CISCO FIREPOWER next-generation Firewall - BOOTCAMP

Ziele der Schulung

In diesem Kurs befassen sich die Teilnehmer mit der Cisco Firepower-Technologie. Dies beinhaltet einen Überblick, eine grundlegende Einführung und eine Vorstellung der Hardware und Software sowie der Setup- und Installationsgrundlagen. Zudem werden Themen wie IP- Routing, Network Address Translation (NAT/PAT), High Availability und Clustering behandelt. Außerdem wird in dem Kurs detailliert auf die NGFW-Funktionen eingegangen und die Konfiguration und Implementierung von Network Discovery, Security Intelligence, File und Malware Detection, Next-generation IPS und Secure Connectivity Technologien behandelt.
Die Teilnehmer werden nach der Schulung in der Lage sein, selbstständig Cisco Firepower Firewalls zu installieren und zu verwalten.

Zielgruppe

- Netzwerktechniker, -installateure und -administratoren
- Systemintegratoren
- Sicherheitsberater
- IT-Sicherheit Analysten und IT-Forensiker
- Personal von Sicherheits- und Netzwerkbetriebszentren (SOC/NOC)
- Lösungsdesigner und -architekten

Voraussetzungen

Es wird empfohlen, dass Teilnehmer bereits Erfahrungen im Umgang mit Cisco ASA Firewalls gesammelt haben, die gängigen Routing-Protokolle und Switching-Technologien kennen, über ein gutes TCP/IP-Verständnis verfügen und idealerweise bereits mit Packet Filtering Technologien gearbeitet haben.

AGENDA

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 und Threat Defense Service Policies

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

8. **Integrationen**
    a. pxGrid
    b. AMP for Endpoints
    c. Threat Intelligence Director (3rd party Intelligence feeds)
    d. Cisco Threat Response (CTR)

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. Einrichtung und Tests der Inline-Set Schnittstellen (IDS/IPS).
8. Konfiguration und Monitoring des QoS auf FTD.
9. Konfiguration und Monitoring von Netzwerk-Discovery.
10. Definierung und Implementierung einer DNS-Richtlinie.
11. Definierung und Implementierung von Security Intelligence.
12. Konfiguration der Datei-Kontrollrichtlinie (AMP).
13. Definierung und Implementierung der Zugriffskontrollrichtlinie mit IPS.
14. Konfiguration und Verifizierung von Ereignis-Korrelation und Gegenmaßnahmen.
15. Systemverwaltung (Aufgabenplanung, Backup, Ereignissuche, FlexConfig).
16. Berichterstattung – Erstellen von Standard und kundenspezifischen Berichten.
17. Implementierung und Tests von IPSec-basierten S2S VPN Tunnel.
18. Konfiguration und Verifizierung der Hochverfügbarkeit mit FTD Sensoren.
19. Fehlerdiagnose und -behebung von FTD System und Benutzerverkehr.
20. Threat Intelligence Director – Implementierung von 3rd party Intelligence Feeds.