ISSA

Information Systems Security Association International

www.issa.org

ISSA Thought Leadership Webinar

*"*Micro-Segmentation 101*"*

November 14, 2018

Micro-Segmentation 101

Today's web conference is generously sponsored by:

Illumio

www.illumio.com

Micro-Segmentation 101

Moderator

David Vaughn, ISSA International Board of Directors, Chairperson for Education & Professional Development

David Vaughn is a decorated military combat veteran. He is an accomplished Information Security Professional with over 20 years of Information Security experience. He maintains a broad range of experience from Enterprise Mobility, to Network Security Infrastructure design and testing. He has managed personnel, provided technical oversight for incident response and countermeasures, performed individual and team based network assessments, information security R&D consulting, and computer forensics. David has a proven track record demonstrating the ability to effectively understand and communicate contextual business requirements to both technical and non-technical groups at any level of leadership to help customers achieve compliance within various regulatory bodies.

Micro-Segmentation 101

Speaker

Vijay Chauhan, Senior Director Product Marketing, Illumio

Vijay Chauhan is Senior Director of Product Marketing at Illumio, where he leads Product Launches and Content. Prior to Illumio, Vijay spent 4+ years at Splunk running Product Management and Strategic Alliances for Splunk's Security business. Vijay started his career as a Security Practitioner in Financial Services, spending 7+ years at Barclays Bank, handling core information security functions including Security Operations, Risk, Security Engineering, Application Security, and Identity & Access Management. Vijay has a BS in Computer Science from Cambridge, MA in Sanskrit from UPenn, and MS in Computer Science from Stanford.

Micro-Segmentation 101

Speaker

Dr. Branden R. Williams, Director, Cyber Security, MUFG Union Bank N.A

Dr. Branden R. Williams has more than twenty years of experience in business, technology, and information security as a consultant, leader, and an executive. His specialty is navigating complex landscapes—be it compliance, security, technology, or business—and finding innovative solutions that propel companies forward while reducing risk.

Micro-Segmentation 101

Speaker

John Donovan, ISSA Silicon Valley Chapter & Rook Security

John is past-president and a board director of the Silicon Valley ISSA Chapter He's a member of the CaC (CISO Advisory Council) for the ISSA's CISO Executive Forum and participant in a number of security events including past CISO Executive Forums, ISSA International and regional conferences such as the Cornerstones of Trust conference in the San Francisco Bay Area. John is a passionate supporter of both the local arts community and cyber-security community in the Silicon Valley and beyond. In his day job, John builds and runs security programs and is currently CISO for an early-stage security technology startup. Past professional positions include developing and managing Security, Risk, IT, and engineering programs for Illumio, Veracode, NetApp, Xilinx, and other technology and security companies .

Micro-Segmentation 101

Speaker

Vijay Chauhan, Senior Director Product Marketing, Illumio

Vijay Chauhan is Senior Director of Product Marketing at Illumio, where he leads Product Launches and Content. Prior to Illumio, Vijay spent 4+ years at Splunk running Product Management and Strategic Alliances for Splunk's Security business. Vijay started his career as a Security Practitioner in Financial Services, spending 7+ years at Barclays Bank, handling core information security functions including Security Operations, Risk, Security Engineering, Application Security, and Identity & Access Management. Vijay has a BS in Computer Science from Cambridge, MA in Sanskrit from UPenn, and MS in Computer Science from Stanford.

ISSA

Information Systems Security Association International

www.issa.org

Micro-Segmentation 101

Vijay Chauhan, Sr Dir of Product Marketing

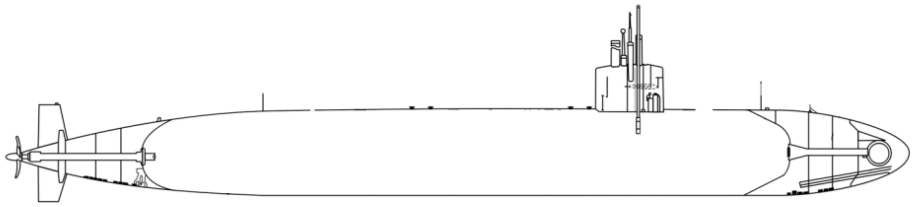
Nov 14 2018

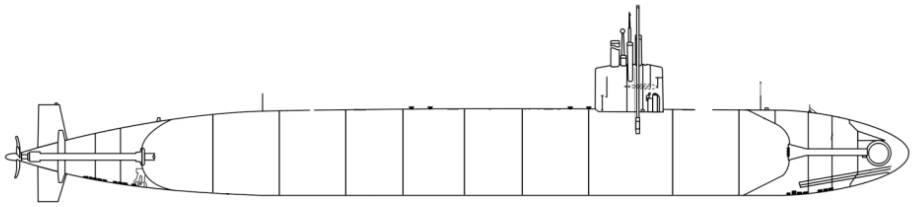
illumio

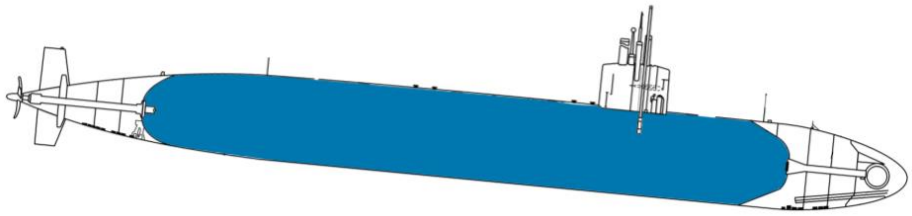
What We'll Cover

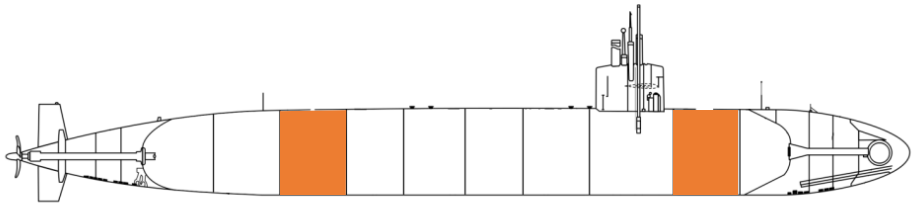
- What is micro-segmentation?
- Why micro-segmentation?
- The principles of micro-segmentation
- How to implement a strategy in 5 steps

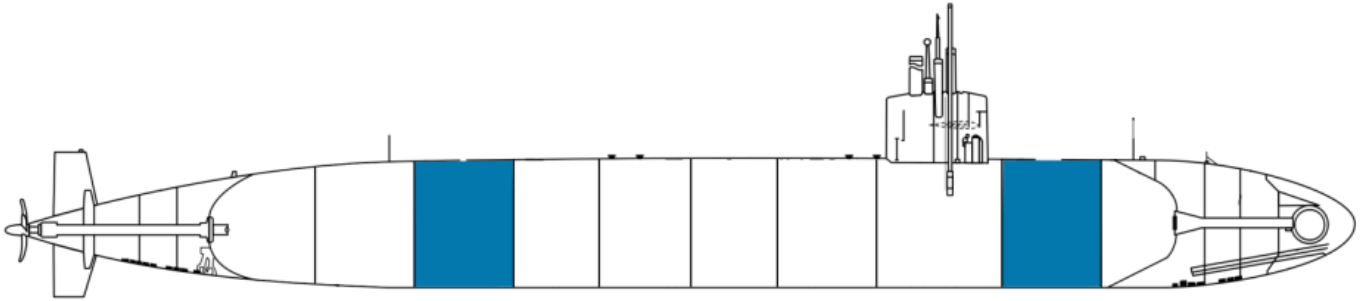
What is Micro-Segmentation?



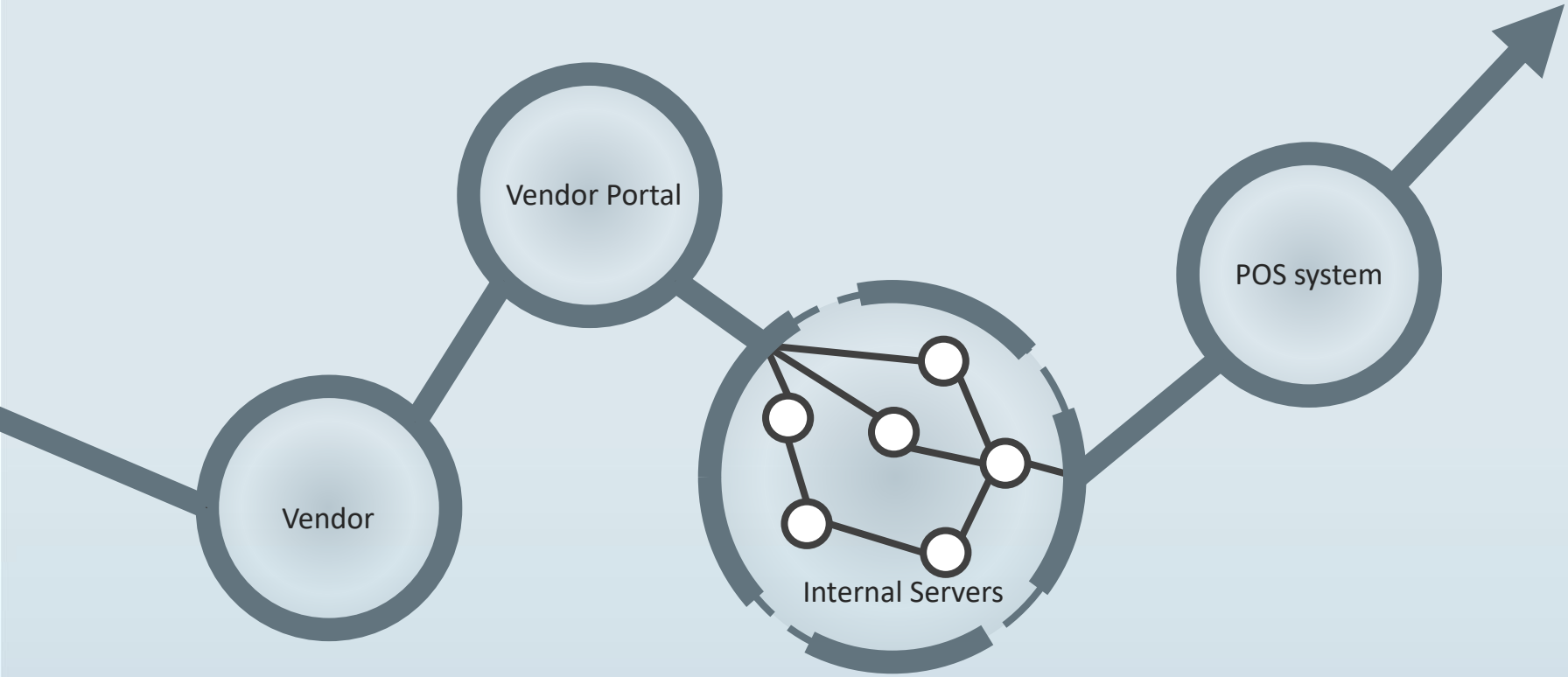




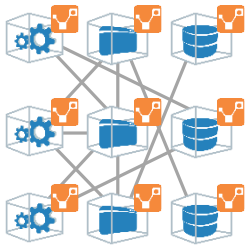




Why Does Micro-Segmentation Matter?


Vendor Portal
POS system
Vendor
Internal Servers

Micro-Segmentation Addresses Key Concerns



Map Application Dependencies

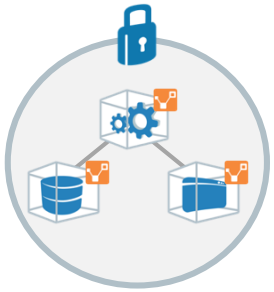
HITRUST Health Information Trust Alliance

SWIFT

PCI DSS COMPLIANT

GDPR The General Data Protection Regulation

Meet Compliance Requirements

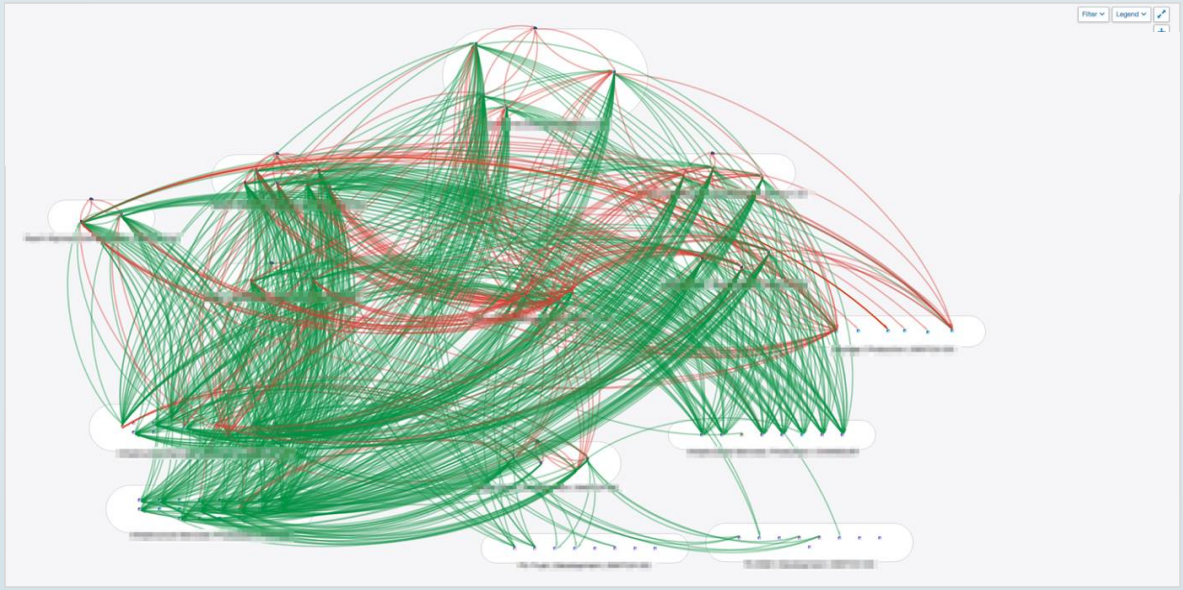


Secure Critical Applications

Securely Move To Cloud

illumio

Sounds great! So what's the issue?



~100 workloads

~200k "flows"

Segmentation the Old Way

59% have little to no visibility into traffic flows

You have to re-architect your apps and network

Up to 4 hours to create a firewall rule for new app

Static policies need to be updated manually

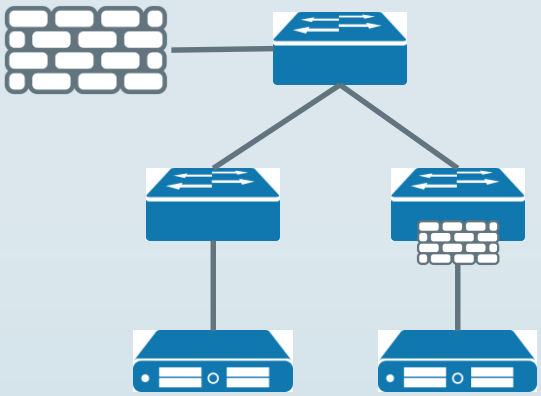
87% reported multiple outages due to configuration

Firewalls won't work in the cloud

Different Micro-Segmentation Approaches

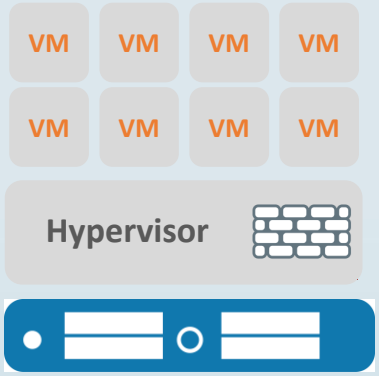
ISSA Information Systems Security Association International

Segment on the Network



Using firewalls or ACLs

Segment in the Hypervisor



Adding a firewall to hypervisors

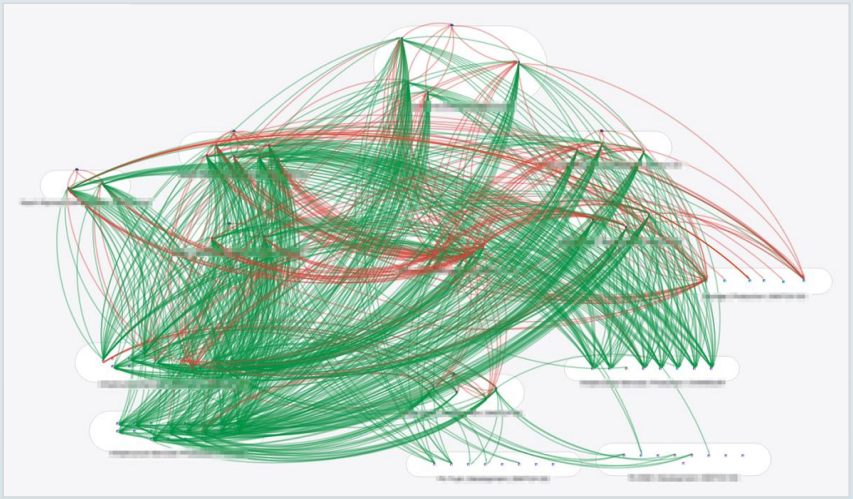
Segment at the Workload

Leveraging the native firewall in the OS

illumio

What Are the Principles of Micro-Segmentation?

What You Need for Micro-Segmentation



- ✓ Support for all environments and platforms
- ✓ Application-centric visibility
- ✓ Centralized policy creation and management
- ✓ Adaptive and automated
- ✓ Customizable granularity

How to Implement a Micro-Segmentation Strategy in 5 Steps

The 5 Steps

It's as much about process as it is about technology.

Closing Advice for Success

1. Start with visibility.
2. Test policy before enforcing.
3. Segment in phases.
4. Build partnerships between security, infrastructure, and application teams.
5. Work with an internal champion who can drive the project.

ISSA

Information Systems Security Association International

www.issa.org

More questions?

Visit

Illumio.com

illumio

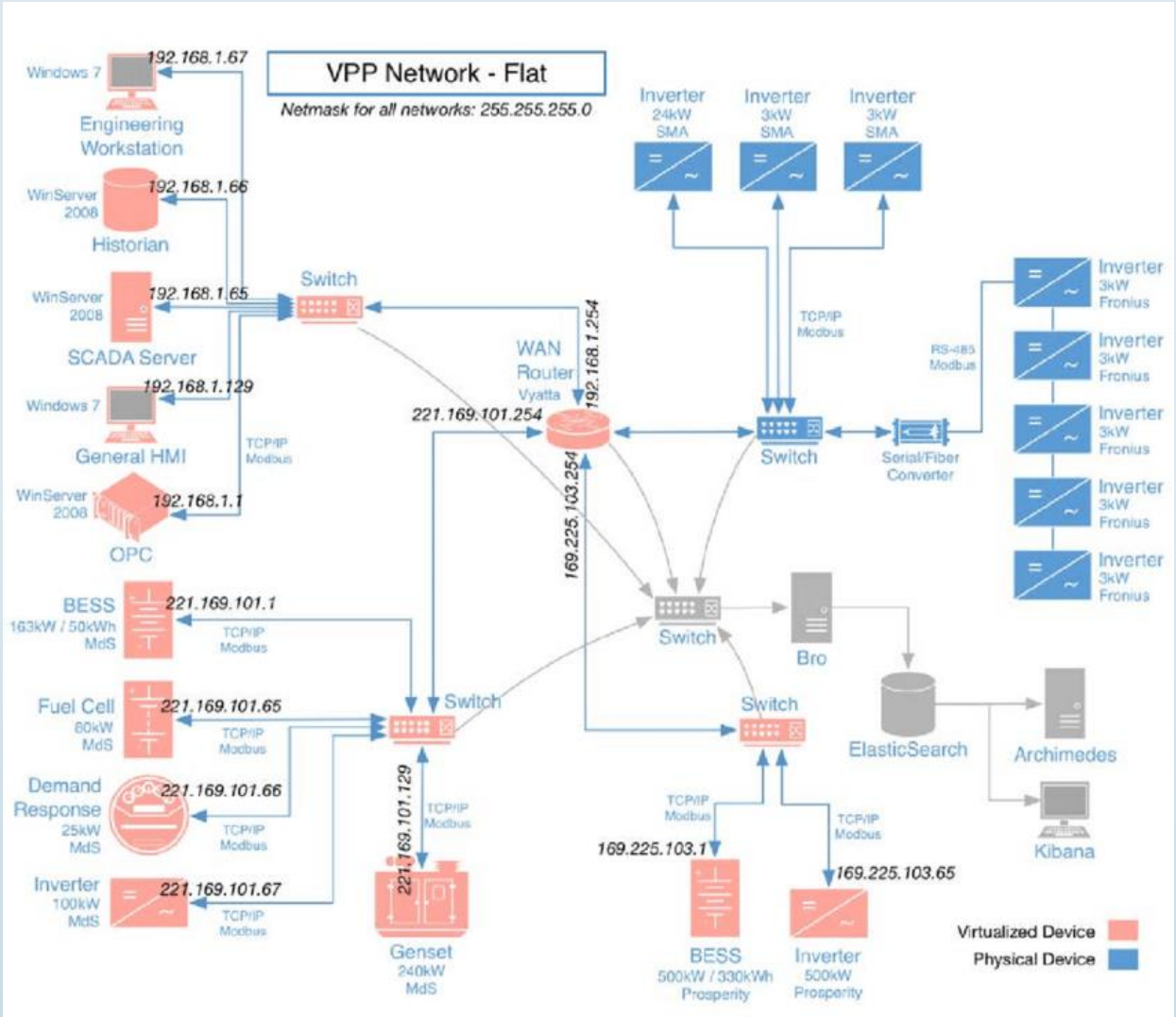
Micro-Segmentation 101

Speaker

Dr. Branden R. Williams, Director, Cyber Security, MUFG Union Bank N.A

Dr. Branden R. Williams has more than twenty years of experience in business, technology, and information security as a consultant, leader, and an executive. His specialty is navigating complex landscapes—be it compliance, security, technology, or business—and finding innovative solutions that propel companies forward while reducing risk.

Shockingly, your network:



Source: https://www.researchgate.net/figure/VPP-flat-network-diagram_fig21_319944813

Why is this hard?

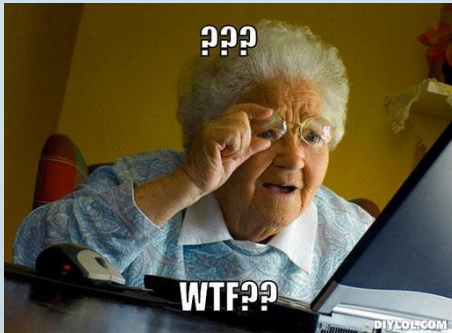
- Information Technology tends to value uptime over all other metrics.
- Makes sense, nobody calls them when it's working.
- IT == Utility!
- Two steps for diagnosing problems:
  - Have you tried turning it off and back on again?
  - Is there a firewall between those two servers? Turn that off please.
- Add multiple topologies, VPNs, affiliates, and cloud? Complex, yo!

Source: https://www.flickr.com/photos/bibihexium/4451056157

Actual MSFT support note

"We do not support restricting or altering network traffic between internal Exchange servers, between internal Exchange servers and internal Lync or Skype for Business servers, or between internal Exchange servers and internal Active Directory domain controllers in any and all types of topologies. If you have firewalls or network devices that could potentially restrict or alter this kind of network traffic, you need to configure rules that allow free and unrestricted communication between these servers (rules that allow incoming and outgoing network traffic on any port—including random RPC ports—and any protocol that never alter bits on the wire)."

- Love, Microsoft



Source: https://www.flickr.com/photos/bibihexium/4451056157

What about basic segments?

- Most firms have at least one network firewall, and many have more than one security zone:
  - Internet Facing
  - Users
- But, can we do better?
  - Sensitive/Regulated Data Zone
  - Affiliate/Contractor Zone
  - Guest Zone
  - IoT Zone
- Starting to get expensive and complex to manage!

Source: https://crmbusiness.wordpress.com/2015/01/22/the-problems-with-complex-code/

SDN: WE CAN DO BETTER!

- If we don't deploy workloads on bare metal servers, why do we design network security controls that way?
- We want security controls to follow data around, so why not apply the same concept to workloads?
  - Containers on internal virtualized servers
  - Serverless/Lambda
  - AWS/Azure/Google Public Cloud
  - *gasp* BYOD?!
- Enter Micro-segmentation:
  - Micro-segmentation is a security technique that enables fine-grained security policies to be assigned to data center applications, down to the workload level. This approach enables security models to be deployed deep inside a data center, using a virtualized, software-only approach. (Source below)

Source: https://www.sdxcentral.com/sdn/network-virtualization/definitions/how-does-micro-segmentation-help-security-explanation/

Dr. B's General Thoughts

Can it actually work?

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

Micro-Segmentation 101

Speaker

John Donovan, ISSA Silicon Valley Chapter & Rook Security

John is past-president and a board director of the Silicon Valley ISSA Chapter He's a member of the CaC (CISO Advisory Council) for the ISSA's CISO Executive Forum and participant in a number of security events including past CISO Executive Forums, ISSA International and regional conferences such as the Cornerstones of Trust conference in the San Francisco Bay Area. John is a passionate supporter of both the local arts community and cyber-security community in the Silicon Valley and beyond. In his day job, John builds and runs security programs and is currently CISO for an early-stage security technology startup. Past professional positions include developing and managing Security, Risk, IT, and engineering programs for Illumio, Veracode, NetApp, Xilinx, and other technology and security companies .

John Donovan

Micro-Segmentation 101 and Beyond

Segmentation 101

- A Segmentation Story
  - the Hotel Model
- Segmentation & Compliance
- Micro-Segmentation & Real Security Controls
- Cloud, Hybrid Cloud, Containerization & …
- Beyond Segmentation to Active Control

Segmentation & Compliance

Segmentation is table-stakes for many compliance and regulatory regimes

- PCI and CDE (Card Holder Data Environment)
- HIPAA & Healthcare
- SOC2, ISO27k, …

Real Security Controls

Real Security Controls require **Control**

- Segmentation strategy is step one
- Put your controls where the ____ is
  - Application
  - Services
  - Data & Critical Assets
  - …
- Maximize the Defenders Advantage

From Data-center to Cloud

Enterprise migration of services from private data-centers to public and private cloud environments continues at an accelerating pace. Many new companies build and launch “only on cloud”.

- Data-center to Cloud Migrations
- Hybrid Cloud and Multi-Cloud
- Cloud native and internet scale providers
- Ephemeral Containers & Container-less services

Beyond Segmentation to ..

Active and Dynamic Control must include the following

- User Identities
  - End Users
  - Administrative Users
- True White-list model
- Segmentation that follows workloads whether Server, container, or server-less (lambda)

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?