**Azure Firewall Rules, NAT behaviours, Concepts and Integration with Azure Firewall Manager.**

In today's cloud-centric world, The Azure Firewall is a cloud -based and intelligent network security utility that protects Azure Virtual Network resources from known and unknown threats. It is a stateful firewall that always keeps track of the state of network connections. Azure Firewall provides east-west and north-south traffic inspection. Coming to Network Address Translation function, Azure Firewall will perform both inbound and outbound NAT, it’s a way to map multiple private addresses inside a local network to a public IP address before transferring the data onto the internet.

In this blog, we will take a methodical approach and understand how to:

1. Azure Firewall rule processing logic by using firewall policy.
2. DNAT rules NAT behaviour.
3. Network rules NAT behaviour.
4. Application rules NAT behaviour.
5. Azure Firewall premium features.
6. Integration with Azure Firewall Manager.

**1. Rule processing logic**:

With Firewall Policy, rules are organized inside Rule Collections and Rule Collection Groups. Each rule collection group can have zero or multiple rule collection types. Either it is DNAT rule collections, Network rule collections or Application rule collections. Each rule collection type must have its own type (NAT, Network, or Application).

Azure Firewall rules are processed based on priority defined by admin as shown in below figure. Priority is any number between 100 (highest priority) to 65,000 (lowest priority). First azure firewall gives the priority to rule collection groups which are inherited from parent policy. Next, regardless of the priority of rule collections, Azure Firewall will systematically handle DNAT rules, Network rules, and Application rules in that order.

Example:A close up of a sign

Description automatically generated

Rule processing order -

DNAT Rule Collection(Priority – 1000),DNAT Rule Collection(Priority -5000),ch DNAT Rule Collection(Priority – 12000), ch DNAT Rule Collection(Priority – 9000), Network Rule Collection(Priority – 2000), Network Rule Collection(Priority – 4000), Network Rule Collection(Priority – 7000), ch Network Rule Collection(Priority – 14000), ch Network Rule Collection(Priority – 8000), Application Rule Collection(Priority – 3000), Application Rule Collection (Priority – 6000), ch Application Rule Collection(Priority – 13000), ch Application Rule Collection(Priority – 10000).

**2.NAT behaviour through DNAT rules:**

Azure Firewall uses DNAT rules from DNAT rule collection group to filter and forward inbound Internet traffic to azure virtual networks by translating firewall’s Public IP to the private IP address of resources inside virtual networks. When flow hits the DNAT rule, Incoming source IP will be translated into one of the IP addresses of *Azurefirewallsubnet* and destination IP in incoming packet will be translated into what we mentioned in DNAT rule as a *Translated* *address*.

For example, from below screenshot client (Source) IP will be translated into one of the IP addresses of *Azurefirewallsubnet* and destination IP (Firewall public IP – 20.172.249.157) will be translated into *translated address* (10.0.0.68) of backed server.

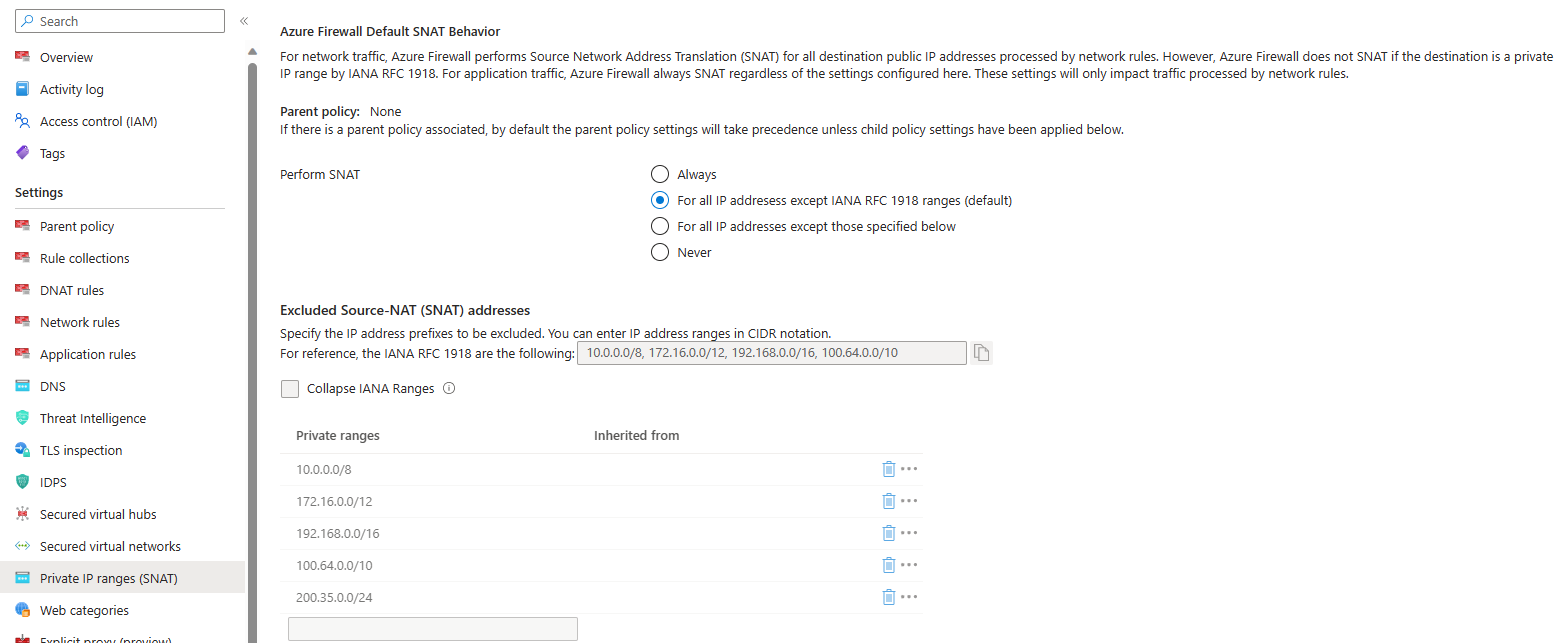
A screenshot of a computer

Description automatically generated

**3. NAT behaviour through Network rules:**

Network rules can allow or deny non-HTTP/S traffic through Azure Firewall based on source, destination, port and protocol (TCP, UDP and ICMP). When discussing the NAT behaviours of Azure Firewall via network rules, it depends on SNAT configuration by admin. There are four types of NAT behaviours as follows:

1. Configuring Azure Firewall to perform SNAT in all cases even though destination address is public IP or within the range of RFC 1918.
2. Configuring Azure Firewall to perform SNAT except the destination address is within the range of RFC 1918. (It is a default setting)
3. Configuring Azure Firewall to perform SNAT for all the IP ranges which are mentioned by admin.
4. Configuring Azure Firewall to not perform SNAT in any case.



**NOTE:**

* Azure Firewall perform SNAT and changes the source IP to one of the IP addresses of *Azurefirewallsubnet* within each-west traffic flow.
* Azure Firewall perform SNAT and changes the source IP to its public IP within north-south traffic flow.

**4.NAT behaviour through Application rules:**

Azure Firewall can filter HTTP/S traffic or SQL traffic through application rules. Azure Firewall always perform SNAT, when flow hits the application rule with ports HTTP, HTTPS or MYSQL. Incoming source IP will be NATed with azure firewall public IP and destination will be translated to *Translated* *address* which mentioned in NAT rule. In both HTTP and TLS inspected HTTPS cases, the firewall ignores the packet's destination IP address and uses the DNS resolved IP address from the Host header.

**5. Azure Firewall premium feature:**

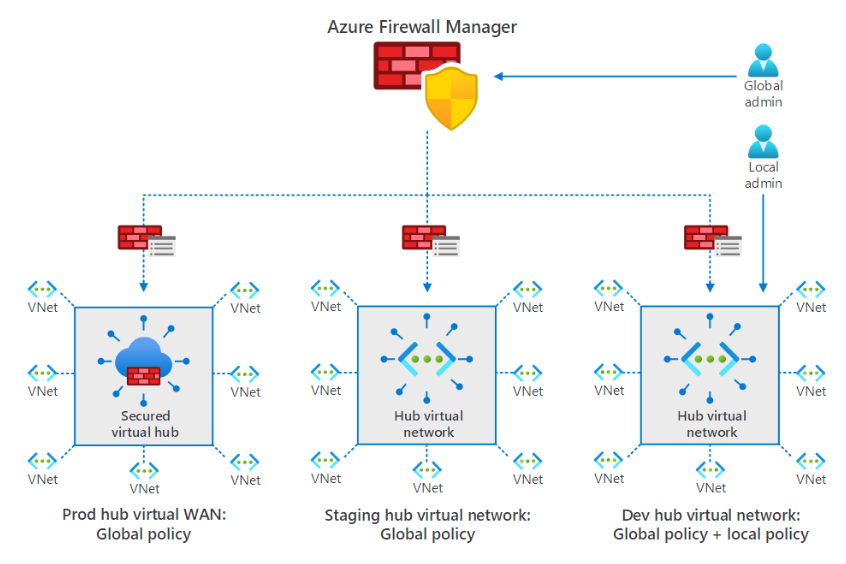
* **IDPS:** Azure Firewall uses signature-based detection for known threats. it will monitor inbound/outbound traffic from network layer to application layer, logs the sessions. It alerts when it finds suspicious traffic patterns and drops the packets based on custom settings. It automatically updates IDPS signatures to detect unknown malicious activities or zero-day attacks. The IDPS having over 67,000 signatures in around 50 categories to provide advanced threat protection for sensitive and regulated environments, like payment, healthcare and government sectors.

A screenshot of a computer

Description automatically generated

**6.Azure Firewall integration with Azure Firewall Manager:**

For example, you have more than 3 or 4 secured virtual networks with azure firewall distributed in all over the world, it is Exceedingly challenging to manage and allow same network, application and NAT rule in all the firewalls. Hence, Microsoft azure providing centralized security service tool for Hub and spoke model also for virtual WAN architecture.



To protect web applications from layer 7 attacks, we use WAF policy in front of application delivery platforms and to protect resources in virtual networks from layer 3&4 attacks, we configure DDoS protection. By using Azure Firewall Manager, we can manage and associate the WAF policies at scale in required application delivery platforms like Azure FrontDoor and Application Gateway.

Key Features:

1. Centralized management.
2. Simplified security operations.
3. Enhansed visibility and Monitoring.
4. Hierarchical policy approach.

**Conclusion:**

As mentioned, Azure firewall’s granular control through application FQDN tagging and threat intelligence helps business in safeguarding against evolving cyber threats. you can find potential network issues Based on incoming/outgoing traffic’s NAT behaviour.

Moreover, by using Azure Firewall manager we can configure and monitor security policies with single click. The scalability and flexibility help wide range of deployment scenarios, from small businesses to large enterprises.