Book of Network Services - Flow Network Security

[PDF generated May 09 2022. For all recent updates please see the Nutanix Bible releases notes located at https://nutanixbible.com/release_notes.html. Disclaimer: Downloaded PDFs may not always contain the latest information.]

Flow Network Security is a distributed, stateful firewall that enables granular network monitoring and enforcement between VMs running on the AHV platform as well as external entities they communicate with.

Supported Configurations

The solution is applicable to the configurations below:

Core Use Case(s):

- Microsegmentation

Management interfaces(s):

- Prism Central (PC)

Supported Environment(s):

- On-Premises:
  - AHV
- Cloud:
  - Nutanix Cloud Clusters on AWS

Upgrades:

- Included in LCM as Flow

Compatible Features:

- Service Chaining
- Security Central
- Calm

Flow Network Security configuration is done via Prism Central by defining policies and assigning categories to VMs. Prism Central can define the security policies and categories of many connected AHV clusters in one place. Each AHV host implements the rules using OVS and OpenFlow as required for distributed enforcement.

Implementation Constructs

Within Flow Network Security, there are a few key constructs:

Categories

Categories are simple text key value pairs used to define groups of VMs that policies are applied to. Typical categories are environment, application type, and application tier. Any key and value tag that is helpful to identify a VM can be used as a category, but some categories such as AppType and AppTier are required for application security policies.

- Category: "Key: Value" or Tag
- Examples Keys: AppType, AppTier, Group, Location

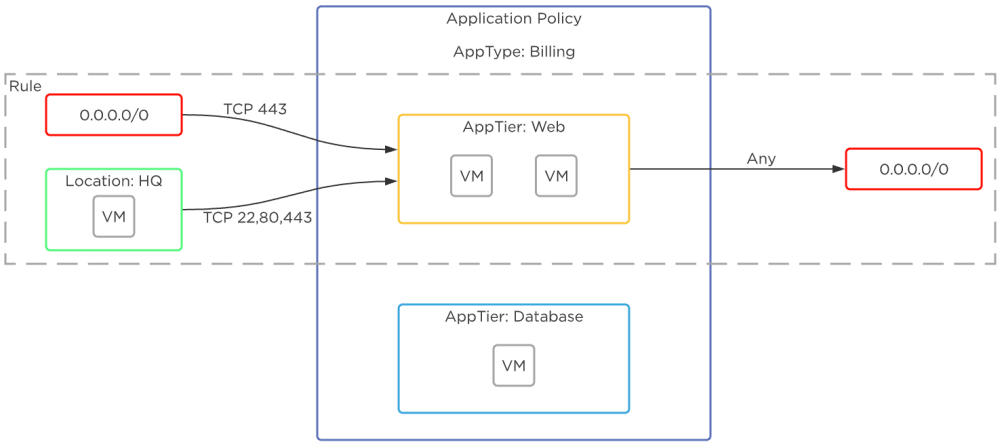
For example, a VM providing production database services may have the following assigned categories:

- AppTier: Database
- AppType: Billing
- Environment: Production

These categories can then be leveraged by security policies to determine what rules or actions to apply. Categories aren't only for Flow Network Security, you can also use these same categories for protection policies.

Security Policies

Security policies are made of defined rules that determine what is allowed between a source and a destination. A rule inside an application policy includes all the inbound and outbound traffic for a specific application tier. A single rule can include multiple sources and multiple destinations. In the following example, there is one single defined rule for AppTier: Web. If we added allowed traffic to and from AppTier: Database, there would then be two rules.



Flow Network Security - Rules

There are a few types of security policies, and they're evaluated in the following order:

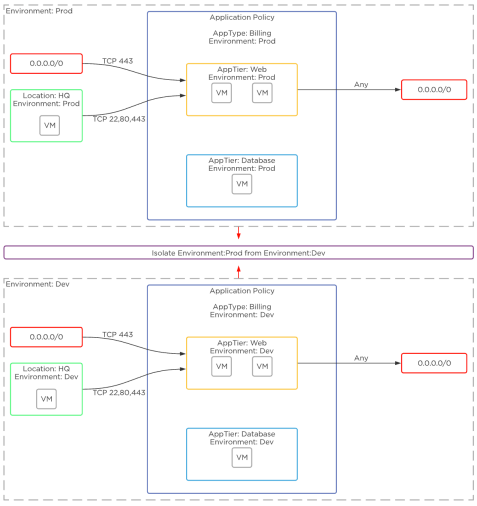
- Quarantine Policy
  - Deny All traffic for specified VM(s): Strict
  - Deny All traffic except specific traffic for investigation: Forensic
  - Example 1: VMs A,B,C infected with a virus, isolate them to stop the virus from further infecting the network
  - Example 2: VMs A,B,C infected. Quarantine them but allow security team to connect to the VMs for analysis

- Isolation Policy
  - Deny traffic between two categories, allow traffic within category
  - Example: separate tenant A from tenant B, clone environment and allow to run in parallel without affecting normal network communication.

- Application Policy
  - This is your common 5-tuple rule allowing you to define what transport (TCP/UDP), Port, and source/destination is allowed.
  - Allow Transport: Port(s) To,From
  - Example: Allow TCP 443 from VMs with category Location:HQ to VMs with category AppTier:Web

- VDI Policy
  - Identity based firewall to apply a category to a VDI VM based on the AD Groups of the logged in user.
  - Implement policy based on the assigned AD groups

The following shows an example utilizing Flow Network Security to control traffic in a sample application:



Flow Network Security - Example Application

Policy State

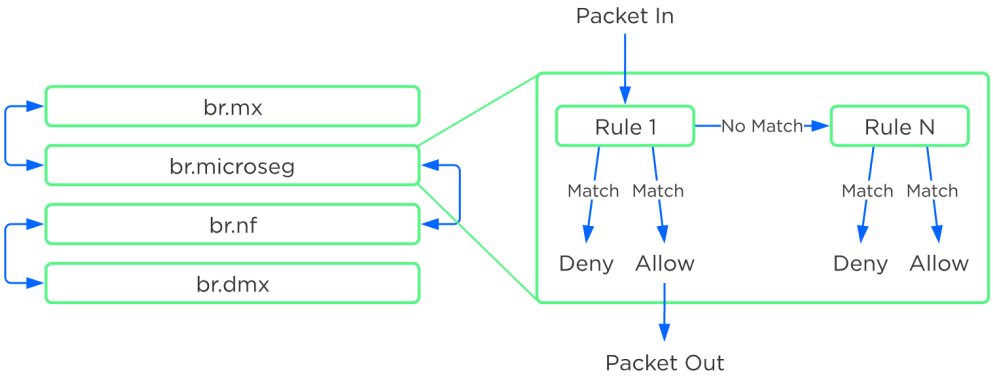
The policy state determines what action is taken when a rule is matched. With Flow Network Security there are two main states:

- Enforce
  - Enforce the policy by allowing only defined flows and dropping all others.

- Monitor
  - Allow all flows, but highlight any packets that would have violated the policy in the policy visualization page.

Rule Enforcement

Flow Network Security policies are applied to a packet once it leaves the UVM, and before it gets to any other VM. This occurs in the microsegmentation bridge (br.microseg) on the AHV host.



Flow Network Security - Rule Order Overview

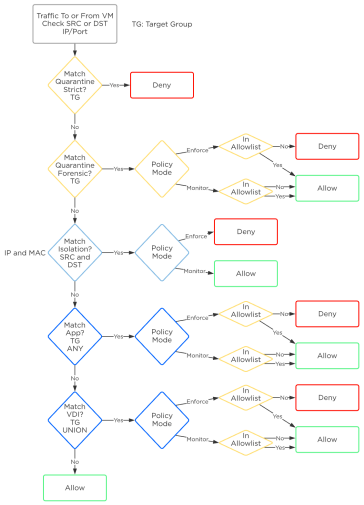
Policies are built based on categories, but rule enforcement happens based on the detected VM IP address. The job of Flow Network Security is to evaluate the categories and policies assigned to all the VMs, and then program the right rules into the br.microseg bridge on the host or hosts where protected VMs run. VMs that use Nutanix AHV IPAM have a known IP address as soon as their NIC is provisioned and the rules are programmed when the VM is powered on. The Nutanix Acropolis process intercepts DHCP and ARP messages to detect the IP address of any VM with static IPs or external DHCP. For these VMs, rules are enforced as soon as the VM IP is known.

Rule evaluation for Quarantine, Application, and VDI policies is based on the detected IPv4 address.

Rule evaluation for Isolation policies is based on both the IPv4 address and the VM MAC address.

Evaluation order is on a first-match basis in the following order.

- Quarantine
- Isolation
- Application
- VDI



Flow Network Security - Policy Order

The first policy matched has the action taken, and all further processing stops. For example, if traffic encounters an Isolation policy that is in monitor mode, the action taken is to forward the traffic and log it as allowed and monitored. No further rules are evaluated, even if an Application or VDI policy further down the list would have blocked this traffic.

Further, VMs can belong to only one AppType category and on AppType category can be in the target group of only a single AppType policy. This means that any VM can only belong in the target group of one AppType policy. All traffic into and out of the VM must be defined in this single AppType policy. There is currently no concept of a VM being at the center of multiple Application policies, and therefore no conflict or evaluation order happens between Application policies.