Firewall Configuration

In this presentation:

- Introduction
- Lab Scenario
- Lab Procedures (Outline)

Introduction

The purpose of a firewall is to moderate and control network traffic, for the purpose of logging network activity and/or blocking potentially harmful traffic.

Firewalls provide a layer of protection between private (trusted) networks and public (untrusted) networks. This need has become increasingly important as more and more individuals and organizations are connected to the Internet.

An improperly configured firewall can provide a false sense of security, so it is important to be able to tailor a firewall configuration to the needs of an organization.

Introduction (cont'd)

One common category of firewalls is a *packet filtering router*, a device which forwards packets between networks.

The router checks each network packet to determine whether it should be forwarded to its intended destination or rejected, based on its set of *rules*. When a rule which matches the packet is found, the corresponding rule action is obeyed.

The rules are searched in order, so only the first match counts; for this reason, these rules are referred to as "*rule chains*."

Introduction (cont’d)

The router in your ICS lab kit is powered by DD-WRT (based on an embedded Linux kernel), so the firewall rules can be configured at the command line using IPTABLES. The default rules provide a reasonable starting point.

Changes made to the configuration take effect immediately, but they are not be permanently saved, so the default configuration can be restored by rebooting the router.

This is an ideal way of testing a new configuration, which can be made permanent later by creating a *script*.

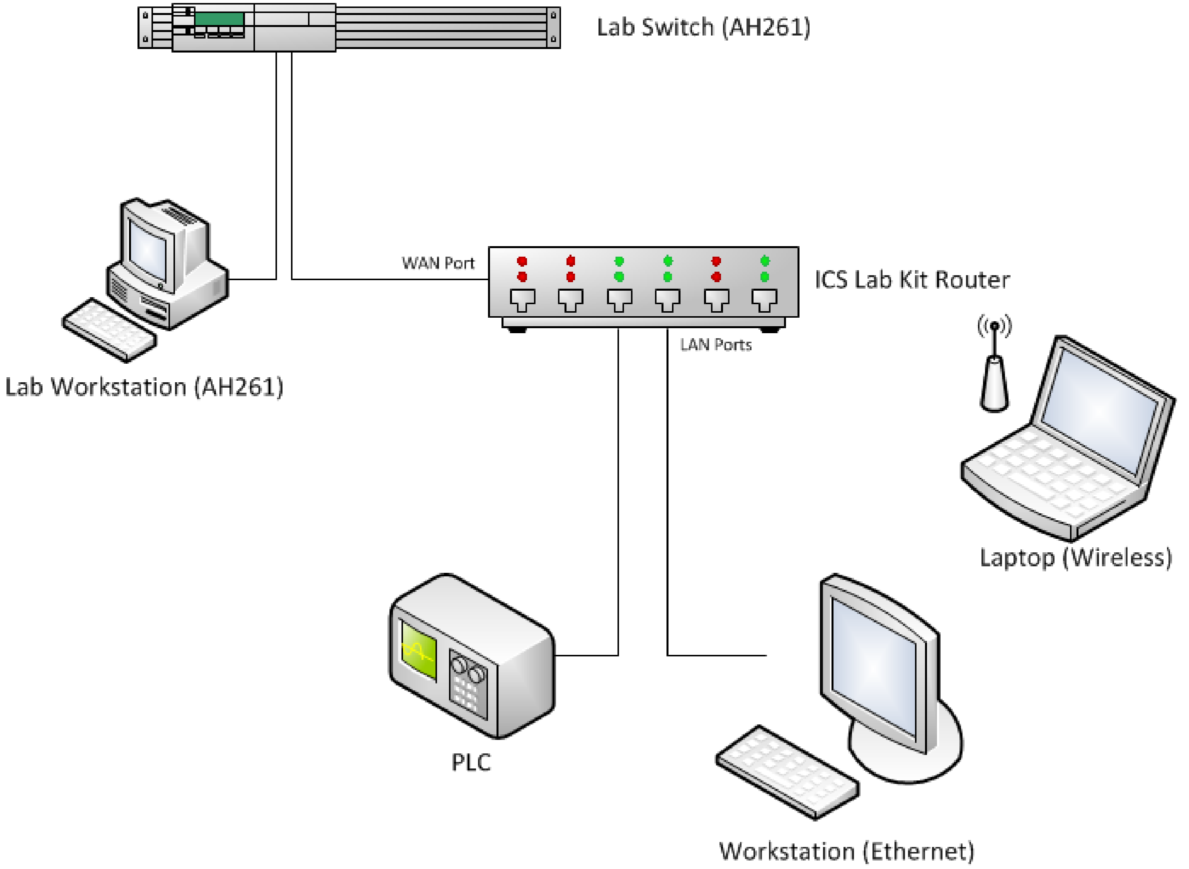
Introduction (cont'd)

The firewall rule chains are divided into *tables*; the default table is the *filter* table, which includes the following chains:

- **INPUT** (for packets destined to or entering the router's local sockets)
- **OUTPUT** (for packets sourced from or leaving the router's local sockets)
- **FORWARD** (for packets being forwarded *through* the router)

Your router's WAN port will be connected to the lab network, and your workstation(s) to the router's internal network. We will test a variety of firewall rules by simulating an attack on the internal network from "Internet hosts" (workstations on the lab network).

Lab Scenario



Lab Procedures

This hands-on lab is intended to walk you through the following steps:

- Configure the PLC with simple firmware which uses Modbus
- Test connectivity with a simple HMI
- Configure the firewall to enable remote Modbus access
- Configure the firewall to deny Modbus access from a specific host
- Configure the firewall to deny and log *all* Modbus access attempts

An important principle which will guide our firewall configuration is *layering*, the idea that multiple policies (in the form of firewall rules) should be in place to protect important services; if one policy fails, the others will prevent exploitation.