

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.ch/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.	
Termine in Deutschland	5 Tage	CHF 3.295,-	
Online Training	5 Tage	CHF 3.295,-	
Termin/Kursort	Kursprache 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

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

