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 |
| 25.01.2013 | V1.0 | Sonicwall TZ-120 logları için dll hazırlanması | Emre BAŞTUĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Sonicwall TZ-120 UTM Firewall - Proxy |
| Versiyonu | 1.0.0 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | SonicWallV\_TZ120\_0\_0UTMRecorder |
| İstek yapan Adı Soyadı | Emre BAŞTUĞ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 25.01.2013 |
| İstek yapılan kurum adı | Kesir Mühendislik |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | UDP:514 syslog |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

**ÖRNEK PARSING -1**

|  |  |
| --- | --- |
| **192.168.3.1:514 : local0.info id=firewall sn=0017C56122AA time="2013-01-25 13:29:04 UTC" fw=none pri=6 c=1024 m=97 n=5468903 src=192.168.3.122:1140:X0:tubakara.kesir.local dst=212.68.59.208:80:X1:static-208-59-68-212.sadecehosting.net proto=tcp/http op=GET rcvd=200 result=403 dstname=cluster.linkz.net arg=/linkz/k?p=10472&ru=http%3A%2F%2Fwww.haber365.com%2FHaber%2FCan\_Tanriyar\_Petek\_Benim\_Kardesimdir%2F&refu=http% code=4 Category="Pornography"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013-01-25 13:29:04** |
| SOURCENAME | **local0.info** |
| EVENTCATEGORY | **GET** |
| EVENTTYPE | **info** |
| USERSID | **tubakara.kesir.local** |
| LOGNAME |  |
| COMPUTERNAME | **192.168.3.1** |
| CUSTOMSTR1 | **Pornography** |
| CUSTOMSTR2 | **tcp/http** |
| CUSTOMSTR3 | **192.168.3.122** |
| CUSTOMSTR4 | **212.68.59.208** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **/Haber/Can\_Tanriyar\_Petek\_Benim\_Kardesimdir/** |
| CUSTOMSTR8 | **www.haber365.com** |
| CUSTOMSTR9 | **cluster.linkz.net** |
| CUSTOMSTR10 | **static-208-59-68-212.sadecehosting.net** |
| CUSTOMINT1 | **403** |
| CUSTOMINT2 | **200** |
| CUSTOMINT3 | **1140** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 | **6** |
| CUSTOMINT6 | **1024** |
| CUSTOMINT7 | **97** |
| CUSTOMINT8 | **5468903** |
| CUSTOMINT9 | **4** |
| CUSTOMINT10 |  |
| DESCRIPTION | **192.168.3.1:514 : local0.info id=firewall sn=0017C56122AA time="2013-01-25 13:29:04 UTC" fw=none pri=6 c=1024 m=97 n=5468903 src=192.168.3.122:1140:X0:tubakara.kesir.local dst=212.68.59.208:80:X1:static-208-59-68-212.sadecehosting.net proto=tcp/http op=GET rcvd=200 result=403 dstname=cluster.linkz.net arg=/linkz/k?p=10472&ru=http%3A%2F%2Fwww.haber365.com%2FHaber%2FCan\_Tanriyar\_Petek\_Benim\_Kardesimdir%2F&refu=http% code=4 Category="Pornography"** |

**TEMEL PARSING YAPISI 1**

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Log Severity/Priority - Log Level |
| EVENTCATEGORY |  |
| EVENTTYPE | Log Severity/Priority - Log Level |
| USERSID | Source user |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 | Proxy Rule Açıklaması |
| CUSTOMSTR2 | Protokol tipi |
| CUSTOMSTR3 | Source ip |
| CUSTOMSTR4 | Destination ip |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef sitenin alt sayfaları |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 | Destination name |
| CUSTOMSTR10 | Hedef sitenin IP adresinin DNS serverdaki PTR kaydı |
| CUSTOMINT1 | Request sonucu |
| CUSTOMINT2 | Alınan paket size ı |
| CUSTOMINT3 | Source port |
| CUSTOMINT4 | Destination port |
| CUSTOMINT5 | Message Priority, Event önem değeri (0=emergency, 7=debug) |
| CUSTOMINT6 | Message Category |
| CUSTOMINT7 | Message ID |
| CUSTOMINT8 | Message Count (olayın kaç kez oluştuğu) |
| CUSTOMINT9 | Blocking Code (Blok Kodu Kategorisi) |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

**ÖRNEK PARSING -2**

|  |  |
| --- | --- |
| **192.168.3.1:514 : local0.error id=firewall sn=0017C56122AA time="2013-01-25 14:00:05 UTC" fw=none pri=3 c=4 m=14 msg="Web site access denied" n=199075 src=192.168.3.121:2004:X0:zarifeyuksell.kesir.local dst=2.23.95.139:80:X1: dstname=connect.facebook.net arg=/en\_US/all.js code=58 Category="Social Networking"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013-01-25 13:29:04** |
| SOURCENAME | **local0.error** |
| EVENTCATEGORY |  |
| EVENTTYPE | **error** |
| USERSID | **zarifeyuksell.kesir.local** |
| LOGNAME |  |
| COMPUTERNAME | **192.168.3.1** |
| CUSTOMSTR1 | **Social Networking** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **192.168.3.121** |
| CUSTOMSTR4 | **2.23.95.139** |
| CUSTOMSTR5 | **Web site access denied** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **/en\_US/all.js** |
| CUSTOMSTR8 | **connect.facebook.net** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **2004** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 | **3** |
| CUSTOMINT6 | **4** |
| CUSTOMINT7 | **14** |
| CUSTOMINT8 | **199075** |
| CUSTOMINT9 | **58** |
| CUSTOMINT10 |  |
| DESCRIPTION | **192.168.3.1:514 : local0.error id=firewall sn=0017C56122AA time="2013-01-25 14:00:05 UTC" fw=none pri=3 c=4 m=14 msg="Web site access denied" n=199075 src=192.168.3.121:2004:X0:zarifeyuksell.kesir.local dst=2.23.95.139:80:X1: dstname=connect.facebook.net arg=/en\_US/all.js code=58 Category="Social Networking"** |
|  |  |

**TEMEL PARSING YAPISI 2**

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Log Severity/Priority - Log Level |
| EVENTCATEGORY |  |
| EVENTTYPE | Log Severity/Priority - Log Level |
| USERSID | Source user |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 | Proxy Rule Açıklaması (hedef site kategori tanımlaması) |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | Source ip |
| CUSTOMSTR4 | Destination ip |
| CUSTOMSTR5 | Request sonucu firewall yanıtı |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef sitenin alt sayfaları |
| CUSTOMSTR8 | Destination site hostname |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | Source port |
| CUSTOMINT4 | Destination port |
| CUSTOMINT5 | Message Priority, Event önem değeri (0=emergency, 7=debug) |
| CUSTOMINT6 | Message Category |
| CUSTOMINT7 | Message ID |
| CUSTOMINT8 | Message Count (olayın kaç kez oluştuğu) |
| CUSTOMINT9 | Blocking Code (Blok Kodu Kategorisi) |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

**ÖRNEK PARSING -3**

|  |  |
| --- | --- |
| **192.168.3.1:514 : local0.debug id=firewall sn=0017C56122AA time="2013-01-25 12:10:54 UTC" fw=none pri=7 c=512 m=46 msg="Broadcast packet dropped" n=12086307 src=192.168.3.100:0:X0: dcsrv1.kesir.local dst=192.168.3.255:40932:: proto=udp/netbios-ns** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013-01-25 12:10:54** |
| SOURCENAME | **local0. debug** |
| EVENTCATEGORY |  |
| EVENTTYPE | **debug** |
| USERSID | **dcsrv1.kesir.local** |
| LOGNAME |  |
| COMPUTERNAME | **192.168.3.1** |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | **udp/netbios-ns** |
| CUSTOMSTR3 | **192.168.3.100** |
| CUSTOMSTR4 | **192.168.3.255** |
| CUSTOMSTR5 | **Broadcast packet dropped** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **0** |
| CUSTOMINT4 | **40932** |
| CUSTOMINT5 | **7** |
| CUSTOMINT6 | **512** |
| CUSTOMINT7 | **46** |
| CUSTOMINT8 | **12086307** |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | **192.168.3.1:514 : local0.debug id=firewall sn=0017C56122AA time="2013-01-25 12:10:54 UTC" fw=none pri=7 c=512 m=46 msg="Broadcast packet dropped" n=12086307 src=192.168.3.100:0:X0: dcsrv1.kesir.local dst=192.168.3.255:40932:: proto=udp/netbios-ns** |

**TEMEL PARSING YAPISI 3**

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Log Severity/Priority - Log Level |
| EVENTCATEGORY |  |
| EVENTTYPE | Log Severity/Priority - Log Level |
| USERSID | Source user |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 | Protokol tipi |
| CUSTOMSTR3 | Source ip |
| CUSTOMSTR4 | Destination ip |
| CUSTOMSTR5 | Request Sonucu Firewall Yanıtı |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | Source port |
| CUSTOMINT4 | Destination port |
| CUSTOMINT5 | Message Priority, Event önem değeri (0=emergency, 7=debug) |
| CUSTOMINT6 | Message Category |
| CUSTOMINT7 | Message ID |
| CUSTOMINT8 | Message Count (olayın kaç kez oluştuğu) |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

**ÖRNEK PARSING -4**

|  |  |
| --- | --- |
| **192.168.3.1:514 : local0.info id=firewall sn=0017C56122AA time="2013-01-25 12:10:54 UTC" fw=none pri=6 c=1024 m=97 n=5449317 src=192.168.3.228:58211:X0:DGS-DGS dst=173.194.67.94:80:X1:wi-in-f94.1e100.net proto=tcp/http op=GET sent=1592 rcvd=335 result=0 dstname=www.google.com.tr arg=/csi?v=3&s=web&action=&ei=SnYCUbusOonb0QWJj4D4BA&e=17259,18168,39523,39977,3300006,3300104,3300122,3300133,330 code=29 Category="Search Engines and Portals"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013-01-25 12:10:54** |
| SOURCENAME | **local0.info** |
| EVENTCATEGORY | **GET** |
| EVENTTYPE | **info** |
| USERSID | **DGS-DGS** |
| LOGNAME |  |
| COMPUTERNAME | **192.168.3.1** |
| CUSTOMSTR1 | **Search Engines and Portals** |
| CUSTOMSTR2 | **tcp/http** |
| CUSTOMSTR3 | **192.168.3.228** |
| CUSTOMSTR4 | **173.194.67.94** |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **/csi?v=3&s=web&action=&ei=SnYCUbusOonb0QWJj4D4BA&e=17259,18168,39523,39977,3300006,3300104,3300122,3300133,330** |
| CUSTOMSTR8 | **www.google.com.tr** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | **wi-in-f94.1e100.net** |
| CUSTOMINT1 | **0** |
| CUSTOMINT2 | **335** |
| CUSTOMINT3 | **58211** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 | **6** |
| CUSTOMINT6 | **1024** |
| CUSTOMINT7 | **97** |
| CUSTOMINT8 | **5449317** |
| CUSTOMINT9 | **29** |
| CUSTOMINT10 | **1592** |
| DESCRIPTION | **192.168.3.1:514 : local0.info id=firewall sn=0017C56122AA time="2013-01-25 12:10:54 UTC" fw=none pri=6 c=1024 m=97 n=5449317 src=192.168.3.228:58211:X0:DGS-DGS dst=173.194.67.94:80:X1:wi-in-f94.1e100.net proto=tcp/http op=GET sent=1592 rcvd=335 result=0 dstname=www.google.com.tr arg=/csi?v=3&s=web&action=&ei=SnYCUbusOonb0QWJj4D4BA&e=17259,18168,39523,39977,3300006,3300104,3300122,3300133,330 code=29 Category="Search Engines and Portals"** |

**TEMEL PARSING YAPISI 4**

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME | Log Severity/Priority - Log Level |
| EVENTCATEGORY |  |
| EVENTTYPE | Log Severity/Priority - Log Level |
| USERSID | Source user |
| LOGNAME |  |
| COMPUTERNAME | Firewall IP |
| CUSTOMSTR1 | Proxy Rule Açıklaması |
| CUSTOMSTR2 | Protokol tipi |
| CUSTOMSTR3 | Source ip |
| CUSTOMSTR4 | Destination ip |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | Hedef sitenin alt sayfaları |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 | Destination name |
| CUSTOMSTR10 | Hedef sitenin IP adresinin DNS serverdaki PTR kaydı |
| CUSTOMINT1 | Request sonucu |
| CUSTOMINT2 | Alınan paket size ı |
| CUSTOMINT3 | Source port |
| CUSTOMINT4 | Destination port |
| CUSTOMINT5 | Message Priority, Event önem değeri (0=emergency, 7=debug) |
| CUSTOMINT6 | Message Category |
| CUSTOMINT7 | Message ID |
| CUSTOMINT8 | Message Count (olayın kaç kez oluştuğu) |
| CUSTOMINT9 | Blocking Code (Blok Kodu Kategorisi) |
| CUSTOMINT10 | Gönderilen Paket size ı |
| DESCRIPTION | Full Log |