Building Enhanced Cisco Security Networks Boot Camp

Längd: 5 Days   Kurskod: BECSN

Sammanfattning:

Studies have shown that over recent years there have been increases in the number of network attacks and the number of simplified tools available to carry out such attacks. Although the number of attacks has increased, the skill required to launch network attacks has decreased. For this reason, the need to secure corporate networks has grown exponentially. Building Enhanced Cisco Security Networks Version 2.0 focuses on securing access to the enterprise network and on securing the data that flows through it.Students who attend the course will configure Layer 2 network security; Layer 3 network security; IP Security (IPsec) VPNs for Cisco® IOS® Software routers; Cisco Secure PIX®; Cisco ASA 5500 Series Adaptive Security Appliances (ASAs); Cisco Catalyst® 6500 Series Firewall Services Modules (FWSMs); Cisco Network Admission Control (NAC); IPsec VPNs using Cisco firewalls and Cisco VPN concentrators; Secure Sockets Layer (SSL) VPNs on Cisco ASAs using the Cisco Adaptive Security Device Manager (ASDM); Cisco intrusion prevention system (IPS) network devices; and Cisco Security Monitoring, Analysis, and Response System (MARS).

Målgrupp:

This course is for technical professionals who: Deploy end-to-end network security for the corporate infrastructure Troubleshoot core network security components and platforms Maintain coexistence between Cisco security technologies

Målsättning:

- Upon completion of this course, you should be able to:
- Describe common network security threats to a given enterprise network at Layer 2, Layer 3, and Layer 7
- Identify components of and configure Cisco Catalyst Integrated Security Features (CISF) throughout the Layer 2 infrastructure
- Describe and deploy Layer 3 network security methods
- Deploy NAC using the Cisco Clean Access platform
- Configure IPsec to secure communications on a network infrastructure that also utilizes Network Address Translation (NAT)
- Deploy Dynamic Multipoint VPN (DMVPN) using routing protocol methods and Next Hop
- Resolution Protocol (NHR)P to provide a dynamic encryption framework
- Deploy SSL VPNs using the Cisco ASA 5520 Adaptive Security Appliance
- Use the Cisco firewall platforms to secure enterprise network segments and provide VPN network termination
- Deploy Cisco IPS network platforms in the given network environment and make sure the device is deployed using Cisco best practices
- Deploy Cisco Security MARS for the given enterprise network and tie in Cisco routers,
- switches, firewalls, and IPS network platforms for monitoring and correlation

Förkunskaper:

- Knowledge about the following is prerequisite for this course:
- Basic routing and switching principles
- Network security best practices
- Cisco firewall products

- IPsec technology and practice
- To locate Cisco courses that cover the listed prerequisites, go to the Cisco Training and Events
- Webpage at www.cisco.com/web/learning/index.html.

Innehåll:

The course outline is as follows:

- Chapter 1: Course Overview

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.

network appliances for network connectivity.

- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and

IPS network appliances for network connectivity.

- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

The lab outline is as follows:

- Chapter 2 Lab Exercise 1: Written Exercise.

Chapter 3 Lab Exercise 2: Layer 2 Security for Enterprise Networks. This lab exercise is designed for the students to configure and troubleshoot Layer 2 network security measures such as virtual LAN access control lists (VLAN ACLs), Port Security, Dynamic Host Configuration Protocol (DHCP) Snooping, Dynamic Address Resolution Protocol (ARP)

Inspection, and IP Source Guard.

- Chapter 4 Lab Exercise 3: Layer 3 Security for Enterprise Networks. Students will configure and troubleshoot Layer 3 network security measures such as ingress and egress network filtering, routing protocol security, and black-h

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network

- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy,

monitor SSL VPNs using the Cisco ASA.

- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.

using multiple security contexts to protect network segments.

- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring

troubleshoot, and monitor SSL VPNs using the Cisco ASA.

- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation

- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for

the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a

- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using

on network routers to provide dynamic network access between network segments.

- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT

Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.

- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for

tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an

- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client

- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco

client network access.

- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network

protection and allow network access.

- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a
- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network

IPS network appliances for standalone network operation and using onboard monitoring capabilities for network

- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

using multiple security contexts to protect network segments.

- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

- Chapter 2: Network Security Overview
- Chapter 3: Layer 2 Network Security
- Chapter 4: Layer 3 Network Security
- Chapter 5: Cisco Firewalls for Enterprise Networks
- Chapter 6: NAC for Enterprise Networks
- Chapter 7: IPsec and NAT Coexistence for IOS Routers and Cisco Firewalls
- Chapter 8 (Review): DMVPN
- Chapter 9: Deploying SSL VPNs Using ASDM with the Cisco ASA
- Chapter 5 Lab Exercise 4: Configuring the Cisco Secure PIX for Network Operation.Students will configure the Cisco Secure PIX firewall to communicate with the network and will configure features such as network routing, Unicast
- Chapter 5 Lab Exercise 5: Configuring the Cisco ASA for Network Operation. Students will configure the Cisco ASA

access.

- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

firewall to communicate with the network and will configure features such as network routing, URPF, IP auditing, a

- Chapter 5 Lab Exercise 6: Configuring the Cisco FWSM for Multiple Context Mode.Students will configure a Cisco FWSM to communicate with the network using multiple security contexts to protect network segments.
- Chapter 6 Lab Exercise 7: Configuring the Cisco NAC Appliance for Network Operation.Students will configure the Cisco NAC appliance for network connectivity and deploy NAC features for client network access.
- Chapter 6 Lab Exercise 8: Cisco Clean Access Agent. Students will configure the Cisco Clean Access agent to allow client protection and allow network access.
- Chapter 7 Lab Exercise 9: Configuring Cisco Routers for IPsec and NAT Coexistence. Students will configure nested IPsec tunneling between Cisco IOS Software routers and utilize route maps to provide coexistence between IPsec an
- Chapter 8 Lab Exercise 10: DMVPN for Enterprise Networks. Students will configure and troubleshoot tunnel creation on network routers to provide dynamic network access between network segments.
- Chapter 9 Lab Exercise 11: Configuring SSL VPNs Using ASDM for the Cisco ASA. Students will use the ASDM management application to deploy, troubleshoot, and monitor SSL VPNs using the Cisco ASA.
- Chapter 10 Lab Exercise 12: Configuring Cisco IPS Devices for Network Operation.Students will configure Cisco IPS network appliances for network connectivity.
- Chapter 10 Lab Exercise 13: Monitoring Networks with Standalone IPS Network Appliances.Students will configure Cisco IPS network appliances for standalone network operation and using onboard monitoring capabilities for network
- Chapter 10: Managing Network Threats with Cisco IPS and Cisco Security MARS

Övrig information:

För mer information eller kursbokning, vänligen kontakta oss på telefon. 020-73 73 73

info@globalknowledge.se

www.globalknowledge.se

Vretenvägen 13, plan 3, 171 54 Solna