pfSense

Make sure to commit ALL changes with SAVE (usually found at the bottom of screen)

1. Connect to pfSense box

   Username: admin

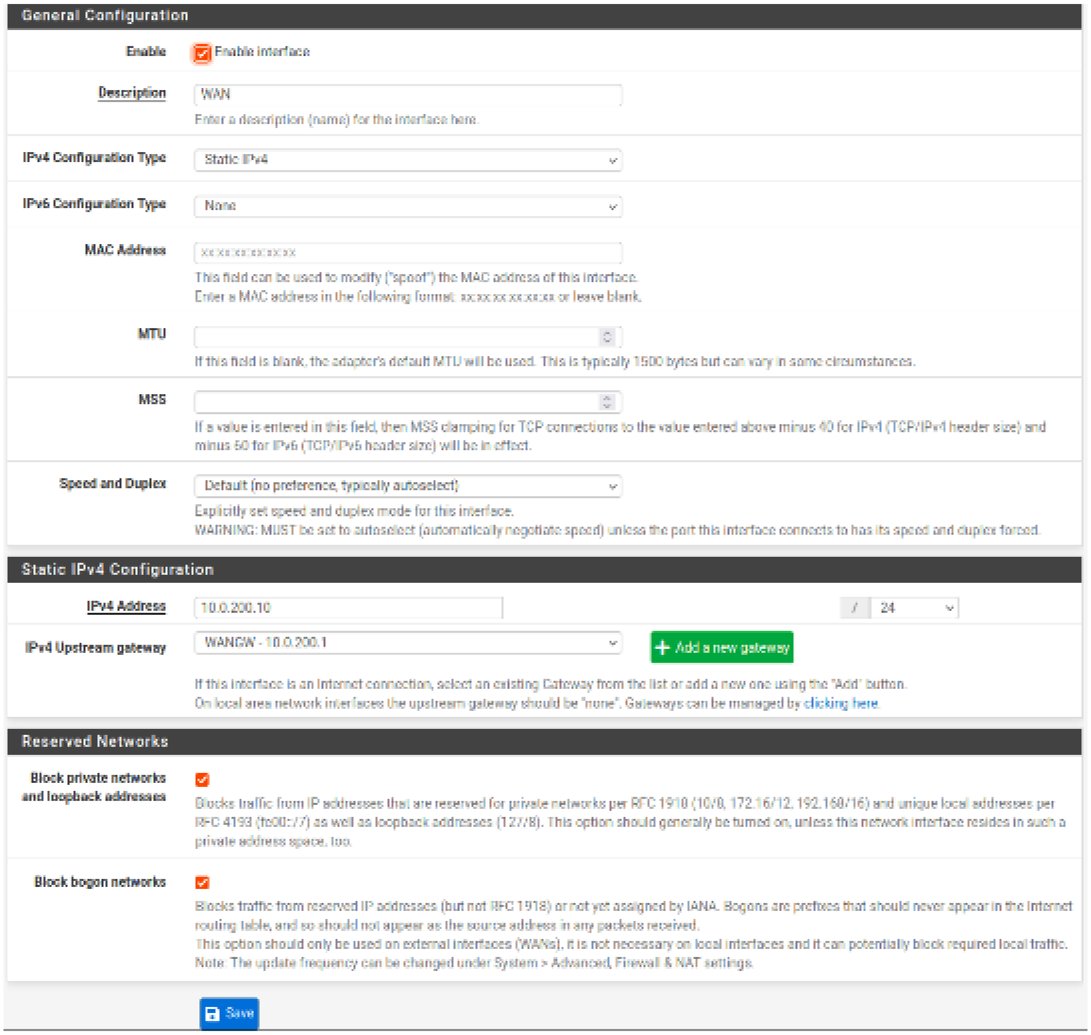
   Password: admin

For WAN, LAN, SOC, and NOC make sure ENABLE INTERFACE (at top) is checked

2. Configure Interfaces:

   Set up WAN and LAN, SOC and NOC

   Interfaces → WAN



General Configuration

Enable: ☑ Enable interface

Description: WAN
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 10.0.200.10 / 24

IPv4 Upstream gateway: WANGW - 10.0.200.1

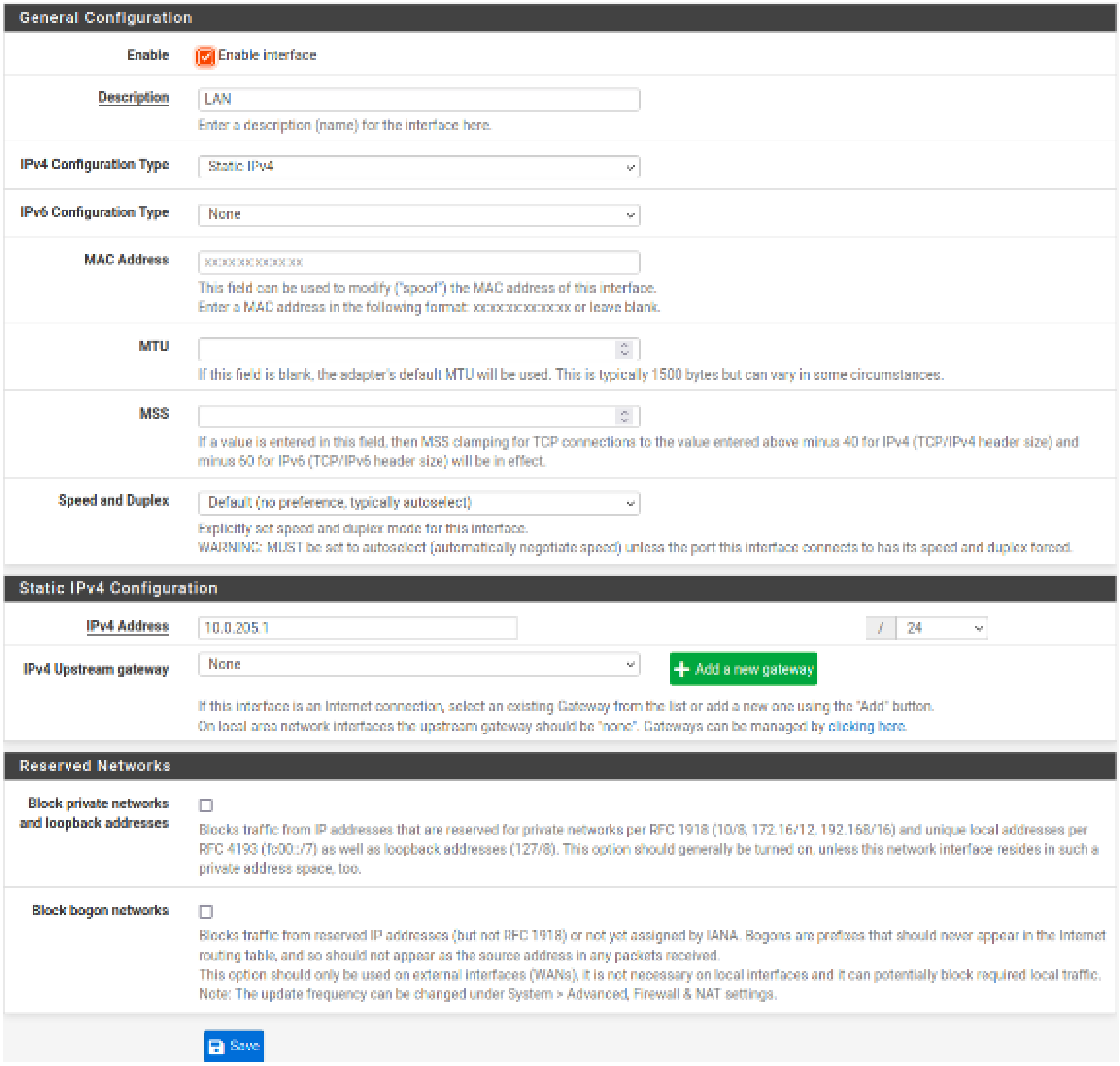
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses: ☑
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks: ☑
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Interfaces → LAN



General Configuration

Enable ☑ Enable interface

Description: LAN
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 10.0.205.1 / 24

IPv4 Upstream gateway: None

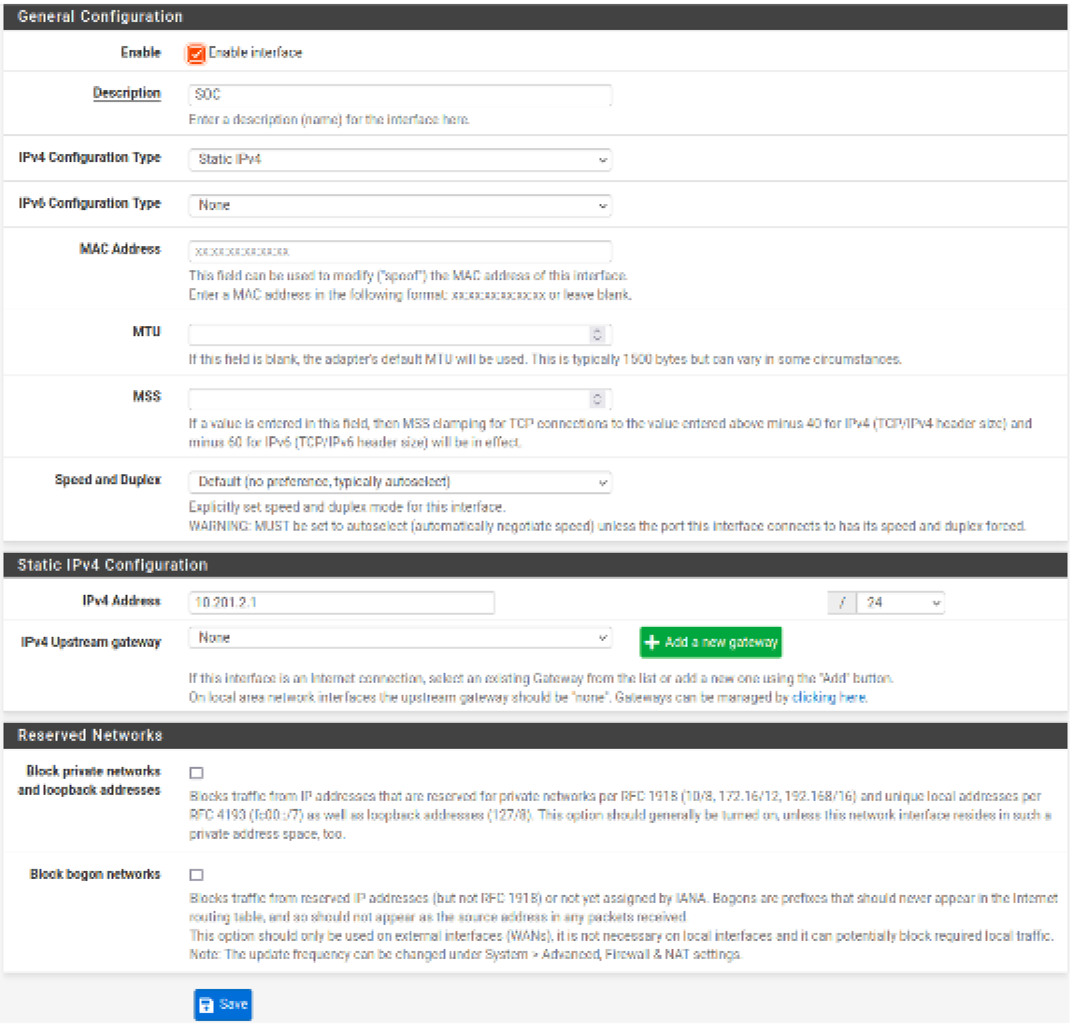
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses ☐
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☐
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Interfaces → SOC



General Configuration

Enable ☑ Enable interface

Description: SOC

Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 10.201.2.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

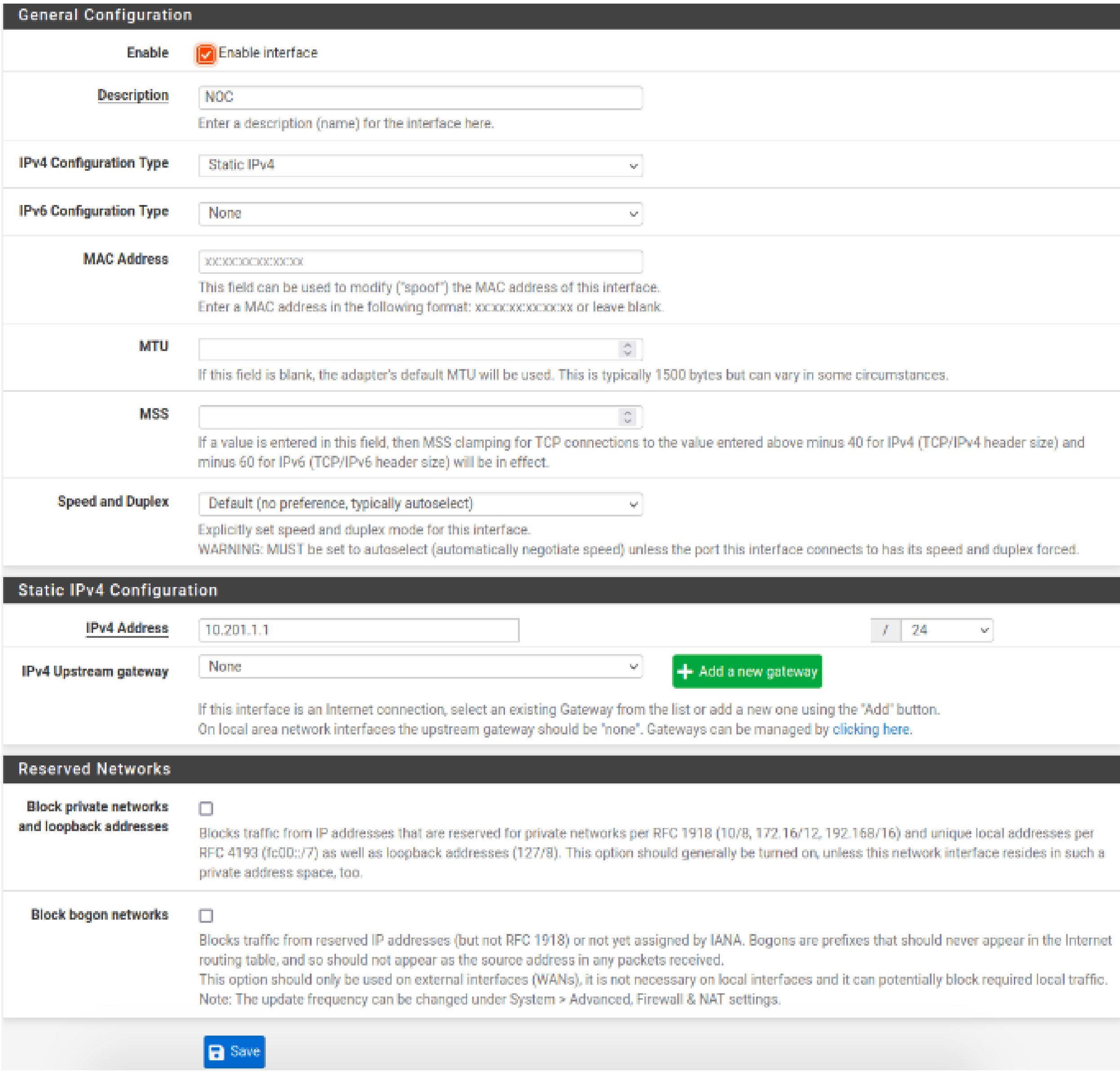
Block private networks and loopback addresses ☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☐

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Interfaces → NOC



General Configuration

Enable ☑ Enable interface

Description NOC

Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 10.201.1.1 / 24

IPv4 Upstream gateway None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses ☐

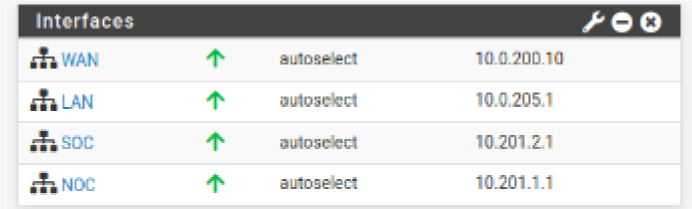
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☐

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

For WAN, LAN, SOC, and NOC make sure ENABLE INTERFACE (at top) is checked
Make sure to commit ALL changes with SAVE (usually found at the bottom of screen)

If it is set up correctly, on the main dashboard (bottom right) it should look like this :

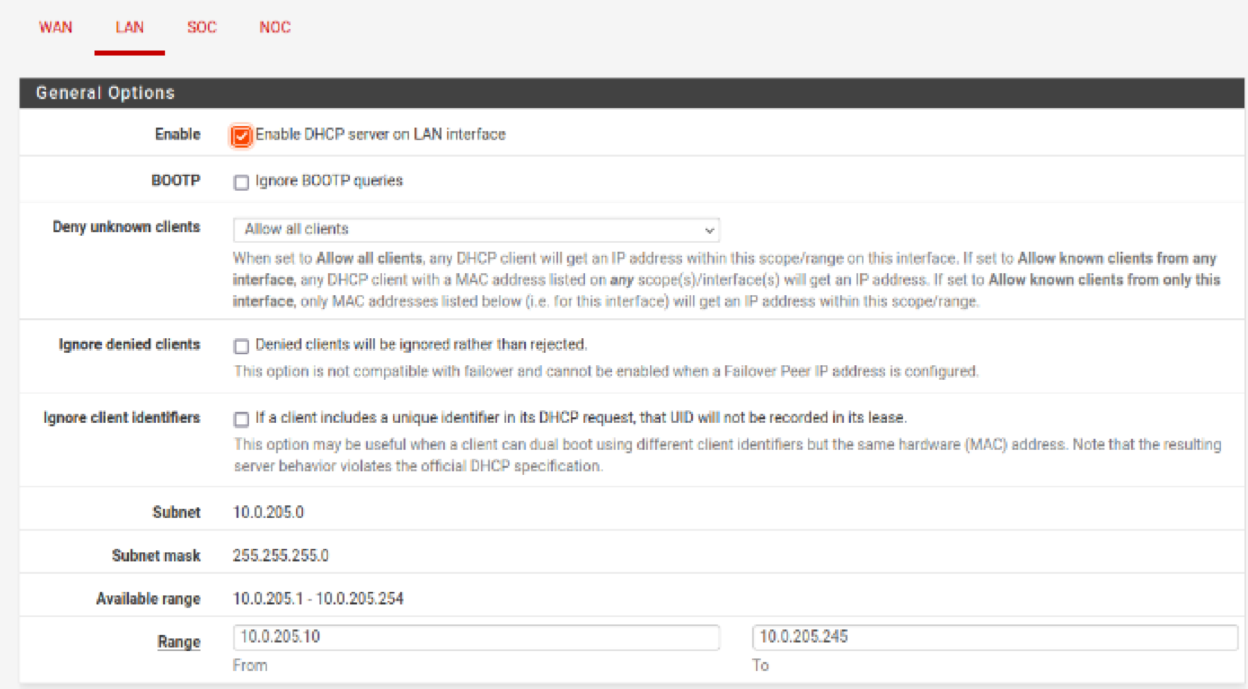


Interfaces

WAN	↑	autoselect	10.0.200.10
LAN	↑	autoselect	10.0.205.1
SOC	↑	autoselect	10.201.2.1
NOC	↑	autoselect	10.201.1.1

3. Enable DHCP
   Services → DHCP Server → LAN/SOC/NOC
   No DHCP server is needed for WAN; main purpose is to set ranges

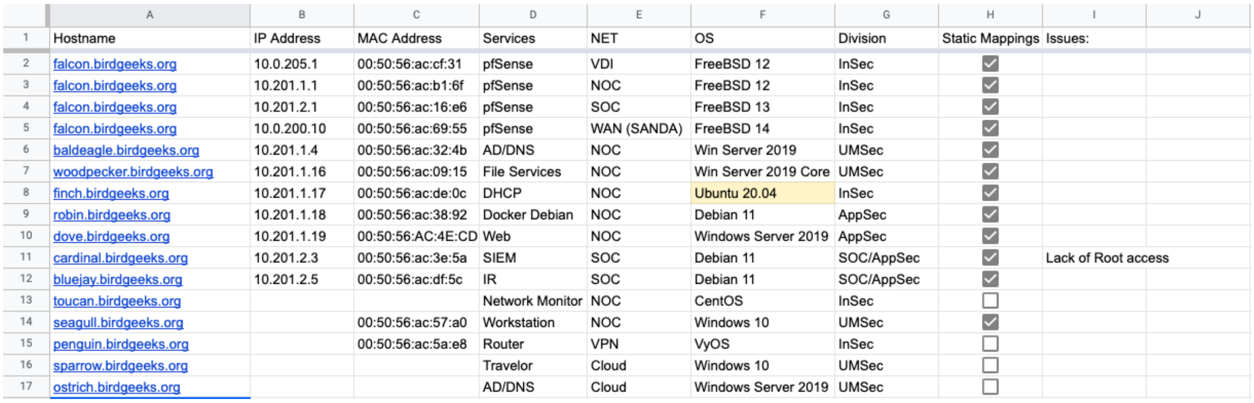
Services → DHCP Server → LAN



General Options

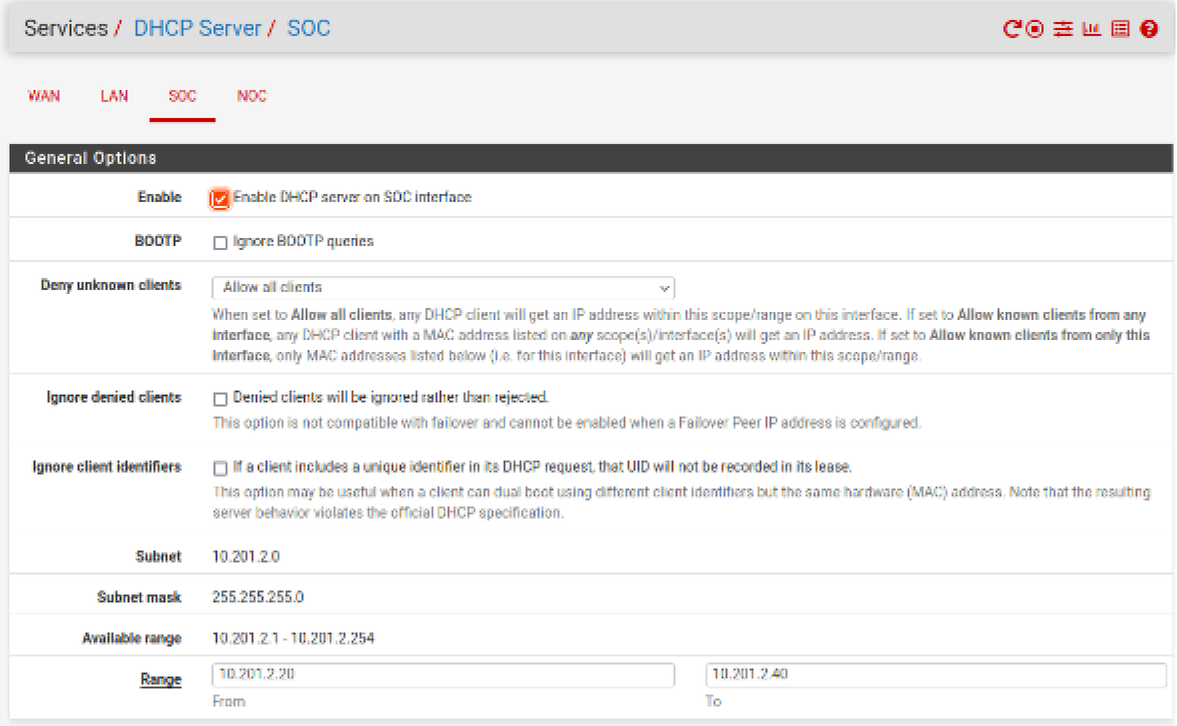
Enable	☑ Enable DHCP server on LAN interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	Allow all clients When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients	□ 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	□ 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	10.0.205.0
Subnet mask	255.255.255.0
Available range	10.0.205.1 - 10.0.205.254
Range	10.0.205.10 (From) — 10.0.205.245 (To)

For SOC/NOC make sure that it is correctly configured with the HOSTs
(CHECK HOST INVENTORY SPREADSHEET FOR MOST UPDATED INFORMATION)



	A	B	C	D	E	F	G	H	I	J
1	Hostname	IP Address	MAC Address	Services	NET	OS	Division	Static Mappings	Issues:	
2	falcon.birdgeeks.org	10.0.205.1	00:50:56:ac:cf:31	pfSense	VDI	FreeBSD 12	InSec	☑		
3	falcon.birdgeeks.org	10.201.1.1	00:50:56:ac:b1:6f	pfSense	NOC	FreeBSD 12	InSec	☑		
4	falcon.birdgeeks.org	10.201.2.1	00:50:56:ac:16:e6	pfSense	SOC	FreeBSD 13	InSec	☑		
5	falcon.birdgeeks.org	10.0.200.10	00:50:56:ac:69:55	pfSense	WAN (SANDA)	FreeBSD 14	InSec	☑		
6	baldeagle.birdgeeks.org	10.201.1.4	00:50:56:ac:32:4b	AD/DNS	NOC	Win Server 2019	UMSec	☑		
7	woodpecker.birdgeeks.org	10.201.1.16	00:50:56:ac:09:15	File Services	NOC	Win Server 2019 Core	UMSec	☑		
8	finch.birdgeeks.org	10.201.1.17	00:50:56:ac:de:0c	DHCP	NOC	Ubuntu 20.04	InSec	☑		
9	robin.birdgeeks.org	10.201.1.18	00:50:56:ac:38:92	Docker Debian	NOC	Debian 11	AppSec	☑		
10	dove.birdgeeks.org	10.201.1.19	00:50:56:AC:4E:CD	Web	NOC	Windows Server 2019	AppSec	☑		
11	cardinal.birdgeeks.org	10.201.2.3	00:50:56:ac:3e:5a	SIEM	SOC	Debian 11	SOC/AppSec	☑	Lack of Root access	
12	bluejay.birdgeeks.org	10.201.2.5	00:50:56:ac:df:5c	IR	SOC	Debian 11	SOC/AppSec	☑		
13	toucan.birdgeeks.org			Network Monitor	NOC	CentOS	InSec	□		
14	seagull.birdgeeks.org		00:50:56:ac:57:a0	Workstation	NOC	Windows 10	UMSec	☑		
15	penguin.birdgeeks.org		00:50:56:ac:5a:e8	Router	VPN	VyOS	InSec	□		
16	sparrow.birdgeeks.org			Travelor	Cloud	Windows 10	UMSec	□		
17	ostrich.birdgeeks.org			AD/DNS	Cloud	Windows Server 2019	UMSec	□		

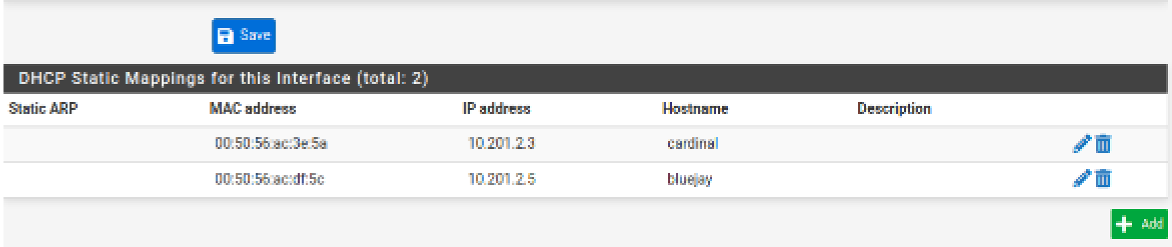
Services → DHCP Server → SOC



General Options

Enable	☑ Enable DHCP server on SOC interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	Allow all clients When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients	□ 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	□ 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	10.201.2.0
Subnet mask	255.255.255.0
Available range	10.201.2.1 - 10.201.2.254
Range	From: 10.201.2.20 To: 10.201.2.40

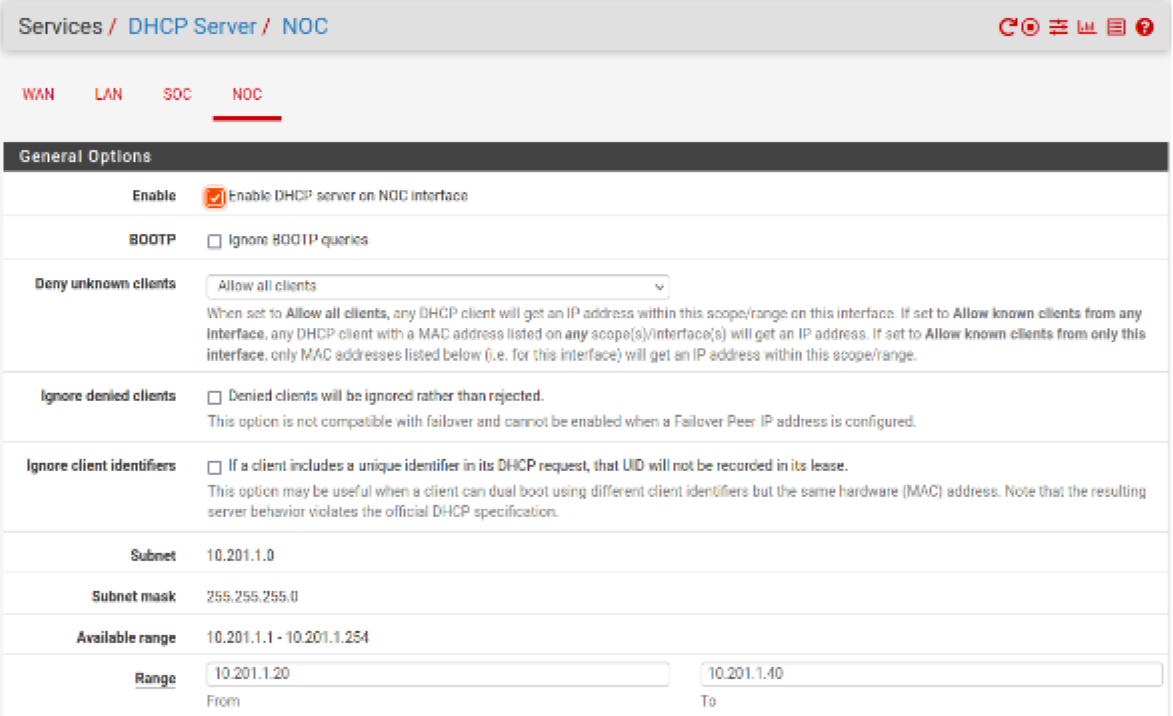
Then the static mappings at the bottom:



DHCP Static Mappings for this Interface (total: 2)

Static ARP	MAC address	IP address	Hostname	Description
	00:50:56:ac:3e:5a	10.201.2.3	cardinal	
	00:50:56:ac:df:5c	10.201.2.5	bluejay	

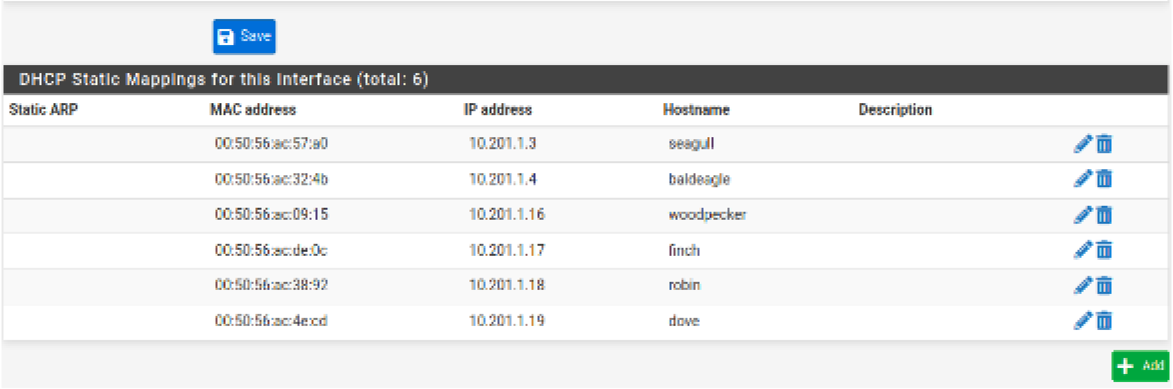
Services → DHCP Server → NOC



General Options

Enable	☑ Enable DHCP server on NOC interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	Allow all clients When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients	□ 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	□ 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	10.201.1.0
Subnet mask	255.255.255.0
Available range	10.201.1.1 - 10.201.1.254
Range	From: 10.201.1.20 To: 10.201.1.40

Then the static mappings at the bottom:



DHCP Static Mappings for this Interface (total: 6)

Static ARP	MAC address	IP address	Hostname	Description
	00:50:56:ac:57:a0	10.201.1.3	seagull	
	00:50:56:ac:32:4b	10.201.1.4	baldeagle	
	00:50:56:ac:09:15	10.201.1.16	woodpecker	
	00:50:56:ac:de:0c	10.201.1.17	finch	
	00:50:56:ac:38:92	10.201.1.18	robin	
	00:50:56:ac:4e:cd	10.201.1.19	dove	

Reminder Checklist:

- □ Are the interfaces configured?
- □ Is the DHCP service enabled?
- □ Are the DHCP pools configured?
- □ Are the static mappings configured?
- □ Is everything saved and applied?