

Konfigurieren von DHCP-Server/Relay auf FTD mit FirePOWER Management Center (FMC)

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [DHCP-Server konfigurieren](#)
- [DHCP-Server aktivieren/DHCP-Pool konfigurieren](#)
- [Konfigurieren des DNS-/WINS-Servers](#)
- [Konfigurieren der erweiterten Parameter](#)
- [DHCP-Relay konfigurieren](#)
- [Konfigurieren des DHCP-Relay-Agenten](#)
- [Externen DHCP-Server konfigurieren](#)
- [Überwachung und Fehlerbehebung](#)
- [Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration des DHCP-Servers und der DHCP-Relay-Services in Firepower Threat Defense (FTD) über FMC beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der FirePOWER-Technologie
- Grundlegende Kenntnisse über Adaptive Security Appliances (ASA)
- Kenntnis des Dynamic Host Control Protocol (DHCP)-Servers/DHCP-Relays

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA Firepower Threat Defense-Image für ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Software-Version 6.0.1 und höher.
- ASA Firepower Threat Defense-Image für ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) mit Software-Version 6.0.1 und höher.
- FMC Version 6.0.1 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hinweis: FTD-Einheit kann beim FMC registriert werden. Klicken Sie auf [Gerät bei einem FireSIGHT Management Center registrieren](#), um das FTD beim FMC zu registrieren.

Hintergrundinformationen

DHCP stellt den DHCP-Clients automatisch Netzwerkkonfigurationsparameter wie IP-Adressen, DNS-Serverdetails und andere Parameter zur Verfügung. Die FTD-Router-Schnittstelle kann als DHCP-Server fungieren, um die IP-Adressen für die Clients bereitzustellen.

FTD stellt die DHCP-Relay-Dienste für den internen Client bereit, wobei Clients mit einer der Schnittstellen des FTD verbunden sind und der externe DHCP-Server mit dem anderen verbunden ist. Der Relay-Service-Betrieb ist für die Clients transparent.

DHCP-Server konfigurieren

Um den DHCP-Server zu konfigurieren, melden Sie sich bei der FMC-GUI an, und navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung)**. Klicken Sie auf die Schaltfläche **Bearbeiten** der FTD-Einheit. Navigieren Sie zur Registerkarte **DHCP**, und klicken Sie auf die Registerkarte **DHCP Server**.

Devices Routing NAT Interfaces Inline Sets **DHCP**

► **DHCP Server**
 DHCP Relay
 DDNS

Ping Timeout: 50 (10 - 10000 ms)
 Lease Length: 3600 (300 - 10,48,575 sec)
 Auto-Configuration:
 Interface*: Inside-2

Override Auto Configured Settings:

Domain Name:
 Primary DNS Server: + Primary WINS Server: +
 Secondary DNS Server: + Secondary WINS Server: +

Server Advanced

Interface	Address Pool	Enable D
Inside	192.168.10.3-192.168.10.7	✓

Führen Sie drei Schritte aus, um den DHCP-Server zu konfigurieren.

Schritt 1: DHCP-Server aktivieren/DHCP-Pool konfigurieren

Schritt 2: Konfigurieren der erweiterten Parameter

Schritt 3: Konfigurieren des DNS-/WINS-Servers

Hinweis: Stellen Sie sicher, dass die IP-Adresse und der logische Name auf den Schnittstellen konfiguriert werden müssen, bevor Sie die DHCP-Konfiguration starten.

Device Management NAT VPN Platform Settings

NGFW
 Cisco Firepower Threat Defense for VMWare

Devices Routing NAT **Interfaces** Inline Sets DHCP

Interface	Logical Name	Type	Security Zone	Mac Address(Active/Standby)
GigabitEthernet0/0	Outside	Physical	Outside	
GigabitEthernet0/1	Inside	Physical	Inside	
GigabitEthernet0/2	Inside-2	Physical	Inside-2	
Diagnostic0/0	diagnostic	Physical		
GigabitEthernet0/3	MGMT	Physical	MGMT	
GigabitEthernet0/4		Physical		

DHCP-Server aktivieren/DHCP-Pool konfigurieren

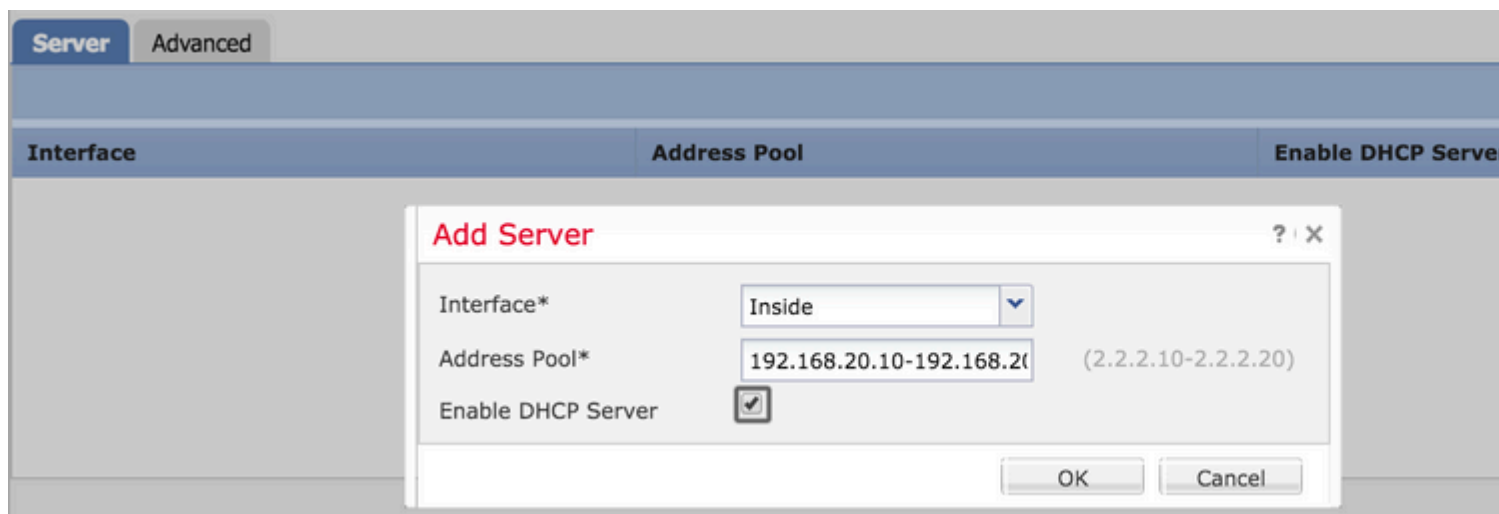
Sie können jede geroutete Schnittstelle als DHCP-Server verwenden, und die IP-Adresse der Schnittstelle fungiert als Gateway für den Endclient. Daher müssen Sie nur den IP-Adressbereich definieren.

Um den DHCP-Server auf einer beliebigen Schnittstelle zu aktivieren, klicken Sie auf der Registerkarte **Server** auf die Schaltfläche **Hinzufügen**.

Interface (Schnittstelle): Geben Sie die Schnittstelle in der Dropdown-Liste an, über die der DHCP-Server aktiviert werden soll.

Address Pool (Adresspool): Geben Sie den IP-Adressbereich an.

Enable DHCP Server (DHCP-Server aktivieren): Aktivieren Sie das Kontrollkästchen, um den DHCP-Server auf dieser Schnittstelle zu aktivieren.



The screenshot shows a configuration window titled "Add Server" with a close button (X) and a help button (?). It contains three main fields: "Interface*" is a dropdown menu currently set to "Inside"; "Address Pool*" is a text input field containing "192.168.20.10-192.168.20.20" with a secondary value "(2.2.2.10-2.2.2.20)" displayed to its right; and "Enable DHCP Server" is a checkbox that is checked. At the bottom right, there are "OK" and "Cancel" buttons.

Klicken Sie auf **OK**, um die DHCP-Konfiguration zu speichern.

Konfigurieren des DNS-/WINS-Servers

Der DHCP-Server stellt dem Endclient die DNS-/WINS-/Domänennamen-Parameter zusammen mit IP-Adressdetails zur Verfügung. Diese Parameter helfen bei der Namensauflösung. Daher ist es wichtig, diese Parameter korrekt zu konfigurieren.

Es gibt zwei Möglichkeiten, dies zu konfigurieren:

Wenn eine FTD-Schnittstelle als DHCP-Client konfiguriert ist, können Sie zuerst die Option **Automatische Konfiguration** auswählen. Bei dieser Methode werden die DNS-/WINS-/Domänennamen-Informationen vom DHCP-Server konfiguriert und dem DHCP-Client die gleichen Informationen bereitgestellt.

Anschließend können Sie eigene DNS-/WINS-Domänennamenparameter festlegen, die dem Endclient zur Verfügung gestellt werden.

Um dies zu konfigurieren, navigieren Sie zur Registerkarte **DHCP**.

- Ping Timeout (Ping-Zeitüberschreitung): Um Adresskonflikte zu vermeiden, sendet das FTD zwei ICMP-Ping-Pakete an eine Adresse, bevor es diese einem DHCP-Client zuweist. Dieser Befehl gibt den Timeout-Wert für diese Pakete an.
- Leasing-Dauer: Dieser Leasing-Zeitraum entspricht der Zeit (in Sekunden), die der Client die ihm

- zugewiesene IP-Adresse verwenden kann, bevor der Lease abläuft
- Automatische Konfiguration: Aktivieren Sie dieses Kontrollkästchen, um die automatische Konfiguration für DNS/WINS/Domänenname zu konfigurieren.
- Schnittstelle: Geben Sie die Schnittstelle an, die als DHCP-Client fungiert.

Override Auto Configured Setting (Automatische konfigurierte Einstellung überschreiben): Konfigurieren Sie diese Option, wenn Sie dem Endclient einen eigenen DNS-/WINS-/Domännennamen zuweisen möchten.

Domain Name (Domänenname): Geben Sie den Domännennamen an.

Primary DNS Server (Primärer DNS-Server): Geben Sie den primären DNS-Server an. Sie können das Netzwerkobjekt entweder aus der Dropdown-Liste auswählen oder auf das Pluszeichen (+) klicken und ein Netzwerkobjekt für den primären DNS-Server erstellen.

Sekundärer DNS-Server: Geben Sie den sekundären DNS-Server an. Sie können das Netzwerkobjekt entweder aus der Dropdown-Liste auswählen oder auf das Pluszeichen (+) klicken und ein Netzwerkobjekt für den sekundären DNS-Server erstellen.

Primary WINS Server (Primärer WINS-Server): Geben Sie den sekundären DNS-Server an. Sie können das Netzwerkobjekt entweder aus der Dropdown-Liste auswählen oder auf das Pluszeichen (+) klicken und ein Netzwerkobjekt für den sekundären DNS-Server erstellen.

Sekundärer WINS-Server: Geben Sie den sekundären DNS-Server an. Sie können das Netzwerkobjekt entweder aus der Dropdown-Liste auswählen oder auf das Pluszeichen (+) klicken und ein Netzwerkobjekt für den sekundären DNS-Server erstellen.

Ping Timeout	<input type="text" value="50"/>	(10 - 10000 ms)
Lease Length	<input type="text" value="3600"/>	(300 - 10,48,575 sec)
Auto-Configuration	<input checked="" type="checkbox"/>	
Interface*	<input type="text" value="Outside"/>	
Override Auto Configured Settings:		
Domain Name	<input type="text" value="example.com"/>	
Primary DNS Server	<input type="text" value="DNS1"/>	<input type="text" value="SER"/>
Secondary DNS Server	<input type="text"/>	<input type="text" value="SER"/>

Konfigurieren der erweiterten Parameter

Der DHCP-Server der FTD-Schnittstelle kann DHCP-Codes und -Optionen enthalten. Beispielsweise können Cisco IP-Telefone eine Anforderung mit der Option (150/66) an den DHCP-Server senden, um die IP-Adresse des TFTP-Servers abzurufen, damit die Telefone die Firmware vom TFTP-Server herunterladen können.

Um dies zu konfigurieren, navigieren Sie zu **DHCP> Erweiterte** Option, und klicken Sie auf **Hinzufügen**.

- Optionscode: Geben Sie den Optionscode gemäß der Auflistung in RFC 2132, RFC 2562, RFC 5510 an.
- Typ: Geben Sie den Typ aus dem Dropdown-Menü an.
- IP Address 1 (IP-Adresse 1): Wenn Sie als Typ option IP (IP) auswählen, geben Sie die IP-Adresse des ersten TFTP-Servers an.
- IP Address 2 (IP-Adresse 2): Wenn Sie als Typ option IP (IP) auswählen, geben Sie die IP-Adresse des ersten TFTP-Servers an.
- ASCII: Wenn Sie die Typoption als ASCII auswählen, geben Sie den ASCII-Wert an.
- HEX: Wenn Sie die Typoption als HEX auswählen, geben Sie den HEX-Wert an.

Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Klicken Sie auf **Speichern**, um die Plattformeinstellung zu speichern. Navigieren Sie zur Option **Deploy (Bereitstellen)**, wählen Sie die FTD-Appliance aus, in der Sie die Änderungen übernehmen möchten, und klicken Sie auf die Schaltfläche **Deploy (Bereitstellen)**, um die Bereitstellung der Plattformeinstellung zu starten.

Klicken Sie auf **Speichern**, um die Plattformeinstellung zu speichern. Navigieren Sie zur Option **Deploy (Bereitstellen)**, wählen Sie die FTD-Appliance aus, in der Sie die Änderungen übernehmen möchten, und klicken Sie auf die Schaltfläche **Deploy (Bereitstellen)**, um die Bereitstellung der Plattformeinstellung zu starten.

DHCP-Relay konfigurieren

FTD-Schnittstelle fungiert als DHCP Relay Agent zwischen Client und externem DHCP-Server. Die Schnittstelle wartet auf die Client-Anforderung und fügt wichtige Konfigurationsdaten hinzu, z. B. die Verbindungsinformationen des Clients, die vom DHCP-Server benötigt werden, um die Adresse für den Client zuzuweisen. Wenn der DHCP-Server antwortet, leitet die Schnittstelle das Antwortpaket zurück an den DHCP-Client weiter.

Die Konfiguration des DHCP-Relay umfasst im Wesentlichen zwei Konfigurationsschritte.

Schritt 1: Konfigurieren Sie den DHCP-Relay-Agent.

Schritt 2: Konfigurieren des externen DHCP-Servers

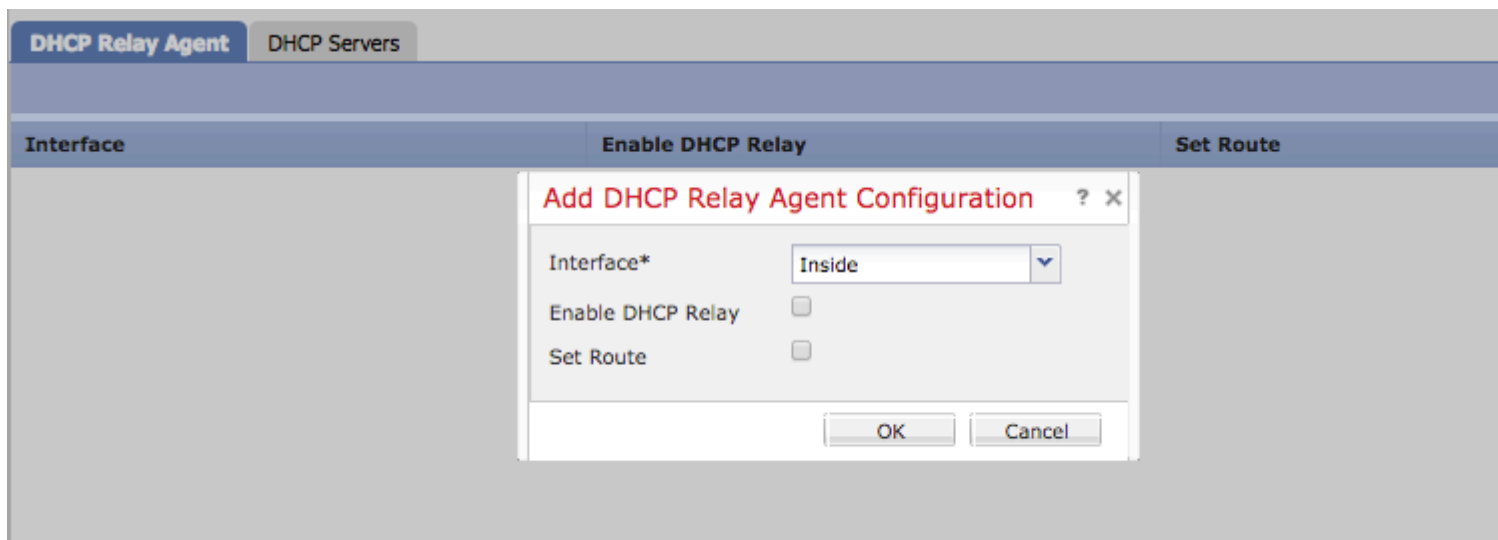
Konfigurieren des DHCP-Relay-Agenten

Navigieren Sie zu **Geräte > Geräteverwaltung**. Klicken Sie auf die Schaltfläche **Bearbeiten der FTD-Einheit**. Navigieren Sie zu **DHCP > DHCP Relay option**. Klicken Sie auf **Hinzufügen**.

Interface (Schnittstelle): Geben Sie in der Dropdown-Liste die Schnittstelle an, die die Client-Anforderung abhört. Der DHCP-Client kann sich für die IP-Adressanforderung direkt mit dieser Schnittstelle verbinden.

Enable DHCP Relay (DHCP-Relay aktivieren): Aktivieren Sie das Kontrollkästchen, um den DHCP-Relay-Service zu aktivieren.

Set Route (Route festlegen): Aktivieren Sie das Kontrollkästchen, um die IP-Adresse der Schnittstelle als Standard-Gateway festzulegen.



Klicken Sie auf die Schaltfläche **OK**, um die Konfiguration des DHCP-Relay-Agenten zu speichern.

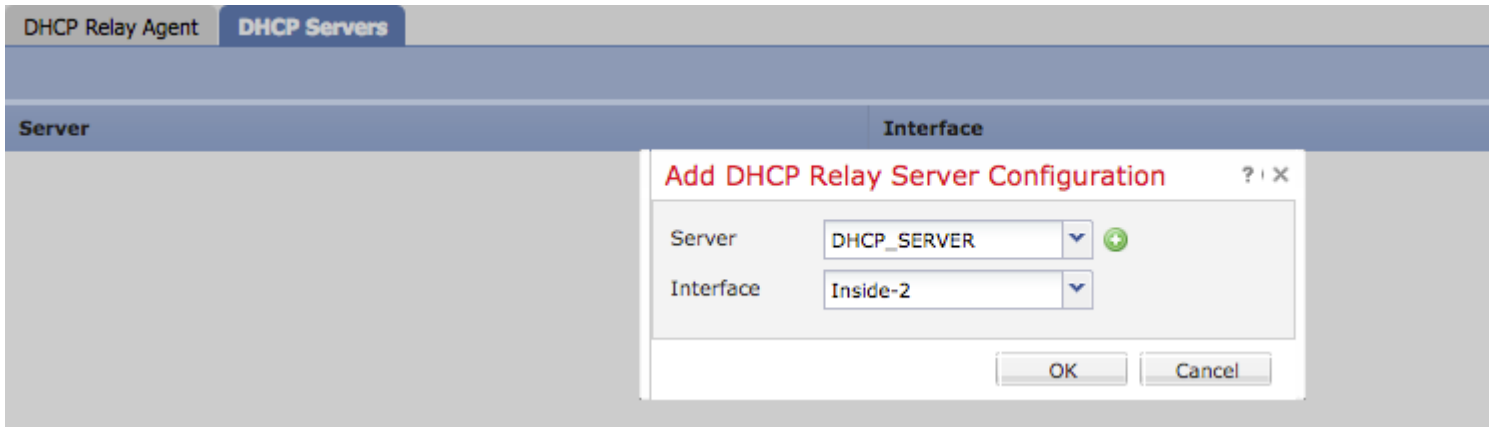
Externen DHCP-Server konfigurieren

Sie müssen die IP-Adresse des externen DHCP-Servers angeben, an den die Client-Anforderung weitergeleitet wird.

Navigieren Sie zum Festlegen des DHCP-Servers zu **DHCP Server**, und klicken Sie auf **Add (Hinzufügen)**.

Server (Server): Geben Sie die IP-Adresse des DHCP-Servers an. Sie können das Netzwerkobjekt entweder aus der Dropdown-Liste auswählen oder auf das Pluszeichen (+) klicken und ein Netzwerkobjekt für den DHCP-Server erstellen.

Schnittstelle: Geben Sie die Schnittstelle an, über die der DHCP-Server eine Verbindung herstellt.



Klicken Sie auf OK, um die Konfiguration zu speichern.

Klicken Sie auf Speichern, um die Plattformeinstellung zu speichern. Navigieren Sie zur Option Deploy (Bereitstellen), wählen Sie die FTD-Appliance aus, in der Sie die Änderungen übernehmen möchten, und klicken Sie auf die Schaltfläche Deploy (Bereitstellen), um die Bereitstellung der Plattformeinstellung zu starten.

Überwachung und Fehlerbehebung

- Stellen Sie sicher, dass das FTD beim FMC registriert ist, bevor Sie mit der Konfiguration des DHCP-Servers/Relays beginnen.
- Überprüfen der Verbindung zum DHCP-Server in der DHCP-Relay-Konfiguration

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# ping <DHCP_SERVER_IP>
```

- Überprüfen der DHCP-bezogenen Konfiguration in der FTD-CLI Sie können sich bei der FTD-CLI bei der Verwaltungsschnittstelle anmelden und den Befehl

```
firepower# show running-config dhcpd.
dhcpd auto_config Inside-2
!
dhcpd address 192.168.10.3-192.168.10.7 Inside
!
```

- Stellen Sie sicher, dass die Richtlinienbereitstellung erfolgreich angewendet wird.
- Stellen Sie sicher, dass Sie den richtigen DNS-/WINS-Servereintrag entweder über die automatische Konfiguration oder die manuelle Konfiguration konfigurieren.
- Der IP-Adresspool kann sich im gleichen Subnetz wie die IP-Adresse der Schnittstelle befinden.

- Stellen Sie sicher, dass die IP-Adresse und der logische Name für die Schnittstellen konfiguriert werden können.
- Sie können die Paketerfassung über die FTD-geroutete Schnittstelle durchführen, um das Problem zu beheben, bei dem der Client keine IP-Adresse erhält. In den Paketerfassungen können Sie den DORA-Prozess des DHCP-Servers überprüfen. Sie können [ASA Packet Captures mit CLI und ASDM Configuration Example](#) verwenden, um die Paketerfassung durchzuführen.
- Überprüfen Sie die DHCP-Statistiken in der Befehlszeile.

```
firepower# show dhcpd statistics
```

- Überprüfen der DHCP-Bindungsinformationen aus der CLI

```
firepower# show dhcpd binding
```

- Aktivieren Sie die entsprechende Protokollierung unter Devices (Geräte) > Platform Settings (Plattformeinstellungen) > FTD Policy (FTD-Richtlinie) > System logging, und stellen Sie die Plattformeinstellungen für das FTD bereit. Melden Sie sich bei FTD CLI an, und führen Sie den Befehl aus, um die Syslog-Meldungen zu überprüfen.

```
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
firepower# show logging
```

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.