Who am I?
Breaking things since I was 12.
Consulting Security Architect
I get to break things and help fix them.
Other interests: traveling, hockey, snobby beer, and my bulldog.

#cyberspace

What's out there and how does it work?

Where are all the SDN Talks?
Because Skynet can defend itself now!

Jon Medina
protiviti
Where are all the SDN Talks?
Because Skynet can defend itself now!
Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby beer, and my bulldog

#cyberspice
Networks are Failing Us

They work too well
- Things are talking that shouldn’t be
- We have to actively PREVENT systems from talking to each other
- Have you seen a firewall rule list lately?

They don't work well enough
- Applications have no network visibility
- Network hardware is getting complicated
- Infrastructure deployment is costly and inefficient
- Network devices are expensive

...And how does this all come together in the cloud?
Software Defined Networking

- Abstraction of the control plane and data plane from devices.
- The brains of network device functions are moved to a centralized location.
- This is not NFV
What's out there and how does it work?
What's out there?

Companies with closed-source implementations:
  • Cisco Application Centric Infrastructure (ACI)
  • VMWare NSX

Companies with Open Source Openflow implementations:
  • Juniper
  • HP
  • Avaya
  • Big Switch
  • ...and dozens more

This is not a new technology
Google, Amazon, Facebook, NSA, most telcos have been using it for years
Core Concepts

- Controller sends flows (think ACLs) to switches
- Switches forward traffic based on flows
- If a switch doesn't have a flow that matches a packet, it asks the controller
- The controller either sends a new flow to the switch, or the packet is dropped
Go with the flow

1. Forward packet to port(s)
2. Encapsulate and forward to controller
3. Drop packet
4. Send to normal processing pipeline

<table>
<thead>
<tr>
<th>Switch Port</th>
<th>MAC src</th>
<th>MAC dst</th>
<th>Eth type</th>
<th>VLAN ID</th>
<th>IP Src</th>
<th>IP Dst</th>
<th>IP Prot</th>
<th>TCP sport</th>
<th>TCP dport</th>
</tr>
</thead>
</table>

Packet + byte counters
Let's Check it Out
So why do we care?

- Absolute control over every aspect of network traffic
- Traffic policies can be applied globally to users and systems
- We can make dynamic decisions about how to treat network traffic based on every layer of the OSI model
- Flow tables created within flow tables
Security Use Cases

• What network ports are users ACTUALLY using? Do users really need to communicate with each other?
• How do you limit access by vendors and outsiders connected to your network?
• How do you control what devices are connected to your network, and how do you handle BYOD? IOT?
Where are all the SDN Talks?

Because Skynet can defend itself now!
Let's talk dynamic security...

- Location based access control
- Multi-factor network authentication
- Granular control over application communications and cloud interactions.
- Vendor agnostic deployment assists in security tool-mageddon

Provision resources based on patterns using machine learning

- User and Service Account Behaviors
- Network traffic patterns
- Bandwidth consumption
- Application usage
Introducing....
Apache Spot (Incubating)

Apache Spot
What is Apache Spot?

- Spot is a community-driven project providing advanced analytics and comprehensive visibility across all security data using an open, scalable platform.

- Spot expedites threat detection, investigation and remediation via machine learning and consolidation of IT Telemetry into a comprehensive Data Lake.

https://spot.incubator.apache.org/
What does Spot Provide?

- **Telemetry**
  - Network Flows (nfcapd)
  - DNS (PCAP)
  - Proxy

- **Parallel Ingest Framework**
  - Open source decoders
  - Load data in Hadoop

- **Machine Learning**
  - Filter billions of events to a few thousand
  - Unsupervised learning

- **Operational Analytics**
  - Visualization, attack heuristics noise filter
Demo Architecture
Finally..... a helpful SDN tool (hopefully)

- Takes sFlow information from a network
- Writes it to a mininet topology
- Communicates active flows to SDN controller
- Can be used to model or migrate production or lab environments

....FloWrita

github: @acksec
Where are all the SDN Talks?
Because Skynet can defend itself now!