flags [DF] |
| CUSTOMSTR9 | proto TCP (6) |
| CUSTOMSTR10 | length 52 |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 11-08-2012 15:59:02 Local0.Info 192.168.192.68 Nov 8 16:05:34 pf: 005133 rule 80/0(match): pass in on em0: (tos 0x60, ttl 127, id 39014, offset 0, flags [DF], proto TCP (6), length 52) 192.168.64.35.49937 > 206.165.250.97.80: S, cksum 0x5f4d (correct), 2348996315:2348996315(0) win 8192 <mss 1386,nop,wscale 2,nop,nop,sackOK> |