SENSS - IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS

Course Code: 5372

Learn to implement and manage security on Cisco ASA firewalls.

---

EXCLUSIVE TO GLOBAL KNOWLEDGE - Accelerate your Cisco learning experience with complimentary access to the IT Skills Video On-Demand Library, Introduction to Cybersecurity digital learning course, course recordings, IT Resource Library, and digital courseware.

Learn more

This training course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions utilizing Cisco switches, Cisco routers, and Cisco Adaptive Security Appliance (ASA) firewalls. You will acquire the foundational knowledge and capabilities to implement and manage security on Cisco ASA firewalls, Cisco routers with the firewall feature set, and Cisco switches. You will gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. At the end of the course, you will be able to reduce the risk to your IT infrastructures and applications using Cisco switches, Cisco ASA, and router security appliance feature, as well as provide detailed operations support for these products.

For on-demand learning, you will have access to this course for 12 months from the purchase date.

This course includes 30 Cisco e-lab credits. Your e-Lab credits are good for 90 days after your course ends and can be used for additional practice on the course you just completed or to explore technologies from other courses in the Global Knowledge e-Lab portfolio. Learn more.
This course supports a certification that is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

What You'll Learn

- Security threat landscape
- Implement Cisco modular network security architectures such as SecureX and TrustSec
- Deploy Cisco infrastructure management and control plane security controls
- Configure Cisco Layer 2 and Layer 3 data plane security controls
- Implement and maintain Cisco ASA Network Address Translations (NAT)
- Implement and maintain Cisco IOS Software NAT
- Designing and deploying Cisco Cyber Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection
- Implement Botnet Traffic Filters
- Deploy Cisco IOS Zone-Based Policy Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW Application Inspection Policy

Who Needs to Attend

Network security engineers
SENSS - IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS

Course Code: 5372

VIRTUAL CLASSROOM LIVE $3,795 USD 5 days

Virtual Classroom Live Outline

1. Secure Design Principles
   - Course Overview
   - Network Security Zoning
   - Cisco Module Network Security Architecture
   - Cisco SecureX Architecture
   - Cisco TrustSec Solution

2. Deploying Network Infrastructure Protection
   - Introducing Cisco Network Infrastructure Protection
   - Deploying Cisco IOS Control Plane Security Controls
   - Deploying Cisco IOS Management Plane Security Controls
   - Deploying Cisco ASA Management Plane Security Controls
   - Deploying Cisco Traffic Telemetry Methods
   - Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls

3. Deploying NAT on Cisco IOS and Cisco ASA
   - Introducing Network Address Translation
   - Deploying Cisco ASA Network Address Translation
   - Deploying Cisco IOS Software Network Address Translation

4. Deploying Threat Controls on Cisco ASA
   - Introducing Cisco Firewall Threat Controls
   - Deploying Basic Cisco ASA Access Policies
   - Deploying Advanced Cisco ASA Application Inspection Policies
   - Deploying Cisco ASA Botnet Traffic Filtering
   - Deploying Cisco ASA Identity Based Firewall

5. Deploying Threat Controls on Cisco IOS Software
   - Deploying Basic Cisco IOS Software with Basic Zone-Based Firewall Access
Policies
• Deploying Advanced Cisco IOS Software ZBFW with Application Inspection Policies

Virtual Classroom Live Labs
Lab 1: Configuring Configure Cisco Policy Protection (CPP) and Management Plane Protection (MPP)
Lab 2: Configure Traffic Telemetry Methods
Lab 3: Configure Layer 2 Data Plan Security
Lab 4: Configure Layer 2 Data Plan Security
Lab 5: Configure NAT on Cisco Adaptive Security Appliance (ASA) Firewall
Lab 6: Configure NAT on Cisco IOS Software
Lab 7: Configure Cisco ASA Access Policy
Lab 8: Configure Cisco ASA Application Inspection Policy
Lab 9: Configure Cisco ASA Identity Based Firewall
Lab 10: Configure Cisco IOS Software Zone-Based Firewall (ZBFW)
Lab 11: Configure Cisco IOS Software ZBFW Application Inspection Policy Lab

Activity Solutions

Jan 13 - 17, 2020 | 11:30 AM - 7:30 PM EST
Feb 3 - 7, 2020 | 8:30 AM - 4:30 PM EST
Mar 16 - 20, 2020 | 9:30 AM - 5:30 PM EST
Apr 27 - May 1, 2020 | 8:30 AM - 4:30 PM EST
SENSS - IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS

Course Code: 5372

ON-DEMAND $1,000 USD

On-Demand Outline

1. Secure Design Principles
   - Course Overview
   - Network Security Zoning
   - Cisco Module Network Security Architecture
   - Cisco SecureX Architecture
   - Cisco TrustSec Solution

2. Deploying Network Infrastructure Protection
   - Introducing Cisco Network Infrastructure Protection
   - Deploying Cisco IOS Control Plane Security Controls
   - Deploying Cisco IOS Management Plane Security Controls
   - Deploying Cisco ASA Management Plane Security Controls
   - Deploying Cisco ASA Botnet Traffic Filtering
   - Deploying Cisco ASA Identity Based Firewall
   - Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls

3. Deploying NAT on Cisco IOS and Cisco ASA
   - Introducing Network Address Translation
   - Deploying Cisco ASA Network Address Translation
   - Deploying Cisco IOS Software Network Address Translation

4. Deploying Threat Controls on Cisco ASA
   - Introducing Cisco Firewall Threat Controls
   - Deploying Basic Cisco ASA Access Policies
   - Deploying Advanced Cisco ASA Application Inspection Policies
   - Deploying Cisco ASA Botnet Traffic Filtering
   - Deploying Cisco ASA Identity Based Firewall

5. Deploying Threat Controls on Cisco IOS Software
   - Deploying Basic Cisco IOS Software with Basic Zone-Based Firewall Access
Policies

• Deploying Advanced Cisco IOS Software ZBFW with Application Inspection Policies

On-Demand Labs

Lab 1: Configuring Configure Cisco Policy Protection (CPP) and Management Plane Protection (MPP)
Lab 2: Configure Traffic Telemetry Methods
Lab 3: Configure Layer 2 Data Plan Security
Lab 4: Configure Layer 2 Data Plan Security
Lab 5: Configure NAT on Cisco Adaptive Security Appliance (ASA) Firewall
Lab 6: Configure NAT on Cisco IOS Software
Lab 7: Configure Cisco ASA Access Policy
Lab 8: Configure Cisco ASA Application Inspection Policy
Lab 9: Configure Cisco ASA Identity Based Firewall
Lab 10: Configure Cisco IOS Software Zone-Based Firewall (ZBFW)
Lab 11: Configure Cisco IOS Software ZBFW Application Inspection Policy
Lab Activity Solutions
SENSS - IMPLEMENTING CISCO EDGE NETWORK SECURITY SOLUTIONS

Course Code: 5372

PRIVATE GROUP TRAINING 5 days

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 11/15/2019 11:36:35 PM
Copyright © 2019 Global Knowledge Training LLC. All Rights Reserved.