

# 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.de/go/ASA1](http://www.experteach.de/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 Deutschland	5 Tage	€ 2.795,-
Online Training	5 Tage	€ 2.795,-
Termine auf Anfrage		

Stand 24.02.2024



# Inhaltsverzeichnis

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

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

