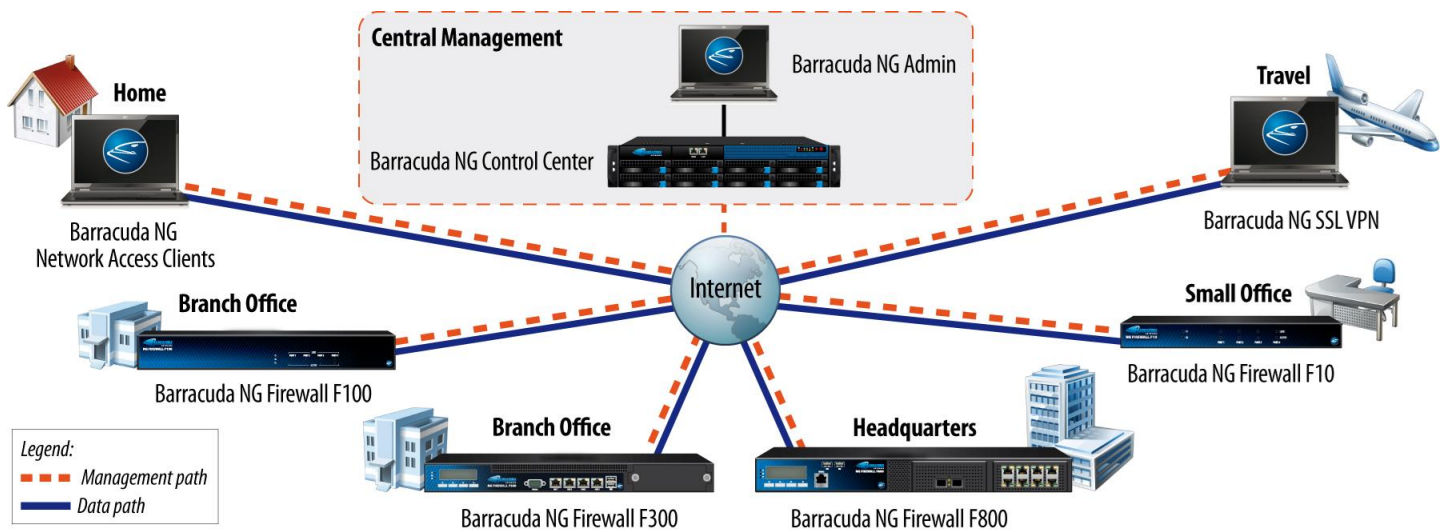


Scope of this document

This document is intended for Barracuda Partners and users who are new to Barracuda NG Firewall and would like to test and review a standalone F201 Barracuda NG Firewall appliance and its core features. For further information and deeper understanding we recommend consulting the [Barracuda NG Firewall Administration Guide](#), the [Barracuda NG Firewall Quickstart Guide](#) or the [Barracuda NG Firewall Quick Configuration Guide](#) which are available from the download portal login.barracuda.com.

1. Introduction: The Next Generation Firewall Designed for Distributed Environments

The Barracuda NG Firewall extends the next generation firewall concept by adding application aware traffic routing and prioritization across the wide area network (WAN), thus optimizing performance and availability. Beyond its powerful network firewall and VPN technologies, the Barracuda NG Firewall integrates a comprehensive set of next generation firewall technologies including identity aware Layer 7 Application Control, Intrusion Detection and Prevention, Web filtering, Anti-Virus and Anti-Spam as well as a comprehensive Network Access Control solution. Industry leading capabilities for centralized management and scalability clearly distinguish the Barracuda NG Firewall from other next generation firewalls and make it the ideal solution for distributed network environments.



Improved Security Posture: From a security perspective, organizations can improve their security posture by integrating previously disparate security functions, including Web filtering, malware protection, email security, intrusion prevention, and layer 7 application profiling into a single firewall-based platform.

Corporate Network Optimization: From a global network management standpoint, they can reduce administrative overhead through centralized management capabilities that serve thousands of nodes and reduce hard dollar costs by better managing WAN links and link bandwidth.

Accelerated Troubleshooting: At a help desk and troubleshooting level, the Barracuda NG Firewall provides unprecedented levels of visibility into individual network flows, arming the network engineer with powerful tools to diagnose and maintain the network.

2. Getting Started

This chapter describes the steps necessary to deploy the Barracuda NG Firewall appliance in your laboratory environment how to establish a connection to your network; and how to import the licenses which are needed for the full scope of evaluation operations.

Deployment Options

The Barracuda NG Firewall evaluation appliance is shipped pre-staged with all services and configurations that are necessary to start the evaluation process immediately:



Pre-staged PORT Connectivity Configurations:

- PORT 1: pre-configured DHCP network (dynamically assigns IP addresses from the pool between [192.168.200.1](#) to [192.168.200.16](#))
- PORT 2: no special pre-staged configuration
- PORT 3: no special pre-staged configuration
- PORT 4: pre-configured DHCP client from your existing network for WAN IP address assignment
- WiFi: pre-configured WiFi network (dynamically assigns IP addresses from the pool between [192.168.201.1](#) to [192.168.201.24](#))



Configuration:

In order to connect the F201 to your network, please follow the instructions of the [Quick Configuration Guide](#), available for download at <http://www.barracudanetworks.com/ns/support/documentation.php>

Licensing

Once connected to the Firewall you will need to activate the licenses. This is an automatic process you can view on the Status page. Licensing can also be manually completed by clicking the link on the status page next to “Activation” located in the Application window.

In the event that your evaluation appliance is shipped without licenses (e.g. due to export restrictions) please follow the steps below or consult the [Barracuda NG Firewall Quick Configuration Guide](#), available for download at <http://www.barracudanetworks.com/ns/support/documentation.php>

- Step 1: Connect to your Barracuda NG Firewall with the [Barracuda NG Admin](#) application.
- Step 2: In the now appearing [Status](#) page, click  [Configuration](#) located within the  [Services](#) area.
- Step 2: In the now appearing [Config](#) page, click  [Licenses](#) located within the [Device Configuration](#) area.
- Step 4: Click , select [Import from File...](#) and import all available licenses for your Barracuda NG Firewall.
- Step 5: Click in the upper-right area to confirm the license import process.

3. Suggested Tests for Functional Evaluation

| ADMINISTRATOR ROLE | USER ROLE | EXPECTED RESULT |
|---|---|---|
| Firewall & Layer 7 Application Control | | |
| Your evaluation unit comes with several Layer 7 Application Control default settings in order to test the detection blocking and throttling of several protocols and applications. In case you want to change these settings, click on the respective firewall rule and changes these settings in the Application/IPS section respectively. A complete list of supported protocols and applications is available under www.barracudanetworks.com | | |
| Blocking of BitTorrent filesharing. | Start your BitTorrent client (e.g. eDonkey, Azureus, Limewire, etc.) and start a download. | Download will be blocked. Browse to the History view and watch the displayed result. |
| Blocking of AOL Instant Messenger traffic. | Start AIM and start chatting with another client. | Chatting will be blocked. Browse to the Firewall History view and watch the displayed result. |
| Allow MSN chat but block MSN file transfer. | Start MSN application and try to transfer a file to another MSN client. | MSN chat will be allowed, the file transfer will be blocked. Browse to the Firewall History view and watch the displayed result. |
| Allow Skype traffic and have the usage detected. | Start Skype on your client, logon and start a Skype VoIP session. | Skype traffic will be shown in the Firewall Live and History view. To narrow down the displayed traffic filter for your IP or the service *skype*. |
| Allow HTTP embedded Flash streaming but throttle its dedicated bandwidth to 100Kbit/s. | Browse to known Flash site like youtube.com or myspace.com and start a stream. | HTTP embedded Flash streaming will be allowed. To narrow down the displayed traffic filter for your IP or the Service *stream*. |
| Block HTTP embedded Flash streaming. | Open the firewall rule LAN-to-Internet-STREAMING , click on Application/IPS on the left hand side and change the Policy from Throttle Bandwidth to Drop Traffic . Commit the change by clicking on Send Changes and Activate and browse again to youtube.com or a similar site and start a stream. | HTTP embedded Flash streaming will be blocked. Watch the result in the Firewall History view. The filter set earlier should be still active. In case you have changed the display filter set a filter for e.g. your IP or the Service "stream" in order to narrow down the display. |
| Block Windows Media Streaming. | Open the Windows Media Player on your client and start a stream. | The Windows Media Stream will be blocked. |
| Allow Facebook but block the usage of Facebook Apps (e.g. Mafiawars, Farmville, etc.) | Browse to facebook.com and logon. Search for Mafiawars and start the application. | Facebook activities (e.g. searching for friends or companies) are allowed. The usage of applications such as Mafiawars is blocked. A block page will be displayed. |
| Blocking of Direct-Download-Links and related file sharing. | Browse to a known DDL Web site like rapidshare.com or similar Web sites and try to upload a file (recommendation: prepare a test word doc or use a mp3 file). | Upload will be blocked. |
| Allow FTP file download. | Browse to a FTP server like ftp://ftp.mozilla.org/ and start a file download | FTP file download is allowed. The active session can be viewed in the Firewall Live display. |
| Block FTP file download. | Open the rule FTP download and change the ACTION type from ALLOW to BLOCK . Commit your changes by clicking Send Changes and Activate . Browse to a FTP server like ftp://ftp.mozilla.org and start a file download | FTP file download is blocked. The blocked session can be viewed in the Firewall History display. |

| Troubleshooting & Diagnostics | | |
|---|--|---|
| Find out what a specific user is doing at the moment. | Browse to the Live view and filter for your IP address. | A list of real-time session related to your IP will be displayed. |
| Find out what a specific user has done in the past. | Browse to the Firewall History view and filter for an IP address. | A list of past activities related to an IP will be displayed. Double click any session to open a detailed summary of the respective session. |
| Re-prioritize an active SSH session by assigning the quality traffic shaping connector on-the-fly | Copy a file by using WinSCP to a target system. Open the Firewall Live view, filter for Service SSH and assign a new forward shaping connector premium to the session by right clicking the session. | The session will be prioritized in terms of its allocated bandwidth. |
| Terminate an active SSH session by using the Firewall Live view. | Right click the session you started earlier and choose Terminate Session . | Session will be terminated immediately. It will be erased from the Firewall Live view. The WinSCP application will stop copying the file. |
| Barracuda NG Malware Protection | | |
| Detect and block a virus infected download. | Download sample virus file from eicar.org or similar web sites. | Downloads will be blocked. |
| Detect and block the download of files that include spyware and ad-ware. | Download sample spyware file from spycar.org/Spycar.html or similar Web sites | Downloads will be blocked. |
| Barracuda NG Webfilter | | |
| Block a certain website category. | Switch to the Webfilter configuration (Simple Configuration View > URL Filter) and add a blocked category e.g. Job_Search . After committing the changes (click Send Changes and Activate) browse to e.g. www.monster.com | The requested web page will be blocked. |
| Traffic Shaping | | |
| Change bandwidth according to your connection item. | Open the Traffic Shaping user interface and enable Traffic Shaping and assign the desired bandwidth by double clicking the network interface , shaping should be performed on. | Basic Traffic Shaping will be performed by limiting the bandwidth of the desired network interface. Active Traffic Shaping can be viewed in real-time in the Firewall Shaping view. |
| Shape FTP download by using a shape connector. | Open the Traffic Shaping user interface and assign the default template Linking up your Company to the desired network interface. Open an existing or create a new firewall rule that handles FTP traffic and assign the shaping connector bulk in the Forward Shaping drop-down menu. | FTP traffic will be shaped according the Traffic Shaping policy defined in the default profile Linking up your Company . Active Traffic Shaping can be viewed in real-time in the Firewall Shaping view. |