

ISERink Installation Guide

Version 1.3

January 1, 2016

Document Change log:

Version 1.1: First version released January 2015

Version 1.2: Added section 3.4 describing how to configure AD to support IScorE. Note: AD is not released as part of ISERink. You can tie IScorE into an existing AD, create a new AD, or use IScorE's built in user account management system.

3.1.2 changed to move details about network configuration elsewhere

3.1.4 was added in order to walk through setting up static IP addresses and DNS (this changed all image numbers in 3.1.* and the step numbers)

3.1.8 added the section to allow SSH through the firewall downloading the images is impossible without this step.

3.3.2 added an alternative method that appeared for me that was needed to verify that the virtual machines were copied over.

3.4.2 was edited to give full details on how to configure IScorE to be publicly accessible old documentation would give 400 and 502 errors

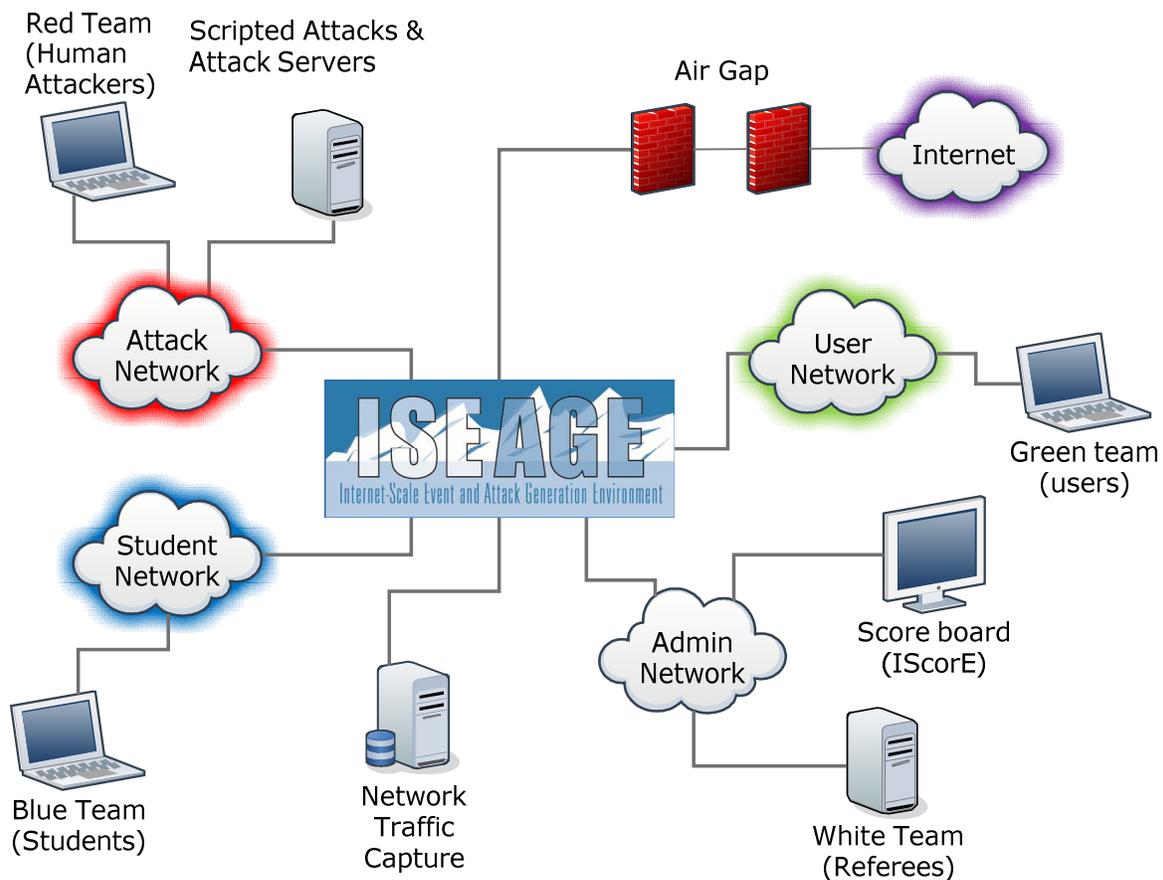
Version 1.3: Instruction corrections made to various sections. Added additional details to define how to install based on two possible ISERINK configurations, one directly connected to the internet and one behind a NAT/FW.

Background

First developed to support cyber defense competitions (CDCs), ISERink is a virtual laboratory environment that allows students an opportunity to undertake hands-on activities focused on networking, cyber security, and penetration testing. As shown below ISERink support 3 network ranges (Blue, Red, Green). Each range consists of multiple subnets and can support dozens of teams. In addition ISERink is connected to the Internet to allow users access to web servers.

It is built upon an Internet testbed named ISEAGE that provides a real world networking environment for students. To the students it appears as if their network, which uses public address space, is directly connected to the Internet. However, the students' traffic is contained in the controlled ISEAGE testbed. This prevents misconfigurations or other beginner mistakes from disrupting a classroom or campus network.

This document will guide you through installing and setting up your own instance of ISERink. The ISERink users guide will walk you through configuring and using ISERink for different uses.



ISERink playground

Document sections:

1. System hardware/software requirements
2. Overview of ISERink
3. Building ISERink
 - a. Downloading and installing VMWare's ESXi.
 - b. Setting up the ESXi virtual networks.
 - c. Downloading and installing the individual Virtual Machines for ISERink.
 - d. Configure servers
 - e. Setting up AD to support IScore
4. Testing ISERink
5. Appendix A: Configuration tables

Section 1: ISERink hardware/software requirements

ISERink consists of several different virtual machines working together to create the playground. The core of ISERink runs on a single VMWare ESXi server. The Blue, Red, and Green team systems are connected to the ISERink via physical network interfaces.

Hardware requirements:

- Machine capable of running VMWare ESXi 5.5 or higher with:
 - 6 network cards
 - 300 GB of disk space (minimum)
 - 24 GB of memory (minimum)
 - Dual quad core processors (recommended)
- Equipment to support the teams (Blue, Red, Green, and White). These can be virtual using any hypervisor, physical machines, or a combination of both.
- A PC running windows to manage the ESXi server
- A windows Active Directory server

Software requirements:

- VMWare ESXi 5.5 or higher
- ISERink VM's

Section 2: Overview of ISERink

ISERink is a cyber-security playground designed to provide a realistic network environment that mimics the Internet. At the heart of ISERink is a collection of virtual machines running UNIX with custom software used to implement the ISEAGE virtual network. Several other virtual machines designed to provide various services (i.e. scoring, DHCP for teams, etc.) are also provided.

ISEAGE is a network testbed developed at Iowa State University with funding from the Department of Justice that is designed to allow for the simulation of various network configurations. The core of the ISEAGE testbed is a routable IP network. The routable IP network supports the traffic to and from the networks and systems under test. The routable IP network is accomplished using a custom program called ISEFlow. The ISEFlow is a modified router that creates virtual networks that can be interconnected to create a large virtual network. The ISEFlow can act as a set of virtual routers so that traffic appears to have routed through the Internet.

You can think of ISERink as 45 subnets interconnected using a backbone network to create what we call the competition network, see Figure 2.1. One physical NIC provides the connection to the Internet for Web traffic, remote access to the scoring system (IScorE), and VM management. In addition a physical NIC is used for the white team to manage ISERink, and another is used to collect the network traffic.

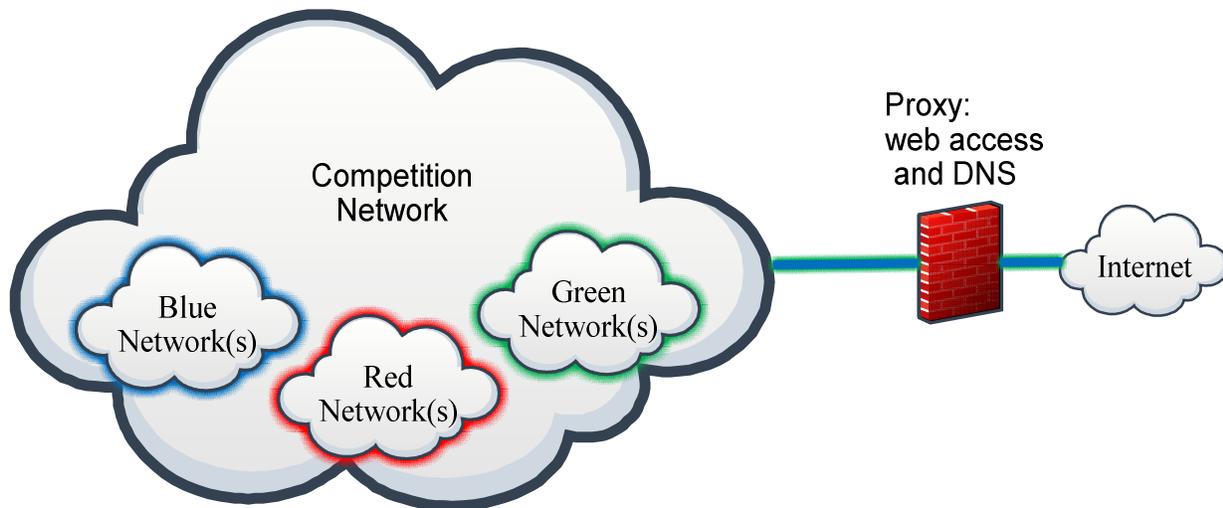


Figure 2.1 ISERink overview

Figure 2.2 shows the topology of the VM machines that create the routable Internet (ISEAGE) along with the machines that create ISERink. As shown in Figure 2.2 ISEAGE supports 45 class C subnets (15 on NIC2, NIC3, and NIC4). In addition NIC 1 is used for the white team to manage ISERink, and NIC5 is used to collect the network traffic.

NOTE: Each of the 45 competition subnets are external to the ESXi machine running ISERink. These subnets are connected to ISERink via the physical NICs (2,3,4). For each subnet ISERink looks like a gateway (egress) router. The address of the gateway for each of the competition subnets is XXX.XXX.XXX.254.

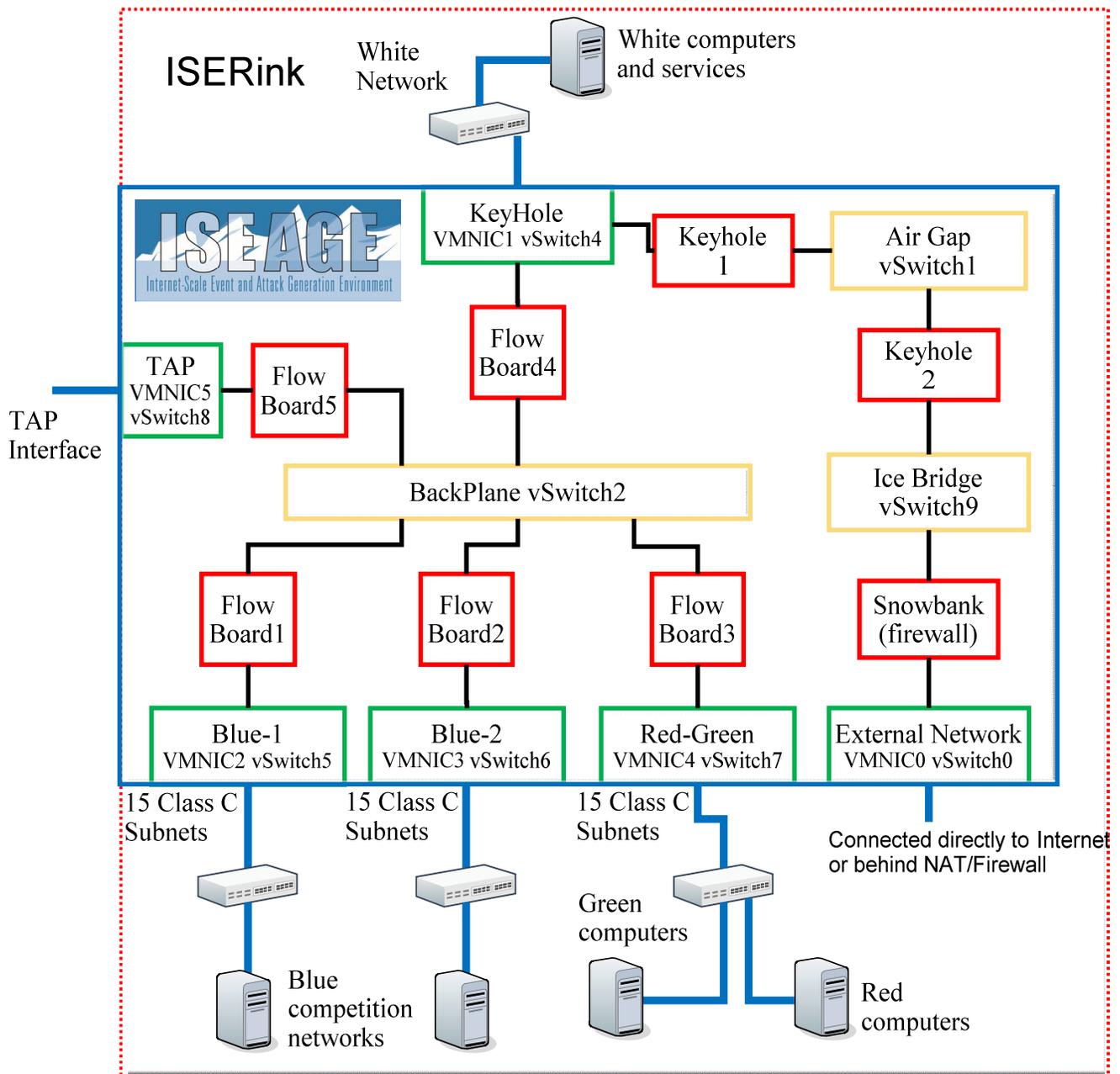


Figure 2.2 ISERink VM topology

ISERink Internet access

In order for ISERink to function it will need access to the Internet. There are three external IP addresses that are used by ISERink: ESXi management, Snowbank, and IScoreE. All access to the Internet is through NIC0. There are two typical methods to connect ISERink to the public Internet. The first is behind a NAT/FW as shown in Figure 2.3 and the second is directly to the Internet (Figure 2.4). For each configuration we will discuss the three IP addresses.

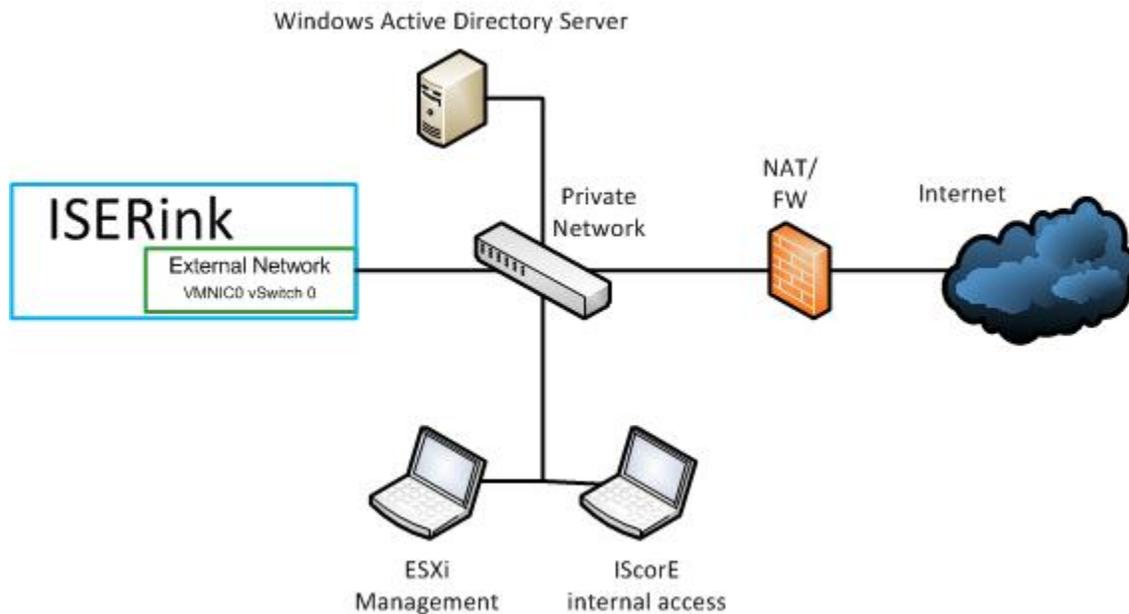


Figure 2.3 ISERink behind a NAT/Firewall

When ISERink is connected to a private network behind a NAT you will need three private IP addresses: one for ESXi management, one for Snowbank, and one for IScoreE.

ESXi Management: The machine used to configure and manage ISERink needs to be on the same network that the ESXi management port (NIC0) is located. While you can configure your firewall or NAT to tunnel the ESXi management traffic, we have found it is easier to have the management PC on the same network.

Snowbank: The devices on the competition network can access the Internet using four protocols (DNS, HTTP, HTTPS, FTP). This is accomplished using an air-gap proxy. The external interface of this proxy needs to be connected to the Internet. This connection is made through Snowbank. Set the WAN interface on Snowbank to one of the three private IP addresses and set the default gateway to the default gateway of your private network.

IScoreE: IScoreE actually is connected to three different networks. First, it is connected to an internal private network that is currently not used, unless you decided to install a dedicated Active Directory to support IScoreE account management. If so this would be the ideal network to connect a dedicated AD. Second, it is connected to the competition network to enable

scanning and to allow the teams to access documents within the competition network. Lastly, it will be connected to your private network using one of the three IP addresses. This will provide access to IScorE on your private network. This can also be made accessible over the internet if you enable port forwarding or tunneling rules through your private networks NAT for HTTP/HTTPS traffic.

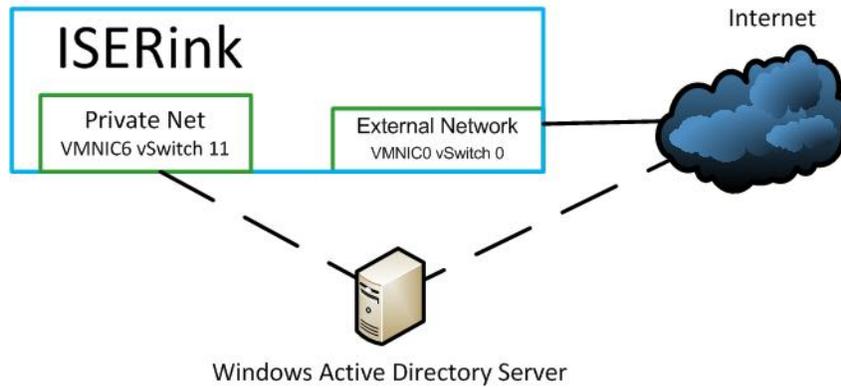


Figure 2.4 ISERink directly connected to the Internet

When ISERink is connected directly to the public Internet you will need up to four public IP addresses: one for Snowbank, one for IScorE if you want it to be accessible from the internet, one for the ESXi server, if you want it to be accessible from the internet, and the last one for Windows Active Directory Server if you decide to use a publically accessible Windows AD for IScorE account management. If you don't already have a publically addressable AD and are planning to build one solely for ISERink, I would strongly advise doing so and connecting it to the private network directly connected to IScorE.

ESXi Server Management: If you choose to set the ESXi server to a public IP then any computer that can access the internet could be used for ESXi Server Management.

Snowbank: The WAN interface requires a Public IP address if ISERink is directly connected to the internet. Set the Default gateway according to your ISP.

IScorE: IScorE actually is connected to three different networks. First, it is connected to an internal private network that is currently not used, however this is a good option if you choose to install a dedicated Active Directory to support IScorE account management. If your server had a spare NIC, then you could attach VMNIC6 to the vSwitch 11 for this, or if your server has capacity to host the AD as a VM then simply connect it that VM to vSwitch 11. Second, it is connected to the competition network to enable scanning and to allow the teams to access documents within the competition network. Lastly, you can place a public IP address on one of the IScorE NIC's and make it accessible on the internet.

ISERink Component Overview

The table below provides a brief overview of the various Virtual Machines in ISERink and their function.

Machine Name	Function
Snowbank	This is the main firewall between ISEAGE and the Internet. All traffic directed to the Internet is routed through here.
Snowflake	This is the machine that controls the configuration and management of ISEAGE running on the Board VMs. The ISEAGE configuration file is stored on this machine and distributed to the Board VMs.
Gatekey	This machine allows for debugging of ISEAGE. It is not necessary for the operation of ISEAGE and is present for debugging and testing purposes.
Keyhole1	This machine has a squid proxy server running on it (http://199.100.16.100:3128) that allows access to HTTPS, HTTP and FTP sites on the internet. This machine also has a Name Server running on it which resolves the internal names of the ISEAGE machines.
Keyhole2	This machine has a squid proxy server running on it that forwards internet requests from Keyhole1 onto Snowbank.
Board 1	Runs the ISEFlow software on which the ISEAGE network traffic is routed through. This particular board is set up to handle the traffic for Blue Teams 1-15.
Board 2	Runs the ISEFlow software on which the ISEAGE network traffic is routed through. This particular board is set up to handle the traffic for Blue Teams 16-30.
Board 3	Runs the ISEFlow software on which the ISEAGE network traffic is routed through. This particular board is set up to handle the traffic for the Red and Green teams.
Board 4	Runs the ISEFlow software on which the ISEAGE network traffic is routed through. This particular board is set up to handle the traffic for the white team.
Board 5	Runs the ISEFlow software on which the ISEAGE network traffic is routed through. This particular board is set up to act as a TAP board. This means that all ISEAGE traffic is routed through this board and can be monitored on the TAP interface.
ISCorE	This VM runs the ISCorE software that monitors the Blue Team machines and sees which services are actively running on the Blue Team machines.
White-DHCP	Used to manage the white team IP address space. Uses a pfSense firewall to provide DHCP services.
Green-KALI	Used to test ISERink.

Section 3: Building ISERink

This section will detail the steps to install ESXi, configure the virtual networks, install the virtual machines and configure ISERink.

Step 3.1: Downloading and installing VMWare's ESXi.

Overview

The first step in building ISERink is to install and configure VMware ESXi to host the various virtual machines on a single server. If you need instructions for installing ESXi you can find help on the VMware Web site. Many of the screenshots in this document are of VMware's ESXi software and the exact images may be different on your installation.

In this section you will download and install ESXi onto your server. ESXi is a bare-metal hypervisor that provide a lightweight framework for Virtual Machines to run on top of. ESXi is free (registration required) bare metal hypervisor that allows guest virtual machines to be run directly on the host server with little additional overhead. ESXi allows virtual networks to be built inside of it with multiple virtual machines.

Your machine running ESXi will use one of the network interfaces for remote management. During installation you will need to give this interface an IP address. The management interface can be on the public Internet or you can place it behind a NAT and/or Firewall. If you place it behind a NAT and or Firewall it will be easier to manage if the management PC is located on the same side of the NAT and/or firewall.

Step 3.1.1: Download ESXi

First, download the image for [ESXi 5.5 or higher](#). Before the image can be downloaded, you must create a free account with VMware and log in. After logging in, download the ISO image for ESXi. Also note, near the top of the page is the license key that you will need to register ESXi with later. It is easiest to burn the ISO on to a CD disk and boot your server from CD to install the software.

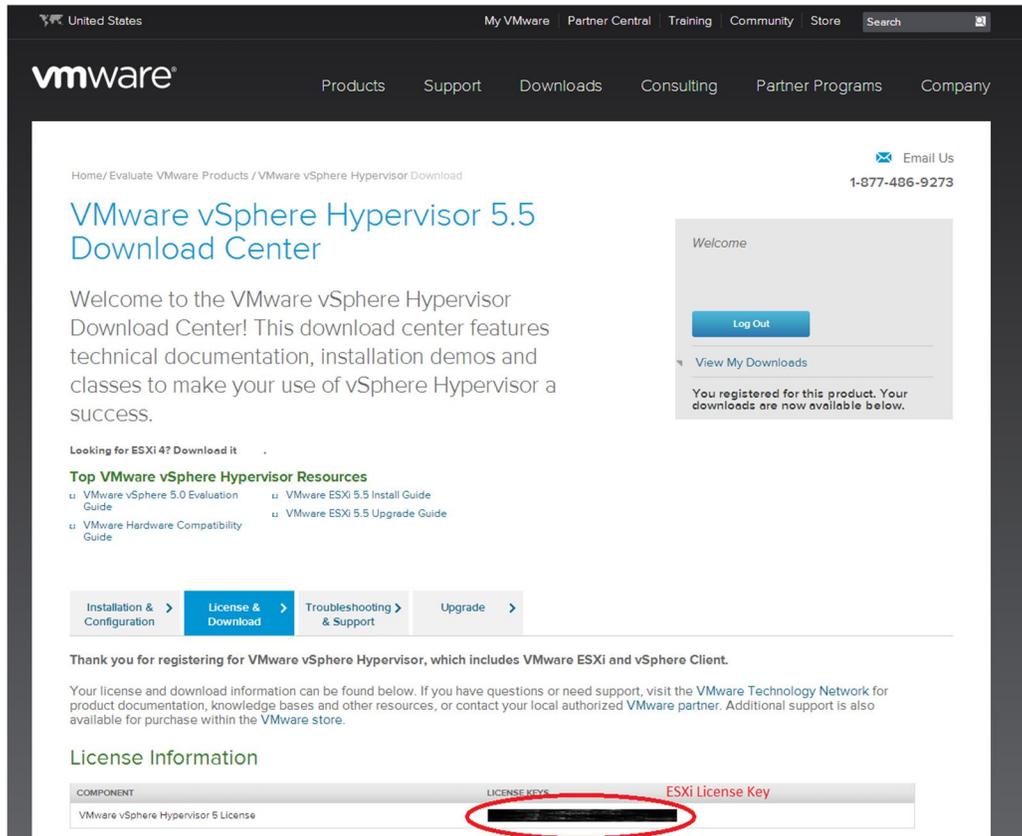


Figure 3.1.1: Location of ESXi key

Step 3.1.2: Install ESXi

After downloading the ESXi ISO image, install ESXi on your server (the default settings are fine). If you need further information on installing ESXi, you can find information online or on the ESXi web site. The most common problem is not having ESXi compatible hardware. The VMware web site has compatibility guides to help determine if your hardware is compatible.

During the installation process you will need to create the root password for the ESXi hypervisor. The root password for the ESXi is used to manage the ESXi system and should not be shared with general users.

After ESXi has been installed, you will be presented with a screen which looks similar to Figure 3.1.2.

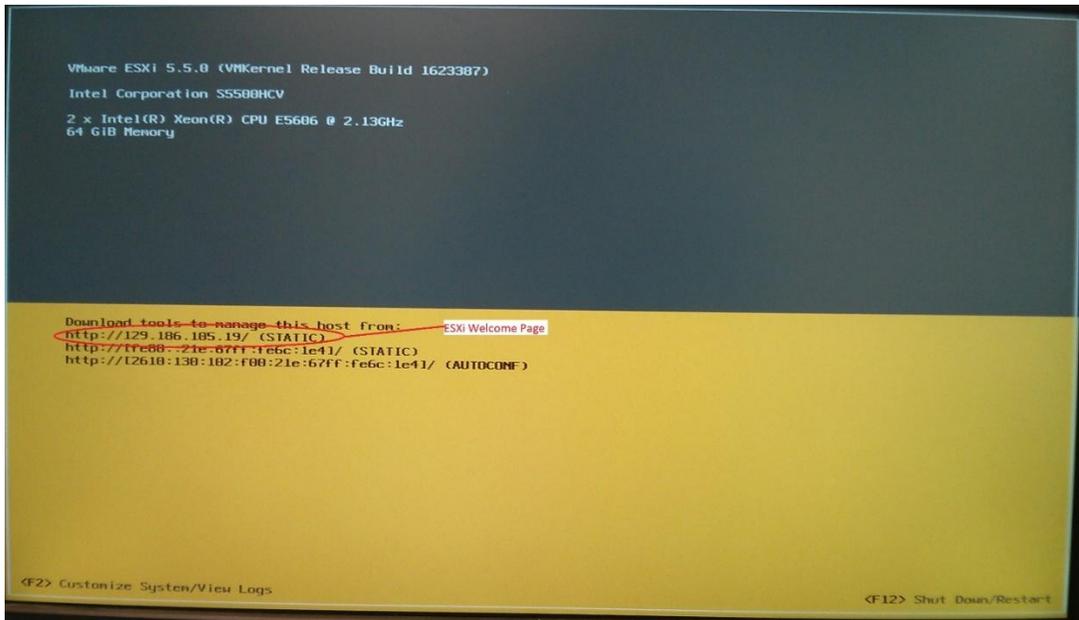


Figure 3.1.2: ESXi Main Screen

Step 3.1.3: Map Network Interfaces on ESXi

After installing ESXi, one of the first things that should be done is to map and label the physical network adapters (NICs) on the server. To do this you will individually hook up the physical NICs to a switch or router and see which interface shows as active in ESXi. First, press the **F2** key to enter the ESXi configuration page. Enter your root password and then press **Enter**.

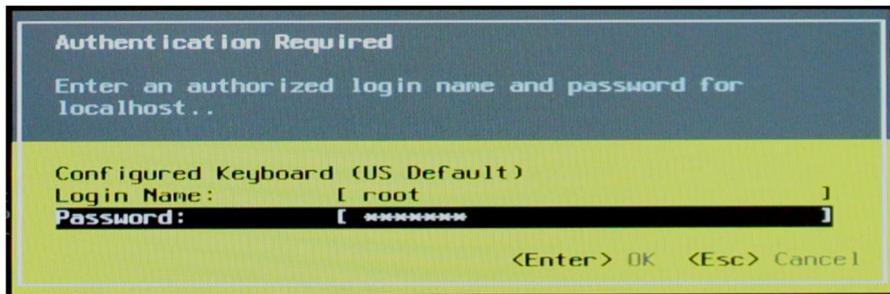


Figure 3.1.3: ESXi Password screen

Use the arrow keys to select **Configure Management Network** as shown in Figure 3.1.4 and then press enter.

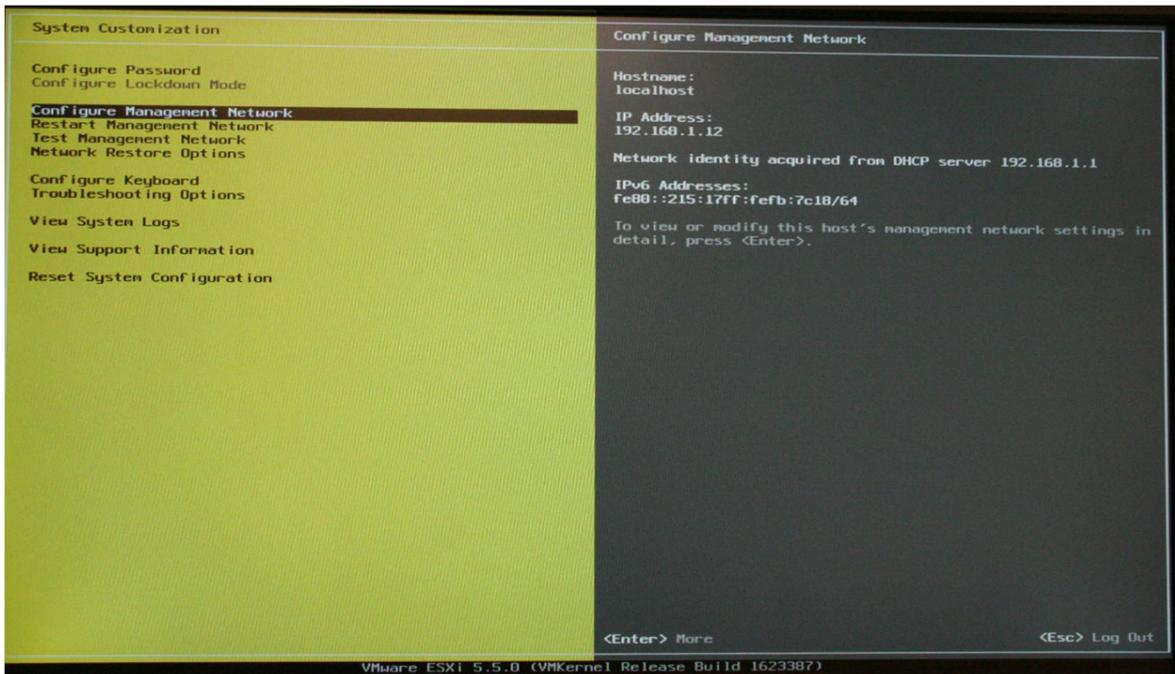


Figure 3.1.4: Configure Management Network

Press enter to select **Network Adapters**. You will then be with a screen that looks similar to Figure 3.1.5.

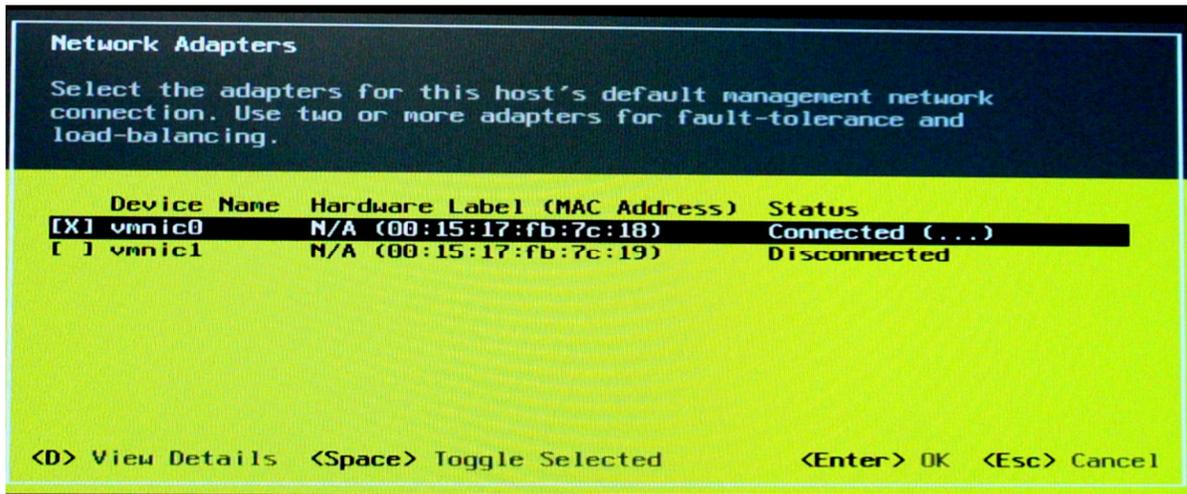


Figure 3.1.5: ESXi Network Adapters

If any of the NICs are currently connected to anything, the status for that NIC will show up as connected on this screen. One by one, hook up to NICs on the server to either a switch or a router. Exit out of the Network Adapters dialog box by pressing the **Esc** key and then re-enter the Network Adapters dialog box by pressing the **Enter** key. The Network Adapters dialog box should now show a different VMNIC as connected. Repeat this process for all of the NICs on the server and either write down the NIC mapping or label the NICs on the server. You will need this information later to properly connect the server. You can use the table in [Appendix A](#) to fill in what you discover.

Step 3.1.4: Configure network settings

Next an IP address must be assigned for the management port. The IP address of the management port is needed to remotely manage the ESXi system. The worksheet in [Appendix A](#) can be used to write down this information for future reference. From the Configure Management Network use the arrow keys to select **IP Configuration** and hit **enter**. You will then be with a screen that looks similar to Figure 3.1.6.

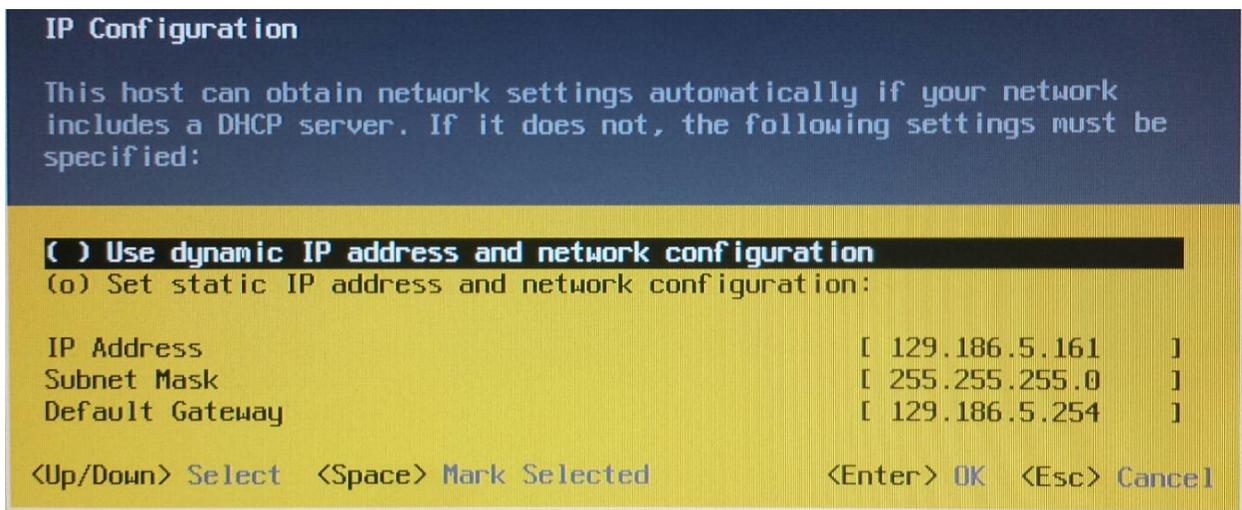


Figure 3.1.6: IP Configuration

Use the arrow keys to highlight **Set static IP address and network configurations:** and hit **Spacebar** to select it. Fill out the IP address for the management port, subnet mask, and default gateway then hit **enter**. If you do not know what to put here contact your system administrator.

From the Configure Management Network use the arrow keys to select **DNS Configuration** and hit **enter**. You will then be with a screen that looks similar to Figure 3.1.7.

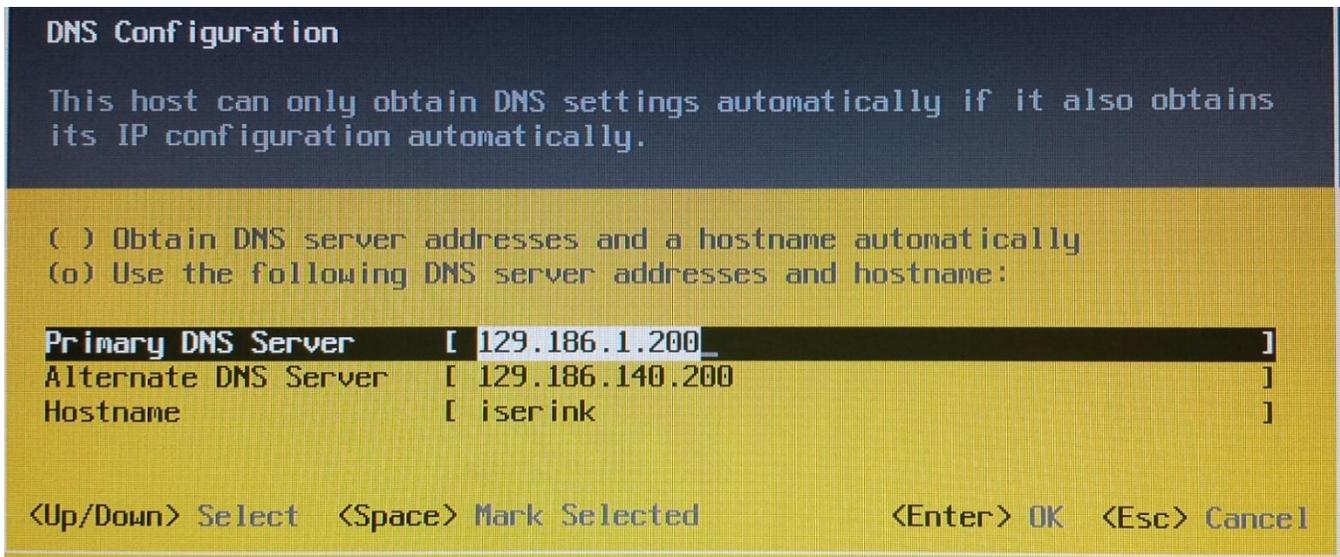


Figure 3.1.7: DNS Configuration

Use the arrow keys to highlight **Use the following DNS server addresses and hostname:** and hit **Spacebar** to select it. Fill out the primary DNS server, Alternate DNS server and, Hostname then hit **enter**. If you do not know what to put here contact your system administrator.

Step 3.1.5: Enable remote management of ESXi

In order to download the ISERink images you will need to use the command line interface of the ESXi hypervisor. This can be done two ways. Either you may use the ESXi shell, or you may remotely access it via SSH. One or both options must be enabled. To enable these options you need to enter the ESXi configuration page as shown in Step 3.1.3. The options are enabled by selecting the menu item “**Troubleshooting Options**” as shown in Figure 3.1.4. There you will see an option “Enable SSH” and an option “Enable ESXi shell”. Once enabled you can access the command line interface. (You will do this later.)

To access the command line interface using the ESXi shell you need to press F1 on the keyboard connected to the ESXi machine. This will bring up a UNIX login prompt and you can enter the username root and the root password. If you choose to use SSH you will need an SSH client on the PC you are using to manage ESXi.

Step 3.1.6: Configuring ESXi

To configure ESXi, you must first download and install the vSphere Client (runs on Windows only). To do this, on a separate Windows machine that is on the same network as the server, open a web browser and navigate to the web address given on the ESXi main screen (see Figure 3.1.2 for a reference of where to find the ESXi server IP address). If you receive a warning about the site's security certificate not being trusted, ignore the warning and proceed

anyway. After navigating to the ESXi server IP address, you will see a screen similar to Figure 3.1.8.

Note: The machine used to configure and manage ISERink needs to be able to access the same network that the ESXi management port is located. While you can configure your firewall or NAT to tunnel the ESXi management traffic, we have found it is easier to have the management PC on the same network.

VMware ESXi

Welcome



Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.

You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.

- [Download vSphere Client](#)

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware vCenter](#)

If you need more help, please refer to our documentation library:

- [vSphere Documentation](#)

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- [Download the Virtual Appliance](#)
- [Download the Windows Installer \(exe\)](#)
- [Download the Linux Installer \(tar.gz\)](#)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- [Learn more about the Web Services SDK](#)
- [Browse objects managed by this host](#)



Copyright © 1998-2014 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit <http://www.vmware.com/info?id=1127> for more information.

Figure 3.1.8: ESXi Server Web Page

Click on the "Download vSphere Client" link to download the vSphere client installer from the ESXi server. After the vSphere client is downloaded, install it. After installing the vSphere client, run the program. You will be presented with a window similar to Figure 3.1.9.

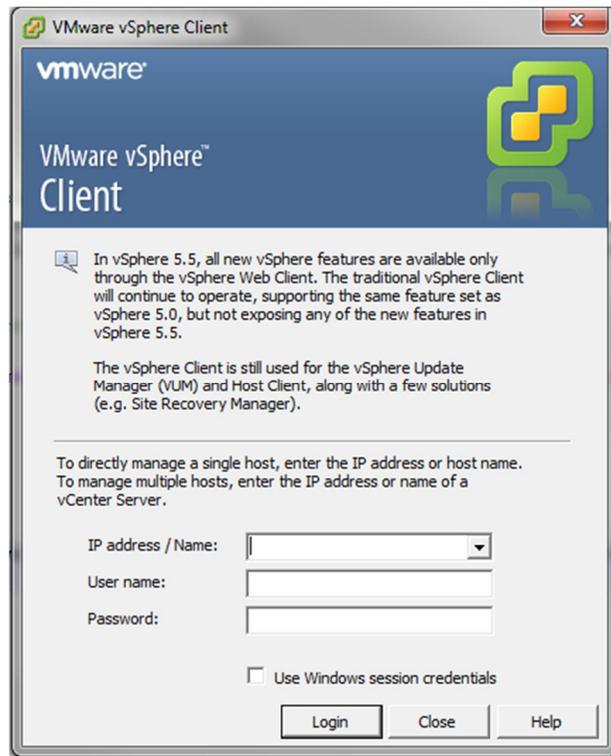


Figure 3.1.9: vSphere client login window

Enter the IP address of your ESXi server (the same one used to download the ESXi client). The username is root, and the password is the password you chose when setting up the ESXi server. After logging into vSphere you should see a screen similar to Figure 3.1.10.

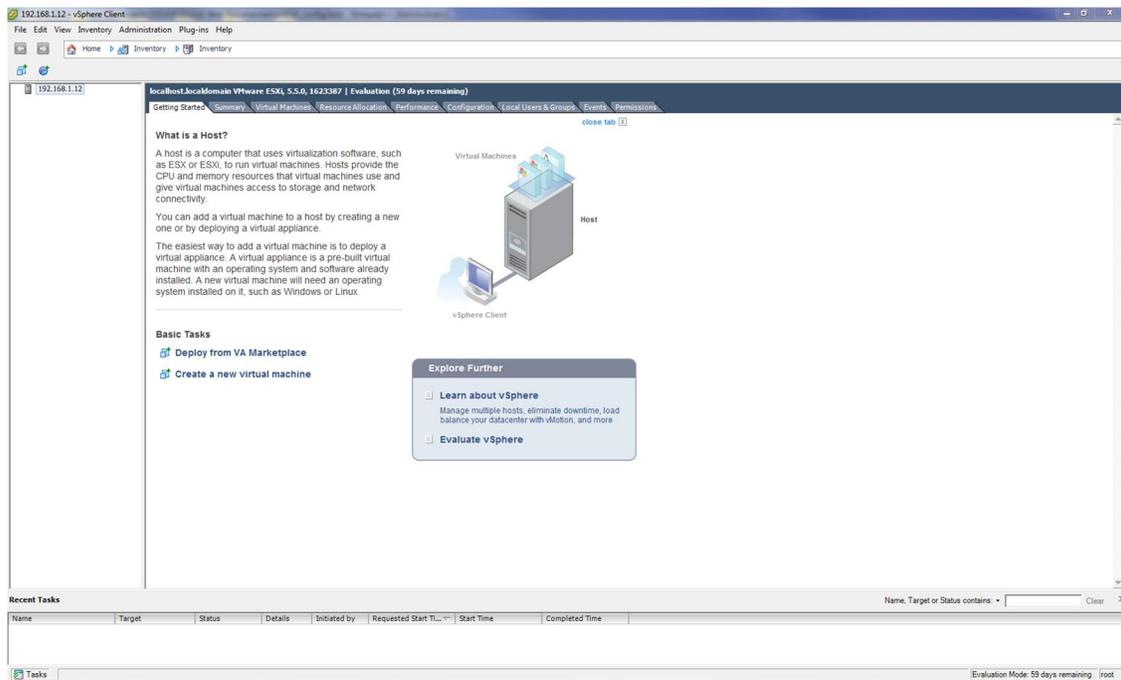


Figure 3.1.10: vSphere Client Main Window

After logging into the vSphere client, the first thing to do is to add the ESXi license key into vSphere.

Step 3.1.7: ESXi License Key Registration

1. After logging into the vSphere client, go to the **Configuration Tab**

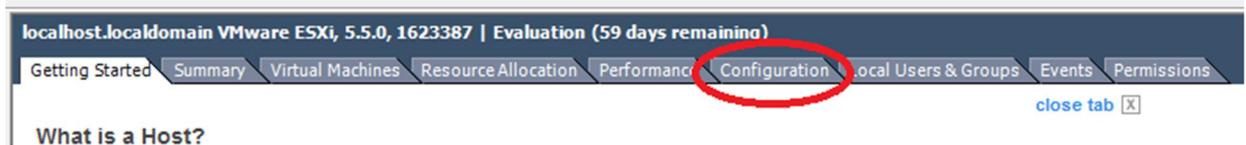


Figure 3.1.11: vSphere Configuration Tab

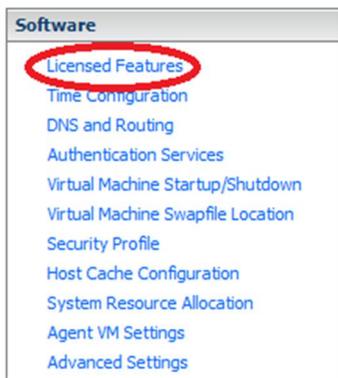


Figure 3.1.12:

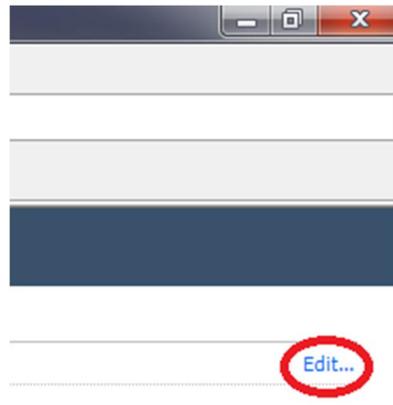


Figure 3.1.13:

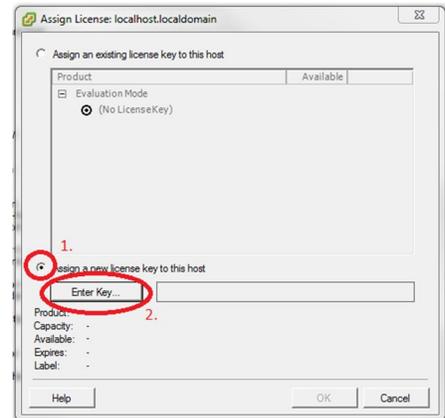


Figure 3.1.14

2. Next, click the **Licensed Features** link inside of the Software box on the left side of the screen Figure 3.1.12.
3. Click the **Edit** link in the upper right hand side of the screen Figure 3.1.13
4. Select the **Assign a new license key to the host** box, Figure 3.1.14
5. Enter your license key in the box and click the **OK** button.

Step 3.1.8: Enable outbound SSH

1. In order to copy the VM images to your ESXi server you will need to enable outbound SSH. This is done through the security profile menu as shown in Figure 3.1.15. Click on the **properties** button on the service window and then highlight the SSH server. Click on the **option** button and select start then click **OK**. The screen will then look like Figure 3.1.13.

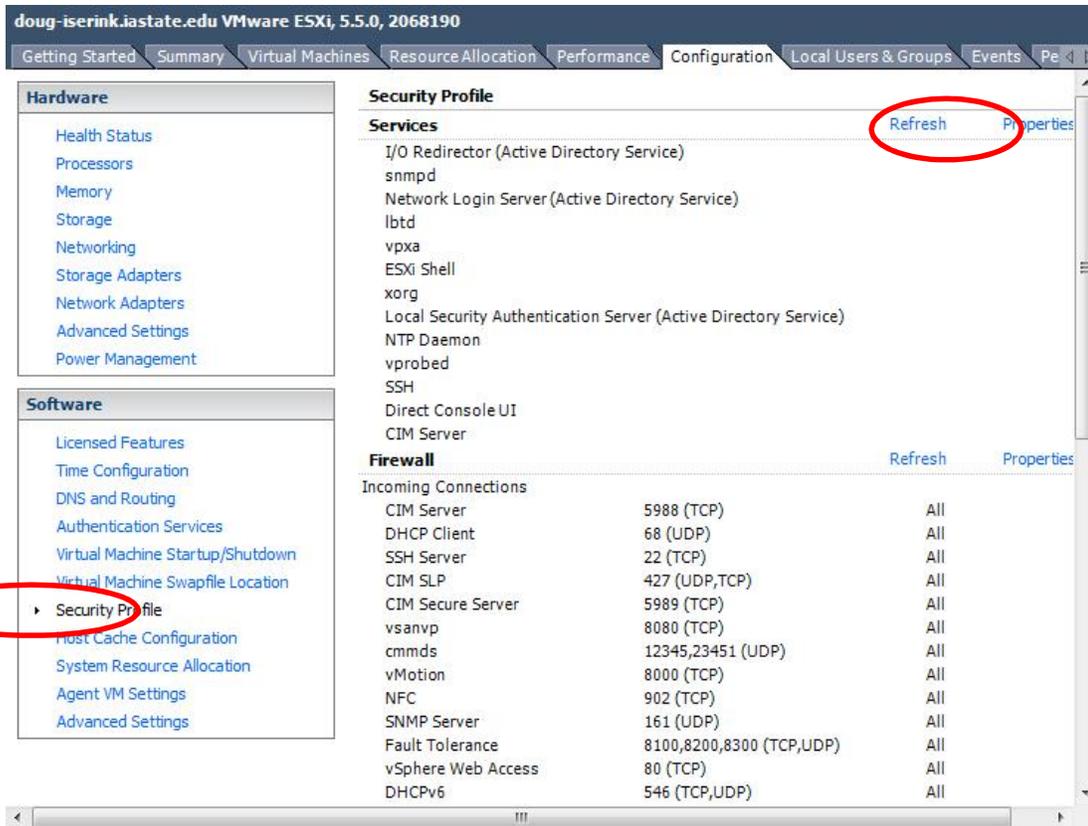


Figure 3.1.15 edit services

Label	Daemon	Status
snmpd	Running	
Network Login Server (Active Directory Service)	Stopped	
lbtd	Running	
vpax	Running	
ESXi Shell	Running	
xorg	Stopped	
Local Security Authentication Server (Active Directory Service)	Stopped	
NTP Daemon	Stopped	
vprobed	Stopped	
SSH	Running	
Direct Console UI	Running	

Figure 3.1.16 Enable SSH

- Next we must enable ssh through the firewall to do this from the security profile menu. Click on the **properties** button on the firewall window as shown in Figure 3.1.17. Check the boxes for SSH server and SSH client then click **OK**. As seen in Figure 3.1.18

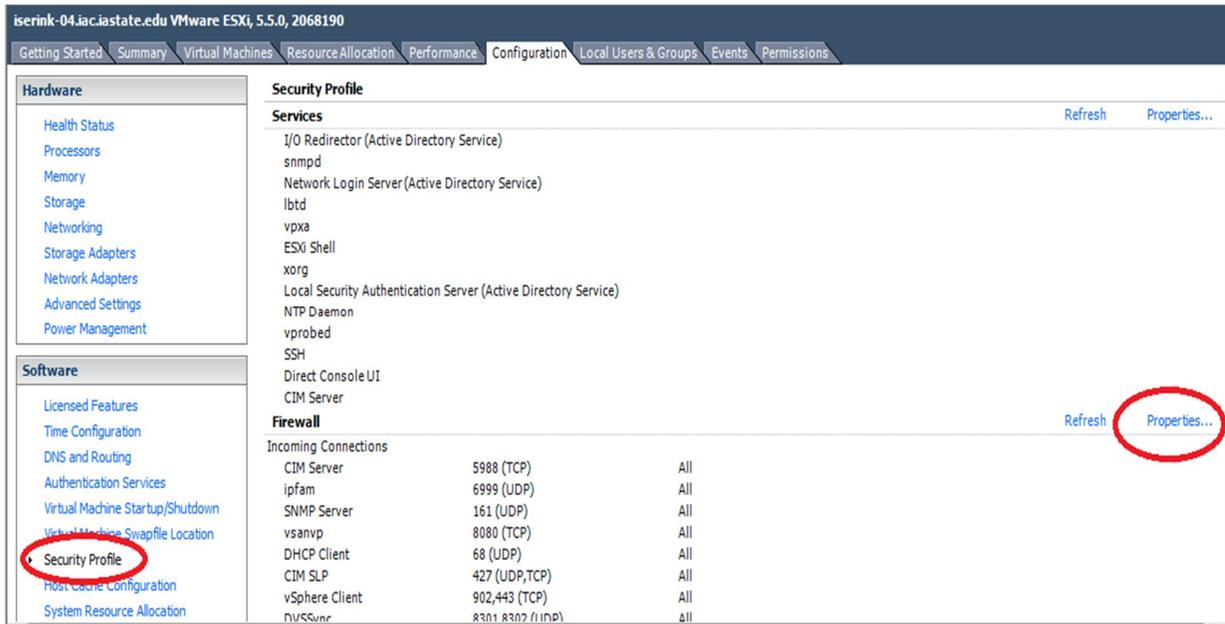


Figure 3.1.17 Edit firewall

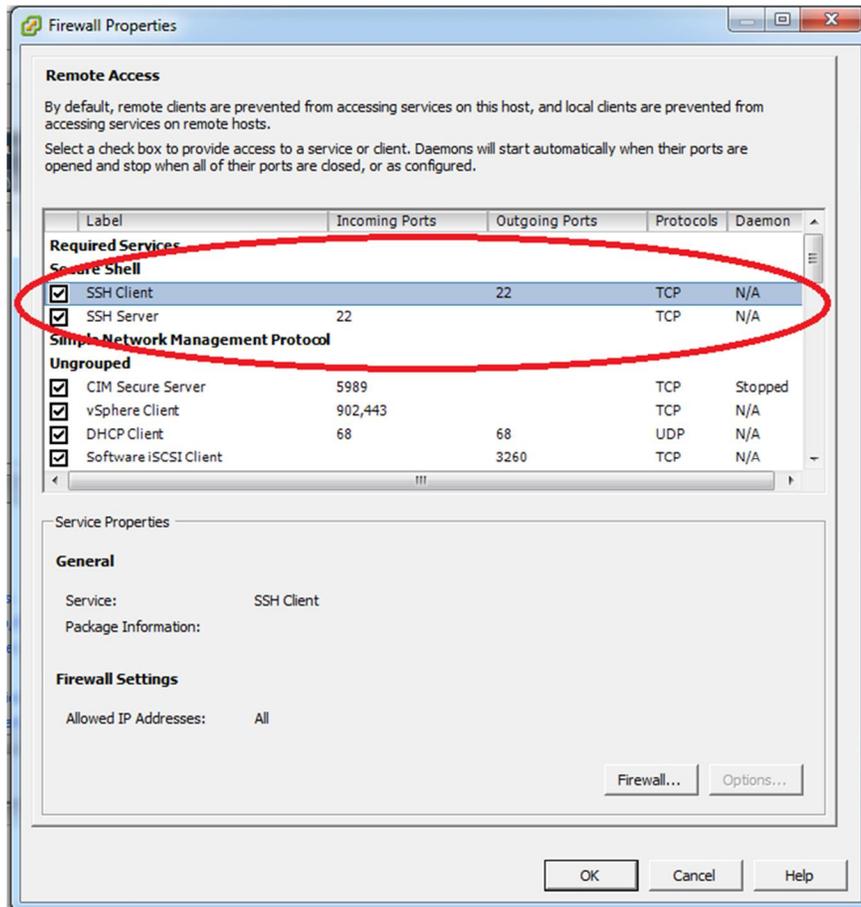


Figure 3.1.18 allow SSH through firewall

NOTE: At this point there is a shortcut we can take to make the installation process faster. The steps will specify the steps here if you would like to use the script it does make the process faster but you will learn more of the internal workings of the networking if you do this manually the first time.

1. Skip to section 3.3.1 and download and decompress the images
2. Run the script by running the command `sh /vmfs/volumes/datastore1/esxi_setup` from the esxi console
3. Continue with the documentation from section 3.4

KNOWN ISSUES: if you do not have 6 physical network connections on your server this script will not set up the physical networking correctly. If you do not have 6 physical network connections on your server it will throw errors while configuring the physical network connections. This script will configure all internal networking and machines correctly. If you decide to use this script anyways review Figure 3.2.12 after running the script to make sure your networks are setup correctly.

Step 3.2: Setting up the ESXi virtual networks.

Overview

In this section you will configure ESXi to create several virtual networks needed to create ISERink.

Step 3.2.1: ESXi Virtual Network Configuration

In this section the virtual network will be created to provide the foundation to connect the various components of ISEAGE. It is important that you name the virtual switches exactly as shown in the directions. That way when you add the pre-built virtual machines later, the network connections will be automatically made.

Note: These instructions are written to include configuration for 6 physical network connections on your server. If your server doesn't have 6 physical network connections to spare, then you will need to decide how to best utilize the physical NIC's that you will use for your ISERink installation.

Alternative configurations: if there are less than 6 physical network connections on your server here are some solutions on how to get by with the fewest issues. If both of these are done an ISERink can use as few as 4 physical network connections with limited impact.

1. **Blue-2:** Blue-1 and Blue-2 both provide 15 class C subnets. If less than 15 subnets will be used then Blue-2 does not need to be on a physical network connection. If this is done then users must make sure the subnets they are using are on blue-1. Since blue-2 will not be available outside the physical machine.

Copyright © 1995-2016, Iowa State University of Science and Technology. All rights reserved.

2. **TAP:** the TAP port is used to listen to all communications in the ISERink, if you do not plan on using this for traffic analysis or anything else this does not need to be mapped to a physical network connection. This will have no effect on the ISERink's operations.

Step 3.2.2: Modify vSwitch0

1. In the vSphere client, go to the **Configuration** tab.
2. Click on the **Networking** link in the **Hardware** box on the left. The initial configuration will look similar to Figure 3.2.1.

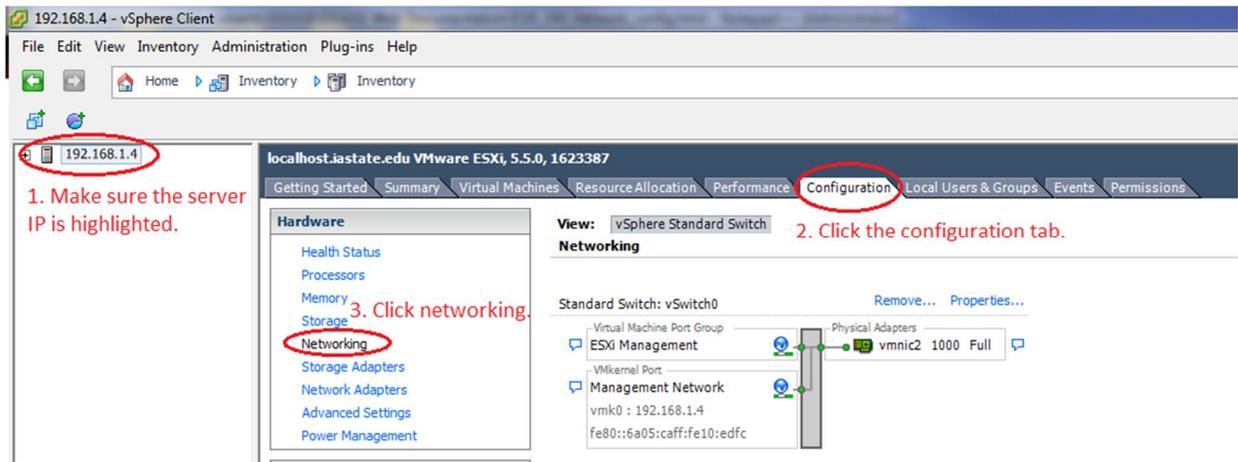


Figure 3.2.1: Network Configuration Section

3. Click on the **Properties...** link next to vSwitch0

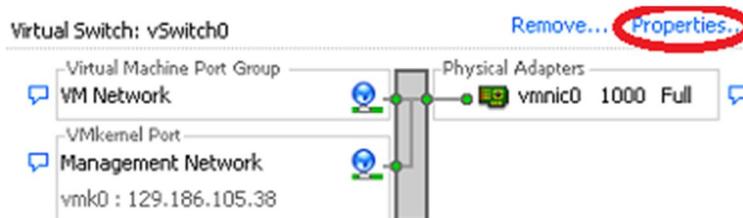


Figure 3.2.2: Initial Network Configuration

4. Make sure that the vSwitch is highlighted and then click the **Edit...** button.

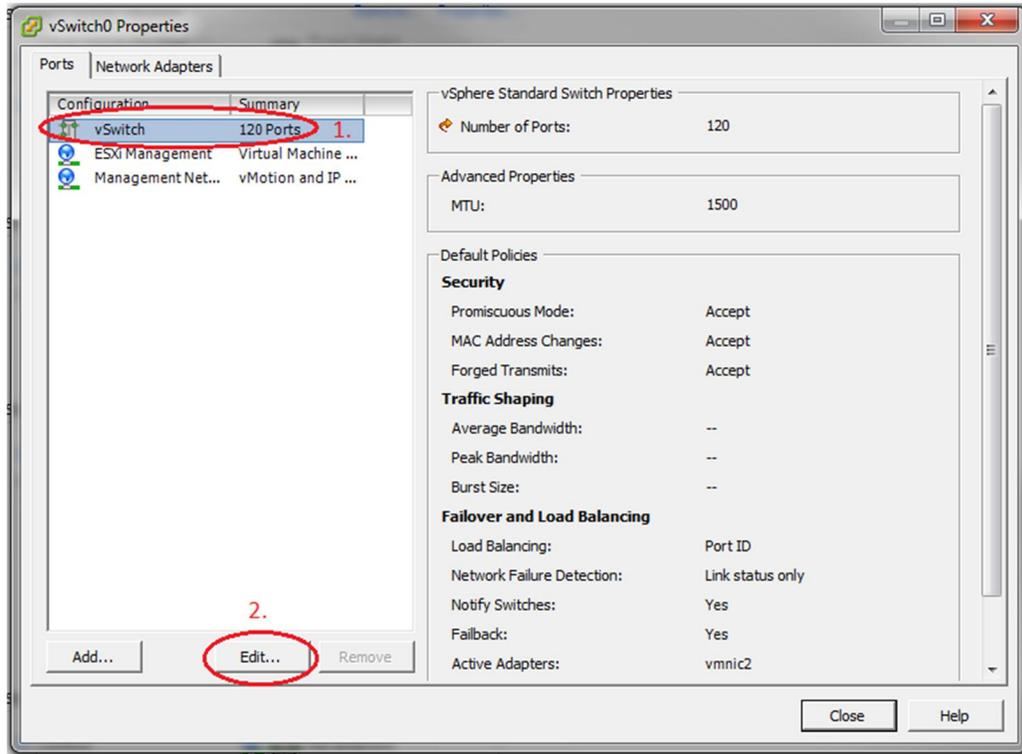


Figure 3.2.3: Switch Settings

5. Go to the **Security** tab and change **Promiscuous Mode** to **Accept** and then click **OK**.

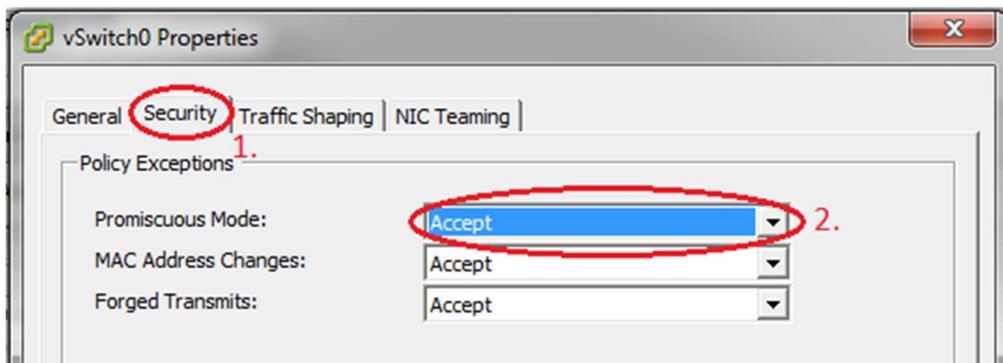


Figure 3.2.4: Promiscuous Mode

6. Next, highlight the second item in the list on the left (the name of the vSwitch) and then click the **Edit...** button.

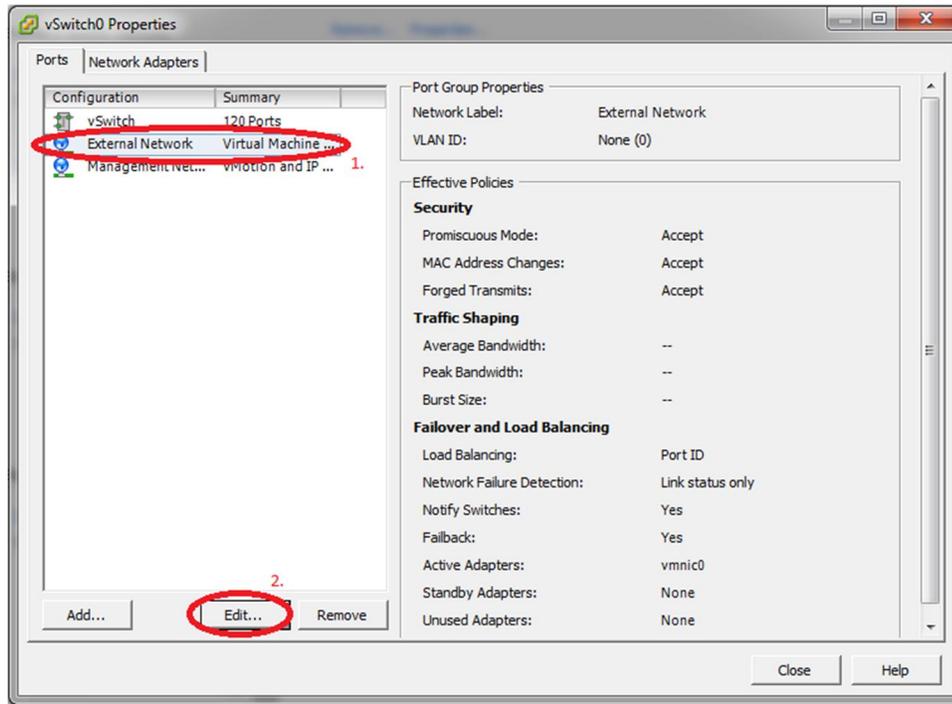


Figure 3.2.5: Edit vSwitch Name

7. Change the name of the vSwitch to be "External Network", click **OK**, and then click the **Close** button on the vSwitch properties window.

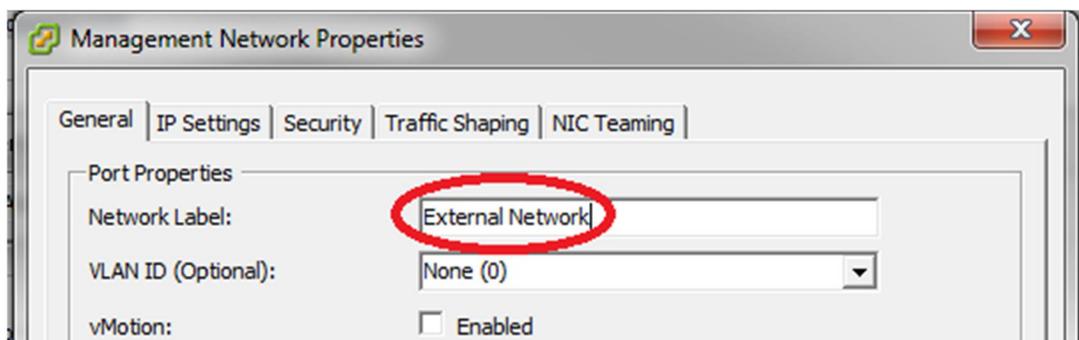


Figure 3.2.6: Change vSwitch Name

Step 3.2.3: Add the other vSwitches

1. Now, click on **Add Networking...** to create a new vSwitch.

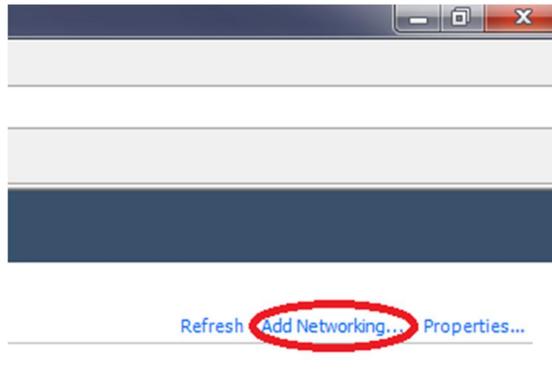


Figure 3.2.7: Add vSwitch

2. Click **Next** to create a Virtual Machine type switch.

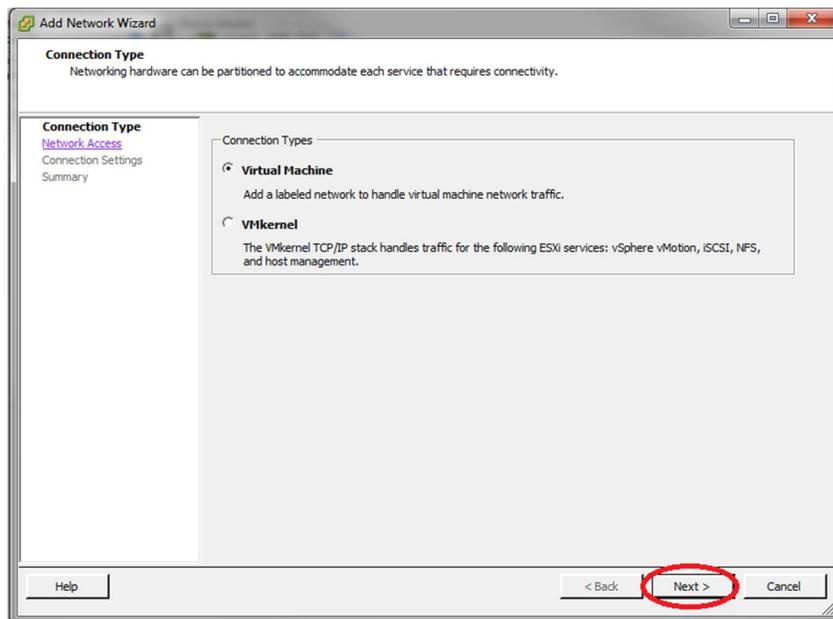


Figure 3.2.8: Create a VM Switch

3. Make sure all of the physical network connection (vmnicX) boxes are unchecked for this switch to create a purely virtual switch and then click **Next**.

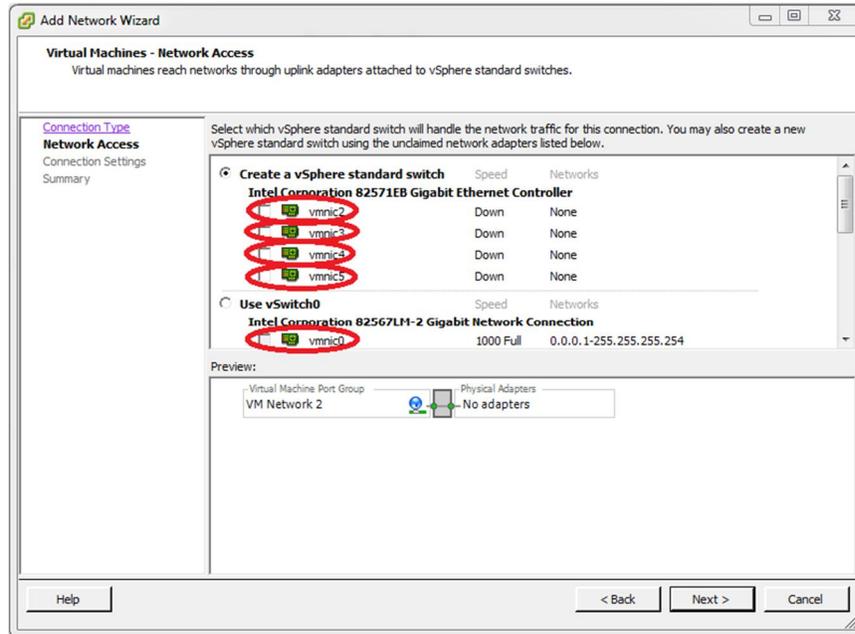


Figure 3.2.9: Edit vSwitch Physical Connections

4. Name the switch "Air Gap", click **Next**, and then click **Finish** on the next screen.

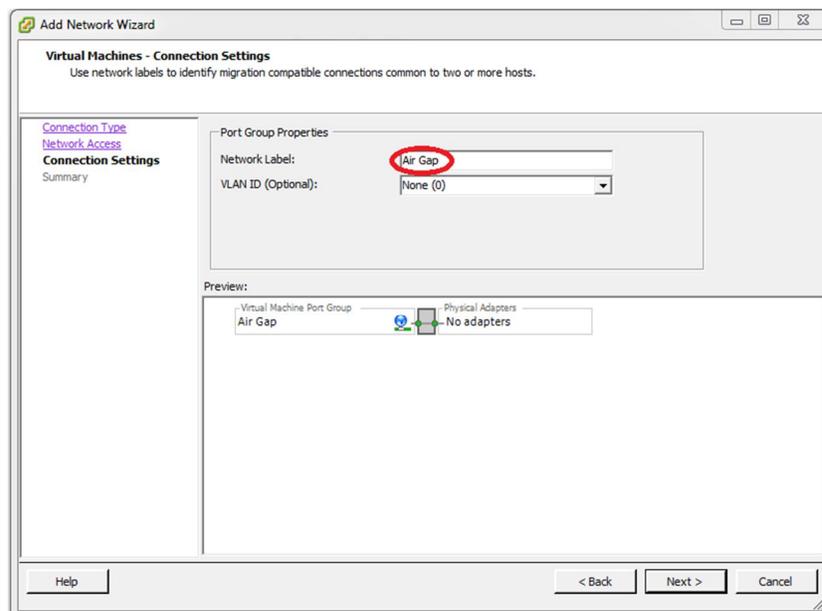


Figure 3.2.10: Name the vSwitch Air Gap

5. Your virtual network layout should now look similar to Figure 3.2.11

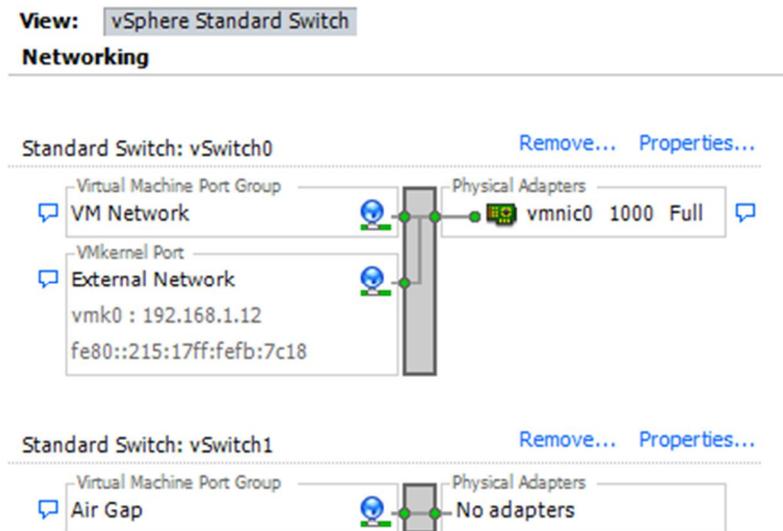


Figure 3.2.11: Network layout

6. Repeat steps 1 through 5 to create all of the switches shown in Table 1 to create the Virtual Network for ISEAGE. Do not worry about the promiscuous column for now. We will take care of this in the next step.

Name	Network Label	Promiscuous	Network Adapter (Vmnics)
vSwitch0	External Network	Yes	Vmnic0
vSwitch1	Air Gap	No	None
vSwitch2	Backplane	Yes	None
vSwitch3	Control	Yes	None
vSwitch4	Keyhole	Yes	Vmnic1
vSwitch5	Blue-1	Yes	Vmnic2
vSwitch6	Blue-2	Yes	Vmnic3
vSwitch7	Red-green	Yes	Vmnic4
vSwitch8	TAP	Yes	Vmnic5
vSwitch9	Ice Bridge	Yes	None
vSwitch10	pfSense WAN	Yes	None
vSwitch11	Private Net	Yes	None (optional)

Figure 3.2.12: Networking configuration overview

7. Now we will go back through the switches we just created and enable promiscuous mode.

8. Click on the **Properties...** link next to vSwitch0

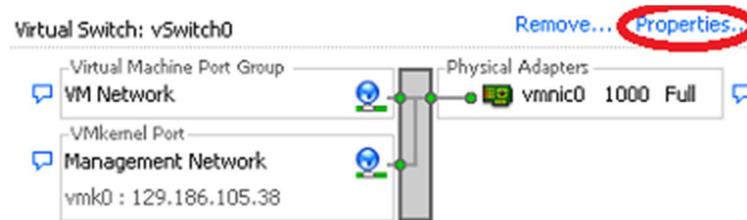


Figure 3.2.13: Initial Network Configuration

9. Make sure that the vSwitch is highlighted and then click the **Edit...** button.

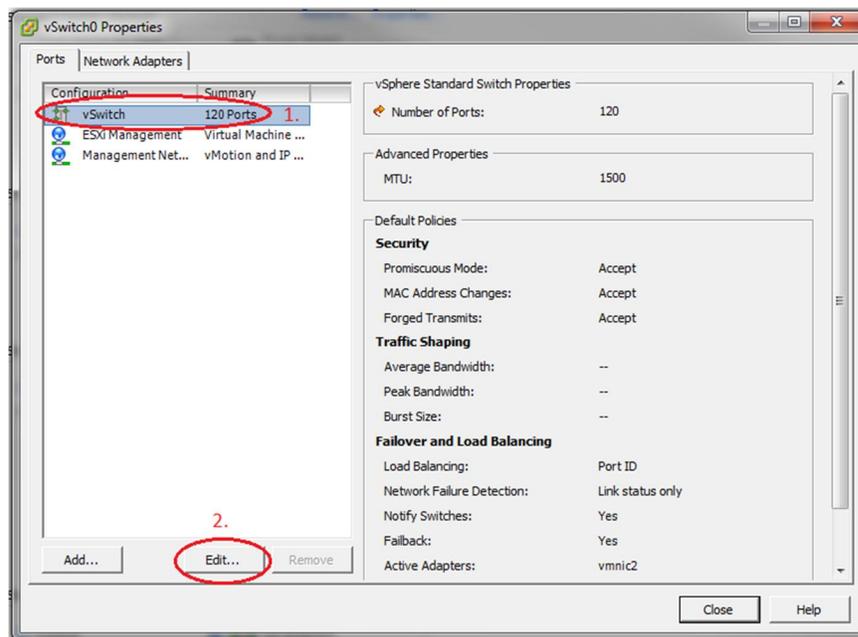


Figure 3.2.14: Switch Settings

10. Go to the **Security** tab and change **Promiscuous Mode** to **Accept** and then click **OK**.

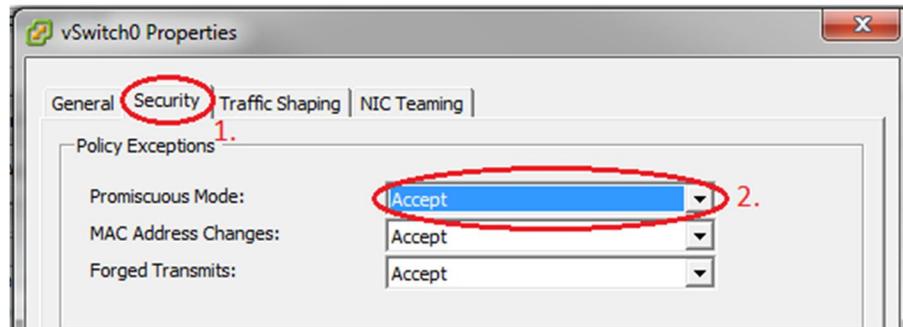


Figure 3.2.15: Promiscuous Mode

11. Repeat steps 8 through 10 for the rest of the switches (except vSwitch1 - Air Gap) to enable promiscuous mode on the rest of the switches.

Step 3.3: Downloading and installing the individual Virtual Machines for ISERink.

Overview

In this section we will download and install the Virtual Machines images to build ISEAGE. All network connections should automatically be made if the network is configured correctly.

Step 3.3.1: Download Virtual Machines

1. Log into the ESXi machine using either the ESXi console or using SSH. The figures shown in this step are from using SSH to access the ESXi server.

- Once you have logged into the system change into the directory that holds the data store as shown in Figure 3.3.1. using the command “cd /vmfs/volumes/datastore1”

```
SSH Secure Shell 3.2.9 (Build 282)
Copyright (c) 2000-2003 SSH Communications Security Corp - http://www.ssh.com/

This copy of SSH Secure Shell is a non-commercial version.
This version does not include PKI and PKCS #11 functionality.

The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
~ # cd /vmfs/volumes/datastore1/
/vmfs/volumes/549ae29b-1b4a64e5-12e0-180373f1e0ab #
```

Figure 3.3.1 Change directory to the datastore

- Copy the virtual machine images from the repository `isechest.iac.iastate.edu` using `scp` command as shown in Figure 3.3.2. The total size of the images is about 10GB in size, so the transfer make take some time. **NOTE:** Use the username and password provided to you when you registered to get access to ISERink.

```
scp "USERNAME@isechest.iac.iastate.edu:/home/downloads/ISERink/v1/*" .
```

```
/vmfs/volumes/54a42edb-a840a048-82b4-180373f1e0ab # scp "iserink001@isechest.iac.iastate.edu:/home/downloads/ISERink/v1/*" .
The authenticity of host 'isechest.iac.iastate.edu (129.186.105.47)' can't be established.
RSA key fingerprint is 2f:5c:11:e3:17:6f:f0:b0:97:b9:ca:ae:f7:83:db:20.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'isechest.iac.iastate.edu,129.186.105.47' (RSA) to the list of known hosts.
Password for iserink001@isechest.iac.iastate.edu:
Board1.tar.gz          100% 337MB 21.1MB/s 00:16
Board2.tar.gz          100% 337MB 22.5MB/s 00:15
Board3.tar.gz          100% 337MB 26.0MB/s 00:13
Board4.tar.gz          100% 337MB 24.1MB/s 00:14
Board5.tar.gz          100% 325MB 23.2MB/s 00:14
Gatekey.tar.gz         100% 3038MB 25.3MB/s 02:00
Green-KALI.tar.gz      100% 3154MB 26.5MB/s 01:59
IScorE.tar.gz          100% 2081MB 25.1MB/s 01:23
Keyhole1.tar.gz        100% 619MB 22.1MB/s 00:28
Keyhole2.tar.gz        100% 564MB 24.5MB/s 00:23
Snowbank.tar.gz        100% 313MB 24.1MB/s 00:13
Snowflake.tar.gz       100% 842MB 27.2MB/s 00:31
White-DHCP.tar.gz      100% 103MB 25.7MB/s 00:04
decompress             100% 330 0.3KB/s 00:00
/vmfs/volumes/54a42edb-a840a048-82b4-180373f1e0ab #
```

Figure 3.3.2 Copying files from `isechest.iac.iastate.edu`

- Once the files have been copied there will be several compressed tar files and a shell script called **decompress**. Note the decompression may take several hours. Type the command:

“sh decompress”

Note: if you are using the script to automate the setup process you can skip to section 3.4

Step 3.3.2: Install the Virtual Machines

- As described in Section 2, ISERink consists of multiple interconnected virtual machines. The table below lists the virtual machines and the virtual networks they are connected to.

Machine Name	OS Type	Adapter 1	Adapter 2	Adapter 3
Snowbank	FreeBSD	External Network	Ice Bridge	
Snowflake	FreeBSD	Ice Bridge	Control	Backplane
Gatekey		Ice Bridge	Control	
Keyhole1	FreeBSD	Keyhole	Air Gap	Control
Keyhole2	FreeBSD	Ice Bridge	Air Gap	Control
Board 1	FreeBSD	Blue-1	Backplane	Control
Board 2	FreeBSD	Blue-2	Backplane	Control
Board 3	FreeBSD	Red-green	Backplane	Control
Board 4	FreeBSD	Keyhole	Backplane	Control
Board 5	FreeBSD	TAP	Backplane	Control
ISCorE	Ubuntu	External Network	Private Net	Keyhole
Green-KALI	KALI Unix	Red-Green		
White-DHCP	PFSense	pfSense WAN	Keyhole	

2. After copying and uncompressing the Virtual Machine images, we need to open up the datastore browser on ESXi. First, log into ESXi if not already, then go to **Configuration** then **Storage** and the right click on your datastore, and then go to **Browse Datastore...**

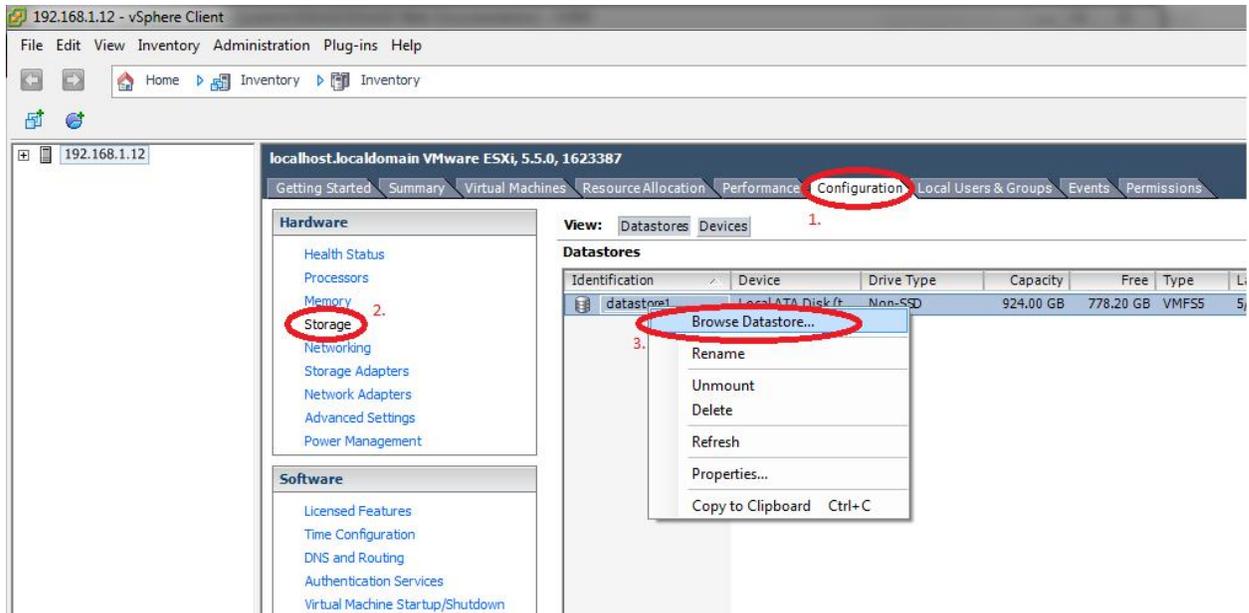


Figure 3.3.3: Browse Datastore

- You must add all of the VMs to ESXi. To do this, click on one of the VM folders. Then find the Virtual Machine file (ending in .vmx) and click it to highlight the file. After highlighting the Virtual Machine file, click on the button in the upper left corner of the Database Browser window to add the virtual machine to the inventory. A window will open. Leave the Virtual Machine name alone and click **next**. On the following window also click **next**. On the final window click **finish**. Repeat these steps for all of the Virtual Machines.

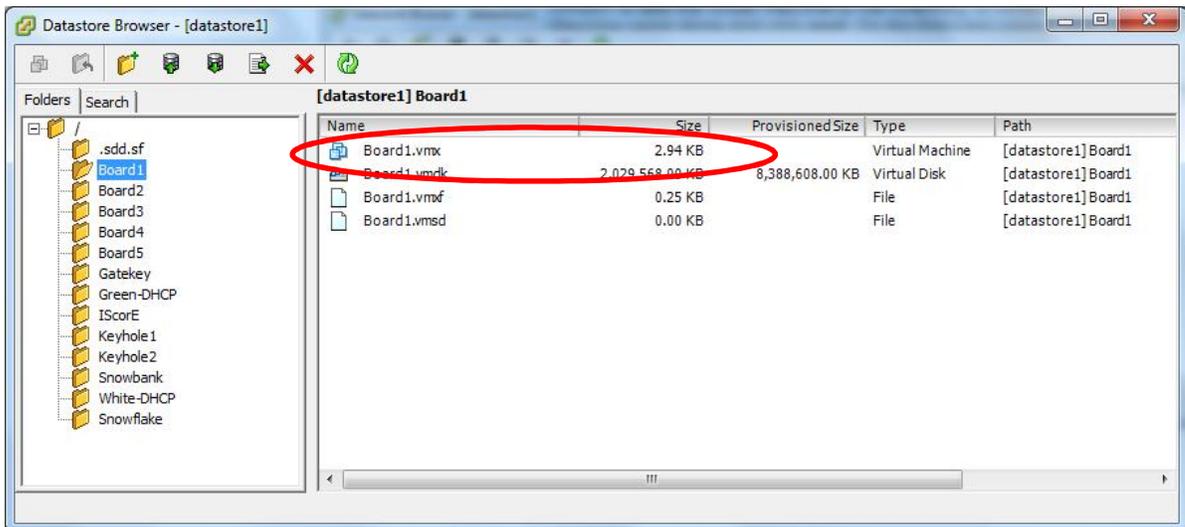


Figure 3.3.4: Add VM to Inventory

- After adding all of the Virtual Machines to the inventory, we need to manually start up all of the Virtual Machines to allow ESXi to update their configuration information. Click on each VM and you will see a window with “Power on the virtual machine” (Figure 3.3.6). Click on that for each machine. Note: you should power on the virtual machines in the following order. (We will later setup ESXi to power them on automatically)

Snowbank
Snowflake
Keyhole1
Keyhole2
Board 1
Board 2
Board 3
Board 4
Board 5
ISCorE
Gatekey
Green-KALI
White-DHCP

Figure 3.4.5 VM List

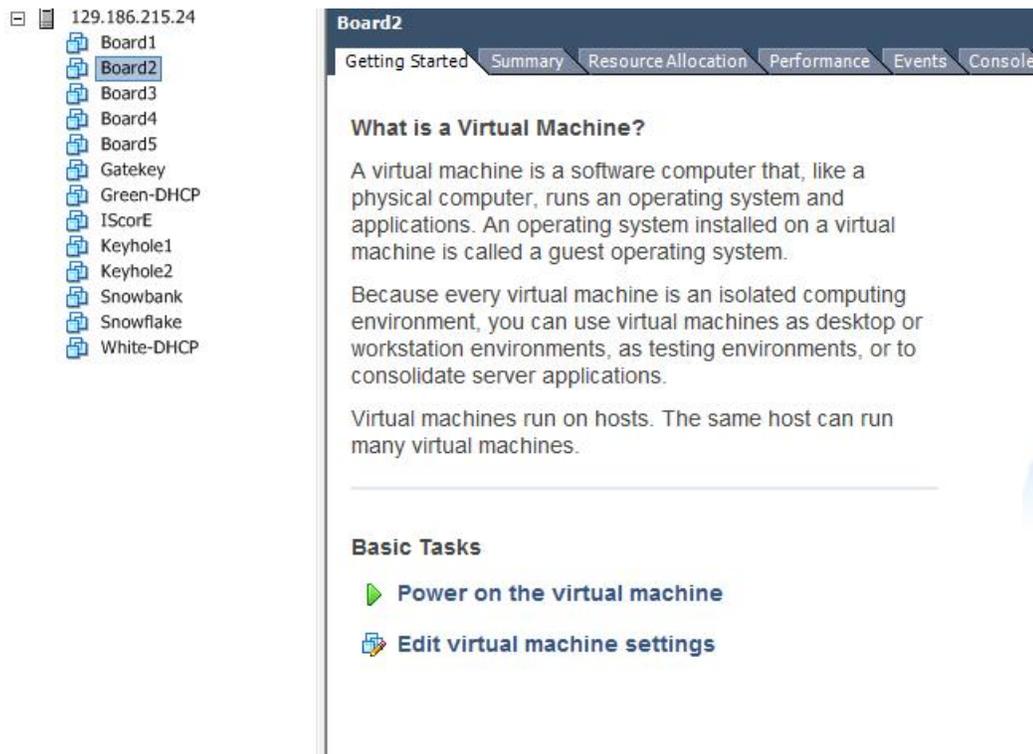


Figure 3.3.6: Power on each VM

5. A window may pop up asking if you moved or copied the Virtual Machine. Check the **Copied it** option and then click **OK** as seen in Figure 3.3.7A. Alternatively you may see the question icon next to your virtual machine name in this case you will have to go to the virtual machines setting tab and Check the **Copied it** option and then click **OK** as seen in Figure 3.3.7B. Repeat these last two steps for the rest of the Virtual Machines.

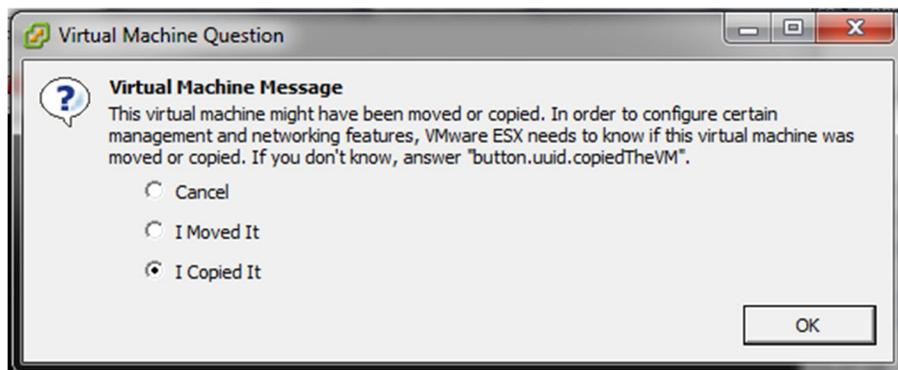


Figure 3.3.7A: VM First Boot Message

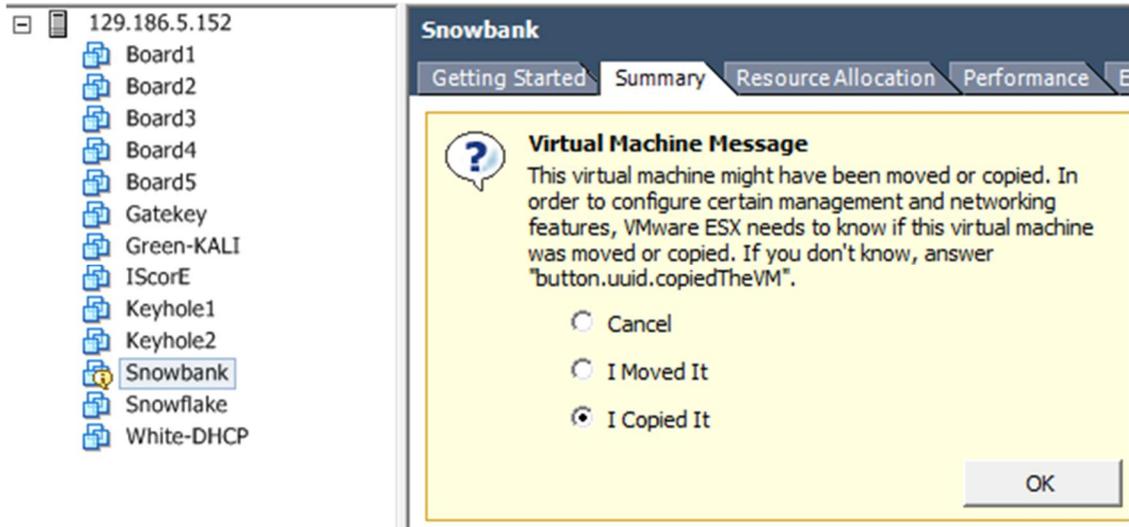


Figure 3.3.7B: VM First Boot Message

- At this point all of the Virtual Machines should be installed and configured correctly. Next, we are going to configure the auto-start feature of ESXi to start up the Virtual Machines in the correct order whenever the physical server is powered up.

Step 3.3.3 Configure Auto-startup

- In this section we will configure the Virtual Machines to automatically start up in the correct order when the physical server is started. Go to the **Configuration** tab, click on **Virtual Machine Startup/Shutdown** and then click **Properties**.

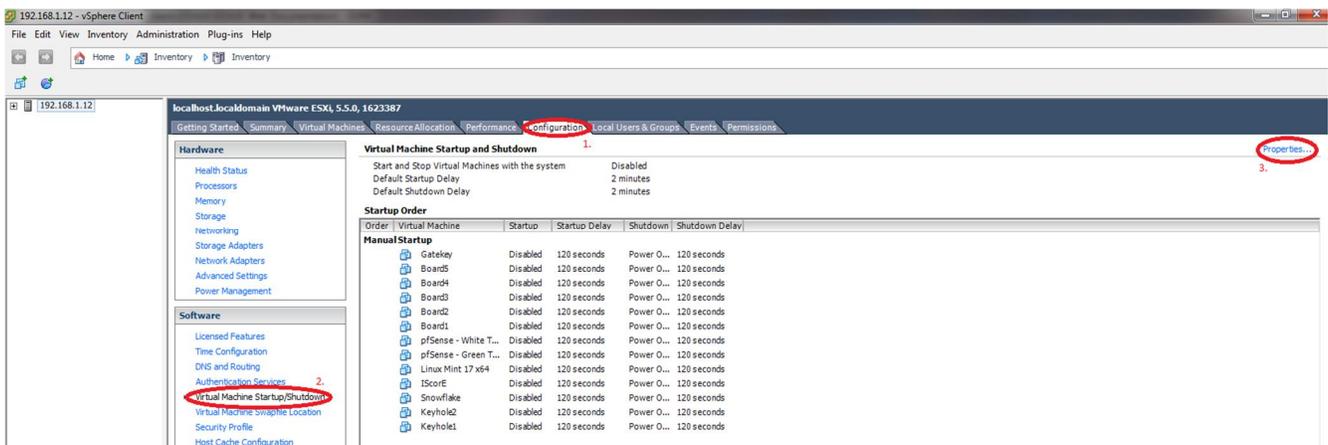


Figure 3.3.8: VM Startup/Shutdown Configuration

- In the configuration window which opens up, check the two options in the upper left side of the window.

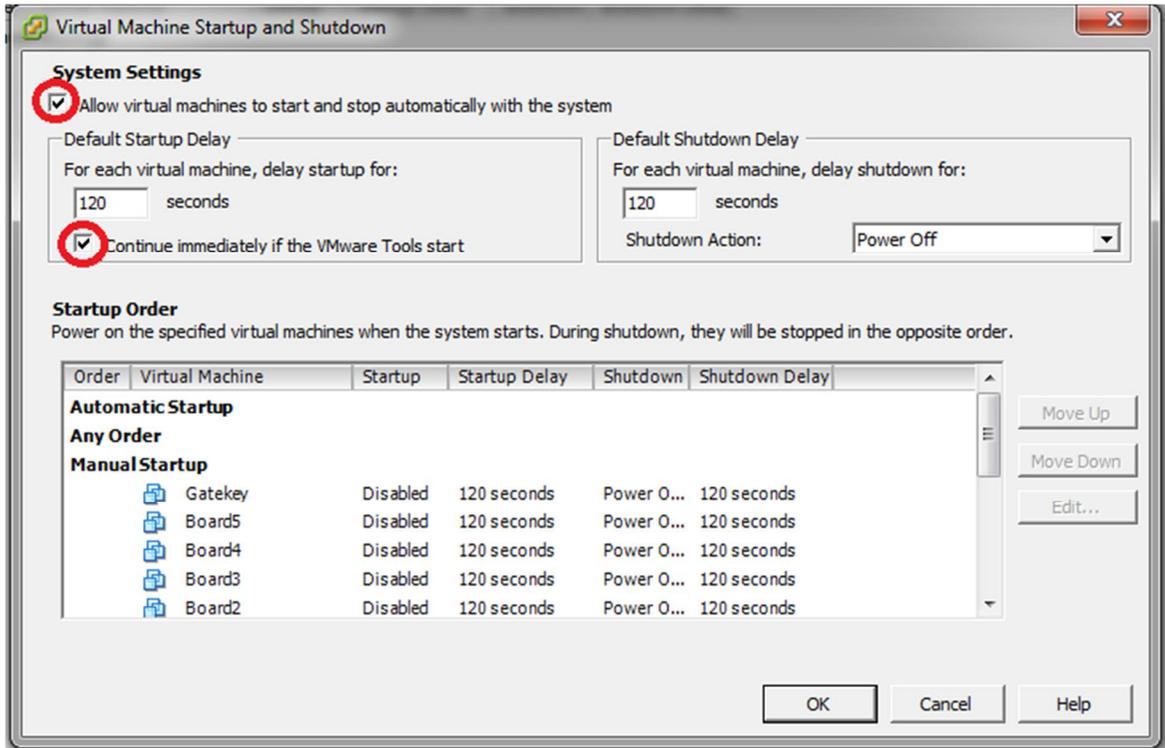


Figure 3.3.9: VM Startup/Shutdown Options

- Now we will configure the order in which the Virtual Machines will start up. First find the **Snowbank** Virtual Machine and click it to highlight it. Now, repeatedly click on the **Move Up** button to move the Snowbank VM into the **Automatic Startup** section.

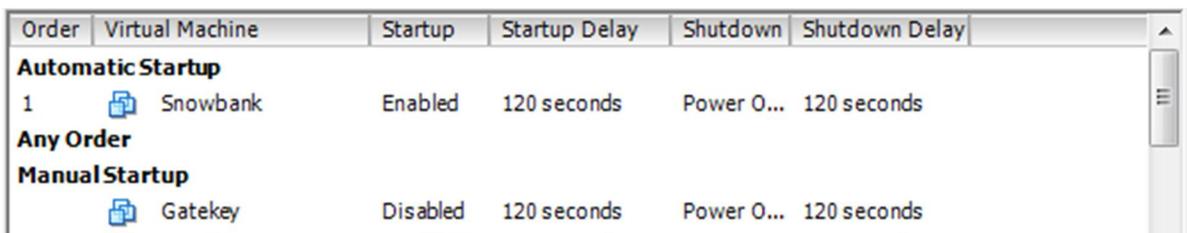


Figure 3.3.10: Snowbank Autostart

- Continue this process for the rest of the VMs until the startup order is the same as in Figure 3.3.11.

Startup Order					
Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	 Snowbank	Enabled	120 seconds	Power O...	120 seconds
2	 Snowflake	Enabled	120 seconds	Power O...	120 seconds
3	 Keyhole2	Enabled	120 seconds	Power O...	120 seconds
4	 Keyhole1	Enabled	120 seconds	Power O...	120 seconds
5	 Board1	Enabled	120 seconds	Power O...	120 seconds
6	 Board2	Enabled	120 seconds	Power O...	120 seconds
7	 Board3	Enabled	120 seconds	Power O...	120 seconds
8	 Board4	Enabled	120 seconds	Power O...	120 seconds
9	 Board5	Enabled	120 seconds	Power O...	120 seconds
10	 IScorE	Enabled	120 seconds	Power O...	120 seconds
11	 Gatekey	Enabled	120 seconds	Power O...	120 seconds
12	 White-DHCP	Enabled	120 seconds	Power O...	120 seconds
13	 Green-KALI	Enabled	120 seconds	Power O...	120 seconds

Figure 3.3.11: Startup Order

Step 3.4: Configure snowbank, Snowflake, keyhole1, Idap, and IScorE

Step 3.4.1: Configure snowbank

- The first step is to login into the ESXi server using vSphere. Once you have logged in you will need to select gatekey in the list of virtual machines and then click the summary tab, as shown in Figure 3.4.11

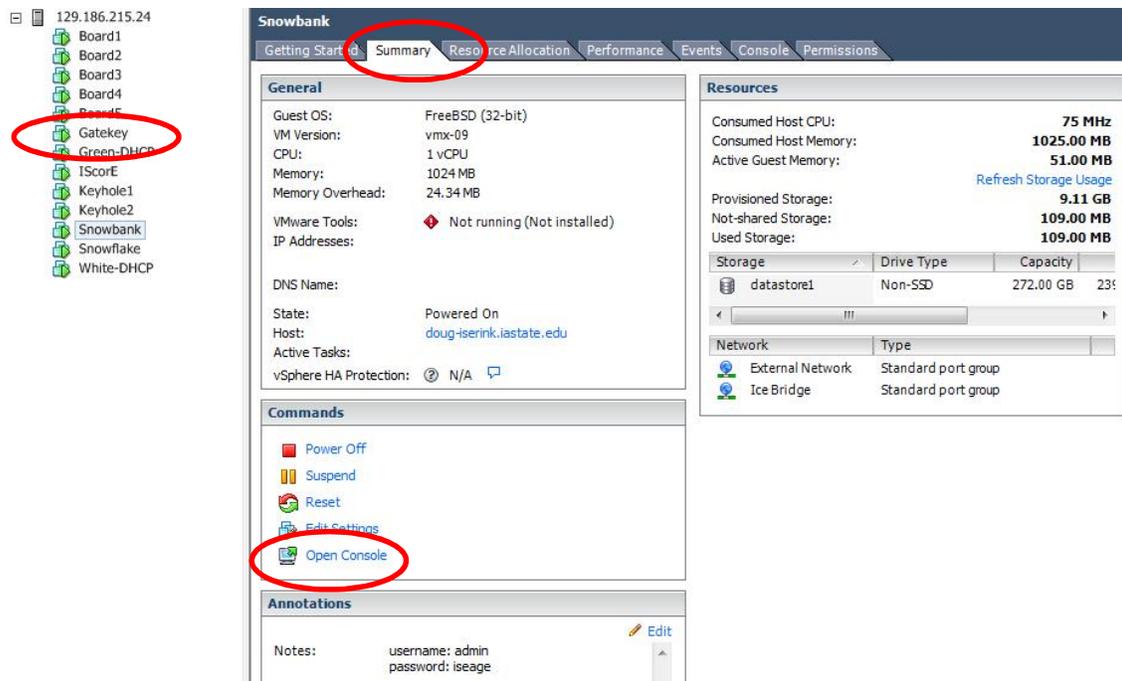


Figure 3.4.1 selecting gatekey virtual machine

2. Select "Open Console". A new window will appear, which is the console window for gatekey which is a GUI based UNIX machine, as shown in Figure 3.4.2. You will need run firefox to access the firewall (snowbank),

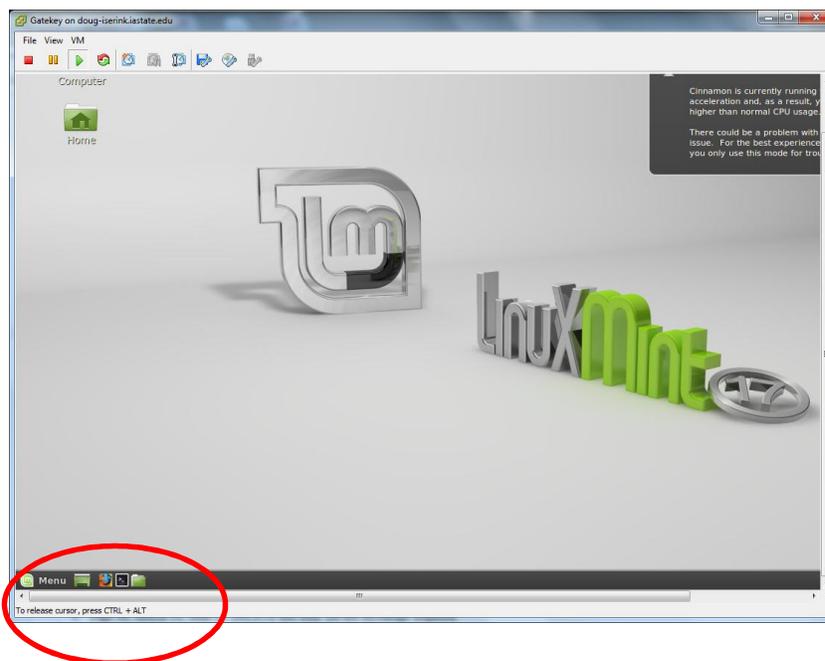


Figure 3.4.2 gatekey console

3. You need to type in the address of snowbank to access the admin console (192.168.1.1). You will see an admin login for the pfSense firewall, see Figure 3.4.3. The default username is “admin” and password is “iseage”.



Figure 3.4.3 Log into the firewall

4. After you have logged in you need to select the WAN interface to edit the WAN address and default gateway. See Figure 3.4.4 for all of the steps. After selecting the WAN interface you will see a place to configure the IPv4 address. If you are installing ISERink directly to the internet, this is where you enter the public IP address that you will be using for ISERink. If you are installing ISERink behind a NAT/FW, this is where you enter the private IP address that resides on your NAT/FW network. Then enter the appropriate IP address for your internet gateway. See your system administrator if you are unsure what this should be. Make sure the default gateway box is checked. After entering the new gateway you need to save the configuration and then apply the changes.



Figure 3.4.4 Changing WAN Addresses.

5. After you have configured the WAN address, you can do a quick test to see if it working by pinging the gateway. You can select that option in the diagnostics menu.

Step 3.4.2: Configure IScorE

1. Next you will need to configure IScorE to setup the external IP address. First you will bring up the console window for IScorE. Log in to the IScorE as root, with initial password of "iseage" after you have logged in then cd directory to "/etc/network", as shown in Figure 3.4.5.
2. After you have changed into the directory then you will need to edit the file "interface". You can use one of the editors installed on IScroE (vi, nano) to edit the file "interfaces". You will see a large number of networks defined as shown in Figure 3.4.6. Here is where you will modify IScorE's eth0 interface. If you are installing ISERink directly to the internet, then you will use a public IP address, if you are installing ISERink behind a NAT/FW, then you will be using a private IP address from your NAT/FW network. Under the line "iface eth0 inet static" you will need to modify the lines address, netmask and gateway. Change the address, netmask, and gateway values to values that match your configuration, as shown in Figure 3.4.6.

3. Next we will edit the “/etc/hosts” and replace iscore.isssl.org with the FQDN of your IScorE. So for example you will change iscore.isssl.org to iscore.myschool.edu.
4. After you have modified the file issue the command “reboot” and wait for IScorE to restart.
5. After IScorE has restarted you are ready to continue with the IScorE configuration.

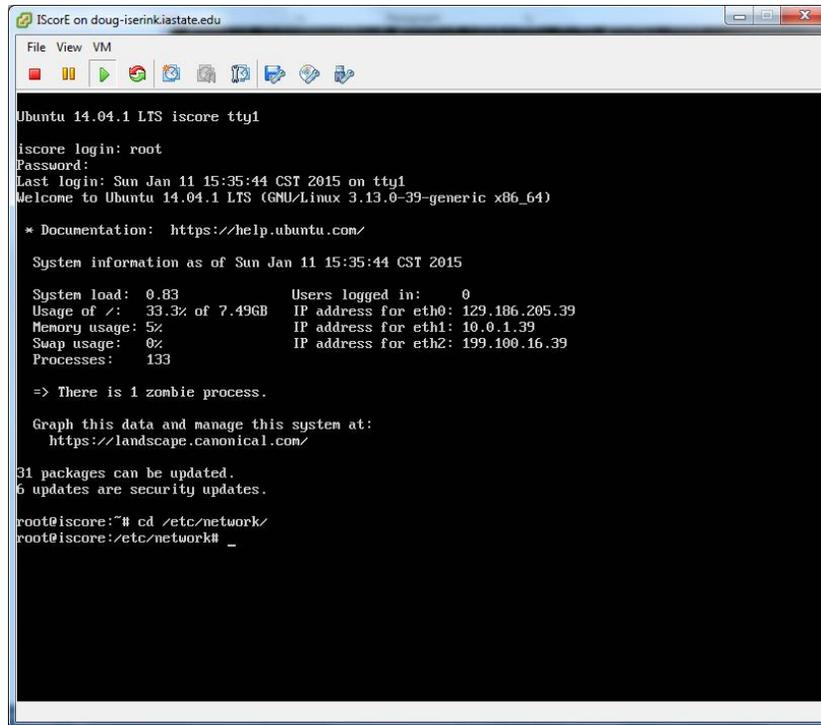


Figure 3.4.5 Login into IScorE

```
IScorE on doug-iserink.iastate.edu
File View VM
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 129.186.205.39
    netmask 255.255.255.0
    gateway 129.186.205.254

auto eth1
iface eth1 inet static
    address 10.0.1.39
    netmask 255.255.0.0

auto eth2
iface eth2 inet static
    address 199.100.16.39
    netmask 255.255.255.0
    dns-nameservers 199.100.16.100
    dns-search iserink.com

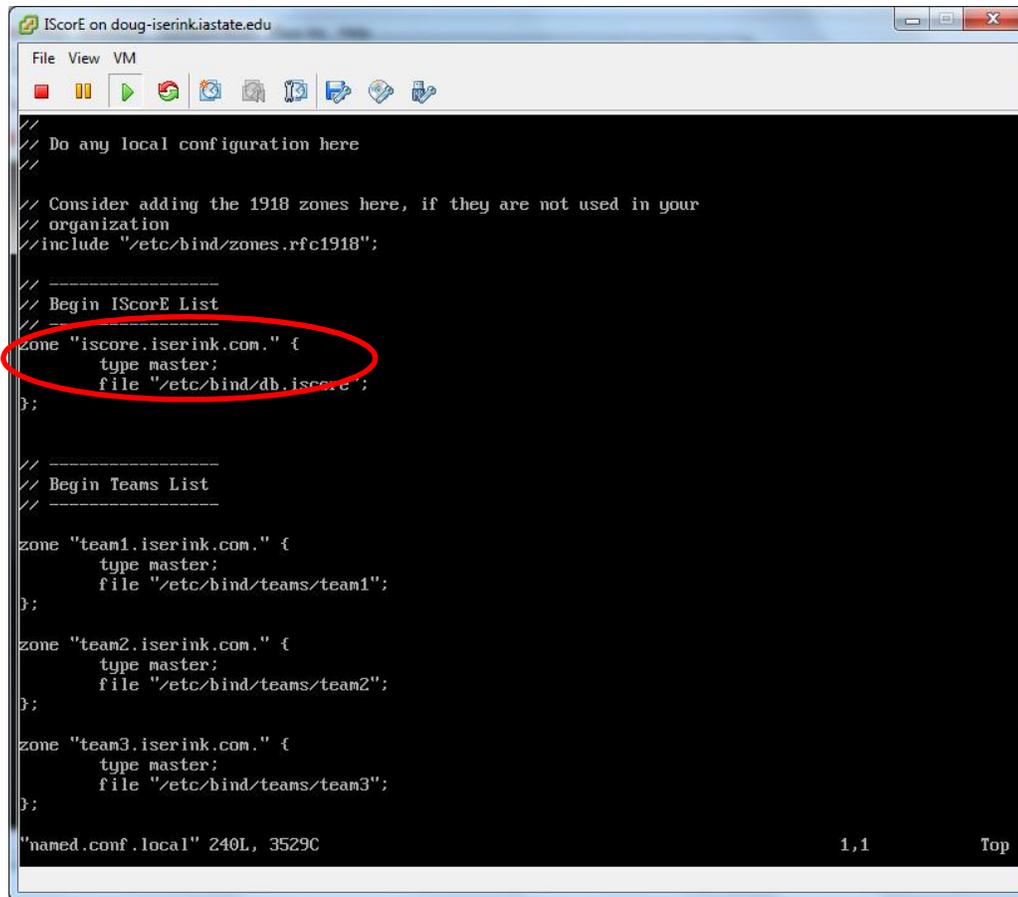
# Static routing to each red/green range
up route add -net 12.110.0.0/16 gw 199.100.16.254 dev eth2

# Static routing to UPN range
up route add -net 10.8.0.0/16 gw 199.100.16.100 dev eth2

# Static routing out to each blue range
up route add -net 64.39.3.0/24 gw 199.100.16.254 dev eth2
up route add -net 33.96.5.0/24 gw 199.100.16.254 dev eth2
up route add -net 201.203.200.0/24 gw 199.100.16.254 dev eth2
"interfaces" 77L, 3347C
1,1 Top
```

Figure 3.4.6 Editing interfaces

- Next you will need to configure IScorE to setup the internal DNS entries. From the command line edit the file `/etc/bind/named.conf.local` as shown in Figure 3.4.7. You will need to change the zone name to match the DNS entry for your IScorE. So for example you will change `iscore.iserink.com` to `iscore.myschool.edu`.



```
IScorE on doug-iserink.iastate.edu
File View VM
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//
//-----
// Begin IScorE List
//
zone "iscore.iserink.com." {
    type master;
    file "/etc/bind/db.iscore";
};
//
//-----
// Begin Teams List
//
zone "team1.iserink.com." {
    type master;
    file "/etc/bind/teams/team1";
};
zone "team2.iserink.com." {
    type master;
    file "/etc/bind/teams/team2";
};
zone "team3.iserink.com." {
    type master;
    file "/etc/bind/teams/team3";
};
"named.conf.local" 240L, 3529C 1,1 Top
```

Figure 3.4.7 Change DNS for IScorE

7. After this step you can restart bind by typing “service bind9 restart”
8. Next we will change the Django settings file “var/www/iscore/settings.py” to tell nginx what host/domain names that IScorE can serve. Make sure the ALLOWED_HOSTS line includes the internal IScorE IP address 199.100.16.39, the FQDN of your ISCORE and the IP for IScorE that you set on IScorE’s Eth0, as seen in Figure 3.4.8. For example you would change iscore.isssl.org to iscore.myschool.edu and 129.186.215.26 to your IP address for IScorE.

```

# Django settings for iscore project.
SETTINGS_PATH = os.path.normpath(os.path.dirname(__file__))
SITE_ROOT = os.path.realpath(os.path.dirname(__file__))
URL_ROOT = '/'
PROFILE_LOG_BASE = os.path.normpath(os.path.dirname(__file__)) + 'logs/'

DEBUG = False # False on Production, True in Development
TEMPLATE_DEBUG = False # False on Production, DEBUG in Development

# A list of strings representing the domain names IScorE can answer too
# Only needed in prod, has no effect when DEBUG = True
ALLOWED_HOSTS = ['199.100.16.39', 'iscore.issl.org', '129.186.215.26']
# ALLOWED_HOSTS = ['*.com', '* edu']
# ALLOWED_HOSTS = [*]

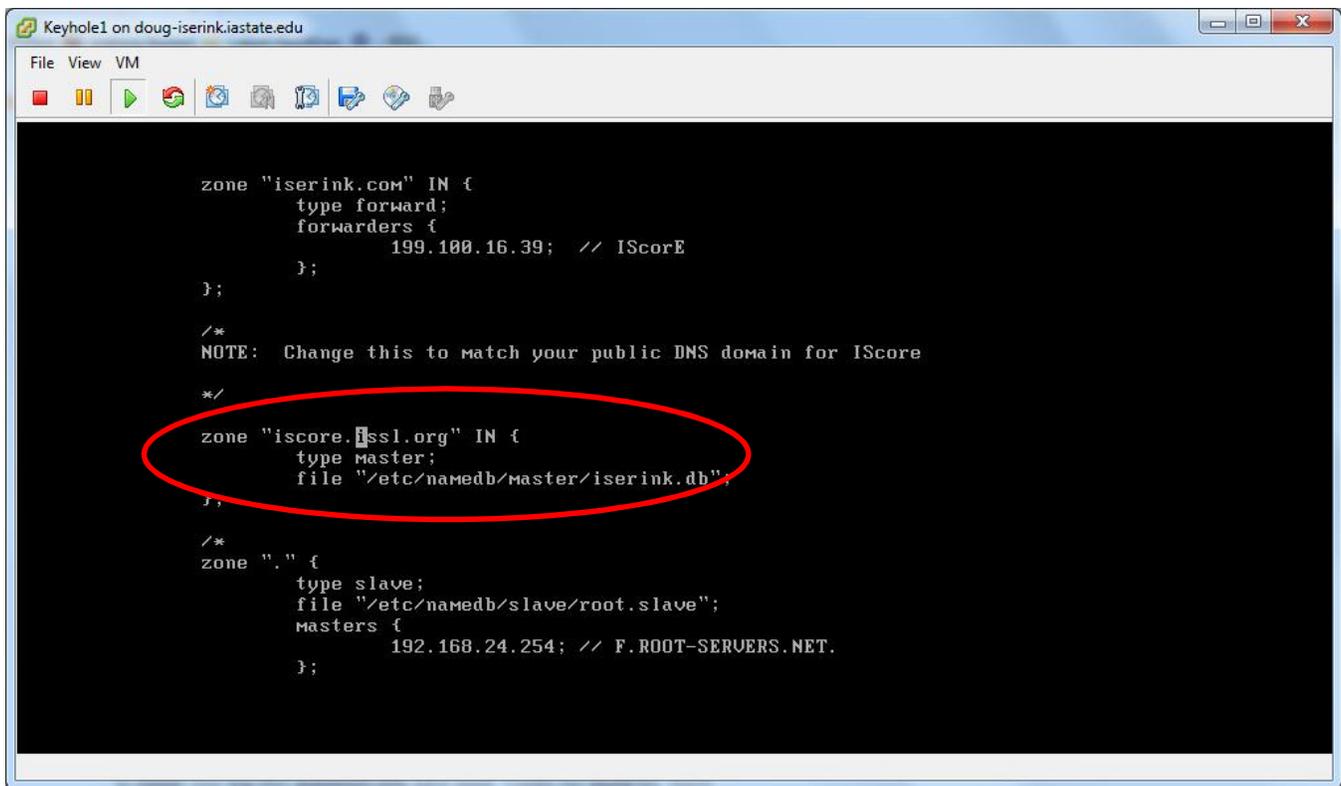
```

Figure 3.4.8 Changing allowed hosts

9. After this step you can IScorE by typing “supervisorctl restart iscore”
10. Next you will need to add an SSL certificate to IScorE. Change into the directory “/etc/nginx/ssl” and type “sh mk_key”. It will ask you several questions, including a password for the key, you only need to remember it while running the script. The password for the key is stripped off during the process. Another important field is the “common name” this needs to be the FQDN of your IScorE.
11. After this step you can restart nginx by typing “service nginx restart”

Step 3.4.3: Configure keyhole1

1. Next you will need to configure keyhole to resolve the DNS entry for your IScorE. In order for users inside the competition network to be able to access IScorE using the same domain name as external users you need to change the file /etc/namedb/named.conf as shown in Figure 3.4.11. First you will bring up the console window for keyhole1. Log in to the IScorE as root, with initial password of “iseage”. Edit the file named “/etc/namedb/named.conf” and change the line shown in the figure to match the public DNS name of your IScorE system. After you have changed the file you can restart named by typing: “/usr/local/etc/rc.d/named restart”.



```
Keyhole1 on doug-iserink.iastate.edu
File View VM
zone "iserink.com" IN {
    type forward;
    forwarders {
        199.108.16.39; // IScore
    };
};
/*
NOTE: Change this to match your public DNS domain for IScore
*/
zone "iscore.issl.org" IN {
    type master;
    file "/etc/namedb/master/iserink.db";
};
/*
zone "." {
    type slave;
    file "/etc/namedb/slave/root.slave";
    masters {
        192.168.24.254; // F.ROOT-SERVERS.NET.
    };
};
```

Figure 3.4.11 Changing named.conf

2. Next we need to add a line to the file located at `/etc/named/master/iserink.db`.
3. Before we can edit this file we have to change it's current permissions with the following command.

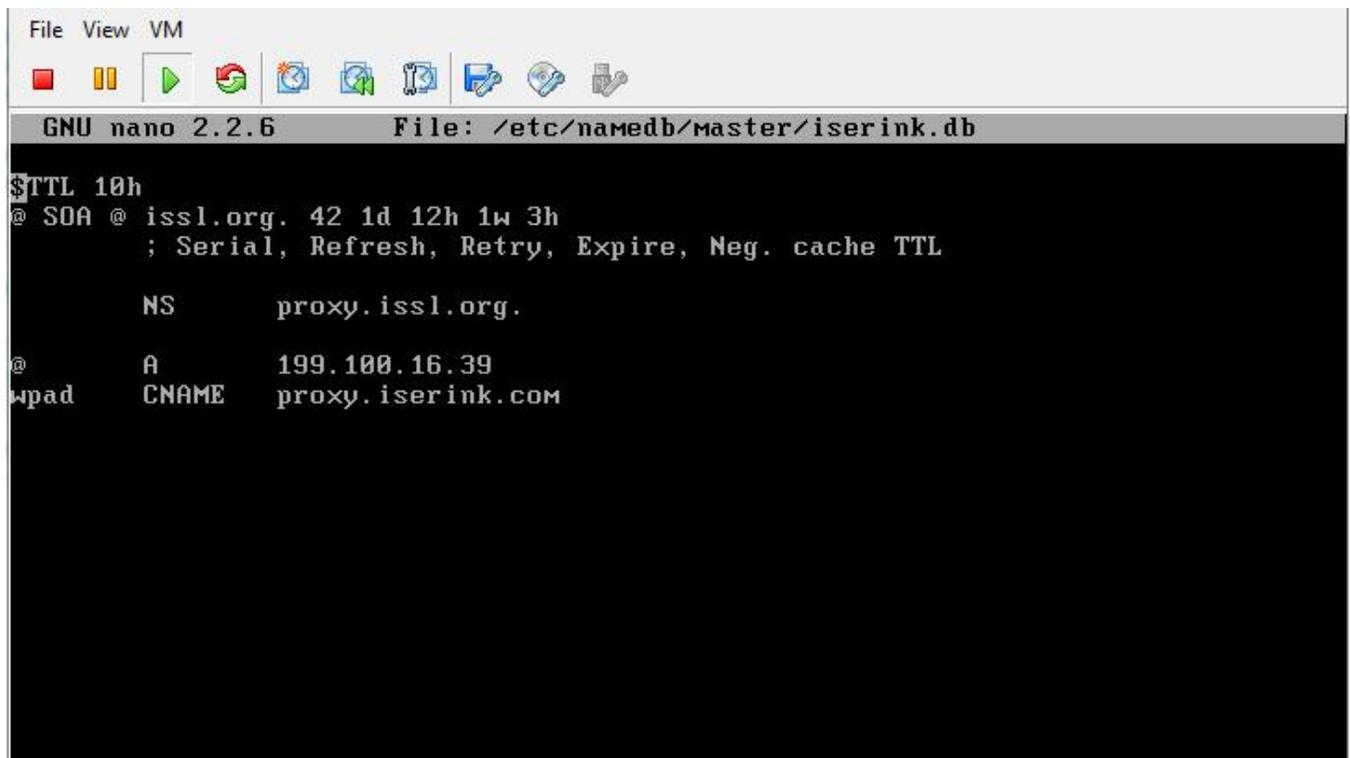
```
chmod 644 /etc/named/master/iserink.db
```

4. Now edit `/etc/named/master/iserink.db` by adding the following line to the end of the file.

```
wpad CNAME proxy.iserink.com
```

5. Save your changes and then change the file perimissions back with the following line.

```
chmod 444 /etc/named/master/iserink.db
```

A screenshot of a terminal window running GNU nano 2.2.6. The window title is "File View VM" and the file being edited is "/etc/namedb/master/iserink.db". The content of the file is a DNS zone file for "issl.org". It includes a SOA record with a TTL of 10h, an NS record pointing to "proxy.issl.org.", an A record for "199.100.16.39", and a CNAME record for "wpad" pointing to "proxy.iserink.com".

```
File View VM
GNU nano 2.2.6 File: /etc/namedb/master/iserink.db
$TTL 10h
@ SOA @ issl.org. 42 1d 12h 1w 3h
; Serial, Refresh, Retry, Expire, Neg. cache TTL

NS proxy.issl.org.

@ A 199.100.16.39
wpad CNAME proxy.iserink.com
```

Figure 3.4.12 Changing iserink.db

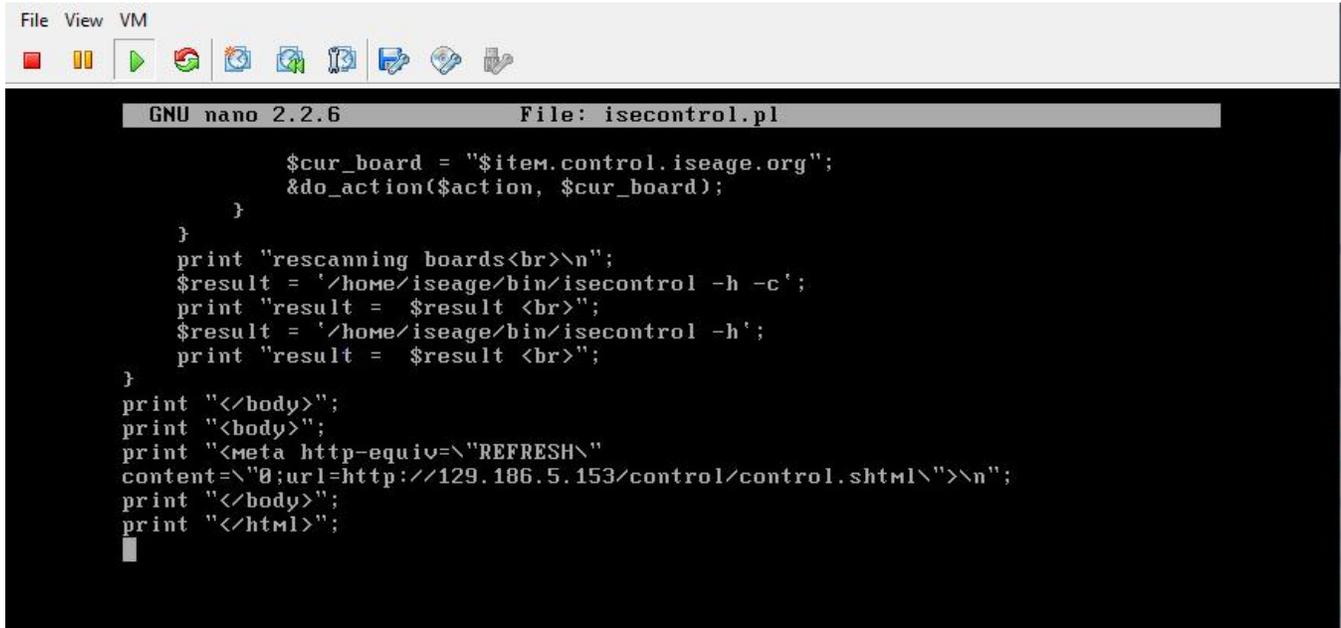
Step 3.4.4: Configure Snowflake

Snowflake provides a web interface to interact with the ISERink boards and restart them if necessary. Access to the snowflakes web site is done via port forwarding rules already configured on Snowbank, but you will need to enter the IP address that you set Snowbank's WAN interface to into the file `/usr/local/www/apache22/cgi-bin/isecontrol.pl`.

Edit the file `/usr/local/www/apache22/cgi-bin/isecontrol.pl`. Find the line below and change the bold text to match your Snowbank WAN interface IP.

```
Content="0:url=http://129.186.5.153/control/control.shtml">\n";
```

Figure 3.4.12 Changing isecontrol.pl

A screenshot of a virtual machine window showing the GNU nano 2.2.6 text editor. The editor is open to a file named isecontrol.pl. The code in the editor is a Perl script that sets a variable \$cur_board to "\$item.control.iseage.org", calls &do_action(\$action, \$cur_board), and prints several lines of HTML and shell commands. The code includes a loop for rescanning boards, a command to run isecontrol -h -c, and another to run isecontrol -h. It also prints HTML tags for body and meta refresh, and a content-type header with a URL to http://129.186.5.153/control/control.shtml.

```
GNU nano 2.2.6 File: isecontrol.pl

    $cur_board = "$item.control.iseage.org";
    &do_action($action, $cur_board);
}
}
print "rescanning boards<br>\n";
$result = '/home/iseage/bin/isecontrol -h -c';
print "result = $result <br>";
$result = '/home/iseage/bin/isecontrol -h';
print "result = $result <br>";
}
print "</body>";
print "<body>";
print "<meta http-equiv=\"REFRESH\"";
content=\"0;url=http://129.186.5.153/control/control.shtml\">\n";
print "</body>";
print "</html>";
```

Step 3.4.5: Final steps

At this point you should have a functioning ISERink. If you are using IScorE you will need to add information to your Active Directory server to support team access to IScorE (section 3.5). To use ISERink you will need to setup your computers for the teams. Information on configuring, using, and troubleshooting ISERink can be found in the ISERink users manual.

Step 3.5: Setting up AD to support IScorE.

IScorE is designed to support scoring for cyber defense competitions. IScorE allows various teams to log in and access materials, post reports, and interact with other teams. IScorE uses AD to authenticate the users. The table below shows the various groups and users that need to be added to the ISERINK domain. This section also shows some of the major steps required to setup your AD to support IScorE. NOTE: these instructions assume you are familiar with setting up AD. If you have never installed and configured an AD before you should refer to materials available from Microsoft and other sources.

Organizational Units:

OU	
CDCUsers	Used to organize all Blue users and groups
GreenTeam	Used to organize all Green users and groups
RedTeam	Used to organize all Red users and groups
White	Used to organize all White users and groups

Groups:

AD Group	Usage	OU
Domain Admins**	IScorE SuperUser account provides access to all aspects of IScorE	
CDCUsers	Group used for each group CDC Team X	CDCUsers
CDC Team X	Used to group blue team members into a team (X is 1 through MAX Teams)	CDCUsers
GreenAdmin	Used for the green team leader	GreenTeam
Green	Group for each green team member	GreenTeam
Red	Group used for the red team members	RedTeam
White	Group for white team members	White

**NOTE: If you are using an existing AD and you don't want your existing Domain Admins to also be SuperUsers of IScorE, then you can create a new group and modify the settings.py on IScorE to match the new group you created. For example, you could create a group called CDCAdmins, add this to the users you want to have superuser access to IScorE and then change the lines in the IScorE settings.py that list "Domain Admins" with "CDCAdmins".

Users:

User	Group Membership
Blue team member	CDCUser, CDC Team X
Green team member	Green
Red team member	Red
White team member	White
Green Leader	Green, GreenAdmin

Step 3.5.1: Build ISERINK.ORG domain (Optional)

NOTE: The following instructions are optional and is designed for installations that don't already have an domain controller or want to have a dedicated domain controller for their ISERink installation. If you do decide to install a dedicated Domain for ISERink, then I would strongly advise connecting this to the currently unused private network that connects directly to IScorE or the White Network.

NOTE: If an existing Active directory server is being used this section should be skipped.

When setting up the AD to support IScorE you need to create the ISERINK.ORG domain. The figure below shows creating a domain within a new forest on an AD that is dedicated to support ISERink (in the next section you will add the groups and users).

1. After you have installed Active Directory Domain Services you will need to upgrade your Active Directory server to a Domain Controller. To do this open Server Manager and you will have a notification that says **Post-deployment Configuration** as seen in Image 3.5.1.

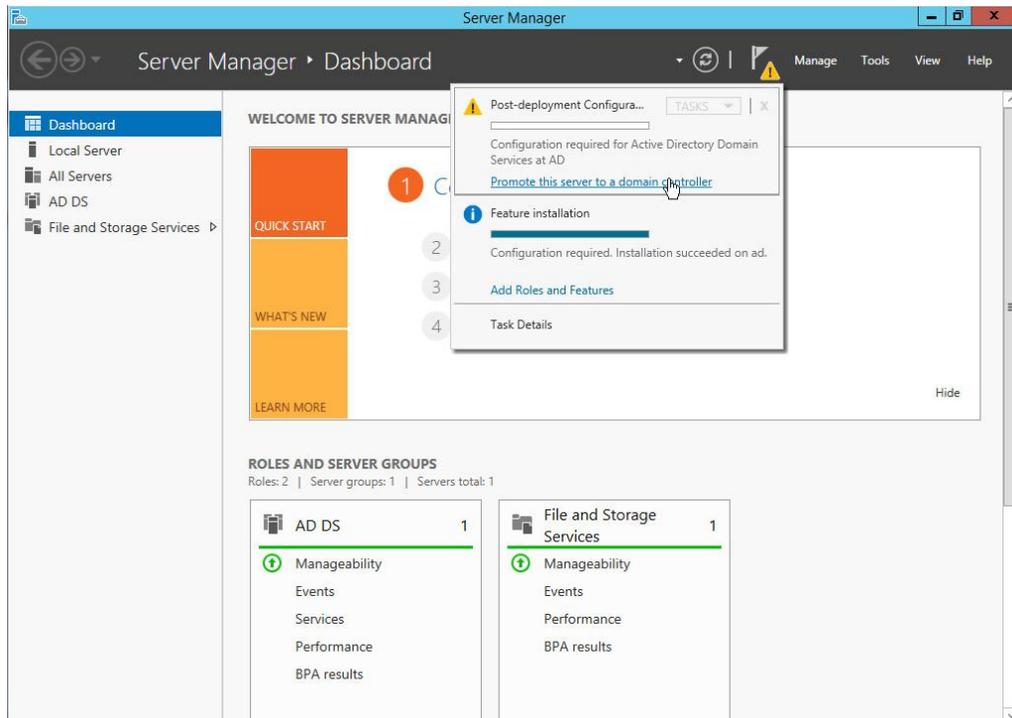


Image 3.5.1: server Manager Notification

2. In the notification click on the link that says "Promote this server to a domain controller" this will launch the Active Directory Domain Services Configuration Wizard
3. In the Deployment Configurations tab select **Add a new forest** and type in iserink.org for the Root domain name as seen in image 3.5.2

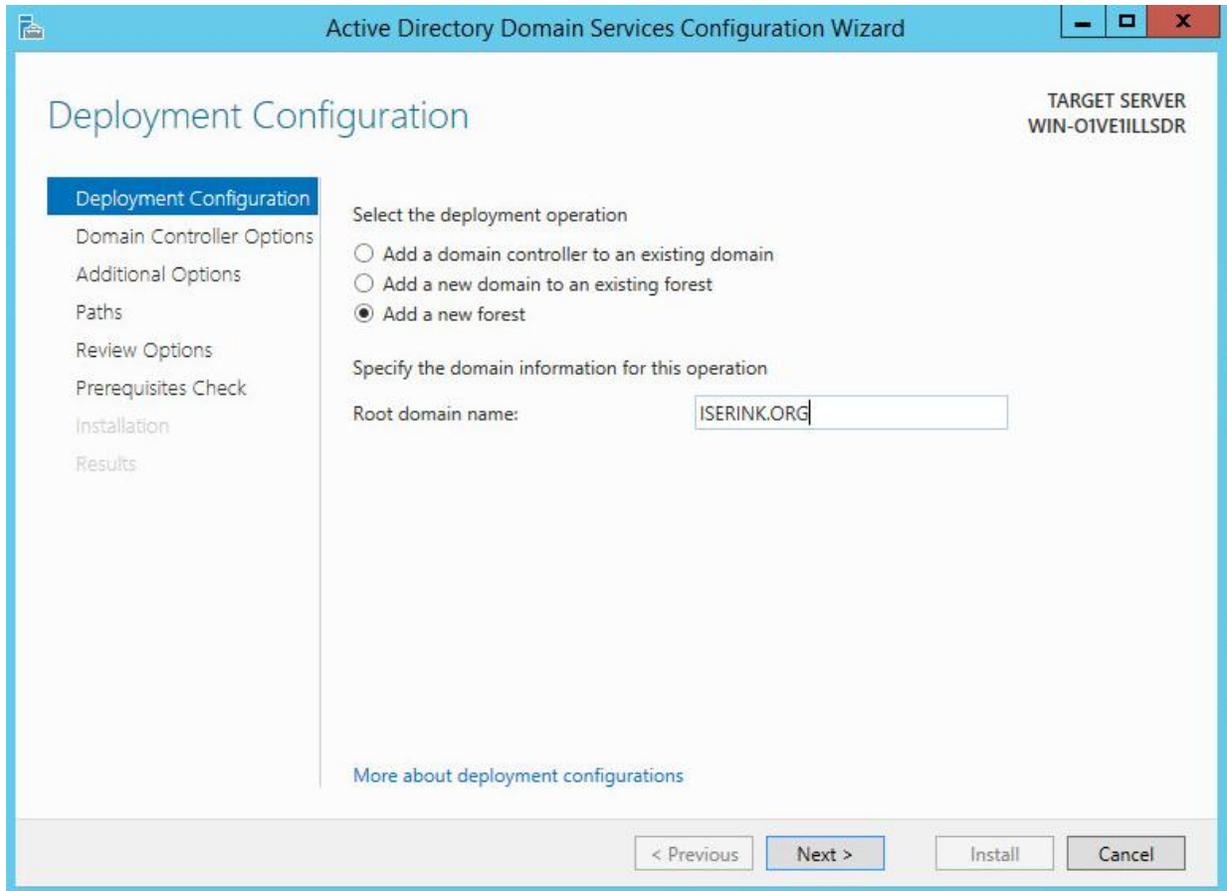


Image 3.5.2: Deployment Configurations tab

4. In the Domain Controller options tab select the function levels as Windows Server 2012, make sure DNS is unchecked and select a Directory Services Restore Mode password you can use the table in [Appendix A](#) to write down this password. These settings can be seen in image 3.5.3

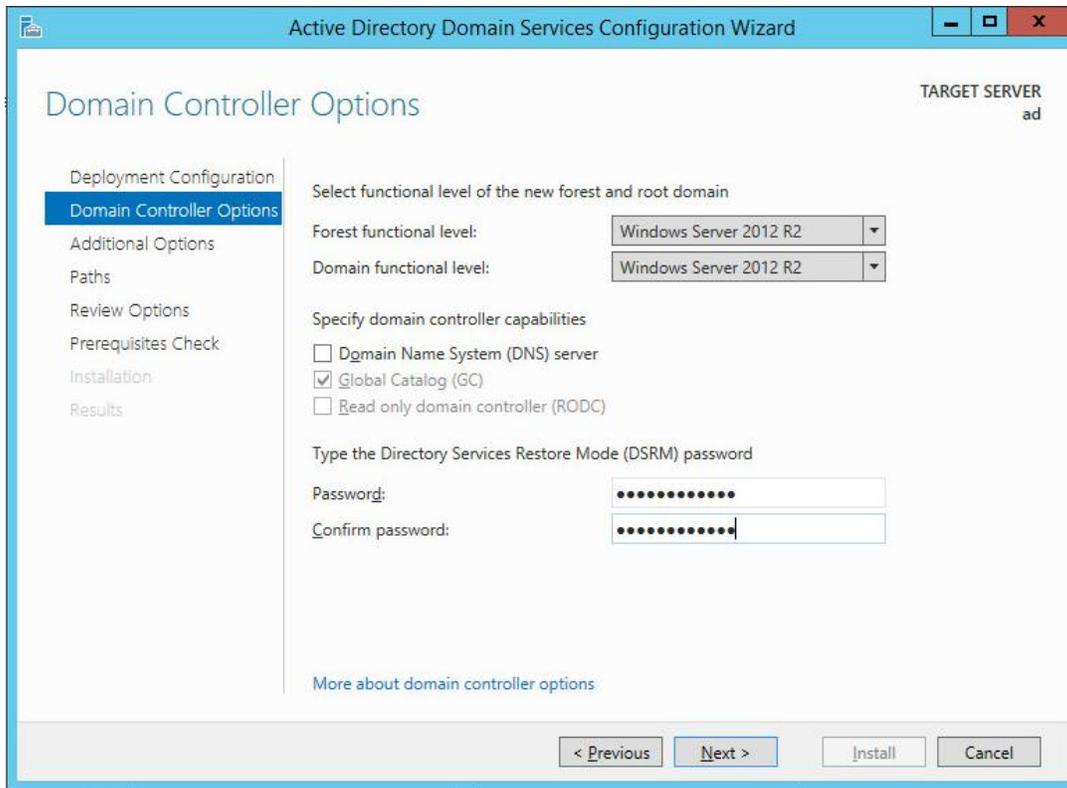


Image 3.5.3: Domain Controller options tab

5. In the Additional Options tab set the NetBIOS name to ISERINK as seen in image 3.5.4 this should automatically populate.

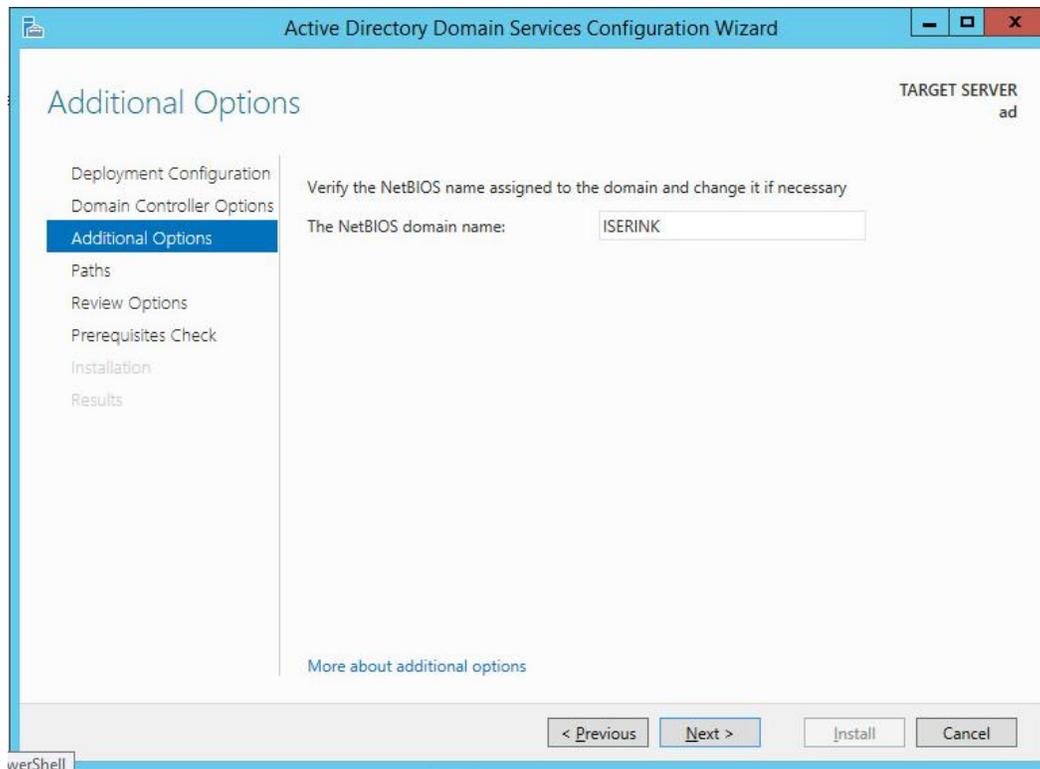


Image 3.5.4: Additional Options tab

6. Leave all setting in the Paths tab as their default settings.
7. Review your settings to make sure they are correct then click install on the final page after your system has verified that all necessary prerequisites are installed.
8. Your server should automatically reboot and your Active Directory is now set as a Domain Controller

After the Active Directory server is completely set up proceed to step 3.5.3

Step 3.5.2: Using an existing Active Directory server

If an existing active directory server is being used it is strongly suggested that you create A new group to be the Administrators for IScorE. Here is an example for how to do this but You are able to organize this in any way to fit the structure of your existing architecture.

1. Create a new OU named CDCAdmin
2. Inside this OU create a group named CDCAdmins
3. Add all users that you would like to have full access to the IScorE admin into this group.

Step 3.5.3: Create AD groups and Organizational Units

Below is instructions to access a PowerShell script to complete the basic AD setup. The script sets up all Organizational Units and groups but, you will have to add the users yourself. It is important that you understand the organization to add the users. More details are provided in section 3.5.3.2

The script is available through SCP on isechest.iac.iastate.edu you will access this using an SCP client on your Active directory server. Download and install WinSCP from www.ninite.com then start WinSCP and log in using the credentials you were provided to download the Virtual Machine images.

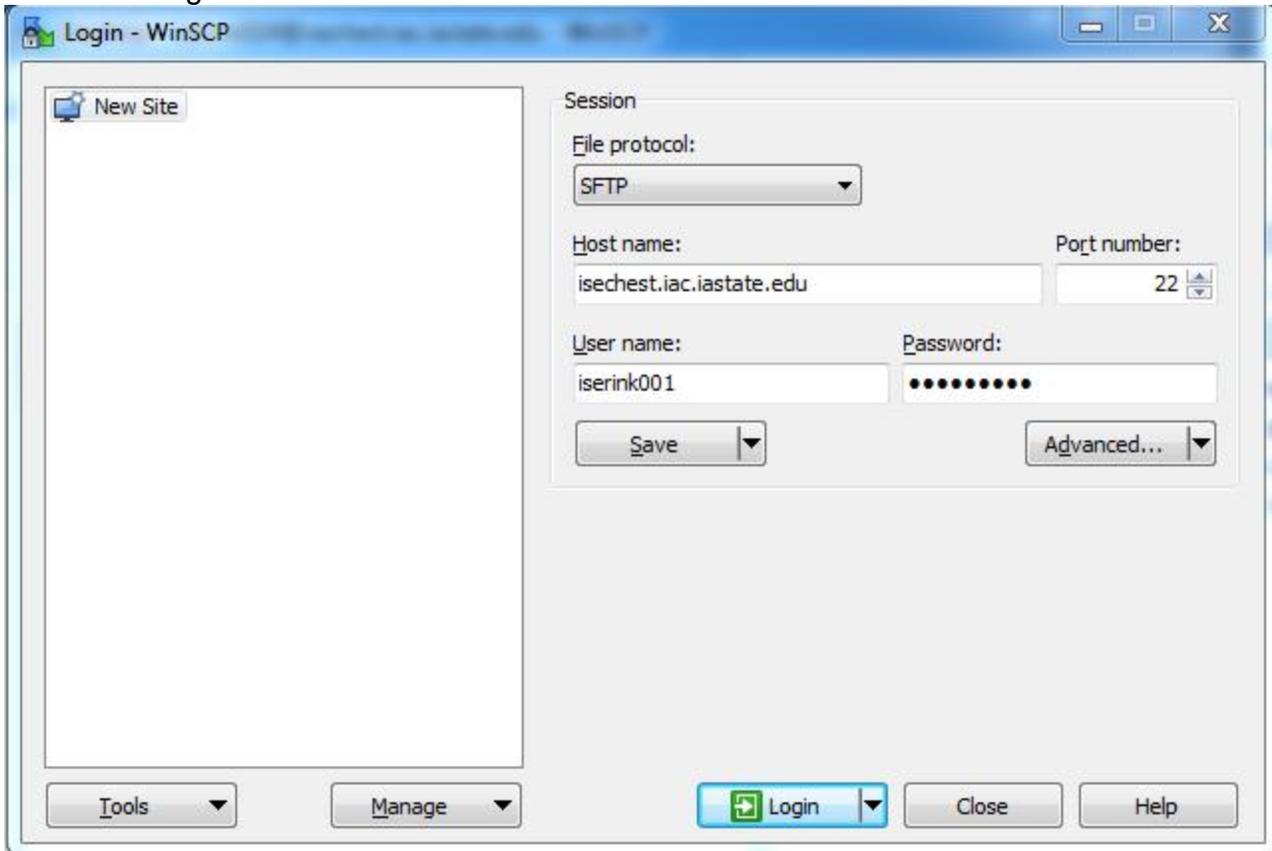


Image 3.5.5: WinSCP Login

Navigate to “/usr/home/downloads/ISERink/scripts/” and download “active_directory_setup” to your desktop. Right click on the file and select “Run with PowerShell”

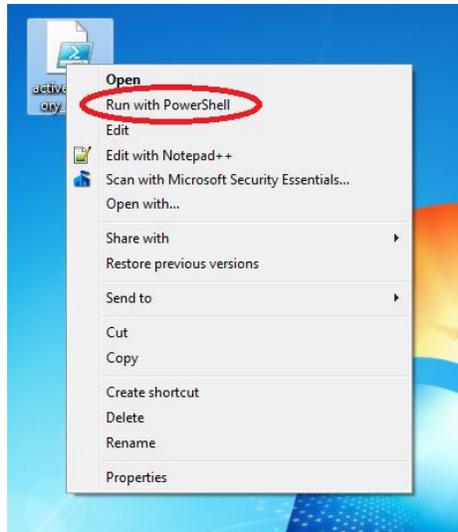


Image 3.5.6: run active_directory_setup

If you launch “Active Directory Users and Computers” you should now see all the users, groups, and Organizational units.

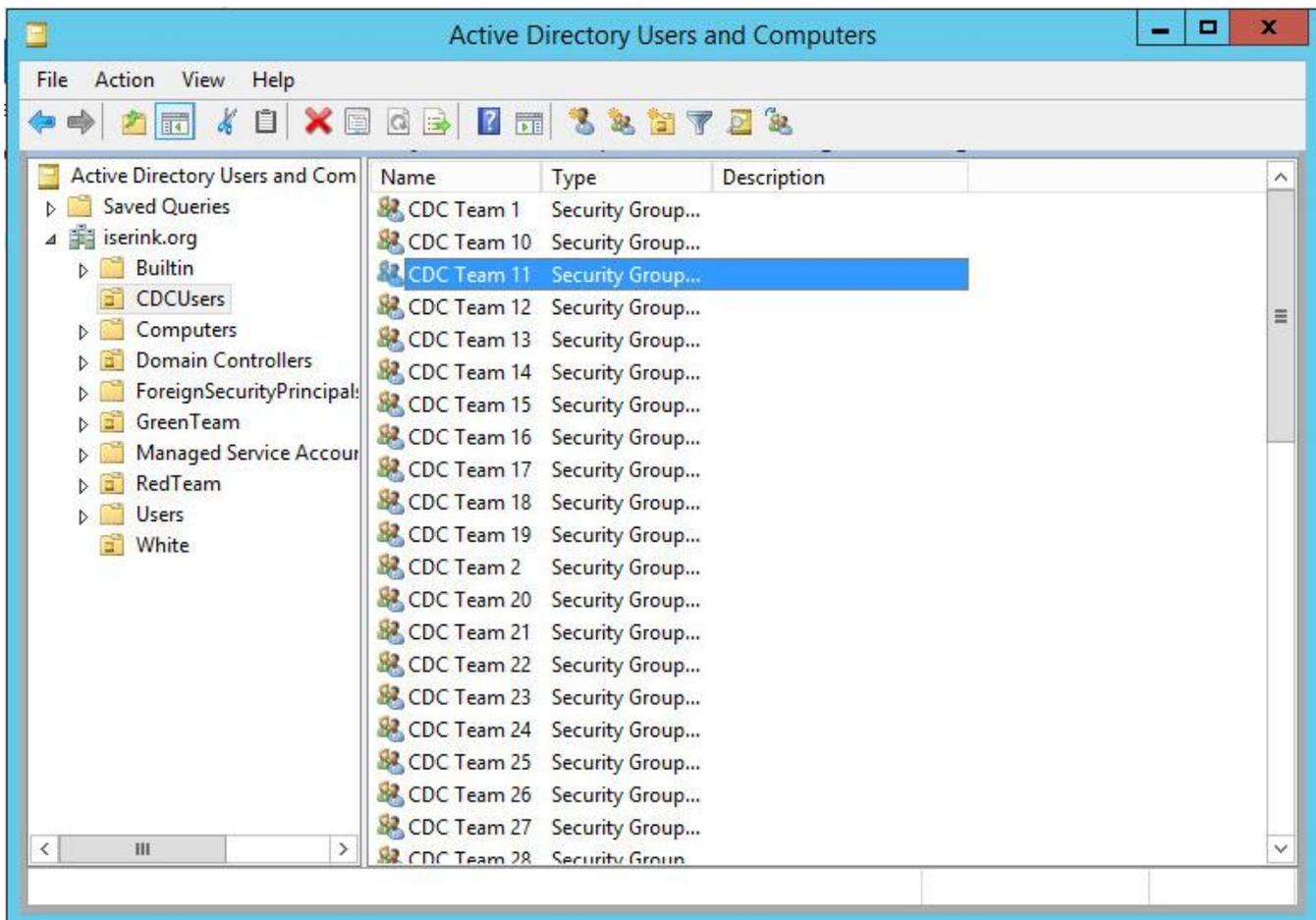


Image 3.5.7: Active directory structure

Step 3.5.4: Create users

Step 3.5.4.1: Create new user

To add a new user right click on the Organizational unit you wish to add a user to and select new and then user.

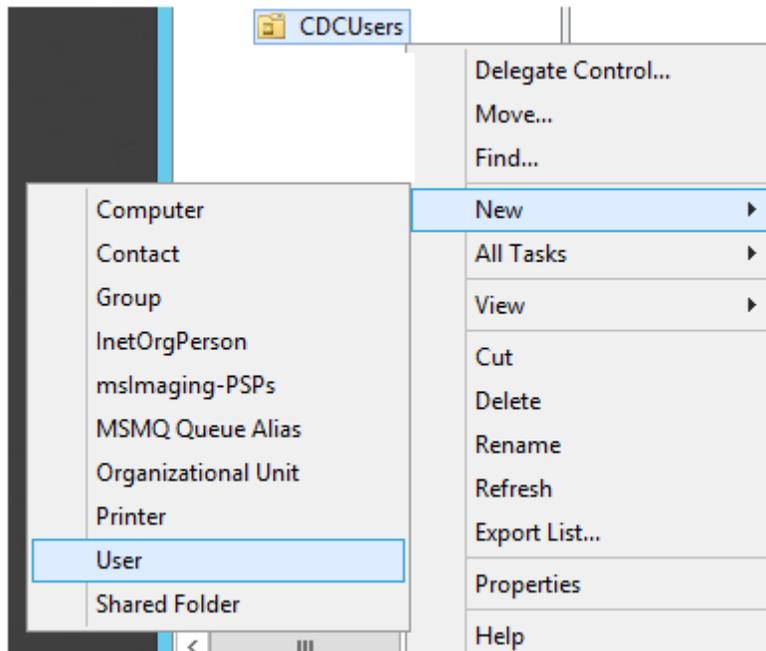


Image 3.5.8: add new user

You will then see a prompt to set the users data. Enter all of this information: at minimum you must enter first name, last name, user, login name, and password.

Step 3.5.4.2: Add user to desired groups

There are four groups of users for IScorE. All users must be set up in one of the ways described below depending on what actions they should be able to perform. To add a user to a group right click on the user and select "Add to a Group..." then enter the group name and hit OK. For details on what groups to add users to, see the discussions below

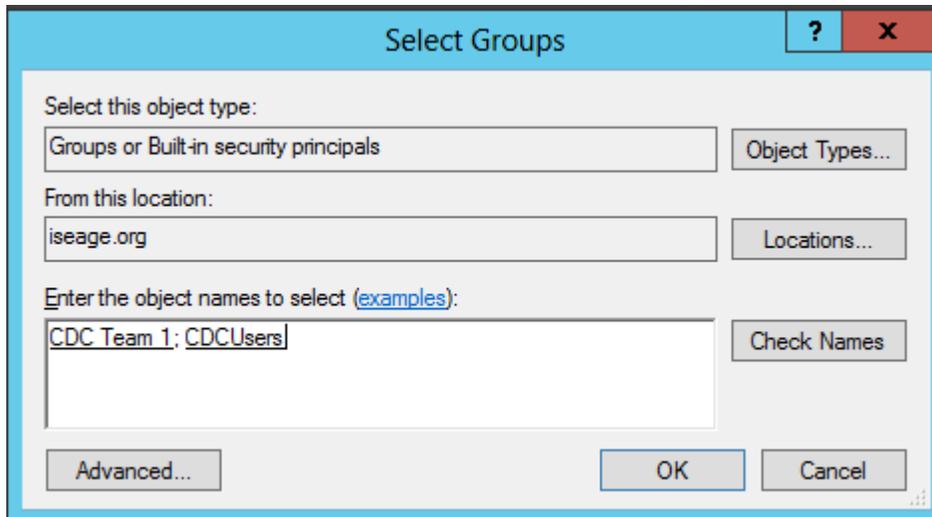


Image 3.5.8: add user to group

Blue user

Blue users are a member of CDCUsers and “CDC Team X” where X is the user’s team number. The CDCUsers OU structure can be seen in the diagram in Image 3.5.5. Each of these users can log into IScorE and preform actions for their team such as view team specific information, download flags, and submit documentation

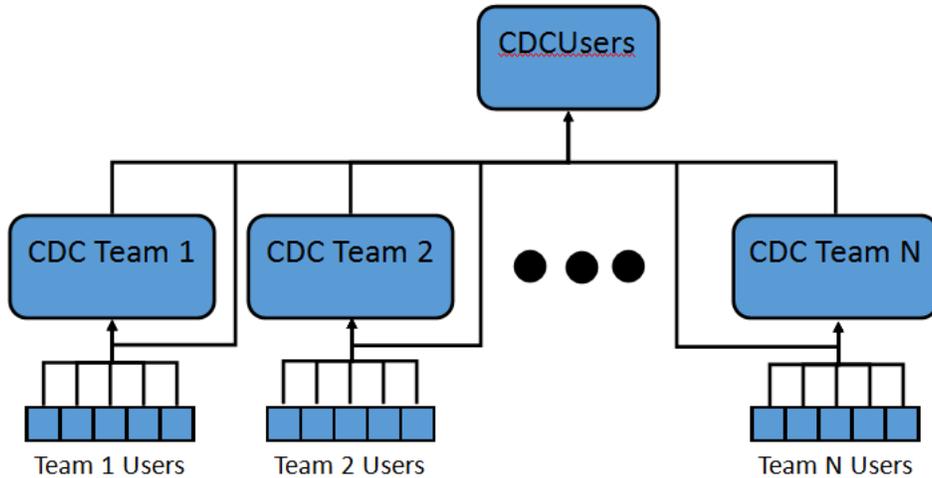


Image 3.5.9: CDCUsers Organizational Unit Diagram

Green user

Green users are a member of the group Green. The GreenTeam OU structure can be seen in Image 3.3.5. Green team users can log in to IScorE and perform tasks necessary for grading teams such as viewing all teams’ team specific info, grade anomalies and, grade documentation.

Green Admin

Green Admins are members of the group GreenAdmin and Green. The GreenTeam OU structure can be seen in Image 3.3.6. Green Admins can log in to IScorE and perform tasks necessary for grading including creating usability checks and, creating anomalies.

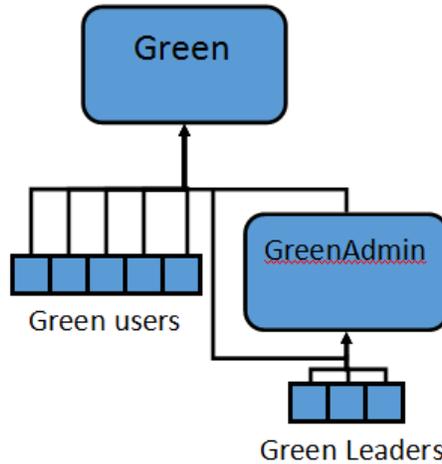


Image 3.5.10: GreenTeam Organizational Unit Diagram

Red user

Red users are a member of the group Red. The RedTeam OU structure can be seen in image 3.5.7. Red team users can log in to IScorE and perform tasks necessary for attacking and scoring the teams such as submitting a captured flag, planting a flag and, grading earnbacks.

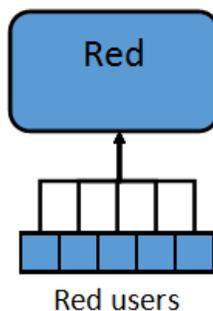


Image 3.5.11: RedTeam Organizational Unit Diagram

White user

White users should be a member of Domain Admins, White. The White OU structure can be seen image 3.5.8. White users can log in and see all areas and preform all actions in IScorE. This includes wiping information, creating new competitions and, overriding team scores.

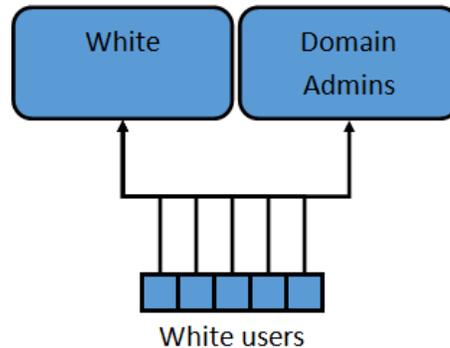


Image 3.5.12: White Organizational Unit Diagram

Step 3.5.5: Configure IScorE

1. Log in to the IScorE as root, with initial password of "iseage".
2. Next you will need to configure IScorE to query the Active Directory that you just set up. From the command line edit the file "/var/www/iscore/settings.py"
3. In the line "AD_DNS_NAME = '129.186.5.162' " replace 129.186.5.162 with the IP address of your Active directory server, as seen in image 3.5.9.
4. If an existing active directory server is being used and you don't want your domain admins to have Admin status on IScorE you can replace Domain Admins in the line "AD_MEMBERSHIP_ADMIN = ['Domain Admins']" to the name of the group you created earlier.

```

#####
# ActiveDirectory Settings
#####
AD_DNS_NAME = '129.186.5.162' # FQDN of your DC
AD_LDAP_PORT = 389
AD_LDAP_URL = 'ldap://s:s' % (AD_DNS_NAME, AD_LDAP_PORT)
# If using SSL use these:
#AD_LDAP_PORT=636
#AD_LDAP_URL='ldaps://s:s' % (AD_DNS_NAME,AD_LDAP_PORT)

AD_SEARCH_DN = 'dc=iserink,dc=org'
AD_NT4_DOMAIN = 'ISERINK.ORG'
AD_SEARCH_FIELDS = ['mail','givenName','sn','sAMAccountName','memberOf']
AD_MEMBERSHIP_ADMIN = ['Domain Admins'] # this ad group gets superuser status in django
AD_MEMBERSHIP_REQ = AD_MEMBERSHIP_ADMIN + ['CDCUsers','Green','White','Red'] # only members of this
group can access
AD_CERT_FILE = False # this is the certificate of the Certificate Authority issuing your DCs certifi
cate
AD_DEBUG = True
AD_DEBUG_FILE = '/var/log/iscore/ldap.debug'
#AD Permission Groups
AD_WHITE_GROUP = ['White']
AD_GREEN_GROUP = ['Green']
AD_GREEN_ADMIN_GROUP = ['GreenAdmin']
AD_RED_GROUP = ['Red']
AD_BLUE_GROUP_PREFIX = 'Blue' # Assuming you have a group for each team: "Blue 1" "Blue 2" then thi
s prefix is "Blue"

AUTHENTICATION_BACKENDS = (
    'auth.ActiveDirectoryAuthenticationBackend',

```

Image 3.5.13: IScore ldap setup

Section 4: ISERink Testing

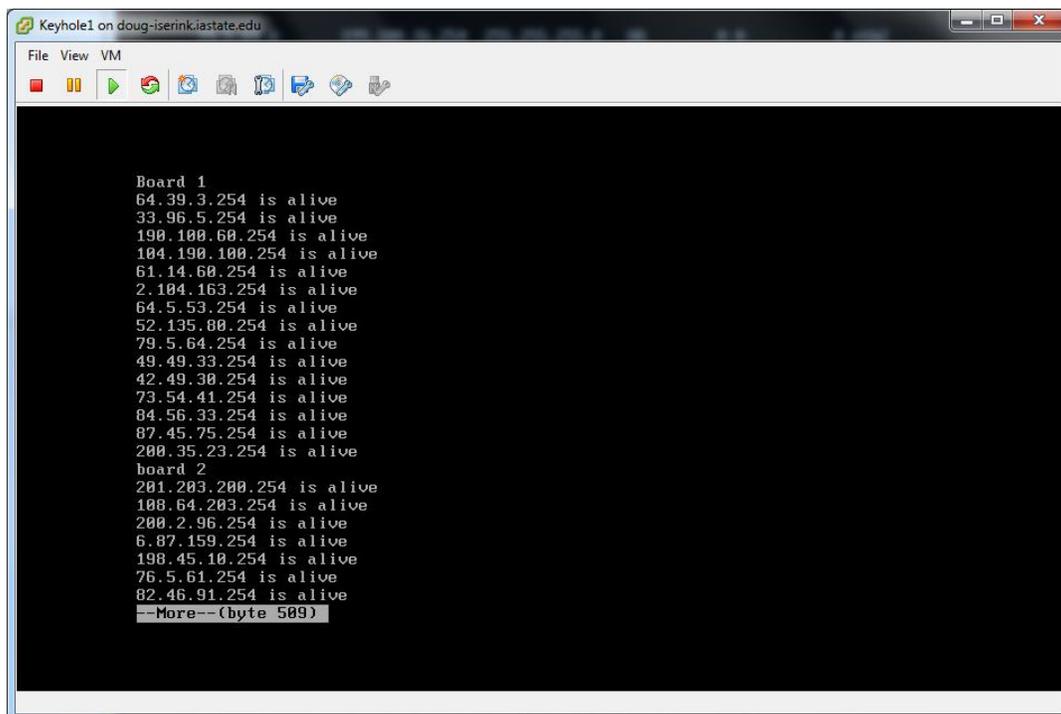
There are several simple steps that test the basic functionality of ISERink. More detailed testing procedures are explained in the ISERink users' guide. If any of these tests fail you should use the support on the ISERink web site. The goals of the testing are to check:

- the connectivity across the competition network
- test the connectivity of ISERink to the Internet
- test IScorE
- test ISEAGE management

Internal connectivity: The goal of these tests are to see if ISEAGE can route traffic. These tests will be run from Keyhole1 and will ping all of the gateways for the 45 subnets. To run this test you will need to bring up the console window on the virtual machine keyhole1. From the console window, you will need to login to Keyhole1 as root with the password of "iseage". Once you have logged in you will run the following command:

```
"sh /home/tests/ISERink-router-test.sh more"
```

You will see a printout similar to the one shown in the Figure 4.1. There should be 15 routers for each board reporting back they are alive.



```
Keyhole1 on doug-iserink.iastate.edu
File View VM
Board 1
64.39.3.254 is alive
33.96.5.254 is alive
190.100.60.254 is alive
104.190.100.254 is alive
61.14.60.254 is alive
2.104.163.254 is alive
64.5.53.254 is alive
52.135.80.254 is alive
79.5.64.254 is alive
49.49.33.254 is alive
42.49.30.254 is alive
73.54.41.254 is alive
84.56.33.254 is alive
87.45.75.254 is alive
200.35.23.254 is alive
board 2
201.203.200.254 is alive
100.64.203.254 is alive
200.2.96.254 is alive
6.87.159.254 is alive
198.45.10.254 is alive
76.5.61.254 is alive
82.46.91.254 is alive
--More-- (byte 589)
```

Figure 4.1 Testing internal connectivity

External connectivity: The goal of this test is to test if Keyhole2 can access the Internet and if the proxy servers work. If you bring up the console window for Green-KALI you can log in (user = root, password = iseage) and run iceweasel this is a browser and you should be able to access web sites.

IScorE testing: The goal is to see if the IScorE web service is running. You should be able to access the website from outside ISERink and from Green-KALI using the FQDN you picked for IScore.

ISEAGE management: The goal is see if the ISEAGE web service is running. If you point your browser to the outside IP address of snowbank you should see a web page with ISEAGE on it.

Appendix A: Configuration tables

The tables on this page can be printed then filled out and kept as a reference.

Management information:

ESXi Root password:	
ESXi Management IP address:	
ESXi server name:	
ESXi DNS server:	
SnowBank WAN IP Address	
SnowBank Default Gateway:	
ISERink server name:	
ISERink DNS server:	
IScorE IP address	

Physical network configuration

VMNIC	External ID or label
Vmnic0	
Vmnic1	
Vmnic2	
Vmnic3	
Vmnic4	
Vmnic5	