

Azure Network Security

Binal Shah Principal Cloud Solution Architect <u>binal.shah@microsoft.com</u>

Zero Trust Network Security Maturity Model



Protection services enabling zero trust



Azure network security

Layered defense approach with cloud native services

- 👌 A Zero Trust approach
- Stop attacks at Network edge
- Use virtual network for network segmentation
- Control routing behavior
- Use Service Endpoints to restrict access to PaaS resources
- Use Private Link to enable private access to your PaaS services
- Use Private Link Service to provide private access to your provider service



Network Security Group

Protects workloads with distributed ACLs

Applied on subnets or NICs

Supports application security groups to enable micro-segmentation

Supports service tags for Azure service IP addresses



Action	Name	Source	Destination	Port
Allow	Webrule	Internet	10.1.1.0/24	443
Allow	Webtoapp	web	арр	80
Deny	DenyAll	Any	Any	Any

Network Security Group

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	•••
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalan	Any	Allow	•••
65500	DenyAllInBound	Any	Any	Any	Any	😣 Deny	•••

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	•••
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	•••
65500	DenyAllOutBound	Any	Any	Any	Any	😣 Deny	•••



Azure Private Link

Access to Azure PaaS services

PaaS service ranges are public IP ranges

Workloads need a public IP address to reach the services.

Firewall needs rules to allow this traffic.



Private Link

Private connectivity to your **specific PaaS resource**

Traffic stays on Microsoft backbone

No firewall rules for public IP ranges

Private access from on-premises

Private access across vnet peers

Data exfiltration protection



Private Endpoint: DNS Integration

Using Custom DNS on Azure Using Private Zone DNS Resolving on Custom DNS on Azure with \checkmark Same connection URL, no change required on Applications \checkmark conditional forwarding for Azure DNS Easy to configure DNS server to resolve from VNet Integrate Private Zone DNS with private \checkmark Internet remains resolving to Public IP address \checkmark record for VNet Resolve from on premises using same \checkmark Custom DNS DNS Private Zone DNS Azure DNS Domain: privatelink.service.windows.net A: myresource -> 10.1.1.20 **DNS Conditional Forwarders On premises Clients** service.windows.net -> Azure DNS name servers Ŷ **Custom DNS** VNet 192.168.1.0/24 10.1.1.20

Private Link Service

Application running behind Standard Load Balancer

Private Link Service tied to Frontend IP configuration of Standard Load Balancer

Frontend IP Configuration can be either Public or Private



Private Link Service





5

DNS





Azure Firewall

Azure Firewall

 Secures digital assets using cloud-native firewall capabilities with built-in high availability, auto-scalability, and zero maintenance.

• Key Benefits

- Network and Application traffic filtering
- Built-in Threat intelligence
- Deploys and scale in minutes
- Supports E-W and N-S traffic filtering

Supported SKUs

- Basic SKU for SMB segment (preview)
- Standard SKU for enterprise & government organizations
- Premium SKU for high-security environments



Our History



Azure Firewall

Secures digital assets using cloud-native firewall capabilities with built-in high availability, auto-scalability, and zero maintenance.

Key Benefits

- Network and Application traffic filtering
- Built-in Threat intelligence
- Deploys and scale in minutes
- Supports E-W and N-S traffic filtering

Supported SKUs

- Basic SKU for SMB segment (Public Preview)
- Standard SKU for enterprise & government organizations
- Premium SKU for high-security environments



Our History



Firewall Use Cases

VNET deployment

- Firewall is in a Hub VNET.
- Secure traffic between spoke VNETs, subnets within VNETs and traffic to the internet.
- Optionally secure traffic to Branch offices via ER/VPN Gateway.

Virtual WAN (aka Secure Hub)

- Firewall is inside a Virtual WAN hub.
- Secure traffic between VNETs, Branch offices and cross hub.
- Automate route configuration to easily attract traffic to the firewall.

Forced Tunnel mode

- Internet breakout is via a 3rd party firewall deployed on-premise or elsewhere.
- Forced tunnel to on-premise firewalls is supported in VNET environments. Virtual WAN environments supports 3P security partner provider for breakout to the internet via CheckPoint & ZScaler.



Azure Firewall Basic

Enterprise-grade security for small and medium businesses

Comprehensive, cloud-native network firewall security

- Network and application traffic filtering
- Threat intelligence to alert on malicious traffic
- Built-in high availability
- Seamless integration with other Azure security services

Simple setup and easy-to-use

- Setup in just a few minutes
- Automate deployment (deploy as code)
- Zero maintenance with automatic updates
- Central management via Azure Firewall Manager

Cost-effective

Designed to deliver essential protection at a price point that meets your needs



Azure Firewall Standard

Cloud native stateful Firewall as a service

A first among public cloud providers

Central governance of all traffic flows

- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection

Filter Outbound, Inbound, Spoke-Spoke and Hybrid Connections traffic (VPN and ExpressRoute)

Centralized logging

Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice.

Best for Azure

DevOps integration, integration with Sentinel and ASC, FQDN Tags, Service Tags, Integration with ASE, Backup and other Azure services.

Includes Basic SKU capabilities DNS Proxy + Custom DNS Web content filtering (web categories) Spoke 1 zure Firewall Sta Threat intel, NAT, network and application traffic filtering rules allows inbound/ outbound access Spoke 2 **Azure Firewall** Traffic is denied bv default **Central VNet** Azure to on- 🔨 prem traffic filtering **Spoke VNets On-premises**

Azure Firewall Premium

Cloud native Next-Gen Firewall as a service

TLS Inspection

- Built-in TLS Inspection for Outbound and East-West traffic
- Inbound TLS termination is supported with Azure Application Gateway
- Customer provided key pair via Azure Key Vault integration

Intrusion Detection Prevention System (IDPS)

- Detect alert and block inbound/outbound malicious traffic
- Supported for both encrypted and plain text protocols
- Signature-based detection that is continuously updated

URL Filtering

- Restrict user access to HTTP/HTTPS Web content
- Support for URL wildcards

Web Categories

- Allow or deny user access to website categories such as gambling, social media and others
- Web categories maintained and continuously updated
- URL based category matching

Azure Firewall Standard

Including all standard firewall capabilities





On-premises

Feature Category	Feature	Firewall Basic Public Preview	Firewall Standard	Firewall Premium
	Application level FQDN filtering (SNI based) for HTTPS/SQL		\checkmark	\checkmark
	Network level FQDN filtering – all ports and protocols		\checkmark	\bigcirc
L3-L7 Filtering	Stateful firewall (5 tuple rules)		\checkmark	
	Network Address Translation (SNAT+DNAT)		\checkmark	
	Availability zones		\checkmark	\checkmark
	Built-in HA		\checkmark	
Reliability & Performance	Cloud scalability (auto-scale as traffic grows)	Up to 250 Mbps	Up to 30 Gbps	Up to 100 Gbps
	Fat Flow support	N/A	1 Gbps	10 Gbps
Face of Management	Central management via Firewall Manager		\checkmark	
Ease of Management	Policy Analytics (Rule Management over time)			
	Full logging including SIEM integration			
	Service Tags and FQDN Tags for easy policy management			
Enterprise Integration	Easy DevOps integration using REST/PS/CLI/Templates/ Terraform		V	
	Web content filtering (web categories)		V	
	DNS Proxy + Custom DNS			
	Threat intelligence-based filtering (known malicious IP address/ domains)	Alert	\checkmark	\checkmark
	Inbound TLS termination (TLS reverse proxy)			Using App GW
Advanced Threat Protection	Outbound TLS termination (TLS forward proxy)			
	Fully managed IDPS			
	URL filtering (full path - incl. SSL termination)			

Azure Firewall

Rules Processing Logic

Threat Intelligence

NAT Rules

Network Rules

Application Rules



Policy Analytics (preview)

Manage Azure Firewall rules over time

Policy Insights

 Highlights key information of the Firewall policy such as Policy limits, Duplicate rules, Wildcard in rules and more.

Policy Recommendations

 Recommendations to improve the Rules in the policy including rules with low/no hits, overly permissive rules, potentially malicious sources.

Rule Analytics

- Visibility into the traffic flows of the rules over time
- Rule hit count for Application, Network and DNAT rules

Single Rule Analysis

- Refine the rules permissions
- Inspect the flows hit per a specific rule

nsignts Rules Flows								
Configure workspaces 💍 Refi	resh 📋 See all recommenda	tions						
Policy limits		Rules with multiple IP ac	ddresses 🕕	₽.	Rules w	vith low utiliza	ation ①	ŧ
2,468 Rules	7000 Max	37 Source IPs > 10		2,468 Total	37 oh	its (all matching	g flows)	2,468 To
6,507 Unique sources	10,000 Max	349 Destination IPs > 10		2,468 Total	863 0	hits (> 20% of	matching flows)	2,468 To
9 629 Unique destinations	10.000 May							
5,025 Onque destinations	10,000 Max							
		See recomm	nendations			See reco	ommendations	
Insights Rules Network flows the table below shows network flows for fire- network traffic in the future. Learn more	walls managed by this policy. You can allo	v or deny a flow to create a rule for matchi	ing					
Insights Rules Network flows the table below shows network flows for firey betwork taffic in the future. Learn more Search Rule c Refresh I Delete rule	walls managed by this policy. You can allow collection name : All Firewalls : Al	v or deny a flow to create a rule for matchi	ing	Show data	or the last : 30	days		
Insights Rules Network flows the table below shows network flows for line etwork traffic in the future. Learn more G Search Rule c P Refeash Delete rule 1-10 of 140 tiems	walls managed by this policy. You can allo collection name : All Firewalls : Al	v or deny a flow to create a rule for matchi	ing	Show data Show 11	for the last : 30	days e V		
Insights Rules Network flows The table below shows network flows for the future. Learn more of Search Rule C Rule C Refresh 10 Delete nule I=10 of 140 items Priority 1 L Rule collect 1 + Ru	valls managed by this policy. You can allo collection name : All Firewalls : Al alle collection 14 Rule 14	v or deny a flow to create a rule for matchi → Add filter Resot Matching flows ↑↓ Source ↑↓	ng Port ↑↓ Protocol	Show data Show 1! ↑↓ Destination ↑↓	for the last : 30) items per pag Hit count ↑,	days e V		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Perfect Rule c Priority 1 Rule collect 1 Rule 100 DefaultNetwork. No	walls managed by this policy. You can allo collection name : All Firewalls : Al ale collection 1↓ Rule 1↓ etRuleCol-A globalNetRule1	v or deny a flow to create a rule for matchi Add filter Resot Matching flows ↑↓ Source ↑↓ 0	ng Port ↑↓Protocol	Show data Show 1 ↑↓ Destination ↑↓	for the last : 30) items per pag Hit count 1, 0	days e v		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Search Rule c Rule c Priority 1 µule collect 1 µ Ru 100 DefaultNetwork. N 100 DefaultNetwork. N	valls managed by this policy. You can allo collection name : All Firewalls : Al ale collection ↑↓ Rule ↑↓ eRFuleCol-A globalNetRule1 eRFuleCol-A globalNetRule2	v or deny a flow to create a rule for matchi	ng Port ↑↓Protocol	Show data Show 11 ↑↓ Destination ↑↓	for the last : 30 Ditems per pag Hit count ↑ 0 0	days e v		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Search Rule c Periority Priority DefaultNetwork 100 DefaultNetwork N 100 DefaultNetwork N 100 DefaultNetwork N N N N N N N N N N N N N	walls managed by this policy. You can allo collection name : All Firewalls : Al ale collection 1↓ Rule 1↓ eRfuleCol-A globalNetRule1 eRfuleCol-A globalNetRule2 etRuleCol-A globalNetRule3	v or deny a flow to create a rule for matchi X → Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192,168.00/32	Port 11 Protocol	Show data Show 11 ↑⊥ Destination ↑↓ 72.56.1	For the last : 30) items per pag Hit count 1 0 0 3	days e ~ 		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Search Rule c Pointing 1: Delete nule Priority 1: Rule collect 1: Rule Priority 1: Rule collect 1: Rule 100 DefaultNetwork No 100 DefaultNetwork No 200 DefaultNetwork	walls managed by this policy. You can allo collection name : All Firewalls : Al ale collection 1↓ Rule 1↓ eREuleCol-A globalNetRule1 eREuleCol-A globalNetRule2 eREuleCol-A globalNetRule3 eREuleCol-B localNetRule1	v or deny a flow to create a rule for matchi X → Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192,168.0.0/32 0	Port 1↓Protocol 80 HTTP	Show data Show 11 ↑⊥ Destination ↑↓ 72.56.1	for the last : 30) items per pag Hit count ↑, 0 0 3 0	days e ~		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Search Rule c Pointing 1: Delete nule Priority 1: Rule collect 1: Rule Priority 1: Rule collect 1: Rule 100 DefaultNetwork 100 DefaultNetwork 200 DefaultNetwork Ne 200 DefaultNetwork	walls managed by this policy. You can allo tollection name : All Firewalls : Al ale collection 1↓ Rule 1↓ etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-A globalNetRule3 etRuleCol-B / localNetRule1 etRuleCol-B / localNetRule2	v or deny a flow to create a rule for matchi X Add filter Resot Matching flows ↑↓ Source ↑↓ 0 0 1 192,168.0.0/32 0 3	Port 11 Protocol 80 HTTP	Show data Show 11 ↑↓ Destination ↑↓ 72.56.1	for the last : 30) items per pag Hit count ↑, 0 3 0 5	days e ~ 		
Insights Rules Network flows The table below shows network flows the table below shows network flows for the future. Learn more of Search Search Rule c Priority 1, Rule collect 1, Ru Priority 1, Rule collect 1, Ru Do DefaultNetwork N D00 DefaultNetwork N 200 DefaultNetwork N 200 DefaultNetwork N	valls managed by this policy. You can allo collection name : All Firewalls : Al alle collection ?↓ Rule ?↓ etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-B localNetRule3 etRuleCol-B v localNetRule2	v or deny a flow to create a rule for matchi X Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192,168,00/32 0 3 10,00,0/24, 10,	Port 12 Protocol 80 HTTP	Show data Show 11 ↑⊥ Destination ↑↓ 72.5.6.1 72.4.6.1, 72.5.6.1_	For the last : 30) items per pag Hit count 1: 0 3 0 5 2 2 2	days e v 		
Insights Rules Network flows The table below shows network flows The table below shows network flows Fearch Search Rule c Periority Rule collect Rule collect Priority Lu0 DefaultNetwork N 200 DefaultNetwork N 200 DefaultNetwork N	valls managed by this policy. You can allo collection name : All Firewalls : Al alle collection 1↓ Rule 1↓ etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-B localNetRule1 etRuleCol-B v localNetRule2	x or deny a flow to create a rule for matchi X → Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192.168.00/32 0 10.00.0/24, 10 192.168.00/32	Port 12 Protocol 80 HTTP 52 UDP	Show data Show 11 ↑⊥ Destination ↑↓ 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.4	For the last : 30 D items per pag Hit count 1: 0 3 0 5 2 2 3	days e ~ 		
Insights Rules Network flows he table below shows network flows for line etwork tarfic in the future. Learn more of Psearch Rule c Rule c Psearch Rule c Priority 1↓ Rule collect 1↓ Ru Priority 1↓ Rule collect 1↓ Ru 100 DefaultNetwork. N 100 DefaultNetwork. N 200 DefaultNetwork. N 200 DefaultNetwork. N 200 DefaultNetwork. N 200 DefaultNetwork. N	valls managed by this policy. You can allo collection name : All Firewalls : Al ale collection ?↓ Rule ?↓ etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-B localNetRule3 etRuleCol-B v localNetRule2	x or deny a flow to create a rule for matchi X x y Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192.168.00/32 192.168.00/32 192.168.00/32	Port ↑↓ Protocol 80 HTTP 52 UDP 52 UDP	Show data Show 11 11 Destination 1↓ 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.4 192.168.4.61	or the last : 30) items per pag Hit count 1, 0 0 3 0 5 2 2 3 3 3	days e ~ 		
Insights Rules Network flows The table balance shows network flows for line tensork traffic in the future. Learn more of Search Rule c Pointly T, Rule collect 1, Rule Priority T, Rule collect 1, Rul Priority T, Rule collect 1, Rul Priority T, Rule collect 1, Rul Do DefaultNetwork. Ne 200 DefaultNetwork. Ne 200 DefaultNetwork. Ne 300 DefaultNetwork. Ne	valls managed by this policy. You can allo collection name : All Firewalls : Al ale collection 12 Rule 12 etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-B localNetRule3 etRuleCol-B v localNetRule3 etRuleCol-C > localNetRule3	x or dery a flow to create a rule for matchi X Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 1 192,168.00/32 0 10.00.0/24, 10 192,168.00/32 192,168.00/32 3	Port 12 Protocol 80 HTTP 52 UDP 52 UDP	Show data Show 11 ↑↓ Destination ↑↓ 72.5.6.1 72.4.6.1, 72.5.6.1_1 192.168.4.4 192.168.4.61	For the last : 30 bitems per page Hit count 1: 0 0 3 0 5 3 2 3 3 3 5	days e v 		
Insights Rules Network flows Insights Rules Network flows Interable below shows network flows for ling sevents traffic in the future. Learn more G Search Rule c Ru	wells managed by this policy. You can allo collection name : All Firewalls : Al ale collection ?↓ Rule ?↓ etRuleCol-A globalNetRule1 etRuleCol-A globalNetRule2 etRuleCol-B // localNetRule3 etRuleCol-B // localNetRule3 etRuleCol-C // localNetRule3 etRuleCol-C // localNetRule3 etRuleCol-C // localNetRule3	x or deny a flow to create a rule for matchi X Add filter Resct Matching flows ↑↓Source ↑↓ 0 0 1 1 192.168.00/32 0 10.00.0/24, 10 1 192.168.00/32 192.168.00/32 3 0	Port ↑↓ Protocol 80 HTTP 52 UDP 52 UDP	Show data Show 1 1 Destination 1 72.5.6.1 72.4.6.1, 72.5.6.1 192.168.4.61	For the last : 30 items per pag Hit count 1, 0 3 0 3 5 2 3 3 3 5 0 0	days e ~ 		

Azure Firewall Workbook and Sentinel Integration

Azure Firewall Data Connector for Azure Sentinel can be used to ingest logs to visualize data in the Firewall Workbook available in Sentinel.

 The workbook can also be downloaded from our GitHub repo (<u>https://aka.ms/AzNetSec</u>) and used with a Log Analytics workspace.

✔Edit 🖫 ♡ Q ☆ ©) ? Help 🔇) Auto refresh: Off				
TimeRange: Last 3 days V	Workspaces: Tob	iPremExqstlog \lor	Azure Firewalls: azfw:	SEA V Show Help (): Yes	No Change Log	Show Resourc
Azure Firewall Resource List						
Firewall ↑↓	Premium ↑↓	Standard \uparrow_{\downarrow}	ProvisionedState \uparrow_{\downarrow}	FirewallPolicy 1	ApplicationRuleClassic \uparrow_{\downarrow}	NetworkRule
DEMO-FW-PREMIUM	Yes	No	Not Running	M DEMO-FWPOLICY-PREMIUM	N/A	N/A
😞 AzureFirewall_VWANHub1	No	Yes	Not Running	🐃 FW-Standard	N/A	N/A
😞 ChrisBoehmFW2	No	Yes	Not Running		N/A	N/A
🥪 mohitku-FWPremium	Yes	No	Not Running	Sector Strategy Sector Strategy Sector Strategy Sector Strategy Sector Strategy Sector Sector Strategy Sector	N/A	N/A
🤿 azfwSEA	Yes	No	Running	🐃 azfwpremSEA	N/A	N/A

Azure Firewall Premium - IDPS



Optimize security with Azure Firewall solution for Microsoft Sentinel (public preview)

Built-in Threat Detection

- Port scan
- Port sweep
- Abnormal deny rate for source IP
- Abnormal Port to protocol
- Multiple sources affected by the same TI destination

Hunting queries

- First time a source IP connects to destination port
- First time source IP connects to a destination
- Source IP abnormally connects to multiple destinations
- Uncommon port for the organization
- Uncommon port connection to destination IP

Automating response and correlation



Response Automation

Azure Firewall Custom Connector

Take different actions against Azure Firewall, Firewall Policy, and IP Groups using Playbooks.

Playbooks

- Add IP to IP Group
- Add IP to Threat Intel Allow List
- Add new rule to block IP

Playbook support for the Classic rules, Standard and Premium policy:

Playbook Name	Premium Policy	Standard Policy	Classic Rules
AzureFirewall-BlockIP- addToIPGroup	Yes	Yes	Yes
AzureFirewall- AddIPtoTIAllowList	No	Yes	No
AzureFirewall-BlockIP- addNewRule	No	No	Yes

	¥
	Gets all the Azure Firewalls in a subscription
	*subscriptionId
	api-version 2020-07-01 X
	Connected to Sentinel work. Change connection.
	T For each Financial
T For each IP Address Entity from Incident	\checkmark
For course pooress cherry norm incident	
For each IP Address from Entity	
* Select an output from previous steps	
V 1/2 X	
	Ip scan report V3 (Preview) ····
	Post an Adaptive Card to a Teams channel and wait for a response (Preview)
	+
	Add IP address to the firewall network rules list based on SOC choice
	Condition - Add the IP address to the Firewall rule collection list or Ignore
	And V
	- u submitA_ x is equal to V OK
	+ Add ~
✓ True	False
 Compose 	Add comment to incident (V3) (Preview)
	\downarrow
D For each rules collection selected	rom Adaptive Card I Add an action
	☐ Add an article
	Adulari acuoni

Azure Firewall Manager



Enterprise challenges

Complex network architecture and constantly changing threat environment



Azure Firewall Manager

Single Pane of glass to manage Azure Firewall, DDoS & WAF across Azure Tenant

Azure Firewall Management

- Deploy Azure Firewall across both VNET and VWAN deployments
- Associate Azure Firewall Policy to one or more Firewalls
- View and modify Azure Firewall Policy
- Gain insights into Firewall Traffic with Policy Insights *Preview*

DDOS management

- View and create DDoS Protection Plans
- Associate DDoS plans to VNETs

WAF management

- Deploy and configure WAF policies
- Upgrade from legacy WAF configuration to WAF policies on Azure Application Gateway



Monitoring Overview	A central security policy and route manage	ement service for cloud-based security	/ perimeters. Learn more 👩
			subscription : multiple selected: 2
Virtual hub security coverage	Virtual network firev	vall security coverage	Virtual network DDoS security coverage
Protected by Acure Frewall Protected by Acure Frewall Protected by Acure Frewall Protected by Acure Frewall and a Security Partner Provider	vider Protected by Azure Firew	S5% Overs	197 vives
• Firewall Manager	■No Azure Firewall deploy	ed	DDoS Protection Plan not enabled
No Azure Firewall deployed Firewall Manager Search (Ctrl+/)	Virtual Networks A Create new Secured Virtual	• Network 💍 Refresh 🚦	Dos Protection Plan not enabled Manage security ~
	Virtual Networks 🖇	• Network 🖒 Refresh 🔓	Dos Protection Plan not enabled Manage security reploy a Firewall with Firewall Policy
No Azure Firewall deployed Firewall Manager Search (Ctrl+/) Getting Started Deployments	Virtual Networks Create new Secured Virtual Filter by name	ed Network () Refresh (D Clear all filters M	Manage security reploy a Firewall with Firewall Policy Anage DDoS Protection Plan (preview)
 No Azure Frewall deployed Search (Ctrl+/) Getting Started Deployments Virtual Networks 	No Azure Firewall deploy Virtual Networks Create new Secured Virtual Filter by name Virtual Networks	ed · Network Ĉ) Refresh Clear all filters ↑↓ Azure Firewa	
 No Azure Frewall deployed Firewall Manager Search (Ctrl+/) Getting Started Deployments Virtual Networks Virtual Hubs 	No Azure Firewall deploy Virtual Networks Create new Secured Virtual Filter by name Virtual Networks Virtual Networks Virtual Networks	ed Network () Refresh (Clear all filters M ↑↓ Azure Firewa ☆ No Firewa	Dos Protection Plan not enabled Manage security ∨ eploy a Firewall with Firewall Policy fanage DDos Protection Plan (preview) all Policy ↑↓ DDos Protection Plan all deployed
 No Azure Firewall deployed Search (Ctrl+/) Getting Started Deployments Virtual Networks Virtual Hubs Security 	No Azure Firewall deploy Virtual Networks	ed Network Ĉ) Refresh Clear all filters ↑↓ Azure Firewa ☆ No Firew ☆ No Firew	Dos Protection Plan not enabled Manage security ✓ eploy a Firewall with Firewall Policy Manage DDoS Protection Plan (preview) all Policy ↑↓ DDoS Protection Plan all deployed all deployed
 No Azure Firewall deployed Search (Ctrl+/) Getting Started Deployments Virtual Networks Virtual Hubs Security Azure Firewall Policies 	No Azure Firewall deploy Virtual Networks	ed Network Ĉ) Refresh Clear all filters M ↑↓ Azure Firewa ☆ No Firew ☆ No Firew ☆ No Firew	Dos Protection Plan not enabled Manage security ∨ eploy a Firewall with Firewall Policy fanage DDos Protection Plan (preview) all Policy
 No Azure Firewall deployed Search (Ctrl+/) Getting Started Deployments Virtual Networks Virtual Hubs Security Azure Firewall Policies Security Partner Providers 	No Azure Firewall deploy Virtual Networks	ed Network () Refresh (Clear all filters M ↑↓ Azure Firewa ☆ No Firew ☆ No Firewa ☆ No Firewa ☆ No Firewa	Dos Protection Plan not enabled Manage security ∨ eploy a Firewall with Firewall Policy fanage DDos Protection Plan (preview) all Policy ↑↓ DDos Protection Plan all deployed all deployed all deployed all deployed all deployed

Central security and policy management

Deploy and configure Azure Firewall policies, Azure WAF policies, and Azure DDoS Protection plans

Span different Azure regions and subscriptions from a single pane of glass.

Enforce consistent configuration across Azure Firewall

Manage Network address translation (NAT), network, and application rule collections, as well as threat intelligence and DNS settings.

DevOps optimized hierarchical Azure Firewall policies

Global firewall policies authored by Central IT with local derived firewall policies for DevOps self-service for better agility.

Manage Azure Firewall Policy independent of Azure Firewall

Azure Firewall Policy is a top-level resource with independent access control and activity tracking.



Multi security provider support (secure hub only)

Combine best of breed security

Azure Firewall for east-west (virtual network to virtual network/branch to virtual network) traffic filtering.

Security partner of your choice for north-south (virtual network to Internet/branch to Internet) traffic filtering.

Use Azure for Edge security

Avoids routing internet traffic to on-premise.

Route internet traffic directly from Azure.

Partners

- Zscaler (currently runs on ZIA cloud, roadmap to run on Azure)
- Check Point (runs on Azure)
- iboss (runs on Azure)

Simplifies connectivity and security

Easily attract traffic to your secured virtual hub for filtering and logging without manipulating User Defined Routes.



Firewall Pricing



Most customers save 30%–50% in comparison to NVAs

When comparing with NVAs, consider the full TCO including licensing, multiple VMs and 2 standard load balancers (traffic + rules charge)

Throughput limit 30 Gbps

Assume at least one firewall per region

Firewall Manager GA Pricing

Azure Firewall in Secured Virtual Hubs

Fixed fee: \$1.25/firewall/hour Variable fee: \$0.016/GB processed by the firewall

Azure Firewall Manager policies

Fixed fee: \$100/Policy/Region Policies that are associated with a single hub are free of charge Policy Analytics

Azure Firewall Manager 3rd party integration Fixed fee: \$0.4/Secured hub/hour Virtual WAN VPN GA charges apply

©Microsoft Corporation Azure





Azure Firewall Premium
Azure Firewall Premium

Cloud native next-gen Firewall as a service

TLS Inspection

Built-in TLS Inspection for Outbound and East-West traffic

Inbound TLS termination is supported with Azure Application Gateway

Customer provided key pair via Azure Key Vault integration

Intrusion Detection Prevention System (IDPS)

Detect alert and block inbound/outbound malicious traffic Supported for both encrypted and plain text protocols Signature-based detection that is continuously updated

URL Filtering

Restrict user access to HTTP/HTTPS Web content

Support for URL wildcards

Web Categories

Allow or deny user access to website categories such as gambling, social media and others

Web categories maintained and continuously updated

URL based category matching



Azure Firewall Premium – without TLS Inspection



Azure Firewall Premium – TLS Inspection



Azure Firewall Premium – TLS Inspection

- Azure Firewall intercepts outbound traffic for inspection
- Intermediary certificate should be uploaded to the Firewall to verify server certificate.



Azure Firewall with web applications





Azure Firewall with web applications





Azure Firewall Premium – TLS Inspection

Enable TLS Inspection in Firewall Policy

Key Vault Integration

Parent policy: None

Disabled This feature will not be enabled on your firewalls.

Enabled

TLS inspection will be used with IDPS and applicable application rules.

() TLS inspection is a premium feature that will not function on standard-tier firewalls. <u>Learn more</u>

Key vault

Select the Key vault where your CA certificate and private key are stored, or auto-generate new certificate by selecting new Manged Identity. <u>Learn more</u>

Managed identity * ①
fw-cert-id-4dELJYCvtZaNg (rg-lab)
Key vault * ①
fw-cert-kv-4dELJYCvtZaNg (rg-lab)
Certificate *
fw-cert-4dELJYCvtZaNg (rg-lab)

Azure Firewall Premium

Cloud native next-gen Firewall as a service

Intrusion Detection Prevention System (IDPS)

Detect alert and block inbound/outbound malicious traffic Signature-based detection that is continuously updated Over 58,000 rules in over 50 categories Detection and Prevention mode IDPS Bypass List

IDPS Private IP ranges (preview)



Azure Firewall Premium Configuration

Home > Firewall Manager > fw-poli	icy1
fw-policy1 IDPS (Firewall Policy I Directory: Mice	(preview) ····
	Rarent policy: None
省 Overview	
Activity log	IDPS mode Signature rules Bypass list
Access control (IAM)	If IDPS is enabled on a parent policy, you can only change to a stricter setting. For example, if the parent policy specifies Alert mode, you can select Alert and deny, but you cannot disable IDPS learn more
🔶 Tags	 Disabled
Settings	This feature will not be enabled on your firewalls.
Parent Policy	 Alert You will receive alerts when suspicious traffic is detected.
Rule Collections	Alert and deny
DNAT Rules	You will receive alerts when suspicious traffic is detected, and that traffic will be denied when the matching signature is from a high confidence category.
Network Rules	
Application Rules	IDPS is a premium feature that will not function on standard-tier firewalls
DNS	
🏮 Threat Intelligence	
🔩 TLS inspection (preview)	
IDPS (preview)	
💥 Secured virtual hubs	
↔ Secured virtual networks	
Private IP ranges (SNAT)	

Azure Firewall Policy



Azure Firewall

Rules Processing Logic



Execution order:



Policy Analytics Preview

Manage Azure Firewall rules over time

Policy Insights

 Highlights key information of the Firewall policy such as Policy limits, Duplicate rules, Wildcard in rules and more.

Policy Recommendations

 Recommendations to improve the Rules in the policy including rules with low/no hits, overly permissive rules, potentially malicious sources.

Rule Analytics

- Visibility into the traffic flows of the rules over time
- Rule hit count for Application, Network and DNAT rules

Single Rule Analysis

• Refine the rules permissions



Configure workspaces 💍 Refresh	📋 See all recommenda	ations					
Policy limits		Rules with multiple I	P addresses ①	9	Rules with	low utilization ①	
					•		
2,468 Rules	7000 Max	37 Source IPs > 10		2,468 Total	37 0 hits	(all matching flows)	2,468
6,507 Unique sources	10,000 Max	349 Destination IPs :	• 10	2,468 Total	863 0 hit	s (> 20% of matching flows)	2,468
9 629 Unique destinations	10.000 14						
9,629 Unique destinations	10,000 Max						
		Coo roc	a second as a second			Coo recommondations	
Insights Rules Network flows The table below shows network flows for firewalls mana network traffic in the future. Learn more I	aged by this policy. You can allo	w or deny a flow to create a rule for n	natching			See recommendations	
Insights Rules Network flows The table below shows network flows for firewals mana setwork traffic in the future. Learn one O Search Dataset D Index one	aged by this policy. You can allor name : All Firewalls : Al	w or deny a flow to create a rule for r	natching	Show data (for the last - 20 day	see recommendations	
Insights Rules Network flows The table below shows network flows for firewalls management for the setwork traffic in the future. Learn more Of P Search Rule collection Rule collection Delete nule	aged by this policy. You can allor name : All Firewalls : Al	w or deny a flow to create a rule for r	natching	Show data 1	for the last : 30 day	see recommendations	
Insights Rules Network flows The table below shows network flows for firewals mana network traffic in the future. Learn more G P Search Rule collection Rule collection Netresh © Delete nule Into of 140 items	aged by this policy. You can allo name : All Firewalls : Al	wordery a flow to create a rule for r	natching	Show data 1 Show 10 Show 10	for the last : 30 day	a v	
Insights Rules Network flows Insights Rules Network flows for freewals mains Persent marking in the future. Learn more D Persent Rule collection Refresh Delete rule NetResh N	aged by this policy. You can allor name : All Firewalls : All tion $\uparrow\downarrow$ Rule $\uparrow\downarrow$ colobalNotBuile	v or deny a flow to create a rule for n I × 1 Add filter Reset Matching flows ↑↓ Source ↑↓	natching Port 14 Protoco	Show data f Show 10 I ↑↓ Destination ↑↓	for the last : 30 day 0 items per page Hit count ↑↓ 0 ····	see recommendations	
Insights Rules Network flows Instable below shows network flows for firewells mana- every traffic in the future. Lear more O Search Rule collection Rule collection Refresh Priority 1↓ Rule collect 1↓ Rule collect Priority 1↓ Rule collect 1↓ Rule collect D0 Default/Network. NetRuleCol D0 Default/Network.	aged by this policy. You can allor name : All Firewalls : Al tion ?↓ Rule ?↓ -A globalNetRule1 -A globalNetRule2	See FeX w or dery a flow to create a rule for r I Y Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0	Introductions	Show data Show 10 1 ↑↓ Destination ↑↓	for the last : 30 day) items per page Hit count ↑↓ 0 ·	see recommendations	
Insights Rules Network flows The table below shows network flows for firewals mana- terwork traffic in the future. Lear more O Search Rule collection Rule collection Refresh Priority 1, Rule collect 1, Rule collect Priority 1, Rule collect 1, Rule collect Priority 1, Rule collect NetRuleCol DO DefaultNetwork NetRuleCol	aged by this policy. You can allor name : All Firewalls : Al tion 1 , Rule 1 , -A globalNetRule1 -A globalNetRule2 -A globalNetRule2	See FeC w or dery a flow to create a rule for r I Y Add filter Reset 0 0 1 192.168.00/	Port 13 Protoco	Show data 1 Show 10 1 12 Destination 12 725.6.1	for the last : 30 day 0 items per page Hit count ↑↓ 0 • 3 •	a 	
Insights Rules Network flows The table below shows network flows for firewals mana- thewak traffic in the future. Lear more O Search Rule collection Rule collection Rule collect ?↓ Rule collect 100 DefaultNetwork NetRuleCol	aged by this policy. You can allor name : All Firewalls : Al tion 1↓ Rule 1↓ -A globalNetRule1 -A globalNetRule2 -A globalNetRule2 -A globalNetRule3 -B localNetRule1	w or deny a flow to create a rule for n I × ▼ Add filter Reset Matching flows ↑↓ Source ↑↓ 0 1 192.168.0.0/ 0	Port 13 Protoco	Show data Show 10 1 12 Destination 12 725.6.1	for the last : 30 day 0 items per page Hit count ↑↓ 0 - 0 - 3 - 0 -	see recommendations	
Insights Rules Network flows the table below shows network flows for firewals mana- network raffic in the future. Lear more Of Search Rule collection Rule collection Rule collect 1J Rule collect 100 DefaultNetwork NetRuleCol	aged by this policy. You can allor name : All Firewalls : Al tion 1↓Rule 1↓ -A globalNetRule1 -A globalNetRule2 -A globalNetRule3 -B localNetRule1 -B v localNetRule1	See FeX w or deny a flow to create a rule for n II × \scalar Add filter Reset Matching flows 1↓ Source 1↓ 0 0 1 192.168.0.0/. 0 3	Port 11 Protoco	Show data Show 10 1 1 1 Destination 1 2 725.6.1	for the last : 30 day D items per page Hit count ↑↓ 0 - 3 - 0 - 5 -	see recommendations	
Insights Rules Network flows the table below shows network flows for firewals mana- network traffic in the future. Lear more Of Search Rule collection Rule collection Rule to f140 items Priority 1; Rule collect 1; Rule collect 100 DefaultNetwork NetRuleCol 100 DefaultNetwork NetRuleCol 200 DefaultNetwork NetRuleCol	aged by this policy. You can allor name : All Firewalls : Al tion 1↓Rule 1↓ -A globalNetRule1 -A globalNetRule2 -A globalNetRule2 -B localNetRule1 -B ∨ localNetRule2	Matching flows 1 Source 14 0 1 192.168.00/ 3 10.00.0/24	Port 12 Protoco	Show data Show 10 1 ↑↓ Destination ↑↓ 72.5.6.1 72.4.6.1,72.5.6.1_ (ior the last : 30 day Ditems per page Hit count 14 0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 • 0 •	<i>s</i> ≥ <i>v</i> ≥	
Insights Rules Network flows the table below shows network flows for firewals mana network traffic in the future. Learn more Of Search Rule collection Rule collection Rule to fl40 items Priority 12 Rule collect 12 Rule collect 100 DefaultNetwork NetRuleCol 100 DefaultNetwork NetRuleCol 200 DefaultNetwork NetRuleCol 2	aged by this policy. You can allor name : All Firewalls : Al tion 1↓Rule 1↓ -A globalNetRule1 -A globalNetRule2 -A globalNetRule2 -B localNetRule1 -B v localNetRule2	Matching flows 1 Source 14 Matching flows 1 Source 14 0 1 192.168.00/ 3 10.00.0/24	Port 12 Protoco 12 80 HTTP 0080 HTTP	Show data Show 10 1 ↑J Destination ↑↓ 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.4	ior the last : 30 day Ditems per page Hit count 1 4 0	a 	
Insights Rules Network flows The table below shows network flows for firewals mana network traffic in the future. Learn more Of Search Rule collection Rule collection Rule to fit40 items Priority 1 kule collect 1 Rule collect Of OD DefaultNetwork NetRuleCol Do DefaultNetwork NetRuleCol DefaultNetwork NetRuleCol DefaultNetwork NetRuleCol DefaultNetwork NetRule	aged by this policy. You can allor name : All Firewalls : Al tion 1↓Rule 1↓ :-A globalNetRule1 :-A globalNetRule2 :-A globalNetRule2 :-B localNetRule1 :-B \lor localNetRule2	See Tex. w or deny a flow to create a rate for r II × > Add filter Reset Matching flows ↑↓ Source ↑↓ 0 1 192.168.00/ 3 10.0.0.0/24 / 192.168.00/ 192.168.00/	Port 12 Protoco 12 80 HTTP 0. ©80 HTTP 12 52 UDP	Show data Show 10 1 1 ↓ Destination 1↓ 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.4 192.168.4.61	for the last : 30 day Disting per page Hit count 7.4 0 - 0 - 3 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0	s v · · · · ·	
Insights Rules Network flows The table below shows network flows for firewals mana- network traffic in the future. Learn more O Search Rule collection Rule co	aged by this policy. You can allor name : All Firewalls : Al tion 1↓ Rule 1↓ :A globalNetRule1 :A globalNetRule2 :A globalNetRule3 :B localNetRule3 :B v localNetRule2	See Tex. w or deny a flow to create a rule for r II × ▼ Add filter Reset Matching flows ↑↓ Source ↑↓ 0 1 192.168.00/24 192.168.00/2 192.168.00/2	Port ↑⊥ Protoco 12 80 HTTP 00 000 HTTP 12 52 UDP	Show data Show 10 1 ↑⊥ Destination ↑↓ 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.61	for the last : 30 day Disms per page Hit count 1 - 1 0	see recommendations	
Insights Rules Network flows The table below shown network flows for freewals mana- tensork tarkin the future. Learn more Priority 12 Rule collect 12 Rule collect NetRule 100 DefaultNetwork. NetRuleCol 100 DefaultNetwork. NetRuleCol 200 DefaultNetwork. NetRuleCol 200 DefaultNetwork. NetRuleCol 300 DefaultNetwork. NetRuleCol	aged by this policy. You can allor name : All Firewalls : Al Firewalls : Al A globalNetRule 1 A globalNetRule 1 A globalNetRule 2 A globalNetRule 3 B localNetRule 3 B localNetRule 3 B localNetRule 3 C > localNetRule 3 C > localNetRule 3	See Tex w or deny a flow to create a rule for r I × • Add filter Reset Matching flows ↑↓ Source ↑↓ 0 0 0 0 0 1 192.168.00/ 0 3 100.00/24 · 192.168.00/ 192.168.00/ 192.168.00/ 3 0 0	Port ¹ 2 Protoco Port ¹ 2 Protoco 2 80 HTTP 0 (0)80 HTTP 12 52 UDP 12 52 UDP	Show data Show 10 1 ↑L Destination ↑L 72.5.6.1 72.4.6.1, 72.5.6.1_ 192.168.4.61	or the last: 30 day) tiens per page - Hit count 1 0 - 3 - 0 - 3 - 0 - 2 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 3 - 4 - 5 - 6 -	see recommendations	



Azure Firewall Demo



Azure Web Application Firewall

Digital transformation brings about new challenges



Enterprises need a modern cloud CDN to protect, optimize and scale their applications

Azure web application protection



Azure Web Application Firewall combined with the global scale of Azure Network Edges provides protection from multiple attack types Azure DDoS Protection Standard combined with Azure Web Application Firewall provides adaptive protection from multiple attack types

Azure Web Application Firewall

Intelligent application protection

- Managed rulesets powered by Microsoft Threat Intelligence to protect against OWASP top 10
- \checkmark Powerful custom rules engine
 - Geo-filtering
 - IP restriction
 - http parameters filtering
 - size restriction
- ✓ Bot protection with Microsoft Threat Intelligence
- ✓ Conditional rate limiting at Azure network edge
- ✓ Built-in DDoS Protection
- ✓ Easy configuration: Portal, API, PS, Cli, Terraform



Azure Front Door

Modern cloud CDN that delivers optimized experiences to users anywhere

Modern Architecture

- Fully REST API driven to automate and streamline deployment
- Tight integration with Azure services including App Service, Storage, API Manager, App Gateway and Azure Sentinel
- Customizable rules for advanced routing
- Advanced analytics to monitor traffic and security in real time

Fast Global Delivery

- Low latency, high throughput content delivery from cloud or on-prem to global users
- Built on Microsoft massively-scaled private global network
- Supports static/dynamic content caching, file, OTT and video ondemand
- SSL offload and dynamic app acceleration at the edge close to user
- Simplified cost model with fewer meters to plan for

Intelligent Security

- WAF, DDoS and Bot Manager protection
- Azure Private Link support to access resources securely
- Powered by Microsoft Threat Intelligence



Azure Front Door WAF

Global and centralized WAF

- Prevents malicious attacks close to the attack sources
- Custom and managed rules
- Fully Integrated with the Premium SKU. Standard SKU limited to custom rules.
- 5 Rate limiting

2

3

4

6

BLOCK, ALLOW, LOG, REDIRECT Actions



6 Bot Protection

Azure WAF with Application Gateway

Protect from common application vulnerabilities

- Highly available, autoscaling, fully platform managed
- 2 Native in region and intra-VNet/hybrid integration
- 3 Support public IP, private IPs, cross region, or on-premises backend pools
- 4 OWASP top 10 out of box protection CRS 3.0, CRS 3.1, CRS 3.2 Custom Rules supported
- 5 Rule configurability, exclusion lists, different rules sets, anomaly scoring
- 6 Near real time monitoring/alerting with Azure Monitor, Azure Security Center integration, Azure Sentinel integration



Azure Web Application Firewall WAF modes

Detection mode

Monitors and logs all threat alerts Does not block incoming requests Turn on Diagnostics and WAF logs

Prevention mode

Blocks attacks identified by the rules "403 Unauthorized access" error



Different WAF Policy Categories

- · Global WAF Policy
 - All sites in Application Gateway are protected with the same policy

- Per-Site WAF Policy
 - Each listener is protected by a WAF policy with unique custom rules, exclusions etc.
- Per-URI WAF Policy
 - URI level specific WAF configuration using Path Based Rule to manage access to resource



WAF Policies Demo



WAF Integration

- Send WAF Data to Azure Sentinel
- Hunting Using WAF Data
- · Generate Incidents using Azure
- Azure Sentinel Analytics
- Respond to Incidents with Playbooks
- Visualize with Azure Monitor Workbooks

s Next steps Prerequisites To integrate with Azure Web Application Firewall (WAF) make sure you have: * Workspace: read and write permissions are required.
Next steps Prerequisites To integrate with Azure Web Application Firewall (WAF) make sure you have: Workspace: read and write permissions are required.
Prerequisites To integrate with Azure Web Application Firewall (WAF) make sure you have: Workspace: read and write permissions are required.
Configuration Connect Azure WAF to Azure Sentinel Go to each WAF resource type and choose your WAF. Open Application Gateway resource > Open Front Door resource > Open Content Delivery Network (CDN) WAF policy > (preview) Inside your WAF resource: 1. Select Diagnostic logs. 2. Select + Add diagnostic setting. 3. In the Diagnostic setting blade: • Type a Name. • Select Send to Log Analytics. • Choose the log destination workspace. • Select the categories that you want to analyze (recommended: ApplicationGatewayAccessLog ApplicationGatewayFirewallLog, FrontdoorAccessLog, FrontdoorWebApplicationFirewallLog, WebApplicationFirewallLogs). • Click Save.

Azure WAF Pricing with Application Gateway v2

Web Application Firewall Application Gateway

Fixed

Capacity Unit¹

\$0.443 per gateway-hour

\$0.0144 per capacity unit-hour



Azure DDoS Protection



What are DDoS attacks?

Bad actors generate malicious traffic to take down the network or application (public) by either impacting the availability or the performance of the network or application.

Why should I care?

Any public IP receiving traffic from the internet is susceptible to DDoS attacks.

Top cause of availability issue for large enterprises.



How real are they?



CY2021 Holiday Season

On November 11, 2021, we mitigated a **3.47 Tbps (340M pps)** DDoS UDP attack in Azure, the largest attack ever reported in history!



In December, we mitigated two more attacks that surpassed 2.5 Tbps – one was a 3.25 Tbps UDP attack, and the other attack was a 2.55 Tbps UDP attack.



Azure DDoS Network Protection

Cloud scale DDoS protection for Virtual Networks in Azure

01	zure global network
----	---------------------

02 Adaptive tuning

- 03 Attack analytics & metrics
- Integration with Microsoft Defender for Cloud & Sentinel
- 05 DDoS Rapid Response (DRR)
 - SLA guarantee and cost protection



06

Azure DDoS IP Protection (Preview)

DDoS protection designed for small & medium businesses



- Cost-effective, enterprise–grade DDoS protection
- Flexibility to enable protection on an individual public IP resource
 - Easy to configure and monitor



03

Integration with Microsoft Defender for Cloud & Sentinel



SKU comparison

Feature	DDoS IP Protection (Preview)	DDoS Network Protection
Active traffic monitoring & always on detection	\checkmark	
L3/L4 Automatic attack mitigation	\checkmark	\bigcirc
Automatic attack mitigation	\checkmark	
Application based mitigation policies	\checkmark	 Image: Contract of the second s
Metrics & alerts	\checkmark	
Mitigation reports	\checkmark	 Image: Contract of the second s
Mitigation flow logs	\checkmark	 Image: Contract of the second s
Mitigation policies tuned to customers application	\checkmark	
Integration with Firewall Manager	\checkmark	\bigcirc
Azure Sentinel data connector and workbook	\checkmark	
DDoS rapid response support		 Image: Contract of the second s
Cost protection		
WAF discount		

Microsoft's DDoS Protection Scale

0

- Available region
- C Announced region
- Edge Site
- WAN Links



80+ Tbps mitigation capacity **2,000** Attack mitigations daily Inbound & Outbound Mitigations

DDoS integration with Azure Firewall Manager

Take actions to protect unprotected virtual networks within Firewall Manager to improve network security posture.

\equiv Microsoft Azure		$\mathcal P$ Search resources, services ar	nd docs	\geq] [[]
Home >					
腾 Firewall manager	Virtual networks 🗈	Ŕ			
✓ Search «	+ Create new virtual network	≡≡ Edit columns 💍 Refresh	🔒 Manage security 🗸 🗸		
🌄 Getting started	The table below shows network flows	for firewalls managed by this policy	. You ca Migrate with a new policy	e for mat	tching
Deployments	network tranic in the future. Learnin		Migrate with an existing p	olicy	
🔆 Virtual hubs	Filter by name Polici	es : All Firewalls : All +	Add f Add DDoS Protection Star	ndard	
👼 Virtual networks	1-10 of 140 items		Add an App Gateway		
🏠 Azure network manager	■ Name ↑↓	Azure firewall policy $\uparrow\downarrow$	Firew Add an NSG	↓ ▼	App Gatewa
	myHubVnet-1	myGlobalPolicy-1	firewall-myHubVnet-1	DOS-Basic	-
Security	myHubVnet-2	myGlobalPolicy-1	firewall-myHubVnet-2	DOS-Basic	-
Azure firewall policies	myHubVnet-3	Managed by rules	firewall-myHubVnet-3 -		-
security partner providers	myHubVnet-4	MyLocalPolicy-A	firewall-myHubVnet-4	DOS-Basic	myAppGW
Web application firewall policies	myHubVnet-5	MyGlobalPolicy-1	firewall-myHubVnet-5	DOS-Basic	-
🏮 DDoS plans	myHubVnet-6	myGlobalPolicy-1	firewall-myHubVnet-6	DOS-Basic	-
💎 Network security groups	myHubVnet-7	1 Managed by rules 🕕	firewall-myHubVnet-7 -		-
Monitoring	myHubVnet-8	1 Managed by peering ①			-
Network flows	myHubVnet-9	🖨 Unmanaged 🕕			-
	myHubVnet-10	🖨 Unmanaged 🕕			-

< Previous Page 1 V of 14 Next >

Inline DDoS protection with Gateway LB and Partner NVAs

Public preview

DDoS attacks on game servers cause outages ranging from 2-10 seconds resulting in game disruption.

Existing solutions are focused to protect a load balanced, stateless, TCP service against attacks that last for minutes/hours.

These are ill-suited to protect against DDoS attacks on game servers.

Gateway LB enables protection of game servers via enabling gaming partners to create an inline DDoS solution.



Adaptive tuning

Protection policies tuned to your application's traffic profile.

Continuously profiles normal Public IP traffic.

Utilizes machine learning algorithms for adaptive tuning and setting mitigation threshold.

Easy to setup with no user configuration is required.


Attack analytics and metrics

Telemetry through Azure Monitor

Provides near real-time network attack mitigation flow logs

Attack data snapshots every 5 mins and full post attack summary

Logging can be integrated with Azure Sentinel, Splunk, OMS, and Azure Storage



Microsoft Defender for Cloud Integration

Recommendations for unprotected public IPs

Alerts Integration into a single dashboard

Regulatory Compliance recommendations based on standards

	0 0 0				
Microsoft Azure ×					
C azureux.azurewebsites.net/Prototypc/7s=d1#MSAZ_b95504bb/MSAZ_oc	1820e4e/MSAZ_475c2b6b				
crosoft Azure > Security Center > Security alerts > Brute Force attempts	were detected		© (
	Security alerts	Brute Force attempts were detected			
T Filter	▼ File				
Image: construction of the sector of the	The contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract of the contract proceeding was also by the contract proceeding wa	the end of	CIS 1.1.0 13 of 26 is 3.2 2 of 33 p 7001 2 of 22 p sp 1 of 13 p	pliance status passed controls assed controls assed controls assed controls	
	A13. Communications security A13.1. Network security manage A13.1. Network control A13.1.1. Network control A13.1.2. Security of network A13.1.2. Secur	ment S Cont services Cont services Cont services Cont services Cont storage account vices (Preview) Cont Cont Cont Cont Cont Cont Cont Cont	RESOURCE TYPE Storage accounts Storage accounts Web applications Web applications (~) Virtual networks	FALLD RESOURCES 44 of 46 43 of 46 8 of 8 8 of 8	

Azure DDoS Protection

Attack analytics and Microsoft Sentinel integration

Azure DDoS Proto cybersecuritysoc	ection Workboo	ok ጵ ֎											×
/ Edit 🖻 🔛 Ŭ													
DDoS Summary DDoS Mr	trics DDoS Investigation	n											
Workspaces: CyberSecurityS4	DC V TimeRange: La	st 7 days 🗸 🌔 P	ublic IP Addresse	s: All 🗸									
Traffic Overview													
392 777	392 758	370 967	370 9	47. 21806.	21 806	4 14	4 14						
TotalPackets 7	otalPacketsDropped Tota	alTCPPackets	TotalTCPPacketsDro	opped TotalUDPPackets	TotalUDPPacketsDropped	TotalOtherPackets	TotalOtherPacketsDropped	d					
						Perource Looku	n based on Most Reco	ent DDoS Attack Re	nort				
Last Ten DDoS Attack Report	s, select attack to provide	resource <mark>l</mark> ookup				Resource Looku id	p, based on Most Rece ਹੈ।	ent DDoS Attack Rep	port	ΛL	tenantid	1	l locat
Last Ten DDoS Attack Report TimeGenerated	s, select attack to provide ↑↓ TopAttackVector	resource lookup ↑↓ TotalPack↑↓	TotalPack↑↓	IPAddress ↑↓		 Resource Looku id SOC-NS-FW 	p, based on Most Rece ↑↓	ent DDoS Attack Rep name ↑↓ ty	port /pe	¢↓	tenantid	↑. £23aa524cc0c	↓ locat
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM	s, select attack to provide ↑↓ TopAttackVector TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M	TotalPack↑↓ 55.17M	IPAddress ↑↓ 52.154.205.58		 Resource Looku id SOC-NS-FW SOCNSEWPI 	p, based on Most Rece ↑↓	ent DDoS Attack Re name ↑↓ ty SOC-NS-FW m	port /pe iicrosoft.network/azurefirewalls	↑↓	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. -f23ae524cc9c	↓ locat centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM	s, select attack to provide ↑↓ TopAttackVector TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M	TotalPack↑↓ 55.17M 7.016M	IPAddress ↑↓ 52.154.205.58 52.154.205.61			p, based on Most Rece †↓ P	ent DDoS Attack Re name 14 ty SOC-NS-FW m SOCNSFWPIP m	port rpe nicrosoft.network/azurefirewalls nicrosoft.network/publicipaddre	↑↓ sses	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. -f23ae524cc9c -f23ae524cc9c -f23ae524cc9c	↓ locat centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM	s, select attack to provide ↑↓ TopAttackVector TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M	TotalPack↑↓ 55.17M 7.016M 2.443M	IPAddress ↑↓ 52.154.205.58 52.154.205.61 52.154.205.58		Resource Looku id SOC-NS-FW SOCNSFWPI <> VN-HUB	p, based on Most Rece ↑↓ P	ent DDoS Attack Re name 1 tu ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor	↑↓ sses s	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. -f23ae524cc9c -f23ae524cc9c -f23ae524cc9c	↓ locat centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM	s, select attack to provide ↑↓ TopAttackVector TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M	TotalPack↑↓ 55.17M 7.016M 2.443M 40.88M	IPAddress ↑↓ 52.154.205.58 52.154.205.61 52.154.205.58 52.154.205.58		Resource Looku id SOC-NS-FW SOCNSFWPI <> VN-HU8	p, based on Most Reco	ent DDoS Attack Rep name 1 ty ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor	î↓ sses Is	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. -f23ae524cc9c -f23ae524cc9c -f23ae524cc9c	↓ locat centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM	s, select attack to provide ↑↓ TopAttackVector TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M	TotalPack↑↓ 55.17M 7.016M 2.443M 40.88M 11.84M	IPAddress ↑↓ 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58		 Resource Looku id SOC-NS-FW SOCNSFWPI SOCNSFWPI VN-HUB 	p, based on Most Reco ↑↓ 1 P	ent DDoS Attack Rep name 1 t ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor	î↓ sses is	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. -f23ae524cc9c -f23ae524cc9c -f23ae524cc9c	↓ locat centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM	s, select attack to provide TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M	TotalPack↑↓ 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M	IPAddress ↑↓ 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58		Resource Looku id SOC-NS-FW SOCNSFWP S	p, based on Most Reco Tu P	ent DDoS Attack Rep name 1 t ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe icrosoft.network/azurefirewalls icrosoft.network/publicipaddre icrosoft.network/virtualnetwor	î↓ sses s	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c	Iocat centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TcP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent o	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M forgin	IPAddress ↑↓ 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.58 52.154.205.61	Countries of Origin	Resource Looku id SOC-NS-FW SOCNSFWP S	p, based on Most Reco T P AS Nut	ent DDoS Attack Rep name 1 t ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor	↑↓ sses s	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c	↓ locat centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent of	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M f orgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 -	Countries of Origin	Resource Looku id SOC-NS-FW SOCNSFWPI <td>p, based on Most Reco T P AS Nur</td> <td>ent DDoS Attack Rep name 1 J ty ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers</td> <td>port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor</td> <td>↑↓ sses s Drop R</td> <td>tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-</td> <td>↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c</td> <td>U locat centr centr centr centr</td>	p, based on Most Reco T P AS Nur	ent DDoS Attack Rep name 1 J ty ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor	↑↓ sses s Drop R	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1-	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c	U locat centr centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent of	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M f orgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 - 52.154.205.58 - 52.154.205.61 - 93.% -	Countries of Origin	Resource Looku id Soc-NS-FW Soc-NS-FWP Soc	p, based on Most Reco Tu P AS Nur reda 0 %	ent DDoS Attack Rep name 1,4 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers	port rpe iicrosoft.network/azurefirewalls iicrosoft.network/publicipaddre iicrosoft.network/virtualnetwor 93.1 %	↑↓ sses s	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons	↑. -123ae524cc9c -123ae524cc9c -123ae524cc9c -123ae524cc9c	locat centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TCP SYN flood TCP SYN flood	resource lookup ↑↓ TotalPack↑↓ 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent of	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M f orgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 - 52.154.205.58 - 52.154.205.61 - 93 % - 7% -	Countries of Origin	Resource Looku id Soc-NS-FW Soc-NS-FWP Soc	p, based on Most Reco ↑↓ 1 p AS Nur reada 10 % 13 %	ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor icrosoft.network/virtualnetwor 93.1% 93.1% 20753 6.877	↑↓ sses 3 Drop R	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 57 0the 28	♀ locat centr centr centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TcP SYN flood TCP SYN flood	resource lookup 1 L TotalPack1 L 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent of	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M forgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 - 52.154.205.58 - 52.154.205.61 - 52.154.205.61 - 93 % - 7% -	Countries of Origin	P Resource Looku id Soc-NS-FW Soc-NS-FWP </td <td>p, based on Most Reco ↑↓ 1 p AS Nur reada 10 % wid states 13 % oldova</td> <td>ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m</td> <td>port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor icrosoft.network/virtualnetwor 93.1% 2075 93.1% 207231 6.87% 0</td> <td>↑↓ sses 3 Drop R</td> <td>tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons</td> <td>↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 77 0the 28 Proto</td> <td>locat centr centr</td>	p, based on Most Reco ↑↓ 1 p AS Nur reada 10 % wid states 13 % oldova	ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m	port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor icrosoft.network/virtualnetwor 93.1% 2075 93.1% 207231 6.87% 0	↑↓ sses 3 Drop R	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 77 0the 28 Proto	locat centr
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TcP SYN flood TCP SYN flood	resource lookup 1 L TotalPack1 L 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent o	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M forgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 - 52.154.205.58 - 52.154.205.61 - 52.154.205.61 - 93 % - 7% -	Countries of Origin		p, based on Most Reco ↑↓ 1 p AS Nur nada 10 % which states 3 % oktora *x mean	ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers	port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor icrosoft.network/virtualnetwor 93.1,1 2072 6.87 % 0 %	↑↓ sses 3 Drop R	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 13. 13. 13. 10. 10. 10. 10. 10. 10. 10. 10	
Last Ten DDoS Attack Report TimeGenerated 9/23/2020, 3:35:56 AM 9/23/2020, 3:25:54 AM 9/23/2020, 3:10:46 AM 9/23/2020, 3:05:38 AM 9/23/2020, 3:00:38 AM 9/23/2020, 2:55:37 AM Protocols	s, select attack to provide TcP SYN flood TCP SYN flood	resource lookup 1 L TotalPack1 L 55.17M 7.016M 2.444M 40.89M 11.84M 7.016M Continent of	TotalPack14 55.17M 7.016M 2.443M 40.88M 11.84M 7.016M forgin	IPAddress ↑↓ 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.58 - 52.154.205.61 - 52.154.205.58 - 52.154.205.61 - 93 % - 7 % -	Countries of Origin	P Resource Looku id Soc-NS-FW Soc-NS-FWP </td <td>p, based on Most Reco ↑↓ 1 p AS Nur reada 10 % wid states 33 % oldboa % mmay %</td> <td>ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers</td> <td>port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor 93.1% 93.1% 16.87% 0% 97.87% 0%</td> <td>↑↓ sses 3 Drop R</td> <td>tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons</td> <td>↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 133. Proto 133. P</td> <td>locat centr c</td>	p, based on Most Reco ↑↓ 1 p AS Nur reada 10 % wid states 33 % oldboa % mmay %	ent DDoS Attack Rep name 14 ty SOC-NS-FW m SOCNSFWPIP m VN-HUB m mbers	port rpe icrosoft.network/azurefirewalls icrosoft.network/virtualnetwor 93.1% 93.1% 16.87% 0% 97.87% 0%	↑↓ sses 3 Drop R	tenantid 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- 4b2462a4-bbee-495a-a0e1- keasons	↑. 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 123ae524cc9c 133. Proto 133. P	locat centr c

©Microsoft Corporation Azure

DDoS Rapid Response (DRR)

Specialized DDoS Rapid Response support during active attacks

Custom mitigation policy configuration

Basics	
NEW SUPPORT REQUEST	
* Issue type	
Technical	
* Subscription	
Can't find your subscription? Show more 🕤	
* Service	
My Services All Services	
DDOS Protection	
* Resource	
test	
* Support plan	
Azure Support Plan	
Problem NEW SUPPORT REQUEST	
* Severity 🕦	
A - Critical impact	
For critical insues, Microsoft Support will call yo Your continuous collaboration is critical to our:	u and work with you 24x7 until resolutio success. Learn more
For critical issues, Microsoft Support will call yo Your continuous collaboration is critical to our Problem type	u and work with you 24x7 until resolutio success. Learn more

Step

Step

DDoS SLA Guarantee and Cost Protection

99.99% SLA guarantee for Azure DDoS Protection service

99.99% SLA guarantee that during attack the target resource will not be impacted

Receive 100% service credits for resource costs incurred as a result of a documented DDoS attack



Azure DDoS Network Protection - Pricing



Examples of resources protected under DDoS cost protection:

- Data process (ingress/egress) for Azure firewall, AppGW/WAF
 - WAF is 100% discounted when DDoS Network Protection is enabled on the VNET; AppGW charges will apply
- Scale out of VMs, AKS
- Data egress for network bandwidth-happens during an amplification attack when DDoS impacted app makes outbound connections.
- Scale out of backend PaaS resources like SQL, CosmosDB, Storage, App Services etc.

Azure DDoS IP Protection (Preview) - Pricing



Azure Secure Hybrid Architecture



Key takeaways

- Complete your defense in depth security with best-in-class cloud native services
- Every Azure Virtual Network and Public IP should be protected by Firewall and DDoS
- Every Web/API/Mobile application should have WAF protection enabled
- Access to VMs should only be via Azure Bastion
- Enable Azure Private Link for the most secure way to access all PaaS services



Resources

- Network security strategies on Azure
- Best practices for network security
- Azure Private Link
- Azure Private Link service
- Azure Firewall Standard features
- Azure Firewall Premium features
- Azure Firewall preview features
- Azure Firewall Architecture with Application Gateways
- Azure Firewall to inspect traffic to Private Endpoints
- Integrate NAT gateway with Azure Firewall
- Azure Secured Virtual Hub (Azure Virtual WAN)
- Azure Web Application Firewall (WAF) policy
- Azure DDoS Protection
- Azure DDoS Protection SKU Comparison



Questions

© Copyright Microsoft Corporation. All rights reserved.



Thank You

© Copyright Microsoft Corporation. All rights reserved.