Mikrotik in Network Operations in NZ - Learnings and Tricks

Or How I Stopped Worrying and Learned to Love Tricks

By Alexander Neilson, Network Manager

UFONE

UFONE

Contents

- General Warnings
- Network Tricks:
  - Triple NAT Trick
  - Multiple Interface PPPoE Trick
- Network Service Reliability
  - 3CX SBC Audio (First Call of the Day)
  - Careful NAT Construction
- Mikrotik PoE Switch – Initial Results

General Warnings

Tricks are still tricks

General Warnings

- The tricks have limits to be aware of (noted with the tricks)
- Every effort should be made to avoid relying on tricks too much*
- Always consider the side effects of any tricks implemented

Network Tricks

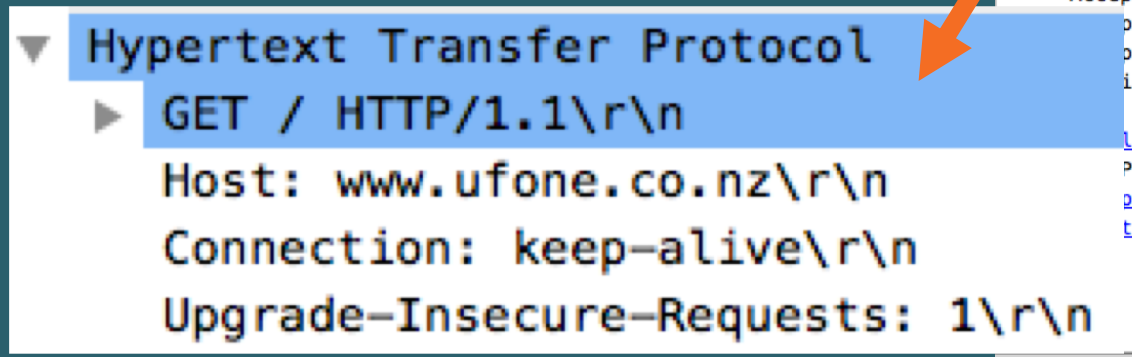
Or lets get this show on the road

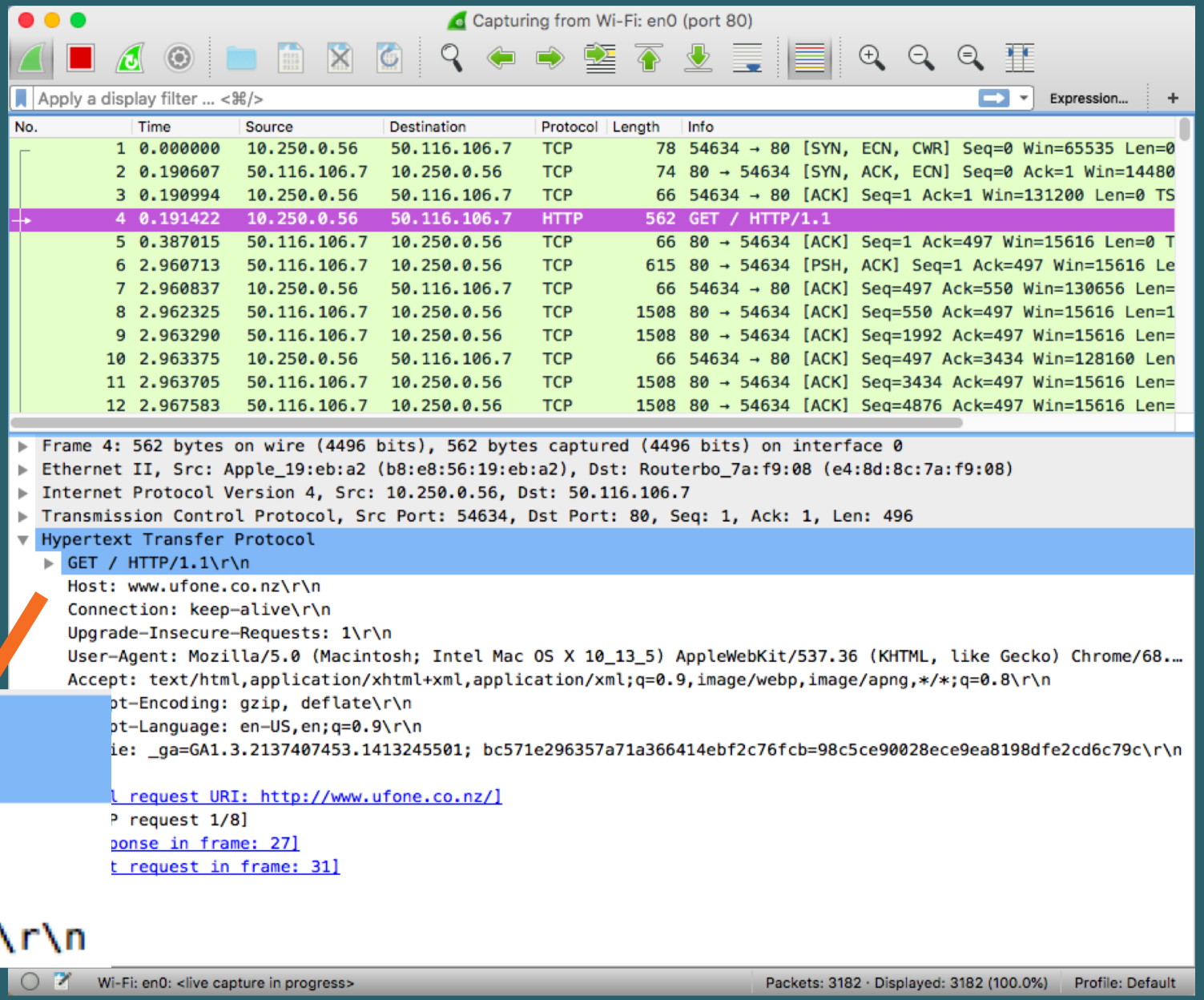
Triple NAT Trick

- Many network devices, to try be more secure, only accept requests from the local subnet (at least by default).
- These requests can be easily handled by a use of pinhole NAT to remotely access through a router (DST NAT followed by SRC NAT)
- However some devices are a little more tricky, these devices check the host header field in the http request and may return a 403 on mismatch

Host Header

The Host Header field is a part of HTTP requests which is used to select which website hosted on the web server is displayed and which certificate to present (in HTTPs). Normally it will be the 'hostname' (or IP Address) put between the http:// and the first / at the end (including a specified port)





So what's the issue?

- The device being accessed compares the Host Header to the IP address and Port configured for management (or internal management in routers)
- If this Header doesn't match the address for management then the device will reply with an error response (using a 403 forbidden – or sometimes a 401 unauthorized)
- This means you will normally be unable to manage this device unless you can directly route to the network (often requiring a VPN) or use this trick

Rough Diagram

1

2

3

End Router

The Trick

1. DSTNAT the IP Address for the management interface of the target router in your local router to the public address of the target
2. DSTNAT the IP Address from the public address of the target to the internal IP Address of the web interface you want to reach
3. SRCNAT the IP Address from your source router to the inside IP Address of the router you pass through

The Code

1. /ip firewall nat
   add action=dst-nat chain=dstnat dst-address=<device management IP> dst-port=<web management port> protocol=tcp to-addresses=<remote public IP> to-ports=<remote public Port>
2. /ip firewall nat
   add action=dst-nat chain=dstnat dst-port=<remote public Port> in-interface=<incoming interface> protocol=tcp to-addresses=<device management IP> to-ports=<web management port>
3. /ip firewall nat
   add action=masquerade chain=srcnat dst-address=<device management IP> src-address=<public IP you come from>

Multiple Interface PPPoE Trick

- Handling the various ”standard” circuit delivery standards in play can be somewhat of a mission
- Even when consistent / planned provisioning errors still abound
- And finally, even when delivered and working a speed change or firmware upgrade either in the exchange or locally can trigger an accidental change

Multiple Interface PPPoE Trick Cont.

- BUBA / EUBA PPPoA (Untagged)
- EUBA / WVS PPPoE / IPoE (Tagged – VLAN 10)
- UFB BS2(a) (Selectable – Untagged / VLAN 10)
- UFB BS3(a) 4 (Selectable – VLAN Transparent)

- Common Issues
- EUBA > VDSL Upgrades
- BS2(a) Provisioning Errors

- /interface vlan
  add interface=ether1 name=VLAN-10 vlan-id=10

- /interface pppoe-client
  add add-default-route=yes disabled=no interface=ether1,VLAN-10
  name=PPPoE-Internet password=secretpassword
  user=user@provider.tld

- The Mikrotik will automatically rotate through the various interfaces provided when it doesn’t have an active PPPoE session
- Very useful to use to avoid truck rolls to restore service or to limit the impact of provisioning errors by circuit providers

- However RADIUS replies need to be very timely
- Slow RADIUS replies cause the router to give up and move on before the reply is properly processed

Network Service Reliability

Lets take care of NAT

3CX SBC Audio (First Call of the Day)

- 3CX made some significant improvements to the SBC they provide to their phone system
- These improvements were focused on improving peak performance and audio quality
- Previously all traffic was tunneled through the SBC in a single TCP tunnel
- V15 continued to carry Signalling in TCP but defaults to trying to send audio in a UDP tunnel

3CX SBC Audio

- Unfortunately a side effect of how calls are setup can cause an issue with NAT rules
- The server may start to send the audio traffic first causing the router to mark the port being in use
- So when the outbound audio stream begins the router makes a mapping to a different port breaking audio for the call

3CX – Why First Call?

- So if it's the mapping of the port, why does it only affect the first call of the day?
- Actually if the call continues for 35 seconds audio will resume working
- After ~30 seconds of no audio 3CX automatically switches to the old TCP tunnel.
- Surely we can fix this!

The Fix

- /ip firewall nat
  add action=dst-nat chain=dstnat in-interface=<Internet Connection> protocol=udp src-address=<3CX Server Public IP> src-port=<Server Tunnel Port> to-addresses=<SBC Private IP>

- The fix matches the initial UDP packet inbound and establishes a NAT mapping from the server
- Using the Tunnel port on the public server catches the UDP tunnel stream and maintains the audio path

Warnings / Limitations

- This rule solves the UDP tunnel audio for only one tunnel endpoint
- Provided all other users only do CTI with their softphone this is a full solution
- If other softphone clients are being used for calls then they can be affected by the same issue

Careful NAT Construction

- If customer / site IP Addresses are static using SRC NAT as the action rather than Masqurade
- Guidance from Mikrotik on SRC NAT https://mum.mikrotik.com/presentations/US17/presentation_4241_1496042977.pdf

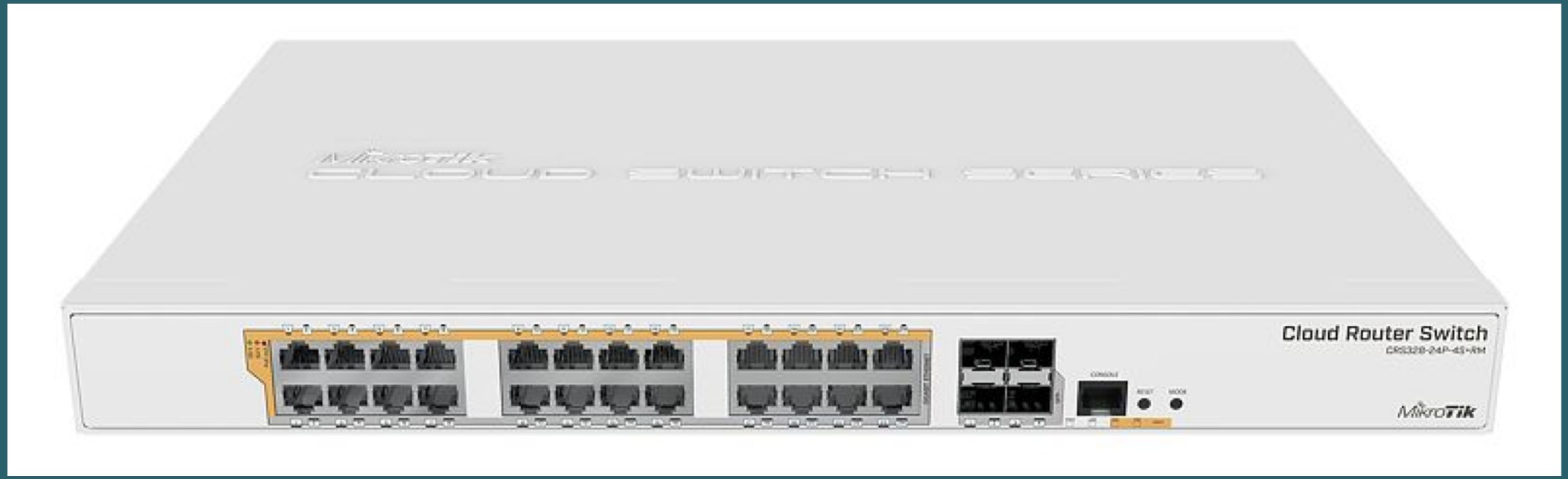
- Order rules in firewall / NAT tables in the order of most frequent matches where possible
- Create jump rules for categories of firewall / NAT rules

Mikrotik PoE Switch

Initial Test Results

I Have The PowEr

More PoE



Questions?

How Can I Help?

Thank You

Alexander Neilson,
Network Manager

alexander@ufone.co.nz

https://www.ufone.co.nz