

## How to Create and Apply User Objects for VPN Users

<https://campus.barracuda.com/doc/96026269/>

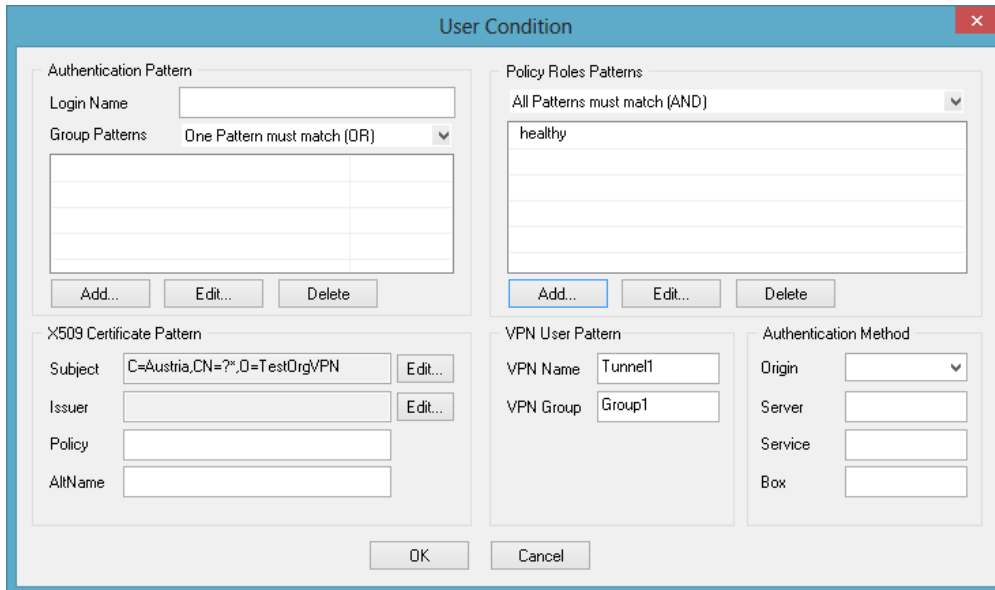
In user objects, you can enter either X.509 certificate patterns or VPN user patterns to reference VPN users and groups. With use of the [Barracuda Network Access Client](#), you can also reference users by policy role patterns.

Combining fields is also possible. For example, you can enforce a VPN connection, by entering required VPN user patterns and require a matching X.509 certificate to be installed in the browser application by entering required X.509 certificate patterns.

### Create a User Object for VPN Users

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, select **Users and Groups**.
4. Right-click the table and select **New**.
5. In the **Edit/Create User Object** window, enter a **Name** for the user object. E.g., VPN Users
6. Click **New** to add a user condition. The **User Condition** window opens.
7. If you are using the [Barracuda Network Access Client](#), enter the policy roles patterns in the **Policy Roles Patterns** section.
  1. Select the required condition from the list.
  2. Click **Add** and select one or more patterns. If a condition must not apply, select the **Negative Match** check box.
8. To use a certificate, click **Edit** in the **X509 Certificate Pattern** section and specify the certificate conditions:
  - **Subject/Issuer** – The subject/issuer of the affected X.509 certificate.

If multiple subject parts (key value pairs) are required, separate them with / (for example, OU=test1 and OU=test2 are required, select OU and enter test1/test2). Using wildcards (?, \*) is allowed. Take into consideration that order is mandatory.
  - **Policy/AltName** – The ISO number and the SubjectAltName according to the certificate.
9. If applicable, enter the required VPN login and group policy the object has to apply to in the **VPN User Pattern** section:
  - **VPN Name** – The required VPN login name. Using wildcards (?, \*) is allowed. For example, enter \*username\* when using external authentication.
  - **VPN Group** – The required VPN group policy that the object has to apply to.
  - **Authentication Method** – In this section, you can specify the following settings:
    - **Origin** – Defines the type of originator (see [User Objects](#)).
    - **Service/Box** – Allows enforcing authentication on a certain service/box.



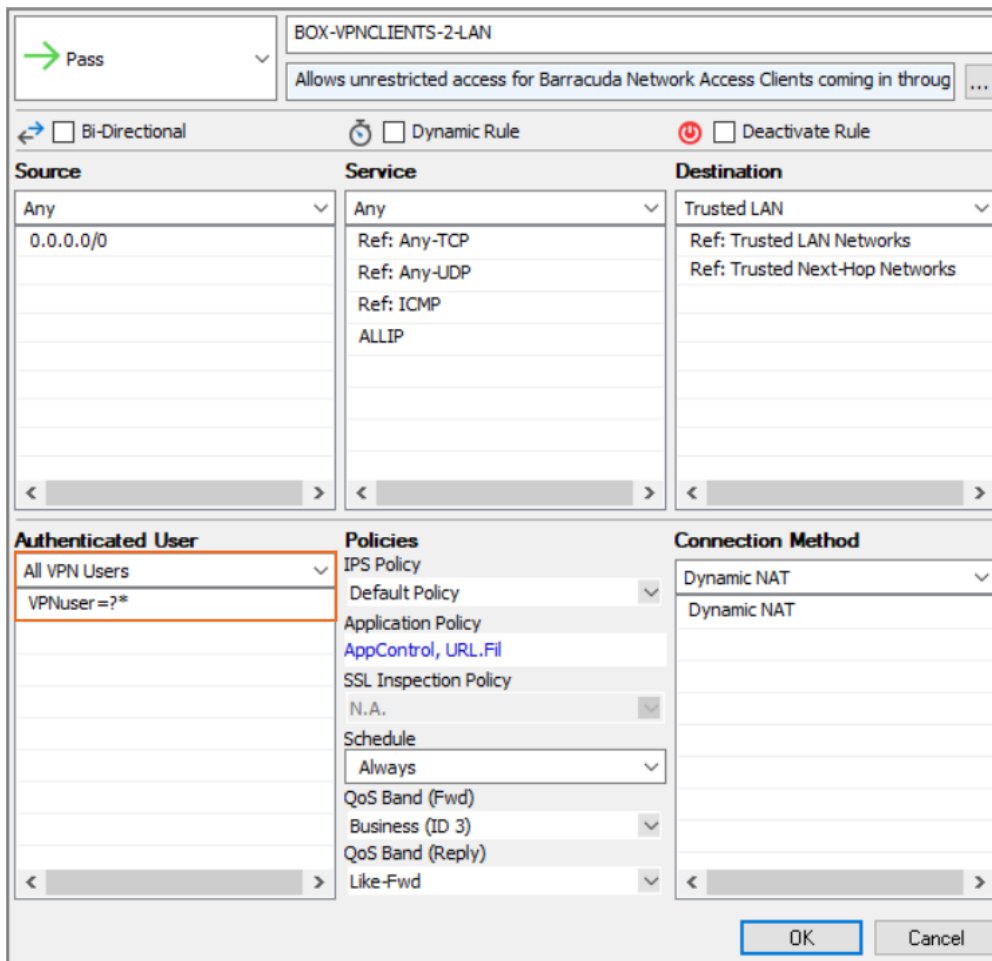
The 'User Condition' dialog box is used to define user authentication patterns. It contains several sections: 'Authentication Pattern' with fields for 'Login Name' and 'Group Patterns' (set to 'One Pattern must match (OR)'); 'Policy Roles Patterns' with a dropdown set to 'All Patterns must match (AND)' and a list containing 'healthy'; 'X509 Certificate Pattern' with fields for 'Subject' (C=Austria,CN=?\*,O=TestOrgVPN), 'Issuer', 'Policy', and 'AltName'; 'VPN User Pattern' with fields for 'VPN Name' (Tunnel1) and 'VPN Group' (Group1); and 'Authentication Method' with fields for 'Origin', 'Server', 'Service', and 'Box'. Buttons for 'Add...', 'Edit...', and 'Delete' are present for the pattern lists. 'OK' and 'Cancel' buttons are at the bottom.

10. Click **OK**.
11. After you specify the conditions for all of the users that you want to include in this object, click **OK** to create the user object.
12. Click **Send Changes** and **Activate**.

If you are using Offline Authentication, ensure that user-specific rules are sequenced after the fwauth rule. For more information, see [How to Configure Offline Firewall Authentication](#).

## Apply a User Object to an Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Edit the access rule that you want to apply the user object to.
4. From the **Authenticated User** list, select the user object.



→ Pass

BOX-VPNCLIENTS-2-LAN

Allows unrestricted access for Barracuda Network Access Clients coming in through ...

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
Any	Any	Trusted LAN
0.0.0.0/0	Ref: Any-TCP	Ref: Trusted LAN Networks
	Ref: Any-UDP	Ref: Trusted Next-Hop Networks
	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
All VPN Users	IPS Policy	Dynamic NAT
VPNUser=?*	Default Policy	Dynamic NAT
	Application Policy	
	AppControl, URL.Fil	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	Business (ID 3)	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

## Figures

1. VPN\_user\_object.png
2. user\_obj\_rule.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.