ACI REF

Introduction to OpenFlow and Why it Matters to You

ACI REF

Introduction to OpenFlow and Why it Matters to You
Goals of the Presentation

- Arm you with a basic understanding of computer networks so that you can provide justification for your “unique” requirements to your fellow IT staff.

- Provide you with a common set of nomenclature that you can use when conversing with research peers regarding data exchange.
Overview

- The Evolution of the Science DMZ
- Software Defined Networking and its Components
- OpenFlow and Why it Matters
The Definition of Science DMZ

Wikipedia Definition:

“The term Science DMZ refers to a computer subnetwork that is structured to be secure, but without the performance limits that would otherwise result from passing data through a stateful firewall. The Science DMZ is designed to handle high volume data transfers, typical with scientific and high-performance computing, by creating a special DMZ to accommodate those transfers. It is typically deployed at or near the local network perimeter, and is optimized for a moderate number of high-speed flows, rather than for general-purpose business systems or enterprise computing.”

http://en.wikipedia.org/wiki/Science_DMZ_Network_Architecture
The “Wordly” of Science DMZ
The Evolution of Science DMZ

Corporate Environment:

Offer Goods and Services
The Evolution of Science DMZ (cont.)

Corporate Environment:

Lock them away in an “online” experience.
The Evolution of Science DMZ (cont.)

Corporate Environment:

And make them available when someone is willing to pay...
The Evolution of Science DMZ (cont.)

Corporate Environment:

“It’s just good business...”
The Evolution of Science DMZ (cont.)

Academic Environment:
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...

- Student Data
- Intellectual Property
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...

- Student Data
- Intellectual Property
- Payroll & Accounting
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...
The Evolution of Science DMZ (cont.)

Academic Environment: A stark contrast...

“Firewall”

“Intrusion Prevention”

“WAN”
Academic Environment: A stark contrast...

- **Bureaucracy** (aka “Paperwork”)
- **“Firewall”**
- **“WAN”**
- **Intrusion Prevention**
The Evolution of Science DMZ (cont.)

Academic Environment: Enter Computational Research...
The Evolution of Science DMZ (cont.)

Academic Environment: Computational Research...
The Evolution of Science DMZ (cont.)

Academic Environment: Computational Research...
The Evolution of Science DMZ (cont.)

Academic Environment: Computational Research...
The Evolution of Science DMZ (cont.)

Computational Research and an Analogy...

Computational Research
The Evolution of Science DMZ (cont.)

Computational Research and an Analogy...

Computational Research
Computational Research and an Analogy...

Computational Research = Velociraptor
The Evolution of Science DMZ (cont.)

Computational Research and an Analogy...

Computational Research $\approx$ Velociraptor
The Evolution of Science DMZ (cont.)

Proof that the analogy is valid...
The Evolution of Science DMZ (cont.)
The Evolution of Science DMZ (cont.)
The Evolution of Science DMZ (cont.)

Agile

Moves Rapidly
The Evolution of Science DMZ (cont.)

Agile
Moves Rapidly
More Effective
In Groups
The Evolution of Science DMZ (cont.)

- Agile
  - Moves Rapidly
- More Effective
  - In Groups
- Consumes All
  - Available Resources
The Evolution of Science DMZ (cont.)

- Agile
- Moves Rapidly
- More Effective In Groups
- Consumes All Available Resources
- Cool!
The Evolution of Science DMZ (cont.)

- Agile
- Moves Rapidly
- More Effective In Groups
- Consumes All Available Resources
- Cool!

Is not reptile

Is reptile
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Pardon me good sirs...
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

I have some important research data...
...that is highly important to myself, the educational community, and all of mankind as a whole. It is imperative that this data be reasonably secured; yet, available to my research peers. The datasets are rather large, as they have been collected over a number of years.
Would it be possible to place this in a secure, reliable, flexible, accessible, as well as high performing infrastructure?
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Lemme check...
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Hey, Jim!
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Gotta guy here. Says he needs stuff.
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

What kinda stuff?
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Something about security and connectivity (maybe).
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

We got plenty of that! Send ‘em in.
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Ye gads!
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Ye gads! AHHHH!!
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Ye gads!
AHHHH!!
THE INHUMANITY!!!
The Evolution of Science DMZ (cont.)

When Computational Science Meets Traditional Networks

Ye gads!

AHHHH!!

THE INHUMANITY!!

HOM! NOM! NOM!
The Evolution of Science DMZ (cont.)

OBSERVATION: The requirements of the computational researcher and the capabilities of the traditional campus computer network do not always align!

Ya’ think?!
The Evolution of Science DMZ (cont.)

This can result in adverse consequences:

- Poor network performance for production systems
- Poor security performance for the campus as a whole
- Bandwidth congestion
- Overutilization of available resources
- Increased Help Desk calls
- General grumbling and complaining
The Evolution of Science DMZ (cont.)

This can result in adverse consequences:

- Poor network performance for production systems
- Poor security performance for the campus as a whole
- Bandwidth congestion
- Overutilization of available resources
- Increased Help Desk calls
- General grumbling and complaining

But how do we overcome this? *I can’t stop my research* just because *the network can’t keep up*!
The Evolution of Science DMZ (cont.)

- Enter the Science DMZ!

https://fasterdata.es.net/science-dmz/science-dmz-architecture/
The Evolution of Science DMZ (cont.)

- What makes the Science DMZ important
  - Dedicated Data Transfer Node to ship datasets
  - Dedicated network resources outside of the campus
  - Dedicated, high-speed capacity (typically 10-Gig)
  - Dedicated “circuits” between research sites
  - “Programmable”
The Evolution of Science DMZ (cont.)

- What makes the Science DMZ important

- Dedicated Data Transfer Node to ship datasets
- Dedicated network resources outside of the campus
- Dedicated, high-speed capacity (typically 10-Gig)
- Dedicated “circuits” between research sites
- “Programmable”

Sounds like it meets my requirements!
The Evolution of Science DMZ (cont.)

• Sort of like an Interstate highway... no stop lights, and dedicated on and off ramps:
The Evolution of Science DMZ (cont.)

Science DMZ and the Campus Network...
The Evolution of Science DMZ (cont.)

Science DMZ and the Campus Network...
The Evolution of Science DMZ (cont.)

Science DMZ and the Campus Network...
The Evolution of Science DMZ (cont.)

Science DMZ and the Campus Network...
The Evolution of Science DMZ (cont.)

Science DMZ and the Campus Network...
ANALOGY RECAP...

Corporate Network

Sealed Vault

Campus Network

Prison
ANALOGY RECAP...

Science DMZ

Interstate

Computational Research

Velociraptor
Remember that “Programmable” Aspect of Science DMZ?
Remember that “Programmable” Aspect of Science DMZ?

The Evolution of Science DMZ (cont.)

- What makes the Science DMZ important
  - Dedicated Data Transfer Node to ship datasets
  - Dedicated network resources outside of the campus
  - Dedicated, high-speed capacity (typically 10-Gig)
  - Dedicated “circuits” between research sites
  - “Programmable”
Remember that “Programmable” Aspect of Science DMZ?

The Evolution of Science DMZ (cont.)

- What makes the Science DMZ important
  - Dedicated Data Transfer Node to ship datasets
  - Dedicated network resources outside of the campus
  - Dedicated, high-speed capacity (typically 10-Gig)
  - Dedicated “circuits” between research sites
  - “Programmable”
Science DMZ is like...
Science DMZ is like...

An onion!
Science DMZ Layers

Science DMZ
Dedicated Paths
Transfer Nodes
perfSONAR
Science DMZ Layers

Science DMZ
- Dedicated Paths
- Transfer Nodes
- perfSONAR

SDN
- Controller
- Network Switches
Science DMZ Layers

Science DMZ
- Dedicated Paths
- Transfer Nodes
- perfSONAR

SDN
- OpenFlow
- Northbound APIs
- East-West Monitoring

SDN
- Controller
- Network Switches
Science DMZ Layers

Science DMZ
- Dedicated Paths
- Transfer Nodes
- perfSONAR

SDN
- OpenFlow
- Northbound APIs
- East-West Monitoring

SDN
- Controller
- Network Switches

Campus Network
Software Defined Networks (SDN)

- Components of SDN
  - Controller
  - Devices
  - Northbound APIs
  - East/West monitoring
  - OpenFlow communications
Software Defined Networks (SDN)

- Components of SDN
  - Controller
  - Devices
  - Northbound APIs
  - East/West monitoring
  - OpenFlow communications

For the purpose of this discussion, we will focus on an SDN that involves OpenFlow!
Software Defined Networks (SDN)
Software Defined Networks (SDN)
Software Defined Networks (SDN)
Software Defined Networks (SDN)
Software Defined Networks (SDN)

OpenFlow

X 1000
Software Defined Networks (SDN)
Software Defined Networks (SDN)
Software Defined Networks (SDN)
Why Even Do SDN?

- Orchestration!
- Flexibility
- Self Service
- Agility
- More “holistic”
Why Even Do SDN?

- Orchestration!
- Flexibility
- Self Service
- Agility
- More “holistic”
Why Even Do SDN?

Imagine if your brain were distributed throughout your body.

How would you walk? Run? Shop?

SDN is just a natural evolution of computer networking.
OpenFlow

- OpenFlow is like the “Nerves” of the body
  - Controller (brain)
  - Devices (arms/legs/mouth/tail)
  - Northbound APIs (eyes/ears/tongue/nose)
  - East/West monitoring (pain/soreness/sick)

- Carries messages from the controller to the devices, and vice-versa.
OpenFlow

“OpenFlow is an open standard network protocol used to manage traffic between commercial Ethernet switches, routers and wireless access points. OpenFlow enables software-defined networking (SDN) for programmable networks and is based on an Ethernet switch, with an internal flow-table and a standardized interface to add and remove flow entries.”

OpenFlow: What you need to know...

- Specifications: Located at the Open Network Foundation web site (www.opennetwork.org)
- Leverages TCP for communication
- Port 6653 is most commonly used
- Specification recommends TLS encryption
OpenFlow: What you need to know... (cont)

- OpenFlow Message Types:
  - OpenFlow 1.3 has 30 different message types
  - Details at [www.flowgrammable.org](http://www.flowgrammable.org)
  - Includes things like table requests, table insertions, ports in, ports out, get config, set config, etc.

Every OpenFlow message begins with the same header structure. This fixed structure serves three roles that are independent of the version of OpenFlow being used. First, the version field indicates the version of OpenFlow which this message belongs. Second, the length field indicates where this message will end in the byte stream starting from the first byte of the header. Third, the xid, or transaction identifier, is a unique value used to match requests to responses. The type field which indicates what type of message is present and how to interpret the payload, is version dependent.
OpenFlow: Lab this afternoon!

You will have the opportunity to see these messages in real time.
In Summary

When properly equipped...

The computational researcher can use Science DMZ, Software Defined Networks, and OpenFlow communications for more effective data collaboration.
Thank You!

https://www.dropbox.com/sh/h7y0c3z9n0eq15b/AAB97wqUY54MzClbZsRKA_RAa?dl=0

Matt Younkins
younkkinsm@ou.edu
Reminder: Lab Prereq's

• Download *and install* both VirtualBox and the VirtualBox extension pack:
  
  https://www.virtualbox.org/wiki/Downloads

• Download the SDN Hub All-in-One App Development Starter virtual machine:
  
  https://github.com/downloads/mininet/mininet/mininet-2.0.0-113012-amd64.ovf.zip

• ***NEW*** Lab instructions can be downloaded here:
  
  https://www.dropbox.com/sh/h7y0c3z9n0eq15b/AAB97wqUY54MzClbZsRKA_RAa?dl=0