Scaling Security Onion to the Enterprise

Mike Reeves
Twitter: @toosmooth
Email: michael.reeves@mandiant.com

About Me

- 15 years InfoSec experience (18 in IT)
- Mostly focussed on IDS and Unix Security
- Came to FireEye from Mandiant acquisition.
- 12 years at a Fortune 5
- Creator of OnionSalt for Security Onion

IDS vs NSM Scenario

IDS

1. Alert comes in
2. Analyst determines it could be malicious
3. Opens a request with IT support
4. IT support reports it has up to date virus signatures and system scan shows clean
5. Tells his co worker in IT that these security guys are horrible

NSM

1. Alert comes in
2. Analyst determines it could be malicious
3. Analyst pulls the transcript from the event where they see second stage download completes
4. Pulling connection events after initial alerts show machine establishing C2 to Ukraine and Turkey
5. Opens a request with IT support
6. IT support reports it has up to date virus signatures and system scan shows clean
7. Analyst provides the binary and connection data in question and when sent to AV vendor it is “something new” and will have a signature within 24 hours
8. Security 1 IT 0

http://www.geekempire.com/2013/05/how-do-you-do-this-without-nsm.html

Challenges of SO in the Enterprise

- Convincing management and network teams it is a good thing
- Sensor placement
- “High Speed” connectivity
- Compliance and Data Privacy
- Managing multiple devices
- **Dealing with the data!**

Compliance.....

- Global deployments come with some interesting challenges. - Work councils, France, Lawyers etc
- Always check with your legal department before embarking on any deployment
- Protect the data! Limit access to your grid
- Learn BPFs.. they can save you
- HIPAA, PCI etc

Convincing Management

- Easiest way? Stand up a Security Onion instance on your main egress - watch the evil flow
- Security Onion can be done well with commodity hardware.
- 243 days on average that attackers are on networks before being detected*

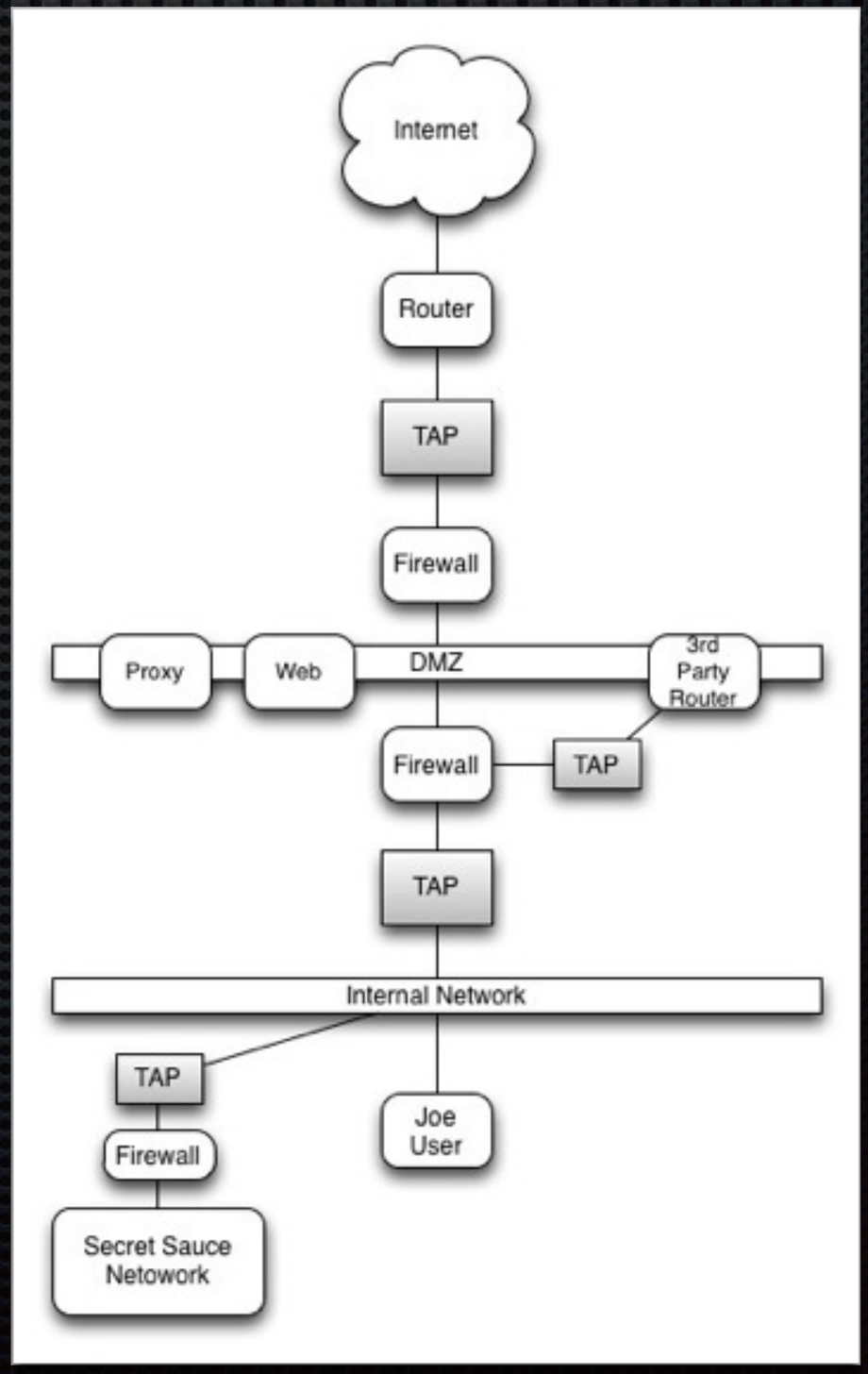
*https://www.mandiant.com/threat-landscape/

Dear Network Team, It's a TAP!

- Taps **scare** network teams and managers
- SPAN ports = FTL.. you just don't get everything
- There is a limit to PPS on a switch backplane!
- Network teams like to steal ports
- Always try and use dumb taps whenever possible
- Label your interfaces that have a tap!

Sensor Placement

- Always try and obtain the true source and true destination
- Ingress/Egress, VPN on the inside, 3rd party connectivity
- In front of important networks/systems
- Try and avoid asynchronous routing where possible

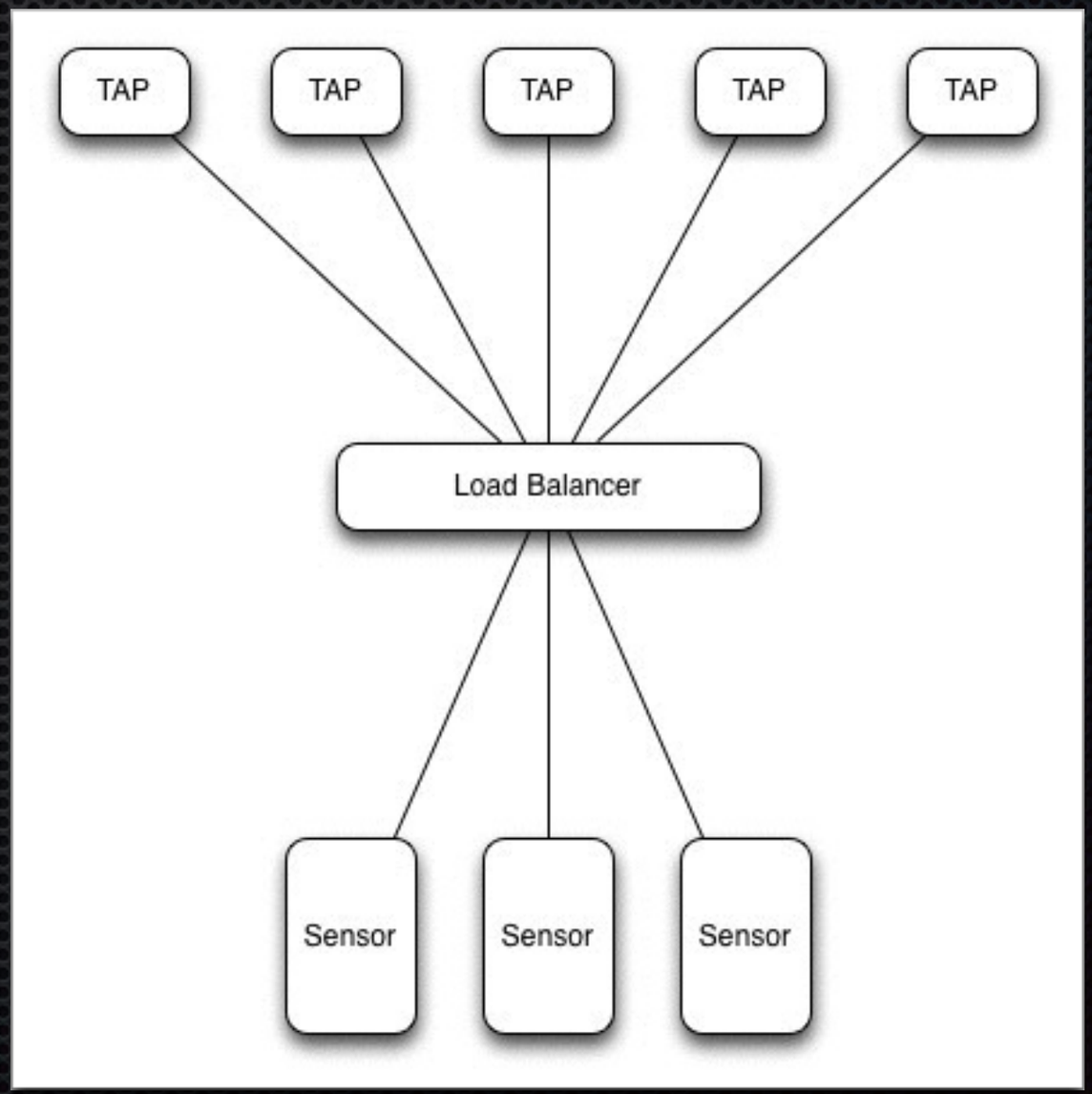


I feel the need.. the need for speed

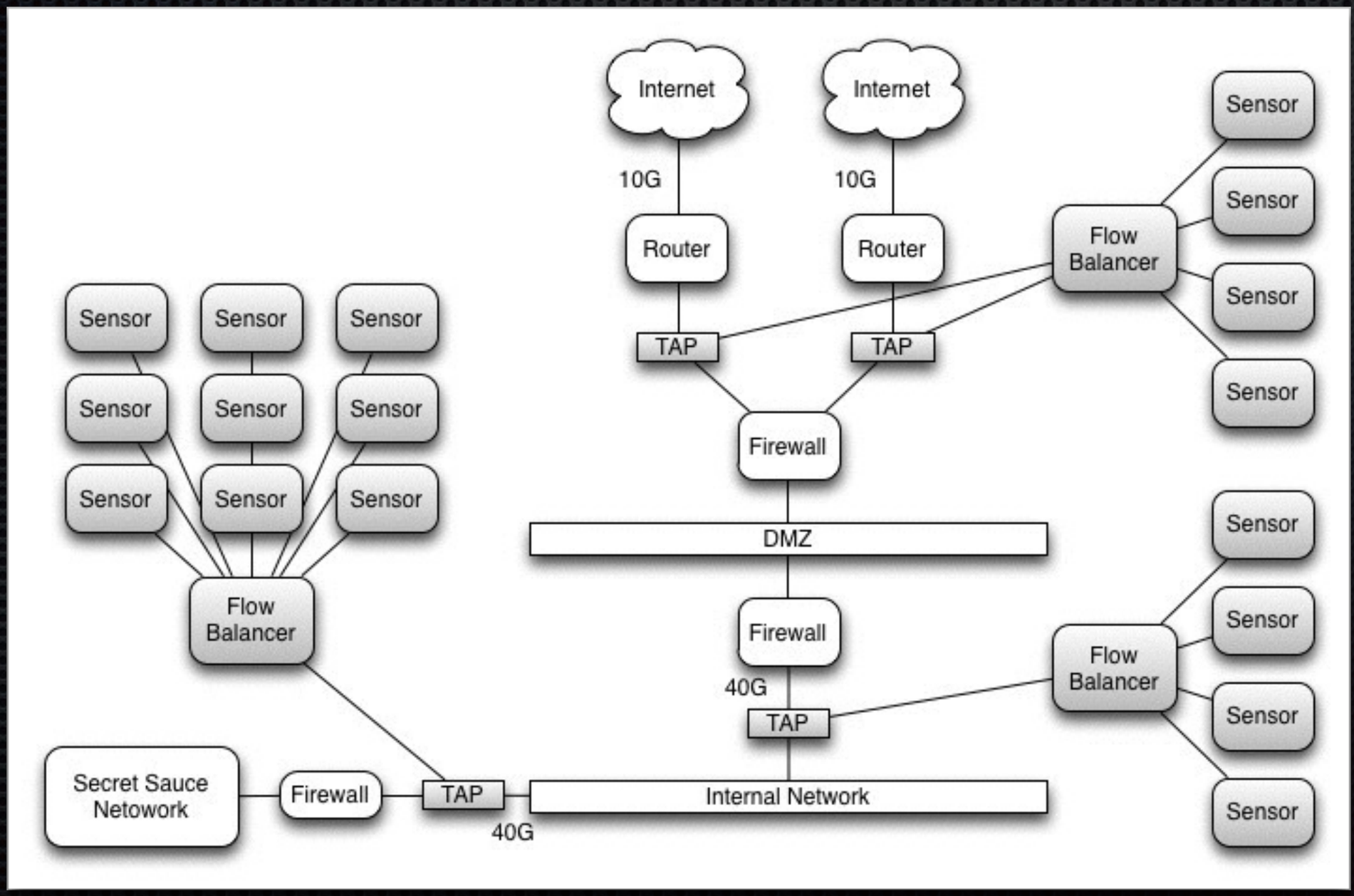
- Network speeds in the enterprise are growing quickly. 100Gbps etc
- Generally a single sensor can do 2Gbps of full NSM. (Lots of factors here!)
- Specialized sensors have specialized gear = $$$$$
- To solve this with cheap commodity gear you need to load balance the flows

Flow Based Load Balancing

- Flow based load balancing balances sessions across multiple nodes
- Each session goes to the same node
- All SO tools need the entire session to be effective
- Load balancing lets you share with others
- Example Vendors: Arista, GigaMon and cPacket



Large Scale Enterprise Deployment



Hardware sizing?!?

- This is the most frequent question I get asked
- Traffic profiles, packet size, total rules, junky rules are all factors
- More cores = more traffic you can handle
- Don’t be cheap… Ram is cheap

Hardware Recommendations - 100Mbps

- 1 x 4 core Intel HT processor
- 16GB RAM
- Software RAID should be acceptable
- Multiple NICs

Hardware Recommendations - 2Gbps

- 2 x 6 core Intel HT processors
- 128GB RAM
- Hardware Raid 5 with as many disks as possible
- PCI Express NICs (Quad NICs work great here)

Knobs you can turn

- /proc/sys/vm/dirty_background_ratio
- /proc/sys/vm/dirty_expire_centiseconds
- pf_ring min_num_slots=XXXX
- netsniff-ng —ring-size
- Pin processes to REAL cores

Dealing with the Data

- No matter how cool this is you still need smart people to look at the output
- This is a topic that could be it's own talk
- Make the console have context to help the analyst. ex. Naming convention - Sensor1-INT, Sensor2-VPN
- Have a development sensor on real traffic for rule testing and tuning
- Stage rollouts of new rules… One bad apple can kill the grid

Let’s get our Onion on...

Security Onion Challenges

- Multiple sensors can become cumbersome to manage
- Rule management is less than ideal
- There are a lot of tools included that you probably won't use
- Even though it is simple there is a learning curve

Security Onion Tips

- Set up your disk and create /nsm before you run sosetup
- Create your bridged interface before running the install
- Turn off all un-needed features
- Use it every day!

Taking Security Onion to the Enterprise with OnionSalt

- Onionsalt uses saltstack to manage multiple sensors
- Enables you to keep conformity of all sensor devices
- Makes user management simple
- Changes Security Onion's rule management
- https://github.com/TOoSmOotH/onionsalt
- http://www.saltstack.com/

User Management

- Users are now managed centrally
- By default all users are granted sudo access
- Users are created with no passwords… You must use key authentication
- Add your user accounts to /opt/onionsalt/pillar/users/init.sls
- Add the user's key to /opt/onionsalt/salt/users/keys/USERNAME.id_rsa.pub

users/init.sls

```
users:
  sensordude:
    fullname: Sensor Guy
    groups:
      - sudo
```

Rules Magic

```
# Watch the Rules and restart when needed

/etc/nsm/rules:
  file.recurse:
    # Don't mess with maxdepth or you will go on a recursed loop of pain
    - maxdepth: 0
    - source: salt://sensor/rules

restart-ids:
  cmd.wait:
    - name: /usr/sbin/nsm_sensor_ps-restart --only-snort-alert
    - cwd: /
    - watch:
      - file: /etc/nsm/rules
```

Bro Intel Framework

```
# Enable the Bro Intel Framework

/opt/bro/share/bro/site/local.bro:
  file.blockreplace:
    - marker_start: "# Begin Onionsalt Awesomeness.. If you edit this do so on the
Onionsalt master"
    - marker_end: "# DONE Onionsalt Awesomeness"
    - content: |
        @load policy/frameworks/intel/seen
        @load frameworks/intel/do_notice
        redef Intel::read_files += {
                "/opt/bro/share/bro/intel/Evil.intel"
        };
    - show_changes: True
    - append_if_not_found: True
```

Bro Intel Framework

Evil.Intel File

#fields indicator indicator_type meta.source meta.desc meta.url

192.168.2.34 Intel::ADDR IntelTeam SomeEvilGrouName http://InternalWiki/SomeEvilGroup
epiclyevil.com Intel::DOMAIN Steve SomeEvilGroupName2 http://InternalWiki/SomeEvilGroup2
yo@momma.com Intel::EMAIL EmailTeam BadDudez -
pwnt.exe Intel::FILE_NAME virus AV Team -

Tips and Tricks with OnionSalt

- Run a command on all sensors and backend:

  salt '*' cmd.run "uname -r"

- Update packages on all sensors:

  salt 'Sensor*' cmd.run “apt-get upgrade"

- Install a specific package on all sensors:

  salt 'Sensor*' cmd.run “apt-get install bwm-ng“

- Reboot all sensors

  salt 'Sensor*' cmd.run "reboot"

OnionSalt Roadmap

- Centralized ELSA
- Multiple Rule Set Support - VPN, Internal, etc
- Retire sosetup for sensors

Questions????