Access Control

https://campus.barracuda.com/doc/2458424/

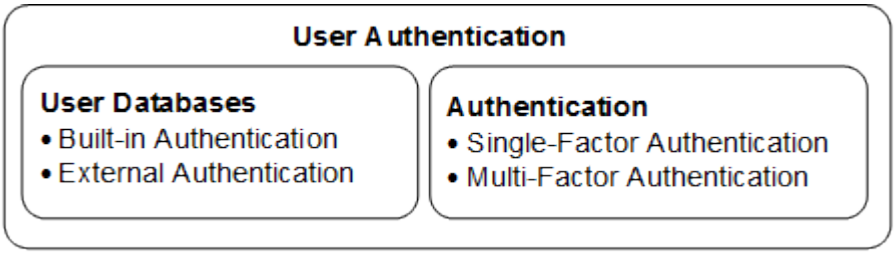
To access and use the resources provided by the Barracuda SSL VPN, a user must be able to authenticate. Additionally, the user´s device must adhere to any configured network access control (NAC) policies. You can configure user authentication as either a single- or multi-factor process, using a combination of information stored in the authentication services and additional authentication procedures defined in the Barracuda SSL VPN. After users log in, the levels of access and privileges assigned to them on a per-resource basis are defined by the policies that you configured.

User databases

Users and groups can be stored locally on the Barracuda SSL VPN´s built-in user database or retrieved from external authentication servers. User databases define where user information is stored. The Barracuda SSL VPN 380 and above can use multiple user databases. You can configure every user database with global access rights and delegate some Super User responsibilities to management users in the user database.

For more information, see How to Configure User Databases.

Authentication



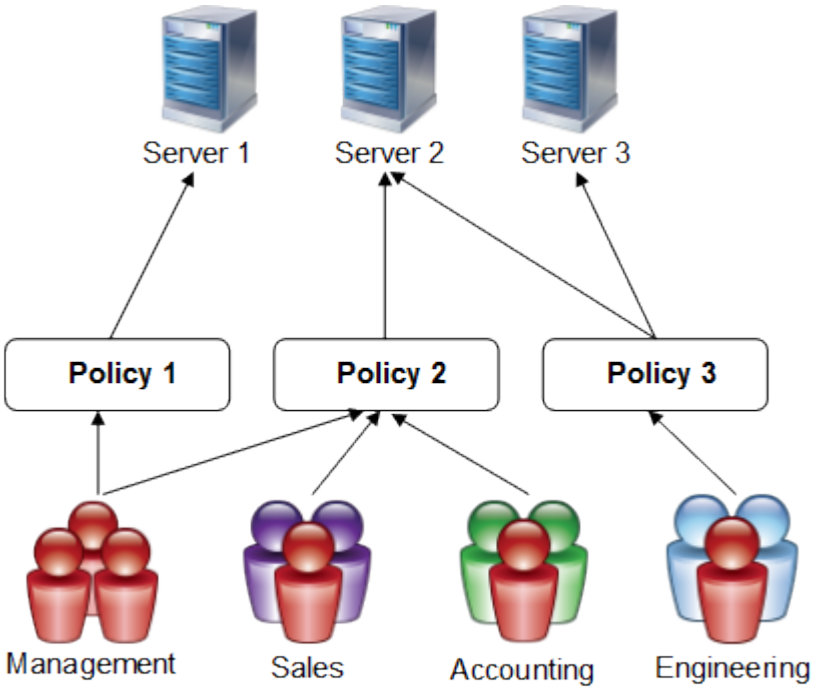
User authentication is not limited to password authentication. For greater security, the Barracuda SSL VPN provides multi-factor authentication. You can choose to activate a combination of the following authentication procedures:

- One-time passwords (sent via SMS or email)
- Authentication key
- Client certificates
- IP authentication
- PIN
- Security questions

- RADIUS
- Hardware token authentication (in combination with RADIUS or Client Certificates)

For more information on the available authentication schemes, see Authentication Schemes.

Policies



Policies are lists of users and groups that are attached to resources. Users can only access a resource if they are included in the policy attached to the resource. A resource can include multiple policies that contain separate lists of users and groups. You can grant different users with varying levels of access to a resource by assigning Access Rights to the user or group. To help you easily assign resources to everybody, a built-in **Everyone** policy is included by default. You can delete the **Everyone** policy, locking out out all users who do not have a specific Profile, Authentication Scheme, or Access Right assigned to them. It is recommended that you create policies for every distinct user group. For example, in a company with three departments, you can create separate policies for each department, management user, and administrator.

For more information on Policies, see How to Configure Policies.

Network Access Control (NAC)

Network access control limits access to network resources, according to a variety of factors that are not connected to the user. Users who fail the NAC check are not allowed to log in until they have a conforming system. You can define exceptions for single users, so that they can continue using the service until they have time to update their system. User systems are evaluated by the following parameters:

- Time of day
- Operating system (type and if it is up-to-date)
- IP and MAC address
- Browser type and version
- Antivirus state (installed/up-to-date)
- Firewall
- Version of plugins installed
- Type of connection (Wi-Fi)
- Domain membership

To configure NAC, go to **Manage System > ACCESS CONTROL > NAC**. To define exceptions, go to **Manage System > ACCESS CONTROL > NAC Exceptions**.

Figures