ISERink Overview

Version 1.1

February 1, 2015

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 provides an overview of the ISERink playground. The web site (www.iserink.org) contains the installation guide that will 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.

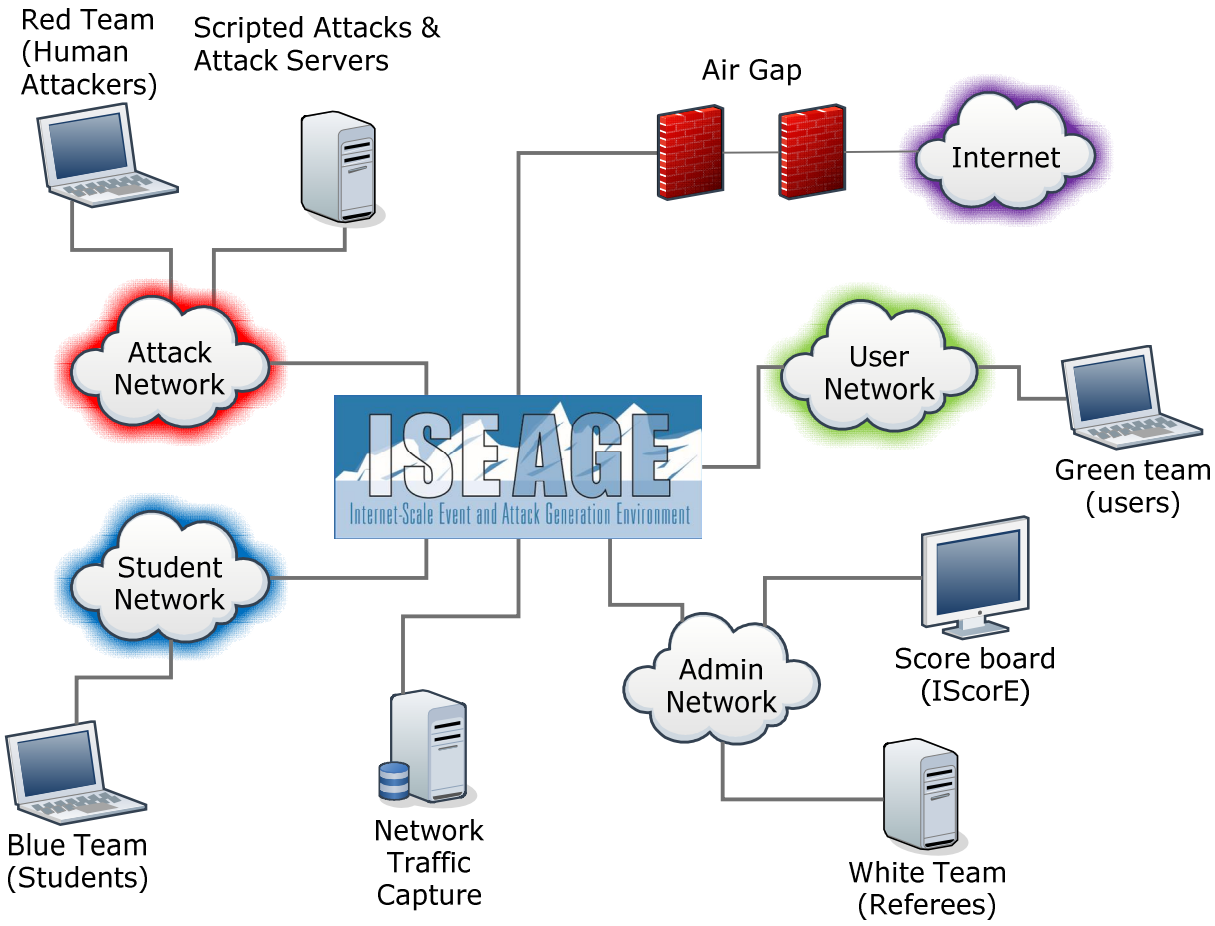

Figure 1 ISERink playground

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 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
- ISERink images (available via scp from isechest.iac.iastate.edu)

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 the figure below. 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.

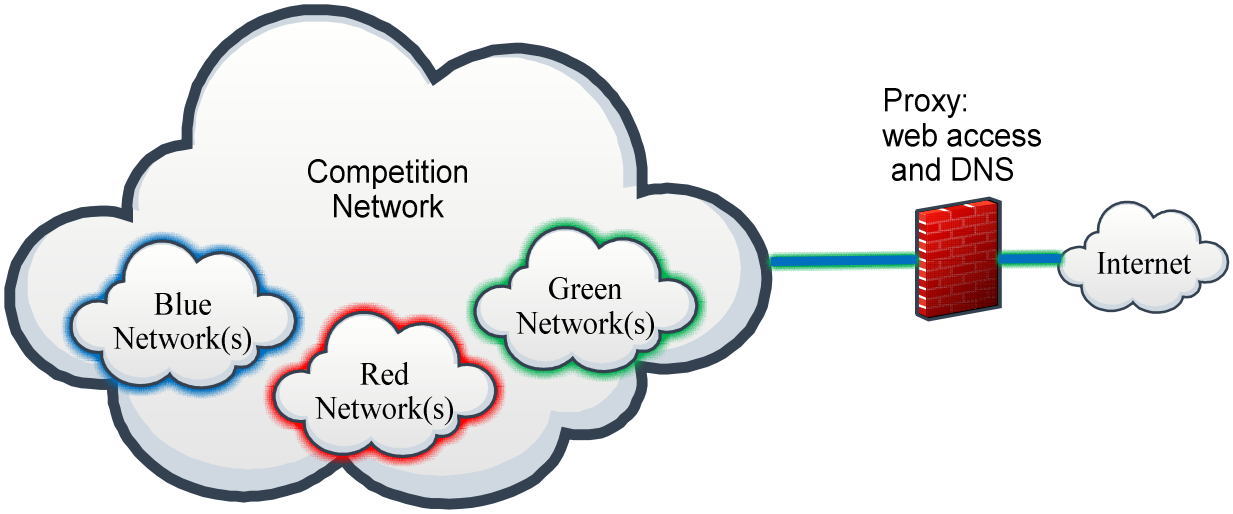

Figure 2 ISERink overview

The figure below shows the topology of the VM machines that create the routable Internet (ISEAGE) along with the machines that create ISERink. As shown in the figure ISEAGE supports 45 class C subnets (15 on NIC1, NIC2, and NIC3). In addition NIC 4 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 (1,2,3). 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.

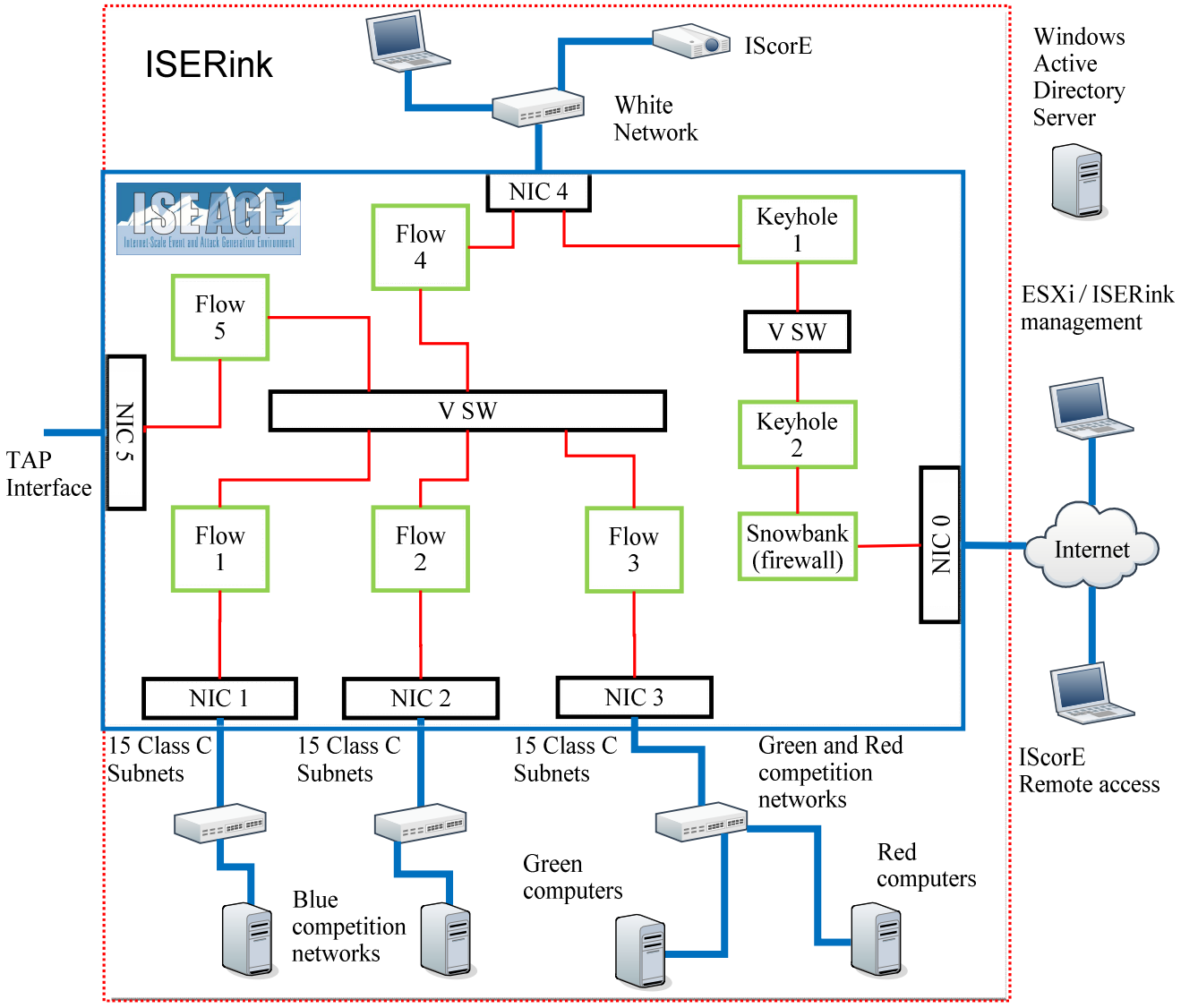

Figure 3 ISERink VM topology

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, Keyhole2, and IScorE. 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 4 and the second is directly to the Internet (Figure 5). For each configuration we will discuss the three IP addresses.

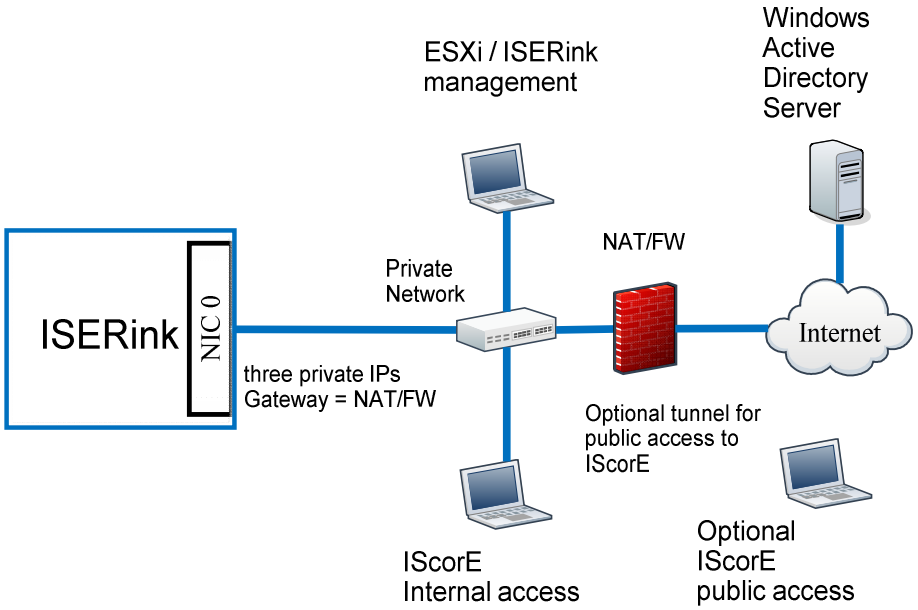

Figure 4 ISERink behind a NAT/Firewall

When ISERink is connected to a private network behind a NAT you will need three private IP addresses: one for ESXi management, one for Keyhole2, and one for IScorE.

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.

Keyhole2: The devices on the competition network can access the Internet using three protocols (DNS, HTTP, FTP). This is accomplished using an air-gap proxy. The external interface of this proxy needs to be connected to the Internet. This connection can be through a NAT and/or Firewall since the connections are only outbound.

IScorE: IScorE actually is connected to three different networks. First, it is connected to an internal private network that is currently not used. Second, it is connected to the competition network to enable scanning and to allow the teams to access documents within the competition network. Third, it is connected to the Internet and has an IP address on your

private network. When ISERink is behind a NAT then access to IScorE is only on the private network unless you create a tunnel through your NAT for HTTP/HTTPS traffic.

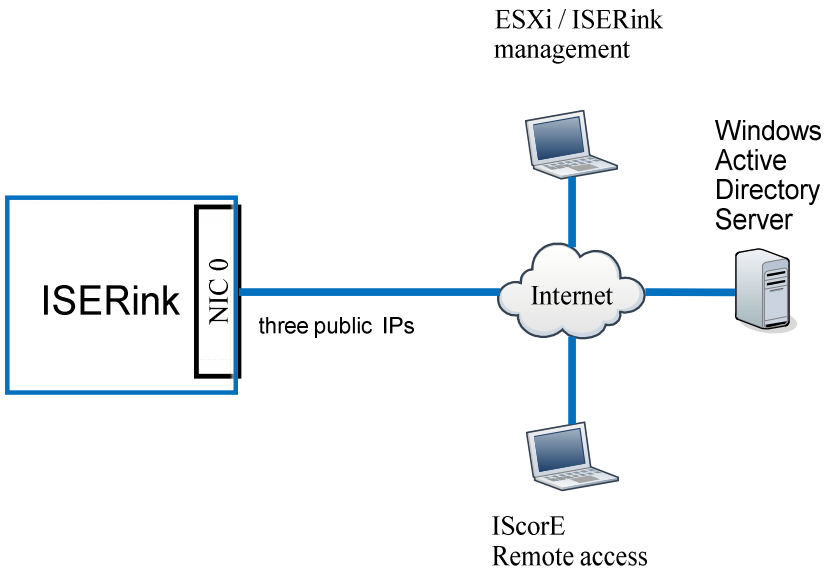

Figure 5 ISERink directly connected to the Internet

When ISERink is connected directly to the public Internet you will need three public IP addresses: one for ESXi management, one for Keyhole2, and one for IScorE.

ESXi Management: When the ESXi management IP address is a public IP address, you can manage and configure ISRink from the Internet.

Keyhole2: The devices on the competition network can access the Internet using three protocols (DNS, HTTP, FTP). This is accomplished using an air-gap proxy.

IScorE: IScorE actually is connected to three different networks. First, it is connected to an internal private network that is currently not used. Second, it is connected to the competition network to enable scanning and to allow the teams to access documents within the competition network. Third, it is connected to the Internet for external access.

Figure 6 shows a more detailed view of ISERink. The additional virtual machines are used to manage ISERink, provide scoring, and to support the Green, and White teams.

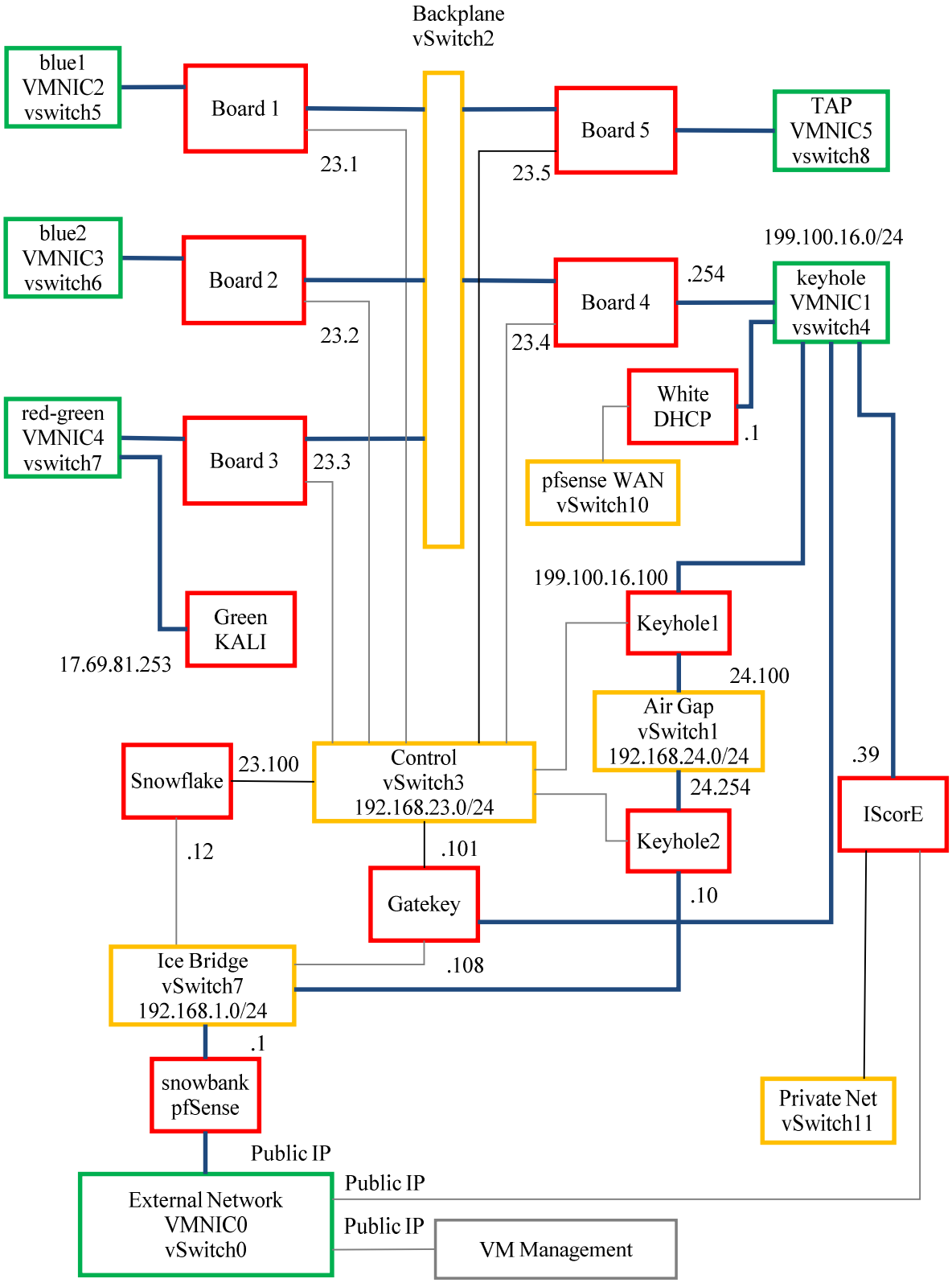

Figure 6 ISERink Virtual Machine Topology

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 HTTP and FTP sites on the internet (no HTTPS). 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.