

## LAB 3

02\_piSense\_Frontend\_Practice

piSense.home.arpa - Services

+

192.168.56.102/services\_unbound.php

OpenVPN Clients

☐ Register connected OpenVPN clients in the DNS Resolver

If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System > General Setup should also be set to the proper value.

Display Custom Options

Display Custom Options

Save

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
internalserver	lab.local	192.168.10.50	Internal test host	<div></div> <div></div>

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'has.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

Add

Domain Overrides

Domain	Lookup Server IP Address	Description	Actions
--------	--------------------------	-------------	---------

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'has.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.

Add

02\_piSense\_Frontend\_Practice

piSense.home.arpa - Services

+

192.168.56.102/services\_unbound.php

mode. The domain in System > General Setup should also be set to the proper value.

Display Custom Options

Display Custom Options

Save

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
internalserver	lab.local	192.168.10.50	Internal test host	<div></div> <div></div>

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'has.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

Add

Domain Overrides

Domain	Lookup Server IP Address	Description	Actions
facebook.com	0.0.0.0	Block social media	<div></div> <div></div>

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'has.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is treated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers available for a domain then make a separate entry for each, using the same domain name.

Add

piSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

02\_pfSense\_Frontend\_Practice x pfSense.home.arpa - Services: x +

← → x Not secure 192.168.56.102/services\_unbound.php ☆ 9 ⋮

Interfaces

WANUP LINK IPv6 Link-Local

LANCORE IPv6 Link-Local

Localhost

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

Strict Outgoing Network Interface Binding

☐ Do not send recursive queries if none of the selected Outgoing Network Interfaces are available.

By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.

System Domain Local Zone Type

Transparent

The local-zone type used for the pfSense system domain (System > General Setup). Transparent is the default.

DNSSEC

☒ Enable DNSSEC Support

Python Module

☐ Enable Python Module

Enable the Python Module.

DNS Query Forwarding

☐ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

☐ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers

When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

DHCP Registration

☐ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.

Static DHCP

☐ Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System >