TODD LAMMLE

Advanced Network Training

Mastering Cisco Firepower/FTD

with Todd Lammle

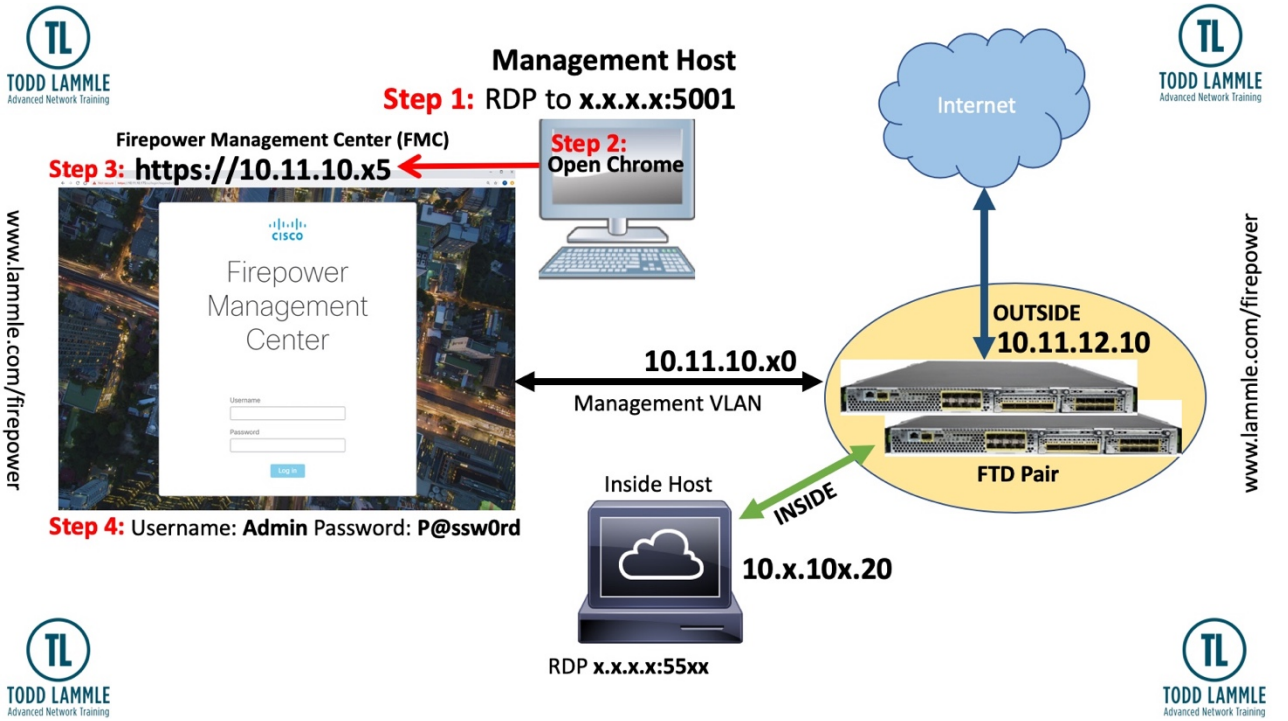
Covers the CCNP Security: Securing Cisco Networks with Firepower (SCNF 300-710)

This is *not* a vanilla Firepower class as *all* the Cisco partners run. Todd Lammle is the most experienced Cisco Firepower instructor in the world, with over 10,000 FTD installs.

His experience is second to none, and most partners have instructors for the Cisco Firepower class, and they have never installed Firepower anywhere.

Todd Lammle has been providing advanced Cisco Firepower training and consulting full time since 2013.

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



Outline

There are over 70-hands-on labs in over 40 chapters to help you really understand the material and how Firepower works! This intense class covers every feature, policy and configuration available on the Cisco Firepower product

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