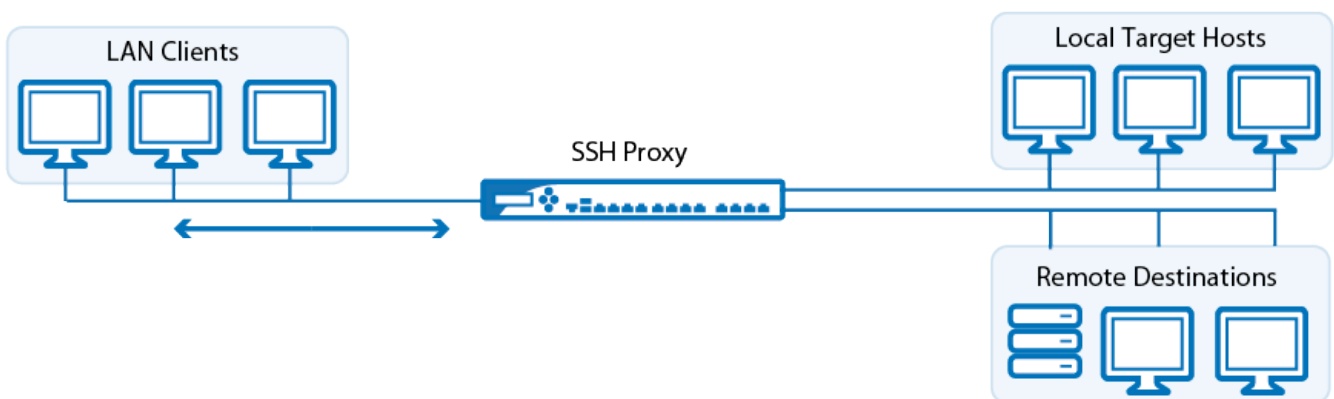


SSH Proxy

<https://campus.barracuda.com/doc/48202911/>

The SSH Proxy service of the Barracuda NextGen Firewall F-Series allows regulating SSH connections. Users can establish SSH sessions over the firewall and connect to remote servers/hosts, e.g., to perform administrative tasks without having to remember login credentials and IP addresses at the target. The SSH Proxy service supports a range of useful features, like user authentication at the gateway via external authentication schemes, public key authentication at the target system, permission profile assignment and DoS protection by configurable login grace time and session limits. The SSH Proxy prevents firewall policy evasion by preventing protocol tunneling inside SSH connections. However, X11 connection forwarding allowed.

Implementing the SSH Proxy Service on the Barracuda NextGen Firewall F-Series



SSH Proxy Configuration

The SSH Proxy service provides configurable SSH protocol support for accessing target systems (v2-only, or v2 and v1). You can specify the port and a local source IP address or hostname (to use policy routing) from which remote systems can be accessed. Target access lists allow definition of target hosts for selection. Additionally, you can configure the reverse DNS lookup behavior of the server for accessing clients, specify client and server alive times, compression and session limits and timeouts.

For more information on how to configure the SSH Proxy service on the F-Series, see [How to Configure the SSH Proxy](#).

Authentication and Access Control

The SSH Proxy service supports user authentication via all configurable and meaningful authentication schemes (not OCSP) with user and password combination. No local user database is required, access is configurable based on group policies, and individual known_hosts files are created for each user. The SSH Proxy service allows you to create default and custom permission profiles where you can specify monitoring settings such as optional session and activity tracing for certain users (console output cloning to file), access control settings based on policies, and configurable network permissions and restrictions.

For more information on how to create permission profiles, see [How to Configure Permission Profiles](#).

Logging

In the SSH Proxy service configuration, you can specify the server and client log level (ssh-client) according to your company's requirements. Log entries are accessible under the Barracuda NextGen Firewall F-Series **Logs** tab.

Figures

1. fw_ssh_proxy.png

© Barracuda Networks Inc., 2019 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.