Siber Savunma Yöntemleri

Emre ÖVÜNÇ
Siber Güvenlik Mühendisi

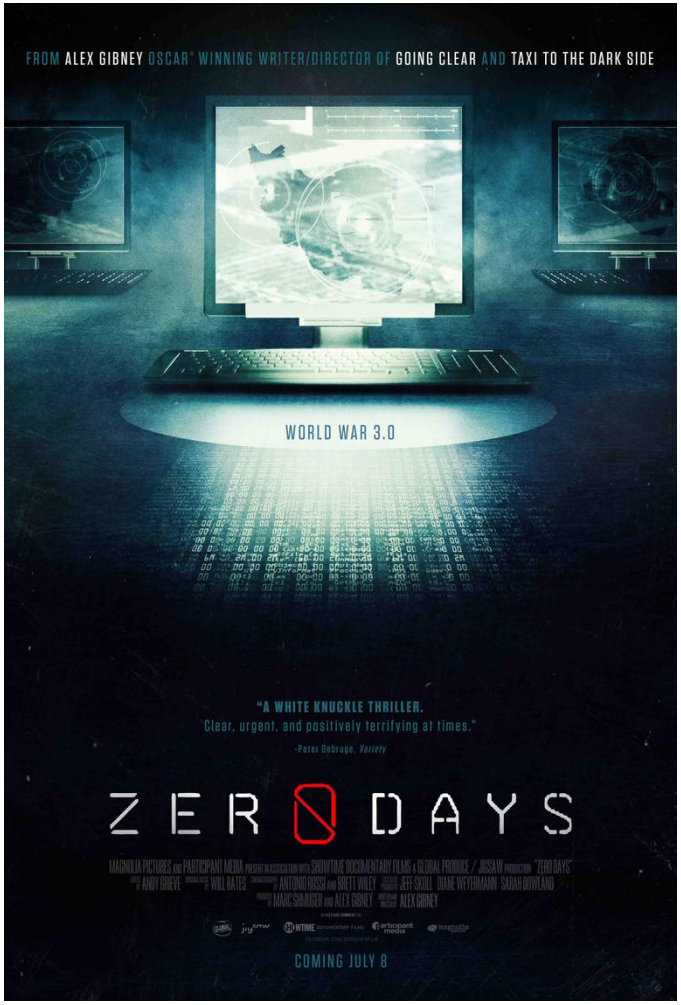
Siber Güvenlik

Siber Savaş

“The next war will begin in cyberspace.” [Rex Hughes]

Stuxnet

- Malware
- İran
- Windows PC
- 0-Day
- USB Disk
- Siemens SCADA



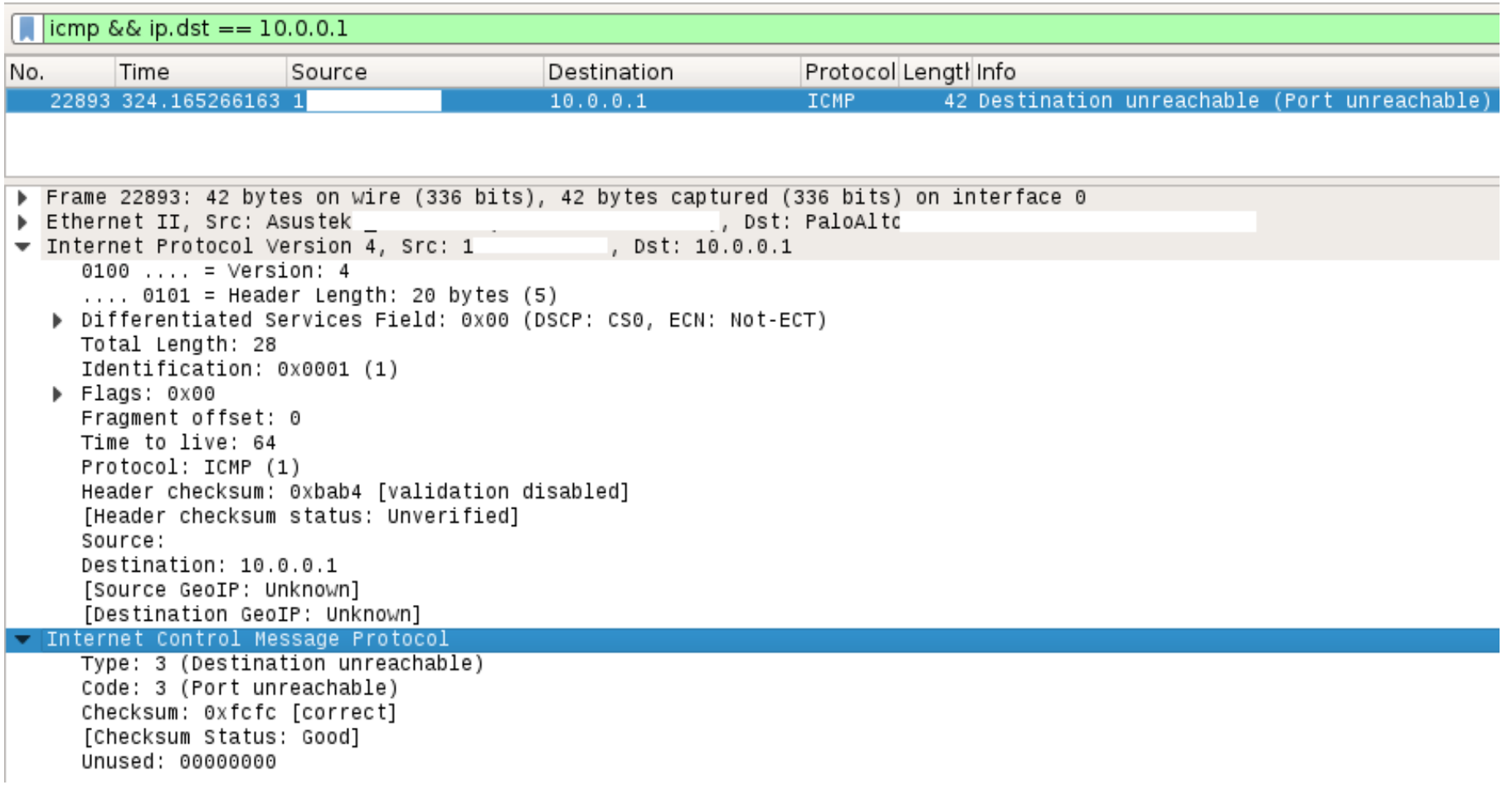
BlackNurse

- ICMP
- İşlemci Gücü
- Palo Alto, Cisco, Zyxel, SonicWall...

Type	Code	Meaning
0	0	echo reply
3	0	network unreachable
3	1	host is unreachable
3	3	port is unreachable
4	0	source quench
5	0	redirect
8	0	echo request
9/10	0	router discovery/advertisement
11	0	time exceed
12	0	parameter problem
13/14	0	time stamp request
17/18	0	network request/reply

Scapy -> ICMP

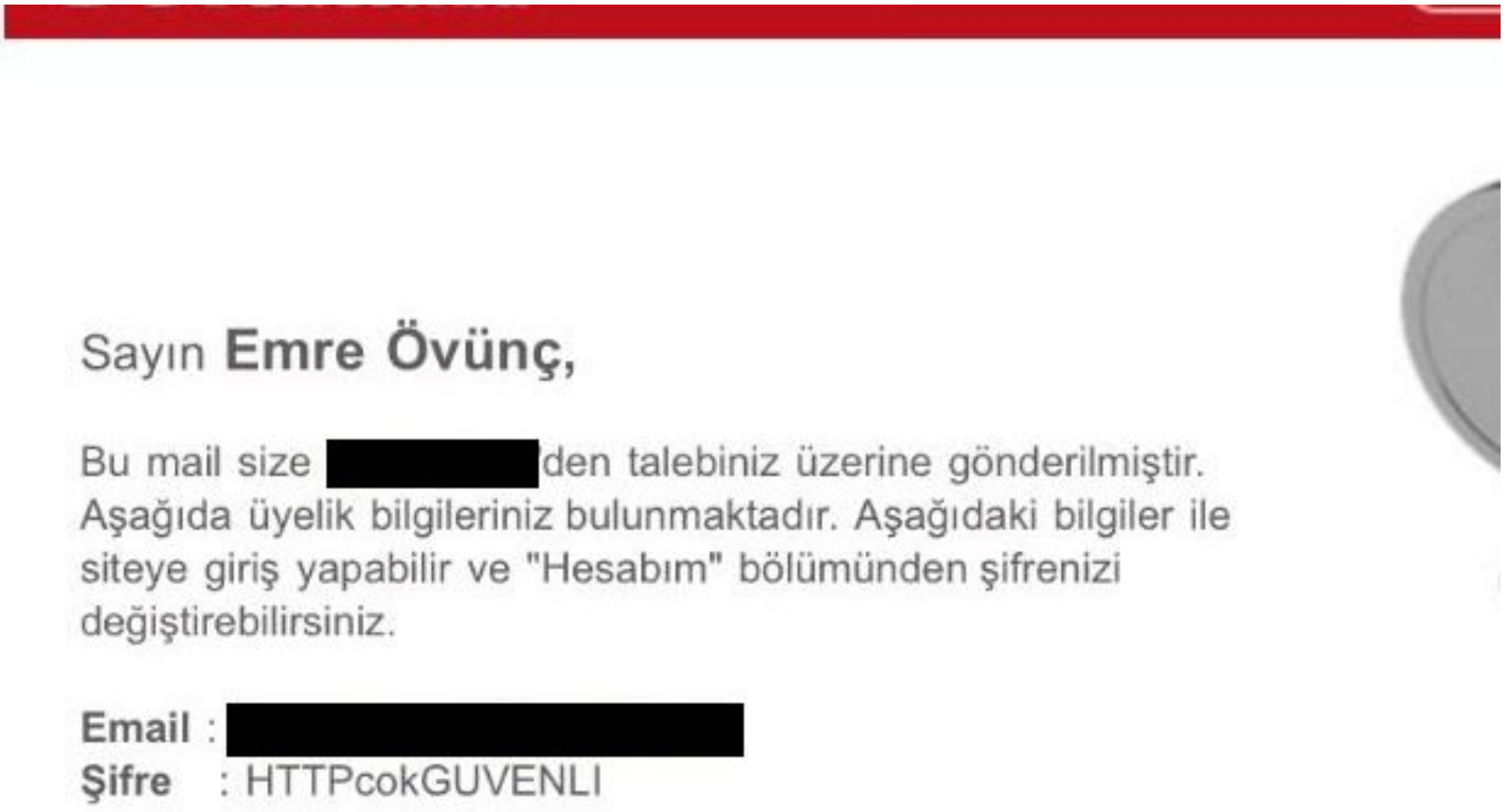
```
from scapy.all import *

icmp_packet = IP(dst='10.0.0.1')/ICMP(type=3, code=3)
send(icmp_packet)
```



Siber Saldırılar

- Malware
- Phishing
- SQL Injections
- Cross-Site Scripting
- DDoS
- Session Hijacking
- Man in the Middle
- Others

Teknoloji Sitesi

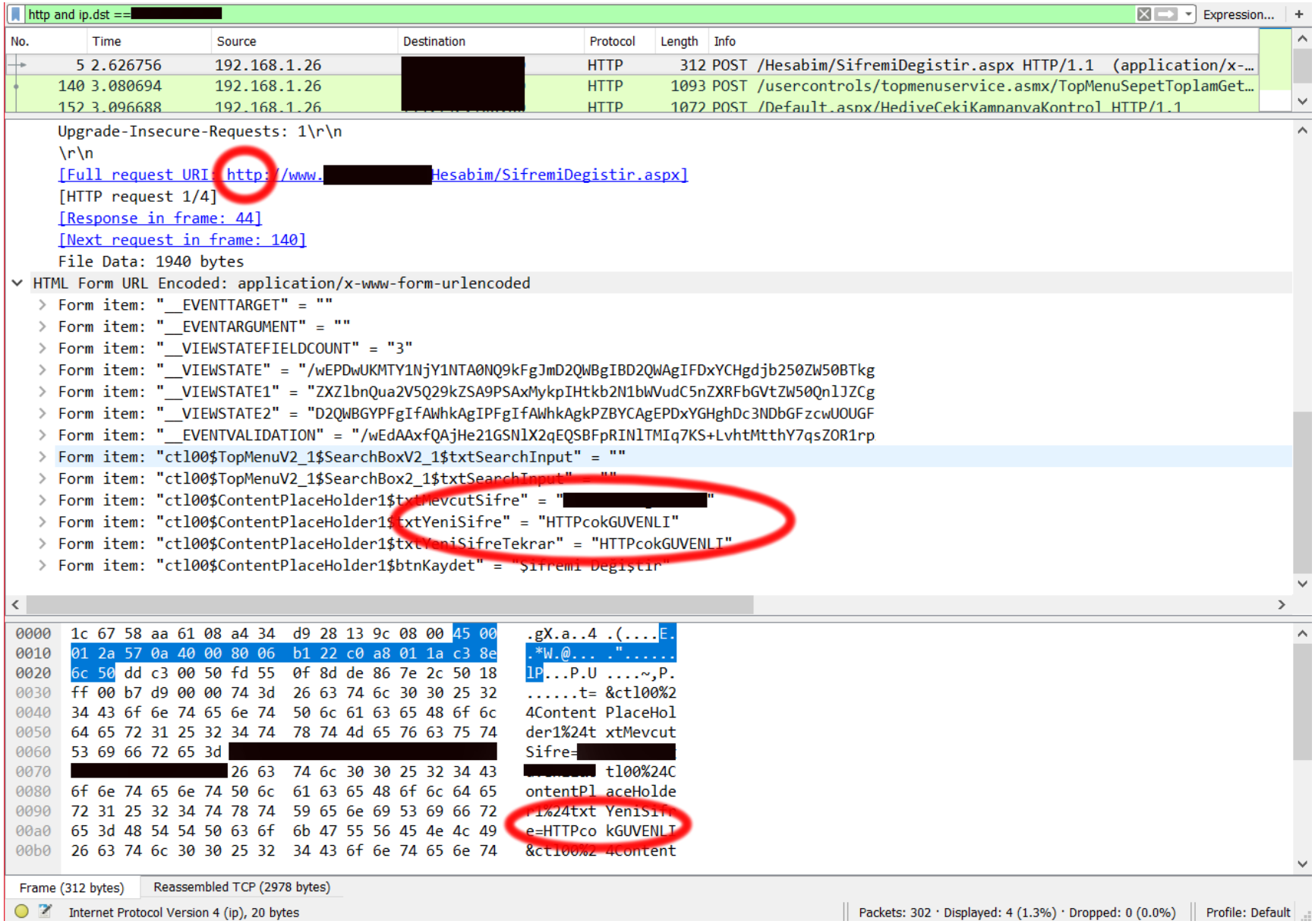


Sayın **Emre Övünç,**

Bu mail size [redacted]den talebiniz üzerine gönderilmiştir. Aşağıda üyelik bilgileriniz bulunmaktadır. Aşağıdaki bilgiler ile siteye giriş yapabilir ve "Hesabım" bölümünden şifrenizi değiştirebilirsiniz.

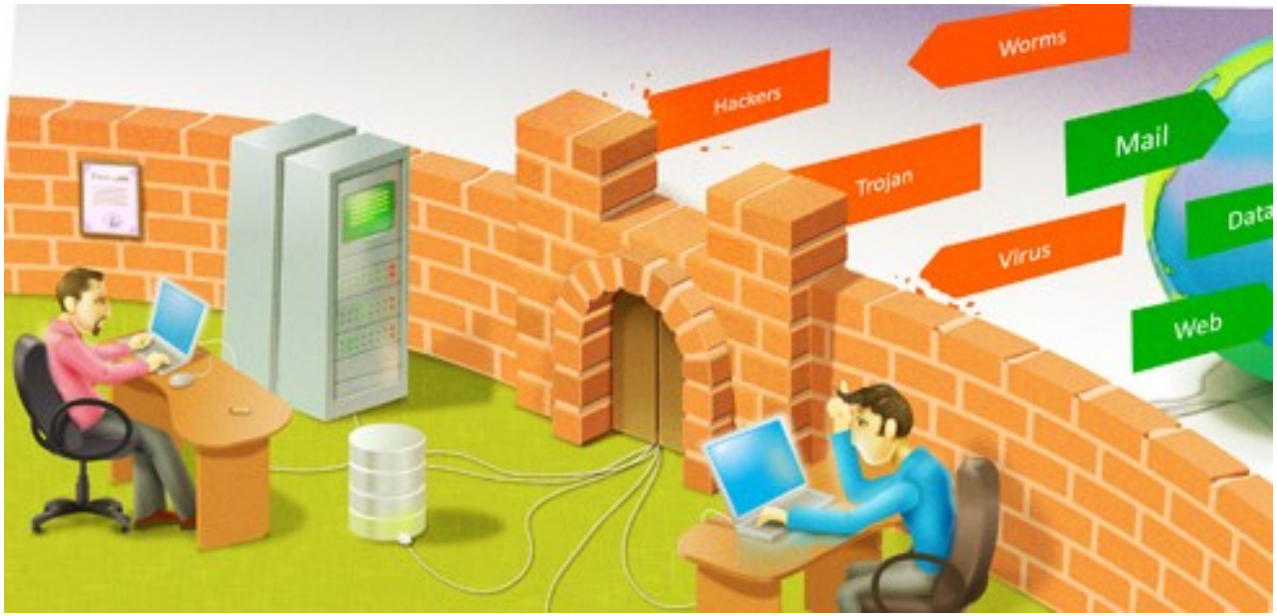
Email : [redacted]
Şifre : HTTPcokGUVENLI

HTTP


http and ip.dst ==[redacted]
Expression...
No. Time Source Destination Protocol Length Info
5 2.626756 192.168.1.26 [redacted] HTTP 312 POST /Hesabim/SifremiDegistir.aspx HTTP/1.1 (application/x-...
140 3.080694 192.168.1.26 [redacted] HTTP 1093 POST /usercontrols/topmenuservice.asmx/TopMenuSepetToplamGet...
152 3.096688 192.168.1.26 [redacted] HTTP 1072 POST /Default.aspx/HediyeCekiKampanyaKontrol HTTP/1.1
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://www.[redacted]Hesabim/SifremiDegistir.aspx]
[HTTP request 1/4]
[Response in frame: 44]
[Next request in frame: 140]
File Data: 1940 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "__EVENTTARGET" = ""
Form item: "__EVENTARGUMENT" = ""
Form item: "__VIEWSTATEFIELDCOUNT" = "3"
Form item: "__VIEWSTATE" = "/wEPDwUKMTY1NjY1NTA0NQ9kFgJmD2QWBgIBD2QWAgIFDxYCHgdjb250ZW50BTkg
Form item: "__VIEWSTATE1" = "ZXZlbnQua2V5Q29kZSA9PSAxMykpIHtkb2N1bWVudC5nZXRFbGVtZW50QnlJZCg
Form item: "__VIEWSTATE2" = "D2QWBGYPFgIfAWhkAgIPFgIfAWhkAgkPZBYCAgEPDxYGHghDc3NDbGFzcwUOUGF
Form item: "__EVENTVALIDATION" = "/wEdAAxfQAjHe21GSNlX2qEQSBFpRINlTMIq7KS+LvhtMtthY7qsZOR1rp
Form item: "ctl00$TopMenuV2_1$SearchBoxV2_1$txtSearchInput" = ""
Form item: "ctl00$TopMenuV2_1$SearchBox2_1$txtSearchInput" = ""
Form item: "ctl00$ContentPlaceHolder1$txtMevcutSifre" = "[redacted]"
Form item: "ctl00$ContentPlaceHolder1$txtYeniSifre" = "HTTPcokGUVENLI"
Form item: "ctl00$ContentPlaceHolder1$txtYeniSifreTekrar" = "HTTPcokGUVENLI"
Form item: "ctl00$ContentPlaceHolder1$btnKaydet" = "Şifremi Değiştir"
0000 1c 67 58 aa 61 08 a4 34 d9 28 13 9c 08 00 45 00 .gX.a..4 .(....E.
0010 01 2a 57 0a 40 00 80 06 b1 22 c0 a8 01 1a c3 8e .*W.@... ."......
0020 6c 50 dd c3 00 50 fd 55 0f 8d de 86 7e 2c 50 18 lP...P.U ....~,P.
0030 ff 00 b7 d9 00 00 74 3d 26 63 74 6c 30 30 25 32 ......t= &ctl00%2
0040 34 43 6f 6e 74 65 6e 74 50 6c 61 63 65 48 6f 6c 4Content PlaceHol
0050 64 65 72 31 25 32 34 74 78 74 4d 65 76 63 75 74 der1%24t xtMevcut
0060 53 69 66 72 65 3d [redacted] Sifre=[redacted]
0070 [redacted] 26 63 74 6c 30 30 25 32 34 43 [redacted] tl00%24C
0080 6f 6e 74 65 6e 74 50 6c 61 63 65 48 6f 6c 64 65 ontentPl aceHolde
0090 72 31 25 32 34 74 78 74 59 65 6e 69 53 69 66 72 r1%24txt YeniSifr
00a0 65 3d 48 54 54 50 63 6f 6b 47 55 56 45 4e 4c 49 e=HTTPco kGUVENLI
00b0 26 63 74 6c 30 30 25 32 34 43 6f 6e 74 65 6e 74 &ctl00%2 4Content
Frame (312 bytes)
Reassembled TCP (2978 bytes)
Internet Protocol Version 4 (ip), 20 bytes
Packets: 302 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

Firewall

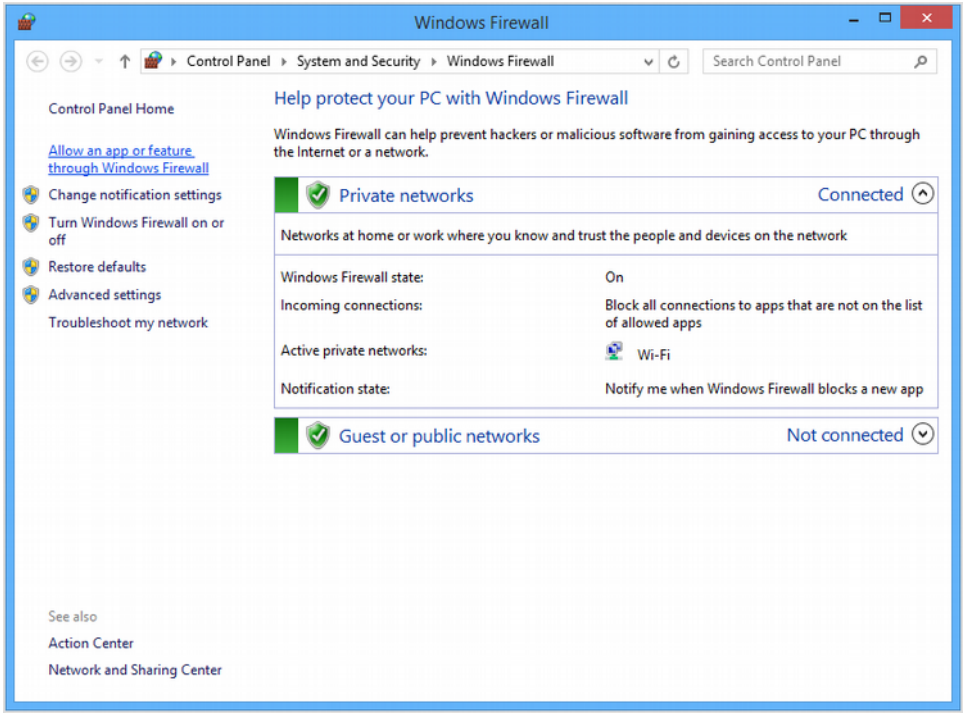
- Dış ağlardan gelecek tehditleri, içerisindeki kurallara göre filtreleyen güvenlik cihazıdır.
- Software
- Hardware

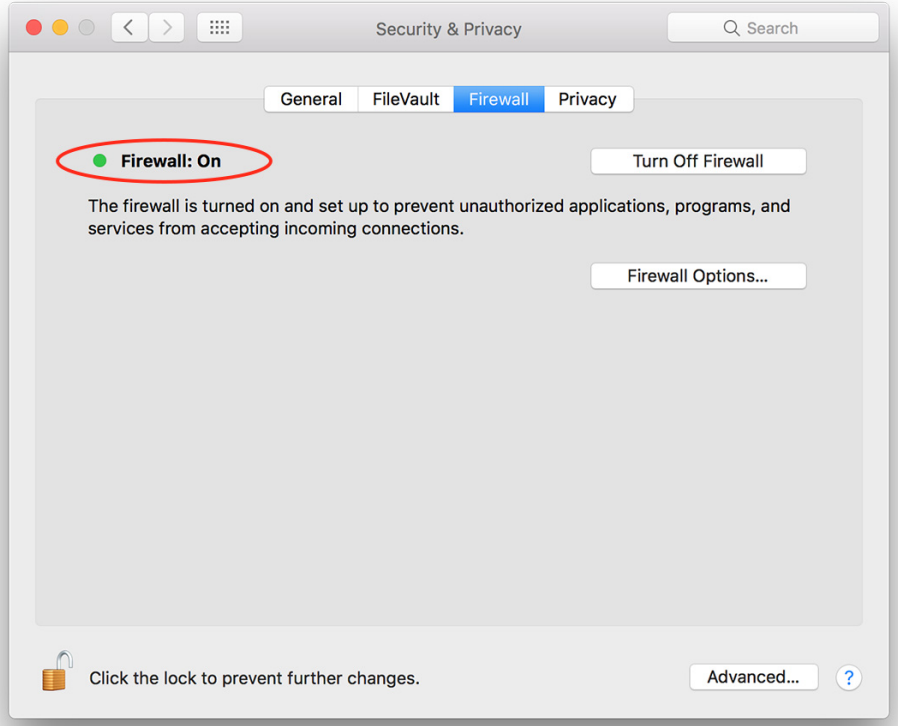


Hardware Firewall

- Ağdaki tüm cihazları korur.
- ~~Self-Configuration~~
- Ticari

Software Firewall





IPTables

```
#!/bin/sh
sudo iptables -F
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT DROP
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -i wlan0 -p udp -m udp --sport 53 -j ACCEPT
sudo iptables -A INPUT -i eth0 -p udp -m udp --sport 53 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -s 192.168.1.254 -i eth0 -p tcp -m tcp --dport 2222 -j ACCEPT
sudo iptables -A INPUT -s 192.168.1.254 -i wlan0 -p tcp -m tcp --dport 2222 -m mac --mac-source AA:BB:CC:11:22:33 -j ACCEPT
sudo iptables -A INPUT -s 10.0.0.1 -i eth0 -p tcp -m tcp --dport 2222 -j ACCEPT
sudo iptables -A OUTPUT -o eth0 -p udp -m udp --dport 53 -j ACCEPT
sudo iptables -A OUTPUT -o wlan0 -p udp -m udp --dport 53 -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
sudo iptables -A OUTPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp -m tcp --sport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -p tcp -m tcp --sport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -d 192.168.1.254 -o eth0 -p tcp -m tcp --sport 2222 -j ACCEPT
sudo iptables -A OUTPUT -d 192.168.1.0/24 -o wlan0 -p tcp -m tcp --sport 2222 -j ACCEPT
sudo iptables -A OUTPUT -d 10.0.0.1 -o eth0 -p tcp -m tcp --sport 2222 -j ACCEPT
sudo iptables-save
```

https://github.com/EmreOvunc/MyDailyScripts/blob/master/Emre_Firewall.sh

IPS & IDS

- IDS
  - NIDS & HIDS
  - Ağ/Sistem trafiğini inceler
  - Signature-based & Anomaly-based
- IPS
  - IPDS
  - Snort, Suricata, OSSEC, Bro ...

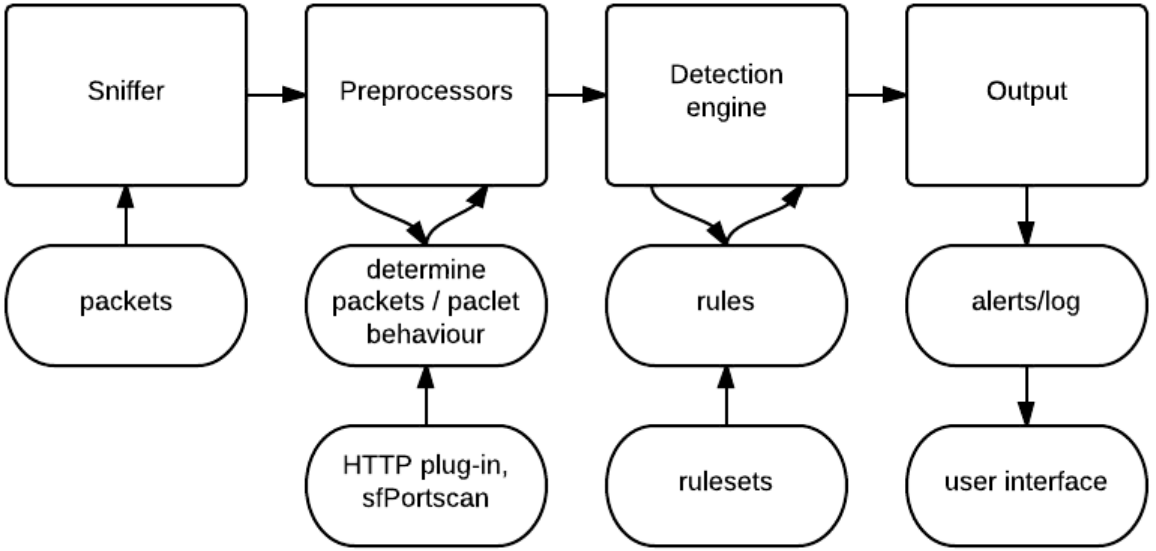
Anomaly Detection

Snort

- Açık kaynak kodlu
- Ücretsiz
- NIPDS
- Rules (Community – Registered – Subscription)
- Snort 2.9 – 3 (Multithreading)
- https://www.snort.org/

Snort Mimarisi

- Paket yakalama
- Paket çözümleme
- Ön işlemci
- Tespit motoru
- Alarm



Snort Modları - 1

- **Packet Sniffer**

  - Ağ kartından geçen tüm trafiği izler ve paketleri detaylarıyla birlikte ekrana basar.

snort -v

```
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.7.0 GRE (Build 149)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''    Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.38 2015-11-23
```

Snort Modları - 2

- **Packet Logger**

  - Yakalanan paketleri disk üzerinde loglaması için kullanılır.

    snort -l ~/snort-logs/

```
Running in packet logging mode

       --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = log
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

       --== Initialization Complete ==--

          -*> Snort! <*-
  ,,_     Version 2.9.7.0 GRE (Build 149)
 o"  )~   By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''   Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.7.4
```

Snort Modları - 3

- **NIPDS**

  - Sızma girişimlerini tespit etme ve önceden tanımlanmış kurallara dayanarak aksiyon alınmasıdır.

snort -A console -Q -c snort.conf -d -y --daq afpacket -i eth0:eth1

```
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830
 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 777
7 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 83
00 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50
002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
```

Snort Kuralları

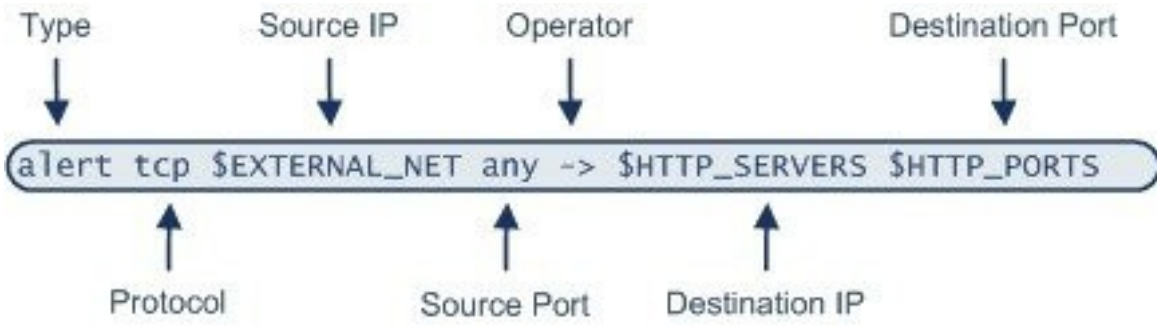
- Ev ağının belirtilmesi

```
#ipvar HOME_NET any
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

- Kuralları aktif hale getirme

```
#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
```

Snort Kural Başlıkları



- **Alert**

  - Belirtilen kural gerçekleştiği zaman uyarı verilmesi için kullanılır.

  - Konsola veya herhangi bir dosyaya uyarıyı kaydedebilir

Snort Kural Başlıkları

- **Log**

  - Paketleri kayıt altına almak için kullanılır.

- **Pass**

  - Kurallara uyan paketlerin (ignore) yok sayılması için kullanılır.

- **Active**

  - Uyarı mesajı geldikten sonra diğer kuralları aktif hale getirebilmek ve daha fazla kural üzerinde test etmek için kullanılır.

Snort Kuralları

- Kurallarda özel bir IP adresi belirtmemiz gerekmiyorsa, ‘any’ ifadesini kullanabiliriz.

```
alert udp any 53 - > $HOME_NET 53
alert udp 10.0.0.1 any - > $HOME_NET any
alert udp !10.0.0.2 any - > $HOME_NET any
```

Snort Kuralları

- **Kural İnceleme**

alert tcp any any - > $HOME_NET 80 (

content: ‘cmd.exe’,

msg: ‘IIS Attack’;

)

- content : Paketin içerisinde ‘cmd.exe’ komutunun bulunup bulunmadığını kontrol eder.

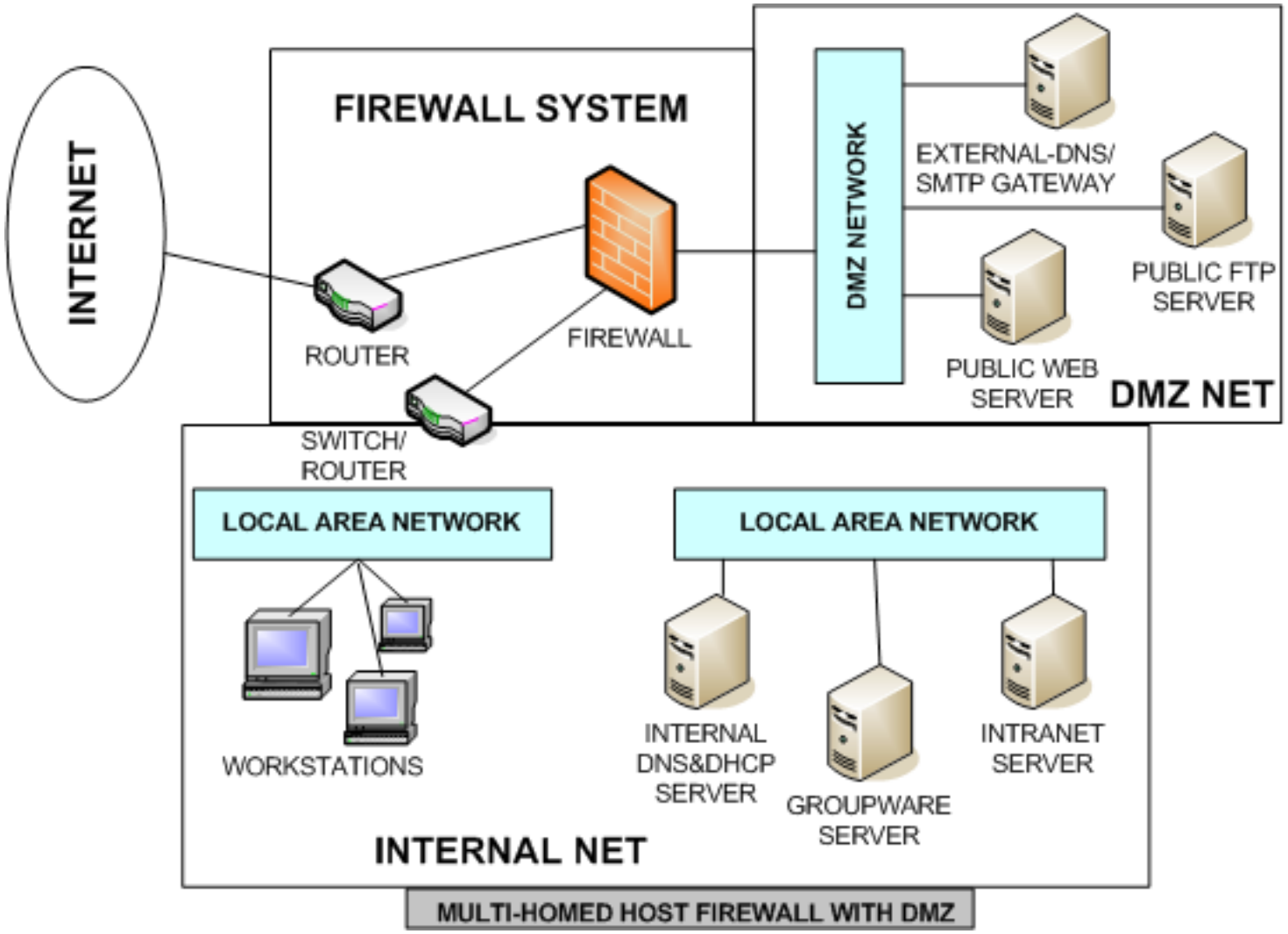
Snort Kuralları

- **İçerik Listeleri**

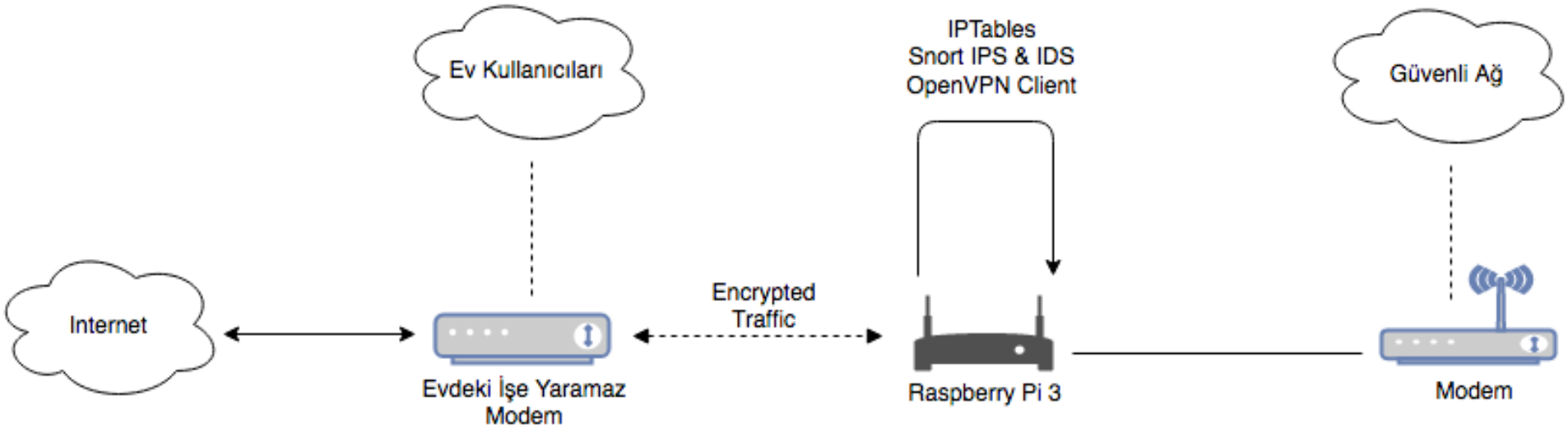
```
alert tcp $HOME_NET any - > any 80 (
                        content-list:‘Engelle.txt’,
                        msg: ‘Oyun Sitesi Erisimi’;
                        )
```

- Ev ağından çıkan ve karşı tarafın 80. portuna giden paketlerden liste içerisindeki sözcüklerin kontrolünü yapan kural.

DMZ


INTERNET
FIREWALL SYSTEM
ROUTER
FIREWALL
SWITCH/
ROUTER
DMZ NETWORK
EXTERNAL-DNS/
SMTP GATEWAY
PUBLIC FTP
SERVER
PUBLIC WEB
SERVER
DMZ NET
LOCAL AREA NETWORK
LOCAL AREA NETWORK
WORKSTATIONS
INTERNAL
DNS&DHCP
SERVER
GROUPWARE
SERVER
INTRANET
SERVER
INTERNAL NET
MULTI-HOMED HOST FIREWALL WITH DMZ

Ev Ağım



Internet Sağlayıcısının
DNS Sunucusu

Kişisel | Public DNS Sunucuları

Kişisel Güvenlik Önlemleri

- **Fiziksel Güvenlik**
  - BIOS parolası
  - USB koruması
  - Laptop kilitleri
- **Ağ Güvenliği**
  - ~~Public WiFi~~
  - Firewall
  - IPS & IDS
- **Bilgisayar Güvenliği**
  - Backup
  - ~~Guest account~~
  - Servislerin kontrolü
  - Encrypted disk


Teşekkürler ...