

Building a World Class Cybersecurity Appliance with MikroTik

Presenter: Troy Wilkinson, CISSP, EnCE, MTCTCE
CEO – Axiom Cyber Solutions

Axiom is Exclusively a Cybersecurity Company

- Intrusion Detection & Prevention
- Distributed Denial of Service Mitigation
- Ransomware, Malware, Spam, Virus Detection and Prevention
- Full Management, Configuration, Monitoring, and Reporting
- Vulnerability Scanning, Penetration Testing
- Security Architecture Design and Implementation
- Continuous Updates
- Polymorphic Threat Intelligence Platform

Axiom is Exclusively a MikroTik Shop

- Why MikroTik?
 - Capabilities
 - Price
 - Flexibility of Deployment
 - Ability to Run Scripts
 - Ability to Update Protections with no Degradation
 - Ability to Connect MikroTik to Our Platform
- hEX – Micro Business / SoHo
- RB3011 – Small Business
- CCR-1009/1036 – Medium Business
- CCR-1072 – Large Business / Data Center

Polymorphic Threat Defense Platform

- Core to our offering.
- Polymorphic because it is continuously changing protections
- Cloud based platform that takes in over 100 open and closed sources of threat intelligence and CVE data
- Parses the relevant threat data points such as IP Addresses, Hosts, URLs, Indicators of Compromise, and others
- Deploys those data points in real-time to our network of clients via the MikroTik hardware
- Updates address lists, block lists, regular expression matching, Layer 7 rules, and firewall rules
- Updates 350,000 data points per day to keep ahead of the latest attack vectors
- Averages one update approximately every 10 minutes
- No memory impact or degradation of throughput to the device, to date.
(another good reason to use MikroTik)

Sources

- Spamhaus
- Abuse.CH
- C&C Tracker
- Forkbomb Labs
- Botnet Tracker
- HoneyDB
- MalShare.com
- PhishTank
- SANS.org / SANS ICS
- Verizon
- + many more paid subscription and open source



Data Points

- IP Addresses – Botnet, Ransomware, Malware, etc.
- URLs
- TOR Nodes
- Malicious Domains
- Layer 7 filter rules for Ransomware
Torrent
Malware
Indicators of Compromise



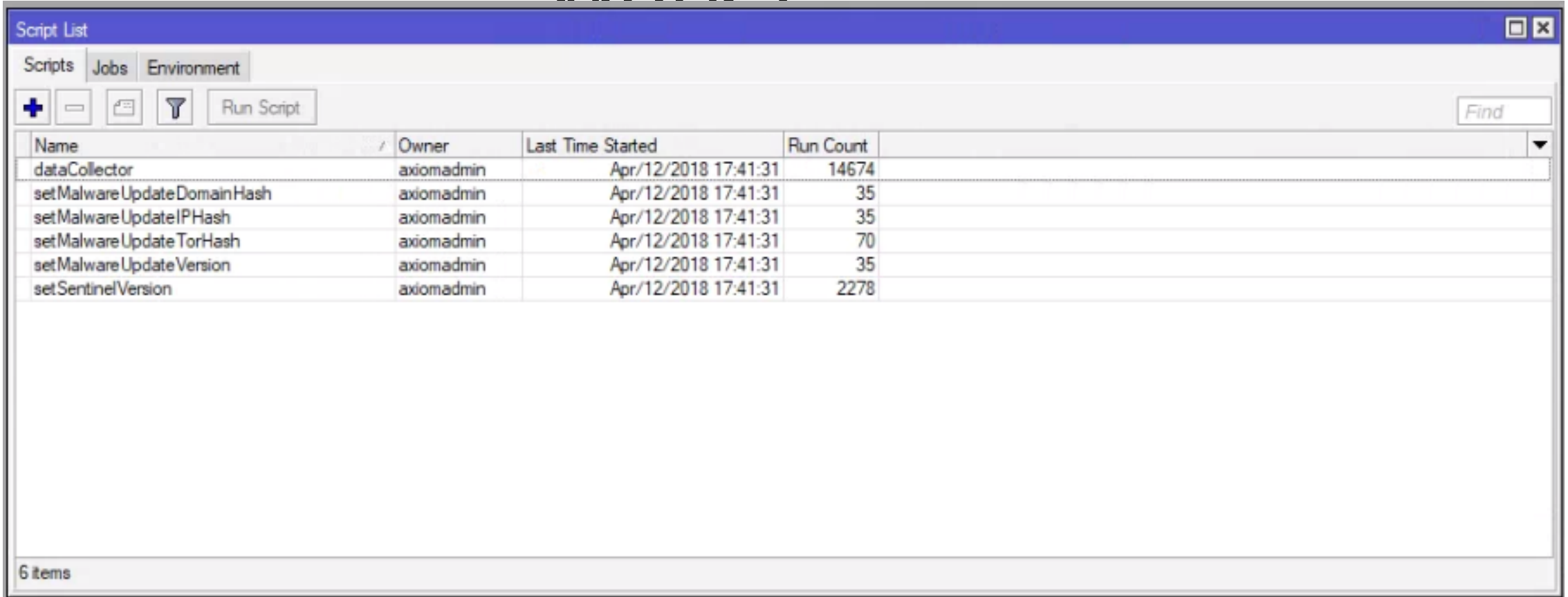
Risk Factor

From the time a vulnerability is disclosed to the world, until you patch against is your risk factor of a breach due to that vulnerability. As time increases so does your risk of a breach.

Updates are crucial. Not just the threat intelligence feeds, but all firewall rules must be dynamic and updated on a frequent basis.

With MikroTik, dynamic firewall rules allow us to add offenders to a custom address list and then take a secondary action such as block for a period of time, tarpit, drop, etc

How It Works



Name	Owner	Last Time Started	Run Count
dataCollector	axiomadmin	Apr/12/2018 17:41:31	14674
setMalwareUpdateDomainHash	axiomadmin	Apr/12/2018 17:41:31	35
setMalwareUpdateIPHash	axiomadmin	Apr/12/2018 17:41:31	35
setMalwareUpdateTorHash	axiomadmin	Apr/12/2018 17:41:31	70
setMalwareUpdateVersion	axiomadmin	Apr/12/2018 17:41:31	35
setSentinelVersion	axiomadmin	Apr/12/2018 17:41:31	2278

6 items

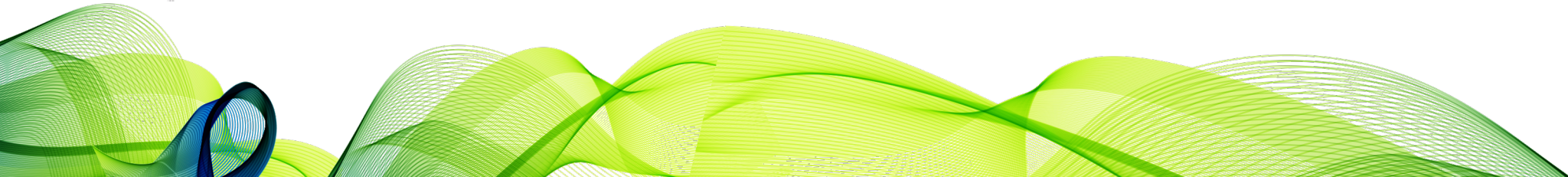
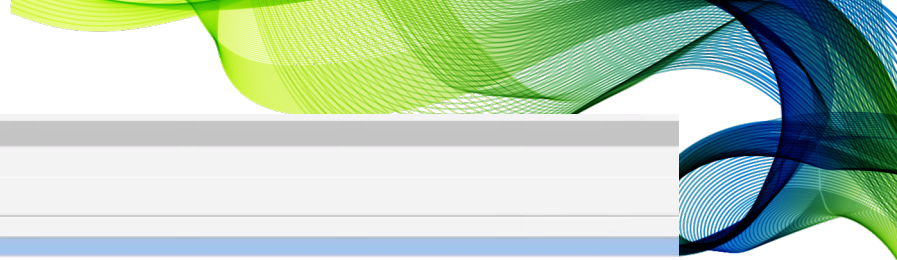
Firewall

Filter Rules NAT Mangle Raw 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	Comment
0	tarpit	input			6 (tcp)					0 B	0	AX001 - Packet Trap
1	drop	input			17 (u...		53	ether1		5.4 KiB	87	AX034 - Drop external DNS - UDP
2	drop	input			6 (tcp)		53	ether1		1188 B	27	AX035 - Drop external DNS - TCP
3	add...	input			6 (tcp)					0 B	0	AX002 - Connection Limit
4	drop	input								0 B	0	AX003 - Drop Chromecast Hack Vector
5	add...	input			6 (tcp)					0 B	0	AX004 - Add Syn Flood IP to the list
6	drop	input								0 B	0	AX005 - Drop to syn flood list
7	add...	input			6 (tcp)					1400 B	35	AX006 - Port Scanner Detect
8	drop	output			6 (tcp)	80				0 B	0	AX007 - Drop Access to WebUI
9	drop	input								2240 B	56	AX008 - Drop to port scan list
10	jump	output			1 (ic...					10.1 MB	73 250	AX009 - Jump for icmp output
11	jump	input			1 (ic...					8.2 MB	52 986	AX010 - Jump for icmp input flow
12	drop	input			6 (tcp)		8291			16.1 KiB	412	AX011 - Block all access to the Sentinel- except to support list # DO NOT ENABLE THIS RULE BEFORE ADD YOUR SUBNET IN THE SUPPORT ADDRESS LIST
13	jump	forward			1 (ic...					10.2 MB	126 042	AX012 - Jump for icmp forward flow
14	drop	forward								0 B	0	AX013 - Drop to bogon list
15	drop	forward								0 B	0	AX036 - Drop to ransomware list
16	drop	forward								0 B	0	AX037 - Drop to TOR list
17	add...	forward			6 (tcp)		25,587			0 B	0	AX014 - Add Spammers to the list for 3 hours
18	drop	forward			6 (tcp)		25,587			0 B	0	AX015 - Avoid spammers action
19 X	acc...	input			17 (u...					0 B	0	Accept DNS - UDP
20 X	acc...	input			6 (tcp)					0 B	0	Accept DNS - TCP
21	acc...	input			6 (tcp)					14.2 MB	186 766	AX016 - Accept to established connections
22	acc...	input			6 (tcp)					0 B	0	AX017 - Accept to related connections
23	acc...	input								32.1 MB	149 186	AX018 - Full access to SUPPORT address list
24	acc...	input			17 (u...	53				272.3 KiB	3 359	Allows DNS Query from Router.
25	drop	forward								0 B	0	AX040 - Drop to Manual BlockList
26	drop	input								11.8 MB	90 225	AX019 - Drop anything else! # DO NOT ENABLE THIS RULE BEFORE YOU MAKE SURE ABOUT ALL ACCEPT RULES YOU NEED
27	acc...	ICMP			1 (ic...					10.5 MB	95 836	AX020 - Echo request - Avoiding Ping Flood
28	acc...	ICMP			1 (ic...					10.3 MB	92 367	AX021 - Echo reply
29	acc...	ICMP			1 (ic...					12.4 KiB	183	AX022 - Time Exceeded
30	acc...	ICMP			1 (ic...					3238.2 KiB	21 250	AX023 - Destination unreachable
31	acc...	ICMP			1 (ic...					2520 B	45	AX024 - PMTUD
32	drop	ICMP			1 (ic...					4544.8 KiB	42 597	AX025 - Drop to the other ICMPs
33	drop	forward								10.4 KiB	11	AX026 - L7 Drop All Connections to Torrent Sites
34	drop	forward			17 (u...		53			0 B	0	AX027 - DNS Drop DNS Requests to Torrent domains
35	drop	forward								772.8 KiB	573	AX028 - DPI Torrent Deep Packet Inspection Drop
36 X	drop	forward								0 B	0	AX029 - DPI Hash Trackers Drop
37	drop	forward								0 B	0	AX030 - DPI Drop all GETPEERS Requests
38	drop	forward								0 B	0	AX031 - DPI Drop all INFO_HASH requests
39	drop	forward								0 B	0	AX032 - DPI Drop all ANNOUNCE_PEER requests
40	drop	forward								320 B	5	AX033 - DPI Drop P2P Protocols



Firewall			
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols			
+ - ✓ ✗ 📁 🔍			
Name	/	Address	Timeout
ransomware	/	149.202.109.202	
ransomware	/	149.202.52.215	
ransomware	/	151.236.14.51	
ransomware	/	151.236.15.226	
ransomware	/	158.255.6.109	
ransomware	/	158.255.6.115	
ransomware	/	158.69.223.5	
ransomware	/	164.132.40.47	
ransomware	/	176.107.185.19	
ransomware	/	176.121.14.95	
ransomware	/	176.31.47.100	
ransomware	/	176.53.21.105	
ransomware	/	176.9.172.166	
ransomware	/	178.62.232.244	
ransomware	/	178.63.238.185	
ransomware	/	185.100.85.150	
ransomware	/	185.102.136.67	
ransomware	/	185.102.136.77	
ransomware	/	185.106.122.38	
ransomware	/	185.115.140.170	
ransomware	/	185.117.153.176	
ransomware	/	185.117.72.105	
ransomware	/	185.117.72.94	
ransomware	/	185.127.25.176	

Firewall			
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols			
+ - ✓ ✗ 📁 🔍			
Name	/	Address	Timeout
tor_nodes	/	185.220.101.9	
tor_nodes	/	185.222.202.104	
tor_nodes	/	185.222.202.12	
tor_nodes	/	185.222.209.32	
tor_nodes	/	185.225.68.13	
tor_nodes	/	185.227.68.250	
tor_nodes	/	185.227.82.9	
tor_nodes	/	185.234.218.251	
tor_nodes	/	185.24.216.42	
tor_nodes	/	185.31.136.244	
tor_nodes	/	185.34.33.2	
tor_nodes	/	185.35.138.92	
tor_nodes	/	185.56.80.242	
tor_nodes	/	185.58.226.243	
tor_nodes	/	185.62.189.76	
tor_nodes	/	185.62.57.91	
tor_nodes	/	185.65.205.10	
tor_nodes	/	185.66.200.10	
tor_nodes	/	185.72.244.24	
tor_nodes	/	185.80.130.234	
tor_nodes	/	185.82.216.233	
tor_nodes	/	185.83.215.22	
tor_nodes	/	185.86.148.90	
tor_nodes	/	185.86.151.21	

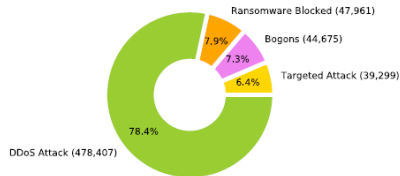
Axiom Reporting Portal



Reporting Period: 01/01/2018 - 01/31/2018

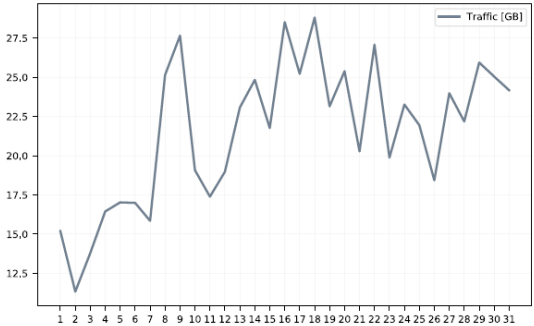
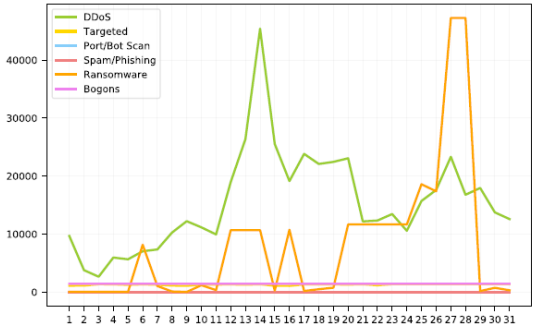
Dear Client,

This month, your Axiom SecureAmerica® firewall (Firewal Name) inspected 687.85 GB of traffic.

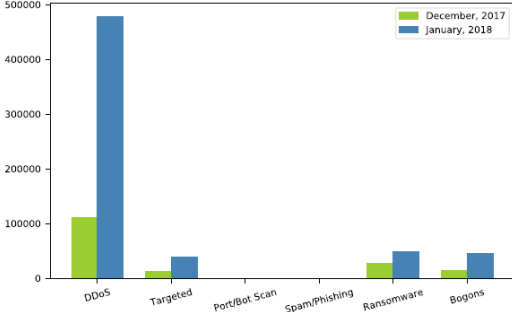


Attack Type	Frequency
DDoS Attack	478,407
Targeted Attack	39,299
Ransomware	47,961
Port/Bot Scan	0
Spam/Phishing	0
Bogons	44,675

Monthly Attacks and Total Traffic



Last Month vs Current Month



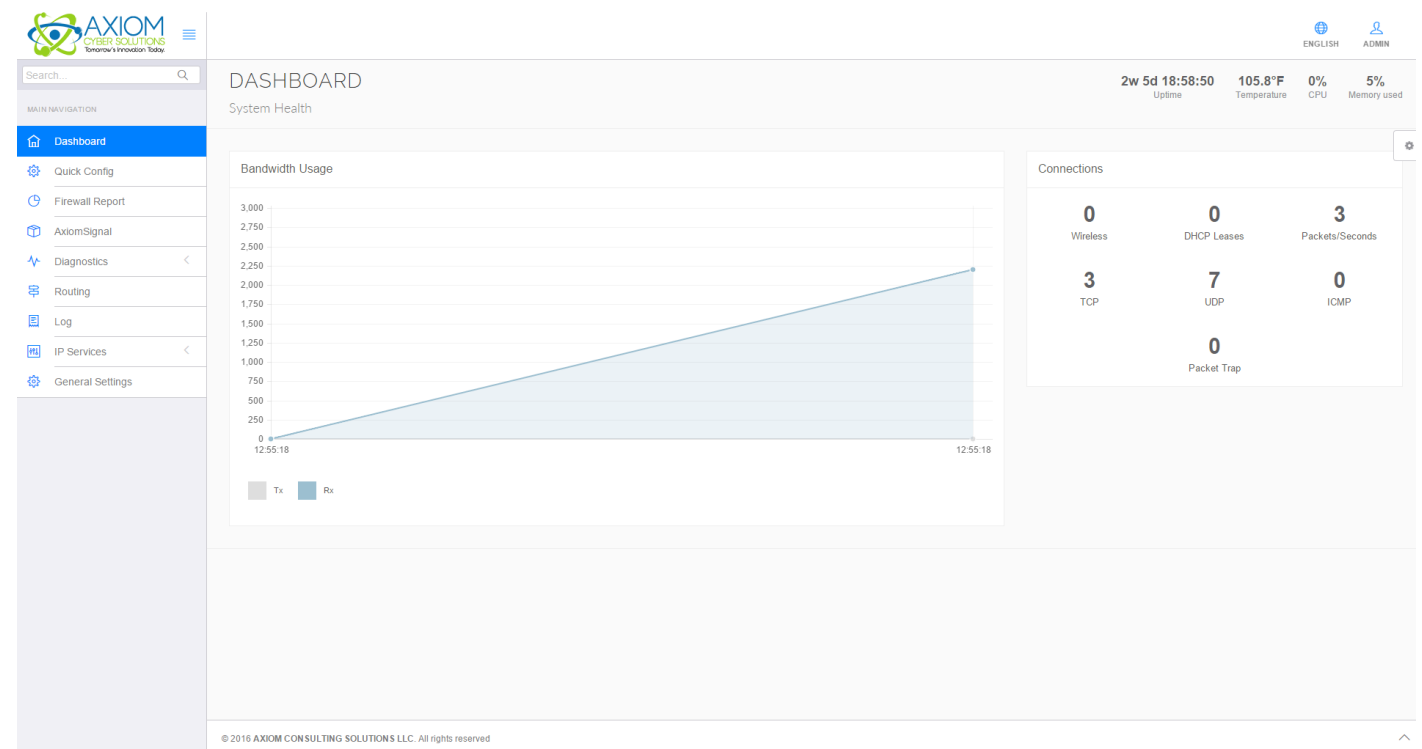
DDoS – Distributed Denial of Service. This is when your firewall sees a traffic flood and blocks suspected traffic. Traffic floods occur more often than you think. Because they often come in low volumes, you may or may not see the effects on your network. Hackers use these as “probes” to test networks and infrastructure for vulnerabilities. The Axiom firewall is designed to absorb these and not reply. This leaves the attacker no information helping your business stay invisible.

Targeted Attack – This is when someone puts in your IP address for a specific attack. This could be many different vectors such as SQL Injection attempt, Cross Site Scripting attempt or a vulnerability scanner. This generally happens with someone has scanned and found your IP with the Bot Scan or they have found your IP from email or web response. In any event, the Axiom firewall will block these attacks. The Axiom firewall keeps track of these offenders and will block them after several attempts.

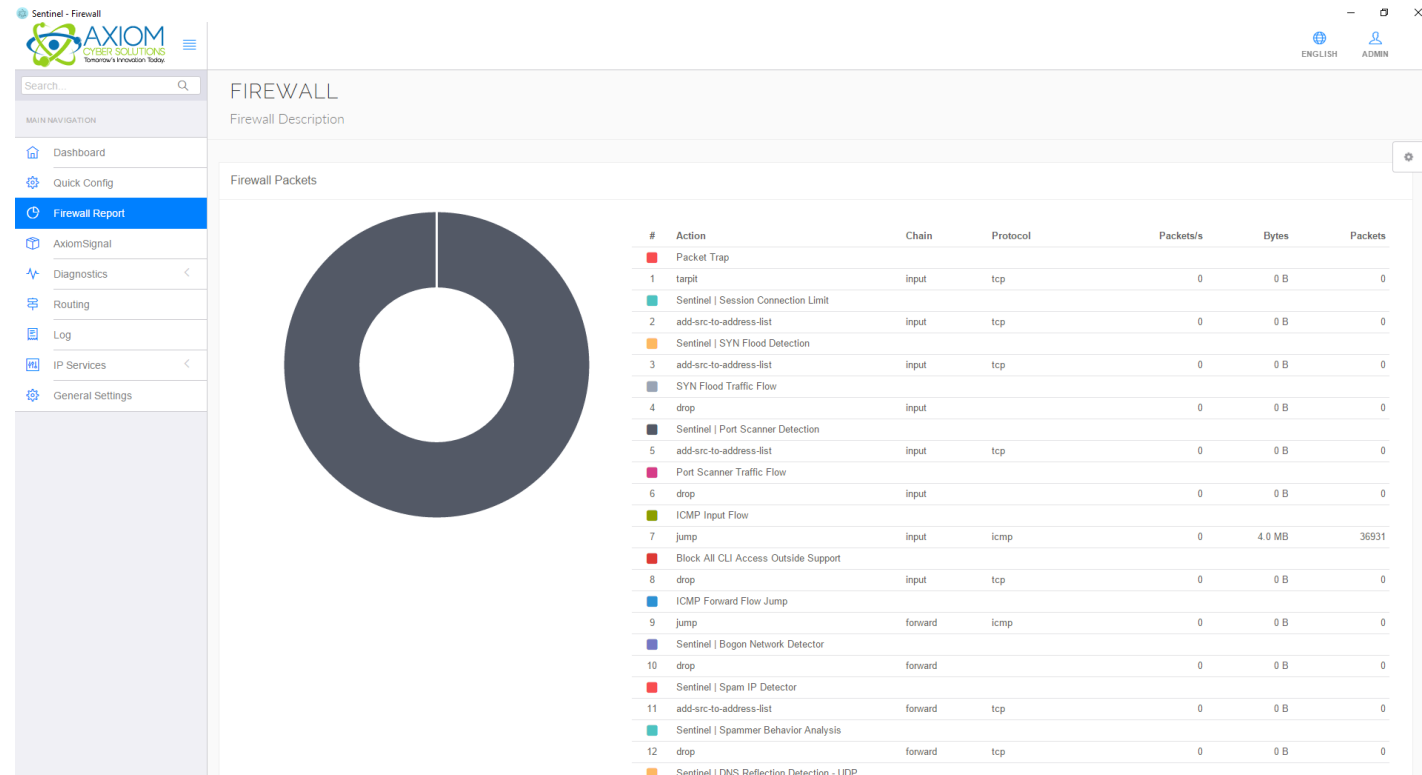
Ransomware – This is when Ransomware has been activated on your network and is reaching out for the encryption key exchange. Ransomware malware makes hundreds, if not thousands of calls out of the business and this number represents the number of packets blocked. This is targeting a specific protocol that Ransomware must have to activate.

Port / Bot Scan – This is when servers or bots on the internet are scanning for open ports or known devices on IP ranges. Each day, thousands of servers (both legitimate and illegitimate) are scanning

Axiom Dashboard – General Statistics



Axiom Dashboard – Firewall Stats



PRIVILEGED AND CONFIDENTIAL

Axiom Dashboard – Advanced Packet Level Diagnostics

The screenshot displays the Axiom Dashboard interface for the TORCH (Realtime traffic monitoring tool). The left sidebar contains a 'MAIN NAVIGATION' menu with options: Dashboard, Quick Config, Firewall Report, AxiomSignal, Diagnostics (selected), Torch, Ping, Traceroute, Routing, Log, IP Services, and General Settings. The top right corner shows 'Sentinel - Torch', 'AXIOM CYBER SOLUTIONS', and user options for 'ENGLISH' and 'ADMIN'.

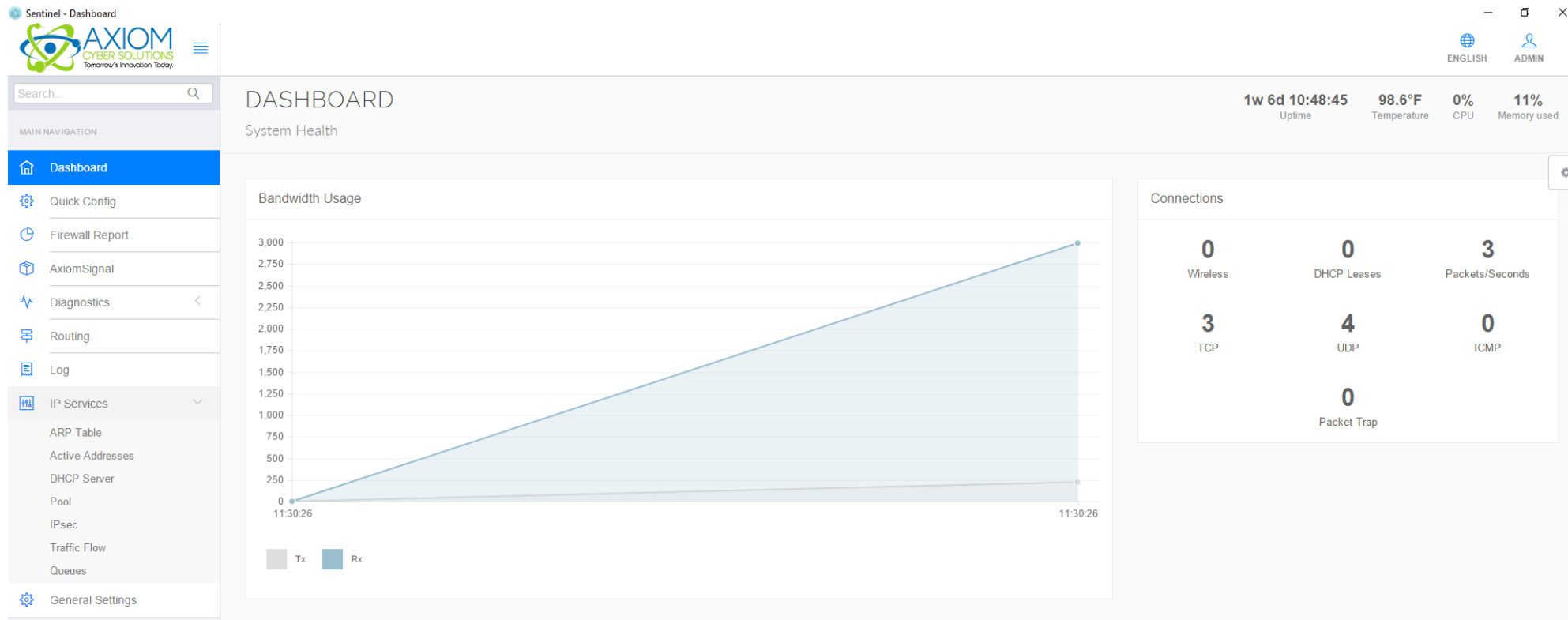
The main content area is titled 'TORCH Realtime traffic monitoring tool'. It features a 'Basic' configuration section with an 'Interface' dropdown set to 'ether1'. Below this is a 'Collect' section with checkboxes for 'Src. Address' (checked), 'Dst. Address' (checked), 'MAC Protocol', 'Protocol', 'Port', and 'VLAN Id'. To the right is a 'Filters' section with dropdowns for 'Source Address' (0.0.0.0/0), 'Destination Address' (0.0.0.0/0), 'MAC Protocol' (any), 'Protocol' (any), 'Port' (any), and 'VLAN Id' (any). 'Start' and 'Stop' buttons are located below the 'Collect' section.

At the bottom, a table displays traffic statistics:

Protocol	Src	Dst	Tx Rate	Rx Rate	Tx Packets	Rx Packets
0 items						
Total Tx: 0 B/s		Total Rx: 0 B/s		Total Tx Packets: 0		Total Rx Packets: 0

PRIVILEGED AND CONFIDENTIAL

Axiom Dashboard – IP Services Menu



Axiom Shield

- Works with MikroTik RouterOS
 - Compatible to 6.2x versions ... but you really need to update to the latest available version!
- Access to Axiom's Polymorphic Threat Defense System
 - Packages Start at \$50/month for dynamic rules & updates



PRIVILEGED AND CONFIDENTIAL