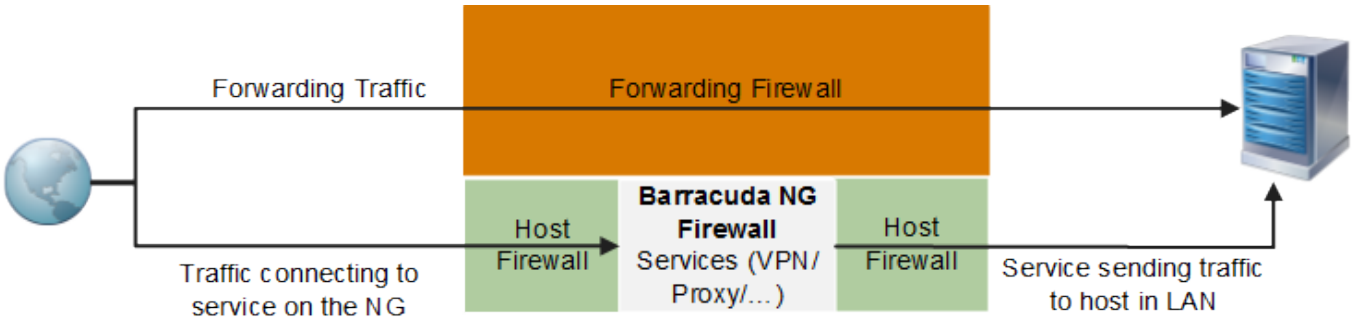
Firewall

https://campus.barracuda.com/doc/43846953/

The Barracuda NG Firewall comes with two firewall services, one for handling local inbound/outbound traffic and the other for handling all forwarding traffic. The Host Firewall service runs on the box layer and cannot be removed. The Forwarding Firewall service can be added to one virtual server on every NG Firewall.



The Host and Forwarding Firewall can handle only IP protocols. Non-IP traffic (such as Spanning Tree Protocol or IPX/SPX) is not forwarded.

Forwarding Firewall

The Forwarding Firewall handles all traffic for which the destination does not match with a listening socket on the Barracuda NG Firewall. You can create one (forwarding) Firewall service on each NG Firewall. This service listens to all IP addresses configured for the virtual server and is responsible for all connections that must be transferred over the Barracuda NG Firewall to a remote host. The firewall rules for the Forwarding Firewall are maintained in the forwarding ruleset. The Forwarding Firewall is tightly integrated with Application Control 2.0, Virus Scanners, Advanced Threat Detection (ATD), Intrusion Prevention System (IPS), and the URL Filter. Examples of connections that use the Forwarding Firewall are:

- A web browser that connects to an external web server without using the HTTP Proxy service on the Barracuda NG Firewall
- The administrator pings an external Linux server
- Incoming and outgoing traffic coming out of a VPN tunnel

For more information, see Forwarding Firewall.

Host Firewall

There is one Host Firewall service running on the box layer of every Barracuda NG Firewall and Barracuda NG Control Center. Host Firewall rules are applied to connections where the target IP address and port number match a listening socket of a service on the Barracuda NG Firewall. The **boxfw** service manages this ruleset and additional traffic handlers such as SIP, RPC, Timer, Audit, Trace, and Sync. Restarting the **boxfw** service reinitializes the service handlers and reloads the ruleset. The **boxfw** service is automatically activated on the Barracuda NG Firewall. You can have only one Host Firewall on a system. Examples of connections that are handled by the Host Firewall are:

- An incoming connection from a web browser to the HTTP Proxy service running on the Barracuda NG Firewall
- An outgoing connection from the HTTP Proxy service running on the Barracuda NG Firewall to a web server on the Internet
- Outgoing and incoming VPN traffic from the Barracuda NG Firewall VPN service to the tunnel endpoint
- Outgoing NTP or DNS queries

For more information, see Host Firewall.

Figures

1. FW_host_FF.png