Web content filtering and log data analysis with MikroTik routers

Paul Greeff
paulg@lucidview.net
Contents

1. The problem

2. Content filtering
   a. Methods (L7 for torrents, L7 for DNS, DNS poisoning)
   b. Pros and Cons

3. Traffic analysis
   a. Methods (Netflow self managed, Netflow cloud)
   b. Pros and Cons

4. MikroTik Enforcer Portal by LucidView

5. Thank you
The problem - Inappropriate content
The problem - Malware
The problem - Torrent management
Methods - MikroTik L7 Filtering

Layer 7 filtering for torrents on MikroTik RouterOS

L7 regular expression matches

```bash
[admin@MikroTik] /ip firewall layer7-protocol> add name=torrentsites regexp="^;+{get|GET},+{torrent
"...
"... thepiratebay|isohunt|entertain|deemonid|btjunkie|mininova|flixflux|
"... torrentz|vertor|h33t|btscene|bitunity|bitnonic|thunderbytes|
"... entertain|zooz|vcdq|bitnova|bitsoup|meganova|fulldls|btbot|
"... flixflux|seedpeer|fenopy|gpirate|commonbits),.*$\n```

[admin@MikroTik] /ip firewall layer7-protocol>
Methods MikroTik L7 filtering

Firewall rules for key words in L7 filter on MikroTik RouterOS

```
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 layer7-protocol=torrentsites action=drop comment=torrentsites
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 protocol=17 dst-port=53 layer7-protocol=torrentsites action=drop comment=dropDNS
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=torrent action=drop comment=keyword_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=tracker action=drop comment=trackers_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=getpeers action=drop comment=get_peers_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=info_hash action=drop comment=info_hash_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=announce_peers action=drop comment=announce_peers_drop
```

What is the problem with the above?
Methods - MikroTik L7 filtering for DNS

L7 DNS filtering on MikroTik RouterOS

```
[admin@MikroTik] /ip firewall layer7-protocol> add name=adult regexp="www.dodgy-site.com|freeporn|tube21.com|www.nakedpapis.com|lustylist.com|
"/... or.com|www.teenpornvideos.pro|www.besthotgirls.net|aladulthebooks.com|www.mygirlfriends
watch|
"/... h.com|chaturbate.com|www.hqcelebrityfakes.com|porn.im.29001300.21973697.hlsint.x.xvide
os.c|
tporz|
"/... n.pro|www.porn.gif.xxx.com|www.redpornnow.com|hornynakedteen.com|img100-541.xvideos.com|
bigs|
cooc|
"/... h.club|www.mhd6.com|v2.allurexxxclub.com|www.animal-taboo.com"
```

Firewall rule to block DNS request

```
[admin@MikroTik] /ip firewall filter> add action=drop chain=forward comment=dropDNS dst-port=53 layer7-protocol=adult protocol=udp src-address=10.31.0.0/24
```
Methods - MikroTik L7 filtering for DNS

Result of L7 DNS filtering on MikroTik RouterOS - test on Ubuntu

```
paulg@chimera ~ $ host lustylist.com 10.31.0.1
;; connection timed out; no servers could be reached
paulg@chimera ~ $ host www.google.co.za
www.google.co.za has address 216.58.223.35
www.google.co.za has IPv6 address 2c0f:fb50:4002:803::2003
paulg@chimera ~ $  
```

Success! Blocked DNS does not resolve.

Other sites resolve successfully.
Pros of Layer 7 filtering on MikroTik RouterOS

- L7 simple to implement and very effective
- Can block on keyword, i.e., Regex: xxx, or domain
- Can block on payload content or DNS query
- Can be done on RouterOS
- Somewhat effective against host entries
Cons Layer 7 filtering

- “Almost all P2P traffic is encrypted, thus inspecting the content wouldn't help much.” - benefit of L7 is diminishing with torrents
- SSL - payload is encrypted
- Gaming
- Skype
- Lists maintained on RouterOS
- Lists limited by MikroTik resources (can impact small MikroTiks)
Methods DIY DNS poisoning

DIY Linux with Bind, PowerDNS or your favourite flavour.

Commercial or free category list, i.e., University Toulouse

- http://www.squidblacklist.org/,
- http://squidguard.mesd.k12.or.us/blacklists.tgz
- http://www.shallalist.de/
- http://urlblacklist.com

Implementation of this outside of the scope of RouterOS
Methods DNS poisoning

DNS request

Poisoned response
Methods - Commercial DNS

**Example: Safe DNS** - Any commercial or free DNS blocking service, OpenDNS (CISCO) etc.

Add IP address of MikroTik to DNS service portal

You can add 2 IP addresses

105.212.91.156

Comment

DNS Server addresses

SafeDNS Nameservers

195.46.39.39
195.46.39.40
Methods - Commercial DNS poisoning

Add address of DNS server on MikroTik RouterOS

```bash
[admin@MikroTik] > /ip dns set servers=195.46.39.39,195.46.39.40
```

Intercept all DNS requests and redirect to MikroTik

```bash
add action=dst-nat chain=dstnat dst-port=53 in-interface=bridge protocol=tcp to-addresses=192.168.88.1 to-ports=53
add action=dst-nat chain=dstnat dst-port=53 in-interface=bridge protocol=udp to-addresses=192.168.88.1 to-ports=53
```

DNS blocking test on Ubuntu - convenient blocking page

```bash
paulg@chimera ~ $ host www.porn.com
www.porn.com has address 195.46.39.1
paulg@chimera ~ $ host 195.46.39.1
1.39.46.195.in-addr.arpa domain name pointer blockpage.safedns.com.
```
Methods - Commercial DNS poisoning

Convenient blocked error page
Pros DNS poisoning

- Commercial DNS offerings - lists maintained by third parties
- Self managed DNS servers
- Free Blocking lists
- Blocking page
Cons DNS poisoning

- New sites not in lists
- Some lists are old
- Subscriptions expensive
Cons DNS poisoning

- Host entries, i.e., 94.199.252.153 www.porn.com porn.com

```bash
paulg@chimera ~ $ ping -c 1 www.porn.com
PING www.porn.com (195.46.39.1) 56(84) bytes of data.
^C
--- www.porn.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

```bash
paulg@chimera ~ $ sudo vi /etc/hosts
```

```bash
paulg@chimera ~ $ ping -c 1 www.porn.com
PING www.porn.com (94.199.252.153) 56(84) bytes of data.
^C
--- www.porn.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

- Tor network
Netflow Traffic analysis - The problem

Graphical traffic representation
Method - MikroTik Netflow log analysis

Enable Traffic flows on MikroTik RouterOS

```
[admin@MikroTik] > /ip traffic-flow set active-flow-timeout=5m cache-entries=64k enabled=yes
[admin@MikroTik] > /ip traffic-flow target add dst-address=10.31.0.253 port=9995
[admin@MikroTik] >
```
Method - Netflow log analysis

Example: nftopng on Ubuntu

Installation of nftopng (free tier) - Ubuntu

$ wget http://apt.ntop.org/18.04/all/apt-ntop.deb

$ sudo dpkg -i apt-ntop.deb

$ sudo apt-get update -y

$ sudo apt-get install nprobe ntopng
Method - Netflow log analysis

Example: nftopng on Ubuntu

$ sudo nprobe -i none -n none -3 9995 --zmq tcp://127.0.0.1:5555

$ mkdir /tmp/ntopng/ ; ntopng -d /tmp/ntopng/ -i tcp://127.0.0.1:5555 -w 8080
### Method - Netflow log analysis

<table>
<thead>
<tr>
<th>Application</th>
<th>L4 Proto</th>
<th>Client</th>
<th>Server</th>
<th>Duration</th>
<th>Breakdown</th>
<th>Actual Thpt</th>
<th>Total Bytes</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_Proxy</td>
<td>TCP</td>
<td>41.50.0.120:http-alt</td>
<td>192.168.88.11:42580</td>
<td>00:15</td>
<td>Client</td>
<td>748.63 kbit/s</td>
<td>4.12 MB</td>
<td>Info</td>
</tr>
<tr>
<td>HTTP_Proxy</td>
<td>TCP</td>
<td>41.50.0.120:http-alt</td>
<td>192.168.88.11:42580</td>
<td>00:15</td>
<td>Client</td>
<td>599.8 kbit/s</td>
<td>3.54 MB</td>
<td>Info</td>
</tr>
<tr>
<td>HTTP_Proxy</td>
<td>TCP</td>
<td>10.31.0.253:42584</td>
<td>41.50.0.120:http-alt</td>
<td>00:15</td>
<td>Client</td>
<td>13.42 kbit/s</td>
<td>83.78 KB</td>
<td>Info</td>
</tr>
<tr>
<td>G+ SSL,Google</td>
<td>TCP</td>
<td>216.58.223.8:https</td>
<td>192.168.88.11:36760</td>
<td>00:59</td>
<td>Client</td>
<td>109.33 bit/s</td>
<td>38.16 KB</td>
<td>Info</td>
</tr>
</tbody>
</table>
Pros

- Visibility
- Own infrastructure
- Analysis in house
- Configurable
- Can be free or subscription
Cons

- Can be expensive
- Maintenance of software and hardware
- Skilled technical resources
- Lots of manual configuration required
- Does not scale
MikroTik Enforcer Portal

Netflow and DNS in cloud

<table>
<thead>
<tr>
<th>VPN IP</th>
<th>Device Serial</th>
<th>DNS Locale</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.224</td>
<td>ABCDEFG123456</td>
<td>UK</td>
</tr>
</tbody>
</table>

**Enforcer Type**

Bolt-On

**Client Email (Optional)**

client@address.com

Please note: By adding an email address here, you complete the process of claiming a device to an email address.

**Friendly Name**

New Client

Populating this name input, will provide an additional reporting field, and a more personalized look n feel. It can be added at a later time.
MikroTik Enforcer Portal - RouterOS scripts

Script generated on MikroTik Enforcer Portal

Generating Enforcer Install Script for Bolt-on Enforcer:

The LucidView Enforcer Bolt-on solution caters for existing Mikrotik installations that will benefit from the content filter and reporting provided by LucidView. The Enforced Mikrotik is still managed by your network team via your preferred tools with the additional functionality of content filter and reporting.

LucidView Unique ID: [Redacted]
Password: [Redacted]
Mikrotik Internal IP: 192.168.88.1
If left blank, the above default IP will be issued.

Once “Generate Script” has been clicked, your download will start automatically.

Ensure that you have read, and understand this document as it contains imperative information regarding the Enforcer type, and its purpose.
MikroTik Enforcer Portal - Technical

Features (script to follow)

- VPN to LucidView Cloud for kill lists
- Traffic flow to Cloud
- DNS via VPN (and syslog)
- DNS failover
- DNS Intercept
- Firewall Kill list
- Category filtering
- Reporting
MikroTik Enforcer Portal - Content filter

The Selected Categories below are blocked.

- **Untrustworthy**: HTTPS sites that do not have valid SSL certificates hosted on them. - EXPERIMENTAL

- **Facebook**: Facebook and Instagram

- **Gaming**: Gaming, and gaming related sites. It is recommended that the "suspicious" also be blocked in conjunction with blocking this category to more effectively block online gaming

- **Anonymizer**: Web based proxies and unblock sites to bypass firewalls content filters

- **Suspicious**: These are connection that are typically used by hackers to gain remote access into your network, through which they attempt to conduct their nefarious activities such as stealing data, or planting ransomware, etc.
MikroTik Enforcer Portal - Dashboard
MikroTik Enforcer Portal - Dashboard
MikroTik Enforcer Portal - Reports

Table View: Top domains per Source IP - Previous Week: 2018-09-03 - 2018-09-09

Source IP shown: 192.168.8.2

Top domains by GBs

The table below shows the top domains for device IP 192.168.8.2 and the amount of data that has been transferred. For a more detailed IP report pull a "Specific Device Report" on the portal.

<table>
<thead>
<tr>
<th>Domain</th>
<th>GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>2.131</td>
</tr>
<tr>
<td>microsoft.com</td>
<td>2.022</td>
</tr>
<tr>
<td>windowsupdate.com</td>
<td>0.837</td>
</tr>
<tr>
<td>google.co.za</td>
<td>0.738</td>
</tr>
<tr>
<td>fbcdn.net</td>
<td>0.728</td>
</tr>
</tbody>
</table>
MikroTik Enforcer RouterOS script

Variables

# Declaring variables
global vpnuser
global vnpass
global mikrotikip
#
#Below are the Unique per Mikrotik VPN settings for the LucidView cloud.
set vpnuser 012345678
set vnpass 0123456789abcdef0123456789abcdef0123456789abcdef|
# Below is the Actual internal IP set on your Mikrotik, that must be available
set mikrotikip 192.168.88.1
MikroTik Enforcer RouterOS script

VPN and cloud access

```bash
# VPN
# In order for the LucidView Cloud to uniquely identify the particular Mikrotik
# Please check that the interface is up. Ping 1.1.1.1 from the Mikrotik to check
# as it will be dropped by the server on the other side.

/interface l2tp-client
add connect-to=red-box.lucidview.net disabled=no name=lvcloud password=\ $vpnpass user=\ $vpnuser

# An SSH key is added for the LucidView cloud server to manage the kill lists. I
# them as the file may not have been created by the time the import command is

/file print file=lvcloud.pub :delay 5
/file set lvcloud.pub contents="ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQA7Ci73rwYcU..."
/user add group=full name=lvcloud password=\ $vpnpass :delay 5
/user ssh-keys import public-key-file=lvcloud.pub.txt user=lvcloud
```
MikroTik Enforcer RouterOS script

Firewall kill lists and DNS Intercept

```plaintext
# Kill lists
# Make sure the kill lists are above any allow all rules so that they are effective.
/ip firewall filter
add action=accept chain=forward comment=lvcloud_whitelist \
  dst-address-list=lvcloud_whitelist
add action=drop chain=forward comment=lvcloud_kill_list_external \
  dst-address-list=lvcloud_kill_list_external
add action=drop chain=forward comment=lvcloud_kill_list_internal \
  src-address-list=lvcloud_kill_list_internal
add chain=input in-interface=lvcloud action=accept comment=lvcloud_input
# Allow DNS requests to the Mikrotik on the firewall.
add chain=input connection-state=new action=accept protocol=udp port=53
add chain=input connection-state=new action=accept protocol=tcp port=53
# Intercept all DNS
/ip firewall nat
add action=dst-nat chain=dstnat comment=lvcloud dst-port=53 protocol=tcp \
  to-addresses=$mikrotikip
add action=dst-nat chain=dstnat comment=lvcloud dst-port=53 protocol=udp \
  to-addresses=$mikrotikip
```
MikroTik Enforcer RouterOS script

Log all DNS requests to Syslog server and enable Traffic flow

```bash
# DNS logging
# DNS requests are sent to the LucidView cloud syslog server for analysis.
/system logging action
add name=syslog remote=${collector} target=remote
/system logging
add action=syslog topics=dns,!packet
# Netflow
# Netflow allows LucidView to perform detailed reporting on all traffic. Traffic
# small Mikrotik struggle to keep track of flows of more than 10 minutes or so
/ip traffic-flow
set enabled=yes interfaces=all
/ip traffic-flow target
add dst-address=${collector} port=9995
/ip traffic-flow set active-flow-timeout=5m
```
MikroTik Enforcer RouterOS script

DNS failover in case of cloud accessibility problem

/system scheduler
add interval=1s name=vpn_dns on-event="/system script run vpn_dns"

\n\nglobal dnspublic\n\nset dnspublic $publicdns\n\nglobal dnsvpn\n\nset dnsvpn $collector\n\n\n\nif [interface get lvcloud running] do {
    \n    if ([/ip dns get servers] != $dnsvpn) do {
        \n        /ip dns set servers=$dnsvpn \n        \n    }\n\n} else {
    \n    if ([/ip dns get servers] != $dnspublic) do {
        \n        /ip dns set servers=$dnspublic\n        \n    }\n\n}"

policy=\nftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \nstart-date=jan/01/1970 start-time=00:00:00
MikroTik Enforcer Portal Pros

- Scales
- Affordable
- DNS and firewall blocking
- Simple to add (download complete script and modify to suit application)
- Detailed reporting
- Automated reporting (i.e., security reports to your inbox)
- Customised branding
- Youtube and Google safe search
- Torrent and Suspect blocking
- Time based rules
MikroTik Enforcer Portal Cons

Leaves you with too much time on your hands.

www.lucidview.net