CISCO SECURE FIREWALL ADVANCED FEATURES, OPERATIONS AND MANAGEMENT

Version 1.0

Blue River Education GmbH, Schoßbachstrasse 20c, 9400 Wolfsberg, Austria
Company Register FN 429823, VAT ID ATU69349314

https://br-experts.eu/
office@blueriveredu.com

1 Course Overview

In this 3-day, lab intense course students will learn about many of the advanced features, day-2 operations and management of Cisco Secure Firewall / Firepower Threat Defense. Through intense lab exercises students will develop the skills to configure, manage and troubleshoot problems with Cisco FTD devices. After a short review of CSF, we will cover advanced features like security intelligence, file control, advanced malware protection, redundancy, external threat intelligence, domain management, SNORT3, and advanced packet flow analysis. We will also have a look at what's new in version 7.x.

You will gain leading-edge skills for high-demand security focused responsibilities.

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 a basic understanding of Cisco Secure Firewall and some hands-on experience working on the device (Cisco Secure Firewall).

If you don't have the pre-requisites described above, then a good way to prepare for this course is to attend our course "Introduction to Cisco Secure Firewall".

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 advanced features of a Next-Generation Firewall
- Explain the newly release features
- Configure advanced and newly released features
- Understand advanced packet flow analysis

6 Course Details

6.1 Overview of Cisco Secure Firewall (CSF)

- Device Configuration
- Traffic Control
- NAT Overview
- Network Discovery
- Overview of Policies

6.2 Next-Generation Features of Cisco Secure Firewall (CSF)

- Security Intelligence (SI)
- File Control and Advanced Malware Protection
- Malware and File Policy
- Overview of Intrusion Prevention and Snort Rules
- Firepower Recommendations

6.3 Cisco Secure Firewall Redundancy

- Overview of High Availability (HA)
- Discuss active / standby HA

6.4 External Threat Intelligence

- Overview of external feeds
- Describe incidents
- Explain Cisco Threat Intelligence Director (CTID)
- Understanding subscription of CTID to external feeds

6.5 Domain Management

- Introduction to multi-tenancy using domains
- Managing domains
- Creating new domains
- Moving devices between domains

6.6 VPNs

- Site-to-Site VPN
- RA-VPN

6.7 SNORT3

- Introduction to Snort3
- Explain Elephant Flow
- Discuss Snort3 recommendations
- Explain rule actions

6.8 Advance Packet Flow Analysis

- Using the “Packet-Tracer” feature
- Using the “Capture with Trace” feature

6.9 What's New in 7.x

- VPN Load Balancing for FMC managed devices
- Explain FQDN NAT
- Understand network wildcard mask object
- Discuss direct Internet access
- Describe AnyConnect with SAML external browser
- Explain encrypted visibility engine
- Discuss enhancement in TLS (focus on TLS 1.3)

7 Lab Exercises

1 Configuring CTID

2 Configure FQDN NAT

3 Using Wildcard Mask

4 Configure Direct Internet Access (DIA) with Policy Based Routing (PBR)

5 Configure Site-to-Site VPN

6 Configuring AnyConnect VPN

7 Configuring and detecting Elephant Flow using Snort3

8 Configuring Snort3 Firepower recommendations

9 Configuring additional rule actions for Snort3

10 Configuring and validating enhanced Captive Portal

11 Setting up Encrypted Visibility Engine for reports, events and telemetry

12 TLS 1.3 ESNI extension (overview/ no hands-on)

13 Advance Packet Flow Analysis

14 Configure High Availability (Active / Standby)

15 Remote deployments, selective deployment and rollbacks (overview/ no hands-on)