AZ-700 Network Security Deep Dive

Mahdi Sheikhi

2025/08/05

CONTENTS

/ 01. NSG Foundations

/ 02. Flow Logging & Validation

/ 03. Bastion & Remote Access

/ 04. Virtual Network Manager

/ 05. Azure Firewall Design

/ 06. WAF on Front Door

CONTENTS

/ 01. WAF on Application Gateway

/ 02. Operational Excellence

NSG Foundations

01

NSG Purpose and Core Concepts

Stateful Distributed Firewall

NSGs intercept traffic at the NIC and subnet layers, tracking connection state to allow return packets automatically without explicit outbound rules, enabling micro-segmentation across every resource in your virtual network.

Rule Anatomy & Evaluation Order

Each rule is a 5-tuple of priority (100–4096), direction, protocol, port, and source/destination; lower numbers win, evaluation stops at first match, and hidden default rules 65000–65599 ensure baseline connectivity.

Default Rules You Cannot Delete

Priority 65000 allows VNet-to-VNet, 65001 allows load balancer health probes, 65500 denies all inbound Internet; understanding these defaults prevents accidental lockout while building least-privilege policies.

Creating and Associating NSGs

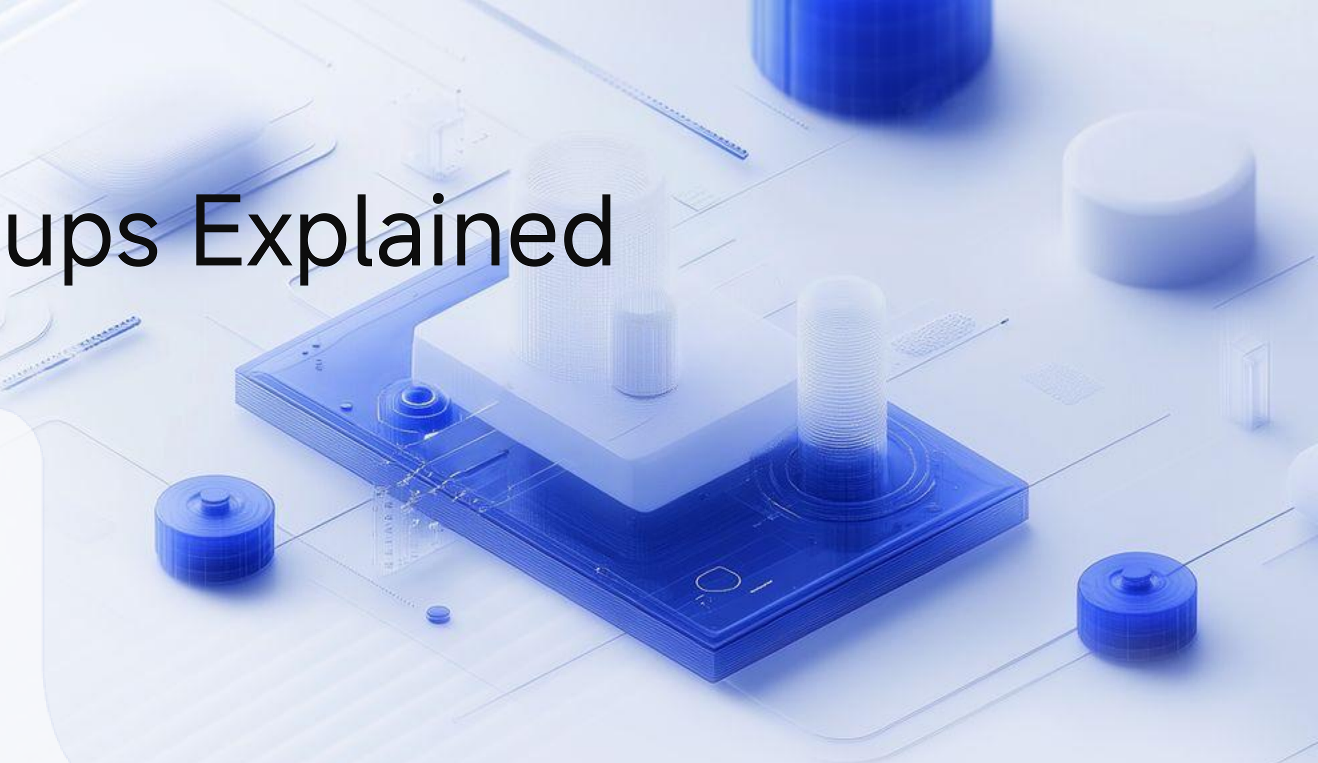
Portal, CLI & IaC Workflows

Use portal for quick demos, CLI ‘az network nsg create’ for scripts, and ARM/Bicep templates for repeatable landing zones; always output the resource ID for subsequent association commands to avoid manual clicks.

Subnet vs NIC Association Impact

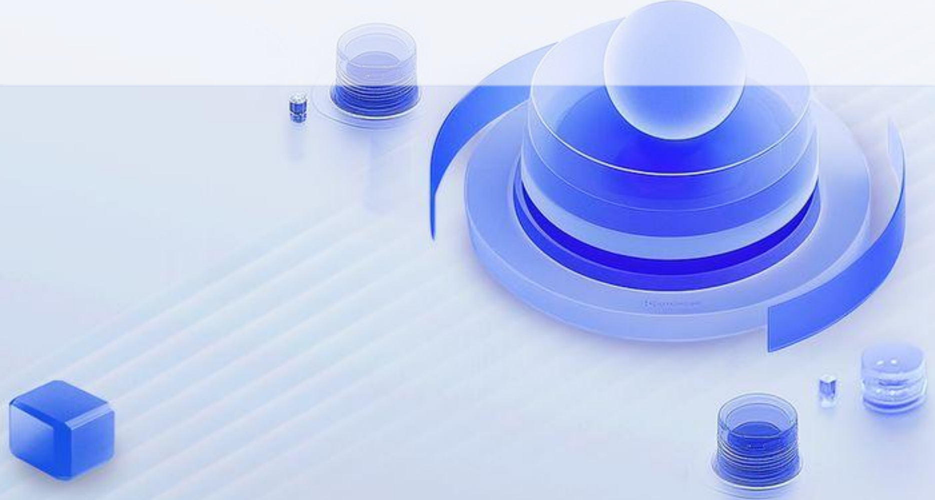
Subnet-level NSG protects all new NICs automatically, while NIC-level enables per-application rules; traffic is evaluated twice—first subnet, then NIC—so plan priorities carefully to avoid unintended denies.

Application Security Groups Explained



Tag NICs, Not IPs

ASGs abstract VMs into roles like ‘WebTier’; when you scale out, new instances inherit rules instantly, eliminating subnet renumbering and reducing rule sprawl from dozens of IP prefixes to a single tag.



Cross-Subnet Flexibility with Limits

Members can live in any subnet of the same VNet, but ASGs cannot span peered networks; each NSG supports up to 100 ASG references, so design hierarchies like ‘App-Prod’ vs ‘App-Test’ to stay within quotas.

Authoring Effective Security Rules

Priority Uniqueness & Overlap Guardrails

Duplicate priorities abort deployments; adopt a naming convention like 1xx for infrastructure, 2xx for applications, leaving gaps for future inserts to minimize renumbering during production changes.

Wildcard Port Pitfalls

Allowing ‘*’ ports exposes ephemeral ranges; restrict to 443, 80, or application-specific ports, and pair with destination ASG to limit blast radius even if the port list changes later.

Service Tags vs CIDR Trade-offs

Use tags such as ‘Storage.EastUS’ to auto-update IP ranges instead of maintaining 50+ prefixes yourself; fall back to CIDR only for on-prem ranges that lack published tags.

RDP Lockdown Template

Create priority 100 rule denying 3389 from Internet, then priority 110 allowing 3389 from ‘BastionSubnet’ ASG; this pattern is repeatable for SSH and SQL, forming a security baseline across every landing zone.

Flow Logging & Validation

02

Enable Virtual Network Flow Logs

01

Network Watcher Prerequisites

Flow logs require a regional Network Watcher auto-enabled in every subscription; verify its presence before deployment, and store logs in a geo-redundant storage account with lifecycle management to archive after 30 days for cost control.

02

Log Analytics Integration

Enable the ‘Send to Log Analytics’ flag to query flows with KQL, build workbooks, and set alerts on suspicious IPs; choose the Network Security Group analytics solution to auto-create dashboards without manual schema mapping.

Decode NSG Flow Log Format

1

Tuple Breakdown in JSON

Each record contains MAC, source/destination IPs, source/destination ports, protocol (TCP=6, UDP=17), direction (I= inbound, O= outbound), and decision (A=allow, D=deny), enabling precise mapping to the rule that triggered the action.

2

Version 2 Schema Benefits

Version 2 adds flow state ('B' begin, 'C' continue, 'E' end) and packet/byte counters, allowing bandwidth calculations and connection duration metrics that feed into cost attribution dashboards.

3

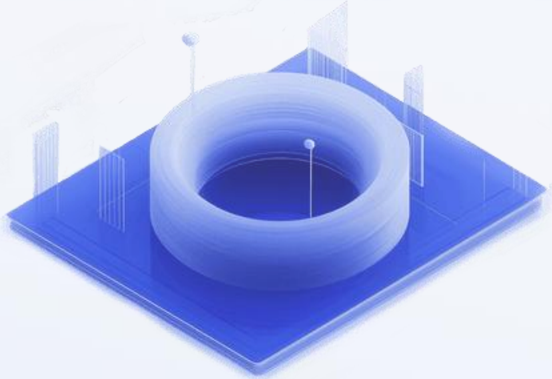
Correlating Priority to Rule

The 'flowRule' field stores the exact priority number; cross-reference with NSG rules to confirm whether traffic hit your intended allow or an unexpected deny, accelerating troubleshooting during incidents.

Validate Rules with IP Flow Verify

Simulate Packets Without Traffic

Network Watcher IP-flow-verify tests a hypothetical 5-tuple against effective NSG rules, returning allow/deny along with the matched priority; perfect for pre-production validation when change windows prohibit real packet injection.



CLI Example & Interpretation

Run ‘az network watcher test-ip-flow’ with VM ID, direction, protocol, port, and remote IP; if result shows deny at priority 1000, you instantly know the rule to adjust, eliminating guesswork and reducing mean time to remediate.

Troubleshoot with Flow Insights

Traffic Analytics Visualizations

Traffic Analytics aggregates flow logs into geo maps, malicious IP feeds, and top talker charts; use the 60-minute latency dataset to spot lateral movement, export to Power BI for executives, and trigger Sentinel playbooks on anomaly scores.

Bastion & Remote Access

03

Hardening RDP SSH with Bastion

1

Subnet & IP Requirements

Deploy Bastion into a dedicated subnet named ‘AzureBastionSubnet’ with /26 or larger to support 50+ concurrent sessions; assign a static public IP with standard SKU and zone redundancy to maintain connectivity during updates.

2

Native Client vs Portal Modes

Enable native client support to SSH directly from local terminal via ‘az network bastion ssh’, avoiding copy-paste limits of browser; session logs still stream to diag storage for audit regardless of access method.

3

Scaling & Cost Controls

Standard SKU autoscales instances every 10 sessions; use Developer SKU in dev/test to cut cost by 70%, but note the 2-session limit and lack of upload/download features, suitable only for transient administrative tasks.

NSG Rules for Bastion Scenarios

01

Inbound Rules on Target VMs

Allow 3389/22 only from ‘AzureBastionSubnet’ ASG at priority 100, then deny all management ports from VirtualNetwork and Internet at priority 200, ensuring that even peered networks cannot reach RDP directly.

02

Outbound Rules for Bastion Host

Bastion needs 443 to Azure API, 80 to CRL servers, and 16863 for KMS; create an outbound rule with service tag ‘AzureCloud’ to prevent accidental denies that break clipboard, file upload, and session logging functions.

Virtual Network Manager

04

Network Manager Global Controls

1

Scope-Based Management Groups

Assign Network Manager at the tenant or management-group level to enforce security rules across hundreds of subscriptions; dynamic membership via Azure Policy ensures new landing zones inherit compliance without manual onboarding.

2

RBAC Separation of Duties

Security admins own security admin rules, while vNet operators cannot override; this split prevents workload teams from relaxing corporate egress blocks, maintaining governance without slowing down development sprints.

Security Admin Rules in Action

01

Override Regular NSGs

Create a deny-all-inbound rule at priority 1 scoped to a regional network group; during incident response, toggle from ‘Audit’ to ‘Enable’ to instantly isolate compromised VNets without touching individual NSGs.

02

Emergency Isolation Pattern

Security admin rules with priority 1–99 execute before any customer NSG rule, making them ideal for global blocks like SMB outbound or TCP 25 egress that must never be relaxed by application teams.

03

Immutable Governance Layer

Because workload owners cannot edit admin rules, you guarantee baseline protection; combine with Azure Policy to audit that every subscription is assigned to the corporate network manager, closing governance gaps.

Deploying Configurations Safely

Audit Before Enforce

Stage configurations in audit mode for 48 hours; Resource Graph queries show which VNets would be impacted, allowing you to refine rules and avoid production outages caused by overly broad deny statements.

Rollback & Versioning

Every configuration deployment creates a new version; if a rule breaks connectivity, redeploy the previous version via portal or REST, achieving near-instant rollback without waiting for change-window approvals.

Azure Firewall Design

05

Firewall Feature Map to Needs

1

Layer 3–7 Inspection in One Service

Azure Firewall filters on IP, port, and FQDN while optional Premium SKU adds TLS inspection and IDPS, consolidating multiple security appliances into a single horizontally scaled service managed through ARM templates.

2

Threat Intel & FQDN Filtering

Built-in Microsoft Threat Intelligence alerts or blocks known malicious IPs and domains; FQDN tags like 'WindowsUpdate' auto-maintain endpoints, eliminating manual whitelist updates across dozens of applications.

3

Compare with NVAs for TCO

No VM patching, built-in HA, and pay-per-GB processing reduce OPEX; at 9 Gbps sustained, Firewall Premium costs 30% less than equivalent third-party NVAs plus virtual machine scale-set overhead.

SKU Selection Criteria

1

Standard vs Premium Differentiators

Premium adds TLS inspection, IDPS signatures, web categories, and 30 Gbps sustained throughput with availability zones; choose Premium for PCI workloads needing outbound SSL decryption, otherwise Standard suffices for most hub-spoke designs.

2

Dev/Test with Basic SKU

Basic offers 250 Mbps and costs 70% less, ideal for sandbox environments; note the lack of threat intel and forced-tunneling support, and remember to resize before production promotion to avoid re-IPing the management subnet.

Hub-Spoke Reference Architecture

Dedicated Firewall Subnet

Create ‘AzureFirewallSubnet’ with /26 minimum to accommodate future scale; never peer this subnet to other VNets to prevent asymmetric routing and ensure all traffic passes through the firewall’s transparent proxy.

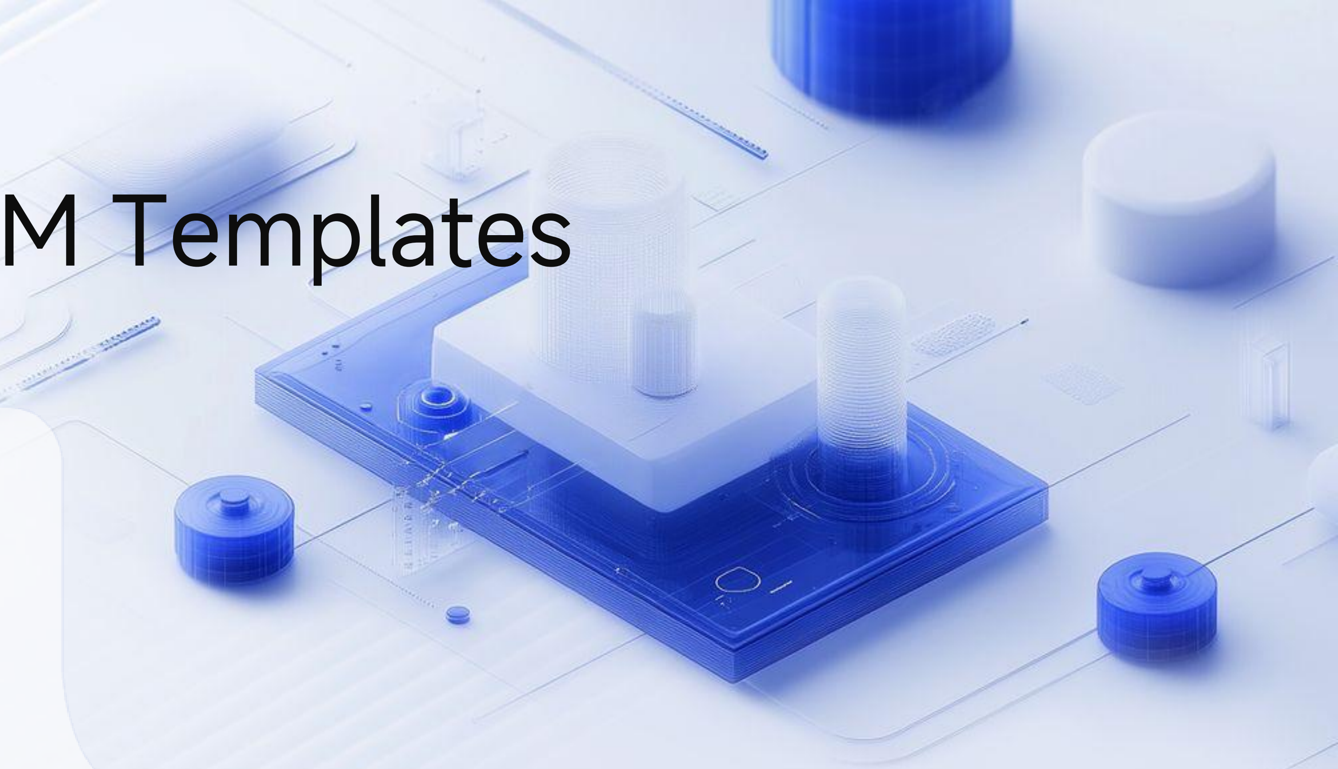
UDR 0.0.0.0/0 via Firewall

Add a user-defined route in each spoke pointing default traffic to the firewall’s private IP; disable BGP route propagation on the route table to stop on-prem routes from bypassing inspection.

Forced Tunneling Caveats

When redirecting outbound Internet to on-prem, set a /0 route in the FirewallSubnet pointing to your NVA; ensure the on-prem device returns traffic through the same path to avoid asynchronous flows that break TLS sessions.

Deploy Firewall with ARM Templates



Template Dependencies Order

Deploy public IP first with zone-redundant standard SKU, then subnet with delegation 'Microsoft.Network/azureFirewalls', finally the firewall resource referencing both; any reorder causes validation failures and wasted pipeline runs.

Enable DNS Proxy & Threat Intel

Set 'enableDnsProxy' to true so spokes can use firewall as DNS resolver, logging every FQDN request; enable 'alert' mode for threat intel during rollout to monitor without blocking, then switch to 'deny' after baselining.

Authoring NAT, App, and Network Rules

Rule Collection Priority Order

DNAT collections evaluate first, then Network, then Application; place inbound SMTP redirection in DNAT with priority 100, followed by Network rules for IP-based filters, and finally FQDN-based Application rules for outbound web traffic.

Non-overlapping SNAT Pools

Each rule collection must reference unique source NAT address ranges to prevent port conflicts; document your 10.100.0.0/24 pool assignments in a shared spreadsheet to avoid collisions when multiple teams deploy rules.

Wildcard Domain Gotchas

CDNs like '*.azureedge.net' rotate backend IPs hourly; instead of whitelisting wildcards, use FQDN tags 'AzureFrontDoor.Backend' to leverage Microsoft-maintained lists, ensuring your app stays online during edge re-mappings.

Firewall Manager Policy Hierarchy

01

Global → Regional → Local Inheritance

Place corporate-wide blocks like TCP 25 in a global policy, regional compliance rules in regional policies, and application-specific FQDNs in local policies; lower levels can override upper levels, providing flexibility without duplicating baseline rules.

02

Draft & Staging Workflow

Save rule changes as drafts, attach to a test firewall policy, and validate with 'what-if' deployments; once traffic logs confirm no breakage, commit the draft to production hubs during maintenance windows with zero downtime.

Secure VWAN Hub with Firewall

Routing Intent Steering

Enable routing intent to automatically inject a /0 route into branch and VNet connections, forcing Internet and private traffic through the firewall; BGP propagates this route to on-prem routers, maintaining consistent security posture across hybrid paths.

Scaling Limits & Cost

Each secure VWAN hub scales up to 50 Gbps aggregate; deploy multiple hubs in larger regions and use hub-to-hub transitive peering to distribute load, monitoring throughput with Azure Monitor metrics to trigger hub sprawl before saturation.

WAF on Front Door

06

WAF Capabilities on Front Door

1

Global Edge Protection

WAF inspects HTTP(S) at every Front Door POP worldwide, blocking OWASP top 10, botnets, and geo-unwanted traffic within 15 seconds of policy update, ensuring consistent defense no matter which edge serves your users.

2

Custom Rules with Server Variables

Write rules using variables like ‘SocketAddr’ and ‘RequestUri’ to block requests older than 30 seconds or containing specific headers; regex transforms like tolower() prevent bypasses via case variation.

3

Rate Limiting by Client Fingerprint

Configure threshold 200 requests per minute per IP or per header value; when exceeded, Front Door returns 429, protecting your origins from credential-stuffing attacks without adding latency to legitimate users.

Design Custom Rule Sets

01

Priority & Match Conditions

Set priority 1 for emergency blocks, 10 for geo filters, 50 for rate limits; use multiple match conditions with AND/OR logic to fine-tune, and enable ‘stop processing’ to skip lower rules for performance.

02

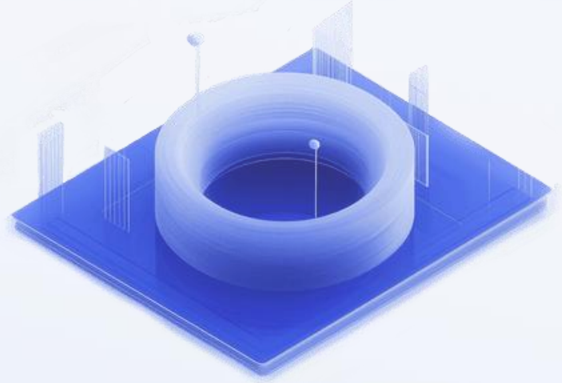
Testing with Detection Mode

Run new rules in detection for 24 hours, query Log Analytics for triggered requests, tune false positives, then switch to prevention; this cycle prevents legitimate traffic loss during iterative hardening.

Enable Detection vs Prevention

Detection Logs for Baselining

In detection mode, WAF logs every matched rule but forwards traffic to origin; analyze the logs to identify legitimate API calls caught by OWASP 942100, then craft exclusions before enabling prevention.



Prevention Mode Enforcement

Once baselined, switch to prevention to block attacks; configure Azure Monitor alerts on blocked request count spikes, and integrate with Sentinel to auto-create incidents when SQLi rules fire repeatedly.

Associate WAF Policy to AFD Endpoint

Route-Level Assignment

Link the WAF policy to the routing rule, not the domain, enabling granular protection per origin group; propagation finishes within 15 seconds globally, so you can stage changes in blue-green deployments without DNS swaps.

WAF on Application Gateway

07

WAF Deployment Modes for Gateway

01

WAF_v2 SKU Autoscaling

Unlike Front Door, App Gateway is regional; place it in the same region as your backends to avoid cross-region latency, and pair with Front Door for global edge protection while App Gateway handles fine-grained CRS tuning.

02

Regional vs Global Placement

Application Gateway v2 with WAF scales from 0 to 40 instances in 2 minutes, supporting 4 Gbps per instance; deploy into dedicated subnet /24 to leave headroom for burst traffic during flash sales or patching events.

03

CRS 3.2 Parity

Both WAF offerings run OWASP CRS 3.2, so rule IDs are consistent; you can export exclusions from App Gateway and reuse them in Front Door policies, reducing dual-maintenance overhead for hybrid architectures.

Tune OWASP Rule Groups

Disable Noisy Rules Selectively

Rule 942450 flags SQL comments in marketing campaign URLs; disable it at the rule group level, but retain 942100-942499 for true SQLi, balancing security with business functionality without blanket disabling the entire group.

Anomaly Score Thresholds

Lower the anomaly score limit from 5 to 3 for payment endpoints, so multiple low-severity rules collectively block requests; keep score 5 for static assets to avoid false positives on legitimate query strings.

Exclusions and False Positive Handling

1

Request Attribute Selectors

Choose ‘RequestHeaderNames’, ‘RequestCookieNames’, or ‘QueryStringArgNames’ to exclude specific fields like ‘utm_source’ that trigger CRS 942440; use exact match instead of contains to minimize attack surface while fixing the false positive.

2

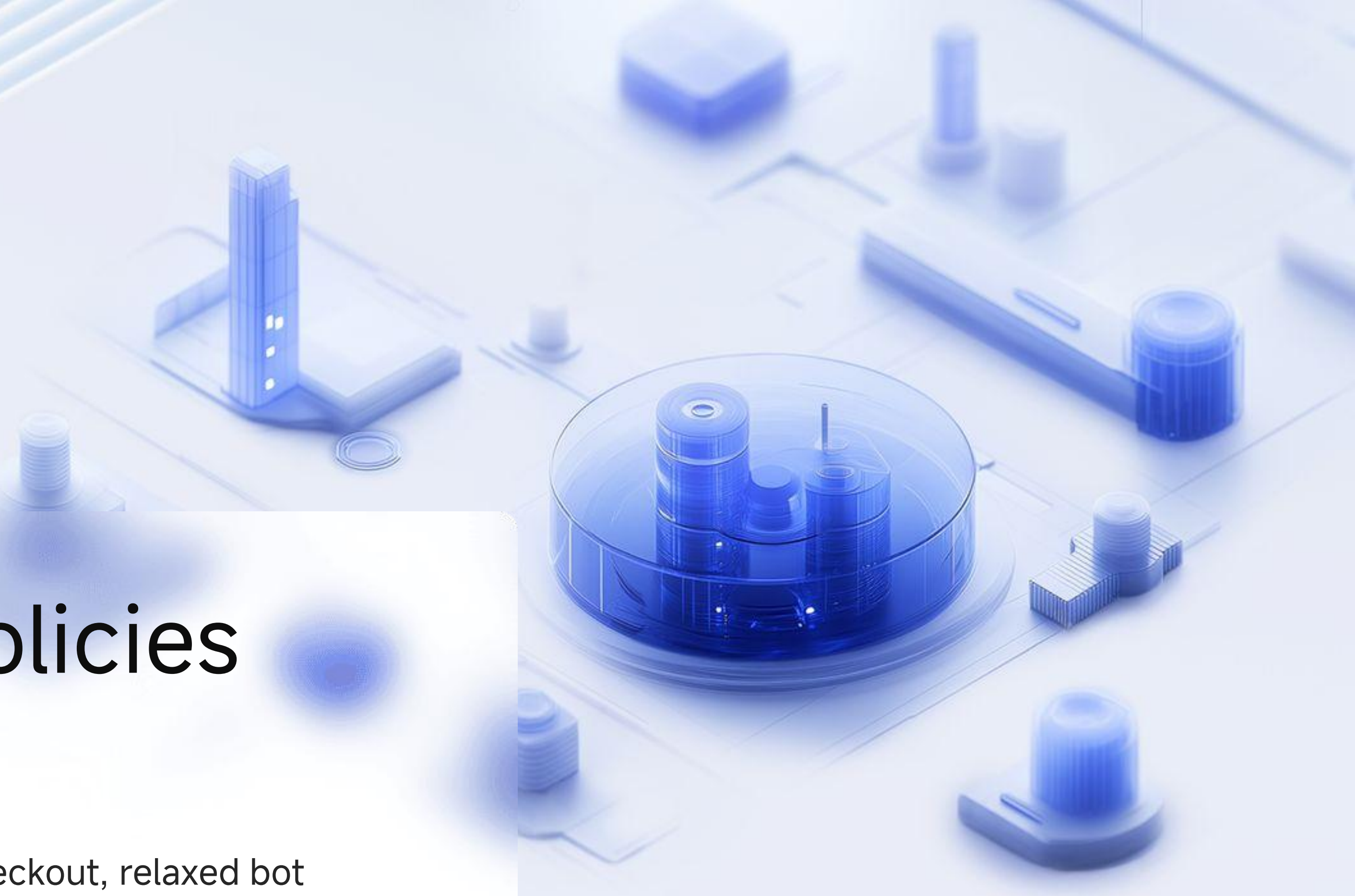
Logging Before Excluding

Query WAF logs for top 10 triggered rules over 7 days, filter by request URI, then add exclusions only where legitimate traffic exceeds 1% of total; this data-driven approach prevents over-permissive rules that could mask real attacks.

Apply Per-Site WAF Policies

Listener-Level Policy Scope

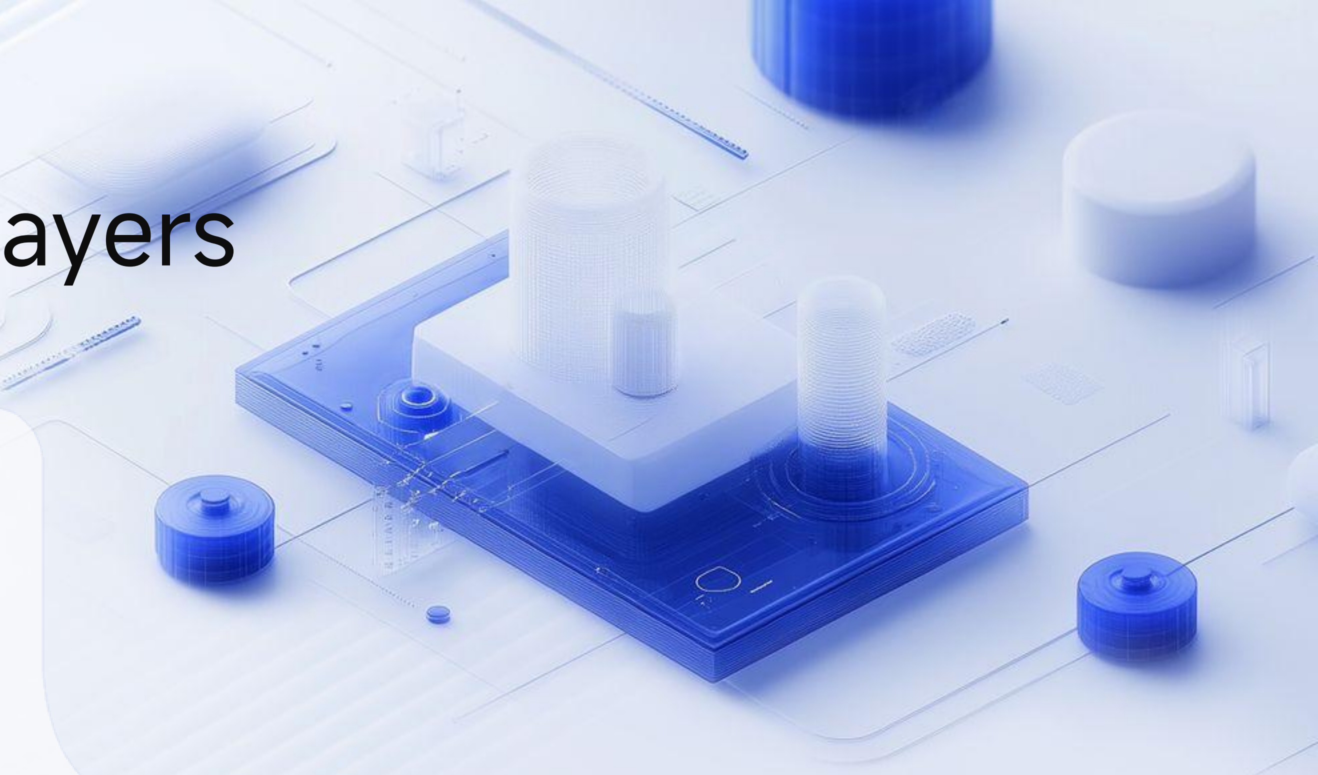
Attach distinct policies to each listener: strict CRS for /checkout, relaxed bot protection for /blog; this granularity lets marketing deploy campaigns without waiting for security to lower global paranoia levels, all within one gateway.



Operational Excellence

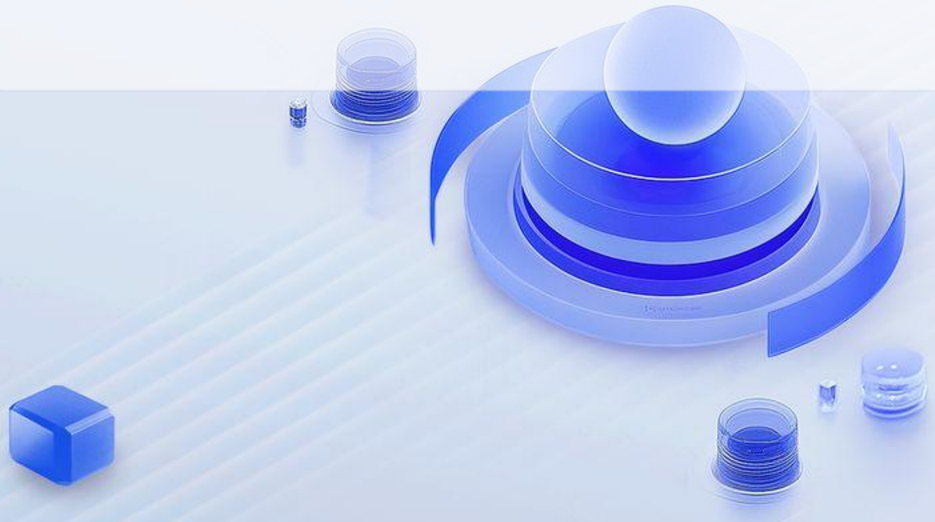
08

Monitoring All Firewall Layers



Single Log Analytics Workspace

Ingest NSG, Azure Firewall, and WAF logs into one workspace; use cross-resource KQL to trace a client IP from edge block to firewall deny to NSG drop, correlating incidents into a single timeline for SOC analysts.



Sample KQL for Port Scan

Use query ‘where DestinationPort in (22,3389,445) and Decision=="D" | summarize Count=count() by SourceIP | where Count > 50’ to detect scanners, then feed results to Sentinel watchlist for automated threat-hunting playbooks.

Backup and Disaster Recovery

01

Policy JSON Export Pipeline

Schedule nightly export of Firewall and WAF policies to an Azure DevOps repo; on region failure, redeploy templates into paired region and re-associate policies to new hubs, achieving recovery time under 30 minutes.

02

Flow Log Retention Strategy

Store logs in GRS storage with 31-day cooling to Cool tier, then move to Archive for 365 days; automate lifecycle policies so compliance data remains searchable without paying Hot-tier prices for aging telemetry.

Cost Optimization Checklist

1

Right-Size Firewall SKU

Run Basic SKU in dev/test at 250 Mbps, scale to Standard for 9 Gbps prod, and only enable Premium when you need TLS inspection; this tiering saves 60% on monthly burn while meeting compliance requirements stage-by-stage.

2

Compress & Tier Flow Logs

Enable GRS write-once, then set lifecycle policy to Cool after 30 days and Archive after 90; compression reduces size by 70%, cutting storage cost from $0.0208/GB to $0.002/GB for year-old forensics.

3

Consolidate WAF Edges

Use Front Door WAF for global sites instead of regional Application Gateway WAFs; one policy covers all edges, eliminating duplicate rules and reducing total cost from $0.18 per million requests across 5 regions to a single fee.

Governance with Azure Policy

01

Built-In Initiative for NSG

Assign policy 'Network interfaces should be associated with a network security group' with deny effect; combine with 'Audit' for WAF mandatory on public IPs, ensuring every new workload inherits security baseline at deployment.

02

Auto-Remediate with Logic Apps

When policy detects missing NSG, Logic App triggers, looks up template, creates NSG with baseline rules, and tags resource for cost center; this closes the gap within minutes while notifying owners via Teams adaptive card.

Troubleshooting Toolkit

1

Connectivity Check Path

Start with Network Watcher connectivity verify to confirm VM can reach gateway, then IP-flow-verify to validate NSG rules, finally packet capture if packets drop silently; this three-step flow reduces MTTR by 50% during outages.

2

502 Gateway Timeout Drill

Check Application Gateway health probes first, then WAF exclusion logs for SQLi false positives blocking login POST, lastly verify backend SNAT port exhaustion; each layer has distinct log streams, so follow the decision tree to avoid rabbit holes.

3

SNAT Port Exhaustion Alert

Monitor metric 'SNAT ports usage' on Firewall; when above 90%, add additional public IPs or enable forced tunneling to offload Internet traffic, preventing outbound connection failures that manifest as intermittent 500 errors.

Exam Re-cap and Tips

Key Differentiators to Memorize

NSG is stateful layer 4, ASG is logical tagging, Azure Firewall is layer 3-7 with threat intel, Front Door WAF is global edge, App Gateway WAF is regional; mixing their scopes is a common exam trap—match requirement to service correctly.

24-Hour Cram Checklist

Lab each scenario once: create NSG with ASG, enable flow logs, deploy Firewall Manager policy, tune WAF exclusion; finish with practice test scoring >85%; sleep early—hands-on muscle memory beats last-minute flashcards on exam day.

THANK YOU FOR READING！

Mahdi Sheikhi

2025/08/05