TODD LAMMLE

Advanced Network Training

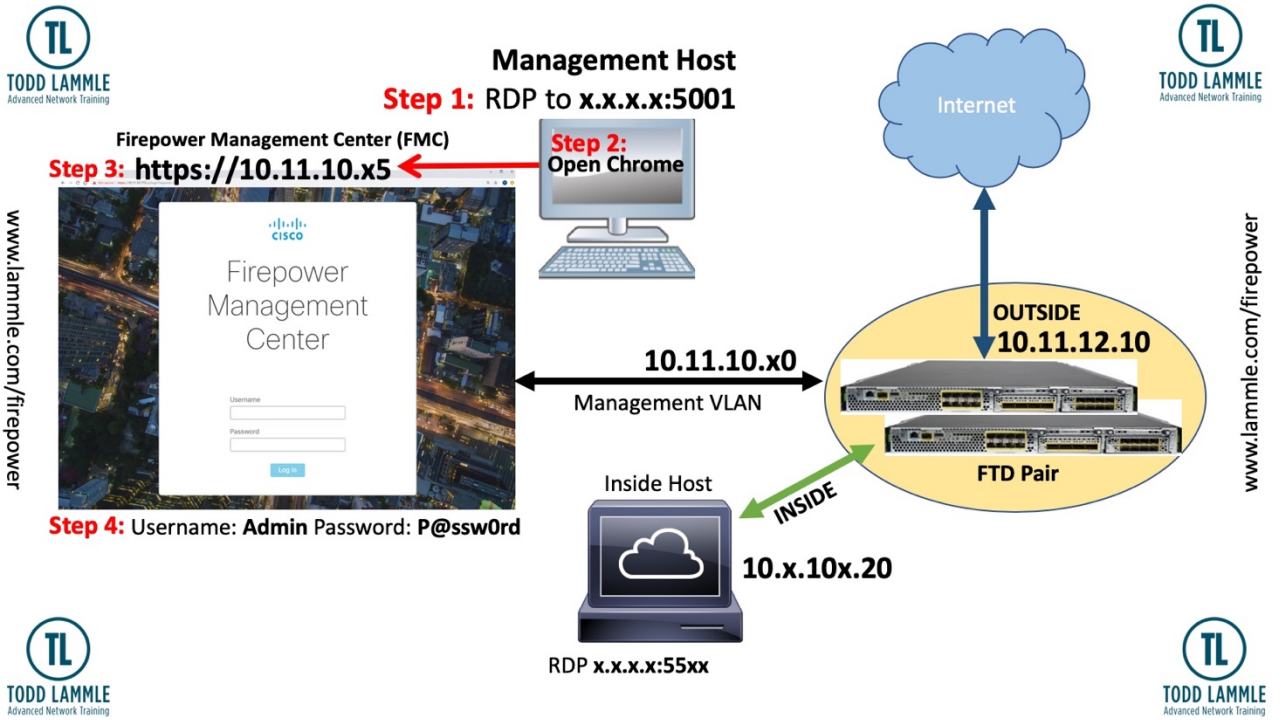
CCNP Security Cisco Network with Firepower (SCNF 300-710) bootcamp

with Todd Lammle

Receive an advanced copy of Todd Lammle's NEW

CCNP Security SCNF Study guide!

You will receive your own pod of gear that you can use all through class, and two additional days after class end date! No sharing of pods!



Course Information:

After taking 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 Cisco 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 Advanced Malware Protection (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

Prerequisites

To fully benefit from this course, you should have:

- Knowledge of TCP/IP and basic routing protocols
- Familiarity with firewall, VPN, and Intrusion Prevention System (IPS) concepts

Outline

- Cisco Firepower Threat Defense Overview
  - Examining Firewall and IPS Technology
  - Firepower Threat Defense Features and Components
  - Examining Firepower Platforms
  - Examining Firepower Threat Defense Licensing
  - Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
  - Firepower Threat Defense Device Registration
  - FXOS and Firepower Device Manager
  - Initial Device Setup
  - Managing NGFW Devices
  - Examining Firepower Management Center Policies
  - Examining Objects
  - Examining System Configuration and Health Monitoring
  - Device Management
  - Examining Firepower High Availability
  - Configuring High Availability
  - Cisco ASA to Firepower Migration
  - Migrating from Cisco ASA to Firepower Threat Defense
- Cisco Firepower NGFW Traffic Control
  - Firepower Threat Defense Packet Processing
  - Implementing QoS
  - Bypassing Traffic
- Cisco Firepower NGFW Address Translation
  - NAT Basics
  - Implementing NAT
  - NAT Rule Examples
  - Implementing NAT
- Cisco Firepower Discovery
  - Examining Network Discovery
  - Configuring Network Discovery
- Implementing Access Control Policies
  - Examining Access Control Policies
  - Examining Access Control Policy Rules and Default Action
  - Implementing Further Inspection

- Examining Connection Events
- Access Control Policy Advanced Settings
- Access Control Policy Considerations
- Implementing an Access Control Policy

- Security Intelligence
  - Examining Security Intelligence
  - Examining Security Intelligence Objects
  - Security Intelligence Deployment and Logging
  - Implementing Security Intelligence
- File Control and Advanced Malware Protection
  - Examining Malware and File Policy
  - Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
  - Examining Intrusion Prevention and Snort Rules
  - Examining Variables and Variable Sets
  - Examining Intrusion Policies
- Site-to-Site VPN
  - Examining IPsec
  - Site-to-Site VPN Configuration
  - Site-to-Site VPN Troubleshooting
  - Implementing Site-to-Site VPN
- Remote-Access VPN
  - Examining Remote-Access VPN
  - Examining Public-Key Cryptography and Certificates
  - Examining Certificate Enrollment
  - Remote-Access VPN Configuration
  - Implementing Remote-Access VPN
- SSL Decryption
  - Examining SSL Decryption
  - Configuring SSL Policies
  - SSL Decryption Best Practices and Monitoring
- Detailed Analysis Techniques
  - Examining Event Analysis
  - Examining Event Types
  - Examining Contextual Data
  - Examining Analysis Tools
  - Threat Analysis

- System Administration
  - Managing Updates
  - Examining User Account Management Features
  - Configuring User Accounts
  - System Administration
- Cisco Firepower Troubleshooting
  - Examining Common Misconfigurations
  - Examining Troubleshooting Commands
  - Firepower Troubleshooting

EXAM Information:

Securing Networks with Cisco Firepower (SNCF 300-710)

Securing Networks with Cisco Firepower v1.0 (SNCF 300-710) is a 90-minute exam associated with the CCNP Security and Cisco Certified Specialist - Network Security Firepower certifications. This exam tests a candidate's knowledge of Cisco Firepower Threat Defense and Firepower, including policy configurations, integrations, deployments, management and troubleshooting. These courses, Securing Networks with Cisco Firepower, and Securing Network with Cisco Firepower Next-Generation Intrusion Prevention System help candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam.

1.0 Deployment

1.1 Implement NGFW modes
- 1.1.a Routed mode
- 1.1.b Transparent mode

1.2 Implement NGIPS modes
- 1.2.a Passive
- 1.2.b Inline

1.3 Implement high availability options

- 1.3.a Link redundancy
- 1.3.b Active/standby failover
- 1.3.c Multi-instance

1.4 Describe IRB configurations

2.0 Configuration

2.1 Configure system settings in Cisco Firepower Management Center

2.2 Configure these policies in Cisco Firepower Management Center

- 2.2.a Access control
- 2.2.b Intrusion
- 2.2.c Malware and file
- 2.2.d DNS
- 2.2.e Identity
- 2.2.f SSL
- 2.2.g Prefilter

2.3 Configure these features using Cisco Firepower Management Center

- 2.3.a Network discovery
- 2.3.b Application detectors (Open AppID)
- 2.3.c Correlation
- 2.3.d Actions

2.4 Configure objects using Firepower Management Center

- 2.4.a Object Management
- 2.4.b Intrusion Rules

2.5 Configure devices using Firepower Management Center

- 2.5.a Device Management
- 2.5.b NAT
- 2.5.c VPN
- 2.5.d QoS
- 2.5.e Platform Settings
- 2.5.f Certificates

3.0 Management and Troubleshooting

3.1 Troubleshoot with FMC CLI and GUI

3.2 Configure dashboards and reporting in FMC

3.3 Troubleshoot using packet capture procedures

3.4 Analyze risk and standard reports

4.0 Integration

4.1 Configure Cisco AMP for Networks in Firepower Management Center
4.2 Configure Cisco AMP for Endpoints in Firepower Management Center
4.3 Implement Threat Intelligence Director for third-party security intelligence feeds
4.4 Describe using Cisco Threat Response for security investigations
4.5 Describe Cisco FMC PxGrid Integration with Cisco Identify Services Engine (ISE)
4.6 Describe Rapid Threat Containment (RTC) functionality within Firepower Management Center