MikroTik Router OS  Firewall Strategies

MikroTik Router OS Network Threats and Countermeasures

Speaker:  Tom Smyth
CTO Wireless Connect Ltd.

Location:  Budapest, Hungary
Date:  10\textsuperscript{th} of March 2011
Wireless Connect Ltd.

- Irish Company Incorporated in 2006
- Operate an ISP in the centre of Ireland.
- Good Infrastructure Expertise.
- Certified MikroTik Partners
  - Training
  - Certified OEM Integrators
  - Consultants
  - Distributor & Value Added Reseller
**Speaker Profile:**

- Studied BEng. Mechanical & Electronic Engineering, DCU, Ireland

- Have been working in Industry since 2000
  - Server Infrastructure Engineer
  - Systems / Network Administrator
  - IS Architect
  - Internet Security Consultant

- 1\textsuperscript{st} MikroTik Certified Trainer in June 2007 in Ireland
Ogma Connect

- A Collaborative Effort involved in the development and support of MikroTik Powered Appliances

- Ogma Connect's name comes from the Ancient God of Communications and eloquence who's name was Oghma

- Oghma was credited with the invention of the written language Ogham which is found carved in stones that mark the land of ancient tribes throughout the once vast Celtic world in northern & western Europe

- We want people to be able to connect with each other eloquently efficiently and elegantly
Presentation Objectives

- IP v4 Firewall Systems Concepts
- Outline what a firewall can and can not do
- Discuss Network Attacks and Mitigation Strategies
- Structure the Firewall
  - In a security centric manner
  - Create policy based rule sets
Sources of Security Information

- OWASP http://owasp.org
- Rits Group – http://www.ritsgroup.com/
- SANS Institute – http://sans.org
- CIS Centre for Internet Security – http://cisecurity.org/
- Open BSD – http://OpenBSD.org/
- Spamhaus.org – http://spamhaus.org
- nmap.org – http://nmap.org
- ha.ckers.org – http://ha.ckers.org/
- Cypherdyne - http://cypherdyne.org/
Firewall Systems

- One **or more** systems combined to achieve a desired security objective
- There are multiple ways firewall systems handle traffic
  - Routing
  - NATing
  - Bridging
  - Proxying
Firewall Design Objectives

- To implement a security policy by classifying, validating, logging and ultimately reacting to traffic
  - Flowing to the system
  - Flowing through the system
  - Flowing from the system
- Legitimate / useful traffic for users and systems should:
  - Not be Blocked
  - Not be Corrupted
  - Not be Slowed or Hampered Beyond Strict Tolerances
- Protect the users / systems behind it and Itself
Ideal firewall interface

- Protect me from bad traffic
- Allow only good traffic
- Protect me from myself
- Read my mind
Current Firewall Capabilities

• Can Identify traffic according to the following

  - Entry interface
  - Exit interface
  - Source Address (Source Address List)
  - Destination Address (destination Address List)
  - Address Types
  - Protocol type (number)
  - Protocol port (source and destination)
  - Message type (ICMP)
  - State of the Connection
  - IP V4 Options
  - TCP Flags
  - Number of Concurrent Connections
  - Packet Rate
  - Packet Size
  - Packet Fragmentation
Payload Inspection

- Packet Inspection inside the netfilter Firewall
- Can use content matcher in Advanced Tab
- Exact Match only
- Safe to use no regular expressions to trip you up
Layer 7 classifier

- Very powerful uses a Regular expressions
- Searches first 10 Packets / 2.5KB of a stream / connection
- Pre-defined signatures / patterns available from http://l7-filter.sourceforge.net/
- User Can generate their own custom pattern matches
- Be careful Layer 7 Rules if incorrectly written can crash
- The longer the search pattern the more processing power required
- Gradually add L7 Rules so that if there is an issue with the Firewall you can easily diagnose which rule is causing the issues
Adding L7 Rules

![Firewall interface with L7 rules](firewall_interface.png)
Firewall Challenges

- Firewalls generally have difficulty with the following
  - Specific protocol Validation / Filtration
  - Deep packet inspection beyond the first 10 packets / 2.5KB of data in the stream
  - Inspection of encrypted data streams such as
    - Ssh sessions
    - Https
    - Ipsec
    - TLS / SSL Protected Connections e.g SSTP
Firewall Limitations … Don’t Worry

- Proxies pick up where firewalls leave off...
- Proxies allow fine control over specific protocols :)
- Limitations are not a problem for inherently safe protocols
- For unsafe protocols proxies help can provide some damage limitation.
- Check out my Presentation Last year, at http://mum.mikrotik.com
Modular Firewall System Example

MTROS Outer Firewall
Block some inbound Traffic, Allow some inbound Traffic?

MikroTik ROS Inner Firewall
Allow some outbound Connections, Block all unsolicited inbound Connections

Internet
Friend or Foe?
WebClient

DMZ
Infrastructure Server
TCP 80

Internal Client
Internal Server Sensitive
Firewall hardening

- Some of the checks may be duplicated, this is ok, belt and braces.
- Check for unusual TCP Flags and drop.
- Drop packets with invalid connection state
- Your Effort will complement and bolster your networking operating software provider's efforts to maintain security
- Ultimately you are responsible for your networks security
Firewall Best Practices

- Populate a Router with the Maximum RAM Configuration
- Use Connection Tracking to achieve state-full packet inspection & perform fragmented packet reassembly
- Disable Administration interfaces from External Interfaces
- Try where possible to use in interfaces rather than source IP address for establishing the level of trust that you have for the
Firewall System Best Practices

• Run as few network services on the firewall hardware as possible
• Turn off all Administration services that are not needed
• Do not use un-encrypted administration protocols
• Shore up un-encrypted services with IPSEC policies
  – SNMP
  – DNS (internal use not for customer use)
  – Http fetch
  – NTP Time updates make sure the NTP Server responses are authenticated.
Disable Un-needed services

- Drastically reduces attack surface of your device
- If a service has a vulnerability your firewall can be compromised (stability, availability, integrity)
- Administration Services are particularly risky as they allow for the change of firewall configuration
- DNS Server services should be offloaded to a Hardened DNS Box
- NTP Server services should be offloaded to a Hardened NTP Box
Unencrypted Administration Risk

- Vulnerable to Sniffing / Replay attacks.
- Packets could be modified in transit.
- Can allow an attacker who can view the traffic to harvest user authentication credentials.
- IPSEC can eliminate this risk by securing the traffic with the best available FIPS grade cryptography protocols.
- IPSEC can be used to increase confidence if encryption quality of an administration service is unknown.
More RAM – More Connections

- NSA Security Guide for Routers suggests that Perimeter routers /firewalls be configured with the maximum available RAM
- The More RAM you have the harder the device is to Crash due to memory exhaustion (DOS / DDOS attacks)
- MT ROS Devices are Optimised against RAM Exhaustion Attacks.
- The firewall can cope better in busy periods.
- Ogma Connect Routers are always Sold with the maximum Supported RAM available :)
- Wireless Connect Customers can avail of RAM upgrades for RB1100 the New
- MikroTik Now Ship 1.5 GB RAM on the Improved RB1100AH :)

http://wirelessconnect.eu/ Copyright 2007 - 2011
Hardware with multiple Physical Interfaces

- The More Interfaces the more you can isolate multiple untrusted interfaces.
- For Clients who require higher levels of Security assurance.
Hardware fit for the Job :)

• As you have seen from the My colleague and Friend Patrik Schaub's presentation on Mikrotik Datacentre products.
RB 1100 / RB1100AH

- 13 Interfaces :) so greater control of your network

- Available from Wireless Connect.
Ogma Connect 2500

- 11 GBE Interfaces by Default
- Up to 19 GBE with Expansion Cards
Connection Tracking

- ConTrack carries out the following essential tasks
  - It monitors the state of all connections / requests flowing in the firewall
  - Allows the firewall to dynamically open / close ports according to the connection state in the firewall
  - Performs IP Packet Reassembly before inspection (prevents IP Fragment Attacks)
Filter Administration Services

- Minimise Risk from outside attacks
- Allow Flexibility of management internally
Firewall Setup Strategy

- Turn on connection tracking
- Break down the security policy into functional groups
- Use chains to define these functional groups
- Granularly control settings within the chains /groups
- Make use of Address lists group hosts together
Security Objectives (policies)

• One Should
  – Detect / Block Traffic to / from Invalid Addresses
  – Detect / Block Traffic that have a large packet size
  – Detect / Block Traffic that has unusual characteristics
  – Detect / Block Traffic from Port Scanners
  – Detect / Block Traffic from Brute Force Hackers
  – Once Traffic has been inspected don't keep reprocessing the same connection.
  – Analyse Traffic originating from and Leaving router
  – Protect Traffic Entering and destined for the router.
  – Update some Rules dynamically (Self Defending Networks)
Invalid Addresses

- Bogons (source and destinations)
  - Un allocated addresses
  - Remove (Special Purpose Allocated Addresses)

- Allocated Special Purpose:
  - Multicast Addresses (source addresses only) 224.0.0.0/4

- Broadcast Addresses 255.255.255.255

- Connected Network Broadcast addresses such as
  - 192.168.0.255 if the router has an ip address of 192.168.0.x/24
  - 192.168.0.127 if the router has an ip address of 192.168.0.x/25

- Private IP Addresses
- Test IP Addresses 192.0.2.0/24
- Loopback Addresses 127.0.0.0/8
Block invalid packets with IP
Broadcast source address
Block Multicast source Address

- Multicast should never be a source address of an IP Packet
- Block it the same way as the previous slide
Blocking IP Directed broadcast

- In forward chain create a rule with “destination address type” = Broadcast.
- Example of IP Directed broadcast 192.168.1.255
Blocking IP Directed Broadcast

In the firewall rule settings, select the 'Extra' tab and configure the source address type to 'broadcast'. This setting helps in blocking IP directed broadcast packets.
Block Bad People Dynamic updates

- Reference Spamhaus DROP List (Dont Route or Peer) updated Weekly
- Reference SANS ISC Top 10 – 10000 (optional if you wish)
- Bogons (un allocated not special Purpose)
- If updating using fetch with dns host name one should use IPSEC for protecting the DNS & the FTP /http Download of rules list
Updating Address Lists automatically

- Use a combination of Scheduler and Scripting tools, and Fetch.
- Fetch is very good because of the ability to use DNS Addresses for ease of management.
- Security Concerns...Updates traversing untrusted networks
  - Use IPSEC Policy for fetch tool,
  - ensure DNS Requests don't traverse untrusted networks or
  - Use Static DNS
Address List Update Script Sample

:global oldbogoncount;

:global totalbogoncount;

/ip firewall address-list set comment="oldbogons" [/ip firewall address-list find list=bogons_address_list]

:set oldbogoncount [ip firewall address-list print count-only value-list where list=bogons_address_list];

/tool fetch mode=http url="http://wirelessconnect.eu/store/images/bogonsnoprivate.rsc"

import bogonsnoprivate.rsc

:set totalbogoncount [ip firewall address-list print count-only value-list where list=bogons_address_list];

:if ($oldbogoncount < $totalbogoncount) do {/ip firewall address-list remove [/ip firewall address-list find comment="oldbogons"] }
Block Packets with Large Size

- Block Packets larger than 1500 bytes to protect legacy clients.
Block Un-needed IP Options

- Strict Source Route
- Loose Source Route
- Route Record
- Timestamp
- Router Alert (if not using RSVP)
Block Port Scanners

- Detect Nmap Scan types (TCP)
  - Christmas Tree
  - SYN FIN
  - FIN
  - ALL
  - SYN/RST

- Detect using MT Port Scan
  - Detect TCP

- Detect and drop scans using ICMP Messages out bound
  - (Port Unavailable)
  - Communications Prohibited
Port Scan Detect

- TCP Scans are Detected Directly
- UDP Scans indirectly
- Drop UDP Scans / Results of UDP Scans (ICMP)
- Add big offenders to Port Scanners blocking list
Checking Rate of matches

- For blacklisting obvious UDP Scanners
- Limit the speed of a scan for 120 ports per minute
Blocking the UDP scanner

- Use Add Dst Address to Address List action
Blocking Port scanners can be abused

- What about spoofing UDP Scans and TCP Syn Scans?
  - Attacker can send the packets does not need the reply?
- An attacker can spoof your Customers IP Address and your Firewall will block the customer IP address
- Your customer will be denied your services
- There is a trade off between high security and service availability for UDP and TCP Syn Scan detection
- Can be over come by using white lists for critical customers / servers
- Differentiate between Connect port scans (bi directional cant be spoofed) and scans that can be spoofed
Before the DOS

Attacker Real IP 1.1.1.1

Friend or Customer

WebClient

Client Real IP address 2.2.2.2

Client is able to use Web Services as normal

MTROS Outer Firewall
Attacker Starts DOS

Attacker Real IP 1.1.1.1

Sends Spoofed SYN Scans from spoofed Src address 2.2.2.2

MTROS Outer Firewall

Friend or Customer

WebClient

Client Real IP address 2.2.2.2
Firewall Responds to Scan

Attacker Real IP 1.1.1.1

MTROS Outer Firewall

MikroTik Firewall Receives spoofed packets with Src address 2.2.2.2

After some time the src address 2.2.2.2 is added to a Port Scanner Address List.

Friend or Customer

WebClient

Client Real IP address 2.2.2.2
DOS Complete

Attacker Real IP 1.1.1.1

MTROS Outer Firewall

MikroTik Firewall still receives spoofed packets with Src address 2.2.2.2

After some time the src address 2.2.2.2 is added to a Port Scanner Address List.

Friend or Customer

 WebClient

Client Real IP address 2.2.2.2 Denied access to services
Port Scan Address Lists

• Create one “definite port scan address list”
  - Longer lockout time
  - Log using syslog for external reporting and follow up

• Create a second “possible port scan address list”
  - Shorter lockout time
  - Log using syslog for internal reporting and analysis
  - Analyse logs for the following
    • Repeated persistent scans denial of service, may have to work with intermediate ISPs to trace the culprit
    • Single scans lasting under an hour ? Most likely a scan and src ip address likely to be in control of your adversary
Develop your own FW signatures

- Identify suspicious Traffic patterns,
- Example Brute Force Password Attacks on servers
  - Some Administrative Services have 1 TCP Connection maintained per Active Admin session
  - Some Administrative Services Disconnect users after a number of Failed Password attempts
  - These include Winbox, SSH, Telnet etc
  - These Do not include HTTP / HTTPs
Brute Force Detection

- Depends on server disconnection after failed authentication attempts.
- Requires that any one administration session is maintained as continuous established connection.
- Based on some cool ideas from the MT User Community
  - On First Connection (First authentication attempt) add src to Management Light Grey List
  - On Second Connection add src to Management Grey List
  - On Third Connection add src to Management Dark Grey List
  - On Fourth Connection add src to Management Black List
- Then insert Rule to Block members of the Management Black List this List on the Router
Port Scan Timings

- You can slip a scan under the radar
- Slow scan one port per hour
- Very slow scan 1 port per week / 1 port per month
- Find the balance
  - time-out values for port scans are proportional to your paranoia :)

http://wirelessconnect.eu/ Copyright 2007 - 2011
Sending Protocols to bruteforce check

- Send selected protocols to the Brute Force Check Chain
Brute Force Detection

The image shows a firewall configuration window with rules for Brute Force Detection. The highlighted rules include:

1. Rule #122: Action: add src to address list | Chain: BruteForce_Detect
2. Rule #123: Action: add src to address list | Chain: BruteForce_Detect
3. Rule #124: Action: add src to address list | Chain: BruteForce_Detect
4. Rule #125: Action: add src to address list | Chain: BruteForce_Detect
5. Rule #126: Action: accept | Chain: BruteForce_Detect

Each rule is configured to add or accept connections related to IP addresses associated with Brute Force Detection.
Last Rule in Detection Chain

- Accept new connection as long as Src Address is not in the management Black List
External Multi system Response

• MikroTik is so powerful that you can
  – Report Suspicious Traffic back to a central Syslog Server
  – Receive real-time updates from an incident response server.
  – Firewalls effectively sharing data on attack sources and other security threats
  – After analysis of Logs system can push out commands to add people to address lists in multiple mikrotik devices using SSH scripts & SSH Keys
Detection & Reporting

Attacker

Attacker Real IP 1.1.1.1

Internet

MTROS Firewall 1

Suspicious Packets matching FW
Syslog 514 UDP

Syslog Analysis Response Box

Friend or Customer

WebClient

Client Real IP address 2.2.2.2
Denied access to services

http://wirelessconnect.eu/ Copyright 2007 - 2011
Incident Response

Attacker
Attacker Real IP 1.1.1.1

Internet

MTROS
Firewall 1

Suspicious Packets
matching FWV
Syslog 514 UDP

Syslog
Analysis
Response
Server

SSH Push Updates
to all network devices

Friend or Customer

 WebClient

Client Real IP
address 2.2.2.2
Denied access
to services
Further Reading

- For more information on firewall rules click on
- http://wirelessconnect.eu
- Sign up for an account and we will send you instructions for setting up the firewalls and Proxies when they are publicly released after the MUM
- Rules will be released first of May This year.
- http://wiki.mikrotik.com
- http://www.cipherdyne.org/
Thank you

- Thanks to the management team at MikroTik
- Thanks to all the support team at Mikrotik
  - For patiently responding to my emails
- Thanks to all who contribute to the wiki
- Thanks to all who contribute positively to the Wiki
- Thank you for listening