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 |
| 18.03.2013 | V.1 | FortiGateSyslogV5\_0\_0Recorder | Deniz Aksoy |
| 14.06.2013 | V.2 | Deniz Bey tarafından istenip geliştirilen  FortiGateSyslogV5\_0\_0Recorder’ın parsing yapısına DHCP loğlarının parsingi eklenmesi gerekmektedir. | Ali Bozdağ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | 01 |
| Ürün Adı | FORTIGATE |
| Versiyonu | 5.0 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | FortiGateSyslogV5\_0\_1Recorder.dll |
| İstek yapan Adı Soyadı | Ali Bozdağ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 14.06.2013 |
| İstek yapılan kurum adı | TIGEM |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | SYSLOG |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# PARSING TRAFFIC

|  |  |
| --- | --- |
| 10.0.0.138:1024 local7.notice date=2013-03-12 time=08:06:47 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.11.74 srcport=49275 srcintf="port19" dstip=80.239.149.35 dstport=80 dstintf="port22" sessionid=18734090 status=close user="SGOKYOKUS" group="fsso.bim" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=49275 service=HTTP proto=6 applist="client.yonetici" duration=102 sentbyte=953 rcvdbyte=744 sentpkt=8 rcvdpkt=7 identidx=1 utmaction=passthrough utmevent=webfilter utmsubtype=urlfilter hostname="crl.microsoft.com"  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:55:28 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.12.112 srcport=51109 srcintf="port19" dstip=80.239.148.94 dstport=80 dstintf="port22" sessionid=18945782 status=close user="MATALAY" group="fsso.cevre" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=51109 service=HTTP proto=6 applist="block-p2p-proxy-botnet" duration=97 sentbyte=1896 rcvdbyte=23650 sentpkt=22 rcvdpkt=22 identidx=6 utmaction=passthrough utmevent=webfilter utmsubtype=ftgd-quota hostname="sphotos-a.ak.fbcdn.net" catdesc="Social Networking"  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:55:20 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.12.98 srcport=50362 srcintf="port19" dstip=80.239.216.146 dstport=80 dstintf="port22" sessionid=18949859 status=close user="FBALANTEKIN" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=50362 service=HTTP proto=6 applist="block-p2p-proxy-botnet" duration=30 sentbyte=268 rcvdbyte=546 sentpkt=5 rcvdpkt=3 identidx=7  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:54:16 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.48 srcport=50420 srcintf="port19" dstip=80.239.149.8 dstport=80 dstintf="port22" sessionid=18938504 status=close user="IUCAR" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=50420 service=HTTP proto=6 applist="block-p2p-proxy-botnet" duration=126 sentbyte=721 rcvdbyte=557 sentpkt=5 rcvdpkt=5 identidx=7 utmaction=passthrough utmevent=webfilter utmsubtype=ftgd-quota hostname="external.ak.fbcdn.net" catdesc="Social Networking"  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:04:56 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.43 srcport=50844 srcintf="port19" dstip=80.239.149.8 dstport=8008 dstintf="port22" sessionid=18729798 status=close user="KUNALDI" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=50844 service=8008/tcp proto=6 applist="block-p2p-proxy-botnet" duration=60 sentbyte=0 rcvdbyte=24021 sentpkt=0 rcvdpkt=18 identidx=7  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:04:56 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.43 srcport=50845 srcintf="port19" dstip=80.239.149.8 dstport=8008 dstintf="port22" sessionid=18729799 status=close user="KUNALDI" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=50845 service=8008/tcp proto=6 applist="block-p2p-proxy-botnet" duration=60 sentbyte=0 rcvdbyte=18057 sentpkt=0 rcvdpkt=14 identidx=7  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:04:56 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.43 srcport=50846 srcintf="port19" dstip=80.239.149.8 dstport=8008 dstintf="port22" sessionid=18729800 status=close user="KUNALDI" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=50846 service=8008/tcp proto=6 applist="block-p2p-proxy-botnet" duration=60 sentbyte=0 rcvdbyte=19695 sentpkt=0 rcvdpkt=16 identidx=7  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:07:34 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.43 srcport=51122 srcintf="port19" dstip=80.239.149.34 dstport=443 dstintf="port22" sessionid=18737556 status=close user="KUNALDI" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=51122 service=HTTPS proto=6 applist="block-p2p-proxy-botnet" duration=97 sentbyte=132 rcvdbyte=132 sentpkt=3 rcvdpkt=3 identidx=7  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:06:47 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.20 srcport=2047 srcintf="port19" dstip=80.239.149.35 dstport=80 dstintf="port22" sessionid=18739760 status=close user="NUNVER" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=62463 service=HTTP proto=6 applist="block-p2p-proxy-botnet" duration=11 sentbyte=934 rcvdbyte=4321 sentpkt=5 rcvdpkt=6 identidx=7 utmaction=blocked utmevent=webfilter utmsubtype=ftgd-cat hostname="static.ak.facebook.com" catdesc="Social Networking"  10.0.0.138:1024 local7.notice date=2013-03-12 time=08:06:48 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.0.10.20 srcport=2049 srcintf="port19" dstip=80.239.149.35 dstport=80 dstintf="port22" sessionid=18739767 status=close user="NUNVER" group="fsso.emlak" policyid=76 dstcountry="Europe" srccountry="Reserved" trandisp=snat transip=212.174.166.144 transport=62465 service=HTTP proto=6 applist="block-p2p-proxy-botnet" duration=11 sentbyte=1022 rcvdbyte=4321 sentpkt=8 rcvdpkt=6 identidx=7 utmaction=blocked utmevent=webfilter utmsubtype=ftgd-cat hostname="static.ak.facebook.com" catdesc="Social Networking" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME | Level |
| EVENT ID |  |
| EVENTCATEGORY | TRAFFIC |
| EVENTTYPE | Subtype |
| USERSID | user,group |
| LOGNAME |  |
| COMPUTERNAME | devname |
| CUSTOMSTR1 | status |
| CUSTOMSTR2 | service |
| CUSTOMSTR3 | srcip |
| CUSTOMSTR4 | dstip |
| CUSTOMSTR5 | app,applist |
| CUSTOMSTR6 | Utmaction |
| CUSTOMSTR7 | Utmevent |
| CUSTOMSTR8 | hostname |
| CUSTOMSTR9 | catdesc |
| CUSTOMSTR10 | vpn |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | srcport |
| CUSTOMINT4 | Dstport |
| CUSTOMINT5 | SentByte |
| CUSTOMINT6 | RcvdByte |
| CUSTOMINT7 | Policyid |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 | Duration |
| DESCRIPTION | ALL DATA |

# PARSING EVENT

|  |  |
| --- | --- |
| 10.0.0.138:1025 : local7.notice date=2013-03-15 time=22:22:04 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037129 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="78b2ee36ed800ce7/1788d8873206e8ed" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success init=remote mode=quick dir=outbound stage=1 role=responder result=OK  10.0.0.138:1025 : local7.notice date=2013-03-15 time=22:22:04 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037133 type=event subtype=vpn level=notice vd="root" msg="install IPsec SA" action=install\_sa remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="78b2ee36ed800ce7/1788d8873206e8ed" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" role=responder in\_spi="003322db" out\_spi="acae81e8"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=22:22:04 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037129 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="78b2ee36ed800ce7/1788d8873206e8ed" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success init=remote mode=quick dir=inbound stage=2 role=responder result=DONE  10.0.0.138:1025 : local7.notice date=2013-03-15 time=22:22:04 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037122 type=event subtype=vpn level=notice vd="root" msg="negotiate IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="78b2ee36ed800ce7/1788d8873206e8ed" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success role=responder esptransform=ESP\_3DES espauth="HMAC\_MD5"  10.0.0.138:1024 : local7.notice date=2013-03-15 time=22:11:24 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0100040704 type=event subtype=system level=notice vd="root" action="perf-stats" cpu=92 mem=57 totalsession=14209 msg="Performance statistics"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=02:32:34 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0102043014 type=event subtype=user level=notice vd="root" src=10.0.12.181 user="MKIRMIZIGUL" server="dc" action=FSSO-logon msg="FSSO-logon event from dc: user MKIRMIZIGUL logged on 10.0.12.181""  10.0.0.138:1025 : local7.notice date=2013-03-15 time=02:00:33 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037135 type=event subtype=vpn level=notice vd="root" msg="delete IPsec phase 2 SA" action=delete\_ipsec\_sa remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="f20455be11d8444d/a45db45242c975fc" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" enc\_spi="acae81bc" dec\_spi="332282"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:59:45 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037129 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="f20455be11d8444d/a45db45242c975fc" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success init=remote mode=quick dir=outbound stage=1 role=responder result=OK  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:59:45 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037133 type=event subtype=vpn level=notice vd="root" msg="install IPsec SA" action=install\_sa remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="f20455be11d8444d/a45db45242c975fc" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" role=responder in\_spi="00332283" out\_spi="acae81bd"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:59:45 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037129 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="f20455be11d8444d/a45db45242c975fc" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success init=remote mode=quick dir=inbound stage=2 role=responder result=DONE  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:59:45 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037122 type=event subtype=vpn level=notice vd="root" msg="negotiate IPsec phase 2" action=negotiate remip=78.187.6.43 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="f20455be11d8444d/a45db45242c975fc" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="ulucanlar.p1" status=success role=responder esptransform=ESP\_3DES espauth="HMAC\_MD5"  10.0.0.138:1024 : local7.notice date=2013-03-15 time=01:56:10 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0100040704 type=event subtype=system level=notice vd="root" action="perf-stats" cpu=72 mem=61 totalsession=15924 msg="Performance statistics"  10.0.0.138:1024 : local7.notice date=2013-03-15 time=01:51:10 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0100040704 type=event subtype=system level=notice vd="root" action="perf-stats" cpu=72 mem=61 totalsession=15748 msg="Performance statistics"  10.0.0.138:1024 : local7.notice date=2013-03-15 time=01:46:10 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0100040704 type=event subtype=system level=notice vd="root" action="perf-stats" cpu=70 mem=61 totalsession=15518 msg="Performance statistics"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:40:26 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0102043029 type=event subtype=user level=notice vd="root" src=10.0.10.33 dst=212.101.122.3 initiator=N/A status=N/A reason="none" scope=ip scope\_data="N/A" rule\_type=directory rule\_data="N/A" offsite=yes expiry="Fri Mar 15 01:45:26 2013" oldwprof="client.genel" newwprof="" msg="User added webfilter warning entry from 10.0.10.33"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:34:17 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037127 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 1" action=negotiate remip=212.174.30.220 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="2c7eeced99157080/5c4bcfd5ae48f112" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="siteler.p1" status=success init=local mode=main dir=outbound stage=3 role=initiator result=OK  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:34:17 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037127 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 1" action=negotiate remip=212.174.30.220 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="2c7eeced99157080/5c4bcfd5ae48f112" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="siteler.p1" status=success init=local mode=main dir=inbound stage=3 role=initiator result=DONE  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:34:17 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037134 type=event subtype=vpn level=notice vd="root" msg="delete IPsec phase 1 SA" action=delete\_phase1\_sa remip=212.174.30.220 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="a9d91c12a0965d8d/23f3b2e575f7cec1" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="siteler.p1"  10.0.0.138:1025 : local7.notice date=2013-03-15 time=01:34:16 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0101037127 type=event subtype=vpn level=notice vd="root" msg="progress IPsec phase 1" action=negotiate remip=212.174.30.220 locip=212.156.63.10 remport=500 locport=500 outintf="port22" cookies="2c7eeced99157080/0000000000000000" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="siteler.p1" status=success init=local mode=main dir=outbound stage=1 role=initiator result=OK | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME | Level |
| EVENT ID |  |
| EVENTCATEGORY | EVENT |
| EVENTTYPE | Subtype |
| USERSID | user,group |
| LOGNAME |  |
| COMPUTERNAME | DevName |
| CUSTOMSTR1 | status |
| CUSTOMSTR2 | action |
| CUSTOMSTR3 | src |
| CUSTOMSTR4 | dst |
| CUSTOMSTR5 | İnit |
| CUSTOMSTR6 | Mode |
| CUSTOMSTR7 | remip |
| CUSTOMSTR8 | locip |
| CUSTOMSTR9 | vpntunnel |
| CUSTOMSTR10 | Msg |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | remport |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 | Policyid |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | ALL DATA |

# PARSING UTM

|  |  |
| --- | --- |
| 10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:49:17 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=78.129.166.149 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=17 service=1434/udp count=28 attackname="udp\_src\_session" srcport=1946 dstport=1434 attackid=285212773 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID285212773" msg="anomaly: udp\_src\_session, 2001 > threshold 2000, repeats 28 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:44:38 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=78.129.155.164 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=17 service=1434/udp count=38 attackname="udp\_src\_session" srcport=2769 dstport=1434 attackid=285212773 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID285212773" msg="anomaly: udp\_src\_session, 2001 > threshold 2000, repeats 38 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:44:02 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=78.129.154.61 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=17 service=1434/udp count=42 attackname="udp\_src\_session" srcport=2404 dstport=1434 attackid=285212773 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID285212773" msg="anomaly: udp\_src\_session, 2001 > threshold 2000, repeats 42 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:30:40 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=109.190.192.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=139/tcp count=7 attackname="tcp\_src\_session" srcport=6000 dstport=139 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 1001 > threshold 1000, repeats 7 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:30:40 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=109.190.192.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=1433/tcp count=4820 attackname="tcp\_port\_scan" srcport=6000 dstport=1433 attackid=100663398 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663398" msg="anomaly: tcp\_port\_scan, 1001 > threshold 1000, repeats 4820 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:30:40 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=109.190.193.77 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=8 attackname="ip\_src\_session" srcport=6000 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 2001 > threshold 2000, repeats 8 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:34 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.192.153 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=32000/tcp count=4869 attackname="tcp\_src\_session" srcport=2896 dstport=32000 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 6138 > threshold 1000, repeats 4869 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:34 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.192.153 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=32000/tcp count=4099 attackname="ip\_src\_session" srcport=2896 dstport=32000 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 6143 > threshold 2000, repeats 4099 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:01 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.124.166 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=12174/tcp count=46266 attackname="tcp\_port\_scan" srcport=6000 dstport=12174 attackid=100663398 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663398" msg="anomaly: tcp\_port\_scan, 1001 > threshold 1000, repeats 46266 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:01 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.124.166 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=12174/tcp count=40 attackname="tcp\_src\_session" srcport=6000 dstport=12174 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 1001 > threshold 1000, repeats 40 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:01 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.125.77 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=5900/tcp count=41 attackname="ip\_src\_session" srcport=6000 dstport=5900 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 2003 > threshold 2000, repeats 41 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:01 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.125.77 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=41 attackname="ip\_src\_session" srcport=6000 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 2002 > threshold 2000, repeats 41 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:28:01 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=94.23.125.78 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=139/tcp count=41 attackname="ip\_src\_session" srcport=6000 dstport=139 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 2001 > threshold 2000, repeats 41 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:14:43 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.35.190 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=39 attackname="tcp\_src\_session" srcport=1887 dstport=3306 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 48859 > threshold 1000, repeats 39 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:14:43 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.35.190 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=39 attackname="ip\_src\_session" srcport=1887 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 49045 > threshold 2000, repeats 39 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:14:13 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.34.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=35 attackname="tcp\_src\_session" srcport=1844 dstport=3306 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 48856 > threshold 1000, repeats 35 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:14:13 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.34.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=35 attackname="ip\_src\_session" srcport=1844 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 49042 > threshold 2000, repeats 35 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:42 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.33.239 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=47255 attackname="tcp\_src\_session" srcport=1805 dstport=3306 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 48855 > threshold 1000, repeats 47255 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:42 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.33.239 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=47395 attackname="ip\_src\_session" srcport=1805 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 49089 > threshold 2000, repeats 47395 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:11 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.32.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=142 attackname="tcp\_port\_scan" srcport=6000 dstport=3306 attackid=100663398 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663398" msg="anomaly: tcp\_port\_scan, 1001 > threshold 1000, repeats 142 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:11 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.32.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=1433/tcp count=1 attackname="tcp\_src\_session" srcport=6000 dstport=1433 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 1002 > threshold 1000"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:11 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.32.167 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=12174/tcp count=1 attackname="tcp\_src\_session" srcport=6000 dstport=12174 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 1001 > threshold 1000"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:13:11 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=91.121.33.14 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=1433/tcp count=501 attackname="ip\_src\_session" srcport=6000 dstport=1433 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 2001 > threshold 2000, repeats 501 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:07:05 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=31.25.184.0 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=17 service=1434/udp count=1 attackname="ip\_src\_session" srcport=3561 dstport=1434 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 5591 > threshold 2000"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:05:07 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=87.233.252.174 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=3306/tcp count=5004 attackname="ip\_src\_session" srcport=1810 dstport=3306 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 20134 > threshold 2000, repeats 5004 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:05:07 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=87.233.252.174 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=1433/tcp count=5004 attackname="ip\_src\_session" srcport=1809 dstport=1433 attackid=16777322 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID16777322" msg="anomaly: ip\_src\_session, 20133 > threshold 2000, repeats 5004 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:05:04 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=87.233.252.61 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=5900/tcp count=4946 attackname="tcp\_src\_session" srcport=1126 dstport=5900 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 20003 > threshold 1000, repeats 4946 times"  10.0.0.138:1024 : local7.alert date=2013-03-14 time=21:03:34 devname=Altindag\_Fortigate devid=FG600C3912800067 logid=0420018432 type=utm subtype=ips eventtype=anomaly level=alert vd="root" severity=critical srcip=10.0.0.30 dstip=87.233.242.116 srcintf="port19" policyid=N/A identidx=N/A sessionid=0 status=detected proto=6 service=5900/tcp count=5091 attackname="tcp\_src\_session" srcport=3117 dstport=5900 attackid=100663402 sensor="DoS-policy2" ref="http://www.fortinet.com/ids/VID100663402" msg="anomaly: tcp\_src\_session, 20140 > threshold 1000, repeats 5091 times" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME | Level |
| EVENT ID |  |
| EVENTCATEGORY | UTM |
| EVENTTYPE | Subtype |
| USERSID | user, group |
| LOGNAME |  |
| COMPUTERNAME | DevName |
| CUSTOMSTR1 | Eventtype |
| CUSTOMSTR2 | service |
| CUSTOMSTR3 | srcip |
| CUSTOMSTR4 | dstip |
| CUSTOMSTR5 | Sensor |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | remip |
| CUSTOMSTR8 | Attackname |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | srcport |
| CUSTOMINT4 | Dstport |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 | Count |
| DESCRIPTION | ALL DATA |

# Parsing DHCP

(Not: DHCP loğları Ana tabloda EvetType = “event”, EventCategory = “router” olarak düşmektedir. Sadece bu kategoriye giren loğlar parse edilecektir. )

|  |  |
| --- | --- |
| 172.16.1.100:1025 : local7.info date=2013-06-14 time=15:38:09 devname=TIGEM\_MERKEZ devid=FGT1KB3910600672 logid=0103026001 type=event subtype=router level=information vd="root" dhcp\_msg="Ack" dir=Sent mac=20:10:7A:4D:4C:E3 ip=172.17.212.12 lease=86400 hostname="ZYILMAN" msg="Assigns IP address/configuration parameters to the client" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | DATE\_TIME |
| SOURCENAME | level |
| EVENT ID |  |
| EVENTCATEGORY | Subtype |
| EVENTTYPE | type |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | devname |
| CUSTOMSTR1 | dir |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | hostname |
| CUSTOMSTR4 | mac |
| CUSTOMSTR5 | ip |
| CUSTOMSTR6 | dhcp\_msg |
| CUSTOMSTR7 | msg |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 | lease |
| DESCRIPTION | All Log |