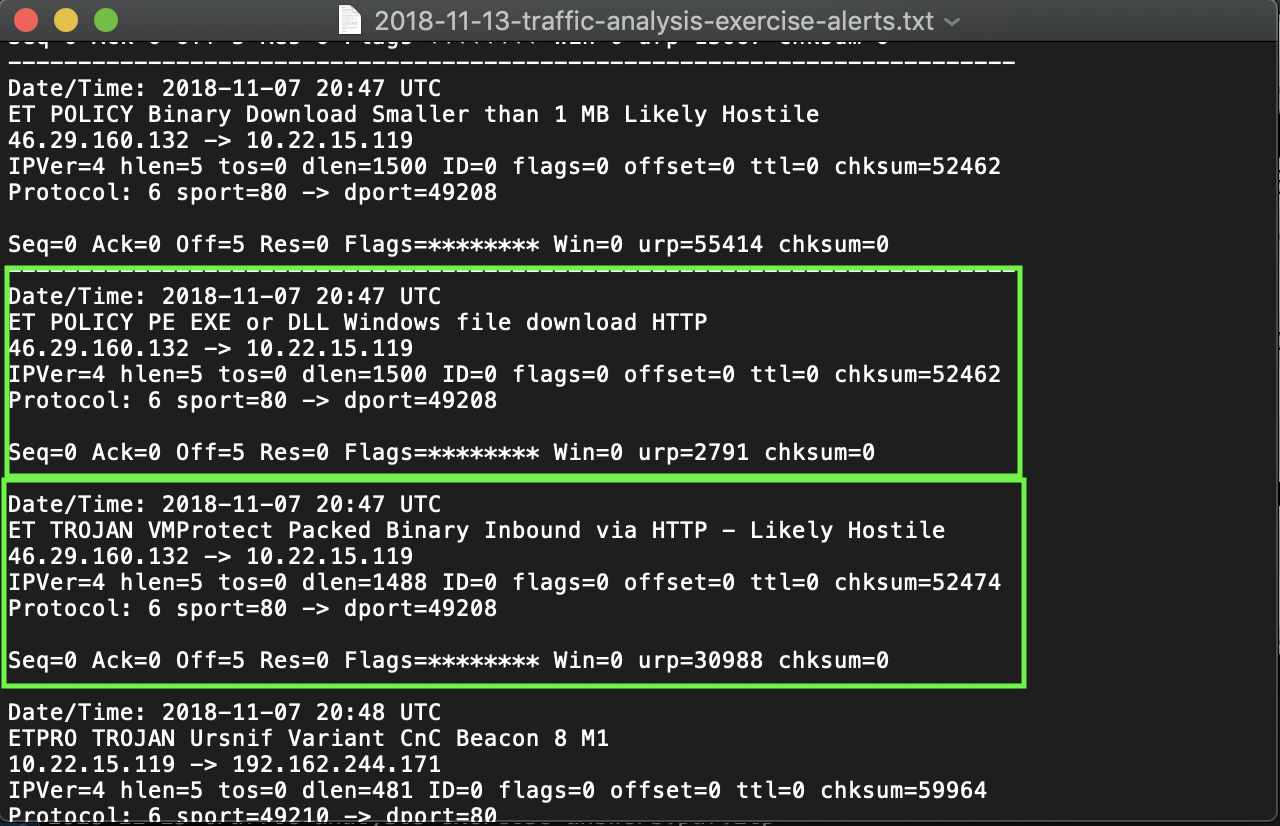
**Post-Incident Report**

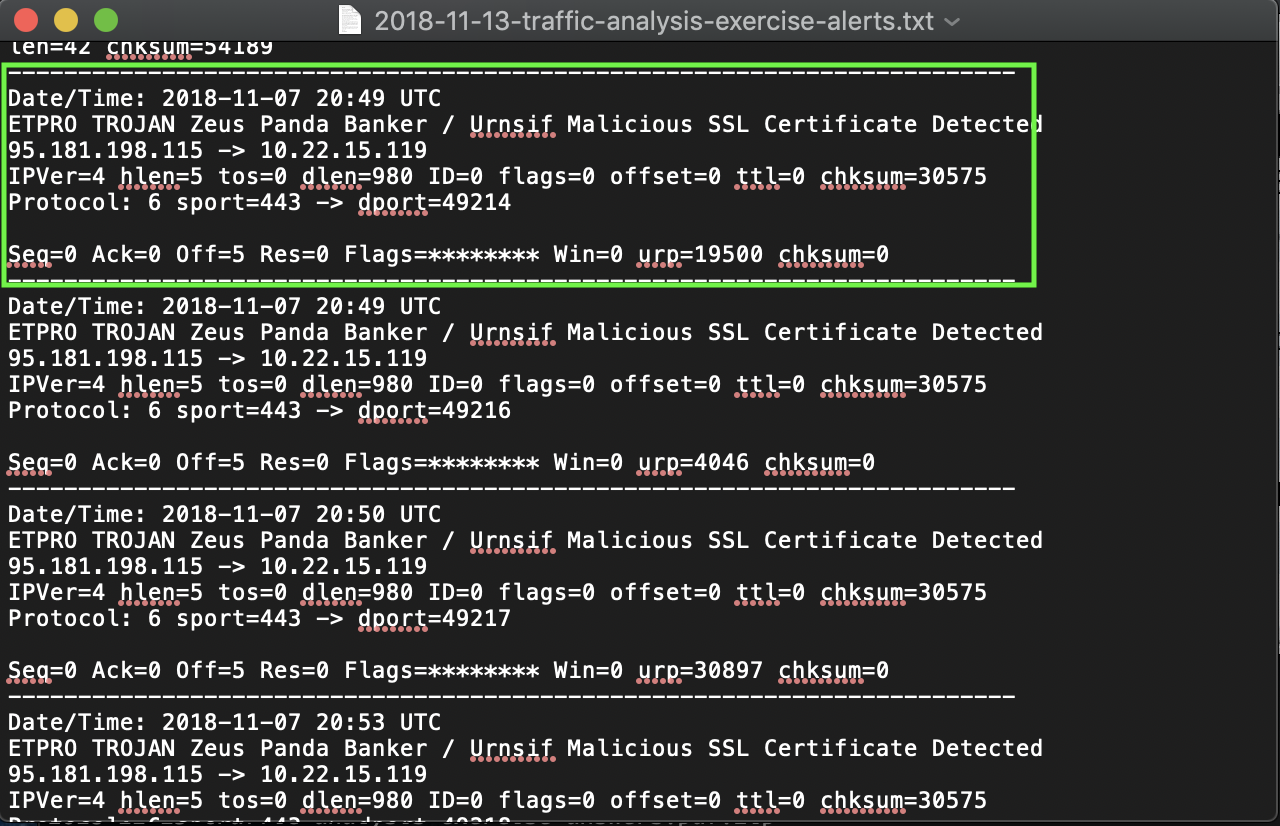
|  |  |
| --- | --- |
| Date of investigation | July 11, 2019 |
| Date of incident | 2018-11-07 20:47 UTC |
| Outcome | True Positive- The file downloaded was Ursnif Malware or the variant Gozi/IFSB |
| Action Taken | Identified Malware & initially infected Host Device  Advise potentially adding firewall rules to block traffic from source of Malware.  Advise restoring host computer to a backup done before the infection date or reimage the hard drive if no back up is present.  Run AV- confirmation that the Malware has been removed and is no longer on the host computer. |
| Reporting tools | Snort, Sguil on Security Onion, and Wireshark (examine .pcap files) |
| Attack Vector | Web-based Malware Attack |
| Source IP  Source Port | 10.22.15.119  80 |
| Destination IP  Destination Port | Shumbildac[.]com/ 46.29.160.132  49208 |

**Narrative**

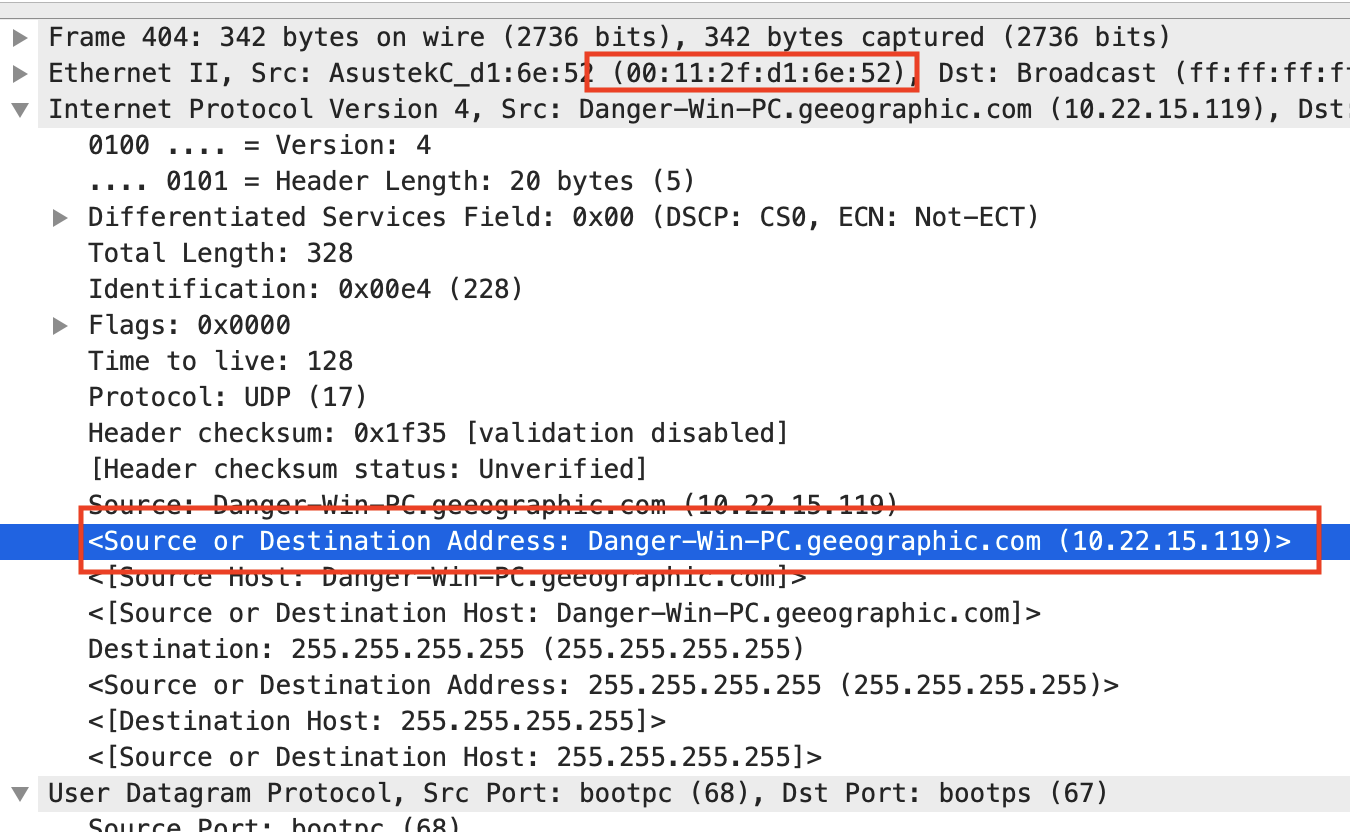
* Alerted by Snort
  + “ET POLICY Binary Download Smaller than 1 MB Likely Hostile”
  + “ET POLICY PE EXE or DLL Windows file download HTTP”
  + “ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile”
  + “ETPRO TROJAN Zeus Panda Banker / Urnsif Malicious SSL Certificate Detected”
* Located the Source and Destination IP Addresses and timestamp from alerts:
  + Src/Prt: 10.22.15.119:80
  + Dst/Prt: 46.29.160.132:49208
  + Time Stamp: 2018-11-07 20:47 UTC
* Identified IP Address and communications from Snort logs:



**Post-Incident Report**

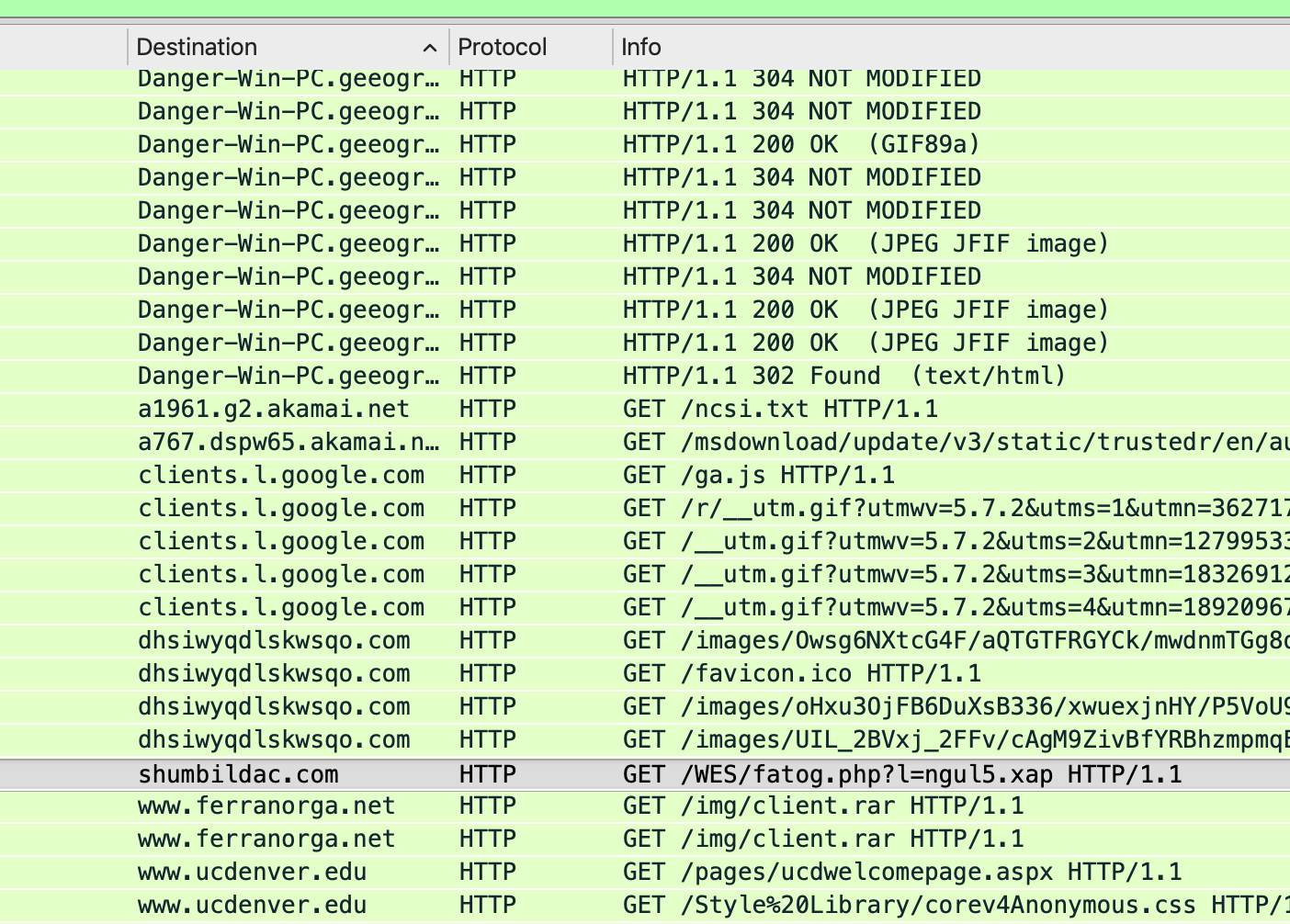


* Identified Hostname and MAC address of infected host computer from \*.pcap:
  + MAC address: 00:11:2f:d1:6e:52
  + Host Name: Danger-Win-PC

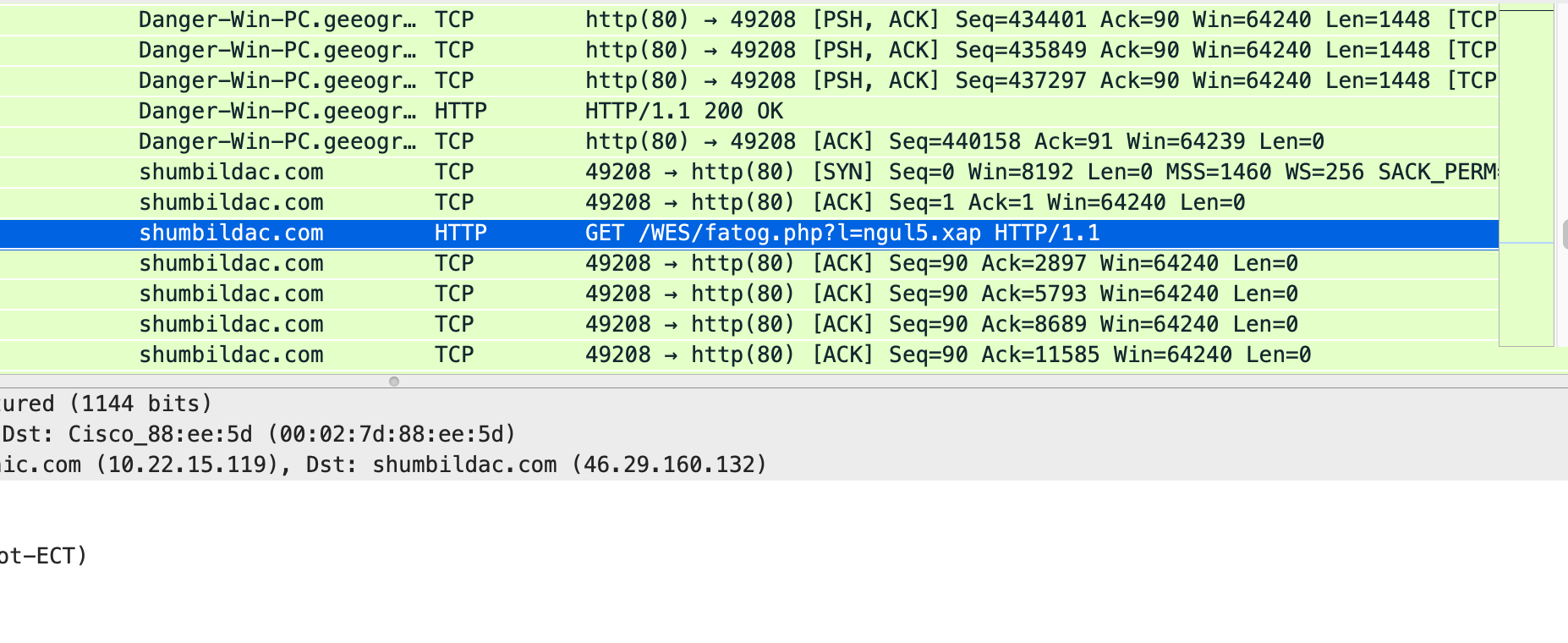


**Post-Incident Report**

* Identified network traffic and potential file download by using the *http* filter in Wireshark.
  + The user was also viewing other sources while this file was downloaded



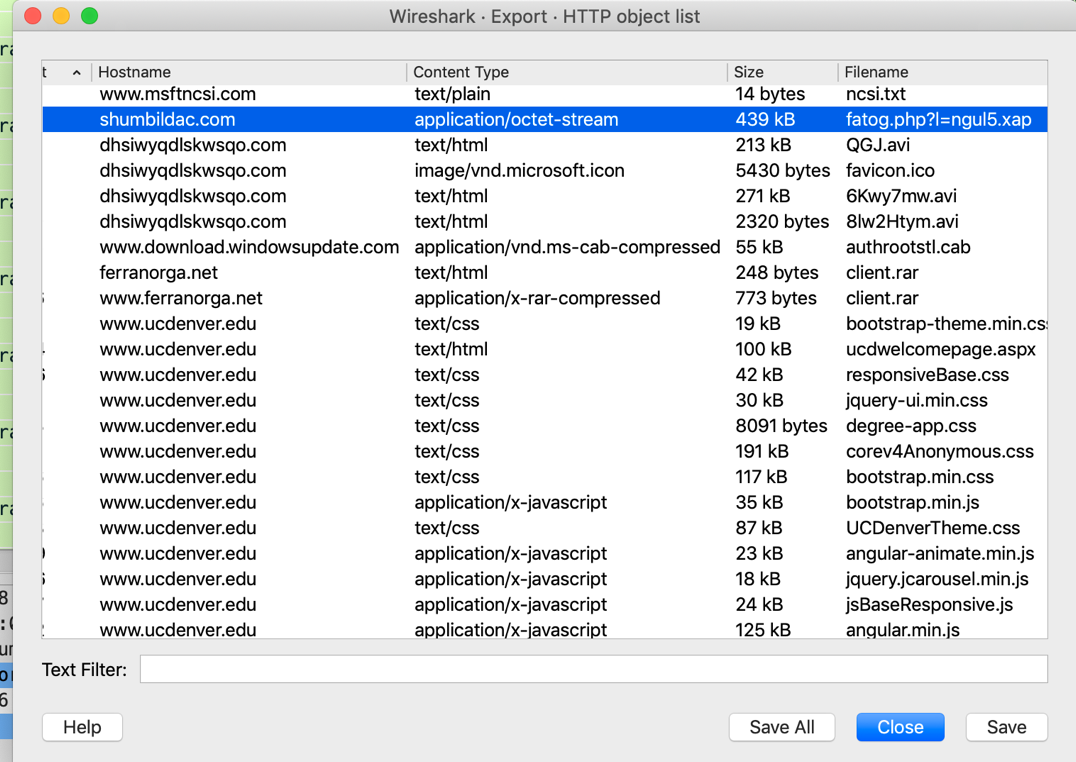
* + By using “ip.addr == 46.29.160.132” as a filter from the Snort logs, I concluded that while looking in the traffic finding file downloads from that IP address might lead to finding the malicious activity.



* Verifying a file was downloaded from the IP Address via alert, a file titled **“ngul5.xap”** has a high potential of being the malicious file.
  + Following the TCP Stream revealed the comment “This program cannot be run in DOS mode.”



* With the DOS header being an indication of a potential malicious item, the following was done:
  + Using Wireshark to download HTTP objects, found the “ngul5.xap”



**Post-Incident Report**

* Upon saving the “\*.xap” file the SHA256 sum needed to be verified to make sure that the download was actually malicious
  + 97f149f146b0ec63c32abff204ae27638f0310536172b0f718f1a91a5672fe71 ngul5.xap
* After inputting the SHA256 Sum into Virustotal the following was confirmed:
  + Virustotal came back with the results of 57/70 AV companies came back as this being malicious.
  + Under the comments section it came back as Ursnif
* Adding a firewall rules to potentially block future infections from this Malware

# IPv4 destination address and port.

* + iptables --append INPUT --in-interface eth0 --protocol tcp --source 46.29.160.132/32 --source-port 80 --jump DROP