Configure VPN Client Load Balance with DNS Round Robin on ASA

Contents

Introduction

This document describes how to configure anyconnect vpn client load balance with DNS round robin on ASA.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You have assigned IP addresses on your ASAs and configured the default gateway.
- Anyconnect VPN is configured on the ASAs.
- VPN users are able to connect to all ASAs with the use of their individually assigned IP address.
- DNS server of VPN users is round robin capable.

Components Used

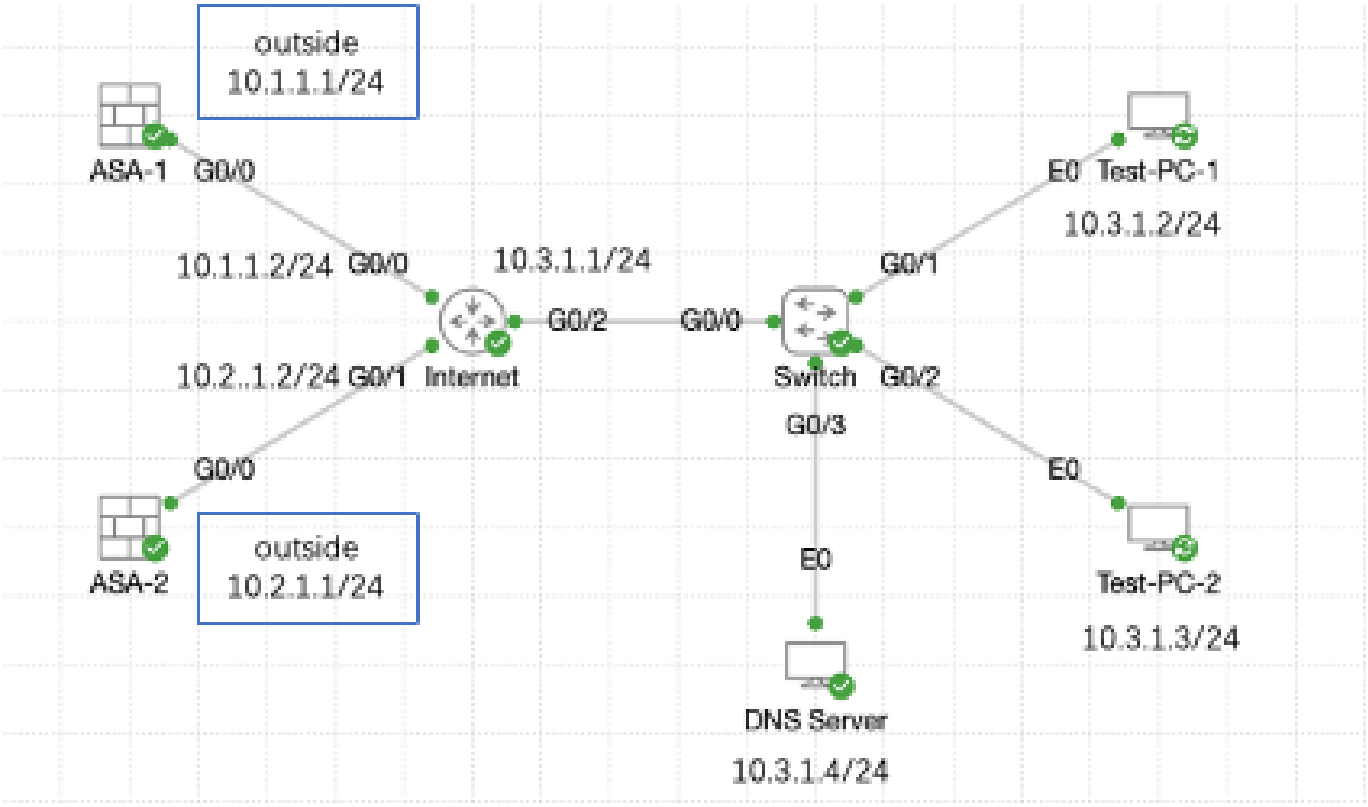
The information in this document is based on these software and hardware versions:

- Anyconnect VPN Client Software Releases 4.10.08025
- Cisco ASA Software Releases 9.18.2
- Window Server 2019

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Network Diagram

Configurations

Step 1. Configure Anyconnect VPN on ASA

For how to configure anyconnect VPN on ASA, refer to this document:

- ASA 8.x : VPN Access with the AnyConnect VPN Client Using Self-Signed Certificate Configuration Example

Here is the configuration of both ASAs in this example:

ASA1:

```
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
```

ASA2:

```
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
```

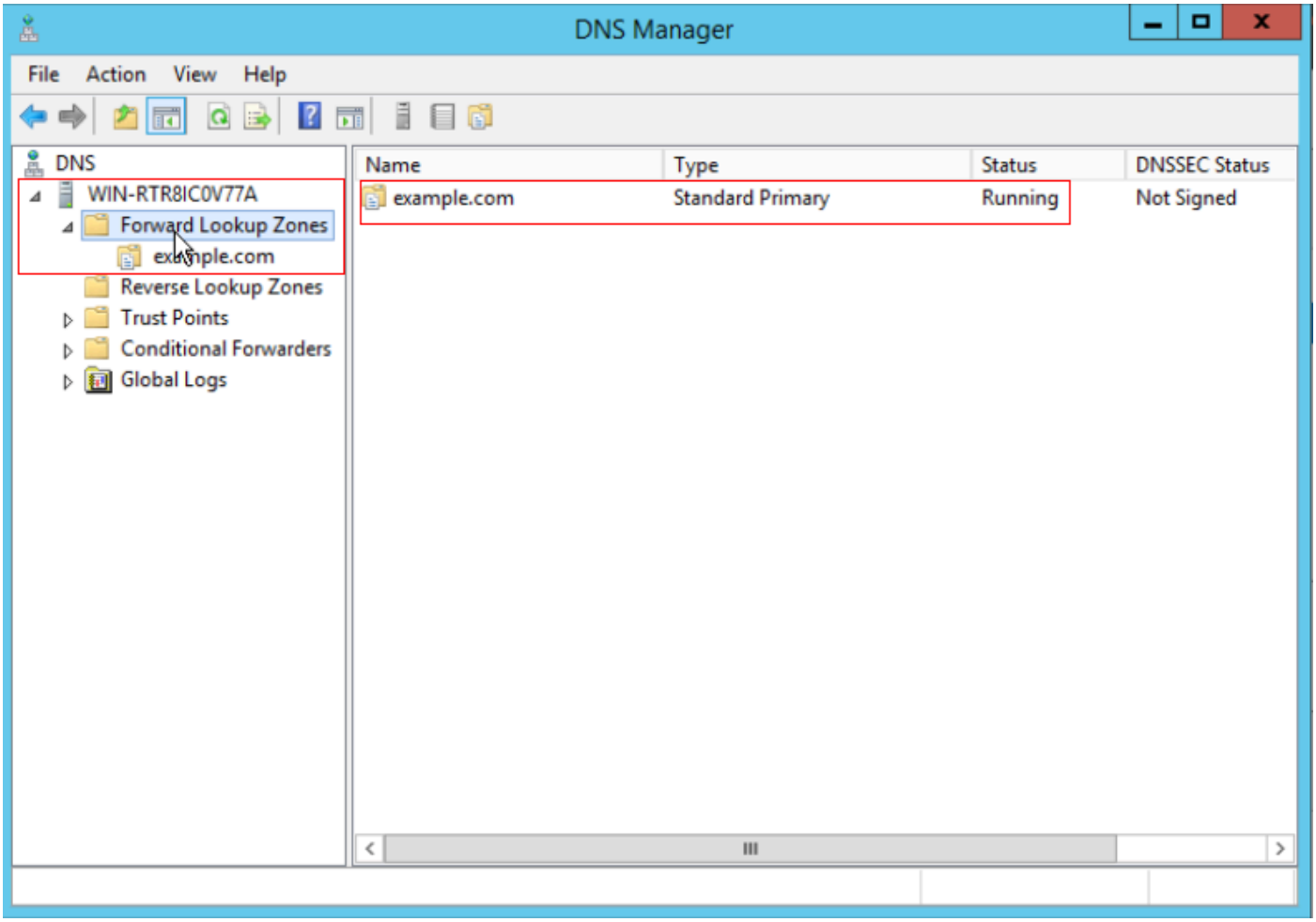
You must be able to connect to both ASAs with the use of their individually assigned IP address before you move to step 2.

Step 2. Configure Round Robin DNS on DNS Server

You can use any round robin capble DNS server, in this example, DNS server on windows server 2019 is used. For how to install and configure DNS server on windows server, refer to this document:

- Install and Configure DNS Server on Windows Server

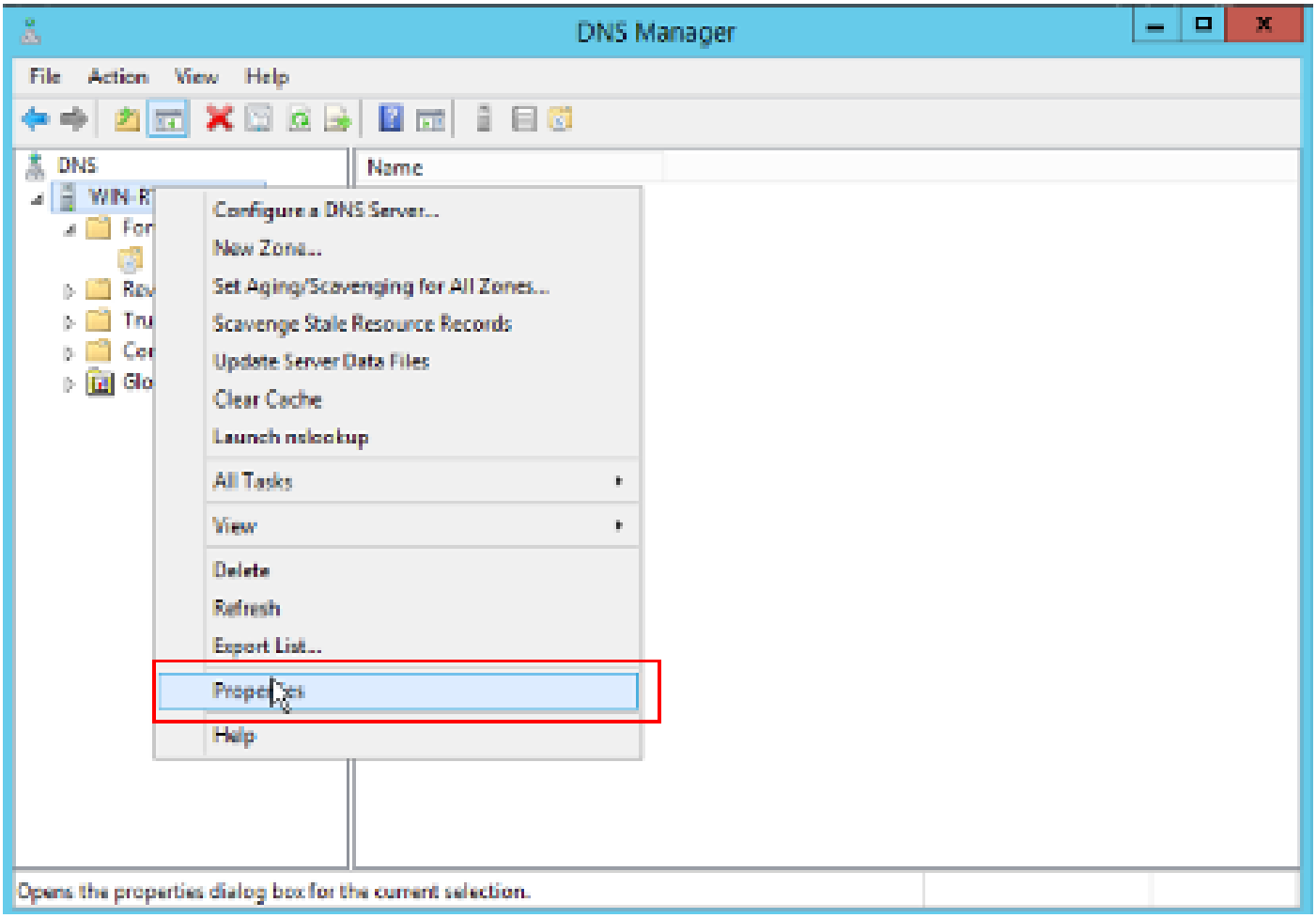
In this example, 10.3.1.4 is the windows server with DNS server enable for domain **example.com**.



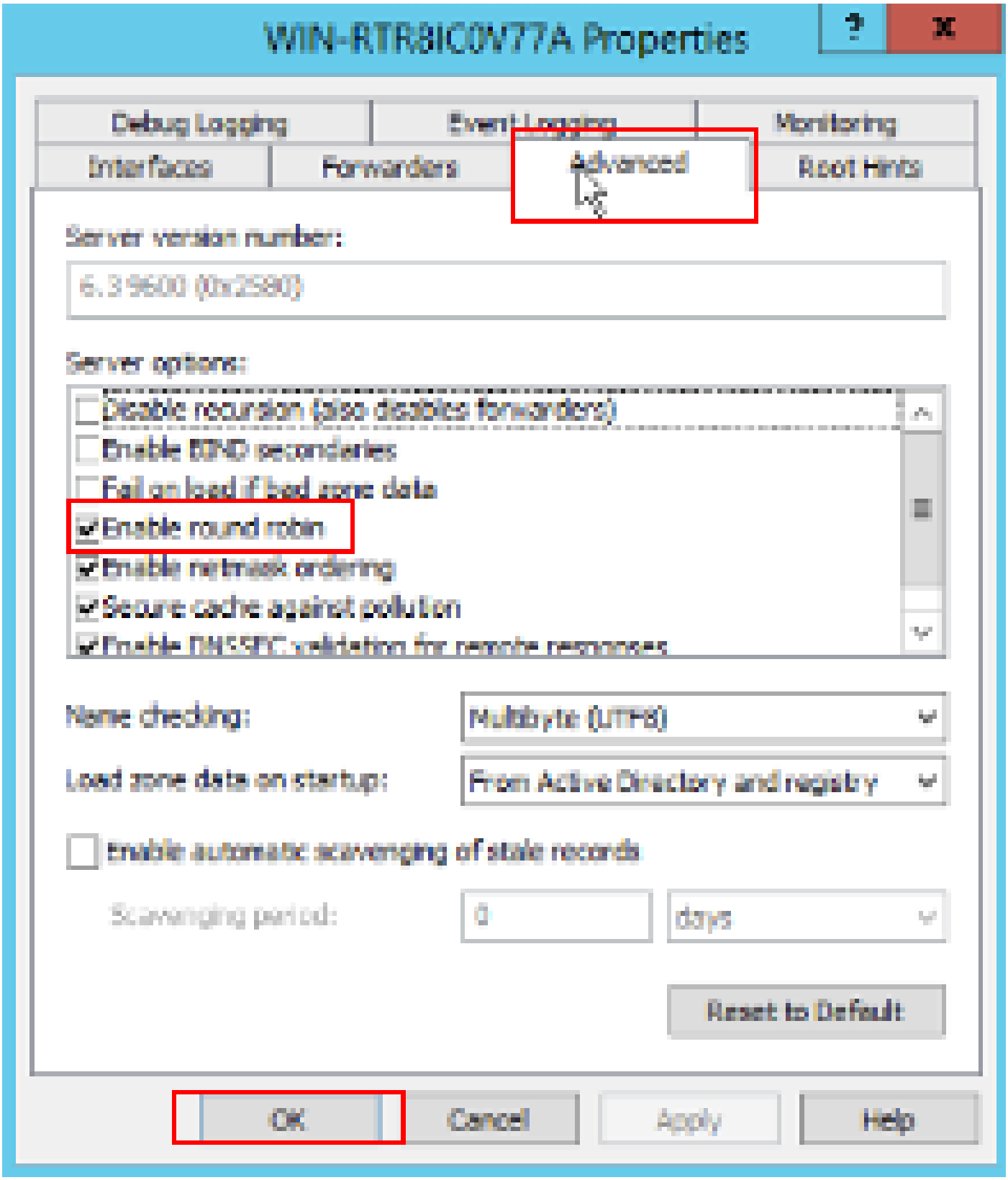
DNS Server

Make sure round robin is enabled for your DNS server:

1. From the Windows desktop, open the **Start** menu, select **Administrative Tools** > **DNS**.
2. In the console tree, choose the DNS server you wish to manage, right-click, then select **Properties**.
3. Under the tab **Advanced**, make sure **Enable round robin** is checked.



Round Robin 1

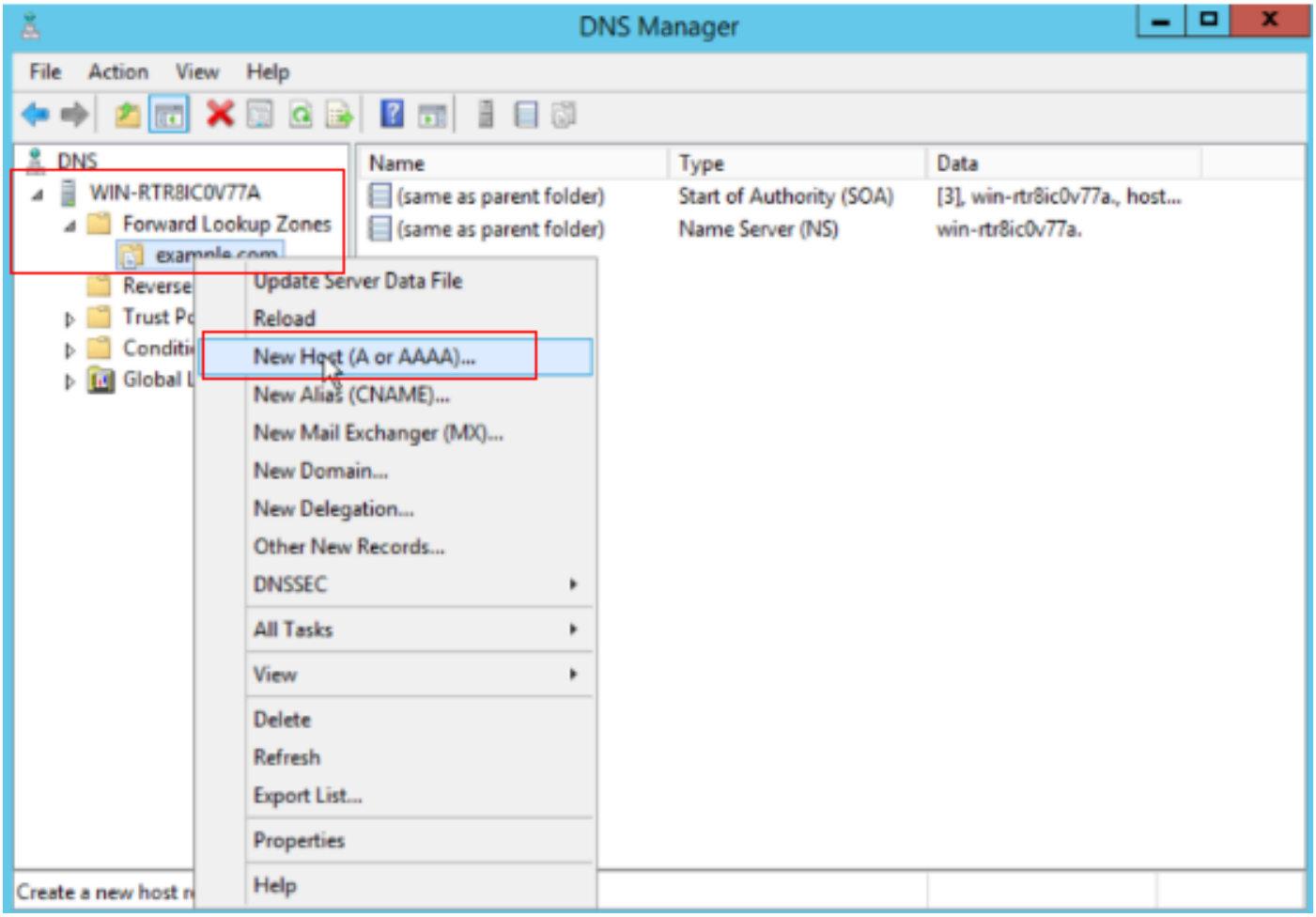


Round Robin 2

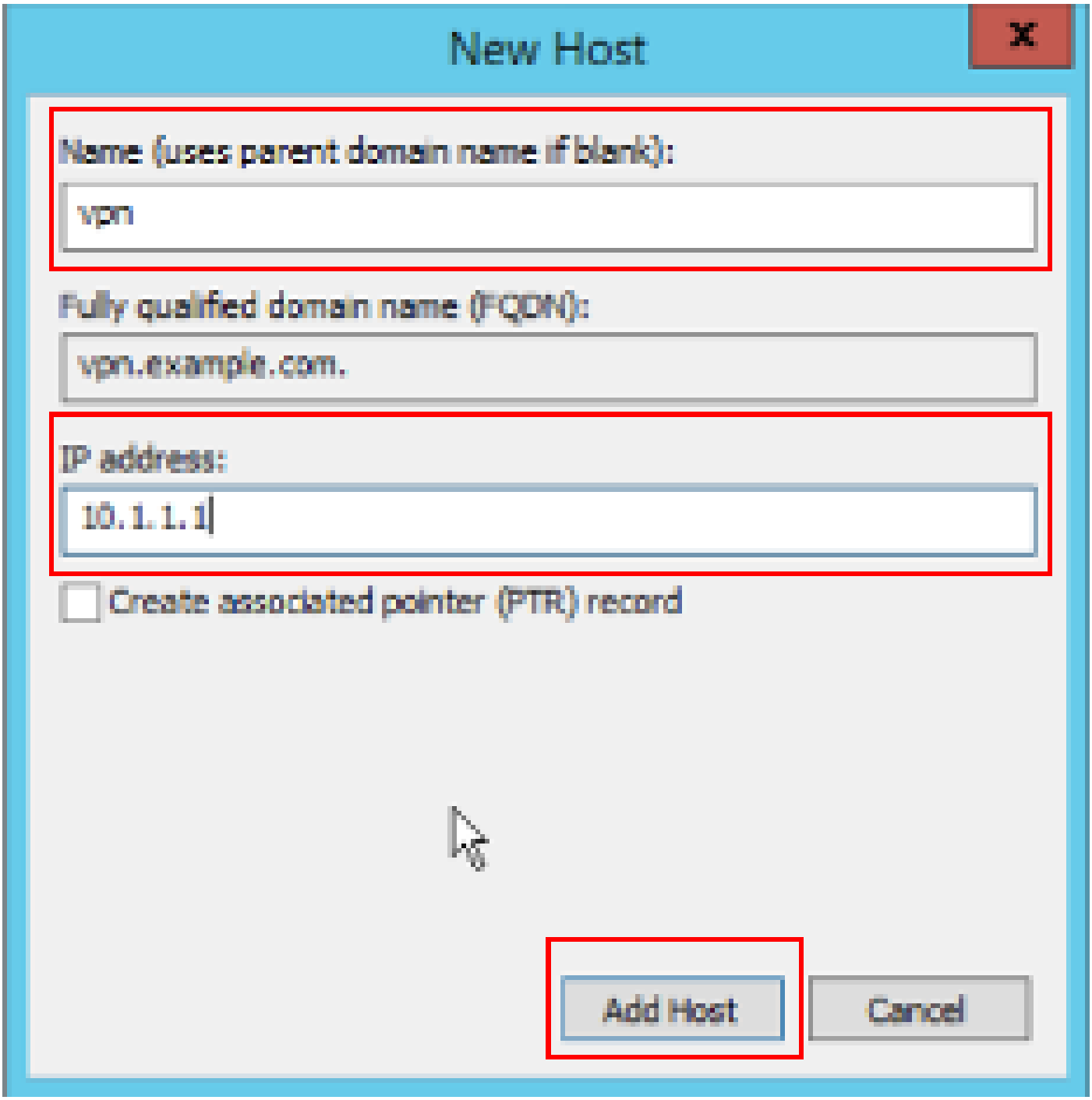
Create two host records for ASA VPN servers:

1. From the Windows desktop, open the **Start** menu, select **Administrative Tools** > **DNS.**
2. In the console tree, connect to the DNS server you wish to manage, expand the DNS server, expand your **Forward Lookup Zone**, right-click, then select **New Host (A or AAAA)**.
3. On the **New Host** screen, specify the **Name** and **IP address** of the host record. In this example, **vpn** and **10.1.1.1**.

4. Select **Add Host** to create the record.

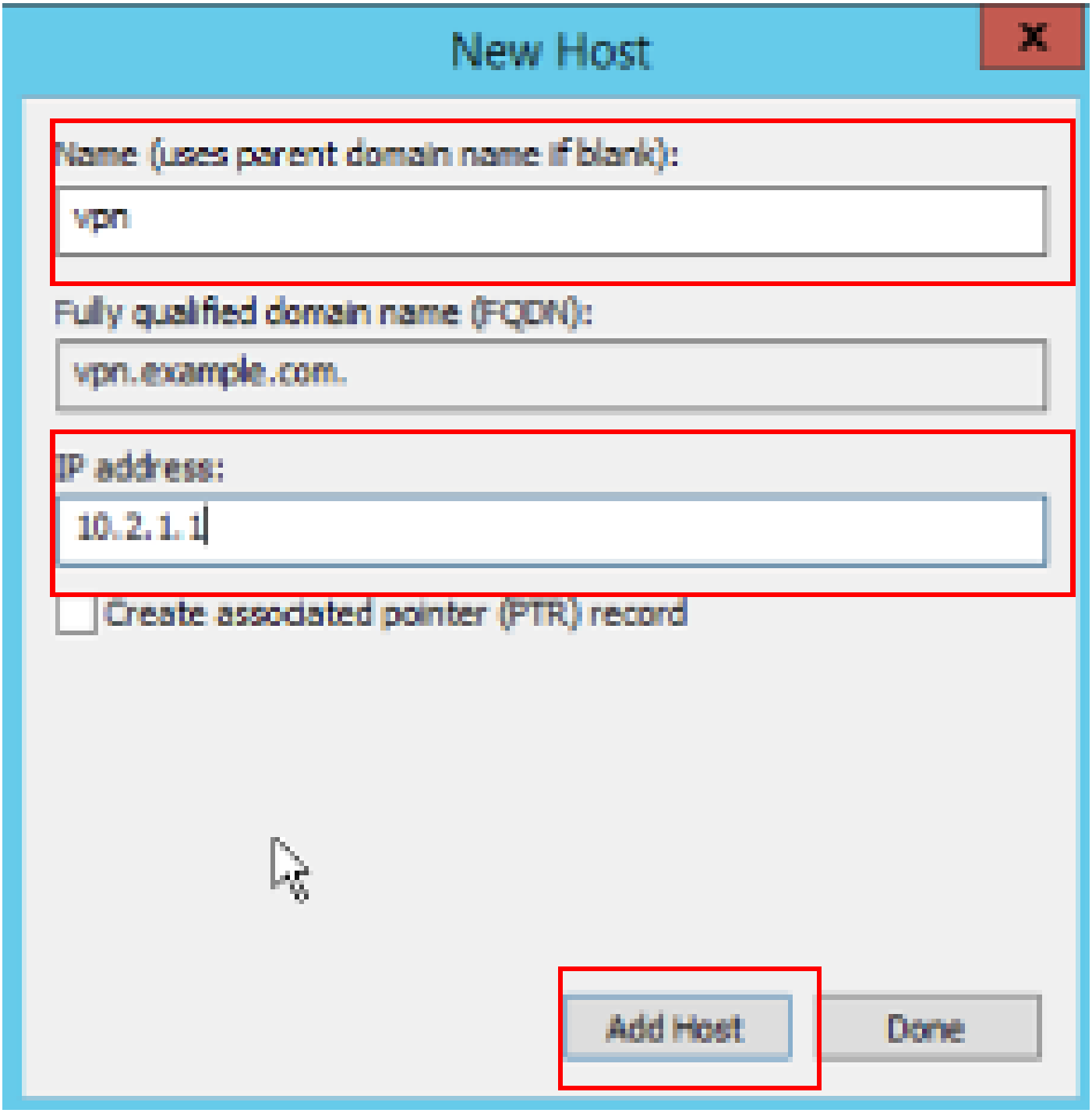


Create New Host



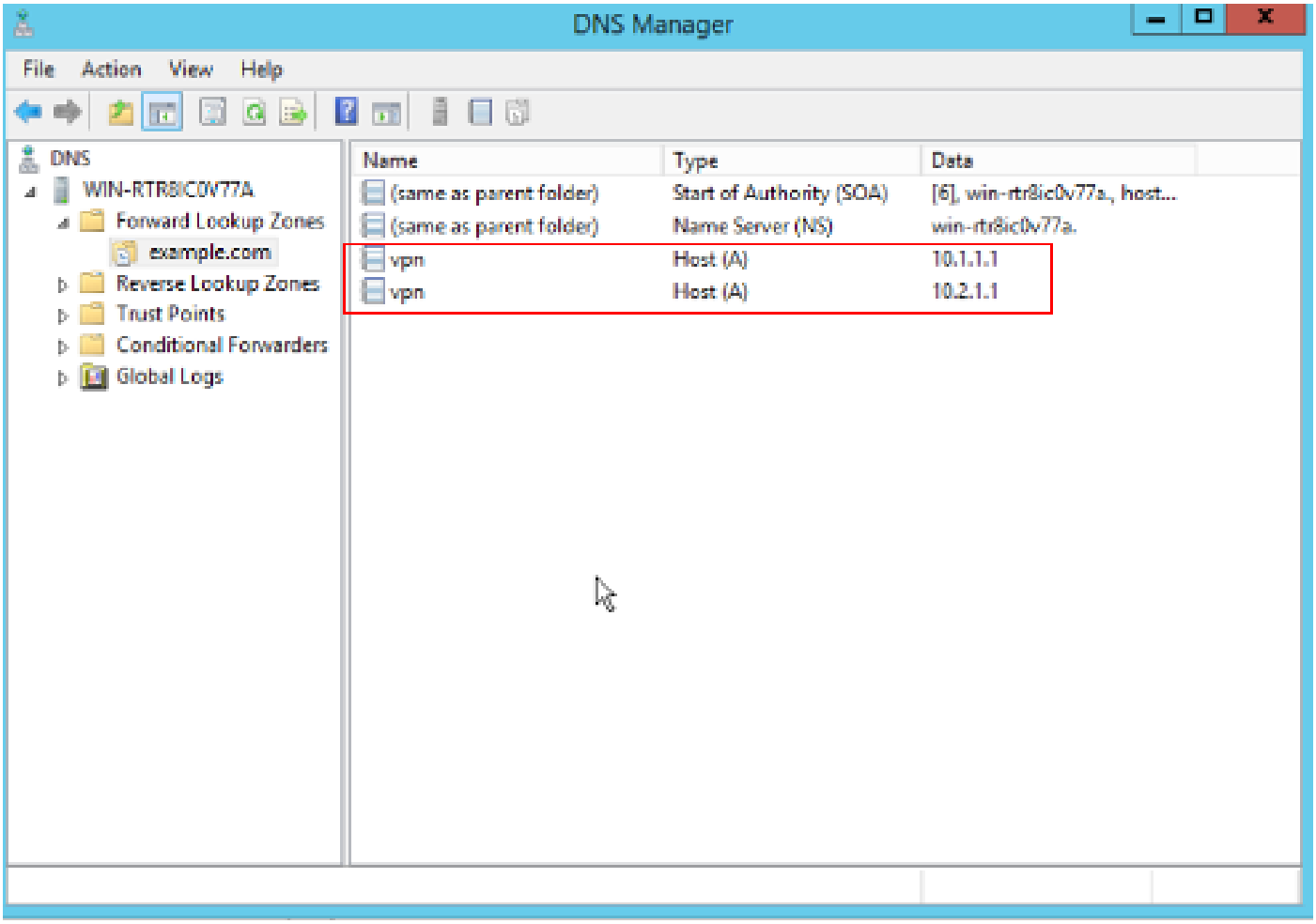
Host Record 1

Repeat similar steps to create another host record and make sure **Name** is the same, in this example, **Name** is **vpn**, **IP address** is **10.2.1.1**.



Host Record 2

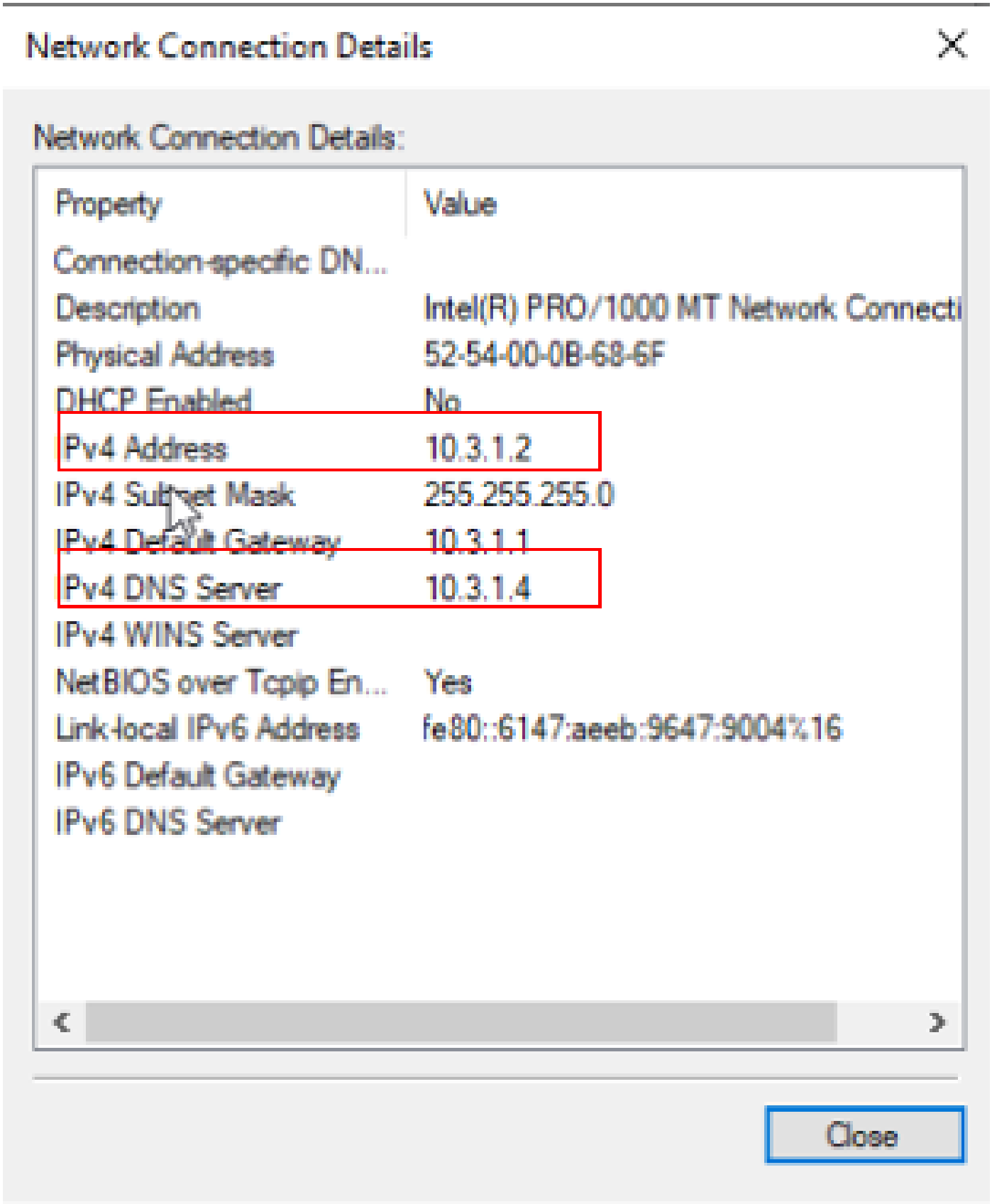
You can find there are two hosts **10.1.1.1** and **10.2.1.1** associate to the same record **vpn.example.com**.



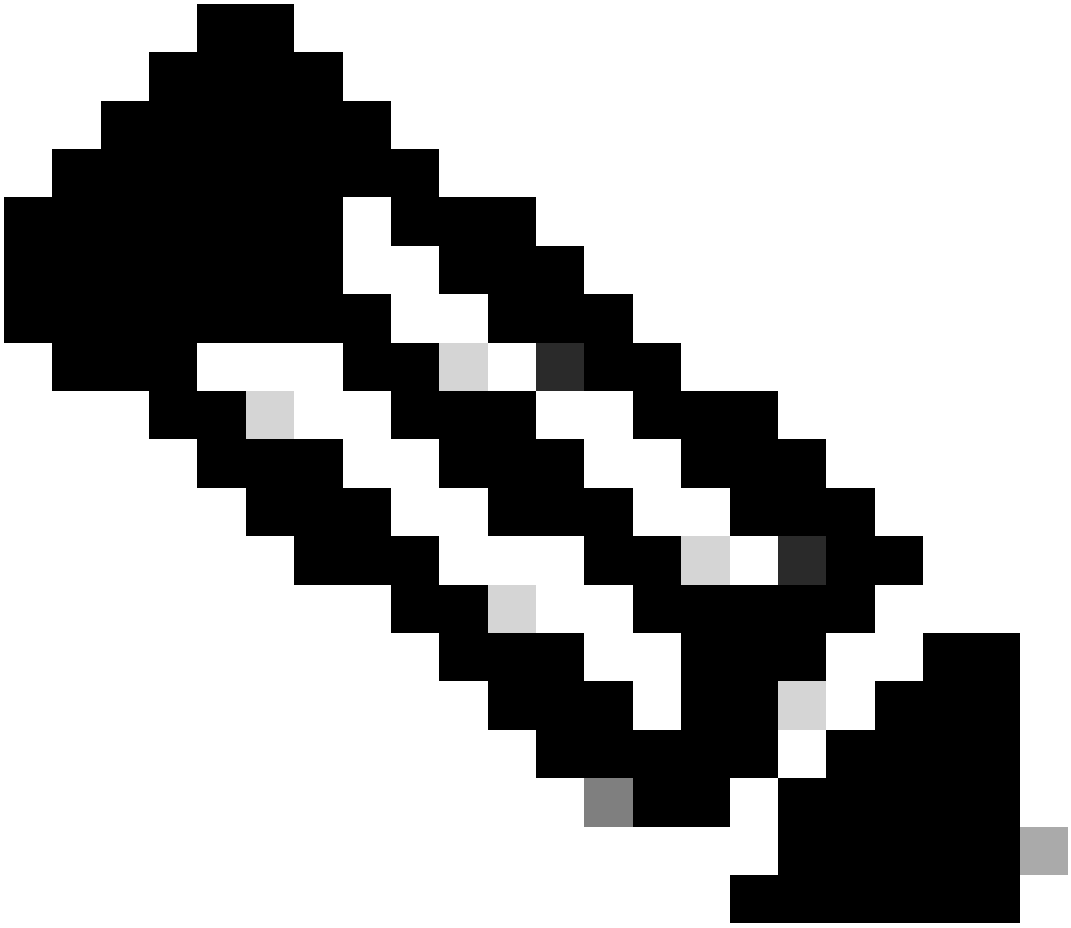
Two Host Records

Verify

Navigate to your client machine where the Cisco AnyConnect Secure Mobility client is installed, in this example Test-PC-1, verify your DNS server is **10.3.1.4**.

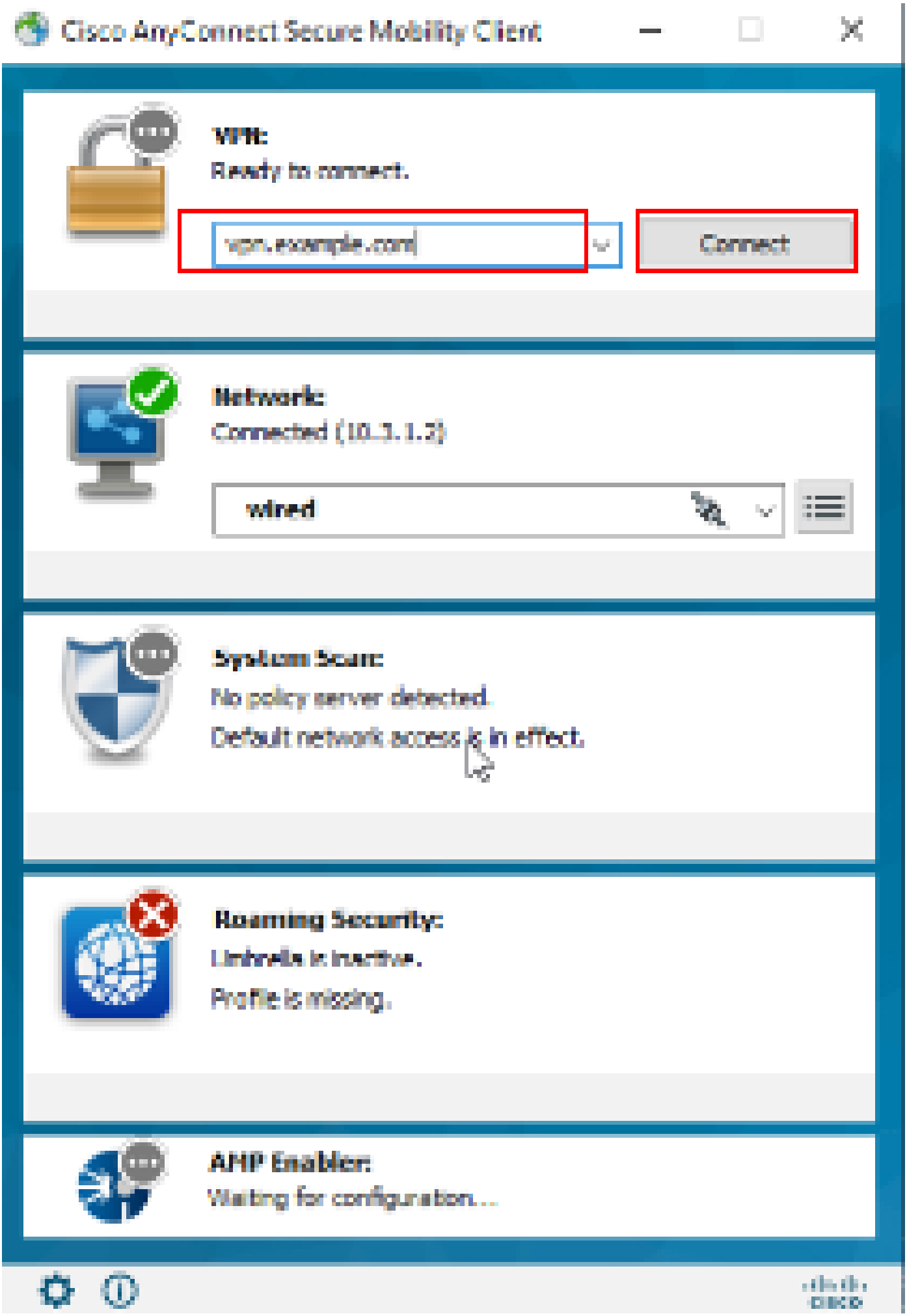


PC1 IP Address



Note: As a self-signed certificate is being used for the Gateway to identify itself, multiple certificate warnings can appear during the connection attempt. These are expected and must be accepted for the connection to continue. In order to avoid these certificate warnings, the self-signed certificate that is presented must be installed in the trusted certificate store of the client machine, or if a third-party certificate is being used then the Certificate Authority certificate must be in the trusted certificate store.

Connect to your VPN headend vpn.example.com and enter the username and credentials.



PC1 Anyconnect VPN

: On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs increase. Do this with caution, especially in production environments.

You can enable debug to diagnostic VPN connection on ASA.

- debug webvpn anyconnect - Displays debug messages about connections to Anyconnect VPN clients.

Refer to this document in order to troubleshoot common issues found on the client side.