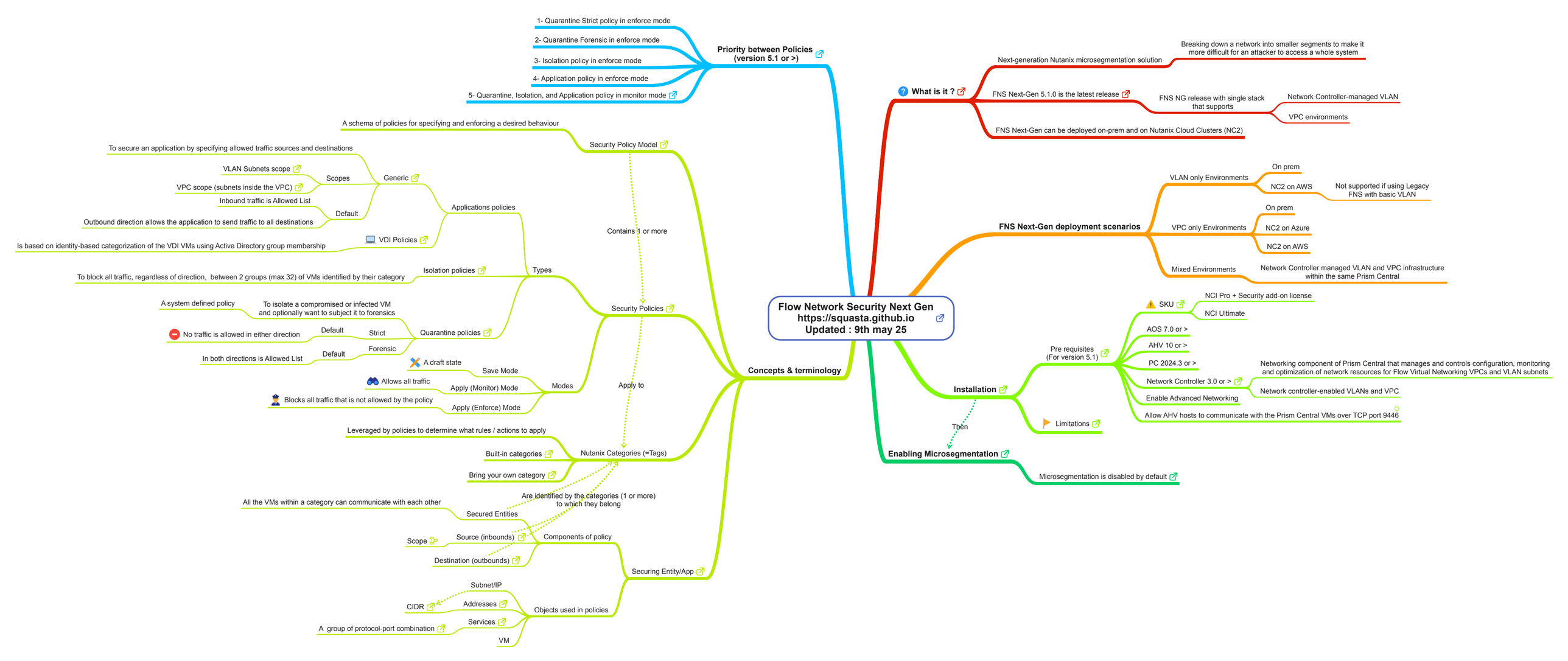
Flow Network Security Next Gen
https://squasta.github.io
Updated : 9th may 25
What is it ?
Next-generation Nutanix microsegmentation solution
Breaking down a network into smaller segments to make it more difficult for an attacker to access a whole system
FNS Next-Gen 5.1.0 is the latest release
FNS NG release with single stack that supports
Network Controller-managed VLAN
VPC environments
FNS Next-Gen can be deployed on-prem and on Nutanix Cloud Clusters (NC2)
FNS Next-Gen deployment scenarios
VLAN only Environments
On prem
NC2 on AWS
Not supported if using Legacy FNS with basic VLAN
VPC only Environments
On prem
NC2 on Azure
NC2 on AWS
Mixed Environments
Network Controller managed VLAN and VPC infrastructure within the same Prism Central
Installation
Pre requisites (For version 5.1)
SKU
NCI Pro + Security add-on license
NCI Ultimate
AOS 7.0 or >
AHV 10 or >
PC 2024.3 or >
Network Controller 3.0 or >
Networking component of Prism Central that manages and controls configuration, monitoring and optimization of network resources for Flow Virtual Networking VPCs and VLAN subnets
Network controller-enabled VLANs and VPC
Enable Advanced Networking
Allow AHV hosts to communicate with the Prism Central VMs over TCP port 9446
Limitations
Then
Enabling Microsegmentation
Microsegmentation is disabled by default
Concepts & terminology
Priority between Policies (version 5.1 or >)
1- Quarantine Strict policy in enforce mode
2- Quarantine Forensic in enforce mode
3- Isolation policy in enforce mode
4- Application policy in enforce mode
5- Quarantine, Isolation, and Application policy in monitor mode
Security Policy Model
A schema of policies for specifying and enforcing a desired behaviour
Contains 1 or more
Security Policies
Types
Applications policies
Generic
To secure an application by specifying allowed traffic sources and destinations
Scopes
VLAN Subnets scope
VPC scope (subnets inside the VPC)
Default
Inbound traffic is Allowed List
Outbound direction allows the application to send traffic to all destinations
VDI Policies
Is based on identity-based categorization of the VDI VMs using Active Directory group membership
Isolation policies
To block all traffic, regardless of direction, between 2 groups (max 32) of VMs identified by their category
Quarantine policies
A system defined policy
To isolate a compromised or infected VM and optionally want to subject it to forensics
No traffic is allowed in either direction
Default
Strict
In both directions is Allowed List
Default
Forensic
Modes
A draft state
Save Mode
Allows all traffic
Apply (Monitor) Mode
Blocks all traffic that is not allowed by the policy
Apply (Enforce) Mode
Apply to
Nutanix Categories (=Tags)
Leveraged by policies to determine what rules / actions to apply
Built-in categories
Bring your own category
Are identified by the categories (1 or more) to which they belong
Securing Entity/App
Components of policy
Secured Entities
All the VMs within a category can communicate with each other
Source (inbounds)
Scope
Destination (outbounds)
Objects used in policies
Subnet/IP
Addresses
CIDR
Services
A group of protocol-port combination
VM