NETWORK SECURITY

By Dennis Burgess

OVERVIEW

- DDOS Attacks
- Client Isolation
- Network Security

DDOS ATTACK

- Common Types of DDOS
  - DNS Amplification
    - Due to Open DNS Resolvers
    - These are DNS servers that respond to anyone for any request.
    - Every MIkroTik that has “Allow-Remote-Requests” turned on is a potential attack vector
    - Attackers like this; it’s a 1:179 bandwidth amplification factor
  - NTP Amplification
    - Open NTP servers
    - Attackers have up to 1:556 bandwidth amplification factor
  - There are others, these are the most common!

DDOS ATTACK

- **DNS Amplification**
  - How does this work
  - Requires Open DNS Recursive resolver
    - Recursive resolver, will go out and find what the answer is, add the answer to its cache and then return the result to the client.
    - non-authoritative answer – it gives an answer when its actually not the server responsible.
    - When you check the “allow remote requests” in IP→ DNS in RouterOS, without any rules, that creates a open DNS recursive resolver. I.e. any public IP on that box will respond to any DNS request.

DDOS ATTACK

- **DNS Amplification**
  - How does this work
  - Attacker
    - Uses his botnet -- Collection of workstations/devices that he has control of.
    - Sends Spoofed IP packets to open DNS resolvers.
    - The spoofed IP is the attacked IP.
    - The Open DNS servers, then respond with the correct answer but seeing that the packet came from the attacked IP (spoofed IPs), the response goes to the attacked IP
    - Many times, a 60-70 byte request can generate many return packets, causing high pps and bandwidth inbound.

DDOS ATTACK

- GOALS for DDOS
  - Take services off-line
    - Fill the pipe so that the server or client is off-line
    - No bandwidth for real world application
    - High latency, services off-line.

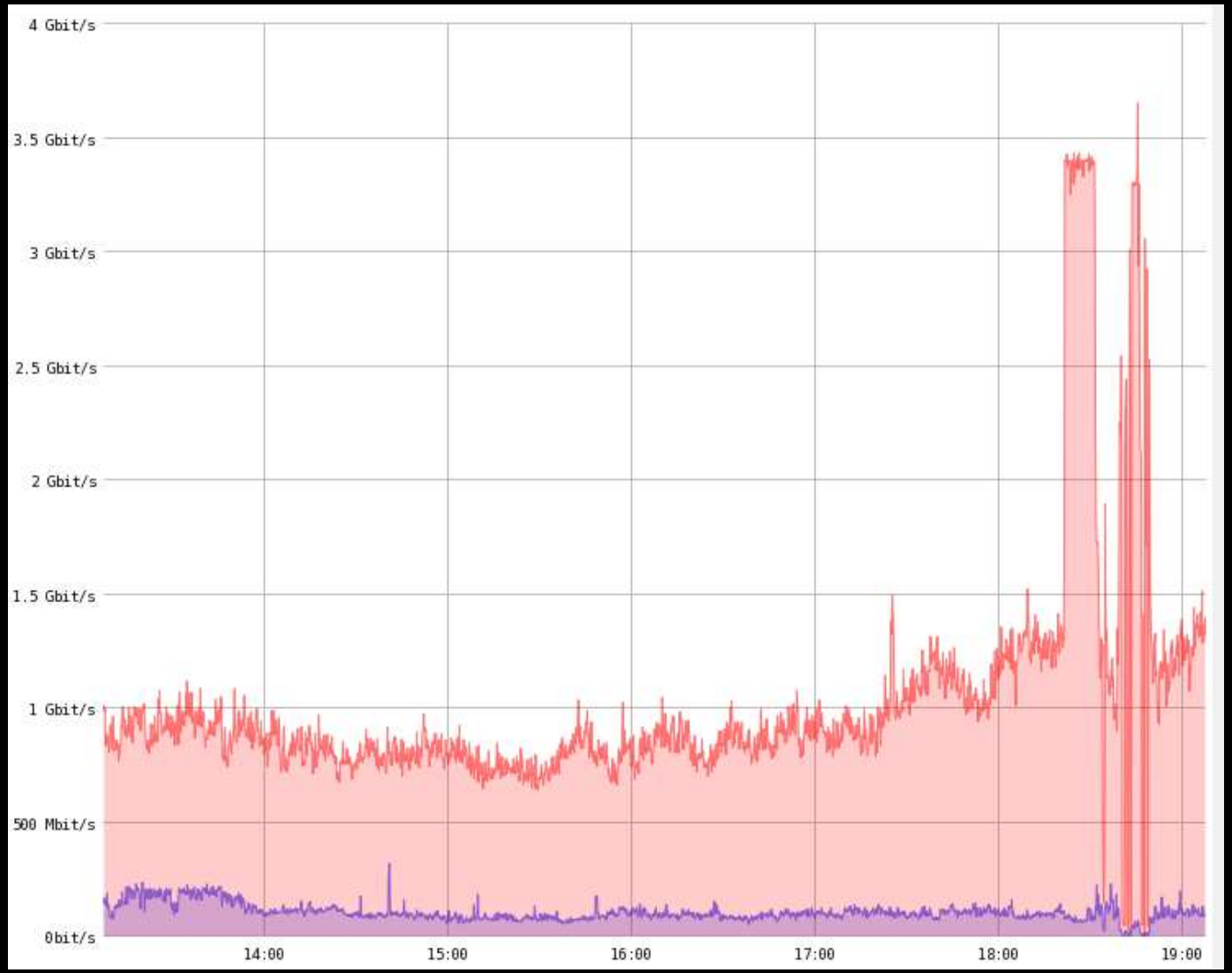
DDOS ATTACK

- GOALS for DDOS
  - Gamers
    - Lots of gamers have found that using DDOS against a fellow gamer can cause high latency
    - Thus they can win the prize if their fellow gamers have high latency.
    - Quite a few of League of Legends users do this!

DDOS ATTACK

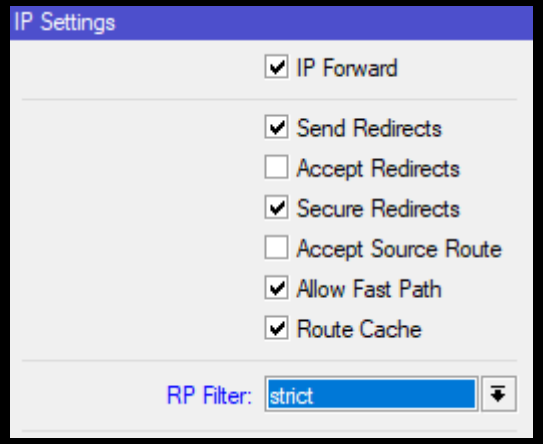
- DDOS
  - Typically large scale, can be 100meg to hundreds of Gigabit's
  - Typically need to be able to weather the storm
  - Need enough bandwidth to absorb the attack and block it from getting in.
  - Rules can include high PPS going to an individual IP address

DDOS ATTACK


4 Gbit/s
3.5 Gbit/s
3 Gbit/s
2.5 Gbit/s
2 Gbit/s
1.5 Gbit/s
1 Gbit/s
500 Mbit/s
0bit/s
14:00
15:00
16:00
17:00
18:00
19:00

DDOS ATTACK

- How to Stop DDOS Attacks
  - First line of defense is to have enough bandwidth
    - 5 gig attack hits a 1 gig port, the port is swamped, and it has succeeded.
  - Second is Black Hole Servers
    - BGP process to send a individual /32 to black hole
    - Back holes route, to that individual /32 dropping traffic before it gets to your edge device.
      - This prevents that /32 from getting out but prevents traffic from filling your entire pipe.
      - This in effect has done what the attacker wants, to take the customer off-line.
  - Third is BCP 38
    - Prevent spoofed packets form leaving your network.
    - If everyone did this, it would make these types of attacks uncommon.
    - You can also use strict reverse path.



DDOS ATTACK

- How to Stop DDOS Attacks
  - First line of defense is to have enough bandwidth
    - If you have enough bandwidth, you can firewall
    - Place rules in to detect high amounts of PPS going to a specific IP address
    - Drop all traffic to that IP address for 10 minutes
      - Most on-line services do this; they route your traffic though their network that has high amounts of bandwidth at datacenters that is purchased on the cheap.
      - They then detect and block the DDOS attack.
      - This does work, but adds latency inside your network
      - Typically are cost prohibitive
    - If the traffic continues add them back in until the traffic stops, this blocks that type of traffic but does not take the customer off-line. This is a failed DDOS.

DDOS ATTACK

- How to Stop DDOS Attacks
  - Second is Black Hole Servers
    - If you don’t have enough bandwidth to survive the attack
    - You advertise a /32 into black hole servers
    - Typically BGP process
    - Your provider must support this and have a documented and automated method
    - Some providers will have you establish a BGP session with their black hole servers
    - Some providers will simply have your add your /32 announcement with a specific community.
    - By advertising, you are telling your upstream(s) to block all traffic to that /32
      - This is YOUR /32, your IP, that IP will be offline, but the attack will not fill your pipe.
    - You can automate this with MIkroTik and several other solutions out there exist to detect and automate.
    - You can setup a BGP peer inside your network that you can get to that a single advertisement on it, advertises it to all of your upstream using the proper method.

DDOS ATTACK

- How to Stop DDOS Attacks
  - If you don’t have BGP, do not have enough bandwidth, and are getting attacked.
    - The only option is to **call your upstream**.
    - Sometimes they will take a statement and/or block traffic going to a specific IP
    - This is non-automated
    - This means that IP will be offline
    - Some providers only have this method ☹
    - Some providers will not black hole! Make sure to ask prior to purchasing.

PREVENTION

- Key is metrics
  - Inbound metrics and pps is important to block attacks, but not block normal traffic
  - Every network is different, don't use my numbers as they may not work for you!

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Dst. Limit/Rate	Bytes	Packets	Comment
27	accept	ddos_prev...			6 (tcp)		4444,135-139,445				92.8 KiB	1 890	Block all Inbound
28	accept	ddos_prev...			17 (u...		4444,135-139,445				5.2 KiB	68	Block all inbound
29	return	ddos_prev...								10000/sec	36.7 GiB	30 289 216	Return normal Traffic
30	add src to addr...	ddos_prev...									57.4 MiB	43 010	Add DST to DDOSe List
31	add src to addr...	ddos_prev...									46.8 MiB	35 109	Add DDOSer to BLOCK List
32	add dst to addr...	ddos_prev...									57.4 MiB	43 010	Add DDOSer to IP List
33	log	ddos_prev...									593.7 KiB	432	Log types of traffic
34	return	ddos_prev...									57.4 MiB	43 010	Return

PREVENTION

- Key is metrics
  - These metrics work for one customer, but not for another.
  - Make sure you understand what you are doing, when you put these kinds of rules in.
  - Note that there is no block rule here, we place that on the forward chain.
    - Make sure you know what you are going to block before blocking!

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Dst. Limit/Rate	Bytes	Packets	Comment
27		accept	ddos_prev...			6 (tcp)		4444,135-139,445				92.8 KiB	1 890	Block all Inbound
28		accept	ddos_prev...			17 (u...		4444,135-139,445				5.2 KiB	68	Block all inbound
29		return	ddos_prev...								10000/sec	36.7 GiB	30 289 216	Return normal Traffic
30		add src to addr...	ddos_prev...									57.4 MiB	43 010	Add DST to DDOSe List
31		add src to addr...	ddos_prev...									46.8 MiB	35 109	Add DDOSer to BLOCK List
32		add dst to addr...	ddos_prev...									57.4 MiB	43 010	Add DDOSer to IP List
33		log	ddos_prev...									593.7 KiB	432	Log types of traffic
34		return	ddos_prev...									57.4 MiB	43 010	Return

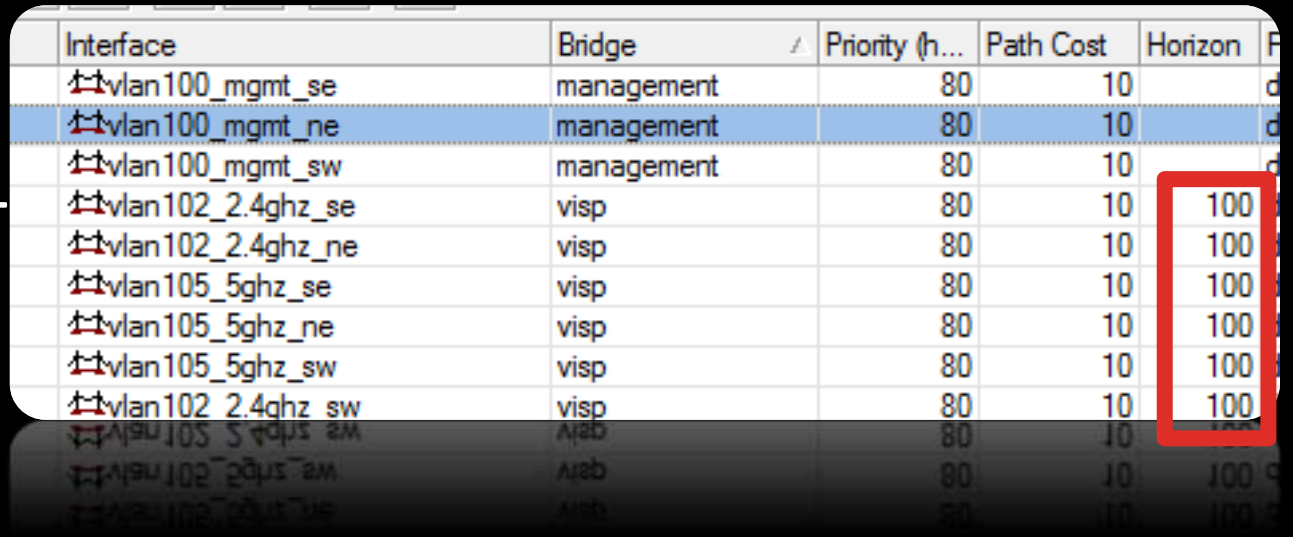
CLIENT ISOLATION

CLIENT ISOLATION

- Every client should be isolated into its own broadcast domain
  - This is not practical in all conditions, but can be done.
  - This allows the client to only talk to the router (their gateway) via ARP
  - Layer 3 connectivity can be used to allow clients to talk to one another, etc.
  - Layer 2 connectivity should never be given to your wireless network or infrastructure.

CLIENT ISOLATION

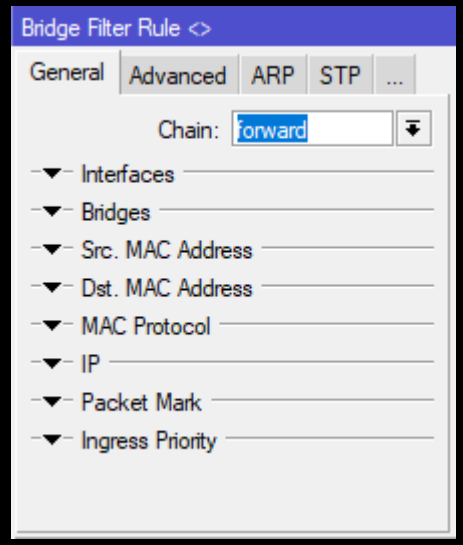
- How to do this?
  - Tower router with VLANs to switching
    - Add ports to bridge group
    - Firewall with Split-Horizon
  - This is hardware blocking
  - Turn off Default-Forward in access point – or disable client-to-client forwarding
    - This then puts each client into their own broadcast domain.
    - /interface bridge port set [find] horizon=100

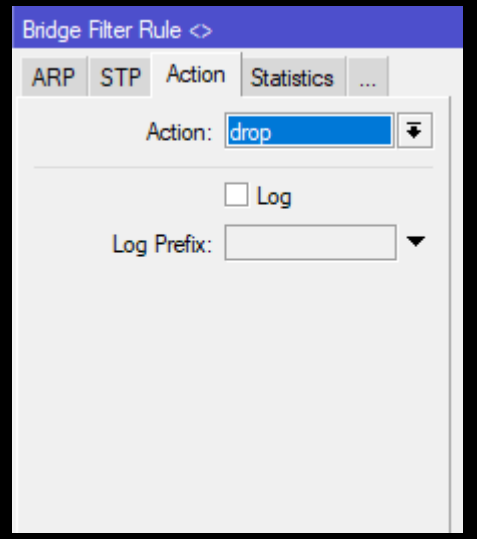


Interface	Bridge	Priority (h...	Path Cost	Horizon
vlan100_mgmt_se	management	80	10	
vlan100_mgmt_ne	management	80	10	
vlan100_mgmt_sw	management	80	10	
vlan102_2.4ghz_se	visp	80	10	100
vlan102_2.4ghz_ne	visp	80	10	100
vlan105_5ghz_se	visp	80	10	100
vlan105_5ghz_ne	visp	80	10	100
vlan105_5ghz_sw	visp	80	10	100
vlan102_2.4ghz_sw	visp	80	10	100

CLIENT ISOLATION

- You can also use
  - Bridge filters to drop all forward traffic.
  - Thus you can allow specific MAC addresses to specific MAC addresses
  - This blocks all data between bridged ports.
  - This is a software feature
    - /interface bridge firewall add chain=forward action=drop





CLIENT ISOLATION

- Rouge DHCP Servers
  - This prevents the effects of Rough DHCP Servers
    - Note, that your client should not have layer 2 access to your network anyways, so should not be an issue.

CLIENT ISOLATION

- Rouge DHCP Servers
  - You can use DHCP-Alert to alert you of other DHCP Servers
  - It will give you the MAC address and IP of the router that is running.
  - However with proper client isolation, this should not matter.

CLIENT ISOLATION

- Switches
  - You can use switches, to do this as well
  - Protected-Port status is a switch port that can’t communicate with other switch ports that is in the same group.

NETWORK SECURITY

NETWORK SECURITY

- Inbound Ports
  - 80,443,8080,8181,81-90, 21-25, 123, 53, 161, 135-139, 445, 110, 143, 8888
  - Common inbound ports to block, both TCP and UDP
    - Blocks common amplification attacks, as well as common web based ports. If a client is smart enough to use other ports than port 80 and 443, then let them but otherwise we block them.
  - Why?
    - Most users are dumb… If they want to take responsibility for their internet connection the they can upgrade to a package that does not have a firewall on it.
  - NAT
    - Is not considered a security mechanism
    - But can be very effective assuming your router is secured

NETWORK SECURITY

- Inbound Ports
  - 80,443,8080,8181,81-90, 21-25, 123, 53, 161, 135-139, 445, 110, 143, 8888
  - Common inbound ports to block, both TCP and UDP
    - What about other ports
    - 8291 – WinBox
  - Your business needs will be what you need to block
  - Separate your business with VLANs, place one subnet on for management, and no vlan for clients
  - Firewall at every router with rules that prevent network access to the management network from your clients IP addresses.
- IP → Services on your MIkroTik – Turn off the ones you don't use! Block management access to only your management network
  - Build a VPN to manage your network.

NETWORK SECURITY

- Forwarding inside your network
  - Typically you consider the inside of your network more secure than the outside.
  - This is a bad idea, as attacks can come from anywhere
  - Secure your infrastructure, your wireless access points, and devices
    - Place them on a VLAN so that you can access them easily enough.
    - Place firewall rules to prevent any client subnets from accessing them.
    - You SHOULD NOT be able to access client devices from the inside of your network
      - Not without a secure VPN
  - Do not forget about IPv6
    - You need to secure your devices and client access devices