An introduction to IDS/IPS…

@__wavelength__

About Me

- New Orleans area native (504/985)
- Worn many hats:
  Datacenter Engineer, Technical Architect, Internet Engineer, CMTS Engineer, Systems and Network Administrator, and Help Desk
- Day Job: Sr Cyber Security Analyst
- Night Job: Network & Security Consultant
- Work with several animal rescue organizations, certified pilot, and nature photographer
- ISO 8601 Compliant
- CISSP (Don't Judge Me…)

North Myrtle Beach, January 2018

Disclaimer

This presentation is meant to introduce IDS/IPS to a wide range of people with various skill levels. I have written this talk on the assumption that the majority of the audience has no prior exposure to this topic.

Agenda

1. What is an IDS/IPS?
2. Quick survey of available IDS/IPS Solutions
3. Introduction of Security Onion
4. Hands On: Exercise #1 Walkthrough (time permitting)
5. Questions and (maybe) Answers

What is an IDS/IPS?

- Intrusion Detection System: a passive system that is able to detect, but not mitigate, network or host intrusions.

- Intrusion Prevention System: an active system that is able to detect and is capable of intervening during a network or host intrusion by blocking or halting malicious activity. Must be deployed in-line.

Two major types of each

Network-based - a system connected to and monitoring that network or networks (NIDS and NIPS)

Host-based - software installed on a server, VM or client that monitors that specific system for unexpected or malicious activity, such as file changes, network traffic, errors logs, etc. (HIDS and HIPS)

Detection Methods

Knowledge-Based / Signature-Based IDS/IPS

Uses information from previously observed attacks or published vulnerabilities, so these systems are only capable of detecting known attacks or vulnerabilities. Also called “Rule-Based”.

Behavior-Based / Anomaly-Based IDS/IPS

Operate by establishing a baseline and then determining if traffic or activities are not normal*. These types have the capability to detect previously unknown attacks.

- Statistical Anomaly - uses a scoring system to determine anomalous traffic and generate alerts based on thresholds
- Traffic Anomaly - observes the traffic within a network and makes determinations based on trends - volume, protocol use, etc.
- Protocol Anomaly - watches for deviations from normal protocol activity to detect misuse or abuse - example, DNS exfiltration

So, why an asterisk on normal in the last slide?

Anomaly-based IDS/IPS systems require a baseline to be established using a training period to determine what is "normal". That training period can be days, weeks or months…

WHAT IF YOU ARE ALREADY COMPROMISED?

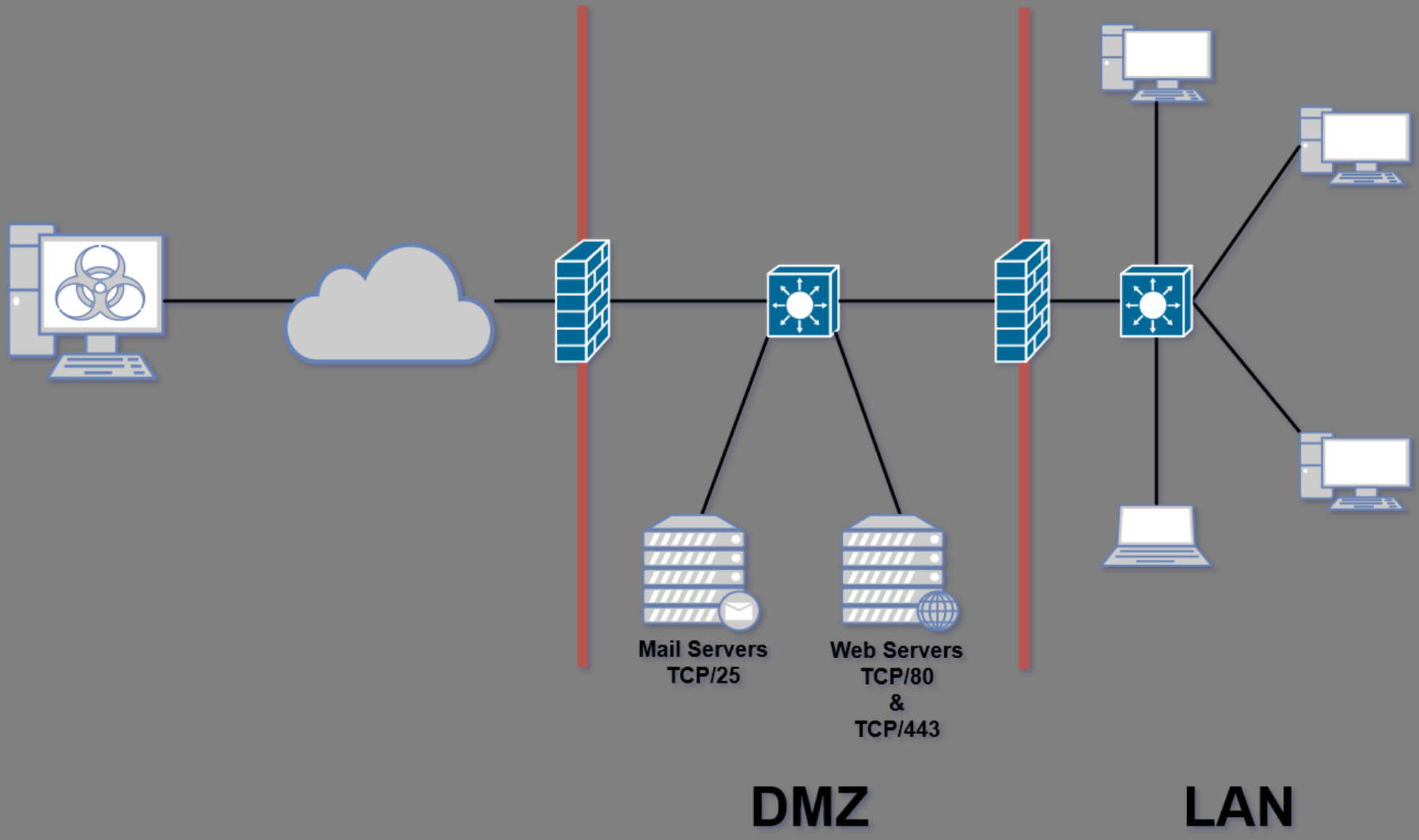
Malicious traffic may be classified as… "Normal"

Ok, but, I have a firewall…

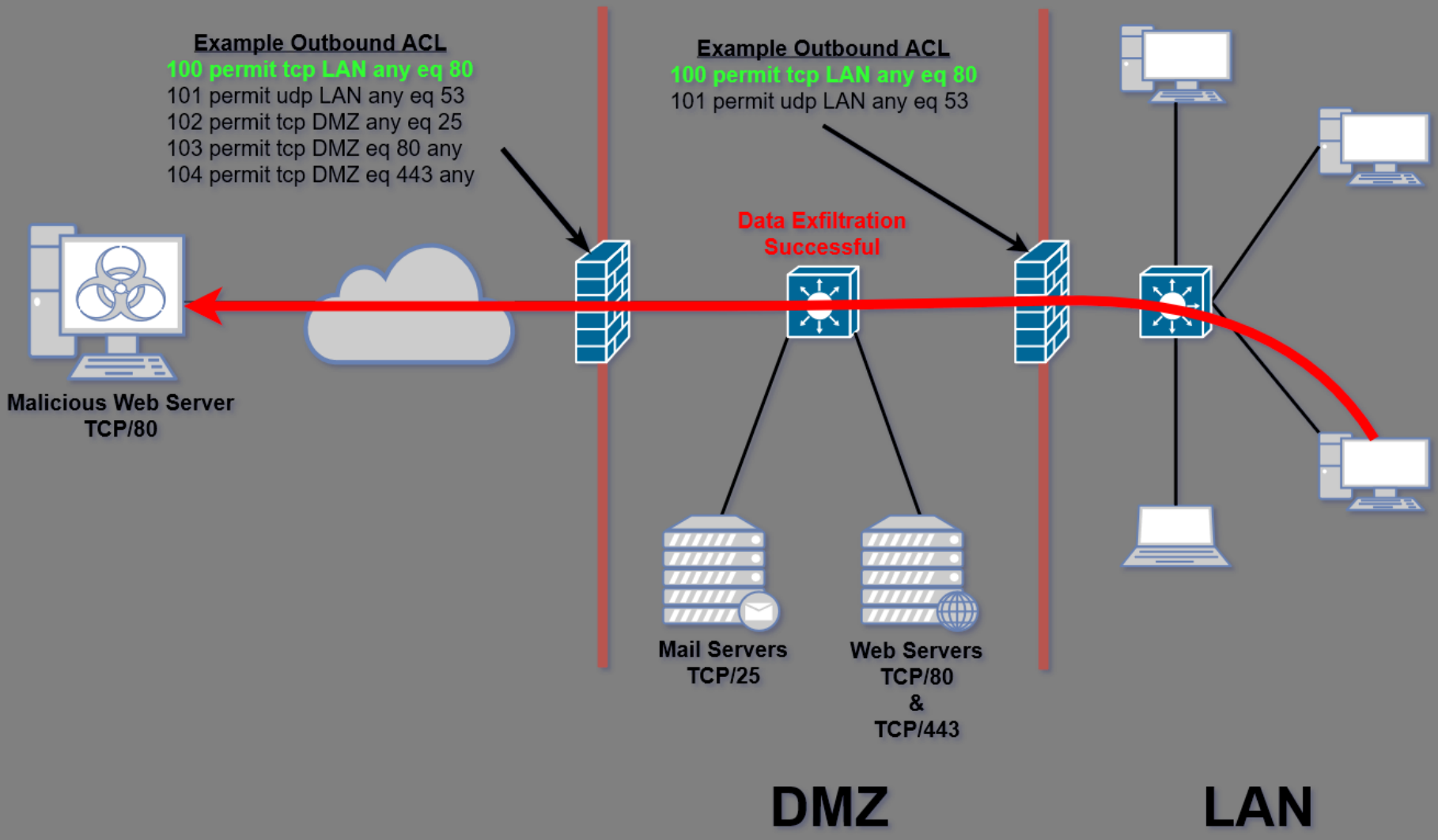
Firewalls are great for coarse source/destination address, port and protocol filtering, but finer grain protection requires something more.

Let's look at some examples of how firewalls can fail to protect on their own…

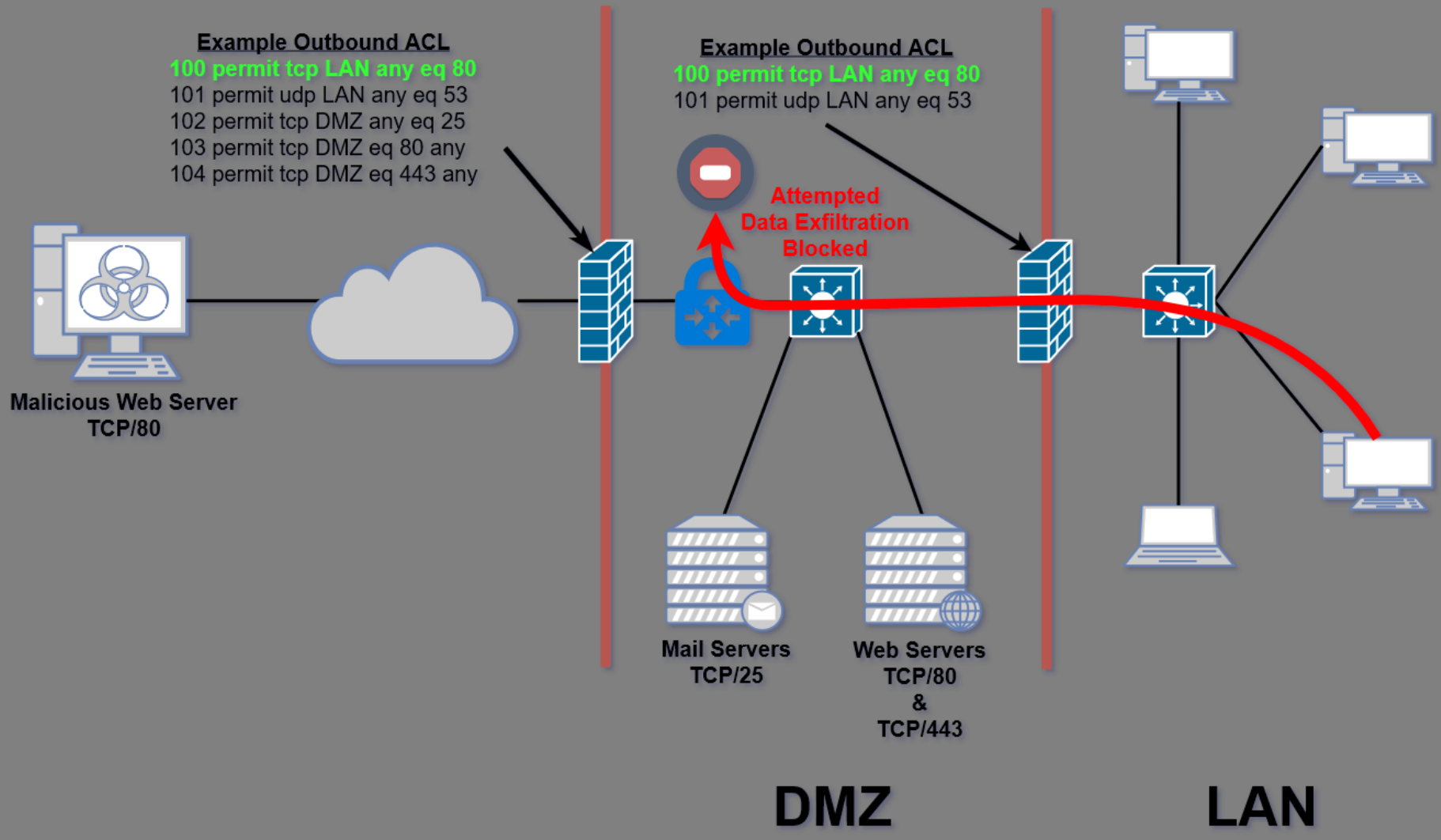
A Network Topology



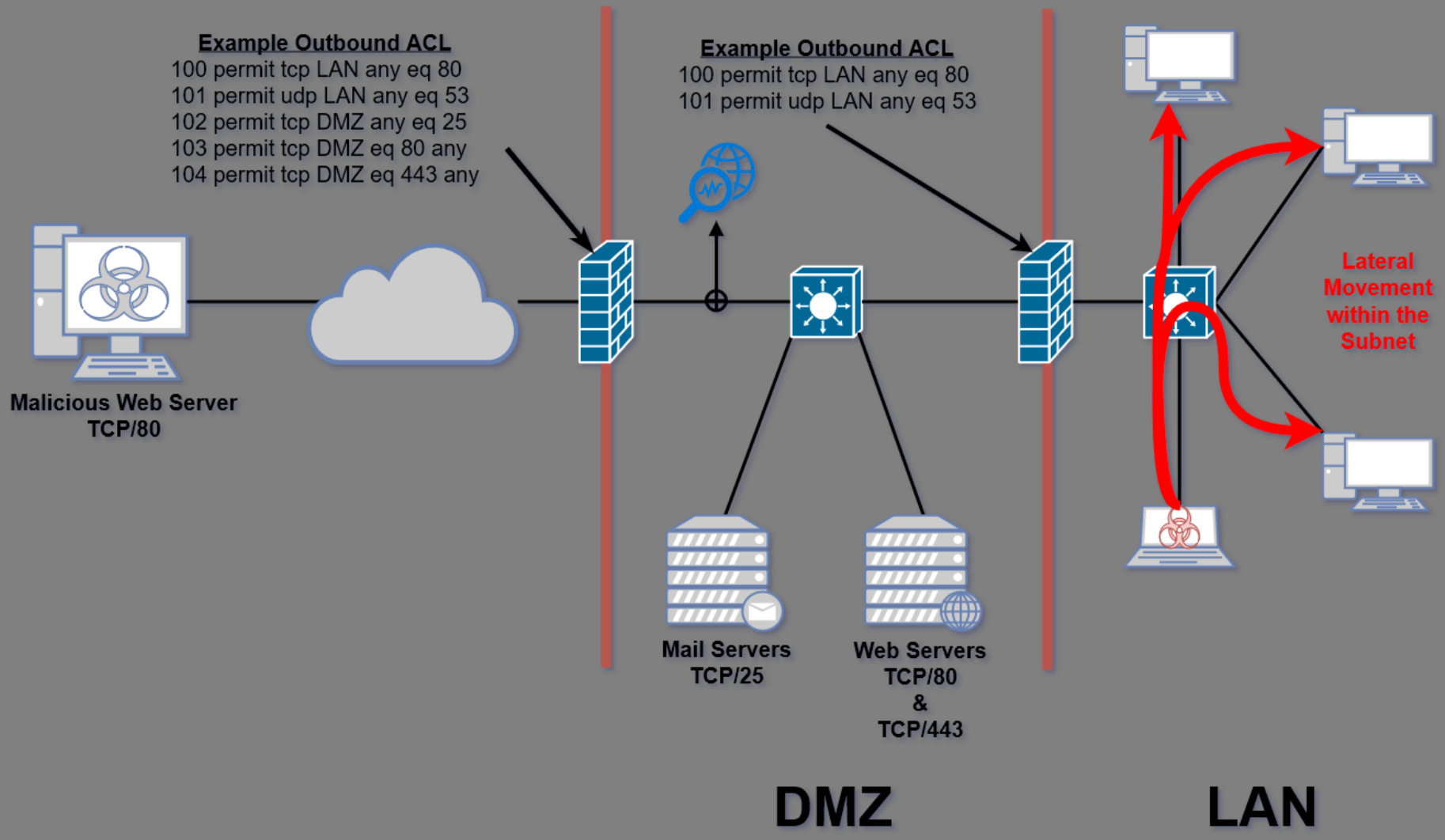
Scenario 1: Outbound Requests



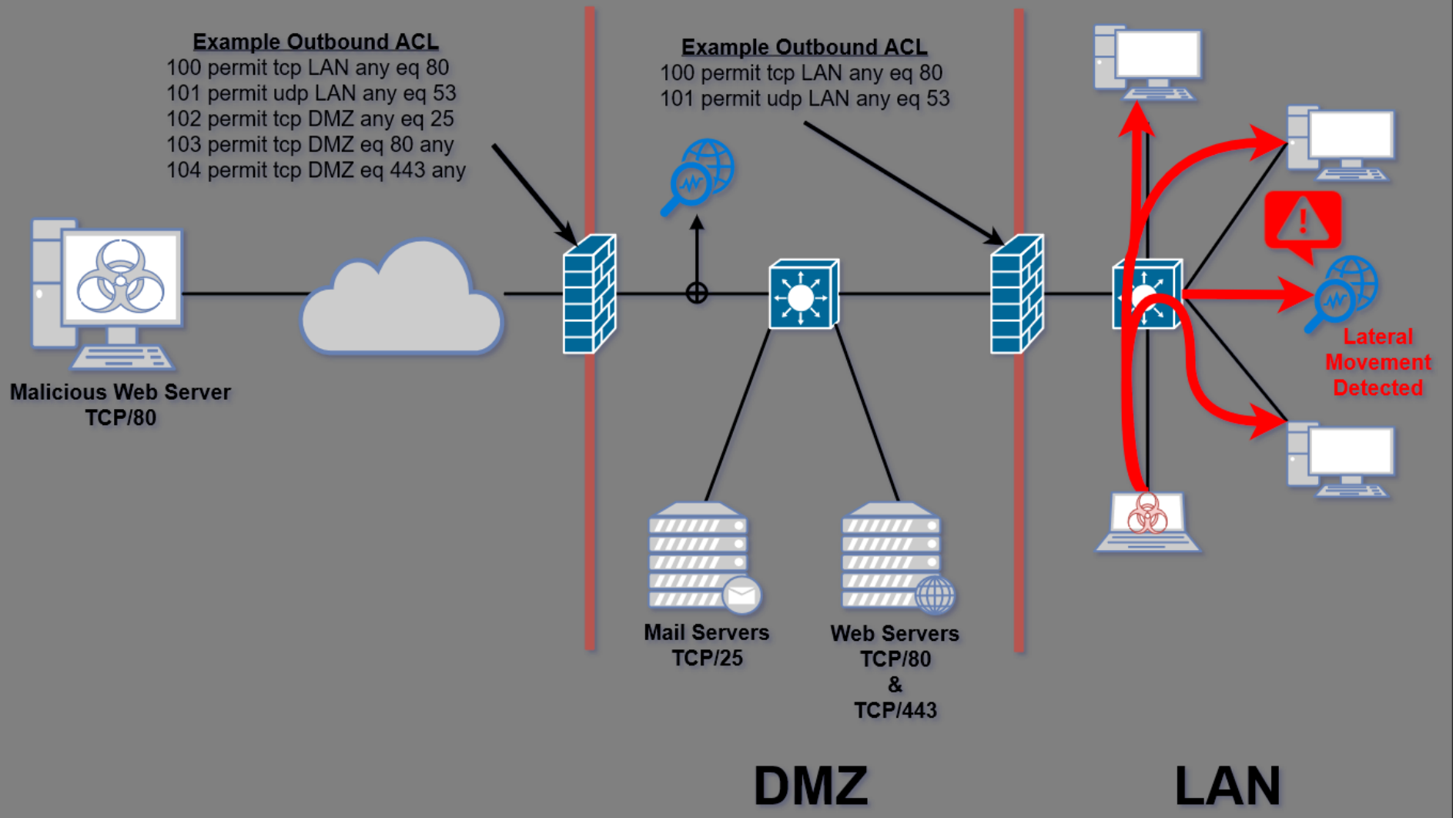
Deployment Topology: Data Exfiltration (IPS)



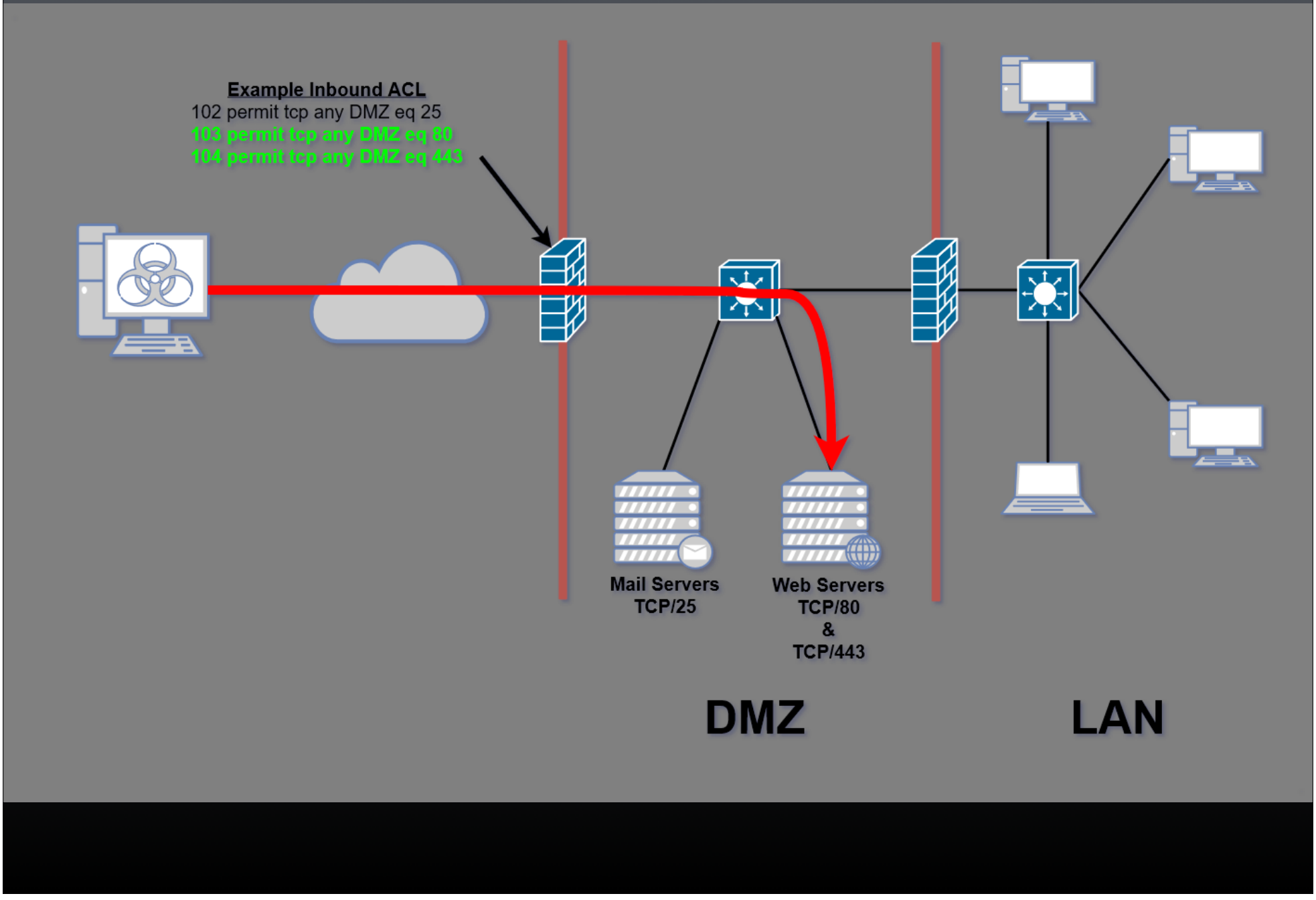
Scenario 2: Host to Host Traffic ("Lateral Movement")



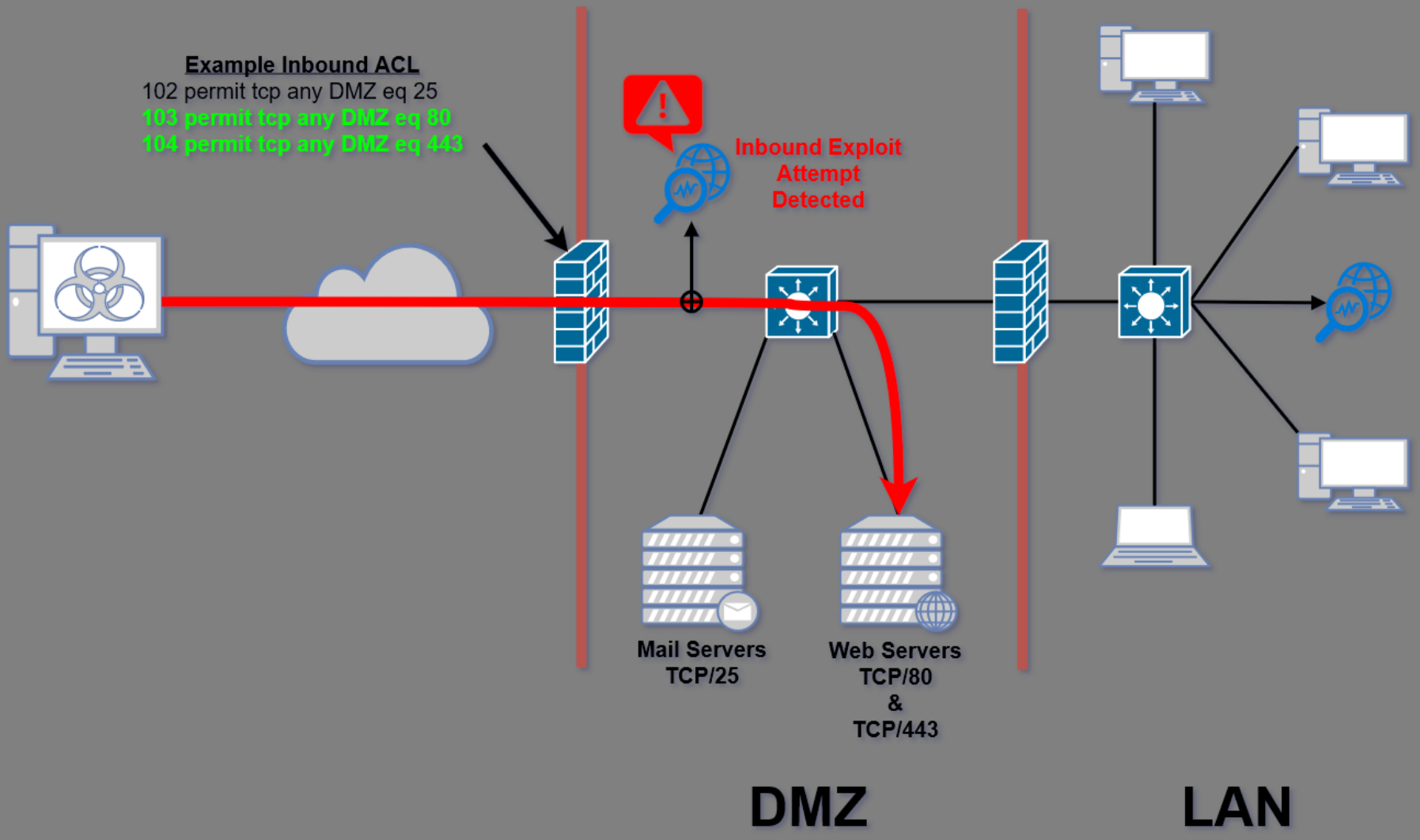
Deployment Topology: Lateral Movement (with IDS)



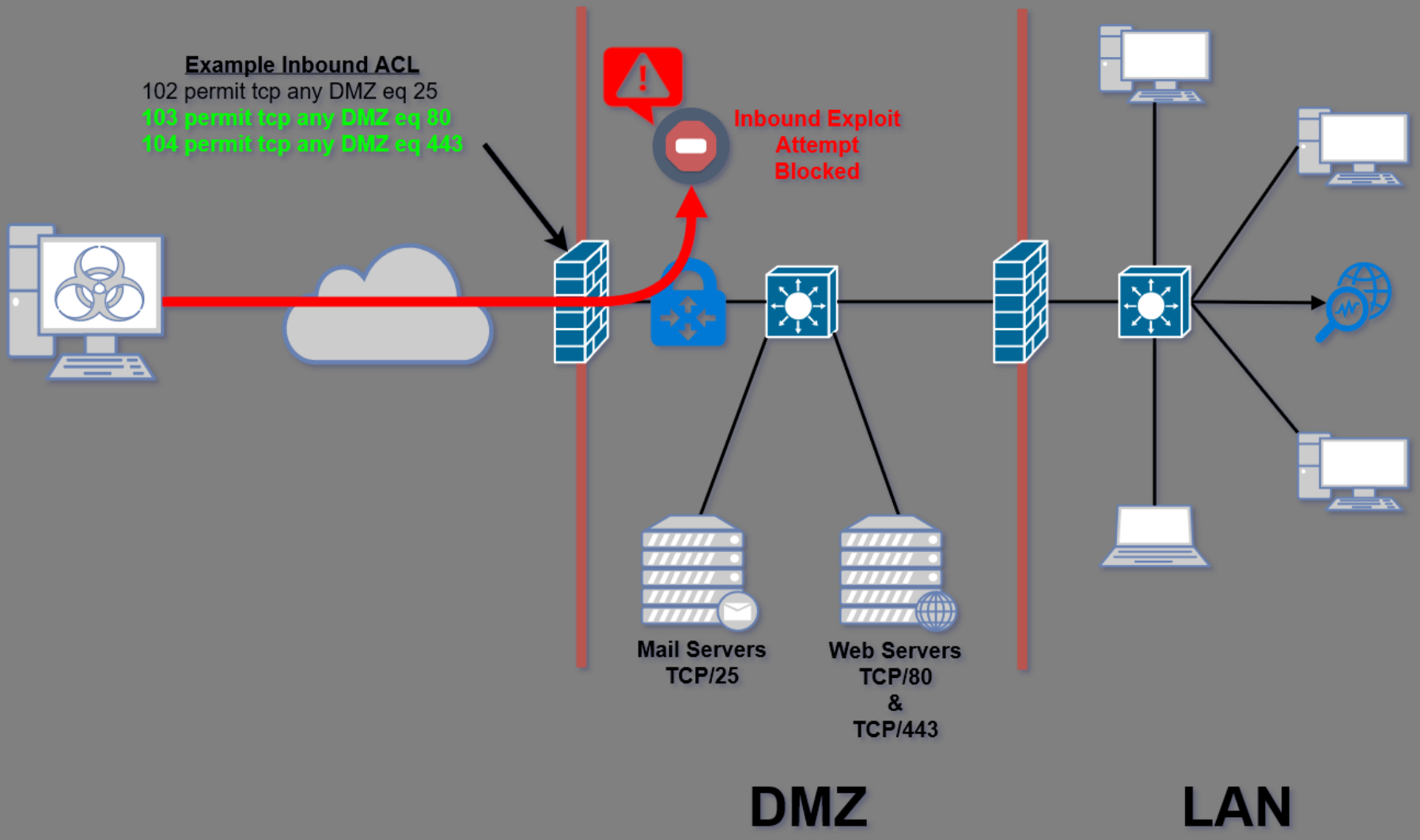
Scenario 3: Inbound requests to DMZ host



Deployment Topology: Inbound Attack (IDS)



Deployment Topology: Inbound Attack (IPS)



What solutions are available?

Commercial Solutions

TREND MICRO™

FORTINET®

McAfee™

CISCO

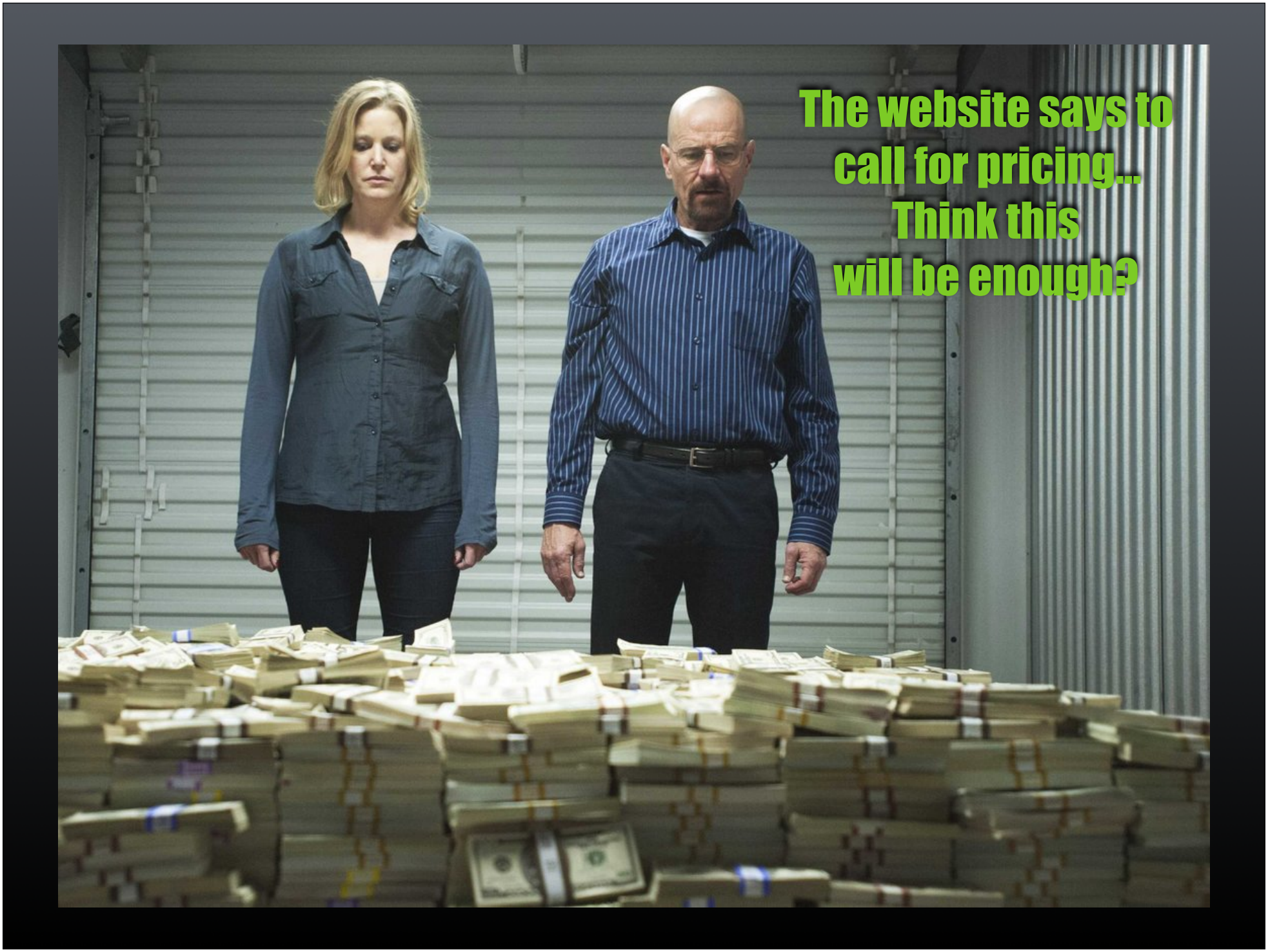
IBM

FireEye™

paloalto NETWORKS

ALERT LOGIC®

And others…


The website says to
call for pricing...
Think this
will be enough?

“Lower-cost” Alternatives

SOPHOS

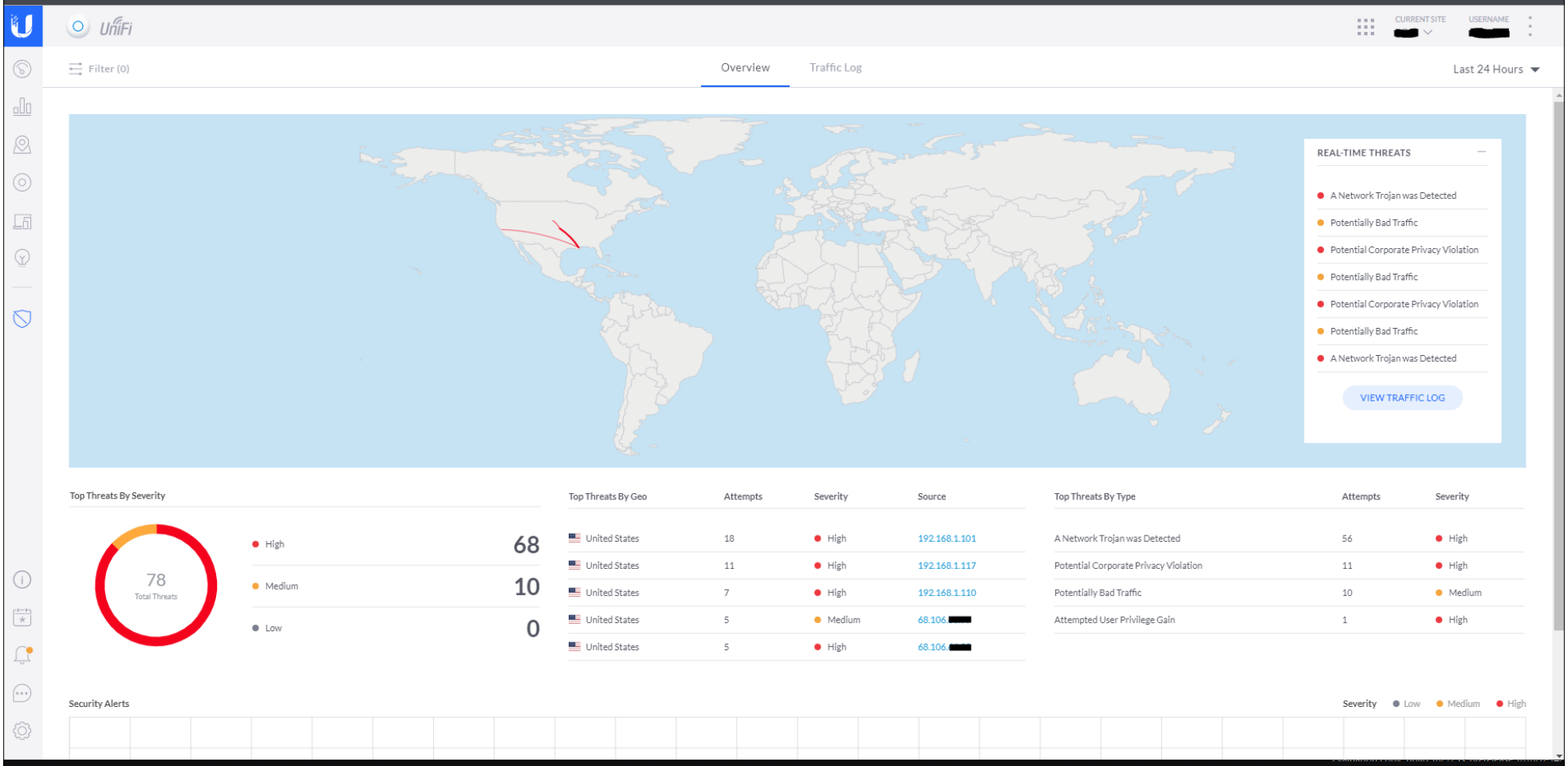
SG Line (SG 135)

- 6 Gbps FW throughput
- 1 Gbps IDS/IPS throughput
- < $2500 (including support)

UBIQUITI NETWORKS

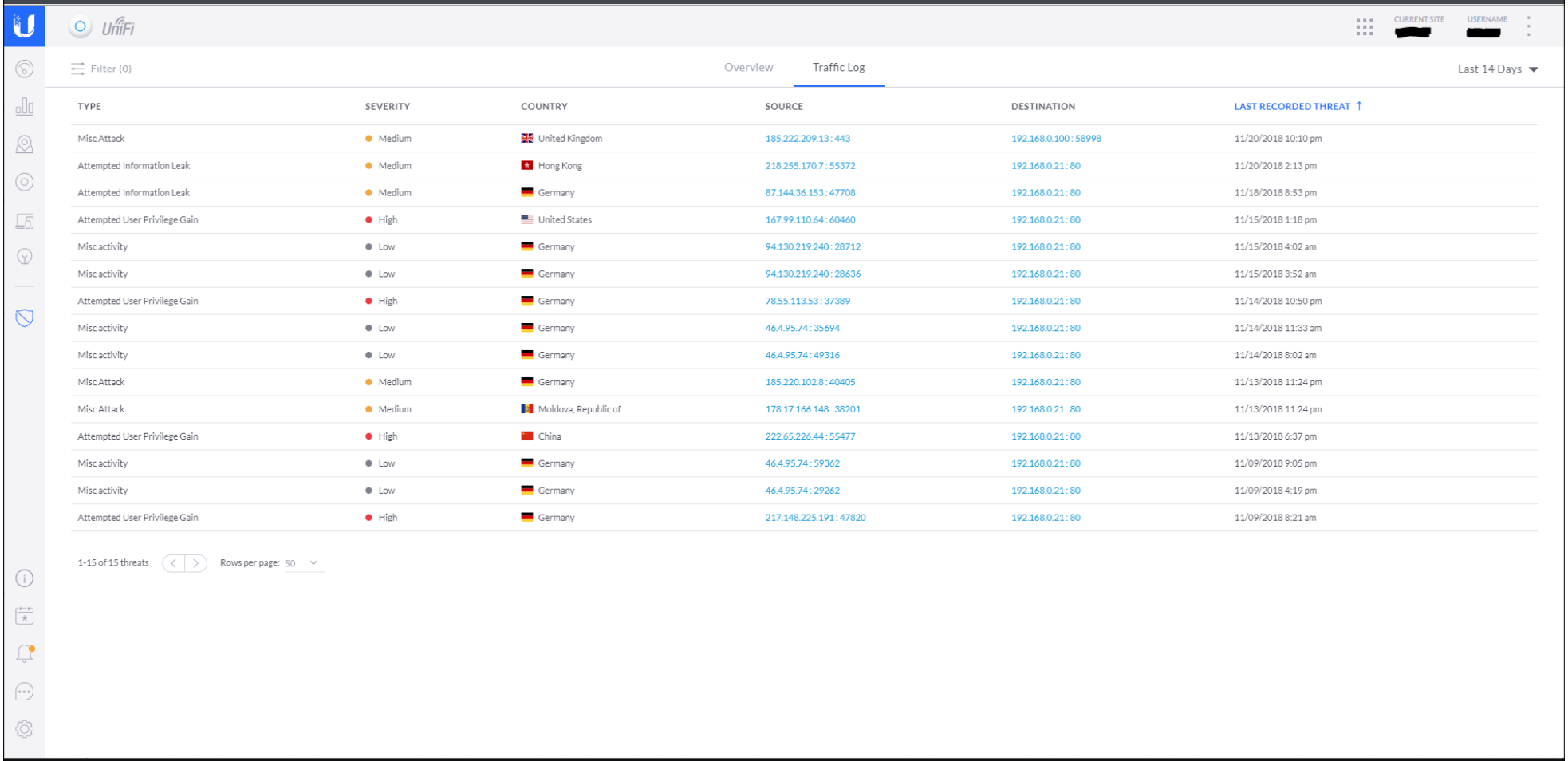
USG 3P	USG Pro	USG XG
>1Gbps throughput (raw)	>1Gbps throughput (raw)	>10Gbps throughput (raw)
85Mbps IDS/IPS throughput	250Mbps IDS/IPS throughput	1Gbps IDS/IPS throughput
$140	$350	$2500

Ubiquiti UniFi IDS/IPS Interface



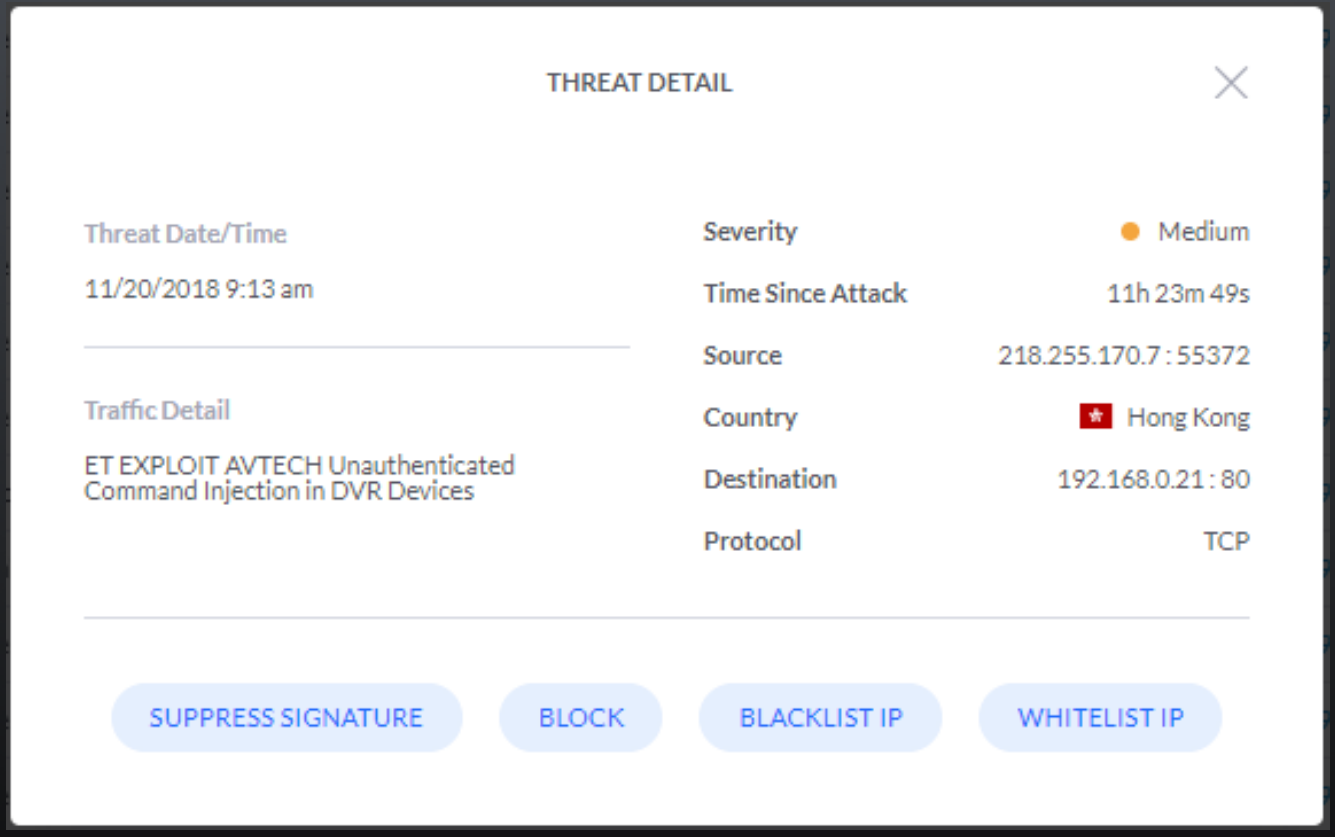
Overview Pane

Ubiquiti UniFi IDS/IPS Interface



Traffic Log Pane

Ubiquiti UniFi IDS/IPS Interface



Attacker attempting to use a known exploit against client's security DVR

FOSS Standalone Options

Network-based

Bro / Zeek

Host-Based

And others…

Bro / Zeek

https://www.bro.org

Development started in 1994, by
Vern Paxson at UC, Berkeley

More than a standard IDS solution - performs deep analysis of network traffic to identify threats, potential vulnerabilities or outdated software packages and systems.

For example, Bro can analyze user-agent strings to spot out of date browsers or Java versions. It can also monitor SSL/TLS connections to identify expired or self-signed certificates.

In 2018, the Bro Leadership Team elected to rename the project “Zeek”
http://blog.bro.org/2018/10/renaming-bro-project_11.html

Snort

https://www.snort.org

Development started in 1998, by Martin Roesch, founder of SourceFire

In 2013, Cisco purchased SourceFire, using Snort as the basis of the FirePower IDS feature; standalone Snort is still open-source.

The Snort engine is written is C. Up until 3.0, which is now in Beta, Snort was single-threaded, requiring multiple processes to scale.

Compatible “real-time” rules are produced by Cisco, Proofpoint and Crowdstrike, all requiring a subscription. The Cisco VRT rules subscription provides the same rules used on Firepower appliances. A personal VRT subscription is $29/year. There are also the Registered user Snort rules for free, but with a 30 day delay behind the paid VRT rules. Snort Community rules are also free, but lack any VRT rules.

Suricata

https://www.suricata-ids.org

Development of Suricata is lead by OISF, the Open Information Security Foundation. The first production version was released in 2010.

Suricata was designed to address some of the perceived deficiencies in Snort. For example, Suricata is multi-threaded by default.

The preferred ruleset for Suricata is the Emerging Threats (Open and Subscription) ruleset, but is capable of using many Snort rules. Some keywords and match terms may result in rules failing to import. Snort shared object ("compiled") rules are not supported on Suricata.

One drawback to Suricata is that the documentation is less developed than the Snort documentation and it has a smaller user community.

Tripwire

https://github.com/Tripwire/tripwire-open-source

The open source version of Tripwire is based on code contributed by Tripwire, Inc. in 2000. The commercial version of the Tripwire software still exists.

Tripwire is a file integrity monitoring system that detects changes to a user-configured list of files or operating system files. When a file is change, Tripwire will generate an alert.

OSSEC

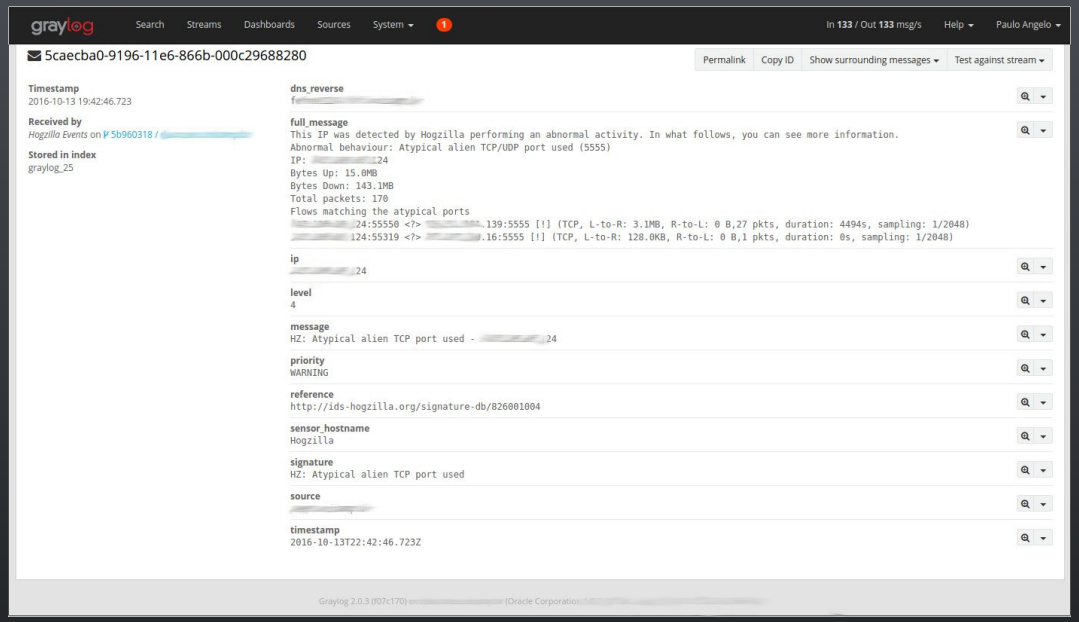
https://www.ossec.net/

Development started in 2005 by Daniel Cid.

The rights to the project were eventually purchased by Trend Micro in 2009, but development on the project continues and remains open source.

OSSEC is a multi-platform HIDS, running on *BSD, Linux and Windows, and has the ability to monitor multiple systems from a single, centralized host. OSSEC features log analysis, file integrity monitoring, policy enforcement, rootkit detection, alerting and active response.

Hogzilla



http://ids-hogzilla.org
First release - 2016*

"Hogzilla is an open source Intrusion Detection System (IDS) supported by Snort, SFlows, GrayLog, Apache Spark, HBase and libnDPI, which provides **Network Anomaly Detection**."

*https://www.linkedin.com/pulse/hogzilla-anomaly-based-ids-first-usable-release-alves-resende/

Rolling your own is an option, but…

Configuring, tuning and tweaking each of these can be complex.

While building these from scratch is a great way to learn, options exist to deploy an open source IDS/IPS much more quickly.

“Turn-key” Options

Bro, Snort or Suricata,
OSSEC, ElasticSearch,
Logstash, Kibana, and others

Primarily a SIEM system with IDS,
OpenVAS, Nagios,
Netflow monitoring features

Sweet Security

Bro, ElasticSearch, Logstash,
Kibana and Critical Stack
on the RPi platform

BriarIDS

Bro and Suricata
on the RPi platform
(and some routers)

SELKS

Suricata, ElasticSearch,
Logstash, Kibana,
Scirius, Evebox

pfSense

IDS/IPS via add-on packages

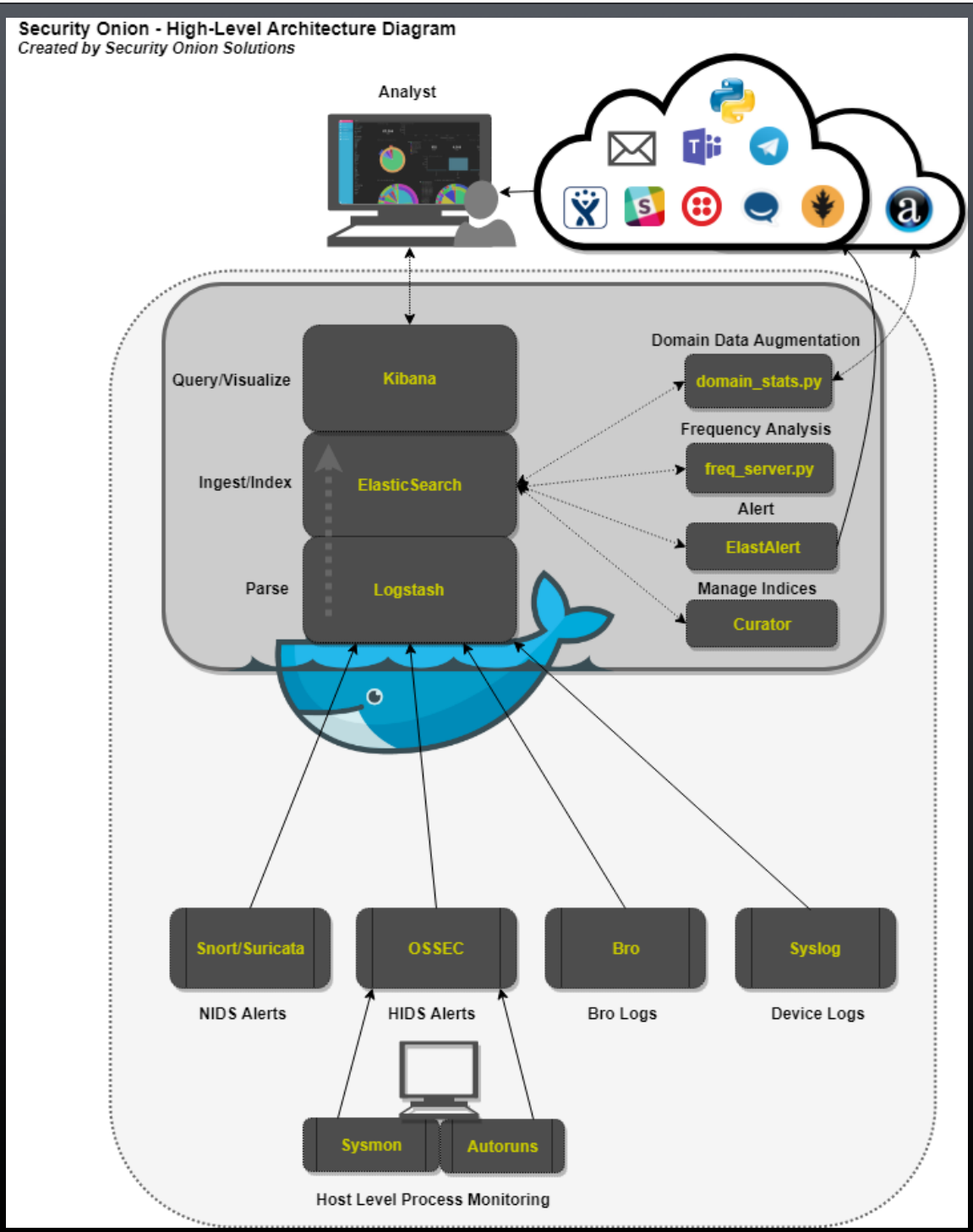
And possibly other smaller projects…

www.securityonion.net

Doug Burks created Security Onion in 2008, with the first release in 2009. In 2012, the distro was rebuilt from the ground up to improve performance and scaleability. It can be installed from a pre-built ISO built on Ubuntu or installed onto an Ubuntu or Ubuntu-like distro using packages

Security Onion includes the following features:

- Bro/Zeek
- Snort and Suricata
- OSSEC (with agents available for several OSes)
- The ELK (Elasticsearch, Logstash and Kibana) stack
- capME!
- squil and squert consoles
- Wireshark and NetworkMiner


Security Onion - High-Level Architecture Diagram
Created by Security Onion Solutions
Analyst
Query/Visualize
Kibana
Ingest/Index
ElasticSearch
Parse
Logstash
Domain Data Augmentation
domain_stats.py
Frequency Analysis
freq_server.py
Alert
ElastAlert
Manage Indices
Curator
Snort/Suricata
NIDS Alerts
OSSEC
HIDS Alerts
Bro
Bro Logs
Syslog
Device Logs
Sysmon
Autoruns
Host Level Process Monitoring

Deployment Types

All-In-One

All services of the Security Onion stack are hosted on a single machine or VM. While not meant for "production" configurations, all-in-one deployments are acceptable for demonstrations and small environments, like your home.

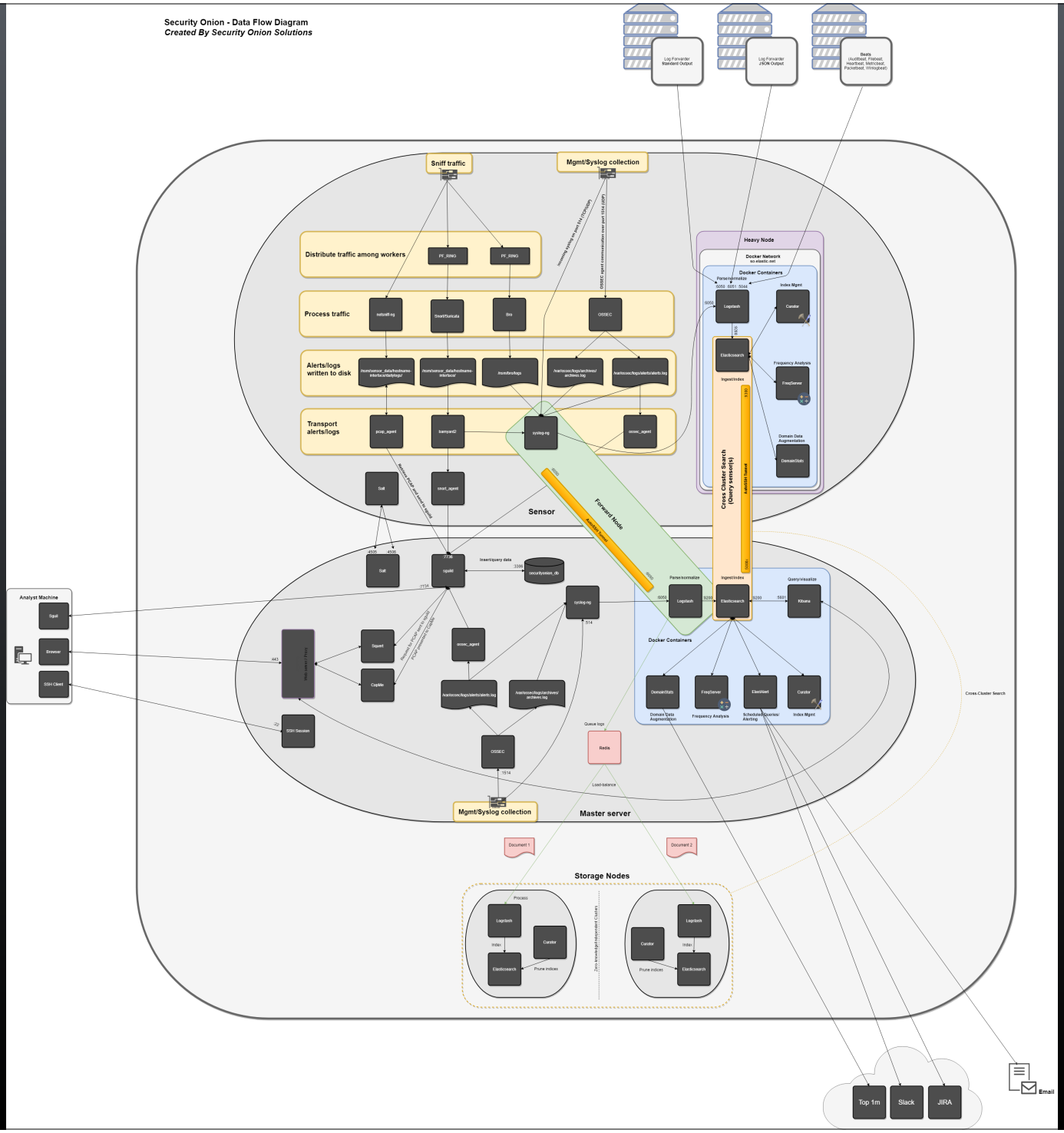
Distributed

Three types of nodes to distribute the processing load to scale to large environments and high volumes of network traffic.

Forward Node (Sensor): Captures packets from network and logs from hosts

Master Node: Runs the analyst interfaces (squil and squert) and the search/curator processes for the logs received

Storage Nodes: Stores and index logs and data forwarded from sensors to expand the storage and search capabilities of the Master Node


Security Onion - Data Flow Diagram
Created By Security Onion Solutions
Log Forwarder Standard Output
Log Forwarder JSON Output
Beats (Auditbeat, Filebeat, Heartbeat, Metricbeat, Packetbeat, Winlogbeat)
Sniff traffic
Mgmt/Syslog collection
Distribute traffic among workers
PF_RING
Process traffic
netsniff-ng
SnortSuricata
Bro
OSSEC
Alerts/logs written to disk
Transport alerts/logs
pcap_agent
barnyard2
syslog-ng
ossec_agent
Salt
snort_agent
Sensor
Forward Node
Heavy Node
Docker Network
Docker Containers
Logstash
Curator
Elasticsearch
Index Mgmt
Frequency Analysis
FreqServer
Domain Data Augmentation
DomainStats
Cross Cluster Search (query across(*))
Analyst Machine
Squil
Browser
SSH Client
Squert
CapMe
Web server Proxy
SSH Session
securityonion_db
OSSEC
Redis
Queue logs
Load-balance
Master server
Mgmt/Syslog collection
Kibana
ElastAlert
Cerebro
Domain Data Augmentation
Frequency Analysis
Scheduled Queries/ Alerting
Index Mgmt
Cross Cluster Search
Document 1
Document 2
Storage Nodes
Process
Index
Prune indices
Zero knowledge/independent Clusters
Top 1m
Slack
JIRA
Email

System Requirements

Minimum System Requirements

64-bit CPUs ONLY

Minimum CPUs - 4 cores

Minimum RAM - 8GB

Minimum of two network interfaces
(One for admin/updates & one for packet captures)

Storage space is dependent on the rate at which packets are captured or logs ingested. For example, a network with an average of 1Mbps of traffic will generate ~324GB of PCAPs per month; 10Mbps is ~3.25TB.

Additional CPU cores and RAM are required as throughput increases.

Detailed Sizing Guidance

https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware

Network Requirements

In order to send packets to Security Onion and other IDS solutions, you must have either (1) a switch capable of SPAN* or port mirroring or (2) a network tap.

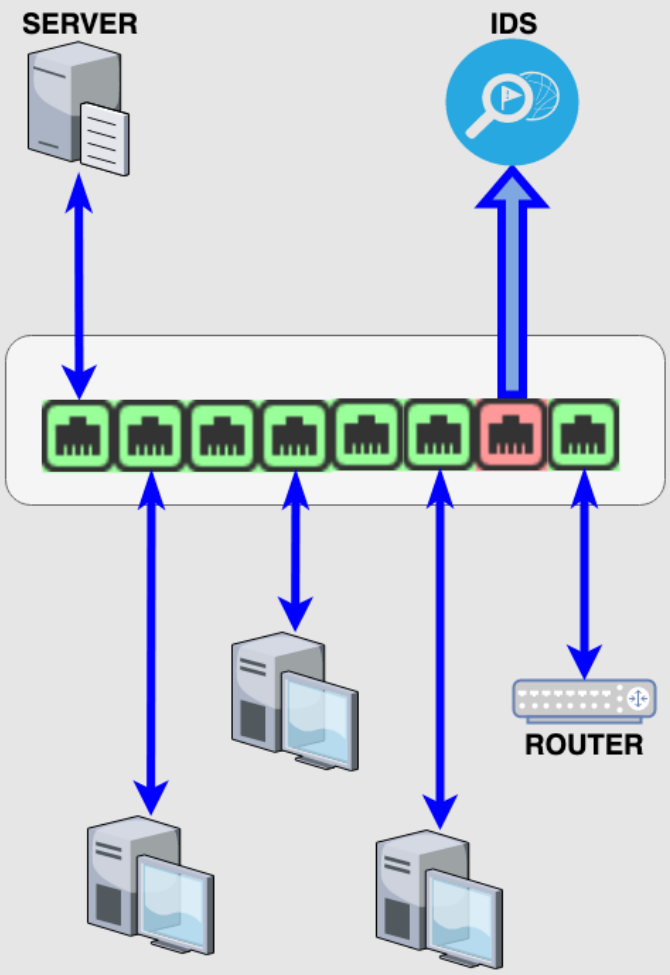
Deploying Security Onion as an IPS requires the system to be deployed in-line (beyond the scope of this intro presentation).

SPAN / Port Mirroring

A switch takes all the Ethernet frames transmitted/received on one port or ports and forwards a copy out of a configured Ethernet port or ports.

This feature is *only* present in managed switches.

*SPAN - Switched Port Analyzer


SERVER
IDS
ROUTER

Switches Capable of Mirroring

Just of few of the options…

D-Link DGS-1210-10
~$90

Linksys LGS308
~$80

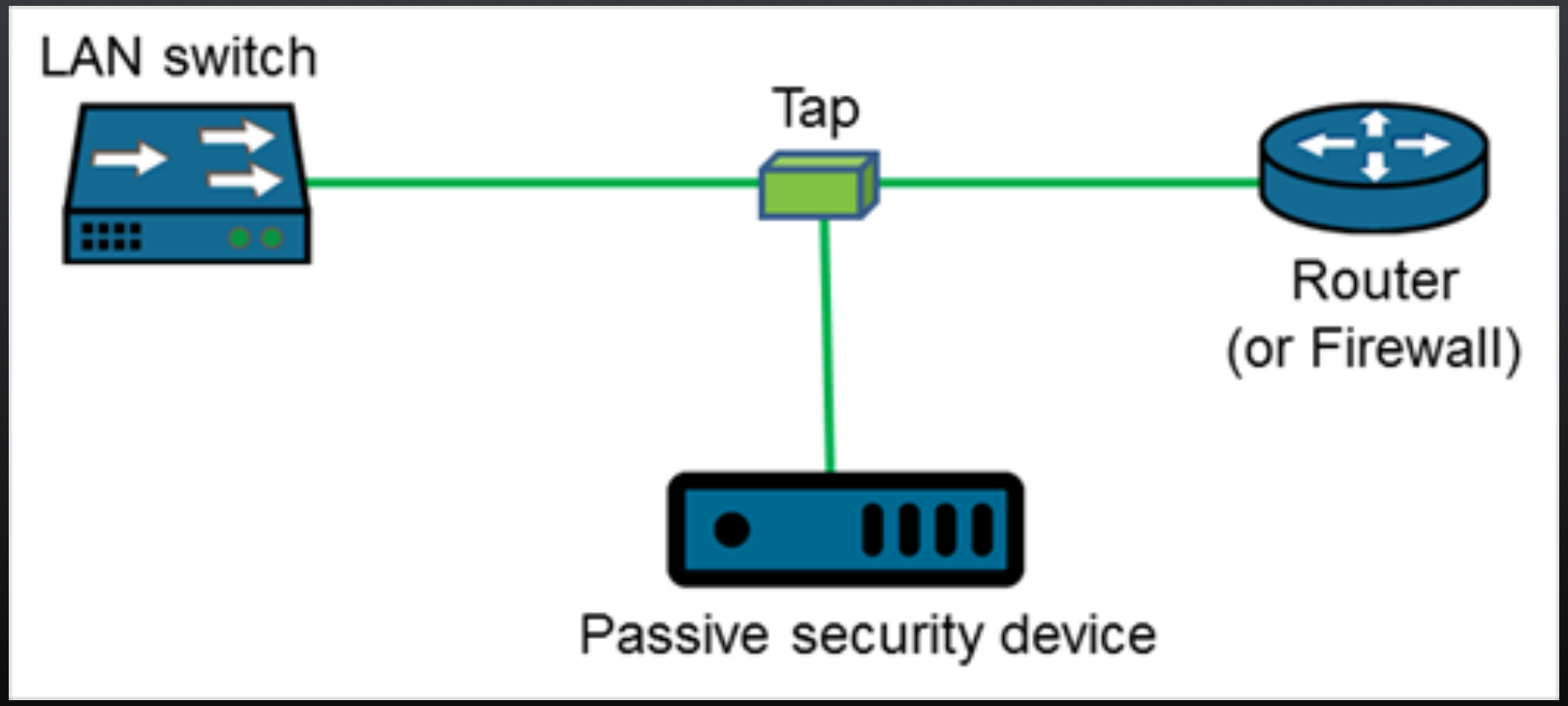
Netgear GS108E
~$70
(popular choice)

Ubiquiti UniFi US-8
~$100

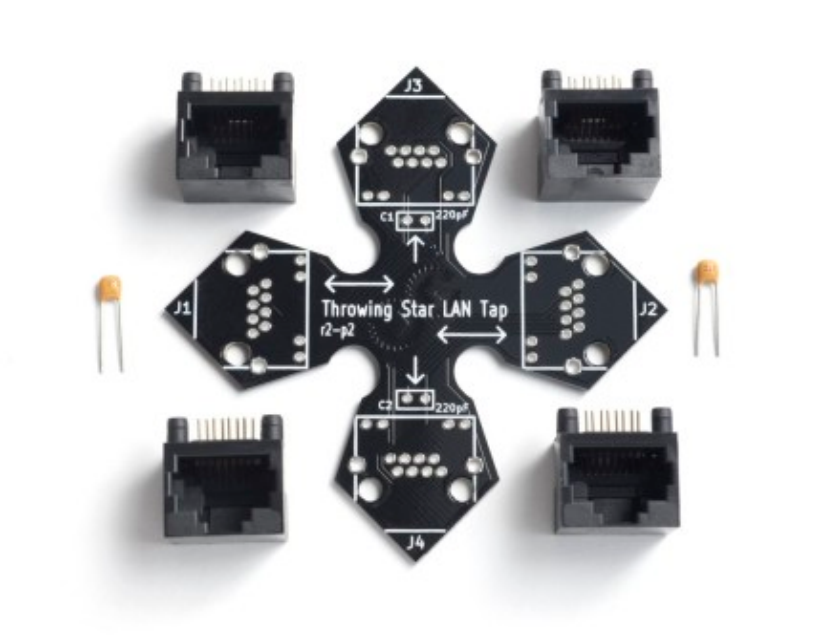
Enterprise-level switches (Aruba, Cisco, Juniper, etc.)
> $1000

Ethernet Taps

Ethernet taps are passive, in-line devices that duplicate Ethernet frames that pass through the device.



Ethernet Taps



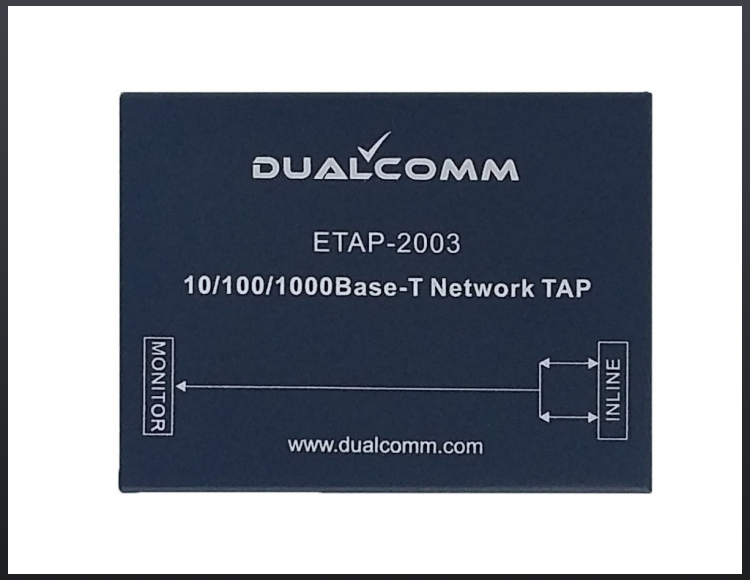
Throwing Star LAN TAP

(suitable for networks up to 100Mbps)

$40

*Note - Each output port taps traffic in only ONE direction.

Ethernet Taps



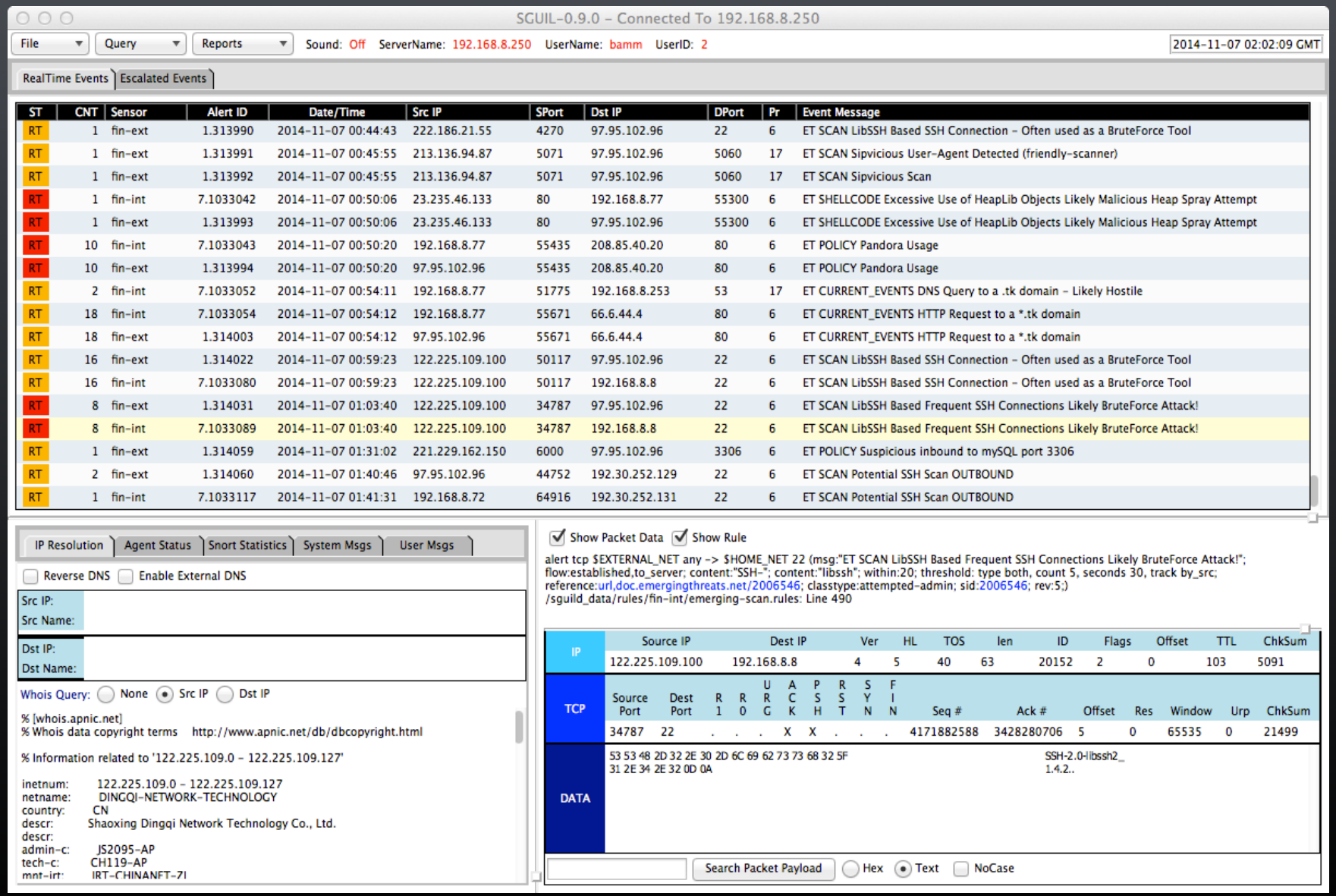
DualComm ETAP-2003
10/100/1000Base-T
~$180

SharkTap 10/100/1G
10/100/1000Base-T
~$180

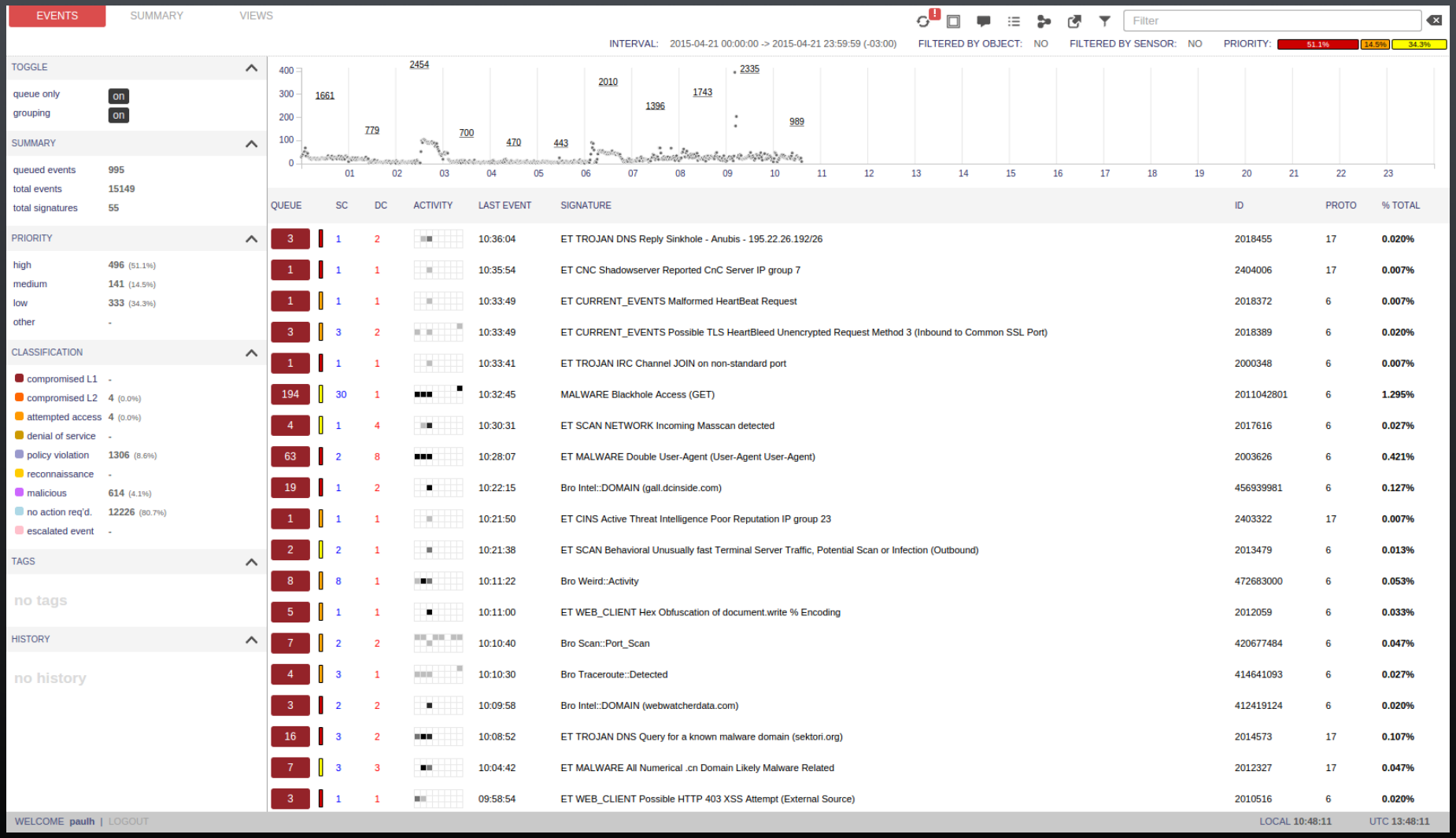
User Interfaces

Ladies and Gents, start your VMs…

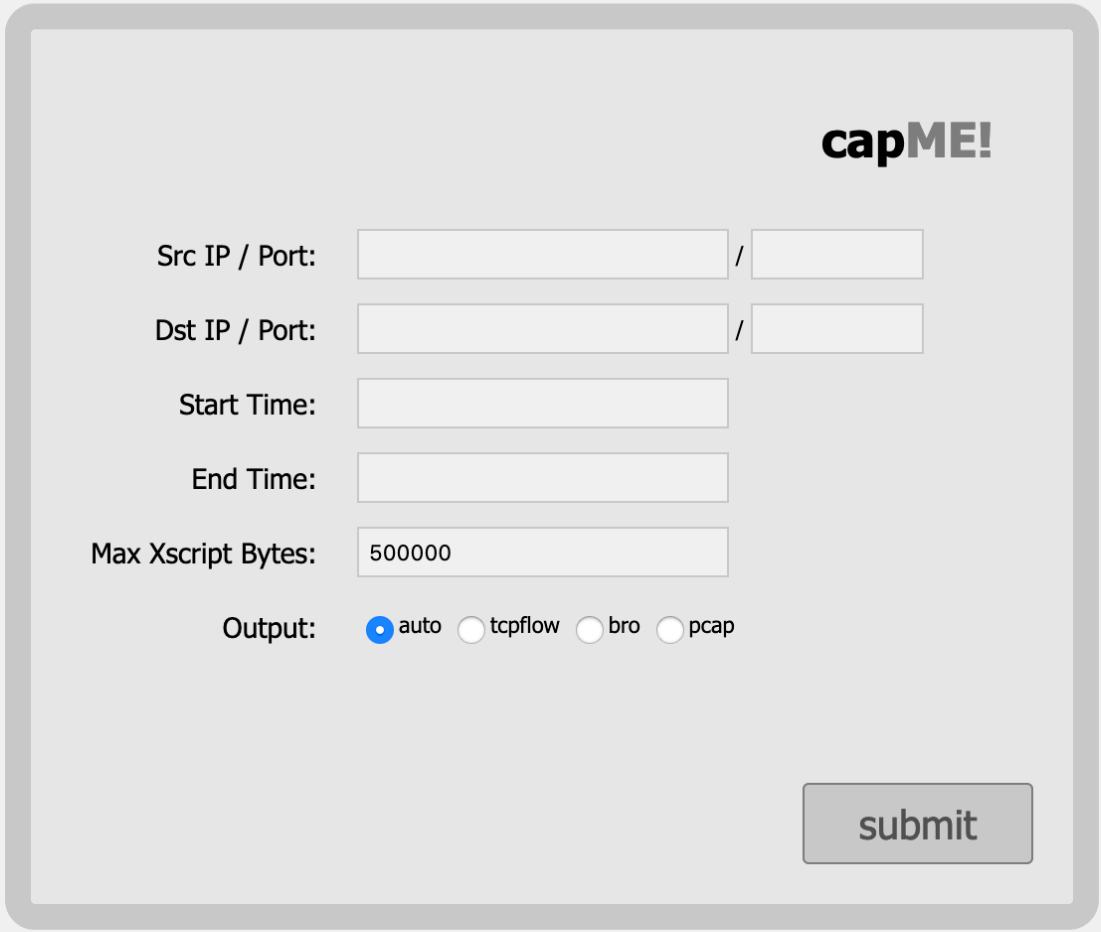
squil


SGUIL-0.9.0 - Connected To 192.168.8.250
File
Query
Reports
Sound: Off
ServerName: 192.168.8.250
UserName: bamm
UserID: 2
2014-11-07 02:02:09 GMT
RealTime Events
Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 fin-ext 1.313990 2014-11-07 00:44:43 222.186.21.55 4270 97.95.102.96 22 6 ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT 1 fin-ext 1.313991 2014-11-07 00:45:55 213.136.94.87 5071 97.95.102.96 5060 17 ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
RT 1 fin-ext 1.313992 2014-11-07 00:45:55 213.136.94.87 5071 97.95.102.96 5060 17 ET SCAN Sipvicious Scan
RT 1 fin-int 7.1033042 2014-11-07 00:50:06 23.235.46.133 80 192.168.8.77 55300 6 ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT 1 fin-ext 1.313993 2014-11-07 00:50:06 23.235.46.133 80 97.95.102.96 55300 6 ET SHELLCODE Excessive Use of HeapLib Objects Likely Malicious Heap Spray Attempt
RT 10 fin-int 7.1033043 2014-11-07 00:50:20 192.168.8.77 55435 208.85.40.20 80 6 ET POLICY Pandora Usage
RT 10 fin-ext 1.313994 2014-11-07 00:50:20 97.95.102.96 55435 208.85.40.20 80 6 ET POLICY Pandora Usage
RT 2 fin-int 7.1033052 2014-11-07 00:54:11 192.168.8.77 51775 192.168.8.253 53 17 ET CURRENT_EVENTS DNS Query to a .tk domain - Likely Hostile
RT 18 fin-int 7.1033054 2014-11-07 00:54:12 192.168.8.77 55671 66.6.44.4 80 6 ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT 18 fin-ext 1.314003 2014-11-07 00:54:12 97.95.102.96 55671 66.6.44.4 80 6 ET CURRENT_EVENTS HTTP Request to a *.tk domain
RT 16 fin-ext 1.314022 2014-11-07 00:59:23 122.225.109.100 50117 97.95.102.96 22 6 ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT 16 fin-int 7.1033080 2014-11-07 00:59:23 122.225.109.100 50117 192.168.8.8 22 6 ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool
RT 8 fin-ext 1.314031 2014-11-07 01:03:40 122.225.109.100 34787 97.95.102.96 22 6 ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT 8 fin-int 7.1033089 2014-11-07 01:03:40 122.225.109.100 34787 192.168.8.8 22 6 ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!
RT 1 fin-ext 1.314059 2014-11-07 01:31:02 221.229.162.150 6000 97.95.102.96 3306 6 ET POLICY Suspicious inbound to mySQL port 3306
RT 2 fin-ext 1.314060 2014-11-07 01:40:46 97.95.102.96 44752 192.30.252.129 22 6 ET SCAN Potential SSH Scan OUTBOUND
RT 1 fin-int 7.1033117 2014-11-07 01:41:31 192.168.8.72 64916 192.30.252.131 22 6 ET SCAN Potential SSH Scan OUTBOUND
IP Resolution
Agent Status
Snort Statistics
System Msgs
User Msgs
Reverse DNS
Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: None Src IP Dst IP
% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '122.225.109.0 - 122.225.109.127'
inetnum: 122.225.109.0 - 122.225.109.127
netname: DINGQI-NETWORK-TECHNOLOGY
country: CN
descr: Shaoxing Dingqi Network Technology Co., Ltd.
descr:
admin-c: JS2095-AP
tech-c: CH119-AP
Show Packet Data
Show Rule
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack!"; flow:established,to_server; content:"SSH-"; content:"libssh"; within:20; threshold: type both, count 5, seconds 30, track by_src; reference:url,doc.emergingthreats.net/2006546; classtype:attempted-admin; sid:2006546; rev:5;)
/sguild_data/rules/fin-int/emerging-scan.rules: Line 490
IP
Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
122.225.109.100 192.168.8.8 4 5 40 63 20152 2 0 103 5091
TCP
Source Port Dest Port R 1 R 0 URG ACK PSH RST SYN FIN Seq # Ack # Offset Res Window Urp ChkSum
34787 22 . . . X X . . . 4171882588 3428280706 5 0 65535 0 21499
DATA
53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 32 5F
31 2E 34 2E 32 0D 0A
SSH-2.0-libssh2_
1.4.2..
Search Packet Payload
Hex
Text
NoCase

squert


EVENTS
SUMMARY
VIEWS
Filter
INTERVAL: 2015-04-21 00:00:00 -> 2015-04-21 23:59:59 (-03:00)
FILTERED BY OBJECT: NO
FILTERED BY SENSOR: NO
PRIORITY: 51.1% 14.5% 34.3%
TOGGLE
queue only on
grouping on
SUMMARY
queued events 995
total events 15149
total signatures 55
PRIORITY
high 496 (51.1%)
medium 141 (14.5%)
low 333 (34.3%)
other -
CLASSIFICATION
compromised L1 -
compromised L2 4 (0.0%)
attempted access 4 (0.0%)
denial of service -
policy violation 1306 (8.6%)
reconnaissance -
malicious 614 (4.1%)
no action req'd. 12226 (80.7%)
escalated event -
TAGS
no tags
HISTORY
no history
1661
2454
779
700
470
443
2010
1396
1743
2335
989
QUEUE SC DC ACTIVITY LAST EVENT SIGNATURE ID PROTO % TOTAL
3 1 2 10:36:04 ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26 2018455 17 0.020%
1 1 1 10:35:54 ET CNC Shadowserver Reported CnC Server IP group 7 2404006 17 0.007%
1 1 1 10:33:49 ET CURRENT_EVENTS Malformed HeartBeat Request 2018372 6 0.007%
3 3 2 10:33:49 ET CURRENT_EVENTS Possible TLS HeartBleed Unencrypted Request Method 3 (Inbound to Common SSL Port) 2018389 6 0.020%
1 1 1 10:33:41 ET TROJAN IRC Channel JOIN on non-standard port 2000348 6 0.007%
194 30 1 10:32:45 MALWARE Blackhole Access (GET) 2011042801 6 1.295%
4 1 4 10:30:31 ET SCAN NETWORK Incoming Masscan detected 2017616 6 0.027%
63 2 8 10:28:07 ET MALWARE Double User-Agent (User-Agent User-Agent) 2003626 6 0.421%
19 1 2 10:22:15 Bro Intel::DOMAIN (gall.dcinside.com) 456939981 6 0.127%
1 1 1 10:21:50 ET CINS Active Threat Intelligence Poor Reputation IP group 23 2403322 17 0.007%
2 2 1 10:21:38 ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Outbound) 2013479 6 0.013%
8 8 1 10:11:22 Bro Weird::Activity 472683000 6 0.053%
5 1 1 10:11:00 ET WEB_CLIENT Hex Obfuscation of document.write % Encoding 2012059 6 0.033%
7 2 2 10:10:40 Bro Scan::Port_Scan 420677484 6 0.047%
4 3 1 10:10:30 Bro Traceroute::Detected 414641093 6 0.027%
3 2 2 10:09:58 Bro Intel::DOMAIN (webwatcherdata.com) 412419124 6 0.020%
16 3 2 10:08:52 ET TROJAN DNS Query for a known malware domain (sektori.org) 2014573 17 0.107%
7 3 3 10:04:42 ET MALWARE All Numerical .cn Domain Likely Malware Related 2012327 17 0.047%
3 1 1 09:58:54 ET WEB_CLIENT Possible HTTP 403 XSS Attempt (External Source) 2010516 6 0.020%
WELCOME paulh | LOGOUT
LOCAL 10:48:11 UTC 13:48:11

CapMe


capME!
Src IP / Port:
/
Dst IP / Port:
/
Start Time:
End Time:
Max Xscript Bytes:
500000
Output:
auto
tcpflow
bro
pcap
submit

CapMe

Logout

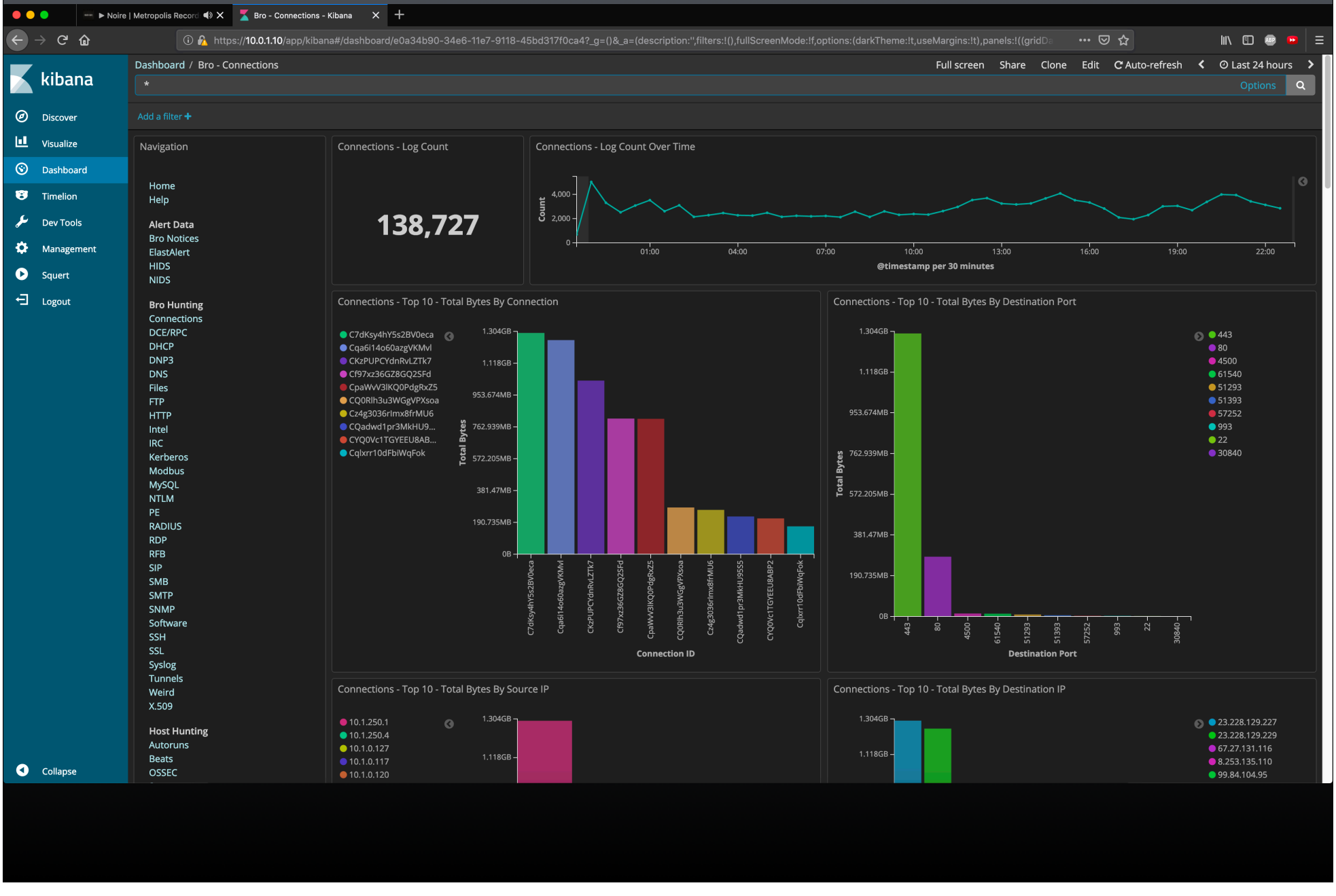
close

10.1.0.156:49392_52.6.141.191:80-6-747067548.pcap

Sensor Name: security-onion-ens224
Timestamp: [redacted]
Connection ID: CLI
Src IP: 10.1.0.156
Dst IP: 52.6.141.191
Src Port: 49392
Dst Port: 80
OS Fingerprint: 10.1.0.156:49392 - UNKNOWN [65535:64:1:64:M1460,N,W7,N,N,T,S,E:PZ:?:?] (up: 4397 hrs)
OS Fingerprint: -> 52.6.141.191:80 (link: ethernet/modem)

SRC: GET /ApiOceanMaSky/api/Config/getConfiguration?device_token=[redacted]
SRC: Host: 52.6.141.191
SRC: Connection: keep-alive
SRC: Accept: */*
SRC: User-Agent:[redacted]
SRC: Accept-Language: en-us
SRC: Authorization: Basic [redacted]
SRC: Accept-Encoding: gzip, deflate
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Cache-Control: no-cache
DST: Pragma: no-cache
DST: Content-Type: application/json; charset=utf-8
DST: Expires: -1
DST: Server: Microsoft-IIS/8.5
DST: X-AspNet-Version: 4.0.30319
DST: X-Powered-By: ASP.NET
DST: Access-Control-Allow-Origin: *
DST: Access-Control-Allow-Headers: Content-Type
DST: Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
DST: Date: [redacted]
DST: Content-Length: 75650
DST:
DST: {"Success":"true","Result":[{"name":"Test Institution","description":"This section is used for a brief description of Museum and contact info \r\n\r\n","mid":"TXVzZXVtQW55V2hlcmU=","museum_status":"1","page_link_label":"Visit Website ","Isfaq":"1","IsProfilePhoto":"0","Ispagelink":"1","page_link":"http://museumanywhere.com","IsfloorPlan":"0","IsguestPass":"1","IsNotification":"1","color_code":"#ff8317","logo":"1542008346.1503497136.logo(1).png","banner_image":"1542008315.1525078730.test_institution.jpg","card_banner_image":"1483537376.main_new.png","card_image":"1542011036.1542008299.1503481175.museum(1).png","blur_card_image":"1488290879.blur_image(new).png","email":"membership@MuseumAnywhere.com","transactionemail":"","lat":"39.0015021","lang":"-77.4489058","block_message":"Your device may have been blocked, please contact organization.","address":"Broderick Dr, Ashburn, VA 20166, USA","IsMemberidHide":"0","contact_number":"(703) 652-6630","search_type":"Membership # Or Phone #","keyboard":"Alpha-numeric","IsCardRestric":"0","cre
DST: ated_at":"2019-01-18 09:26:05","updated_at":"2019-01-18 09:26:05","imagepath":"http://54.164.146.171:8003/uploads/TestInstitution","pass_search_type":"1","barcode_member_type":"2","IsReciprocal":"1","IsChildCount":"1","child_count_label":"Number of children","NotificationFrequency":"45,30,15,5,1","IsEnvelopBypass":"1","DonationAmounts":"","DonationLabel":"","CustomDonationText":"","IsTransactionBuy":false,"IsTransactionRenew":false,"IsTransactionGift":false,"IsTransactionDonate":false,"IsAddressLine":true,"IsSeprateOrg":0,"InApp_show":0,"having_version_control":0,"IsSelected":null,"language_id":"","contact_ext":"11","RenewLink":"","ituneID":1161384548,"wallet_Identifier":"pass.com.infi.EcardDemo","team_Identifier":"ERPN25DUP3","pass_member_since":"1","pass_valid_though":"1","pass_member_type":"1","wallet_cert_name":"PassCertAll.p12","wallet_cert_password":"1234567","IsImgCentrAlign":1,"IsBenefitBtnShow":true,"IsImprovedBarcode":true,"IsNamePopUp":false,"device_details":[],"languages":[{"id":1,"title":"English","short_code":"","Organisation_key":"TXVzZXVtQW55V2hlcmU="}],"extra_menu_item":[{"Id":1,"Organisation_key":"TXVzZXVtQW55V2hlcmU=","Key":"Google","Value":"http://www.google.com"},{"Id":2,"Organisation_key":"TXVzZXVtQW55V2hlcmU=","Key":"LinkedIn","Value":"http://www.linkedin.com"}]},{"name":"NEW Zoo & Adventure Park","description":"The Northeastern Wisconsin Zoo is located near Green Bay, Wisconsin.","mid":"TkVXIFpvbyAmIE
DST: FkdmVudHVyZSBQYXJr","museum_status":"1","page_link_label":"","Isfaq":"1","IsProfilePhoto":"0","Ispagelink":"0","page_link":"","IsfloorPlan":"1","IsguestPass":"0","IsNotification":"1","color_code":"#0d2f06","logo":"1489044230.logo.png","banner_image":"1518526196.NEWZoo&AdventurePark.jpg","card_banner_image":"1488446886.PenguinHeader-actualcard.jpg","card_image":"1489044651.Card_new_zoo.png","blur_card_image":"1489044528.logo.png","email":"info@newzoo.org","transactionemail":"info@newzoo.org","lat":"44.6603403","lang":"-88.0893326","block_message":"Your device may have been blocked, please contact membership.","address":"4378 Reforestation Rd, Suamico, WI 54313, USA","IsMemberidHide":"0","contact_number":"(920) 434-7841","search_type":"Membership # Or Phone #","keyboard":"Alpha-numeric","IsCardRestric":"0","created_at":"2018-02-13 12:50:22","updated_at":"2018-02-13 12:50:22","imagepath":"http://54.164.146.171:8003/uploads/NEWZoo&AdventurePark","pass_search_type":"1","barcode_member_type":"2","IsReciprocal":"1","IsChildCount":"1","child_count_label":"Number of children","NotificationFrequency":"60,45,30,15,5,1","IsEnvelopBypass":"1","DonationAmou

Kibana


Bro - Connections - Kibana
https://10.0.1.10/app/kibana#/dashboard/e0a34b90-34e6-11e7-9118-45bd317f0ca4?_g=()&_a=(description:'',filters:!(),fullScreenMode:!f,options:(darkTheme:!t,useMargins:!t),panels:!((gridD
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Dashboard / Bro - Connections
Full screen
Share
Clone
Edit
Auto-refresh
Last 24 hours
*
Options
Add a filter +
Navigation
Home
Help
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS
Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird
X.509
Host Hunting
Autoruns
Beats
OSSEC
Connections - Log Count
138,727
Connections - Log Count Over Time
Count
4,000
2,000
0
01:00
04:00
07:00
10:00
13:00
16:00
19:00
22:00
@timestamp per 30 minutes
Connections - Top 10 - Total Bytes By Connection
C7dKsy4hY5s2BV0eca
Cqa6i14o60azgVKMvl
CKzPUPCYdnRvLZTk7
Cf97xz36GZ8GQ2SFd
CpaWvV3lKQ0PdgRxZ5
CQ0Rlh3u3WGgVPXsoa
Cz4g3036rImx8frMU6
CQadwd1pr3MkHU9...
CYQ0Vc1TGYEEU8AB...
Cqlxrr10dFbiWqFok
1.304GB
1.118GB
953.674MB
762.939MB
572.205MB
381.47MB
190.735MB
0B
Total Bytes
Connection ID
Connections - Top 10 - Total Bytes By Destination Port
443
80
4500
61540
51293
51393
57252
993
22
30840
Destination Port
Connections - Top 10 - Total Bytes By Source IP
10.1.250.1
10.1.250.4
10.1.0.127
10.1.0.117
10.1.0.120
Connections - Top 10 - Total Bytes By Destination IP
23.228.129.227
23.228.129.229
67.27.131.116
8.253.135.110
99.84.104.95

Hands on time…

Lab Instructions

https://github.com/wave-length/Presentations/

Go to MAR19-DC919-SecurityOnion

Contact Information

@__wavelength__

(two underscores before/after)

darkwavelength@protonmail.ch