INTRODUCTION TO CISCO SECURE FIREWALL

Version 1.0

1 Course Overview

In this 3-day course students will learn to deploy, configure and manage Cisco Secure Firewall/ Firepower Threat Defense. This hands-on course will help develop the skills to use and configure Cisco FTD, starting with the initial device setup and configuration. Students will learn to implement Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS) features. Students will also learn to analyze events, system administration, and basic troubleshooting.

2 Who Should Attend

- Network Security Administrators
- Network Security Engineers
- Network Security Managers
- Security Sales Engineers
- Security System Engineers
- Anyone else who wants to learn about Cisco Secure Firewall

3 Prerequisites

Before taking this course, it would be good to have some understanding of Network Security fundamentals. Exposure to working with any Network firewall will be an advantage.

4 Why Attend a Blue River Experts Course

Our courses are not delivered by instructors but by consulting system engineers who have vast experience regarding real life design, deployment, and troubleshooting of actual customer installations. Besides delivering courses, our engineers usually design and deploy large enterprise solutions or perform real world POVs (proof of value) and POCs (proof of concept) for large customers. We are often requested and contracted by product vendors to help customers make buying decisions based on their particular use case. This allows us to discuss real world use cases, designs, and operational situations with our students.

If you would like to get educated by experts who will explain to you the whole life cycle from day 0 to day 2 as they have comprehensive knowledge from having written numerous business requirements documents, customer requirements documents, high level design and detailed design documents and having deployed and troubleshooted many customer installations then you should choose to attend one of our courses.

5 Course Objectives

After completing this course, students will be able to:

- Describe the operating principles of a Next-Generation Firewall
- Configure any Cisco Secure Firewall using the GUI
- Ensure that proper perimeter security is enabled using Cisco Secure Firewall
- Describe the different common use cases of Cisco Secure Firewall

6 Course Details

6.1 Overview of Cisco Secure Firewall (CSF)

- Basic firewall and IPS terminologies
- Understand CSF features
- Examine different platforms
- Examine licensing
- General implementation use cases

6.2 Device Configuration

- Device Registration
- Differentiate between FXOS and FTD image
- Differentiate between management options FDM and FMC
- Initial device activation and configuration
- Examining different policies
- Define objects
- Explore system configuration
- Configure Health Monitoring
- Discuss device/ platform management options
- Overview of High Availability

6.3 Cisco Secure Firewall Traffic Control

- Describe packet processing
- Explain traffic bypassing
- Discuss pre-filter policy

6.4 Network Address Translation (NAT) Configurations

- Overview of NAT
- Different NAT rule types
- Implementing and configuring NAT

6.5 Network Discovery

- Explain Network Discovery
- Configure Network Discovery

6.6 Access Control Policies

- Overview of Access Control Policies (ACP)
- Describe Access Control Policy rules and default action
- Define further inspection feature in a rule
- Overview of logging options for a rule
- Advanced Settings in an ACP
- Deploying the change in an ACP

6.7 Security Intelligence

- Overview of Security Intelligence (SI)
- Configure Security Intelligence objects
- Deploy SI

6.8 File Control and Advanced Malware Protection

- Overview of malware and file policy
- Discuss Advanced Malware Protection

6.9 Next-Generation Intrusion Prevention Systems

- Overview of Intrusion Prevention and Snort rules
- Explain variables and variable sets
- Configure intrusion policies
- Describe firepower recommendations

6.10 Analyzing different Events

- Discuss different types of events
- Explore analysis tools
- Analyze threats

6.11 General System Administration

- Manage device updates
- Explore user account management features
- Configuring different user accounts

6.12 Basic Troubleshooting

- Identify common misconfigurations
- Basic troubleshooting commands
- Using packet tracer

7 Lab Exercises

7.1 Initial Device Setup

- FTD initial boot up and n/w configuration (walkthrough/ no hands-on)
- FMC initial boot up and n/w configuration (walkthrough/ no hands-on)
- FTD onboarding to FMC

7.2 Basic Configuration and Verification

- Verify/ create different objects
- Verify/ create interface and routing configuration

7.3 Configure Security Intelligence

- Configure Security Intelligence objects
- Modify/ customize Security Intelligence

7.4 Configure Intrusion Policy

- Reuse base IPS policy (SNORT2/ SNORT3)
- Create a new IPS policy (SNORT2/ SNORT3)

7.5 Configure/ Modify the Access Control Policy

- Allow internal/ DMZ access (inbound)
- Allow Internet access (outbound)
  [Use a SNORT2/ SNORT3 Intrusion Policy configured in exercise 4]

7.6 Configure NAT Policies

- Dynamic NAT
- Static NAT

7.7 Configure/ Modify Network Discovery Policy

- Understand/ differentiate hosts, users and applications
- Configure/ tune the network discovery policy based on your environment

7.8 Deploy Changes

- Review the changes that will apply to the NGFW
- Deploy all the configuration changes to the NGFW

7.9 Test/ Analyze the NGFW Traffic

- Connectivity
- IPS functionality
- Malware blocking capabilities

7.10 System Administration Overview

- Health Monitoring
- Device Backup and Restore
- Reporting Overview
- Scheduling Tasks
- Change Reconciliation