

A five day workshop course designed to give engineers and IT administrators the hands-on experience necessary to design secure networks using devices such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), email filters and Virtual Private Networks (VPNs). Beyond the design aspect, students will build and configure secure networks using VLANs to create security zones and Firewall hardware to both secure network access and to terminate Virtual Private Networks (VPNs). Basic traffic handling theory is covered, as is the security concepts required to understand the operation of VPNs.

Each attendee will receive a free copy of the book Cisco Security Specialist's Guide to PIX Firewall.

### Who Should Attend:

The Designing & Implementing a Secure Network is ideal for anyone who wants to become familiar with the design and implementation concepts and strategies required to successfully run a secured network. This includes engineers, IT managers and IT administrators.

### Format:

50% lecture, 50% exercises and hands-on labs with one Cisco VLAN switch, one PIX Firewall and two PCs per pod. (Two students per pod).

### Course Content:

- Secure Network Design
- The Importance of Security
- Creating a Security Policy
- Firewall Concepts
- Intrusion Detection
- Proxy servers
- Workgroup servers
- Layer 2 Security
- Using VLANs to create security zones

### Firewalls

- Introduction to Firewalls
- Overview of Firewalls
- Controlling Traffic
- Types of Firewalls
- Packet Filtering Firewalls
- Stateful Firewalls
- Application Gateways (Proxy Firewalls)
- Host-Based Firewalls
- Firewall Design
- ASA/PIX Firewall Features
- Firewall Setup and Traffic Filtering
- Firewall Configurations
- Handling Access to the PIX
- Command-Line Interface
- Setup Script Utility
- Configuration Files
- Basic PIX Configuration Commands
- Management Commands
- Viewing PIX Information
- PIX Characteristics
- Network Configuration Example
- Traffic Flow and Address Translation
- Protocol Overview
- Translations and Connections
- Address Translation
- Configuring Your PIX for Inside-to-Outside Access
- Traffic Entering Your Network
- Viewing the PIX's Translations and Connections
- Filtering Traffic with Access Lists
- ACLs and the PIX
- Object

Grouping

ICMP Traffic and the PIX

Configuring VPNs

IPSec Overview

Security and Cryptography Tutorial

VPN Overview

IPSec Overview

Methods of IPSec Data Protection

Setting Up an IPSec VPN Connection

IPSec Configuration

Preparing for IPSec Connections

Site-to-Site Connections

Remote Access Connections

Advanced Firewall Features

Web Traffic Filtering

HTTP Traffic

Filtering Java Applets and ActiveX Scripts

Filtering Web Content

Protocol Fixup Feature

Issues with Protocols and Applications

Established Connections

Application Inspection

Application Inspection Configuration

Application Inspection for FTP

Attack Guard and IDS Features

Attack Guard Features

Intrusion Detection System (IDS)

Spoofing Protection

Firewall Management

PIX Device Manger

PDM Overview

Requirements for PDM

Preparing to Use PDM

Accessing PDM

Using PDM

Centralising Security

Centralizing Security

Server and Authentication Configuration

Shell Access

Cut-Through Proxy

Other Types of Traffic

Changing Authentication Parameters

Configuring Accounting

Testing and Troubleshooting AAA

Configuring System Management

Configuring Logging

Configuring Remote Access

Labs

Basic Firewall Configuration

Basic PIX Firewall Configuration

Configuring PIX Firewall Interfaces

Configuring NAT

Configuring PAT

Logical Interfaces and the DMZ

Configuring (ACLs) to control traffic

Configuring a PIX Firewall VPN

Configuring a PIX Remote Access VPN

Configuring PIX Device Manager (PDM)