AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

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)

AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

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

AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

Data Points

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

AXIOM CYBER SOLUTIONS
Tomorrow's Innovation Today

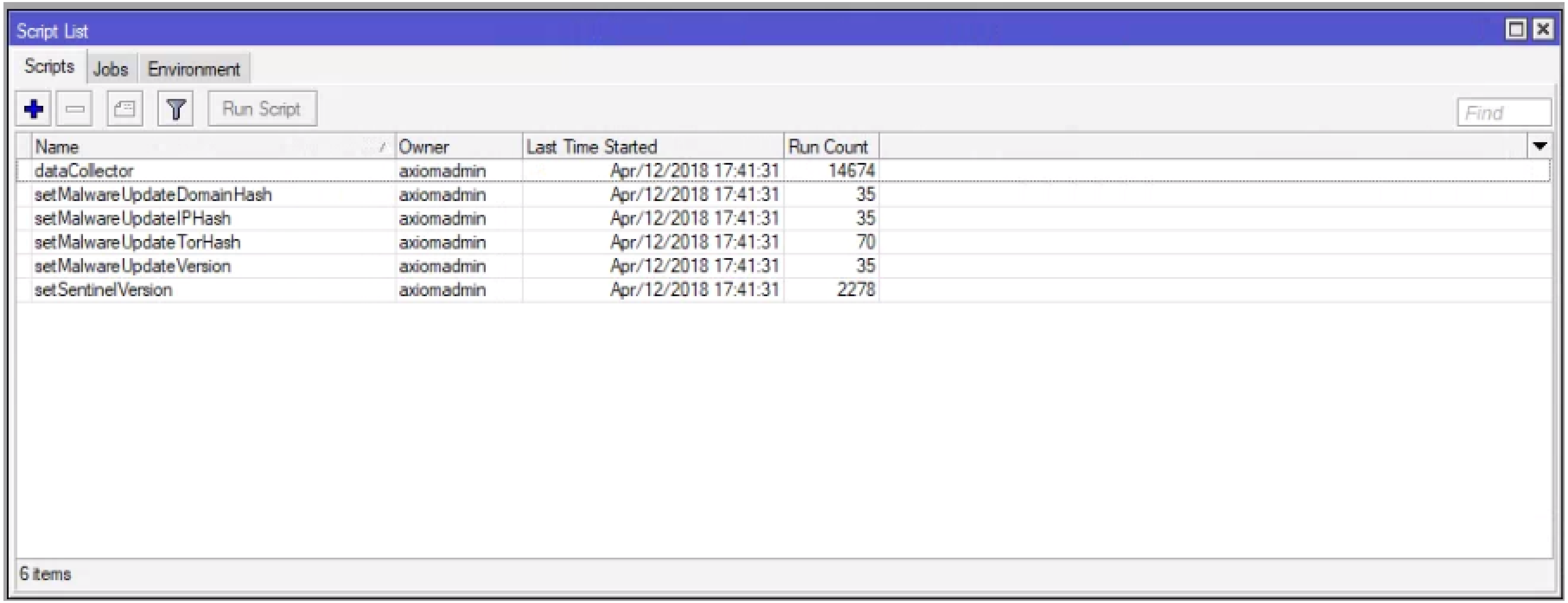
Risk Factor

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

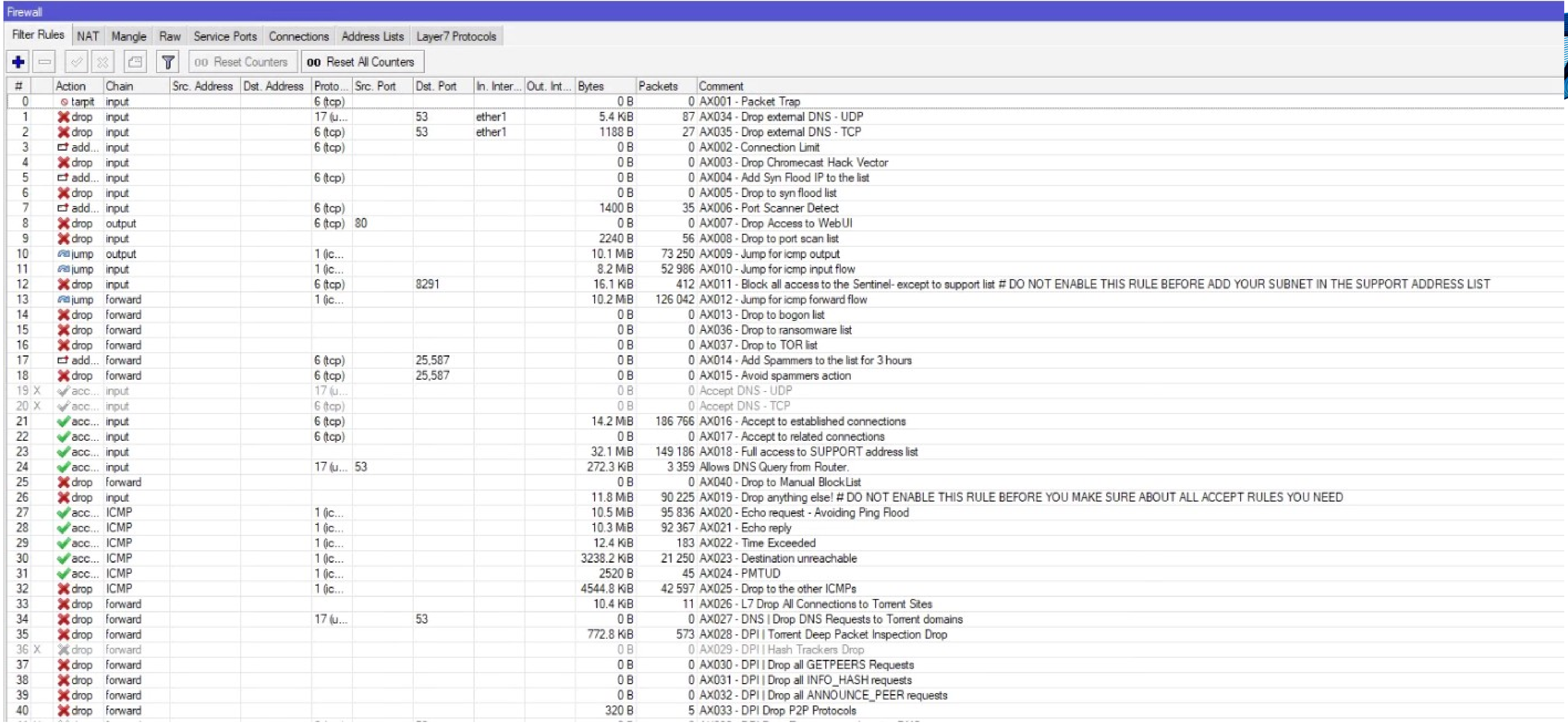
How It Works



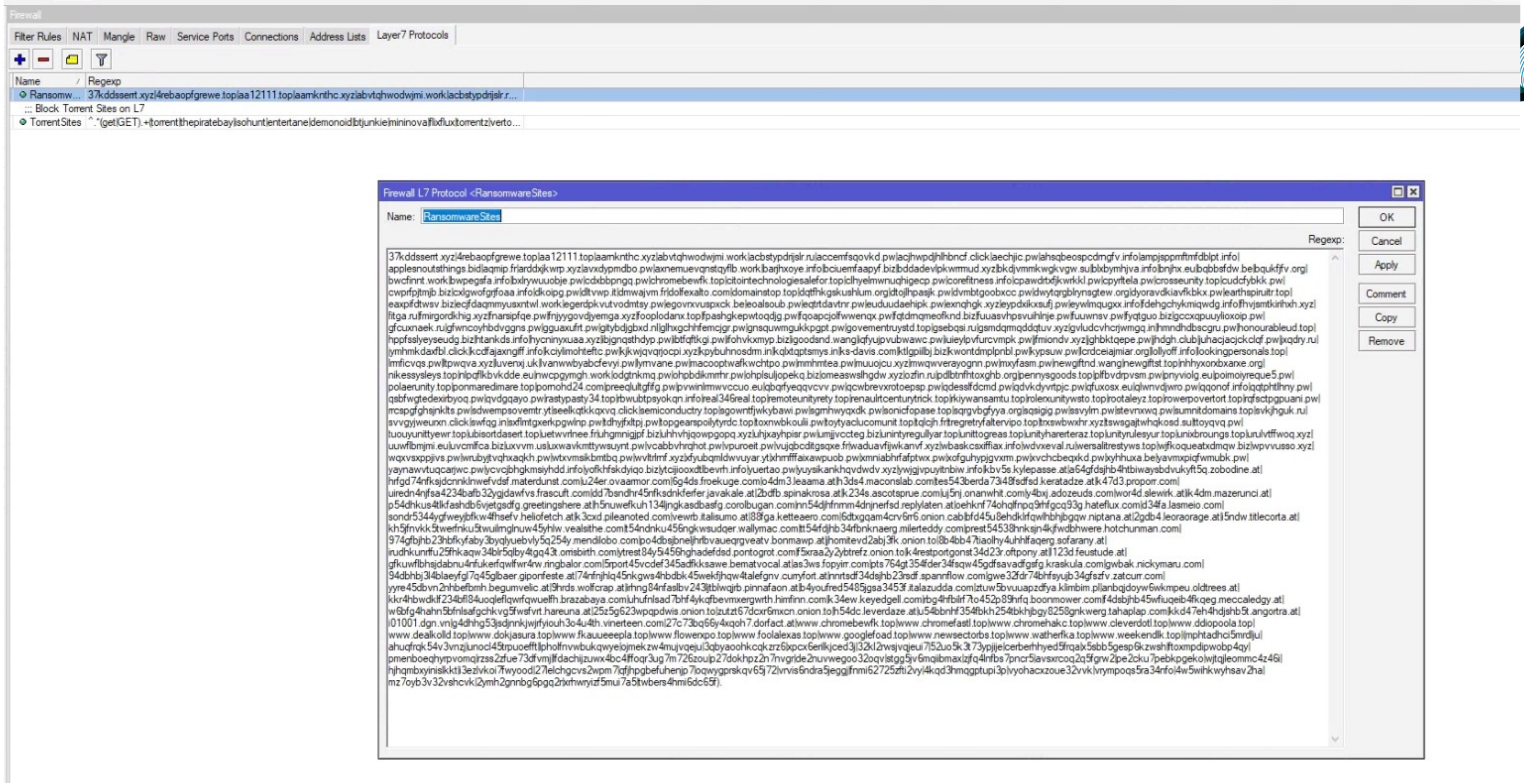
Name	Owner	Last Time Started	Run Count
dataCollector	axiomadmin	Apr/12/2018 17:41:31	14674
setMalwareUpdateDomainHash	axiomadmin	Apr/12/2018 17:41:31	35
setMalwareUpdateIPHash	axiomadmin	Apr/12/2018 17:41:31	35
setMalwareUpdateTorHash	axiomadmin	Apr/12/2018 17:41:31	70
setMalwareUpdateVersion	axiomadmin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

6 items

AXIOM CYBER SOLUTIONS
Tomorrow's Innovation Today



#		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 MiB	73 250	AX009 - Jump for icmp output
11		jump	input			1 (ic...					8.2 MiB	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 MiB	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 MiB	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 MiB	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 MiB	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 MiB	95 836	AX020 - Echo request - Avoiding Ping Flood
28		acc...	ICMP			1 (ic...					10.3 MiB	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

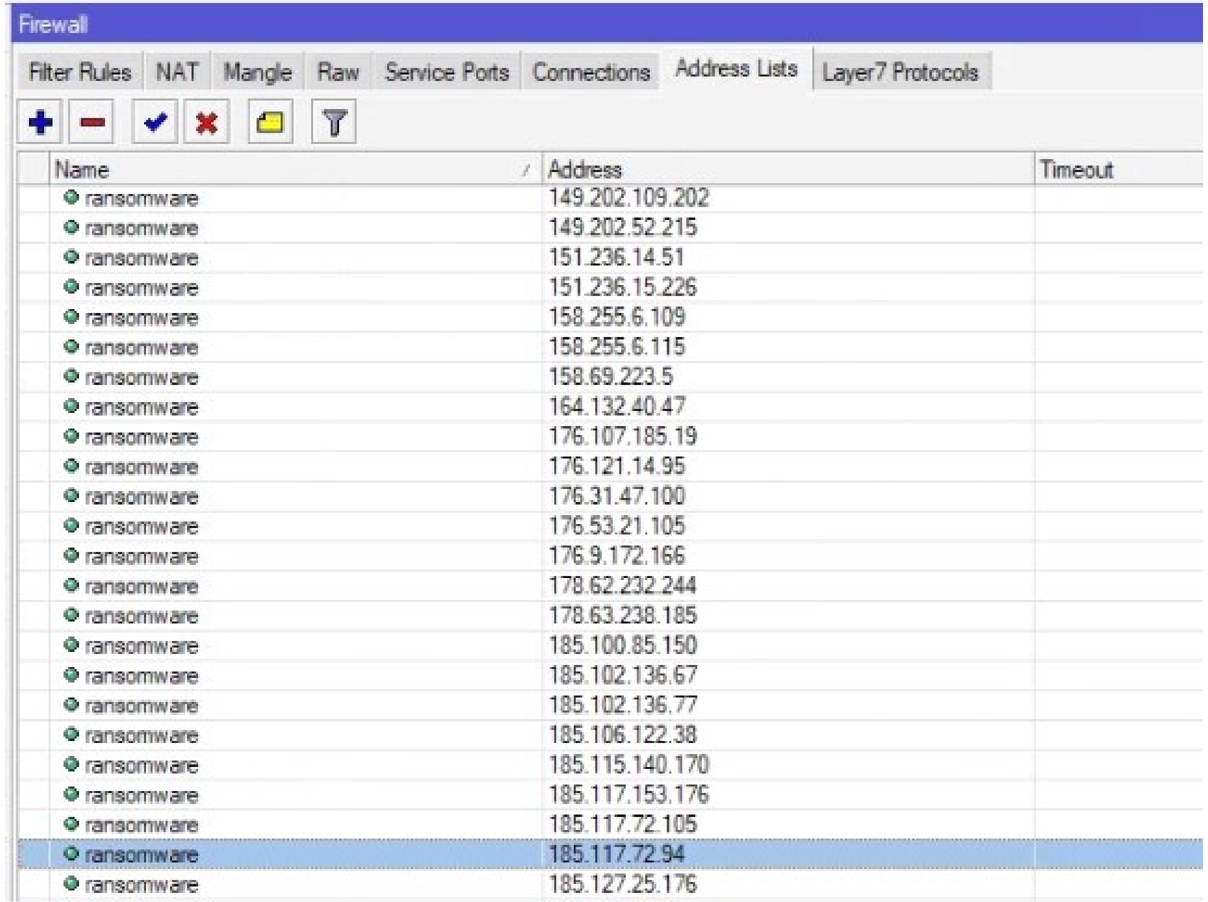


Name	Regexp
Ransomw...	37kddssert.xyz|4rebaopfgrewe.top|aa12111.top|aamknthc.xyz|abvtqhwodwjmi.work|acbstypdrijslr.r...
::: Block Torrent Sites on L7	
TorrentSites	^.*(get|GET).+(torrent|thepiratebay|isohunt|entertane|demonoid|btjunkie|mininova|flixflux|torrentz|verto...

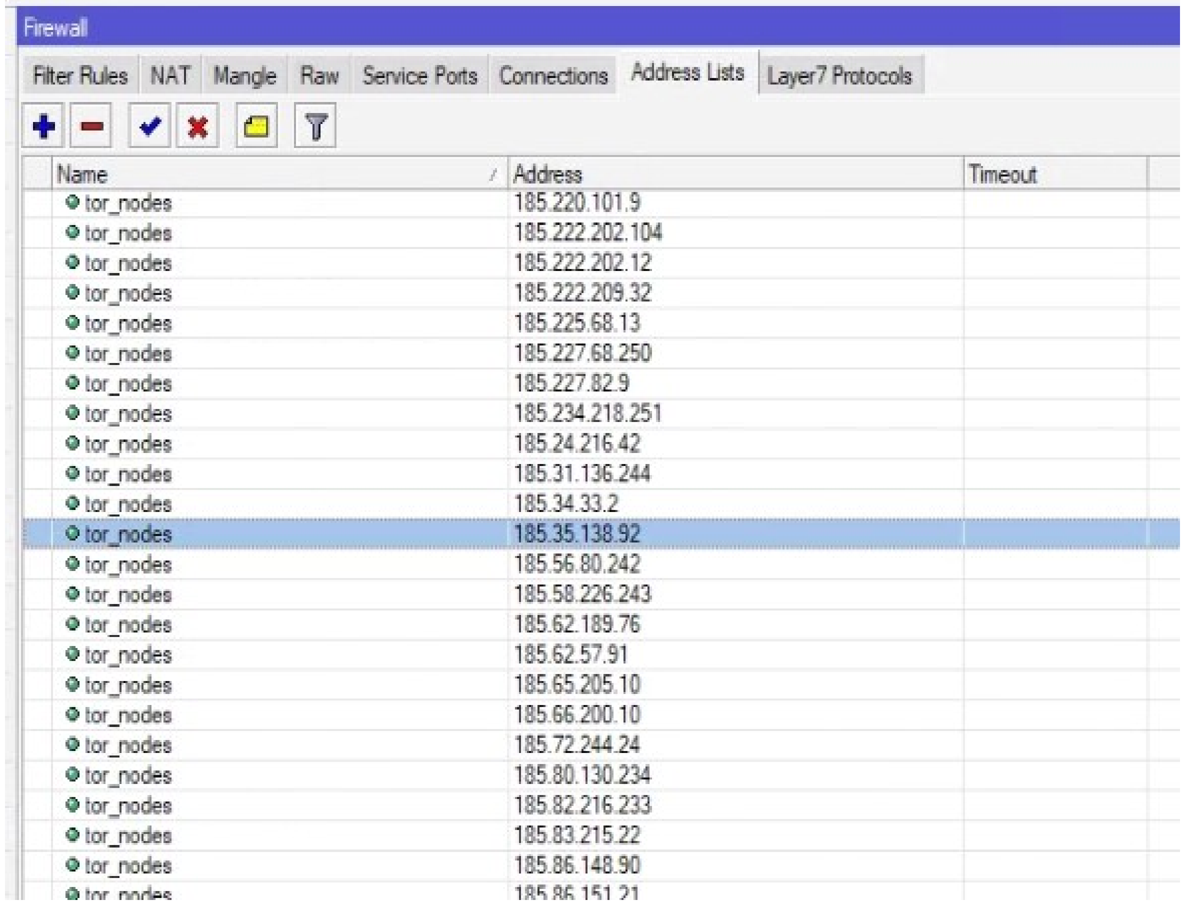
Name: RansomwareSites

Regexp:

```
37kddssert.xyz|4rebaopfgrewe.top|aa12111.top|aamknthc.xyz|abvtqhwodwjmi.work|acbstypdrijslr.ru|accemfsqovkd.pw|acjhwpdjhlhbncf.click|aechjic.pw|ahsqbeospcdmgfv.info|ampjsppmftmfdblpt.info|
applesnoutsthings.bid|aqmip.fr|arddxjkwrp.xyz|avxdypmdbo.pw|axnemuevqnstqyflb.work|barjhxoye.info|bciuemfaapyf.biz|bddadevlpkwrmud.xyz|bkdjvmmkwgkvgw.su|blxbymhjva.info|bnjhx.eu|bqbbsfdw.be|bqukfjfv.org|
bwcfinnt.work|bwpegsfa.info|bxlrywuuobje.pw|cdxbbpngq.pw|chromebewfk.top|citointechnologiesalefor.top|clhyelmwnuqhigecp.pw|corefitness.info|cpawdrtxfjkwrkkl.pw|cpyrltela.pw|crosseunity.top|cudcfybkk.pw|
cwprfpjtmjb.biz|cxlgwofgrjfoaa.info|dkoipg.pw|dltvwp.it|dmwajvm.fr|dolfexalto.com|domainstop.top|dqtfhkgskushlum.org|dtojlhpasjk.pw|dvmbtgoobxcc.pw|dwytqrgblrynsgtew.org|dyoravdkiavfkbkx.pw|earthspiruitr.top|
eaxpifdtwsv.biz|ecjfdaqmmyusxntwl.work|egerdpkvutvodmtsy.pw|egovrxvuspxck.be|eoalsoub.pw|eqtrtdavtnr.pw|euduudaehipk.pw|exnqhgk.xyz|eypdxikxsufj.pw|eywlmqugxx.info|fdehgchykmiqwdg.info|fhvjsmtkirihxh.xyz|
fitga.ru|fmirgordkhig.xyz|fnarsipfqe.pw|fnjyygovdjyemga.xyz|fooplodanx.top|fpashgkepwtoqdjg.pw|fqoapcjolfwwenqx.pw|fqtdmqmeofknd.biz|fuuasvhpsvuihlnje.pw|fuuwnsv.pw|fyqtguo.biz|gccxqpuuylioxoip.pw|
gfcuxnaek.ru|gfwncoyhbdvggns.pw|gguaxufrt.pw|gitybdjgbxd.nl|glhxgchhfemcjgr.pw|gnsquwmgukkpgpt.pw|govementruystd.top|gsebqsi.ru|gsmdqrmqddqtuv.xyz|gvludcvhcrjwmgq.in|hmndhdbscgru.pw|honourableud.top|
hppfsslyeyseudg.biz|htankds.info|hycninyxuaa.xyz|ibjgnqsthdyp.pw|ibtfqftkgi.pw|ifohvkxmyp.biz|igoodsnd.wang|iqfyujpvubwawc.pw|iuieylpvfurcvmpk.pw|jfmiondv.xyz|jghbktqepe.pw|jhdgh.club|juhacjacjckclqf.pw|jxqdry.ru|
jymhmkdaxfbl.click|kcdfajaxngiff.info|kciylimohteftc.pw|kjkwjqvqrjocpi.xyz|kpybuhnosdm.in|kqlxtqptsmys.in|ks-davis.com|ktlgpiilbj.biz|kwontdmplpnbl.pw|kypsuw.pw|lcrdceiajmiar.org|lollyoff.info|lookingpersonals.top|
lmficvqs.pw|ltpwqva.xyz|luvenxj.uk|lvanwwbyabcfevyi.pw|lymvane.pw|macooptwafkwchtpo.pw|mmhmtea.pw|muuojcu.xyz|mwqwverayognn.pw|mxyfasm.pw|newgiftnd.wang|newgiftst.top|nhhyxorxbxarxe.org|
nikessysleys.top|nlpqflkbvkdde.eu|nwcpgymgh.work|odgtnkmq.pw|ohpbdikmrrhr.pw|ohplsuljopekq.biz|omeaswslhgdw.xyz|ozfin.ru|pdlbtnfhtoxghb.org|pennysgoods.top|plfbvdrpvsm.pw|pnyviolg.eu|poimoiyreque5.pw|
polaerunity.top|ponmaredimare.top|pornohd24.com|preeqlultgffg.pw|pvwinlmwvccuo.eu|qbqrfyeqqvcvv.pw|qcwbrevxrotoepsp.pw|qdesslfdcmd.pw|qdvkdyvrtpjc.pw|qfuxosx.eu|qlwnvdjwro.pw|qqonof.info|qqtphtlhny.pw|
qsbfwgtedexirbyoq.pw|qvdgqayo.pw|rastypasty34.top|rbwubtpsyokqn.info|real346real.top|remoteunityrety.top|renaulrtcenturytrick.top|rkiywansamtu.top|rolerxunitywsto.top|rootaleyz.top|rowerpovertort.top|rqfsctpgpuani.pw|
rcspgfghsjnklts.pw|sdwempsovemtr.yt|seelkqtkkqxvq.click|semiconductry.top|sgowntfjwkybawi.pw|sgmhwyqxdk.pw|sonicfopase.top|sqrgvbgfyya.org|sqsigig.pw|ssvylm.pw|stevnxwq.pw|sumnitdomains.top|svkjhguk.ru|
svvgyjweurxn.click|swfqg.in|sxflmtgxerkpgwlnp.pw|tdhyjfxltpj.pw|topgearspoilytyrdc.top|toxnwbkoulii.pw|toytyaclucomunit.top|tqlcjh.fr|tregretryfaltervipo.top|trxswbwxhr.xyz|tswsgajtwhqkosd.su|ttoyqvq.pw|
tuouyunittyewr.top|ubisortdasert.top|uetwvrlnee.fr|uhgmnigjpf.biz|uhhvhjqowpgopq.xyz|uhjxayhpisr.pw|umjjvccteg.biz|unintyregullyar.top|unittogreas.top|unityharerteraz.top|unityrulesyur.top|unixbroungs.top|urulvtffwoq.xyz|
uuwflbmjmi.eu|uvcmlfca.biz|uxvvm.us|uxwavkmttywsuynt.pw|vcabbvhrqhot.pw|vpuroeit.pw|vujqbcditgsqxe.fr|waduavfijwkanvf.xyz|wbaskcsxiffiax.info|wdvxeval.ru|wersalitrestyws.top|wjfkoqueatxdmqw.biz|wpvvusso.xyz|
wqxvsxppjivs.pw|wrubyjtvqhxaqkh.pw|wtxvmsikbmtbq.pw|wvltrlmf.xyz|xfyubqmldwvuyar.yt|xhmfffaixawpuob.pw|xmniabhrfafptwx.pw|xofguhypjgvxrm.pw|xvchcbeqxkd.pw|xyhhuxa.be|yavmxpiqfwmubk.pw|
yaynawvtuqcarjwc.pw|ycvcjbhgkmsiyhdd.info|yofkhfskdyiqo.biz|ytcijiooxdtlbevrh.info|yuertao.pw|yuysikankhqvdwdv.xyz|ywjgjvpuyitnbiw.info|kbv5s.kylepasse.at|a64gfdsjhb4htbiwaysbdvukyft5q.zobodine.at|
hrfgd74nfksjdcnnklnwefvdsf.materdunst.com|u24er.ovaamor.com|6g4ds.froekuge.com|o4dm3.leaama.at|h3ds4.maconslab.com|tes543berda73i48fsdfsd.keratadze.at|k47d3.proporr.com|
uiredn4njfsa4234bafb32ygjdawfvs.frascuft.com|dd7bsndhr45nfksdnkferfer.javakale.at|2bdfb.spinakrosa.at|k234s.ascotsprue.com|uj5nj.onanwhit.com|y4bxj.adozeuds.com|wor4d.slewirk.at|ik4dm.mazerunci.at|
p54dhkus4tlkfashdb6vjetgsdfg.greetingshere.at|h5nuwefkuh134ljngkasdbasfg.corolbugan.com|nn54djhfnmm4dnjnerfsd.replylaten.at|oehknf74ohqlfnpq9rhfgcq93g.hateflux.com|d34fa.lasmeio.com|
sondr5344ygfweyjbfkw4fhsefv.heliofetch.at|k3cxd.pileanoted.com|vewrb.italisumo.at|88fga.ketteaero.com|6dtxgqam4crv6rr6.onion.cab|bfd45u8ehdklrfqwlhbhjbgqw.niptana.at|2gdb4.leoraorage.at|i5ndw.titlecorta.at|
kh5jfnvkk5twerfnku5twuilmglnuw45yhlw.vealsithe.com|t54ndnku456ngkwsudqer.wallymac.com|tt54rfdjhb34rfbnknaerg.milerteddy.com|prest54538hnksjn4kjfwdbhwere.hotchunman.com|
974gfbjhb23hbfkyfaby3byqlyuebvly5q254y.mendilobo.com|po4dbsjbnejhrlbvaueqrgveatv.bonmawp.at|jhomitevd2abj3fk.onion.to|8b4bb47tiaolhy4uhhlfaqerg.sofarany.at|
irudhkunrlfu25fhkaqw34blr5qlby4tgq43t.omisbirth.com|ytrest84y5i456hghadefdsd.pontogrot.com|f5xraa2y2ybtrefz.onion.to|k4restportgonst34d23r.oftpony.at|l123d.feustude.at|
gfkuwflbhsjdabnu4nfukerfqwlfwr4rw.ringbalor.com|5rport45vcdef345adfkksawe.bematvocal.at|as3ws.fopyirr.com|pts764gt354fder34fsqw45gdfsavadfgsfg.kraskula.com|gwbak.nickymaru.com|
94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at|74nfnjhlq45nkgws4hbdbk45wekfjhqw4talefgnv.curryfort.at|nnrtsdf34dsjhb23rsdf.spannflow.com|gwe32fdr74bhfsyujb34gfszfv.zatcurr.com|
yyre45dbvn2nhbefbmh.begumvelic.at|9hrds.wolfcrap.at|irhng84nfaslbv243ljtblwqjrb.pinnafaon.at|b4youfred5485jgsa3453f.italazudda.com|ztuw5bvuuapzdfya.klimbim.pl|anbqjdoyw6wkmpeu.oldtrees.at|
kkr4hbwdklf234bfl84uoqleflqwrfqwuelfh.brazabaya.com|uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com|k34ew.keyedgell.com|rbg4hfbilrf7to452p89hrfq.boonmower.com|f4dsbjhb45wfiuqeib4fkqeg.meccaledgy.at|
w6bfg4hahn5bfnlsafgchkvg5fwsfvrt.hareuna.at|25z5g623wpqpdwis.onion.to|zutzt67dcxr6mxcn.onion.to|h54dc.leverdaze.at|u54bbnhf354fbkh254tbkhjbgy8258gnkwerg.tahaplap.com|kkd47eh4hdjshb5t.angortra.at|
i01001.dgn.vn|g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com|27c73bq66y4xqoh7.dorfact.at|www.chromebewfk.top|www.chromefastl.top|www.chromehakc.top|www.cleverdotl.top|www.ddiopoola.top|
www.dealkolld.top|www.dokjasura.top|www.fkauueeepla.top|www.flowerxpo.top|www.foolalexas.top|www.googlefoad.top|www.newsectorbs.top|www.watherfka.top|www.weekendlk.top|lmphtadhci5mrdju|
ahuqfrqk54v3vnzj|unocl45trpuoefft|lpholfnvwbukqwye|ojmekzw4mujvqeju|3qbyaoohkcqkzrz6|xpcx6erlkjced3j|32kl2rwsjvqjeui7|52uo5k3t73ypjije|cerberhhyed5frqa|x5sbb5gesp6kzwsh|ftoxmpdipwobp4qy|
pmenboeqhyrpvomq|rzss2zfue73dfvmj|lfdachijzuwx4bc4|ffoqr3ug7m726zou|p27dokhpz2n7nvgr|de2nuvwegoo32oqv|stgg5jv6mqiibmax|zjfq4lnfbs7pncr5|avsxrcoq2q5fgrw2|pe2cku7pebkpgeko|wjtqjleommc4z46i|
hjhqmbxyinislkkt|i3ezlvkoi7fwyood|27lelchgcvs2wpm7|qfjhpgbefuhenjp7|oqwygprskqv65j72|vrvis6ndra5jeggj|fnmi62725zfti2vy|4kqd3hmqgptupi3p|vyohacxzoue32vvk|vrympoqs5ra34nfo|4w5wihkwyhsav2ha|
mz7oyb3v32vshcvk|2ymh2gnnbg6pgq2r|xrhwryizf5mui7a5|twbers4hmi6dc65f).
```



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	



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	

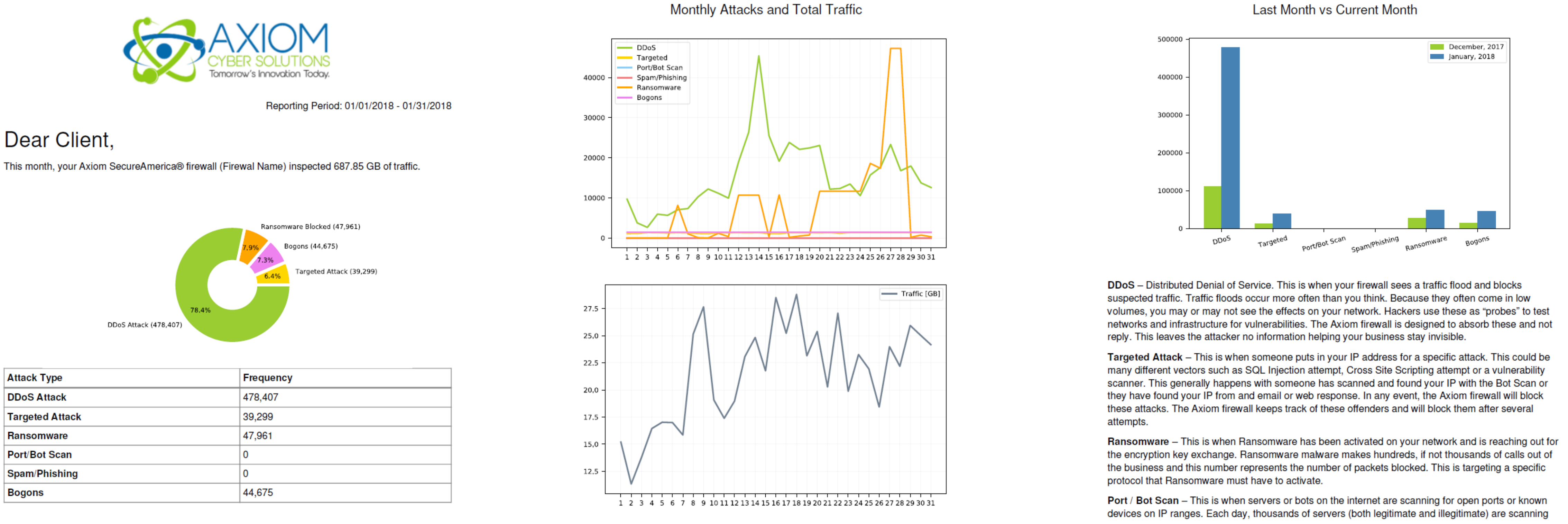
AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

Benefits

- Allows cybersecurity without having to purchase other products or hardware
- Allows full layer 7 filtering of threats
- Not a UTM – Leave virus and spam filters to the endpoint
- Network receives over 75% of attacks, not endpoint
- Protects the IoT devices
- Based on MikroTik's firewall best practices and improved in house and through the MikroTik community
- Perfect for Edge/Perimeter or segmentation to Managed Clients
- Protections must by dynamic, static rules and address lists are quickly out of date

AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

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

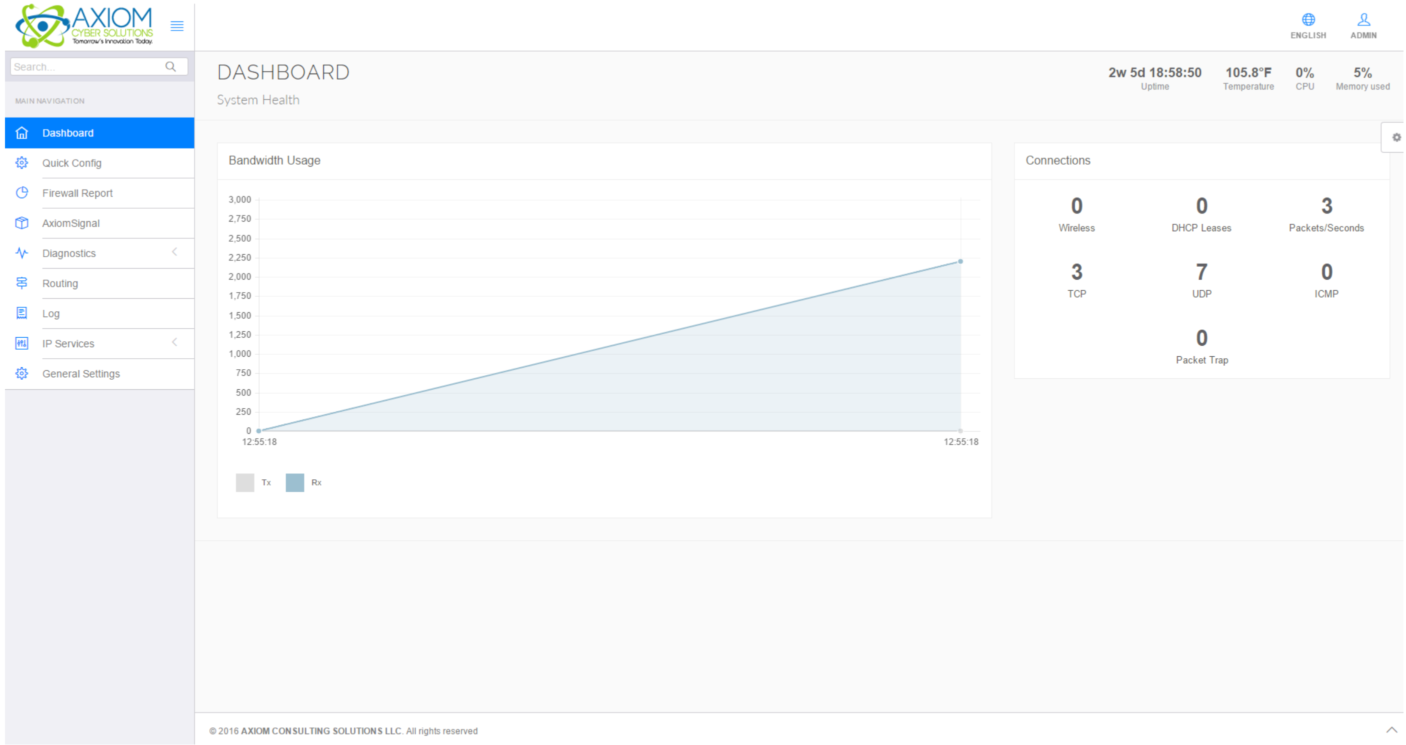
DDoS – Distributed Denial of Service. This is when your firewall sees a traffic flood and blocks suspected traffic. Traffic floods occur more often than you think. Because they often come in low volumes, you may or may not see the effects on your network. Hackers use these as “probes” to test networks 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 and 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



DASHBOARD

System Health

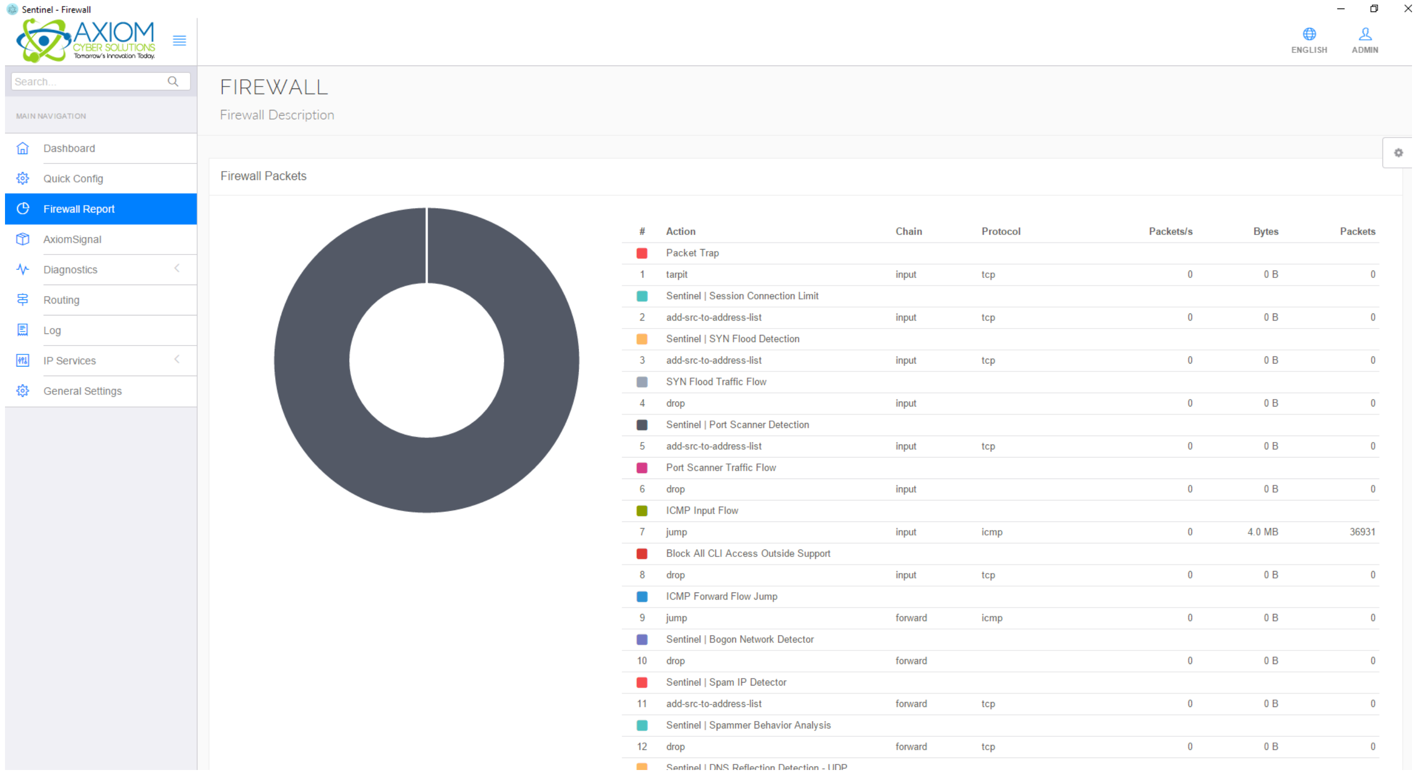
2w 5d 18:58:50	105.8°F	0%	5%
Uptime	Temperature	CPU	Memory used

Connections

0 Wireless	0 DHCP Leases	3 Packets/Seconds
3 TCP	7 UDP	0 ICMP
	0 Packet Trap	

AXIOM
CYBER SOLUTIONS
Tomorrow's Innovation Today

Axiom Dashboard – Firewall Stats



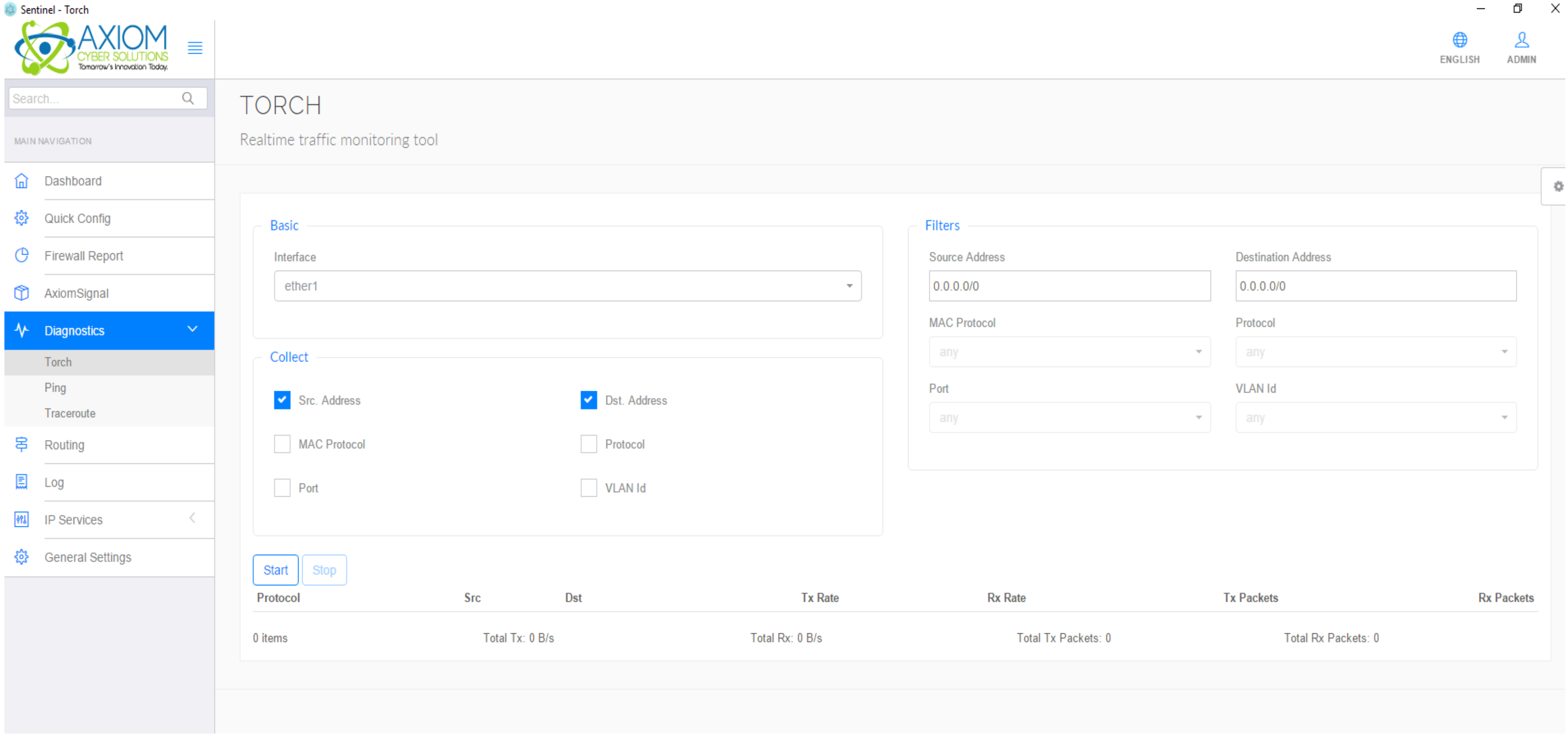
FIREWALL

Firewall Description

Firewall Packets

#	Action	Chain	Protocol	Packets/s	Bytes	Packets
🟥	Packet Trap					
1	tarpit	input	tcp	0	0 B	0
🟦	Sentinel | Session Connection Limit					
2	add-src-to-address-list	input	tcp	0	0 B	0
🟧	Sentinel | SYN Flood Detection					
3	add-src-to-address-list	input	tcp	0	0 B	0
⬜	SYN Flood Traffic Flow					
4	drop	input		0	0 B	0
⬛	Sentinel | Port Scanner Detection					
5	add-src-to-address-list	input	tcp	0	0 B	0
🟪	Port Scanner Traffic Flow					
6	drop	input		0	0 B	0
🟩	ICMP Input Flow					
7	jump	input	icmp	0	4.0 MB	36931
🟥	Block All CLI Access Outside Support					
8	drop	input	tcp	0	0 B	0
🟦	ICMP Forward Flow Jump					
9	jump	forward	icmp	0	0 B	0
🟪	Sentinel | Bogon Network Detector					
10	drop	forward		0	0 B	0
🟥	Sentinel | Spam IP Detector					
11	add-src-to-address-list	forward	tcp	0	0 B	0
🟦	Sentinel | Spammer Behavior Analysis					
12	drop	forward	tcp	0	0 B	0
🟧	Sentinel | DNS Reflection Detection - UDP					

Axiom Dashboard – Advanced Packet Level Diagnostics



TORCH

Realtime traffic monitoring tool

Basic

Interface: ether1

Collect

☑ Src. Address ☑ Dst. Address

□ MAC Protocol □ Protocol

□ Port □ VLAN Id

Filters

Source Address: 0.0.0.0/0

Destination Address: 0.0.0.0/0

MAC Protocol: any

Protocol: any

Port: any

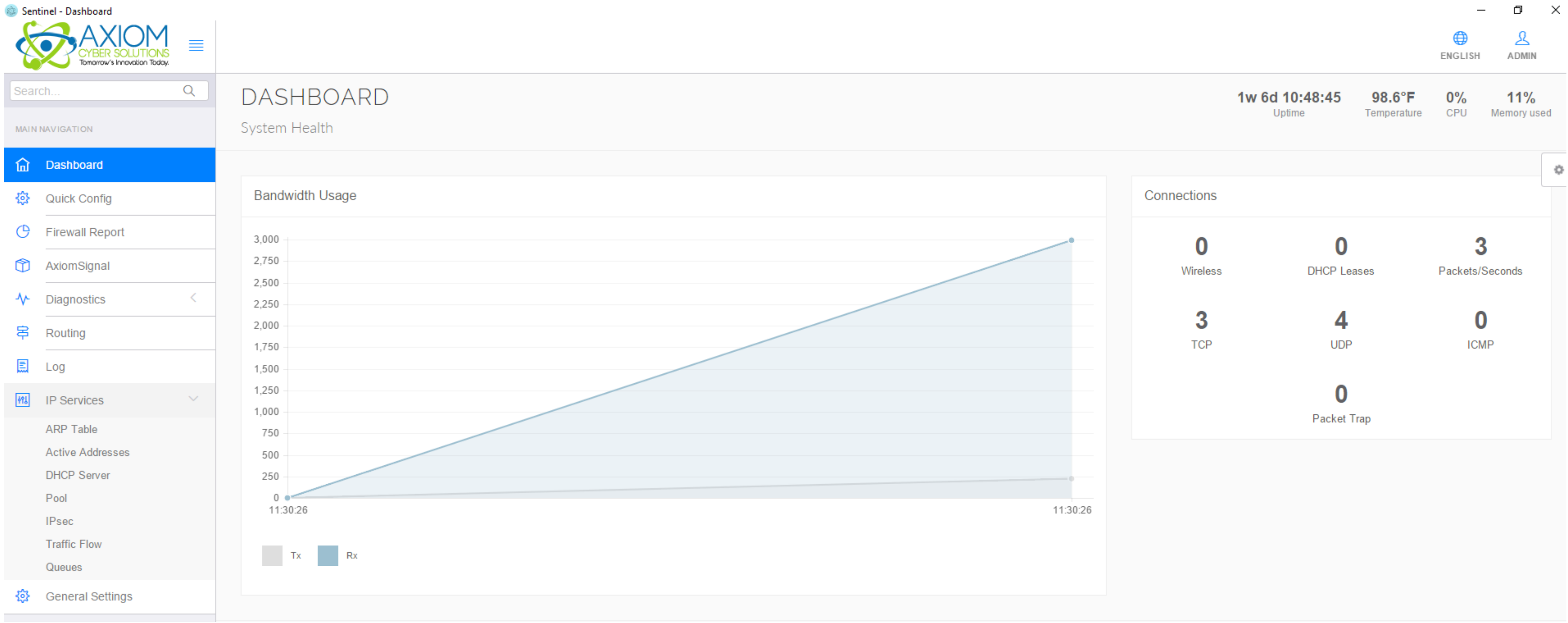
VLAN Id: any

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

AXIOM CYBER SOLUTIONS
Tomorrow's Innovation Today

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!
- Contact – Troy Wilkinson, CEO – troy.wilkinson@axiomcyber.com
- www.axiomcyber.com/shield
- First month free code: SHIELD1M