criticalstack

BRO-IDS
HIGH SPEED TAPPING

Presented by
Liam Randall

CONFIDENTIAL

This communication contains information that is confidential, proprietary in nature, and may also be attorney-client privileged and/or work product privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s) or the person responsible for delivering it to the intended recipient(s), please note that any form of dissemination, distribution or copying of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender and delete the original communication. Thank you for your cooperation.

BRO DEPLOYMENT OVERVIEW

Planning & Preparation

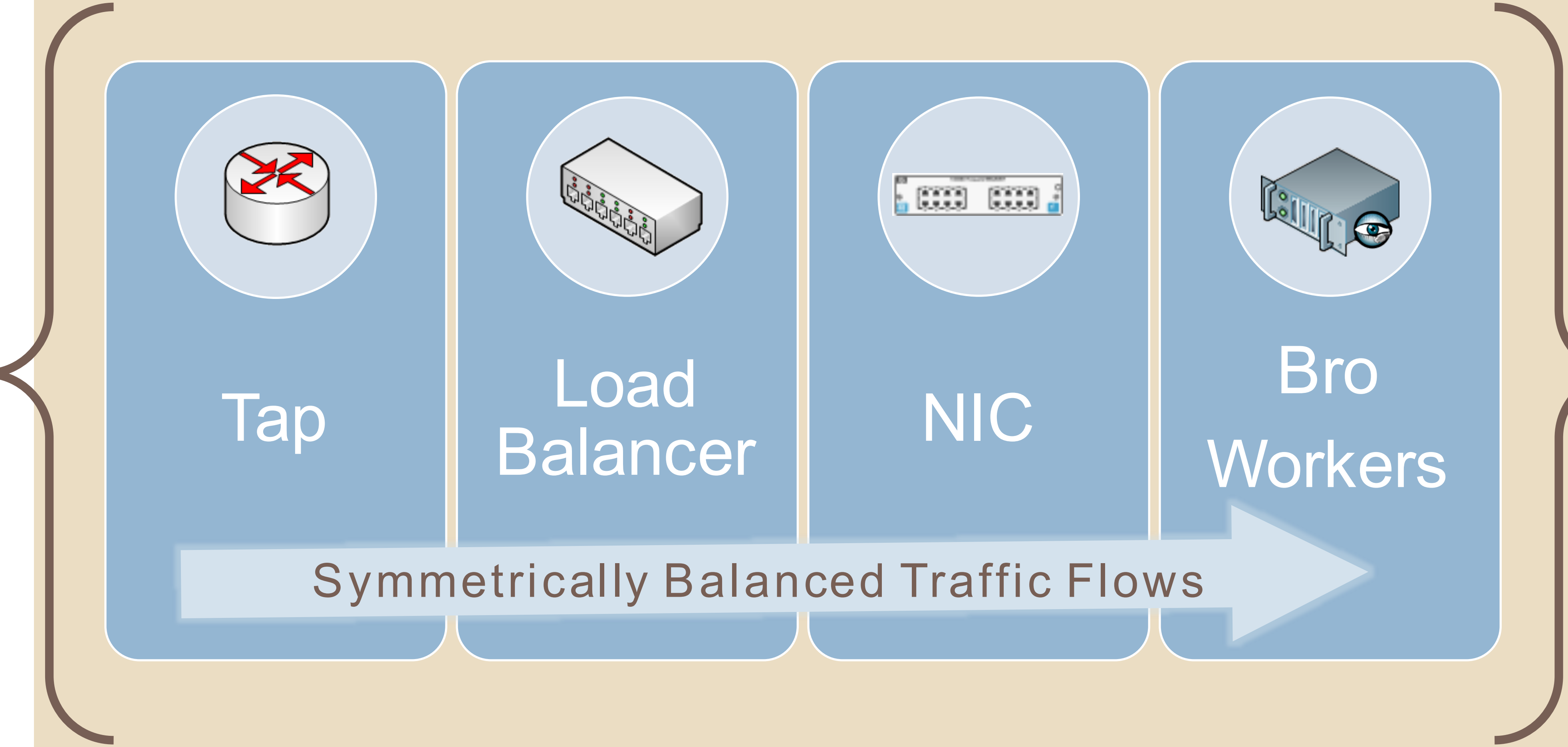
- Network Overview
- Requirements
  - Regulatory Domain: Contractual / Legal
- Replay Traffic
- Measure & Project
- Pilot
- Provision
- Sensor Tuning- continual process

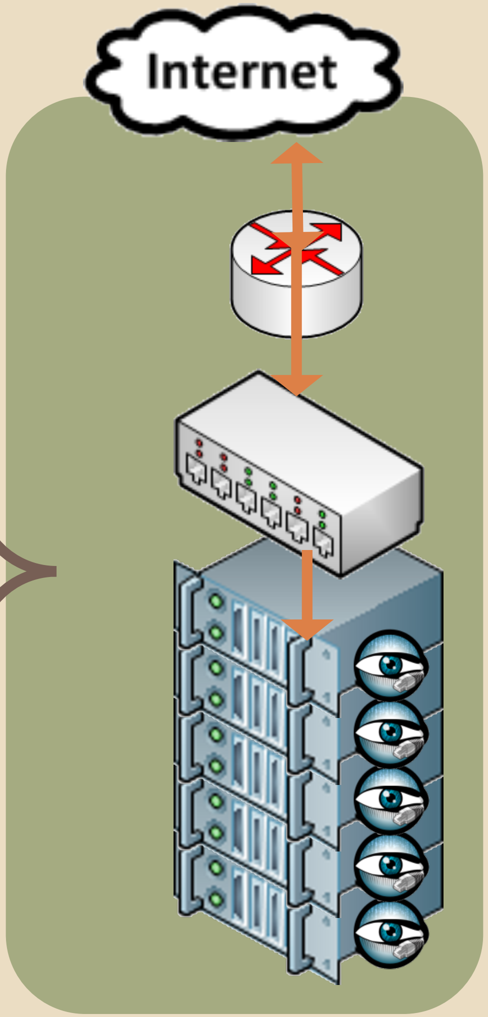
Sensor Deployment

- Tap
- Load Balancer
- NIC
- Bro Workers

BRO-IDS CLUSTER OVERVIEW

4 Basic Components





TAP OPTIONS

Heavily influenced by Net Topology

Span Port

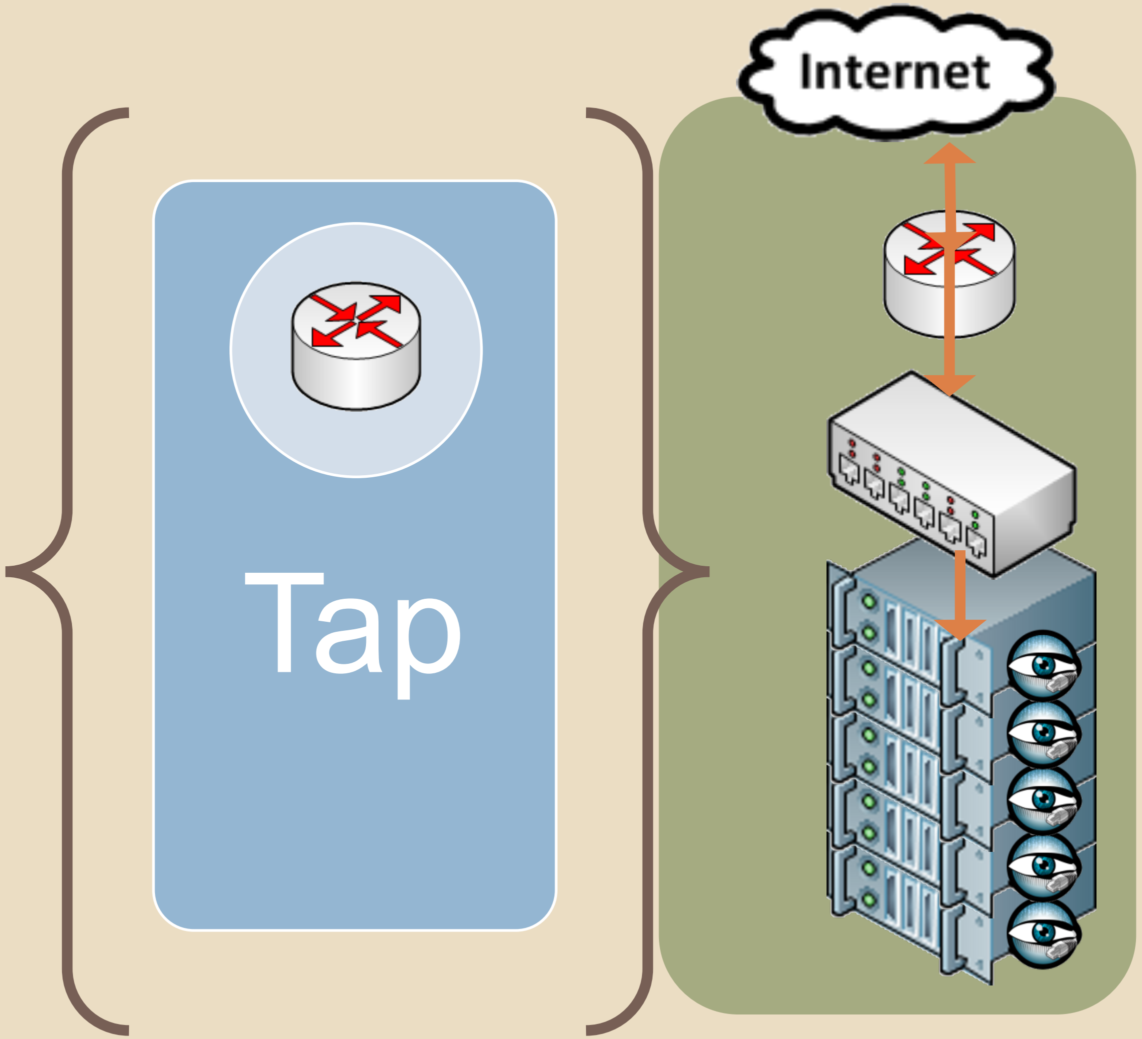
+ Inexpensive
+ Commodity
+ Already in Place

- Complexity
- Packet Drops

Hard Tap

+ Performance
+ Features
+ Multiple Sensors
+ ALSO Balance?

-Cost



TAP VENDORS

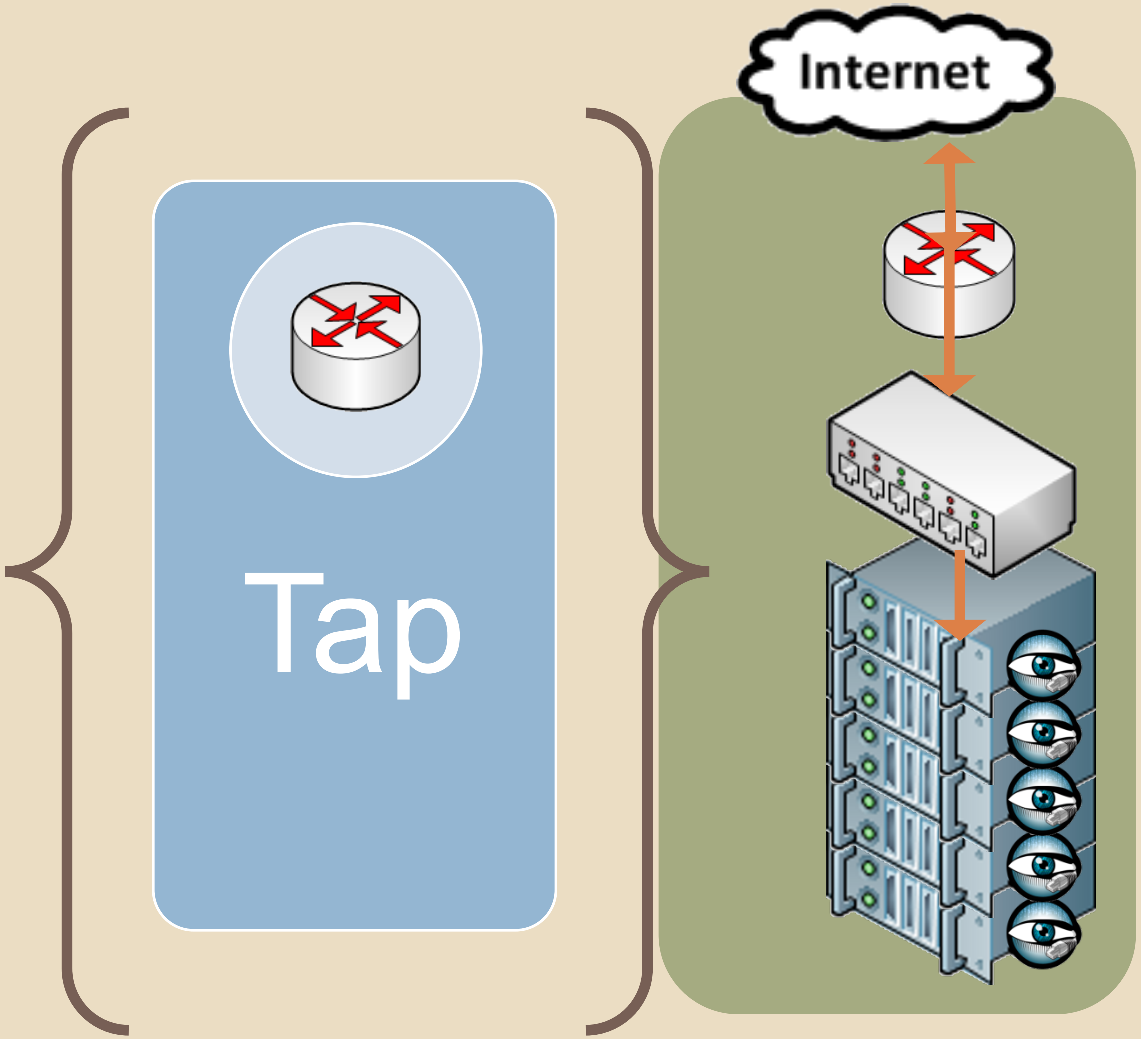
May also load balance

Span Port

- + Cisco
- + HP
- + Juniper
- + Extreme
- + Other..

Hard Tap

- + cPacket
- + VSS Monitoring
- + Net Optics
- + Gigamon
- + Apcon



Tap

Internet

LOAD BALANCERS

Moving Target

Dedicated

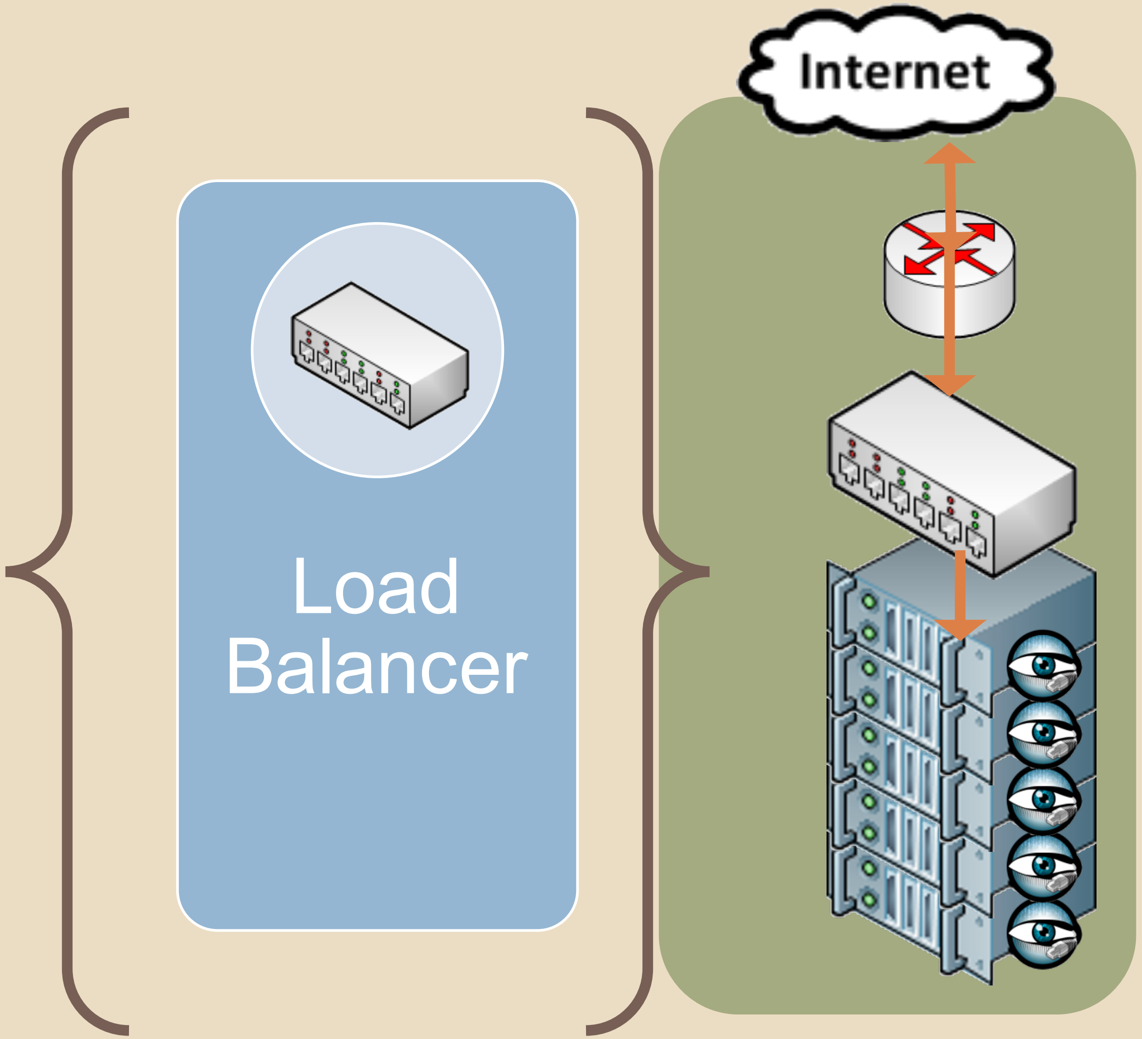
+ Performance
+ Features
- 3/4/5 Tuple
- Cost

OpenFlow

+ Cost
- Hash Based Balancing
- Hot Spotting

Hybrid Options

+ Fast Moving Space
- Hash Based balancing



LOAD BALANCERS VENDORS

Dedicated

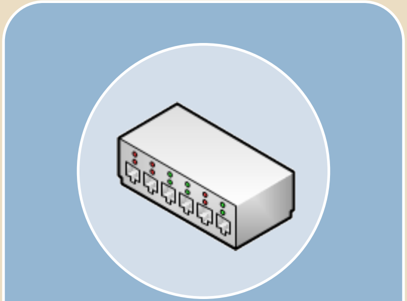
+ cPacket
+ VSS Monitoring
+ Apcon
+ Gigamon

OpenFlow

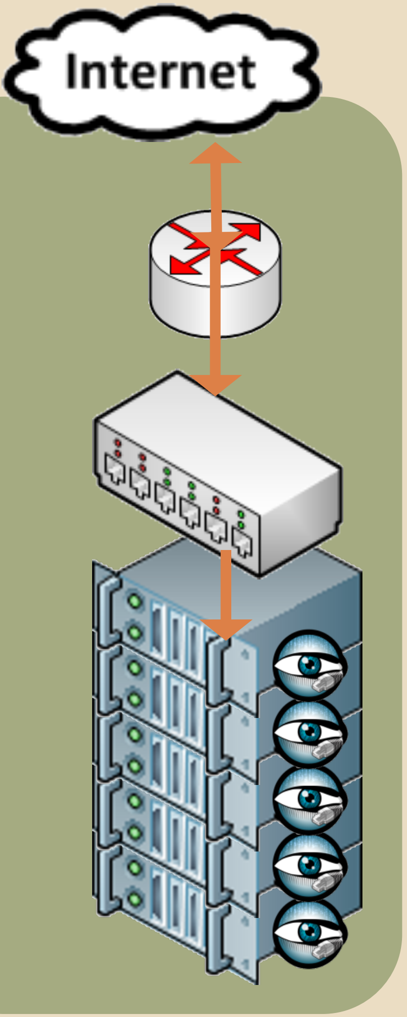
+ Arista
+ IBM
+ HP
+ Brocade
+ Big Switch

Hybrid Options

Ex: Arista Switches → hash based Load Balancers



Load Balancer



NIC OPTIONS

Requires OS Zero Copy Mechanism

1 Gpbs

+ Cost
+ Commodity
+ OS Support
+ Availability

- Throughput

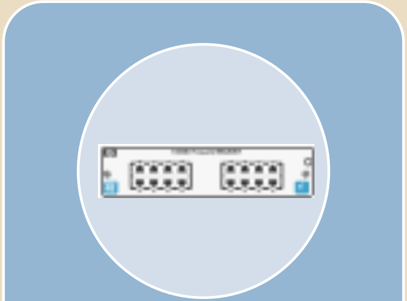
10 Gpbs

+ Cost
+ Commodity
+ OS Support

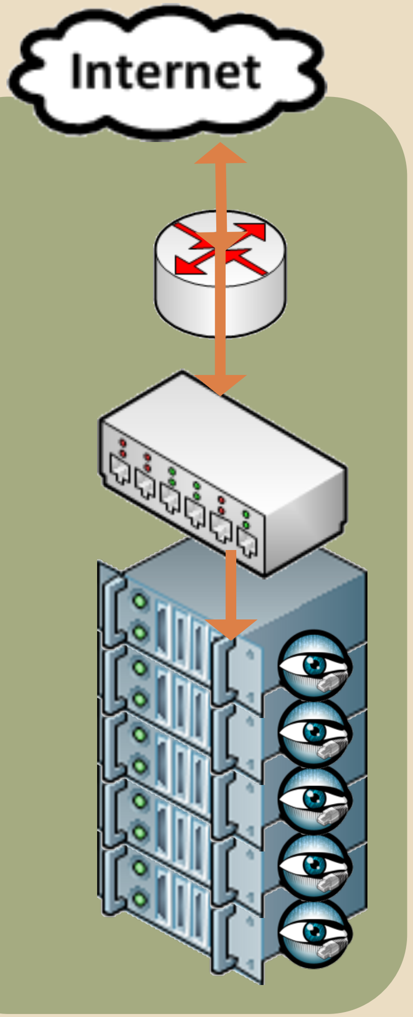
- Availability

Hybrid Options

+ Performance → Endace DAQ
+ Incredible Efficiencies
- Cost



NIC Options



BRO WORKERS

1 Process per 1 Core

Bro Model is Multithreaded

Hardware

+ Commodity

+ High Core Count

+ Memory

+ Any Vendor

+ Usually Multiple Nodes

OS

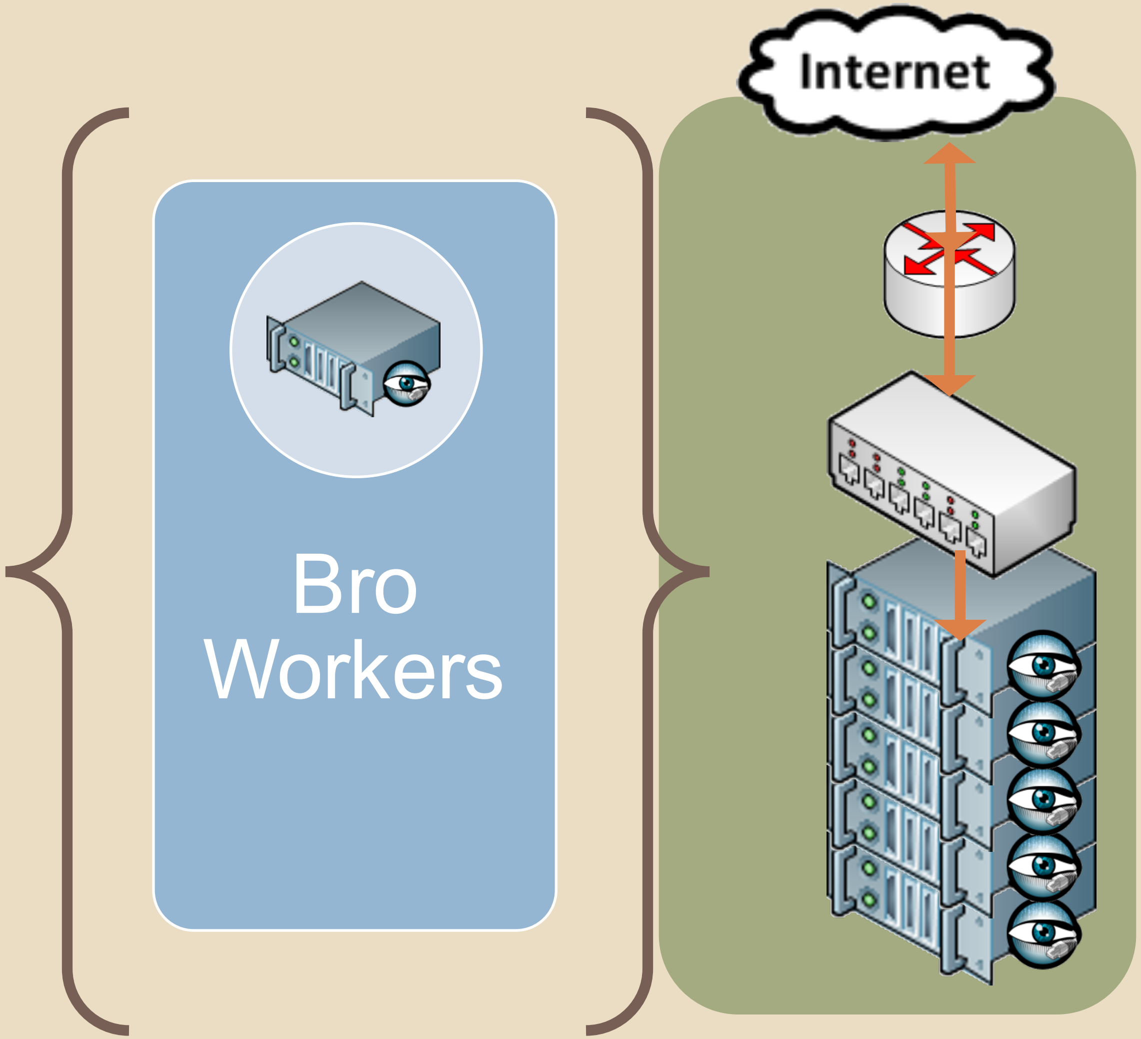
+ BSD/Linux

+ 0-Copy

++ pfring

++ DAQ..

++ AF_Packet

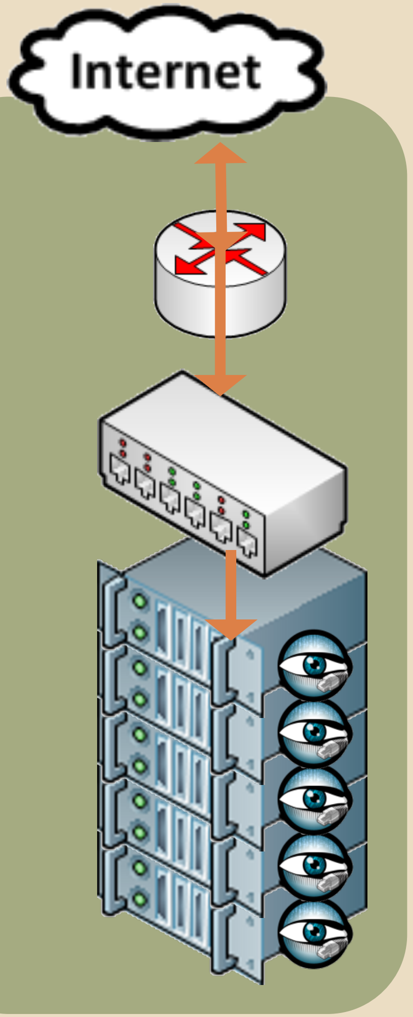


BRO CASE STUDIES

Wide Variety in Installs

+ Widely deployed in high speed REN
+ Internet 2, Research Networks
+ 15 Year Production Deployments
+ 10 Gbps in 2006
+ 40 Gbps in 2010

+ 100 Gbps- Deployed, 2014

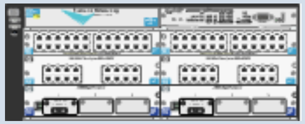


BRO CASE STUDY

- + Sustained 9 Gbps
- + 12 Dell r610, 48 Gb RAM, 2 x Quad Core Intel E5620 RHEL 6.2
- + 2 Proxy Nodes, 1 Manager Node w/ 10 Gig Nic
- + 40 Tb Log Storage, 500 Gb Raid 10 SSD Scratch
- + Visualization: Arcsight, Splunk, Native

Load Balancer

cPacket cFlow

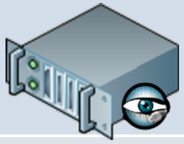


HP Switch

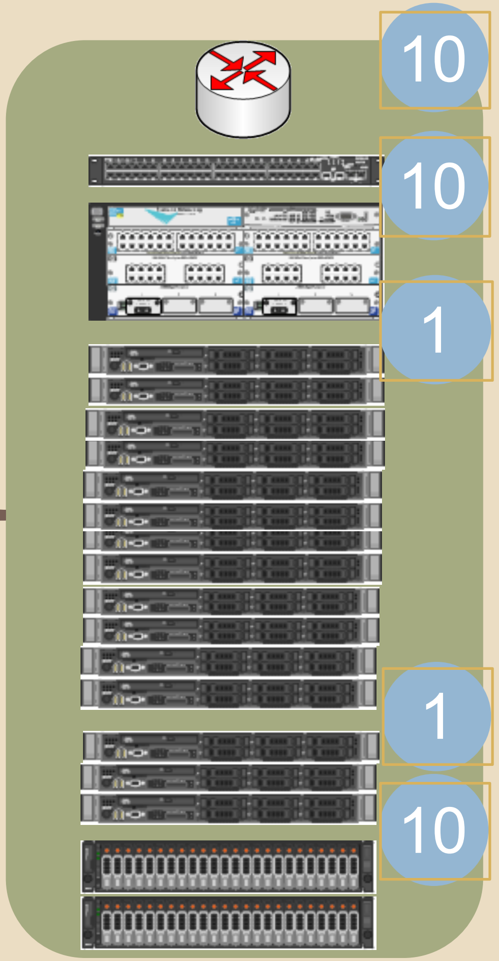
3 10 Gbps

30 1Gbps

Qty 2 Intel Gigabit ET



4 Workers Per Node

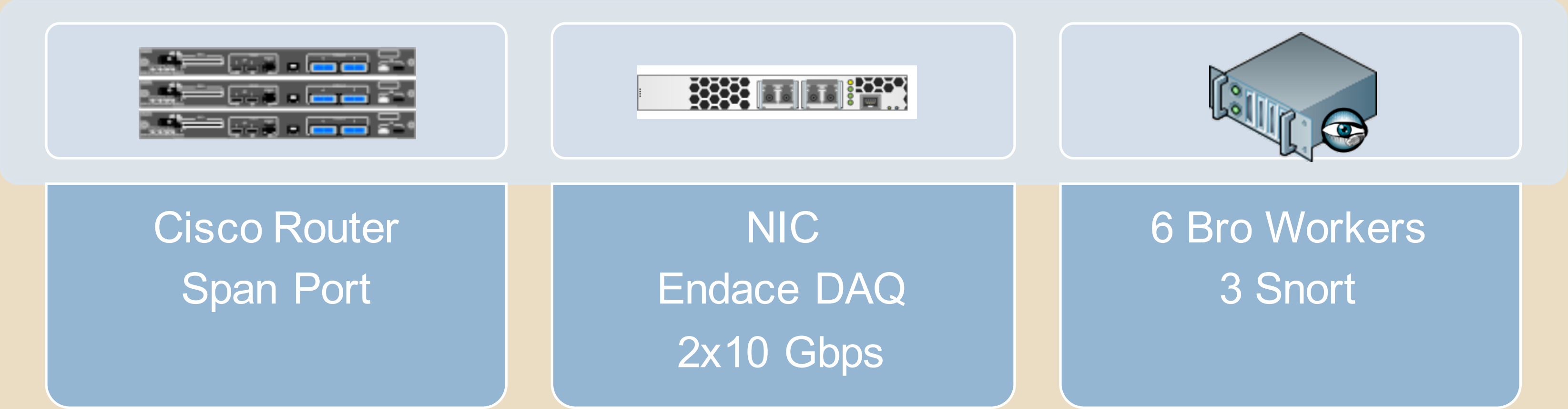


BRO NETWORK SECURITY MONITOR

BRO CASE STUDY

criticalstack

- + Sustained 4 Gbps
- + 1 Dell r710, 72 Gb RAM, 2 x Quad Core Intel x5677
- + 1 Endace DAQ
- + RHEL 6.2
- + 20 Tb Log Storage
- + Visualization: Splunk, Native


Cisco Router
Span Port
NIC
Endace DAQ
2x10 Gbps
6 Bro Workers
3 Snort