




































LAN Rules

Rules (Drag to Change Order)												
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	1 / 1.81 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	  408 / 3.19 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	   	
<input type="checkbox"/>	 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	   	

VLAN Rules

Rules (Drag to Change Order)												
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks		
<input type="checkbox"/>	  0 / 10 KiB	IPv4 *	VLAN3 net	*	192.168.1.0/24	*	*	none			   	
<input type="checkbox"/>	  0 / 336 B	IPv4 ICMP any	VLAN3 net	*	*	*	*	none			   	
<input type="checkbox"/>	  0 / 0 B	IPv4 *	VLAN3 net	*	WAN net	*	*	none			   	

LAN DHCP Server

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<div>192.168.1.10192.168.1.245</div> <div>FromTo</div>

Other relevant info for LAN DHCP server(other sections are not marked up)

Servers	
WINS servers	<div>WINS Server 1</div> <div>WINS Server 2</div>
DNS servers	<div>DNS Server 1</div> <div>DNS Server 2</div> <div>DNS Server 3</div> <div>DNS Server 4</div>
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

VLAN 3 DHCP Server

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on VLAN3 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.3.0
Subnet mask	255.255.255.0
Available range	192.168.3.1 - 192.168.3.254
Range	<div><div>192.168.3.10</div><div>192.168.3.50</div><div>FromTo</div></div>

Other relevant information (other sections are not marked up)

Servers	
WINS servers	<div>WINS Server 1</div>
	<div>WINS Server 2</div>
DNS servers	<div>DNS Server 1</div>
	<div>DNS Server 2</div>
	<div>DNS Server 3</div>
	<div>DNS Server 4</div>
	Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

DNS Resolver used for all bridges

General DNS Resolver Options	
Enable	<input checked="" type="checkbox"/> Enable DNS resolver
Listen Port	<div>53</div> <div>The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.</div>
Enable SSL/TLS Service	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate	<div>webConfigurator default (5f96434909cd3)</div> <div>The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.</div>
SSL/TLS Listen Port	<div>853</div> <div>The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.</div>
Network Interfaces	<div><div>All WAN LAN VLAN3 VLAN10</div><div>Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.</div></div>
Outgoing Network Interfaces	<div><div>All WAN LAN VLAN3 VLAN10</div></div>

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.

System Domain Local Zone Type

Transparent

The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the [unbound.conf\(5\)](#) manual pages.

DNSSEC

☐ Enable DNSSEC Support

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 DHCP/PPP on WAN (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. 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 > General Setup](#) should also be set to the proper value.

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) 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
------	-----------------------	-----------------------	-------------	---------

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', '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
example.com	192.168.1.1	Primary DNS Server	Edit Delete
example.com	192.168.1.2	Secondary DNS Server	Edit Delete
example.com	192.168.1.3	Tertiary DNS Server	Edit Delete

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', '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.

+ Add

Here's the Tomato Router

Note the connection across the WAN (actually I am not even using the WAN)

VLAN on the Tomato Router

VLAN Settings

[illegible]

WAN Settings

Type

Disabled

Wireless Client Mode

Disabled

Bridge WAN port to primary LAN
(br0)



LAN

Bridge ^	STP	IP Address	Netmask	DHCP	IP Range (first/last)	Lease Time (mins)
br0	Disabled	192.168.1.2	255.255.255.0	Disabled	-	
br1	Disabled	192.168.3.2	255.255.255.0	Disabled	-	