Blocking External Client DNS Queries

Blocking External Client DNS Queries

This procedure configures the firewall to block DNS requests from local clients to servers outside the local network. With no other accessible DNS servers, clients are forced to send DNS requests to the DNS Resolver or DNS Forwarder on pfSense® software for resolution.

Note

Blocking is effective but does not gracefully handle the situation. Clients must manually adjust their configuration to use the firewall for DNS. Redirecting DNS requests to the firewall is a more seamless solution. See Redirecting Client DNS Requests for details.

- Navigate to **Firewall > Rules**, **LAN** tab
- Create the block rule as the first rule in the list:
  - Click fa-level-up **Add** to create a new rule at the top of the list
  - Fill in the following fields on the rule:

    Action
    : *Reject*

    Interface
    : *LAN*

    Protocol
    : *TCP/UDP*

    Destination
    : *Any*

    Destination Port Range
    : *DNS (53)*

    Description
    : `Block DNS to Everything Else`
- Create the pass rule to allow DNS to the firewall, above the block rule:
  - Click fa-level-up **Add** to create a new rule at the top of the list

- Fill in the following fields on the rule:
  Action
    Pass
  Interface
    LAN
  Protocol
    TCP/UDP
  Destination
    LAN Address
  Destination Port Range
    DNS (53)
  Description
    `Pass DNS to the Firewall`
- Click fa-check **Apply Changes** to reload the ruleset

When complete, there will be two rule entries that look like the following picture:

./images/blockdns.png
Image not found or type unknown

Certain local PCs could be allowed to use other DNS servers by placing a pass rule for them above the block rule.

DNS over TLS

Another concern is that clients could use DNS over TLS to resolve hosts. DNS over TLS sends DNS requests over an encrypted channel on an alternate port, `853`.

This traffic can be blocked with a firewall rule for port `853` using the same procedure used for `53`. Though if the firewall will not be providing DNS over TLS service to clients, do not add the pass rule.

DNS over HTTPS

Similar to DNS over TLS, clients may also use DNS over HTTPS (DoH). This is harder to block as it uses port `443`. Blocking port `443` on common public DNS servers may help (e.g. `1.1.1.1`, `8.8.8.8`).

Some browsers automatically attempt to use DNS over HTTPS because they believe it to be more secure and better for privacy, though that is not always the case. Each browser may have its own methods of disabling this feature. Firefox uses a “canary” domain `use-application-dns.net` by default. If Firefox cannot resolve this name, Firefox disables DNS over HTTPS.

To prevent Firefox from using DNS over HTTPS, add the following to the DNS Resolver custom options:

```
server:
local-zone: "use-application-dns.net" always_nxdomain
```

Revision #2
Created 29 December 2023 03:33:55 by ColtM
Updated 27 February 2025 20:49:19 by ColtM