3-1-7
ISP Intrusion Detection

ISP Intrusion Detection

- Monitor your own network—but that’s no different than any other enterprise
- Monitor your customers
  - Good: you can help them by detecting problems
  - Good: you can prevent them from clogging your infrastructure
  - Bad: it can be privacy-invasive

Signature Detection

Look for known-bad types of traffic coming from your customers

Perhaps run Bro on your upstream links

Example: connection attempts to your dark space

Example: Connections to your email submission server from too many strange places

Example: Connections to known botnet controller

Anomaly Detection

Could monitor upstream links for odd traffic

However—a lot of misbehavior shows up in traffic metadata (even if you're not the NSA)

Use Netflow to spot oddities or *changes* in customer behavior

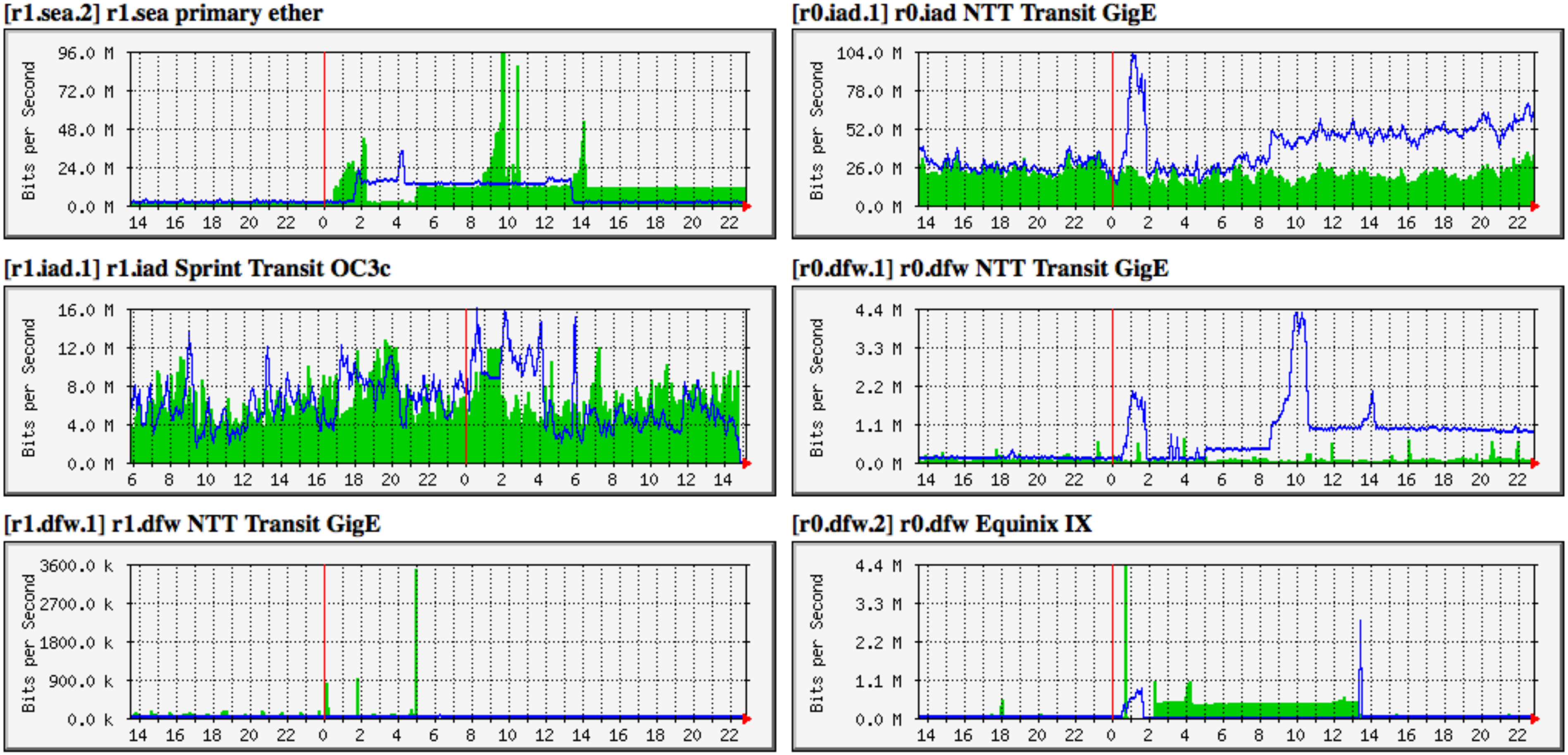
But—watch out for new applications, or new-to-this-customer applications

Monitor Your Network Traffic

SNMP/MRTG

NetFlow/NFSEN

Monitor Traffic



[r1.sea.2] r1.sea primary ether

[r0.iad.1] r0.iad NTT Transit GigE

[r1.iad.1] r1.iad Sprint Transit OC3c

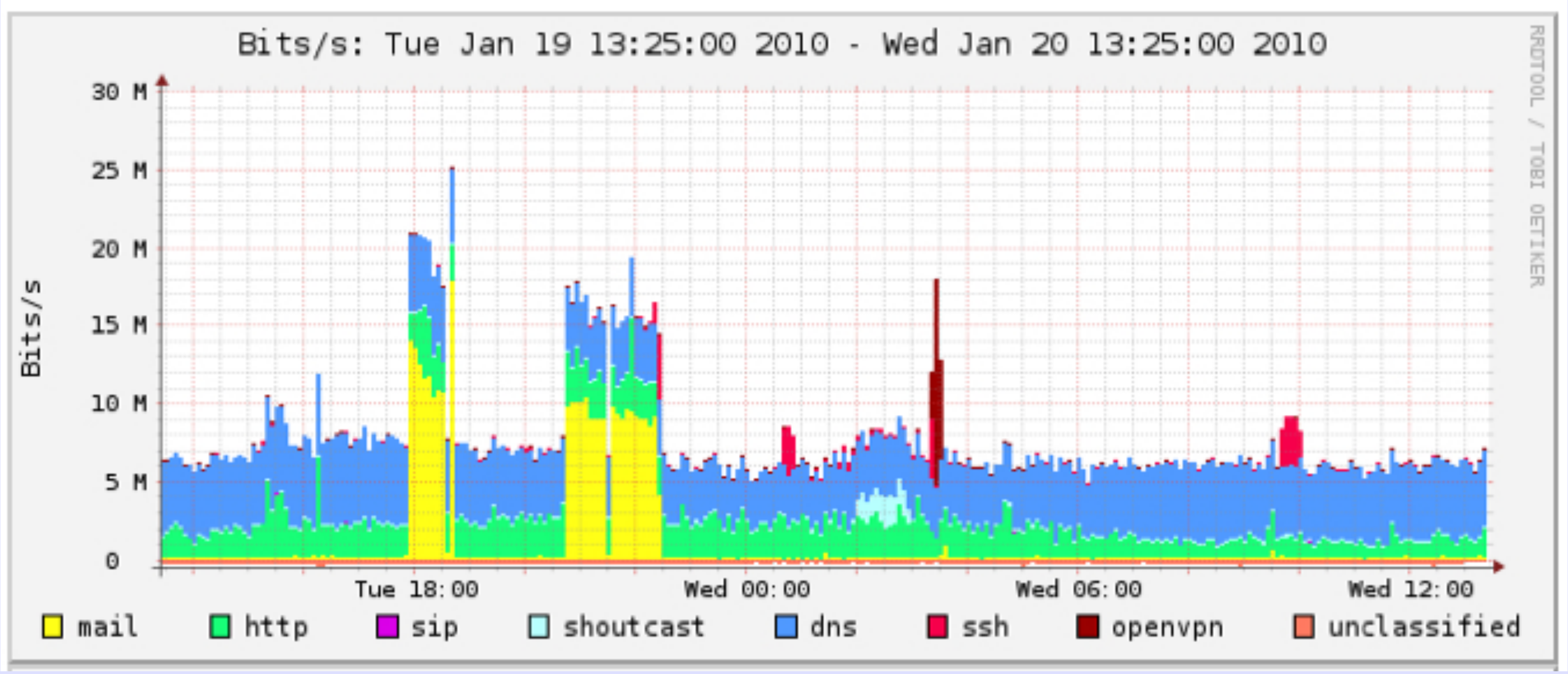
[r0.dfw.1] r0.dfw NTT Transit GigE

[r1.dfw.1] r1.dfw NTT Transit GigE

[r0.dfw.2] r0.dfw Equinix IX

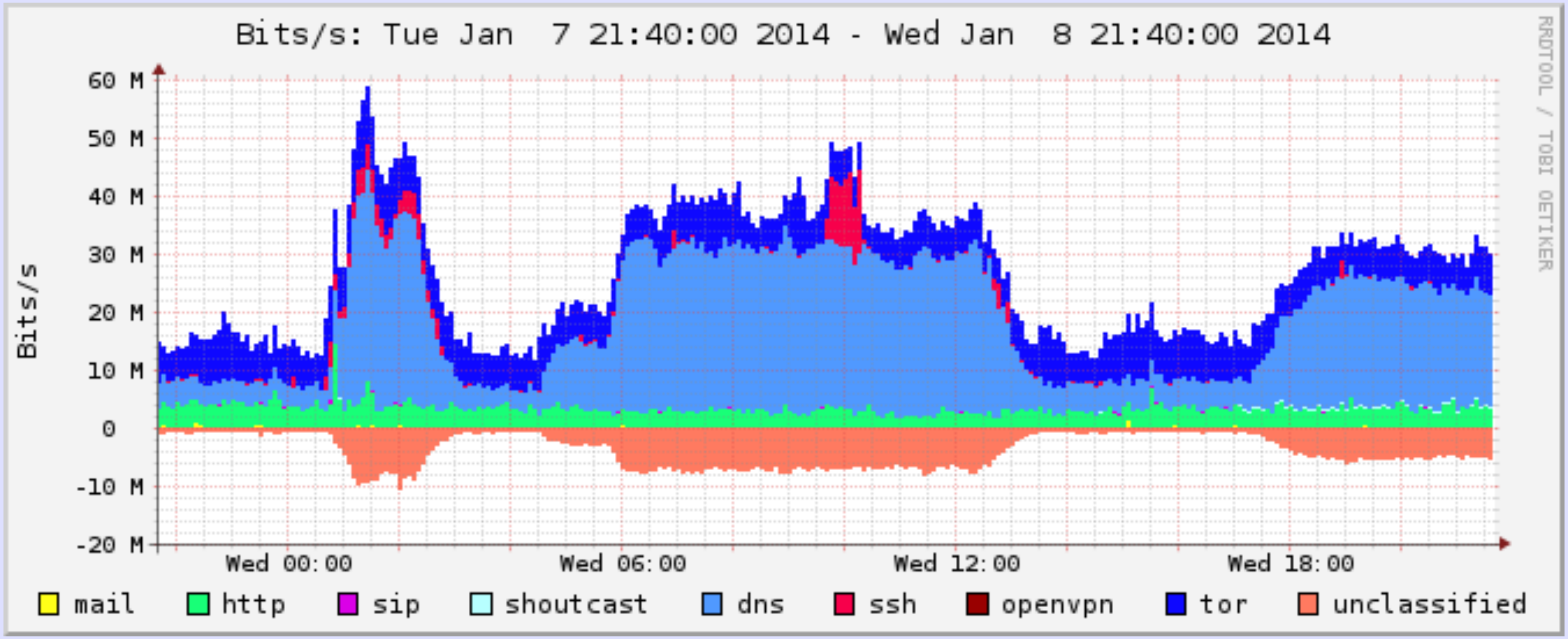
Traffic Graphs using MRTG

Sudden Spikes in Mail Volume



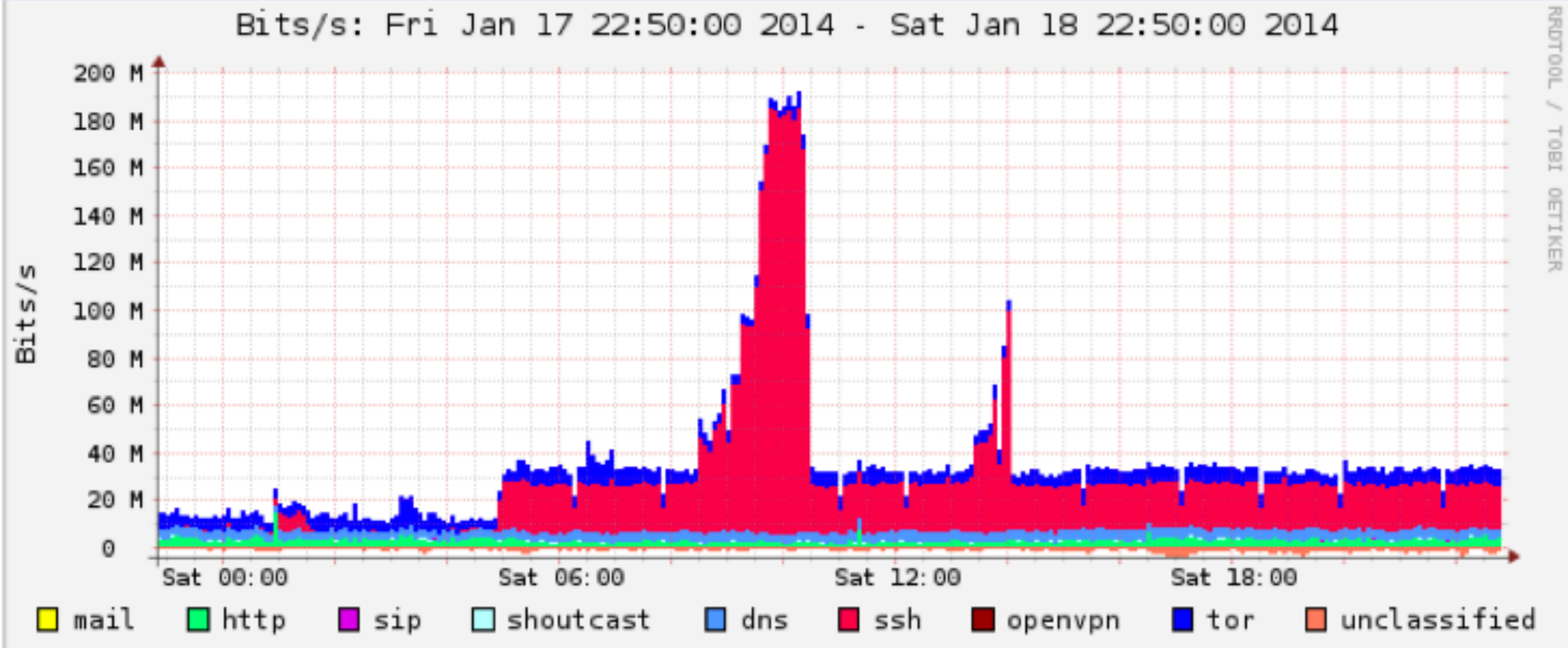
Graphs by NFSEN using NetFlow data

Too Much DNS Traffic



NetFLow Graph Using NFSEN/NFDUMP

It's Not an Attack
It is Backup


Bits/s: Fri Jan 17 22:50:00 2014 - Sat Jan 18 22:50:00 2014
Bits/s
200 M
180 M
160 M
140 M
120 M
100 M
80 M
60 M
40 M
20 M
Sat 00:00
Sat 06:00
Sat 12:00
Sat 18:00
🟨 mail
🟩 http
🟪 sip
□ shoutcast
🟦 dns
🟥 ssh
🟥 openvpn
🟦 tor
🟧 unclassified
RRDTOOL / TOBI OETIKER