Securing Networks with Cisco Firepower Threat Defense NGFW (Firepower200)

COURSE OVERVIEW:

Securing Networks with Cisco Firepower Threat Defense NGFW (Firepower200). This course will show students how to use and configure Cisco Firepower Threat Defense technology, beginning with initial device setup and configuration and including routing, high availability, Cisco ASA to Firepower Threat Defense migration, traffic control, and Network Address Translation (NAT).

The course will then explore how to implement advanced Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features, including network intelligence, file type detection, network-based malware detection, and deep packet inspection.

Students will also learn how to configure site-to-site VPN, remote-access VPN, and SSL decryption before moving on to detailed analysis, system administration, and troubleshooting. This course combines lecture materials and hands-on labs throughout to make sure that students are able to successfully deploy and manage the Cisco Firepower system.

WHO WILL BENEFIT FROM THIS COURSE?

The primary audience for this course is system installers, system integrators, system administrators, network administrators, and solutions designers who need to know how to deploy and manage a Cisco Firepower Threat Defense NGFW in their network environments. This course focuses on the features of Firepower Threat Defense that relate to the network edge use case, where the Firepower system functions primarily as a VPN headend and security gateway.

This class would be suitable for customers that are replacing Cisco ASA devices with Firepower Threat Defense.

PREREQUISITES:

We recommend that you have the following knowledge and skills before taking this course:

- Knowledge of TCP/IP and basic routing protocols, and familiarity with firewall, VPN, and IPS concepts

OBJECTIVES:

Upon completion of this course, you should be able to:

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios
- Perform initial Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services

- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security Intelligence features
- Describe Cisco AMP for Networks and the procedures for implementing file control and Advanced Malware Protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect©_
- Describe SSL decryption capabilities and usage

COURSE OUTLINE:

- Module 1: Cisco Firepower Threat Defense Overview
- Module 2: Firepower NGFW Device Configuration
- Module 3: Firepower NGFW Traffic Control
- Module 4: Firepower NGFW Address Translation
- Module 5: Firepower Discovery
- Module 6: Implementing Access Control Policies
- Module 7: Security Intelligence
- Module 8: File Control and Advanced Malware Protection
- Module 9: Next-Generation Intrusion Prevention Systems
- Module 10: Site-to-Site VPN
- Module 11: Remote-Access VPN
- Module 12: SSL Decryption
- Module 13: Detailed Analysis Techniques
- Module 14: System Administration
- Module 15: Firepower Troubleshooting

LAB OUTLINE:

- Lab 1: Initial Device Setup
- Lab 2: Device Management
- Lab 3: Configuring High Availability
- Lab 4: Migrating from Cisco ASA to Firepower Threat Defense
- Lab 5: Implementing QoS
- Lab 6: Implementing NAT
- Lab 7: Configuring Network Discovery
- Lab 8: Implementing an Access Control Policy
- Lab 9: Implementing Security Intelligence
- Lab 10: Implementing Site-to-Site VPN
- Lab 11: Implementing Remote Access VPN
- Lab 12: Threat Analysis
- Lab 13: System Administration
- Lab 14: Firepower Troubleshooting

SUNSET LEARNING INSTITUTE (SLI) DIFFERENTIATORS:

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their cloud technology investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience.
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes at any of our established training facilities or from the convenience of your home or office with the use of our HD-ILT network (High Definition Instructor Led Training)
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- Dedicated account manager to suggest the optimal learning path for you and your team
- Enthusiastic Student Services team available to answer any questions and ensure a quality training experience