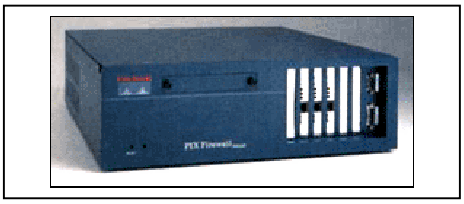
Microsoft Certified Solution Provider

TCY Technologies
"Excellence in training since 1989!"

Cisco Systems
Authorized Resellers

500 EIGHTH Ave, Suite 1203, New York, NY. 10018



CCSP Bootcamp
Security Training
(Securing Network with Routers and Switches, PIX, IPS, VPN, etc)

Course Length: 10 weeks (80 hours), Instructor-led
Skill Development: Understand Cisco network security products
Prerequisites: CCNA (CCNP recommended)
Target Audience: Network engineers desiring to acquire hands-on skills in Cisco security products
Course Objective: Acquire advanced knowledge and skills required to secure Cisco networks and to pass exams required for CCSP
Exams covered: Cisco CCSP exams (CSVPN, SNRS, SNPA, IPS, and SND)
Lab: One-year onsite and remote access (via web)

Topics to be covered:

Securing Networks with PIX and ASA (SNPA)

I. Install & configure a security appliance for network connectivity
II. Advanced knowledge and skills required to secure Cisco netwrks
III. Configure a security appliance to provide secure connectivity using site-to-site VPNs
IV. Configure AAA services for access through security appliance
V. Configure routing and switching on a security appliance
VI. Configure a modular policy on a security appliance
VII. Monitor and manage an installed security appliance

Securing Cisco Network Devices (SND)

I. Describe the products in the Cisco security portfolio
II. Describe the security features available for a Cisco Layer 2 device in a secure network
III. Describe and configure Cisco IPS and HIPS
IV. Configure and verify basic remote access on a Cisco VPN 3000 Concentrator
V. Implement a Cisco PIX security appliance

Securing Networks Using Intrusion Prevention Systems (IPS)

I. Describe how Cisco IDS/IPS sensors are used to mitigate network appropriate response to network attacks.
II. Describe Cisco IDS/IPS sensors and configure essential system Parameters

Cisco Secure Virtual Private Networks (CSVPN)

I. Configuring the Cisco VPN 3000 concentrator for remote access using pre-shared keys and digital certificates
II. Configuring the Cisco Virtual Private Network firewall feature for IPSec software client
III. Configure Cisco Virtual Private Network client auto-initiation feature
IV. Monitor and administer VPN 3000 remote access networks
V. Configure the Cisco VPN 3002 hardware client for remote access and software auto-update & backup server and load balancing
VI. Configure the Cisco VPN 3000 series concentrator for the IPSec Over UDP and IPSec over TCP
VII: Cisco VPN 3000 series concentrator LAN-to-LAN with pre-shared keys, NA and digital certificates.

Securing Networks with Cisco Routers & Switches (SNRS)

I. Implement Layer 2 security
II. Configure Cisco IOS Firewall features to meet security requirements; configure IOS-based IPS to identify and mitigate threats to network resources; configure basic IPSec VPNs to secure site-to-site and remote access to network resources
III. Configure authentication, authorization and accounting to provide basic secure access control for networks
IV. Use management applications to configure and monitor IOS security features

Open Lab Hours: Monday through Thurs, 10:00am to 9:30pm, Fri/Sat/Sun 9:30a to 5:30p

Phone: 212-695-4810 | **HTTP://www.TCYTech.com** | **Fax: 212-695-5359**