

# **Pfsense and Security Onion (Advance level)-Custom Training**

## **Course Delivery and Duration**

Delivery method can be Classroom and Online

Duration of Training: **5 Days**

## **Course Outline**

### **Advanced Pfsense:- 3 Day's**

#### **Module 1: Pfsense, The Basics**

We cover installation, configuration, GUI, backup, restore, upgrades and interfaces.

#### **Module 2: The Firewall**

Basic rules, aliases, best practices, interface grouping, and advanced firewall options.

#### **Module 3: Nat 101**

Interaction with firewall rules, port forwards, 1:1 NAT, and outbound network address translation.

#### **Module 4: Services**

DHCP and relay, DNS forwarding, dynamic DNS, SNMP, NTP server, Wake on LAN

#### **Module 5: HAProxy**

- Use cases for HAProxy
- How it works and key concepts
- How to do SSL offloading
- How to do URL Switching
- Proper health checking and server pool configuration
- Demonstration of complete configuration

### **Cryptography and VPN:- 1 Day**

#### **Module 1: Cryptography**

- Cryptography Overview
- Crypto Core
- Encryption
- Hashing with HMAC
- Digital Signature
- Digital Certificate

- Next Generation Cryptography Algorithm

## **Module 2: Site to Site VPN**

Overview, selecting the appropriate VPN, remote access with IPsec, OpenVPN and PPTP, Site to Site with IPsec and OpenVPN.

## **IPS and IDS Using Snort:- 1 Day**

### **Module 1: Security Onion Overview**

### **Module 2: IPS and IDS Using Snort**

- Installing and configuring Snort
- How Snort works
- Understanding Snort rules
- Tuning Snort to remove false-positives
- Demonstration of complete configuration