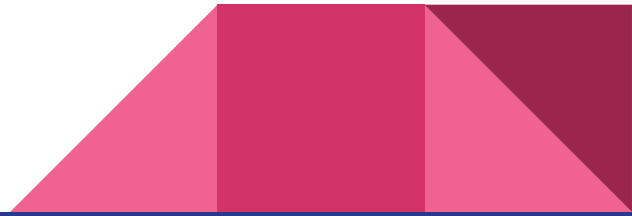
Web content filtering and log data analysis with MikroTik routers

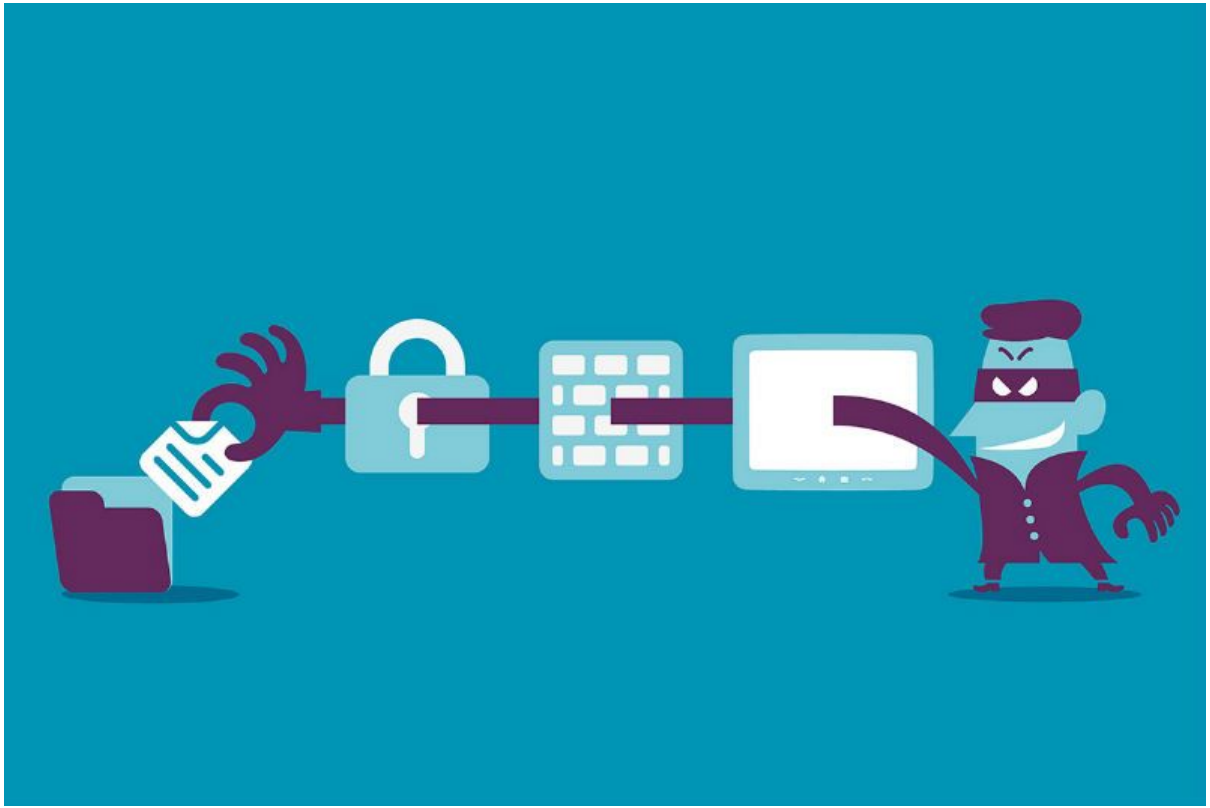
Paul Greeff
paulg@lucidview.net

Contents



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

```
[admin@MikroTik] /ip firewall layer7-protocol> add name=torrentsites regexp="^.*(get|GET).+(torr
ent|\
"\...       thepiratebay|isohunt|entertane|demonoid|btjunkie|mininova|flixflux|\
"\...       torrentz|vertor|h33t|btscene|bitunity|bittoxic|thunderbytes|\
"\...       entertane|zoozle|vcdq|bitnova|bitsoup|meganova|fulldls|btbot|\
"\...       flixflux|seedpeer|fenopy|gpirate|commonbits).*\$\
"\...       "
[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=getpeer
s action=drop comment=get_peers_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=info_ha
sh action=drop comment=info_hash_drop
[admin@MikroTik] /ip firewall filter> add chain=forward src-address=10.31.0.0/24 content=announc
e_peers action=drop comment=announce_peers_drop
[admin@MikroTik] /ip firewall filter>
```

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|freepor
ntube21.com|www.nakedpapis.com|lustylist.com|\
"\...      www.pussy.joburg|www.karupsgalleries.com|blackhoetube.com|www.porn-sex-xxx.info|dirty-
doct\
"\...      or.com|www.teenpornvideos.pro|www.besthotgirls.net|aladultebooks.com|www.mygirlfriends
watc\
"\...      h.com|chaturbate.com|www.hqcelebrityfakes.com|porn.im.29001300.21973697.hlsint.x.xvide
os.c\
"\...      om|tubeq.xxx|www.wotube.com|momspussy.net|www.juicycloseups.com|x-blackporn.com|www.fa
tpor\
"\...      n.pro|www.porngifxxx.com|www.redpornnow.com|hornynakedteen.com|img100-541.xvideos.com|
bigs\
"\...      exmom.com|www.xxxha.com|www.humiliationpov.com|www.girlsdoporn.com|adultshowsonly.com|
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

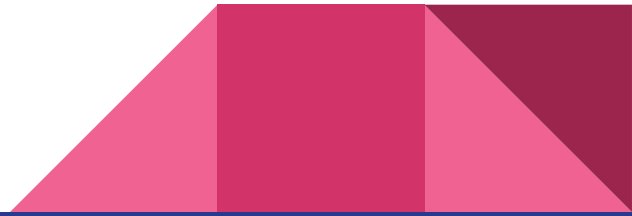
```
paulg@chimera ~ $ host lustylist.com 10.31.0.1
;; connection timed out; no servers could be reached
paulg@chimera ~ $ host www.google.co.za
www.google.co.za has address 216.58.223.35
www.google.co.za has IPv6 address 2c0f:fb50:4002:803::2003
paulg@chimera ~ $
```

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

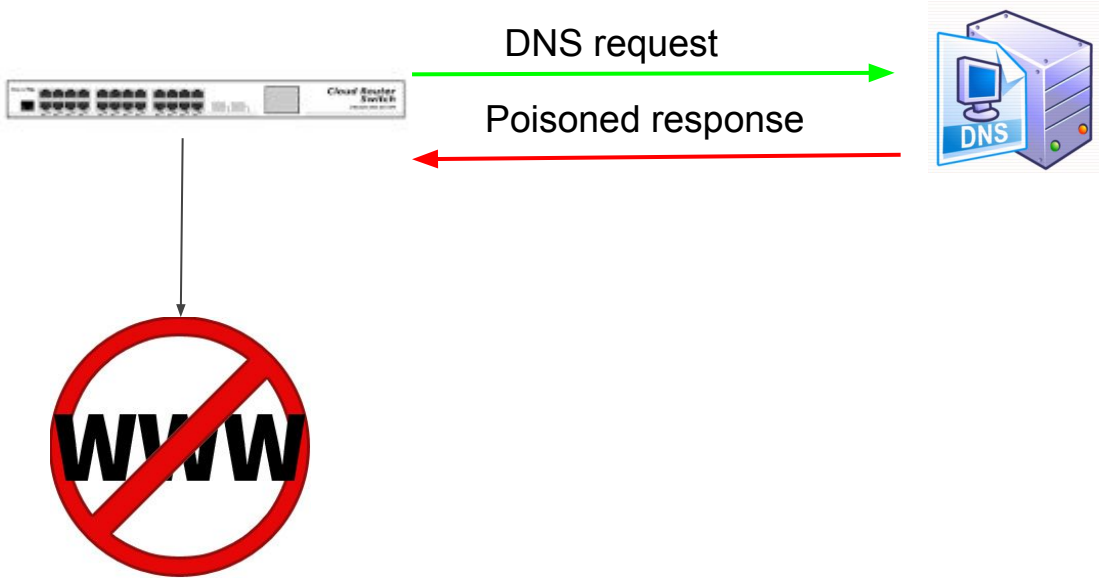
- http://dsi.ut-capitole.fr/blacklists/index_en.php
- http://www.squidblacklist.org/,
- http://squidguard.mesd.k12.or.us/blacklists.tgz
- http://www.shallalist.de/
- http://urlblacklist.com

Implementation of this outside of the scope of RouterOS

Example of categories

Category	Number
adult	2016767
agressif	360
arjel	69
associations_religieuses	1

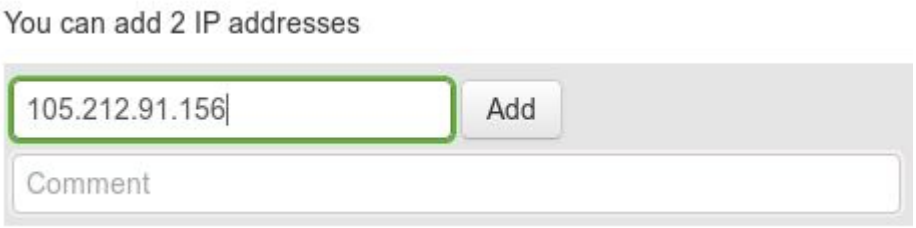
Methods DNS poisoning



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



DNS Server addresses

Methods - Commercial DNS poisoning

Add address of DNS server on MikroTik RouterOS

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

Intercept all DNS requests and redirect to MikroTik

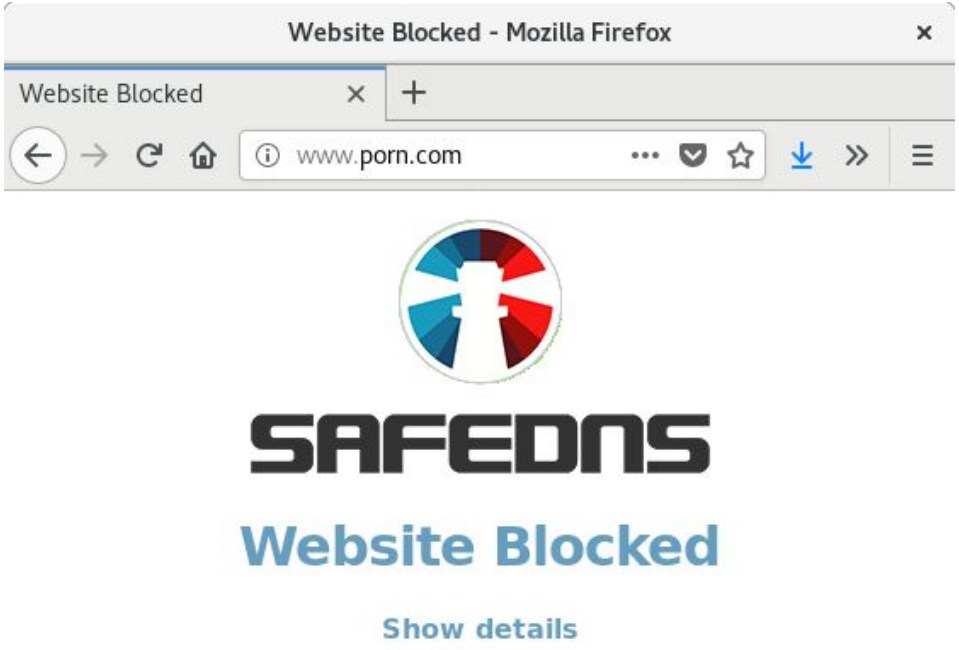
```
add action=dst-nat chain=dstnat dst-port=53 in-interface=bridge protocol=tcp to-addresses=192.168.88.1 to-ports=53
add action=dst-nat chain=dstnat dst-port=53 in-interface=bridge protocol=udp to-addresses=192.168.88.1 to-ports=53
```

DNS blocking test on Ubuntu - convenient blocking page

```
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



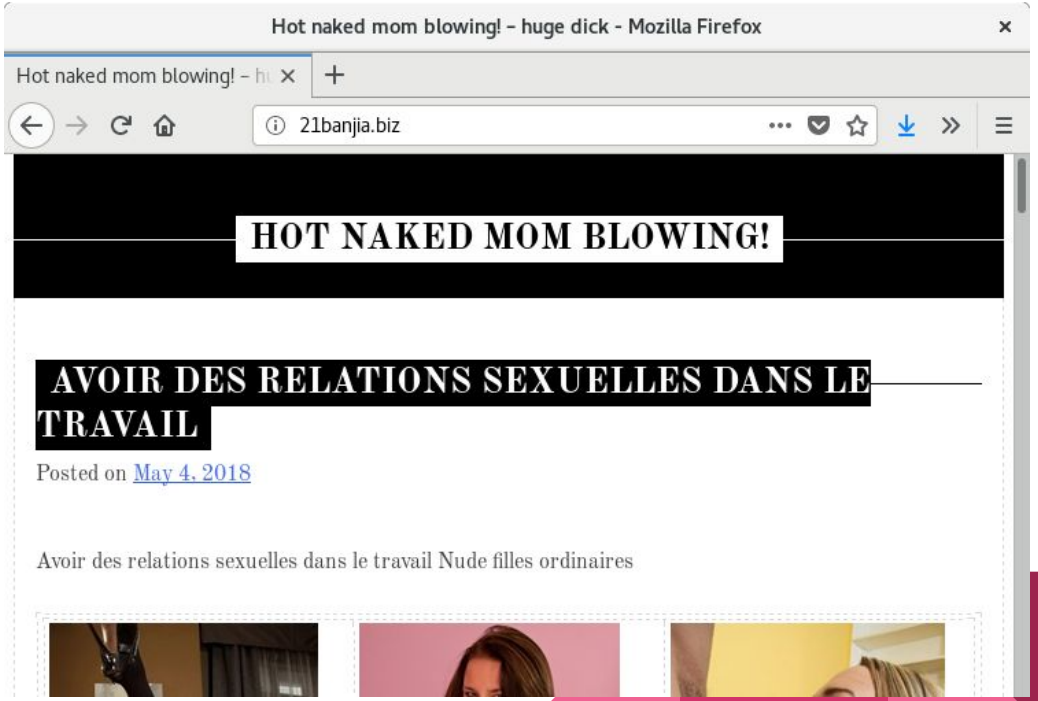
Pros DNS poisoning

- 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

```
paulg@chimera ~ $ host 21banjia.biz
21banjia.biz has address 104.28.28.72
21banjia.biz has address 104.28.29.72
21banjia.biz has IPv6 address 2400:cb00:2048:1::681c:1c48
21banjia.biz has IPv6 address 2400:cb00:2048:1::681c:1d48
```



Cons DNS poisoning

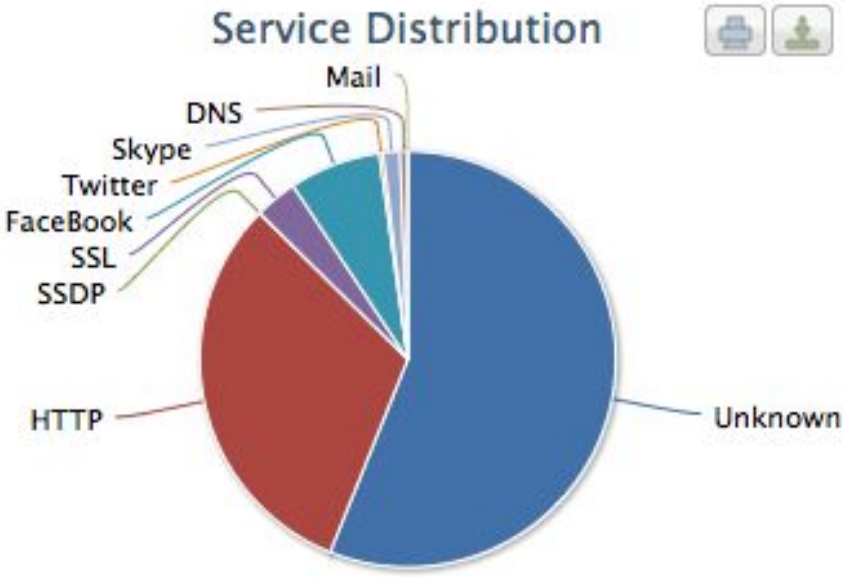
- Host entries, i.e., `94.199.252.153 www.porn.com porn.com`

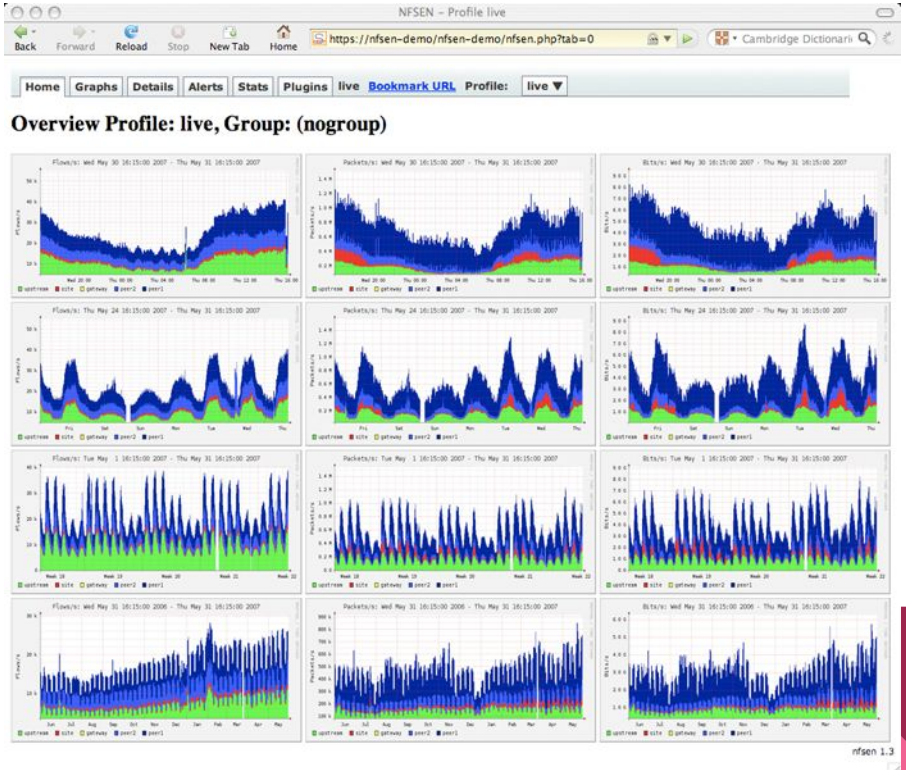
```
paulg@chimera ~ $ ping -c 1 www.porn.com
PING www.porn.com (195.46.39.1) 56(84) bytes of data.
^C
--- www.porn.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

paulg@chimera ~ $ sudo vi /etc/hosts
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

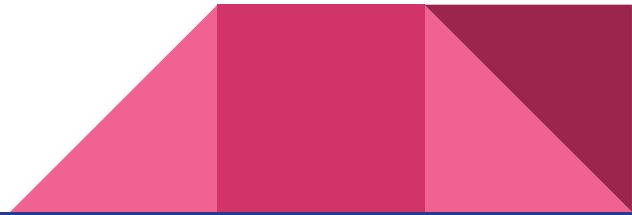
$ sudo apt-get install nprobe ntopng

Method - Netflow log analysis

Example: nftopng on Ubuntu

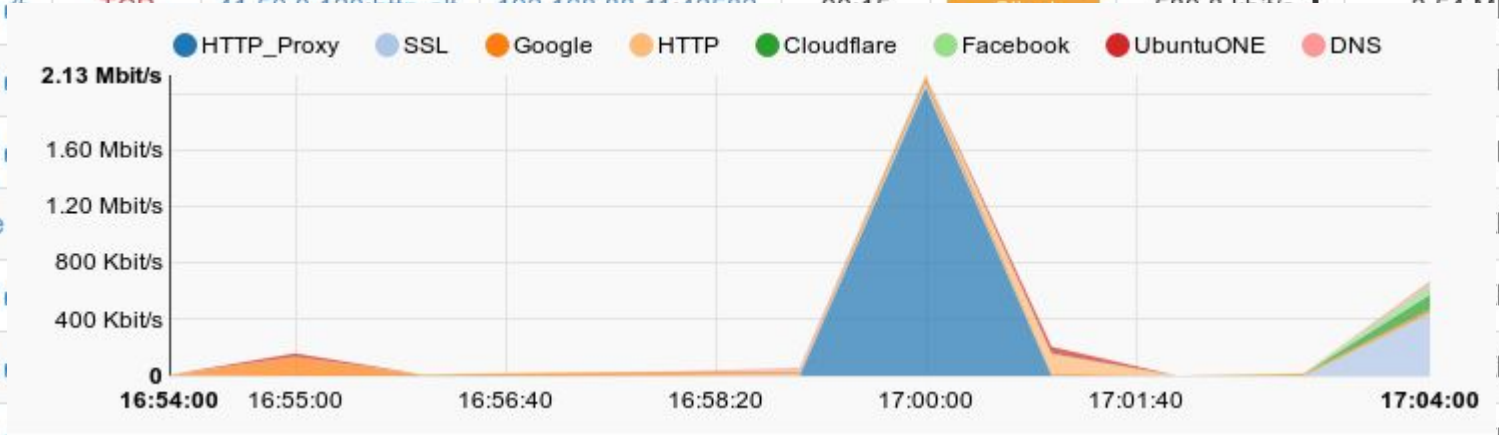
$ sudo nprobe -i none -n none -3 9995 --zmq tcp://127.0.0.1:5555

$ mkdir /tmp/ntopng/ ; ntopng -d /tmp/ntopng/ -i tcp://127.0.0.1:5555 -w 8080



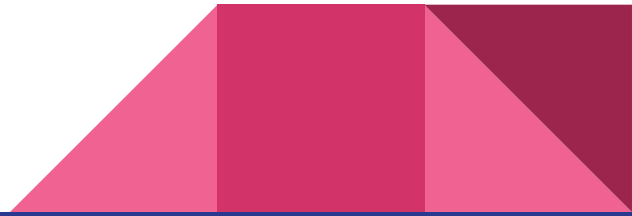
Method - Netflow log analysis

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP_Proxy	TCP	41.50.0.120:http-alt	192.168.88.11:42580	00:15	Client	748.63 kbit/s ↓	4.12 MB	
Info	HTTP_Proxy							B	
Info	HTTP_Proxy							B	
Info	HTTP_Proxy							B	
Info	Google							B	
Info	HTTP_Proxy							B	
Info	HTTP_Proxy							B	
Info	HTTP_Proxy							B	
Info	HTTP_Proxy	TCP	10.31.0.253:42584	41.50.0.120:http-alt	00:15	Client	13.42 kbit/s ↓	83.78 KB	
Info	SSL.Google	TCP	216.58.223.8:https	192.168.88.11:36760	00:59	Client	109.33 bit/s ↑	38.16 KB	



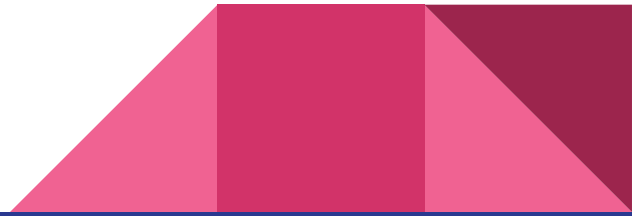
Pros

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



Cons

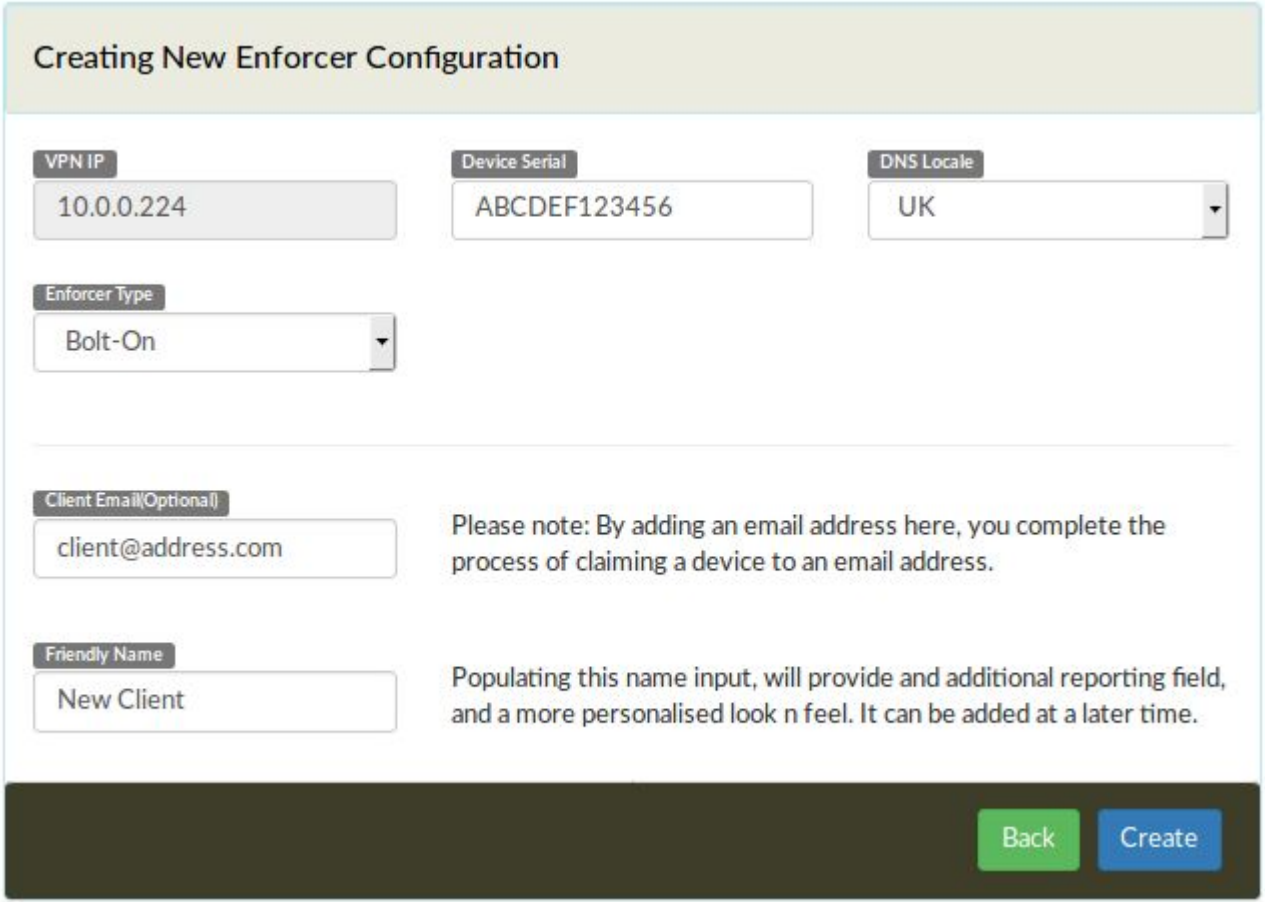
- Can be expensive
- Maintenance of software and hardware
- Skilled technical resources
- Lots of manual configuration required
- Does not scale



LucidView’s MikroTik Enforcer Portal

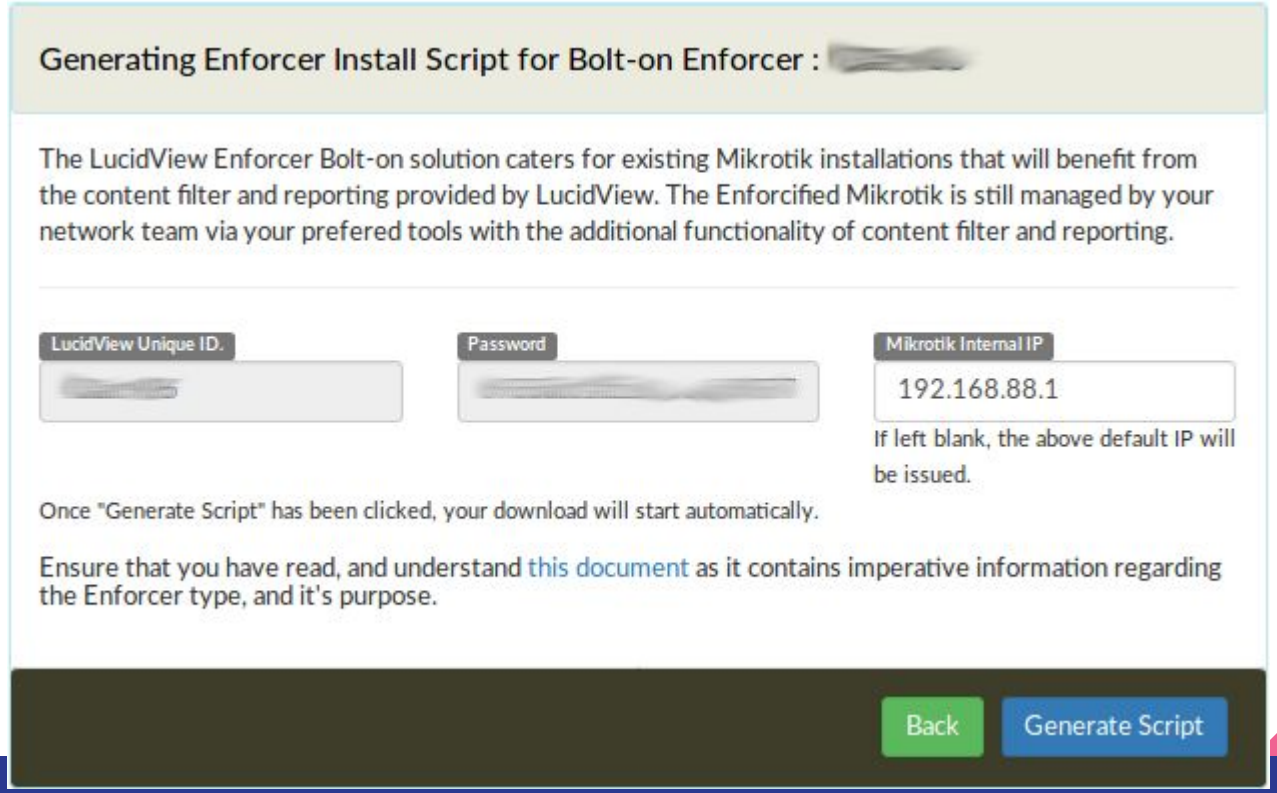
MikroTik Enforcer Portal

Netflow and DNS in cloud



MikroTik Enforcer Portal - RouterOS scripts

Script generated on MikroTik Enforcer Portal



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

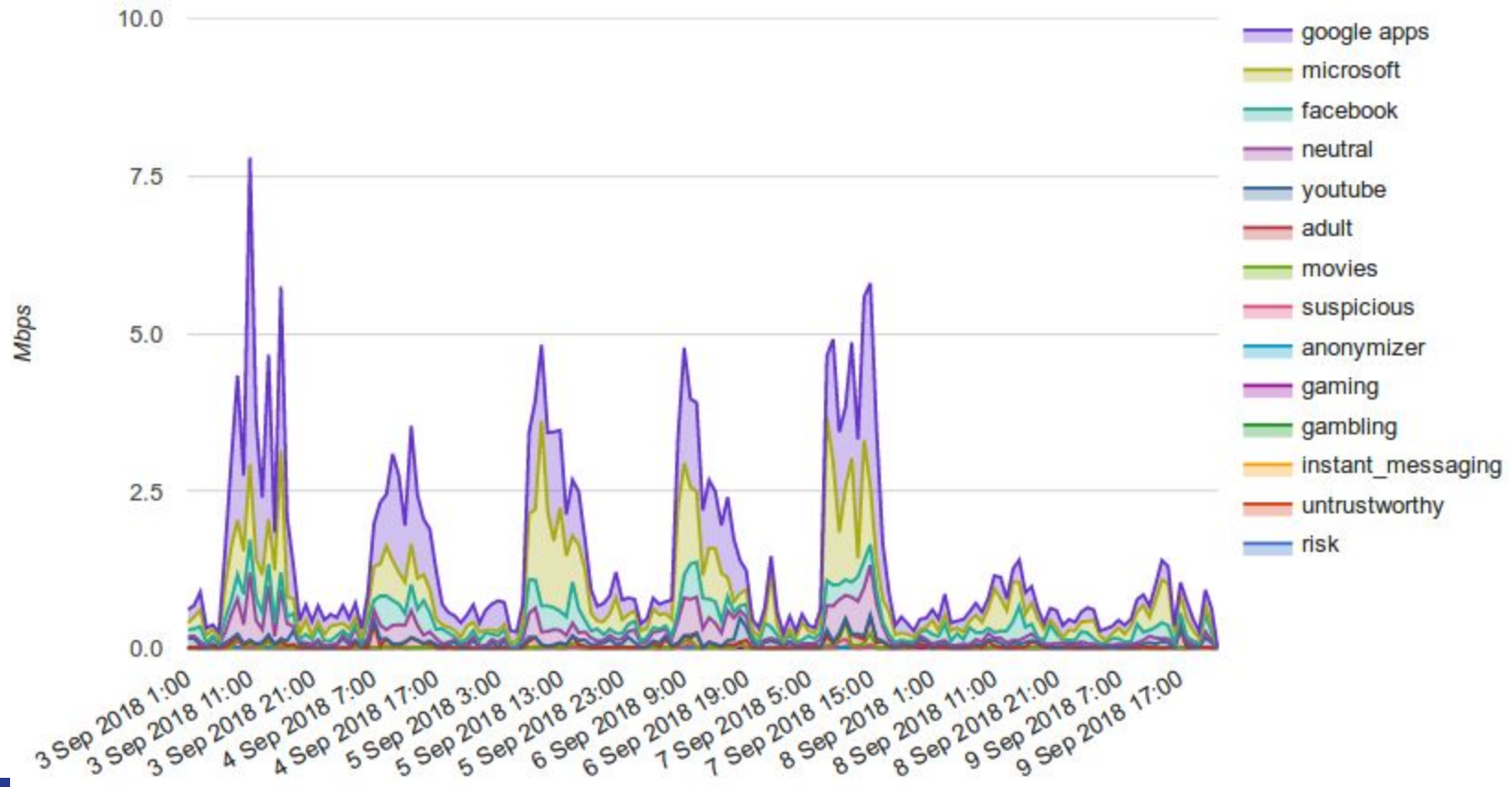
Anonymizer ☑

Web based proxies and unblock sites to bypass firewalls content filters

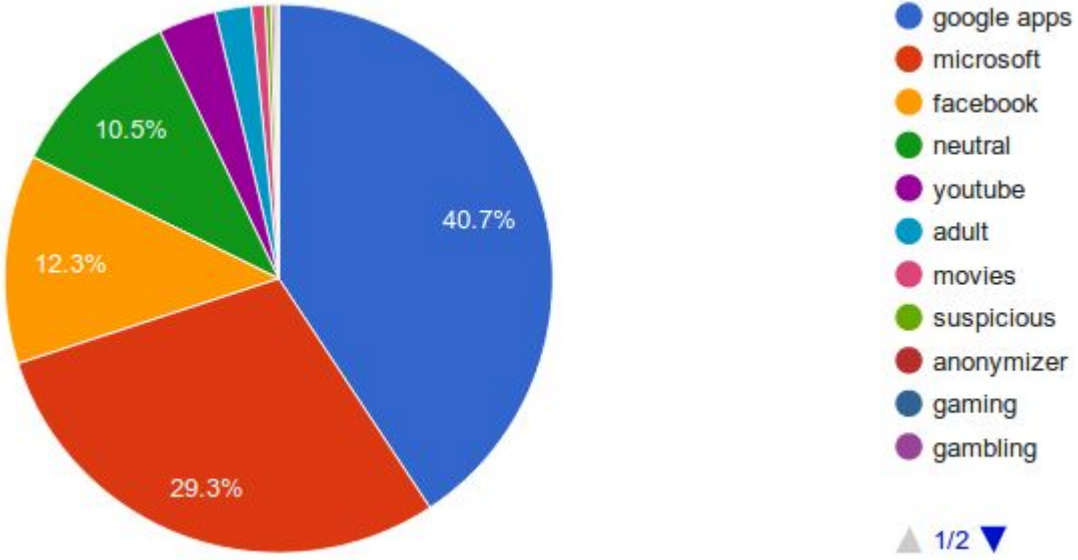
Suspicious ☑

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.

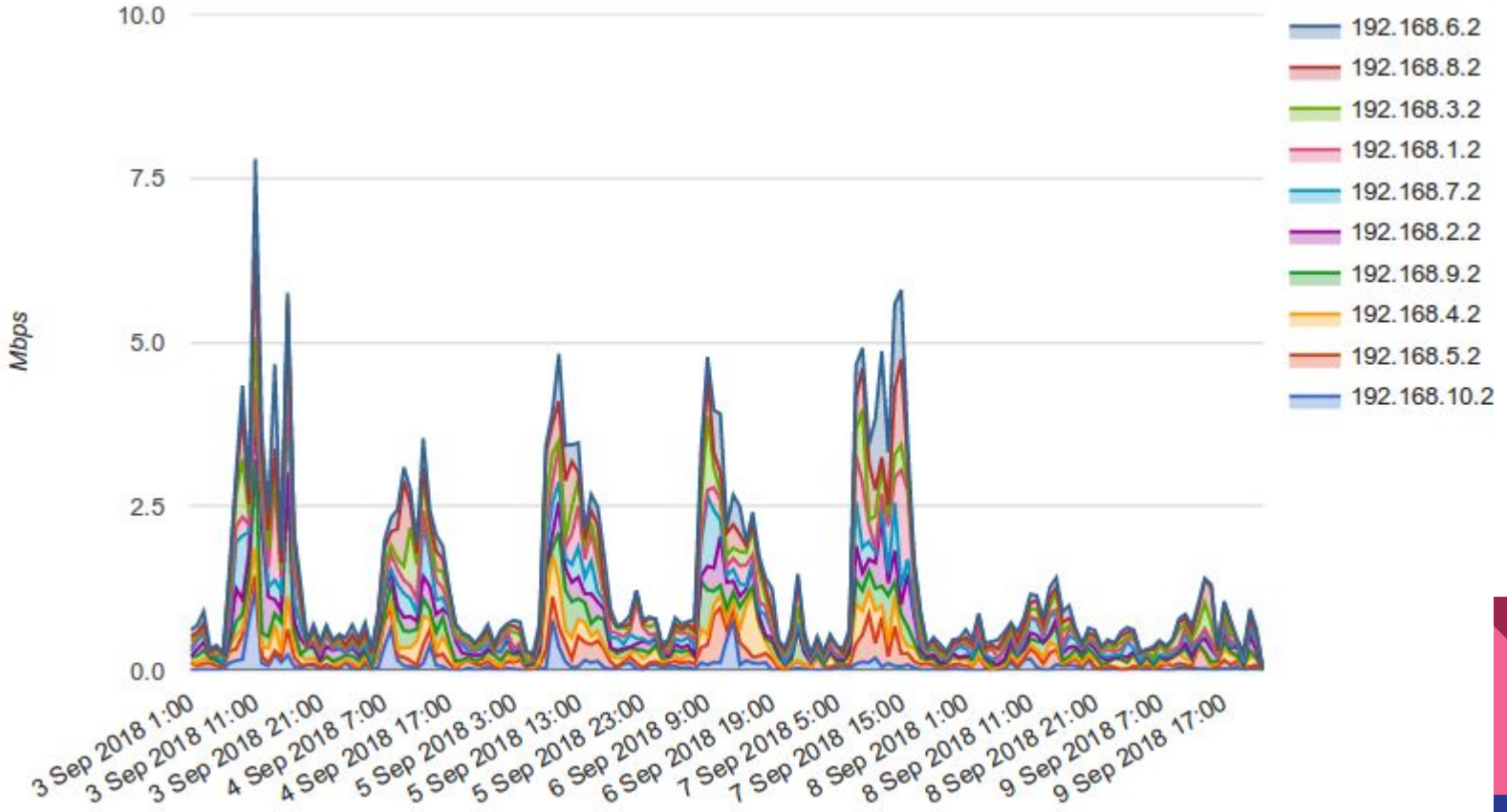
MikroTik Enforcer Portal - Dashboard



MikroTik Enforcer Portal - Dashboard



MikroTik Enforcer Portal - 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.

Domain	GB
google.com	2.131
microsoft.com	2.022
windowsupdate.com	0.837
google.co.za	0.738
fbcdn.net	0.728

MikroTik Enforcer RouterOS script

Variables

```
# Declaring variables
global vpnuser
global vpnpass
global mikrotikip
#
#Below are the Unique per Mikrotik VPN settings for the LucidView cloud.
set vpnuser 012345678
set vpnpass 0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
# 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

```
# VPN
# In order for the LucidView Cloud  to uniquely identify the particular Mikroti
# Please check that the interface is up. Ping 1.1.1.1 from the Mikrotik to chec
# 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.
# 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 AAAAB3NzaC1yc2EAAAADAQABAAABAQCij3rwYcU
/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

```
# Kill lists
# Make sure the kill lists are above any allow all rules so that they are effec
/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

```
# DNS logging
# DNS requests are sent to the LucidView cloud syslog server for analysis.
/system logging action
add name=syslog remote=$collector target=remote
/system logging
add action=syslog topics=dns,!packet
# Netflow
# Netflow allows LucidView to perform detailed reporting on all traffic. Traffi
# small Mikrotiks struggle to keep track of flows of more than 10 minutes or so
/ip traffic-flow
set enabled=yes interfaces=all
/ip traffic-flow target
add dst-address=$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\r\
   \n:global dnspublic\r\
   \n:set dnspublic $publicdns\r\
   \n:global dnsvpn\r\
   \n:set dnsvpn $collector\r\
   \n\r\
   \n:if [interface get lvcloud running] do {\r\
   \n    :if ([/ip dns get servers] != \$dnsvpn) do {\r\
   \n     /ip dns set servers=\$dnsvpn \r\
   \n    }\r\
   \n} else { \r\
   \n    :if ([/ip dns get servers] != \$dnspublic) do {\r\
   \n     /ip dns set servers=\$dnspublic\r\
   \n    }\r\
   \n}" policy=\
   ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
   start-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