TECHNICAL PRESENTATION ON AZURE FIREWALL AND ANSIBLE

Exploring security automation and cloud firewall solutions

INTRODUCTION TO AZURE FIREWALL

Cloud-native Firewall

Azure Firewall provides stateful, cloud-native firewall protection for Azure Virtual Networks.

Integrated Monitoring

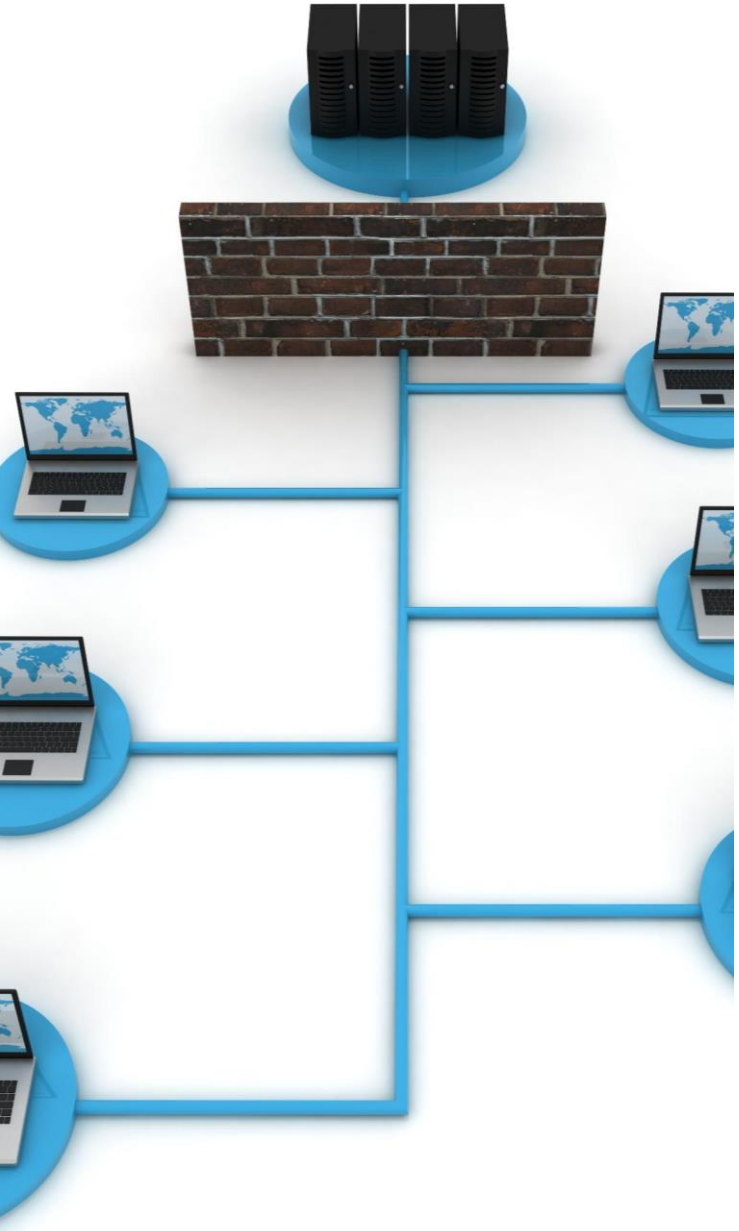
Fully integrated with Azure Monitor for logging and analytics to enhance security insights.

Comprehensive Traffic Control

Supports inbound and outbound filtering with centralized management via Azure Firewall Manager.

Advanced Security Features

Offers threat intelligence filtering, deep packet inspection, and logging for enterprise deployments.



AZURE FIREWALL CONFIGURATION & DEPLOYMENT

Deployment Methods

Azure Firewall can be deployed via Azure Portal, ARM templates, or automation tools like Terraform and Ansible.

Network Architecture

Typical setup includes Virtual Network, dedicated firewall subnets, and route tables directing traffic through the firewall.

Firewall Policies

Firewall policies offer centralized management, scalability, and advanced features compared to classic rules.

Monitoring & Logging

Integration with Azure Monitor and Log Analytics enables detailed traffic logging and security auditing.

ADVANCED FEATURES & REAL-WORLD SCENARIOS

Threat Intelligence Filtering

Blocks traffic from known malicious IPs using alert or deny modes for flexible threat management.

DNAT and SNAT Rules

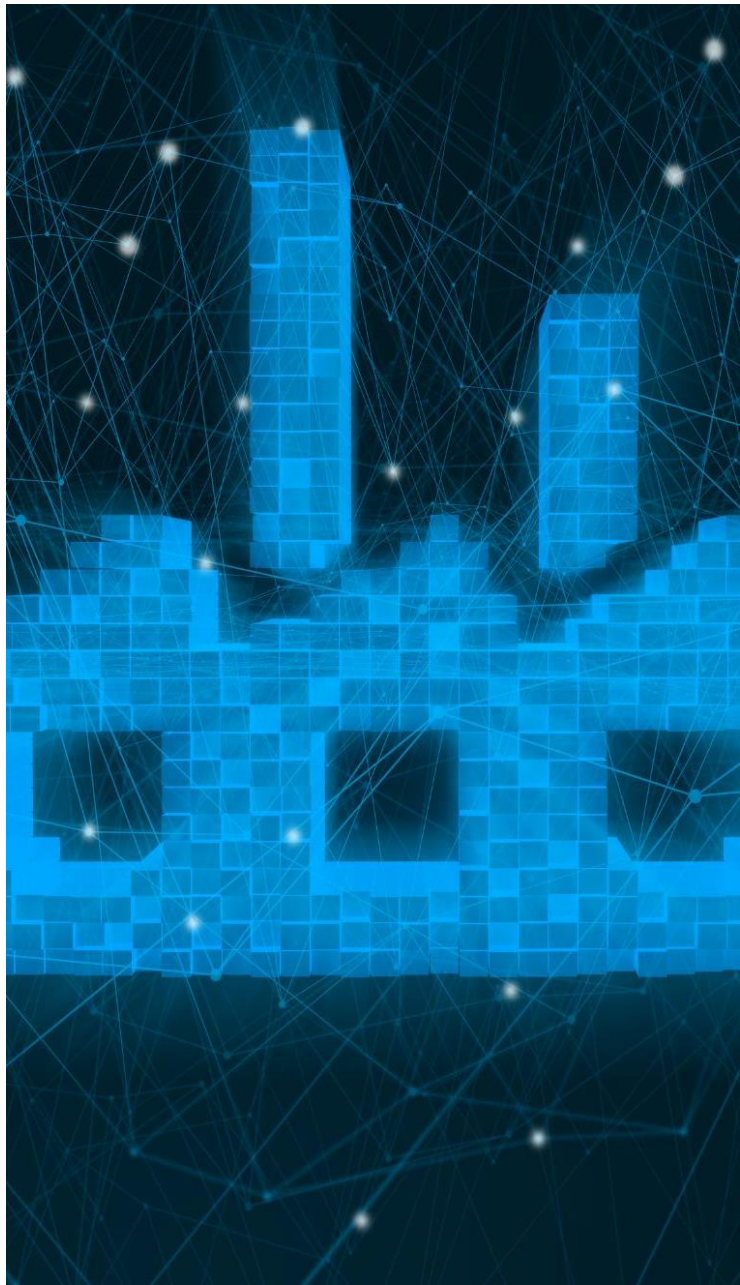
Manages traffic routing effectively with destination and source network address translation rules.

Application & Network Rules

Defines granular access controls based on protocols, ports, and IP addresses with prioritized rule collections.

Real-World Use Cases

Secures multi-tier web apps and hybrid environments controlling traffic between on-premises and cloud.



ANSIBLE

INTRODUCTION TO ANSIBLE

Open-source Automation Tool

Ansible is an open-source tool for automation, configuration, and deployment tasks.

Agentless Architecture

Ansible requires no agents installed on target machines, simplifying management.

YAML-based Playbooks

Uses easy-to-read YAML playbooks to define and automate tasks.

Core Components

Inventory, playbooks, modules, and roles organize and execute automation tasks.

ANSIBLE FOR AZURE AUTOMATION

Azure Resource Management

Ansible modules enable creating, updating, and deleting Azure resources efficiently.

Secure Authentication

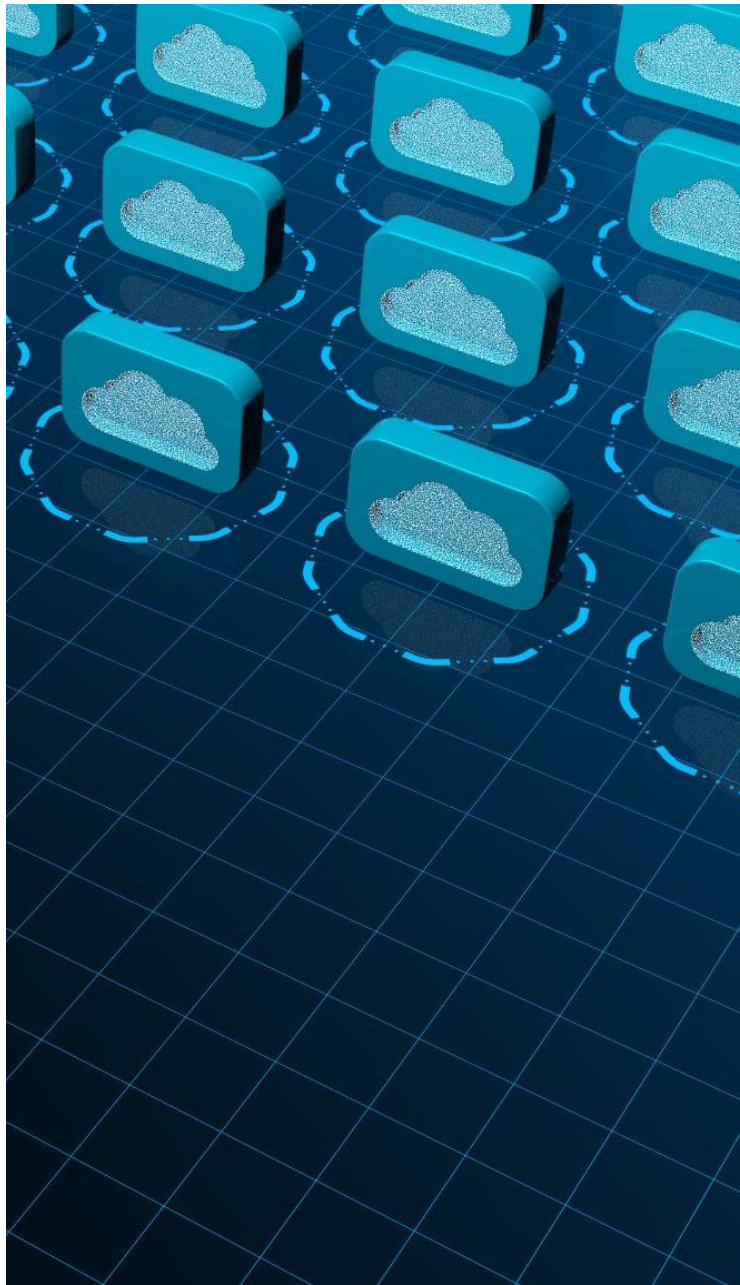
Service principals and managed identities ensure secure access to Azure APIs.

Playbook Automation

Playbooks define and automate desired Azure states, deployable manually or via CI/CD.

Dynamic Inventory

Dynamic inventory queries Azure for current resources, aiding in managing large environments.



INTEGRATING ANSIBLE WITH AZURE FIREWALL

Automation of Firewall Rules

Ansible automates deployment and management of Azure Firewall rules efficiently.

Use of Azure Modules

Ansible uses Azure modules to create and update firewall rule collections and policies.

Dynamic Inventory and Tagging

Resource tagging helps manage firewall rules applied to specific resource groups easily.

CI/CD Pipeline Integration

Playbooks integrate with CI/CD tools for automated, version-controlled firewall deployments.