

Azure Cloud Network Security Workshop



Learn how to design, deploy, and manage your organization's cloud network security through integration with industry leading NVAs.



Improve security for your Azure workloads with automated network security management and upgrades, and increase visibility into your environment



Help IT teams deliver network-related work more efficiently and with faster deployments



Implement infrastructure as code and incorporate security controls directly into application development workflows to accelerate development and time to market.

"The Total Economic ImpactTM of Microsoft Azure Network Security, a commissioned study conducted by Forrester Consulting, found that Azure network security reduces firewall management by 80 percent, security policy management by 15 percent, and security audit process by **96 percent."** -Forrester 2020 Microsoft 365 Enterprise Total Economic Impact Study

Whether you're moving workloads or modernizing apps on Azure, it's important to understand how security controls differ in cloud environments. This workshop will enable you to understand integration capabilities with industry-leading network virtual appliances such as Palo Alto, Check Point, and Fortinet..

Ensure your organization can meet and exceed threat inspection and prevention capabilities along your journey to the cloud.

EITS' Cloud Network Security Workshop gives IT professionals the opportunity to learn the best practices approach to deploying highly secure virtual environments through a hands-on real-time implementation.

Why you should attend

Our workshop provides everything you need set up, configure, and deploy secure virtual networks. Learn how to effectively configure policies, secure threat vectors, network virtual appliances, traffic profiles and more.



Get real-time security at enterprise scale

Dynamically scale your organization's cloud infrastructure as needed to meet traffic demands during peak times or seasonal spikes.



Detect and prevent threats quickly

Get more informative insights into the behavior of users, devices, resources and detects anomalies right away.



Achieve greater cloud security and capability

Get the guidance you need to effictively integrate Azure with leading security products like Palo Alto, Check Point, and Fortinet.



Workshop Phases and Activities

Kick-Off Meeting Pre-engagement call Introductions · Engagement walk-through · Engagement walk-through · Engagement tools Expectations Expectations · What's next · What's next Pre-Configuration Milestone · Policy Configuration Day 1 Day 2 **Days 3-5** Prerequisite Milestone Workshop questionnaire **Pre-Configuration Milestone** · Setup new or existing VNET · Fill in and return the questionnaire · Management and Services Configuration · Permissions and IP's provided in • Bootstrap Prerequisites (optional) Review Configure engagement tools customer environment Logging Configuration · Authentication Configuration · Hardening Configuration Implementation Milestone 2 Days 12-13 Day 11 **Pre-Configuration Milestone** Day 10 **Deployment Details for Azure Networking and Firewall Policies:** · Threat Configuration · Configuring Outbound and Implementation Milestone 1 Implementation Milestone 1.1 Pre-Deployment Milestone **East-West Traffic Profiles Deployment Details for VM-Series Deployment Details for VM-Series** · Create Basic Azure Firewall Configs Firewalls: Firewalls: Deploying VM-Series · Creating and Configuring Azure Common Resources for VM-Firewalls on Azure Series Firewalls Configuring Inbound Access Traffic Profile Days 15-16 Days 17-18 Days 19-22 (Public Load Balancer Option) Implementation Milestone 3 Implementation Milestone 3.1 Validation Milestone Deployment Details for a Backhaul · Configuring a Resilient Backhaul Connection · Validate Configuration







· Confirm VM-Series Threat Policy Enforcement

Connection:

for a Backhaul

Configuring Azure Networking

· Using Panorama to Configure Security and

NAT for Backhaul

Expand Azure's Capabilities Via NVA Integration

Feature	Azure Firewalls	NVAs
FQDN filtering (no SSL termination)	⊗	\otimes
Inbound/Outbound traffic filtering rules by IP address (source and destination), port, and protocol (5-tuple rules)	⊗	\otimes
Network Address Translation (SNAT+DNAT)	⊗	\otimes
Traffic filtering based on threat intelligence feed to identify high risk sources/destinations (e.g., C&C, botnet, etc.)	⊗	\otimes
Full logging including SIEM integration	\otimes	\otimes
HA with cloud scalability (auto scale as traffic grows)	\otimes	\otimes
Service Tags and FQDN Tags for easy policy management	⊗	\otimes
Integrated monitoring and management	\otimes	\otimes
Easy DevOps integration using REST/PS/CLI/Templates	⊘	Templates
SSL termination with Deep Packet Inspection (DPI) to identify known threats (e.g., viruses, spyware)	Private Preview Q3 CY2020	\otimes
Traffic filtering rules by target URI (full path - incl. SSL termination)	Private Preview Q3 CY2020	\otimes
Central management	Firewall Manager	\otimes
Application and user aware traffic filtering rules	Roadmap	\otimes
IPSEC and SSL VPN gateway	Azure VPN GW	\otimes
Advanced Next Generation Firewall features (e.g. Sandboxing)	Roadmap	Vendor Dependent



Industry Leading Integration Options









Why choose EITS?

A better approach to cloud security for the modern workplace

By leveraging industry-leading solutions, EITS assists its clients in developing comprehensive cyber security strategies. As a professional services organization, EITS focuses on maximizing customers' cyber security and technology investments. Second to none expertise in automating and integrating tailor-fit security solutions sets us apart from the competition.



Azure Cloud Platform Microsoft 365 Security Administration



