KRAUSS INTERNATIONAL

CALL FOR SALES: 9717387778 / 9910416231 EMAIL: SALES@KC-INDIA.COM

Firewall for ISP/TSP/OSPs

PRESENTED BY MANKOMAL SINGH (KRAUSS INTERNATIONAL)

About the speaker

- Has been a student(yes I still learn from you also) of networking for past 16 years
- 16 years of experience in IT & Communication Industry
- Is certified trainer of Mikrotik (MTCNA, MTCWE)
- Is certified trainer for wireless and networking technologies
- Designed and implemented wide array of networks for corporates and ISPs
- Running our own ISP in Punjab, Maharashtra, Tamil Nadu

Objectives

- Understanding some of the problems faced with Service Providers in India
  - Mikrotik's Firewall basic understanding of chains
  - Implementing some basic firewalls
  - Understanding DDoS
  - Some basic implementation of DDoS
  - BCP38
  - Understanding Amplification Attack

Downloading this presentation

- This will be available at http://mum.mikrotik.com under archives
- Or you can send email to us we will forward to you

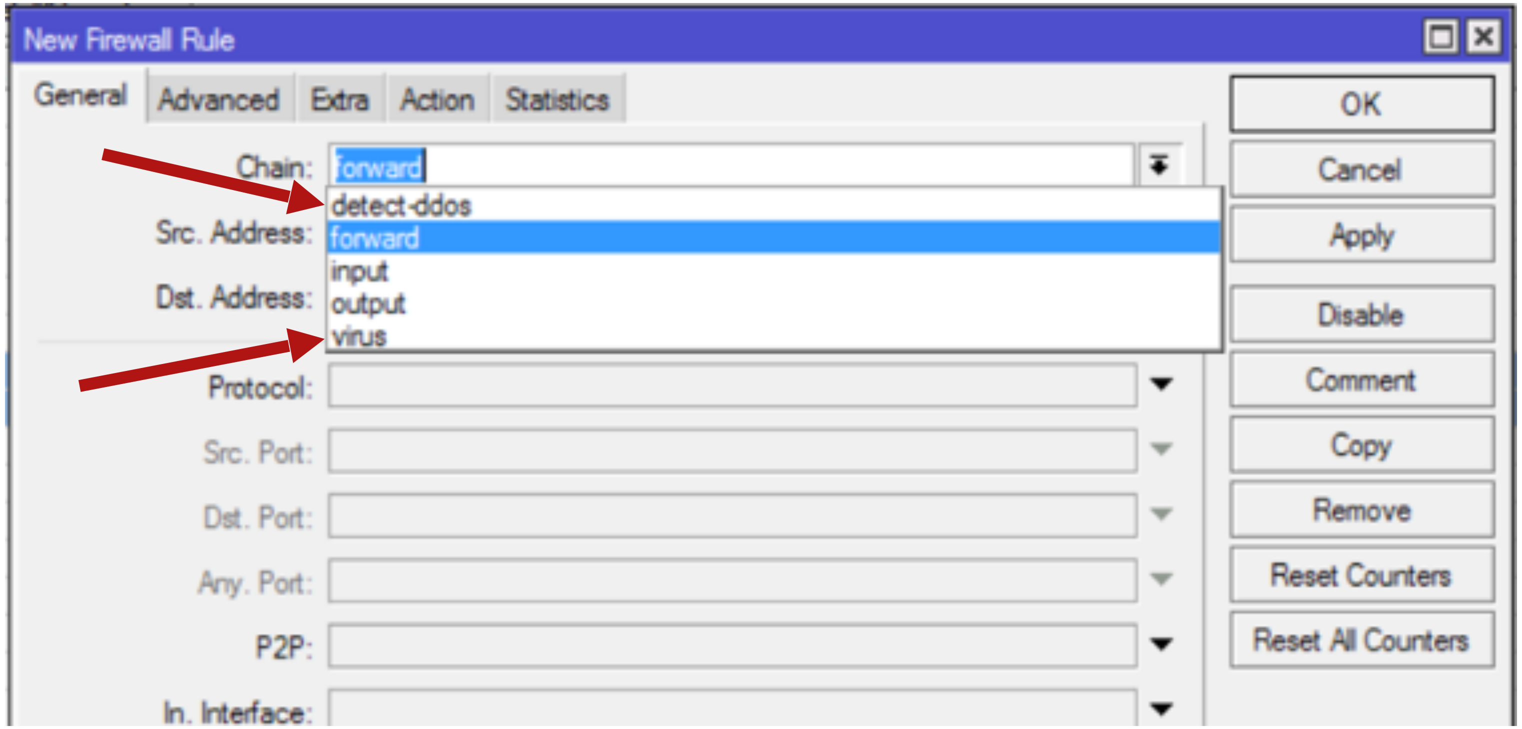
- We have no problem in sharing because knowledge is power and we expect you to give more inputs so that we can increase the knowledge base of all customers.

General Understanding

- Input Chain – Any packet which is **destined** for the router itself, e.g. SSH, Telnet, WinBox etc
- Output Chain – Any packet that is generating **from** router for e.g. Radius calls, SSH/Telnet into other devices from Winbox etc.
- Forward Chain – Any packet that is going **thru** the router or packets that are neither generating from and destined for router but for a network behind the router. For e.g. HTTP/TP/SMTP traffic of clients, etc

Note: In Mikrotik you can have your own custom named chain, but these will be children chain of one of the three above which will act as a parent chain.

The Chains

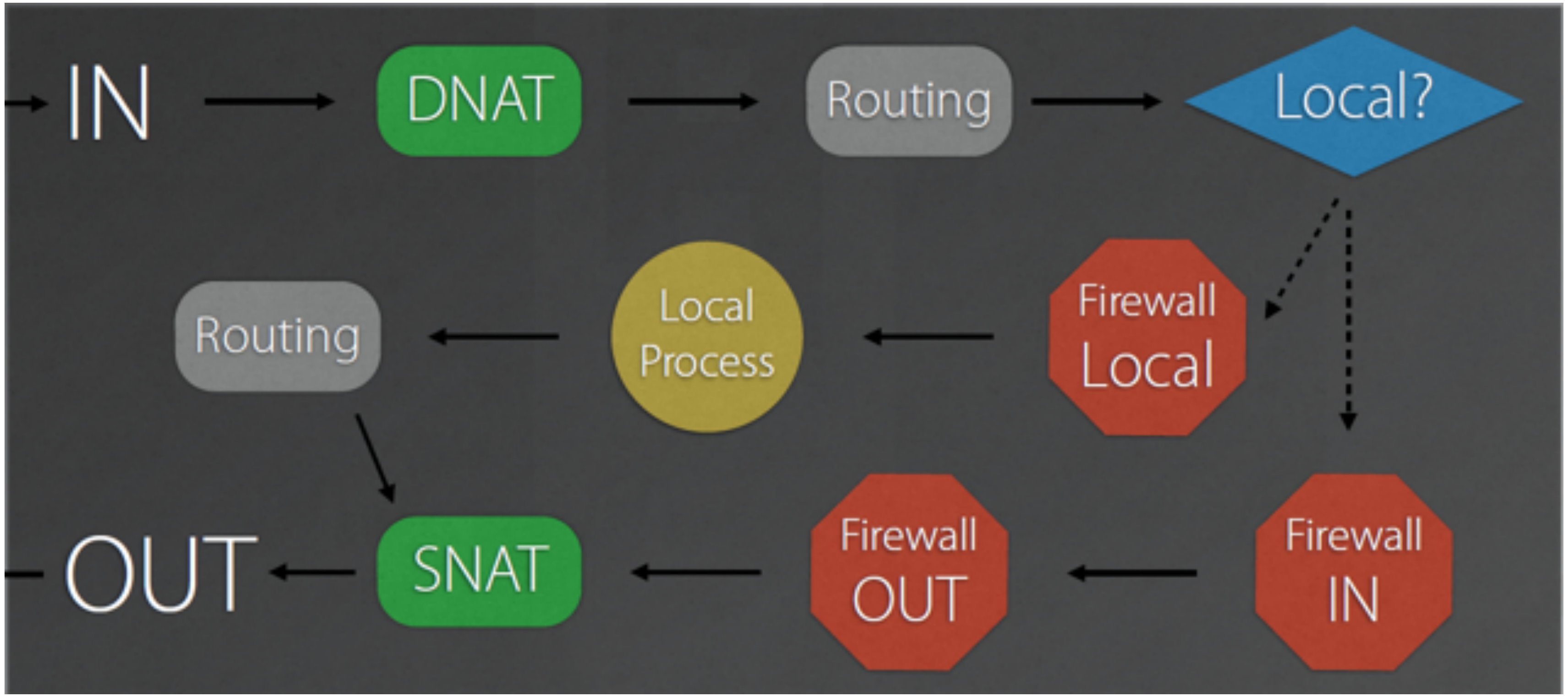


Chain: forward

Apart from 3 basic chains there are 2 more chains which are shown here, which are basically children chain of *forward* chain, created by *Action->Jump*. This is just to create more meaning for chain.

Call: 9717387778/9910416231 email: sales@kc-india.com

Understanding Packet Flow



Port blocking

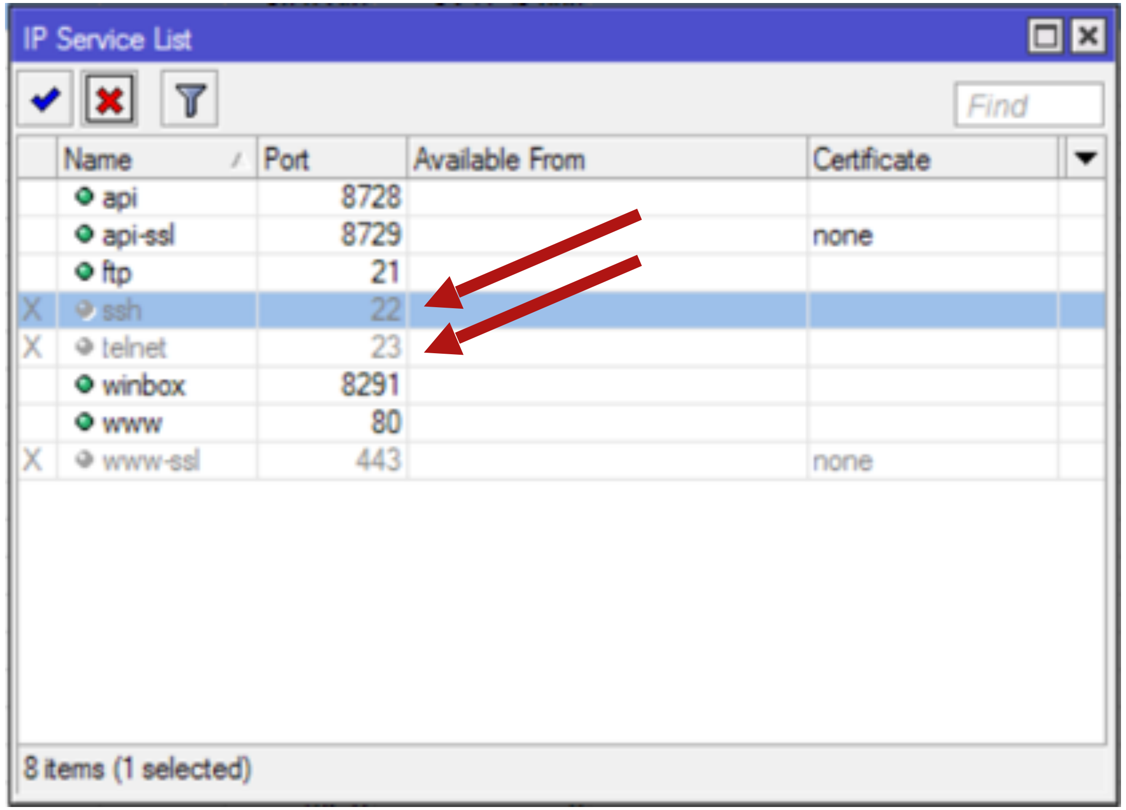
Some known malicious ports

- Blaster Worm (TCP/UDP: Port 135-139,445)
- Messenger Worm (UDP: Port 135-139)
- Sub7 Trojan (TCP/UDP Port: 27374)
- MyDOOM (TCP: Port 1080,3127-3128)

*complete list of these ports can be found annexed with the presentation

Although its not wise to block ports alone and think that the network will be secured, this is an amateur way of securing. Behaviour of the traffic is to be taken into account. But knowingly leaving ports open which are malicious in nature and time again proven to be bad is also not wise.

Firewall Tips & Tricks(services)



	Name	Port	Available From	Certificate
	● api	8728		
	● api-ssl	8729		none
	● ftp	21		
X	● ssh	22		
X	● telnet	23		
	● winbox	8291		
	● www	80		
X	● www-ssl	443		none

8 items (1 selected)

Although you can block SSH/Telnet and other services to secure your router but is it the best solution ???

Not really, in this age of technology where most of the work is done on your Smart Phones, and with Mikrotik still haven't released "official" WinBox for SP, till then we will have to use SSH and Telnet etc. (this is just one of the examples)

Firewall Tips & Tricks(services)

So what options do we have instead of blocking port for this case?

- We can restrict access of SSH/Telnet from certain IPs only

(But the problem with this is that we are on 3G/4G travelling and we get random IPs and feeding this kind of information is just not viable, right ?)

- We need to understand what are the implications of leaving the network open i.e. WHAT IS THE WORSE THING THAT CAN HAPPEN?

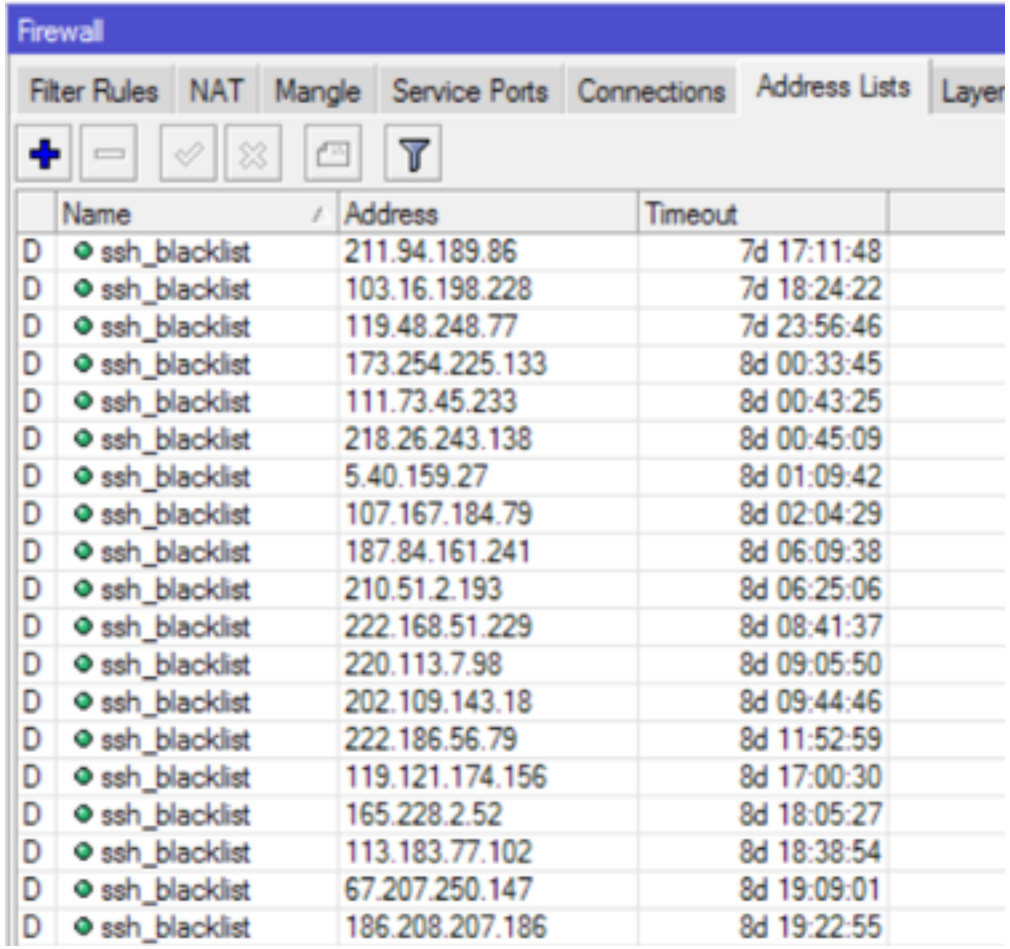
Obvious answer is HACK, but how can someone hack a password like **3X6=A%$** ???

Answer: ???

Firewall Tips & Tricks(services)

BRUTE FORCE ATTACKS
Or
Guess work on logic and BS dictionary

Firewall Tips & Tricks(services)



	Name	Address	Timeout
D	● ssh_blacklist	211.94.189.86	7d 17:11:48
D	● ssh_blacklist	103.16.198.228	7d 18:24:22
D	● ssh_blacklist	119.48.248.77	7d 23:56:46
D	● ssh_blacklist	173.254.225.133	8d 00:33:45
D	● ssh_blacklist	111.73.45.233	8d 00:43:25
D	● ssh_blacklist	218.26.243.138	8d 00:45:09
D	● ssh_blacklist	5.40.159.27	8d 01:09:42
D	● ssh_blacklist	107.167.184.79	8d 02:04:29
D	● ssh_blacklist	187.84.161.241	8d 06:09:38
D	● ssh_blacklist	210.51.2.193	8d 06:25:06
D	● ssh_blacklist	222.168.51.229	8d 08:41:37
D	● ssh_blacklist	220.113.7.98	8d 09:05:50
D	● ssh_blacklist	202.109.143.18	8d 09:44:46
D	● ssh_blacklist	222.186.56.79	8d 11:52:59
D	● ssh_blacklist	119.121.174.156	8d 17:00:30
D	● ssh_blacklist	165.228.2.52	8d 18:05:27
D	● ssh_blacklist	113.183.77.102	8d 18:38:54
D	● ssh_blacklist	67.207.250.147	8d 19:09:01
D	● ssh_blacklist	186.208.207.186	8d 19:22:55

Brute force is a trial and error method used by application programs to decode encrypted data such as passwords

Think about it that your bank passwords have restricted tries and after that you are blocked out until you call the bank to unlock it.

We can implement similar.

Here you see an example of IPs blocked for SSH login for 10 days.

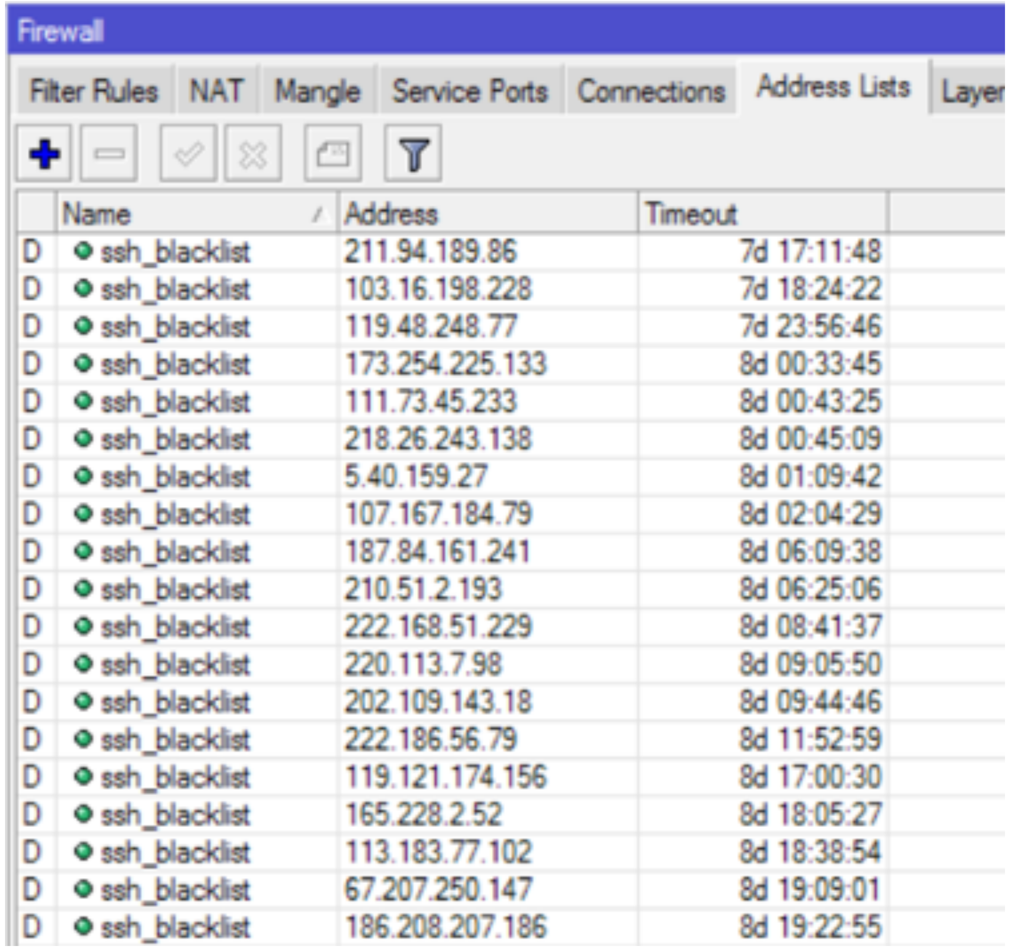
Firewall Tips & tricks(services) Configuration

Configuration to stop SSH Brute attack

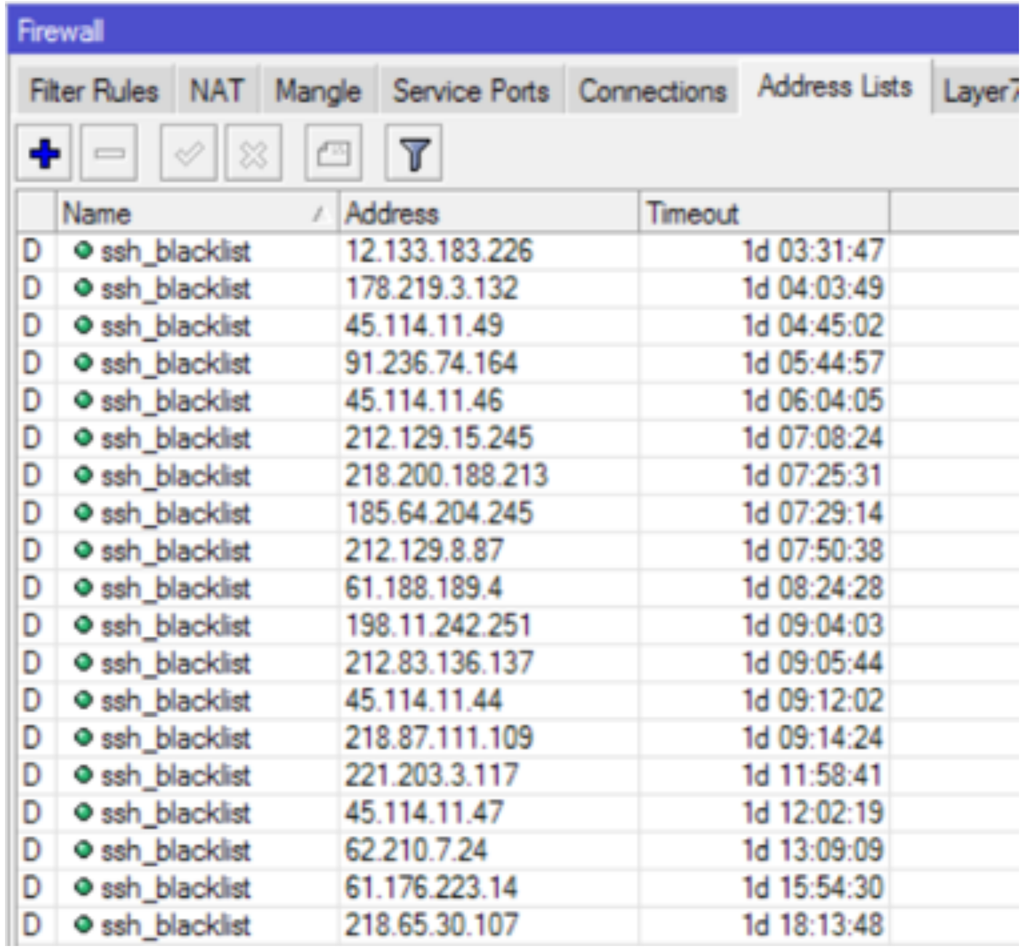
```
add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m comment="" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist address-list-timeout=10d comment="" disabled=no
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop comment="drop ssh brute forcers" disabled=no
```

- Assumed you are in /ip firewall filter
- All these configurations are annexed with the presentation

The result of policy



	Name	Address	Timeout
D	● ssh_blacklist	211.94.189.86	7d 17:11:48
D	● ssh_blacklist	103.16.198.228	7d 18:24:22
D	● ssh_blacklist	119.48.248.77	7d 23:56:46
D	● ssh_blacklist	173.254.225.133	8d 00:33:45
D	● ssh_blacklist	111.73.45.233	8d 00:43:25
D	● ssh_blacklist	218.26.243.138	8d 00:45:09
D	● ssh_blacklist	5.40.159.27	8d 01:09:42
D	● ssh_blacklist	107.167.184.79	8d 02:04:29
D	● ssh_blacklist	187.84.161.241	8d 06:09:38
D	● ssh_blacklist	210.51.2.193	8d 06:25:06
D	● ssh_blacklist	222.168.51.229	8d 08:41:37
D	● ssh_blacklist	220.113.7.98	8d 09:05:50
D	● ssh_blacklist	202.109.143.18	8d 09:44:46
D	● ssh_blacklist	222.186.56.79	8d 11:52:59
D	● ssh_blacklist	119.121.174.156	8d 17:00:30
D	● ssh_blacklist	165.228.2.52	8d 18:05:27
D	● ssh_blacklist	113.183.77.102	8d 18:38:54
D	● ssh_blacklist	67.207.250.147	8d 19:09:01
D	● ssh_blacklist	186.208.207.186	8d 19:22:55



	Name	Address	Timeout
D	● ssh_blacklist	12.133.183.226	1d 03:31:47
D	● ssh_blacklist	178.219.3.132	1d 04:03:49
D	● ssh_blacklist	45.114.11.49	1d 04:45:02
D	● ssh_blacklist	91.236.74.164	1d 05:44:57
D	● ssh_blacklist	45.114.11.46	1d 06:04:05
D	● ssh_blacklist	212.129.15.245	1d 07:08:24
D	● ssh_blacklist	218.200.188.213	1d 07:25:31
D	● ssh_blacklist	185.64.204.245	1d 07:29:14
D	● ssh_blacklist	212.129.8.87	1d 07:50:38
D	● ssh_blacklist	61.188.189.4	1d 08:24:28
D	● ssh_blacklist	198.11.242.251	1d 09:04:03
D	● ssh_blacklist	212.83.136.137	1d 09:05:44
D	● ssh_blacklist	45.114.11.44	1d 09:12:02
D	● ssh_blacklist	218.87.111.109	1d 09:14:24
D	● ssh_blacklist	221.203.3.117	1d 11:58:41
D	● ssh_blacklist	45.114.11.47	1d 12:02:19
D	● ssh_blacklist	62.210.7.24	1d 13:09:09
D	● ssh_blacklist	61.176.223.14	1d 15:54:30
D	● ssh_blacklist	218.65.30.107	1d 18:13:48

Understanding DDoS/DoS

- DoS stands for Denial of Service which is self explanatory of what this kind of attack is which is to make network/resource unavailable for the user/users for which it was intended.
- DDoS (Distributed Denial of Service) is where the attack source is more than one IP address.

A famous case happened in 2006 where a company Universal Tube sued www.youtube.com, because many would-be users of YouTube went to utube.com instead of youtube.com and this actually crashed the site of utube.com as the servers were not able to handle the traffic and they had to actually invest more money in their network infrastructure.(This is a good example of unintentional DoS attack)

Background Information: Denial of Service Attacks

- **Denial of Service Attack:** Effects of the attack are spikes in usage of resources such as Bandwidth, CPU usage, RAM usage
- **Objectives of an attacker:** Very evidently the primary objective is to disrupt the service to legitimate users of the resources. This will lead in ruining the reputation of the company giving the services, ultimate loss of business to the service provider to their peers.

Types of DoS

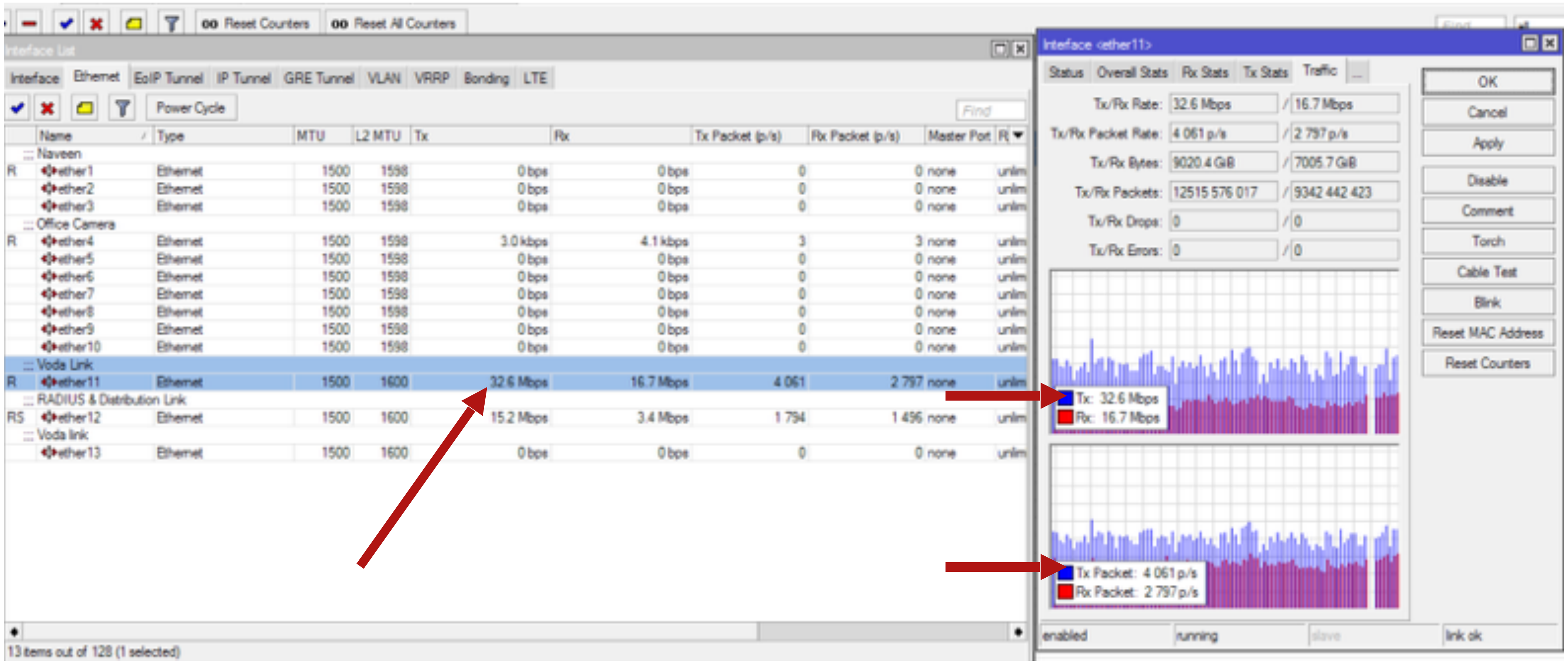
- Single source DoS attack: it could be of great effect if not attended to , the attacker can be identified comparatively easily, its easier to limit the damage.
- Distributed DoS attack: compared to single source its very damaging, even if detected could still cause lot of damage, identification of attacker is not easily identifiable as the source of attack is usually coordinated by various IPs
- Smurf/ Amplication attack: Very damaging as attack is basically huge amount of data is sent to the target, identification of attacker is difficult to identify, could be CATASTROPHIC

Difficulty in dealing with DDoS

- The most important aspect in DoS is to understand the attack, only then a defence can be made
- We need to find out what kind of attack is it e.g. Network level, OS level, Application level etc
- We need to find out what is the effect of the attack on our Equipment which is getting effected, is our OS getting effected, host computer etc
- What we need to remember is although we can control and limit traffic leaving our system what we cannot control is traffic coming from uplink network

Call: 9717387778/9910416231 email: sales@kc-india.com

Example: DNS amplification attack



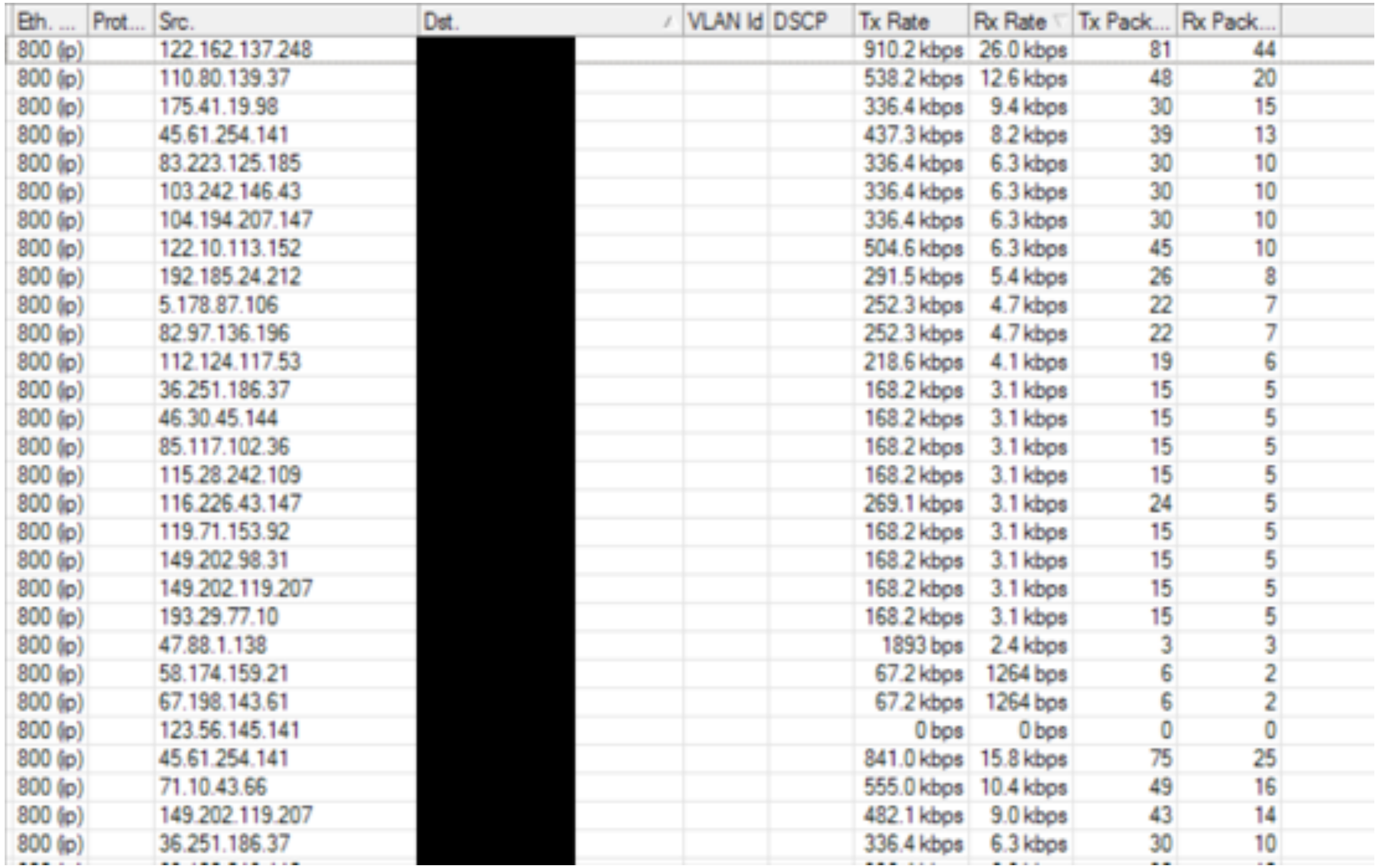
	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	Master Port	R
	::: Naveen									
R	ether1	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	::: Office Camera									
R	ether4	Ethernet	1500	1598	3.0 kbps	4.1 kbps	3	3	none	unlim
	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether6	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether7	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether8	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether9	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether10	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	::: Voda Link									
R	ether11	Ethernet	1500	1600	32.6 Mbps	16.7 Mbps	4 061	2 797	none	unlim
	::: RADIUS & Distribution Link									
RS	ether12	Ethernet	1500	1600	15.2 Mbps	3.4 Mbps	1 794	1 496	none	unlim
	::: Voda link									
	ether13	Ethernet	1500	1600	0 bps	0 bps	0	0	none	unlim

13 items out of 128 (1 selected)

Tx/Rx Rate: 32.6 Mbps / 16.7 Mbps
Tx/Rx Packet Rate: 4 061 p/s / 2 797 p/s
Tx/Rx Bytes: 9020.4 GiB / 7005.7 GiB
Tx/Rx Packets: 12515 576 017 / 9342 442 423
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0

enabled running slave link ok

Example: Contd…

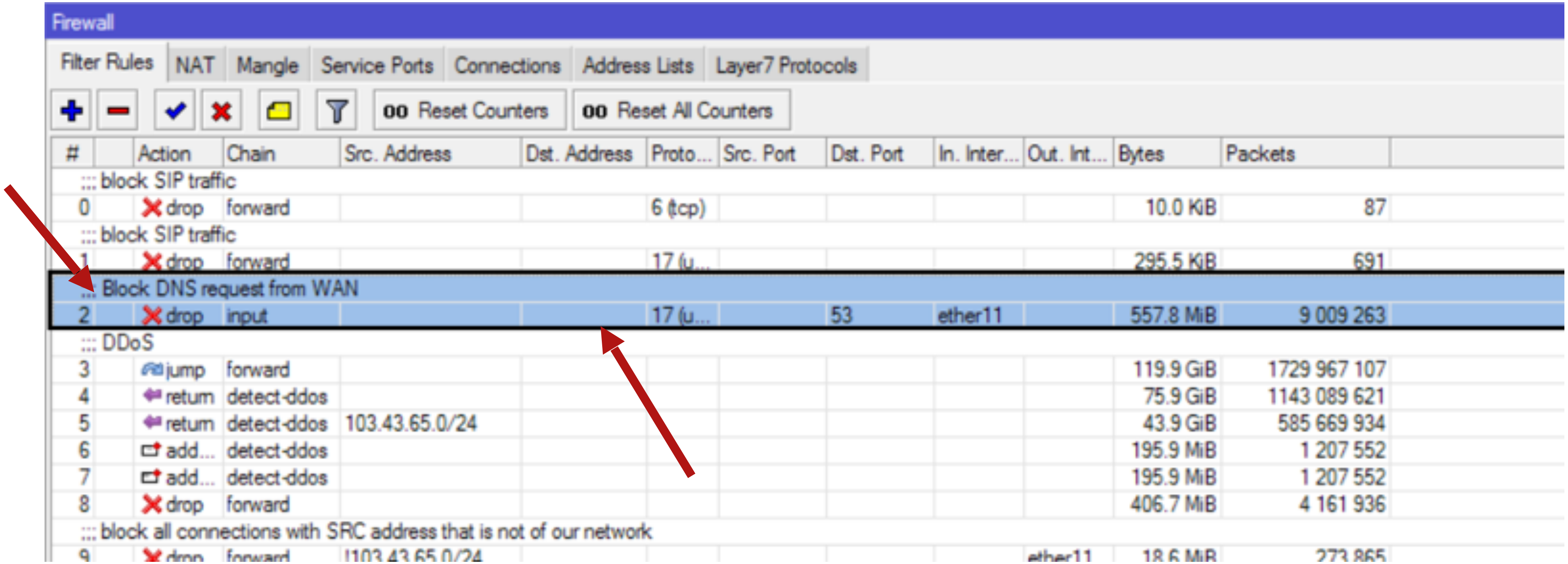


Eth. ...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		122.162.137.248	[redacted]			910.2 kbps	26.0 kbps	81	44
800 (ip)		110.80.139.37	[redacted]			538.2 kbps	12.6 kbps	48	20
800 (ip)		175.41.19.98	[redacted]			336.4 kbps	9.4 kbps	30	15
800 (ip)		45.61.254.141	[redacted]			437.3 kbps	8.2 kbps	39	13
800 (ip)		83.223.125.185	[redacted]			336.4 kbps	6.3 kbps	30	10
800 (ip)		103.242.146.43	[redacted]			336.4 kbps	6.3 kbps	30	10
800 (ip)		104.194.207.147	[redacted]			336.4 kbps	6.3 kbps	30	10
800 (ip)		122.10.113.152	[redacted]			504.6 kbps	6.3 kbps	45	10
800 (ip)		192.185.24.212	[redacted]			291.5 kbps	5.4 kbps	26	8
800 (ip)		5.178.87.106	[redacted]			252.3 kbps	4.7 kbps	22	7
800 (ip)		82.97.136.196	[redacted]			252.3 kbps	4.7 kbps	22	7
800 (ip)		112.124.117.53	[redacted]			218.6 kbps	4.1 kbps	19	6
800 (ip)		36.251.186.37	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		46.30.45.144	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		85.117.102.36	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		115.28.242.109	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		116.226.43.147	[redacted]			269.1 kbps	3.1 kbps	24	5
800 (ip)		119.71.153.92	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		149.202.98.31	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		149.202.119.207	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		193.29.77.10	[redacted]			168.2 kbps	3.1 kbps	15	5
800 (ip)		47.88.1.138	[redacted]			1893 bps	2.4 kbps	3	3
800 (ip)		58.174.159.21	[redacted]			67.2 kbps	1264 bps	6	2
800 (ip)		67.198.143.61	[redacted]			67.2 kbps	1264 bps	6	2
800 (ip)		123.56.145.141	[redacted]			0 bps	0 bps	0	0
800 (ip)		45.61.254.141	[redacted]			841.0 kbps	15.8 kbps	75	25
800 (ip)		71.10.43.66	[redacted]			555.0 kbps	10.4 kbps	49	16
800 (ip)		149.202.119.207	[redacted]			482.1 kbps	9.0 kbps	43	14
800 (ip)		36.251.186.37	[redacted]			336.4 kbps	6.3 kbps	30	10

Example: The problem

- Port of attack was generally unknown as it didn’t showed up on *tool->torch*
- May be Mikrotik will be able to help us out on this and add this facility in their tool so that we can pin point attacks better…
- So how did the tech guys solve this problem???
- More of a hunch deduced on various factors, these were and should not be limited to :
  - Traffic was leaving router more than what was coming in, signifying router hunting for some data on request something like DNS
  - DNS cache websites cached were random and not something you see normally
  - Using Packet sniffer to detect the ports of the packets

Example: The Solution



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: block SIP traffic												
0		✗ drop	forward			6 (tcp)					10.0 KiB	87
::: block SIP traffic												
1		✗ drop	forward			17 (u...					295.5 KiB	691
::: Block DNS request from WAN												
2		✗ drop	input			17 (u...		53	ether11		557.8 MiB	9 009 263
::: DDoS												
3		jump	forward								119.9 GiB	1729 967 107
4		return	detect-ddos								75.9 GiB	1143 089 621
5		return	detect-ddos	103.43.65.0/24							43.9 GiB	585 669 934
6		add...	detect-ddos								195.9 MiB	1 207 552
7		add...	detect-ddos								195.9 MiB	1 207 552
8		✗ drop	forward								406.7 MiB	4 161 936
::: block all connections with SRC address that is not of our network												
9		✗ drop	forward	!103.43.65.0/24						ether11	18.6 MiB	273 865

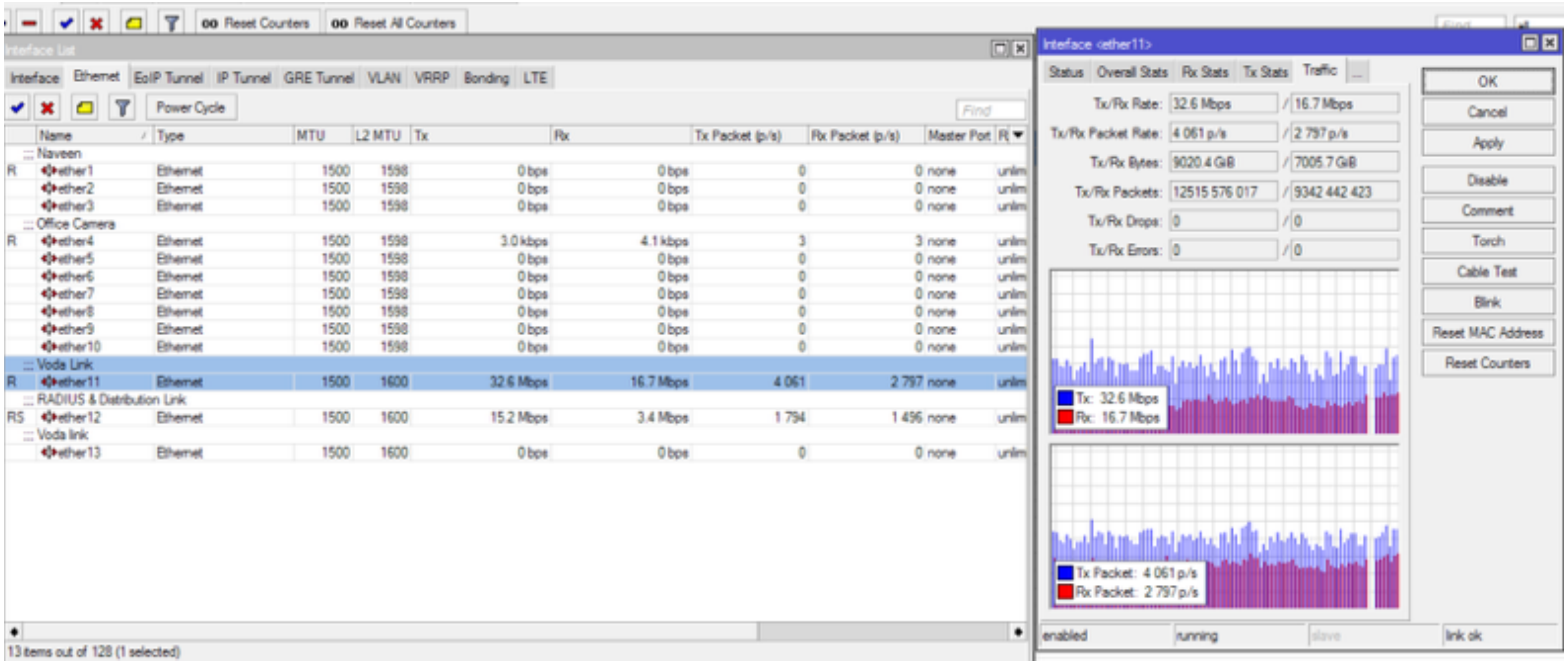
Example: Conclusion

- At the time of writing this document the immediate solution that was taken was to block the port UDP/TCP:53
- In long run this is not effective as the attack could shift to other ports/ services offered by service provider
- Although in this particular case this is important as your DNS server/cache should not listen to any entry which is not originating from within your network
- Its always good to talk to the TELCO providing you the service and getting the filters applied there, as the packets are reaching your router and then getting dropped, so your downstream is still being used.

Protecting your customers

- Before you start protecting what we need to do is understand the attack
- Constant vigilance of the network using numerous tools available e.g. Dude, Traffic Flow(Netflow), Cacti, etc
- Working with the customer(s) is an important aspect as they are sitting behind your systems and their being under attack is waste of your resources

What an attack looks like



	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	Master Port	R
	::: Naveen									
R	ether1	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	::: Office Camera									
R	ether4	Ethernet	1500	1598	3.0 kbps	4.1 kbps	3	3	none	unlim
	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether6	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether7	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether8	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether9	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	ether10	Ethernet	1500	1598	0 bps	0 bps	0	0	none	unlim
	::: Voda Link									
R	ether11	Ethernet	1500	1600	32.6 Mbps	16.7 Mbps	4 061	2 797	none	unlim
	::: RADIUS & Distribution Link									
RS	ether12	Ethernet	1500	1600	15.2 Mbps	3.4 Mbps	1 794	1 496	none	unlim
	::: Voda link									
	ether13	Ethernet	1500	1600	0 bps	0 bps	0	0	none	unlim

13 items out of 128 (1 selected)

Tx/Rx Rate: 32.6 Mbps / 16.7 Mbps

Tx/Rx Packet Rate: 4 061 p/s / 2 797 p/s

Tx/Rx Bytes: 9020.4 GiB / 7005.7 GiB

Tx/Rx Packets: 12515 576 017 / 9342 442 423

Tx/Rx Drops: 0 / 0

Tx/Rx Errors: 0 / 0

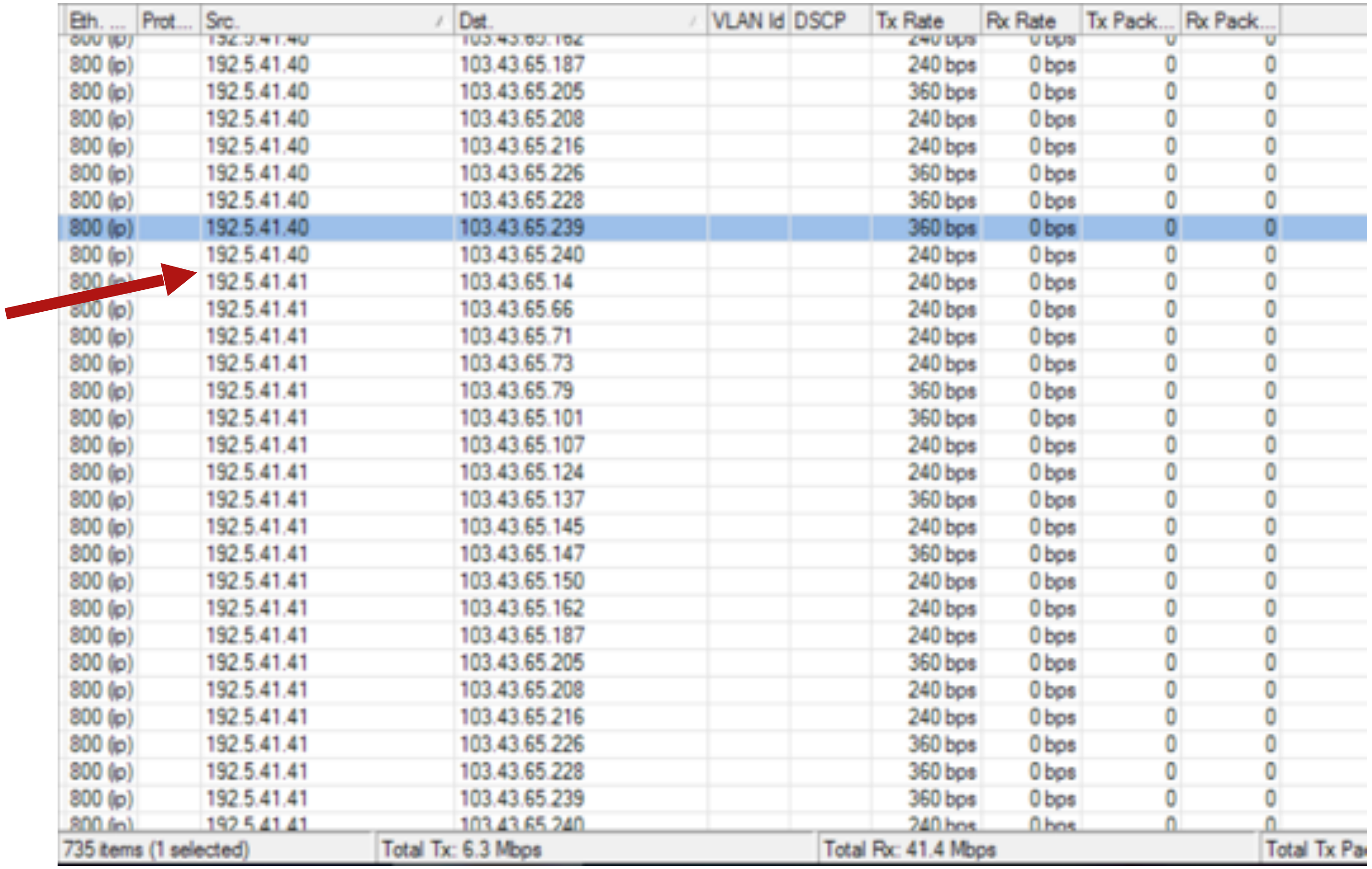
■ Tx: 32.6 Mbps
■ Rx: 16.7 Mbps

■ Tx Packet: 4 061 p/s
■ Rx Packet: 2 797 p/s

enabled | running | slave | link ok

Call: 9717387778/9910416231 email: sales@kc-india.com

What an attack looks like



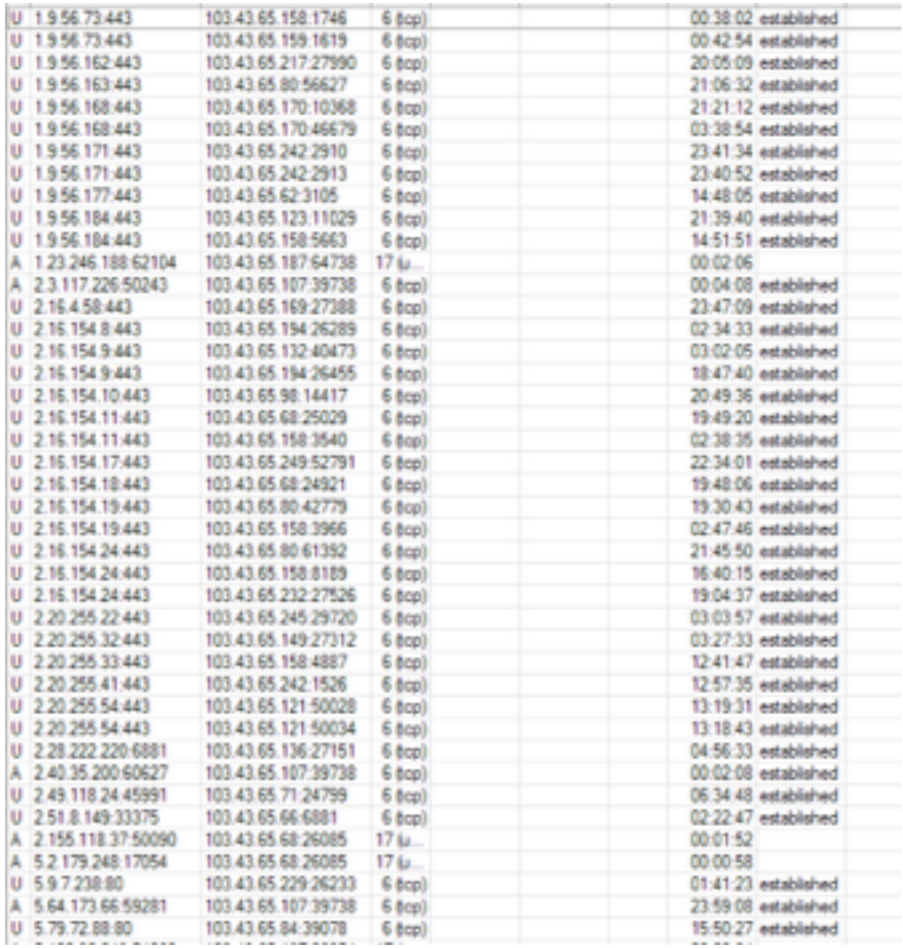
Eth. ...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.5.41.40	103.43.65.182			240 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.187			240 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.205			360 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.208			240 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.216			240 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.226			360 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.228			360 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.239			360 bps	0 bps	0	0
800 (ip)		192.5.41.40	103.43.65.240			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.14			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.66			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.71			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.73			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.79			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.101			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.107			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.124			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.137			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.145			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.147			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.150			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.162			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.187			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.205			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.208			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.216			240 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.226			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.228			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.239			360 bps	0 bps	0	0
800 (ip)		192.5.41.41	103.43.65.240			240 bps	0 bps	0	0

735 items (1 selected) | Total Tx: 6.3 Mbps | Total Rx: 41.4 Mbps | Total Tx Pa

The IP range belongs to Navy Network Information Centre(USA) now why would they be connecting to so many of the clients at one go ??

Call: 9717387778/9910416231 email: sales@kc-india.com

What an attack looks like



U	1.9.56.73:443	103.43.65.158:1746	6 (tcp)			00:38:02	established
U	1.9.56.73:443	103.43.65.159:1619	6 (tcp)			00:42:54	established
U	1.9.56.162:443	103.43.65.217:27990	6 (tcp)			20:05:09	established
U	1.9.56.163:443	103.43.65.80:56627	6 (tcp)			21:06:32	established
U	1.9.56.168:443	103.43.65.170:10368	6 (tcp)			21:21:12	established
U	1.9.56.168:443	103.43.65.170:46679	6 (tcp)			03:38:54	established
U	1.9.56.171:443	103.43.65.242:2910	6 (tcp)			23:41:34	established
U	1.9.56.171:443	103.43.65.242:2913	6 (tcp)			23:40:52	established
U	1.9.56.177:443	103.43.65.62:3105	6 (tcp)			14:48:05	established
U	1.9.56.184:443	103.43.65.123:11029	6 (tcp)			21:39:40	established
U	1.9.56.184:443	103.43.65.158:5663	6 (tcp)			14:51:51	established
A	1.23.246.188:62104	103.43.65.187:64738	17 (u...			00:02:06	
A	2.3.117.226:50243	103.43.65.107:39738	6 (tcp)			00:04:08	established
U	2.16.4.58:443	103.43.65.169:27388	6 (tcp)			23:47:09	established
U	2.16.154.8:443	103.43.65.194:26289	6 (tcp)			02:34:33	established
U	2.16.154.9:443	103.43.65.132:40473	6 (tcp)			03:02:05	established
U	2.16.154.9:443	103.43.65.194:26455	6 (tcp)			18:47:40	established
U	2.16.154.10:443	103.43.65.98:14417	6 (tcp)			20:49:36	established
U	2.16.154.11:443	103.43.65.68:25029	6 (tcp)			19:49:20	established
U	2.16.154.11:443	103.43.65.158:3540	6 (tcp)			02:38:35	established
U	2.16.154.17:443	103.43.65.249:52791	6 (tcp)			22:34:01	established
U	2.16.154.18:443	103.43.65.68:24921	6 (tcp)			19:48:06	established
U	2.16.154.19:443	103.43.65.80:42779	6 (tcp)			19:30:43	established
U	2.16.154.19:443	103.43.65.158:3966	6 (tcp)			02:47:46	established
U	2.16.154.24:443	103.43.65.80:61392	6 (tcp)			21:45:50	established
U	2.16.154.24:443	103.43.65.158:8189	6 (tcp)			16:40:15	established
U	2.16.154.24:443	103.43.65.232:27526	6 (tcp)			19:04:37	established
U	2.20.255.22:443	103.43.65.245:29720	6 (tcp)			03:03:57	established
U	2.20.255.32:443	103.43.65.149:27312	6 (tcp)			03:27:33	established
U	2.20.255.33:443	103.43.65.158:4887	6 (tcp)			12:41:47	established
U	2.20.255.41:443	103.43.65.242:1526	6 (tcp)			12:57:35	established
U	2.20.255.54:443	103.43.65.121:50028	6 (tcp)			13:19:31	established
U	2.20.255.54:443	103.43.65.121:50034	6 (tcp)			13:18:43	established
U	2.28.222.220:6881	103.43.65.136:27151	6 (tcp)			04:56:33	established
A	2.40.35.200:60627	103.43.65.107:39738	6 (tcp)			00:02:08	established
U	2.49.118.24:45991	103.43.65.71:24799	6 (tcp)			06:34:48	established
U	2.51.8.149:33375	103.43.65.66:6881	6 (tcp)			02:22:47	established
A	2.155.118.37:50090	103.43.65.68:26085	17 (u...			00:01:52	
A	5.2.179.248:17054	103.43.65.68:26085	17 (u...			00:00:58	
U	5.9.7.238:80	103.43.65.229:26233	6 (tcp)			01:41:23	established
A	5.64.173.66:59281	103.43.65.107:39738	6 (tcp)			23:59:08	established
U	5.79.72.88:80	103.43.65.84:39078	6 (tcp)			15:50:27	established

https (443) for CPEs trying to be opened by the same subnet of multiple routers…

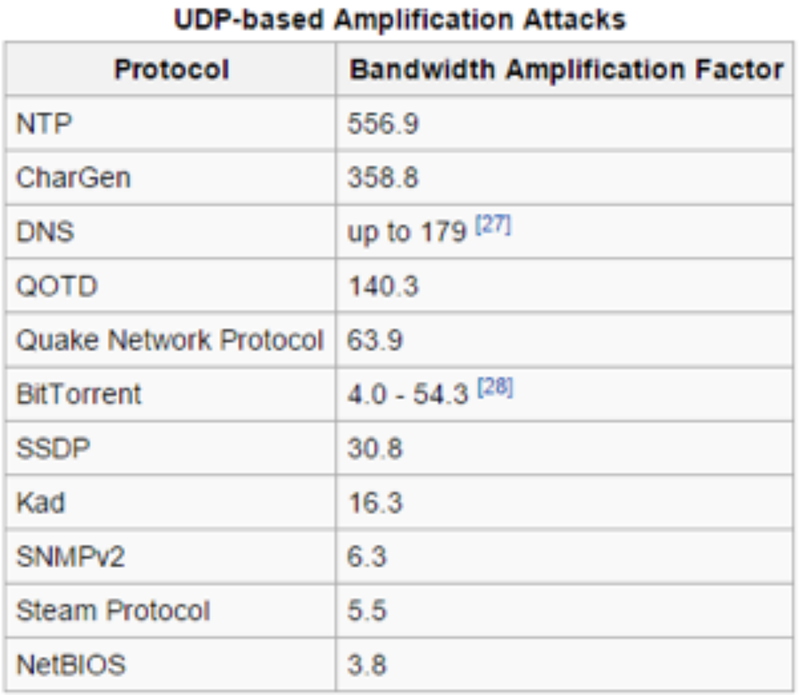
DDoS using CPEs/Computers

- It is not a certainty that you are always the victim, but yur client's CPE or computers may be facilitating an attack on someone else
- CPEs at customer end are configured incorrectlywhich allow attackers to make them ZOMBIES
- Like core router CPE at client side with open DNS cache access to internet will result in amplification attack
- This is not limited to DNS but can be on other services like NTP, SNMP (notice UDP services)

Why these services?

- Attackers love using DNS, NTP and SNMP as a reflector for amplification attack
- Being a UDP attack source cannot verified
- A small packet sent can be amplified into something much **larger**

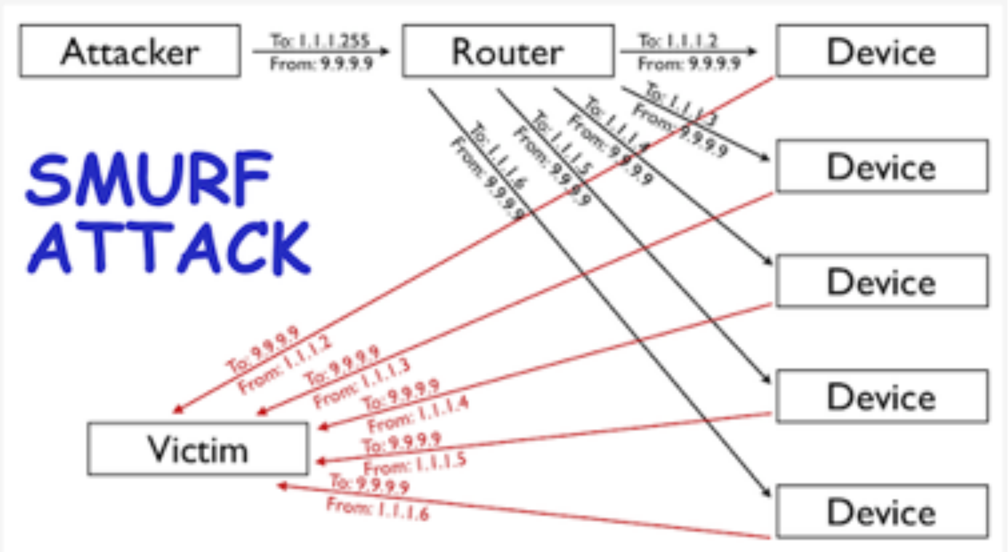
Amplification Factors



UDP-based Amplification Attacks

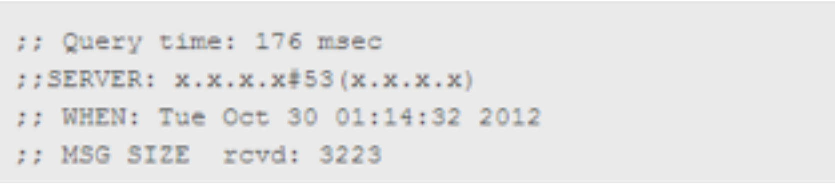
Protocol	Bandwidth Amplification Factor
NTP	556.9
CharGen	358.8
DNS	up to 179 [27]
QOTD	140.3
Quake Network Protocol	63.9
BitTorrent	4.0 - 54.3 [28]
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

Smurf attack



Smurf demystified

- DNS being UDP requires no handshake so basically fire and forget as a result the source can be spoofed and the receiver has no way of verifying the response
- Also DNS has a capability of creating huge amount of response a small 64 byte query can result in 3,223 bytes of response so an attacker can attain 50x the amplification

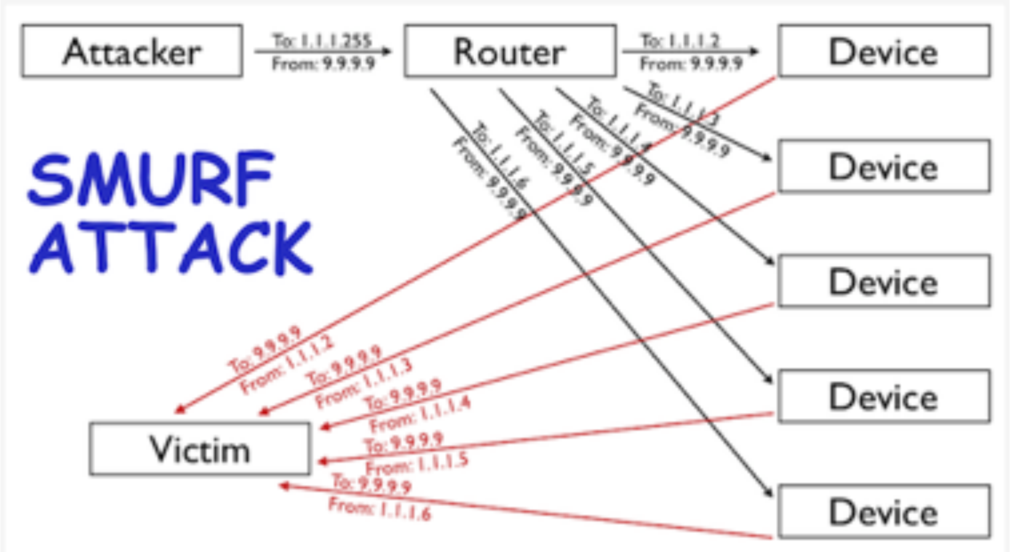


```
;; Query time: 176 msec
;;SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Tue Oct 30 01:14:32 2012
;; MSG SIZE  rcvd: 3223
```

Illustration

Now say the attacker is able to send 100Mbs of spoofed DNS request towards open DNS resolver, the victim will get hit by 50x that is 5Gb/s of traffic

That is One SICK attack



How to safe yourself

- Well as we discussed earlier first thing to do is not allow DNS request from WAN side of router
- Its not just DNS primarily all UDP traffic new and invalid UDP packets coming from WAN should be blocked
- Disable all UDP services, or if you are using them disable it from hearing request from the WAN

BCP 38

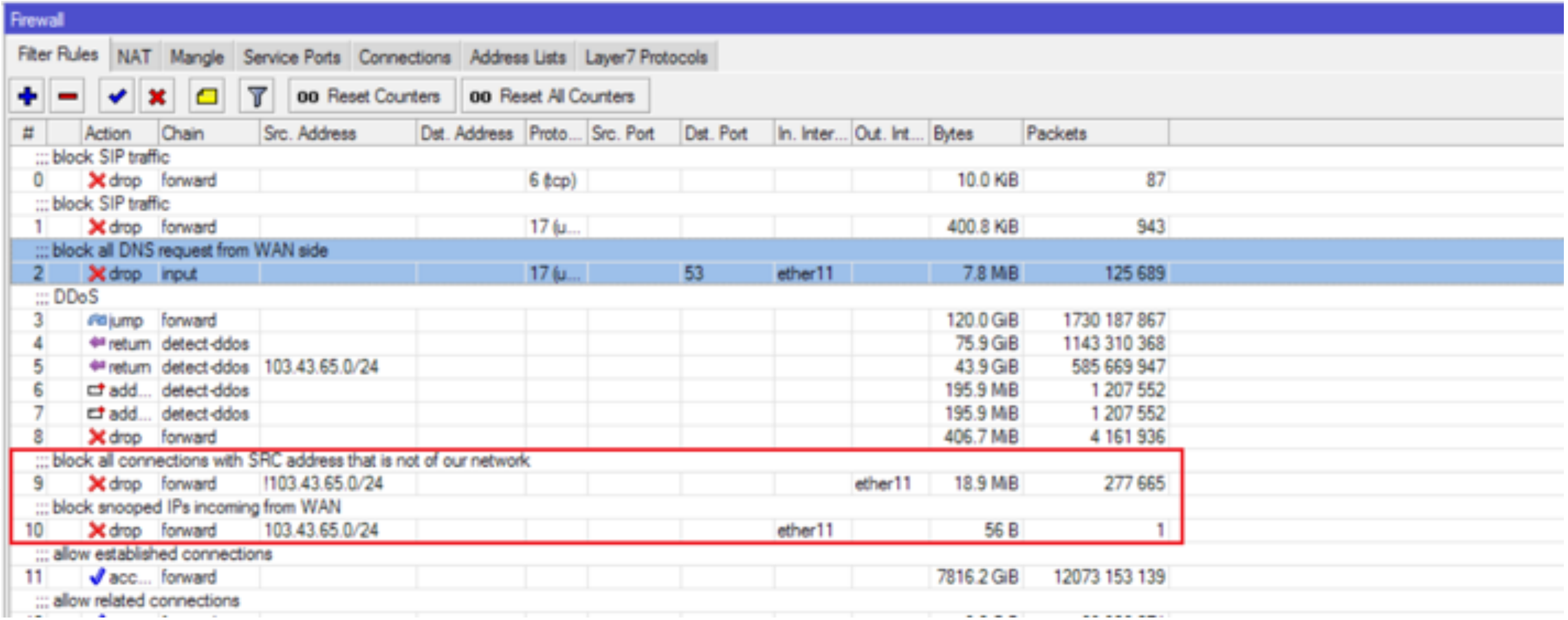
- Continuing on our earlier topic of DoS some simple implementation can be effective for network security and client security
- Best Current Practices 38 / RFC 2827 as documented by IETF (Internet Engineering Task Force) is a way to restrict forged traffic
  - Think about your network as a country and you need any person coming in with a valid passport and a valid visa
  - Although you cannot tell if the passport of another country is legitimate or not but when citizen of your country come or leave the port you know the legitimacy of the document. Right ?

BCP 38 : The implementation

- As was clear from the example our network works 2 ways data coming in from WAN forwarded to LAN and vice versa, so :
  - We need to protect our customers/network from spoofed IP/Forged IP. i.e. any ingress from WAN interface of your IP is not possible so you can safely **drop** that
  - Now we need to see if there is data flowing outside our network which is not generated per-se legitimately from our clients i.e. anything which is not generated from your network IPs going out thru WAN can be safely **dropped**

Call: 9717387778/9910416231 email: sales@kc-india.com

BCP 38 : The Result



Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

✚ ━ ✓ ✖ ▭ ⊽ 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; block SIP traffic											
0	✖ drop	forward			6 (tcp)					10.0 KiB	87
;;; block SIP traffic											
1	✖ drop	forward			17 (u...					400.8 KiB	943
;;; block all DNS request from WAN side											
2	✖ drop	input			17 (u...		53	ether11		7.8 MiB	125 689
;;; DDoS											
3	jump	forward								120.0 GiB	1730 187 867
4	return	detect-ddos								75.9 GiB	1143 310 368
5	return	detect-ddos	103.43.65.0/24							43.9 GiB	585 669 947
6	add...	detect-ddos								195.9 MiB	1 207 552
7	add...	detect-ddos								195.9 MiB	1 207 552
8	✖ drop	forward								406.7 MiB	4 161 936
;;; block all connections with SRC address that is not of our network											
9	✖ drop	forward	!103.43.65.0/24						ether11	18.9 MiB	277 665
;;; block snooped IPs incoming from WAN											
10	✖ drop	forward	103.43.65.0/24					ether11		56 B	1
;;; allow established connections											
11	✓ acc...	forward								7816.2 GiB	12073 153 139
;;; allow related connections											

BCP 38 : Limitation

- While you have protected the network of other people by not allowing spoofed traffic to go out but will they do the same for you ?

(You are only as good as your best player and as bad as your worst player)

- So if your neighbour is not being vigilant of attacks originating from their system, what will happen to them when attacks from some other system targets them ??

BCP 38 : Benefits

- You will be able to restrict the spoofed traffic (atleast the known one) at the border of Service provider's router
- Its easier to implement and maintain
- Reduction in reflected attacks

Protect yourself more

- So now you have no traffic leaving your network which was not originating from within your system
- And you are not getting any traffic from uplink which is of your system. Is this enough ?
- Filtering out the bogus is the next thing on our agenda

BOGON Filtering

- The term comes from *hacker jargon* defined as quantum of bogosity or property of being bogus
- Fancy definition what does it mean ?
  - Bogon is informal name for an IP Packet on the public internet that claims to be from an area of the IP address space reserved but not yet allocated or delegated by IANA (Internet Assigned Number Authority)
  - E.g.: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, 169.254.0.0/16 are example of private networks

BOGON a.k.a MARTIANs

- You can subscribe to TEAM CYMRU and filter out the Martians (private and reserved IP addresses as defined by RFC 1918, RFC 5735 and RFC 6598) and netblocks that have not been allocated yet by IANA
- Service providers can block source address of BOGONs and safely drop them as these are nothing but malicious packets with even more malicious intent

Questions?

Q & A

Thank you

- Thanks for listening and attending the session
- I hope to gain knowledge from you and share mine with you
- In case there is anything we can discuss after session also

- I have one more slide after this for everyone in the room

Call: 9717387778/9910416231 email: sales@kc-india.com

Why Share?

- One of the popular beliefs in India is if you share your solution your advantage with the client goes, I believe this is BS
- Sharing will result in increase of knowledge all over
- No time should be wasted on a problem that has already been solved, share so that new problems can be solved and addressed to
- I urge all to share on one of these platforms as they are rarely available to us as WISPs and we should make the best use of this.