

# Cisco Next Generation Firewall

## Sichere Netze mit Firepower

Mit den Firepower Appliances bzw. der Cisco Secure Firewall bietet Cisco eine Next-Generation Firewall, die sich neben der vereinheitlichten Konfiguration über ein Policy-Modell weiterhin sehr stark auf den Schutz vor Bedrohungen im Netzwerk-Umfeld konzentriert.

Neben den klassischen Firewall-Funktionalitäten bieten die verschiedenen Firepower-Systeme auch Application Control, Threat Prevention und Advanced Malware Protection und IPS. Dieser Kurs vermittelt solide Kenntnisse der Einsatz- und Konfigurationsmöglichkeiten der Cisco NGFW. Sie werden in die Lage versetzt, alle relevanten Firewallfunktionen der NGFW zu verstehen und kompetent zu nutzen. Dieser Firepower Kurs konzentriert sich auf das Management mit dem Firepower Management Center.

### Kursinhalt

- Konzepte der Cisco Firepower Thread Defense (FTD) Appliance
- Funktionen der NGFW
- Initiale Konfiguration und Management der Firepower Appliance
- Firepower Management Center
- Network Discovery
- Routing mit FTD
- NAT und PAT mit FTD
- Access Control Policy
- Application und URL Filter
- High Availability (Active/Standby Failover)
- FlexConfig
- SSL-Proxy
- Quality of Service
- Licensing, Upgrade und Backup

**E-Book** Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

### Zielgruppe

Der Kurs richtet sich an Personen in der Security- und Netzwerk-Administration, die eine Firepower Thread Defense Appliance in Betrieb nehmen und verwalten werden. Der Fokus liegt dabei auf der Funktionalität der Next-Generation Firewall. Sollten Sie planen, die Cisco ASA in ihrem Netzwerk durch FTD zu ersetzen, sind Sie ebenfalls richtig in diesem Kurs.

### Voraussetzungen

Sie sollten zu diesem Kurs grundlegende Kenntnisse des TCP/IP-Protokolls und seiner Sicherheitsrisiken sowie Grundlagen des Switchings und Routings mitbringen. Außerdem sollten sie bereits 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/CFPF](http://www.experteach.ch/go/CFPF)

### 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>3 Tage CHF 2.635,-</b>
<b>Termine in Österreich</b>	<b>3 Tage CHF 2.635,-</b>
<b>Termine in der Schweiz</b>	<b>3 Tage CHF 3.190,-</b>
<b>Online Training</b>	<b>3 Tage CHF 2.635,-</b>
<b>Termin/Kursort</b>	Kursprache Deutsch
23.06.-25.06.25  Hamburg	13.10.-15.10.25  Online
23.06.-25.06.25  Online	13.10.-15.10.25  Wien
28.07.-30.07.25  Düsseldorf	10.11.-12.11.25  Hamburg
28.07.-30.07.25  Online	10.11.-12.11.25  Online
01.09.-03.09.25  Frankfurt	15.12.-17.12.25  Düsseldorf
01.09.-03.09.25  Online	15.12.-17.12.25  Online
01.09.-03.09.25 Zürich	

Stand 07.05.2025



# Inhaltsverzeichnis

## Cisco Next Generation Firewall – Sichere Netze mit Firepower

<b>1</b>	<b>Die Grundkonfiguration von FTD</b>	<b>3.1.2</b>	Abarbeitung der NAT-Regeln	<b>4.5.1</b>	CA einrichten
<b>1.1</b>	Next Generation Firewall	<b>3.1.3</b>	Dynamisches Auto NAT	<b>4.5.2</b>	Decryption Policy
<b>1.2</b>	Hardware: Die Modellreihen	<b>3.1.4</b>	Statisches Auto NAT	<b>4.5.3</b>	Decryption Policy: Best Practice
<b>1.2.1</b>	Firewall Performance Estimator	<b>3.1.5</b>	Statisches Manual NAT	<b>4.6</b>	Snort 3
<b>1.3</b>	Software: FXOS und FTD	<b>3.1.6</b>	Statisches Manual NAT: Twice NAT	<b>4.6.1</b>	Snort 3: Neue Funktionen
<b>1.4</b>	Lizenzen	<b>3.1.7</b>	Dynamisches Manual NAT	<b>5</b>	<b>Maintenance</b>
<b>1.5</b>	Initiale Konfiguration und Management	<b>3.2</b>	Troubleshooting: Packet Tracer und Capture	<b>5.1</b>	Updates
<b>1.5.1</b>	Die ersten Schritte im CLI	<b>3.2.1</b>	Packet Capture	<b>5.2</b>	Update des FMC
<b>1.5.2</b>	Die ASA-Console	<b>3.2.2</b>	capture-traffic	<b>5.3</b>	FXOS Upgrade
<b>1.5.3</b>	Firewall Device Manager	<b>3.3</b>	Access Control Policy	<b>5.4</b>	FTD-Update
<b>1.6</b>	Das Firewall Management Center	<b>3.3.1</b>	Access Control Policy: Actions	<b>5.4.1</b>	Content Updates
<b>1.6.1</b>	Die Menüstruktur	<b>3.3.2</b>	Access Control Policy: Regeln	<b>5.5</b>	Password Recovery
<b>1.6.2</b>	FMC: Benutzerverwaltung	<b>3.3.3</b>	Access Control Policy: Networks	<b>5.6</b>	Backup & Restore
<b>1.6.3</b>	Das Management-Netz	<b>3.3.4</b>	Access Control Policy: Ports	<b>5.6.1</b>	Backup Profiles
<b>1.6.4</b>	Konfiguration des Managers auf FTD-Geräten	<b>3.3.5</b>	Access Control Policy: Vererbung	<b>5.6.2</b>	Backup von FTD-Geräten
<b>1.6.5</b>	Object Management	<b>3.3.6</b>	Access Control Policy: URL Filter	<b>5.6.3</b>	Restore des Management Centers
<b>1.6.6</b>	Deploy	<b>3.3.7</b>	Access Control Policy: Weitere Parameter	<b>5.6.4</b>	Restore der FTD-Geräte
<b>1.6.7</b>	Smart Licensing	<b>3.3.8</b>	Access Control Policy: Users	<b>5.7</b>	Wiederkehrende Aufgaben
<b>1.6.8</b>	License Reservation	<b>3.3.9</b>	Logging in der Access Control Policy	<b>5.7.1</b>	Beispiel: Backups
<b>1.6.9</b>	Interface-Konfiguration	<b>3.3.10</b>	Access Control Policy: Organisation	<b>5.7.2</b>	Beispiel: Deployment und Updates
<b>1.6.10</b>	Interface-Zonen und -Gruppen	<b>3.3.11</b>	Access Control Policy: Vererbung	<b>5.8</b>	Migration von ASA zu FTD
<b>1.7</b>	Die Systemzeit	<b>3.3.12</b>	Access Control Policy: Lock Policy	<b>A</b>	<b>Übungen</b>
<b>1.7.1</b>	Systemzeit der FTD-Geräte	<b>3.3.13</b>	Access Control Policy: Connections Events	<b>A.1</b>	Netzwerktopologie
<b>1.8</b>	DNS-Gruppen	<b>3.3.14</b>	Security Intelligence	<b>A.2</b>	Anlegen eines neuen Benutzers (optional)
<b>1.9</b>	Die Health Policy	<b>3.3.15</b>	DNS Policy	<b>A.3</b>	Einbinden in das FMC
<b>1.9.1</b>	Health Monitor	<b>3.4</b>	Prefilter Policy	<b>A.4</b>	Kontrolle der Grundkonfiguration
<b>1.10</b>	Die Network Discovery Policy	<b>3.5</b>	Encrypted Visibility Engine	<b>A.5</b>	Interfacekonfiguration
<b>1.10.1</b>	Die Network Map	<b>3.6</b>	Paketverarbeitung im FTD	<b>A.6</b>	Zeitsynchronisation
<b>1.11</b>	Logging und Debugging	<b>3.7</b>	Performance	<b>A.7</b>	Health und Discovery Policy
<b>1.11.1</b>	Logging der FTD-Geräte	<b>3.7.1</b>	Performance: LINA Engine	<b>A.8</b>	Logging auf dem Management Center
<b>1.11.2</b>	Debugging	<b>3.7.2</b>	Snort Engine: FMC	<b>A.9</b>	Logging auf dem FTD-Gerät
<b>1.12</b>	SNMP	<b>3.7.3</b>	Snort Engine: CLI	<b>A.10</b>	Statisches Routing
<b>1.12.1</b>	SNMP im FTD (außer 4100, 9300)	<b>3.7.4</b>	Elephant Flows	<b>A.11</b>	NAT
<b>2</b>	<b>Routing mit FTD</b>	<b>3.7.5</b>	FMC Performance	<b>A.12</b>	Access Control Policy
<b>2.1</b>	Die Routing-Tabelle	<b>3.7.6</b>	Access Control Policy	<b>A.13</b>	Active/Standby Failover
<b>2.1.1</b>	Routing und Management-Interfaces	<b>3.8</b>	Die Connection Table	<b>A.14</b>	SSL-Proxy (optional)
<b>2.2</b>	Virtual Routers (VRF-Lite)	<b>3.8.1</b>	Timeouts	<b>A.15</b>	Lösungsvorschläge
<b>2.3</b>	Statische Routen	<b>3.9</b>	Service Policy Rules	<b>A.15.1</b>	Benutzer anlegen
<b>2.4</b>	OSPF	<b>4</b>	<b>Weitere Funktionen</b>	<b>A.15.2</b>	Einbinden in das FMC
<b>2.4.1</b>	OSPF: Konfiguration	<b>4.1</b>	FlexConfig	<b>A.15.3</b>	Kontrolle der Grundkonfiguration
<b>2.4.2</b>	Interface-Eigenschaften	<b>4.1.1</b>	FlexConfig Objekte	<b>A.15.4</b>	Interfacekonfiguration
<b>2.4.3</b>	OSPF: Kontrolle	<b>4.1.2</b>	FlexConfig Policy: Protocol Inspection	<b>A.15.5</b>	Zeitsynchronisation
<b>2.5</b>	OSPFv3	<b>4.1.3</b>	FlexConfig: Netflow	<b>A.15.6</b>	Health- und Discovery Policies
<b>2.6</b>	BGP	<b>4.2</b>	Domain Management	<b>A.15.7</b>	Logging auf dem FMC
<b>2.6.1</b>	BGP: Kontrolle	<b>4.2.1</b>	Domain-Verwaltung	<b>A.15.8</b>	Logging auf dem FTD-Gerät
<b>2.7</b>	Routing-Entscheidungen	<b>4.3</b>	Quality of Service	<b>A.15.9</b>	Statisches Routing
<b>2.8</b>	Equal-Cost Multi-Path (ECMP)	<b>4.4</b>	Redundanz	<b>A.15.10</b>	NAT
<b>2.9</b>	Policy Based Routing	<b>4.4.1</b>	Active/Standby Failover	<b>A.15.11</b>	Access Control Policy
<b>2.9.1</b>	PBR: Konfiguration	<b>4.4.2</b>	Etherchannel	<b>A.15.12</b>	URL-/Application Filter
<b>3</b>	<b>FTD als Firewall</b>	<b>4.4.3</b>	Redundant Interfaces	<b>A.15.13</b>	Service Policy
<b>3.1</b>	NAT	<b>4.4.4</b>	Cluster		
<b>3.1.1</b>	Auto NAT vs. Manual NAT	<b>4.4.5</b>	Redundanz des FMC		
		<b>4.5</b>	FTD als SSL-Proxy		

