

Cisco Secure Firewall ASA

Auf ASA- und Firepower-Plattformen

Je stärker sich Unternehmensabläufe in der IT-Infrastruktur widerspiegeln, desto notwendiger werden abgesicherte Netzstrukturen und der Schutz der Daten. Firewalls sind aus modernen Netzen nicht mehr wegzudenken. Dieser Kurs vermittelt solide Kenntnisse der Einsatz- und Konfigurationsmöglichkeiten der Cisco Secure Firewall ASA als Firewall. Die Teilnehmer werden in die Lage versetzt, alle relevanten Firewall-Funktionen der Software zu verstehen und kompetent zu nutzen. Der Kurs betrachtet die Installation und den Betrieb sowohl auf den klassischen ASA-Plattformen als auch auf den Firepower-Geräten. Zusätzlich erhalten die Teilnehmer einen ersten Einblick in die Next Generation Firewall von Cisco in Form von Cisco Secure Firewall Threat Defense (FTD).

Kursinhalt

- Grundkonfiguration und Management der ASA
- Betrieb der ASA-Software auf Firepower- und ASA-Plattformen
- Routing
- Access-Rules und Objects
- NAT und PAT
- Contexte
- Inspection
- Redundanzkonzepte und Clustering
- Transparent Firewall
- Layer 7 Inspection
- Firepower
- Troubleshooting-Werkzeuge der ASA

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Der Kurs richtet sich an Netzwerker, die bereits praktische Erfahrungen mit der Konfiguration von Cisco Routern gesammelt haben und in diesem Kurs die Firewall Features der ASA kennen lernen wollen.

Voraussetzungen

Dieser Kurs setzt grundlegendes, produktspezifisches Know-how des Cisco IOS, Kenntnisse des TCP/IP-Protokolls und seiner Sicherheitsrisiken sowie Grundlagen des Switchings und Routings voraus. Die Teilnehmer sollten außerdem mit der Arbeitsweise von Paketfiltern und Firewalls vertraut sein.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/ASA1

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in der Schweiz	5 Tage CHF 3.790,-
Online Training	5 Tage CHF 3.075,-
Termine auf Anfrage	

Stand 24.02.2024



Inhaltsverzeichnis

Cisco Secure Firewall ASA – Auf ASA- und Firepower-Plattformen

1 Die Grundkonfiguration der ASA	3.3.5 Abarbeitung der NAT-Regeln	5.8.3 Access Control Policy: URL Filter
1.1 ASA als Firewall	3.3.6 Die Xlate-Tabelle	5.8.4 Access Control Policy: Users
1.2 ASA-Modellreihe	3.3.7 Connections	5.9 Das Konzept hinter AMP
1.3 Firepower-Modellreihen	3.3.8 NAT und IPv6	5.9.1 Die Analyse
1.4 FPR4100/9300: FXOS und Applikationen	3.4 Inspection	5.10 Einsatz als IPS oder IDS
1.5 ASA Software	3.4.1 Editieren einer Policy	5.10.1 Interfaces
1.5.1 ASA – Die ersten Schritte im CLI	3.4.2 Troubleshooting und Monitoring	5.10.2 Evasion Attacks
1.5.2 Das CLI (Serien 4100, 9300)	3.5 Accelerated Security Path ASP	5.11 Firepower als SSL-Proxy
1.5.3 Das CLI (Serien 1000, 2100 und 3100)	3.6 Paketverarbeitung	
1.5.4 Die Konfigurationsdateien	3.7 Packet Tracer	
1.6 Lizenzen	3.8 Packet Capture	
1.6.1 Lizenzierung mit PAK	3.8.1 Packet Capture: CLI	
1.6.2 Smart Licensing		
1.6.3 Lizenzen und Failover		
1.7 Initiale Konfiguration	4 Advanced Topics	6 ASA-Maintenance
1.8 Remote-Zugriff	4.1 Contexte	6.1 ASA: Image Upgrades
1.8.1 Management mit dem ASDM	4.1.1 Der Admin Context	6.2 Firepower-Modul: Installation
1.8.2 Management-Zugriff: Konfiguration	4.1.2 Anlegen weiterer Contexte	6.3 FPR2100: Installation und Upgrade der ASA
1.9 Das Security-Konzept der ASA	4.1.3 Zuteilung von Ressourcen	6.3.1 Konvertieren zum Platform Mode
1.10 Interface-Konfiguration	4.1.4 Die Sicht im ASDM	6.3.2 FRP1000, 2100, 3100: Upgrade der ASA
1.10.1 Interface-Konfiguration: FPR1010 und 5506-X	4.1.5 Zuordnung der Pakete	6.4 FPR4100/9300: Chassis-Management
1.10.2 Interface-Konfiguration: Routed Ports	4.1.6 Contexte – die Kontrolle	6.4.1 Interface-Typen
1.10.3 ASDM – Interface-Konfiguration	4.2 Redundanz	6.4.2 Konfiguration der Interfaces
1.11 Die Systemzeit	4.2.1 Redundant Interface und Etherchannel	6.4.3 Chassis-Management: FXOS
1.12 Logging und Debugging	4.2.2 Active/Standby Failover	6.5 Installation der ASA als Logical Device: CLI
1.13 SNMP	4.2.3 Active/Active Failover	6.5.1 Konfiguration der App Instance
1.14 NetFlow	4.2.4 Firewall Cluster	6.5.2 Konfiguration des Logical Devices
	4.3 Transparent Firewall	6.5.3 Löschen des Logical Devices
	4.3.1 Sichtweise des ASDM	6.6 Installation der ASA als Logical Device: FCM
	4.3.2 Bridging	6.6.1 Monitoring
	4.3.3 Ethertype ACLs	6.7 FPR4100/9300: Software-Update
2 Routing	4.4 Layer 7 Inspection	6.8 Password Recovery
2.1 Die Routing-Tabelle		6.8.1 Password Recovery bei FPR1000, 2100, 3100
2.1.1 Routing-Entscheidungen		6.8.2 Password Recovery bei FPR 4100, 9300
2.2 Statische Routen		6.9 Disaster Recovery
2.3 OSPF	5 Firepower	6.10 Backup und Restore
2.3.1 OSPFv3	5.1 Das Konzept Firepower	
2.4 EIGRP	5.1.1 IPS	A Cisco Secure Firewall ASA – Übungen
2.5 BGP	5.1.2 Advanced Malware Protection	A.1 Netzwerktopologie
	5.2 Firepower auf der ASA	A.2 Interfacekonfiguration
	5.2.1 Firepower-Modul: Einbinden in das Netzwerk	A.3 Administrativer Zugriff
3 Basic Firewall	5.3 FTD: Das Management-Netz	A.4 Statisches Routing
3.1 Access-Listen	5.4 Paketverarbeitung	A.5 Accesslisten
3.1.1 Objects und Object Groups	5.5 On-Box-Management	A.6 NAT
3.1.2 Time-based Access-Lists	5.6 Firepower Management Center	A.7 Inspections
3.1.3 Access-Listen und IPv6	5.6.1 Die Menüstruktur	A.8 Active/Standby Failover
3.2 TrustSec	5.6.2 Einbindung in das Management Center	A.9 Contexte und Active/Active Failover
3.3 NAT	5.7 Lizenzmodell des Firepower-Moduls	A.10 Lösungsmöglichkeit für die ACL-Übung
3.3.1 Dynamisches Network Object NAT	5.8 Access Control Policy	A.11 Lösung für die NAT-Übung
3.3.2 Statisches Network Object NAT	5.8.1 Access Control Policy: Actions	A.12 Lösung für die Inspection-Übung
3.3.3 Dynamisches Manual NAT	5.8.2 Access Control Policy: Applications	
3.3.4 Statisches Manual NAT		

