e·quinux

VPN Configuration Guide

Cisco ASA 5500 Series

© 2010 equinux AG and equinux USA, Inc. All rights reserved.

Under copyright law, this configuration guide may not be copied, in whole or in part, without the written consent of equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinux has been advised of the possibility of such damages.

Every effort has been made to ensure that the information in this configuration guide is accurate. equinux is not responsible for printing or clerical errors.

Configuration guide revision 2

Created using Apple Pages.

www.equinux.com

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your Cisco ASA to establish a VPN connection between them.

Using the Configuration Guide

Part 1 – VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your Cisco ASA device using the Cisco Adaptive Security Device Manager (ASDM) application. In the appendix you will find a complete listing of the resulting configuration in case you prefer to use the CLI (SSH or telnet) to configure your device.

This guide is a supplement to the documentation included with your Cisco device, it can't replace it. Please read this documentation before starting.

Part 2 – VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN tunnel.

Part 3 – Troubleshooting and Advanced Topics

Troubleshooting advice and additional tips can be found in the final part of this guide.

If you are setting up VPN on your device for the first time, we strongly recommend you keep to the tutorial-style setup in the first and second part of this document and make modifications only after you have tested the basic setup.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

http://equinux.com

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Tips and Tricks

This configuration guide contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Warnings

This exclamation mark warns you when there is a setting or action where you need to take particular care.

Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

Prerequisites

Your VPN Gateway

- This guide applies to Cisco ASA 5500 series devices
- Make sure you have the newest firmware version installed that is available for your device. This guide is based on Cisco Adaptive Security Appliance Software Version 8.3

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6

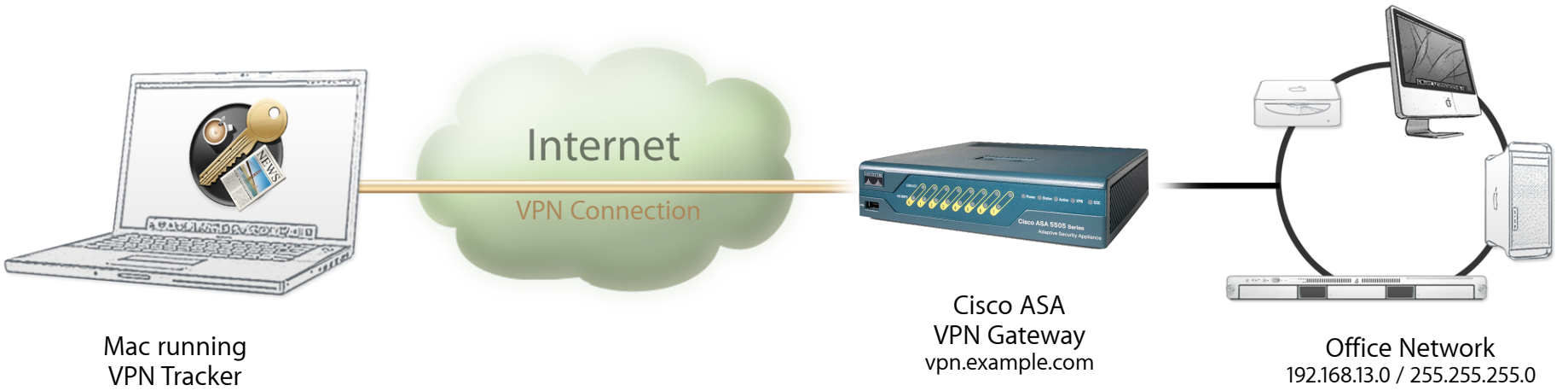
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram on the bottom of this page illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's Cisco ASA device (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address or DNS host name. In our example setup, we will be using a host name: vpn.example.com.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 192.168.13.0/24 (which is the same as 192.168.13.0/255.255.255.0). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.



Terminology

A VPN connection is often called a "tunnel" (or "VPN tunnel"). Every VPN tunnel is established between two "endpoints". In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is called the other endpoint's "peer".

Please note that for each endpoint, the settings on the other endpoint are considered to be "remote", while its own settings are considered to be "local". That means a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

The sample configuration described in this guide is called a "Host to Network" configuration: a single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

My VPN Gateway Configuration

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print out this checklist to help keep track of the various settings of your Cisco ASA device.

IP Addresses

❶ WAN IP Address: _____._____._____._____ or hostname _____

User Authentication (XAUTH)

❷ Username: _____

❸ Password: _____

IPsec Connection Profile

❹ Profile Name (Tunnel Group): _____

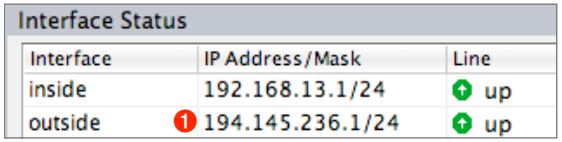
❺ Pre-Shared Key: _____

Task 1 – VPN Gateway Configuration

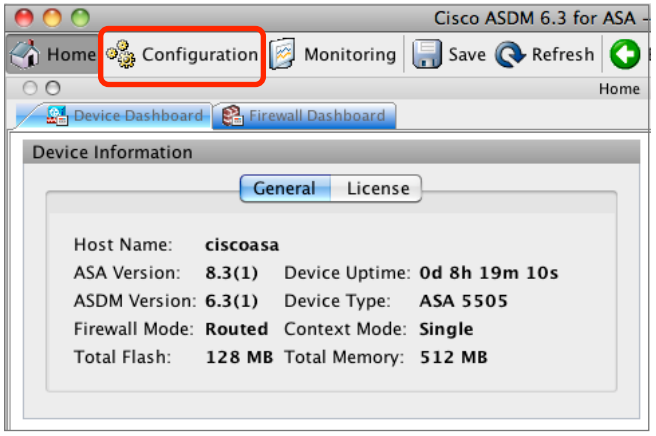
We will first set up VPN on the ASA device. If you already have VPN in place, it's helpful to follow along this tutorial to see how settings on the ASA fit together with VPN Tracker.

Step 1 – Outside Interface (WAN) Settings

- Open ASDM and connect to your ASA device
- Go to **Home** > **Device Dashboard** > **Interface Status**

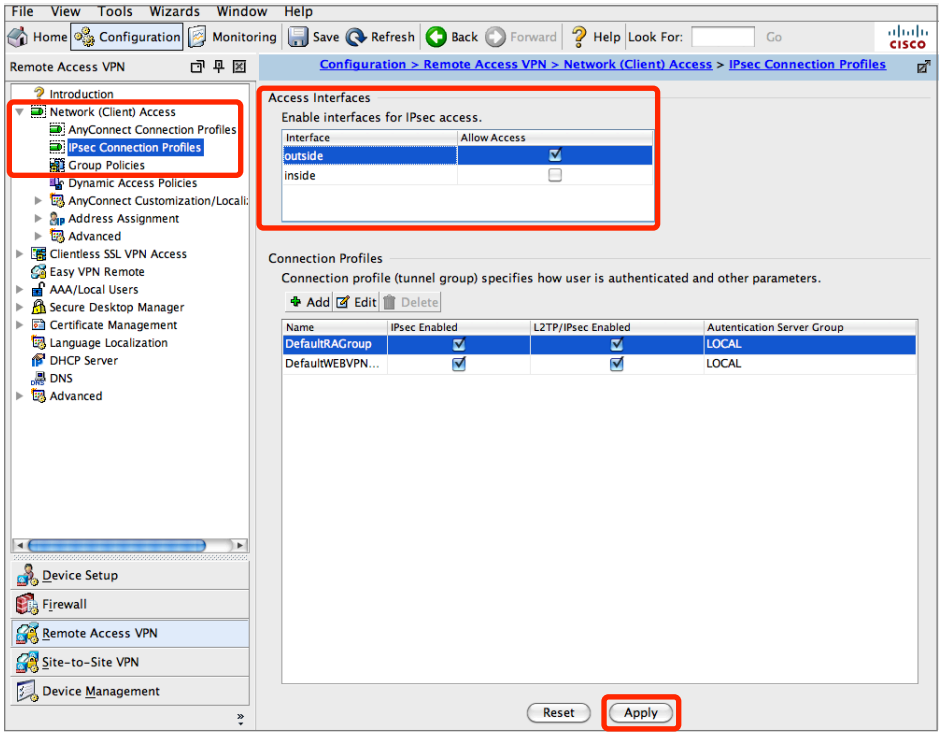


- Write down the IP address of the **outside** interface (the part before the forward slash "/") as ❶ on your → *Configuration Checklist*
- Go to **Configuration**



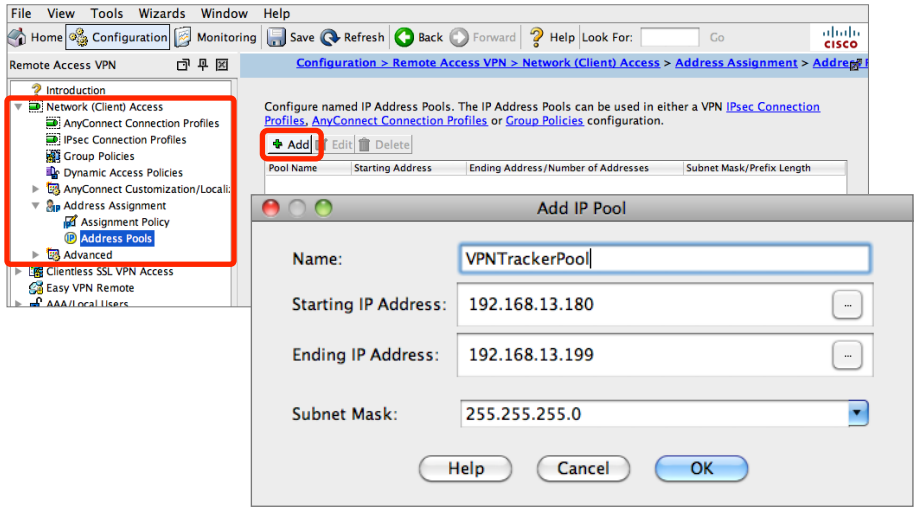
If you prefer the command line interface (CLI), please refer to the end of this document to see the corresponding commands for each configuration step.

Step 2 – Enable VPN



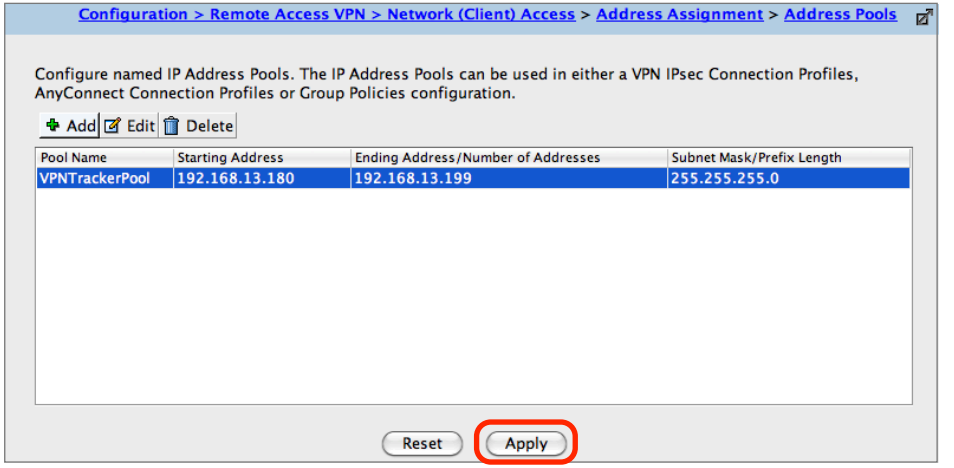
- Open the **Remote Access VPN** Section
- Go to **Network (Client) Access > IPsec Connection Profiles**
- Check the box **Allow Access** for the **outside** interface
- Click **Apply**

Step 3 – Add an IP Address Pool



- Go to **Network (Client) Access > Address Assignment > Address Pools**
- Click **Add**
- **IP Pool Settings:**
  - **Name**: Enter a name that allows you to recognize your address pool later (e.g. VPNTrackerPool). The name cannot contain any spaces.
  - **Starting IP Address**: Enter the first IP address in the address pool
  - **Ending IP Address**: Enter the last IP address in the address pool
  - **Subnet Mask**: Enter the subnet mask of the network the IP addresses come from. This ensures that broadcast and network addresses are not used for IP address assignment.
- Click **OK**

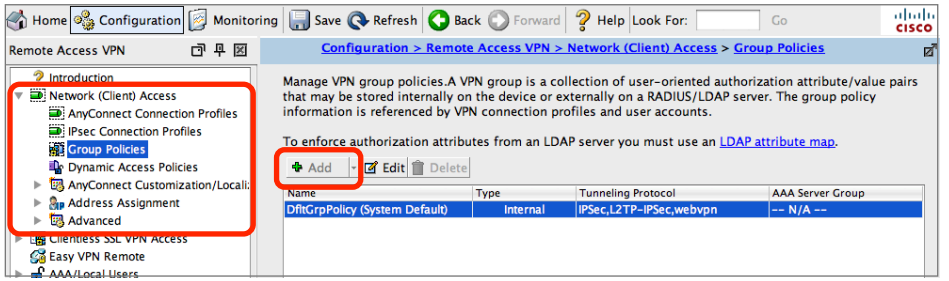
The IP address pool can be part of your ASA's inside network, however, it does not necessarily have to. If you expect to have more VPN clients than free IP addresses on your inside network, simply take your address pool from an arbitrary private network that is not in use anywhere on your network.



- Click "**Apply**" to save the new address pool

If you choose to use an address pool that is **not** part of your ASA's inside network, the ASA will not act as an ARP proxy. To ensure that hosts on the ASA's inside network know where to send traffic for VPN clients, **your ASA must be the default gateway (router) in its network** or a suitable routing setup must be in place on the default gateway to ensure that the VPN client IP pool is routed to the ASA.

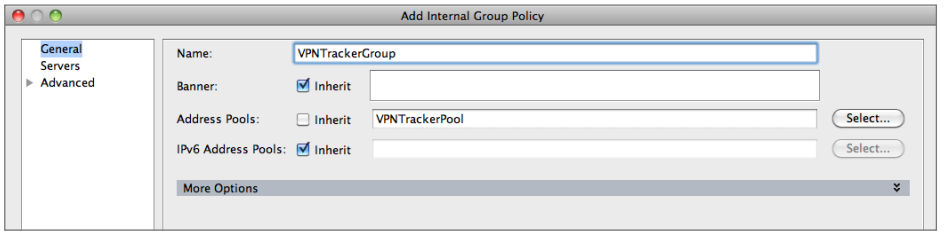
Step 4 – Add a Group Policy



- Go to **Network (Client) Access > Group Policies**
- Click **Add**

This guide assumes that the default group policy from which other policies inherit settings has not been modified. If you modified your ASA's default group policy, you may have to make changes to those settings that are set to "inherited" in the policy we're about to create.

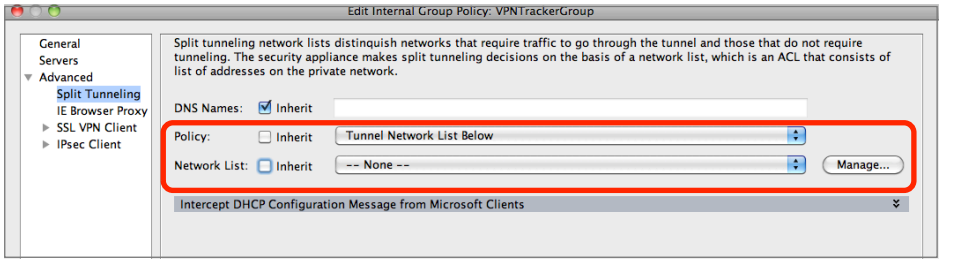
General Settings



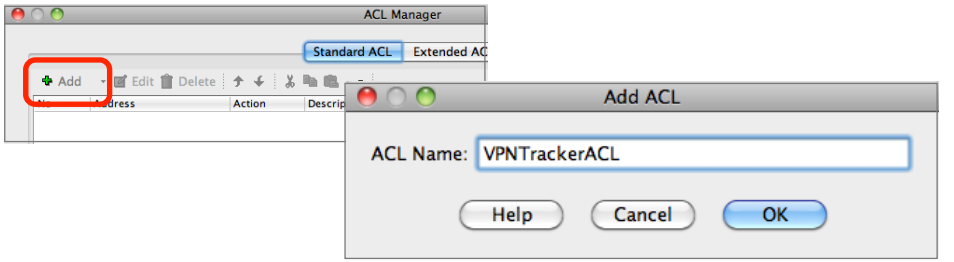
- **Name**: Enter a name that will allow you to recognize this group later. The name cannot contain any spaces
- **Address Pools**: Uncheck the box **Inherit** and enter the name of the address pool you created in the previous step (here: **VPNTrackerPool**)

We will be setting up the VPN for **split tunneling**, i.e. only the traffic destined for the ASA's internal network(s) will go through the VPN. A VPN Tracker user's remaining Internet traffic will continue to go out normally through their ISP. If you wish to tunnel all traffic through the VPN, please refer to → *Tunnel All Networks / Host to Everywhere Connections* for details.

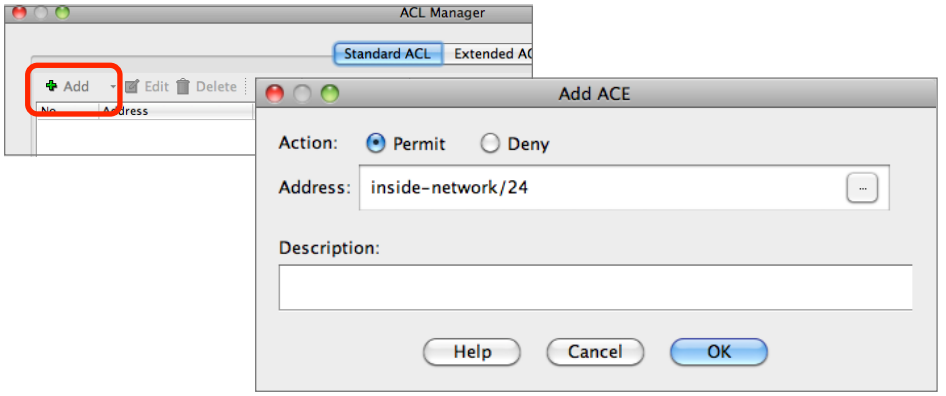
Split Tunneling Settings



- **Policy**: Uncheck **Inherit** and select **Tunnel Network List Below**
- **Network List**: Uncheck **Inherit** and click **Manage** to add a new network list



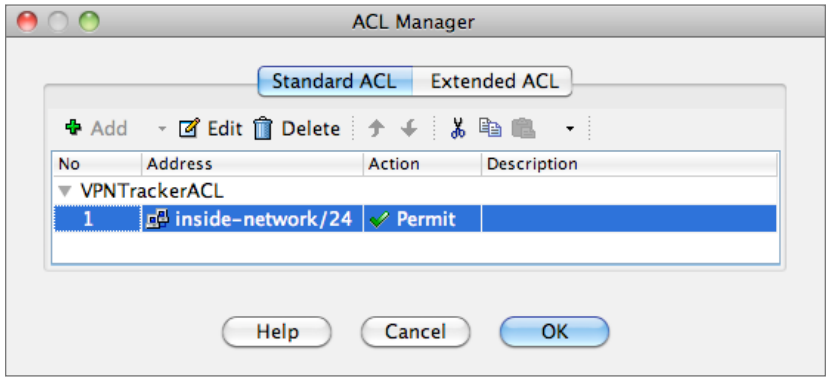
- In the ACL Manager, click **Add** > **Add ACL**
- **ACL Name**: Enter a name for the new ACL, e.g. **VPNTrackerACL**
- Click **OK**



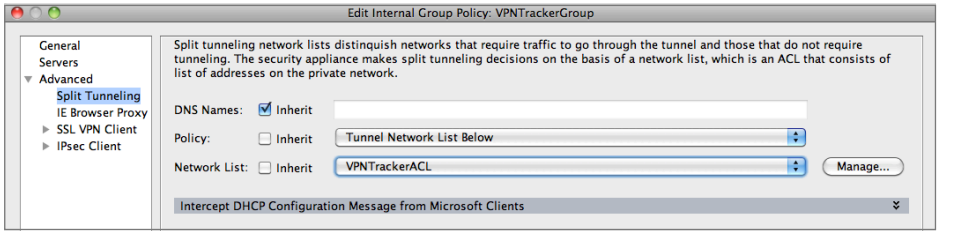
- In the ACL Manager, click **Add** > **Add ACE**
- **Action**: Make sure **Permit** is selected
- **Address**: Enter the address object representing your inside network (usually **inside-network/24**). Click the ".." button to create new address objects or to see what's available
- **Description**: If you wish, enter a description for this entry

---

If your VPN Tracker users will have access to more than one network, now is a good time to add the additional networks.

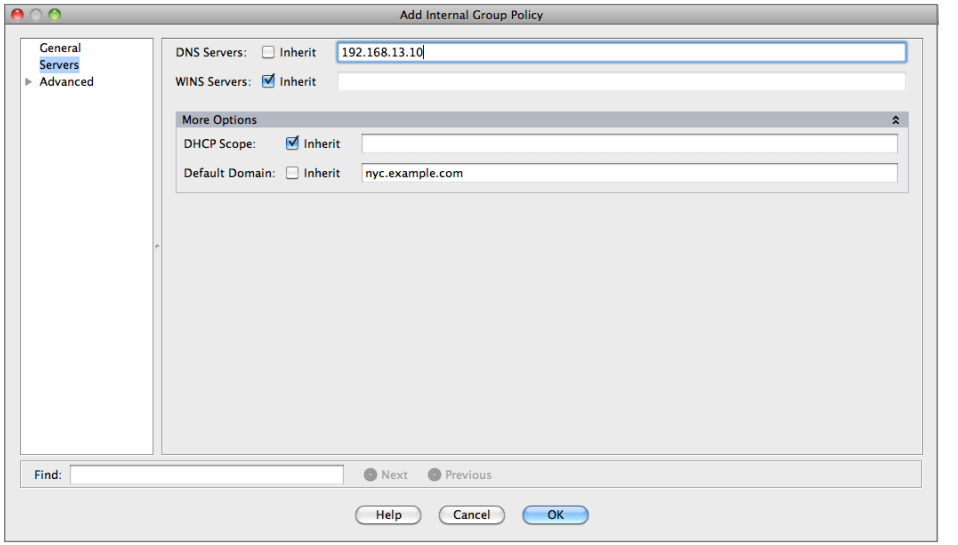


- Click **OK** when you're done adding entries to your ACL



- **Network List:** Select the newly created **ACL**
- Click **OK,** or continue with the optional **Remote DNS** setup (if you don't set up Remote DNS, click **Apply** so your configuration changes become active)

Servers Settings (Optional)

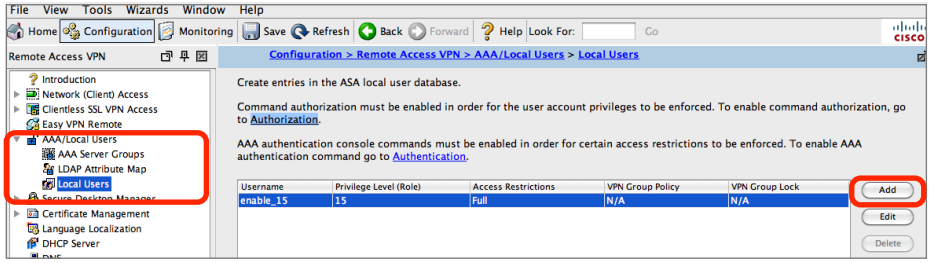


If you wish, you can set up DNS for your VPN clients. This makes sense if you already operate an internal DNS server for your organization.

- Go to the **Servers** section

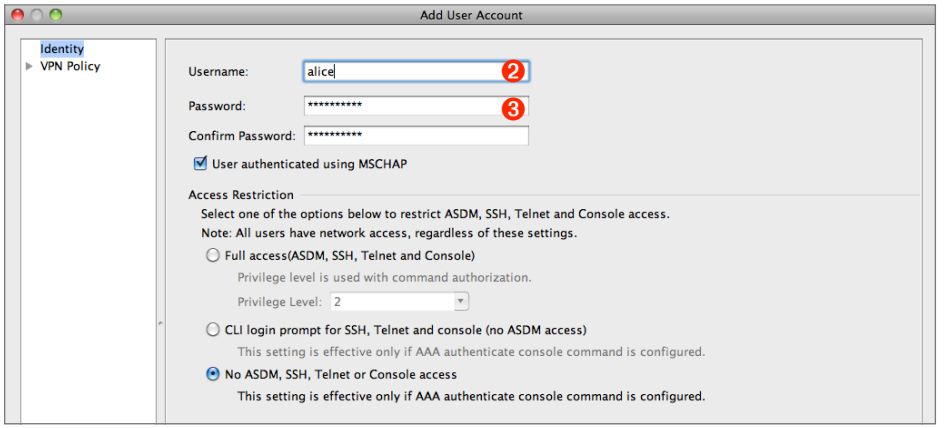
- **DNS Servers**: Uncheck the **Inherit** checkbox and enter the IP addresses of up to two DNS servers (comma-separated), in our example there's an internal DNS server operating at 192.168.13.10
- **Default Domain**: Uncheck the **Inherit** checkbox and enter a search domain (i.e. the domain the DNS server(s) should apply to), in our example we're connecting to our organization's New York office that uses nyc.example.com for its internal hosts.
- Click **OK**
- Don't forget to click **Apply** so your configuration changes become active

Step 5 – Add a User



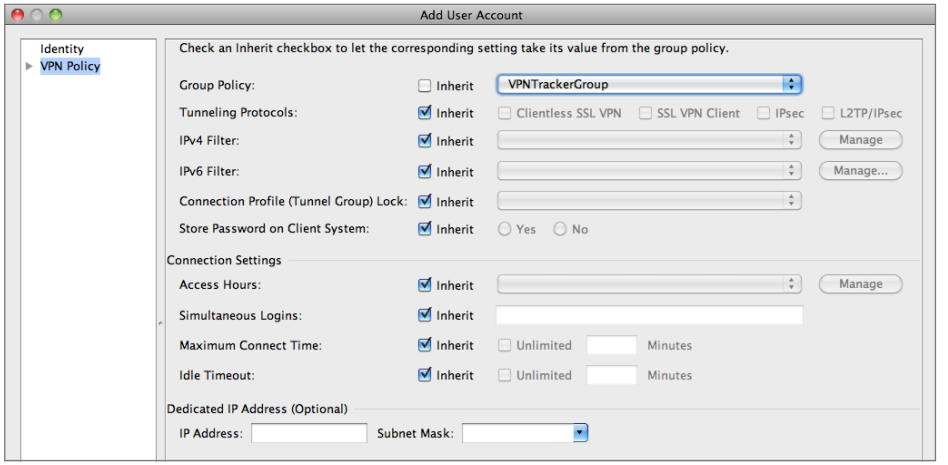
- Go to **AAA/Local Users** > **Local Users**
- Click **Add**

Identity Settings



- **Username**: Enter a username for the new user (here: **alice**). Write down the user name as ❷
- **Password**: Enter a password for the new user and confirm it. Make sure to remember the password, or write it down as ❸
- **User authenticated using MSCHAP** (optional): Check the box if you would like to avoid storing the password in plain text
- **Access Restrictions** (optional): Access to ASDM or CLI is not necessary for VPN users, so you can select **No ASDM, SSH, Telnet or Console access**

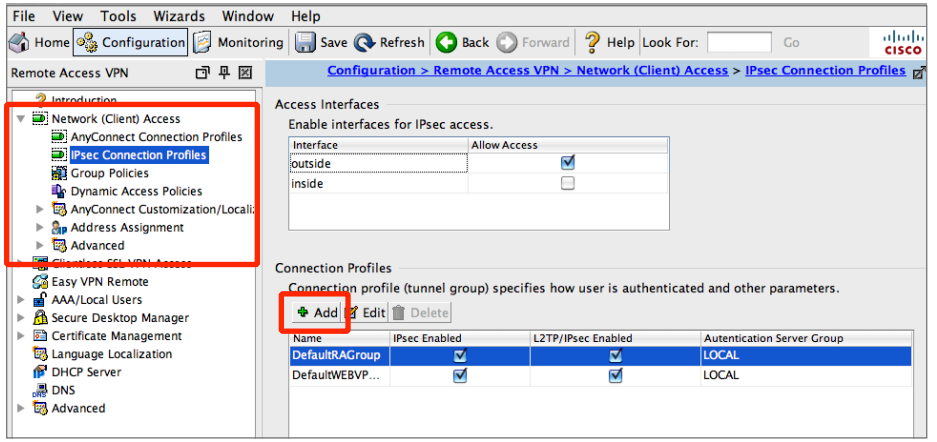
VPN Policy Settings



- **Group Policy**: Uncheck the box Inherit and select the group you created in the previous step (here: **VPNTrackerGroup**)
- Click **OK** to finish adding the user
- Don't forget to click **Apply** so your configuration changes become active

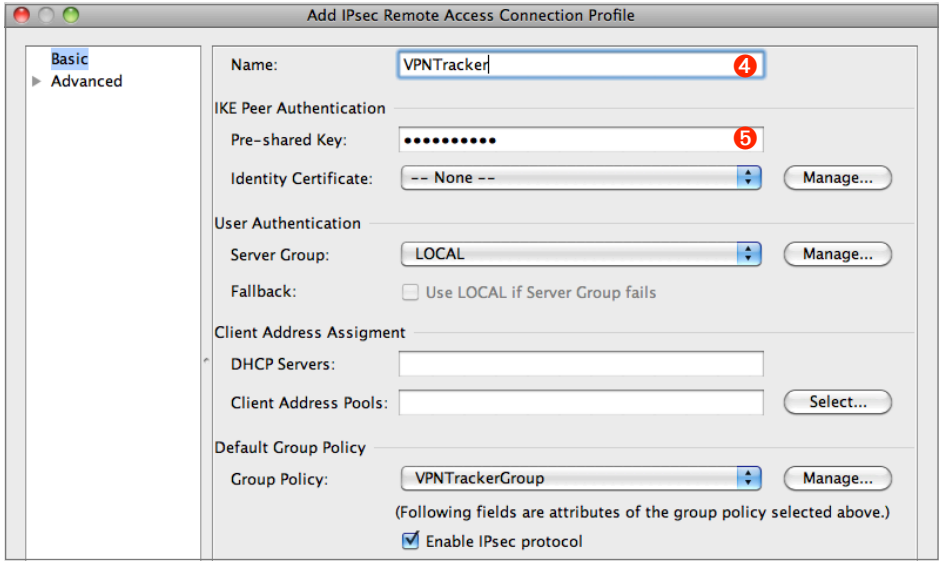
To add more VPN users later, simply repeat this step.

Step 6 – Add an IPsec Connection Profile



- Go to **Network (Client) Access** > **IPsec Connection Profile**
- Click **Add**

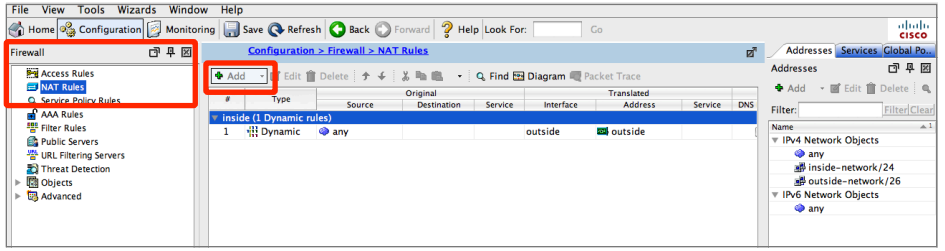
Remote Access Connection Profile Settings



- **Name**: Enter a name for the connection profile. Your users will later use the profile name in VPN Tracker as the **Local Identifier**. Write it down as ❹
- **Pre-Shared Key**: Enter a shared password for all users of this connection profile and write it down as ❺ In addition to this shared password, each user needs their individual username and password to authenticate.
- **Group Policy**: Select the group you created in the previous step (here: **VPNTrackerGroup**)
- Click **OK** to add the connection profile
- Don't forget to click **Apply** so your configuration changes become active

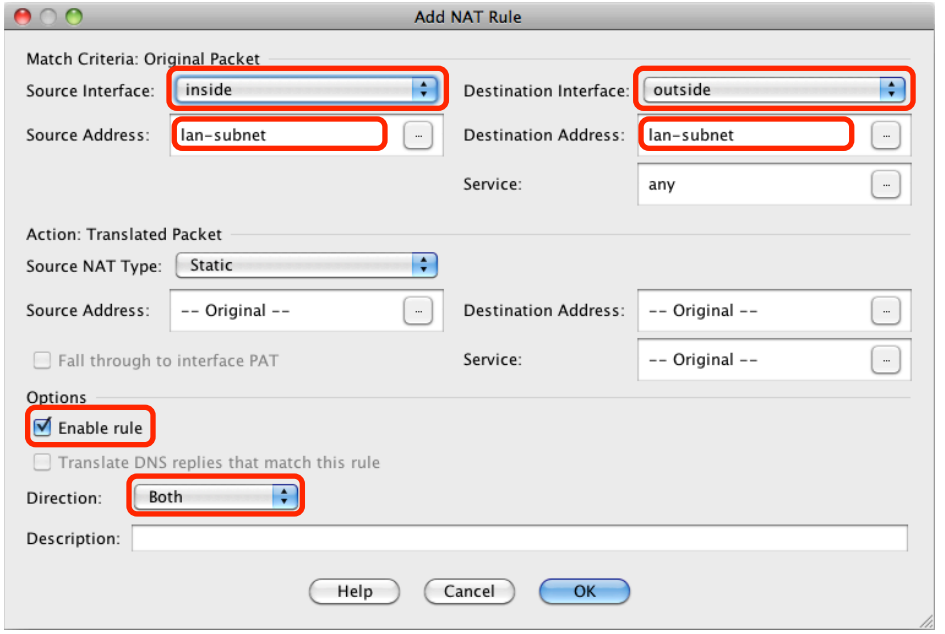
Step 7 – Exempt VPN Clients from NAT

If you normally have Network Address Translation (NAT) between your inside and outside interfaces, you will need to disable it for your VPN clients.

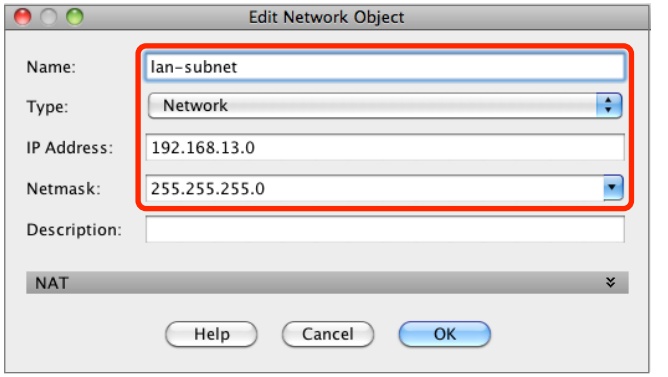


- Switch to the **Firewall** section
- Go to **NAT Rules**
- Click **Add** > **Add NAT Rule…**

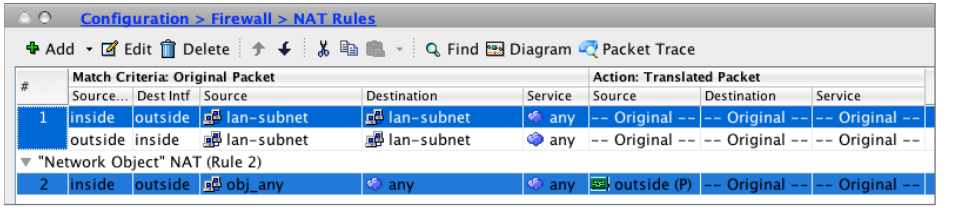
Rule Settings (for IP Pools that are part of the inside network)



- **Source Interface**: Choose **inside**
- **Source Address**: If you do not yet have an address object representing your inside network, create it (here: **lan-subnet**)

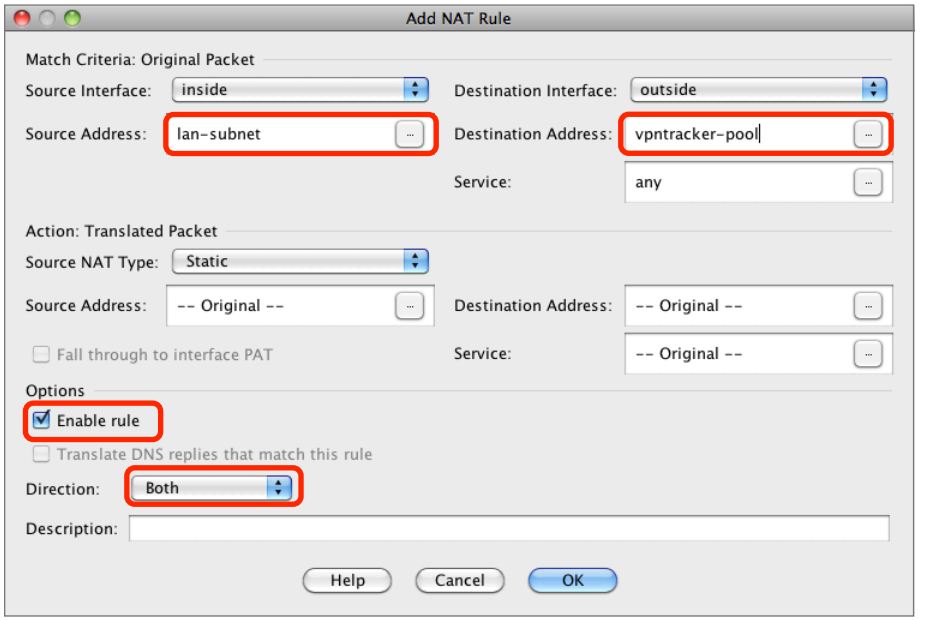


- **Destination Interface**: Choose **outside**
- **Destination Address**: Choose same address object as in **Source Address**
- Check the box **Enable rule**
- **Direction**: Choose **Both**
- Click **OK** to add the exemption

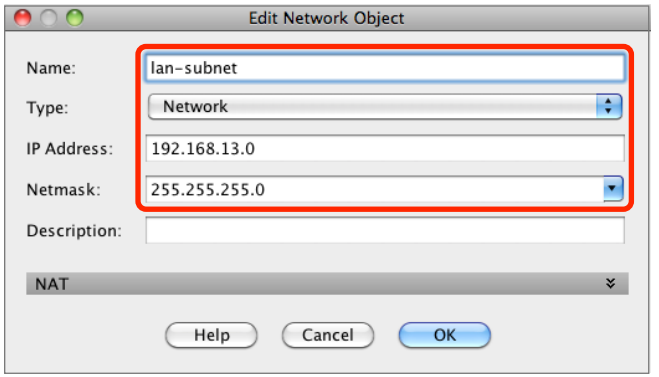


- Don't forget to click **Apply** so your configuration changes become active

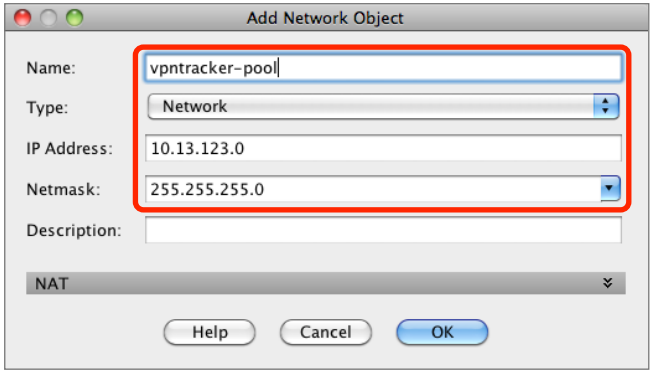
Rule Settings (for IP Pools from a different subnet)



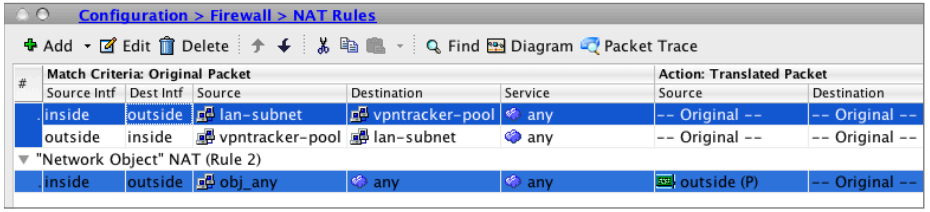
- **Source Interface**: Choose **inside**
- **Source Address**: If you do not yet have an address object representing your inside network, create it (here: **lan-subnet**)



- **Destination Interface**: Choose **outside**
- **Destination Address**: Create new address object (here: **vpntracker-pool**) representing the IP addresses your VPN clients will have (i.e. containing the IP pool you created earlier).



- Check the box **Enable rule**
- **Direction**: Choose **Both**
- Click **OK** to add the exemption



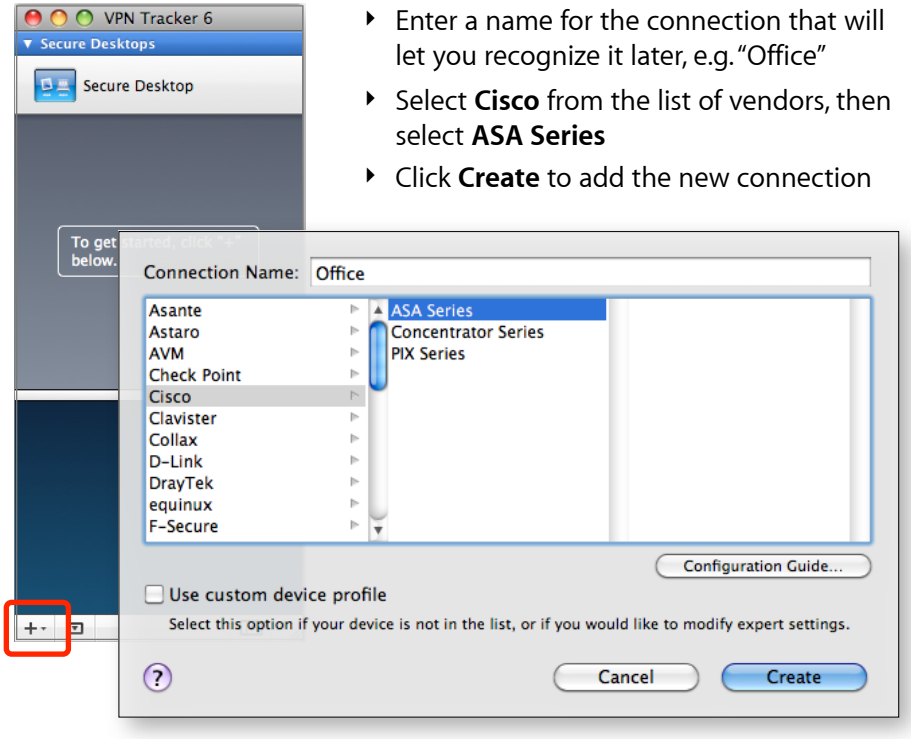
- Don't forget to click **Apply** so your configuration changes become active

Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *configuration checklist* containing your Cisco ASA's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

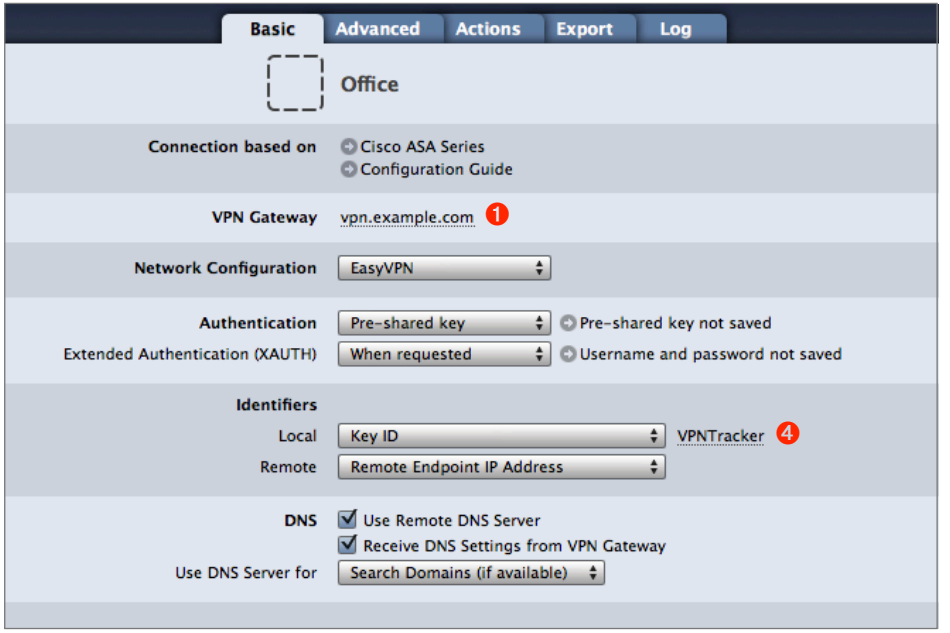
Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:



- Enter a name for the connection that will let you recognize it later, e.g. "Office"
- Select **Cisco** from the list of vendors, then select **ASA Series**
- Click **Create** to add the new connection

Step 2 – Configure the VPN Connection

Once you have added the new connections, there are a few settings that need to be customized to match what is configured on your ASA.



VPN Gateway

Enter the outside (WAN) IP address of your ASA that you wrote down as ❶. If your ASA has a DNS host name (such as vpn.example.com in our example), you can use it instead.

Local Identifier

Enter the name of the Connection Profile (Tunnel Group) ❹. Make sure the capitalization is the same as on your ASA.

DNS

If you did not configure DNS in your Group Policy (Step 4), uncheck **Use Remote DNS Server**.

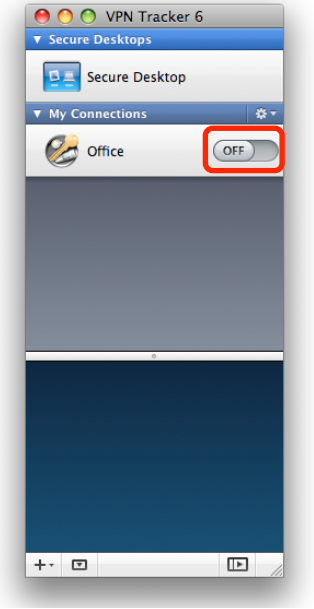
Task 3 – Test the VPN Connection

This section explains how to start and test your VPN connection.

It's time to go out!

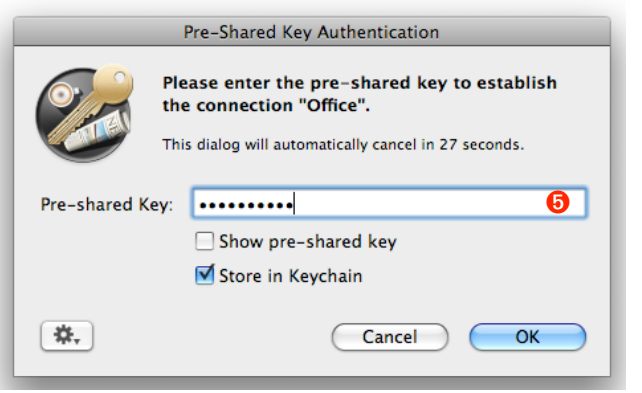
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. In order to test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting up a VPN connection to your home network, test it from an Internet cafe, or go visit a friend.

Start your connection



- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and try to connect to http://www.equinux.com
- Open VPN Tracker if it's not already running
- Slide the On/Off slider for the connection you have just configured to **On**

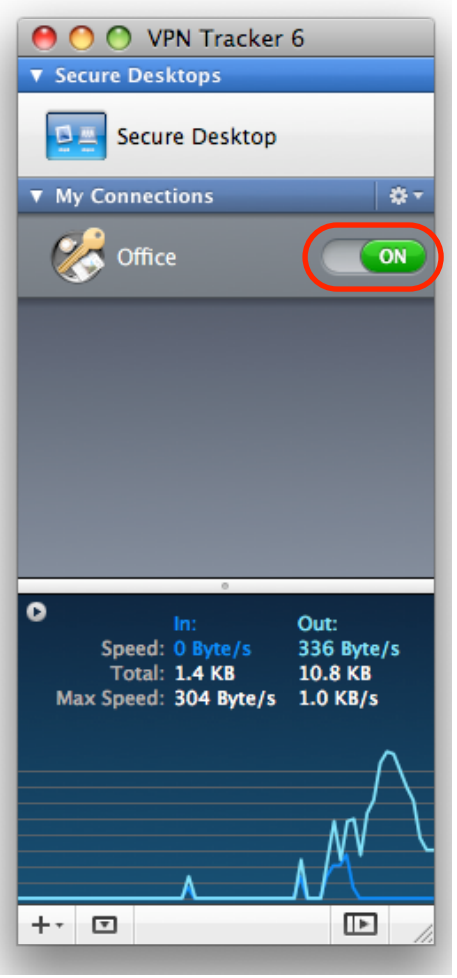
If you are prompted for your pre-shared key:



- **Pre-shared key**: Enter the passphrase that you configured on the ASA for your Connection Profile ❺
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**

If you are prompted for your Extended Authentication (XAUTH) credentials:

- User Name: Enter the name of the user you have added on the ASA ❷
- Password: Enter the password for the user ❸
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**



- If the slider goes back to **Off** after starting the connection, or after entering your pre-shared key or your XAUTH credentials, please read the → *Trouble-shooting* section of this document
- If the slider goes to **On** and turns green after a while, you have successfully established a connection
- Congratulations!
-

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

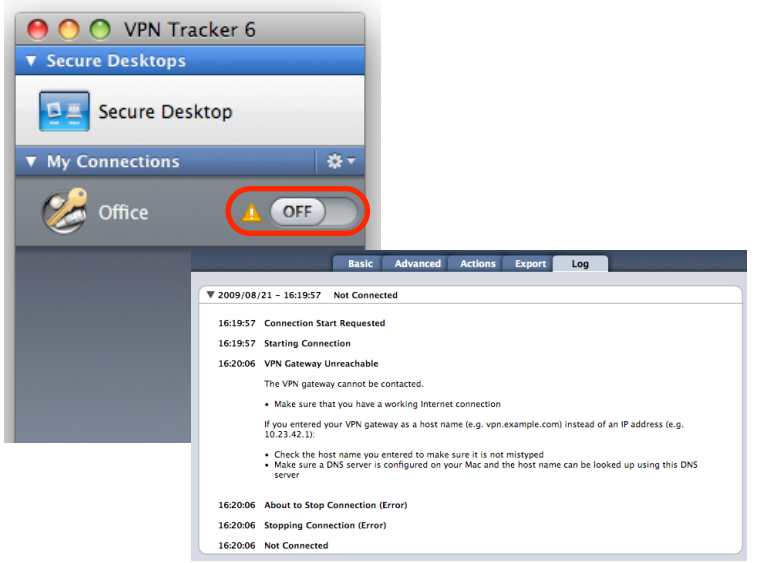
VPN Connection Fails to Establish

On/Off Slider goes back to "Off" right away

If the slider goes back to "Off" right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

On/Off Slider goes back to "Off" after a while

If the connection ON/OFF slider goes back to "OFF" a while after attempting to start the connection, please go to the "Log" tab to get more information about the error (or click the warning triangle to be automatically taken to the "Log" tab). VPN Tracker will display detailed suggestions for a solution:



No Access to the Remote Network

If the connection slider goes to ON and turns green, but you cannot access resources (servers, email, etc.) in the VPN, please check the following points.

Connect to an IP address (instead of a host name)

If you are not connecting to the resource by IP address (e.g. 192.168.13.42), but are using a host name (e.g. server.example.com), please try using the resource's IP address instead. If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server or the "Remote DNS" server that you have configured on your ASA is able to resolve this host name to an IP address.

Test VPN Availability again

In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

- Select "Tools > Test VPN Availability" from the menu
- Click "Test Again" and wait until the test has completed
- Try connecting again

Check that the IP address you are connecting to is part of the network(s) permitted in the split tunneling setup

Check that the IP address you are connecting to is actually part of the remote network(s) you permitted using the ACL in step 4. Also double-check the network mask that you have configured for the remote network(s) there.

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

http://www.equinux.com/support

If you need to contact equinux Technical Support

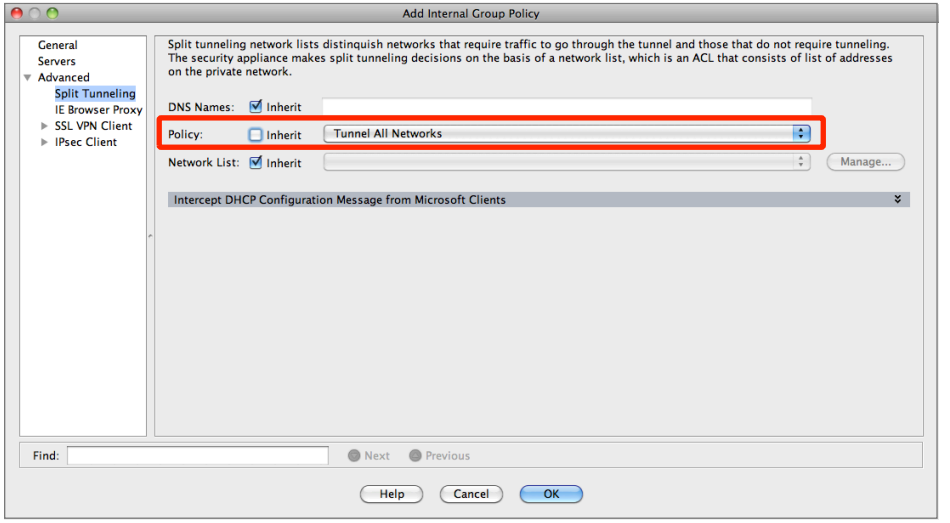
If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- The manufacturer and model and firmware revision of the VPN gateway
- A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- A description of the problem and the troubleshooting steps you have taken

Tunnel All Networks / Host to Everywhere Connections

In some situations, such as when connecting from a public wireless network, it can be useful to direct all Internet traffic through the VPN. The following changes are necessary to tunnel all Internet traffic through the VPN.

Disable Split Tunneling

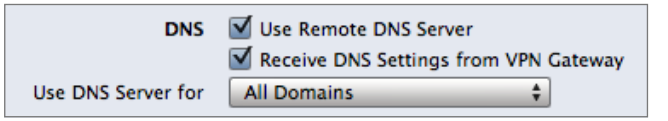


- On your **ASA**, edit the **Group Policy**
- Change the **Split Tunneling Policy** to **Tunnel All Networks** (if you are using the default settings for your default Group Policy, you can also simply click the **Inherit** checkbox

Configure DNS

Since all your Internet traffic will be going through the VPN, you will need to ensure that DNS resolution (looking up host names, such as www.google.com, and translating them to IP addresses) still works. Otherwise, it will seem as if you are cut off from the Internet.

If Remote DNS on your ASA is properly configured (**Servers** setting of your **Group Policy**), it will automatically transmit a suitable DNS server through EasyVPN. To use this DNS server, make sure to check the boxes **Use Remote DNS Server** and **Receive DNS Setting from VPN Gateway**, and set this DNS server to be used for **All Domains**:



If you already have a **working Remote DNS setup** in VPN Tracker, you will normally not have to change it.

Command Line (CLI) Setup

Configuring VPN on your ASA is also possible through the command line. This chapter lists the commands corresponding to each step in the first part of this document (steps that do not modify the configuration are not listed).

Commands for → *Step 2 – Enable VPN*

Enable IPsec VPN:

```
crypto isakmp enable outside
```

Using ADSM to enable VPN not only enables ISAKMP on the outside interface, it also adds a number of additional settings such as IPsec transforms, a crypto map and an ISAKMP policy. **The settings shown here are the defaults when enabling VPN through ADSM on a device with 3DES/AES license**.

ISAKMP Policies (Advanced > Phase 1 in VPN Tracker)

```
crypto isakmp policy 5
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
```

IPsec Transforms and Maps (Advanced > Phase 2 in VPN Tracker):

```
crypto ipsec security-association lifetime seconds 28800
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
```

```
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
```

You are free to change these settings according to your requirements. If you make changes, ensure that the settings in VPN Tracker (Advanced > Phase 1 / 2) match what is configured on your ASA.

Commands for → *Step 3 – Add an IP Address Pool*

IP Address pool from the inside network:

```
ip local pool VPNTrackerPool 192.168.13.180-192.168.13.199 mask 255.255.255.0
```

IP Address pool from a different private subnet (e.g. 10.13.123.0/255.255.255.0):

```
ip local pool VPNTrackerPool 10.13.123.1-10.13.123.254 mask 255.255.255.0
```

Commands for → *Step 4 – Add a Group Policy*

```
access-list VPNTrackerACL standard permit 192.168.13.0 255.255.255.0

group-policy VPNTrackerGroup internal
group-policy VPNTrackerGroup attributes
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value VPNTrackerACL
 address-pools value VPNTrackerPool

! optional DNS settings
! dns-server value 192.168.13.10
! default-domain value nyc.example.com
```

Commands for → *Step 5 – Add a User*

```
username alice password 9zuAO9H+/EaHeskPsLla/g== nt-encrypted
username alice attributes
 vpn-group-policy VPNTrackerGroup
 service-type remote-access
```

Commands for → *Step 6 – Add an IPsec Connection Profile*

```
tunnel-group VPNTracker type remote-access
tunnel-group VPNTracker general-attributes
 default-group-policy VPNTrackerGroup
tunnel-group VPNTracker ipsec-attributes
 pre-shared-key *****
```

Commands for → *Step 7 – Exempt VPN Clients from NAT*

IP Address pool from the inside network:

```
object network lan-subnet
 subnet 192.168.13.0 255.255.255.0

nat (inside,outside) source static lan-subnet lan-subnet destination static lan-subnet lan-subnet
```

IP Address pool from a different private subnet (e.g. 10.13.123.0/255.255.255.0):

```
object network vpntracker-pool
 subnet 10.13.123.0 255.255.255.0

nat (inside,outside) source static lan-subnet lan-subnet destination static vpntracker-pool vpntracker-pool
```