Authentication

https://campus.barracuda.com/doc/96026625/

Beyond its powerful network firewall and VPN technologies, the Barracuda CloudGen Firewall provides seamless integration with all authentication methods (e.g., Active Directory, RADIUS, LDAP/s, etc.) to facilitate policy configuration based on the actual user and group information and not just IP addresses. User visibility and control is a significant factor for handling network traffic and creating policies. If you do not have an external authentication server available, you can create and maintain a list of local users and groups on the CloudGen Firewall. The firewall can also use the Barracuda DC Agents on the MSAD server and the Barracuda Terminal Server Agents on the Microsoft Terminal server to provide fully transparent user authentication.

You can use local and external authentication for the following services and features:

- Forwarding Firewall and Firewall Authentication
- HTTP Proxy
- URL Filter
- VPN Service (C2S VPN and SSL VPN)
- Access Control Service
- Administrator Accounts

External Authentication

By integrating the CloudGen Firewall with your authentication server, you can configure policies that apply to specific users and groups. The firewall lets you configure a range of external authentication schemes, such as

- Microsoft Active Directory (MSAD)
- Barracuda DC Agent
- MS-CHAP
- SAML/ADFS Authentication
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial In User Service (RADIUS)
- Terminal Access Controller Access Control System (TACACS+)
- RSA-ACE SecurID
- MSNT
- Barracuda Web Security Gateway
- Barracuda Terminal Server Agent
- How to Configure Access Control Policies for One-Time Password Authentication
- Wi-Fi AP Authentication
- Time-based One-time Password (TOTP)
- Online Certificate Status Protocol (OCSP)

- Kerberos

Local Authentication

If no external authentication service is available, NGF Local Authentication locally manages users and groups on your CloudGen Firewall.

For more information, see: How to Configure NGF Local Authentication.

Authentication Redirection

Authentication redirection is used when a CloudGen Firewall or a Control Center serves as an authentication proxy and forwards credentials from a CloudGen Firewall to a specific authentication server.

For more information, see How to Redirect Authentication from a CloudGen Firewall to a Specific Authentication Server.

© 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.