Course Outline

Enterprise Firewall (NSE 7) – Formerly FortiGate III

Course Summary

Description

In this three-day class, you will learn how to isolate and fix the most common issues in networks with FortiGate. In interactive labs, you will explore how to configure BGP and OSPF and to resolve misconfigurations and improve performance.

Objectives

At the end of this course, students will be able to:

- Monitor traffic passing through FortiGate.
- Optimize FortiGate memory usage.
- Diagnose using FortiGate tools such as the built-in sniffer and “diagnose debug flow” command.
- Monitor statistics for user traffic, traffic shaping, user authentication, IPsec, web proxy, BGP, OSPF, and HA.
- Troubleshoot issues with conserve mode, high CPU, firewall policies, session helpers, user authentication, IPsec, FortiGuard, UTM inspection, explicit web proxy, routing, and HA.
- Describe the processing flow of FortiGate packet inspection.
- Configure FortiGate for external BGP and OSPF.

Topics

- Troubleshooting Concepts
- System Resources
- Network Troubleshooting
- Firewall Policies
- Firewall Authentication
- FSSO
- IPsec VPN
- Security Profiles
- Explicit Web Proxy
- Operation Modes
- External BGP
- OSPF
- HA

Audience

This course is for networking and security professionals involved in the administration and support of a security infrastructure using FortiGate appliances.

Prerequisites

Students should possess knowledge of network protocols and network security concepts, as well as completion of FortiGate I and FortiGate II or their equivalents.

Duration

Three days

Course Outline

Course Name

Course Outline

I. *Troubleshooting Concepts*

II. *System Resources*

III. *Network Troubleshooting*

IV. *Firewall Policies*

V. *Firewall Authentication*

VI. *FSSO*

VII. *IPsec VPN*

VIII. *Security Profiles*

IX. *Explicit Web Proxy*

X. *Operation Modes*

XI. *External BGP*

XII. *OSPF*

XIII. *HA*