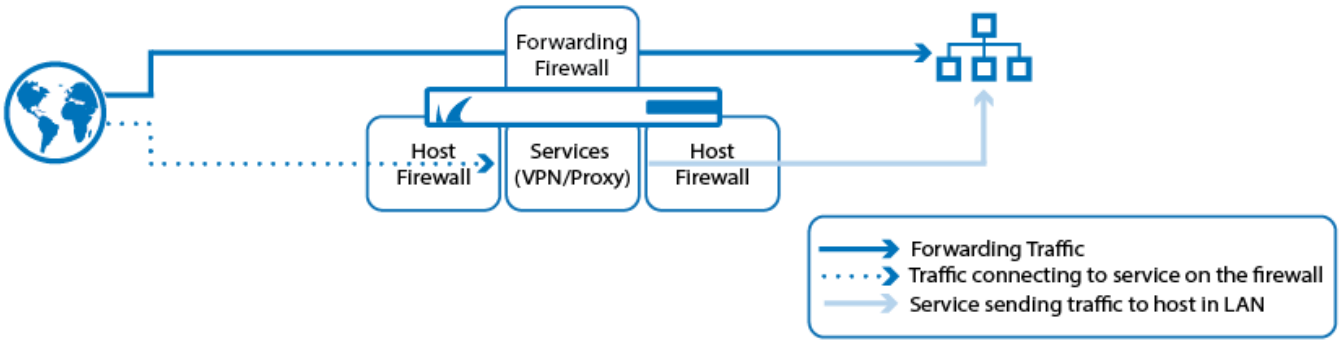
Firewall

The primary purpose of a firewall is to apply access and security policies to traffic entering and leaving your networks. Two different firewall services are responsible, depending on the destination of the traffic:

- **Host Firewall** – The host firewall handles local inbound and outbound traffic. The host firewall runs on box level.
- **Forwarding Firewall** – The forwarding firewall service handles traffic passing through the firewall. The forwarding firewall runs as a service in a virtual server.



Host Firewall

The host firewall runs on the box layer of every F-Series Firewall and Control Center and cannot be removed. The host firewall handles connections where the target IP address and port number match a listening socket of a service on the firewall. The **boxfw** is the system process for the host firewall. In addition to managing local traffic, the **boxfw** also manages other traffic handlers such as SIP, RPC, Timer, Audit, and Sync. Restarting the **boxfw** service reinitializes the service handlers and reloads the ruleset. The **boxfw** service is always running. 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.
- An outgoing connection from the HTTP Proxy service running on the firewall to a web server on the Internet.
- Outgoing and incoming VPN traffic from the VPN service to the tunnel endpoint.
- Outgoing NTP or DNS queries.

For more information, see Host Firewall.

Forwarding Firewall

The forwarding firewall runs as a service on a virtual server. It handles all traffic that does not match a listening socket on the firewall. You can create one (forwarding) Firewall service on each F-Series Firewall. This service listens to all IP addresses configured for the virtual server and is responsible for all connections that are transferred over the firewall to a remote host. The access rules for the forwarding firewall are maintained in the forwarding ruleset. The forwarding firewall is tightly integrated with all Application Control features, such as the Virus Scanner, Advanced Threat Protection (ATP), Intrusion Prevention System (IPS), or 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.
- A ping to an external Linux server.
- Traffic coming out of a VPN tunnel.

For more information, see Forwarding Firewall.

Limitations

- Only one forwarding firewall service is allowed per F-Series Firewall.
- The firewall handles only IP protocols. Non-IP traffic, such as Spanning Tree Protocol or IPX/SPX, is not forwarded.

Figures