Cisco Training: Mastering Network Security  
(CSCADV, 4 days)

Description
The course Mastering Network Security (Cisco Training) delves into the details of Cisco network security. Every aspect of the security policy implementation is covered, starting with basic protocol considerations to the use of firewalls, IPS and IPv6. The training includes ACLs, tunneling and routing protocols.

Pricing
- Individual Pricing: $2,775/person
- Guaranteed date and automatic 10% discount when you register 2 people.

Outline
- Security fundamentals
  - Introduction to Network Security
  - The Need for Network Security
  - Why Do Hackers Hack?
  - General Network Security Goals
  - Social Engineering and Privilege Escalation Attacks

- Understanding Ping Sweeps and Basic Network Auditing
  - Understanding Ping Sweeps
  - Basic Network Auditing

- Introduction to SDM (Security Device Manager)
  - Cisco's Security Device Manager (SDM)
  - Pre-Installation Configuration
  - Installing, Launching and Loading SDM

- SDM Settings and Configuration
  - SDM Monitoring
  - Authentication, Authorization, and Accounting (AAA)
  - Overview of "What is AAA?"
  - TACAS+ vs. Radius Configuration
  - Overview of Authentication Principals
  - Accounting
  - Authorization
  - Configuring AAA with SDM

- Layer 2 Security
  - Basic L2 Security Features
  - Port Security Overview
  - Configuring or Misconfiguring Port Security
  - Aging Time for Secure Access and Sticky Addresses
  - Cisco Lightweight Extensible Authentication Protocol (LEAP)
  - Local and Remote SPAN Configuration
  - Filtering Intra-VLAN Traffic
  - VLAN Access List (VACL)
  - Private VLAN

- DHCP Snooping and Dynamic ARP Inspection
  - IP Source Guard
  - MAC Address Flooding Attacks and VLAN Hopping
  - Root and BPDU Guard

- Layer 3 Security
  - Configuring and Encrypting Passwords in Cisco IOS
  - Privileged Levels
  - Creating and Testing Minimum Length Password Policy
  - Strong vs. Weak Passwords
  - "Salting" your MD5
  - Network Time Protocol (NTP)
  - Synchronizing and Configuring NTP
  - Telnet and SSH Remote Access
  - Different Types of Network Attacks
  - Denial of Services (DoS) and SYN Flooding Attack
  - ICMP (Ping) Sweep, Port Scan, and Port Sweep
Ping Attacks and Floods
Packet Sniffers and Queries
Introduction to Security Auditing
Viruses and Worms
Differences Between SDM and AutoSecure
The Intrusion Prevention System (IPS)
Intrusion Detection (IDS) vs. Intrusion Prevention (IPS)
Signatures and Signature Types
NIPS and HIPS
Honeypots
Viewing and Editing Security
Verifying a IPS Configuration
Firewalls
The Basic of Firewalls
Stateless vs. Stateful Firewalls
Application Layer Gateway (ALG)
The Cisco IOS Firewall Feature Set Components
Authentication Proxy
ACL Review and Extended Access Control List
TCP and UDP Generic Inspection
Deep Packet Inspection (DPI)
Zone-Based Firewall Configuration
Class Maps and Policy-Maps
Basic Zone Configuration and Commands
Firewall with SDM
Cryptography and Virtual Private Networks (VPNs)
Introduction to Cryptography Techniques
Asymmetric and Symmetric Algorithms
Overview of Common Cryptographic Algorithms
What is a VPN?
VPN Terminology and Theory
Introduction to PKI and the Certificate of Authority
Public Key Cryptography Standards and Internet Key Exchange
Policy Match Criteria and Crypto ACLs
Using SDM to Configure Site-to-Site VPN
Generic Routing Encapsulation (GRE) Over IPSec
Using SDM to Configure GRE over IPSec
Introduction to Cisco Network Solutions
System Development Life Cycle
Cisco SDLC Phases
Disaster Recovery Techniques
Cisco Self-Defending Network
Cisco Security Management Suite
Cisco Security Agent and Interceptors