Managing VM Security

Tim Warner
AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim timw.info

MVP
Microsoft®
Most Valuable Professional

Microsoft
CERTIFIED
Trainer

Solutions Expert

Cloud Platform and Infrastructure

Overview

Configure resource-level (RBAC) security

Configure storage security

Configure network security

- NSG, JIT VM Access

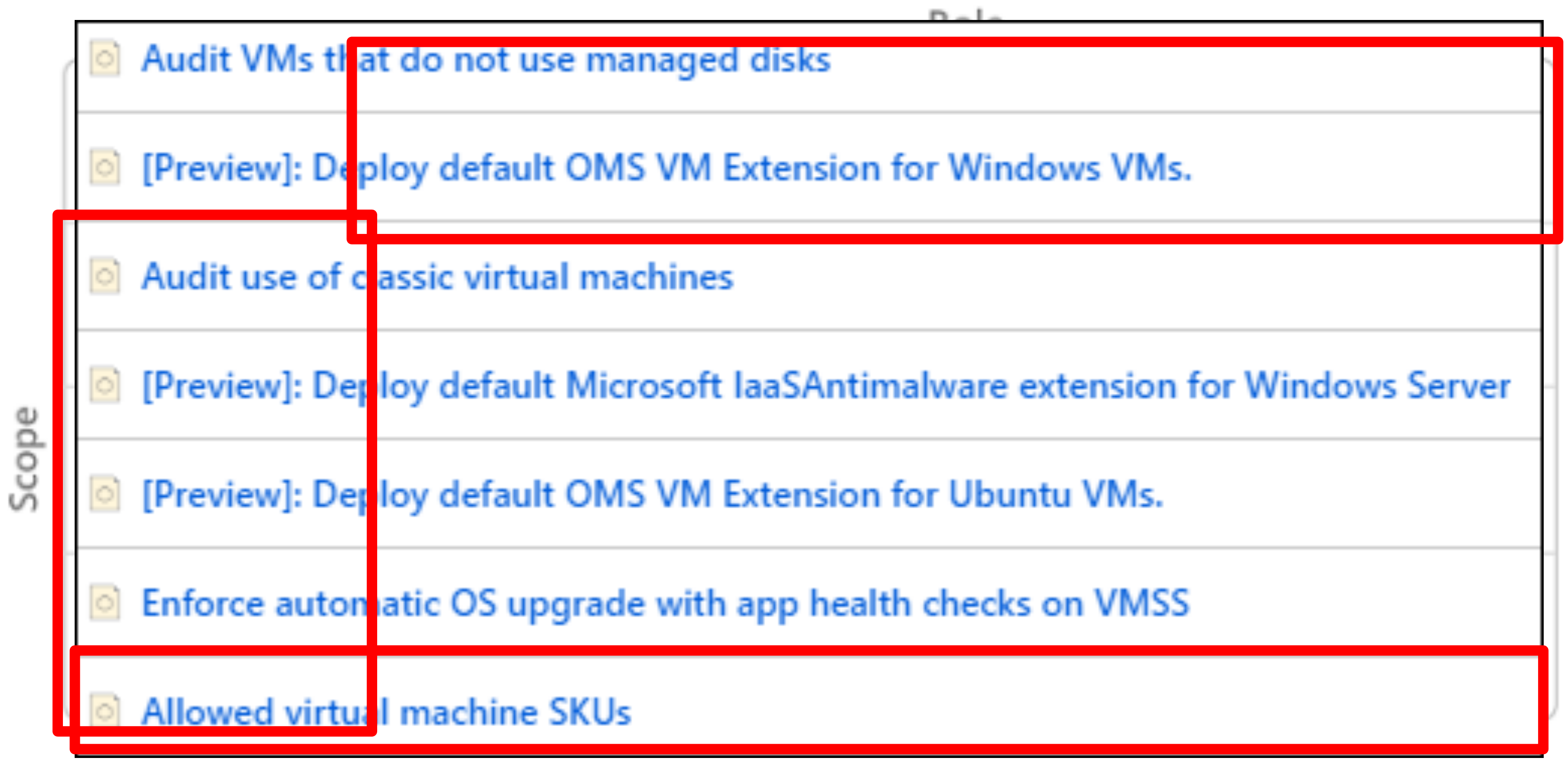
Use Azure Security Center

RBAC Security

Role-Based Access Control (RBAC)

Authorization system (not authentication) in ARM that provides fine-grained access to Azure resources.

Azure RBAC Permission Scopes



Audit VMs that do not use managed disks

[Preview]: Deploy default OMS VM Extension for Windows VMs.

Audit use of classic virtual machines

[Preview]: Deploy default Microsoft IaaSAntimalware extension for Windows Server

[Preview]: Deploy default OMS VM Extension for Ubuntu VMs.

Enforce automatic OS upgrade with app health checks on VMSS

Allowed virtual machine SKUs

Custom roles are defined in JSON

RBAC focuses on user actions at different scopes

By contrast, Azure Policy focuses on resource properties during deployment

Common VM-Related Roles

Owner

Contributor

VM Contributor

Reader

Demo

1

RBAC (Grant Reader at the resource group level)

Storage Security

Azure Storage Security

Storage Service Encryption

- Protects data at rest in storage account
- 128-bit AES encryption
- Azure manages encryption keys
- You can manage them yourself with Azure Key Vault

Azure Disk Encryption

- BitLocker for Windows Server VMs
- DM-Crypt library for Linux VMs
- Protects OS and data disks
- Azure- or customer-managed keys

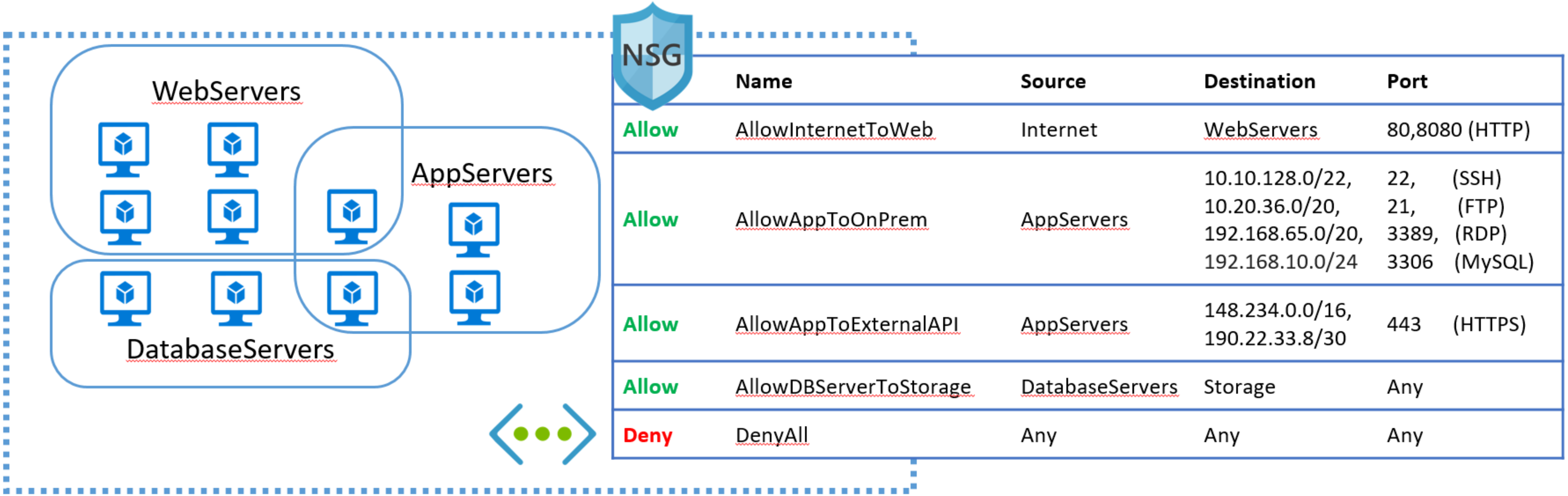
Demo

2

Enable ADE for a Windows Server VM OS disks

Network Security

Network Security Groups (NSGs)



	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

Stateful firewall

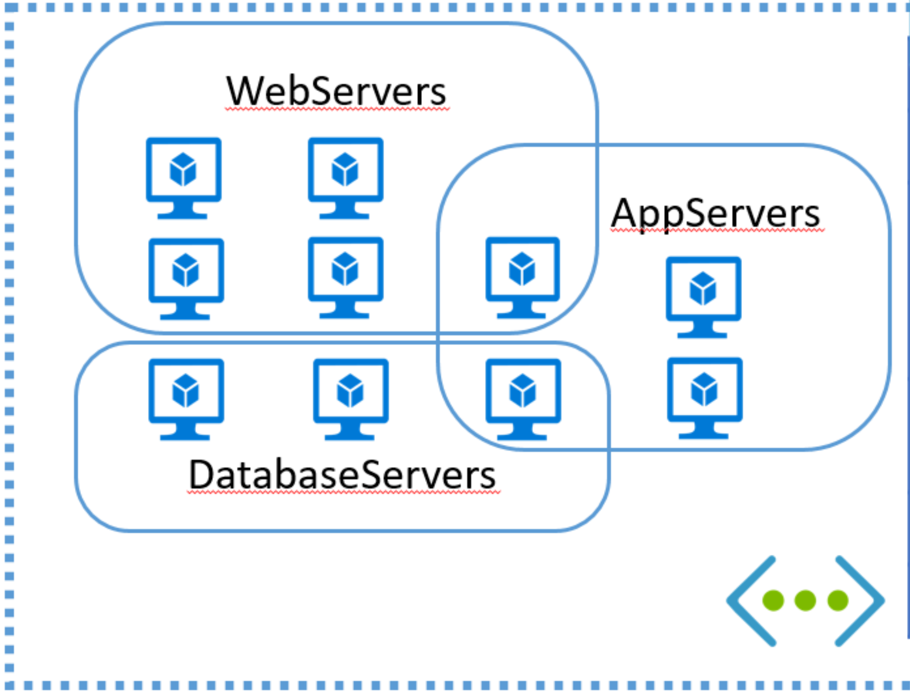
Traffic streams identified with 5-tuple hash

Inbound and outbound rules

Augmented security rules

Service tags

Application Security Groups (ASGs)



NSG	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

Logically group VMs (by role, for instance)

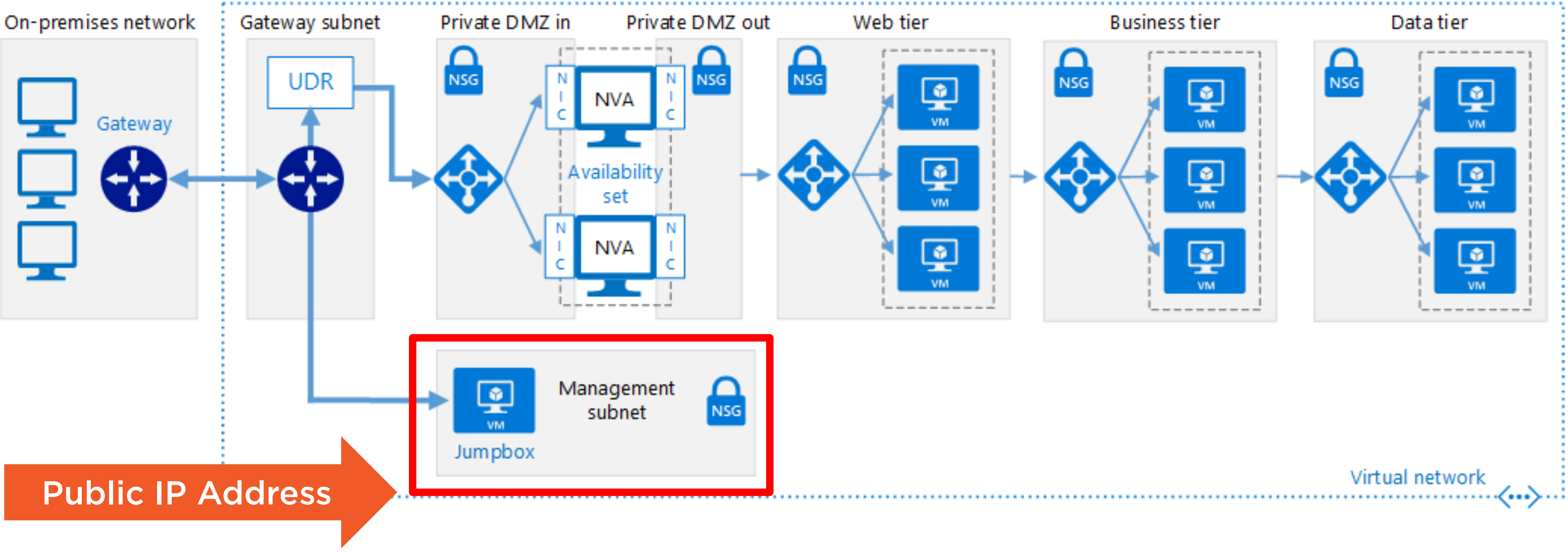
Define ASGs

Include ASGs in NSG rules

“Don’t forget about the host firewall!”

Tim’s consulting advice

Jumpbox Architecture



timw.info/arch

Demo

3

Create an ASG rule

Add the ASG rule to an NSG in the portal

Azure Security Center

Azure Security Center (ASC)

Centralized security policy management

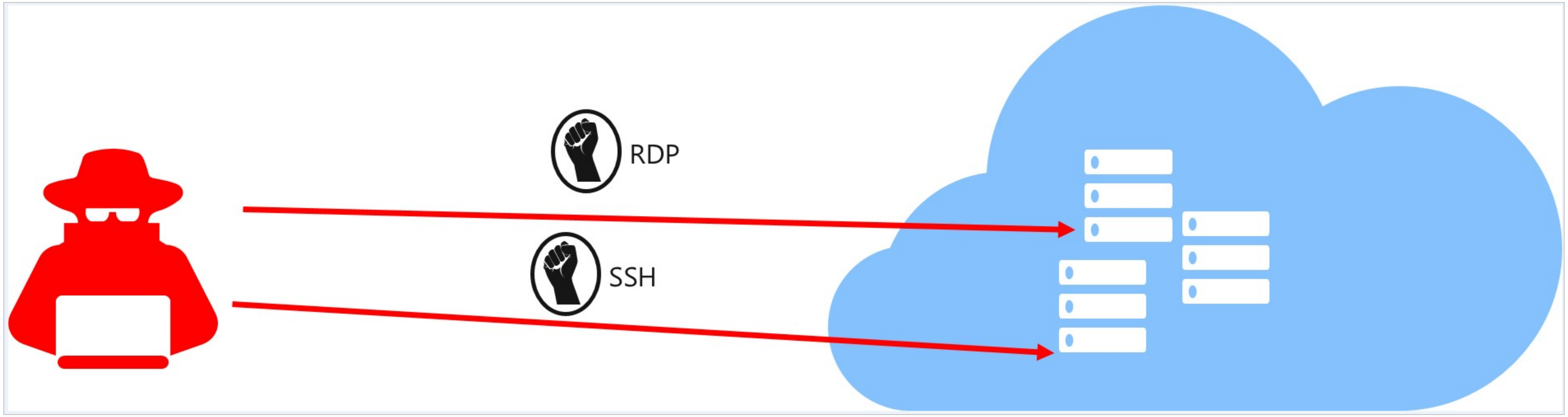
Continuous security assessment

Actionable recommendations

Prioritized alerts and incidents

Integrated security solutions

Just-in-Time (JIT) VM Access



Locks down inbound administrative port access

Time-restricted access to specific IP address(es)

Requires Azure Security Center Standard

Demo

4

JIT VM Access

Summary

Always keep least privilege foremost in mind

- In this respect, Azure and on-premises environments are exactly the same

Never forget the shared responsibility model in cloud computing

Thank you!

Twitter: @TechTrainerTim

Email: timothy-warner@pluralsight.com