SSL VPN Access Control Policies

https://campus.barracuda.com/doc/73719135/

Access Control Policies (ACPs) provide granular control over access to the SSL VPN by qualifying users based on the following information: the groups they belong to, the technology they use, and how they authenticate. Users can be added to groups to differentiate between roles. Information about operating system, browser, and browser plugin versions helps to distinguish the various technologies and authentication methods employed by users from different clients.

Technologies such as MS-AD, RADIUS, and LDAP contain the core authentication information in username/password pairs in terms of an identity scheme. One or more authentication schemes can be defined when creating an Access Control Policy. SSL VPN network access control (NAC) criteria can be used to restrict the availability of an Access Control Policy based on the user's operating system, browsers, and browser plugins. Applications like CudaLaunch can also be part of such NAC criteria. Informal attributes like Block exclude users from authenticating with a special technology; Allow grants access in case all additional authentication criteria are met when logging in. Where both Allow and Block are defined, Allow has the higher priority over Block.

In order to maximize flexibility, multiple Access Control Policies can be created and used for authentication.

Multi-Factor and Multi-Policy Authentication

Multi-Factor Authentication (MFA) and Multi-Policy Authentication (MPA) are two methods of using Access Control Policies.

- Multi-Factor Authentication evaluates the username and password against multiple authentication schemes within an Access Control Policy.
- Multi-Policy Authentication evaluates which Multi-Factor Authentication the user may select to authenticate with based on the username and user information (group membership, NAC).

For more information, see How to Configure Access Control Policies for Multi-Factor and Multi-Policy Authentication.

Google Authenticator

Google Authenticator is an authentication method based on the Time-Based One-Time Password algorithm (TOTP).

For more information, see How to configure Access Control Policies for Google Authentication.