UPAS Sensor Deployment: Network Environment Inspection and Configuration Guide

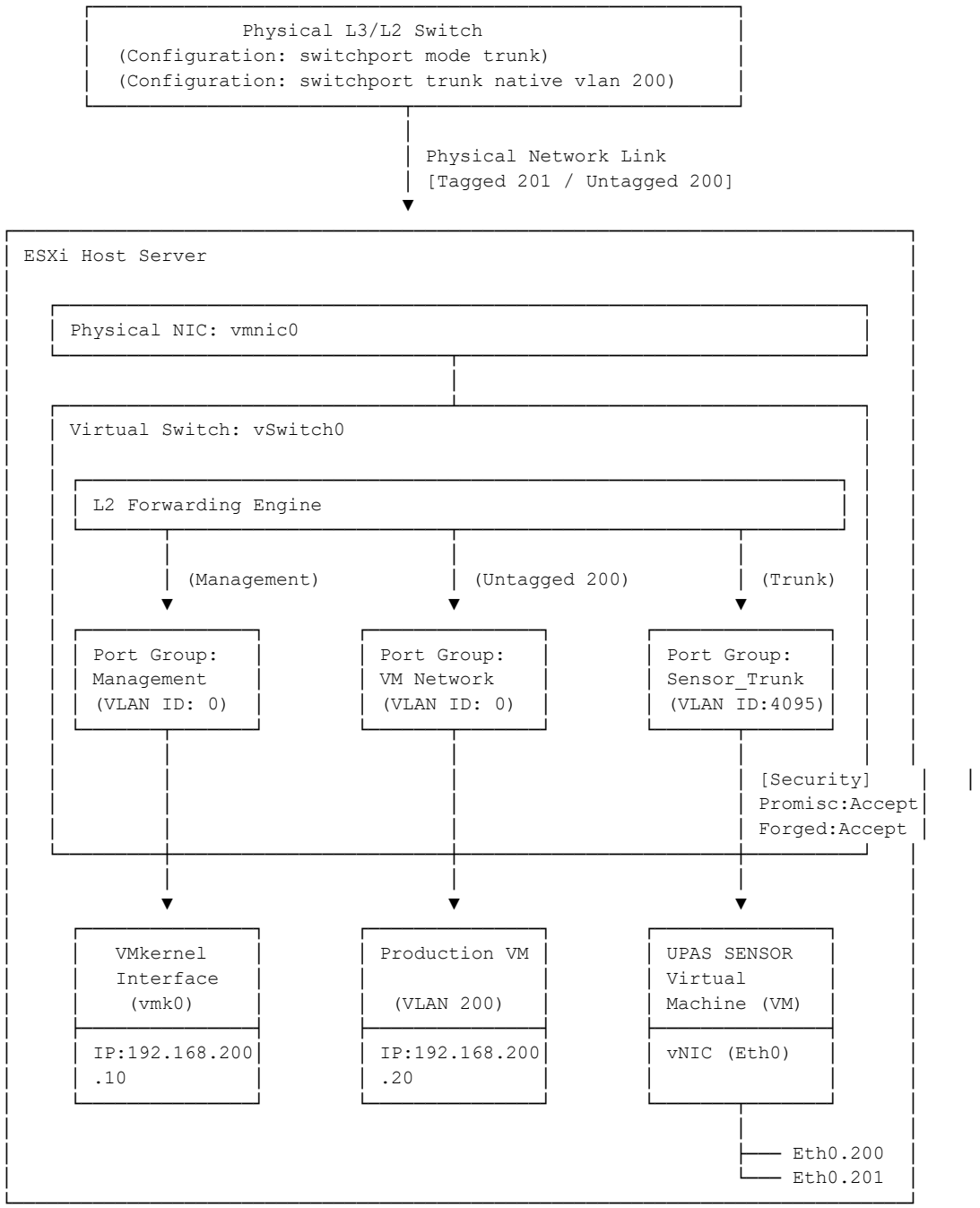
1. Objective and Scope

This document outlines the standard network deployment specifications for the UPAS Intranet Security Management System (Sensor module) within VMware vSphere (ESXi 7.0 / 8.0) virtualized environments.

To ensure the UPAS Sensor can successfully execute cross-VLAN endpoint security management via Layer 2 packet analysis and ARP blocking mechanisms, this guide provides instructions for configuring Trunk mode on physical switches and setting up VLAN 4095 passthrough and requisite security policies on ESXi virtual switches (vSwitch).

2. Network Architecture and Packet Flow Diagram

The following diagram illustrates the Layer 2 packet flow from the physical switch to the virtual machines within the ESXi host. To ensure zero downtime for the management network and existing production services, establishing a Native VLAN is mandatory when transitioning to Trunk mode.



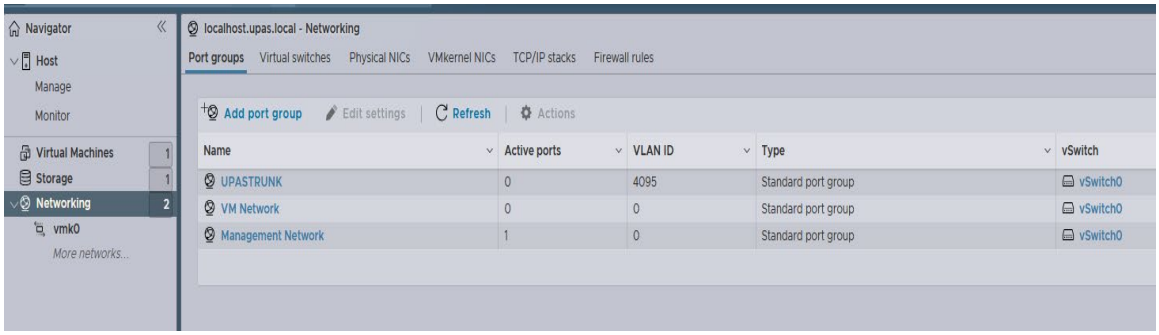
3. Current Network Environment Inspection Procedures

Before implementing network changes, verify the VLAN tagging status (Tagged/Untagged) of the ESXi management adapter (VMkernel) and existing production Port Groups.

3.1 Inspection via vSphere Client UI

1. Navigate to the Networking > Port groups tab.

2. Review the VLAN ID column: 0 indicates Untagged; 1~4094 indicates Tagged.



3.2 Inspection via ESXi CLI

Execute the following commands:

➤ esxcli network vswitch standard portgroup list

➤ esxcli network ip interface list

```
[root@localhost:~] esxcli network vswitch standard portgroup list
Name               Virtual Switch  Active Clients  VLAN ID
-----------------  --------------  --------------  -------
Management Network  vSwitch0                1        0
UPASTRUNK           vSwitch0                0     4095
VM Network          vSwitch0                0        0
[root@localhost:~] esxcli network ip interface list
vmk0
   Name: vmk0
   MAC Address: 00:0c:29:93:c6:50
   Enabled: true
   Portset: vSwitch0
   Portgroup: Management Network
   Netstack Instance: defaultTcpipStack
   VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1500
   TSO MSS: 65535
   RXDispQueue Size: 4
   Port ID: 67108870
```

4. Standard Configuration and Implementation Steps

Critical Notice: If the management and production networks are Untagged (VLAN ID 0), a Native VLAN MUST be declared on the physical switch when converting to Trunk mode to prevent service disconnection.

Step 1: Physical Switch Configuration

The existing untagged network (e.g., VLAN 200) must be configured as the Native VLAN.

(Cisco IOS Configuration Example)

interface GigabitEthernet0/5

switchport trunk encapsulation dot1q

switchport trunk native vlan 200

switchport mode trunk

spanning-tree portfast

Step 2: ESXi Virtual Switch (vSwitch) Configuration

1. Add a port group named Sensor_Trunk_4095 with VLAN ID 4095.

2. Expand the Security menu and manually set Promiscuous mode, MAC address changes, and Forged transmits to Accept.

Step 3: Sensor VM Network Attachment

Change the Network Label of the UPAS Sensor VM's adapter to Sensor_Trunk_4095. Power on the VM and configure the VLAN sub-interfaces within the OS.