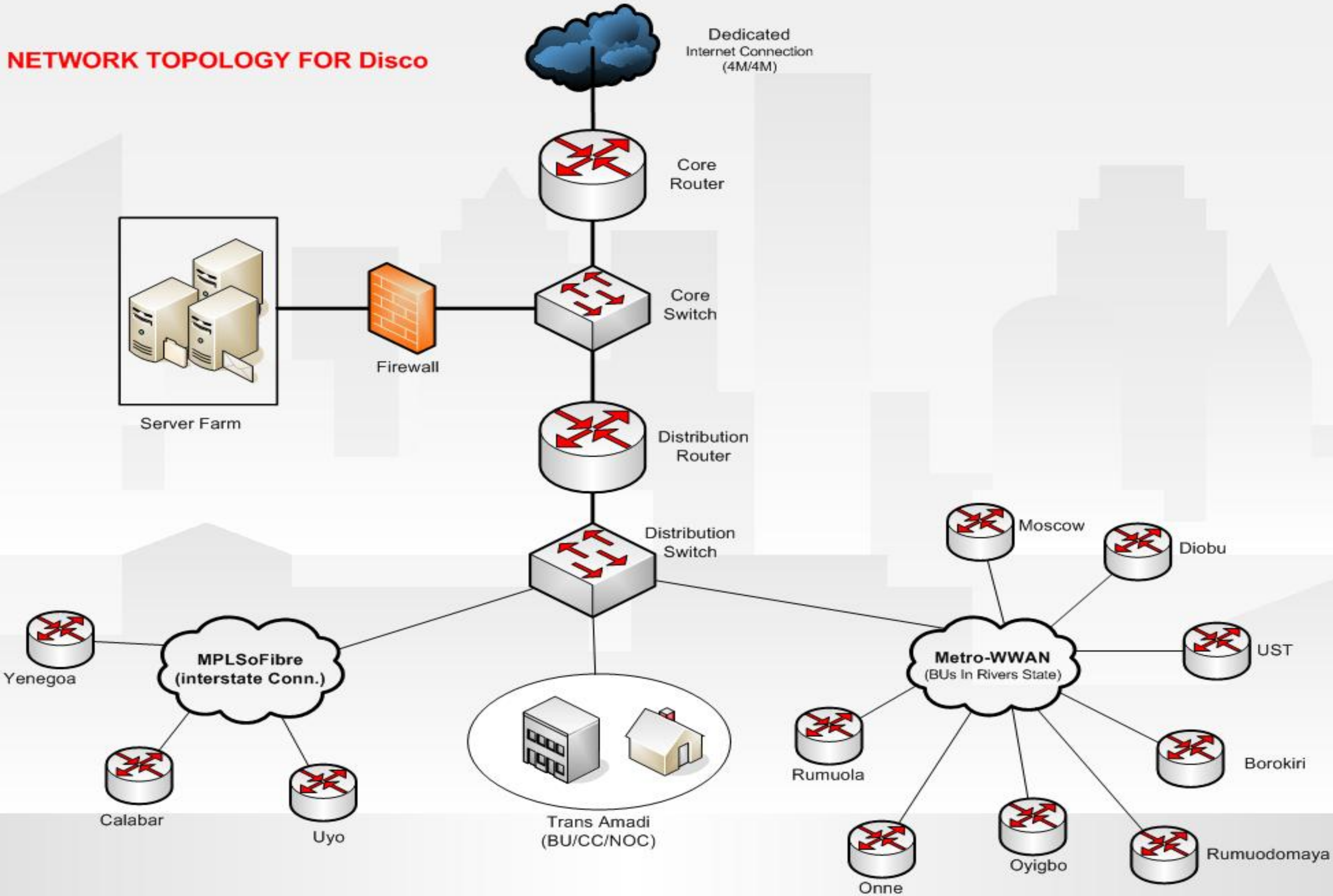
Firewall and QoS in Enterprise Network

About Me

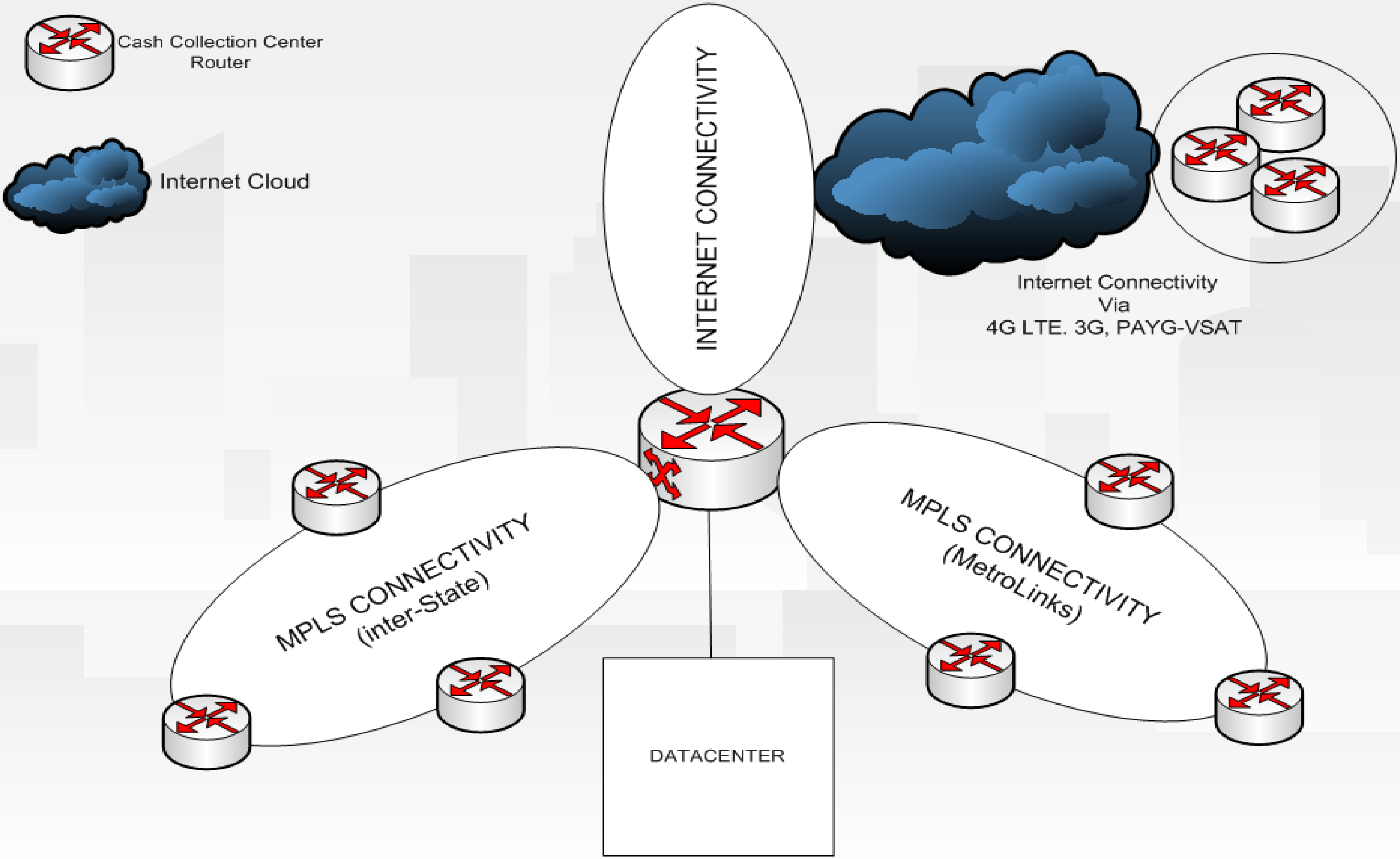
Abiola Oseni – CEO, Trisat Communications Limited, Nigeria

- Using Mikrotik RouterOS since 2005
- Mikrotik Certified Consultant since 2007
- Mikrotik Certified Trainer since 2009
- Trained and Certified over 500 Mikrotik Users Across Africa
- Deployed Mikrotik RouterOS for WISP and Corporate Organizations in various horizontal markets such as Oil & Gas, Utilities – (Electricity, Water), Banks, Maritime, Telecoms, IT Retails, etc.

Recent Project Electricity Distribution Company



Recent Project Electricity Distribution Company

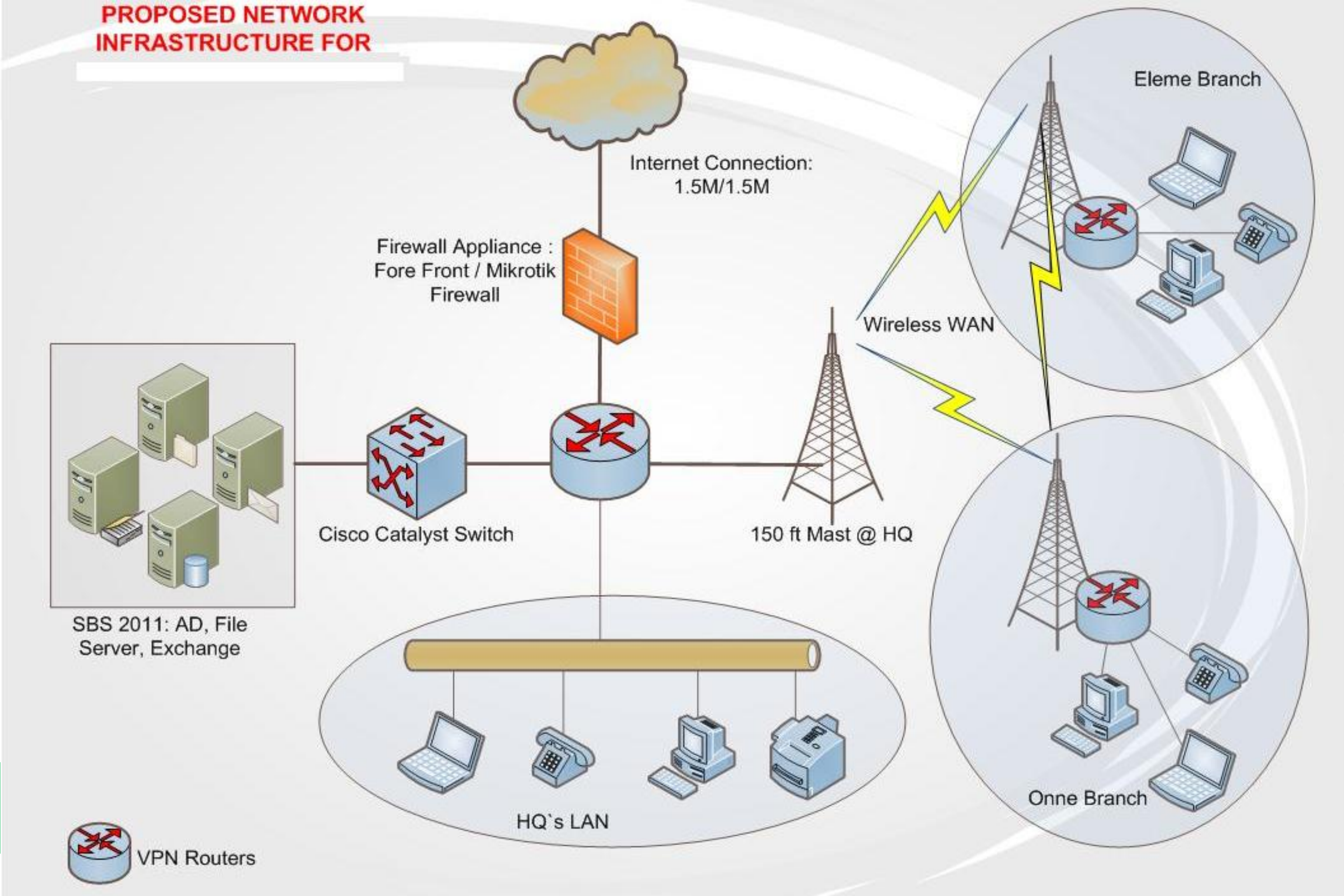


Recent Project

Electricity Distribution Company

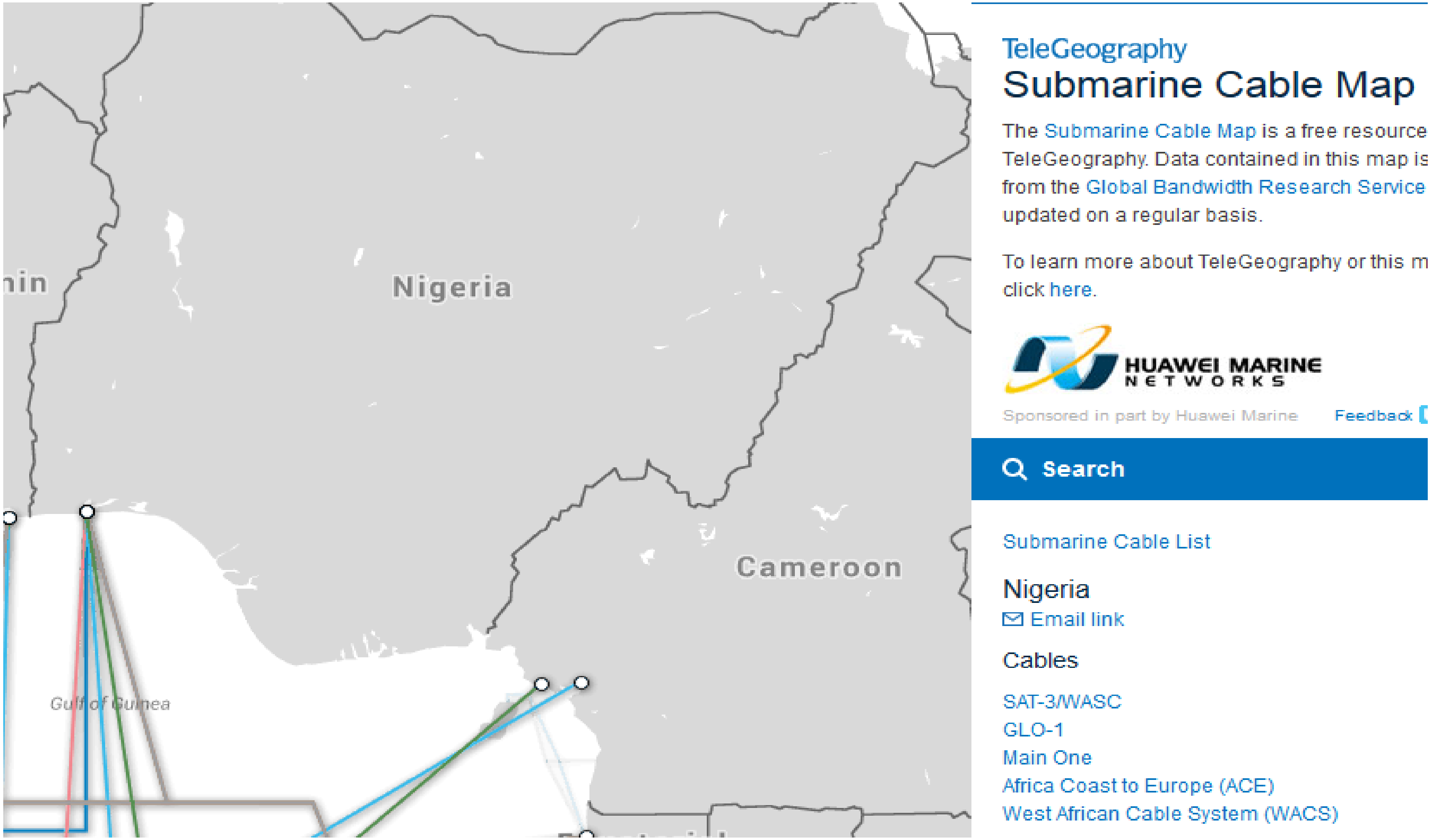
Recent Project

Oil & Gas Servicing Company


PROPOSED NETWORK INFRASTRUCTURE FOR
Internet Connection: 1.5M/1.5M
Firewall Appliance : Fore Front / Mikrotik Firewall
Eleme Branch
Wireless WAN
Cisco Catalyst Switch
150 ft Mast @ HQ
SBS 2011: AD, File Server, Exchange
HQ`s LAN
Onne Branch
VPN Routers

Recent Project Oil & Gas Servicing Company

State of Internet In Nigeria



TeleGeography

Submarine Cable Map

The Submarine Cable Map is a free resource TeleGeography. Data contained in this map is from the Global Bandwidth Research Service updated on a regular basis.

To learn more about TeleGeography or this m click here.

HUAWEI MARINE NETWORKS

Sponsored in part by Huawei Marine

Feedback

Search

Submarine Cable List

Nigeria

Email link

Cables

SAT-3/WASC
GLO-1
Main One
Africa Coast to Europe (ACE)
West African Cable System (WACS)

Case Study Oil & Gas Servicing Company

Client Profile:

A leading distributor of drilling and completion fluids used by global hydrocarbon recovery and processing industries. – Chemical Plant

Case Study

Oil & Gas Servicing Company

Client Profile:
A specialist in Bulk Methanol Delivery - Warehouse

Case Study Oil & Gas Servicing Company

Project Objectives:

- To centralize all Line of Business (LOB) Application at the HQ. This Includes Email Server, ERP, VoIP Gateway etc

- To deploy CCTV in all 3 locations; HQ, Warehouse & the Chemical Plant

- Access to the CCTV from anywhere through the Internet & WAN without delay or buffering.

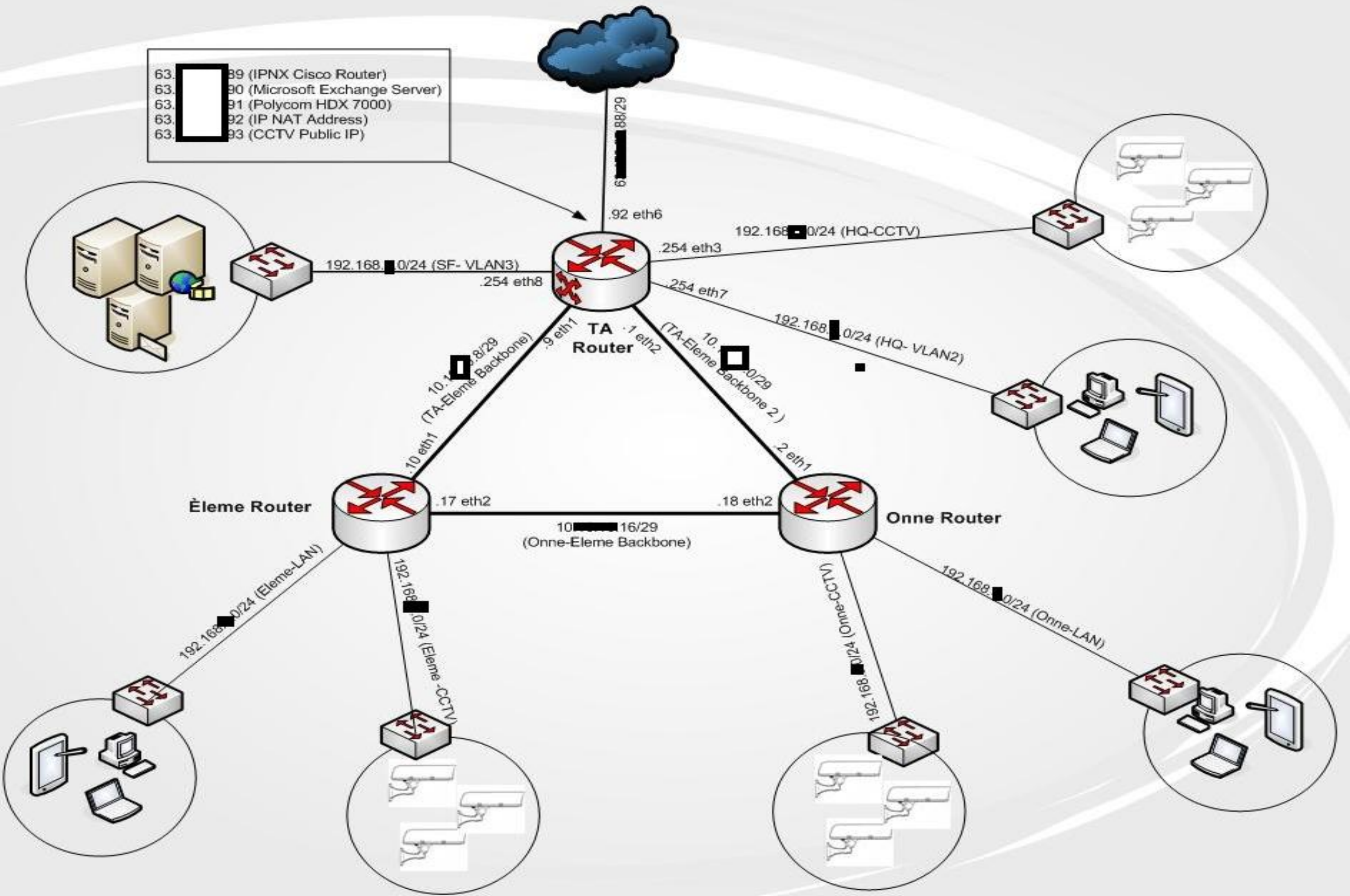
- To optimize WAN and Internet Connectivity for 98.5% Uptime availability for the LOB application and CCTV surveillance

- To ensure that Internet Bandwidth is guaranteed for the LOB application and the surveillance system. Total Bandwidth is 4Mbps/4Mbps

- Project goal must be achieved with the most cost-saving approach

Case Study

Oil & Gas Servicing Company



63.[redacted]89 (IPNX Cisco Router)
63. 90 (Microsoft Exchange Server)
63. 91 (Polycom HDX 7000)
63. 92 (IP NAT Address)
63. 93 (CCTV Public IP)

6[redacted]88/29
.92 eth6
192.168[redacted]0/24 (HQ-CCTV)
.254 eth3
192.168.[redacted]0/24 (SF- VLAN3)
.254 eth8
.254 eth7
192.168.[redacted]0/24 (HQ- VLAN2)
TA Router
.9 eth1
.1 eth2
10.1[redacted].8/29 (TA-Eleme Backbone)
10.[redacted]0/29 (TA-Eleme Backbone 2)
.10 eth1
.2 eth1
Èleme Router
.17 eth2
.18 eth2
10[redacted]16/29 (Onne-Eleme Backbone)
Onne Router
192.168[redacted]0/24 (Eleme-LAN)
192.168[redacted]0/24 (Eleme -CCTV)
192.168.[redacted]0/24 (Onne-CCTV)
192.168.[redacted]0/24 (Onne-LAN)

Case Study Oil & Gas Servicing Company

Project Approach:

To deploy Mikrotik RouterOS with the following functionalities:

- Advanced Firewall Configuration for:
  - Packet Filtering – Deny unproductive traffic
  - Content Filtering – Denying unproductive content during working hours
  - Heavy download policy – To throttle down bandwidth-sapping application.

- Advanced QoS to prioritize bandwidth demand by the LOB application and CCTV above unproductive traffic such as web-browsing .

Tips:

1. Create custom chains for each category of firewall polices. E.g “Allowed Services” for Packet Filtering

2. Connection – State rules that must be applied in the in-built chains

3. Jump from the in-built chains to the custom chains

4. Use address-list for common policies – Exemptions, destination host, source host etc

5. Optimize your policies by placing them in appropriate order

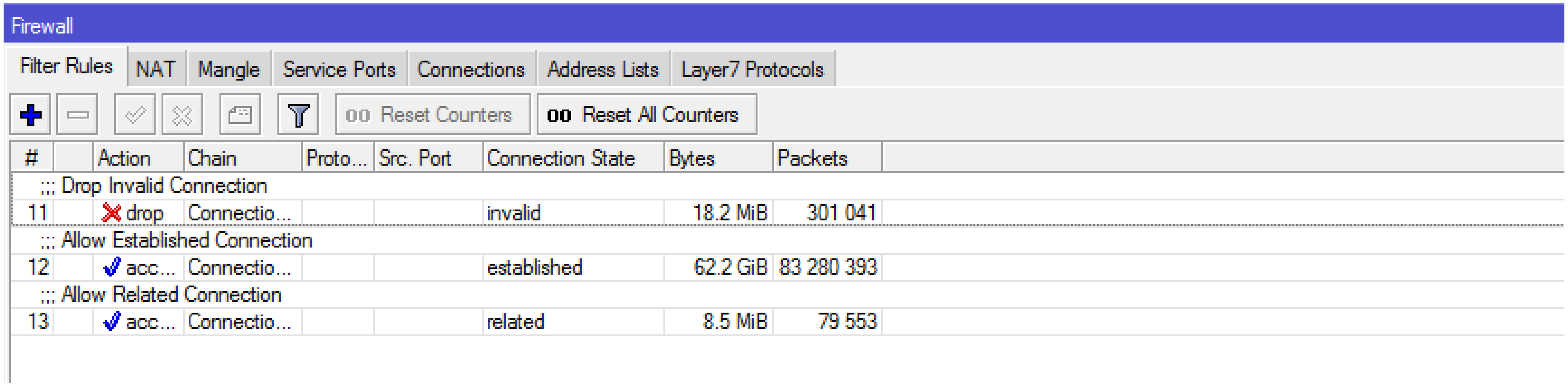
6. Ensure your router is protected from DoS attack & Scan Detection

Advanced Firewall Configuration

Configuration Order:

1. Configure Connection-State rules; Chain = “Connection-State”
2. Configure rules to protect the router; Chain = “Router-Services”
3. Configure rules for packet filtering; Chain = “Allowed Services”
4. Configure rules for content filtering; Chain = “Restricted Sites”
5. Configure rules for heavy downloaders; Chain = “heavy – downloaders”
6. Apply rules in in-built chains with “jump” rules
7. Create Exemption for some hosts.

Adv FW Config Connection-State

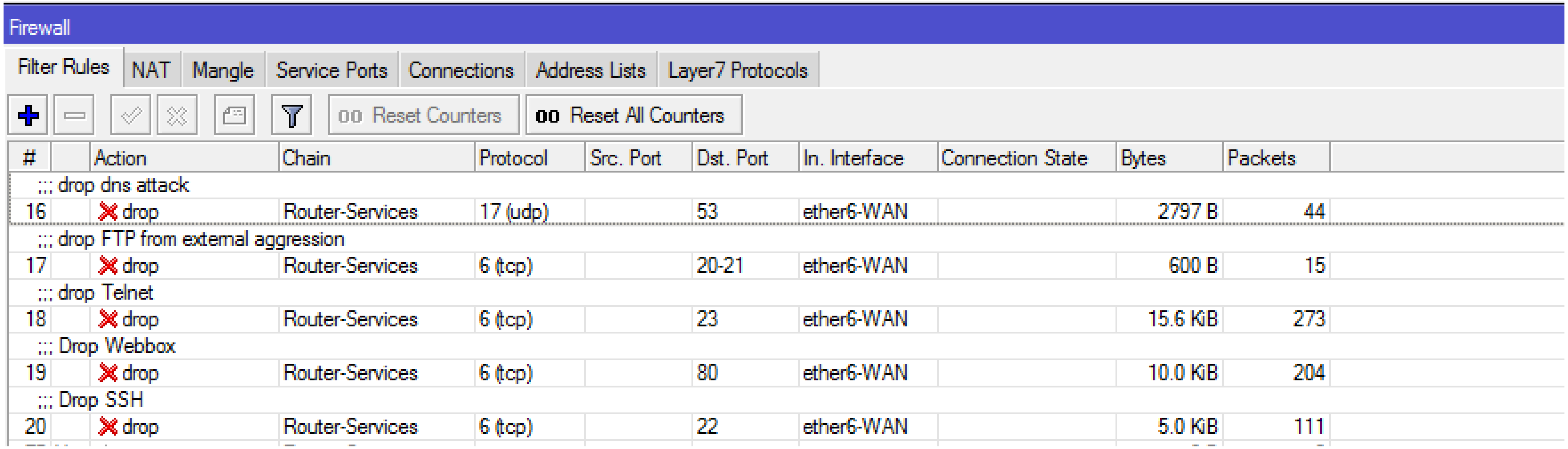


#		Action	Chain	Proto...	Src. Port	Connection State	Bytes	Packets
	;;; Drop Invalid Connection							
11		✗ drop	Connectio...			invalid	18.2 MiB	301 041
	;;; Allow Established Connection							
12		✓ acc...	Connectio...			established	62.2 GiB	83 280 393
	;;; Allow Related Connection							
13		✓ acc...	Connectio...			related	8.5 MiB	79 553

```
/ip firewall filter
add action=drop chain=Connection-State comment="Drop Invalid Connection" \
    connection-state=invalid
add chain=Connection-State comment="Allow Established Connection" \
    connection-state=established
add chain=Connection-State comment="Allow Related Connection" \
    connection-state=related
```

Adv FW Config

Router-Services

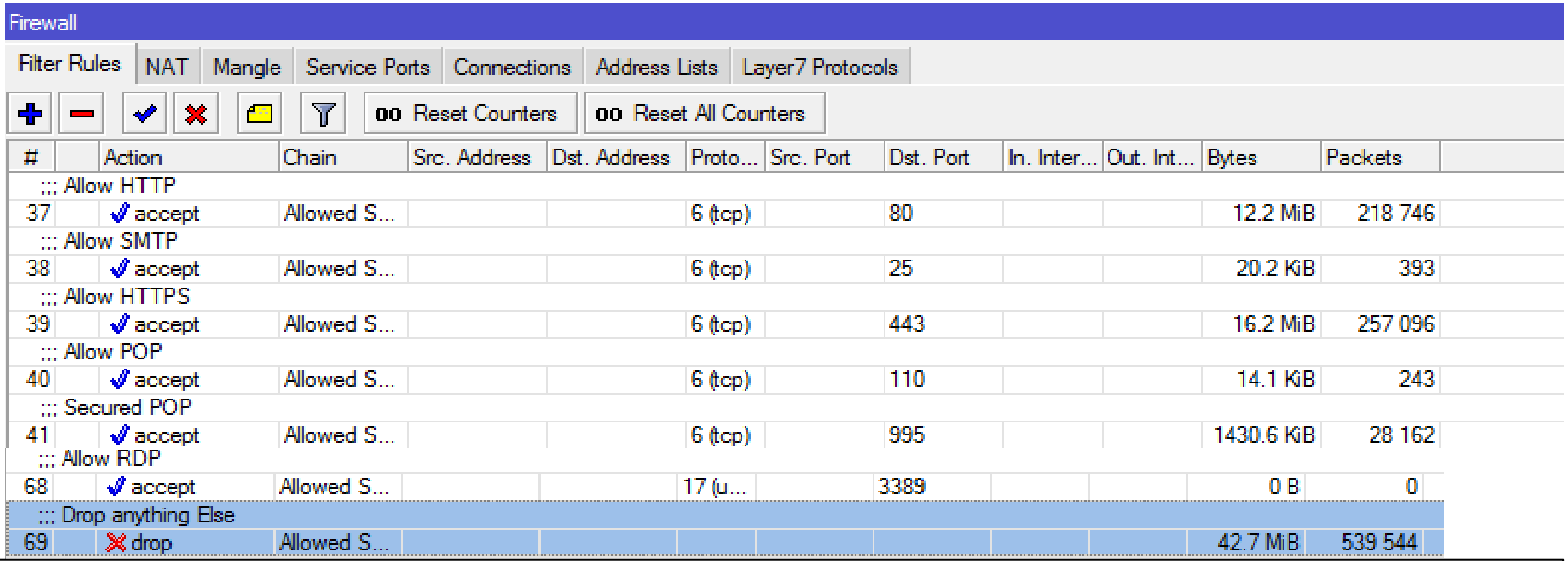


#		Action	Chain	Protocol	Src. Port	Dst. Port	In. Interface	Connection State	Bytes	Packets
;;; drop dns attack										
16		✗ drop	Router-Services	17 (udp)		53	ether6-WAN		2797 B	44
;;; drop FTP from external aggression										
17		✗ drop	Router-Services	6 (tcp)		20-21	ether6-WAN		600 B	15
;;; drop Telnet										
18		✗ drop	Router-Services	6 (tcp)		23	ether6-WAN		15.6 KiB	273
;;; Drop Webbox										
19		✗ drop	Router-Services	6 (tcp)		80	ether6-WAN		10.0 KiB	204
;;; Drop SSH										
20		✗ drop	Router-Services	6 (tcp)		22	ether6-WAN		5.0 KiB	111

```
/ip firewall filter
add action=drop chain=Router-Services comment="drop dns attack" dst-port=53 in-interface=ether6-WAN
protocol=udp

add action=drop chain=Router-Services comment="drop FTP from external aggression" dst-port=20-21
in-interface=ether6-WAN protocol=tcp

add action=drop chain=Router-Services comment="drop Telnet" dst-port=23 in-interface=ether6-WAN protocol=tcp

add action=drop chain=Router-Services comment="Drop Webbox" dst-port=80 in-interface=ether6-WAN
protocol=tcp

add action=drop chain=Router-Services comment="Drop SSH" dst-port=22 in-interface=ether6-WAN protocol=tcp
```

Adv FW Config

Allowed Services



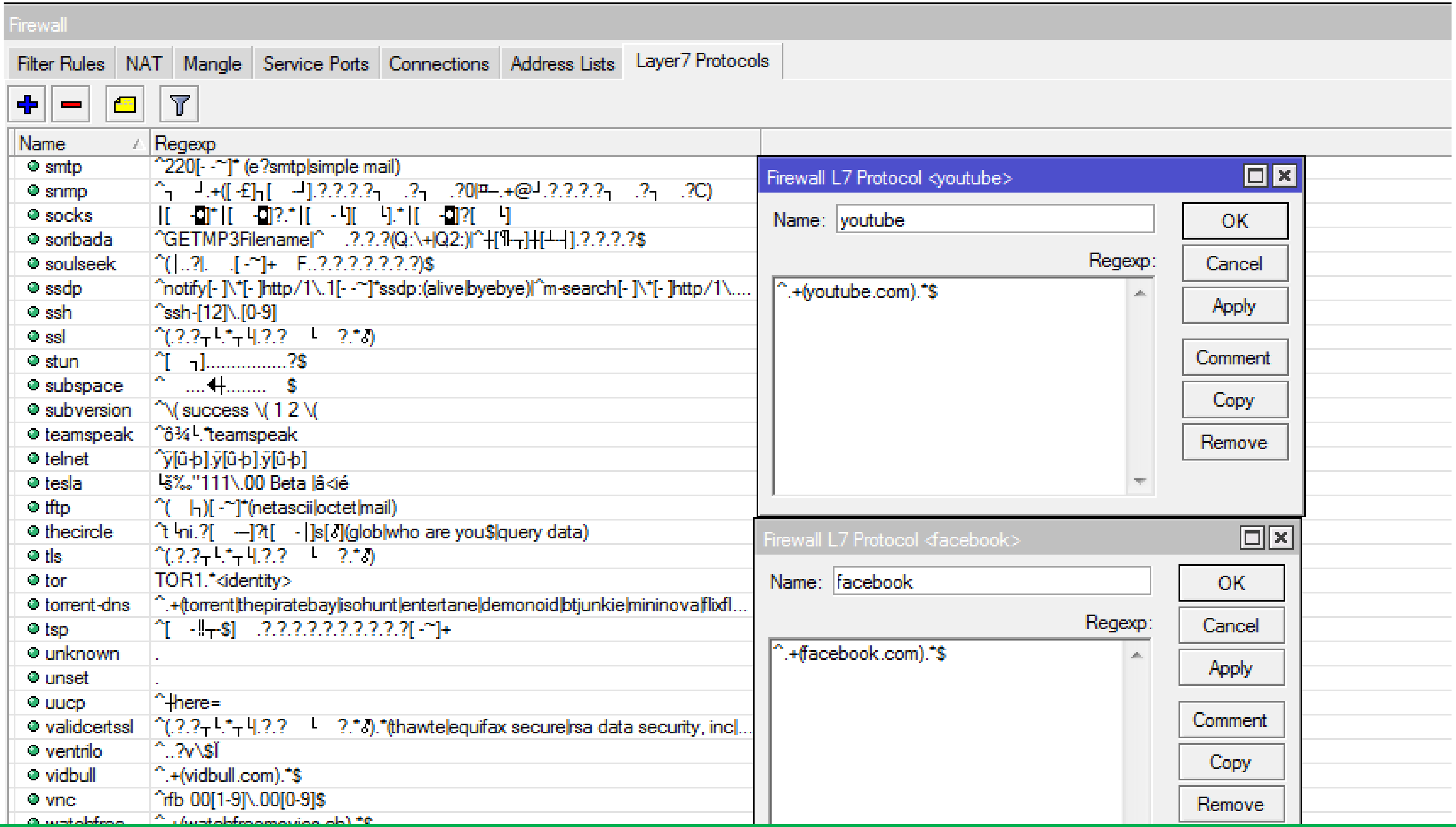
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Allow HTTP											
37	✓ accept	Allowed S...			6 (tcp)		80			12.2 MiB	218 746
;;; Allow SMTP											
38	✓ accept	Allowed S...			6 (tcp)		25			20.2 KiB	393
;;; Allow HTTPS											
39	✓ accept	Allowed S...			6 (tcp)		443			16.2 MiB	257 096
;;; Allow POP											
40	✓ accept	Allowed S...			6 (tcp)		110			14.1 KiB	243
;;; Secured POP											
41	✓ accept	Allowed S...			6 (tcp)		995			1430.6 KiB	28 162
;;; Allow RDP											
68	✓ accept	Allowed S...			17 (u...		3389			0 B	0
;;; Drop anything Else											
69	✗ drop	Allowed S...								42.7 MiB	539 544

```
/ip firewall filter
add chain="Allowed Services" comment="Allow HTTP" dst-port=80 protocol=tcp
add chain="Allowed Services" comment="Allow SMTP" dst-port=25 protocol=tcp
add chain="Allowed Services" comment="Allow HTTPS" dst-port=443 protocol=tcp
add chain="Allowed Services" comment="Allow POP" dst-port=110 protocol=tcp
add chain="Allowed Services" comment="Secured POP" dst-port=995 protocol=tcp
add chain="Allowed Services" comment="Allow TCP/DNS" dst-port=53 protocol=tcp
add action=drop chain="Allowed Services" comment="Drop anything Else"
```

Adv FW Config

Restricted Services

This requires combination of L7 Protocols and Filter Rules



Name	Regexp
smtp	^220[- -~]* (e?smtp|simple mail)
snmp	^┐ ┘.+([-£]┐[┘].?.?.?.?┐ .?┐ .?0|¤─.+@┘.?.?.?.?┐ .?┐ .?C)
socks	|[-◘]*|[-◘]?.*|[-╝][╝].*|[-◘]?[╝]
soribada	^GETMP3Filename|^ .?.?.?(Q:\\+|Q2:)|^┼[¶┬]┼[┴┤].?.?.?.?$
soulseek	^(|..?|. .[-~]+ F..?.?.?.?.?.?.?.?)$
ssdp	^notify[-]*[-]http/1\\.1[- -~]*ssdp:(alive|byebye)|^m-search[-]*[-]http/1\\....
ssh	^ssh-[12]\\.[0-9]
ssl	^(.?.?┬└.*┬╣.?.? └ ?.*♂)
stun	^[┐]...............?$
subspace	^ ....◄┼........ $
subversion	^\\(success \\(1 2 \\(
teamspeak	^ô¾└.*teamspeak
telnet	^ÿ[û-þ].ÿ[û-þ].ÿ[û-þ]
tesla	╘š‰"111\\.00 Beta |â<ié
tftp	^(┤)[-~]*(netascii|octet|mail)
thecircle	^t └ni.?[—]?t[-|]s[♂](glob|who are you$|query data)
tls	^(.?.?┬└.*┬╣.?.? └ ?.*♂)
tor	TOR1.*<identity>
torrent-dns	^.+(torrent|thepiratebay|isohunt|entertane|demonoid|btjunkie|mininova|flixfl...
tsp	^[-‼┬$] .?.?.?.?.?.?.?.?.?.?[-~]+
unknown	.
unset	.
uucp	^┼here=
validcertssl	^(.?.?┬└.*┬╣.?.? └ ?.*♂).*(thawte|equifax secure|rsa data security, inc|...
ventrilo	^..?v\\$Ï
vidbull	^.+(vidbull.com).*$
vnc	^rfb 00[1-9]\\.00[0-9]$
watchfree	^.+(watchfreemovies.ch).*$

Firewall L7 Protocol <youtube>

Name: youtube

Regexp:

```
^.+(youtube.com).*$
```

Firewall L7 Protocol <facebook>

Name: facebook

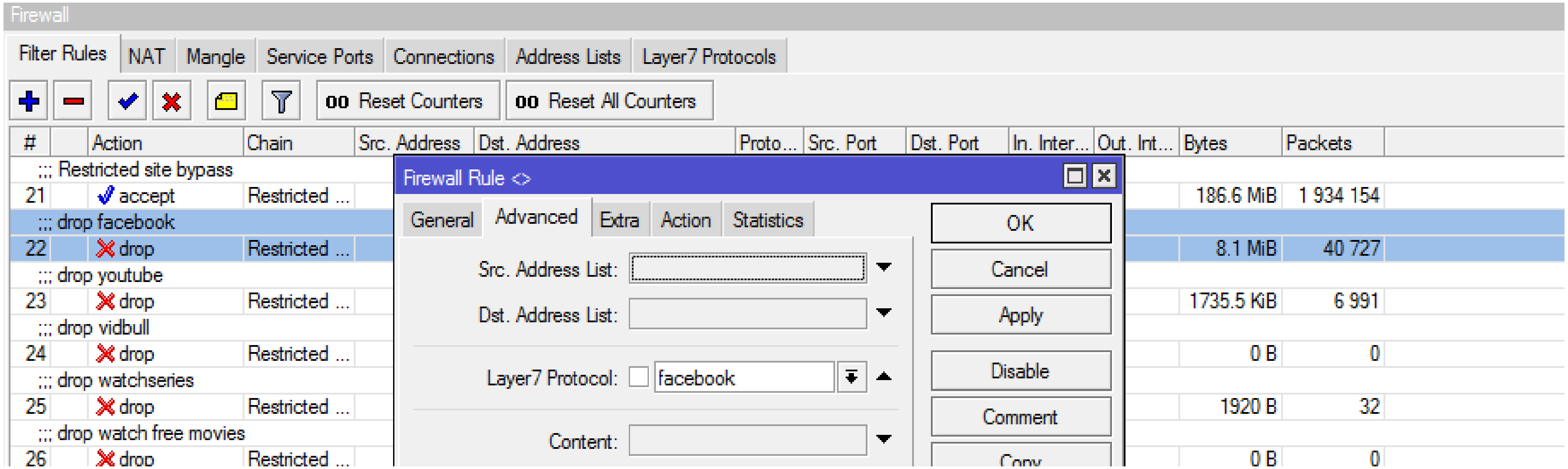
Regexp:

```
^.+(facebook.com).*$
```

Adv FW Config

Restricted Services

This requires combination of L7 Protocols and Filter Rules



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: Restricted site bypass											
21	✓ accept	Restricted ...								186.6 MiB	1 934 154
::: drop facebook											
22	✗ drop	Restricted ...								8.1 MiB	40 727
::: drop youtube											
23	✗ drop	Restricted ...								1735.5 KiB	6 991
::: drop vidbull											
24	✗ drop	Restricted ...								0 B	0
::: drop watchseries											
25	✗ drop	Restricted ...								1920 B	32
::: drop watch free movies											
26	✗ drop	Restricted ...								0 B	0

Src. Address List:

Dst. Address List:

Layer7 Protocol: ☐ facebook

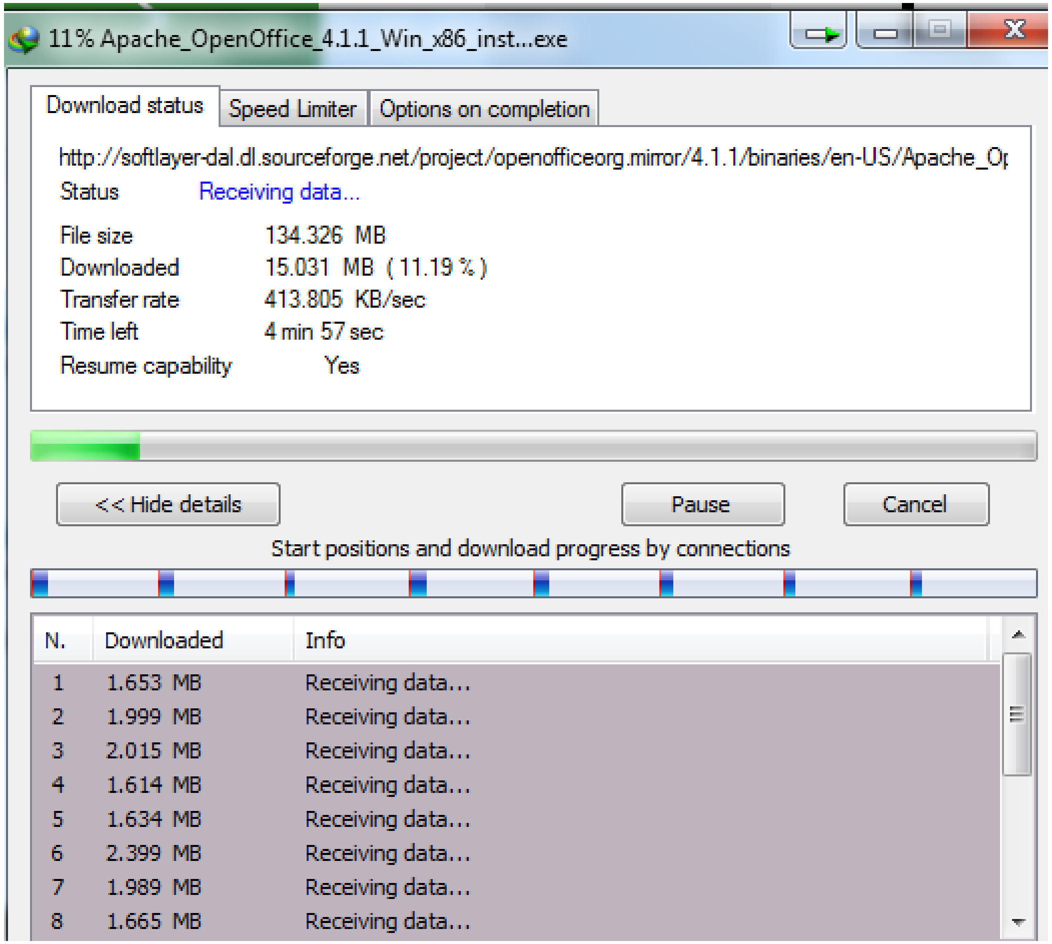
Content:

```
/ip firewall filter
add action=drop chain="Restricted sites" comment="drop facebook“
 layer7 protocol=facebook
add action=drop chain="Restricted sites" comment="drop youtube" \
   layer7-protocol=youtube
add action=drop chain="Restricted sites" comment="drop watchseries" \
   layer7-protocol=watchseries
add action=drop chain="Restricted sites" comment="drop watch free movies" \
   layer7-protocol="watchfree movies"
```

Adv FW Config heavy-downloaders

Heavy downloaders are bandwidth-hungry applications and devices. These include

- Smart devices
- Download Accelerator Program (DAP)
- Internet Download Manager (IDM)
- Orbit
- Video-Streaming applications



http://softlayer-dal.dl.sourceforge.net/project/openofficeorg.mirror/4.1.1/binaries/en-US/Apache_Op

Status	Receiving data...
File size	134.326 MB
Downloaded	15.031 MB (11.19 %)
Transfer rate	413.805 KB/sec
Time left	4 min 57 sec
Resume capability	Yes

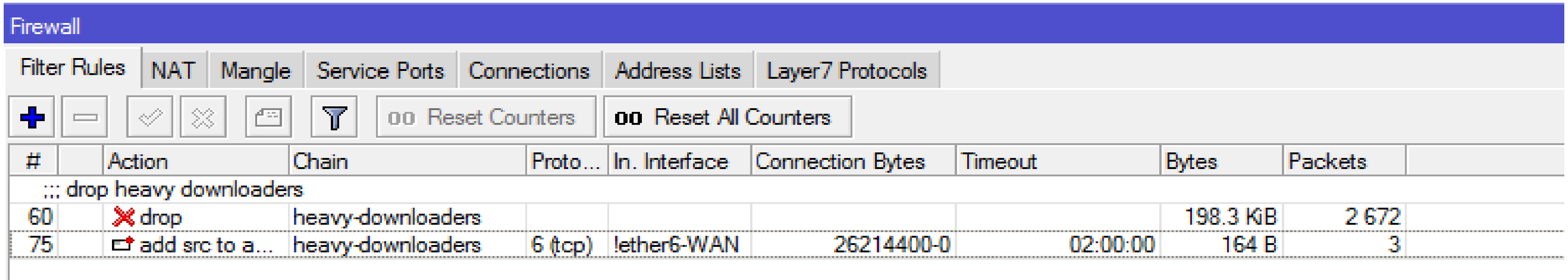
Start positions and download progress by connections

N.	Downloaded	Info
1	1.653 MB	Receiving data...
2	1.999 MB	Receiving data...
3	2.015 MB	Receiving data...
4	1.614 MB	Receiving data...
5	1.634 MB	Receiving data...
6	2.399 MB	Receiving data...
7	1.989 MB	Receiving data...
8	1.665 MB	Receiving data...

Adv FW Config

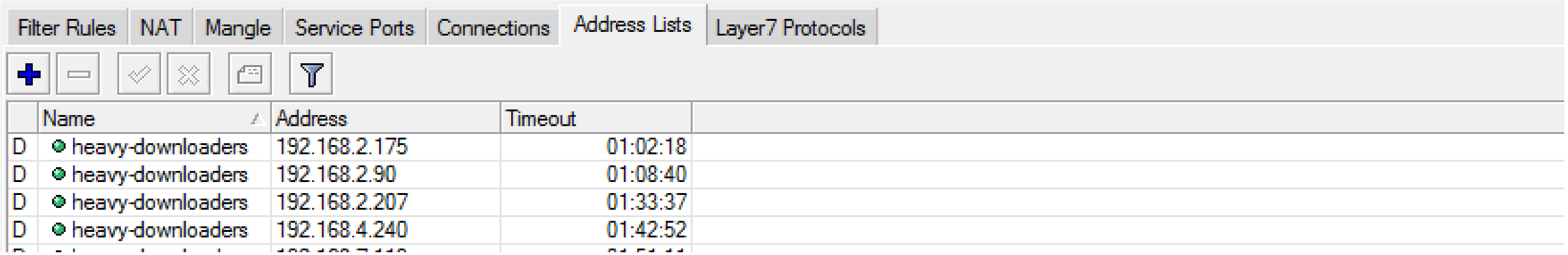
heavy-downloaders

Heavy-downloaders’ policy violators are denied access to internet for 2 hours.



#		Action	Chain	Proto...	In. Interface	Connection Bytes	Timeout	Bytes	Packets
;;; drop heavy downloaders									
60		drop	heavy-downloaders					198.3 KiB	2 672
75		add src to a...	heavy-downloaders	6 (tcp)	!ether6-WAN	26214400-0	02:00:00	164 B	3

```
/ip firewall filter
add action=drop chain=heavy-downloaders comment="drop heavy downloaders" dst-address-type="" src-address-list=heavy-downloader

add action=add-src-to-address-list address-list=heavy-downloaders address-list-timeout=2h chain=heavy-downloaders connection-bytes=26214400-0 dst-address-type="" in-interface=!ether6-WAN protocol=tcp
```



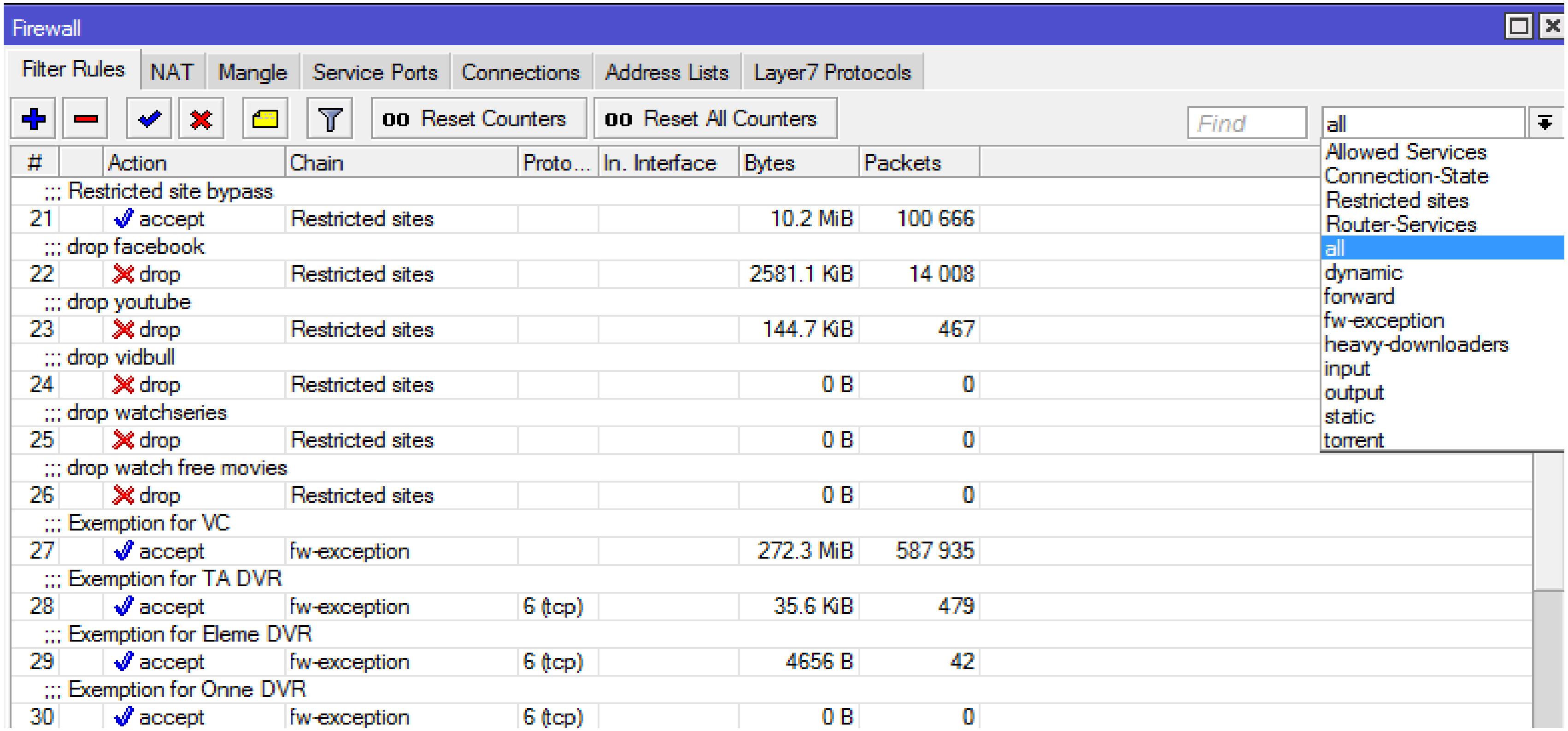
	Name	Address	Timeout
D	heavy-downloaders	192.168.2.175	01:02:18
D	heavy-downloaders	192.168.2.90	01:08:40
D	heavy-downloaders	192.168.2.207	01:33:37
D	heavy-downloaders	192.168.4.240	01:42:52

Adv FW Config

Connecting the dots

Custom Chains Vs. in-built Chains

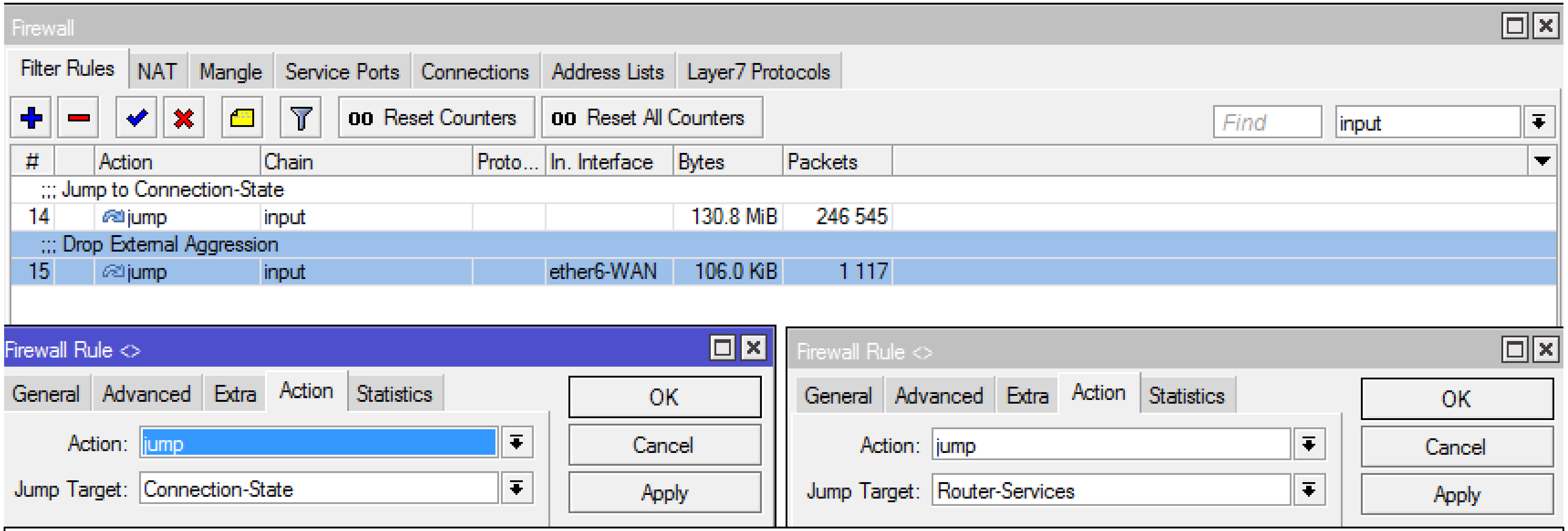
Connecting customs chain to in-built chains using “jump” action



#	Action	Chain	Proto...	In. Interface	Bytes	Packets
;;; Restricted site bypass						
21	✓ accept	Restricted sites			10.2 MiB	100 666
;;; drop facebook						
22	✗ drop	Restricted sites			2581.1 KiB	14 008
;;; drop youtube						
23	✗ drop	Restricted sites			144.7 KiB	467
;;; drop vidbull						
24	✗ drop	Restricted sites			0 B	0
;;; drop watchseries						
25	✗ drop	Restricted sites			0 B	0
;;; drop watch free movies						
26	✗ drop	Restricted sites			0 B	0
;;; Exemption for VC						
27	✓ accept	fw-exception			272.3 MiB	587 935
;;; Exemption for TA DVR						
28	✓ accept	fw-exception	6 (tcp)		35.6 KiB	479
;;; Exemption for Eleme DVR						
29	✓ accept	fw-exception	6 (tcp)		4656 B	42
;;; Exemption for Onne DVR						
30	✓ accept	fw-exception	6 (tcp)		0 B	0

Adv FW Config — Connecting the dots

Input Chain - Jump to “Connection-State” and “Router Services”



input

#	Action	Chain	Proto...	In. Interface	Bytes	Packets
::: Jump to Connection-State						
14	jump	input			130.8 MiB	246 545
::: Drop External Aggression						
15	jump	input		ether6-WAN	106.0 KiB	1 117

Action: jump

Jump Target: Connection-State

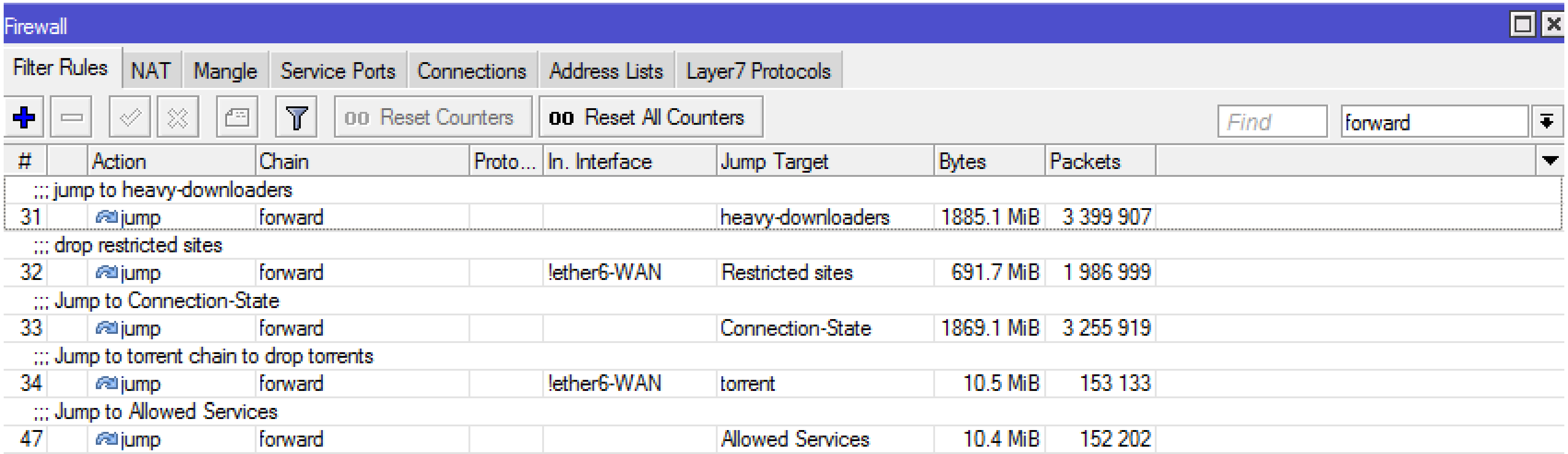
Action: jump

Jump Target: Router-Services

```
/ip firewall filter

add action=jump chain=input comment="Jump to Connection-State" jump-target=Connection-State

add action=jump chain=input comment="Drop External Aggression" in-interface=ether6-WAN jump-target=Router-Services
```

Adv FW Config Connecting the dots

Forward Chain - Jump to “heavy-downloaders”, “Restricted Sites”, “Connection-State”, “Allowed Services”



#	Action	Chain	Proto...	In. Interface	Jump Target	Bytes	Packets
;;; jump to heavy-downloaders							
31	jump	forward			heavy-downloaders	1885.1 MiB	3 399 907
;;; drop restricted sites							
32	jump	forward		!ether6-WAN	Restricted sites	691.7 MiB	1 986 999
;;; Jump to Connection-State							
33	jump	forward			Connection-State	1869.1 MiB	3 255 919
;;; Jump to torrent chain to drop torrents							
34	jump	forward		!ether6-WAN	torrent	10.5 MiB	153 133
;;; Jump to Allowed Services							
47	jump	forward			Allowed Services	10.4 MiB	152 202

```
/ip firewall filter
add action=jump chain=forward comment="jump to heavy-downloaders" jump-target=heavy-downloaders
add action=jump chain=forward comment="drop restricted sites" in-interface=!ether6-WAN jump-target="Restricted sites"
add action=jump chain=forward comment="Jump to Connection-State" jump-target=Connection-State
add action=jump chain=input comment="Jump to Connection-State" jump-target=Connection-State
add action=jump chain=input comment="Drop External Aggression" in-interface=ether6-WAN jump-target=Router-Services
```

Adv FW Config

Exemptions

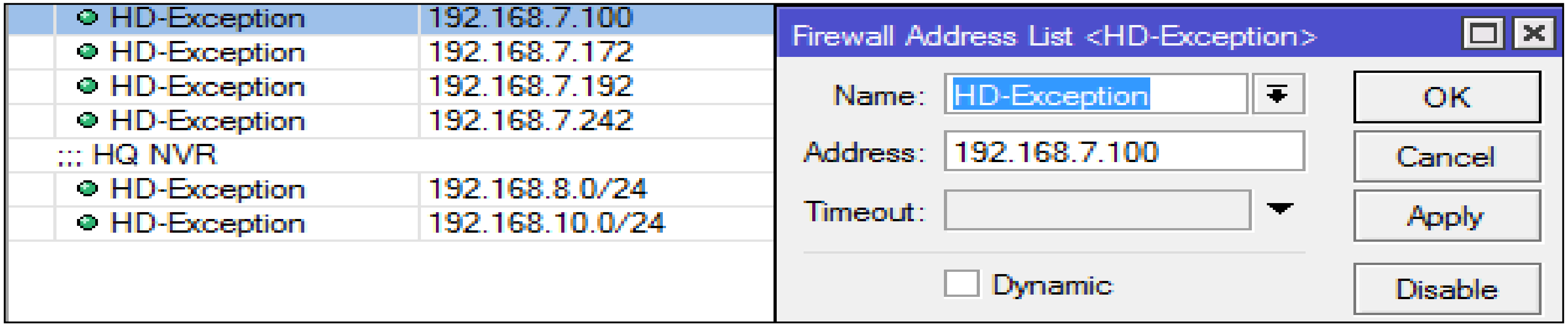
Exemptions can be applied on the rules in each chain such as:

- Heavy download Chain
- Restricted Sites Chain
- Allowed Services Chain
- Forward Chain

With combination of address-list and filter rules, exemption can be applied to host with common policy.

Exemptions

Heavy download



● HD-Exception	192.168.7.100
● HD-Exception	192.168.7.172
● HD-Exception	192.168.7.192
● HD-Exception	192.168.7.242
;;; HQ NVR	
● HD-Exception	192.168.8.0/24
● HD-Exception	192.168.10.0/24

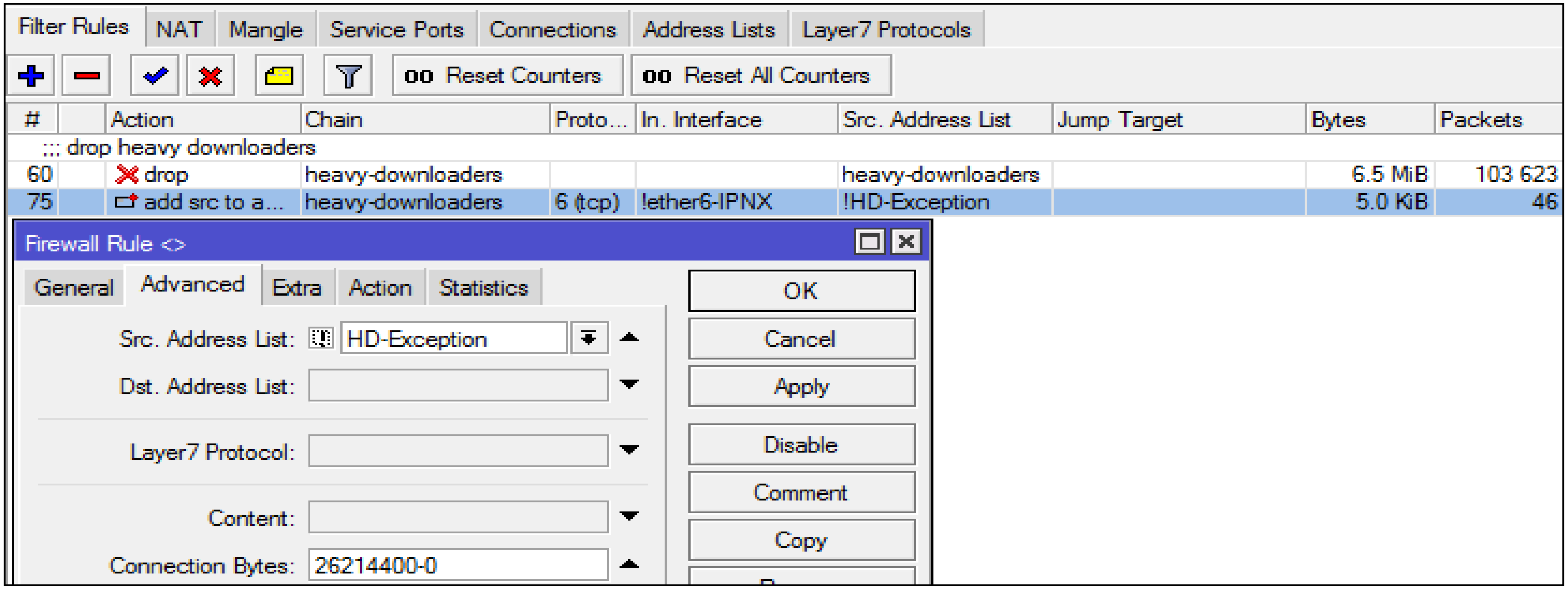
Firewall Address List <HD-Exception>

Name: HD-Exception

Address: 192.168.7.100

Timeout:

□ Dynamic



#		Action	Chain	Proto...	In. Interface	Src. Address List	Jump Target	Bytes	Packets
;;; drop heavy downloaders									
60		✗ drop	heavy-downloaders			heavy-downloaders		6.5 MiB	103 623
75		add src to a...	heavy-downloaders	6 (tcp)	!ether6-IPNX	!HD-Exception		5.0 KiB	46

Firewall Rule <>

Src. Address List: ! HD-Exception

Dst. Address List:

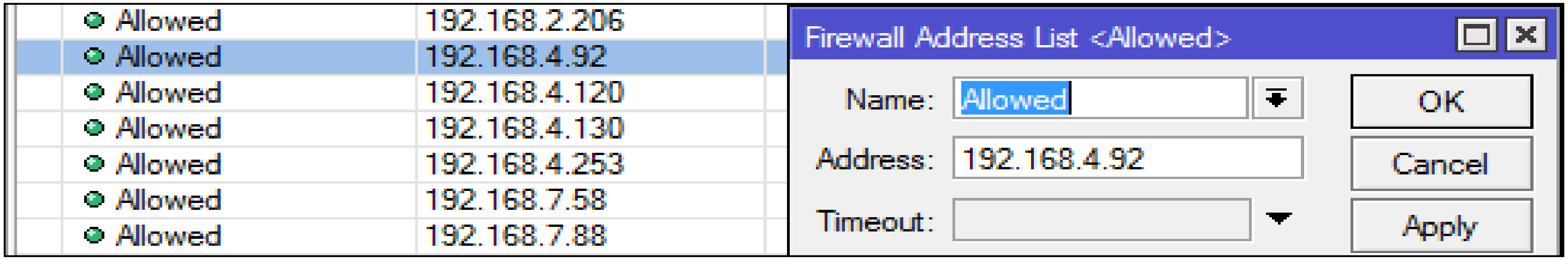
Layer7 Protocol:

Content:

Connection Bytes: 26214400-0

Exemptions

Restricted Sites



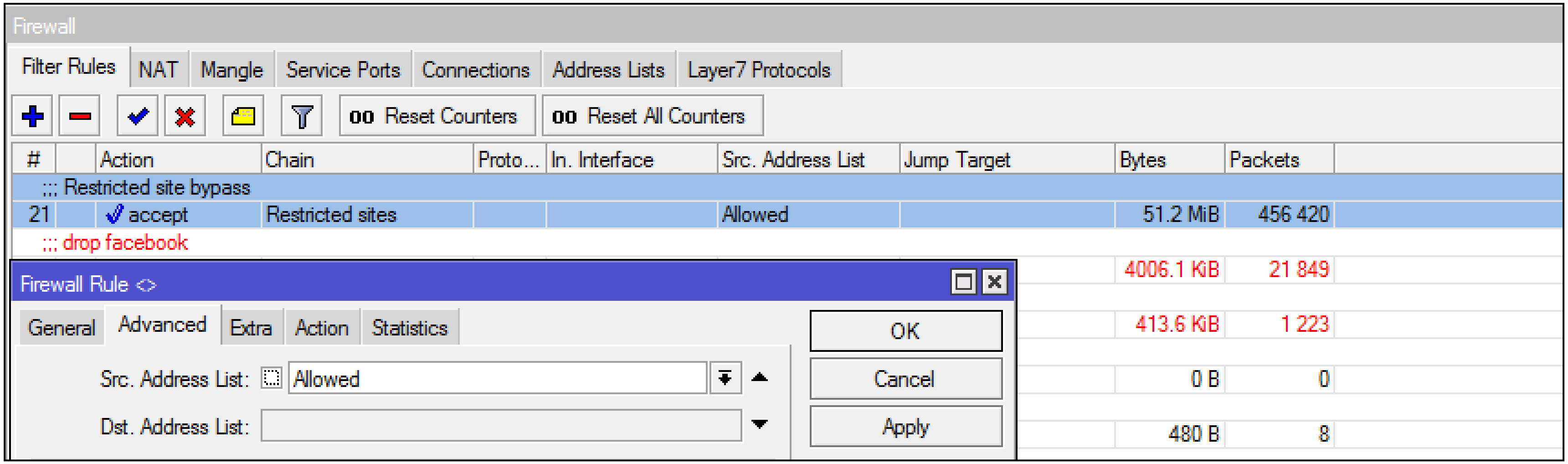
Allowed	192.168.2.206
Allowed	192.168.4.92
Allowed	192.168.4.120
Allowed	192.168.4.130
Allowed	192.168.4.253
Allowed	192.168.7.58
Allowed	192.168.7.88

Firewall Address List <Allowed>

Name: Allowed

Address: 192.168.4.92

Timeout:



#		Action	Chain	Proto...	In. Interface	Src. Address List	Jump Target	Bytes	Packets
;;; Restricted site bypass									
21		✓ accept	Restricted sites			Allowed		51.2 MiB	456 420
;;; drop facebook									
								4006.1 KiB	21 849
								413.6 KiB	1 223
								0 B	0
								480 B	8

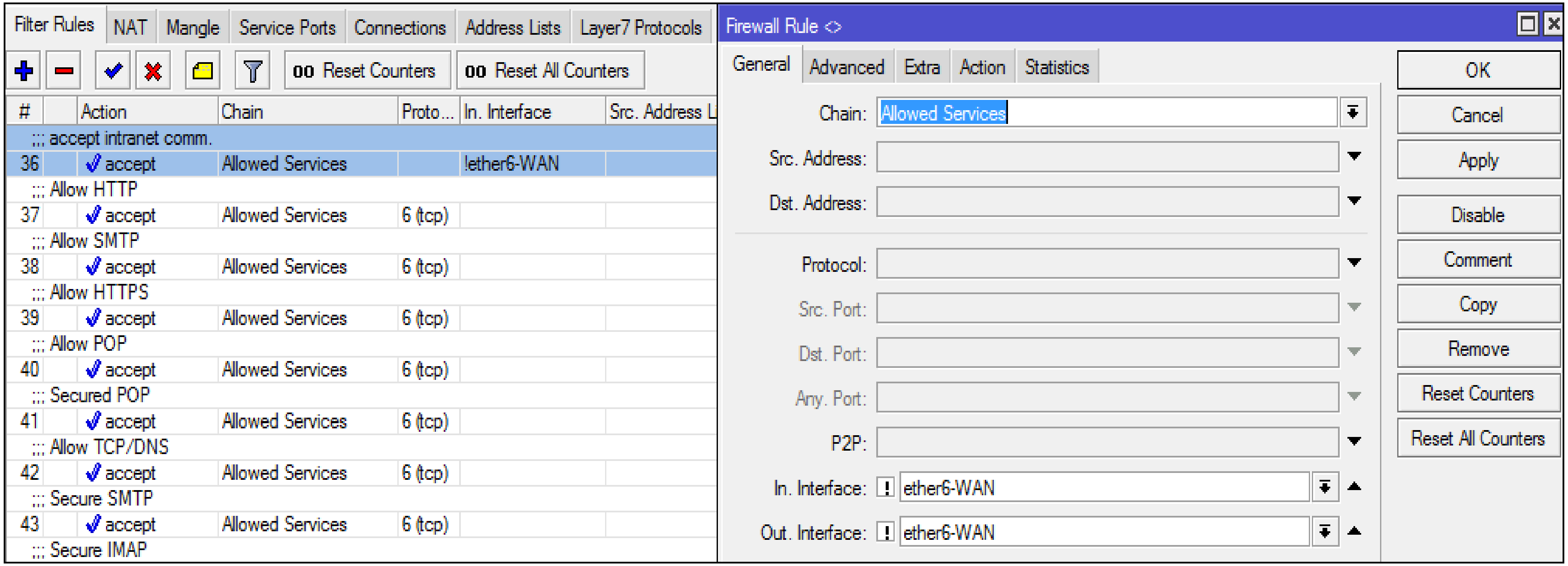
Firewall Rule <>

Src. Address List: □ Allowed

Dst. Address List:

Exemptions

Allowed Services



#		Action	Chain	Proto...	In. Interface	Src. Address L
;;; accept intranet comm.						
36		✓ accept	Allowed Services		!ether6-WAN	
;;; Allow HTTP						
37		✓ accept	Allowed Services	6 (tcp)		
;;; Allow SMTP						
38		✓ accept	Allowed Services	6 (tcp)		
;;; Allow HTTPS						
39		✓ accept	Allowed Services	6 (tcp)		
;;; Allow POP						
40		✓ accept	Allowed Services	6 (tcp)		
;;; Secured POP						
41		✓ accept	Allowed Services	6 (tcp)		
;;; Allow TCP/DNS						
42		✓ accept	Allowed Services	6 (tcp)		
;;; Secure SMTP						
43		✓ accept	Allowed Services	6 (tcp)		
;;; Secure IMAP						

Chain: Allowed Services
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface: ! ether6-WAN
Out. Interface: ! ether6-WAN

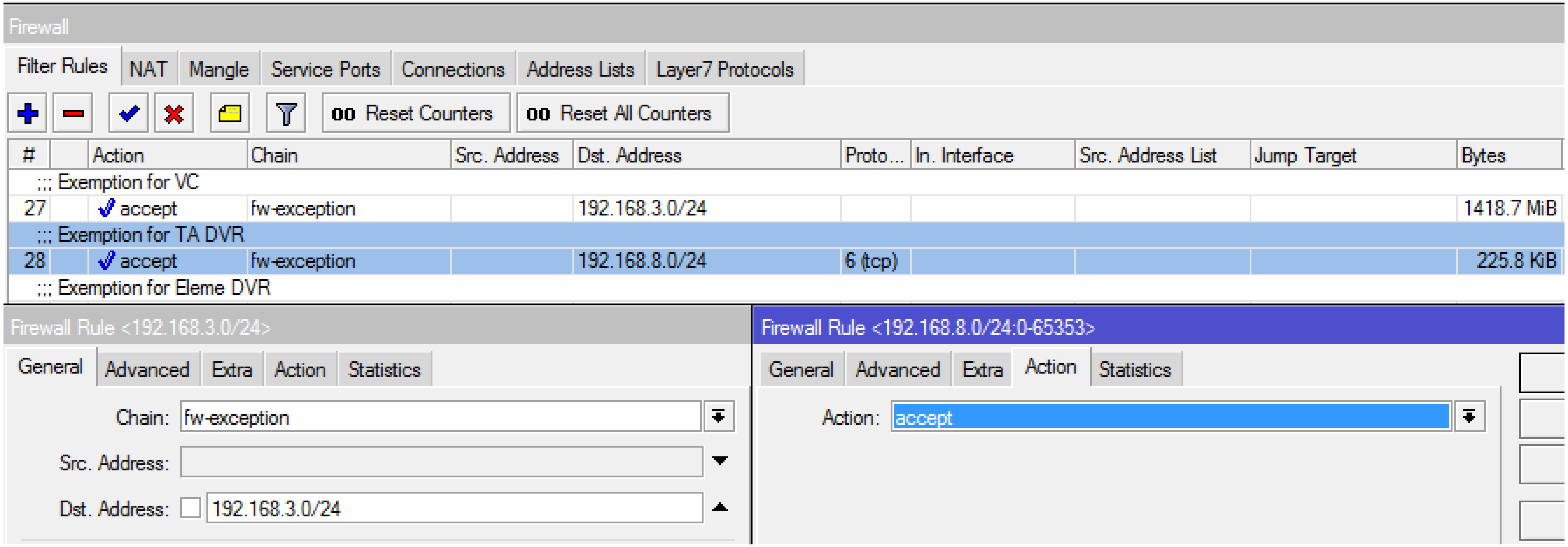
Interface-based exemption is applied on all Local Interfaces except WAN Interface.
The exemption rule is placed above all rules .

Exemptions

Forward Chain

Create a custom chain; “fw-exception”

All the subnet of Server farm and CCTV DVR that require exemption



#		Action	Chain	Src. Address	Dst. Address	Proto...	In. Interface	Src. Address List	Jump Target	Bytes
;;; Exemption for VC										
27		✓ accept	fw-exception		192.168.3.0/24					1418.7 MiB
;;; Exemption for TA DVR										
28		✓ accept	fw-exception		192.168.8.0/24	6 (tcp)				225.8 KiB
;;; Exemption for Eleme DVR										

Firewall Rule <192.168.3.0/24>

Chain: fw-exception

Src. Address:

Dst. Address: □ 192.168.3.0/24

Firewall Rule <192.168.8.0/24:0-65353>

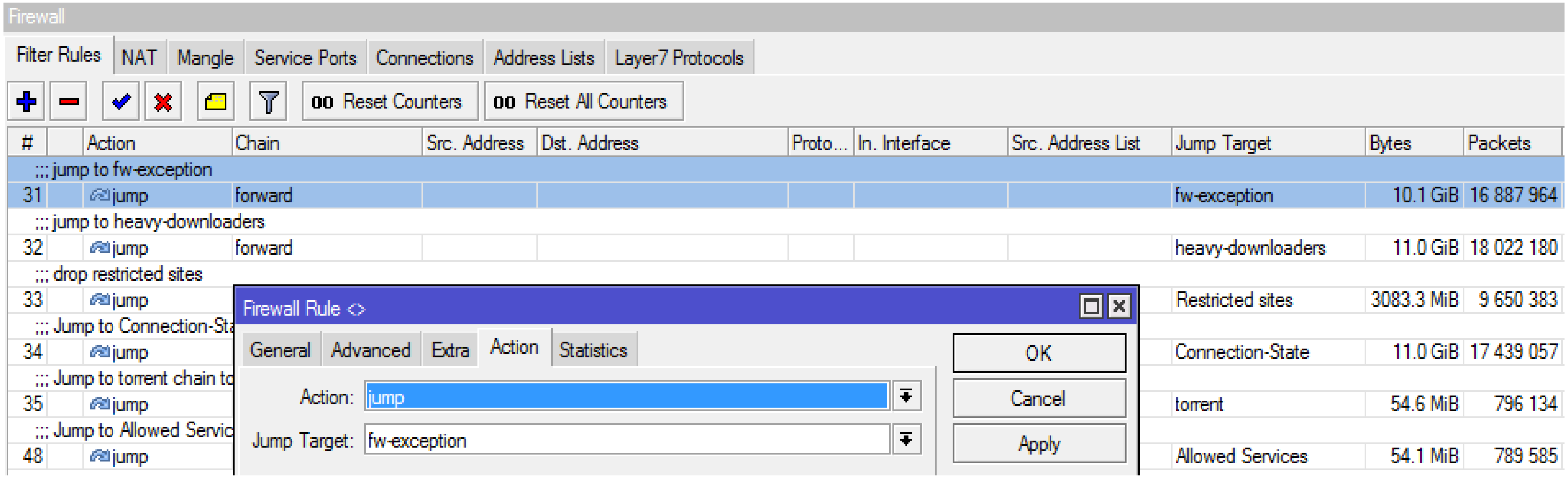
Action: accept

```
/ip firewall filter
add chain=fw-exception comment="Exemption for VC" dst-address=192.168.3.0/24
add chain=fw-exception comment="Exemption for TA DVR" dst-address=192.168.8.0/24
dst-port=0-65353 protocol=tcp
```

Exemptions

Forward Chain

Jump to “fw-exception” chain from the forward chain
Place the jump rules above all rules



#		Action	Chain	Src. Address	Dst. Address	Proto...	In. Interface	Src. Address List	Jump Target	Bytes	Packets
;;; jump to fw-exception											
31		jump	forward						fw-exception	10.1 GiB	16 887 964
;;; jump to heavy-downloaders											
32		jump	forward						heavy-downloaders	11.0 GiB	18 022 180
;;; drop restricted sites											
33		jump							Restricted sites	3083.3 MiB	9 650 383
;;; Jump to Connection-Sta											
34		jump							Connection-State	11.0 GiB	17 439 057
;;; Jump to torrent chain to											
35		jump							torrent	54.6 MiB	796 134
;;; Jump to Allowed Servic											
48		jump							Allowed Services	54.1 MiB	789 585

Action: jump

Jump Target: fw-exception

Quality of Service

Quality of Service

Simple Queue can be used for:

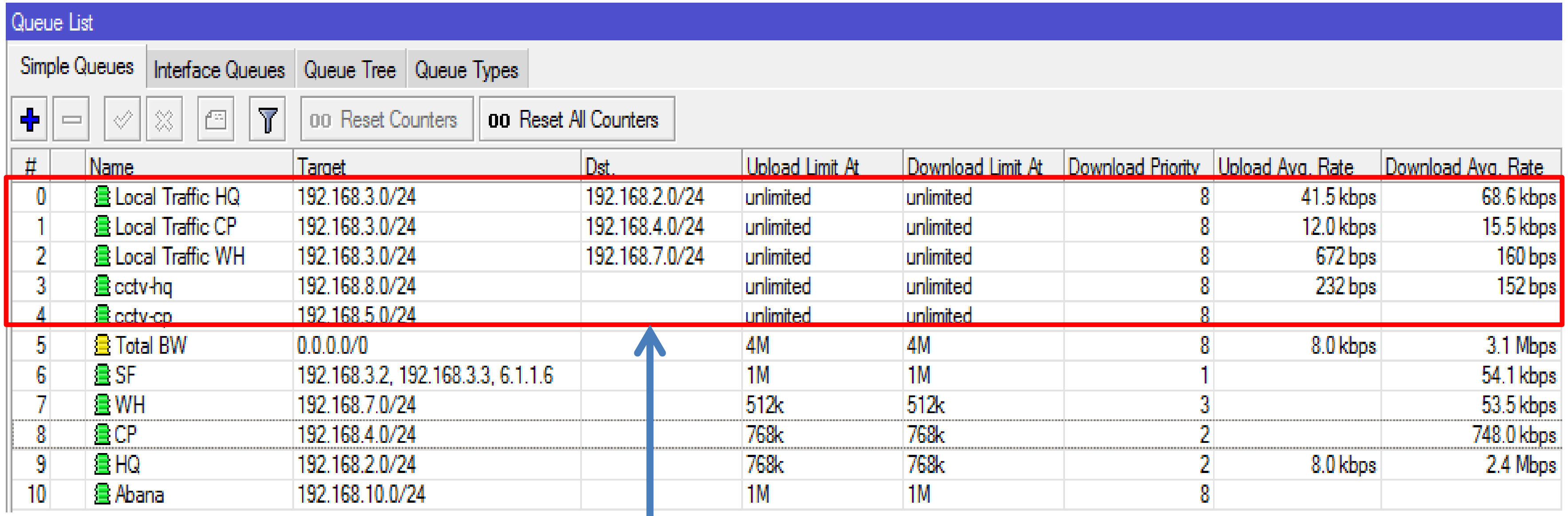
- Speed Limit
- Quality of Service

Speed Limit is the apportionment of interface bandwidth to target host

QoS means guarantee of bandwidth for specify application and hosts.
QoS uses mechanism such as HTB, Priority, MIR and CIR
Priority sets the precedence – order of importance

Speed Limit

Simple Queue can be used for:

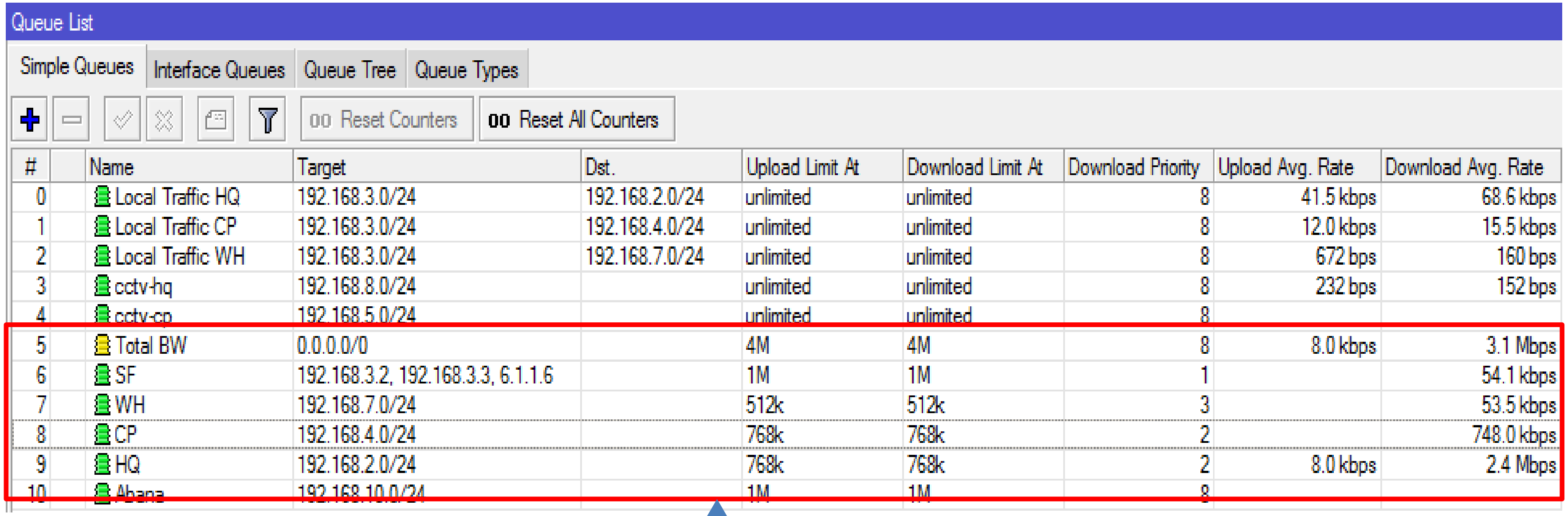


Queue List

#		Name	Target	Dst.	Upload Limit At	Download Limit At	Download Priority	Upload Avg. Rate	Download Avg. Rate
0		Local Traffic HQ	192.168.3.0/24	192.168.2.0/24	unlimited	unlimited	8	41.5 kbps	68.6 kbps
1		Local Traffic CP	192.168.3.0/24	192.168.4.0/24	unlimited	unlimited	8	12.0 kbps	15.5 kbps
2		Local Traffic WH	192.168.3.0/24	192.168.7.0/24	unlimited	unlimited	8	672 bps	160 bps
3		cctv-hq	192.168.8.0/24		unlimited	unlimited	8	232 bps	152 bps
4		cctv-cp	192.168.5.0/24		unlimited	unlimited	8		
5		Total BW	0.0.0.0/0		4M	4M	8	8.0 kbps	3.1 Mbps
6		SF	192.168.3.2, 192.168.3.3, 6.1.1.6		1M	1M	1		54.1 kbps
7		WH	192.168.7.0/24		512k	512k	3		53.5 kbps
8		CP	192.168.4.0/24		768k	768k	2		748.0 kbps
9		HQ	192.168.2.0/24		768k	768k	2	8.0 kbps	2.4 Mbps
10		Abana	192.168.10.0/24		1M	1M	8		

Unlimited Speed Limit for the Local traffic
(Server Farm to the Remote and the HQ LAN_

Simple Queue can be used for:



#		Name	Target	Dst.	Upload Limit At	Download Limit At	Download Priority	Upload Avg. Rate	Download Avg. Rate
0		Local Traffic HQ	192.168.3.0/24	192.168.2.0/24	unlimited	unlimited	8	41.5 kbps	68.6 kbps
1		Local Traffic CP	192.168.3.0/24	192.168.4.0/24	unlimited	unlimited	8	12.0 kbps	15.5 kbps
2		Local Traffic WH	192.168.3.0/24	192.168.7.0/24	unlimited	unlimited	8	672 bps	160 bps
3		cctv-hq	192.168.8.0/24		unlimited	unlimited	8	232 bps	152 bps
4		cctv-cp	192.168.5.0/24		unlimited	unlimited	8		
5		Total BW	0.0.0.0/0		4M	4M	8	8.0 kbps	3.1 Mbps
6		SF	192.168.3.2, 192.168.3.3, 6.1.1.6		1M	1M	1		54.1 kbps
7		WH	192.168.7.0/24		512k	512k	3		53.5 kbps
8		CP	192.168.4.0/24		768k	768k	2		748.0 kbps
9		HQ	192.168.2.0/24		768k	768k	2	8.0 kbps	2.4 Mbps
10		Abana	192.168.10.0/24		1M	1M	8		

QoS Setup to guarantee Internet Bandwidth for LOB Application, HQ and the Remote

Questions ?

Contact

W : www.trisatcom.net

E : abiola@trisatcom.net , holler4eva@gmail.com

Ph: +2348182556717

Contact Address: 5 Okorodo Street, D-Line (Behind NITEL Exchange – Garrison) Port Harcourt , Rivers State.

Skype: habholler1