CISCO FIREPOWER Training - Kursübersicht

1. **Einführung in die Thematik NGFW**
   a. Entwicklung der Firewalls
   b. Bedrohungen und Cyber-Berichte
   c. Cyber Kill Chain Model

2. **Cisco Firepower – Überblick**
   a. Modele und Hardware Dimensionierung (Hardware Architektur, Software Varianten)
   b. Firewall Verwaltung – Möglichkeiten und Voraussetzungen
   c. Lizensierung (Classic vs Smart)
   d. ASA to FTD Migration

3. **Design- und Implementierungsleitfäden**
   a. Erster Bootvorgang und Installation
   b. Routed vs Transparent Mode
   c. BVI (bridged, L2) und L3 (routed) Ports
   d. Hochverfügbarkeit (HA) und Clustering

4. **NGFW und IP-Verkehrskontrolle**
   a. Paketfluss und Datenverarbeitung
   b. Wiederverwendbare Objekte und Objekt-Manager
   c. Routing-Protokolle (Static, OSPF, BGP)
   d. Netzwerkadressübersetzung (NAT / PAT)
   e. Vorfilter-Richtlinie (Fast-path)
   f. Intelligent Application Bypass
   g. Netzwerk Discovery und Host Profiling
   h. Security Intelligence (DNS Policy, Sinkholes, DNS and IP Reputation)
   i. SSL-Richtlinie
   j. Preprocessors, Netzwerkanalyse und IPS (Intrusion Prevention System)
   k. Identitätsrichtlinie (Realms für AD-Integration, Cisco User Agent)
   l. Dateikontrolle und erweiterter Malware-Schutz (AMP)
   m. Zugriffskontrollrichtlinie und FW-Regelwerk
   n. Quality of Service (QoS) auf FTD
   o. Ereignis-Korrelation und Gegenmaßnahmen

5. **Systemmanagement und -verwaltung**
   a. Benutzerkonten
   b. Verbindungsereignisse und Protokollierung
   c. Backup und Aktualisierungen / Upgrades
   d. Berichterstattung
   e. FlexConfig

6. **Sichere Remote-Verbingungen**
   a. Site-to-Site IPSec-basiertes VPN
   b. Remote Access VPN

7. **NGFW Fehlerdiagnose und -behebung**
   a. Werkzeuge (GUI und CLI)
   b. Expert mode
   c. System und NGFW-Dienste

Praktische Laborübungen:

1. Cisco ASA (SFR) – einfaches Setup in Routed-Mode (L3) und Netzwerk-Discovery.
2. Cisco FTDv – einfaches Setup (On-box / FMC Verwaltung) und Netzwerk-Discovery.
3. FMCv – Review und Konfiguration (Einstellungen, Verwaltungsrichtlinie).
4. Konfiguration von wiederverwendbaren Objekten (Zonen, Applikationsfilter).
5. Implementierung des Routings (Statische Routen, OSPF, BGP).
6. Implementierung der statischen und dynamischen NAT/PAT Regeln.
7. Konfiguration und Monitoring des QoS auf FTD.
8. Konfiguration und Monitoring von Netzwerk-Discovery (FMC).
9. Definierung und Implementierung einer DNS-Richtlinie (ASA SFR / FMC).
10. Definierung und Implementierung von Security Intelligence (ASA SFR / FMC).
11. Konfiguration der Datei-Kontrollrichtlinie (AMP).
12. Definierung und Implementierung der Zugriffskontrollrichtlinie mit IPS (SFR/FMC).
13. Konfiguration und Verifizierung von Ereignis-Korrelation und Gegenmaßnahmen.
14. Systemverwaltung (Aufgabenplanung, Backup, Ereignissuche, FlexConfig).
15. Berichterstattung – Erstellen von Standard und kundenspezifischen Berichten (FMC).
16. Implementierung und Tests von IPSec-basierten S2S VPN Tunnel.
17. Konfiguration und Verifizierung der Hochverfügbarkeit mit FTD Sensoren.
18. Fehlerdiagnose und -behebung von FTD System und Benutzerverkehr.

Lab Layout: