

# Cisco Secure Firewall ASA

## Konfiguration und Inbetriebnahme von Firewall und VPN Features

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 sowohl für den Einsatz als Firewall, als auch für den Einsatz als VPN-Gateway. 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.

### Kursinhalt

- Grundkonfiguration und Management der ASA
- Routing
- Access-Rules und Objects
- NAT und PAT
- Inspection/Application Layer Gateway
- Contexte
- Redundanzkonzepte und Clustering
- VPN-Grundlagen
- Site-to-Site VPN
- Remote Access VPN
- Troubleshooting-Werkzeuge der ASA
- Maintainance

**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 die Firewall und VPN-Features der ASA kennen lernen wollen.

### Voraussetzungen

Dieser Kurs setzt Kenntnisse des TCP/IP-Protokollstacks und seiner Sicherheitsrisiken sowie Grundlagen des Switchings und Routings voraus.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/ASA3](http://www.experteach.at/go/ASA3)

### 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.	
<b>Termine in Deutschland</b>	<b>5 Tage</b>	<b>€ 2.995,-</b>	
<b>Online Training</b>	<b>5 Tage</b>	<b>€ 2.995,-</b>	
<b>Termin/Kursort</b>	Kurssprache Deutsch 		
24.06.-28.06.24	 Hamburg	09.09.-13.09.24	 Online
24.06.-28.06.24	 Online	02.12.-06.12.24	 Hamburg
09.09.-13.09.24	 Frankfurt	02.12.-06.12.24	 Online

Stand 28.04.2024



# Inhaltsverzeichnis

## Cisco Secure Firewall ASA – Konfiguration und Inbetriebnahme von Firewall und VPN Features

<b>1 Die Grundkonfiguration der ASA</b>	<b>4.1.4</b> Die Sicht im ASDM – Admin-Context	<b>7 SSL VPNs</b>
<b>1.1</b> ASA als Firewall	<b>4.1.5</b> Zuordnung der Pakete	<b>7.1</b> SSL VPN: Varianten
<b>1.2</b> Firepower-Modellreihen	<b>4.1.6</b> Contexte – die Kontrolle	<b>7.1.1</b> Das Konzept: Vererbung der Rechte
<b>1.3</b> ASA-Software	<b>4.2</b> Redundanz	<b>7.1.2</b> Grundlegende SSL/TLS-Einstellungen
<b>1.3.1</b> FPR4100 und 9300: FXOS und Applikationen	<b>4.2.1</b> Redundant Interface und Etherchannel	<b>7.2</b> Der Cisco Secure Client
<b>1.3.2</b> ASA – Die ersten Schritte im CLI	<b>4.2.2</b> Active/Standby Failover	<b>7.2.1</b> Anpassung des Secure Client
<b>1.3.3</b> Das CLI des FXOS	<b>4.2.3</b> Failover und Lizenzen	<b>7.3</b> Benutzerauthentisierung per AAA
<b>1.3.4</b> Die Konfigurationsdateien	<b>4.2.4</b> Active/Active Failover	<b>7.3.1</b> 2-Faktor-Authentisierung
<b>1.4</b> Smart Licensing	<b>4.2.5</b> Firewall Cluster	<b>7.4</b> Konfiguration von RA SSL VPNs
<b>1.5</b> Initiale Konfiguration		<b>7.4.1</b> Das Connection Profile
<b>1.5.1</b> Management-Zugriff	<b>5 VPN-Grundlagen</b>	<b>7.4.2</b> Die Group Policy
<b>1.6</b> Management mit dem ASDM	<b>5.1</b> VPN-Varianten von Cisco	<b>7.4.3</b> Secure Client Image
<b>1.6.1</b> Management-Zugriff	<b>5.1.1</b> Verschiedene Wege bei VPNs	<b>7.4.4</b> Secure Client Profile
<b>1.7</b> Das Security-Konzept der ASA	<b>5.2</b> Der Secure Client	<b>7.4.5</b> Die Konfiguration im CLI
<b>1.8</b> Interface-Konfiguration	<b>5.2.1</b> Lizenzen	<b>7.4.6</b> Authentisierung mit externem AAA-Server
<b>1.8.1</b> Interface-Konfiguration: Desktop-Modelle	<b>5.3</b> Die Struktur von IPsec	<b>7.4.7</b> Kontrolle auf dem Client
<b>1.8.2</b> Interface-Konfiguration: Routed Ports	<b>5.4</b> IPsec – Die Betriebsarten	<b>7.4.8</b> Kontrolle auf der ASA
<b>1.8.3</b> ASDM – Interface-Konfiguration	<b>5.5</b> Die IPsec-Protokolle	<b>7.4.9</b> Client-Authentisierung mit Zertifikaten
<b>1.9</b> Die Systemzeit	<b>5.5.1</b> ESP: Vertraulichkeit und Integrität	<b>7.4.10</b> Tunnelgruppen und Zertifikate
<b>1.10</b> Logging und Debugging	<b>5.5.2</b> IPsec und NAT	<b>7.5</b> HostScan/Posture und DAP
<b>1.11</b> SNMP	<b>5.5.3</b> Anti Replay – Sequence Number	<b>7.5.1</b> Host Scan/Secure Firewall Posture
<b>1.12</b> NetFlow	<b>5.5.4</b> Überprüfung des Paketes beim Empfang	<b>7.5.2</b> Dynamic Access Policies
<b>2 Routing</b>	<b>5.6</b> IKEv2	<b>7.5.3</b> ISE Posture
<b>2.1</b> Die Routing-Tabelle	<b>5.6.1</b> Security Associations	
<b>2.1.1</b> Routing-Entscheidungen	<b>5.6.2</b> IKEv2 – der Ablauf	<b>8 ASA-Maintenance</b>
<b>2.2</b> Statische Routen	<b>5.6.3</b> Die Authentisierung	<b>8.1</b> Upgrade der ASA
<b>2.3</b> OSPF	<b>5.6.4</b> Option: Extensible Authentication Protocol	<b>8.2</b> Upgrade der Serien FPR4100 und 9300
<b>2.3.1</b> OSPFv3	<b>5.6.5</b> Option: Remote Access VPN	<b>8.2.1</b> Interface-Typen
<b>3 Firewalling</b>	<b>5.7</b> TLS – Transport Layer Security	<b>8.2.2</b> Konfiguration der Interfaces
<b>3.1</b> NAT	<b>5.7.1</b> Der TLS Verbindungsaufbau	<b>8.2.3</b> Chassis-Management: FXOS
<b>3.1.1</b> Objects und Object Groups	<b>5.7.2</b> Sichere Datenübertragung	<b>8.2.4</b> Installation der ASA als Logical Device
<b>3.1.2</b> Dynamisches Network Object NAT	<b>6 IPsec Site-to-Site VPNs</b>	<b>8.2.5</b> Installation der ASA als Logical Device: FCM
<b>3.1.3</b> Statisches Network Object NAT	<b>6.1</b> Site-to-Site VPNs: Das Konzept	<b>8.2.6</b> Monitoring
<b>3.1.4</b> Dynamisches Manual NAT	<b>6.2</b> Konfiguration per Assistent	<b>8.2.7</b> FPR4100/9300: Software-Update
<b>3.1.5</b> Statisches Manual NAT	<b>6.3</b> Manuelle Konfiguration	<b>8.3</b> Passwort und Disaster Recovery
<b>3.1.6</b> NAT und IPv6	<b>6.3.1</b> Connection Profile und Tunnel Group	<b>8.3.1</b> Password Recovery bei FPR 4100, 9300
<b>3.1.7</b> Abarbeitung der NAT-Regeln	<b>6.3.2</b> Die Group Policy	<b>8.4</b> Backup und Restore
<b>3.1.8</b> Die Xlate-Tabelle	<b>6.3.3</b> Die Crypto Map	
<b>3.2</b> Troubleshooting	<b>6.3.4</b> Die IKE Policies	<b>A Cisco Secure Firewall – Übungen</b>
<b>3.2.1</b> Packet Tracer	<b>6.3.5</b> IKE Parameter	<b>A.1</b> Netzwerktopologie
<b>3.2.2</b> Packet Capture	<b>6.3.6</b> IPsec Transform Sets	<b>A.2</b> Interfacekonfiguration
<b>3.3</b> Access-Listen	<b>6.3.7</b> System Options	<b>A.3</b> Administrativer Zugriff
<b>3.3.1</b> Objects und Object Groups in ACLs	<b>6.3.8</b> Kontrolle im ASDM	<b>A.4</b> Statisches Routing
<b>3.3.2</b> Time-based Access-Lists	<b>6.3.9</b> Kontrolle im CLI	<b>A.5</b> NAT
<b>3.3.3</b> Access-Listen und IPv6	<b>6.3.10</b> NAT	<b>A.6</b> Accesslisten
<b>3.3.4</b> Connections	<b>6.4</b> Kontrolle im CLI	<b>A.7</b> Inspections
<b>3.4</b> Inspection	<b>6.4.1</b> Debugging	<b>A.8</b> Active/Standby Failover
<b>3.4.1</b> Editieren einer Policy	<b>6.5</b> Authentisierung mit Zertifikaten	<b>A.9</b> Site-to-Site VPN mit PSK
<b>3.4.2</b> Troubleshooting und Monitoring	<b>6.5.1</b> Stammzertifikat	<b>A.9.1</b> Authentisierung mit Zertifikaten
<b>3.4.3</b> Management Policy	<b>6.5.2</b> Identity Certificate	<b>A.10</b> SSL VPN mit dem Cisco Secure Client
<b>3.5</b> Paketverarbeitung	<b>6.5.3</b> Zertifikate und Tunnel Groups	<b>A.10.1</b> AAA mit externer Authentisierung
<b>3.5.1</b> Accelerated Security Path ASP	<b>6.5.4</b> Konfiguration im CLI	<b>A.10.2</b> Zertifikat auf dem Client
<b>4 Contexte und Redundanzkonzepte</b>	<b>6.6</b> Dynamische IP-Adressen	<b>A.11</b> Contexte und Active/Active Failover (optional)
<b>4.1</b> Contexte	<b>6.6.1</b> Die dynamische Crypto Map	<b>A.12</b> Lösungsmöglichkeit für die ACL-Übung
<b>4.1.1</b> Der Admin-Context	<b>6.7</b> Virtual Tunnel Interfaces	<b>A.13</b> Lösung für die NAT-Übung
<b>4.1.2</b> Anlegen weiterer Contexte	<b>6.7.1</b> VTI: Konfiguration im ASDM	<b>A.14</b> Lösungsmöglichkeit für die Inspection-Übung
<b>4.1.3</b> Zuteilung von Ressourcen	<b>6.7.2</b> VTI-Konfiguration im CLI	<b>A.15</b> Lösungsmöglichkeit für RA VPN
	<b>6.7.3</b> VTI: Kontrolle	

