Cisco TrustSec How-To Guide: Promiscuous Mode with VMware

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

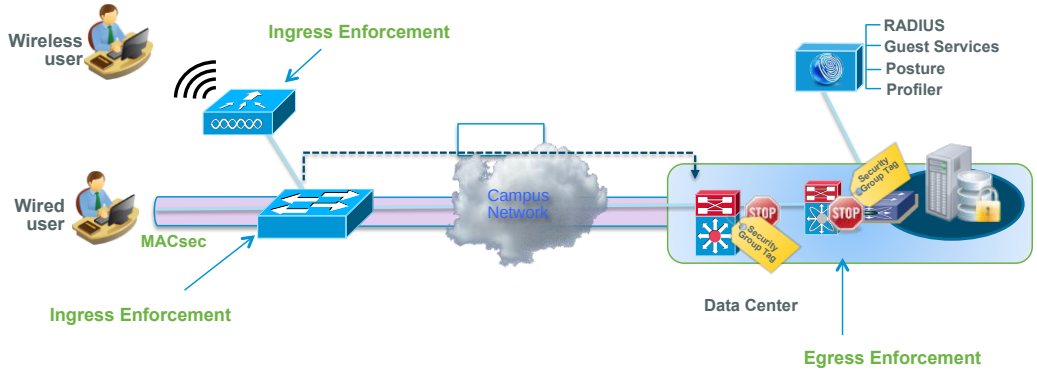
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

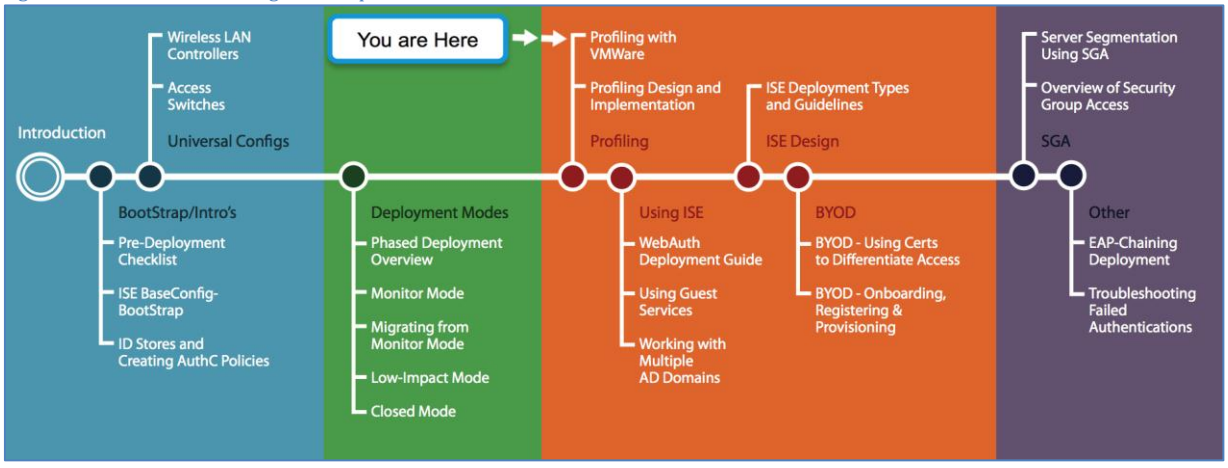


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "TrustSec certified". The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

VMware Deployments

Introduction

This How-To Guide explains how to enable device profiling probes using ISE on a VMware virtual machine (VM). It demonstrates the steps in configuring a Promiscuous VMware Network and to enable a Switched Port Analyzer (SPAN) session. The guide assumes you understand the requirements for installing Cisco Identity Services Engine (ISE) on a VMware VM and know how to configure both VMware ESX servers and other VMware servers. For the details on configuring ISE for a VMware deployment, please refer to the ISE 1.1 Hardware Installation Guide at http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html.

Note: Please refer to HowTo-04-ISE_Bootstrapping Guide for more information on enabling device profiling probes.

How to Configure a Promiscuous VMware Network

Procedure 1 Configure a Promiscuous VMware Network.

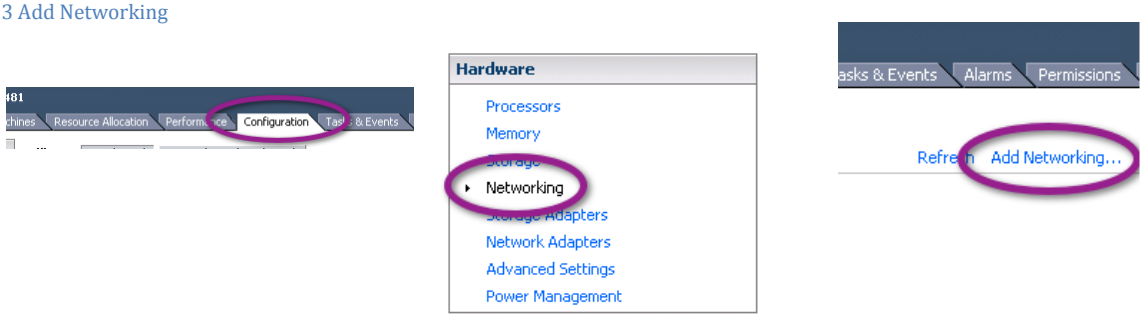
If Cisco ISE is deployed in a virtual environment, it is important to configure the VMware networking appropriately to allow a promiscuous interface to work properly. If Cisco ISE is deployed in a physical appliance form factor, skip to the section "Configure the SPAN Session on the Switch".

Use this procedure to configure and dedicate an interface on the VMware ESX server as a promiscuous interface. If the physical interface on the ESX server cannot be dedicated for SPAN, follow Procedure 2 later in this document.

Note: If deploying with VMware, pay close attention to the specs listed in the installation guide at http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html. Specifically, disk size can be a real concern. It can be catastrophic to a deployment if Cisco ISE is running in VMware with a lot of logged events and it runs out of disk space. Always follow the recommendations for VMware sizing.

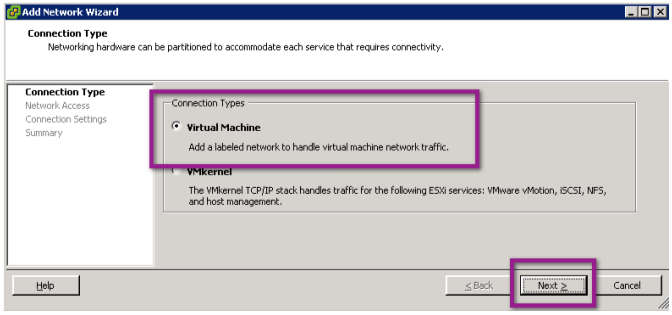
Step 1 Select the physical ESX server in VMware VSphere client. Select Configuration → Networking, and then select Add Networking (Figure 3).

Figure 3 Add Networking



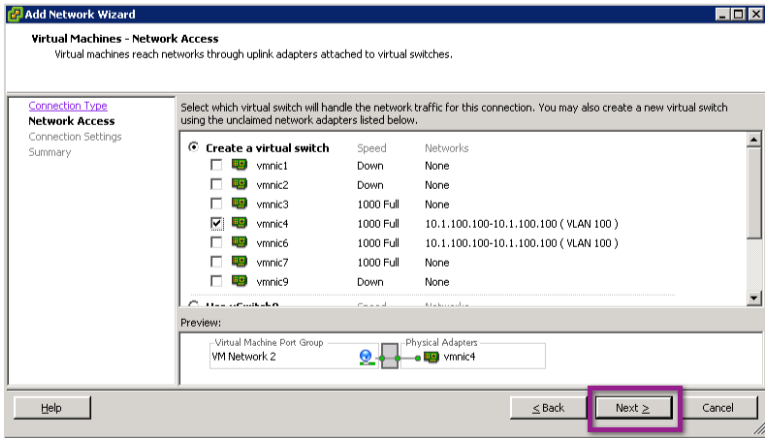
Step 2 The Add Network Wizard is launched. Under Connection Types, choose Virtual Machine, and click Next (Figure 4)

Figure 4 Add Network Wizard



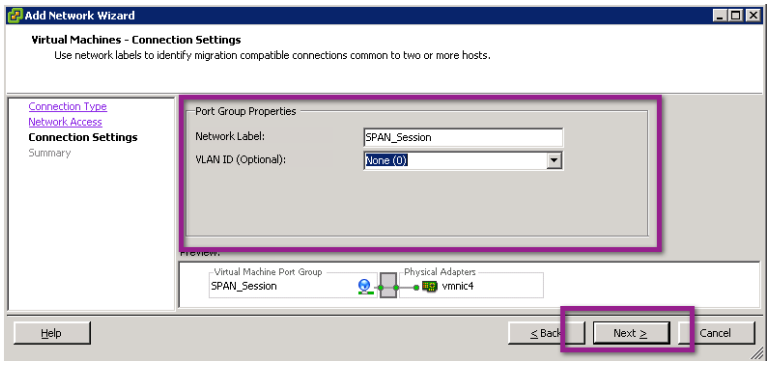
Step 3 Select the Physical Interface that will be connected to the SPAN port on the switch, and click Next (Figure 5).

Figure 5 Selecting the Physical Interface



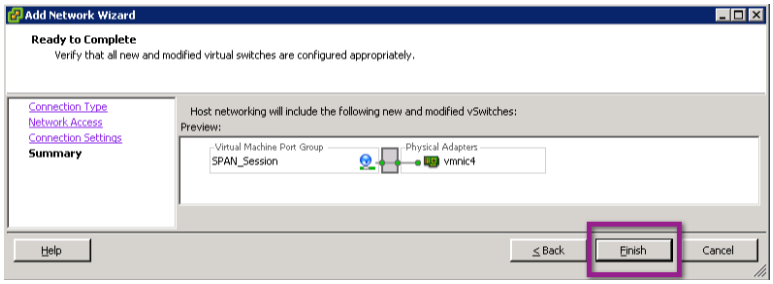
Step 4 Name the network **SPAN_Session** or any other logical name (Figure 6).

Figure 6 Naming the Network



Step 5 Select Finish (Figure 7).

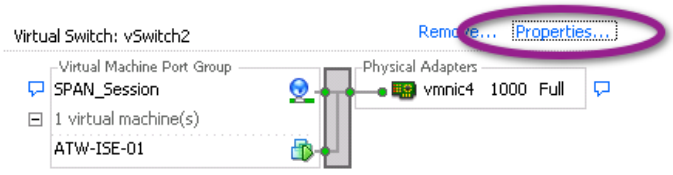
Figure 7 Completing the Configuration of the Virtual Switch



Step 6 To enable promiscuous traffic on the newly created virtual switch, select Properties (Figure 8).

Note: By default, any VMware network rejects promiscuous traffic.

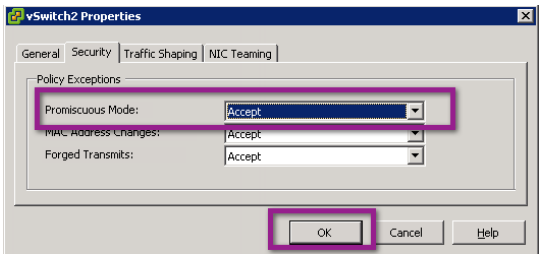
Figure 8 Setting vSwitch2 Properties



Step 7 Highlight the new virtual switch and select Edit.

Step 8 Select the Security tab, and then select Accept from the Promiscuous Mode drop-down menu and click OK (Figure 9).

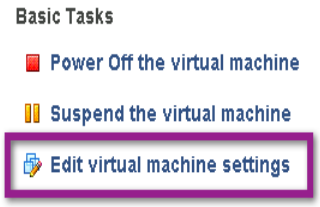
Figure 9 Accepting Promiscuous Mode



Step 9 Close the vSwitch Properties window.

Step 10 Edit the Cisco ISE Virtual Machine Settings (Figure 10).

Figure 10 Edit Virtual Machine Settings

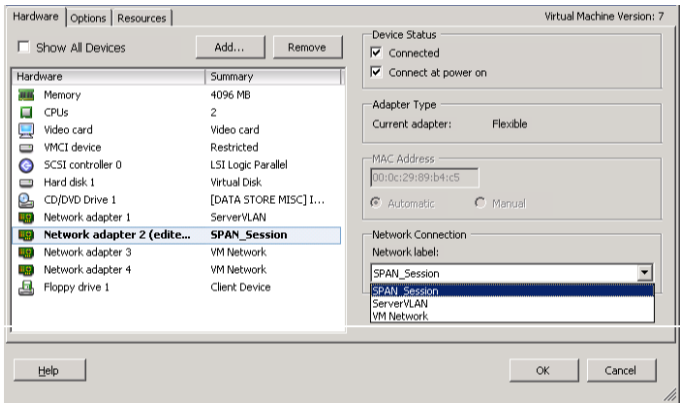


Step 11 Select the appropriate Network Adaptor for Cisco ISE (usually Network Adaptor 2, for GigabitEthernet 1 in Cisco ISE).

Step 12 Ensure that the Device Status is set to Connected and that Connect at power on is also enabled (Figure 11).

Step 13 From the Network Connection drop-down menu, select the newly created SPAN_Session network (Figure 11).

Figure 11 Virtual Machine Settings

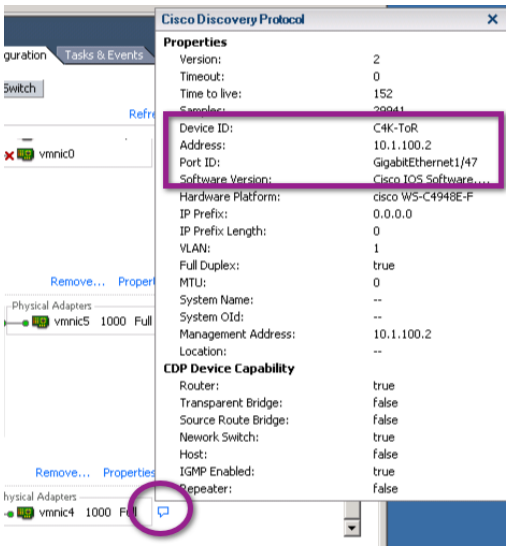


Step 14 Click OK.

Step 15 Make note of the switch port that the promiscuous interface is connected to, for use in the next section.

Note: The VMware ESX server has a user-friendly feature of displaying Cisco Discovery Protocol information for its connected interfaces. Figure 12 shows this display.

Figure 12 Cisco Discovery Protocol



How to Configure a Promiscuous VMware Port Group

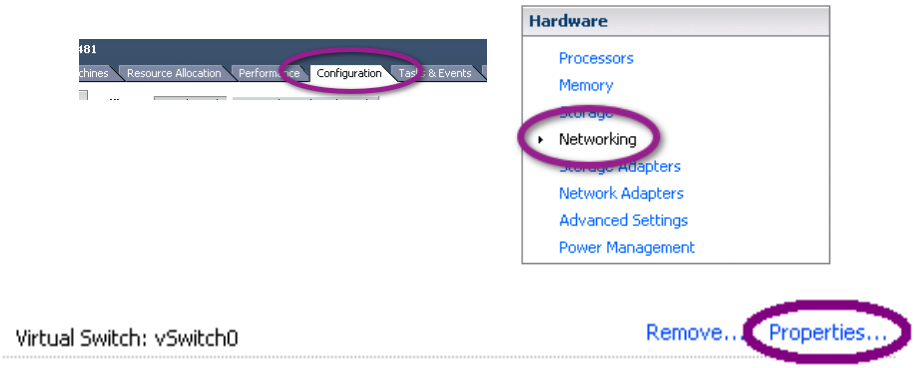
Procedure 1 Configure a Promiscuous VMware Port Group (Optional)

A second approach to configuring a promiscuous VMware network is to create a promiscuous port group on an existing vSwitch. This deployment is important if it is either not possible to dedicate a physical SPAN port to the Cisco ISE virtual machine or if the nature of virtual deployment is such that not all traffic can be copied from the physical switch and must be obtained from the vSwitch itself.

Step 1 Select the physical ESX server in VMware VSphere client.

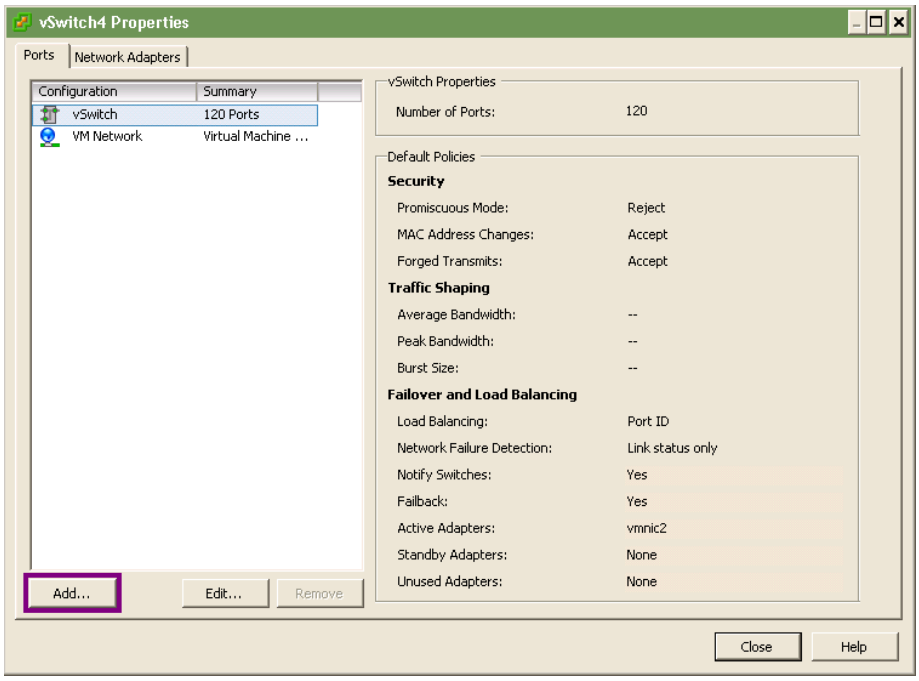
Step 2 Select Configuration → Networking, and then choose your vSwitch and click Properties (Figure 13).

Figure 13 Configuration → Networking



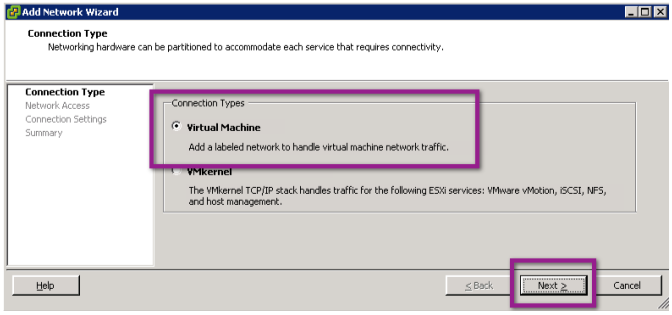
Step 3 In the vSwitch Properties window, in the Ports tab, click Add at the bottom left [[do they have to be sure that vSwitch 120 Ports is selected?]] (Figure 14).

Figure 14 vSwitch Properties



Step 4 The Add Network Wizard is launched. Under Connection Types, choose Virtual Machine and click Next (Figure 15).

Figure 15 Connection Type

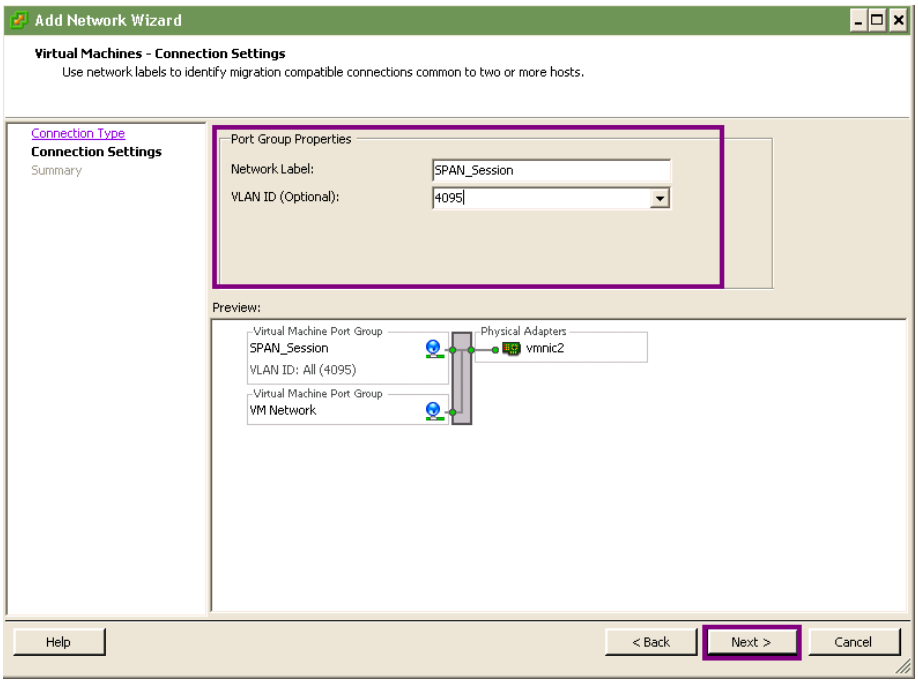


Step 5 Name the port group **SPAN_Session** or any other logical name.

Step 6 Set the VLAN to **4095** and click Next (Figure 16).

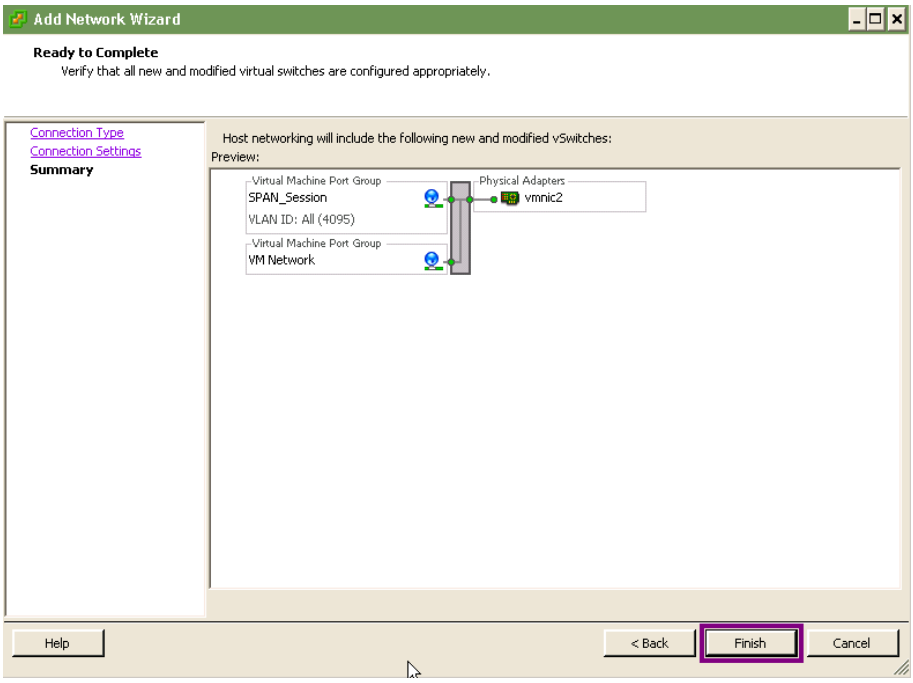
Note: This VLAN is a special VMware VLAN that listens to all other VLANs on that vSwitch.

Figure 16 Port Group Properties



Step 7 Select Finish (Figure 17).

Figure 17 Preview



Step 7 Highlight the new port group.

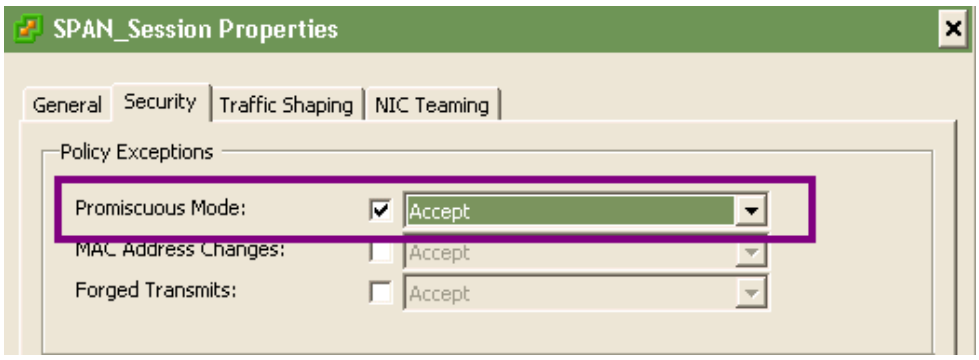
Step 8 Choose Edit.

Step 9 Select the Security tab.

Step 10 Select Accept from the Promiscuous Mode drop-down menu.

Step 11 Click OK.

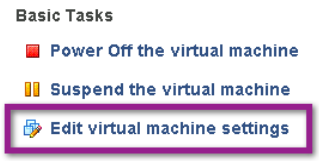
Figure 18 Promiscuous Mode



Step 12 Close the vSwitch Properties window.

Step 13 Edit the Cisco ISE Virtual Machine Settings (Figure 19).

Figure 19 Edit Virtual Machine Settings

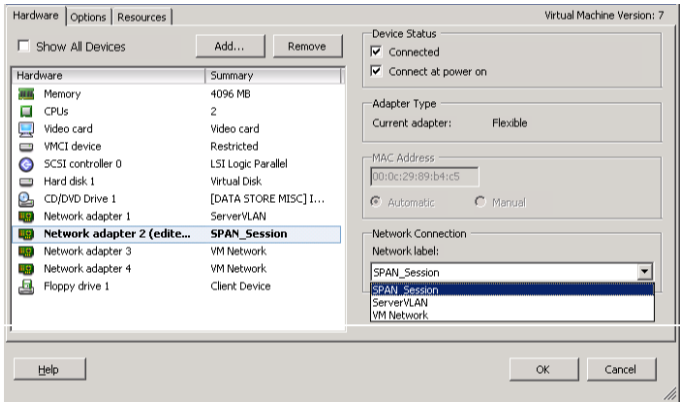


Step 14 Select the appropriate Network Adaptor for Cisco ISE (usually Network Adaptor 2 for GigabitEthernet1 in Cisco ISE).

Step 15 Ensure that the Device Status is set to Connected and that Connect at power on is also enabled.

Step 16 From the Network Connection drop-down menu, select the newly created SPAN_Session network (Figure 20).

Figure 20 VM Settings



Step 17 Click **OK**.

How to Configure the SPAN Session

Procedure 1 Configure the SPAN Session on the Switch

Step 1 Enter Global Configuration**.** [[Where? Be more explicit.]]

Step 2 Configure the SPAN session source. An example follows:

```
C4K-ToR(config)#monitor session 1 source vlan 100 both
```

Step 3 Configure the SPAN session destination. An example follows:

```
C4K-ToR(config)#monitor session 1 destination interface g 1/47
```

Step 4 Verify that the port is now in monitoring mode.

```
C4K-ToR(config)#do show int status | i 47
Gi1/47  monitoring   1    a-full a-1000 10/100/1000-TX
```

Procedure 2 Configure the IP HELPER Statements

To work along with the DHCP probe for Cisco ISE profiling, the Cisco ISE policy node(s) should be added to the **ip helper-address** statements on the Layer 3 interfaces in the network. This node addition will send a copy of all DHCP requests to the Cisco ISE, in addition to the production DHCP servers in the environment.

Step 1 Enter Global Configuration mode**.** [[Where? Be more explicit.]]

Step 2 Enter the Interface configuration mode for the Access VLAN Layer 3 interface and add Cisco ISE as another destination for **ip helper-address**. An example follows:

```
interface Vlan10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.100.100  ! – this is the DHCP Server
 ip helper-address 10.1.100.3    ! – this is the ISE Server
```

Appendix A: References

Cisco TrustSec System:

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html