Configure Network Obfuscation

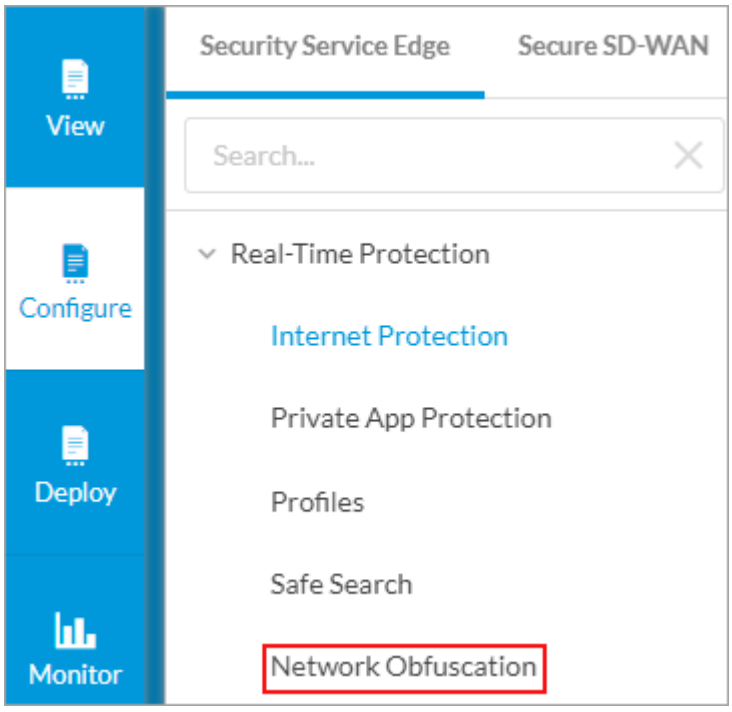
For supported software information, click here.

You can configure network obfuscation to hide the internal network topology and remote Versa SASE clients from each other. With network obfuscation, you can obscure the physical resource hosting the application (that is, the server IP address) from end users, thus helping to secure devices against attack vectors, such as port scanning and lateral movement.

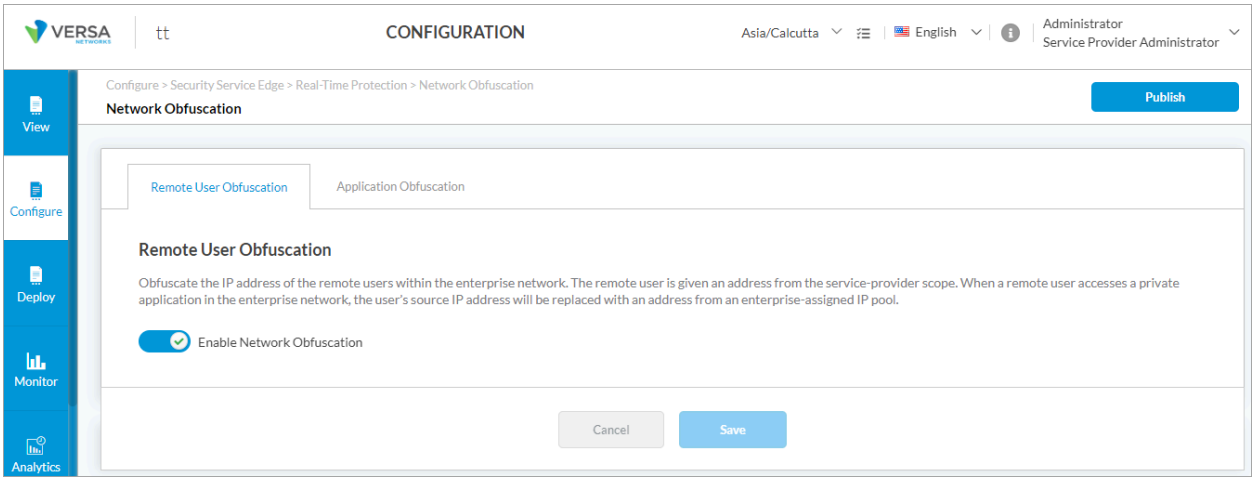
You can enable network obfuscation for remote Versa SASE clients and private applications. When you enable application obfuscation, you select the VPN instance name as the traffic source and one or more private applications. You can also create a group of applications to exclude from obfuscation.

To configure network obfuscation:

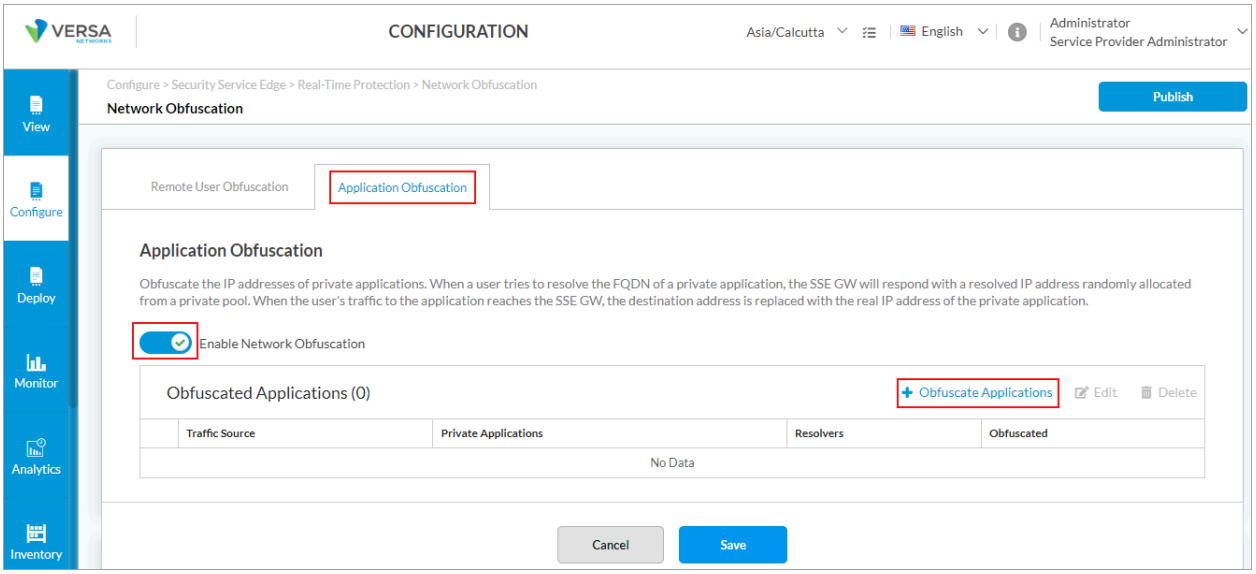
1. Go to Configure > Secure Services Edge > Real-Time Protection > Network Obfuscation.



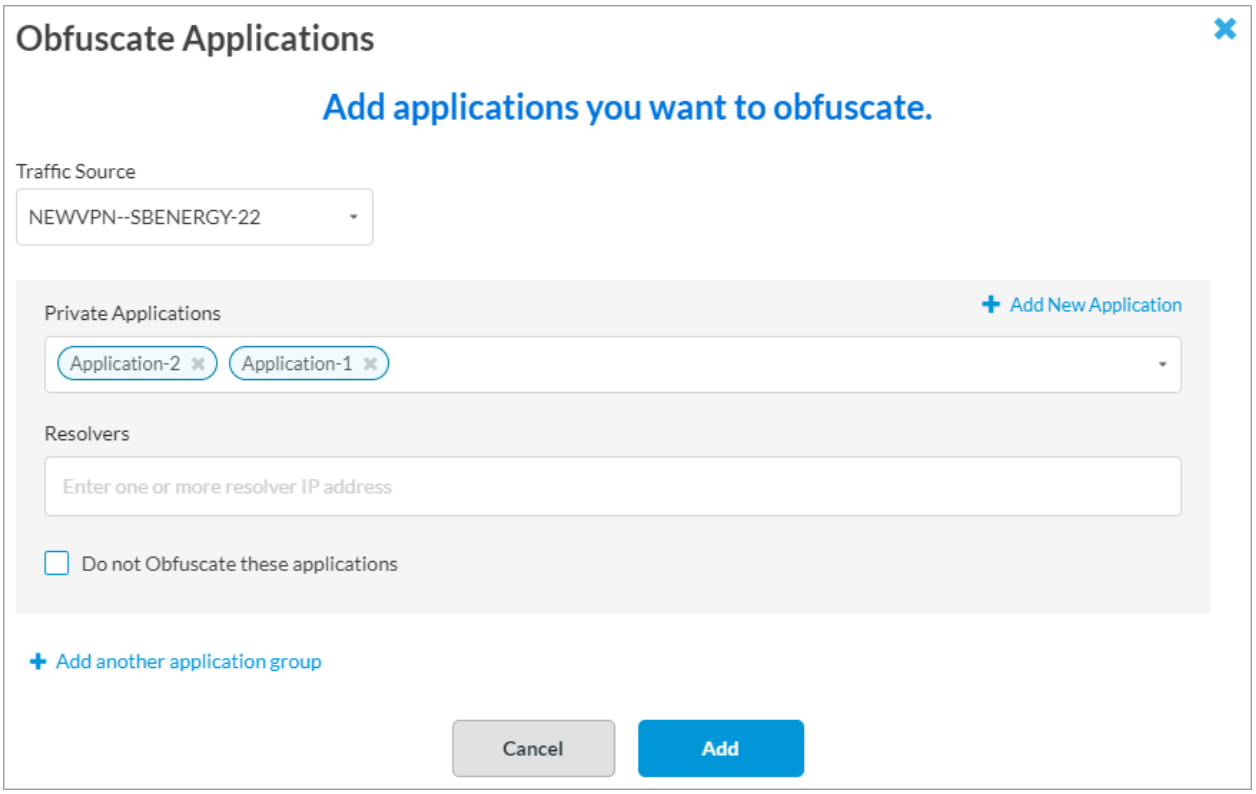
2. To enable remote user obfuscation, which obfuscates all Versa SASE client IP addresses from the remote servers, select the Remote User Obfuscation tab, and then slide the toggle to Enabled.



3. Click Save.
4. To enable obfuscation for an application, select the Application Obfuscation tab, and then slide the toggle to Enabled. When you enable application obfuscation, the selected applications are made intentionally unclear for all the tenant's users regardless of how they access gateways, that is, whether they are using the Versa SASE client, SD-WAN, or site-to-site tunnels.

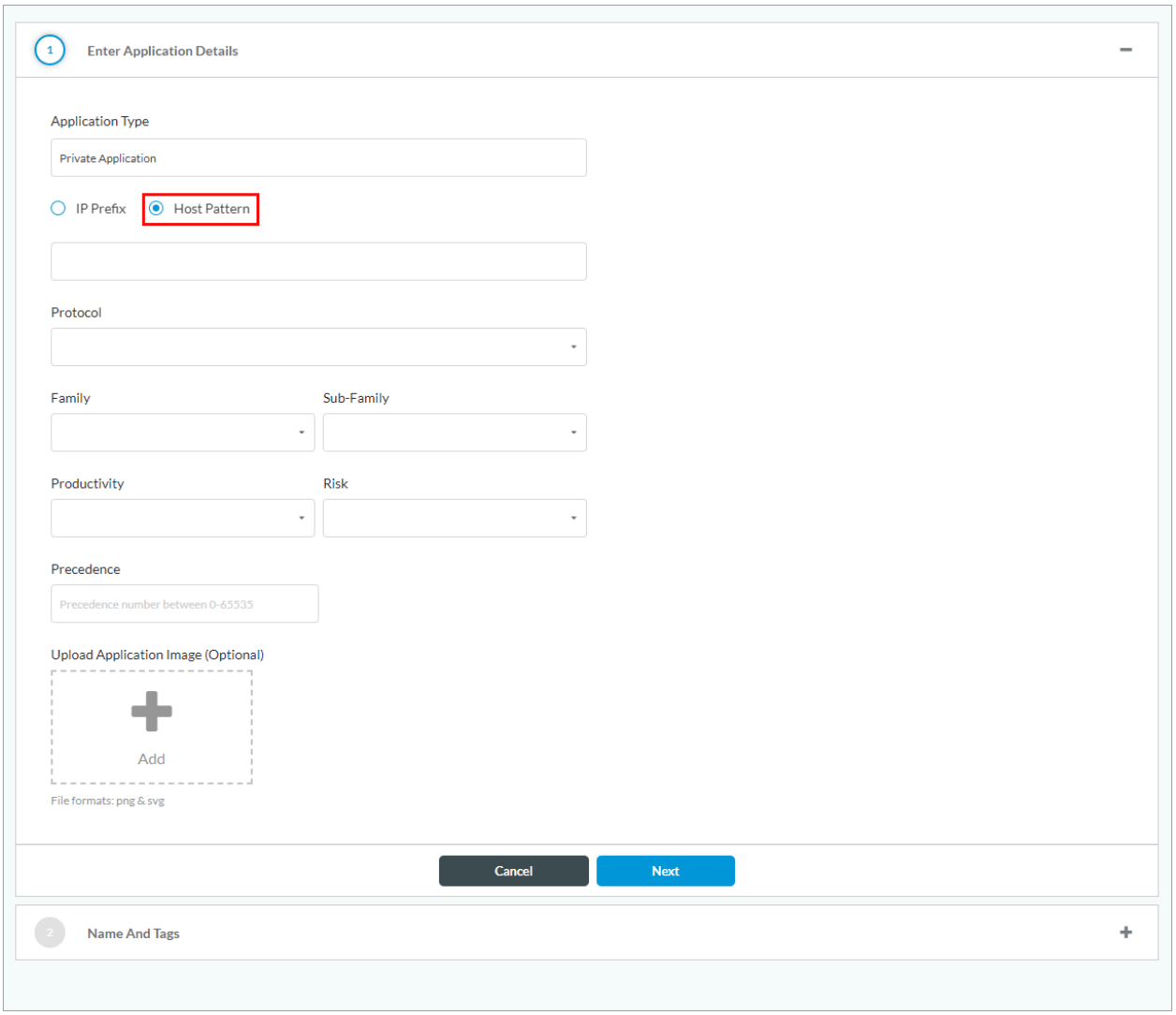


5. Click + Obfuscation Applications to select private applications to obfuscate or not to obfuscate. In the Obfuscate Applications screen, enter information for the following fields.

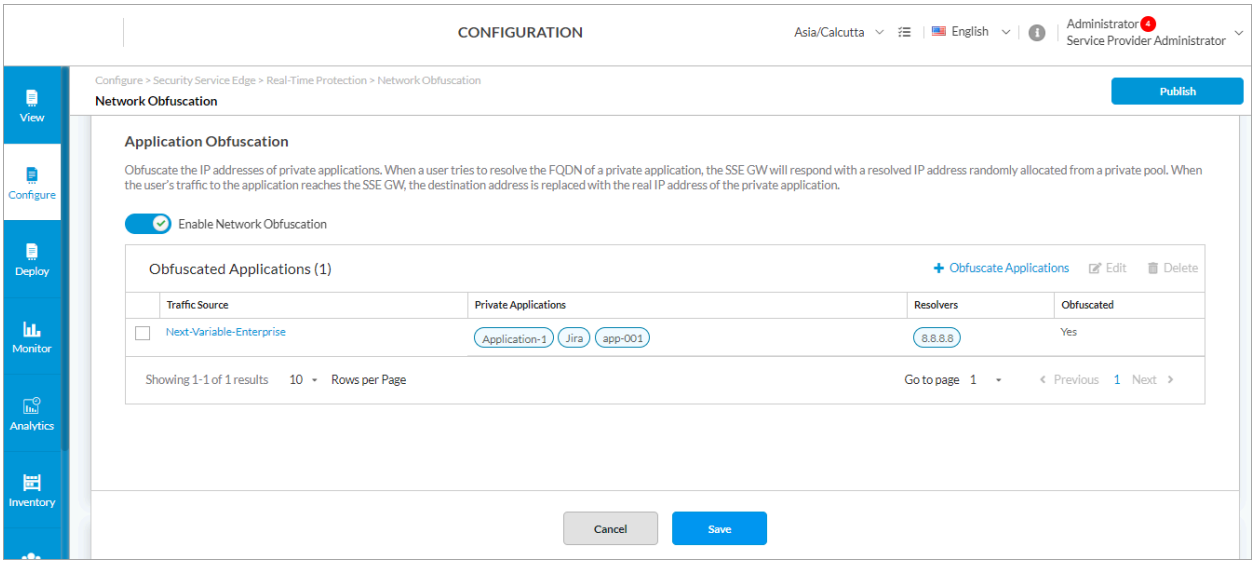


Field	Description
Traffic Source	Select the VPN instance as the traffic source.
Private Applications	Select one or more private applications. To add a new application, click + Add New Application. The Application screen displays. For more information, see Configure Private Applications.
Resolvers	Enter one or more DNS server resolver IP addresses for the private applications.
Do Not Obfuscate These Applications	Click to exclude the private applications you selected from obfuscation.

6. Click + Add Another Application Group to create another group of private applications with different resolvers or a different obfuscation choice. For more information, see Configure SASE Private Application Protection Rules.
7. To add a private application, click + Add New Application. The Application screen displays.



8. Select Host Pattern. Note that only applications with a configured host pattern are displayed in the Private Applications field in the Obfuscate Applications window. Applications with a configured IP prefix are not displayed.
9. For information about configuration other parameters, see Configure SASE Private Application Protection Rules.
10. Click Add. The Application Obfuscation dashboard displays the configuration for each set of private applications.



11. Click Save.

Supported Software Information

Releases 11.4.1 and later support all content described in this article.

Additional Information

Configure SASE Private Application Protection Rules
Configure SASE User-Defined Objects