



# Real-Life Software-Defined Security

Ivan Pepelnjak ([ip@ipSpace.net](mailto:ip@ipSpace.net))  
Network Architect

ipSpace.net AG

# Who is Ivan Pepelnjak (@ioshints)

## Past

- Kernel programmer, network OS and web developer
- Sysadmin, database admin, network engineer, CCIE
- Trainer, course developer, curriculum architect
- Team lead, CTO, business owner



## Present

- Network architect, consultant, blogger, webinar and book author

## Focus

- SDN and network automation
- Large-scale data centers, clouds and network virtualization
- Scalable application design
- Core IP routing/MPLS, IPv6, VPN

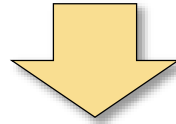


**What is Software-  
Defined Security?**

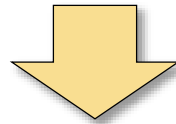
**Mostly Marketing**

**Every Well-Defined  
Repeatable Task  
Can Be Automated**

# Automation

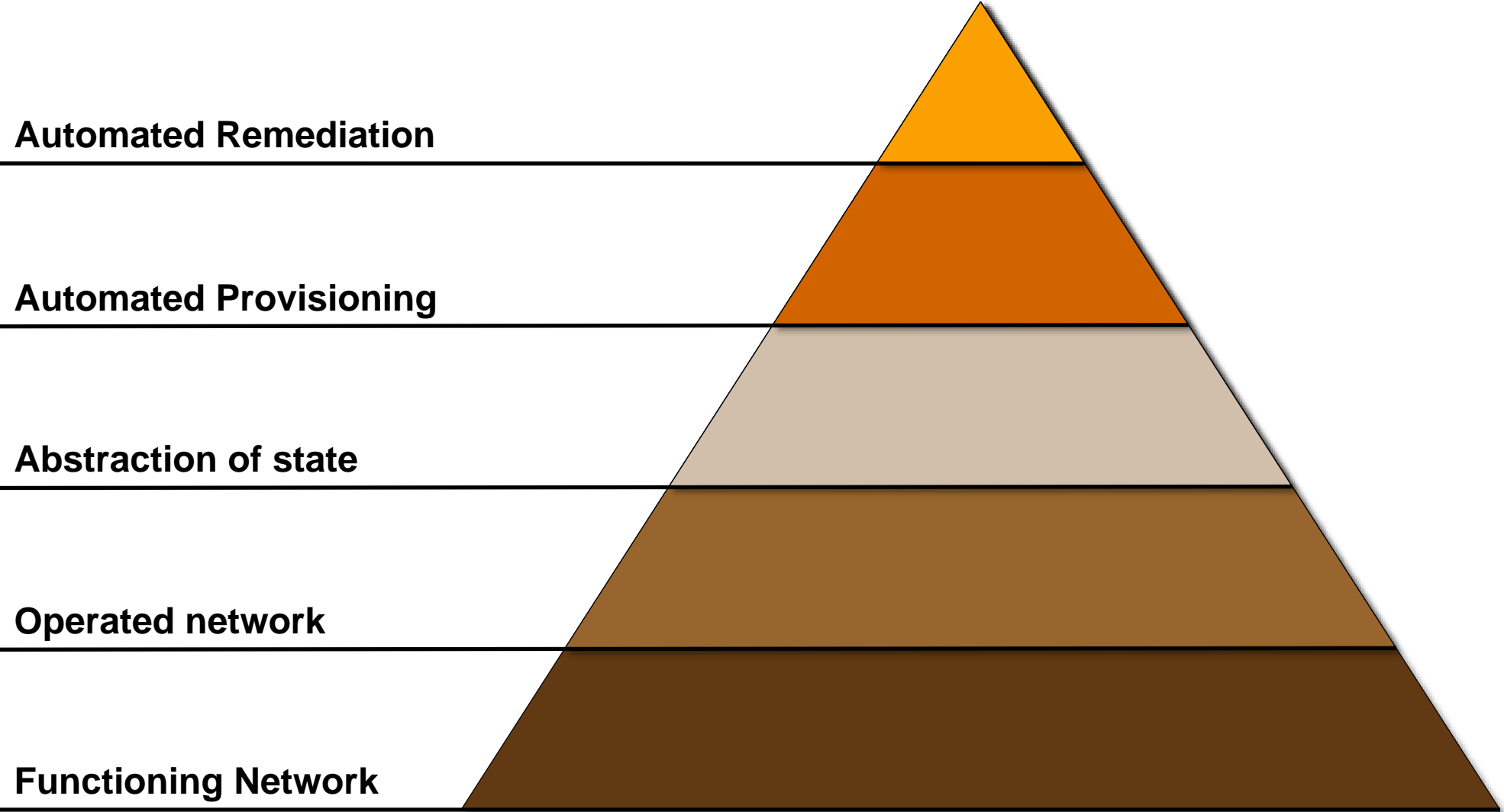


# Repeatability



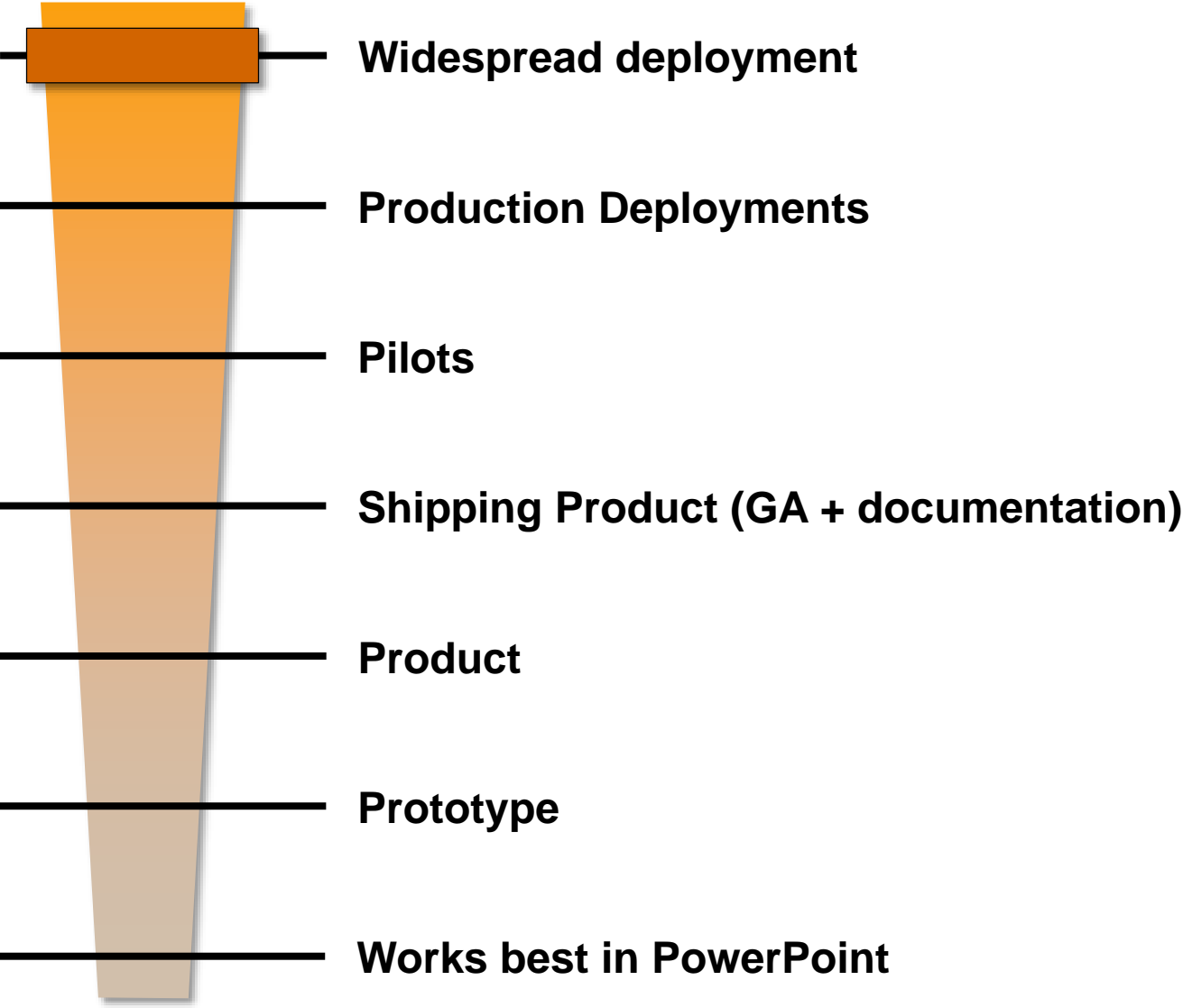
# Validation

# Hierarchy of Network Needs (also Applies to Security)

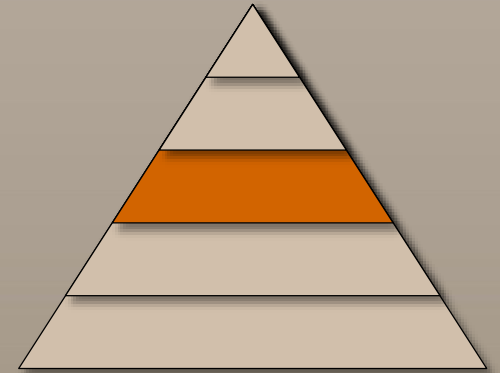
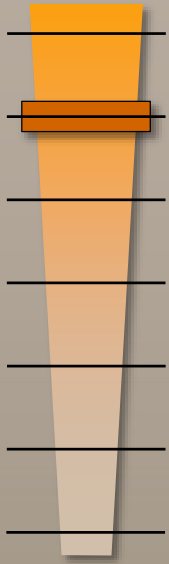


Source: Jeremy Stretch, packetlife.net

# Deployment Readiness (aka Reality Check)

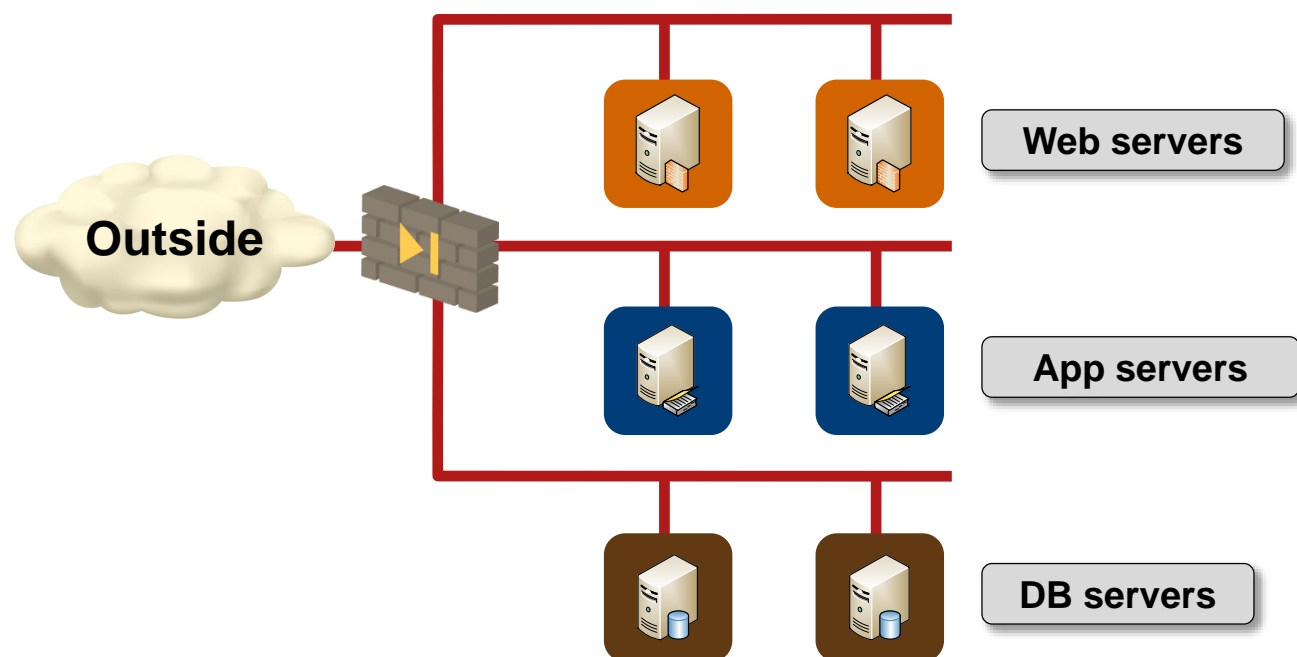


# Microsegmentation





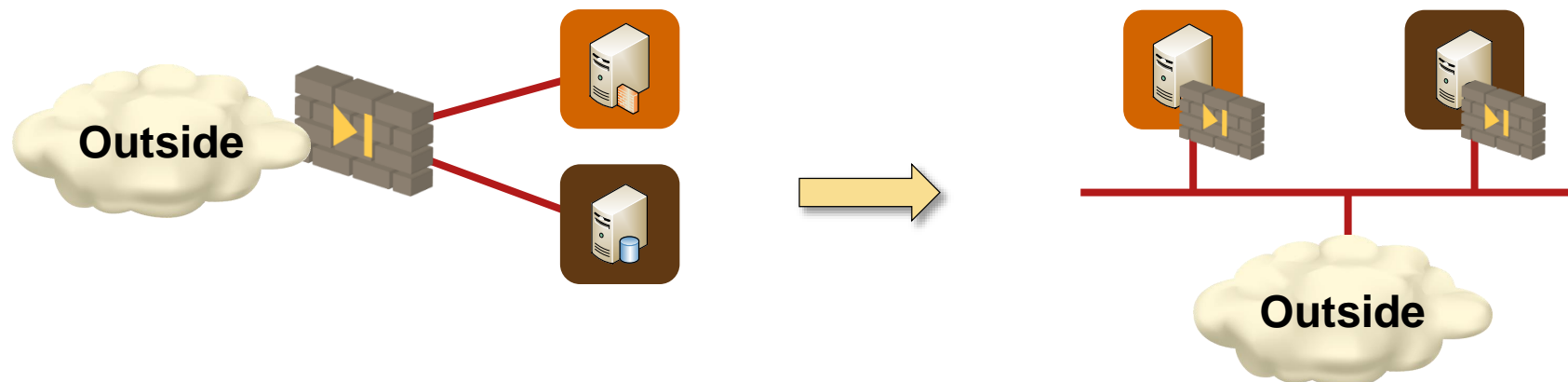
## Traditional Virtual Segments



- Security zones implemented with virtual L2/L3 segments
- Multiple applications are typically deployed in the same zone
- Inter-zone traffic is inspected, intra-zone traffic is not → an intruder can easily move laterally and break into other applications

More in *IPv6 Microsegmentation* webinar

# Microsegmentation: Changing the Security Paradigm



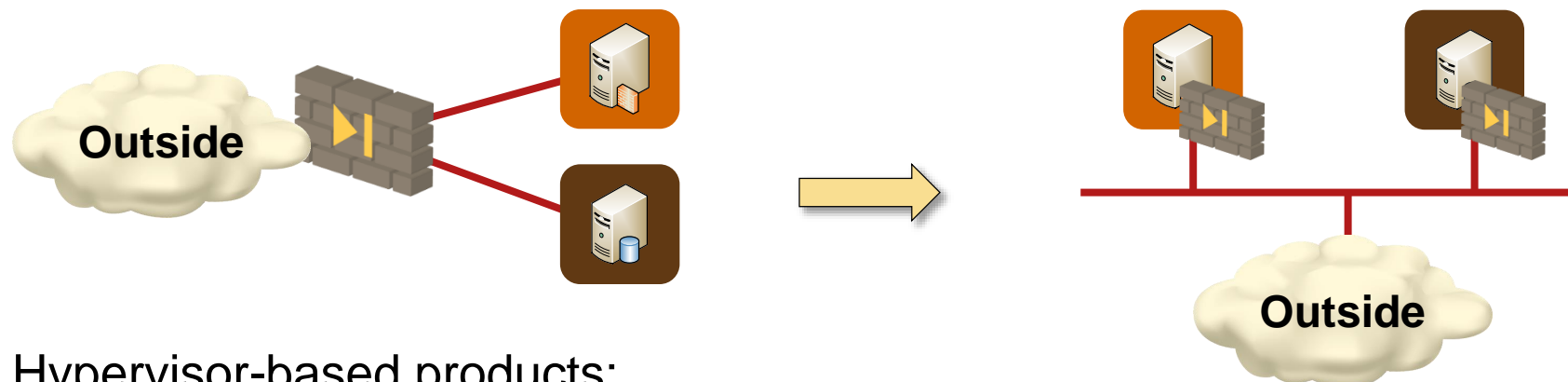
## Microsegmentation 101

- More-or-less stateful firewall (usually reflexive ACL) protects every server
- Implemented in hypervisors (VM NIC firewalls) or ToR switches
- Centrally managed security policies
- Controller pushes policies to network edge devices

## Benefits

- Every server is protected, even against other servers in the same tier
- Centralized security policies
- VLANs are no longer a security mechanism

## Microsegmentation: Sample Products



Hypervisor-based products:

- OpenStack and CloudStack security groups (implemented with KVM iptables)
- VMware NSX
- Microsoft Hyper-V
- Nuage VSP
- Juniper Contrail
- Cisco ACI with AVS

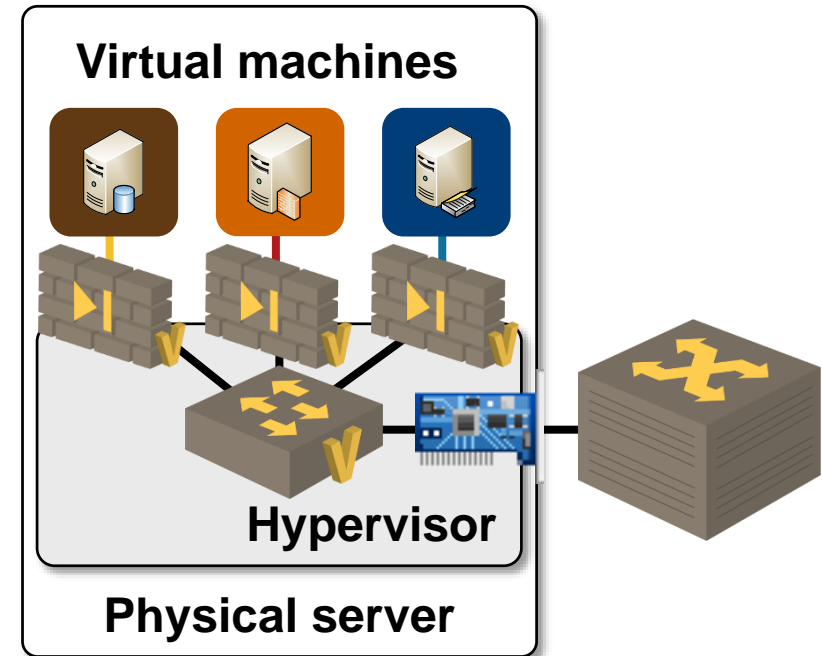
ToR-based products:

- Cisco ACI (pure packet filters, also less effective in virtualized environments)

More in *Virtual Firewalls* webinar

## Questions to Ask

- How are security rules created?
- Stateless or stateful?
- Is state moved with the VM?
- Filtering in kernel module or userland?
- Per-hypervisor control VM?
- Is control VM involved in flow setup?
- What happens when control VM fails?



# VMware NSX for vSphere Distributed Firewall

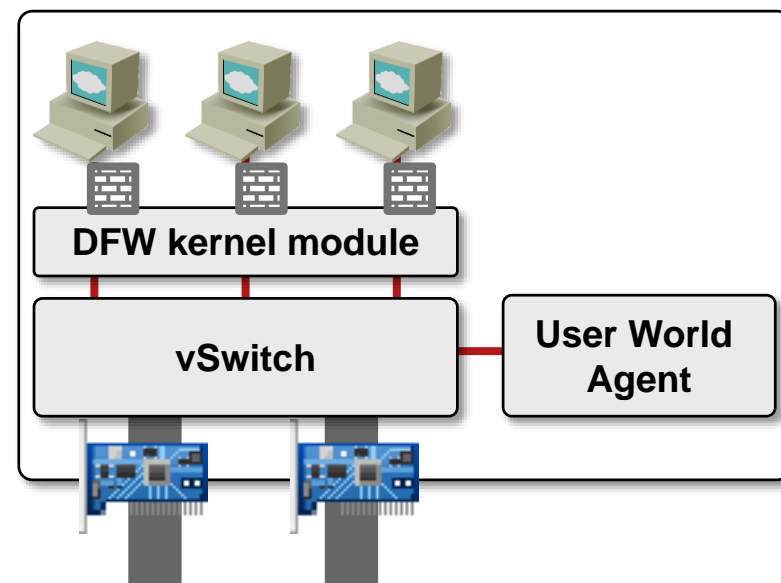
- Per-host in-kernel firewall + agent
- Central management (NSX Manager)

## Performance enhancements

- Firewalling in a loadable kernel module
- Firewallled traffic no longer traverses userland
- No per-host firewalling or management VM
- Managed through UWA

## Firewalling functionality:

- Stateful L3/4 firewall, matching on IP addresses or vSphere objects
- ARP and other L2 traffic filters
- Source IP address validation
- DHCP snooping and ARP snooping (NSX 6.2)
- IPv4 and IPv6



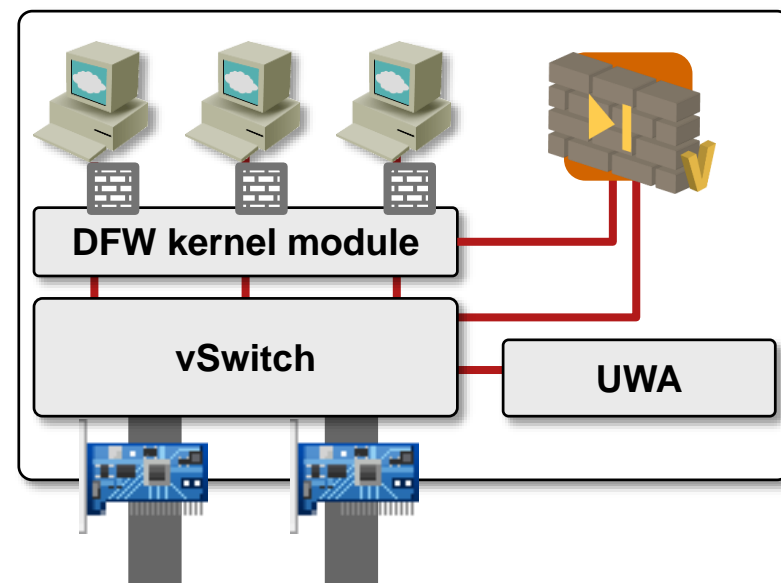
More in VMware NSX Architecture webinar

## NSX for vSphere Third-Party Firewalls

- Distributed firewall rule redirects traffic to third-party firewall
- Third-party solution resides in a VM on the same host
- Configured through NSX Manager firewall rules or service composer

### Example: Palo Alto Networks integration

- Simple filtering rules implemented in NSX distributed firewall
- Application-level inspection implemented in Palo Alto virtual firewall
- Central management through NSX Manager and Panorama
- Automatic creation of security groups from vCenter VM attributes



# Microsegmentation in Public Clouds

Summary **Inbound Rules** Outbound Rules Tags

Cancel **Save**

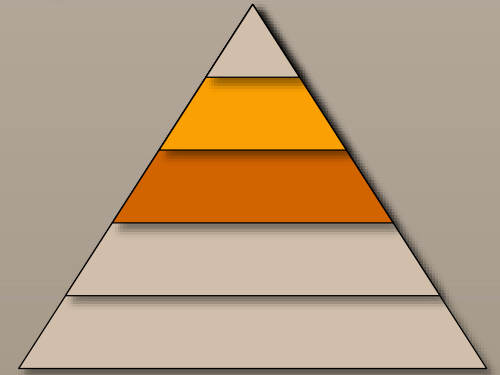
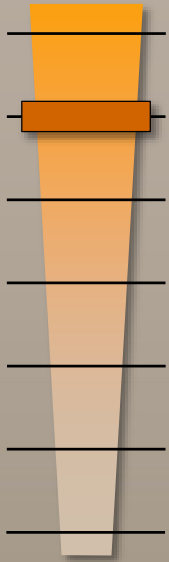
Type	Protocol	Port Range	Source	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0 <i>i</i>	<b>X</b>
HTTPS (443)	TCP (6)	443	0.0.0.0/0 <i>i</i>	<b>X</b>
SSH (22)	TCP (6)	22	192.0.2.0/24 <i>i</i>	<b>X</b>
RDP (3389)	TCP (6)	3389	192.0.2.0/24 <i>i</i>	<b>X</b>

Add another rule

Source: Amazon VPC documentation

- Amazon EC2/VPC security rules
- OpenStack or CloudStack security groups
- Simple rules, no ALG
- Deployed in real time

# Automating Microsegmentation

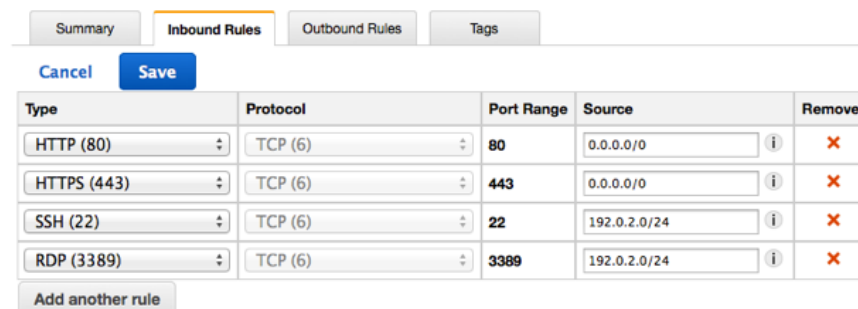












# Automating Microsegmentation

Every microsegmentation solution has a well-defined API

- Amazon EC2
- CloudStack, OpenStack
- VMware NSX



The screenshot shows a web interface for configuring microsegmentation rules. It has tabs for 'Summary', 'Inbound Rules', 'Outbound Rules', and 'Tags'. Below the tabs are 'Cancel' and 'Save' buttons. A table lists four inbound rules:

Type	Protocol	Port Range	Source	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0	 
HTTPS (443)	TCP (6)	443	0.0.0.0/0	 
SSH (22)	TCP (6)	22	192.0.2.0/24	 
RDP (3389)	TCP (6)	3389	192.0.2.0/24	 

Below the table is an 'Add another rule' button.

Automate deployments of security rules by using microsegmentation API

- Cloudify (AWS, OpenStack, CloudStack, vSphere, vCloud...)
- Ansible (Openstack, CloudStack, EC2)
- PowerShell (vSphere, NSX, Microsoft Hyper-V)

Works best with automated application deployment process

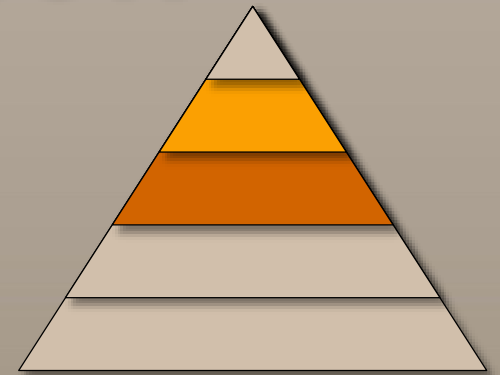
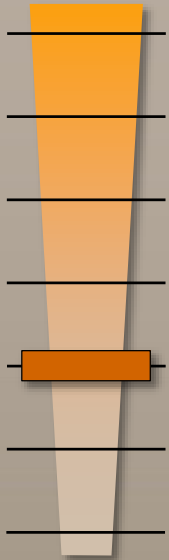
## Example: Creating OpenStack Security Rule in Ansible

```
# Create a security group
- os_security_group:
  cloud: mordred
  state: present
  name: foo
  description: security group for foo servers

- os_security_group_rule:
  cloud: mordred
  security_group: foo
  protocol: tcp
  port_range_min: 80
  port_range_max: 80
  remote_ip_prefix: 0.0.0.0/0
```

More in *Network Automation* workshop

# Validating Microsegmentation



# Example: Amazon Inspector

Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. [Learn more.](#)

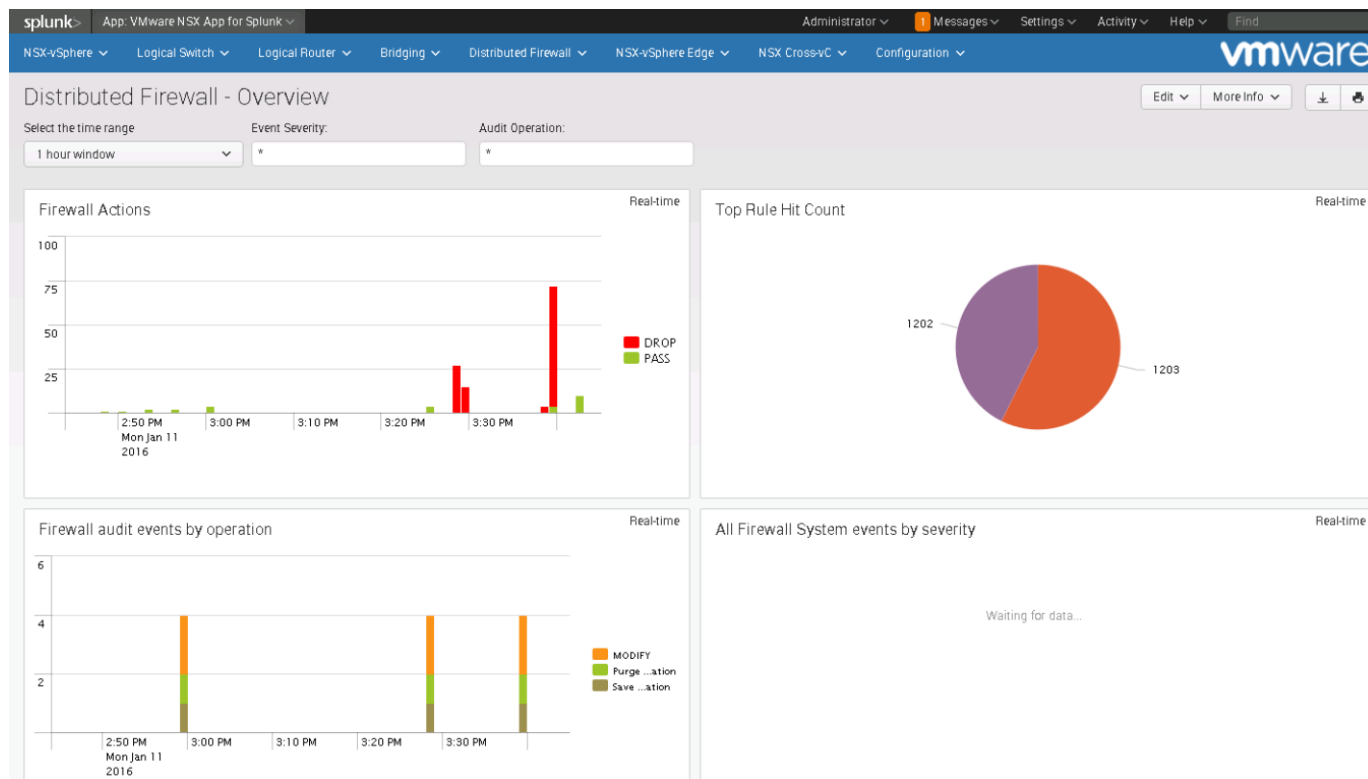
[Add/Edit attributes](#) Last updated on September 24, 2015 4:12:42 PM (20m ago)

<input type="checkbox"/>	Severity	Application	Assessment	Rule package	Finding
<input type="checkbox"/>	High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c4e
<input type="checkbox"/>	High	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c4e
<input type="checkbox"/>	High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password com
<input type="checkbox"/>	Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	Instance i-aac4c4e
<input type="checkbox"/>	Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	The machine i-aac
<input type="checkbox"/>	Informational	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential securi
<input type="checkbox"/>	Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	The machine i-aac
<input type="checkbox"/>	Informational	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential securi
<input type="checkbox"/>	Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	Instance i-aac4c4e
<input type="checkbox"/>	Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	A machine with Ins

Viewing 1-10

- Hundreds of built-in rules
- Custom rules (tailored to your security requirements)
- Automatically evaluated and reported

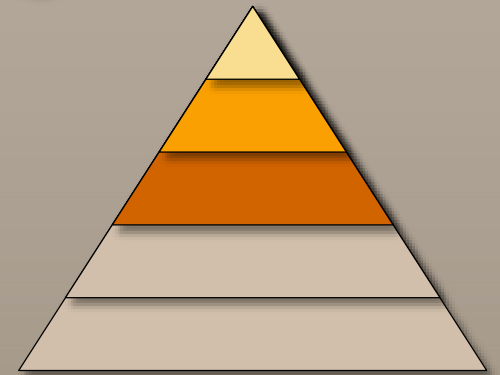
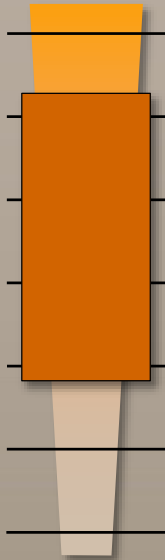
# VMware NSX Plug-in for Splunk



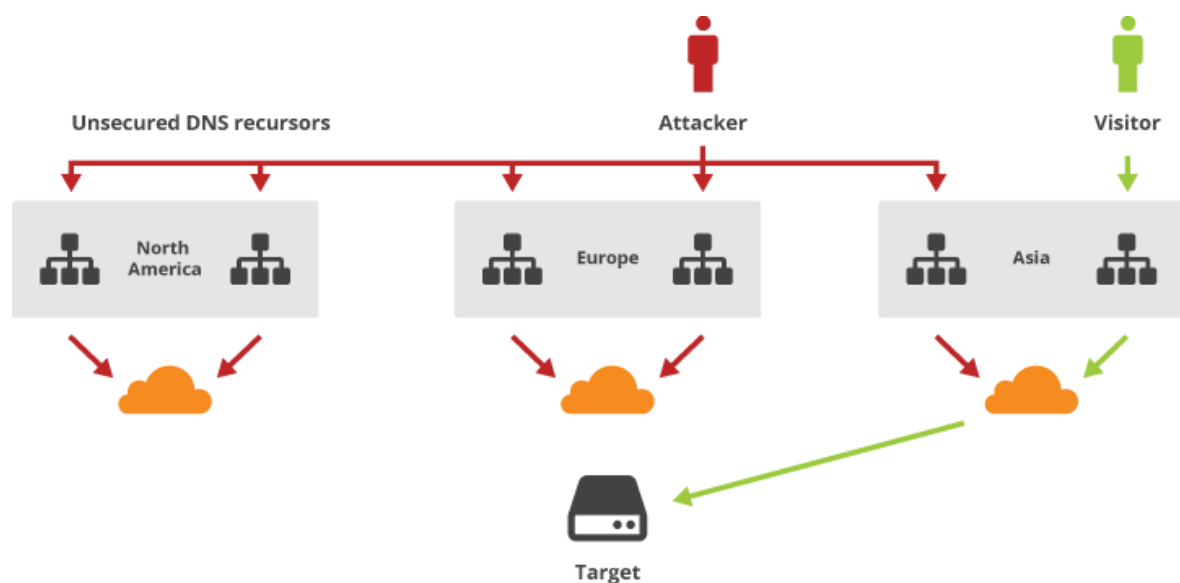
- Generic rules applied to VMware distributed firewall
- Splunk logs used to create additional (more refined) security rules
- Detailed security rules are inspected and deployed (manually)
- Generic rules are removed after a while

**I wouldn't use this approach (see also: *halting problem*)**

# DoS Detection and Mitigation Tools

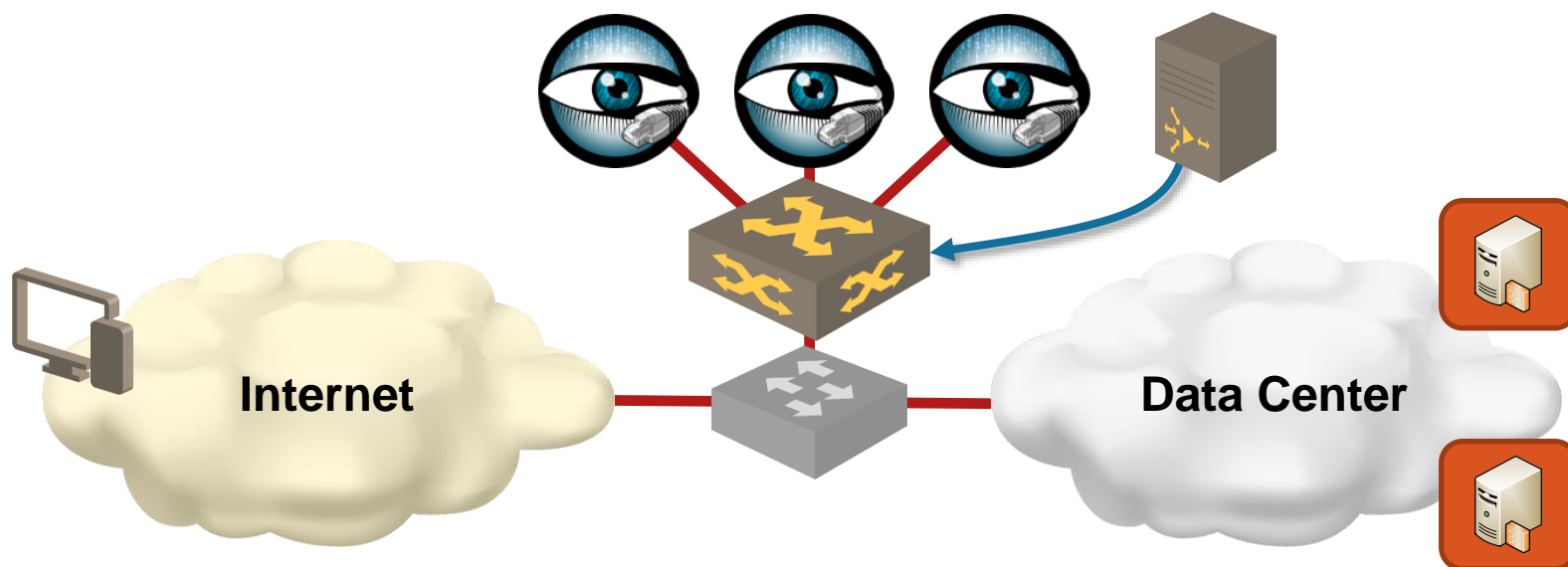


## Example: CloudFlare

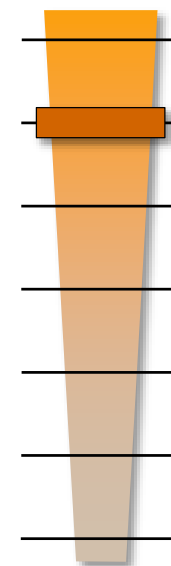


- Automatic DDoS detection and mitigation
- All visitor traffic passes through CloudFlare servers
- Automatic adjustments (or bypass) through CloudFlare API
- User-written Ansible module ;)

# Scale-Out IDS with Coarse-Grained Flow Forwarding



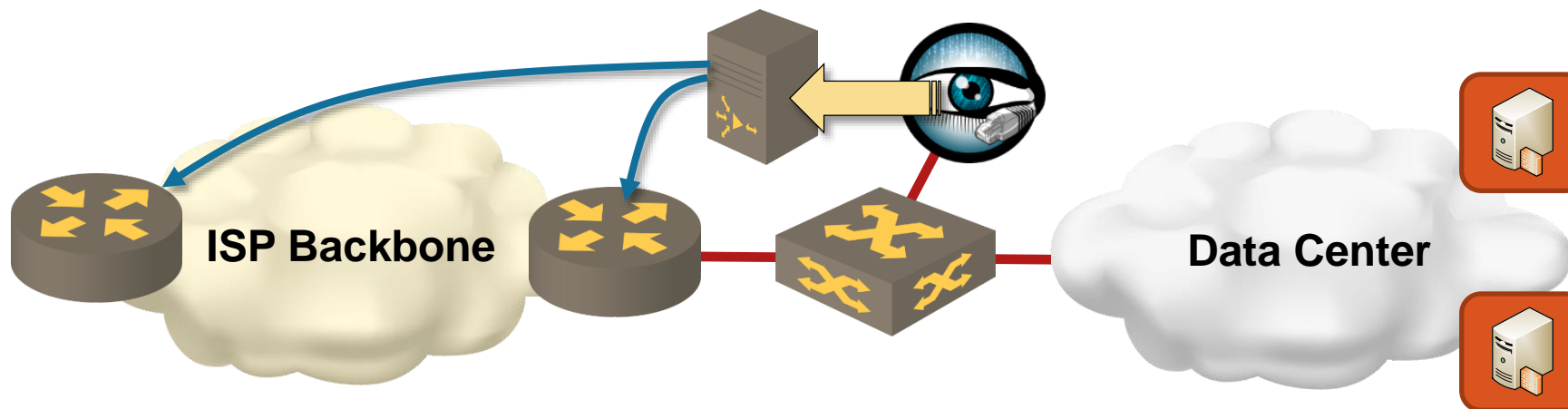
- Traffic from Internet link is mirrored to a distribution switch
- Coarse-grained flows (PBR rules) deployed on the switch
- Flow granularity adjusted in real time if needed
- Each appliance receives all traffic from a set of endpoints → complete session and endpoint behavior visibility



Open-Source tool: SciPass (Indiana University)



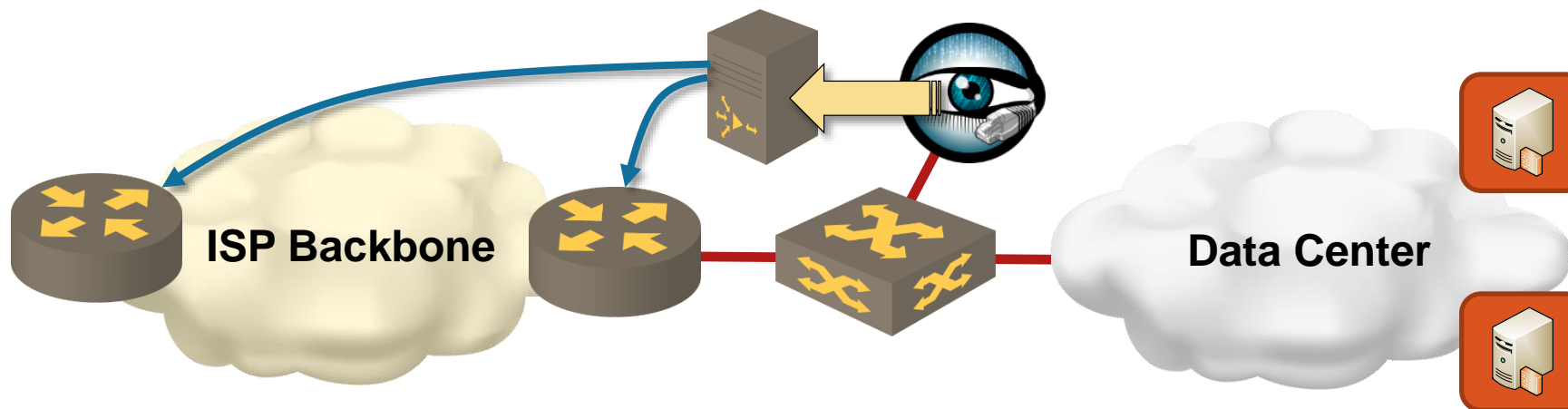
# Remote-Triggered Black Hole: a Decade of SDN



- Install a host route to a bogus IP address (RTBH address) pointing to *null* interface on all routers
- Use BGP to advertise host routes of attacked hosts (modified next-hop or BGP community)
- Use uRPF to drop traffic *from* DoS sources

Widely used in ISP environments

## BGP FlowSpec: RTBH on Steroids



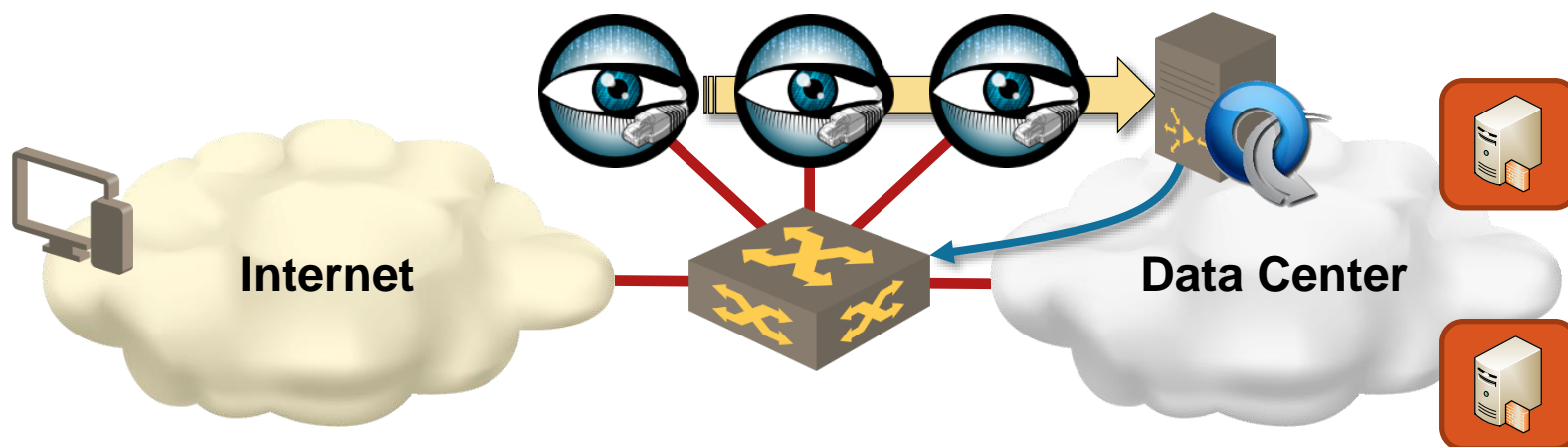
Controllers can use BGP to install PBR-like forwarding entries into Flowspec (RFC 5575)-capable routers

- Matches on source/destination IP prefixes and ports, IP protocol, ICMP code, TCP flags, packet length, DSCP code ...
- Functionality almost identical to OpenFlow

Use cases: distributed fine-grained filters or PBR

Implemented on Juniper, Cisco and ALU devices, used by CloudFlare

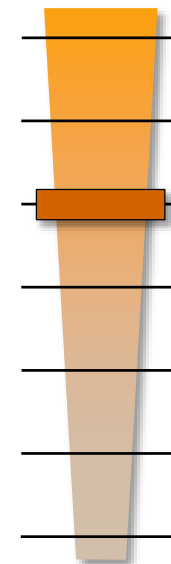
# Scale-Out IDS Using OpenFlow to Block Traffic



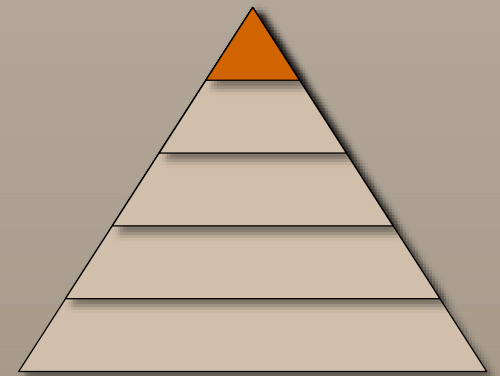
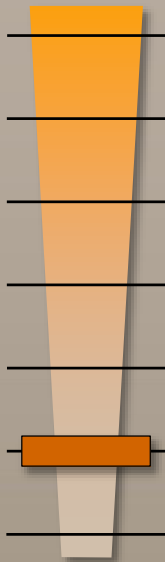
DoS detection system reports offending X-tuples

- Source IP addresses
- Targeted servers
- Applications (port numbers)

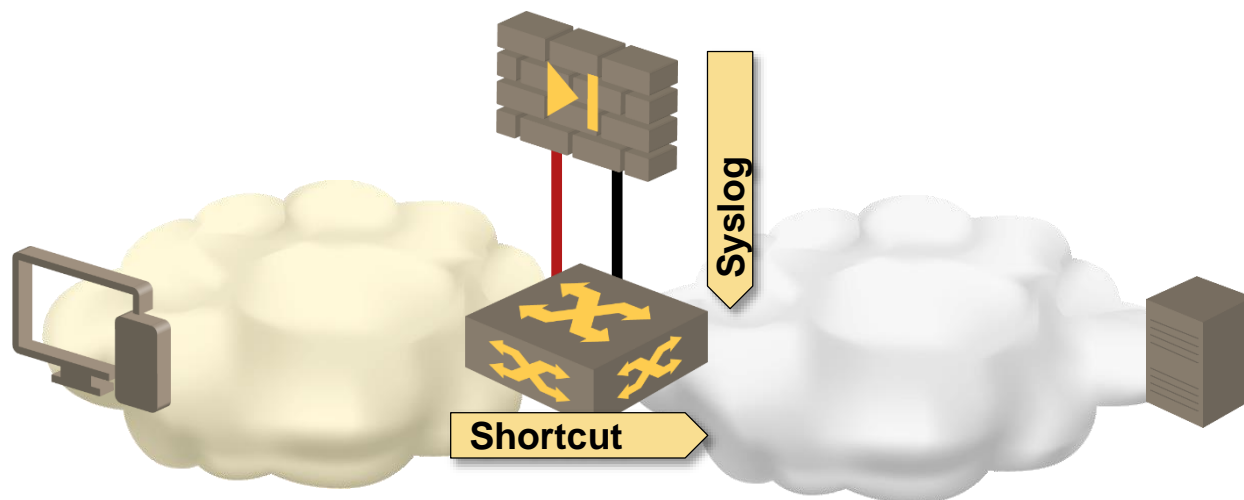
OpenFlow controller installs *drop* flows



# Firewall Bypass



## Demonstration: Arista + Palo Alto



- Arista switch runs *syslog* server
- Palo Alto firewall logs permitted sessions via *syslog* to Arista switch
- Arista switch installs shortcut entries for predefined class of flows

Use case: reduce firewall load by shortcutting high-volume flows

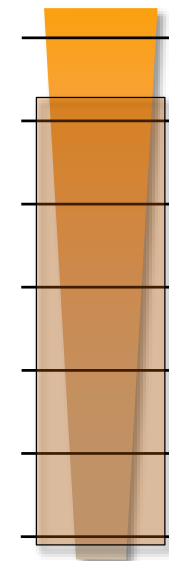
# Other Security- Related SDN Use Cases

## Other Security-Related SDN Use Cases

- Software-defined WAN
- Service insertion
- Programmable network taps
- Tap aggregation networks
- Network monitoring
- Scale-out Network Services
- Consistent edge policy enforcement

### Deployment readiness

- Products, concepts, open-source...
- From shipping products to DIY frameworks
- Explore → evaluate → pilot → deploy

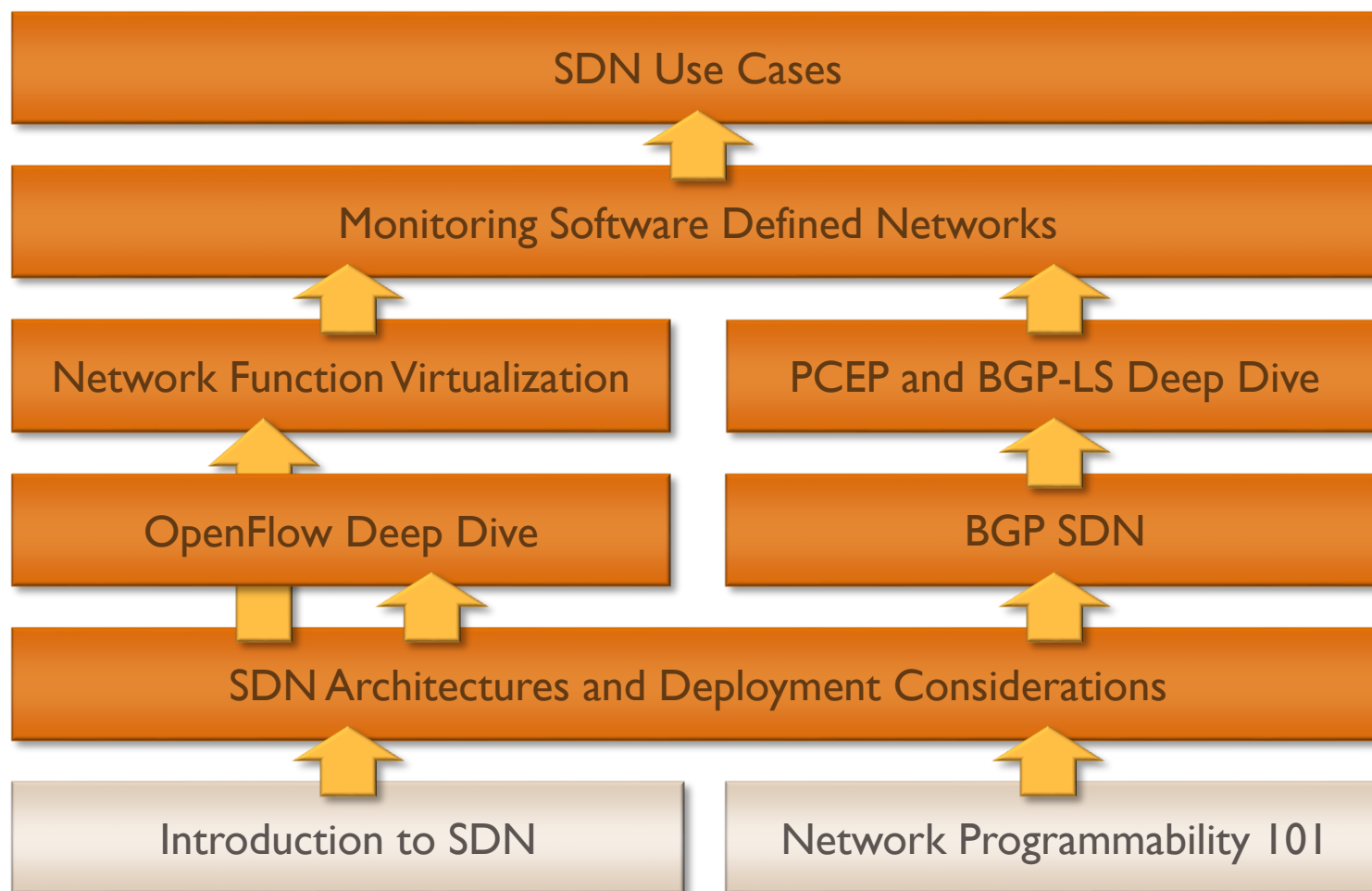


**Goal: you'll be speaking about your deployment experience @ Troopers 2017 ;)**

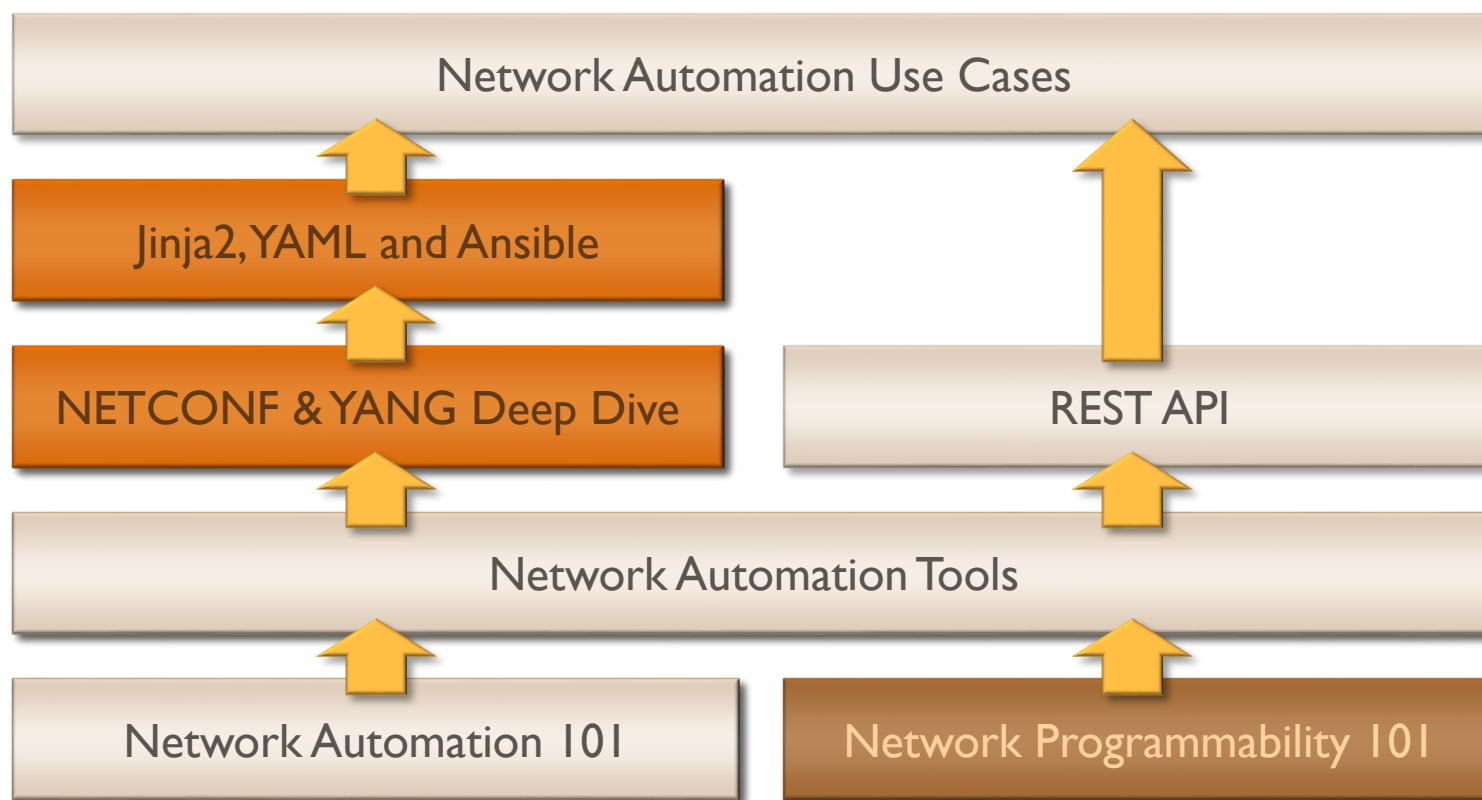
# More Information



# Advanced SDN Track



# Network Automation Track



00 0110 000 0110 01 1010 0  
00 0110 000 0110 01 1010 0

**Advance your professional career by gaining SDN skills.**  
Join the Advanced SDN Training now! [CLICK HERE](#)

**SUBSCRIBE to SDN mailing list**  
Get SDN tips, training announcements, presentations, videos and blog posts straight into your Inbox.

**NAME:**

**EMAIL:**

[SIGN UP](#)

## SDN, OPENFLOW AND NFV RESOURCES ON IPSPACE.NET

Software-defined networking (SDN) can mean anything, from programmable network elements to architectures in which control- and forwarding planes reside on different devices.

The resources listed on this page will help you understand SDN, its implications and its applicability in your environment.

### SDN TRAINING AND CONSULTING



- [On-site and online consulting](#)
- [SDN, OpenFlow and NFV Workshop](#)
- [Software Defined Data Centers \(SDDC\) Workshop](#)
- [Advanced SDN Training](#)
- [Introduction to SDN](#)
- [Customized webinars and workshops](#)

### INDIVIDUAL SDN WEBINARS

- [NETCONF and YANG](#)
- [Network Programmability 101](#)
- [SDN Architectures and Deployment Considerations](#)
- [VMware NSX Architecture](#)

[MORE SDN WEBINARS](#)

### SDN-RELATED BOOKS



- [Overlay Virtual Networks in Software-Defined Data Centers](#)

[BUY NOW](#)

- [SDN and OpenFlow](#)

[BUY NOW](#)

### PRESENTATIONS

- [SDN - 4 Years Later \(video\)](#)
- [What is SDN?](#)
- [Should I program my network? \(video\)](#)
- [Virtual Routers](#)
- [From Traditional Silos to SDDC \(video\)](#)
- [What Matters is Your Business \(video\)](#)
- [Automating Network Security, Troopers 15](#)

[MORE SDN PRESENTATIONS](#)

[MORE SDDC PRESENTATIONS](#)

## Stay in Touch

Web: [ipSpace.net](http://ipSpace.net)  
Blog: [blog.ipSpace.net](http://blog.ipSpace.net)  
Email: [ip@ipSpace.net](mailto:ip@ipSpace.net)  
Twitter: [@ioshints](https://twitter.com/ioshints)



SDN: [ipSpace.net/SDN](http://ipSpace.net/SDN)  
Webinars: [ipSpace.net/Webinars](http://ipSpace.net/Webinars)  
Consulting: [ipSpace.net/Consulting](http://ipSpace.net/Consulting)



A young child stands in the center of a large-scale floor installation. The floor is covered with a large, light-colored map of Europe, with several cities labeled in black text: 'Paris', 'London', 'Brussel', and 'Kobe'. Three black network devices, likely routers or switches, are placed on the floor. They are interconnected by a complex network of colorful cables (red, blue, yellow, green, black) that snake across the map. The child is wearing a white t-shirt with red sleeves and dark pants. The floor is made of grey tiles.

Questions?

Send them to [ip@ipSpace.net](mailto:ip@ipSpace.net) or [@ioshints](https://twitter.com/ioshints)