

The *NetScreen Remote Access 500 Getting Started* guide included in NetScreen-RA 500 appliance box explains how to configure and begin using your product. This addendum serves to replace “Step 4: Specify IP address information for Network Connect” on pages 9-10 of the printed guide. Refer to this addendum to complete Step 4 of the configuration process, which changes slightly with the 4.2 release of the NetScreen-RA 500 service package. Continue using the printed guide to complete “Step 5: Verify user accessibility” and to learn access management basics presented in Part II of the printed guide.

Step 4: Specify IP address information for Network Connect

When Network Connect runs on a user machine, all traffic to and from the client is transmitted over the secure Network Connect tunnel. This tunnel exists between a server-side process and client-side agent, each of which requires an IP address. You specify one IP address for the Network Connect server-side process to use for all Network Connect user sessions. When the NetScreen-RA 500 receives a client request to start a Network Connect session, it assigns an IP address to the client-side Network Connect agent from a Network Connect Connection Profile. The NetScreen-RA 500 assigns these IP addresses based on the connection profile that applies to a user’s role.

A **user role** is an entity that defines session parameters and personalization settings for users, as well as enables the Network Connect access feature. The NetScreen-RA 500 maps an authenticated user to one or more roles. The session options and Network Connect resource policies and connection profiles specified for the role(s) define accessible resources and IP address pools. For more information about roles, see “Define a user role” on page 15.

To specify IP address information for Network Connect:

1. In the Web console, choose **Resource Policies > Network Connect > NC Connection Profiles**.
2. On the **Network Connect Connection Profiles** page, click **New Profile**.
3. On the **New Profile** page, enter:
 - A name to label this policy.
 - A description of the policy (optional).
4. In the **IP address pool** section, specify IP addresses or a range of IP addresses for the NetScreen-RA 500 to assign to clients that run the Network Connect service. You can specify an IP range as “a.b.c.d-e” where the last component of the IP address is a range delimited by a hyphen (-). Special characters are not allowed.

Example: 10.10.10.1-100
5. In the **Roles** section, specify:
 - **Policy applies to ALL roles** — To apply this policy to all users.
 - **Policy applies to SELECTED roles** — To apply this policy only to users who are mapped to roles in the **Selected** roles list. Make sure to add roles to this list from the **Available** roles list.

- **Policy applies to all roles OTHER THAN those selected below** — To apply this policy to all users except for those who map to the roles in the **Selected** roles list. Make sure to add roles to this list from the **Available** roles list.



For information about user roles, see “Define a user role” on page 15.

6. Click **Save Changes**.
7. Choose **System > Network > Network Connect**.
8. Under **Network Connect Server IP Address**, enter an IP address for the Network Connect server-side process to use for all Network Connect user sessions. Make sure that the IP address is in the same sub-network as one of your IP Address Pool resource policies.

Example: 10.10.10.200

9. Click **Save**.

After you create a Network Connect Connection Profile for client-side processes and specify an IP address for the server-side process, you are ready to verify user accessibility.