Konfigurieren des VPN-Client-Lastenausgleichs mit DNS Round Robin auf der ASA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Lastenausgleich des AnyConnect VPN-Clients mit dem DNS-Round-Robin auf der ASA konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Sie haben den ASAs IP-Adressen zugewiesen und das Standard-Gateway konfiguriert.
- AnyConnect VPN wird auf den ASAs konfiguriert.
- VPN-Benutzer können sich über ihre jeweils zugewiesene IP-Adresse mit allen ASAs verbinden.
- Der DNS-Server der VPN-Benutzer ist Round-Robin-fähig.

Verwendete Komponenten

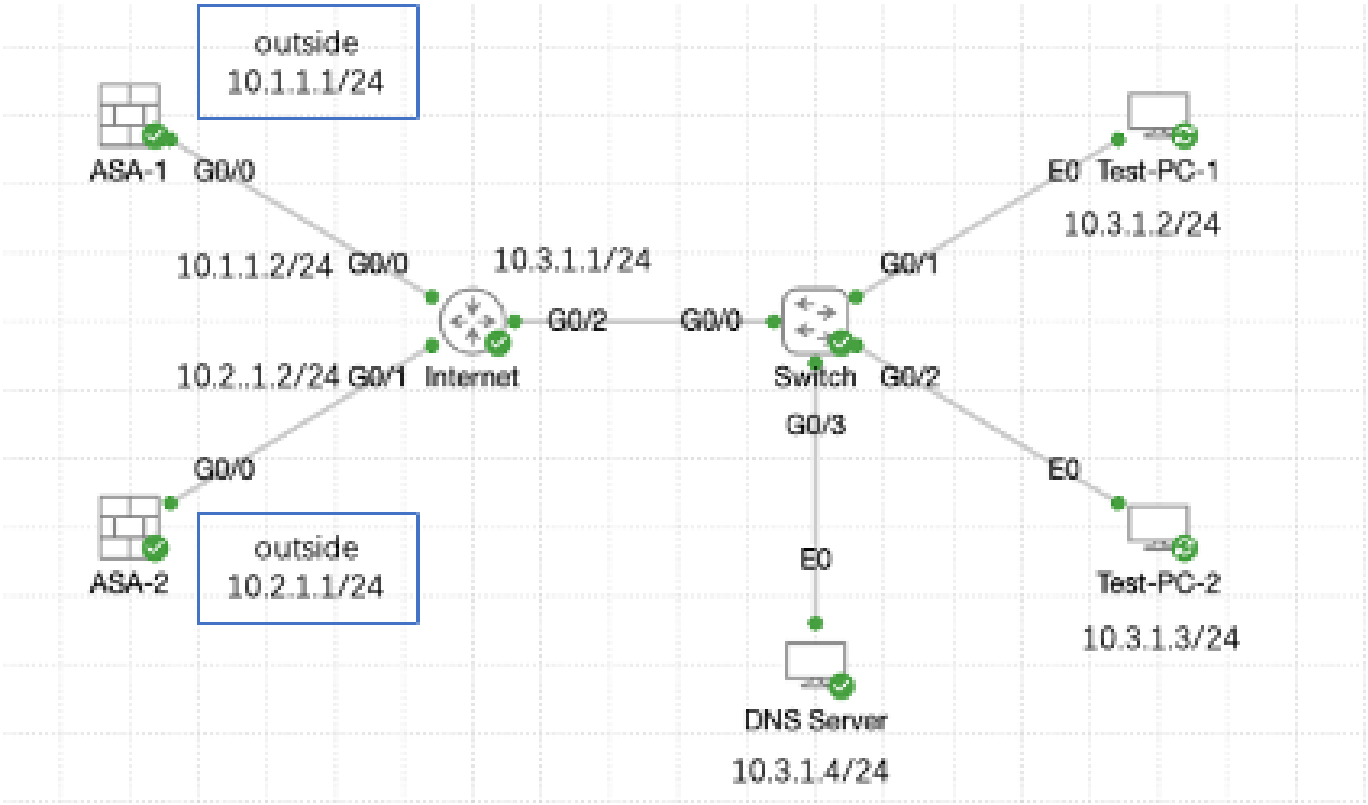
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AnyConnect VPN Client Software-Versionen 4.10.08025
- Cisco ASA Software-Versionen 9.18.2
- Windows Server 2019

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.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurationen

Schritt 1: Konfigurieren von AnyConnect VPN auf ASA

Informationen zur Konfiguration von AnyConnect VPN auf ASA finden Sie in diesem Dokument:

- ASA 8.x : VPN-Zugriff mit dem AnyConnect VPN-Client unter Verwendung eines selbstsignierten Zertifikats - Konfigurationsbeispiel

Nachfolgend finden Sie die Konfiguration der beiden ASAs in diesem Beispiel:

ASA 1:

```
ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0
```

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 10.1.1.2 1

webvpn
 enable outside
 anyconnect enable
 tunnel-group-list enable

group-policy anyconnect internal
group-policy anyconnect attributes
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ssl-client
 default-domain value example.com

username example1 password *****
username example1 attributes
 vpn-group-policy anyconnect
 service-type remote-access

tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
 address-pool anyconnect
 default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
 group-alias example enable
```

ASA 2:

```
ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.2.1.1 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 10.2.1.2 1

webvpn
 enable outside
 anyconnect enable
 tunnel-group-list enable

group-policy anyconnect internal
group-policy anyconnect attributes
```

```
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ssl-client
 default-domain value example.com

username example1 password *****
username example1 attributes
 vpn-group-policy anyconnect
 service-type remote-access

tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
 address-pool anyconnect
 default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
 group-alias example enable
```

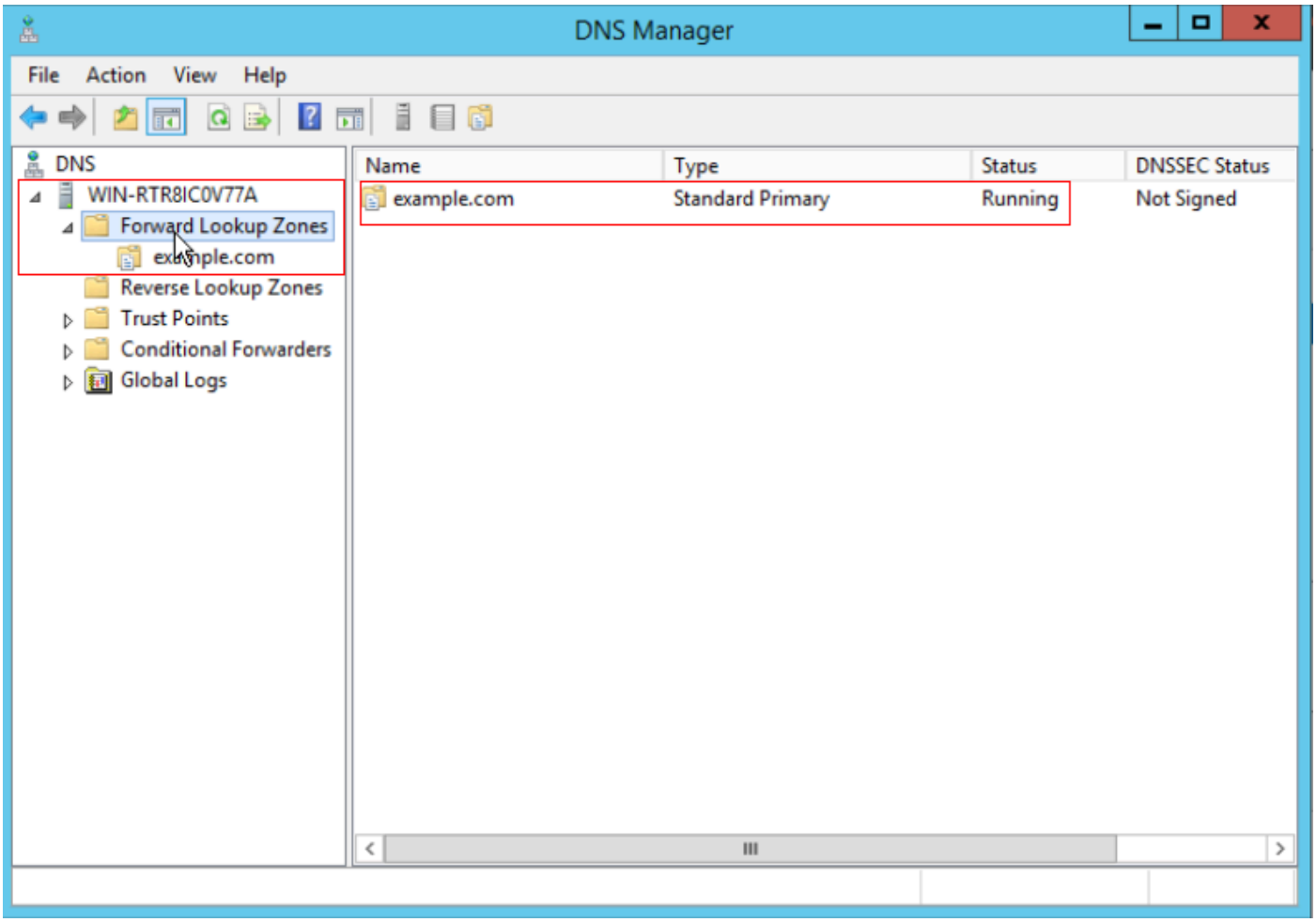
Bevor Sie mit Schritt 2 fortfahren, müssen Sie in der Lage sein, eine Verbindung zu beiden ASAs unter Verwendung der jeweils zugewiesenen IP-Adresse herzustellen.

Schritt 2: Round-Robin-DNS auf DNS-Server konfigurieren

Sie können einen beliebigen Round-Robin-fähigen DNS-Server verwenden. In diesem Beispiel wird der DNS-Server auf dem Windows-Server 2019 verwendet. Informationen zur Installation und Konfiguration von DNS-Servern auf Windows-Servern finden Sie in diesem Dokument:

- Installieren und Konfigurieren des DNS-Servers auf Windows Server

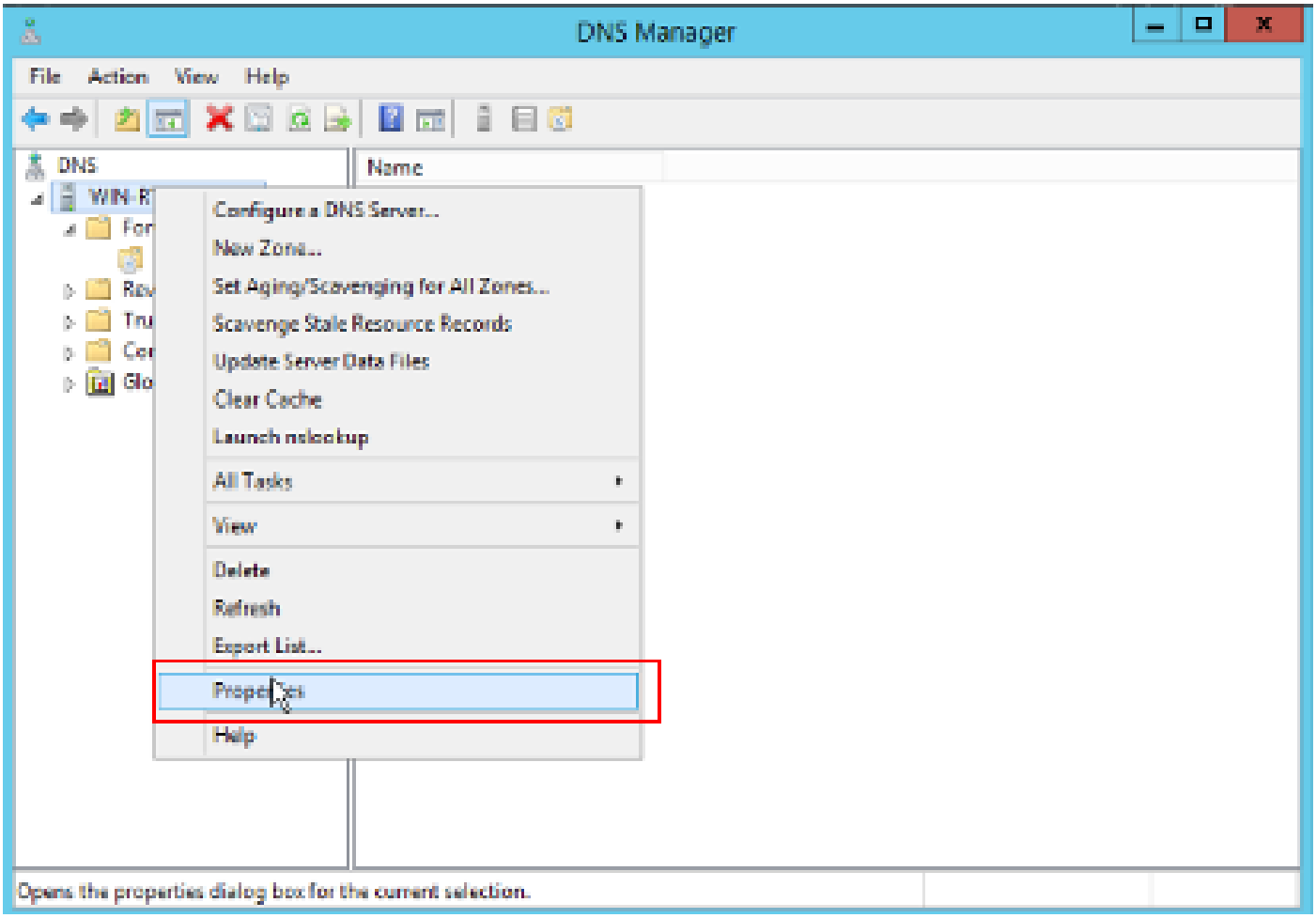
In diesem Beispiel ist 10.3.1.4 der Windows-Server mit aktiviertem DNS-Server für die Domäne example.com.



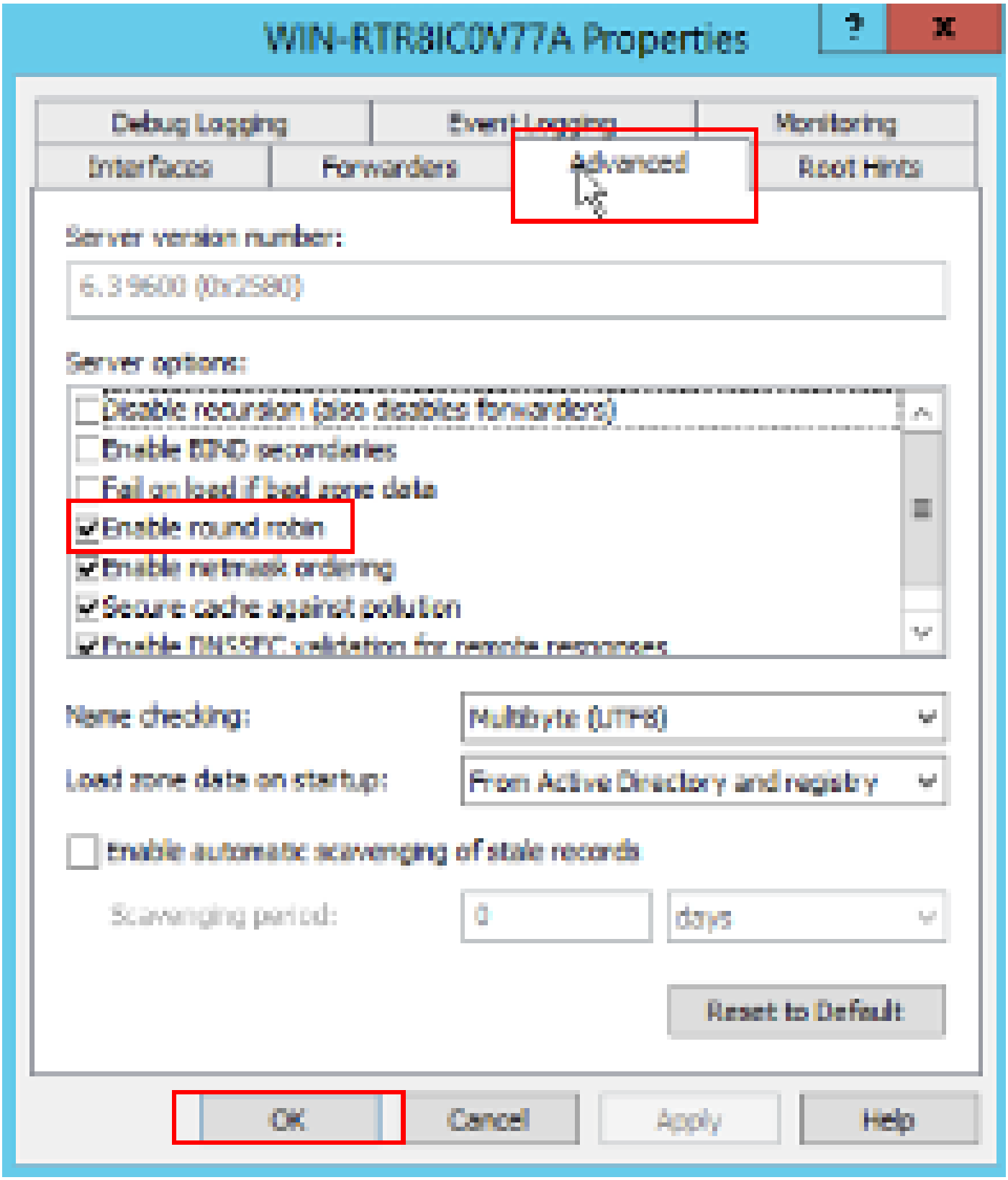
DNS-Server

Stellen Sie sicher, dass Round Robin für Ihren DNS-Server aktiviert ist:

1. Öffnen Sie auf dem Windows-Desktop das Menü Start, und wählen Sie Verwaltung > DNS aus.
2. Wählen Sie in der Konsolenstruktur den DNS-Server aus, den Sie verwalten möchten, klicken Sie mit der rechten Maustaste, und wählen Sie dann Eigenschaften aus.
3. Vergewissern Sie sich unter der Registerkarte Erweitert, dass Rundlauf aktivieren aktiviert ist.



Round Robin 1



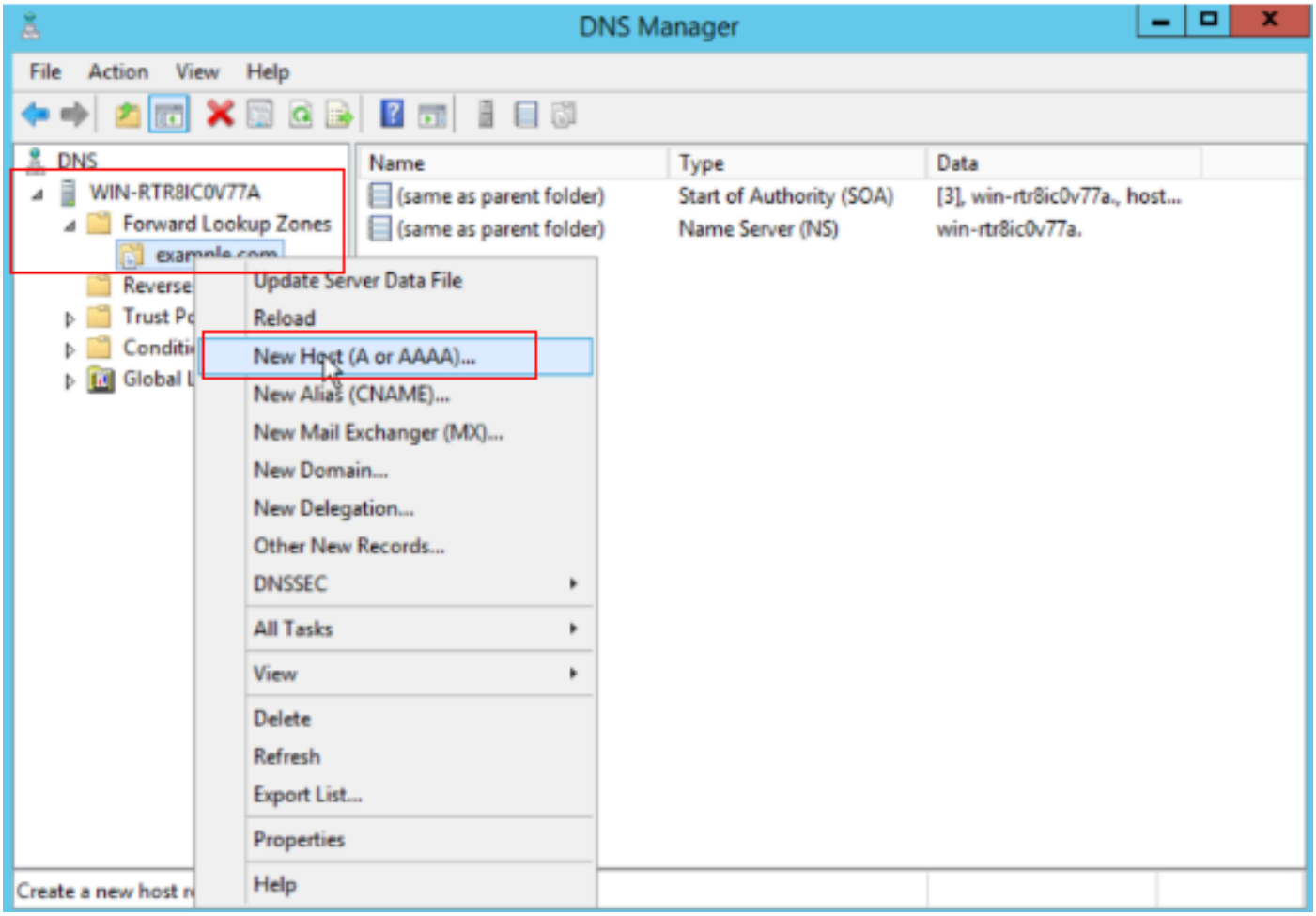
Round Robin 2

Erstellen Sie zwei Host-Datensätze für ASA VPN-Server:

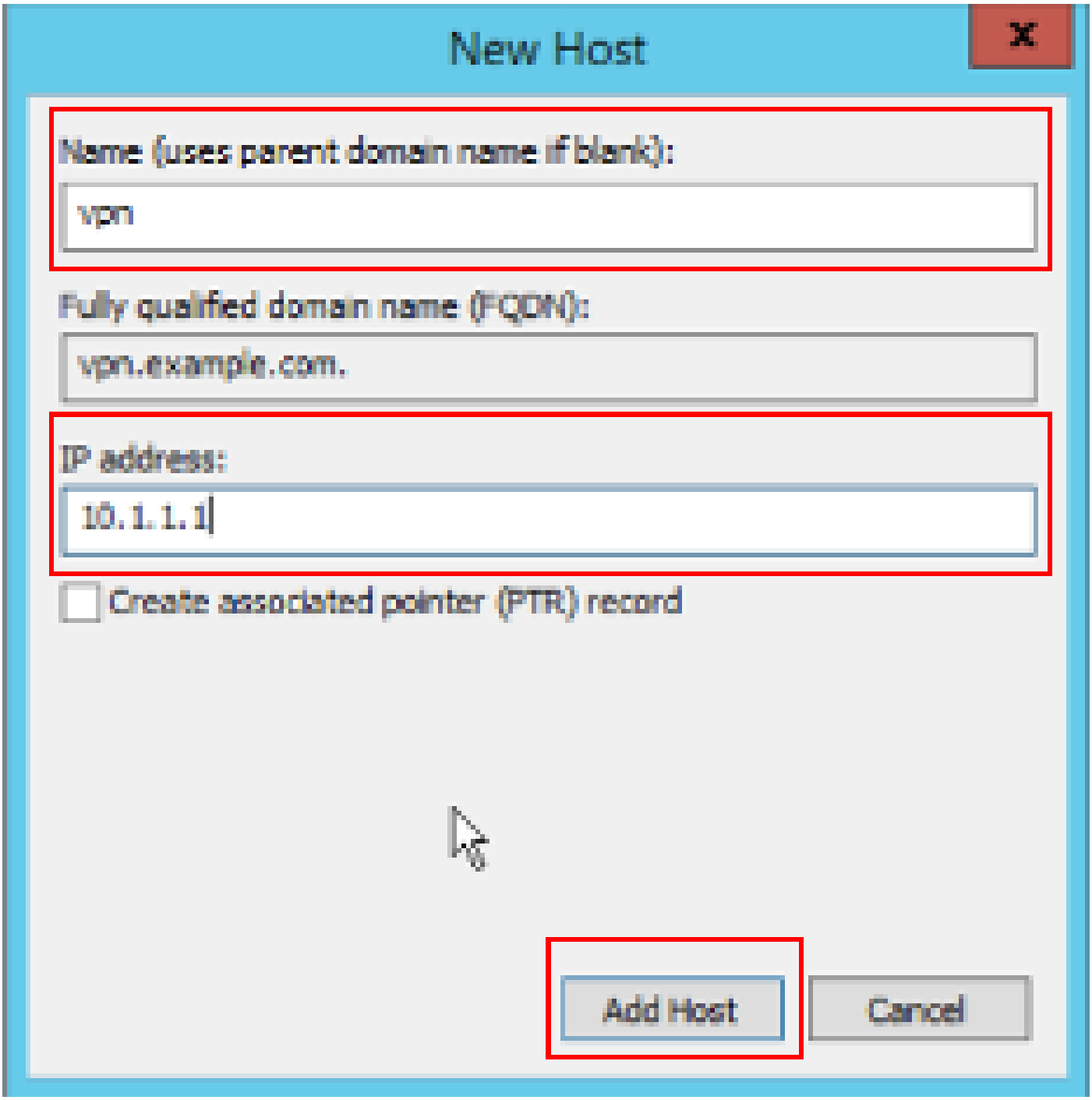
1. Öffnen Sie auf dem Windows-Desktop das Menü Start, und wählen Sie Verwaltung > DNS aus.
2. Stellen Sie in der Konsolenstruktur eine Verbindung mit dem DNS-Server her, den Sie verwalten möchten, erweitern Sie den DNS-Server, erweitern Sie die

Weiterleitungssuchzone, klicken Sie mit der rechten Maustaste, und wählen Sie dann Neuer Host (A oder AAAA).

3. Geben Sie im Bildschirm New Host (Neuer Host) den Namen und die IP-Adresse des Host-Datensatzes an. In diesem Beispiel vpn und 10.1.1.1.
4. Wählen Sie Host hinzufügen, um den Datensatz zu erstellen.

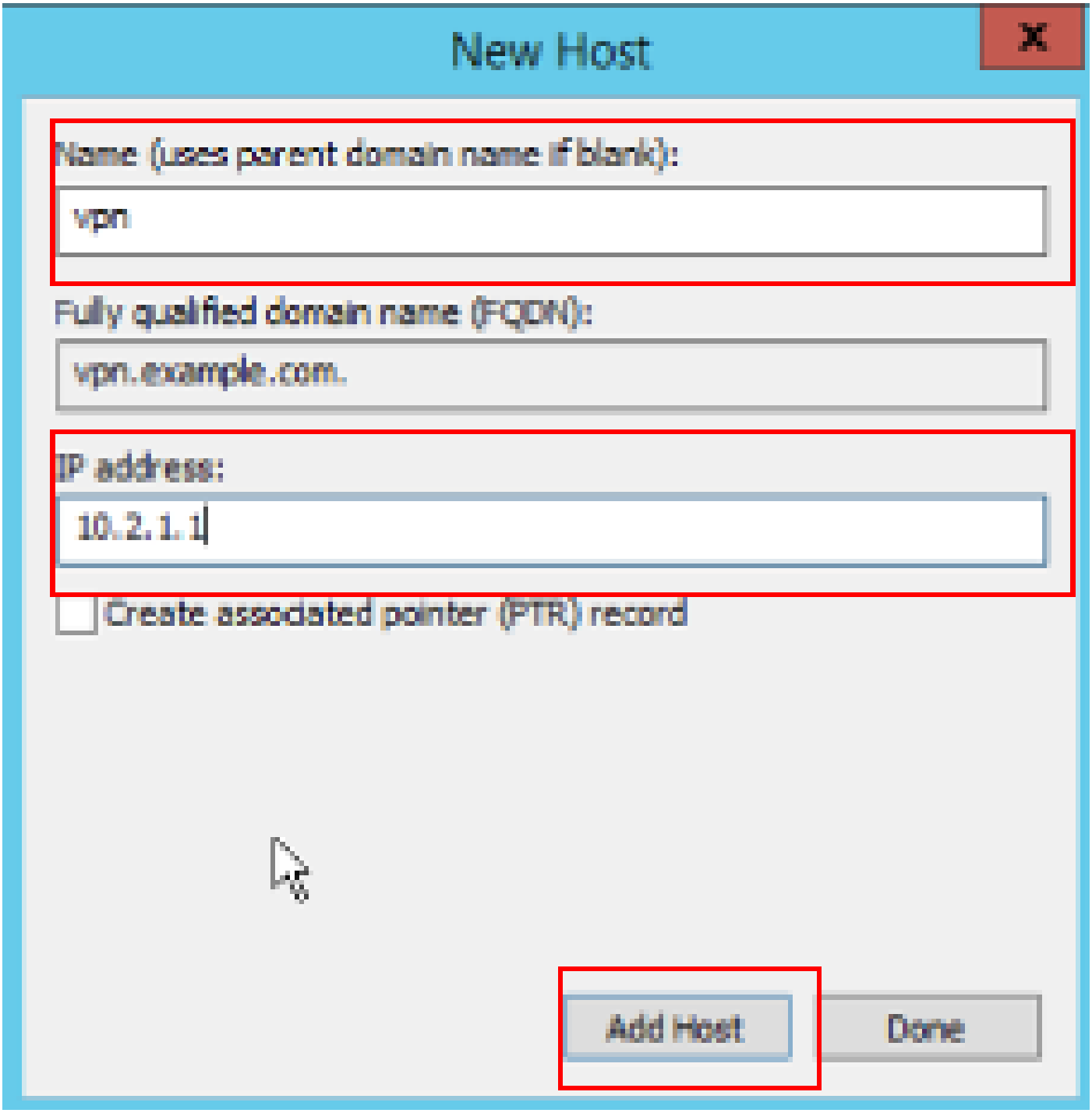


Neuen Host erstellen



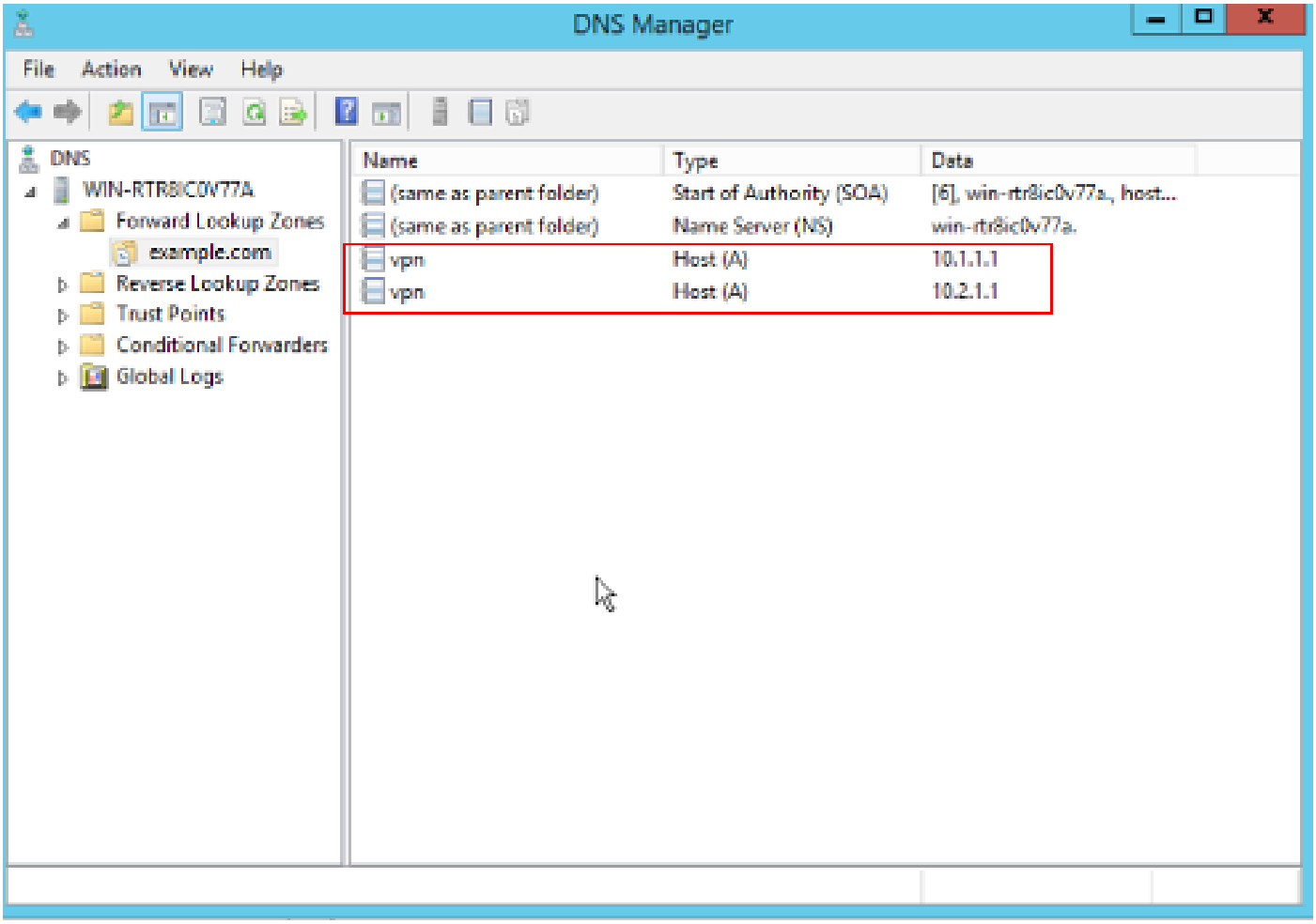
Host-Datensatz 1

Wiederholen Sie ähnliche Schritte, um einen weiteren Hostdatensatz zu erstellen, und stellen Sie sicher, dass Name identisch ist. In diesem Beispiel ist Name vpn, die IP-Adresse ist 10.2.1.1.



Host-Datensatz 2

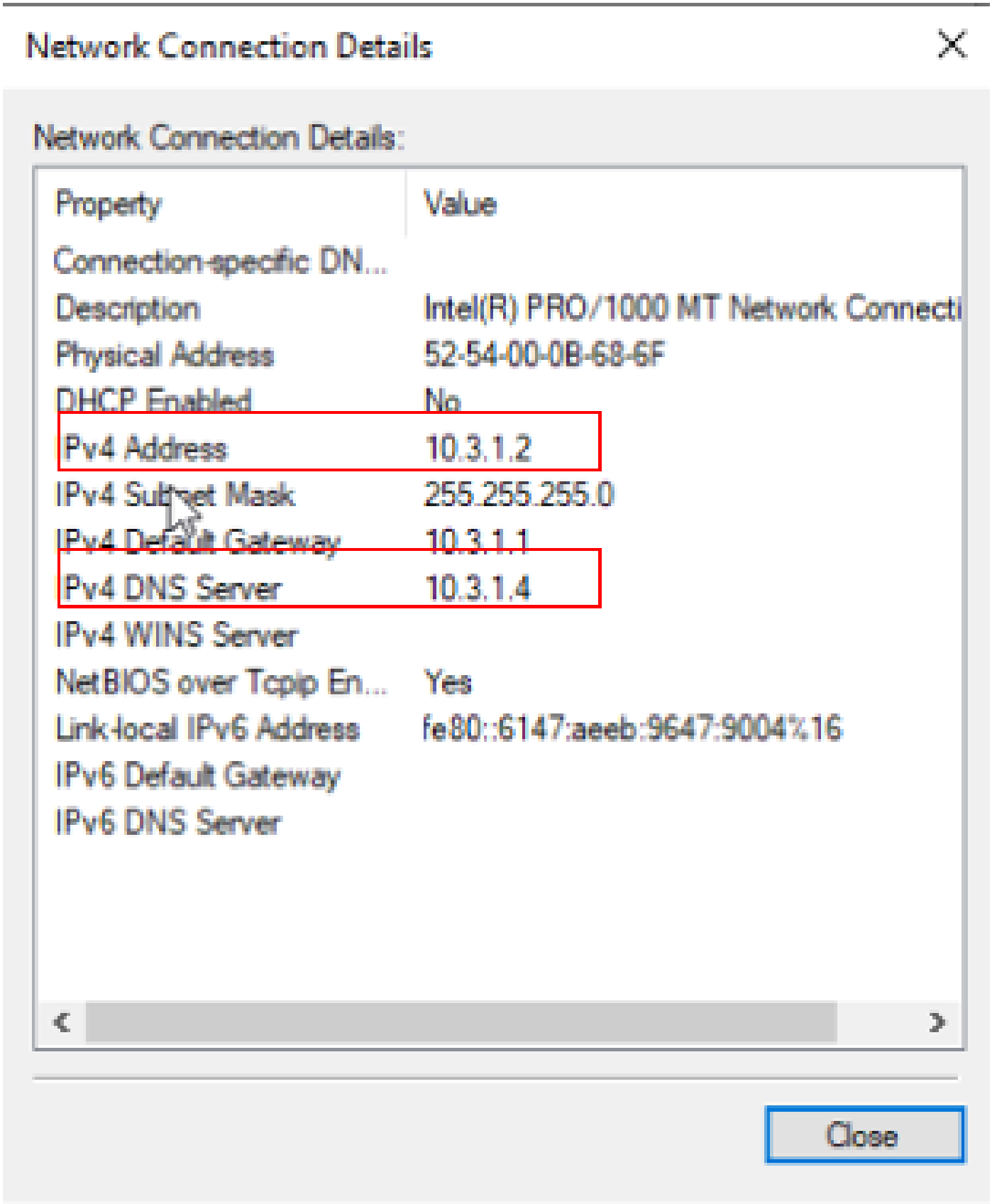
Es gibt zwei Hosts, die 10.1.1.1 und 10.2.1.1 mit demselben Datensatz vpn.example.com verknüpft sind.



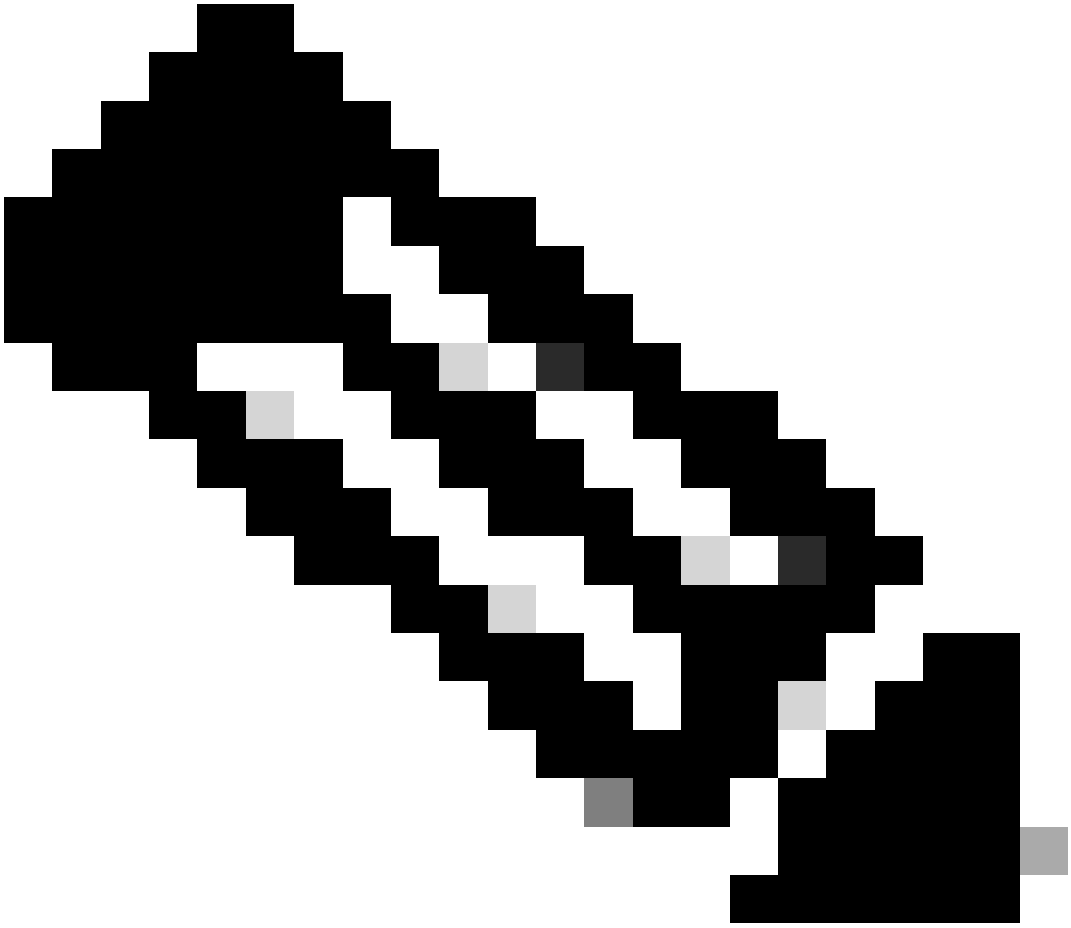
Zwei Host-Datensätze

Überprüfung

Navigieren Sie zu dem Client-Computer, auf dem der Cisco AnyConnect Secure Mobility Client installiert ist. In diesem Beispiel wird Test-PC-1 verwendet. Stellen Sie sicher, dass der DNS-Server 10.3.1.4 lautet.

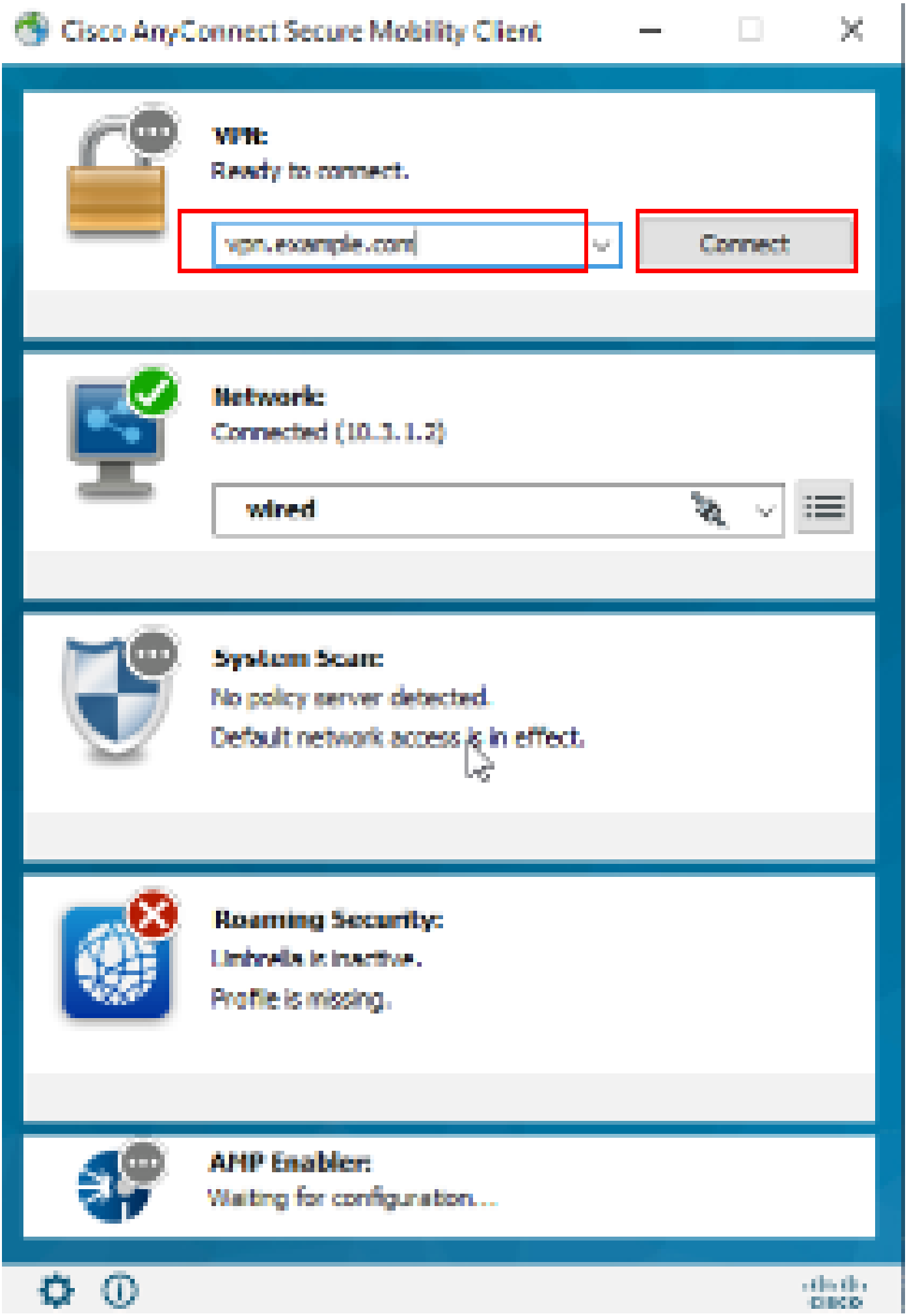


PC1-IP-Adresse



Hinweis: Da das Gateway zur Identifizierung eines selbst signierten Zertifikats verwendet wird, können während des Verbindungsversuchs mehrere Zertifikatwarnungen angezeigt werden. Diese werden erwartet und müssen akzeptiert werden, damit die Verbindung fortgesetzt werden kann. Um diese Zertifikatwarnungen zu vermeiden, muss das bereitgestellte selbstsignierte Zertifikat im vertrauenswürdigen Zertifikatspeicher des Clientcomputers installiert sein. Wenn ein Zertifikat eines Drittanbieters verwendet wird, muss sich das Zertifikat der Zertifizierungsstelle im vertrauenswürdigen Zertifikatspeicher befinden.

Stellen Sie eine Verbindung mit Ihrem VPN-Headend vpn.example.com her, und geben Sie den Benutzernamen und die Anmeldeinformationen ein.



PC1 AnyConnect-VPN

: Auf der ASA können verschiedene Debug-Ebenen festgelegt werden. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, wird die Ausführlichkeit der Debugs erhöht. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

Sie können das Debugging aktivieren, um die VPN-Verbindung auf der ASA zu diagnostizieren.

- debug webvpn anyconnect - Zeigt Debug-Meldungen über Verbindungen zu AnyConnect VPN-Clients an.

Lesen Sie dieses Dokument, um häufige Probleme auf der Client-Seite zu beheben.

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.