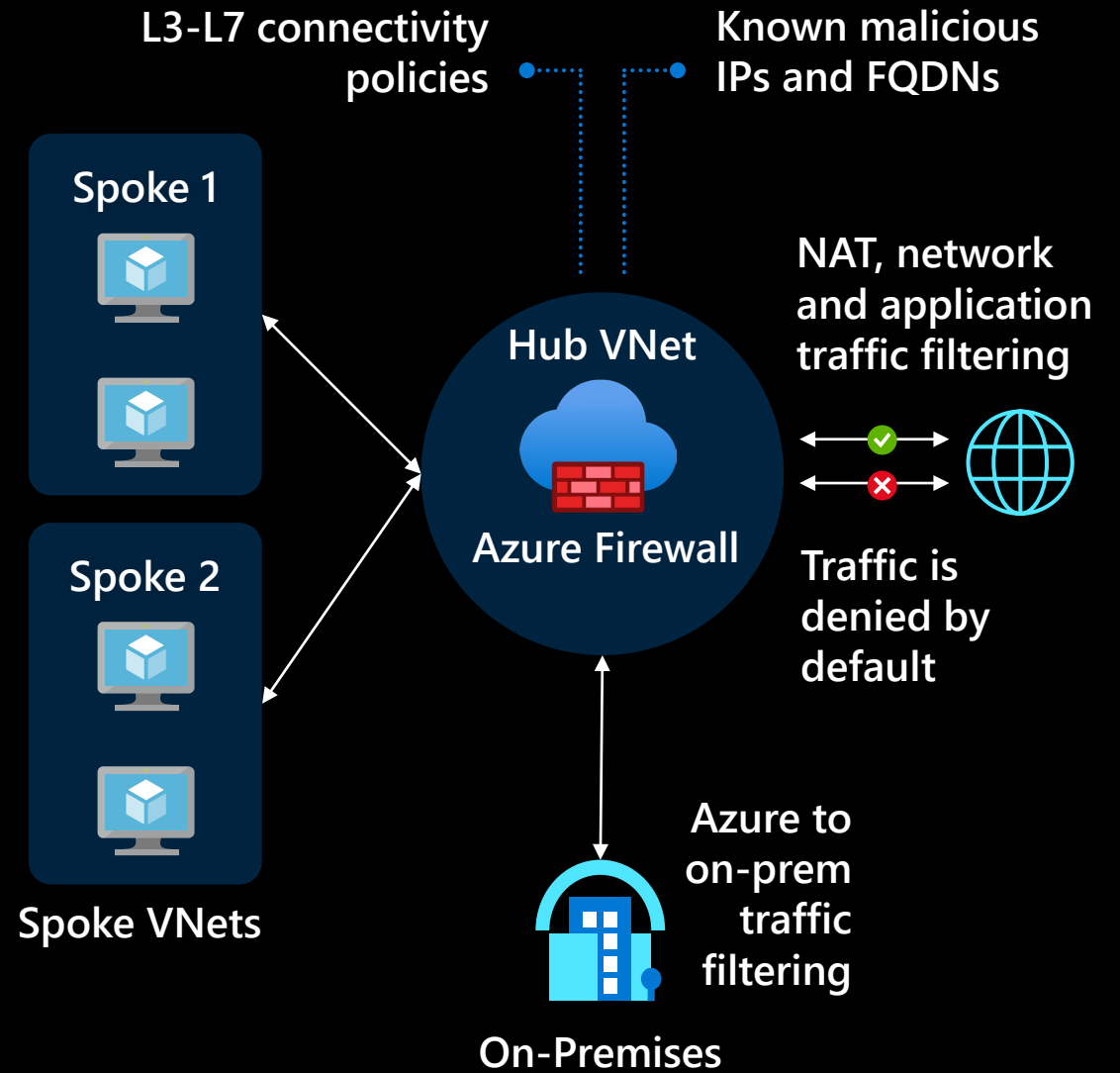


Azure Firewall



Azure Firewall

Filter traffic between cloud resources.

Example: VMs in Spoke 1 can communicate with VMs from Spoke 2.

Filter outbound traffic to the internet. Protects against data exfiltration.

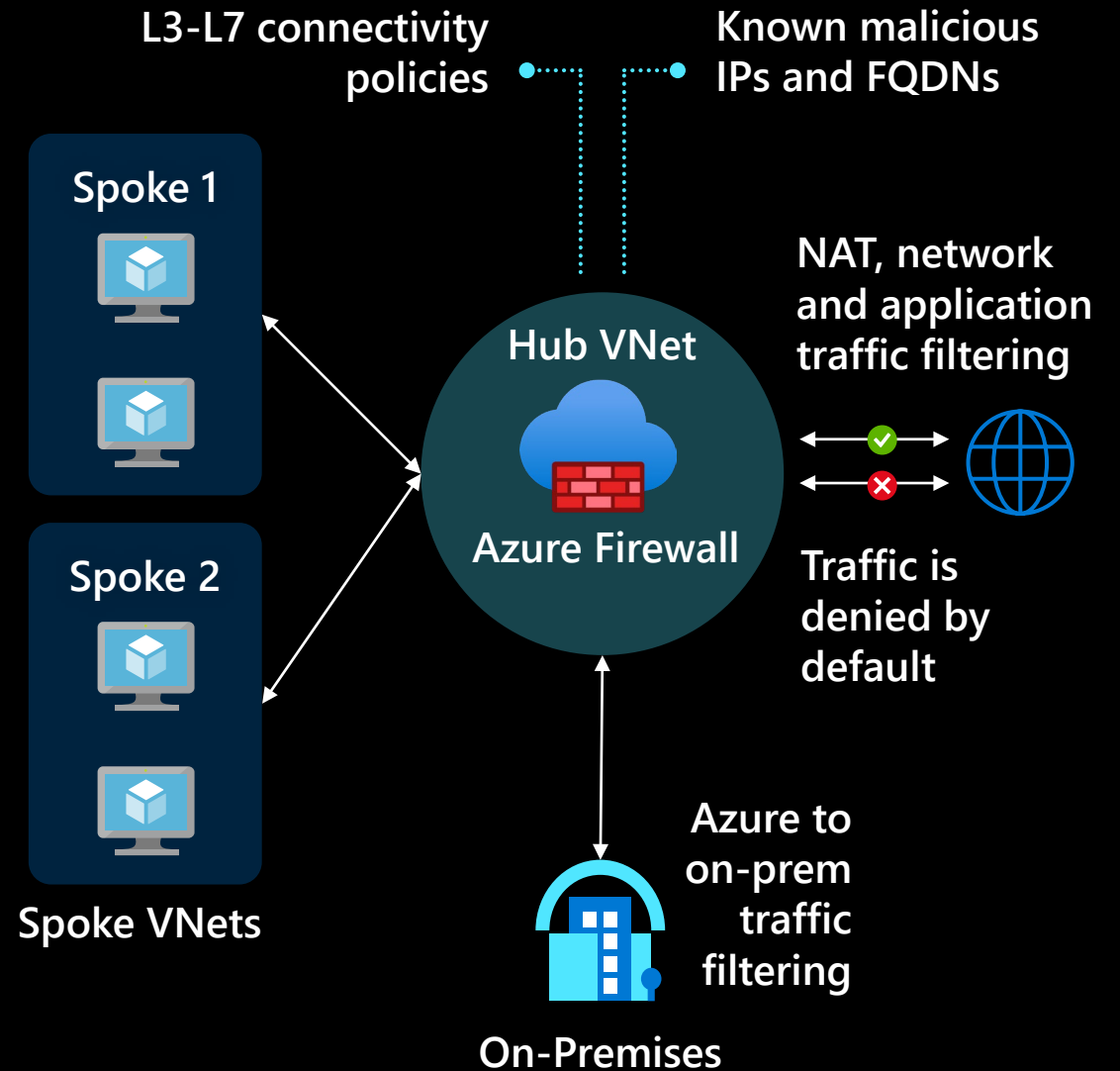
Example: All Spoke 1 VMs could not connect to internet, except some required API endpoints.

Filter traffic to/from on premise networks.

Source and destination Network Address Translation (SNAT and DNAT) support.

Example: All outbound traffic will use Firewall public IP addresses.

By default, all traffic is denied.



Creating Firewall

Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#)

Project details

Subscription * Microsoft-Azure-T
Resource group * (New) rg-fw
[Create new](#)

Instance details

Name * azfw
Region * West Europe
Availability zone ① Zones 1

Firewall SKU

- ☐ Basic
☒ Standard
☐ Premium

Firewall management

- ☒ Use a Firewall Policy to manage this firewall
☐ Use Firewall rules (classic) to manage this firewall

Firewall policy *

(New) fwpolicy
[Add new](#)

Choose a virtual network

- ☒ Create new
☐ Use existing

Virtual network name *

vnet-hub ✓

Address space

Address space *

10.0.0.0/16 ✓
10.0.0.0 - 10.0.255.255 (65536 addresses)

Subnet

AzureFirewallSubnet

IPv4 subnet *

10.0.0.0/24 ✓
10.0.0.0 - 10.0.0.255 (256 addresses)

Public IP address *

(New) pip-fw
[Add new](#)

Forced tunneling ⓘ

☐ Disabled

Azure Firewall Policy application rules

Filter on layer 7 (FQDN). **All traffic is denied by default.**

Example: allow access to `www.microsoft.com`.

Home > rg-hub > firewall-p

firewall-p

Firewall Policy

Search

Settings

Parent policy

Rule collections

DNAT rules

Network rules

Application rules

DNS

Threat Intelligence

TLS inspection

IDPS

Edit rule collection

Name

allow-microsoft.com

Rule collection type

Application

Priority *

600

Rule collection action

Allow

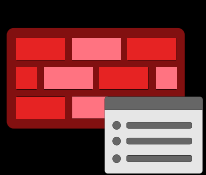
Rule collection group *

policy-group-allow

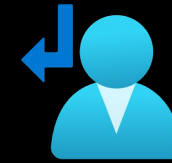
Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
allow-microsoft.com	IP Address	10.1.0.0/16	Http:80,Https:443	<input type="checkbox"/> TLS inspection	FQDN	www.microsoft.com
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql:...	<input type="checkbox"/> TLS inspection	FQDN	*,*.microsoft.com,*...

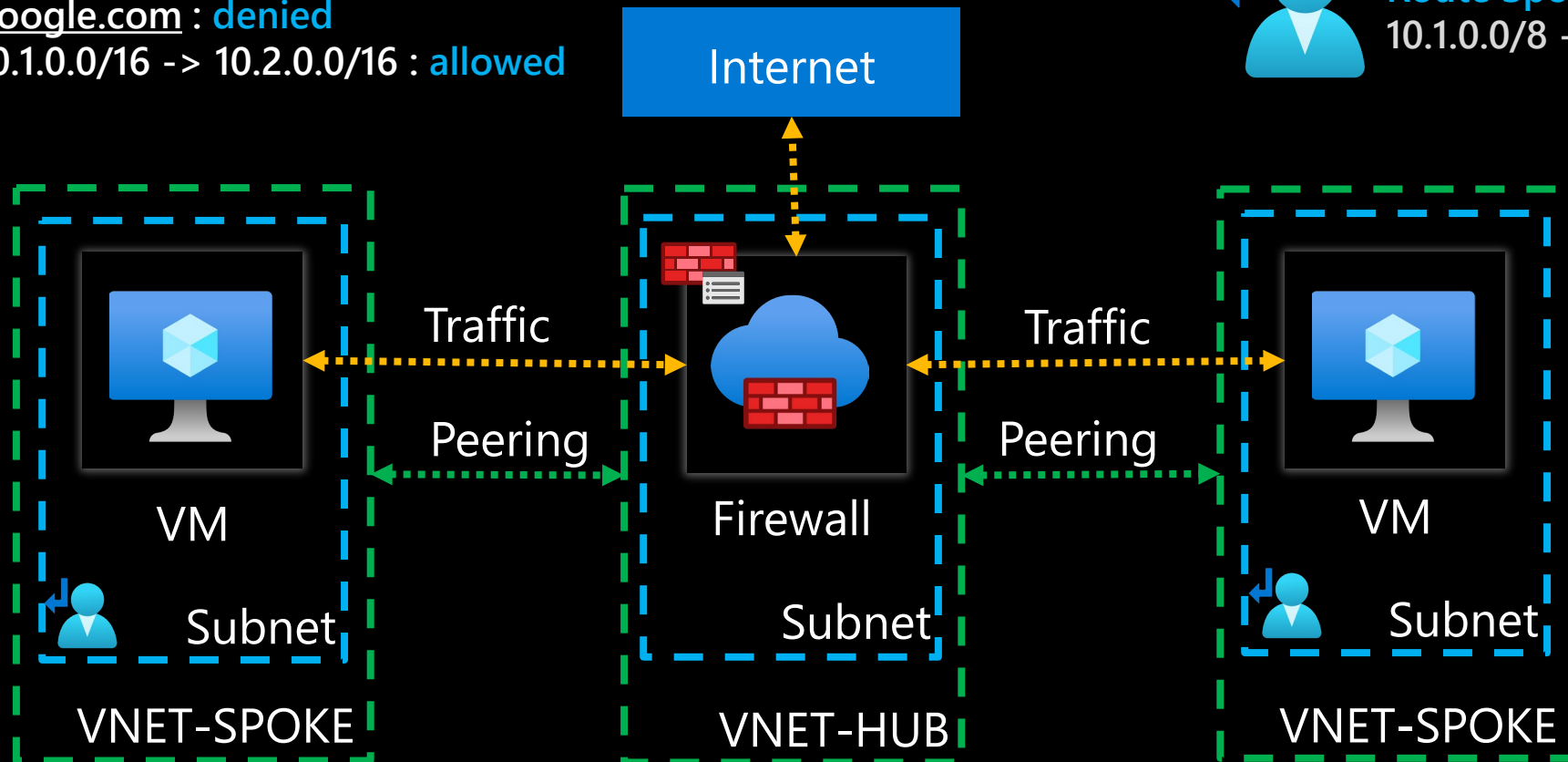
Azure Firewall Policy application rules



microsoft.com : **allowed**
google.com : **denied**
10.1.0.0/16 -> 10.2.0.0/16 : **allowed**



Route Spoke to Firewall
10.1.0.0/8 -> 172.16.0.4



Azure Firewall Policy network rules

Filter on Layer 3-4 (IP address, Port number, Protocol), like NSGs.

Example: allow communication between spokes.

Name

allow-spokes-traffic

Rule collection type

Network

Priority *

500

Rule collection action

Allow

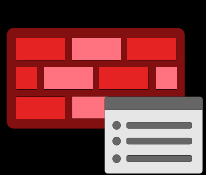
Rule collection group *

policy-group-allow

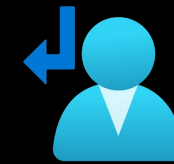
Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
allow-spoke1-to-sp...	IP Address	10.1.0.0/16	4 selected	*	IP Address	10.2.0.0/16
allow-spoke2-to-sp...	IP Address	10.2.0.0/16	TCP,UDP,ICMP,Any	*	IP Address	10.1.0.0/16
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	Service Tag	*,10.0.0.1,10.1.0.0/1...

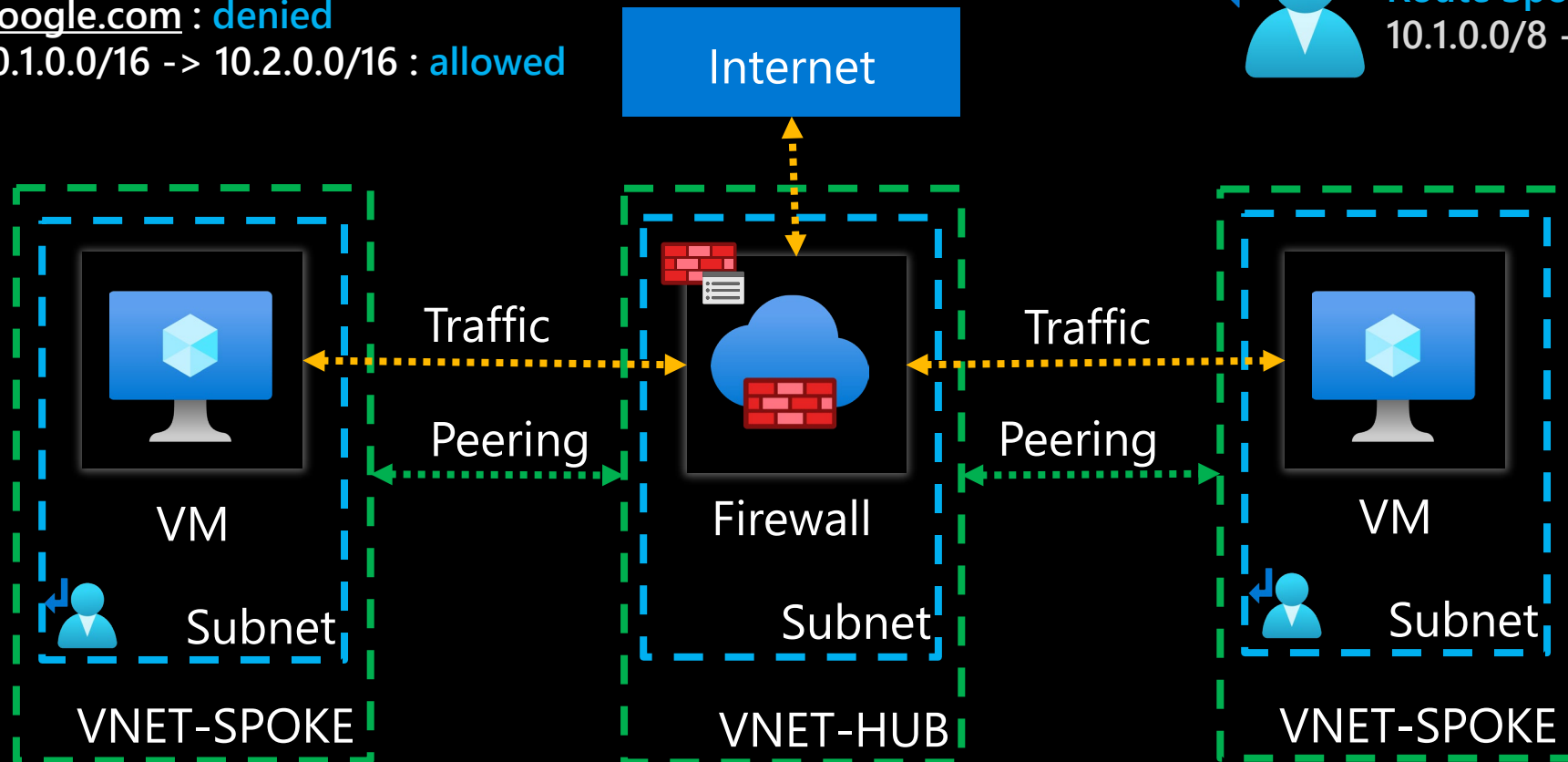
Azure Firewall Policy network rules



microsoft.com : **allowed**
google.com : **denied**
10.1.0.0/16 -> 10.2.0.0/16 : **allowed**



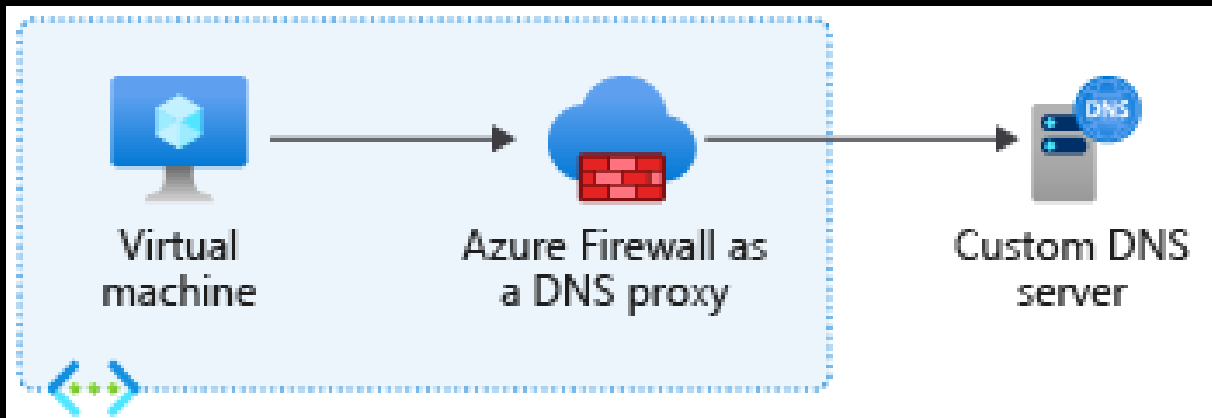
Route Spoke to Firewall
10.1.0.0/8 -> 172.16.0.4



Azure Firewall DNS Proxy

Could be a DNS proxy.

Could use Custom DNS Server.



learn.microsoft.com/en-us/azure/firewall/dns-settings

firewall-policy | DNS ☆ ...
Firewall Policy

Search

Settings

- Parent policy
- Rule collections
- DNAT rules
- Network rules
- Application rules
- DNS**
- Threat Intelligence
- TLS inspection
- IDPS
- Secured virtual hubs
- Secured virtual networks

☐ Disabled
This feature will not be enabled on your Azure Firewall Policy

☒ Enabled
DNS settings will be applied on the policy

DNS Servers

☐ Default (Azure provided)

☒ Custom

Custom DNS serv...

168.63.129.16	⋮
<input type="text" value="168.63.129.16"/>	

DNS Proxy

☐ Disabled

☒ Enabled

vnet-spoke1 | DNS servers ☆ ...
Virtual network

Search

DNS servers

- Firewall
- Microsoft Defender for Cloud
- Network manager
- DNS servers**
- Peerings
- Service endpoints

DNS servers ⓘ

☐ Default (Azure-provided)

☒ Custom

IP Address

172.16.0.4	⋮
<input type="text" value="Add DNS server"/>	

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

Firewall providers

Azure Firewall

Palo Alto Firewall

F5 Firewall

Barracuda CloudGen Firewall

Fortinet Fortigate

Aviatrix

Zscaler

The screenshot displays the Azure Marketplace interface for finding firewall solutions. The top navigation bar includes the Microsoft logo, 'Azure Marketplace', and a search bar. A left-hand sidebar lists various categories, with 'Networking >' expanded to show sub-categories like 'Featured', 'Appliance Managers', 'Connectivity', 'Firewalls', 'Load Balancers', 'Private MEC', 'All', 'Security', and 'Storage'. The main content area features filters for 'Trials' (All), 'Operating System' (All), 'Publisher' (Partners), 'Pricing Model' (All), and 'Product Type' (All). Below these filters, the text 'All results' is shown. Eight product cards are displayed in a grid:

- msh-managed_vwan** (By Azure Marketplace): Includes a 'Get it now' button and a heart icon.
- SonicWall NSv (Firewall/Security/VPN/...)** (By SonicWall Inc.): Features a 4-star rating and a 'Price varies' note. Includes a 'Get it now' button and a heart icon.
- F5 BIG-IP Virtual Edition - BETTER (PAYG)** (By F5, Inc.): Lists features like 'Advanced Load Balancing, GSLB, DNS & Network Firewall'. Includes a 'Free software trial' button and a heart icon.
- Barracuda CloudGen Firewall and SD-WAN fo...** (By Barracuda Networks, Inc.): Includes a 'Bring your own license' button and a heart icon.
- Fortinet FortiGate Next-Generation Firewall (VM)** (By Fortinet): Features a 5-star rating and a 'Starts at \$0.36/hour' price. Includes a 'Free software trial' button and a heart icon.
- CyberControl** (By Ness Israel): Includes a 'Get it now' button and a heart icon.
- ManageEngine OpManager - Professio...** (By ManageEngine): Includes a 'Get it now' button and a heart icon.
- Microsoft Azure Managed Services & Compliance f...** (By Computer Systems Integration Ltd): Includes a 'Get it now' button and a heart icon.

Azure Firewall - pricing

	Basic	Standard	Premium
Deployment per hour	\$0.395	\$1.25	\$1.75
Data Processing per GB	\$0.065	\$0.016	\$0.016
Deployment per month	\$ 284	\$ 900	\$1260

<https://azure.microsoft.com/en-us/pricing/details/azure-firewall/>