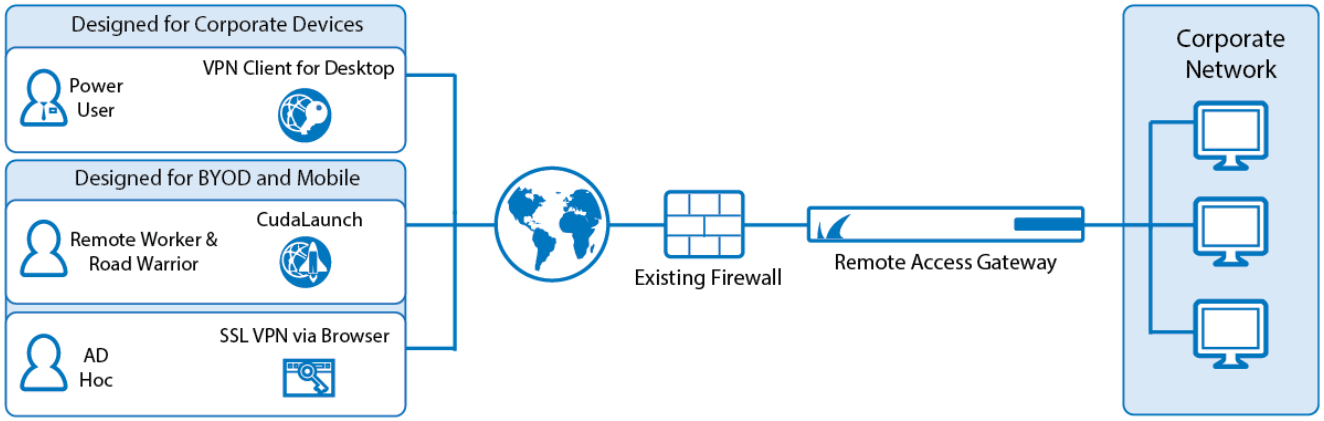
Deploy as Remote Access Gateway

https://campus.barracuda.com/doc/73702148/

Deploy the CloudGen Firewall as a remote access gateway for VPN traffic. The Remote Access Gateway wizard takes you through the necessary steps to configure a client-to-site VPN and enable SSL VPN with support for CudaLaunch. A Remote Access Premium subscription is required.



Before You Begin

Make sure you have the following information on hand:

- If you are using Active Directory as your method of authentication, you must have the Active Directory configuration information.
- The network that the client-to-site VPN clients will be assigned to (client network).
- The networks that will be available to the client-to-site VPN clients (published networks).

Step 1. Complete the Remote Access Gateway Wizard

This wizard allows you to configure the firewall as a remote access gateway that can work in conjunction with your existing firewall.

1. To launch the wizard, go to **Advanced > Wizards** and click **Start** next to **Remote Access Gateway**.
2. Enter the **VPN IP** address for the VPN service.

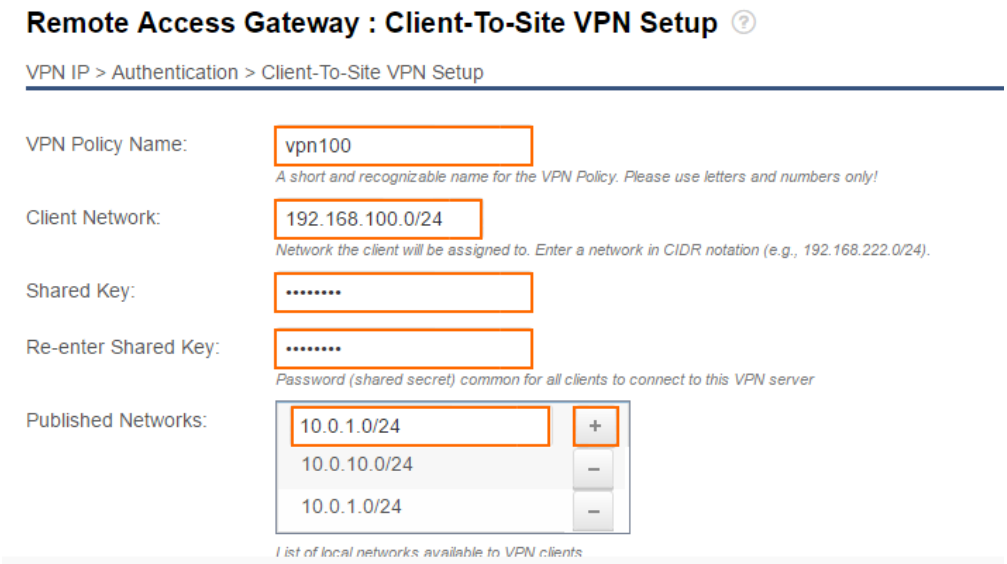
3. Click **Next**.
4. Select the authentication **Type** for the VPN service.
   When choosing **Local Authentication**:
   - Enter **Username** and **Password**.

   When choosing **Active Directory**, specify the following settings:
   - **Domain Controller Name** – Enter the fully qualified name of the domain controller.
   - **Domain Controller IP** – Enter the IP address of the domain controller.
     When using SSL, the name should be used instead of the IP address.
   - **Searching User** – Enter the username of the MSAD searching user.
   - **Searching User Password** – Enter the password for the MSAD searching user.
   - **Base DN** – Enter the distinguished name (DN) at which to start the search in the LDAP database, specified as a sequence of relative distinguished names, connected with commas, with or without blank spaces. Make the base DN as specific as possible in order to speed the lookup and avoid timeouts. For example, if your domain is yourcompany.com, your search base DN might be as follows: `DC=yourcompany, DC=com, OU=sales`
   - **Cache MSAD Groups** – Enable caching of MSAD groups.
   - **Offline Sync** – Enable offline synchronization.
   - **Use SSL** – Select to use SSL for connections to the authentication server.

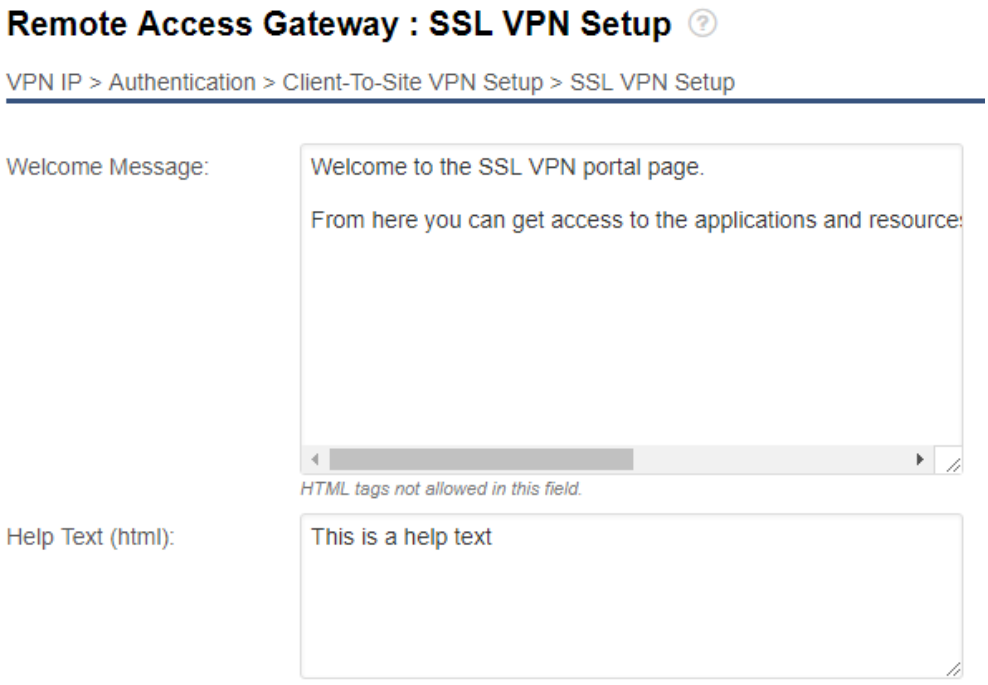
5. Click **Next**.
6. Configure the settings for client-to-site VPN:
   1. Enter a **VPN Policy Name**. This name is referred to as group name (iOS) or IPsec identifier (Android) on mobile VPN clients.
   2. In the **Client Network** field, enter an unused network in CIDR notation (e.g.,

192.168.222.0/24). IP addresses from this network will be assigned to connected VPN clients. Ensure that this network is not already defined on the **NETWORK > IP Configuration** page.

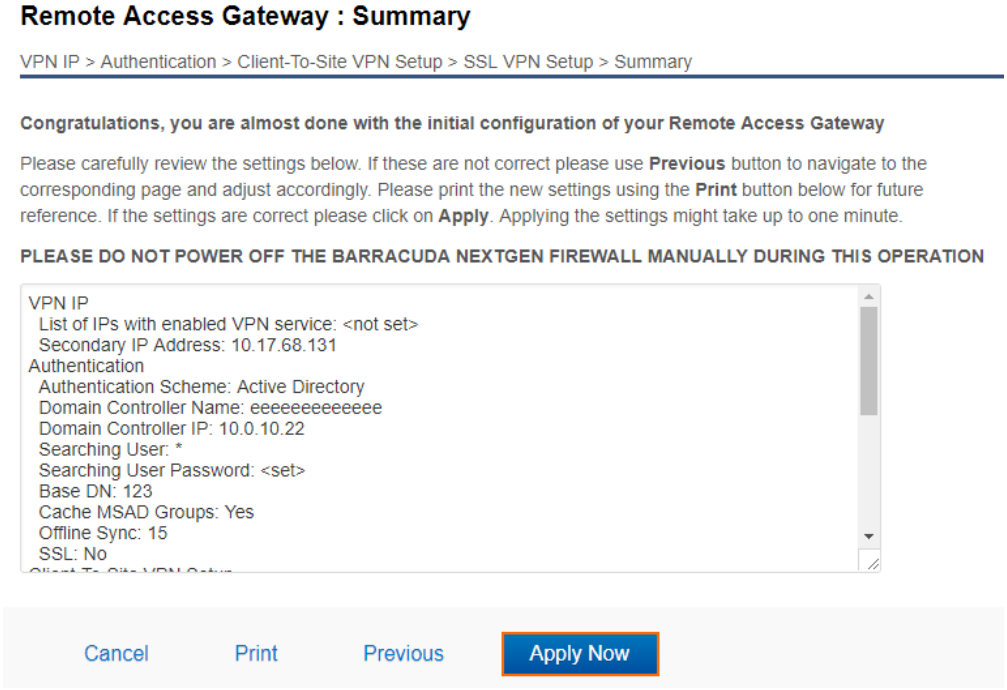
3. Enter a **Shared Key** to authenticate the client.
1. In the **Published Networks** field, enter all of the networks that the VPN clients will be able to access. Enter IP addresses and networks in CIDR format (X.X.X.X□X) and click **+** after each entry.



7. Click **Next**.
8. Configure the settings for SSL VPN:
   1. (optional) Customize the **Welcome Message** for the SSL VPN portal.
   2. (optional) Customize the **Help Text** to be displayed to the user. Only ASCII characters are allowed in the **Welcome Message** and **Help Text** fields.



9. Click **Next**. The Remote **Access Gateway: Summary** window opens.



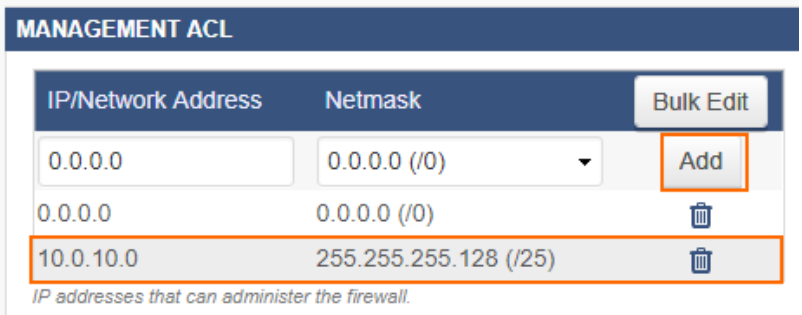
10. Review your configuration settings.
11. (optional) Click **Print**.
12. Click **Apply Now**.

Step 2. Configure the Administrator IP/Range

If administrators always use the same IP range, you can restrict access to the web interface of the firewall by specifying a range of allowed IP addresses or networks to increase security.

Misconfigurations of the administrator IP/range may cause the management web interface of the firewall to be unreachable. Contact Barracuda Networks Technical Support to recover connectivity.

1. Go to **BASIC > Administration**.
2. In the **Management ACL** section, enter the **IP/Network Address** and **Netmask** for the networks allowed to access the web interface. For a single IP address, set the **Netmask** field to **255.255.255.255**.
3. Click **Add**.



4. Click **Save**.

Next Steps

Configure the SSL VPN resources. For more information, see SSL VPN.

Figures

1. rag_wizard_00.png
2. rag_wizard_01.png
3. rag_wizard_02.png
4. rag_wizard_03.png
5. rag_wizard_04.png
6. rag_wizard_05.png
7. snmp_01_67a.png