# Book of Network Services - Flow (Microsegmentation)



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

## Supported Configurations

The solution is applicable to the configurations below (list may be incomplete, refer to documentation for a fully supported list):

Core Use Case(s):

- Microsegmentation

Management interfaces(s):

- Prism Central (PC)

Supported Environment(s):

- On-Premise:
  - AHV (As of AOS 5.10)
- Cloud: +

Upgrades:

- Part of AOS

Compatible Features:

- Service Chaining
- Calm
- Epoch

The configuration is done via Prism Central by defining policies and assigning to categories. This allows the configuration to be done in a central place and pushed to many Nutanix clusters. Each AHV host implements the rules using OpenFlow.

## Implementation Constructs

Within Nutanix Flow, there are a few key constructs:

## Category

Categories are used to define groups of entities which policies and enforcement are applied to. They typically apply, but are not limited to: environment, application type, application tier, etc.

- Category: Key/Value "Tag"
- Examples: app | tier | group | location | subnet | etc.

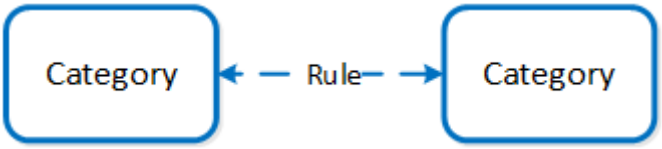
For example, a VM providing production database services may have the following assigned categories:

- AppTier: Database
- AppType: MySQL
- Environment: Production

These categories can then be leveraged by policies to determine what rules / actions to apply (also leveraged outside of the Flow context).

## Security Rule

Security rule(s) are the defined rules and determine what is allowed between defined categories.

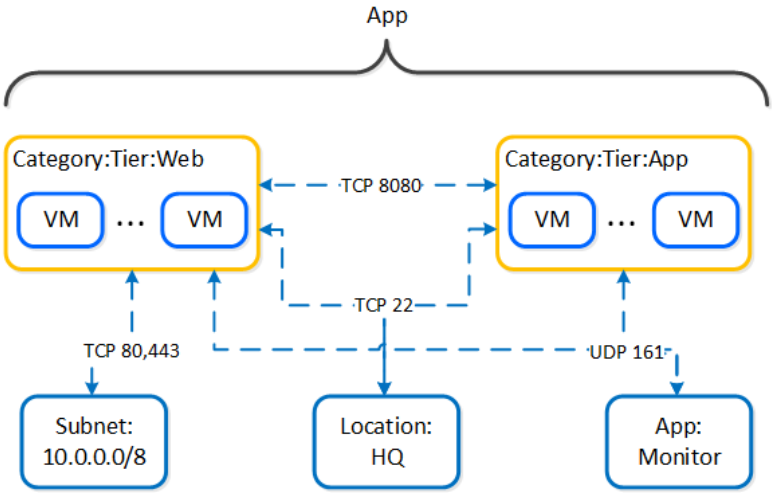



Flow - Microsegmentation - Rules

There are a few types of security rules:

- App Rule
  - This is your common rule allowing you to define what transport (TCP/UDP), Port, and source/destination is allowed/denied.
  - [Allow|Deny] Transport: Port(s) [To|From]
  - Example: Allow TCP 8080 from Category:Tier:Web to Category:Tier:App
- Isolation Rule
  - Deny traffic between two categories, allow traffic within category
  - Example: seperate tenant A from tenant B, clone environment and allow to run in parallel without affecting normal network communication.
- Quarantine Rule
  - Deny All traffic for specified VM(s)/categories
  - Example: VMs A,B,C infected with a virus, isolate them to stop the virus from further infecting the network

The following shows an example utilizing Flow - Microsegmentation to control traffic in a sample application:




Flow - Microsegmentation - Example Application

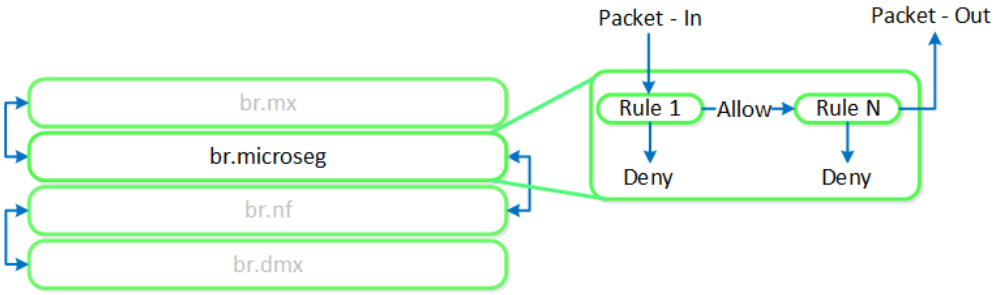
## Enforcement

Enforcement determines what action is taken when a rule is matched. With AHV Flow - Microsegmentation there are two types of enforcement:

- Apply
  - Enforce the policy by allowing 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.

Flow - Microsegmentation rules are the first applied to a packet once it leaves the UVM. This occurs in the microsegmentation bridge (br.microseg):




Flow - Microsegmentation - Flow