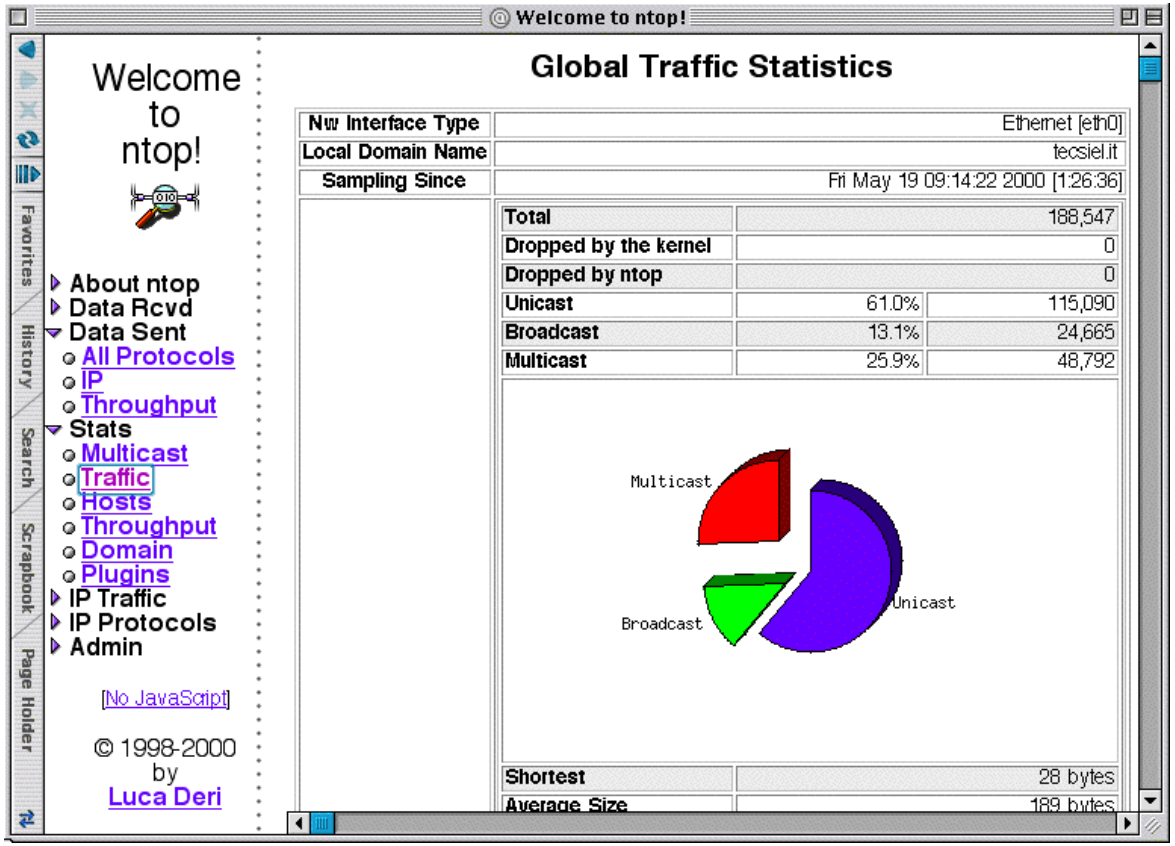
How to Monitor What Matters

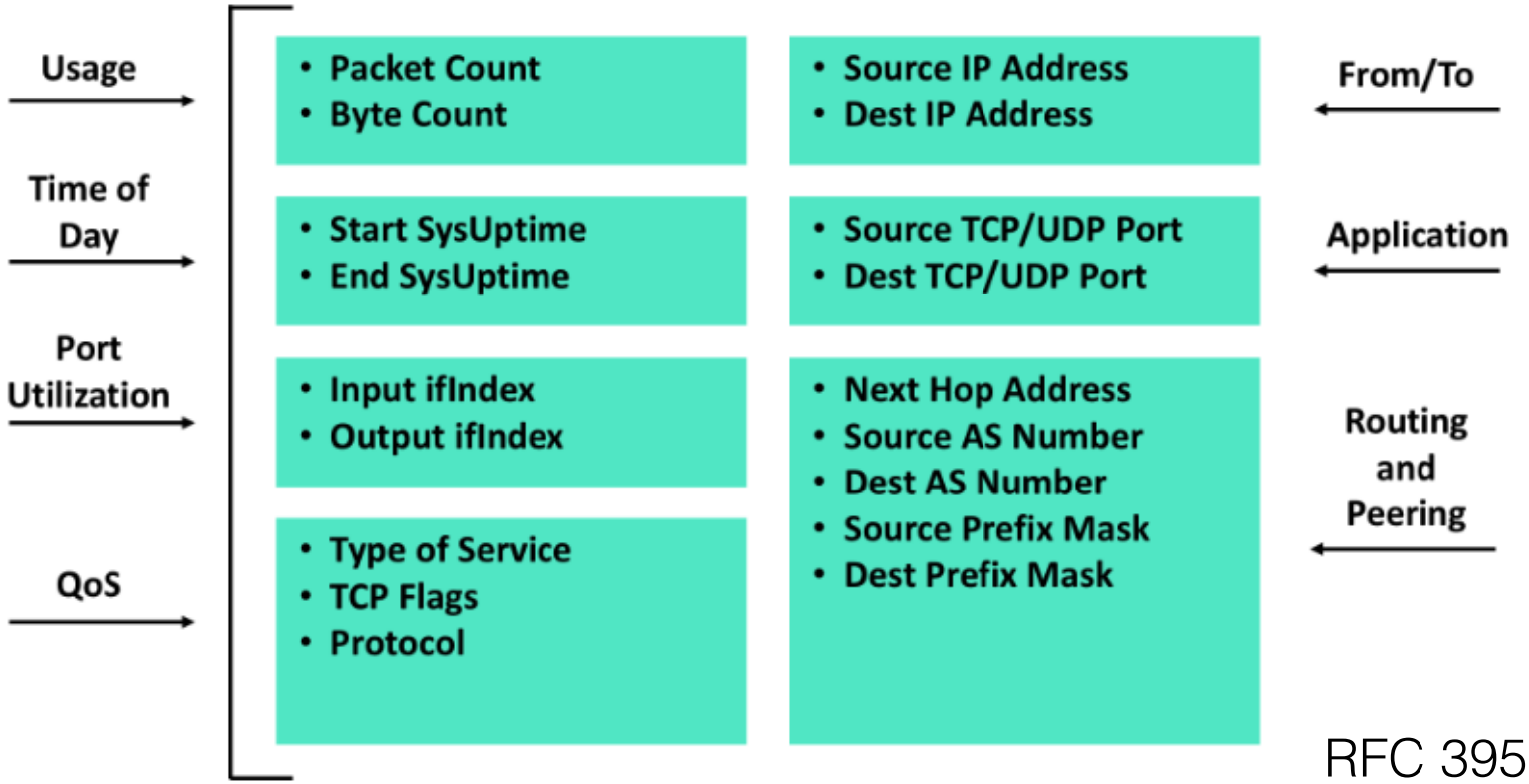
Luca Deri <deri@ntop.org>
@lucaderi

ntop

25 Years Ago (1998)



What's Inside a Flow ? (2004)



RFC 3954

Flow Analysis: Pros and Cons

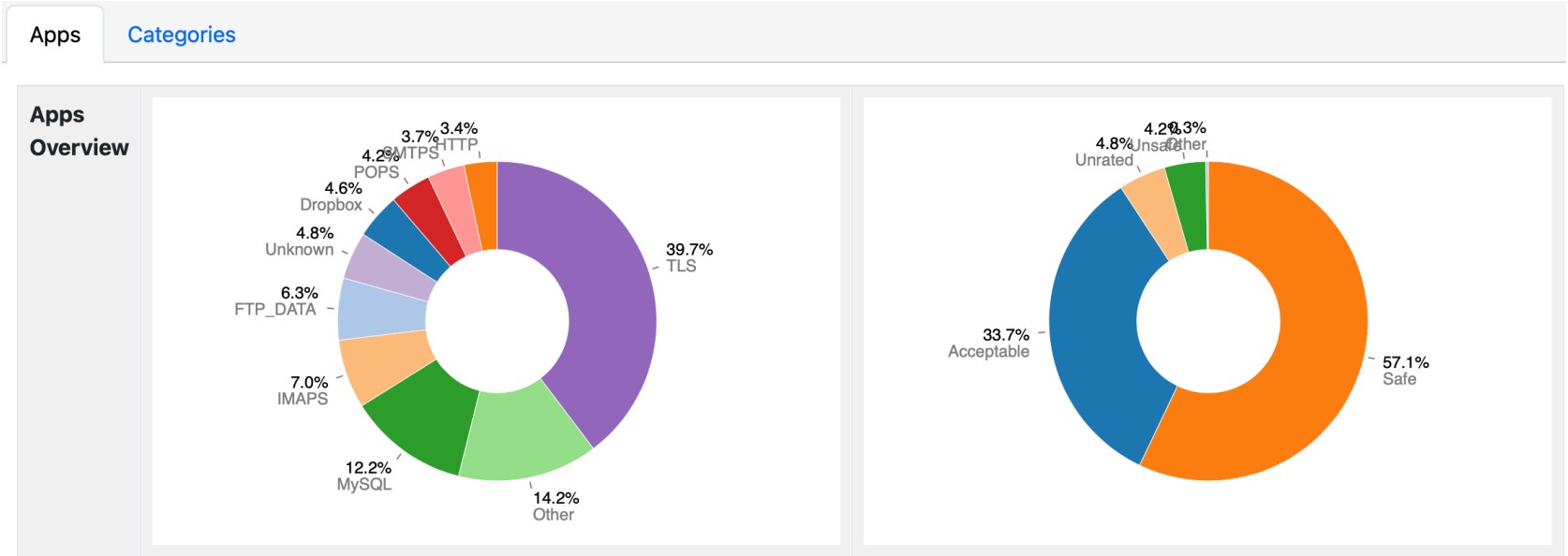
- Many network vendors are not fully compliant with standard, making flow-based measurement a nightmare.
- Cloud providers defined new proprietary (AWS Cloud VPC, 2009):

```
account-id action az-id bytes dstaddr dstport end flow-direction instance-id interface-id log-status packets pkt-dst-
aws-service pkt-dstaddr pkt-src-aws-service pkt-srcaddr protocol region srcaddr srcport start sublocation-id
sublocation-type subnet-id tcp-flags traffic-path type version vpc-id
421717577885 ACCEPT use1-az6 396 10.113.39.219 80 1640154903 ingress - eni-0afec37a7c4be140d OK 5 - 10.113.39.219 -
10.113.39.208 6 us-east-1 10.113.39.208 7652 1640154859 - - subnet-048dbd0af4e64ae1f 3 - IPv4 5 vpc-0f4cdb08d3b1bcdf6
421717577885 ACCEPT use1-az6 1895 10.113.39.208 7652 1640154903 egress - eni-0afec37a7c4be140d OK 5 - 10.113.39.208 -
10.113.39.219 6 us-east-1 10.113.39.219 80 1640154859 - - subnet-048dbd0af4e64ae1f 19 1 IPv4 5 vpc-0f4cdb08d3b1bcdf6
```

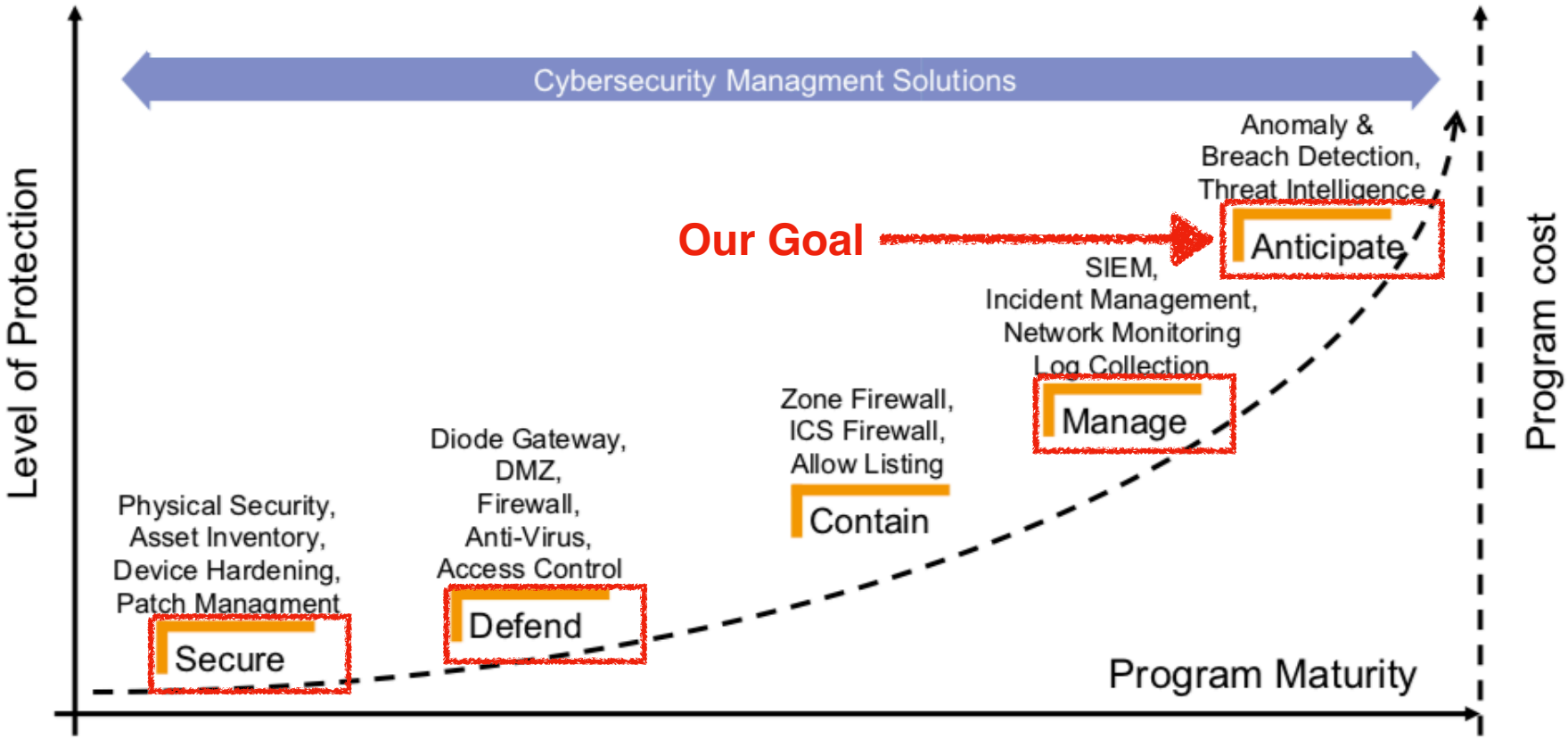
- Traditional traffic analysis is often still limited to simple top/bottom X (elephants/mice) statistics: top talkers/ASs/protocols.
- In summary: no application protocol visibility, lack of detailed network metrics, and pool vendor implementations prevented advances in this area for a long time.

nDPI (2012)

- Inspect packet payload (including encrypted content) and detect the used application protocol (e.g. TLS.Teams).
- Enhanced flows providing contextual information.



From “Manage” to “Anticipate” (2021)

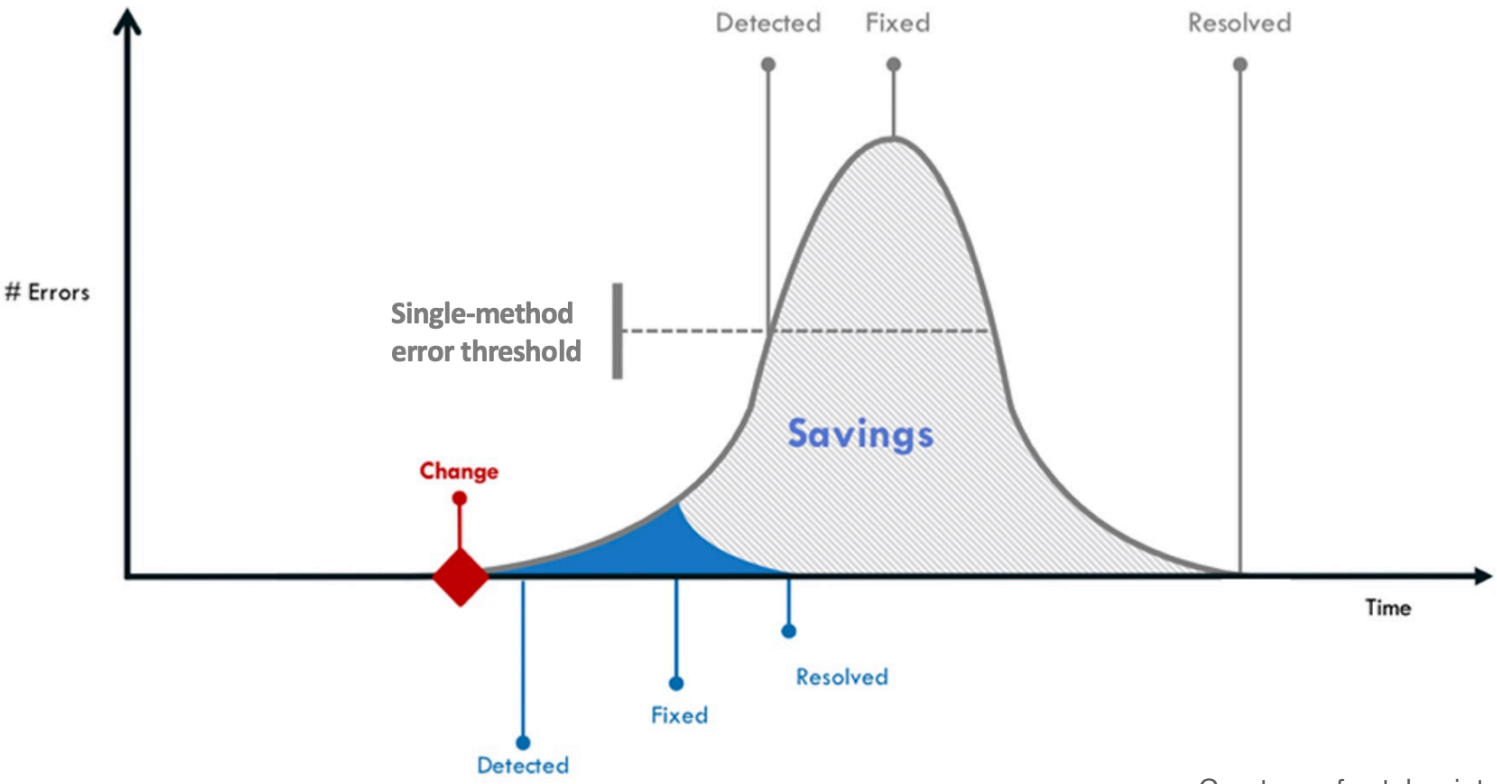


Courtesy of switch.ch

How Can we Anticipate a Problem?

- Monitoring can show you when a problem is happening or (better) what are metrics that can be an indication of a future problem.
- Modern observability systems provide many metrics that human operators cannot analyse fully, as they are simply too many.
- System visibility is required to complement network visibility and predict issues when network signals are hidden (e.g. by cryptography).
- How can we make our monitoring systems smarter and simpler to use for users.

Detect, Identify, Fix. Faster.



Courtesy of catchpoint.com

Make Invisible Visible

- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- TLS connections not carrying HTTPS (e.g. a VPN over TLS)
- Suspicious DGA domain contacted
- Malformed packet
- SSH/SMB obsolete protocol or application version
- TLS suspicious ESNI usage
- Unsafe Protocol used
- Suspicious DNS traffic
- TLS with no SNI
- XSS (Cross Site Scripting)
- SQL Injection

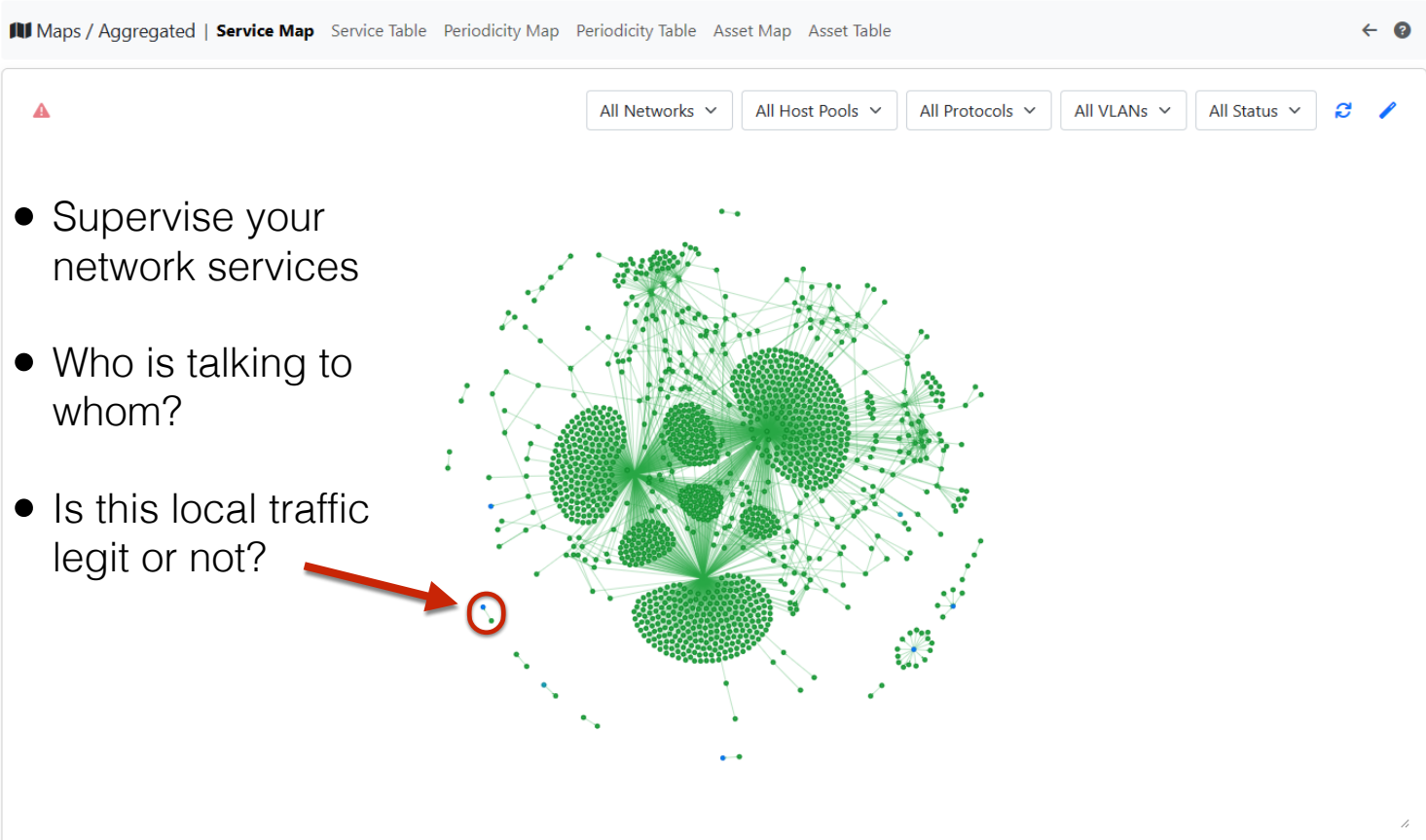
- Arbitrary Code Injection/Execution
- Binary/.exe application transfer (e.g. in HTTP)
- Known protocol on non standard port
- TLS self-signed certificate
- TLS obsolete version
- TLS weak cipher
- TLS certificate expired
- TLS certificate mismatch
- DNS suspicious traffic
- HTTP suspicious content
- Risky ASN
- Risky Domain Name
- Malicious JA3 Fingerprint
- Malicious SHA1 Certificate
- Desktop of File Sharing Session
- TLS Uncommon ALPN

- TLS Certificate Validity Too Long
- Suspicious TLS Extension
- TLS Fatal Alert
- Suspicious Protocol traffic Entropy
- Clear-text Credentials Exchanged
- DNS Large Packet
- DNS Fragmented Traffic
- Invalid Characters Detected
- Possible Exploit Detected
- TLS Certificate Close to Expire
- Punycode/IDN Domain
- Error Code Detected
- Crawler/Bot Detected
- Anonymous Subscriber
- Unidirectional Traffic
- HTTP Obsolete Server
- ……

Legenda: Clear Text Only, Encrypted/Plain Text, Encrypted Only

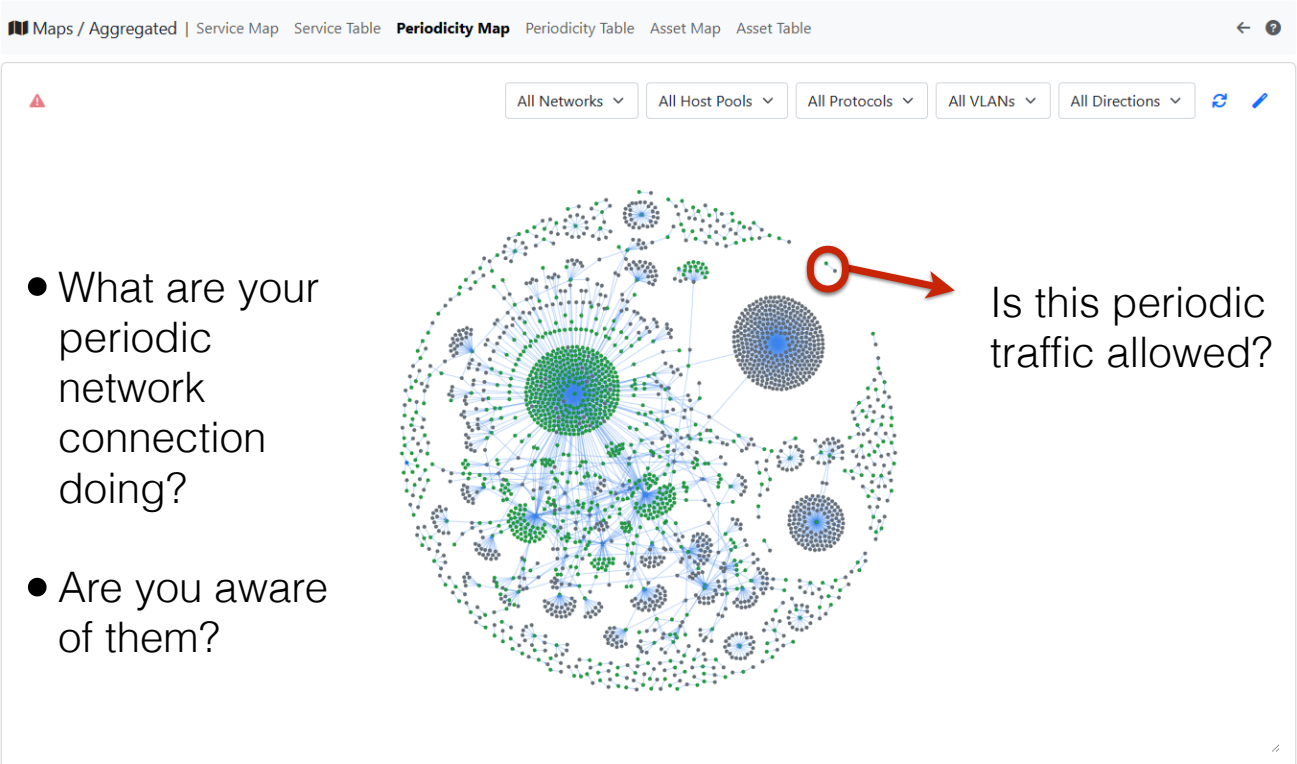
ntop

Detect Changes



- Supervise your network services
- Who is talking to whom?
- Is this local traffic legit or not?

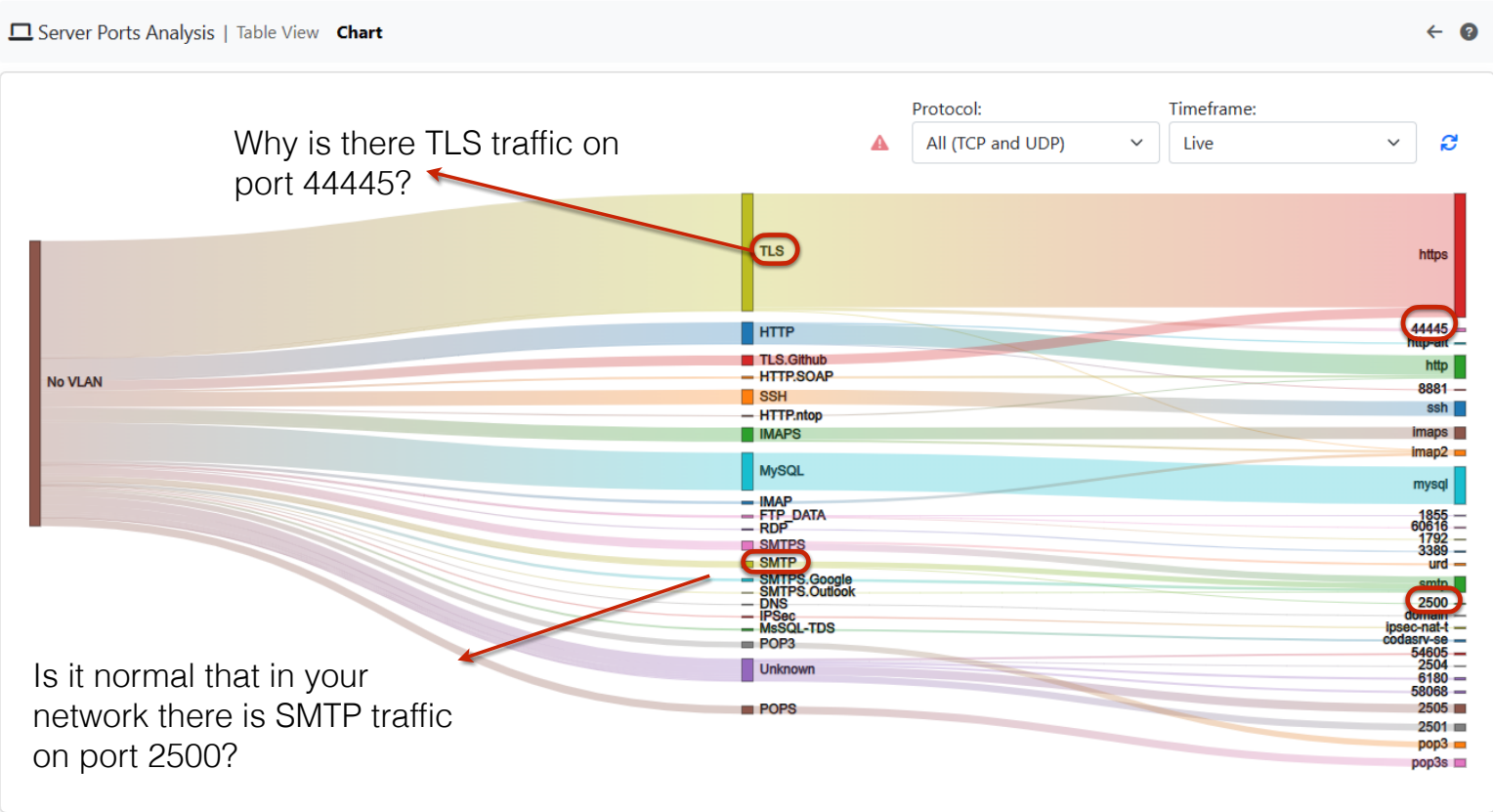
Identify Beaconing



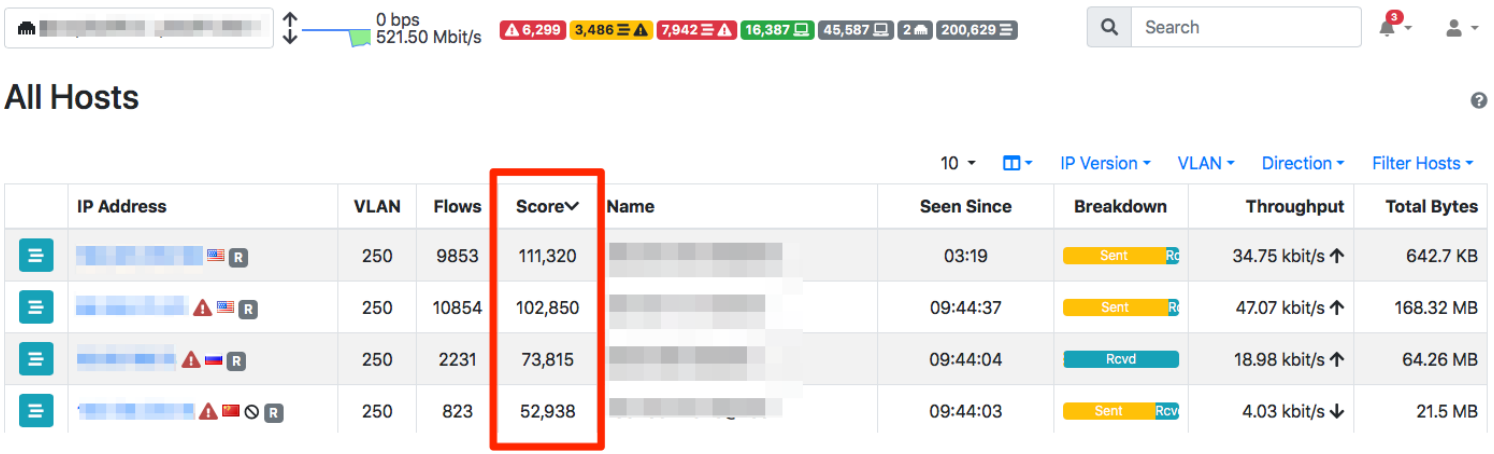
- What are your periodic network connection doing?
- Are you aware of them?

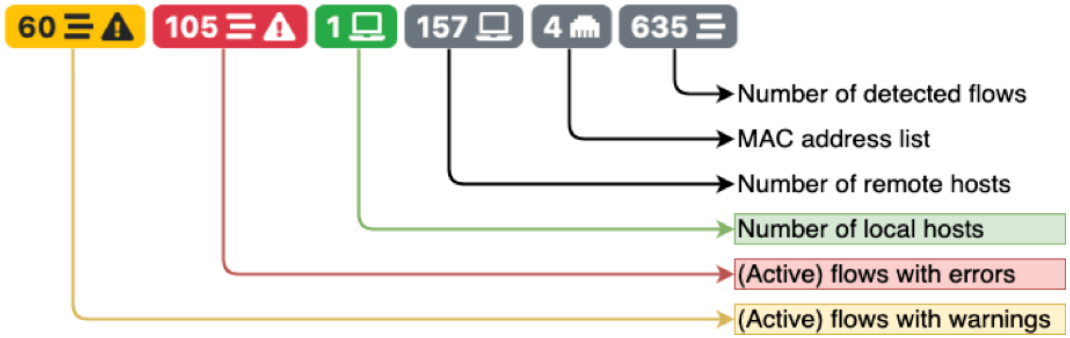
Is this periodic traffic allowed?

Fix Unwanted Traffic

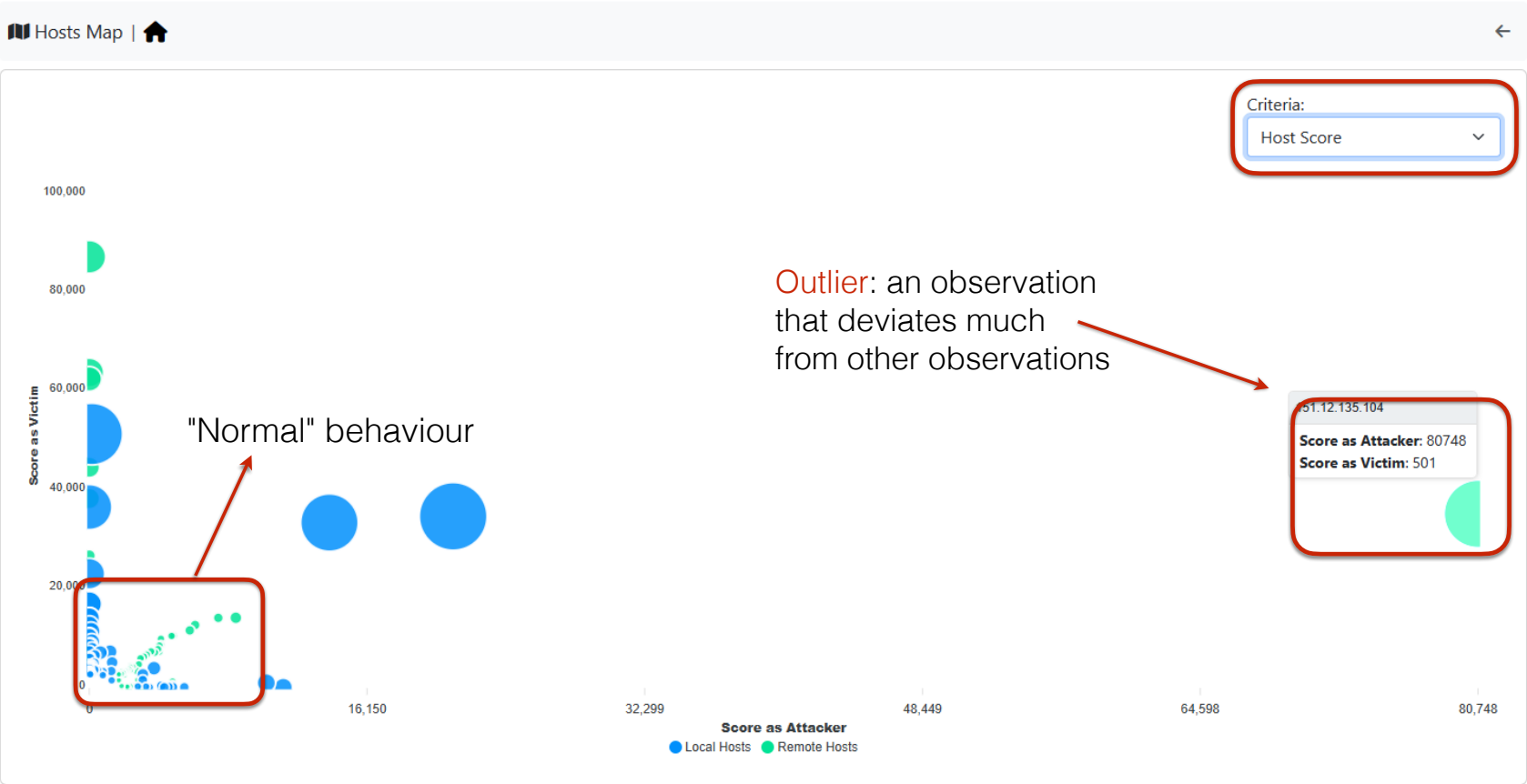


Label “Unhealthy” Activities





Spot CyberThreats



Burglar Alarms

Device/MAC Address Tracking List | **Devices**

The Device/MAC Address Tracking is still learning the devices...

Show 10 Entries

What is it doing here?

Search:

Actions	Device	IP Address	Manufacturer	First Seen	Last Seen	Device Status	Trigger Disconnection Alert
	00:04:96:E4:AA:CD	192.168.2.237	Extreme Networks, Inc.	08:33:02	10:31:53	Denied	✕
	AC:1F:6B:AD:6A:2C	192.168.2.134	Super Micro Computer, Inc.	08:33:04	10:31:50	Allowed	✕
	00:0C:29:95:B1:4C	fe80::20c:29ff:fe95:b14c	VMware, Inc.	08:32:51	10:33:09	Allowed	✕
	0C:C4:7A:CC:4E:6E	fe80::ec4:7aff:fecc:4e6e	Super Micro Computer, Inc.	08:32:34	10:32:34	Allowed	✕
	00:0C:29:6C:EB:A2	fe80::20c:29ff:fe6c:eba2	VMware, Inc.	08:33:43	10:32:51	Allowed	✕
	20:FD:F1:CB:87:BE	192.168.2.175	3Com Europe Ltd	08:35:01	10:30:15	Allowed	✕
	00:0C:29:37:0D:05	fe80::20c:29ff:fe37:d05	VMware, Inc.	08:33:10	10:31:44	Allowed	✕
	09:00:09:00:00:67			09:46:15	10:32:15	Allowed	✕
	54:9F:35:19:69:C6		Dell Inc.	10:02:29	10:21:29	Allowed	✕
	44:A8:42:3B:32:5E	192.168.2.178	Dell Inc.	08:32:00	10:33:05	Allowed	✕

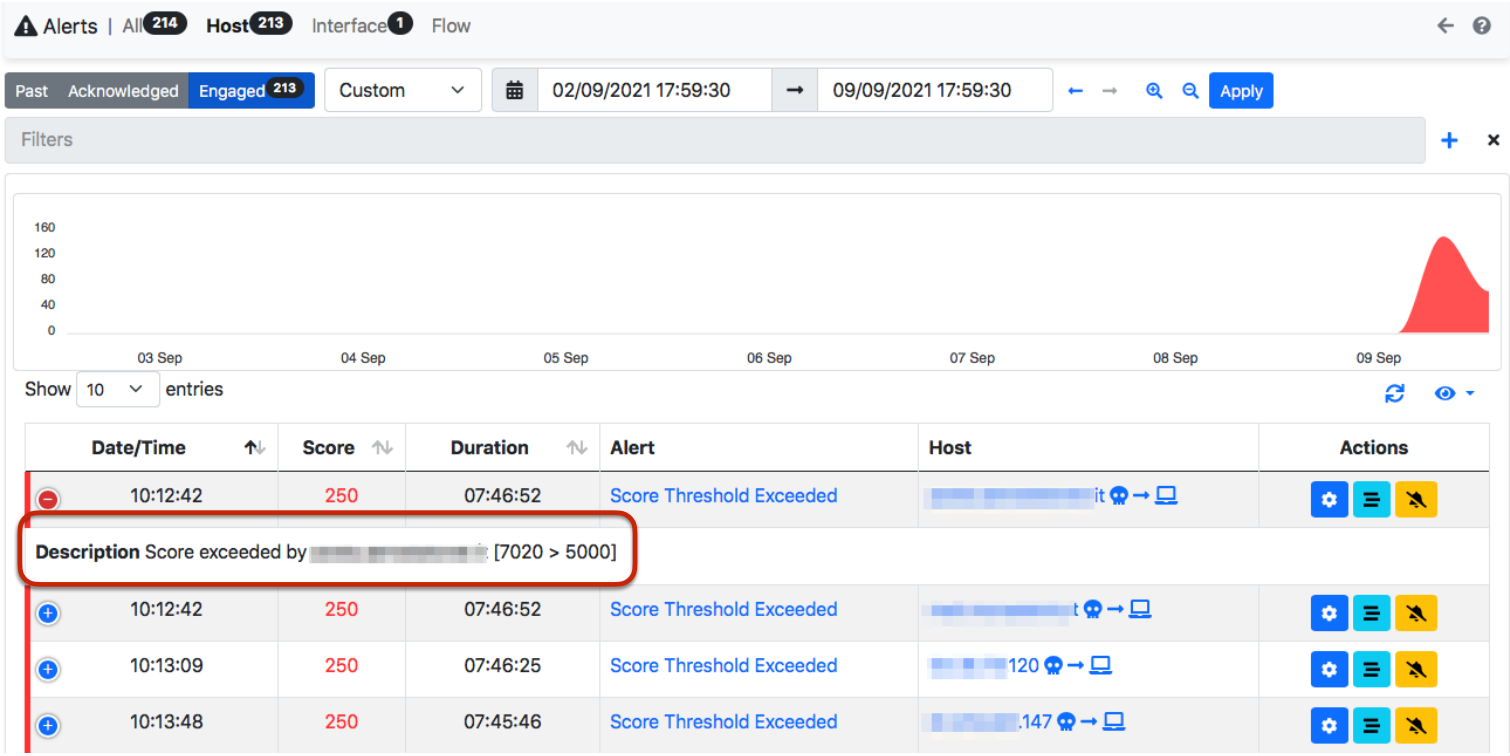
Showing page 1 of 4: total 34 rows

< 1 2 3 4 >

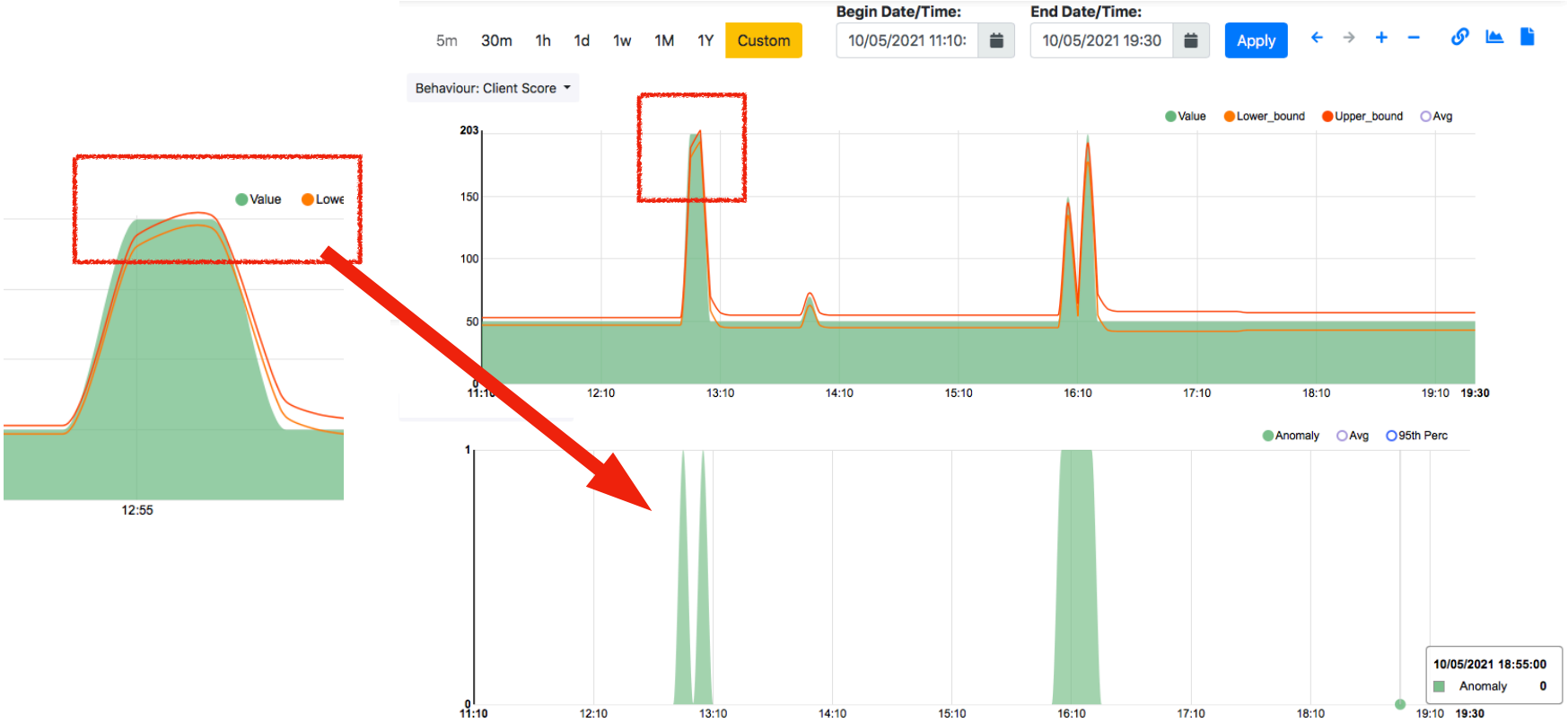
Alert me if hosts disconnect

When did it happen?

Threshold-based Alerts



Behavioural Alerts



User Experience Monitoring

Skype_TeamsCall Flows

0 bps | Total Bytes: 1.22 MB
0 bps | Total Throughput: 0 bps

Flow Idle Timeout: 60 sec

10 · Hosts · Status · Severity · Direction · L7 Protocol · Categories · DSCP · Host Pool · Networks · IP Version · Protocol

Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	STUN.Skype_T... DPI	UDP	imacm1 R :50014	host-82-51-138-80.retail.telecomital... R :59225	< 1 sec	50	Client Server	0 bps	726.86 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	192.168.1.125 R :50042	imacm1 R :50044	< 1 sec	50	Server	0 bps	400.04 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50054	52.114.227.13 R :nat-stun-port	< 1 sec	10	Client	0 bps	58.76 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50014	52.114.227.31 R :nat-stun-port	< 1 sec		Client S	0 bps	8.87 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50020	52.114.227.44 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.74 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50032	52.114.227.38 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.31 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50032	host-82-51-138-80.retail.telecomital... R :57022	< 1 sec	50	Client	0 bps	7.03 KB	Video Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50054	host-82-51-138-80.retail.telecomital... R :52292	< 1 sec	50	Client	0 bps	5.46 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50044	52.114.227.31 R :nat-stun-port	< 1 sec	10	Client	0 bps	3.4 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50020	host-82-51-138-80.retail.telecomital... R :49621	< 1 sec	50	Client S	0 bps	3.27 KB	Video Stream

```
[NFv9 57626][IPFIX 35632.154][Len 4] %RTP_IN_JITTER              RTP jitter (ms * 1000)
[NFv9 57627][IPFIX 35632.155][Len 4] %RTP_OUT_JITTER             RTP jitter (ms * 1000)
[NFv9 57628][IPFIX 35632.156][Len 4] %RTP_IN_PKT_LOST            Packet lost in stream (src->dst)
[NFv9 57629][IPFIX 35632.157][Len 4] %RTP_OUT_PKT_LOST           Packet lost in stream (dst->src)
[NFv9 57902][IPFIX 35632.430][Len 4] %RTP_IN_PKT_DROP            Packet discarded by Jitter Buffer (src->dst)
[NFv9 57903][IPFIX 35632.431][Len 4] %RTP_OUT_PKT_DROP           Packet discarded by Jitter Buffer (dst->src)
[NFv9 57633][IPFIX 35632.161][Len 1] %RTP_IN_PAYLOAD_TYPE        RTP payload type
[NFv9 57630][IPFIX 35632.158][Len 1] %RTP_OUT_PAYLOAD_TYPE       RTP payload type
[NFv9 57631][IPFIX 35632.159][Len 4] %RTP_IN_MAX_DELTA           Max delta (ms*100) between consecutive pkts (src->dst)
[NFv9 57632][IPFIX 35632.160][Len 4] %RTP_OUT_MAX_DELTA          Max delta (ms*100) between consecutive pkts (dst->src)
[NFv9 57820][IPFIX 35632.348][Len 64 varlen] %RTP_SIP_CALL_ID    SIP call-id corresponding to this RTP stream
[NFv9 57906][IPFIX 35632.434][Len 4] %RTP_MOS                    RTP pseudo-MOS (value * 100) (average both directions)
[NFv9 57842][IPFIX 35632.370][Len 4] %RTP_IN_MOS                 RTP pseudo-MOS (value * 100) (src->dst)
[NFv9 57904][IPFIX 35632.432][Len 4] %RTP_OUT_MOS                RTP pseudo-MOS (value * 100) (dst->src)
[NFv9 57908][IPFIX 35632.436][Len 4] %RTP_R_FACTOR               RTP pseudo-R_FACTOR (value * 100) (average both directions)
[NFv9 57843][IPFIX 35632.371][Len 4] %RTP_IN_R_FACTOR            RTP pseudo-R_FACTOR (value * 100) (src->dst)
[NFv9 57905][IPFIX 35632.433][Len 4] %RTP_OUT_R_FACTOR           RTP pseudo-R_FACTOR (value * 100) (dst->src)
[NFv9 57853][IPFIX 35632.381][Len 4] %RTP_IN_TRANSIT             RTP Transit (value * 100) (src->dst)
[NFv9 57854][IPFIX 35632.382][Len 4] %RTP_OUT_TRANSIT            RTP Transit (value * 100) (dst->src)
[NFv9 57852][IPFIX 35632.380][Len 4] %RTP_RTT                    RTP Round Trip Time (ms)
```

User Satisfaction Level	MOS	R-Factor
Maximum using G.711	4.4<	93
Excellent	4.3 – 5.0	90 – 100
Good	4.0 – 4.3	80 – 90
Satisfied	3.6 – 4	70 – 80
Dissatisfied	3.1 – 3.6	60 – 70
Fully dissatisfied	2.6 – 3.1	50 – 60
Not recommended	1.0 – 2.6	Less than 50

Patch Your CVEs

Vulnerability Scan | Open Ports **Scan Details**

Vulnerability Scan Report of 192.168.2.172 at 11:17:45

```
22/tcp   open  ssh      Dropbear sshd 2013.60 (protocol 2.0)
 vulscan: cve.csv:
[CVE-2012-0920] Use-after-free vulnerability in Dropbear SSH Server 0.52 through 2012.54, when command restriction and public key authentication are enabled, al
[CVE-2009-3340] Unspecified vulnerability in FreeSSHD 1.2.4 allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certa
[CVE-2008-3234] sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinu
[CVE-2006-5794] Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been
[CVE-2006-1283] opiepasswd in One-Time Passwords in Everything (OPIE) in FreeBSD 4.10-RELEASE-p22 through 6.1-STABLE before 20060322 uses the getlogin function
[CVE-2002-0460] Bitvise WinSSHD before 2002-03-16 allows remote attackers to cause a denial of service (resource exhaustion) via a large number of incomplete co

80/tcp   open  http     ATEN/Supermicro IPMI web interface
 vulscan: cve.csv:
[CVE-2013-4785] The web interface for Dell iDRAC 6 firmware 1.7, and possibly other versions, allows remote attackers to modify the CLP interface for arbitrary
[CVE-2013-4731] ajax.cgi in the web interface on the Choice Wireless Green Packet WIXFMR-111 4G WiMax modem allows remote attackers to execute arbitrary command
[CVE-2013-4620] Cross-site scripting (XSS) vulnerability in interface/main/onotes/officecommentsfull.php in OpenEMR 4.1.1 allows remote attackers to inject arbi
[CVE-2013-4038] The Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) on IBM BladeCenter, Flex System, Syste
[CVE-2013-4037] The RAKP protocol support in the Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) and Integ
[CVE-2013-4031] The Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) and Integrated Management Module II (I
[CVE-2013-3633] The web interface on Siemens Scalance X200 IRT switches with firmware before X-200IRT 5.1.0 relies on client-side privilege checks, which allows
[CVE-2013-3581] ajax.cgi in the web interface on the Choice Wireless Green Packet WIXFMR-111 4G WiMax modem allows remote attackers to obtain sensitive informat
[CVE-2013-3500] The Foundation webapp admin interface in GroundWork Monitor Enterprise 6.7.0 uses the nagios account as the owner of writable files under /usr/l
[CVE-2013-3457] Absolute path traversal vulnerability in the web interface in Cisco Finesse allows remote attackers to read directory contents via a direct requ
[CVE-2013-3440] Multiple cross-site scripting (XSS) vulnerabilities in the administrative web interface in Cisco Unified Operations Manager allow remote attacke
[CVE-2013-3428] The web interface in Cisco Secure Access Control System (ACS) does not properly suppress error-condition details, which allows remote authentica
[CVE-2013-3423] Cross-site scripting (XSS) vulnerability in the web interface in Cisco Secure Access Control System (ACS) allows remote attackers to inject arbi
[CVE-2013-3380] The administrative web interface in the Access Control Server in Cisco Secure Access Control System (ACS) does not properly restrict the report
[CVE-2013-3080] VMware vCenter Server Appliance (vCSA) 5.1 before Update 1 allows remote authenticated users to create or overwrite arbitrary files, and conseque
```

Agent vs Agent-Less Monitoring

Live Flows | Analysis

Recently Live Flows

10 Hosts Status Severity Direction L7 Protocol Categories DSCP Host Pool Networks IP Version Protocol

Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes
	? Unknown Unknown	TCP	192.168.2.153@luca R:58266	dell@luca L:3000	00:03 sec	50	Server	1.90 Mbps	4.62 MB
	? Unknown Unknown	TCP	192.168.2.153@luca R:58263	dell@luca L:3000	00:01 sec	50			
	? Unknown Unknown	TCP	192.168.2.153@luca R:58277	dell@luca L:3000	< 1 sec				
	SNMP DPI	UDP	dell@luca L:36161 [>_ ntopng]	192.168.2.237@luca R:snmp	00:05 sec				
	SNMP DPI	UDP	dell@luca L:43437 [>_ ntopng]	192.168.2.169@luca R:snmp	00:04 sec				
	? Unknown Unknown	TCP	192.168.2.153@luca R:58273	dell@luca L:3000	< 1 sec				
	SNMP DPI	UDP	dell@luca L:41436 [>_ ntopng]	192.168.2.175@luca R:snmp	00:04 sec				
	SNMP DPI	UDP	dell@luca L:40879 [>_ ntopng]	192.168.2.106@luca R:snmp	00:03 sec				
	? Unknown Unknown	TCP	192.168.2.153@luca R:58267	dell@luca L:3000	< 1 sec	50			
	SNMP DPI	UDP	dell@luca L:36455 [>_ ntopng]	192.168.2.222@luca R:snmp	< 1 sec				

Host: dell | Traffic Packets Ports Peers ICMP Apps DNS SNMP Processes

Show 10 entries Search:

Protocol	Port	Process	Package Name
tcp4	22	/usr/sbin/sshd	openssh-server
tcp6	22	/usr/sbin/sshd	openssh-server
tcp4	25	/usr/lib/postfix/sbin/master	postfix
udp4	53	/usr/sbin/dnsmasq	dnsmasq-base
tcp4	53	/usr/sbin/dnsmasq	dnsmasq-base
udp4	67	/usr/sbin/dnsmasq	dnsmasq-base
udp4	68	/usr/sbin/dhclient	
udp4	123	/usr/sbin/ntpd	ntp
udp6	123	/usr/sbin/ntpd	ntp
udp4	161	/usr/sbin/snmpd	snmpd

Showing 1 to 10 of 20 entries

« < 1 2 > »

Notify Me When Something Goes Wrong

In Summary

- Monitor what matters, not what vendors decide
  - Focus is on monitoring every aspect of the internet stack
- Catch issues before they become incidents
  - HD real-time data (bytes/packets are no longer enough)
  - Advanced correlation (monitoring system knows my network better)
  - Experience and cyber scores (quality and security)
  - Analysis/drill-down tools (from alerts to flows to packets

25 Years of Open Source

- ntopng
- nProbe (Agent)
- n2disk (with Smart Recording)
- nBox UI
- nDPI
- PF_RING

https://github.com/ntop/