Konfigurieren des Verbindungs-Timeouts für bestimmten Datenverkehr auf ASA mit ASDM

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Verbindungs-Timeouts auf ASA und ASDM für ein bestimmtes Anwendungsprotokoll wie HTTP, HTTPS, FTP oder andere Protokolle beschrieben. Der Timeout für Verbindungen ist der Zeitraum, nach dem eine Firewall oder ein Netzwerkgerät eine inaktive Verbindung beendet, um Ressourcen freizugeben und die Sicherheit zu erhöhen. Die erste Frage lautet: Was ist die Voraussetzung für diese Konfiguration? Wenn Anwendungen über korrekte TCP-Keepalive-Einstellungen verfügen, ist das Konfigurieren des Verbindungs-Timeouts auf einer Firewall häufig nicht erforderlich. Wenn Anwendungen jedoch nicht über die richtigen Keepalive-Einstellungen oder Timeout-Konfigurationen verfügen, ist in diesem Fall die Konfiguration des Verbindungs-Timeouts auf einer Firewall von entscheidender Bedeutung für das Management von Ressourcen, die Verbesserung der Sicherheit, die Verbesserung der Netzwerkleistung, die Gewährleistung der Compliance und die Optimierung der Benutzerumgebung.

Anforderungen

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

- Zugriffskontrollliste (ACL)

- Service-Richtlinie
- Verbindungs-Timeout

Verwendete Komponenten

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

- ASA 9.17(1)
- ASDM 7.17(1)

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.

Standardwerte

Hinweis: Standard-Timeout

Das Standard-Embryonalzeitlimit beträgt 30 Sekunden.

Der Timeout für halb geschlossene Inaktivität beträgt standardmäßig 10 Minuten.

Der standardmäßige Wert für dcd max_retries ist 5.

Der Standardwert dcd retry_interval beträgt 15 Sekunden.

Das tcp-Leerlaufzeitlimit beträgt standardmäßig 1 Stunde.

Das udp idle-Timeout ist standardmäßig 2 Minuten.

Der icmp-Timeout für Leerlauf ist standardmäßig 2 Sekunden.

Das SIP-Leerlaufzeitlimit beträgt standardmäßig 30 Minuten.

Das Timeout für freie Medienzugriffe beträgt standardmäßig 2 Minuten.

Die Standardzeitüberschreitung esp und ha idle beträgt 30 Sekunden.

Bei allen anderen Protokollen beträgt das Timeout bei Inaktivität standardmäßig 2 Minuten.

Geben Sie 0:0:0 ein, um keine Zeitüberschreitung zu vermeiden.

Verbindungstimeout konfigurieren

ASDM

Wenn ein bestimmter Datenverkehr über eine Verbindungstabelle verfügt, hat er eine bestimmte Leerlaufzeitüberschreitung. In diesem Artikel ändern wir beispielsweise die Verbindungszeitüberschreitung für DNS-Datenverkehr.

Im Netzwerkdiagramm dieses Datenverkehrs können Sie unter Berücksichtigung der folgenden Optionen das Connection Timeout (Verbindungstimeout) für bestimmten Datenverkehr konfigurieren:

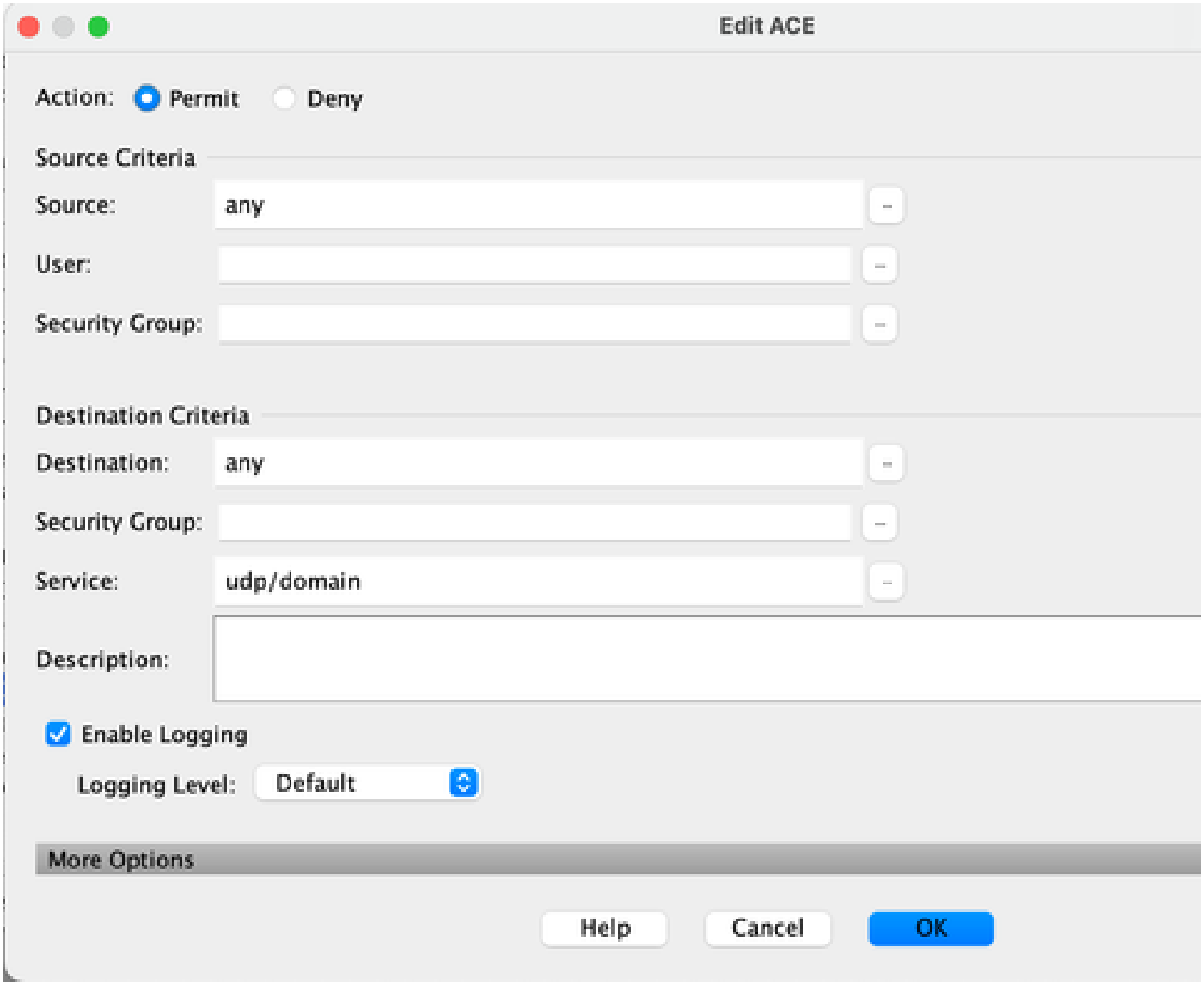
Client ----- [Schnittstelle: MNG] Firewall [Schnittstelle: OUT] ----- Server

Es besteht die Möglichkeit, der Schnittstelle eine ACL zuzuweisen.

Schritt 1: Erstellen einer ACL

Wir können Quelle, Ziel oder Dienst zuweisen.

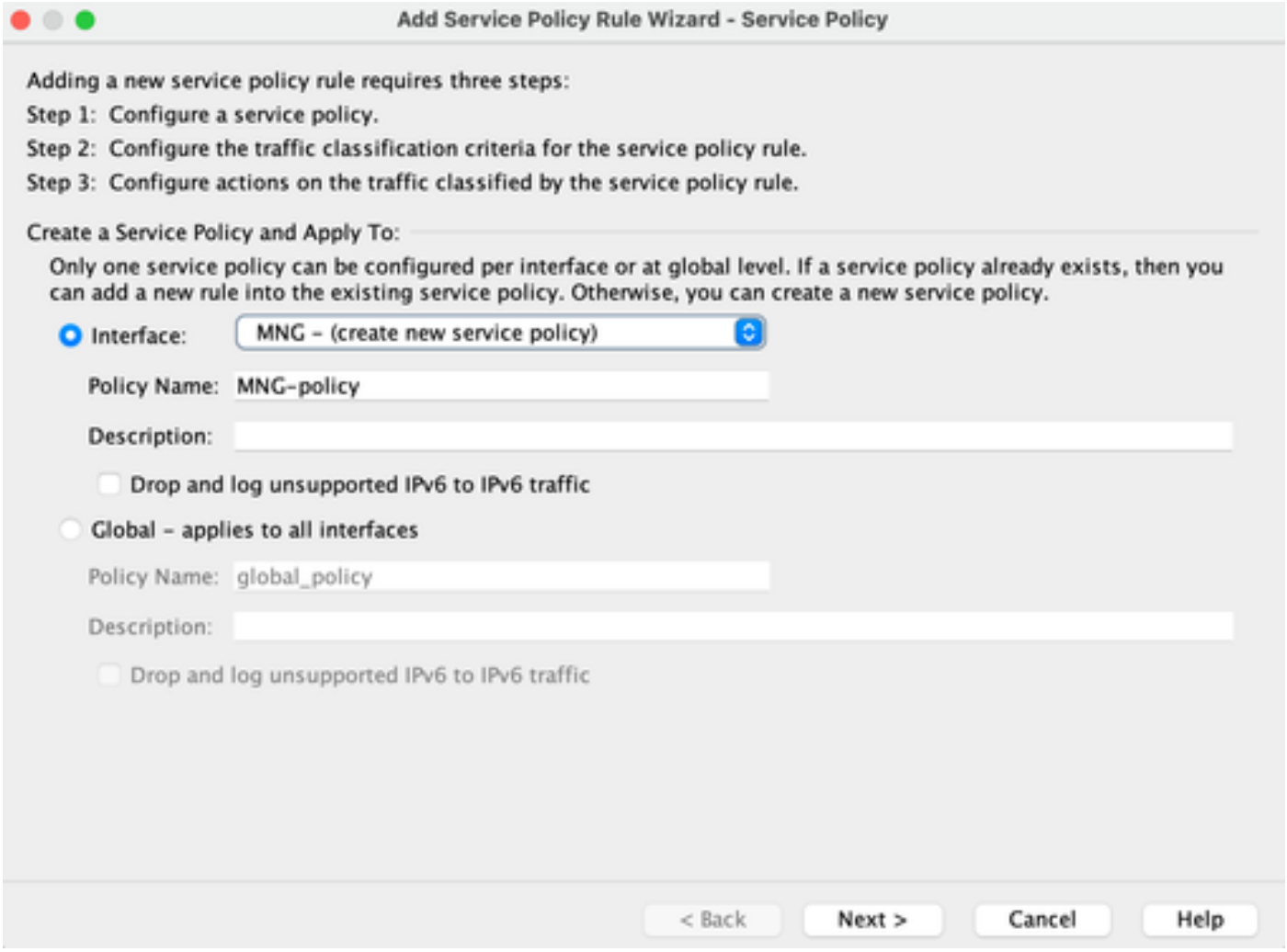
ASDM > Konfiguration > Firewall > Advanced > ACL Manager



Schritt 2: Servicerichtlinien-Regel erstellen

Sie können den letzten Schritt überspringen, wenn Sie Ihre ACL bereits besitzen, oder Sie können einen dieser Parameter (Quelle, Ziel oder Dienst) der Service Policy to the Interface zuweisen.

ASDM > Konfiguration > Firewall > Servicerichtlinien-Regeln

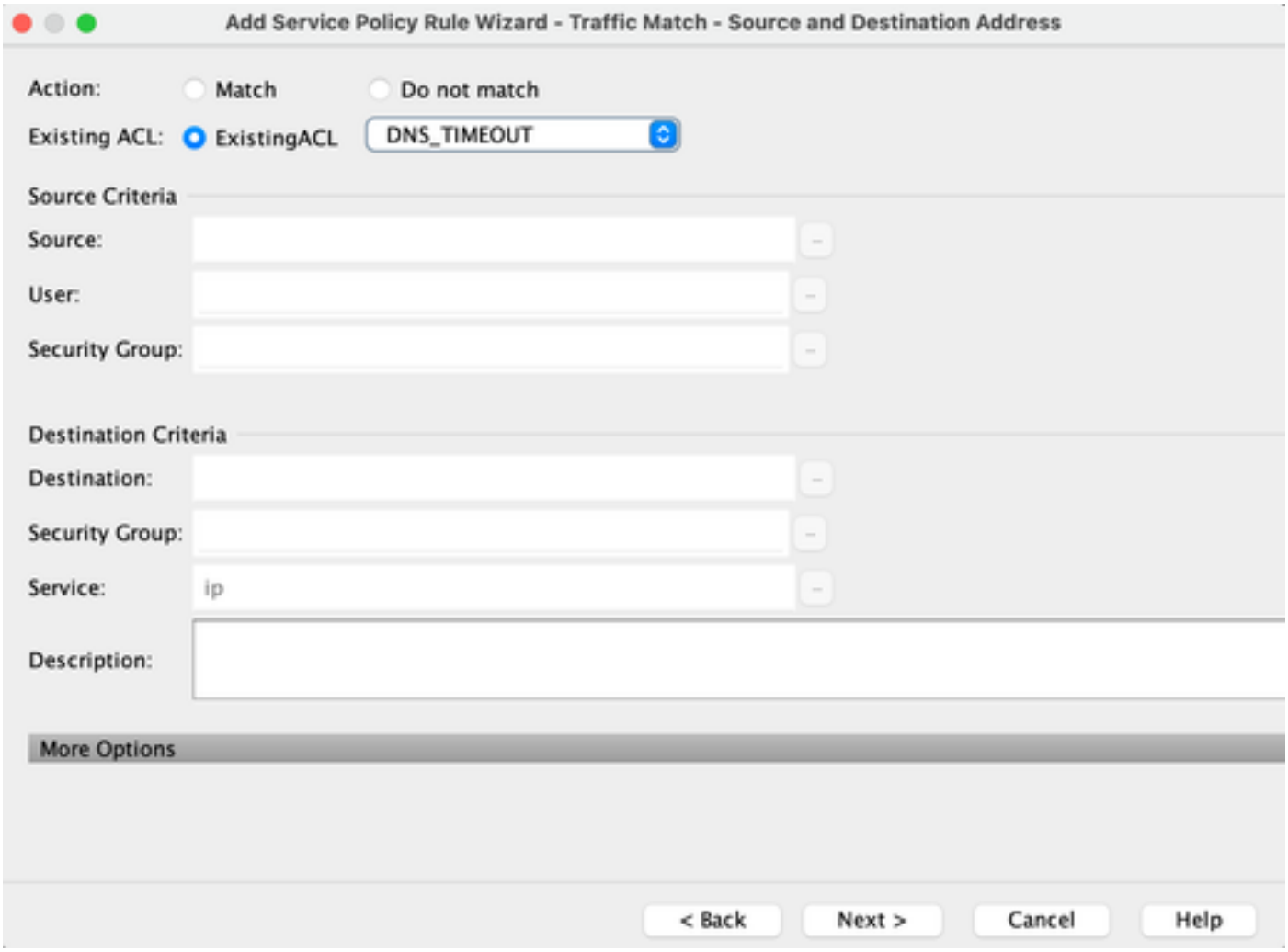


Schritt 3: Verkehrsklasse erstellen

Es besteht die Möglichkeit, die Quell- und Ziel-IP-Adresse auszuwählen (verwendet ACL).

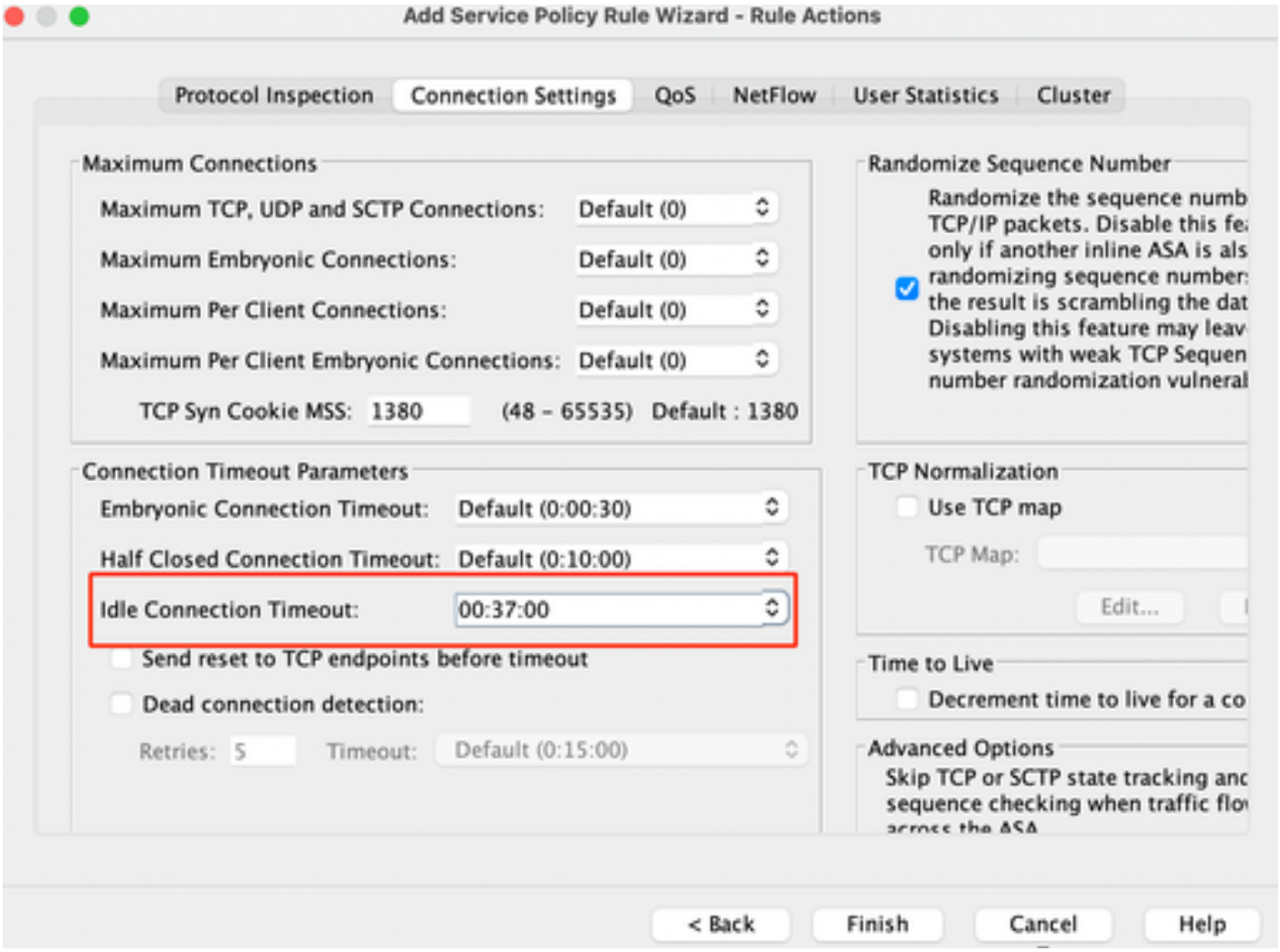
Schritt 4: ACL zuweisen

In diesem Schritt können Sie die vorhandene ACL zuweisen oder Übereinstimmungsbedingungen auswählen (Quelle, Ziel oder Dienst)



Schritt 5: Konfigurieren des Parameters "Idle Timeout"

Auf Basis des gültigen Formats HH:MM:SS die Leerlaufzeitüberschreitung konfigurieren.



klare Verbindungen für den jeweiligen Datenverkehr:

#clear conn addressGeben Sie eine IP-Adresse oder einen IP-Adressbereich ein. #clear conn protocolGeben Sie dieses Schlüsselwort ein, um nur SCP-/TCP-/UDP-Verbindungen zu löschen

ASA-Kommandozeile

Sie können alle diese Einstellungen über die CLI konfigurieren:

ACL: access-list DNS_TIMEOUT extended permit udp any any any eq domain Klassenzuordnung: Class-Map MNG-Klasse Zugriffsliste für Übereinstimmung DNS_TIMEOUT

Richtlinienzuweisung:

policy-map MNG-policy
Klasse MNG
set connection timeout idle 0:37:00

Wenden Sie die Policy-Map auf die Schnittstelle an:

service-policy MNG-policy interface MNG

Überprüfung

Tipp: Wenn wir diesen Befehl ausführen, können wir das Timeout für Verbindungen im DNS-Datenverkehr bestätigen:

ASA CLI > enable mode > show conn long

Beispiel: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle 17s, uptime 17s, timeout 2m0s, bytes 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle 40s, uptime 40s, timeout 2m0s, bytes 36

Nach der Konfiguration können wir die Leerlaufzeitüberschreitungskonfiguration bestätigen:

Beispiel: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle 8s, uptime 8s, timeout 37m0s, bytes 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle 5s, uptime 5s, timeout 37m0s, bytes 41

Referenzen

Was sind die Verbindungseinstellungen?

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.