Administration

You can use already existing services in your network, such as DNS, NTP or SCEP servers, when deploying the Barracuda NextGen F-Series Firewall. The F-Series supports multiple administrator accounts and restricting access based on source IP address or network.

Administrators

An administrator account on an F-Series Firewall contains multiple parameters that specify the permissions and restrictions for an administrator. Administrator rights are split into predefined administrative roles, defining which services an administrator is allowed to use and which operations the administrator is allowed to perform within the different services.

For more information, see Managing Access for Administrators.

Changing the Root Password and Management ACLs

The Management ACL specifies which IP addresses can access the system. In the system access configuration, you can also change the password for the *root* user.

For more information, see How to Change the Root Password and Management ACL.

Administrative Session Time Limits

Session timeouts mitigate the security risk from authenticated, unsupervised connections to the firewall by defining the session time-out for idle administrative sessions. After the session has been terminated, the admin has to log in again.

For more information, see How to Set Idle Administrative Session Time Limits.

DNS

Introduce either a network DNS server or a DNS server assigned by your ISP on the firewall. When resolving DNS requests, the F-Series can alter the response (DNS Interception) and redirect or block queries for specific domains by using black and whitelisting. You can use the same namespace internally and externally and redirect external clients to use one IP address, and internal clients to use an internal path to the same hostname (Split DNS). DNS queries can be forwarded to or cached from the DNS server.

For more information, see How to Configure DNS Settings and How to Configure DNS Interception.

NTP

You can define one or more NTP server(s) to act as a master clock for the firewall. The current time on the system is synchronized via Network Time Protocol (NTP). Time settings apply to all time-related services on the F-Series and affect data accounting, logging, and event notifications. Correct time settings are also important for HA synchronization.

For more information, see How to Configure Time Server (NTP) Settings.

Global HTTP Proxy Settings

To configure the F-Series Firewall to connect to the Internet via a proxy server, specify global connection and authentication settings for your system.

For more information, see How to Configure Global HTTP Proxy.

Email Notifications

Some services, such as the virus scanner, can send email notifications. You can configure the email address and the SMTP server used to for email notifications.

For more information, see How to Configure System Email Notifications.

SCEP

The SCEP (Simple Certificate Enrollment) protocol supports secure certificate issuing. You can configure the F-Series Firewall to use an SCEP server to use in TINA or IPsec Site-to-Site VPN tunnels.

For more information, see How to Configure SCEP Settings.