Network Services - Flow Network Security

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 applies 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

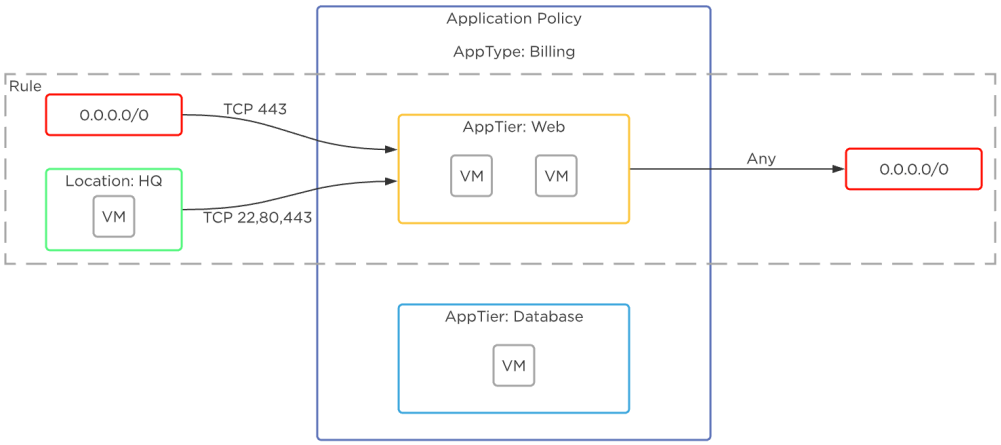
For example, a VM providing production database services may have the following assigned categories:

- 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:

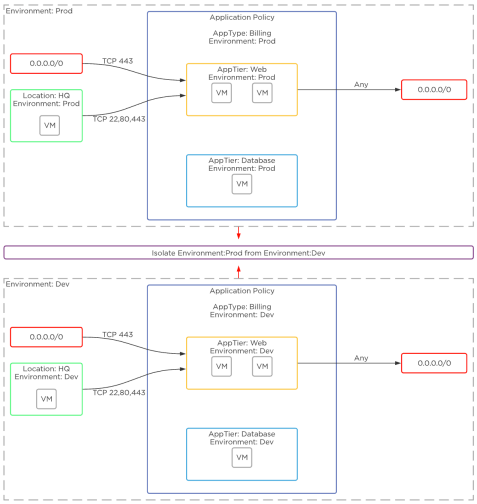
- Quarantine Policy
  - Deny All traffic for specified VM(s): Strict
  - Deny All traffic except specific traffic for investigation: Forensic
  - Example 1: VMs A,B,C infected with a virus, isolate them to stop the virus from further infecting the network
  - Example 2: VMs A,B,C infected. Quarantine 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 using Flow Network Security to control traffic in a sample application:



Flow Network Security - Example Application

Policy State

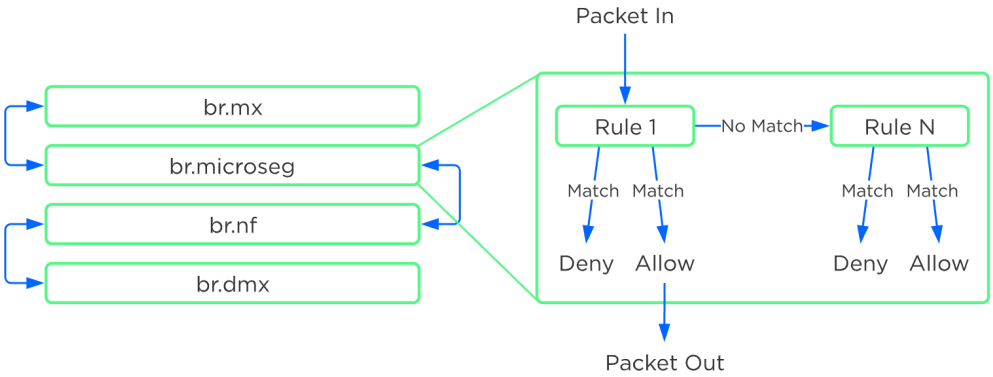
The policy state determines what action is taken when a rule is matched. With Flow Network Security there are two main states:

- 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

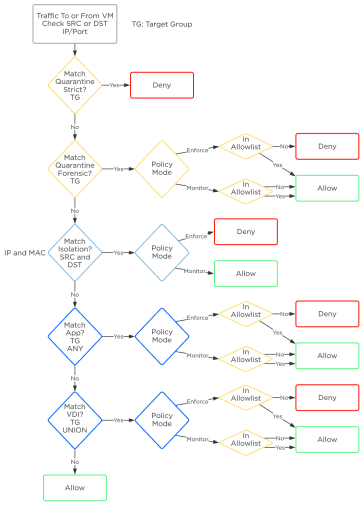
Policies are built based on categories, but rule enforcement happens based on the detected VM IP address. The job of Flow Network Security is to evaluate the categories and policies assigned to all the VMs, and then program the right rules into the br.microseg bridge on the host or hosts where protected 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.

Flow Network Security Next-Generation

Flow Network Security Next-Gen (FNS NG) provides a new security policy model that improves security policy flexibility and scalability while enabling new capabilities not found in previous versions of Flow Network Security. Enhancements made to the networking stack with the network controller, allow Nutanix to introduce the next-generation policy model for Flow Network Security.

Supported Configurations

The solution applies to the configurations below:

Core Use Case(s):

- Microsegmentation for network controller-enabled VLAN subnets
- Microsegmentation in VPC overlay subnets

Management interfaces(s):

- Prism Central (PC)

Supported Environment(s):

- On-Premises:
  - AHV

Prerequisites:

- Nutanix network controller enabled
- Protected entities must use network controller-enabled VLAN subnets or VPC overlay subnets

Upgrades:

- Included in LCM as Flow Network Security 4.0.1

Compatible Features:

- Security Central
- Calm

Flow Network Security Next-Gen 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. Prism Central and the network controller implement the configured security rules on the virtual switch of each AHV host.

Implementation Constructs

Within FNS NG, there are a few key constructs:

Categories

Categories are text key-value pairs used to define groups of VMs that policies are applied to. Traditional system-defined categories are environment, application type, and application tier. With FNS NG, administrators can create security policies using any system-defined or user-created categories to protect applications. This enhancement provides flexibility, allowing a user to define categories that align with their application constructs and naming conventions.

- Category: "Key: Value" or Tag
- Examples System defined Keys: AppType, AppTier, Group, Location
- Examples User Defined Keys: AccessType, Service, Team

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

- AppTier: Database
- AppType: Billing
- Environment: Production
- AccessType: SecureAdmin
- Service: Monitor

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.

FNS NG Security Policies

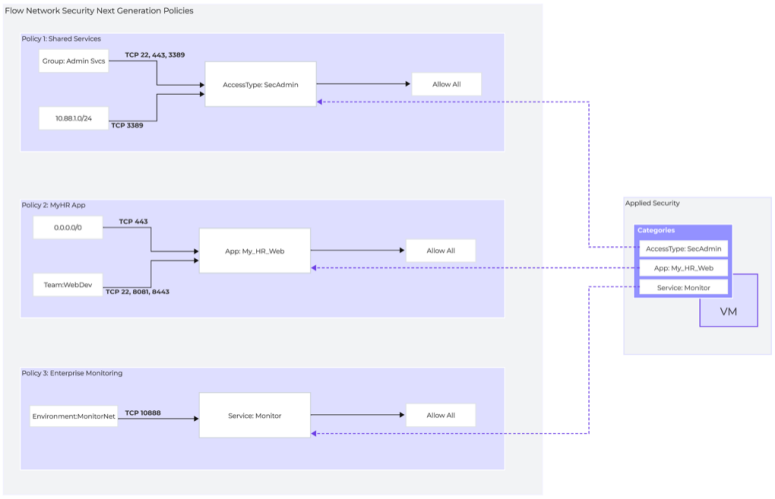
Security policies are constructed of defined rules that determine what is allowed between a source and a destination. A rule inside an application policy includes all the inbound and outbound traffic for specific secured entities. A single rule can include multiple sources and multiple destinations. With FNS 4.0.1 and later, a VM can be a secured entity in multiple security policies, as opposed to requiring a VM to appear in only a single, monolithic policy in previous FNS versions. This allows users to create broader policies applied to a wide range of VMs to address requirements like shared services, monitoring, and even a default catch-all security policy, while still having a tightly focused security policy to protect applications. Using the multiple-policy approach streamlines security policy management, making it easier to update a policy when requirements or resources change.

For example, here’s how monolithic policies are used in the original FNS policy model. When an organization has 15 different applications to secure, each application has its own security policy for a total of 15 policies. Each of those application security policies contains rules specific to the requirements of the protected application. There are additional rules within each policy to secure VM management access and system monitoring. In this example, a change to the monitoring platform or the method used to monitor the component VMs of an application would require a change to each security policy. There are 15 security policies that would need to be updated. Each policy change increases the risk of a configuration error that could introduce an unwanted security exposure. Applying multiple security policies to a VM helps reduce or eliminate this risk.

Policy Interaction

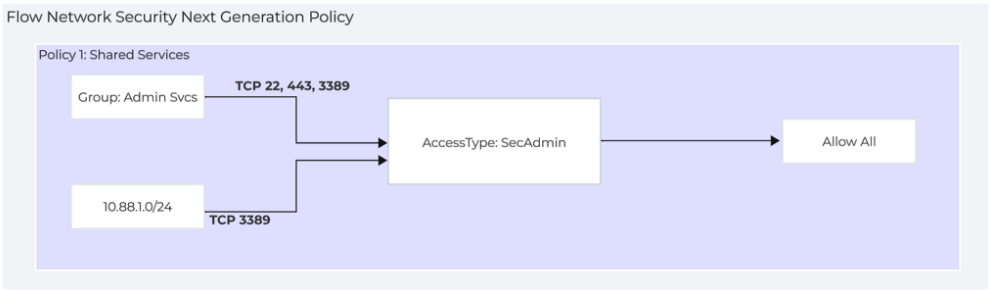
Let's investigate the multiple combined policy capabilities in FNS NG. Using the same example scenario previously mentioned, the applications are each protected with security policies specific to the requirements of the application, these are now 15 specific policies. In addition, the component VMs that make up the application could have a security policy applied that addresses management access and another security policy used for monitoring. With this method, a change to the monitoring platform or the method used to monitor the component VMs of an application would only require an update to the security policy that is used to restrict monitoring access. This is a change to only one security policy, monitoring, leaving the 15 security policies for the applications unaltered.

In the following example, we have a VM that is a secured entity in three separate security policies, Shared Services, MyHR App, and Enterprise Monitoring. It's important to note that this same VM is protected with three separate categories. A single category can't appear as a security entity in multiple policies.



Flow Network Security Next Generation - Security Policies

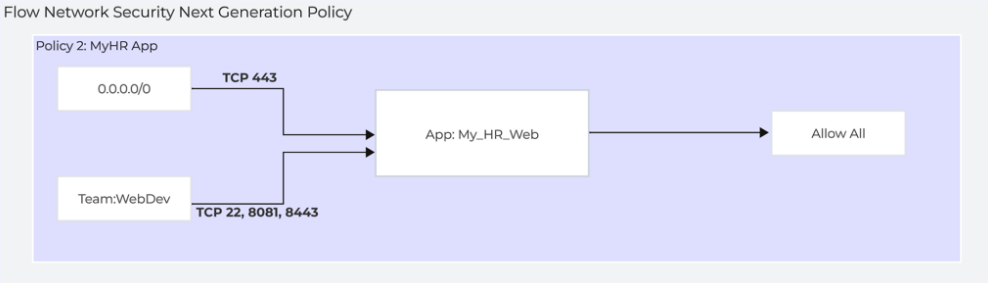
Policy 1: Shared Services



Flow Network Security Next Generation - Policy 1: Shared Services

This example Shared Services policy is used to permit secure administrative access to VMs that are in the category AccessType:SecAdmin This policy can be applied to multiple VMs and used as a default secure administrative access policy.

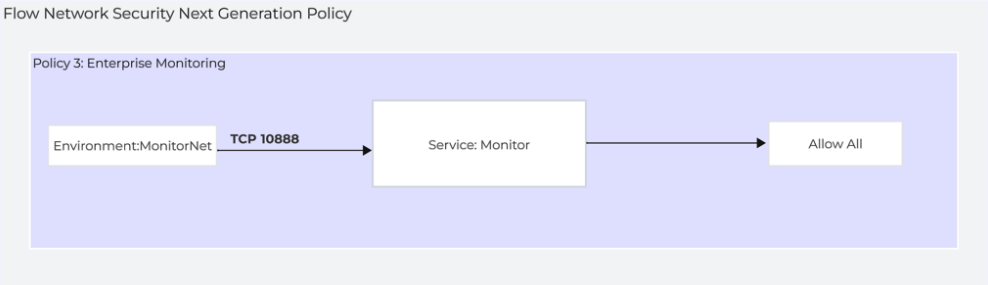
Policy 2: MyHR App



Flow Network Security Next Generation - Policy 2: MyHR App

The example MyHR App policy is used to restrict access to a specific application. VMs in the category App: HR_Web are protected by this policy.

Policy 3: Enterprise Monitoring



Flow Network Security Next Generation - Policy 3: Enterprise Monitoring

The Enterprise Monitoring policy is used to restrict application monitoring services to a specific source group. This is a good example of a policy that can be applied to many VMs independent of the application they are a part of. This could be a good default policy for new applications.

Security Policy Management

FNS NG introduces new policy mode constructs to enhance policy management. These additions streamline the task of administration at scale by making it easy to create new policies from templates or existing policies.

Security Policy Management options:

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

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

- Save
  - The save option allows you to create a policy and make changes without applying the policy. This is helpful as information and requirements for the policy are being defined. You can create the policy and iterate changes as you solidify requirements. In this mode, the policy is saved in a draft state.

- Clone
  - The clone option allows administrators to make a copy of an existing security policy. With this functionality, users can create a security policy with configured default security rules, and then save the policy to be used as a template for new application policies. Any time there is a new application that needs to be secured, users can clone the saved template policy and then update the secured entities of the policy to reflect the requirements of the application. This is a good method for maintaining the default security rules required for all apps.