

## **Internet Security Basics**

### **Course Summary**

#### **Description**

This class covers the fundamentals of internet security, beginning with the background of firewalls and internet security in general, with a discussion of the three main types of firewalls: packet filter, stateful inspection, and proxy. This is followed by a discussion of major firewall manufacturers and their product lines, including the positives and negatives of each. Once the background has been established, the class will continue with a hands-on configuration of a security appliance as a firewall. Once the basic firewall has been configured, the class will continue with the configuration of a virtual private network (VPN) between the security appliances. The class will conclude with a technical testing of the overall security of the firewalls that have been configured. This segment will conclude with the running of some common assessment tools against the firewalls. Once the class has been completed, you will leave with a free security appliance.

#### **Objectives**

At the end of this course, students will be able to:

- Understand the basics of Internet Security
- Understand the basics of firewalls
- Use the major manufacturers and their products
- Configure a firewall and VPN
- Understand the basics of testing Internet security and some common configuration mistakes

#### **Topics**

- Perimeter security devices
- Firewall types
- Intrusion detection systems
- Access control lists on routers.

#### **Audience**

This class is designed for students who are beginning in the technical avenues of information security, and for managers who wish to get a better feel for information security technology. T

#### **Prerequisites**

There are no prerequisites required for this course.

#### **Duration**

Two days