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 |
|  |  |  |  |
| 08.01.2012 | V.1 | Beşiktaş Belediyesi için Squid loğlarının syslog ile alımının yapılması gerekmektedir. | Emrehan Mert |
| 14.01.2013 | v.1.0.1 | Pfsense web proxy nin gönderdiği full url adlarında yalnızca site isminin ayrı bir kolona parse edilmesi çalışması | Emre BAŞTUĞ |
| 24.06.2013 | v.1.0.2 | Proxy loglarının yeniden düzenlenmesi ve Firewall loglarının da parsinge dahil edilmesi. | Emre BAŞTUĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | PFSENSE Proxy |
| Versiyonu | Current: 2.7.9 pkg v.4.3.1 Installed: 2.7.9\_4.1 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | SquidSyslogV\_1\_0\_1Recorder |
| İstek yapan Adı Soyadı | Emre BAŞTUĞ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 14.01.2013 |
| İstek yapılan kurum adı | Beşiktaş Belediyesi |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no | - |
| İlgili ham log yolu/dosya ismi | Syslog udp 514 |
| İlişkili form adı | - |
| Servis Yetkilisi Notları | - |
| Geliştirici Notları | - |

# ÖRNEK PARSING -1

|  |  |
| --- | --- |
| **172.16.1.25:514 : local4.info Jan 7 13:53:09 squid[44380]: 1357559589.677 1117 172.16.10.115 TCP\_MISS/200 16071 GET http://www.google.com.tr/extern\_chrome/e1b299cac46c21f3.js - DIRECT/173.194.70.94 text/javascript** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jan 7 13:53:09** |
| SOURCENAME |  |
| EVENTCATEGORY | **TCP\_MISS** |
| EVENTTYPE | **GET** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | **text/javascript** |
| CUSTOMSTR3 | **172.16.10.115** |
| CUSTOMSTR4 | **DIRECT** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **173.194.70.94** |
| CUSTOMSTR8 | **www.google.com.tr** |
| CUSTOMSTR9 | **/extern\_chrome/e1b299cac46c21f3.js** |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **200** |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local4.info Jan 7 13:53:09 squid[44380]: 1357559589.677 1117 172.16.10.115 TCP\_MISS/200 16071 GET http://www.google.com.tr/extern\_chrome/e1b299cac46c21f3.js - DIRECT/173.194.70.94 text/javascript |

# TEMEL PARSING YAPISI -1

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY | TCP\_MISS : Response işlemi tamamlandı. |
| EVENTTYPE | Http istek tipi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 | Request edilen web objesi sunucudan fetch edildi |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef Url in IP adresi |
| CUSTOMSTR8 | Hedef Url Adı |
| CUSTOMSTR9 | Hedef url içerik kategorisi |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | Http status code (bağlantı ok) |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -2

|  |  |
| --- | --- |
| **172.16.1.25:514 : local4.info Jun 21 10:18:57 squid[42013]: 1371799137.675 1392 172.16.10.85 TCP\_HIT/200 304974 GET http://s.ytimg.com/yts/swfbin/watch\_as3-vflBp0oGe.swf - NONE/- application/x-shockwave-flash** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jun 21 10:18:57** |
| SOURCENAME |  |
| EVENTCATEGORY | **TCP\_HIT** |
| EVENTTYPE | **GET** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | **application/x-shockwave-flash** |
| CUSTOMSTR3 | **172.16.10.85** |
| CUSTOMSTR4 | **NONE** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | **s.ytimg.com** |
| CUSTOMSTR9 | **/yts/swfbin/watch\_as3-vflBp0oGe.swf** |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **200** |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local4.info Jun 21 10:18:57 squid[42013]: 1371799137.675 1392 172.16.10.85 TCP\_HIT/200 304974 GET http://s.ytimg.com/yts/swfbin/watch\_as3-vflBp0oGe.swf - NONE/- application/x-shockwave-flash |

# TEMEL PARSING YAPISI -2

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | Tarih |
| SOURCENAME |  |
| EVENTCATEGORY | TCP\_HIT : Local Cache den dönen Response işlemi tamamlandı. |
| EVENTTYPE | Http istek tipi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 | Squid unusual bir request aldığında NONE olarak tag lemektedir. |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | Hedef Url Adı |
| CUSTOMSTR9 | Hedef Url İçerik Kategorisi |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | Http status code (bağlantı ok) |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -3

|  |  |
| --- | --- |
| **172.16.1.25:514** : **local4.info** **Jun 24 15:53:05** **squid[32700]:** **1372078385.667 63346** **172.16.10.97** **TCP\_MISS/200** **1894 CONNECT** **ssl.google-analytics.com**:**443** - **DIRECT**/**173.194.35.62** - | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jun 24 15:53:05** |
| SOURCENAME |  |
| EVENTCATEGORY | **TCP\_MISS** |
| EVENTTYPE | **CONNECT** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.10.97** |
| CUSTOMSTR4 | **DIRECT** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **173.194.35.62** |
| CUSTOMSTR8 | **ssl.google-analytics.com** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **200** |
| CUSTOMINT2 | **443** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local4.info Jun 24 15:53:05 squid[32700]: 1372078385.667 63346 172.16.10.97 TCP\_MISS/200 1894 CONNECT ssl.google-analytics.com:443 - DIRECT/173.194.35.62 - |

# TEMEL PARSING YAPISI -3

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | Tarih |
| SOURCENAME |  |
| EVENTCATEGORY | TCP\_MISS : Response işlemi tamamlandı. |
| EVENTTYPE | Http istek tipi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 | Request edilen web objesi sunucudan fetch edildi |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef Url in IP adresi |
| CUSTOMSTR8 | Hedef Url Adı |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | Http status code (bağlantı ok) |
| CUSTOMINT2 | Hedef Port |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -4

|  |  |
| --- | --- |
| **172.16.1.25:514 : local0.info Jun 21 10:19:02 pf: 028130 rule 45/0(match): pass in on le0: (tos 0x0, ttl 128, id 42988, offset 0, flags [none], proto UDP (17), length 59) 172.16.1.26.63541 > 208.78.71.34.53: 14570 A?. (31)** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jun 21 10:19:02** |
| SOURCENAME | **le0** |
| EVENTCATEGORY | **UDP** |
| EVENTTYPE | **pass** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.1.26** |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **208.78.71.34** |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | **53** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local0.info Jun 21 10:19:02 pf: 028130 rule 45/0(match): pass in on le0: (tos 0x0, ttl 128, id 42988, offset 0, flags [none], proto UDP (17), length 59) 172.16.1.26.63541 > 208.78.71.34.53: 14570 A?. (31) |

# TEMEL PARSING YAPISI -4

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Local Ethernet |
| EVENTCATEGORY | Tcp / Udp protocol tipi |
| EVENTTYPE | Firewall blokladı / izin Verdi bilgisi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef Url in IP adresi |
| CUSTOMSTR8 | Hedef Url Adı |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | Port bilgisi |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -5

|  |  |
| --- | --- |
| **172.16.1.25:514 : local0.info Jun 24 15:53:05 pf: 571253 rule 78/0(match): block**  **in on le1: (tos 0x0, ttl 120, id 56920, offset 0, flags [DF], proto TCP (6),**  **length 576) 188.132.199.50.53374 > 95.0.126.2.23449: . 0:536(536) ack 1 win**  **64240** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jun 24 15:53:05** |
| SOURCENAME | **le1** |
| EVENTCATEGORY | **TCP** |
| EVENTTYPE | **block** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **188.132.199.50** |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **95.0.126.2** |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | **23449** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local0.info Jun 24 15:53:05 pf: 571253 rule 78/0(match): block  in on le1: (tos 0x0, ttl 120, id 56920, offset 0, flags [DF], proto TCP (6),  length 576) 188.132.199.50.53374 > 95.0.126.2.23449: . 0:536(536) ack 1 win  64240 |

# TEMEL PARSING YAPISI -5

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Local Ethernet |
| EVENTCATEGORY | Tcp / Udp protocol tipi |
| EVENTTYPE | Firewall blokladı / izin Verdi bilgisi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef Url in IP adresi |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | Port bilgisi |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING -6

|  |  |
| --- | --- |
| **172.16.1.25:514 : local0.info Jun 24 15:53:05 pf: 275141 rule 45/0(match): pass**  **in on le0: (tos 0x0, ttl 128, id 29025, offset 0, flags [DF], proto TCP (6),**  **length 56) 172.16.4.21.57007 > 95.0.139.179.443: S, cksum 0x2460 (correct),**  **513236376:513236376(0) win 8192 <mss 1460,sackOK,timestamp 1405078651 0>** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **Jun 24 15:53:05** |
| SOURCENAME | **le0** |
| EVENTCATEGORY | **TCP** |
| EVENTTYPE | **pass** |
| USERSID |  |
| LOGNAME | SquidSyslogV\_1\_0\_0Recorder |
| COMPUTERNAME | **172.16.1.25:514** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **172.16.4.21** |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **95.0.139.179** |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | **443** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 172.16.1.25:514 : local0.info Jun 24 15:53:05 pf: 275141 rule 45/0(match): pass  in on le0: (tos 0x0, ttl 128, id 29025, offset 0, flags [DF], proto TCP (6),  length 56) 172.16.4.21.57007 > 95.0.139.179.443: S, cksum 0x2460 (correct),  513236376:513236376(0) win 8192 <mss 1460,sackOK,timestamp 1405078651 0> |

# TEMEL PARSING YAPISI -6

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Local Ethernet |
| EVENTCATEGORY | Tcp / Udp protocol tipi |
| EVENTTYPE | Firewall blokladı / izin Verdi bilgisi |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Request gönderen local ip |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef Url in IP adresi |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 | Port bilgisi |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |