DYNICS

ICS-Defender

User Guide

www.dynics.com

Contents

Revision History

Revision	Date	Comment
V.01	7/1/2017	Draft Created
V.02	8/11/2017	Industrial Protocol Section Updated
V.03	8/21/2017	New features added for Industrial Protocol
V.04	8/22/2017	Added sections on how to PING and access WebGUI from WAN
V1.0	9/7/2017	Initial Release
V1.1	8/11/2018	Updated for new features since last update
V1.2	8/12/2020	Updated for new features and changes to verbiage

Additional Documentation

Documentation is consistently being updated as more features and functionality is added and refined in ICS-Defender. If this document doesn't include needed information, please contact Dynics.

Document Conventions

Document Abbreviations

Abbreviation	Full Description
ICS	Industrial Control System
NIC	Network Interface Card
RA	Remote Access
NAT	Network Address Translation
1:1	One to One (a type of NAT)
LAN	Local Area Network
WAN	Wide Area Network
NTP	Network Time Protocol
DHCP	Dynamic Host Configuration Protocol
CIDR	Classless Inter Domain Routing
CA	Certificate Authority
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
SSL	Secure Socket Layer
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
CIP	Common Industrial Protocol (EtherNet/IP)
Jump Server	A jump server or secure administrative host is a (special-purpose) computer on a network typically used to manage devices in a separate security zone.

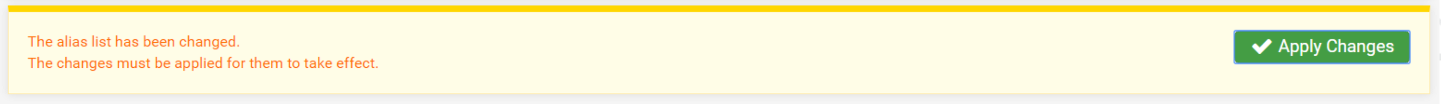
Subnet Mask to CIDR Quick Reference

Subnet Mask	CIDR	Notes
255.255.255.255	/32	Single IP address
255.255.255.254	/31	unusable
255.255.255.252	/30	2 useable IP addresses
255.255.255.248	/29	6 useable IP addresses
255.255.255.240	/28	14 useable IP addresses
255.255.255.224	/27	30 useable IP addresses
255.255.255.192	/26	62 useable IP addresses
255.255.255.128	/25	126 useable IP addresses
255.255.255.0	/24	254 useable IP addresses
255.255.254.0	/23	508 useable IP addresses
255.255.252.0	/22	1016 useable IP addresses
255.255.248.0	/21	2032 useable IP addresses
255.255.240.0	/20	4064 useable IP addresses

Common WebGUI Interactions

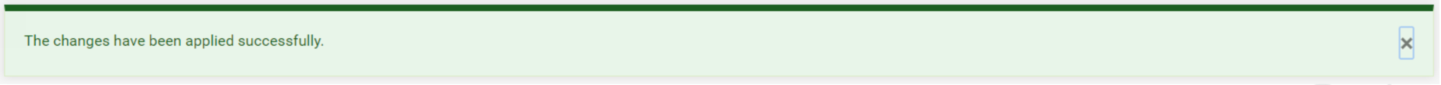
Applying Changes

When making adding or making changes in the configuration via the ICS-Defender WebGUI, in many cases, after the change is saved, the WebGUI will require that the changes be "applied". The change is saved, but has not "gone live" in ICS-Defender yet.



The alias list has been changed.
The changes must be applied for them to take effect.

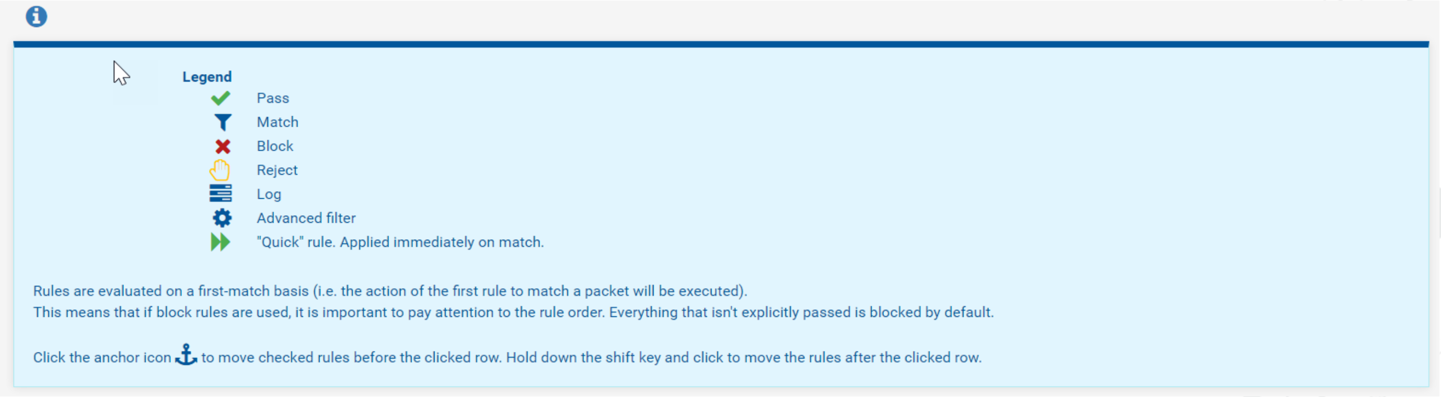
Once the changes are applied, they become active. ICS-Defender will display a confirmation that the changes have been applied successfully. Click the X on the right side of the confirmation to close it.



The changes have been applied successfully.

Context Help / Additional Information

The ℹ information icon will appear in various locations through the WebGUI. When clicked, additional information about a given topic will be displayed.



Legend

✓	Pass
▼	Match
✖	Block
✋	Reject
☰	Log
⚙	Advanced filter
⏩	"Quick" rule. Applied immediately on match.

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed).
This means that if block rules are used, it is important to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

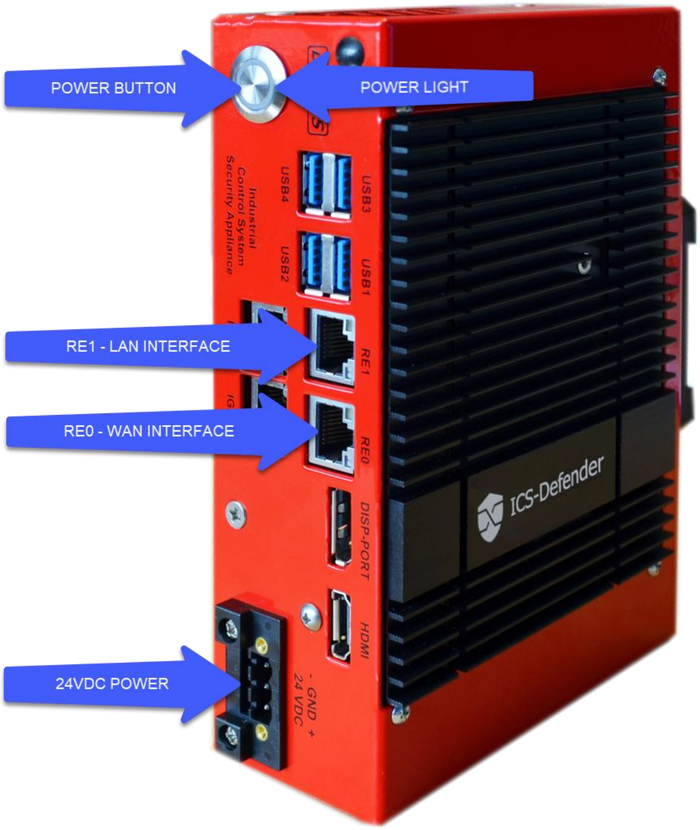
Click the anchor icon ⚓ to move checked rules before the clicked row. Hold down the shift key and click to move the rules after the clicked row.

Important: ICS-Defender is shipped with a secure profile (default) on the WAN interface. The LAN interface is open and not considered secure.

Quick Start

Powering Up

ICS-Defender requires a 24vdc supply. After connecting to a 24vdc supply (see product documentation for proper wiring and power connections), power up ICS-Defender by pressing the round power button.



Connecting

ICS-Defender is available in several versions. ICS-Defender Pro and ICS-Defender Standard both include four (4) Ethernet ports (NICS) while ICS-Defender RA, ICS-Defender NAT, and ICS-Defender Lite include two (2) Ethernet ports.

For each of these versions, the hardware includes two NICS labeled RE0 and RE1. On the ICS-Defender Pro and Standard versions, the two additional NICS are labeled IGB0 and IGB1. All NICS support speeds up to 1GB.

While these NICS can be configured for multiple purposes, "out of the box", RE0 is the "WAN" or enterprise NIC and RE1 is the "LAN" or local network NIC.

Default User, Password, and IP Address

Default Username:	**admin**	**Default IP Address:**	**192.168.200.1**
Default Password:	**icsdefender**	Default Subnet Mask:	**255.255.255.0**

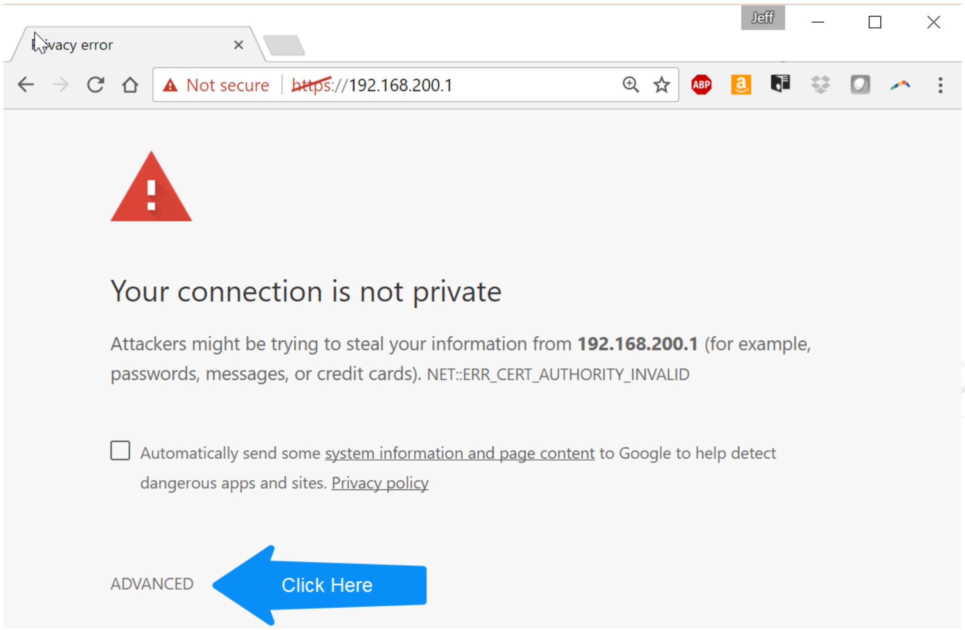
Accessing the Web GUI

IMPORTANT: It is very important to change the default password when creating a configuration for ICS-Defender. Secure configurations should include multiple user levels and multiple passwords for those levels.

ICS-Defender, depending on the version, can take up to slightly more than a minute to bootup.

The computer connecting to the ICS-Defender for the first time must be a part of the 192.168.200.x network. After connecting an Ethernet RJ45 cable to the LAN port (RE1), launch a web-browser and enter the default IP address

When connecting to an unconfigured ICS-Defender, web browsers may indicate an unsecure connection. This notice is normal as the current configuration of the security appliance doesn't contain the necessary settings to prevent the warning. If this screen does not appear, continue to the next section.



Your connection is not private

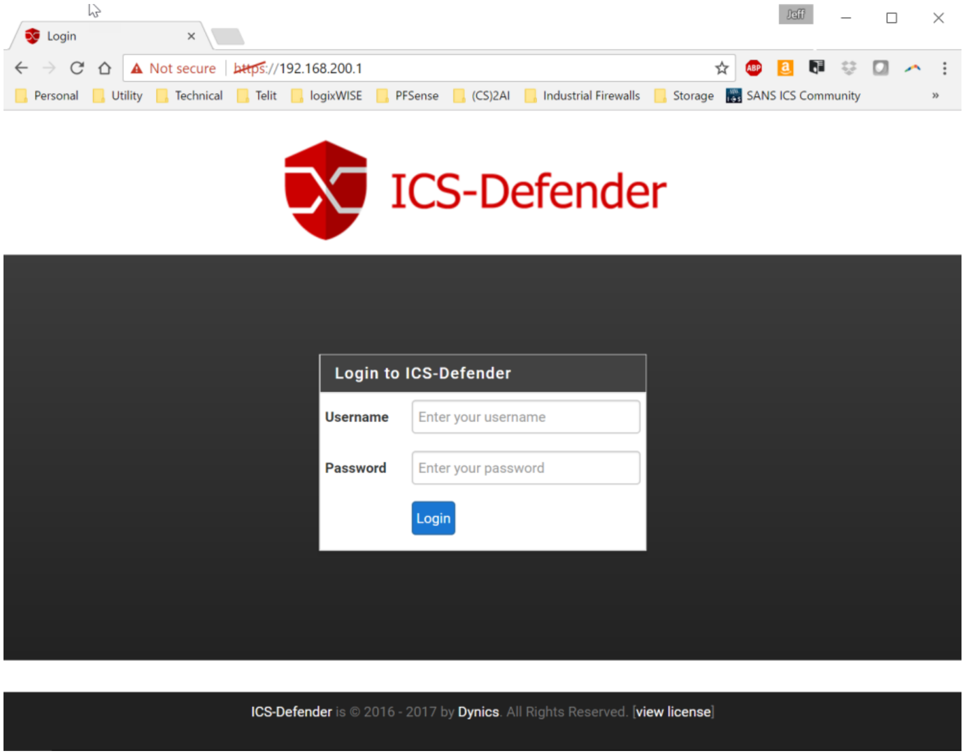
Attackers might be trying to steal your information from **192.168.200.1** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Click "ADVANCED" and select "Proceed to 192.168.200.1 (unsafe)".

Logging In

On the ICS-Defender login page, enter the default username and password.



Login to ICS-Defender

Username: Enter your username

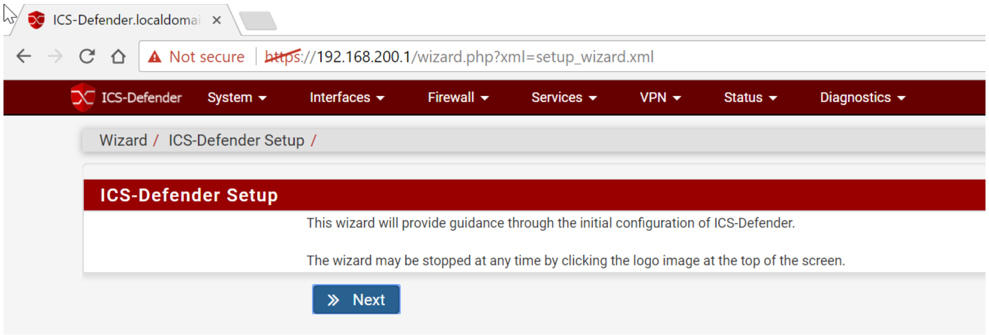
Password: Enter your password

ICS-Defender is © 2016 - 2017 by Dynics. All Rights Reserved. [view license]

Setup Wizard

When browsing to the WebGUI, the initial screen is a login screen. For the username enter "**admin**" and for the password, enter "**icsdefender**". Since this is the first time visiting the WebGUI, the Setup Wizard will begin automatically, and resembles Figure 6.2.

Note: Using the setup wizard is optional. To create a more complex configuration or if the default values are acceptable, click the logo at the top of the wizard to get back to the firewall configuration.


ICS-Defender.localdomai ×
Not secure
~~https~~://192.168.200.1/wizard.php?xml=setup_wizard.xml
ICS-Defender
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Wizard / ICS-Defender Setup /
Next

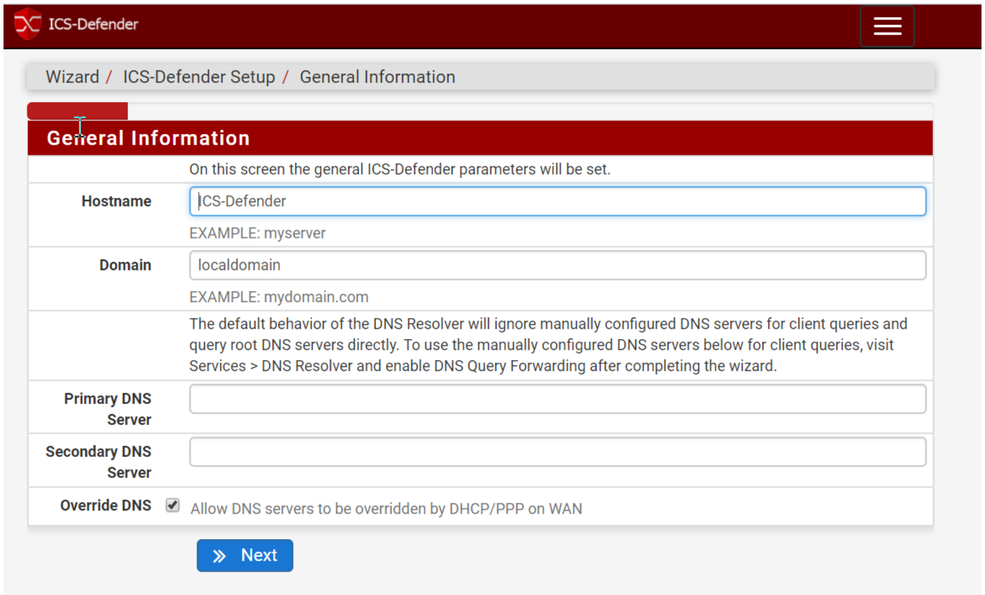
ICS-Defender Setup

This wizard will provide guidance through the initial configuration of ICS-Defender.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Figure 6.2

Step #1 - General setup



Wizard / ICS-Defender Setup / General Information

General Information

On this screen the general ICS-Defender parameters will be set.

Hostname ICS-Defender

EXAMPLE: myserver

Domain localdomain

EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

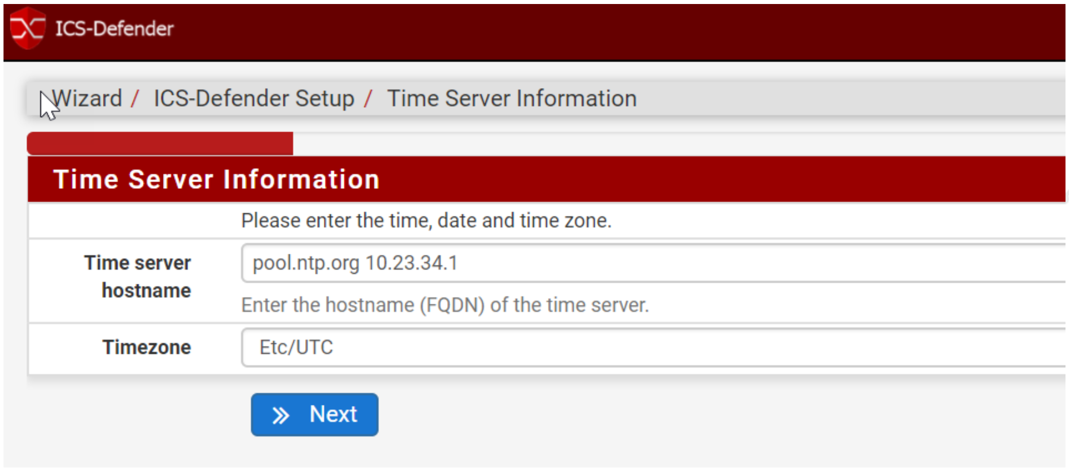
Override DNS ☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

Setting	Description
Hostname	This is a unique name assigned to this ICS-Defender. The hostname must start with a letter, and then it may contain only letters, numbers, or a hyphen. It is recommended to create a standard naming convention for the ICS-Defenders in an organization. The name could consist of 2 or 3-character abbreviations for areas in a manufacturing plant such as Site, Plant, and Line. ICS-DefSSPPLL01 ***Important: Unique hostnames are important when certificates are created using the ICS-Defender internal certificate authority and management.***
Domain	If the domain is unknown or there is no domain, an entry such as <mytext>.localdomain, can be used; where <mytext> can be a company name, a last name, nickname, etc. The hostname and domain name are combined to make up the fully qualified domain name of ICS-Defender.
DNS Options	If DNS information is available, enter it here. Otherwise, leave these fields blank.

Click >> NEXT when ready to continue.

Step #2 - Time Server Setup

The next screen (Figure *NTP and Time Zone Setup Screen*) has a place for a



Time Server Information

Please enter the time, date and time zone.

Time server hostname: pool.ntp.org 10.23.34.1

Enter the hostname (FQDN) of the time server.

Timezone: Etc/UTC

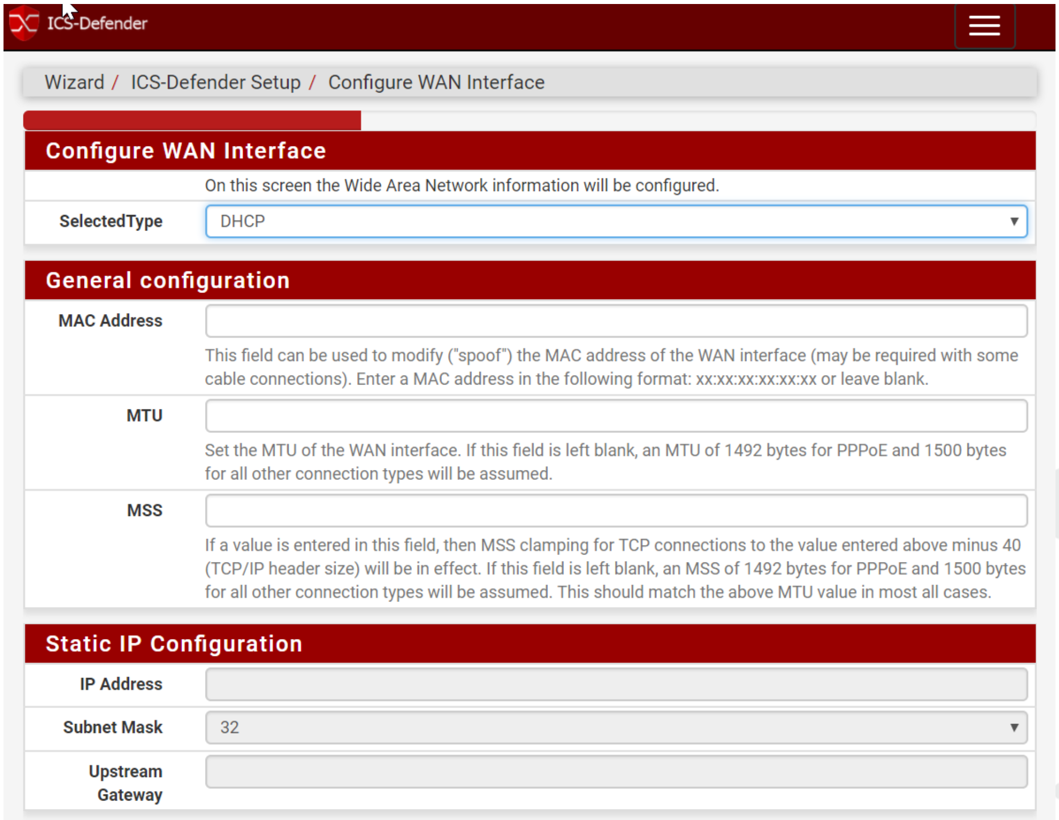
Setting	Description
Time server hostname	Network Time Protocol (NTP) server, and the time zone in which this server resides. Unless a specific preference is required for an NTP server such as one inside the LAN, it is best to leave the Time server hostname at the default *pool.ntp.org.* Leaving the default will pick a random server from a pool of known-good NTP hosts. If multiple time servers are desired, they may be added in the same box, separating each server by a space.
Timezone	Choose a geographically named zone which best matches the ICS-Defender system's final location.

Click >> NEXT when ready to continue.

Step #3 - Configure WAN Interface

These next few paragraphs and their associated images will help guide through setting up the WAN interface on the ICS-Defender system. Since this is the side which may be facing an ISP or upstream router, there are configuration choices to support several common ISP connection types. The first choice is for the WAN Type (Figure *WAN Configuration*).

Possible choices are Static, DHCP, PPPoE, and PPTP. If static is selected, the IP address and subnet mask fields must be populated. If the necessary WAN type is not available in the wizard, or more information is needed about the WAN types found here, detailed information can be found in Interface Types and Configuration.



Wizard / ICS-Defender Setup / Configure WAN Interface

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: DHCP

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

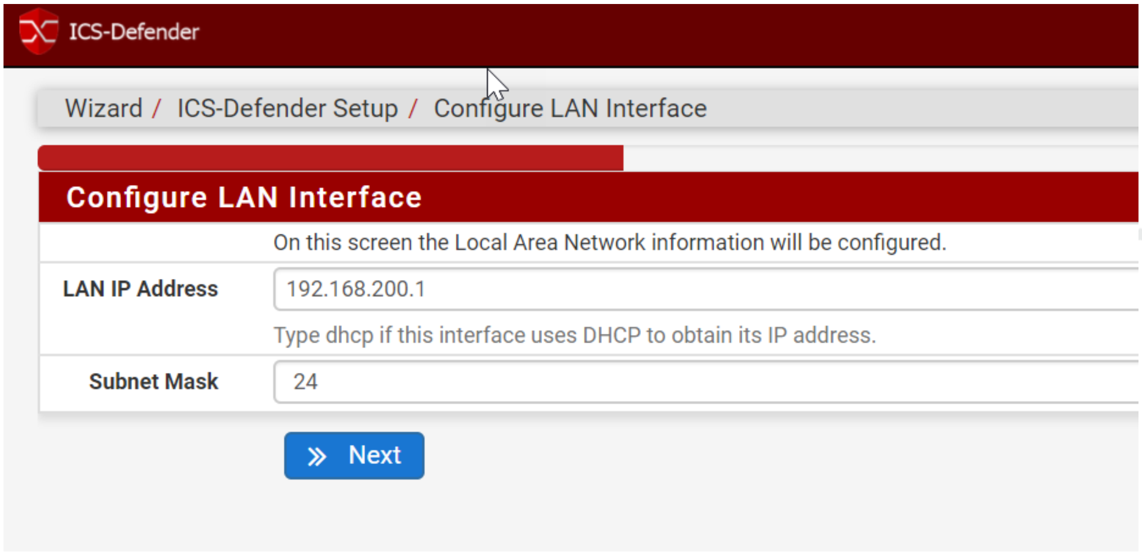
IP Address:

Subnet Mask: 32

Upstream Gateway:

Click >> NEXT when ready to continue.

Step #4 - Configure LAN Interface



ICS-Defender

Wizard / ICS-Defender Setup / Configure LAN Interface

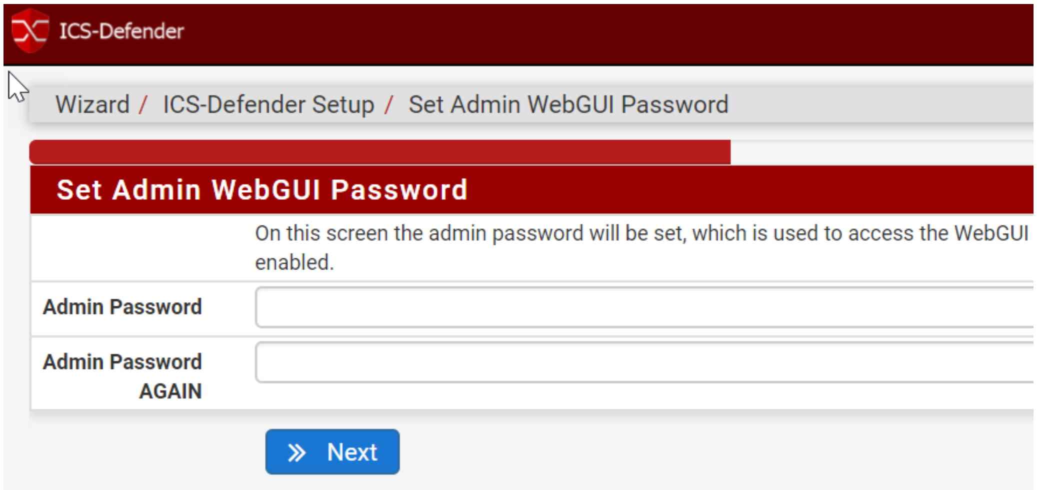
Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.200.1 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24

Click >> NEXT when ready to continue.

Step #5 - Set Administrator Password



Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI enabled.

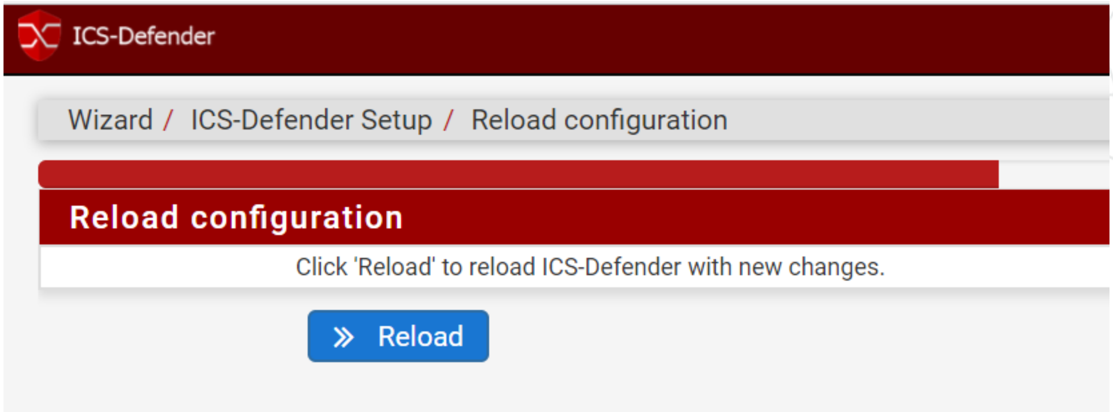
Admin Password

Admin Password AGAIN

Setting	Description
Admin Password	Change the admin password to a more secure value. This password should be something strong and secure, but no restrictions are automatically enforced.
Admin Password AGAIN	Re-enter the admin password entered in the above field. They must match.

Click >> NEXT when ready to continue.

Step #6 - Reload Configuration

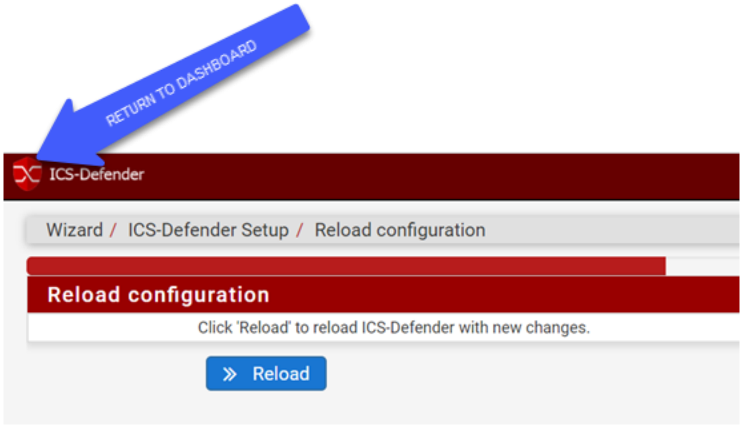


Reload configuration

Click 'Reload' to reload ICS-Defender with new changes.

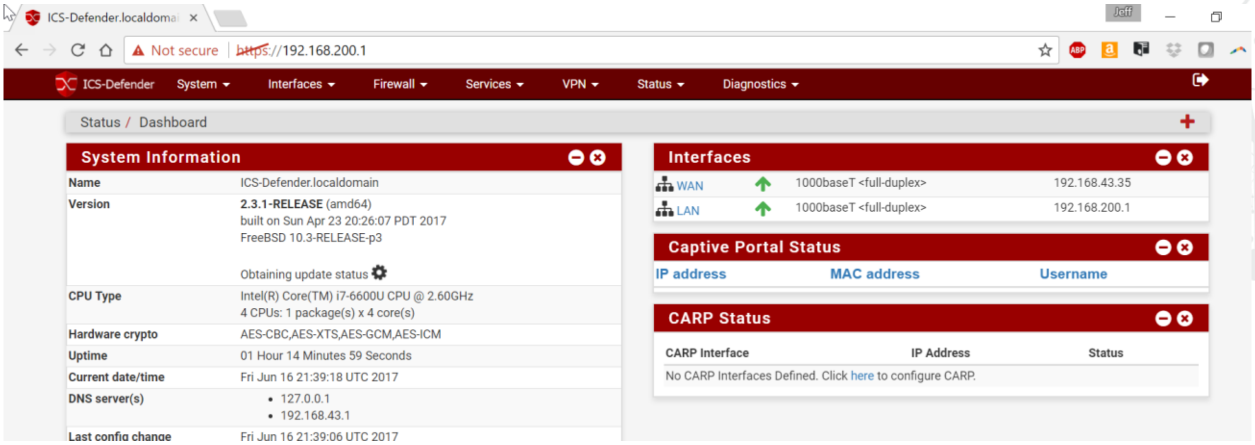
Click >> RELOAD to restart ICS-Defender with the updated configuration.

After a few moments, if the screen doesn't automatically refresh showing the ICS-Defender dashboard, click the ICS-Defender logo in the upper left corner of the WebGUI to force a refresh. Once clicked, the dashboard should be displayed.



Reload configuration

Click 'Reload' to reload ICS-Defender with new changes.



System Information

Name	ICS-Defender.localdomain
Version	**2.3.1-RELEASE** (amd64) built on Sun Apr 23 20:26:07 PDT 2017 FreeBSD 10.3-RELEASE-p3 Obtaining update status
CPU Type	Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz 4 CPUs: 1 package(s) x 4 core(s)
Hardware crypto	AES-CBC,AES-XTS,AES-GCM,AES-ICM
Uptime	01 Hour 14 Minutes 59 Seconds
Current date/time	Fri Jun 16 21:39:18 UTC 2017
DNS server(s)	• 127.0.0.1 • 192.168.43.1
Last config change	Fri Jun 16 21:39:06 UTC 2017

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.43.35
LAN	↑	1000baseT <full-duplex>	192.168.200.1

Captive Portal Status

IP address	MAC address	Username

CARP Status

CARP Interface	IP Address	Status
No CARP Interfaces Defined. Click here to configure CARP.		

More advanced configurations, beyond the scope of this document, can be created from within the WebGUI.

Troubleshooting

Power

Power light does not energize

After depressing the power button on ICS-Defender, if the power light does not energize, confirm the presence and polarity of 24VDC to the appliance. Note that the power connector only fits into the plug on ICS-Defender a certain way. The polarity (+ / -) is printed above the connector on the front of the appliance.

WebGUI

Logging into the WebGUI

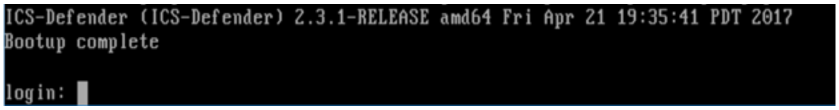
After typing the default IP address into a browser window, if ICS-Defender login or security challenge doesn't appear, check the following.

1. Make sure the appliance is powered up by observing the white power light surrounding the power button.
2. Confirm that an RJ45 Ethernet cable is connected to the LAN interface (RE1) from the PC.
3. Confirm that the PC from which the login is attempted has an IP address in the 192.168.200.x address range.

Console

Visual Confirmation of Startup

The front panel on the appliance has two video and four USB ports. Connecting a display to one of the video ports should provide visual confirmation that ICS-Defender is powered up and has successfully started.



```
ICS-Defender (ICS-Defender) 2.3.1-RELEASE amd64 Fri Apr 21 19:35:41 PDT 2017
Bootup complete

login: █
```

Helpful Settings during Setup/Configuration Development

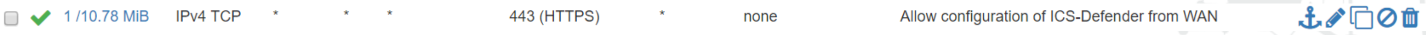
Access WebGUI from the WAN

To temporarily access the WebGUI from the WAN a firewall rule can quickly be added. It is generally recommended to disallow editing the ICS-Defender from the WAN, but in some cases, it may be necessary. A jump server can be used for this purpose and the access to the WebGUI from the WAN can be limited to its IP address only.

To allow access to the WebGUI from the WAN navigate to **Firewall→ Rules→ WAN** and click the "Add" button. Set the following options for the rule. Any settings not specified here remain at their default setting.

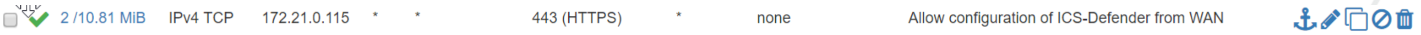
Action:	Pass
Disabled:	Uncheck
Interface:	WAN
Address Family:	IPv4
Protocol:	TCP
Source:	Any
Source Port:	Any
Destination:	Any
Destination Port:	443 (HTTPS)
Description:	All configuration and management of ICS-Defender from WAN

Save and apply the rule and it should resemble the following. Enter the WAN Interface IP into a web-browser remembering to use HTTPS://xxx.xxx.xxx.xxx to manage ICS-Defender.



```
□ ✓  1 /10.78 MiB   IPv4 TCP   *   *   *   443 (HTTPS)   *   none   Allow configuration of ICS-Defender from WAN
```

To enable managing from a jump server or specified IP address, edit the rule and set Source to "Single Host or Alias" and enter the IP address of the "jump server" as the source. Note, this should be done with static or IP addresses that are reserved and always assigned to the same PC. In this example, 172.21.0.115 is the laptop used for configuration.



```
□ ✓  2 /10.81 MiB   IPv4 TCP   172.21.0.115   *   *   443 (HTTPS)   *   none   Allow configuration of ICS-Defender from WAN
```

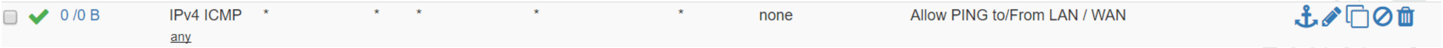
Ping ICS-Defender from WAN or LAN

By default, ICS-Defender will not respond to a PING request (ping is a function of a protocol called ICMP). To enable PING responses from ICS-Defender on either the LAN or the WAN interface a firewall rule must be created to do so.

To ping the WAN, navigate to **Firewall→ Rules→ WAN** and add a rule. To create the rule on the LAN navigate to **Firewall→ Rules→ LAN** instead.

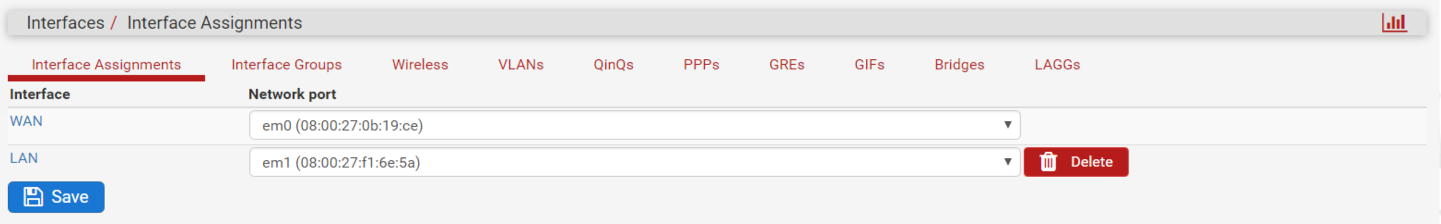
Action:	Pass
Disabled:	Uncheck
Interface:	WAN for WAN Interface, LAN for LAN Interface.
Address Family:	IPv4
Protocol:	ICMP (optionally specify “echo request” and “echo response”)
Source:	Any
Source Port:	Any
Destination:	Any
Destination Port:	Any
Description:	Allow PING to/From LAN / WAN

Create or move this rule to the top of the rules list on the respective interface to be evaluated first as the rules are being processed.



□	✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none	Allow PING to/From LAN / WAN	⚓✎⧉⊘🗑

Interfaces



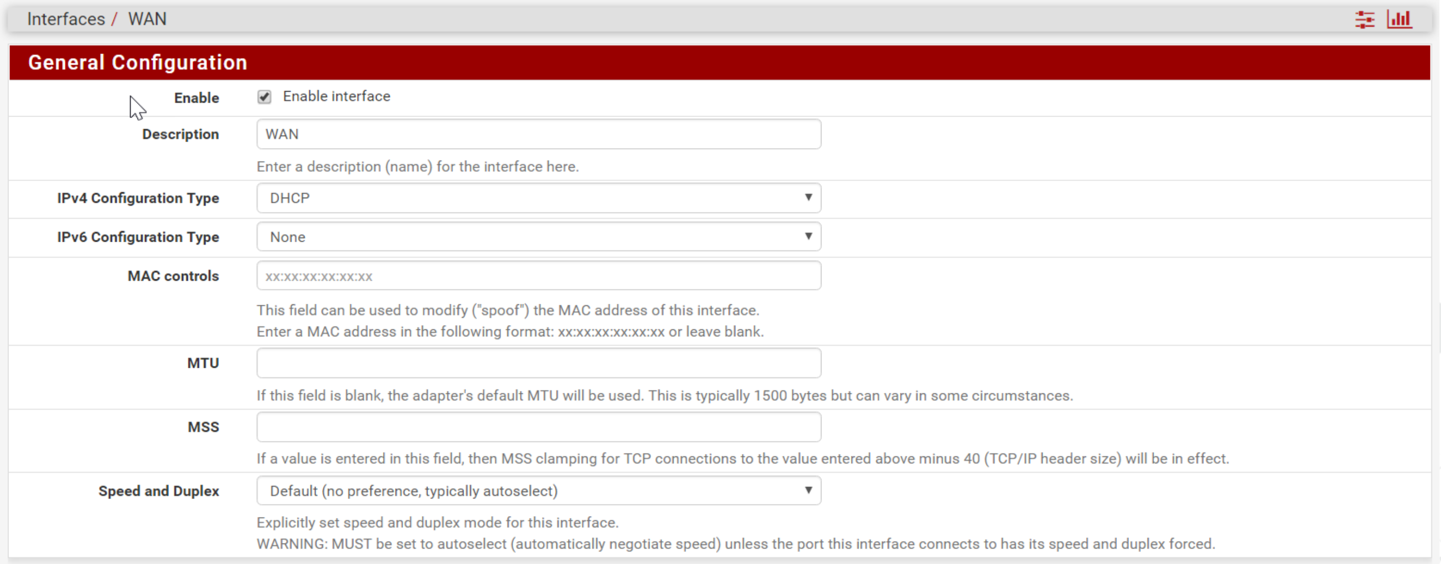
Interface	Network port
WAN	em0 (08:00:27:0b:19:ce)
LAN	em1 (08:00:27:f1:6e:5a)

There are two interfaces which include default names, WAN and LAN. Adding additional interfaces will generate defaults names such as OPT1, OPT2, etc. The WAN and LAN interfaces can be renamed. In many industrial settings, it's common to rename the LAN interface with a name more closely aligned to the network on the "Inside" of the appliance. For example, renaming the LAN interface to "PA" for process area network or "Fieldbus" may be more descriptive and helpful to those less familiar with the application of the appliance.

Naming Guidelines

Interface names may only contain letters, numbers, and underscores.

General Configuration



Enable	☑ Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	None
MAC controls	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 (TCP/IP 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.

Enable: Checking this box enables the interface.

Description: The name assigned to the interface.

IPv4 Configuration Type: The method by which this interface will be assigned an IPv4 address. Typically, in an industrial environment, a static IP address is assigned and that static IP address has a reservation set in the upstream DHCP server so that duplicate addressing can't occur. Selecting a type other than static will result in additional configuration entry sections and fields becoming visible. DHCP may also be used on the WAN interface if desired. For any needs regarding this feature-set options beyond Static or DHCP, please contact Dynics.

IPv6 Configuration Type: The method by which this interface will be assigned an IPv6 address. Additional documentation is in development for details surrounding the use of IPv6.

MAC Controls: By default, physical interfaces are assigned the MAC address of the physical hardware or NIC. In some cases, when replacing an appliance due to an issue with the appliance, it may be necessary to “clone” the MAC address of the appliance being replaced. ICS-Defender allows a MAC address to be entered which overrides the hardware MAC address of the interface. It is important to note that cloning the MAC address is not recommended. There are several cases in which this might be desirable but those cases are rare. For example, if there is a concern that about upstream ARP caches and upstream routers. In some cases, upstream systems use static ARP or somehow filters on MAC address. Cable modems often use the MAC address of the downstream router/device so if ICS-Defender is deployed via remote connectivity using a cable modem, this may be necessary until a new MAC can be registered with the service provider.

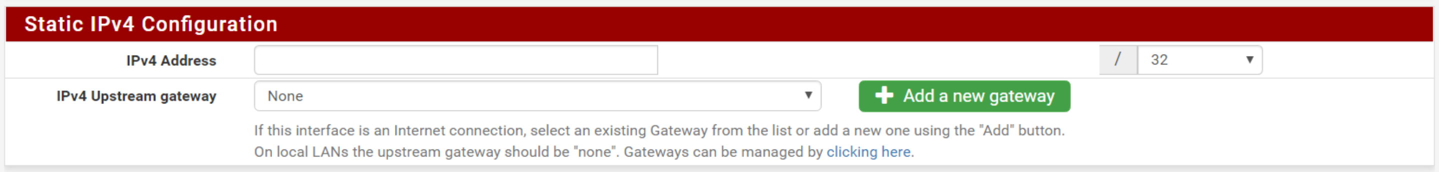
To return to using the hardware MAC, clear the MAC address entry field and restart ICS-Defender.

MTU: Allows overriding the hardware NICS default MTU. Default setting is blank.

MSS: When a value is configured, MSS clamping for TCP connections to the entered value (minus 40 for TCP/IP header size) will be enabled. Default setting is blank.

Speed and Duplex: Set to “Default” will enable full auto-negotiation. Selecting a setting other than “Default” will force the interface to the selection.

Static IPv4 Configuration



Static IPv4 Configuration

IPv4 Address: / 32

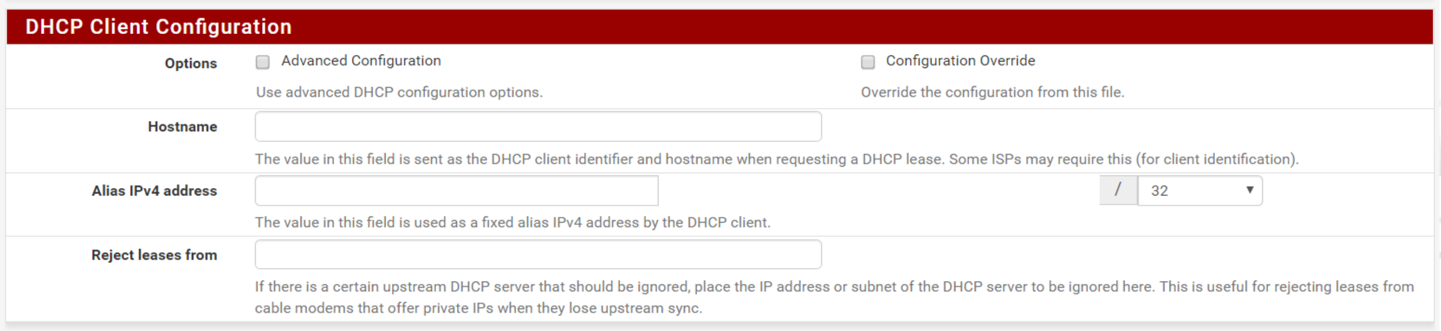
IPv4 Upstream gateway: None

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 LANs the upstream gateway should be "none". Gateways can be managed by clicking here.

IPv4 Address: Enter the four octet IPv4 address to be assigned to this interface and select the subnet mask from the CIDR drop down menu. Subnet Mask to CIDR conversion is provided in Subnet Mask to CIDR Quick Reference.

IPv4 Upstream Gateway: On a controls network or local LAN, the default setting of “None” typically applies. If this interface connects to an upstream network, a gateway is generally necessary. Consult with the corporate networking team for the appropriate gateway address to use and select + Add a new gateway to add it to the configuration and interface or select it if already configured and available in the drop-down list.

IPv4 DHCP Configuration



DHCP Client Configuration

Options	□ Advanced Configuration Use advanced DHCP configuration options.	□ Configuration Override Override the configuration from this file.
Hostname	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).	
Alias IPv4 address	The value in this field is used as a fixed alias IPv4 address by the DHCP client.	/ 32 ▾
Reject leases from	If there is a certain upstream DHCP server that should be ignored, place the IP address or subnet of the DHCP server to be ignored here. This is useful for rejecting leases from cable modems that offer private IPs when they lose upstream sync.	

Options: Advanced Configuration & Configuration Override. For any needs regarding this feature-set, please contact Dynics.

Hostname: Default is Empty. Some ISP's may require a DHCP client identifier and hostname when requesting a DHCP lease. Typical configurations will not require a value other than empty.

Alias IPv4 address: The value in this field is used as a fixed alias IPv4 address by the DHCP client. This option is useful for accessing a device on a separate, statically numbered network, outside of the scope of DHCP.

Reject leases from: Reject leases allows entry of an IPv4 address of a DHCP server that should be ignored. In other words, when a response is received from a DHCP server, whose IP address is defined here, it will be ignored.

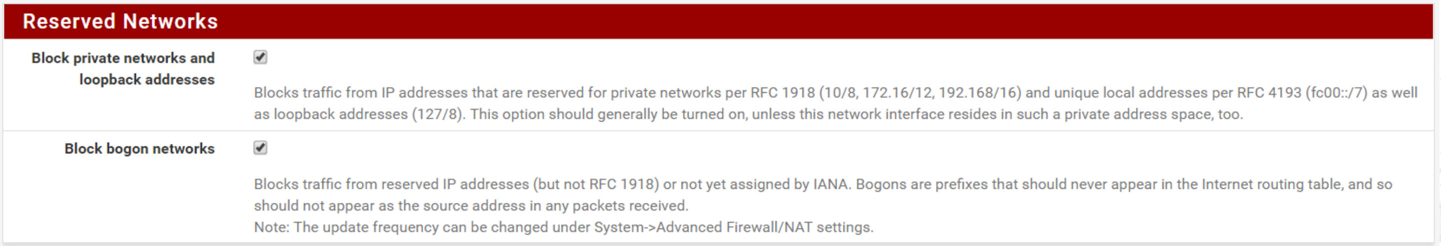
PPP, PPPoE, PPTP, and L2TP

For any needs regarding this feature-set, please contact Dynics.

IPv6 & IPv6 DHCP

For any needs regarding this feature-set, please contact Dynics.

Private and Bogon Network Options



Reserved Networks

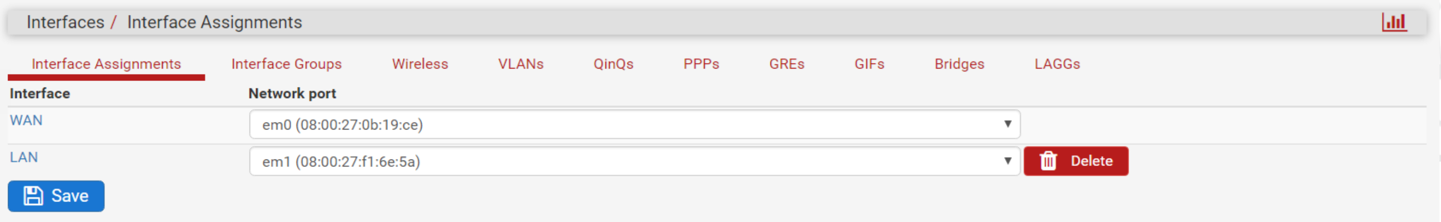
Block private networks and loopback addresses	☑ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless 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. Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Block private networks and loopback addresses: ICS-Defender will insert a rule automatically that will prevent any RFC 1918 networks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) and loopback (127.0.0.0/8) from communicating on that interface. This option is usually only desirable on WAN type interfaces, to prevent the possibility of privately numbered traffic coming in over a public interface. ***Note: If this interface is a controls network or local LAN, disable this option.***

Block bogon networks: Block traffic from unallocated or reserved IP addresses. Bogons are prefixes which should not appear in an internet routing table and thus should not appear in the source address in any packets received.

Physical and Virtual Interfaces

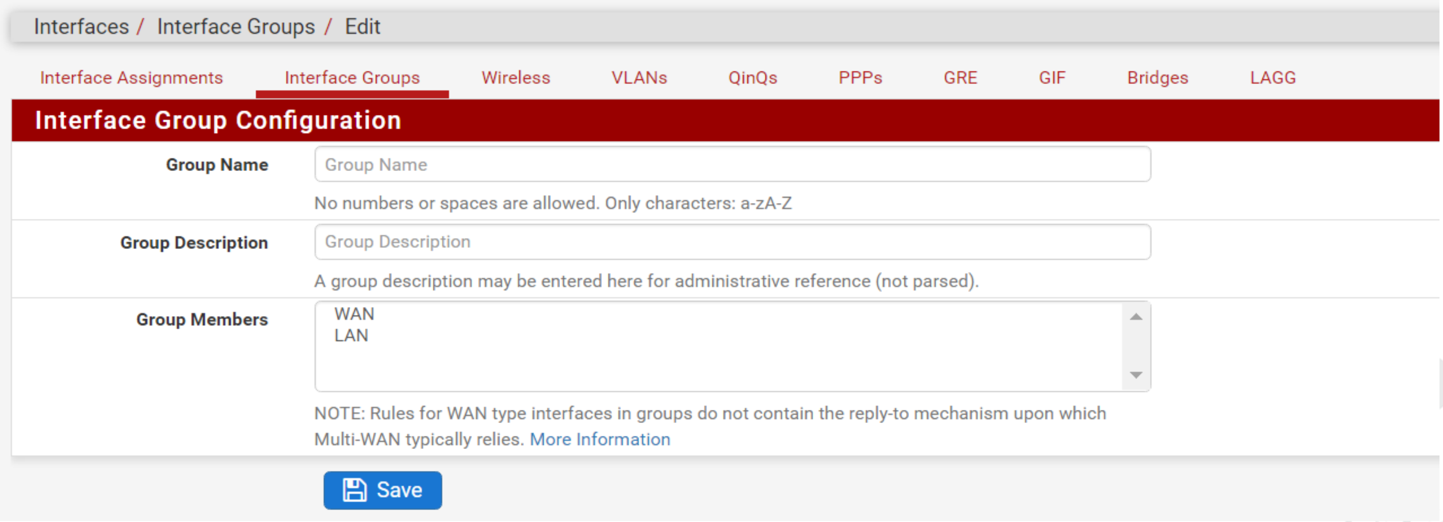
Interfaces discussed in this section can be used as **WAN**, **LAN**, or an **OPT**ional interface under **Interfaces→ Interface Assignments.**



Interface	Network port
WAN	em0 (08:00:27:0b:19:ce)
LAN	em1 (08:00:27:f1:6e:5a)

Various combinations of options are available to use the interfaces themselves, or use multiple networks and protocols on single interface. For example, on a single physical NIC, both a control device network could be setup on 192.168.1.0 and a switch management network could be setup on 192.168.101.0. This would allow access to both networks via the same physical NIC. Multiple VLANS can even be assigned to a single interface via use of virtual interfaces.

Interface Groups



Interface Group Configuration

Group Name: Group Name

No numbers or spaces are allowed. Only characters: a-zA-Z

Group Description: Group Description

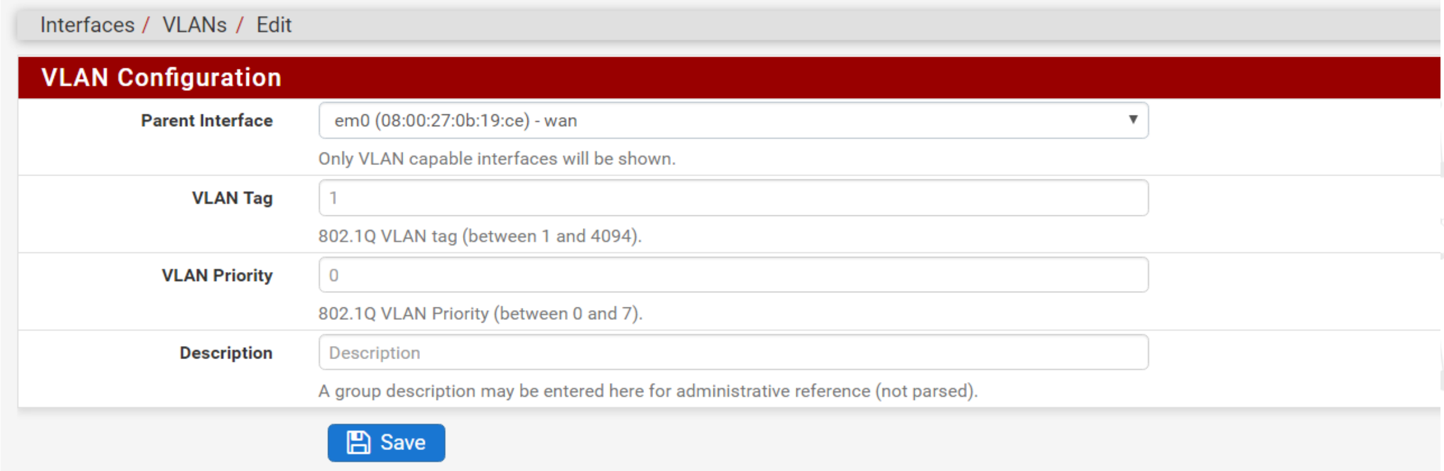
A group description may be entered here for administrative reference (not parsed).

Group Members: WAN
LAN

NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. More Information

Interface groups allow interfaces to be grouped together under a single name to aid in applying firewall or NAT rules to multiple interfaces simultaneously.

VLANS



Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface	em0 (08:00:27:0b:19:ce) - wan Only VLAN capable interfaces will be shown.
VLAN Tag	1 802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).
Description	Description A group description may be entered here for administrative reference (not parsed).

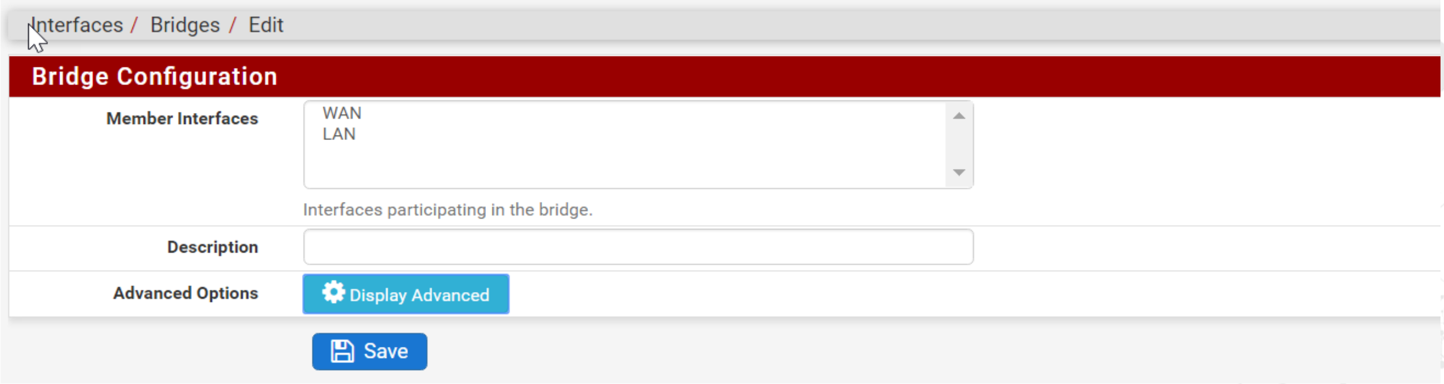
The VLANS tab allows an interface to be assigned and used for a specific VLAN. VLANS are covered in more detail in **<Virtual LANS>**.

QinQ, PPPs, GREs, GIFs and LAGGS

For any needs regarding this feature-set, please contact Dynics.

Bridge Connections

Creating a bridge allows multiple ports may be bound together. Each bridge created via the WebGUI will create a bridge interface in the system. These bridge interfaces will show up and can be assigned and used like any other interface in the system.



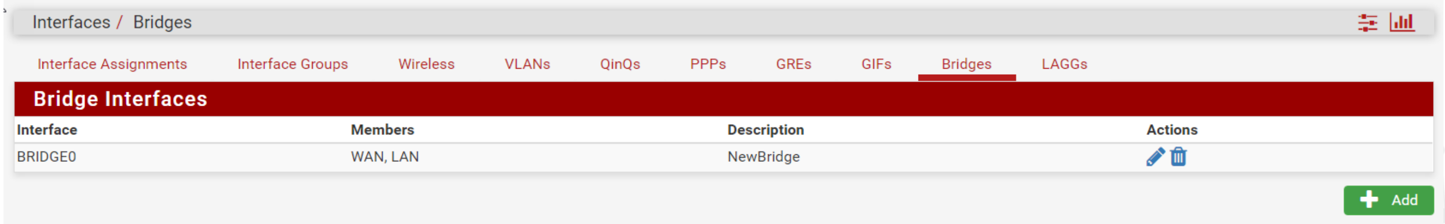
Interfaces / Bridges / Edit

Bridge Configuration

Member Interfaces	WAN LAN Interfaces participating in the bridge.
Description	
Advanced Options	Display Advanced

Creating a bridge between interfaces requires selection of the participating interfaces and saving the configuration. Hold down the CTRL key to select multiple interfaces.

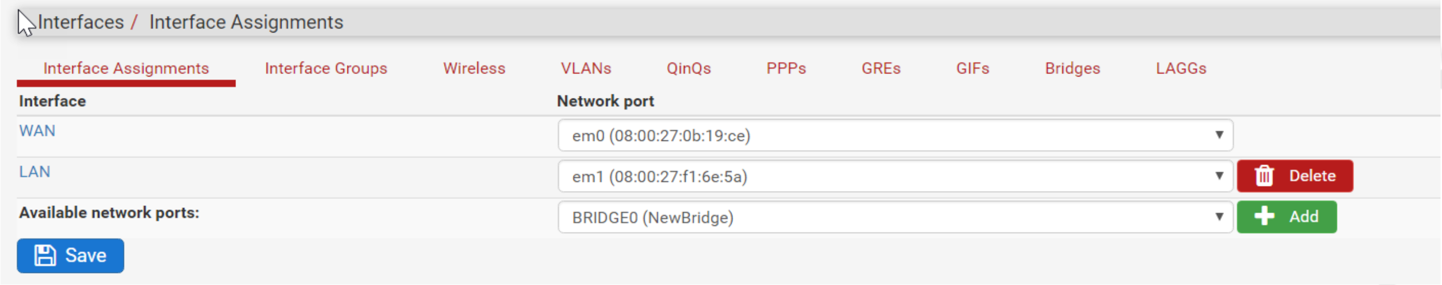
In this example, once a bridge is created with the WAN and LAN interfaces it is listed under **Interfaces→ Bridges**. Bridges are created numerically (BRIDGE0, BRIDGE1, BRIDGE2, etc.)



Bridge Interfaces

Interface	Members	Description	Actions
BRIDGE0	WAN, LAN	NewBridge	

Under **Interfaces→Interface Assignments**, the newly created bridge is listed and available to be added to the system as any physical interface or virtual interface could be added and configured.



Interface	Network port
WAN	em0 (08:00:27:0b:19:ce)
LAN	em1 (08:00:27:f1:6e:5a)
Available network ports:	BRIDGE0 (NewBridge)

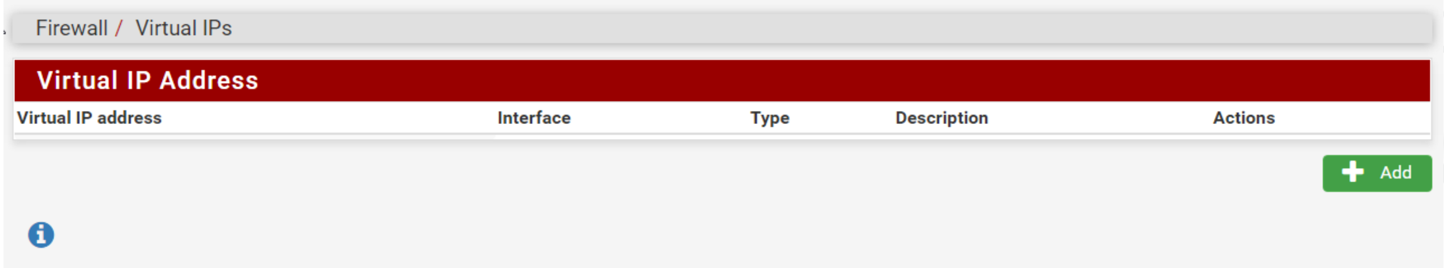
Advanced Bridge Options

For any needs regarding this feature-set, please contact Dynics.

Virtual IP Address

Multiple WAN IP addresses can be used in conjunction with NAT or other services through the use of Virtual IP addresses. There are several type of Virtual IP Addresses which include those used for aliasing an IP address, failover (CARP), Proxy ARP and Other.

Virtual IP Addresses can be found at **Firewall → Virtual IPs**.



Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions

Virtual IP Types

IP Alias

An IP Alias behaves exactly like any other IP Address on the interface to which it is assigned. An IP Alias will respond to layer 2 (ARP), ICMP (pings) and can be bound to services such as ICS-Defender failover. They can also be used to handle multiple subnets on the same interface. IP Alias is by far the most common use of a Virtual IP Address.

Proxy ARP

Proxy ARP operates strictly at layer 2. Using Proxy ARP provides ARP replies for the specified IP address or CIDR range of IP addresses. This allows ICS-Defender to forward traffic destined to addresses based on a NAT configuration.

Failover

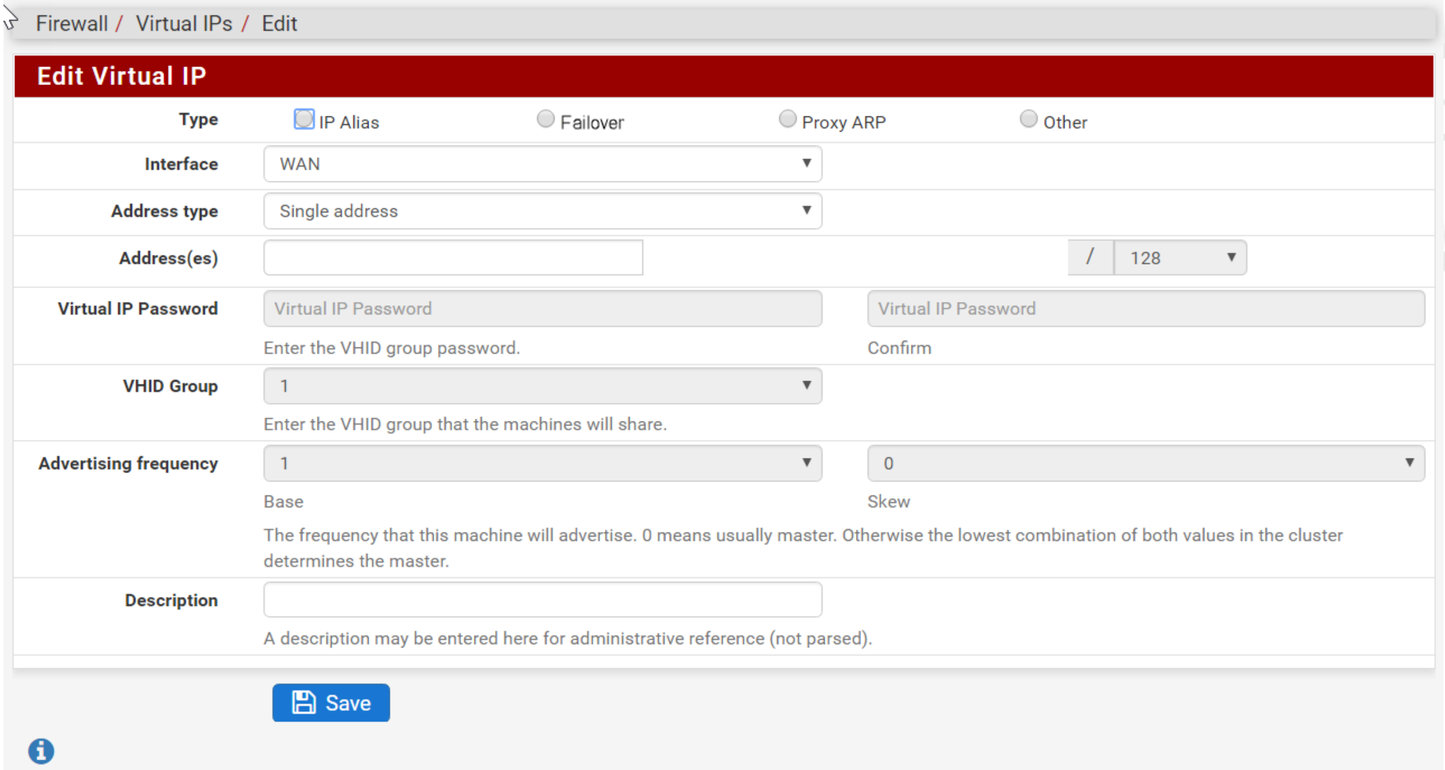
Failover Virtual IP addresses are only used with redundant / high availability configurations.

Other

This option allows definition of additional IP addresses for use when ARP replied for the IP address is not required.

Creating a Virtual IP

Clicking + Add opens the "Edit Virtual IP" screen.



Firewall / Virtual IPs / Edit

Edit Virtual IP

Type	☐ IP Alias ○ Failover ○ Proxy ARP ○ Other	
Interface	WAN ▾	
Address type	Single address ▾	
Address(es)		/ 128 ▾
Virtual IP Password	Virtual IP Password Enter the VHID group password.	Virtual IP Password Confirm
VHID Group	1 ▾ Enter the VHID group that the machines will share.	
Advertising frequency	1 ▾ Base	0 ▾ Skew
	The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.	
Description	 A description may be entered here for administrative reference (not parsed).	

Type: The type check boxes allow specific behaviors for the Virtual IP.

Interface: The interface that the IP Alias exists on, typically WAN or LAN.

Address Type: The address type for the Virtual IP. When selecting all but Proxy ARP, this option defaults to "Single Address" and cannot be changed.

Address(es): The IP address assigned to the Virtual IP. The subnet mask is expressed in CIDR notation. Subnet Mask to CIDR conversion is provided in Subnet Mask to CIDR Quick Reference.

Virtual IP Password: Used for failover configuration only and discussed separately.

VHID Group: Used for failover configuration only and discussed separately.

Advertising Frequency: Used for failover configuration only and discussed separately.

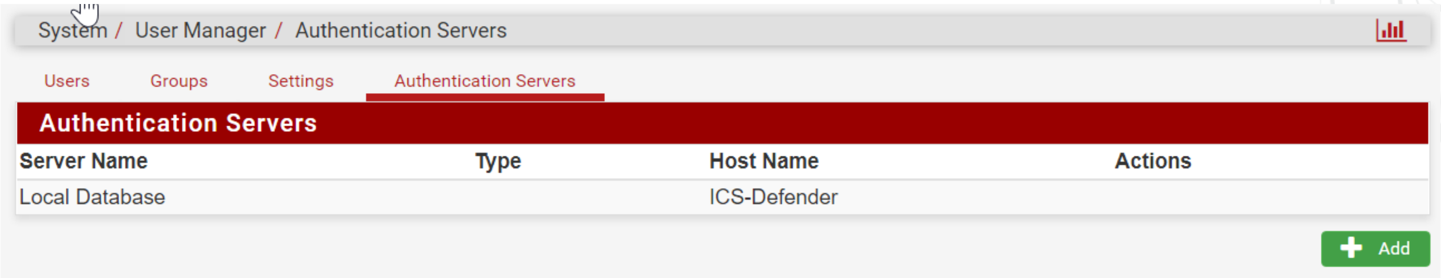
Description: Used for descriptive notes or text regarding the Virtual IP.

User Management

Users are created and managed from within the WebGUI at **System→ User Manager**.

Note: In most cases it's useful to determine ahead of time if ICS-Defender will act as local Certificate Authority or if an enterprise or external certificate authority will be used. Certificates can be assigned to users at a later date if this information is unavailable or undecided at the time the user is created.

Authentication Servers



Authentication Servers

Server Name	Type	Host Name	Actions
Local Database		ICS-Defender	

Local

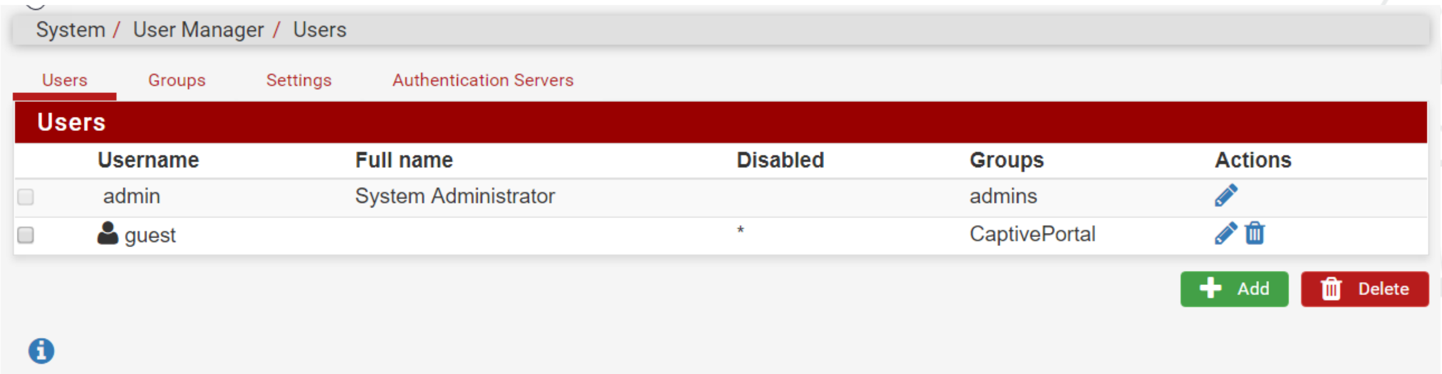
By default, ICS-Defender manages users from an internal database. All privileges and actions are stored locally on the appliance. This allows ICS-Defender to fit well into standalone manufacturing environments which do not have sophisticated user management systems such as Active Directory or RADIUS or there is simply no desire to use anything beyond local management.

LDAP, RADIUS

ICS-Defender Pro supports local user management, LDAP (including Active Directory) and RADIUS authentication for users. For any needs regarding this feature-set, please contact Dynics.

Users

User creation involves two actions. First, creating the user and saving the user. Second, assign the appropriate privileges to the user. The user list is available at **System→ User Manager→Users**.



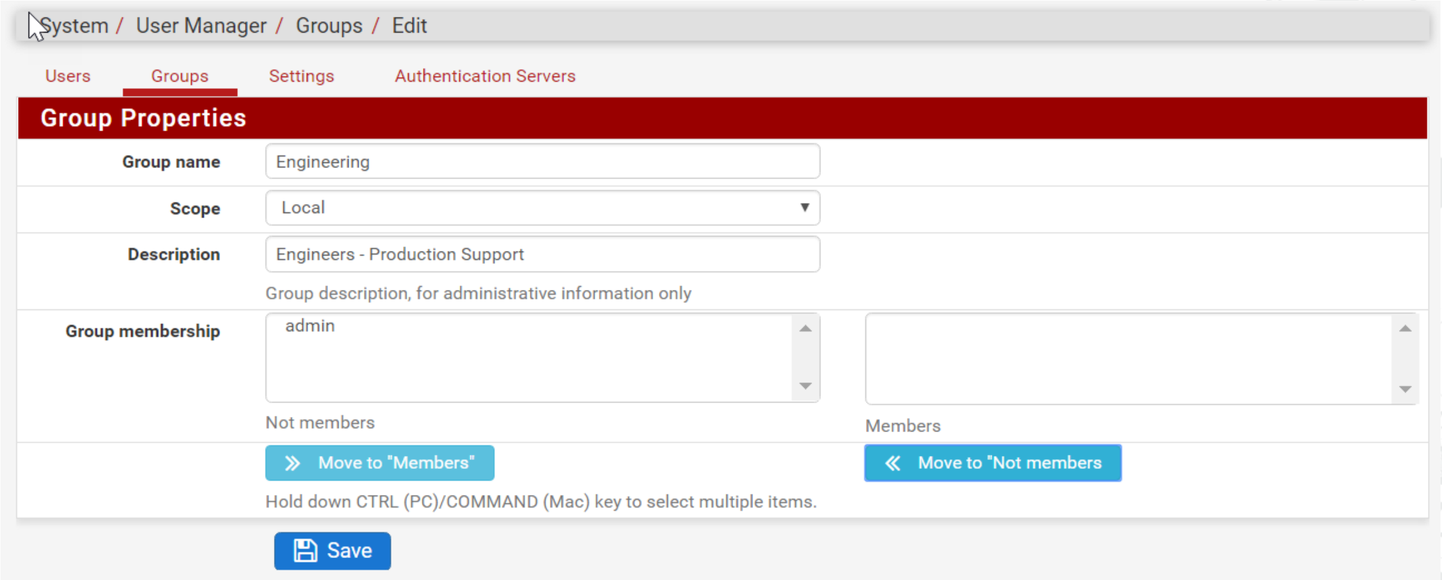
System / User Manager / Users

Users

	Username	Full name	Disabled	Groups	Actions
□	admin	System Administrator		admins	
□	guest		*	CaptivePortal	

Adding a Group

Creating groups before users is a good way to manage groups of users, the permissions can be assigned to the groups once and apply to any users in the group. For example, a typical configuration may include an admin group, engineering group, IT group, and perhaps "view only" group that is able to troubleshoot only, but not make configuration changes. Groups are found at **System→User Manager→Groups**. Groups can be members of other groups.



System / User Manager / Groups / Edit

Group Properties

Group name	Engineering
Scope	Local
Description	Engineers - Production Support Group description, for administrative information only
Group membership	Not members: admin Members:

Move to "Members"
Move to "Not members
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Save

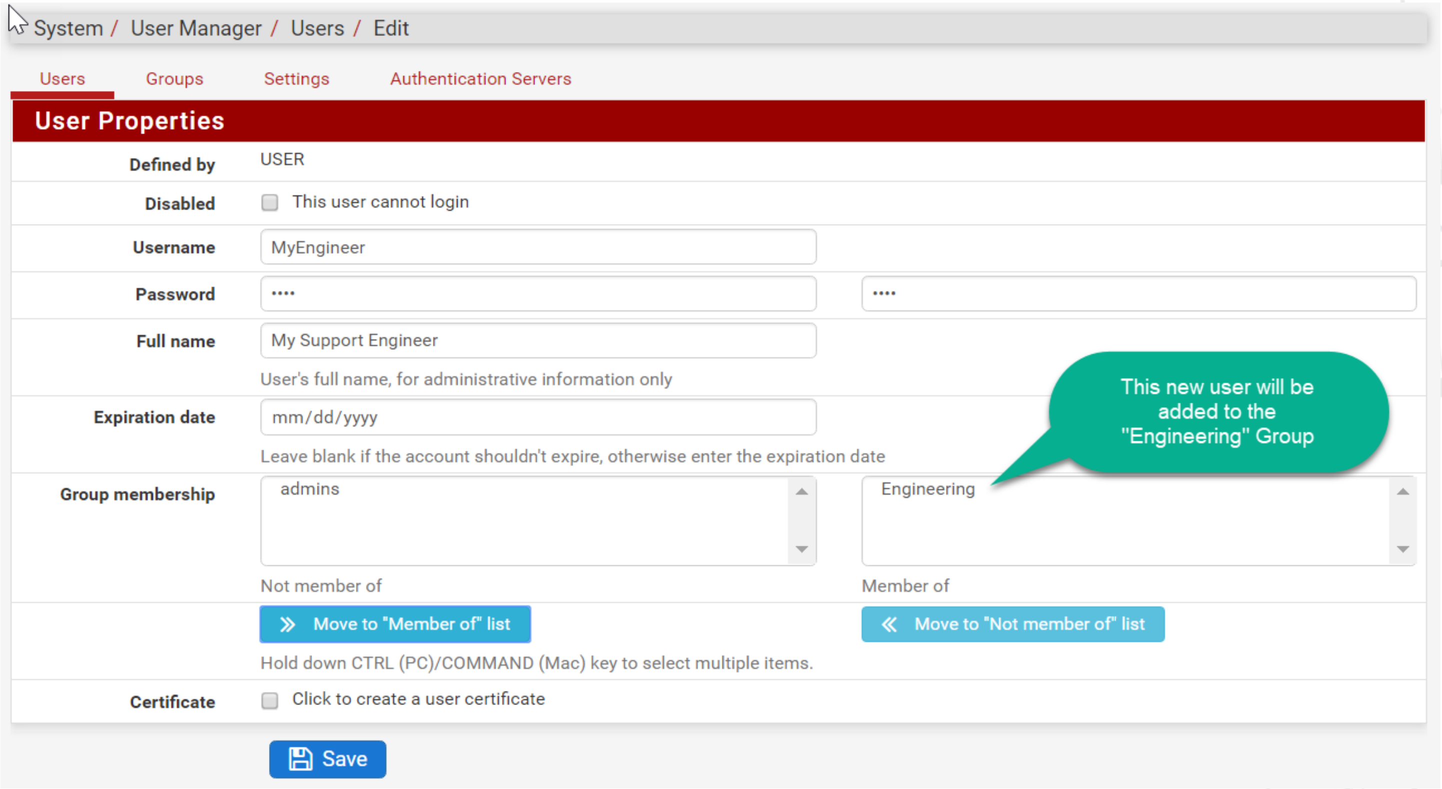
Group Name: The name used to reference the group.

Scope: By default, "Local" is selected meaning the group is managed by the local ICS-Defender.

Description (Optional): A descriptive name for the group, purely for administrative purposes.

Group Membership: If this group should be a member of another group.

Adding a New User



User Properties

Defined by	USER	
Disabled	□ This user cannot login	
Username	MyEngineer	
Password	••••	••••
Full name	My Support Engineer User's full name, for administrative information only	
Expiration date	mm/dd/yyyy Leave blank if the account shouldn't expire, otherwise enter the expiration date	
Group membership	admins Not member of	Engineering Member of
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Certificate	□ Click to create a user certificate	

This new user will be added to the "Engineering" Group

Disabled: This user is disabled and will not be permitted to log into the appliance.

Username: The name the user will log in with. The name of the user can include letters and numbers, but no special character's other than an underscore.

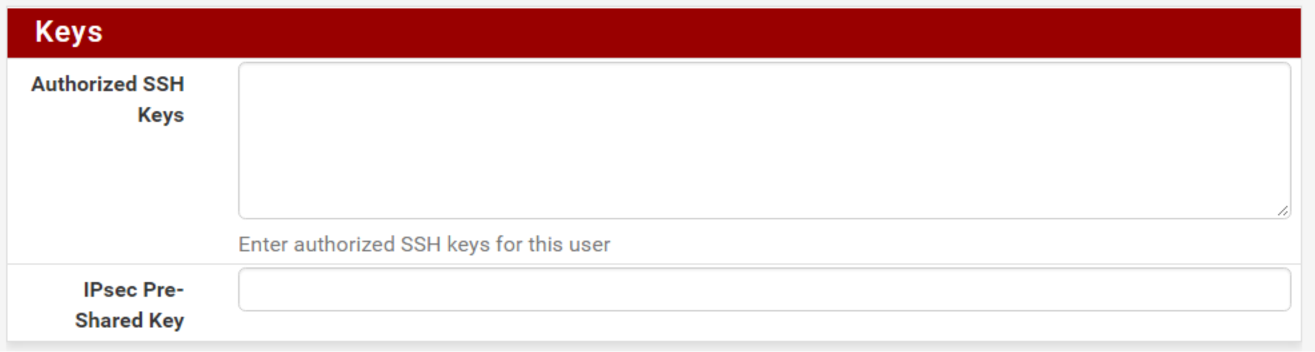
Password: Enter the user's password in this field and the matching password in the "confirm password" field.

Full Name: Enter the users full name for administrative purposes. This field is optional, but recommended.

Expiration Date: Enter the date the user account should expire (automatically disabled) or leave blank for no date. The default duration for a user is 10 years.

Group Membership: Sets this user as a member of a group(s). In this example, the user is assigned to the recently created "Engineering" group.

Keys



Keys

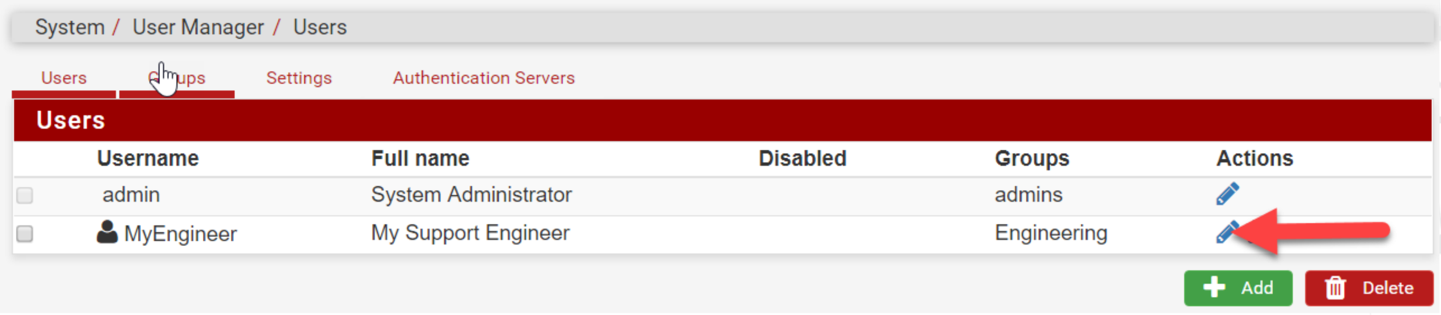
Authorized SSH Keys	Enter authorized SSH keys for this user
IPsec Pre-Shared Key	

Authorized SSH Keys: Default=Blank. For any needs regarding this feature-set, please contact Dynics.

IPsec Pre-Shared Key: Default=Blank. For any needs regarding this feature-set, please contact Dynics.

Assigning Privileges

User privileges and group privileges are assigned in much the same way. After creating and saving a new user or group, edit the group by navigating to **System→ User Manager→Group (or Users)** and clicking the edit ✏ button to the right of the appropriate group (or user).



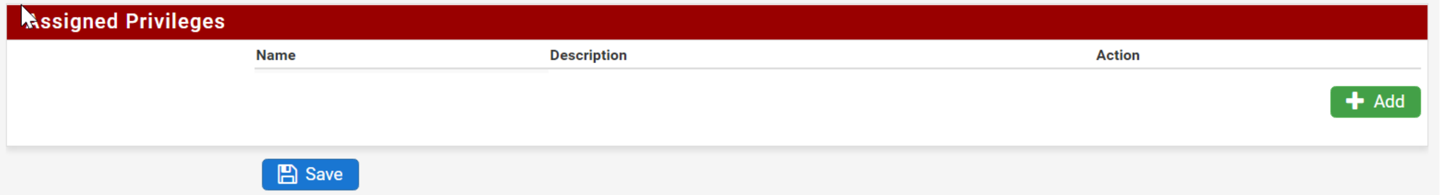
System / User Manager / Users

Users

	Username	Full name	Disabled	Groups	Actions
□	admin	System Administrator		admins	✏
□	MyEngineer	My Support Engineer		Engineering	✏

A new data entry area is now available to add permissions to this group (or user). This option wasn't visible at the time the user or group was initially created. The difference between the data entry area for users or group is the title. For users, they are called "effective privileges" and for groups they are identified as "assigned privileges".

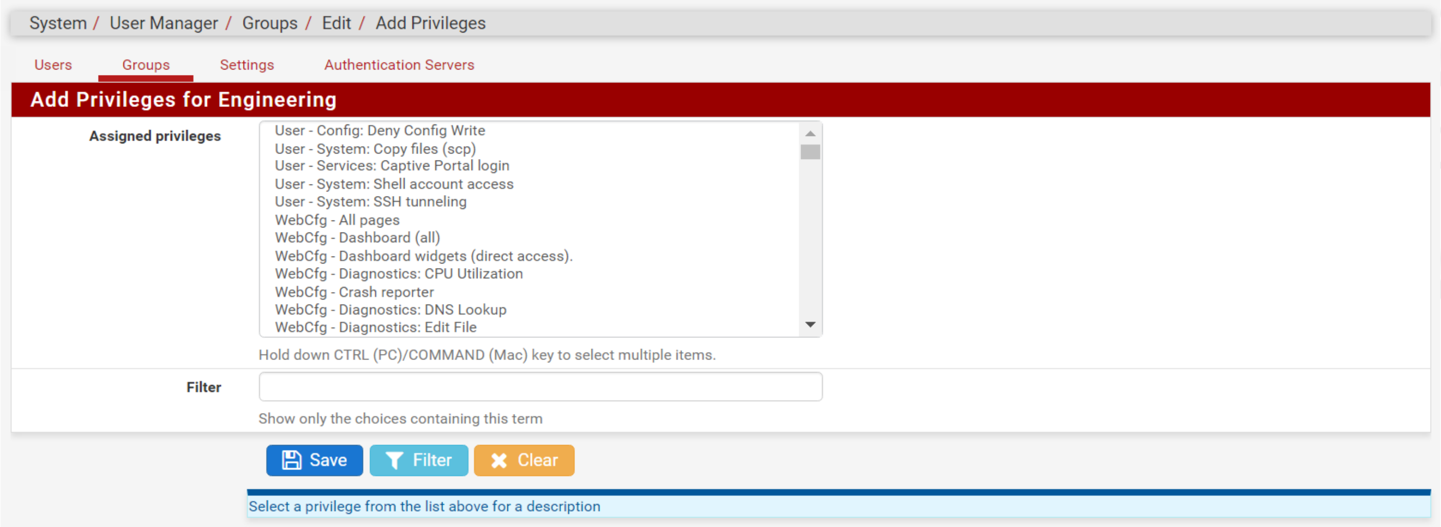
Note: it is highly recommended to assign privileges by group, not individual users.



Assigned Privileges

Name	Description	Action

Clicking the ✚ Add button displays a comprehensive list of permissions. Adding privileges to this list effectively disables all other permissions in this list for the selected group or user. CTRL + mouse click selects individual, CTRL + A selects the entire list.



Add Privileges for Engineering

Assigned privileges

User - Config: Deny Config Write
User - System: Copy files (scp)
User - Services: Captive Portal login
User - System: Shell account access
User - System: SSH tunneling
WebCfg - All pages
WebCfg - Dashboard (all)
WebCfg - Dashboard widgets (direct access).
WebCfg - Diagnostics: CPU Utilization
WebCfg - Crash reporter
WebCfg - Diagnostics: DNS Lookup
WebCfg - Diagnostics: Edit File

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

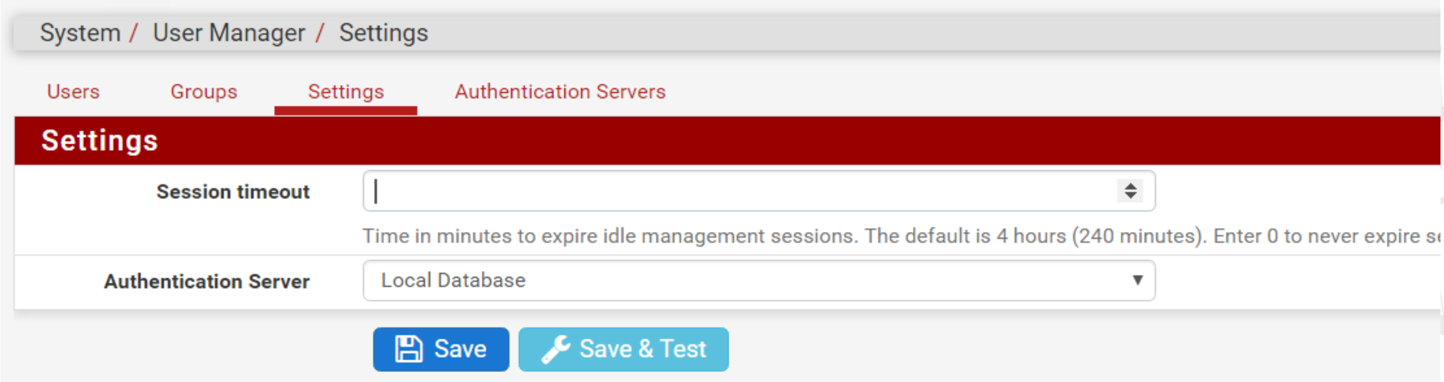
Select a privilege from the list above for a description

Once selected, click save and the permissions are assigned to the user or group.

The assigned permissions are displayed. From this screen, individual permissions can be removed by clicking the 🗑 trashcan icon to the right of the desired permission.

Settings

The **System→User Manager→Settings** configuration is used to configure basic behaviors of the user manager.



Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire se

Authentication Server: Local Database

Session Timeout: This setting determines how long to wait before terminating an idle management session. If a user connects to the appliance with administrative privileges and does not log out, this setting will determine how long to wait before automatically logging that user out. The default is 4 hours, setting this to 0 will disable auto-logout. Note:

Disabling automatic logging out is not recommended. Setting this value to a number less than the default of 240 minutes (4 hours) is.

Authentication Server: The selected method of authentication. Local Database, LDAP (active directory), or RADIUS. The default is local database and is the only method displayed in the dropdown unless either LDAP or RADIUS are defined on **System→User Manager→Authentication Servers**. Refer to Authentication Servers for more information.

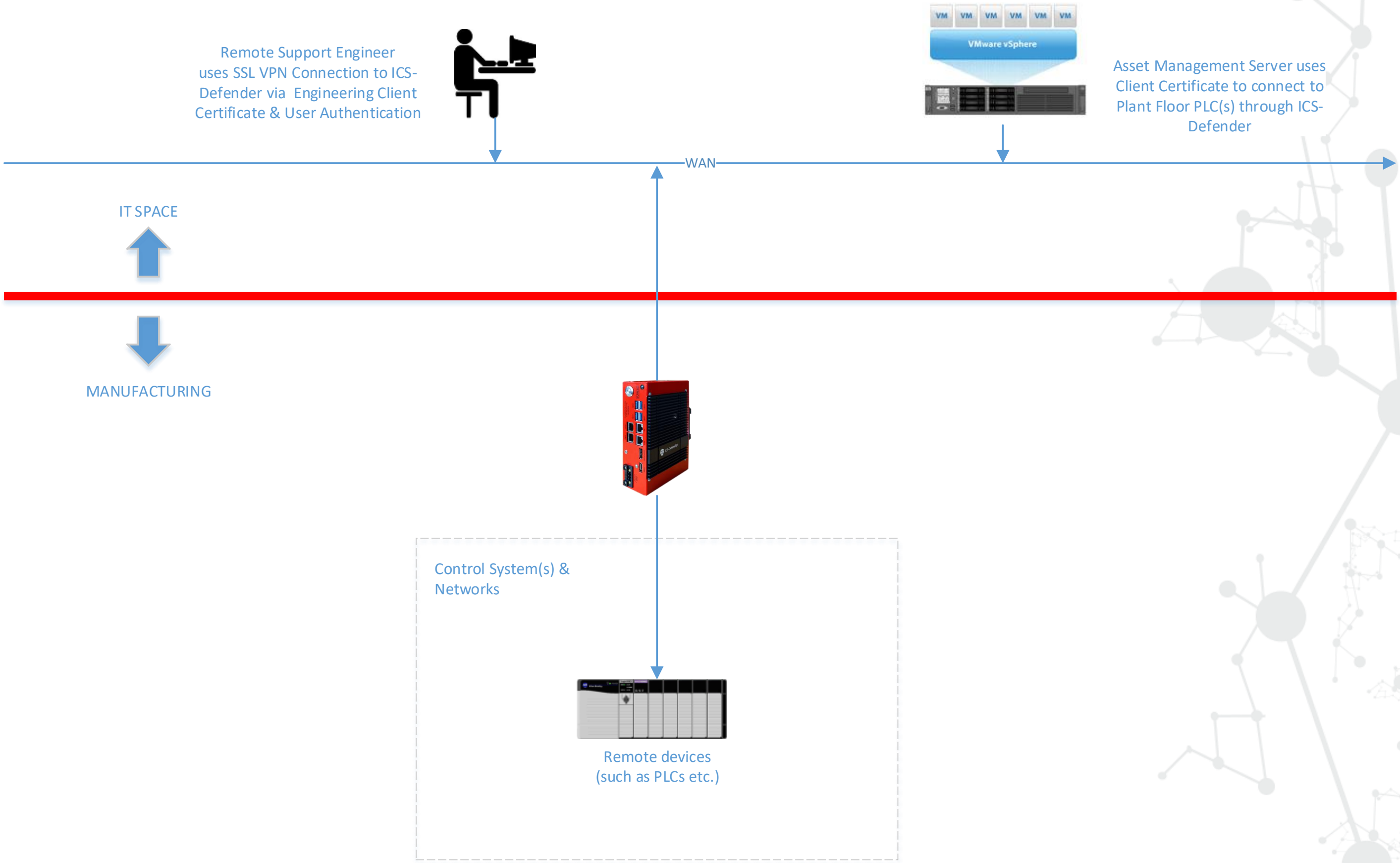
Certificate Management

Certificates are an important part of securing connectivity to and from a control system or plant floor network. This is true primarily for users but also for external systems, such as a server, to access plant floor equipment such as a PC, PLC, or other device.

Why use Certificates?

There are two types of certificates used in ICS-Defender, server certificates and client certificates. Server certificates are used to identify the owner of a host, such as an ICS-Defender at ics-defender@localdomain (the example name used in the Step #1 - General setup of this document. Client certificates are used to identify the client/individual that is accessing a server such as connecting via an SSL VPN to an ICS-Defender. Certificates make sure that the connection between the client and the server isn't listened to by an outside entity.

The example diagram shows both an asset management server (such as Rockwell's AssetCentre" and a user connecting to plant floor devices. Each connection is using a client server certificate to make the connection is secure.


Remote Support Engineer uses SSL VPN Connection to ICS-Defender via Engineering Client Certificate & User Authentication
VM
VMware vSphere
Asset Management Server uses Client Certificate to connect to Plant Floor PLC(s) through ICS-Defender
WAN
IT SPACE
MANUFACTURING
Control System(s) & Networks
Remote devices (such as PLCs etc.)

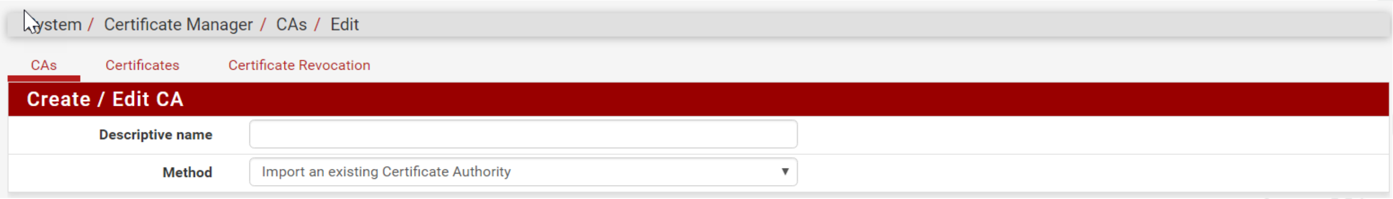
Certificate Authority

ICS-Defender can act as its own internal certificate authority (CA) or utilize a certificate authority already established in an organization. For standalone or small control systems, acting as the certificate authority can be very beneficial. In larger systems, connected to more advanced networks, such as enterprise grade networks with existing certificate authorities, it allows use of a centralized authority without having to manage it locally on a given ICS-Defender.

This section covers what is necessary to use ICS-Defender with an internal certificate authority. For information regarding connecting to a remote certificate authority, please contact Dynics.

Important: The CA created here will likely be used as a basis, and once assigned and used can't be changed. It can be very time consuming if the email address must be changed in a CA for example, a new CA must be created and significant effort is required to change all downstream configuration to the new CA. A good practice is to create a set of data for this CA (user, town, email etc.) that is not going to be a problem later if the equipment is moved, or an employee of the company leaves.

Navigate to **System→ Cert. Manger** to add a certificate authority. Clicking the + Add button displays the necessary entry fields to create a certificate authority.



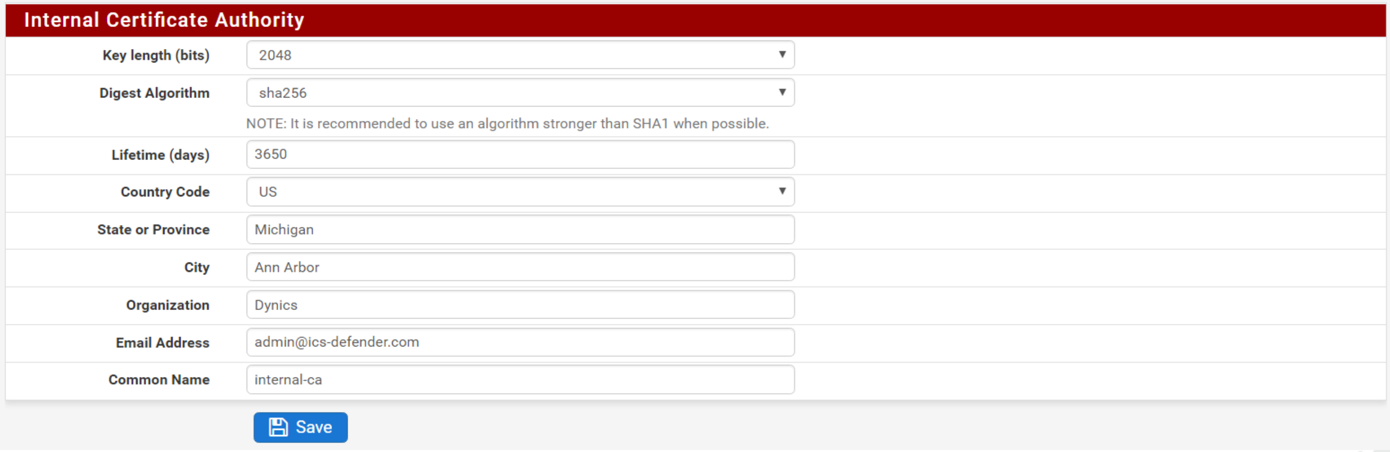
System / Certificate Manager / CAs / Edit

CAs Certificates Certificate Revocation

Create / Edit CA

Descriptive name	
Method	Import an existing Certificate Authority ▼

Descriptive Name: The name by which this CA will be identified.
Method: The default is to "Import an existing Certificate Authority", change this option to "Create an Internal Certificate Authority". Doing so will display the settings necessary to create a unique CA.



Internal Certificate Authority

Key length (bits)	2048 ▼
Digest Algorithm	sha256 ▼ NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Lifetime (days)	3650
Country Code	US ▼
State or Province	Michigan
City	Ann Arbor
Organization	Dynics
Email Address	admin@ics-defender.com
Common Name	internal-ca

Save

In almost all cases, leaving the Key Length (bits), Digest Algorithm, and Lifetime (days) fields at their defaults is recommended. The only exception might be the Lifetime (days) as the default of 3650 is 10 years.

Country Code: The country code for the CA.

State or Province: The state or province to assign to the CA.

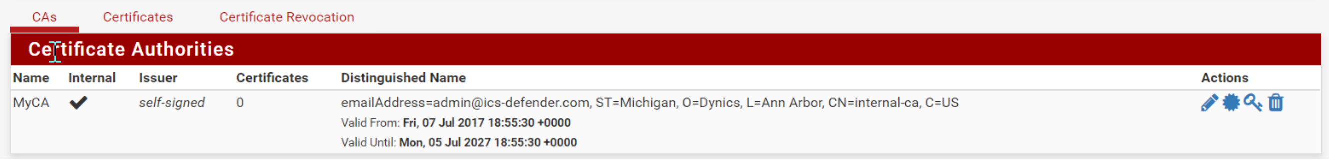
City: The city to assign to the CA.

Organization: Company name is recommended.

Email Address: A unique, non-person specific email address is recommended. Perhaps ics-defender@<your-company.com>, or ics-security@<your-company.com>.

Common Name: Default is “internal-ca”. Should not need to change.

Once saved, the certificate shows in the list and can be exported along with the key.



Certificate Authorities

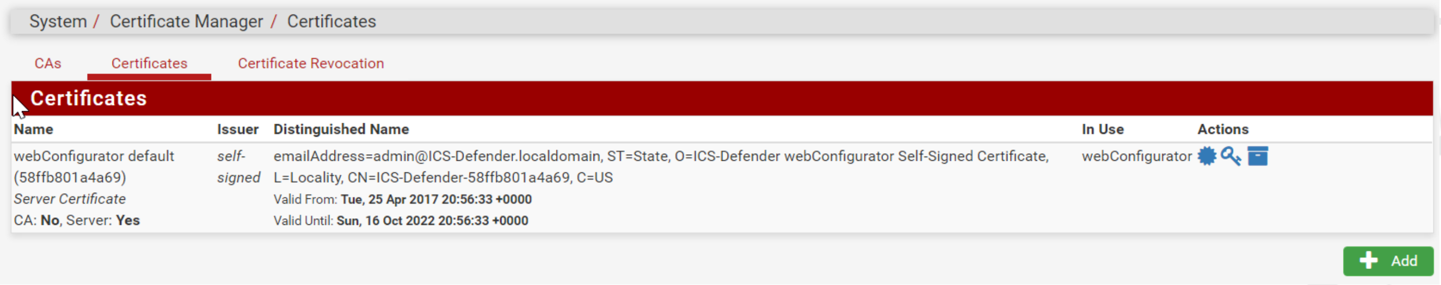
Name	Internal	Issuer	Certificates	Distinguished Name	Actions
MyCA	✓	*self-signed*	0	emailAddress=admin@ics-defender.com, ST=Michigan, O=Dynics, L=Ann Arbor, CN=internal-ca, C=US Valid From: **Fri, 07 Jul 2017 18:55:30 +0000** Valid Until: **Mon, 05 Jul 2027 18:55:30 +0000**	

Important: If a private key for a certificate authority is exported, an attacker could generate new certificates that would be valid against the certificate authority.

User and Server Certificates

Certificates are created and managed by navigating to System→Cert. Manager→Certificate tab where they can be added, edited, exported, or deleted.

Certificates for a user requiring user authentication as well as the certificate to connect to ICS-Defender can also be created from the user manager by editing an existing user.

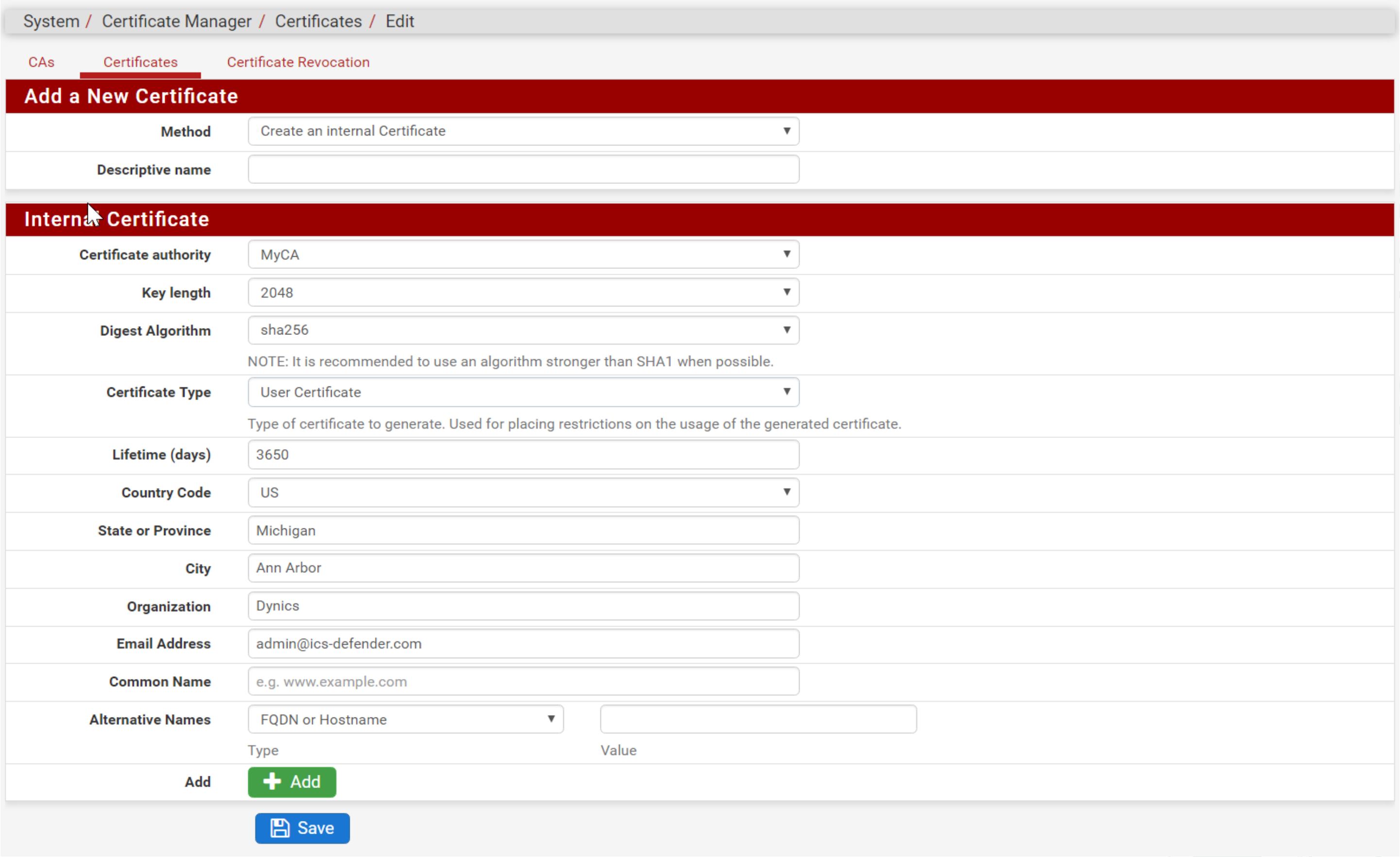


Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (58ffb801a4a69) *Server Certificate* CA: **No**, Server: **Yes**	*self-signed*	emailAddress=admin@ICS-Defender.localdomain, ST=State, O=ICS-Defender webConfigurator Self-Signed Certificate, L=Locality, CN=ICS-Defender-58ffb801a4a69, C=US Valid From: **Tue, 25 Apr 2017 20:56:33 +0000** Valid Until: **Sun, 16 Oct 2022 20:56:33 +0000**	webConfigurator	

ICS-Defender creates an automatic server certificate to allow access to the WebGUI. Additional certificates can be created for users. How many and what is used for server certificates will depend upon the level of security required by each organization. User certificates will also be dependent upon the level of security desired by the organization.

At various places in the configuration of an ICS-Defender, the user interface will allow you to create a certificate to match the content being configured. For example, when creating a VPN Server, the configurator will specify a server certificate. In general, server certificates are used for VPN or HTTPS servers, the certificate can only be used in a server role. Client certificates are used to connect to VPN servers but are not capable of being used as a server. This prevents a user from using their own certificate to impersonate a server.



System / Certificate Manager / Certificates / Edit

Add a New Certificate

Method	Create an internal Certificate
Descriptive name	

Internal Certificate

Certificate authority	MyCA
Key length	2048
Digest Algorithm	sha256 NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.
Certificate Type	User Certificate Type of certificate to generate. Used for placing restrictions on the usage of the generated certificate.
Lifetime (days)	3650
Country Code	US
State or Province	Michigan
City	Ann Arbor
Organization	Dynics
Email Address	admin@ics-defender.com
Common Name	e.g. www.example.com
Alternative Names	FQDN or Hostname (Type), Value
Add	Add

Method: Set this to "Create an internal Certificate"

Descriptive Name: The name of the certificate. It may be useful to prefix the certificate with a SC or CC followed by an underscore and description. For example, a Server Certificate used by a VPN Server for Remote Access might be SC_RemoteAccess and the client certificate to access that remote access server may be prefixed with CC_ for Client Certificate.

Certificate Authority: By default, the internal CA that was created is selected. By selecting a CA, the values for country code through email address are auto-populated.

Key Length: The larger the number, the more secure the certificate is with regard to encryption. However, larger numbers will also require more CPU time to process. The default value of 2048 shouldn't be changed unless necessary.

Digest Algorithm: Leave at the default of sha256.

Certificate Type: Create a user or server certificate.

Lifetime (days): The number of days the certificate is valid (10 years).

Country Code: The country code for the CA.

State or Province: The state or province to assign to the CA.

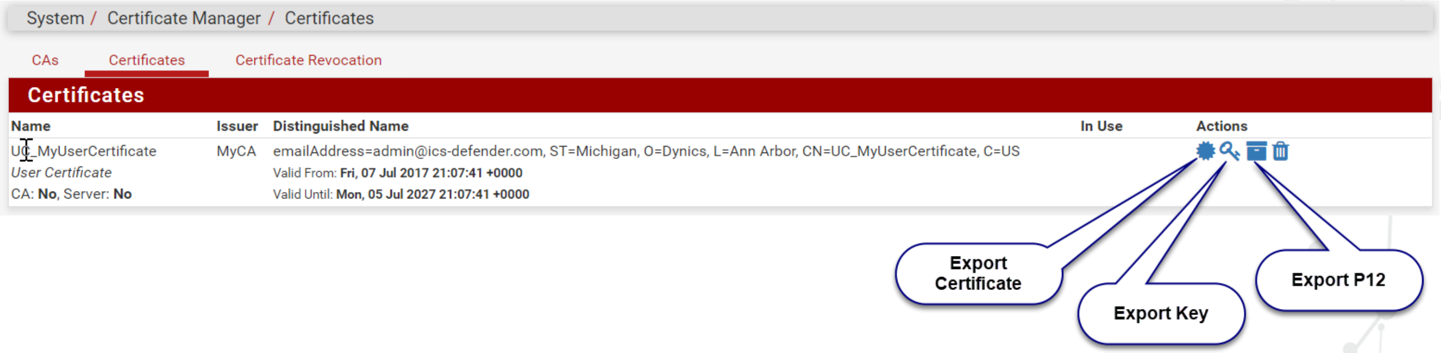
City: The city to assign to the CA.

Organization: Company name is recommended.

Email Address: A unique, non-person specific email address is recommended. Perhaps ics-defender@<your-company.com>, or ics-security@<your-company.com>.

Common Name: The common name for a certificate should be a hostname (ICS-DefenderSSPPLL01) for a server certificate or username or group of users for a client certificate.

Once saved, the certificate is created and the components can be exported if necessary.



System / Certificate Manager / Certificates

CAs   Certificates   Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
UC_MyUserCertificate *User Certificate* CA: **No**, Server: **No**	MyCA	emailAddress=admin@ics-defender.com, ST=Michigan, O=Dynics, L=Ann Arbor, CN=UC_MyUserCertificate, C=US Valid From: **Fri, 07 Jul 2017 21:07:41 +0000** Valid Until: **Mon, 05 Jul 2027 21:07:41 +0000**		

Certificate Revocation List

Certificates can be revoked by using certificate revocation. Common practice is to create one certificate revocation list per certificate authority (CA). However, in ICS-Defender, multiple revocation lists can be created for a single CA. Certificate Revocation Lists are created at **System→Cert. Manager→Certificate Revocation**.

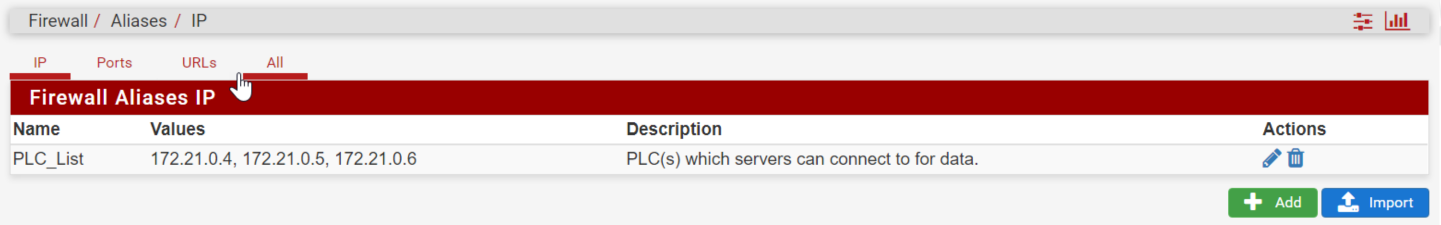
Certificate revocation lists which have been previously created and exported can be imported to the same or other ICS-Defender configurations to provide for easier distribution of changes to the list.

Aliases

Aliases allow the use of a single name to represent a single IP address, multiple IP addresses, ports, or hosts. Aliases also allow grouping of the same to minimize entry in firewall rules and NAT configurations. A particularly useful reason to use aliases as opposed to direct addresses or ports is when duplicating configurations. Exporting the configuration to an XML file and editing the area dedicated to aliases will effectively edit the IP addresses or ports used by the alias throughout the entire configuration.

Note: Alias names can only be alphanumeric and underscore.

Aliases can be created by navigating to **Firewall→ Aliases** in the WebGUI.



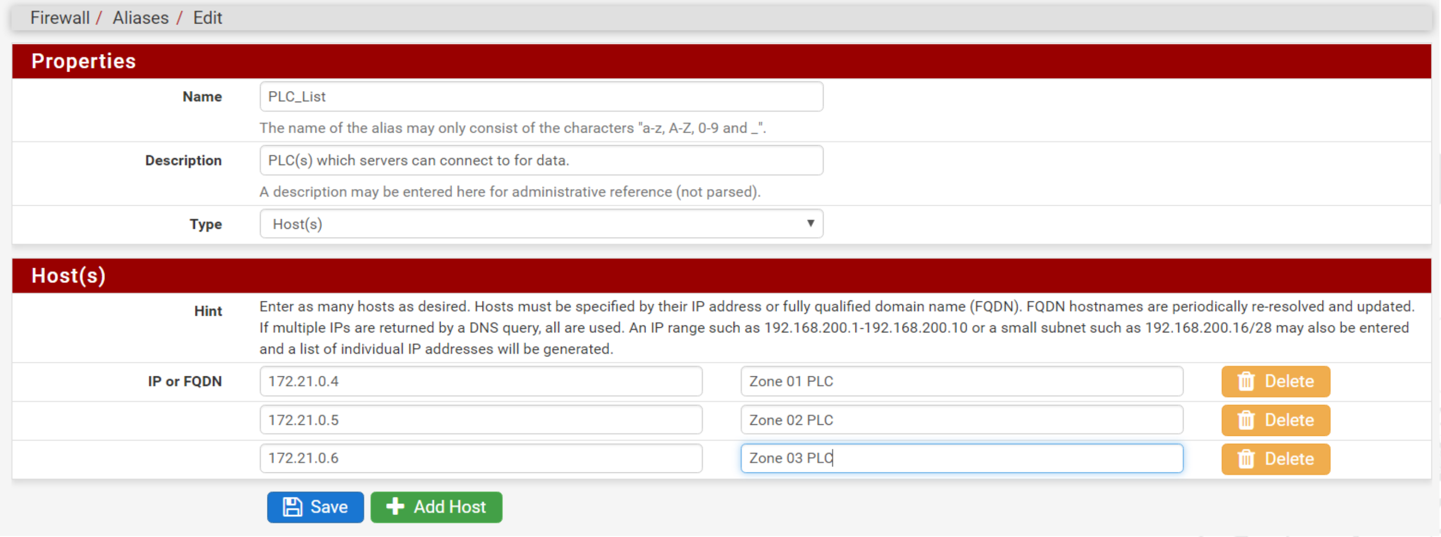
Firewall / Aliases / IP

IP | Ports | URLs | All

Firewall Aliases IP

Name	Values	Description	Actions
PLC_List	172.21.0.4, 172.21.0.5, 172.21.0.6	PLC(s) which servers can connect to for data.	✎ 🗑

A list of any configured aliases is shown. To add an alias, click the + Add key. In the below example, an alias named PLC_List is created which contains a list of hosts (IP Addresses) for each PLC that a server or data collection application can touch on the network. VPN or Firewall settings can reference this alias instead of having to contain separate references to each PLC IP Address.



Firewall / Aliases / Edit

Properties

Name	PLC_List The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	PLC(s) which servers can connect to for data. A description may be entered here for administrative reference (not parsed).
Type	Host(s)

Host(s)

Hint: Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.200.1-192.168.200.10 or a small subnet such as 192.168.200.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN		
172.21.0.4	Zone 01 PLC	Delete
172.21.0.5	Zone 02 PLC	Delete
172.21.0.6	Zone 03 PLC	Delete

Name: The name of the alias. This is the name that will be used elsewhere in the ICS-Defender configuration to reference the hosts, networks, or ports listed within.

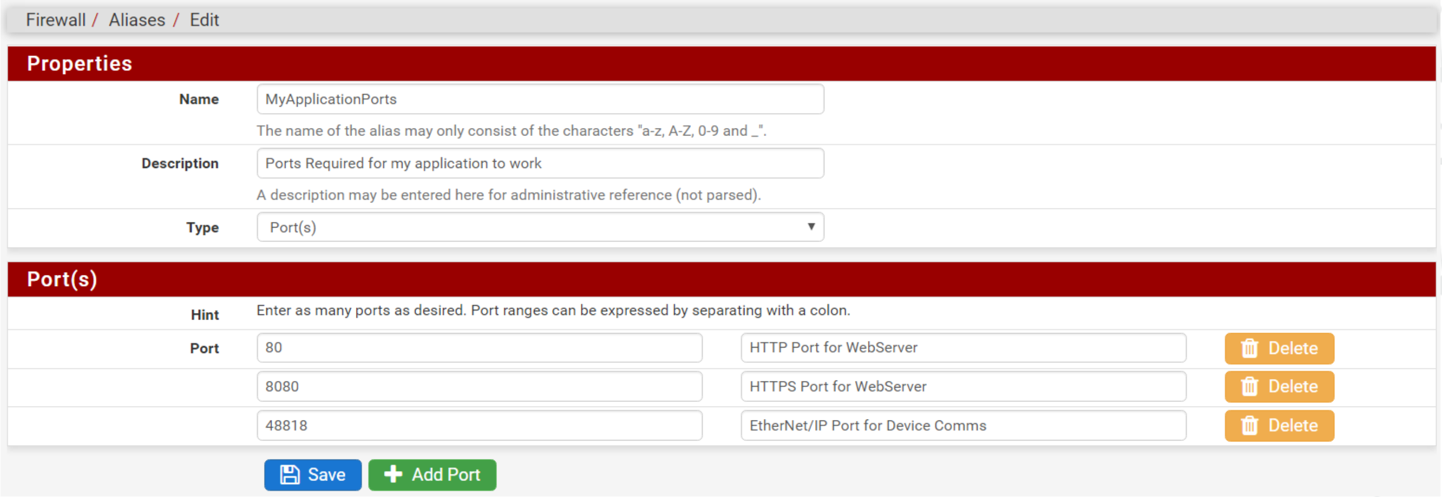
Description: Text which describes what the alias contains or will be used for.

Type: Hosts, Networks, or Ports selection.

Clicking the + Add Host button allows more hosts or ports to be added to the list.

Port Alias

A common use for aliases is to combine ports that an application might use into a single alias. In the following example, “MyApplicationPorts” is the alias for ports 80, 8080, and 48818.



Firewall / Aliases / Edit

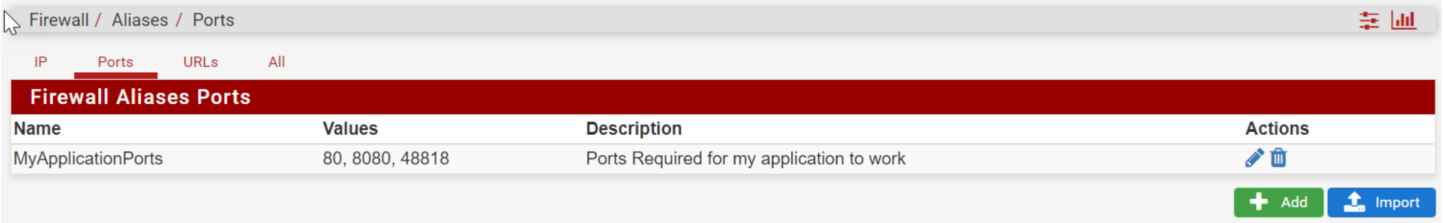
Properties

Name	MyApplicationPorts The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	Ports Required for my application to work A description may be entered here for administrative reference (not parsed).
Type	Port(s) ▾

Port(s)

Hint	Enter as many ports as desired. Port ranges can be expressed by separating with a colon.		
Port	80	HTTP Port for WebServer	Delete
	8080	HTTPS Port for WebServer	Delete
	48818	EtherNet/IP Port for Device Comms	Delete

After saving, the alias is displayed at **Firewall→ Aliases→ Ports**.



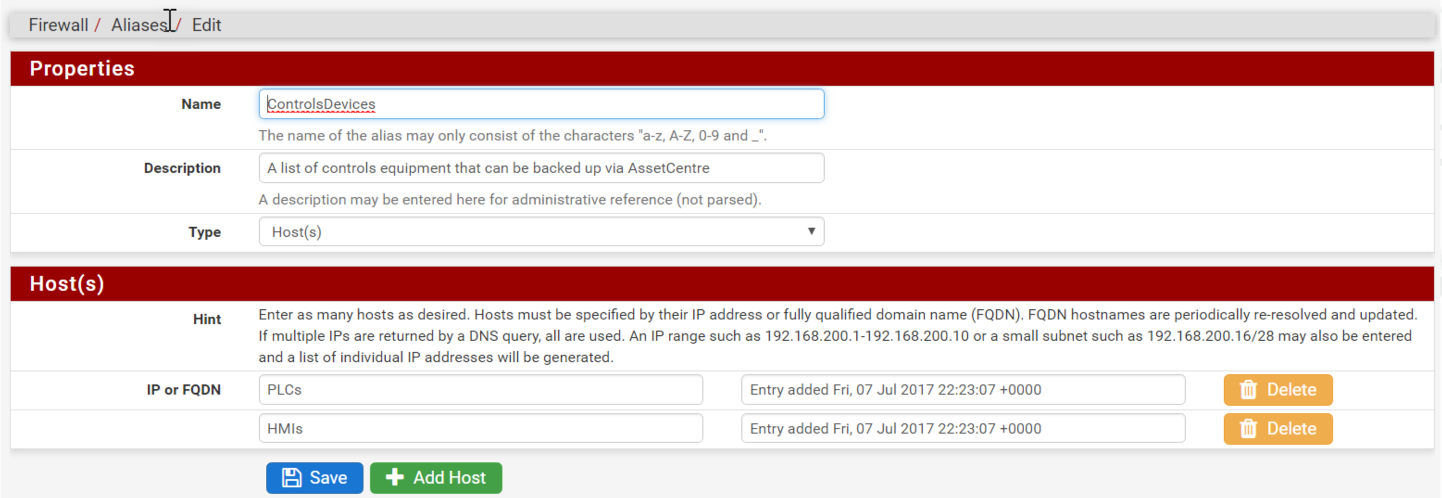
Firewall / Aliases / Ports

Firewall Aliases Ports

Name	Values	Description	Actions
MyApplicationPorts	80, 8080, 48818	Ports Required for my application to work	

Nesting Aliases

Aliases allow nesting of one alias inside another. For example, an alias with PLCs and an alias with HMIs could be part of an alias called ControlsDevices.



Firewall / Aliases / Edit

Properties

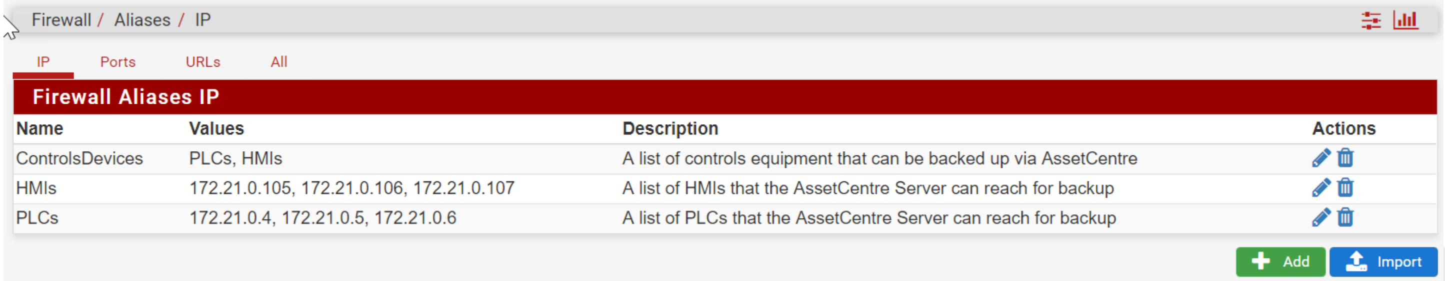
Name	ControlsDevices The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	A list of controls equipment that can be backed up via AssetCentre A description may be entered here for administrative reference (not parsed).
Type	Host(s)

Host(s)

Hint: Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.200.1-192.168.200.10 or a small subnet such as 192.168.200.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	PLCs	Entry added Fri, 07 Jul 2017 22:23:07 +0000	Delete
	HMIs	Entry added Fri, 07 Jul 2017 22:23:07 +0000	Delete

When saved, the alias is listed on the aliases page.



Firewall / Aliases / IP

Firewall Aliases IP

Name	Values	Description	Actions
ControlsDevices	PLCs, HMIs	A list of controls equipment that can be backed up via AssetCentre	
HMIs	172.21.0.105, 172.21.0.106, 172.21.0.107	A list of HMIs that the AssetCentre Server can reach for backup	
PLCs	172.21.0.4, 172.21.0.5, 172.21.0.6	A list of PLCs that the AssetCentre Server can reach for backup	

Industrial Protocols

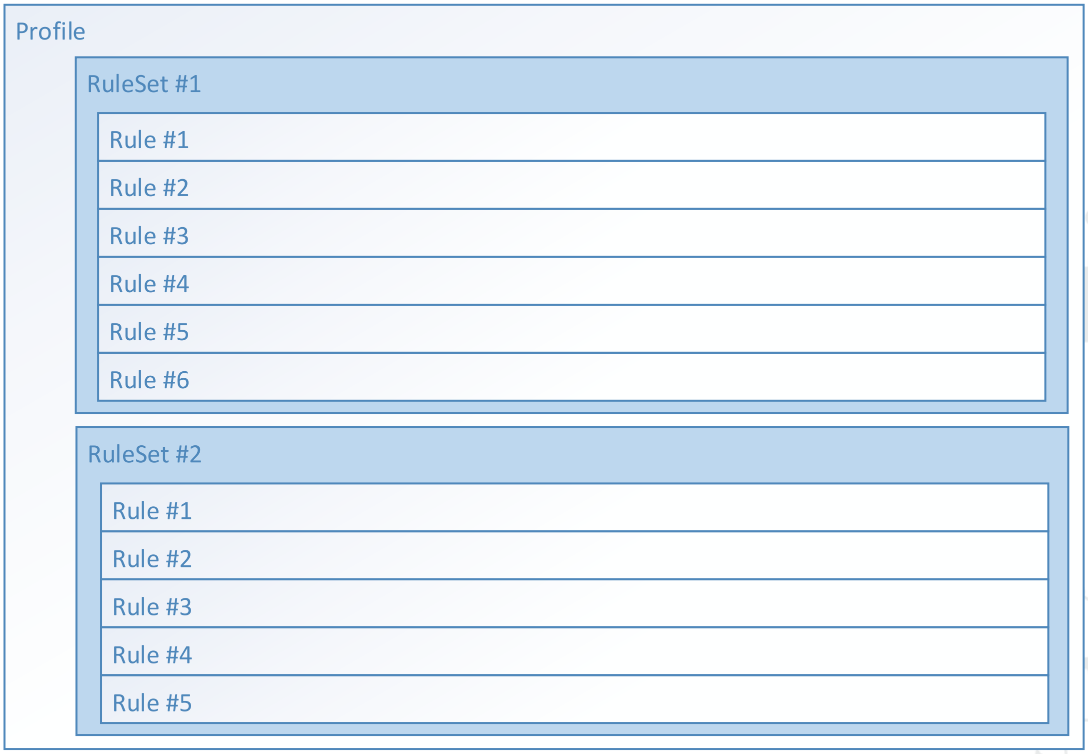
ICS-Defender supports packet and protocol filtering of industrial protocols such as Modbus-TCP and EtherNet/IP. These protocols are filtered with an inline deep packet inspection engine which is unequaled in the industry for speed and accuracy.

ICS-Defender allows manual creation of rules, or can learn network traffic via packet capture and generate a set of rules. The learned rules can be applied via either a block or pass, essentially creating a traffic whitelist with little effort.

Rules can be grouped into Rulesets and then one or more Rulesets can be applied to profiles. Once a profile is created, the profile can be applied to firewall rules on any interface configured in ICS-Defender.

Rules can also be applied directly to profiles, though it is highly recommended to only apply rules to a Ruleset. Rulesets allow import/export of rules so they can be easily moved from one ICS-Defender to another.

Note: Dynics recommends creating rulesets and using either a single ruleset in a profile or combining multiple rulesets into a profile as needed.



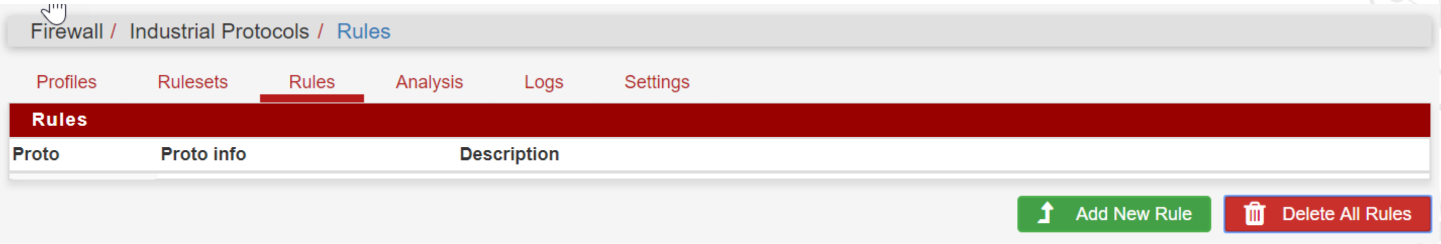
Rules

Rules can be created manually which necessitates significant knowledge of the protocol for which the rule is to be created. There are several alternative methods to implement deep packet inspection rules for industrial protocols in ICS-Defender which are much quicker, require less intimate knowledge of the protocol, and are generally a better approach.

Manual Creation

Manual rule creation should only be used if necessary, importing pre-defined rulesets and using the analysis/learning feature of ICS-Defender is a much more robust means to create rules and apply them.

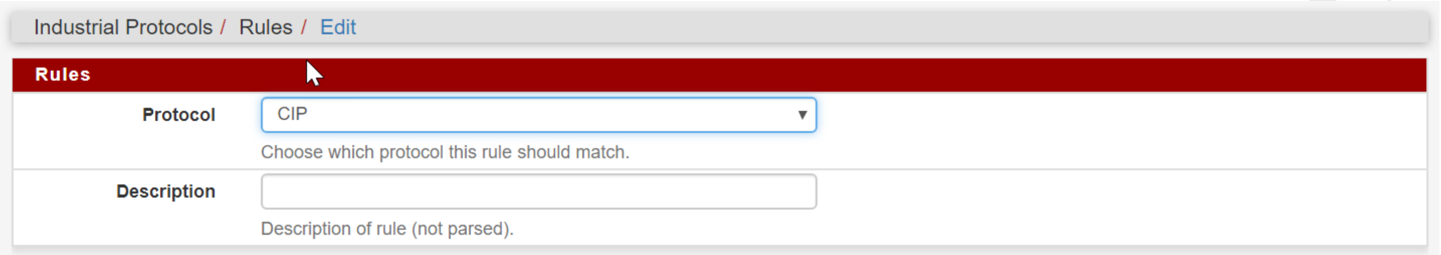
Navigate to Firewall→Industrial Protocol→Rules and click the “Add New Rule” button.



Rules

Proto	Proto info	Description

There are two protocols that are supported currently, EtherNet/IP and Modbus TCP, with Profinet, DNP3, and Synchrophasor in the testing stages as of this printing. The example below will cover the CIP protocol.



Rules

Protocol CIP
Choose which protocol this rule should match.

Description
Description of rule (not parsed).

Protocol: Select the protocol to be used in the rule creation.

Description: Text which describing the rule such as its intended purpose.

Once the desired protocol is chosen, the remainder of the page will contain fields relative to that protocol. It is beyond the scope of this document to cover the fields as they are protocol dependent and configuring rules this way requires in depth knowledge of the target protocol.

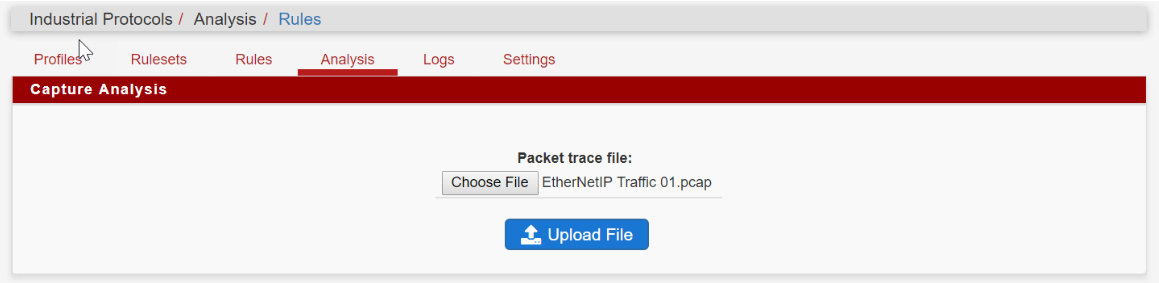
Learn Mode

Learn mode is a very easy means to create rules or “whitelist” industrial traffic. Using learning, ICS-Defender automatically generates rules based on the traffic from a PCAP (packet capture). The packet capture can be generated by ICS-Defender by navigating to **Diagnostics→Packet Capture** or by using a tool such as Wireshark.

Analysis

Once a packet capture is created, ICS-Defender can analyze the traffic and generate rules based on what is found in the traffic.

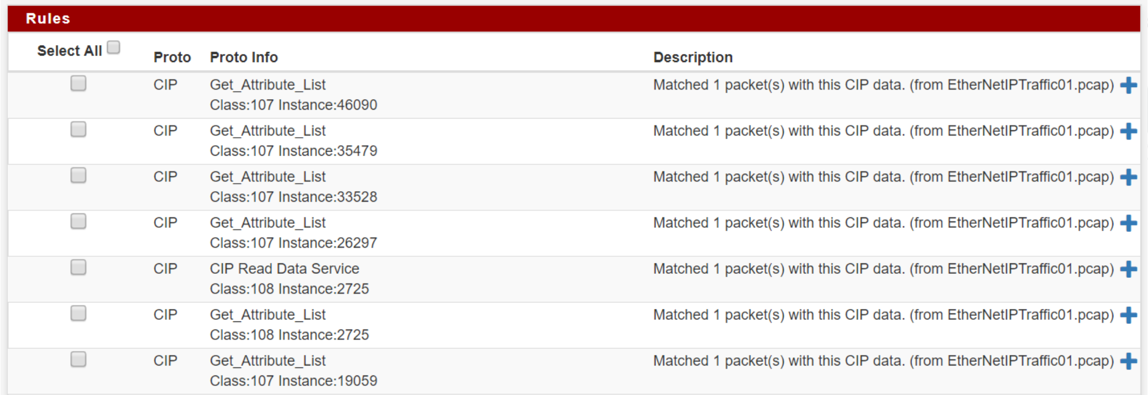
Firewall→Industrial Protocols→Analysis



Packet trace file:

Choose File EtherNetIP Traffic 01.pcap

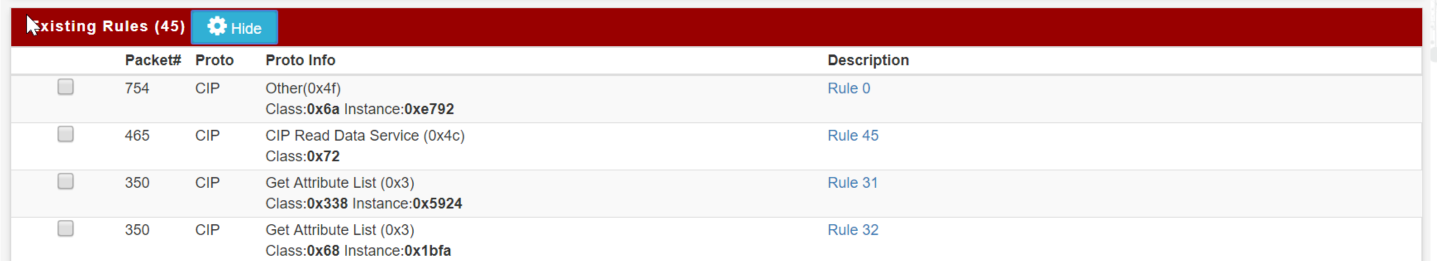
Choose a packet capture file to analyze and “Upload File”. ICS-Defender will analyze the packets and display a list with all potential rules generated.


Rules

Select All □	Proto	Proto Info	Description
□	CIP	Get_Attribute_List Class:107 Instance:46090	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	Get_Attribute_List Class:107 Instance:35479	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	Get_Attribute_List Class:107 Instance:33528	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	Get_Attribute_List Class:107 Instance:26297	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	CIP Read Data Service Class:108 Instance:2725	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	Get_Attribute_List Class:108 Instance:2725	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +
□	CIP	Get_Attribute_List Class:107 Instance:19059	Matched 1 packet(s) with this CIP data. (from EtherNetIPTraffic01.pcap) +

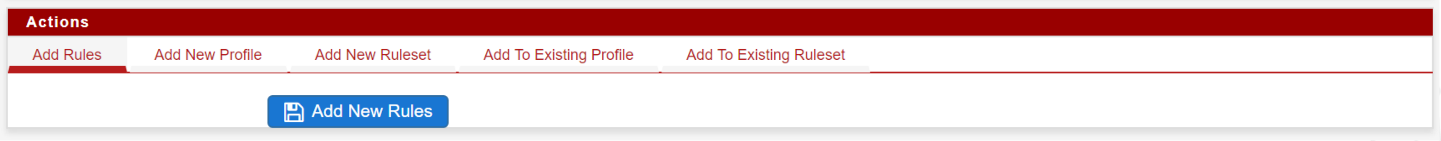
Either “Select All” or select via checkbox those packets which should be included in either the ruleset or the profile being created. This document assumes the creation of a ruleset is desired as that is the recommended approach.

Note that any analyzed rules that would match an already existing rule in ICS-Defender are shown in a second grouping of rules. These rules can be included in a new ruleset if selected.


Existing Rules (45)

	Packet#	Proto	Proto Info	Description
□	754	CIP	Other(0x4f) Class:**0x6a** Instance:**0xe792**	Rule 0
□	465	CIP	CIP Read Data Service (0x4c) Class:**0x72**	Rule 45
□	350	CIP	Get Attribute List (0x3) Class:**0x338** Instance:**0x5924**	Rule 31
□	350	CIP	Get Attribute List (0x3) Class:**0x68** Instance:**0x1bfa**	Rule 32

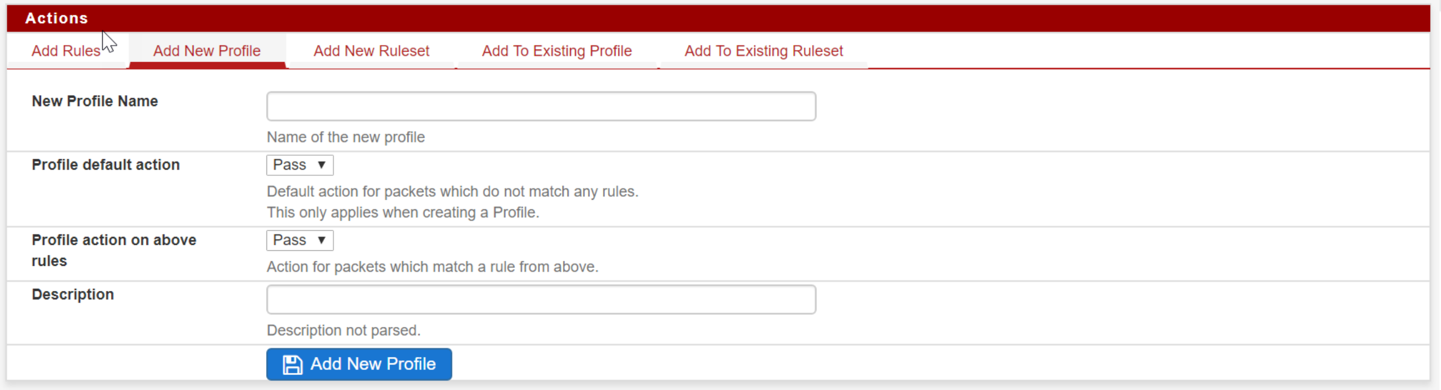
At the bottom of the presented list, the options to create rules, rulesets, and profiles are available.



- The rules can be simply added, without organization, by selecting "Add Rules".

Add rules directly to a new Profile

Note: Adding rules directly to a profile isn't recommended, combining rulesets in a profile is recommended.



New Profile Name	Name of the new profile
Profile default action	Pass ▾ Default action for packets which do not match any rules. This only applies when creating a Profile.
Profile action on above rules	Pass ▾ Action for packets which match a rule from above.
Description	Description not parsed.

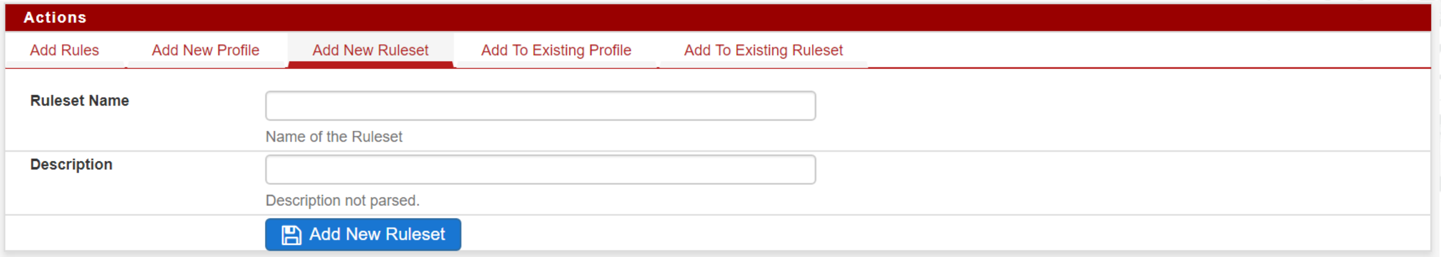
Name: Enter a name for the profile or that describes the contents or purpose.

Description: Text which describes the profile.

Profile Default Action: This option will set the default behavior for the profile. Generally, when white listing traffic, selecting "Block" will prevent all traffic EXCEPT that traffic that matches the packets/rules from passing through whichever interface is selected.

Profile Action on Above Rules: In conjunction with the "Profile default action" from above, this option dictates how ICS-Defender will handle packets through a selected interface which ***match*** rules in the profile. Generally, when white listing traffic, selecting "Pass" will allow only the learned traffic through the selected interface.

Add rules to a new Ruleset



Ruleset Name	Name of the Ruleset
Description	Description not parsed.

Name: Enter a name for the ruleset or that describes the contents or purpose.
Description: Text which describes the ruleset

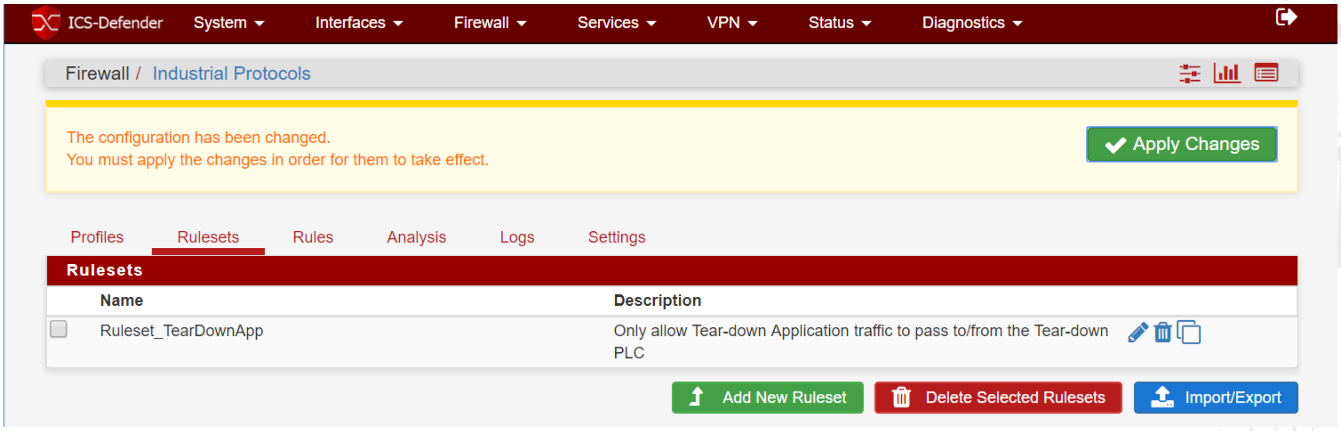
Add to Existing Profile or Ruleset

When adding rules to an existing profile or ruleset a dropdown is presented allowing selection of the destination profile or ruleset. The other selections mirror those found when adding a new profile or ruleset and were discussed previously.

Apply Changes

Selecting any option to add additional rules will result require clicking “Apply Changes” to commit the change to ICS-Defender.

Note: At this stage it’s only created, it is not effecting or being used in the evaluation of network traffic.



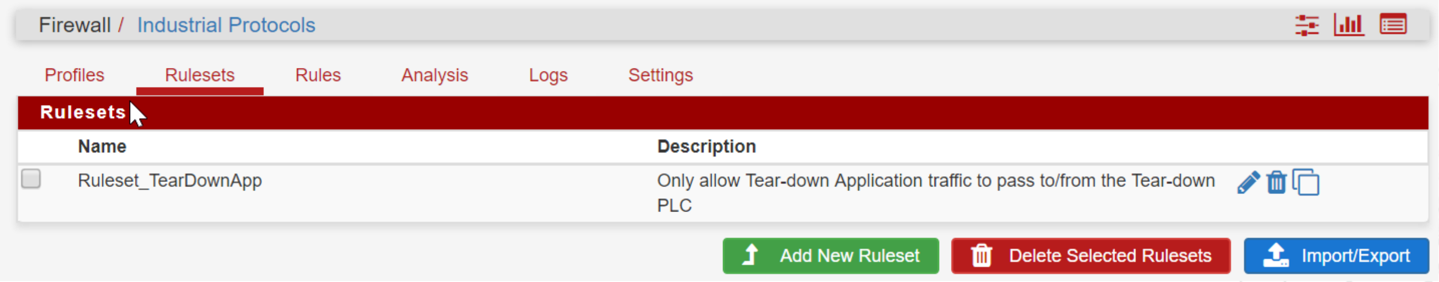
The configuration has been changed.
You must apply the changes in order for them to take effect.

Rulesets

	Name	Description
□	Ruleset_TearDownApp	Only allow Tear-down Application traffic to pass to/from the Tear-down PLC

Rulesets

Rulesets are created by importing pre-created rulesets, or those exported from another ICS-Defender. They can also be created and rules can be added one at a time to the ruleset. After creating or importing a ruleset, the available rulesets are listed at **Firewall→Industrial Protocols→Rulesets**.

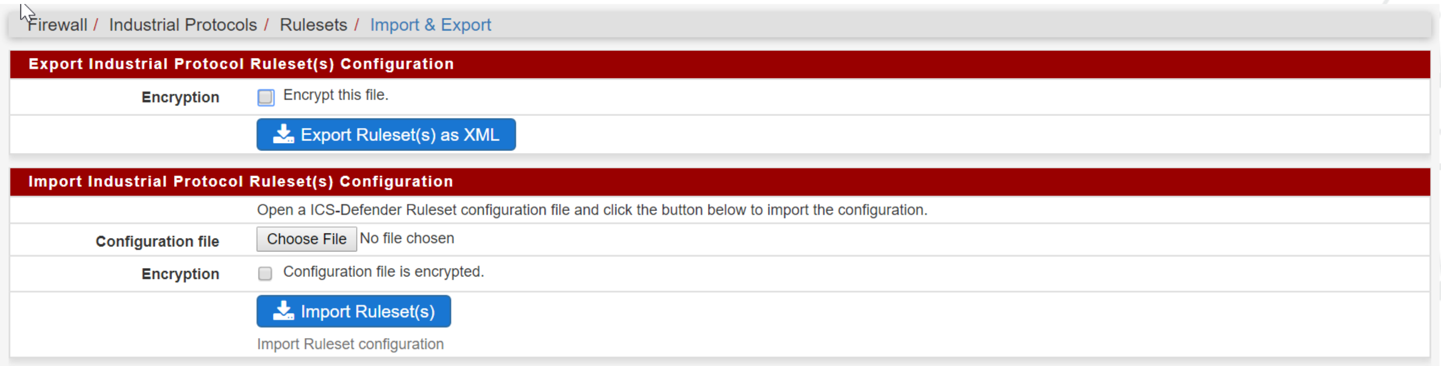


Rulesets

	Name	Description
□	Ruleset_TearDownApp	Only allow Tear-down Application traffic to pass to/from the Tear-down PLC

Import/Export Rulesets

Rulesets can be imported or exported from ICS-Defender. There are predefined importable rulesets available from Dynics. The ruleset export files are in XML format.



Firewall / Industrial Protocols / Rulesets / Import & Export

Export Industrial Protocol Ruleset(s) Configuration

Encryption	□ Encrypt this file.
	Export Ruleset(s) as XML

Import Industrial Protocol Ruleset(s) Configuration

Open a ICS-Defender Ruleset configuration file and click the button below to import the configuration.

Configuration file	Choose File No file chosen
Encryption	□ Configuration file is encrypted.
	Import Ruleset(s) Import Ruleset configuration

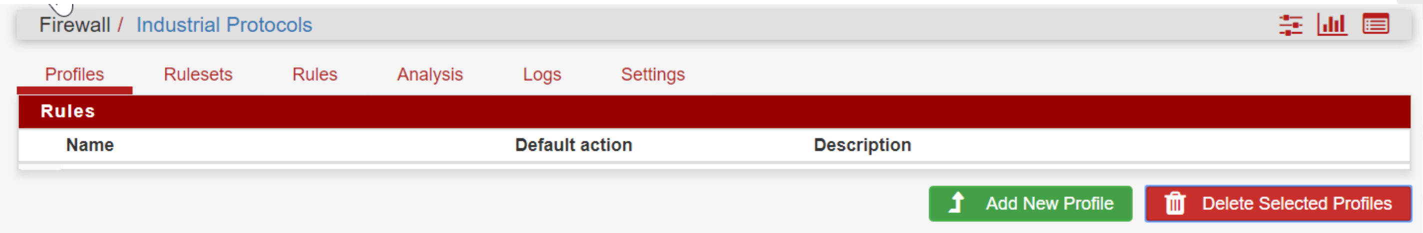
Profiles

Once rulesets or rules are added to ICS-Defender, profiles can be created as a container for the various rules in the system. For example, after creating a ruleset by analyzing a packet capture, that ruleset must be added to a profile before it can be used in a firewall rule.

Example: Rulesets – White List Application Traffic

In this example, a profile is created by analyzing captured traffic from a Tear-down Application located on a PC talking to a single PLC on the Controls Network. The goal is to only allow that traffic needed by the Tear-down application through the interface on ICS-Defender.

Navigate to **Firewall→ Industrial Protocols→ Profiles**

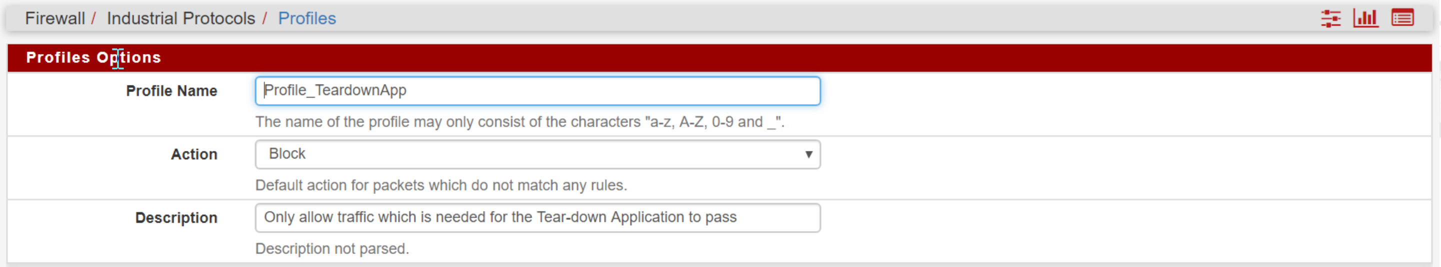


Firewall / Industrial Protocols

Rules

Name	Default action	Description

Click “Add New Profile” to create a new profile and add the tear-down application ruleset.



Firewall / Industrial Protocols / Profiles

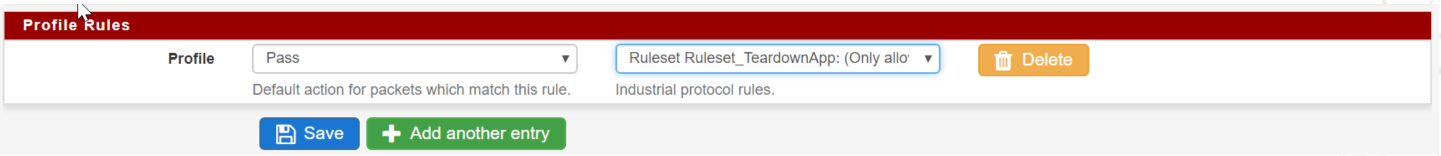
Profiles Options

Profile Name	Profile_TeardownApp The name of the profile may only consist of the characters "a-z, A-Z, 0-9 and _".
Action	Block Default action for packets which do not match any rules.
Description	Only allow traffic which is needed for the Tear-down Application to pass Description not parsed.

Profile Name: Enter a name for the Profile which describes the contents or purpose, such as “Profile_TearDownApp”.

Action: When creating a profile from rulesets, this option will set the default behavior for the profile. Generally, when white listing traffic, selecting "Block" will prevent all traffic EXCEPT that traffic that matches the packets/rules from passing through whichever interface is selected.

Description: Text which describing the Profile "Only allow Tear-down Application traffic to pass to/from the Tear-down PLC".



Profile Rules

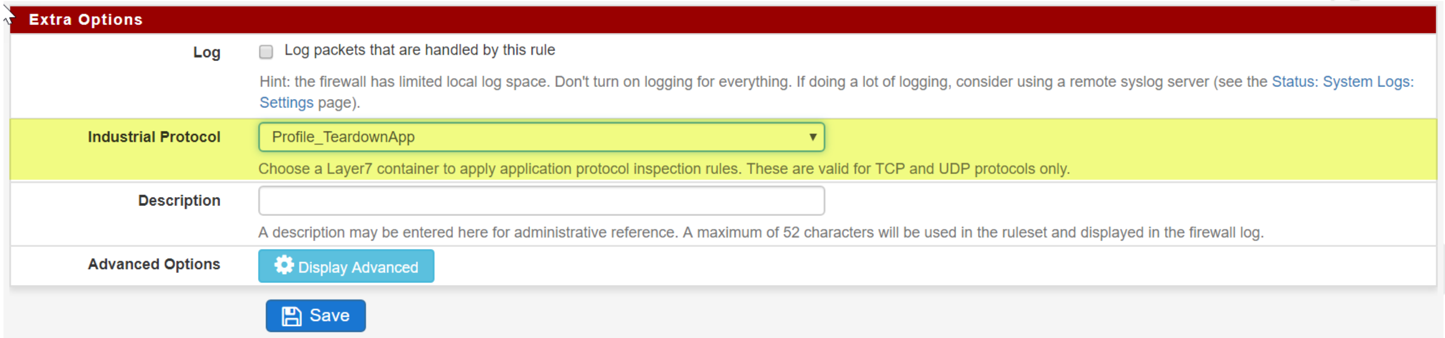
Profile	Pass Default action for packets which match this rule.	Ruleset Ruleset_TeardownApp: (Only allo Industrial protocol rules.

Rulesets and individual rules can be added to the profile.

Profile: Pass or Block individual rules or rulesets are selected on the right dropdown. The dropdown will list rulesets first, followed by individual rules.

Additional entries may be added with "Add another entry". When complete, save the profile and apply.

Navigate to **Firewall→ Rules→ WAN, LAN, or OpenVPN** and add or edit a rule to reference the profile. Traffic that matches the rule will be filtered through the DPI engine using this profile.



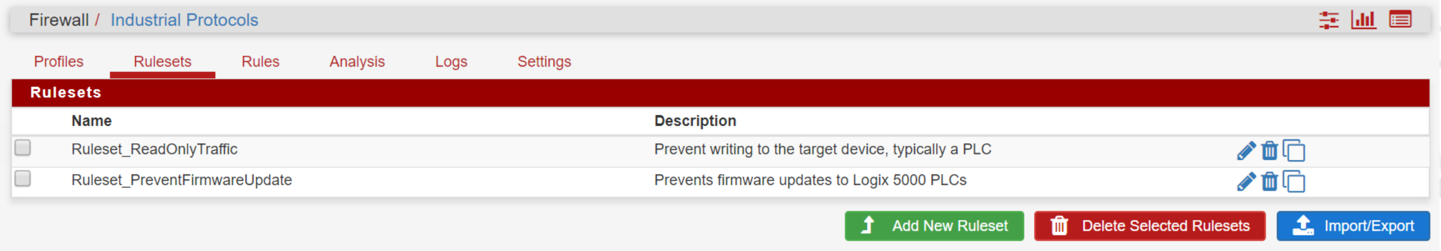
Extra Options

Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Industrial Protocol	Profile_TeardownApp Choose a Layer7 container to apply application protocol inspection rules. These are valid for TCP and UDP protocols only.
Description	 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Display Advanced

Example – Rulesets: Read Only PLC

Predefined rulesets are available to perform tasks such as setting traffic to a PLC as “read only”, “prevent firmware updates”, etc. Users can also create their own rulesets using the methods described in previous sections. These rulesets can be added to a profile to prevent undesired communication or activity.

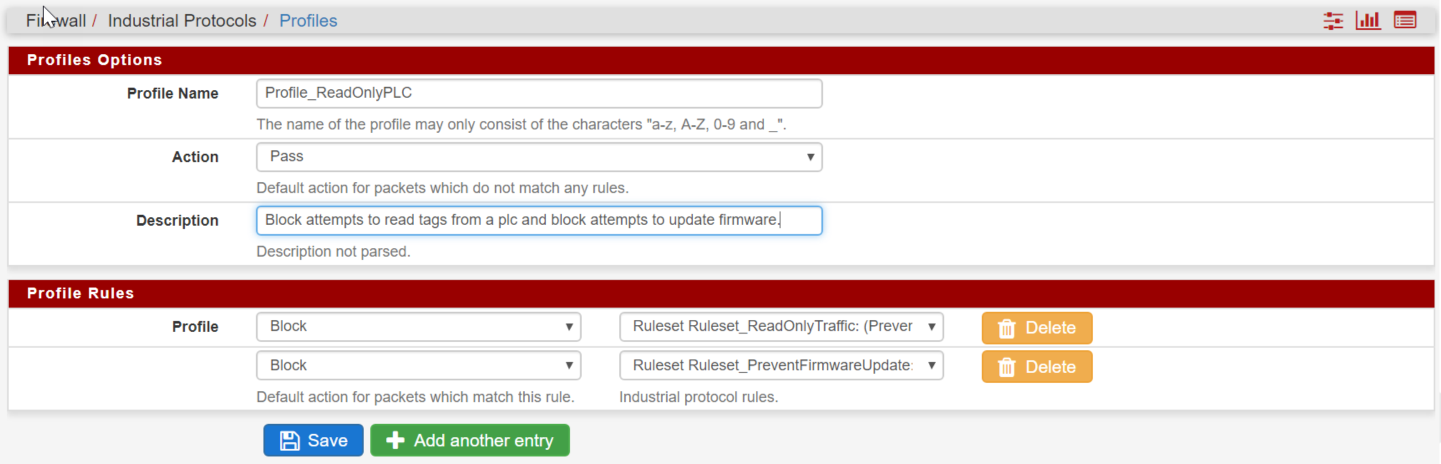
In this example, the objective is to prevent any writes to the PLC and prevent the PLC from being firmware updated.



Rulesets

	Name	Description
□	Ruleset_ReadOnlyTraffic	Prevent writing to the target device, typically a PLC
□	Ruleset_PreventFirmwareUpdate	Prevents firmware updates to Logix 5000 PLCs

These predefined rulesets, after import, can be added to a profile.



Profiles Options

Profile Name: Profile_ReadOnlyPLC
The name of the profile may only consist of the characters "a-z, A-Z, 0-9 and _".

Action: Pass
Default action for packets which do not match any rules.

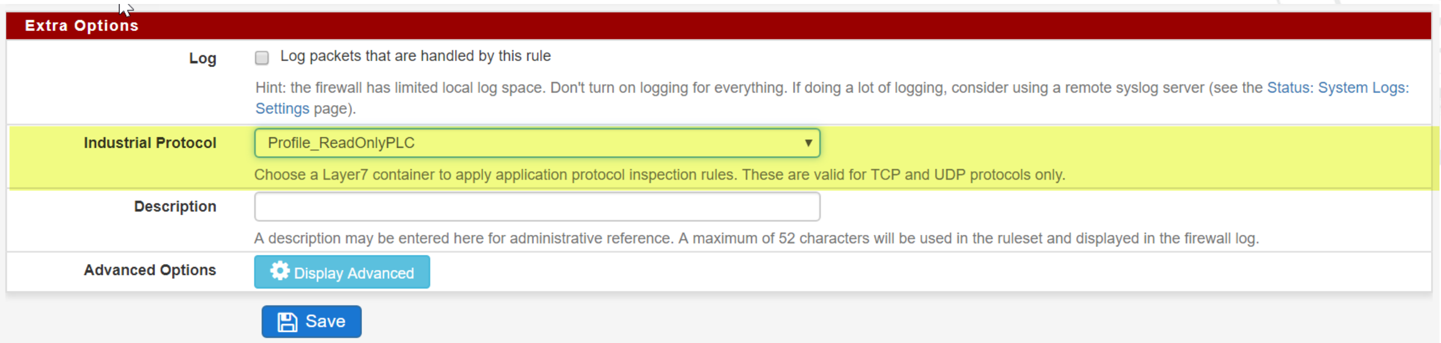
Description: Block attempts to read tags from a plc and block attempts to update firmware.
Description not parsed.

Profile Rules

Profile: Block — Ruleset Ruleset_ReadOnlyTraffic: (Prever — Delete
Block — Ruleset Ruleset_PreventFirmwareUpdate: — Delete
Default action for packets which match this rule. Industrial protocol rules.

In this example, the profile is created with the default action PASS for packets which do NOT match any of the rules, and each individual profile rule setting is set to BLOCK. The rulesets for ready only traffic and prevent firmware flashing are selected.

Navigate to **Firewall→ Rules→ WAN, LAN, or OpenVPN** and add or edit a rule to reference the profile. Traffic that matches the rule will be filtered through the DPI engine using this profile.



Extra Options

Log: □ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Industrial Protocol: Profile_ReadOnlyPLC
Choose a Layer7 container to apply application protocol inspection rules. These are valid for TCP and UDP protocols only.

Description:
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

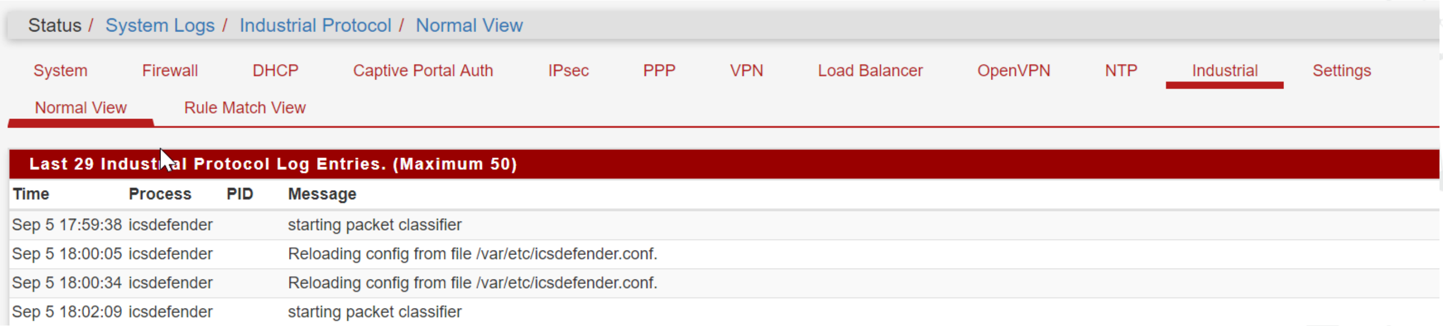
Advanced Options: Display Advanced

Logs

Industrial Protocol related log files. The link found at Firewall→Industrial Protocol→Logs is a shortcut to Status→System Logs→Industrial Protocols.

Normal View

The “Normal View” shows various activity related to the industrial protocol engine.

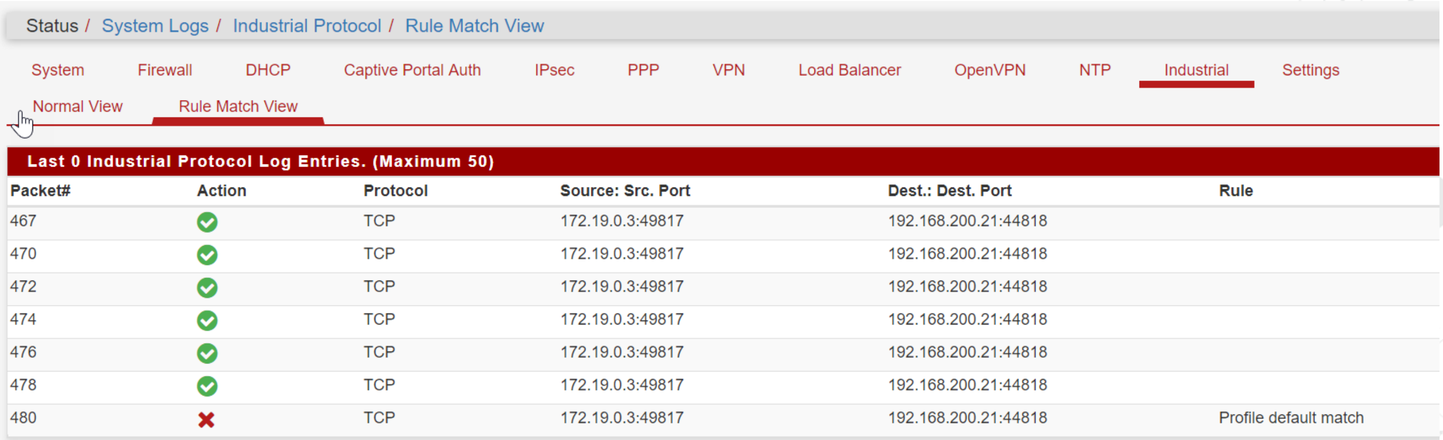


Last 29 Industrial Protocol Log Entries. (Maximum 50)

Time	Process	PID	Message
Sep 5 17:59:38	icsdefender		starting packet classifier
Sep 5 18:00:05	icsdefender		Reloading config from file /var/etc/icsdefender.conf.
Sep 5 18:00:34	icsdefender		Reloading config from file /var/etc/icsdefender.conf.
Sep 5 18:02:09	icsdefender		starting packet classifier

Rule Match View

Rule match view shows the pass/block status of packets being processed by the protocol engine. Also shown are the protocol, source IP and source port, and destination IP and destination port.



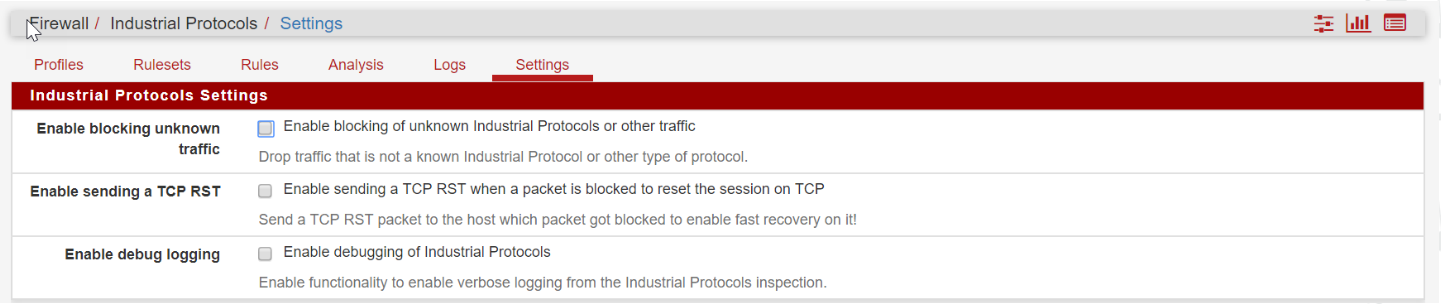
Last 0 Industrial Protocol Log Entries. (Maximum 50)

Packet#	Action	Protocol	Source: Src. Port	Dest.: Dest. Port	Rule
467	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
470	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
472	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
474	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
476	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
478	✓	TCP	172.19.0.3:49817	192.168.200.21:44818	
480	✗	TCP	172.19.0.3:49817	192.168.200.21:44818	Profile default match

Settings

Settings which log traffic should be used during debug and setting up ICS-Defender. As a general rule, it’s not a good idea to enable logging indefinitely as PCAP files require physical storage on ICS-Defender.

Industrial Protocol Settings



Industrial Protocols Settings

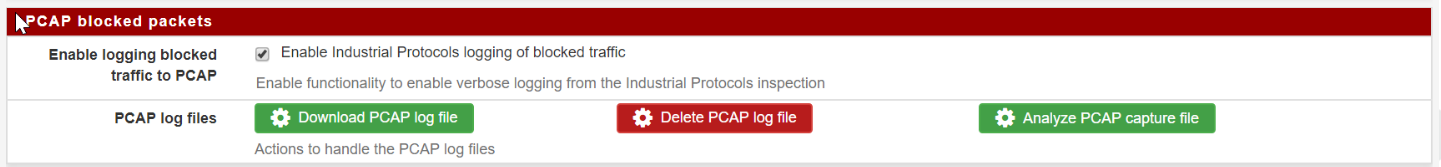
Enable blocking unknown traffic	☐ Enable blocking of unknown Industrial Protocols or other traffic Drop traffic that is not a known Industrial Protocol or other type of protocol.
Enable sending a TCP RST	☐ Enable sending a TCP RST when a packet is blocked to reset the session on TCP Send a TCP RST packet to the host which packet got blocked to enable fast recovery on it!
Enable debug logging	☐ Enable debugging of Industrial Protocols Enable functionality to enable verbose logging from the Industrial Protocols inspection.

Enable blocking unknown traffic: Protocols which are unrecognized, either industrial or other, will be blocked.

Enable sending a TCP RST (reset): In some applications when their traffic is blocked by rules, their TCP session gets out of sync and they will take a long time to recover. Enabling TCP RST (reset) will cause ICS-Defender to respond to the source of the packets with a TCP reset when a packet from that source is blocked to speed up the recovery process.

Enable debug logging: Enables verbose logging of packets from the Industrial Protocol Inspection (DPI) Engine.

PCAP Blocked Packets

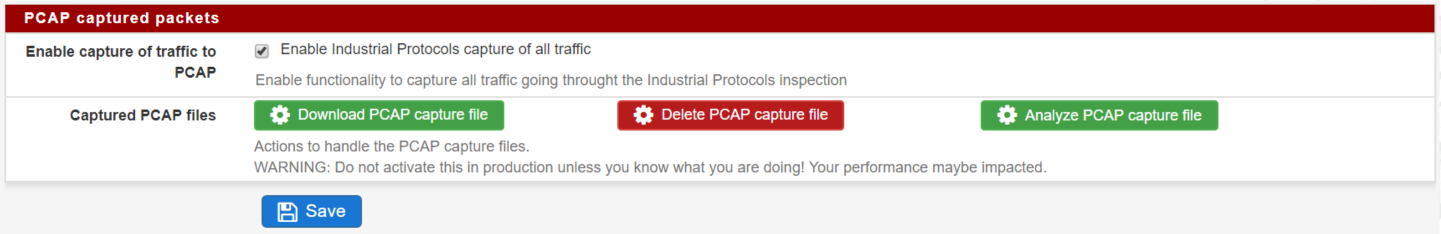


PCAP blocked packets

Enable logging blocked traffic to PCAP	☑ Enable Industrial Protocols logging of blocked traffic Enable functionality to enable verbose logging from the Industrial Protocols inspection
PCAP log files	Actions to handle the PCAP log files

Enable Logging blocked traffic to PCAP: Logs traffic blocked by the DPI engine to a PCAP file for review later in a tool such as Wireshark or allows analysis of the packet directly in ICS-Defender by using the “Analyze PCAP capture file”

PCAP Captured (All) Packets



PCAP captured packets

Enable capture of traffic to PCAP	☑ Enable Industrial Protocols capture of all traffic Enable functionality to capture all traffic going throught the Industrial Protocols inspection
Captured PCAP files	Actions to handle the PCAP capture files. WARNING: Do not activate this in production unless you know what you are doing! Your performance maybe impacted.

Enable capture of traffic to PCAP: Logs all traffic evaluated by the DPI engine to a PCAP file for review later in a tool such as Wireshark or allows analysis of the packet directly in ICS-Defender by using the “Analyze PCAP capture file”

How to use “PCAP Blocked Packets”

If, after creating a ruleset or profile, there is a need to see what packets are being blocked by the protocol engine, reviewing blocked packets is a great way to see what is being blocked.

Also, assuming a configuration is created and up and running for a while, should new traffic be generated by a new application whose industrial traffic goes through ICS-Defender, capturing blocked traffic, analyzing it, and adding to an existing ruleset or new ruleset is a great way to extend the configuration without having to start over and create a whole new set of rules.

Network Address Translation (NAT)

Port Forwards

Port forwards allows opening of a specific port, port range or protocol to a privately addressed device on the internal network.

Risks of Port Forwarding

In a default configuration, ICS-Defender does not let in any traffic initiated on the WAN. This provides protection from malicious attacks on the WAN interface. When a port forward is added, ICS-Defender will allow any traffic matching the corresponding firewall rule. ICS-Defender doesn't know the difference from a packet with a malicious payload and a packet with a benign payload. If a packet matches the firewall rule, it is allowed. With this approach, it's important to rely on host based controls to secure any services allowed through the appliance.

Port Forwarding and Local Services

Port forwards take precedence over any services running locally on the appliance, such as the web interface, SSH, and any other services running. For example, if remote web interface access is allowed from the WAN using HTTPS on TCP port 443 and a port forward on WAN for TCP 443 is added, that port forward will work and web interface access from WAN will no longer function. This does not affect access on other interfaces, just the interface containing the port forward.

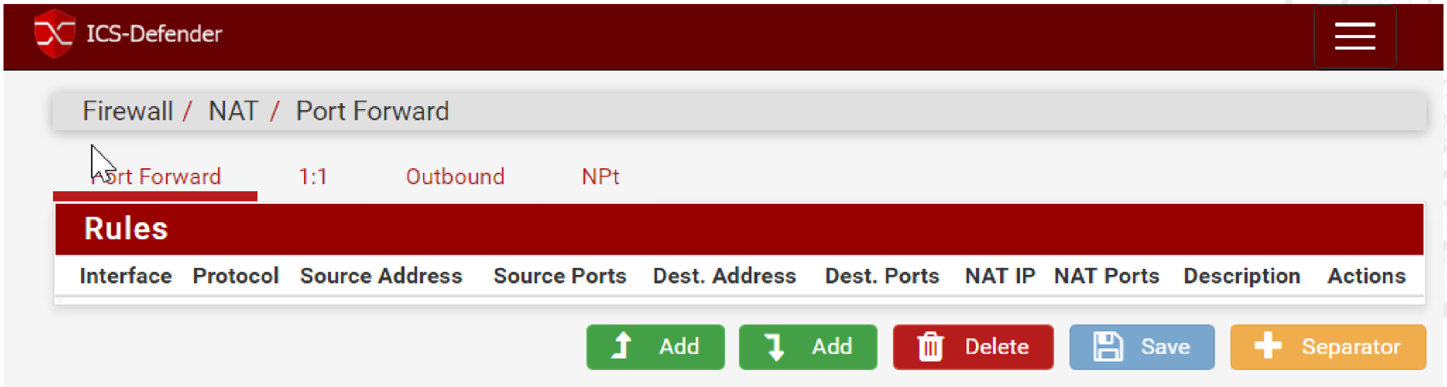
Port Forwarding and 1:1 NAT

Port forwards also take precedence over 1:1 NAT. If a port forward exists on one external IP address forwarding a port to a host, and a 1:1 NAT entry on the same external IP address forwarding to a different host, then the port forward will still be active and working sending that one port to the original host.

Adding Port Forwards

Port Forwards are managed at **Firewall → NAT→Port Forward tab**. The rules on this screen are managed in the same manner as other firewall rules.

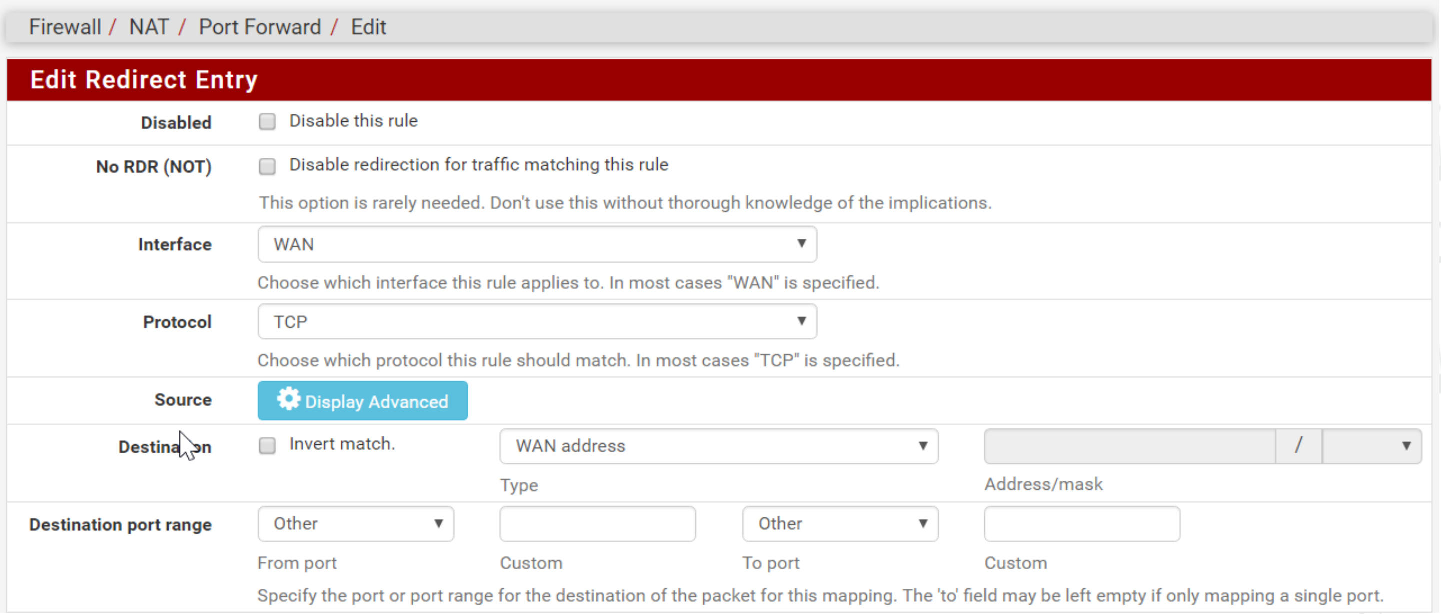
To begin adding a port forward entry, click the ⮥ Add button.



Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions

Add Port Forward



Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled	□ Disable this rule
No RDR (NOT)	□ Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN ▾ Choose which interface this rule applies to. In most cases "WAN" is specified.
Protocol	TCP ▾ Choose which protocol this rule should match. In most cases "TCP" is specified.
Source	Display Advanced
Destination	□ Invert match. · Type: WAN address ▾ · Address/mask: / ▾
Destination port range	From port: Other ▾ · Custom: · To port: Other ▾ · Custom: Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Disabled: When checked, this rule/port forward is disabled.

No RDR (NOT): When checked, the behavior of the port forward is negated meaning that no redirection should be performed when the rule is matched, versus the default behavior of redirecting when the rule is matched. In most common configurations, this option remains unchecked.

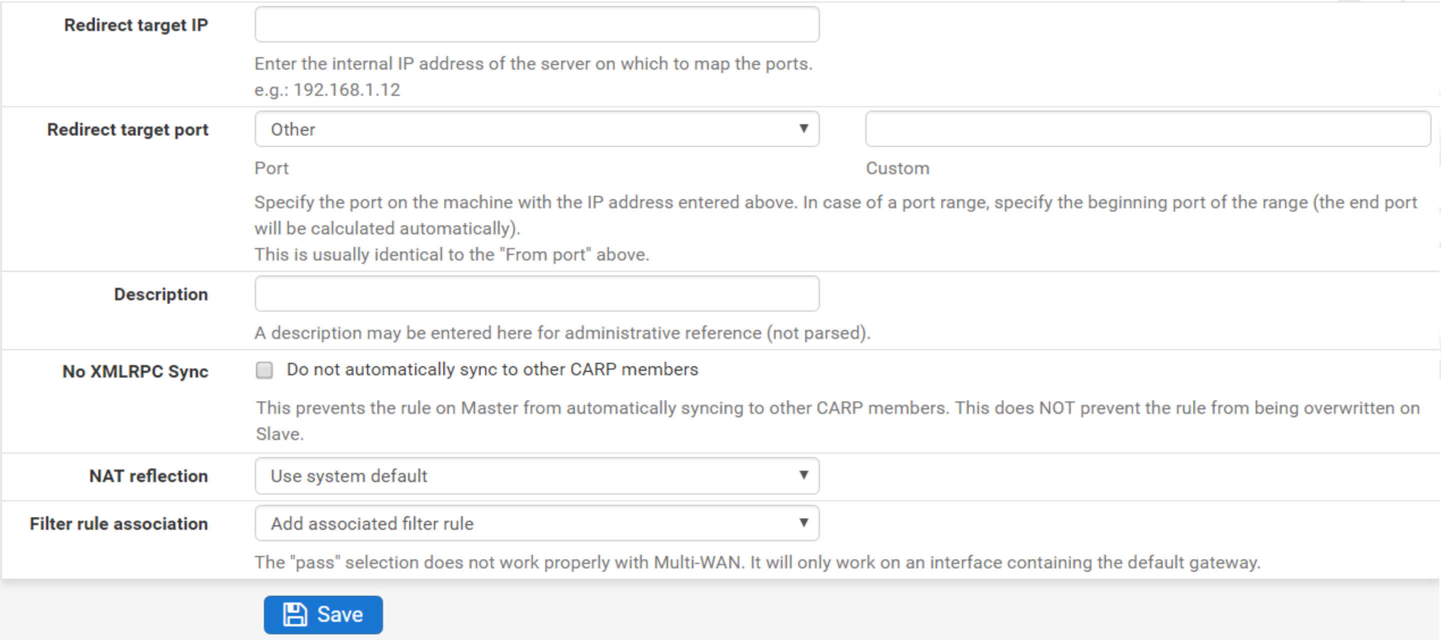
Interface: Selected interface to which the port forward will be added. This interface is where the traffic is initiated and will commonly be set to WAN.

Protocol: The protocol must be set to match the type of traffic or service being forwarded. Select the appropriate type of traffic, in most cases TCP, UDP, or TCP/UDP. Other types are available but require more advanced knowledge of the various available protocols.

Source: The Display Advanced button hides various options for setting the source and is by default set to any source. The options hidden by the display advanced button allow restriction of source IPs and Ports which can access this port forward entry. In general, modifying these advance options is not necessary.

Destination: The destination is the IP address where the forwarded traffic is intended. Port forwarding on the WAN interface would mean that an IP address on the WAN network would be used. An alias may also be used to select a list of specific IP addresses.

Destination Port Range: This setting allows specifying the original destination port of the traffic before it's redirected to the specified target. When forwarding a single port, the entry is made in the "from port" custom field, leaving the "to port" field empty. Drop down selections are available for common services in both the to and from fields. Ports can also be aliased to allow multiple ports to be selected.



Redirect target IP	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12
Redirect target port	Other ▾ Port Custom Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.
Description	A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync	□ Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default ▾
Filter rule association	Add associated filter rule ▾ The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Redirect Target IP: This is the IP where the traffic will be forwarded.

Redirect Target Port: This is the target port where the forwarded port range will begin. When forwarding a range of ports such as 19000-19100, a single port entry is used as the starting point for the forward. Source and target ports much match 1:1. Using this field allows opening of a different port on the outside than the port the host on the inside is listening on. For example, external port 8888 may forward to local port 80 for HTTP on an internal server. Selections are available via drop down containing a list of common services/ports.

Description: This field is used to allow the user to add a comment or description of the port forward.

No XMLRPC Sync: This field is only used when the ICS-Defender is part of a failover cluster. This option, on a master in a failover cluster, prevents this setting from being synchronized to the slaves in the cluster.

NAT Reflection: NAT Reflection can be enabled or disabled on a per-rule basis to allow overriding the global default. For any needs regarding this feature-set, please contact Dynics.

Filter Rule Association: When creating a port forward entry, the entry only defines which traffic should be redirected, it does not inherently create the necessary firewall rule needed to pass traffic through the port forward/redirection.

"*Add associated filter rule*" is the default setting and creates a firewall rule that is linked to this NAT port forward and changes made to the NAT port forward are automatically applied to the linked firewall rule. This is the most common setting and should be used unless more advanced functionality is needed. After saving the port forward, a link will be displayed to redirect the user to the newly created linked firewall rule.

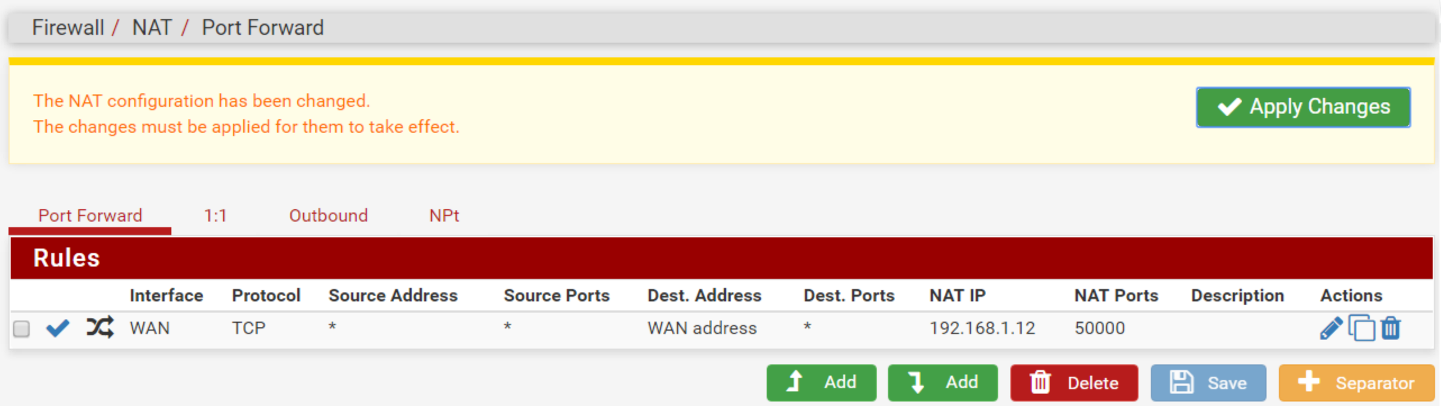
"*None*" will prevent ICS-Defender from creating any firewall rule to enable this port forward.

"*Unassociated filter rule*" creates a firewall rule that is not linked to this NAT port forward. Changes made to the NAT port forward must then be manually accounted for in the firewall rule. This option is useful when additional settings to the firewall rule must be made.

"*Pass*" is a special keyword on the NAT port forward that causes traffic to be passed through without the need of a firewall rule. NAT port forwards using this option will only work on the interface containing ICS-Defender's configured default gateway.

Click Save when finished.

The new NAT port forward has been saved but will not become active until ✔ Apply Changes is clicked.



Firewall / NAT / Port Forward

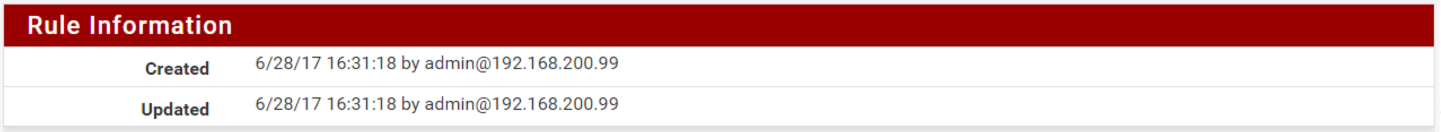
The NAT configuration has been changed.
The changes must be applied for them to take effect.

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤨	WAN	TCP	*	*	WAN address	*	192.168.1.12	50000		✎ ⧉ 🗑

Tracking Changes to Port Forwards

After creating an audit field is added to the bottom of the configuration screen. This field shows when and who created the initial rule as well as any updates that have been made since its creation.



Rule Information

Created	6/28/17 16:31:18 by admin@192.168.200.99
Updated	6/28/17 16:31:18 by admin@192.168.200.99

Port Forward Limitations

You can only forward a single port to one LAN host for each WAN IP address available.

Traffic Redirection with Port Forwards

Another use of port forwards is for transparently redirecting traffic from the LAN network. Port forwards specifying the LAN interface or another internal interface will redirect traffic matching the forward to the specified destination.

1:1 NAT

1:1 (one to one) NAT maps one WAN IPv4 address to one LAN IPv4 address. All traffic from that LAN IPv4 address will be mapped to the WAN IPv4 address defined in the 1:1 NAT mapping, overriding the Outbound NAT configuration. All traffic initiated on the WAN destined for the specified WAN IPv4 address will be translated to the LAN IPv4, then evaluated by the WAN firewall ruleset. If the traffic is permitted by firewall rules to a target LAN IPv4 address, it will be passed to the internal host.

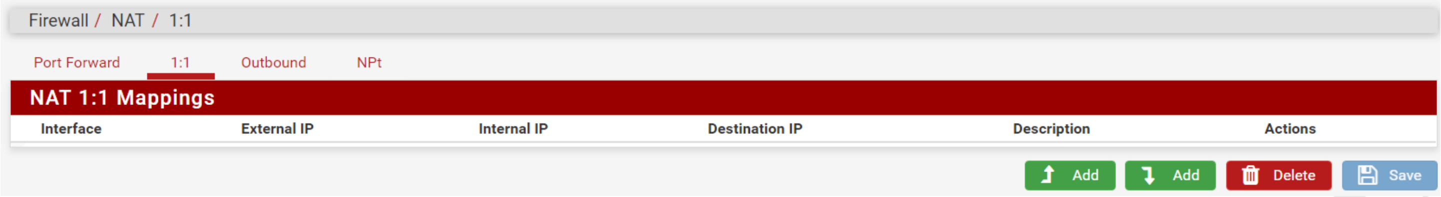
Risks of 1:1 NAT

The risks of 1:1 NAT are largely the same as port forwards. Allowing traffic to pass directly through ICS-Defender, potentially harmful traffic is being permitted into the LAN network.

There is a slight added risk when using 1:1 NAT in that firewall rule mistakes can have more dire consequences. With port forward entries, traffic is constrained to that allowed within the NAT port forward, as well as that traffic allowed by the matching firewall rule. More specifically, when port forwarding, only that specified port will be accessible from the LAN to the WAN so even using an “allow all” rule has less potential issue. When using a 1:1 NAT, and an “allow all” rule, all traffic on the LAN will be accessible from the WAN via the NAT addresses.

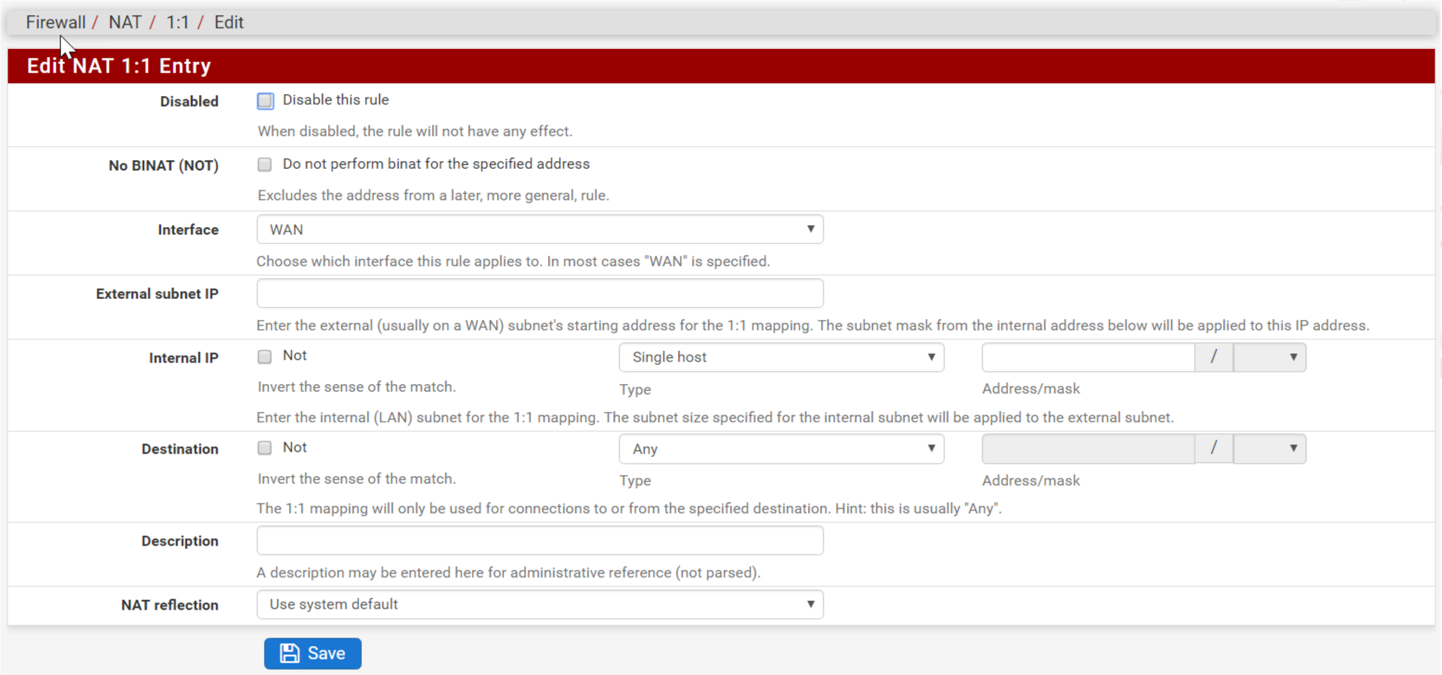
Configuring 1:1 NAT

To configure 1:1 NAT, add an IP Alias for the WAN IP to be used for the 1:1 NAT entry as described in Virtual IPs. Then browse to **Firewall→ NAT→1:1**.



Interface	External IP	Internal IP	Destination IP	Description	Actions

To begin adding a 1:1 NAT entry, click the Add button.



Firewall / NAT / 1:1 / Edit

Edit NAT 1:1 Entry

Disabled	□ Disable this rule When disabled, the rule will not have any effect.
No BINAT (NOT)	□ Do not perform binat for the specified address Excludes the address from a later, more general, rule.
Interface	WAN ▾ Choose which interface this rule applies to. In most cases "WAN" is specified.
External subnet IP	Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.
Internal IP	□ Not — Invert the sense of the match. Single host ▾ — Type / ▾ — Address/mask Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.
Destination	□ Not — Invert the sense of the match. Any ▾ — Type / ▾ — Address/mask The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".
Description	A description may be entered here for administrative reference (not parsed).
NAT reflection	Use system default ▾

Disabled: When checked, this NAT entry is disabled.

No BINAT (NOT): Excluding the gateway and broadcast address from a 1:1 NAT of a full subnet.

Interface: The interface, typically WAN, where the 1:1 NAT will occur.

External Subnet IP: Is the external (typically WAN) address to which the Internal IP will be translated as it enters or leaves the interface. This is typically an IP address on the interface subnet, a virtual IP on the interface, or an IP address routed to the firewall on the interface.

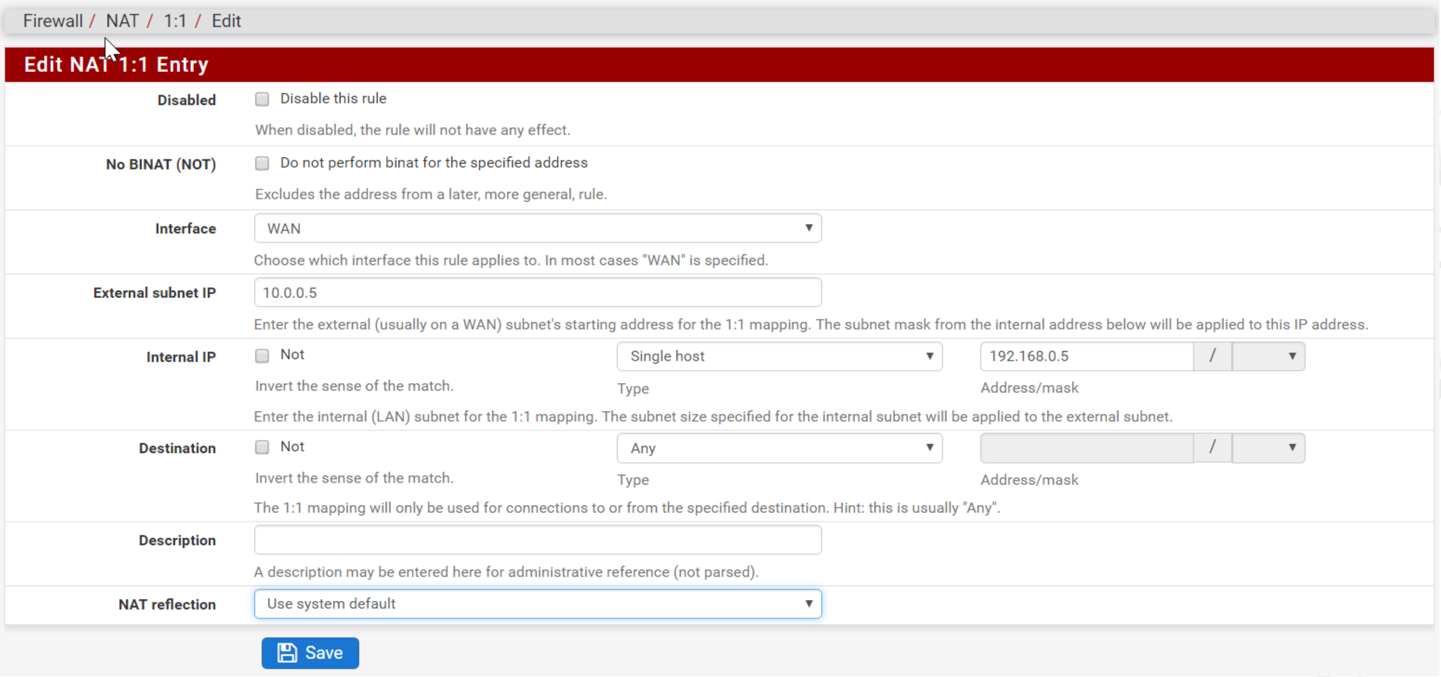
Internal IP: The IP address on the internal network (typically LAN) that will be translated to the External Subnet IP Address. This is usually an address on the LAN interface that uses this ICS-Defender as it's gateway, directly (attached), or indirectly (via static route). Specifying a subnet mask on the Internal IP entry field will translate the entire network matching the subnet mask. For example, using 192.168.1.0/24 will translate all the addresses between 192.168.1.1 and 192.168.1.255. Subnet Mask to CIDR conversion is provided in Subnet Mask to CIDR Quick Reference.

Destination (optional): This is an optional restriction that limits the 1:1 NAT to only take effect when traffic is going from the Internal IP address to the Destination address on the way out, or from the Destination address to the External subnet IP address on the way into the appliance. You may use an alias in the Destination field.

Description: An optional text description to explain the purpose of this entry.

NAT reflection: This option overrides the global NAT reflection options. For any needs regarding this feature-set, please contact Dynics.

Example single IP 1:1 configuration

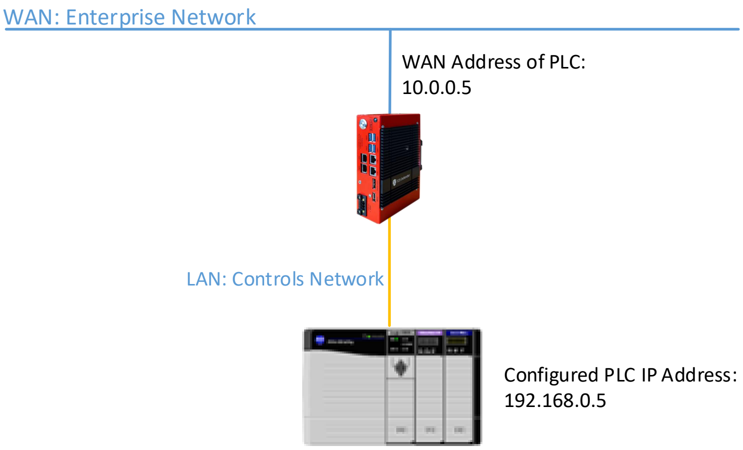


Firewall / NAT / 1:1 / Edit

Edit NAT 1:1 Entry

Disabled	□ Disable this rule When disabled, the rule will not have any effect.
No BINAT (NOT)	□ Do not perform binat for the specified address Excludes the address from a later, more general, rule.
Interface	WAN ▾ Choose which interface this rule applies to. In most cases "WAN" is specified.
External subnet IP	10.0.0.5 Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.
Internal IP	□ Not — Invert the sense of the match. Type: Single host ▾ Address/mask: 192.168.0.5 / ▾ Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.
Destination	□ Not — Invert the sense of the match. Type: Any ▾ Address/mask: / ▾ The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".
Description	 A description may be entered here for administrative reference (not parsed).
NAT reflection	Use system default ▾

1:1 NAT PLC on Controls Network to Enterprise Network



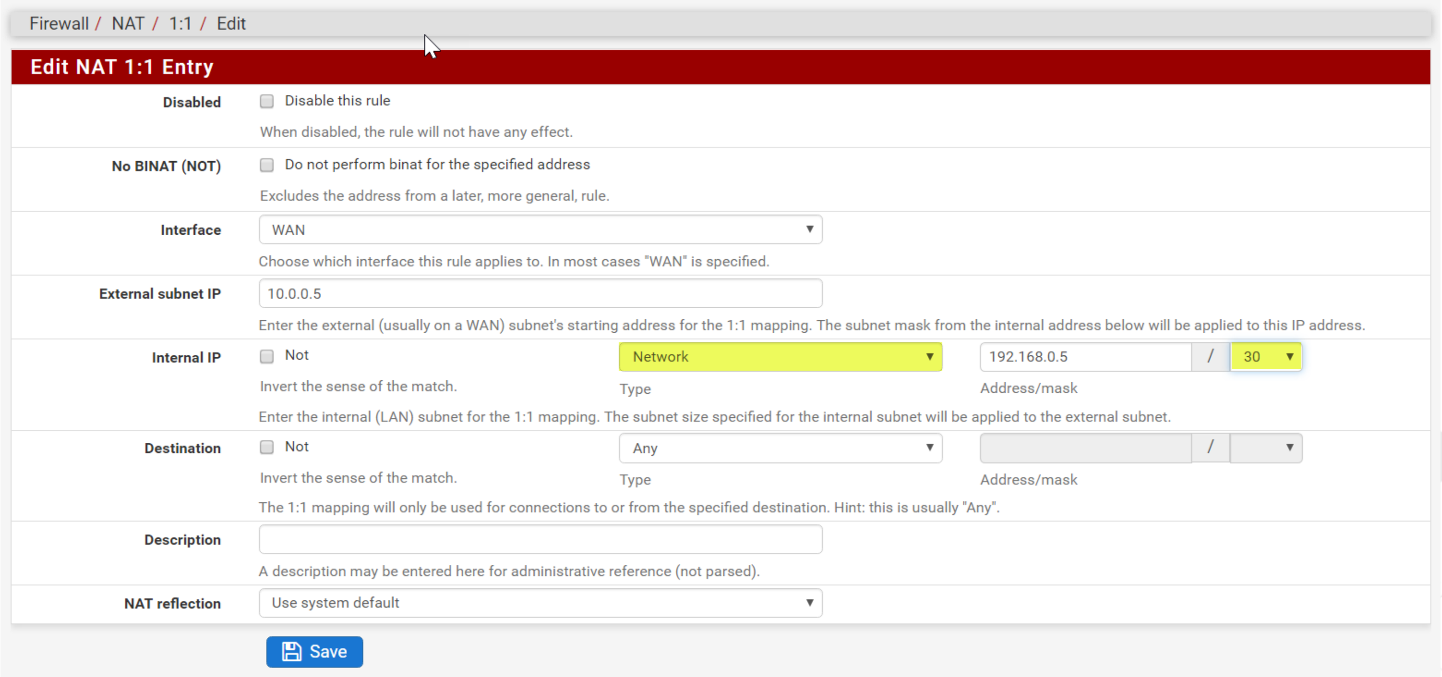
1:1 NAT can be configured for multiple IPs by using CIDR ranges. This section covers configuration of 1:1 NAT for a /30 CIDR range of IPs.

With a matching final octet

192.168.0.5/30 → 10.0.0.5/30

LAN IPs		WAN-IPs
192.168.0.5	→	10.0.0.5
192.168.0.6	→	10.0.0.6
192.168.0.7	→	10.0.0.7
192.168.0.8	→	10.0.0.8

Note that the only difference between single IP 1:1 NAT is the change to "Network" and the "/CIDR" notation. Subnet Mask to CIDR conversion is provided in Subnet Mask to CIDR Quick Reference.



Edit NAT 1:1 Entry

Disabled	□ Disable this rule When disabled, the rule will not have any effect.
No BINAT (NOT)	□ Do not perform binat for the specified address Excludes the address from a later, more general, rule.
Interface	WAN Choose which interface this rule applies to. In most cases "WAN" is specified.
External subnet IP	10.0.0.5 Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.
Internal IP	□ Not — Invert the sense of the match. Type: Network Address/mask: 192.168.0.5 / 30 Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.
Destination	□ Not — Invert the sense of the match. Type: Any Address/mask: / The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".
Description	 A description may be entered here for administrative reference (not parsed).
NAT reflection	Use system default

The last octet of the IP addresses need not be the same on the inside and outside, but it's recommended to do so whenever possible. For example, the following table is also valid.

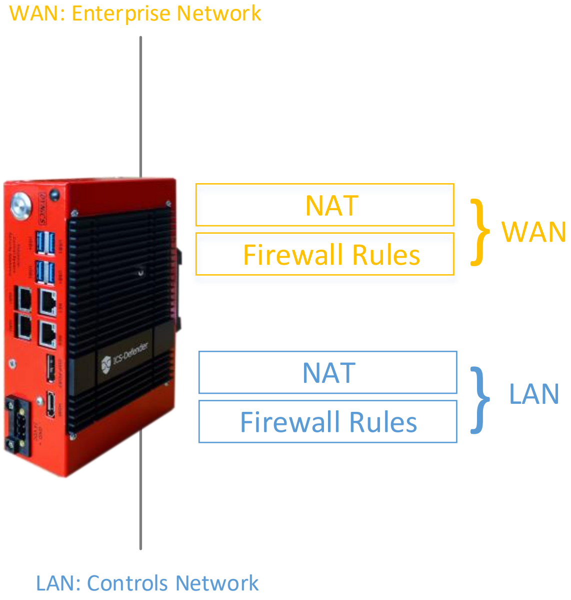
Non-Matching Final Octet

192.168.0.11/30 → 10.0.0.5/30

LAN IPs		WAN-IPs
192.168.0.11	→	10.0.0.5
192.168.0.12	→	10.0.0.6
192.168.0.13	→	10.0.0.7
192.168.0.14	→	10.0.0.8

Ordering of NAT and Firewall Rule Processing

Understanding the order in which Firewall rules and NAT occurs is important when configuring NAT and Firewall rules. The Figure Ordering of NAT and Firewall Rule processing illustrates this ordering.

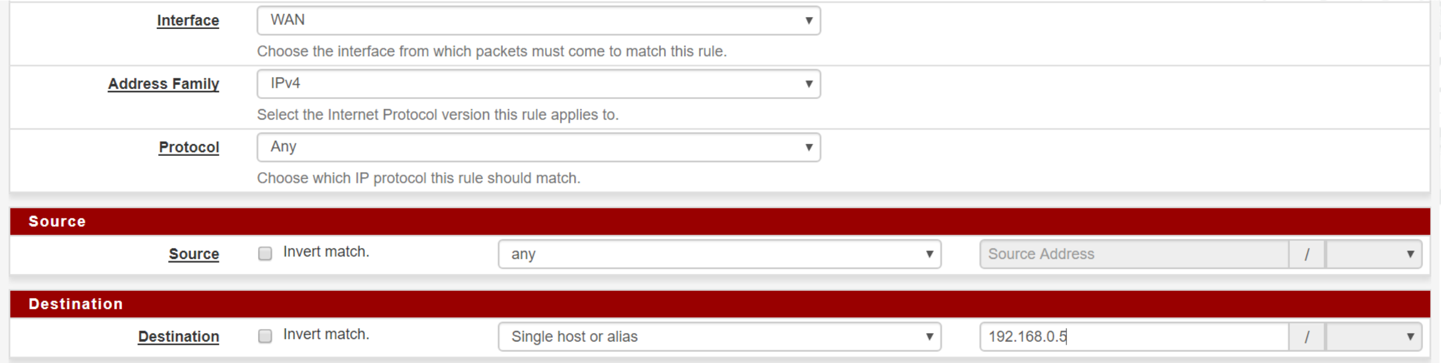


Extrapolating to additional interfaces

The previous diagrams only illustrate a basic two interface LAN and WAN deployment. When working with optional interfaces with OPT and OPT WAN interfaces, the same rules apply. All OPT interfaces behave the same as LAN, and all OPT WAN interfaces behave the same as WAN. Traffic between two internal interfaces behaves the same as LAN to WAN traffic, though the default NAT rules will not translate traffic between internal interfaces so the NAT layer does not apply in those cases. Defining Outbound NAT rules that match traffic between internal interfaces, it will apply as shown.

Rules for NAT

For rules on WAN or OPT WAN interfaces, because NAT translates the destination IP of the traffic before the appliance rules evaluate it, WAN Firewall rules must always specify the private IP address as the destination. For example, with a WAN IP of 10.0.0.5 translated to a PLC (LAN) address of 192.168.0.5 a rule must be created on the WAN firewall rules tab that targets the PLC IP address (or alias containing those addresses).



Interface	WAN ▾ Choose the interface from which packets must come to match this rule.		
Address Family	IPv4 ▾ Select the Internet Protocol version this rule applies to.		
Protocol	Any ▾ Choose which IP protocol this rule should match.		

Source

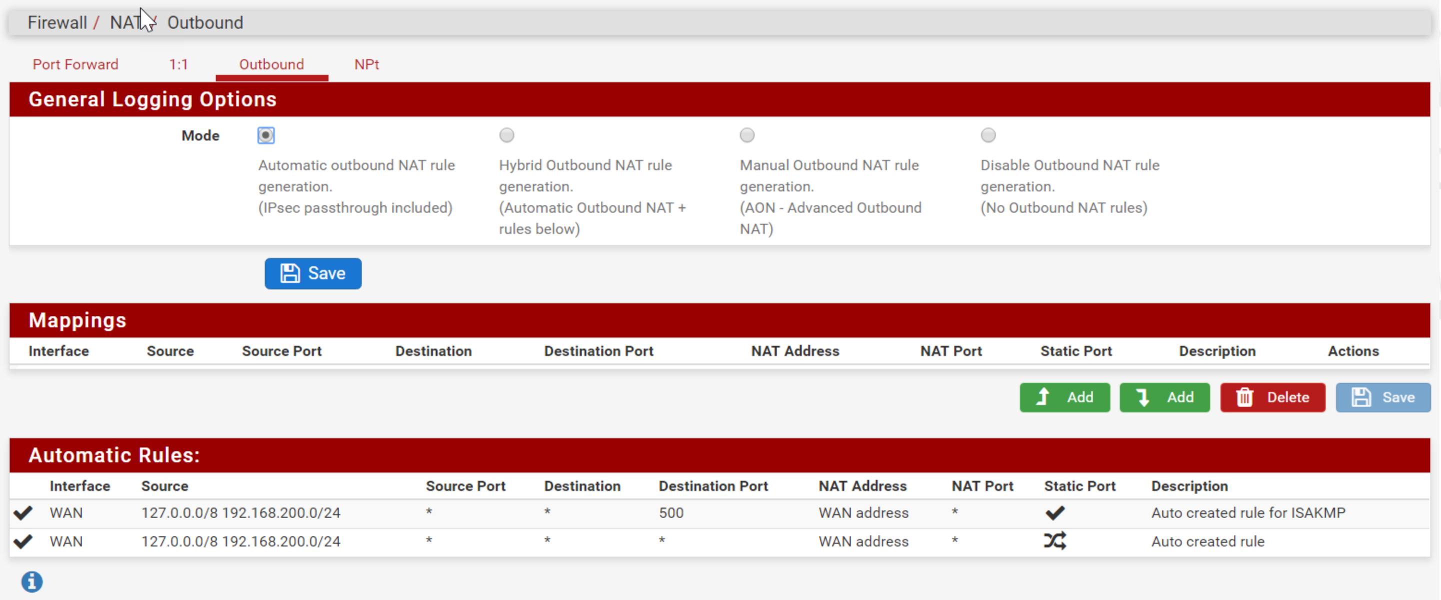
Source	□ Invert match.	any ▾	Source Address / ▾

Destination

Destination	□ Invert match.	Single host or alias ▾	192.168.0.5 / ▾

Outbound NAT

Outbound NAT, also known as “Source NAT” in some instances, controls how traffic leaving an interface of ICS-Defender will have its source address and ports translated. For configuration, navigate to **Firewall → NAT → Outbound tab**.



Firewall / NAT / Outbound

Port Forward | 1:1 | Outbound | NPt

General Logging Options

Mode

● Automatic outbound NAT rule generation. (IPsec passthrough included)

○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)

○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)

○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions

Add | Add | Delete | Save

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 192.168.200.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 192.168.200.0/24	*	*	*	WAN address	*	🔀	Auto created rule

There are four configuration options for Outbound NAT in ICS-Defender,

- Automatic outbound NAT rule generation
- Hybrid outbound NAT rule generation
- Manual outbound NAT generation
- Disabled

As with other rules in ICS-Defender, rules are considered from the top of the list down, and the first match is used. Even if rules are present in the Outbound NAT screen, they will not be evaluated unless Outbound NAT is set to Manual outbound NAT rule generation.

Note: Manual Outbound NAT only controls what happens to traffic as it leaves an interface. It does not control the interface though which traffic will exit the appliance. That is handled by the routing table (Static Routes) or policy routing.

Default Outbound NAT Rules

When using the default Automatic outbound NAT, ICS-Defender will automatically create NAT rules translating traffic leaving any internal network to the IP address of the WAN interface which the traffic leaves. Static route networks and remote access VPN networks are also included in the automatic NAT rules.

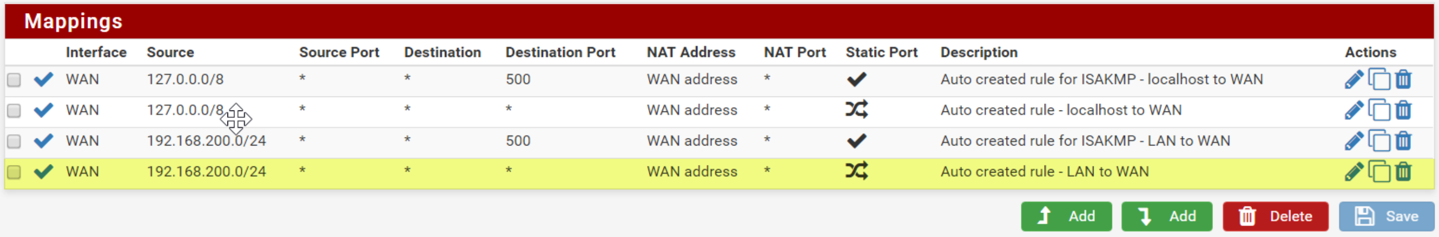
If no rules exist in the Outbound NAT list and the radio buttons switch to Manual Outbound NAT, upon being saved, a full set of rules will be created that are the equivalent of the automatic rules.

Static Port

By default, ICS-Defender rewrites the source port on all outgoing packets. Some operating systems do a poor job of source port randomization, if it's done at all. Unfortunately, that makes it easier to spoof IP addresses and makes it possible to fingerprint hosts behind ICS-Defender from its outbound traffic. Rewriting the source port eliminates these potential (but unlikely) security vulnerabilities.

However, doing so occasionally breaks applications. There are built in rules when Advanced Outbound NAT is disabled that don't do this for UDP 500 (IKE for VPN traffic) because it will almost always be broken by rewriting the source port. All other traffic has the source port rewritten by default.

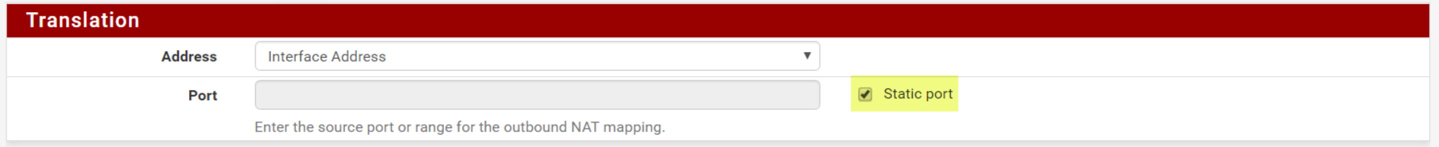
Certain protocols do not work properly when the source port gets rewritten. To disable this functionality, use the static port option. On the **Firewall→ NAT→ Outbound tab**. Select Manual Outbound NAT rule generation and save the configuration. A rule is created at the bottom of the page labeled "Auto created rule – LAN to WAN".



Mappings

		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
□	✓	WAN	127.0.0.0/8	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	✎ ⧉ 🗑
□	✓	WAN	127.0.0.0/8	*	*	*	WAN address	*	⤮	Auto created rule - localhost to WAN	✎ ⧉ 🗑
□	✓	WAN	192.168.200.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - LAN to WAN	✎ ⧉ 🗑
□	✓	WAN	192.168.200.0/24	*	*	*	WAN address	*	⤮	Auto created rule - LAN to WAN	✎ ⧉ 🗑

Click the ✎ button to the right of the rule to edit. Check the Static Port option, save, and apply changes.



Translation

Address: Interface Address

Port: ☑ Static port

Enter the source port or range for the outbound NAT mapping.

After making this change, the source port on outgoing traffic will be preserved. This can also be done more selectively by adding a rule at the top of the list to match only a specific device. It is better to do this in a more selective fashion, to avoid any potential conflict if two local hosts use the same source port to talk to the same remote server and port.

Disabling Outbound NAT

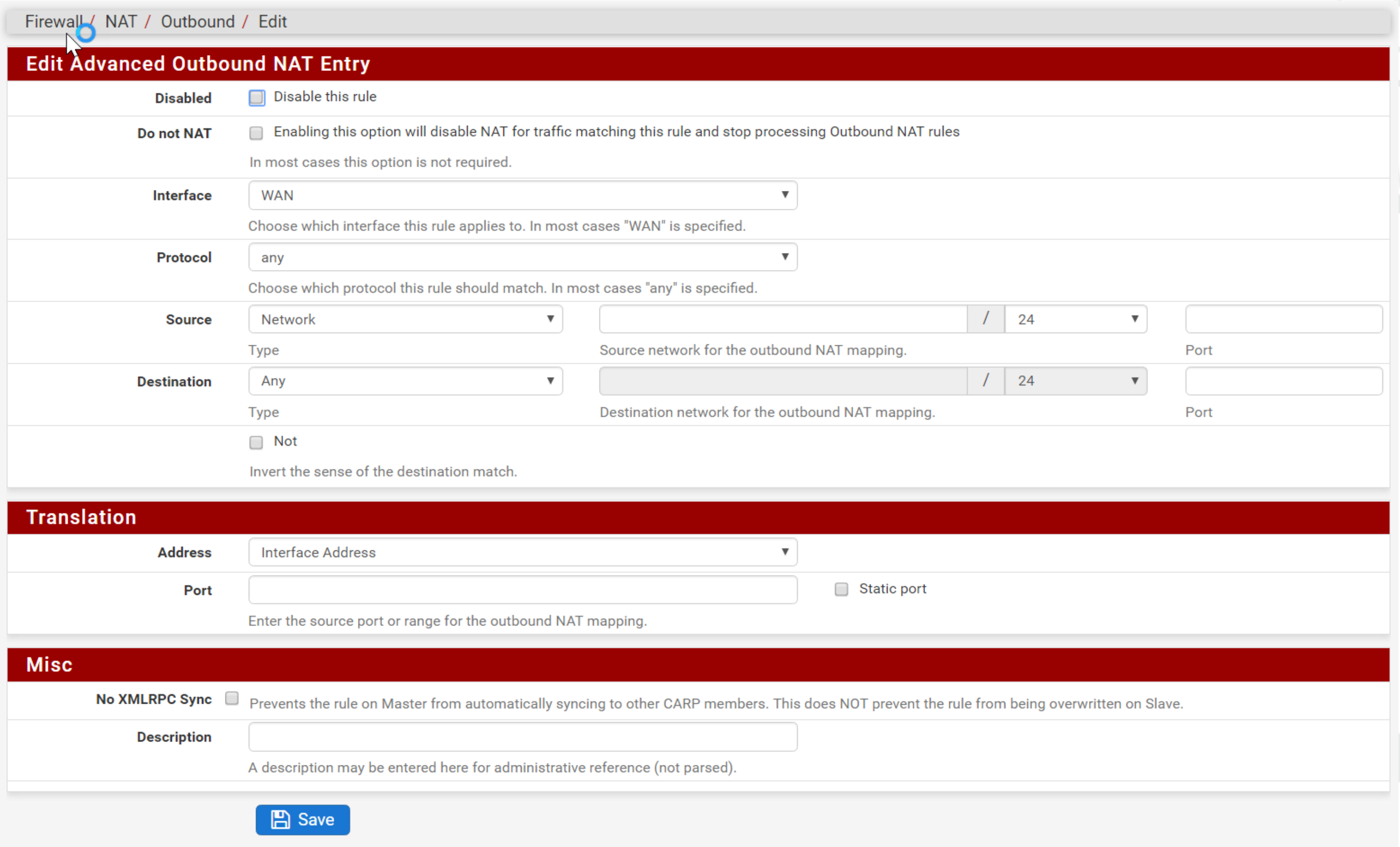
If using public IP addresses on local interfaces, and thus do not need to apply NAT to traffic passing through the appliance, 🗑 disable NAT for that interface. To do this, change the Outbound NAT setting to Manual Outbound NAT and save. After that change, one or more rules will appear in the list on the Outbound NAT screen. Delete the rule or rules specifying the source of the public IP subnets by clicking each line once (or check the box at the start of the line) and then click the button at the bottom of the list. Click ***Apply Changes*** to complete the process.

Once all the rules have been deleted, outbound NAT will no longer be active for those source IP addresses, and ICS-Defender will then route public IP addresses without translation.

To completely disable outbound NAT, delete all of the rules that are present when using Manual Outbound NAT.

Working with Manual Outbound NAT Rules

Manual Outbound NAT rules are very flexible and can translate traffic in many ways. Outbound NAT rules are managed and processed like many other rule types in ICS-Defender. The rules are matched from the top-down, and the first match is used. Because the NAT rules are shown in a single page the Interface column is a source of confusion for some; As traffic leaves an interface, only the outbound NAT rules for that interface are consulted.



Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled	□ Disable this rule
Do not NAT	□ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules In most cases this option is not required.
Interface	WAN ▾ Choose which interface this rule applies to. In most cases "WAN" is specified.
Protocol	any ▾ Choose which protocol this rule should match. In most cases "any" is specified.
Source	Network ▾ (Type) / 24 ▾ (Source network for the outbound NAT mapping.) Port
Destination	Any ▾ (Type) / 24 ▾ (Destination network for the outbound NAT mapping.) Port □ Not Invert the sense of the destination match.

Translation

Address	Interface Address ▾
Port	□ Static port Enter the source port or range for the outbound NAT mapping.

Misc

No XMLRPC Sync	□ Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
Description	A description may be entered here for administrative reference (not parsed).

Do not NAT: Checking this option will cause packets matching the rule to not have NAT applied as they leave. This would only be needed if the traffic would otherwise match a NAT rule, but should not have NAT. One common use for this is to add a rule exception so that the appliance's IPs do not get NAT applied.

Interface: This is the interface where this NAT rule will apply, when traffic is leaving via this interface. Typically, this is WAN or an OPT WAN, but in some special cases it could be LAN or other internal interface.

Protocol: In most cases Outbound NAT should be applied to all protocols, but in certain cases it may be necessary to restrict the protocol upon which the NAT will act.

Source: The source is the local network which will have its address translated as it leaves Interface. This is typically the LAN, DMZ, or a VPN subnet. The Source Port should almost always be left blank to indicate "any".

Destination: In most cases, the destination is left set to "any" so that traffic going out this interface will be translated. However, the destination can be restricted as needed to translate in a certain way when going to a specific destination.

Translation: The address field inside of the translation section controls exactly what happens to the source address of the traffic when this rule is matched. Most commonly, this is set to Interface Address so the traffic is translated to the IP address of Interface, e.g. the WAN IP address. The Address drop-down also contains all Virtual IPs, host aliases, and Other Subnet to manually enter a subnet for translation.

Port: Specify a specific source port for translation. This is most always left blank, but could be required if the client selects a random source port but the server requires a specific source port. Checking the Static Port option will cause the original source port of the client's traffic to be maintained after the source IP address has been translated. Some protocols require this, like IPsec without NAT-T, and some protocols behave better with this, such as SIP and RTP.

No XMLRPC Sync: Only used if this ICS-Defender is part of a failover cluster If this ICS-Defender is the master in a failover cluster checking this option will prevent this rule from being synchronized to the other members of a failover cluster, which is usually undesirable. This option is only effective on master nodes, it does not prevent a rule from being overwritten on slave nodes.

Description: An optional text reference to explain the purpose of this rule.

Note: Subnet Mask to CIDR conversion is provided in Subnet Mask to CIDR Quick Reference.

NAT and Protocol Compatibility

Some protocols do not work well and some not at all with NAT. Some protocols embed IP addresses within packets, some do not work properly if the source port is rewritten. This section covers the protocols that have difficulties with NAT, and how to work around these issues where possible.

FTP

FTP poses problems with both NAT and appliances because of the design of the protocol. FTP was initially designed in the 1970s, and the current standard defining the specifications of the protocol was written in 1985. Since FTP was created more than a decade prior to NAT, and long before appliances were common, it does some things that are very NAT and firewall unfriendly. ICS-Defender uses an in-kernel FTP proxy.

FTP servers behind NAT

FTP servers behind NAT must use port 21 by default, as the FTP proxy will only launch when port 21 is specified. The FTP proxy can be configured to attach on other ports by setting a system tunable.

FTP modes

FTP can act in multiple modes that change the behavior of the client and server, and which side listens for incoming connections. The complications of NAT and appliance rules depend on these modes and whether hosting a server or acting as a client.

Active Mode

With Active Mode FTP, when a file transfer is requested, the client listens on a local port, and then tells the server the client IP address and port. The server will then connect back to that IP address and port to transfer the data. This is a problem for firewalls because the port is typically random, though modern clients allow for limiting the range that is used. In the case of a client behind NAT, the IP address given would be a local address, unreachable from the server. Not only that, but an appliance rule would need to be added and a port forward allowing traffic into this port.

When the FTP proxy is in use, it attempts to do three things. First, it will rewrite the FTP PORT command so that the IP address is the WAN IP address of the appliance, and a randomly chosen port on that IP address. Next, it adds a port forward that connects the translated IP address and port to the original IP address and port specified by the FTP client. Finally, it allows traffic from the FTP server to connect to that "public" port.

When everything is working as it should, this all happens transparently. The server never knows it's talking to a client behind NAT, and the client never knows that the server isn't connecting directly.

In the case of a server behind NAT, this is not usually a problem since the server will only be listening for connections on the standard FTP ports and then making outbound connections back to the clients.

Passive Mode

Passive Mode (PASV) acts somewhat in reverse. For clients, it is more NAT and firewall friendly because the server listens on a port when a file transfer is requested, not the client. Typically, PASV mode will work for FTP clients behind NAT without using any proxy or special handling.

When a client requests PASV mode the server will have to give its IP address and a random port to which the client can attempt to connect. Since the server is on a private network, that IP address and port will need to be translated and allowed through the appliance.

Extended Passive Mode

Extended Passive Mode (EPSV) works like PASV mode but makes allowances for use on IPv6. When a client requests a transfer, the server will reply with the port to which the client should connect. The same caveats for servers in PASV mode apply here.

FTP Servers and Port Forwards

To ensure the FTP proxy works properly for port forwards, a port forward NAT rule should be set for exactly the FTP port, e.g. 21, and not a range or alias containing multiple ports.

TFTP (Trivial File Transfer Protocol)

Standard TCP and UDP traffic initiate connections to remote hosts using a random source port in the ephemeral port range (range varies by operating system, but falls within 1024-65535), and the destination port of the protocol in use. Replies from server to client reverse that the source port is the client's destination port, and the destination port is the client's source port. This is how ICS-Defender associates the reply traffic with connections initiated from inside the network.

TFTP does not follow this methodology. The standard defining TFTP, RFC 1350, specifies the reply from the TFTP server to client will be sourced from a pseudo-random port number. The TFTP client may choose a source port of 10325 (as an example) and use the destination port for TFTP, port 69. The server for other protocols would then send the reply using source port 69 and destination port 10325. Since TFTP instead uses a pseudo-random source port, the reply traffic will not match the state pf has created for this traffic. Hence the replies will be blocked because they appear to be unsolicited traffic from the Internet.

To pass TFTP through the ICS-Defender, there is a TFTP proxy that is configurable **System→ Advanced→ Firewall & NAT tab**.

IPv6 Network Prefix Translation (NPt)

Network Prefix Translation or NPt for short, works similarly to 1:1 NAT. NPt can be found under **Firewall→ NAT→ NPt tab**. NPt will take one prefix and translate it to another.

ICS-Defender can translate * 2001:db8:1111:2222::/64 to be 2001:db8:3333:4444::/64 and though the prefix changes, the remainder of the address will be identical for a given host on that subnet.

With NPt, a "private" IPv6 space (fc00::/7) on the LAN can be used and have it translated to a routed IPv6 prefixes as it comes and goes from the LAN.

Troubleshooting NAT

NAT can be a complex animal, and in all but the most basic environments, there are bound to be some issues getting a good working configuration. This section will go over a few common problems and some suggestions on how they might be solved.

Port Forward Troubleshooting

Port forwards can be tricky, since there are many things to go wrong, many of which could be in the client configuration and not ICS-Defender. Most issues encountered users have been solved by one or more of the following suggestions.

Port forward entry incorrect

Before any other troubleshooting task, review the settings for port forward. Go over the process in Adding Port Forwards again, and double check that the values are correct. If the NAT IP or the Ports are changed it's necessary to adjust the matching firewall rule if not using linked firewall rules. Common things to check for:

1. Correct interface (usually should be WAN, or wherever traffic will be entering the ICS-Defender box).
2. Correct NAT IP, which must be reachable from an interface on the ICS-Defender router.
3. Correct port range, which must correspond to the service you are trying to forward.
4. Source and source port should almost always be set to any.

Missing or incorrect appliance rule

After checking port forward settings, double check that the appliance rule has the proper settings. An incorrect appliance rule would also be apparent by viewing the appliance logs. The destination for the appliance rule should be the internal IP address of the target system and not the address of the interface containing the port forward.

Port is enabled on the target machine

Another consideration is that ICS-Defender may be forwarding the port properly, but the target machine may be blocking the traffic or not allow connections to a particular port. If there is a firewall on the target system, check its logs and settings to confirm whether or not the traffic is being blocked at that point.

ICS-Defender is not the target system's gateway

For ICS-Defender to properly forward a port for a local system, ICS-Defender must be the default gateway for the target system. If ICS-Defender is not the gateway, the target system will attempt to send replies to port forward traffic out whatever system is the gateway.

Target machine is not listening on the forwarded port

If, when the connection is tested, the request is rejected instead of timing out, likely ICS-Defender is forwarding the connection properly and the connection is rejected by the target system. This can happen when the target system has no service listening on the port in question, or if the port being forwarded does not match the port on which the target system is listening.

Outbound NAT Troubleshooting

When using manual outbound NAT, and there are multiple local subnets, an outbound NAT entry will be needed for each. This applies if traffic is intended to exit with NAT after coming into the ICS-Defender router via a VPN connection such as PPTP or OpenVPN.

One indication of a missing outbound NAT rule would be seeing packets leave the WAN interface with a source address of a private network.

NAT is configured in two directions inbound and outbound. Outbound NAT defines how traffic leaving the LAN network destined for the WAN is translated. Inbound NAT refers to traffic entering the LAN network from the WAN. The most common type of inbound NAT and the one most are familiar with is port forwards.

Default NAT Configuration

This section describes the default NAT configuration of ICS-Defender. The most commonly suitable NAT configuration is generated automatically. In some environments, there may be reason to modify this configuration, and ICS-Defender fully enables customization entirely from the web interface.

Default Outbound NAT Configuration

The default NAT configuration in ICS-Defender with a two interface LAN and WAN deployment automatically translates Internet-bound traffic to the WAN IP address. When multiple WAN interfaces are configured, traffic leaving any WAN interface is automatically translated to the address of the WAN interface being used.

Static port is automatically configured for IKE (part of IPsec). Static port is covered in more detail in Outbound NAT about Outbound NAT.

For detecting WAN-type interfaces for use with NAT, the system looks for the presence of a gateway selected on the interface if it’s static IP, or assumes it is a WAN if it is a dynamic type such as PPPoE or DHCP.

Default Inbound NAT Configuration

By default, nothing is allowed in from the WAN interface. If traffic initiated on the WAN to a device on the LAN is necessary, configure port forwards or 1:1 NAT.

Firewall Rules

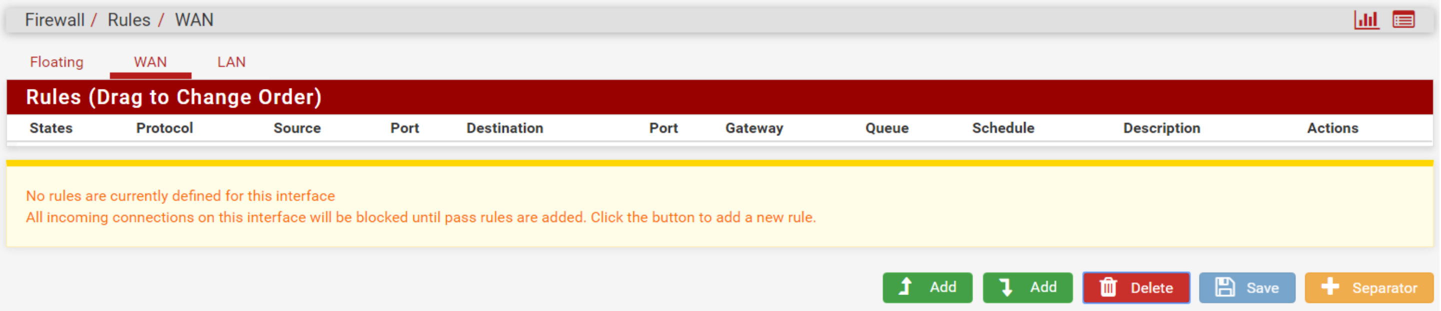
Navigating to **Firewall→ Rules** will display the WAN Interface specific firewall rules.

Important: The first matching rule of a packet in a list of rules wins, no further rules will be evaluated.

Legend

- ✓ Pass
- ▼ Match
- ✖ Block
- ✋ Reject
- ≡ Log
- ⚙ Advanced filter
- ⏩ "Quick" rule. Applied immediately on match.

Note: The difference between block and reject is when rejected, a packet is returned to the sender often indicating that the packet was rejected, whereas when a packet is blocked, the packet is dropped silently. In either case, the original packet is discarded.



Firewall / Rules / WAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

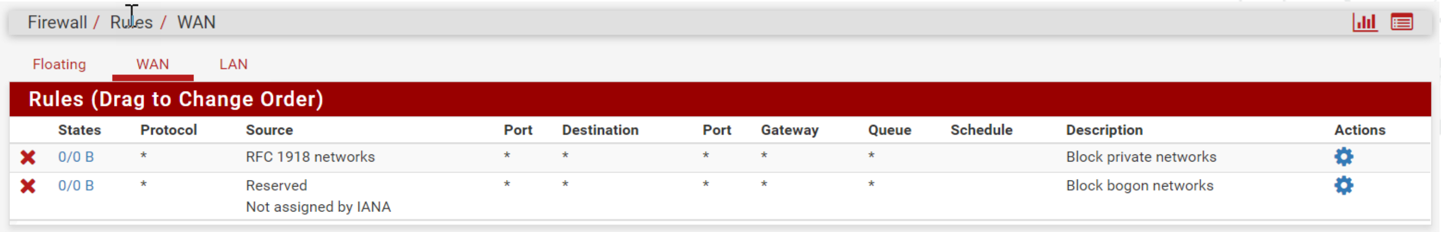
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Note that the names WAN and LAN maybe renamed in their Interface configuration, if so, the changed name is displayed instead of WAN or LAN.

Rule Categories:

- **Floating**: Rules can apply to all interfaces selected at the time configured.
- **WAN**: Rules apply to only the WAN interface
- **LAN**: Rules apply to only the LAN interface

WAN Rules



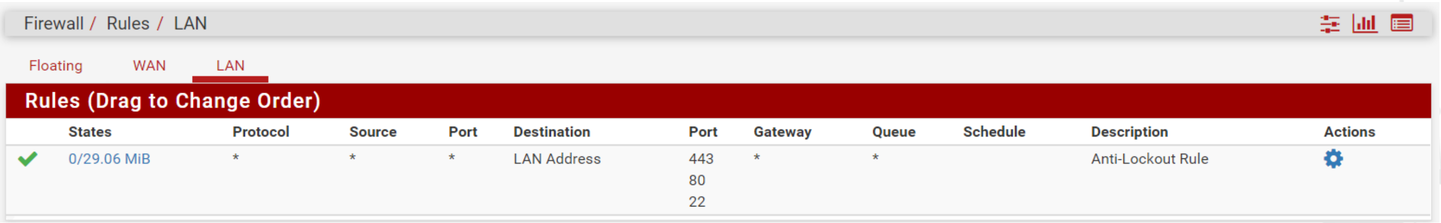
Firewall / Rules / WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✖	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✖	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

There may exist two rules in the WAN rules list based on the check box settings when defining the interface. The rules are auto-generated or removed based on the state of the check box for private and bogon network traffic.

LAN Rules



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/29.06 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	⚙

Every ICS-Defender configuration (unless a user deletes it) includes an anti-lockout rule for the LAN interface. This is done to prevent a user from locking themselves out of the WebGUI completely. Accessing the ICS-Defender on the LAN interface, at the assigned IP address, should present the WebGUI login screen.

Rule Editing Buttons

Add   Add a rule above the currently selected rule.

Add   Add a rule below the currently selected rule.

Delete   Delete all rules which are checked.

Separator   Creates an organizational rule separator with text description and color coding.

Save   Save any re-ordered firewall rules or newly created separators.

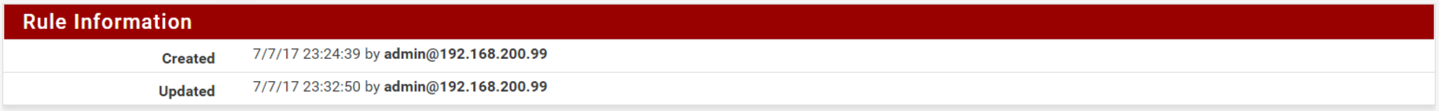
Reorder Rules

Rules can be reordered by clicking and dragging them before and after other rules in the list. Clicking the ⚓ button will move all checked rules before the row with the clicked ⚓ .

The Save button must be pressed to make the reordering of the rules permanent.

Rule Change Tracking

At the bottom of each configuration page for a rule is the creation date and time and the user who created the rule. Also included is the date, time, and user of the last update to the rule.



Rule Information

Created	7/7/17 23:24:39 by **admin@192.168.200.99**
Updated	7/7/17 23:32:50 by **admin@192.168.200.99**

Rule Order of Evaluation

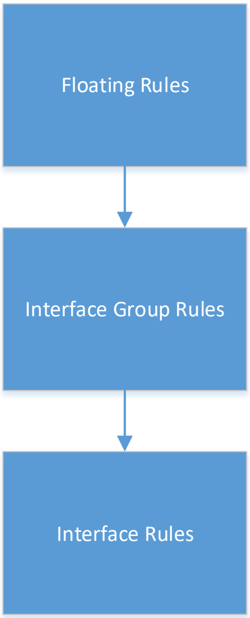
General Methodology

Rules on an interface are processed on a per interface basis, always on the inbound direction on that interface. That means traffic initiated from the LAN is filtered on the LAN rules tab. Traffic initiated from the WAN is filtered with the WAN rules. All rules in ICS-Defender are Stateful by default, a state table entry is created when traffic matches an allow rule. All reply traffic is automatically permitted by that same state table entry.

The exception to this behavior are Floating Rules, which can act upon any interface using inbound, outbound, or both directions. Outbound rules are not required as filtering is applied on the inbound direction of every interface.

Order of Rule-Set Precedence

There are three sets or classes of rules. These sets include interface rules, floating rules, and interface group rules. The order of processing of these rules is important to understanding how to use them effectively.



As the rules process packets, they are compared in the order shown above. It's important to note that a rule designed to block traffic X in the "Interface Rules" will not be effective if there is a rule in the "Interface Group Rules" or "Floating Rules" designed to pass that same traffic.

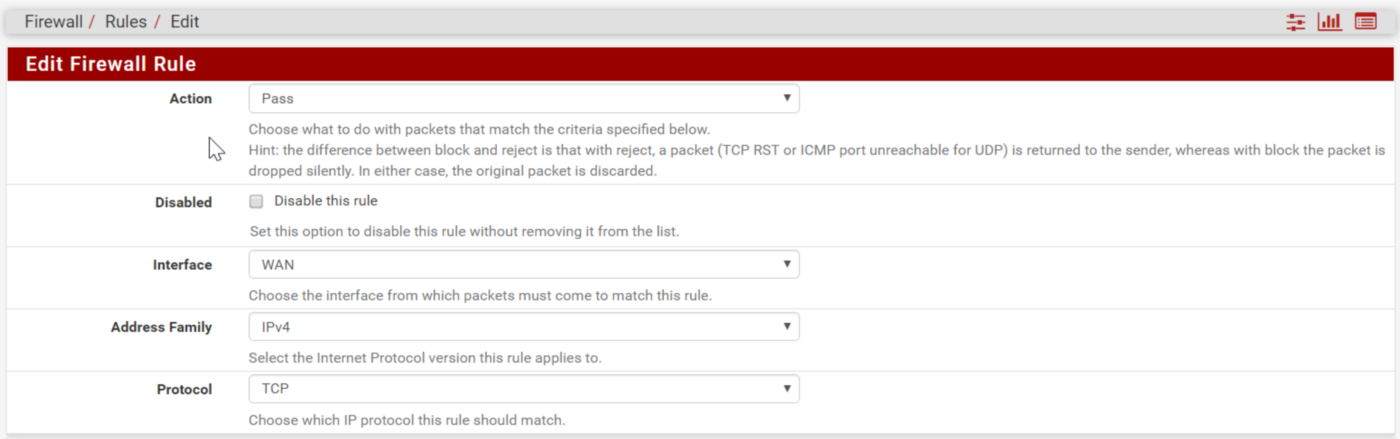
Floating Rules

Floating rules have additional options over interface or interface group rules. For any needs regarding this feature-set, please contact Dynics.

Anti-Spoofing Rules

ICS-Defender has the capability to block spoofed traffic. Providing Unicast Reverse Path Forwarding (uRPF) functionality as defined in RFC 3704. ICS-Defender checks each packet against its routing table and if a connection attempt comes from a source IP on an interface where it is known the network doesn't reside, the packet is dropped. For example, a packet entering the WAN interface with a source IP of the LAN or an Internal network is dropped. Any traffic initiated on the internal network with a source IP that does not reside on the internal network is dropped as well.

Configuring Firewall Rules



Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass ▾ Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN ▾ Choose the interface from which packets must come to match this rule.
Address Family	IPv4 ▾ Select the Internet Protocol version this rule applies to.
Protocol	TCP ▾ Choose which IP protocol this rule should match.

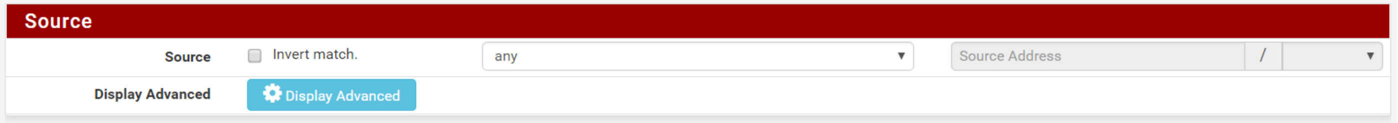
Action: Pass, Block, or Reject any packets that match the criteria or conditions specified in the rule.

Disabled: Disable or enable the rule.

Interface: This is the interface from which the packets must come to match the rule.

Address Family: IPv4, IPv6, or both.

Protocol: Which protocol the rule must match.



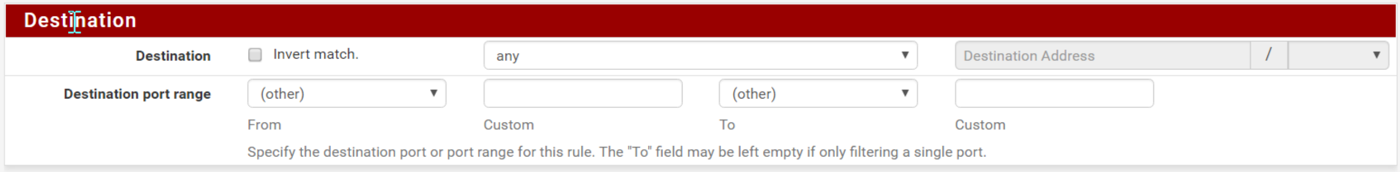
Source

Source	□ Invert match.	any ▾	Source Address / ▾
Display Advanced	Display Advanced		

Source: Specify the source IP address, subnet, or alias that will match this rule.

- **Any**: Matches any address
- **Single Host or Alias**: Match a single IP address, hostname, or alias.
- **Network**: Enter both an IP address and subnet mask to match a range or addresses
- **Presets**: WAN Address, LAN Address, LAN Subnet etc.

Display Advanced: For any needs regarding this feature-set, please contact Dynics.



Destination

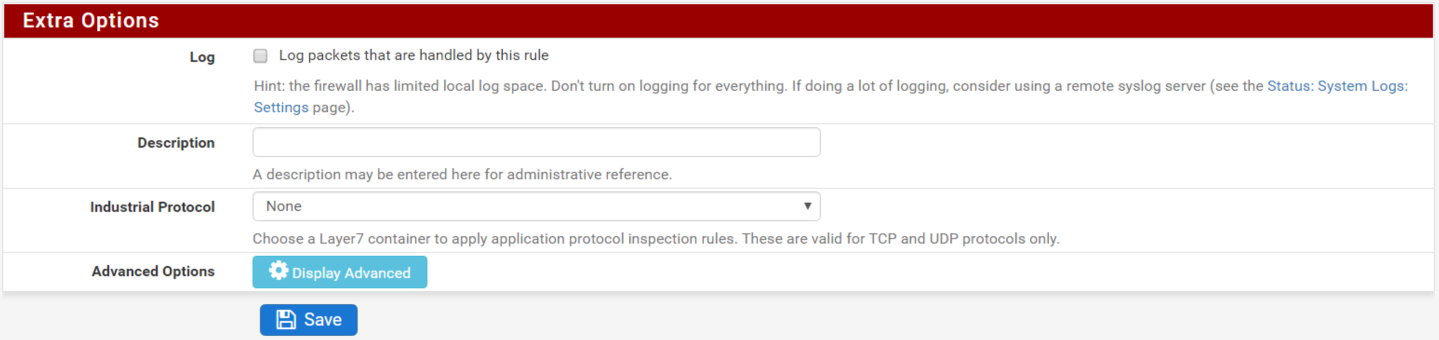
Destination	□ Invert match.	any ▾	Destination Address / ▾	
Destination port range	(other) ▾ From	Custom	(other) ▾ To	Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Destination: The destination IP address, subnet, or alias that will match this rule.

- **Any**: Matches any address
- **Single Host or Alias**: Match a single IP address, hostname, or alias.
- **Network**: Enter both an IP address and subnet mask to match a range or addresses
- **Presets**: WAN Address, LAN Address, LAN Subnet etc.

Destination Port Range: The port or port range to match against when checking a packet against this rule.



Extra Options

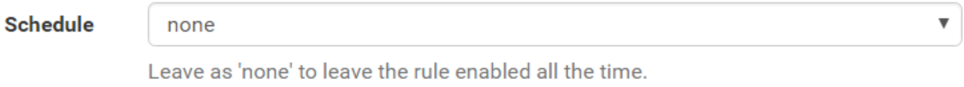
Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	A description may be entered here for administrative reference.
Industrial Protocol	None ▾ Choose a Layer7 container to apply application protocol inspection rules. These are valid for TCP and UDP protocols only.
Advanced Options	Display Advanced

Log: Specifies whether packets which match this rule will be logged to the firewall log.

Description (optional): A description of the rule and what it is intended to do.

Industrial Protocol: Choose a profile for an industrial protocol such as EtherNet/IP or Modbus-TCP to use in evaluating this firewall rule.

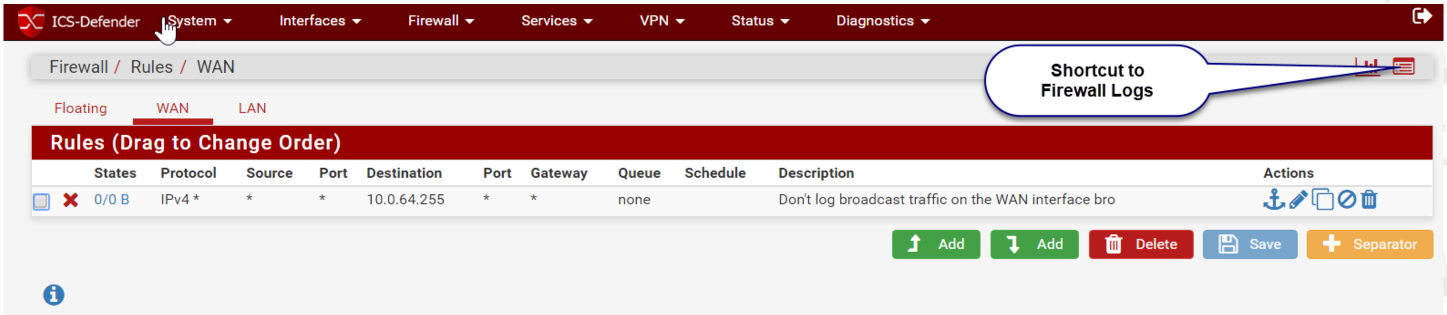
Advanced Options: For any needs regarding this feature-set, please contact Dynics. However, when using a schedule for a rule, the option field to select the schedule is found under "Extra Options" in the rule configuration. If I schedule has been defined, to apply it to this rule, select it from this drop down.



Schedule	none ▾ Leave as 'none' to leave the rule enabled all the time.

Firewall Logs

Firewall logs can be viewed by navigating to Status→System Logs→Firewall or by clicking the shortcut from the Firewall screen.

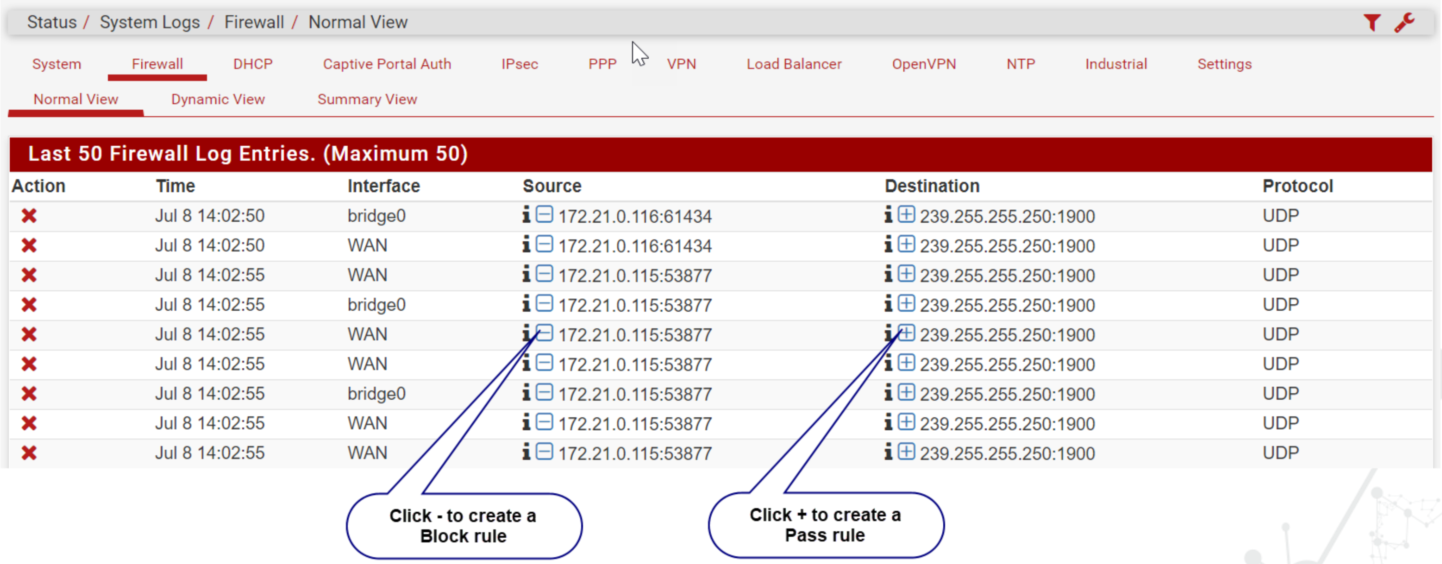


Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0/0 B	IPv4 *	*	*	10.0.64.255	*	*	none		Don't log broadcast traffic on the WAN interface bro	

Easy Rules

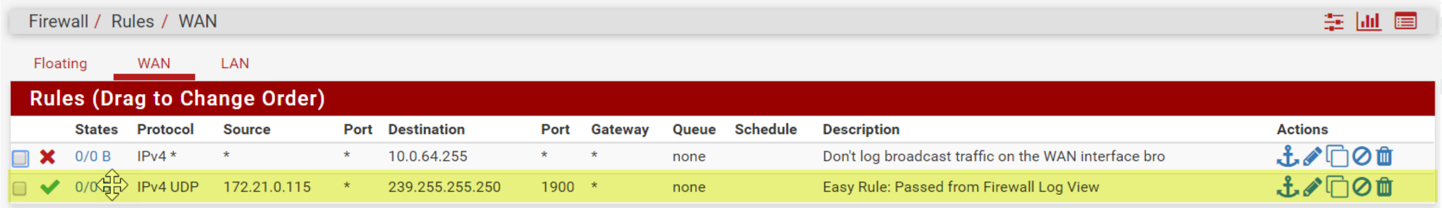
Easy rules are created from the log screen by simply identifying what packet should be passed or blocked and clicking the appropriate button to automatically add such a rule.



Last 50 Firewall Log Entries. (Maximum 50)

Action	Time	Interface	Source	Destination	Protocol
✗	Jul 8 14:02:50	bridge0	172.21.0.116:61434	239.255.255.250:1900	UDP
✗	Jul 8 14:02:50	WAN	172.21.0.116:61434	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	WAN	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	bridge0	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	WAN	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	WAN	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	bridge0	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	WAN	172.21.0.115:53877	239.255.255.250:1900	UDP
✗	Jul 8 14:02:55	WAN	172.21.0.115:53877	239.255.255.250:1900	UDP

Clicking the + to pass a rule generates an entry in the firewall rules list on the specified interface. In this example, a “Pass” easy rule was created. Note the description field in the rule indicates how it was created. The description field should be updated to accurately describe the reason for the rule.



Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0/0 B	IPv4 *	*	*	10.0.64.255	*	*	none		Don't log broadcast traffic on the WAN interface bro	
□	✓	0/0 B	IPv4 UDP	172.21.0.115	*	239.255.255.250	1900	*	none		Easy Rule: Passed from Firewall Log View	

Firewall Rule Best Practices

Deny! Deny! Deny!

Firewall rules should always follow a default behavior of DENY. Rules should be configured to only allow the absolute necessary minimum amount of traffic. In other words, deny all traffic and expressly permit only that traffic which is needed.

Short Rulesets

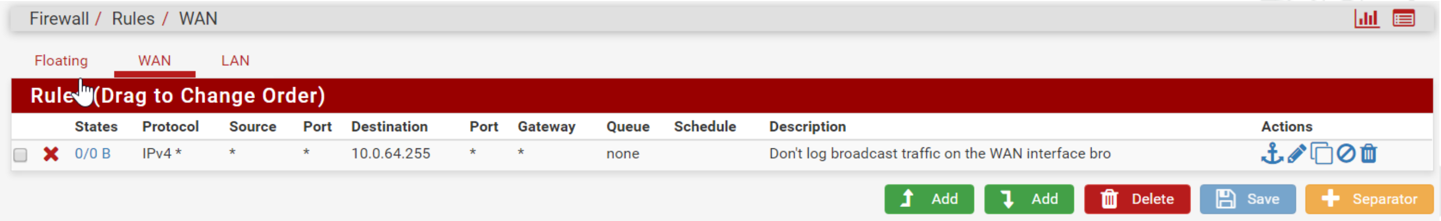
Using aliases is a very powerful methodology to keep rulesets short. Longer rulesets are difficult to manage and are prone to error.

Documentation

Use of the description fields in both the firewall and NAT configuration areas is highly recommended. After time or with change of personnel it's often difficult to recall or understand the "why" of a particular rule. A full configuration document which is kept up to date is also very important to maintain a solid control over the appliance and it's configuration.

Reduce Log Noise

By default, a deny rule in ICS-Defender will log blocked traffic. Add a block rule on the WAN interface for traffic that would be considered normal and frequent. For example, create a rule that blocks traffic on the broadcast address of the WAN interface, otherwise all of the broadcast traffic on the WAN network may be logged by the firewall. Assuming 10.0.64.255 is the broadcast address of the WAN interface.

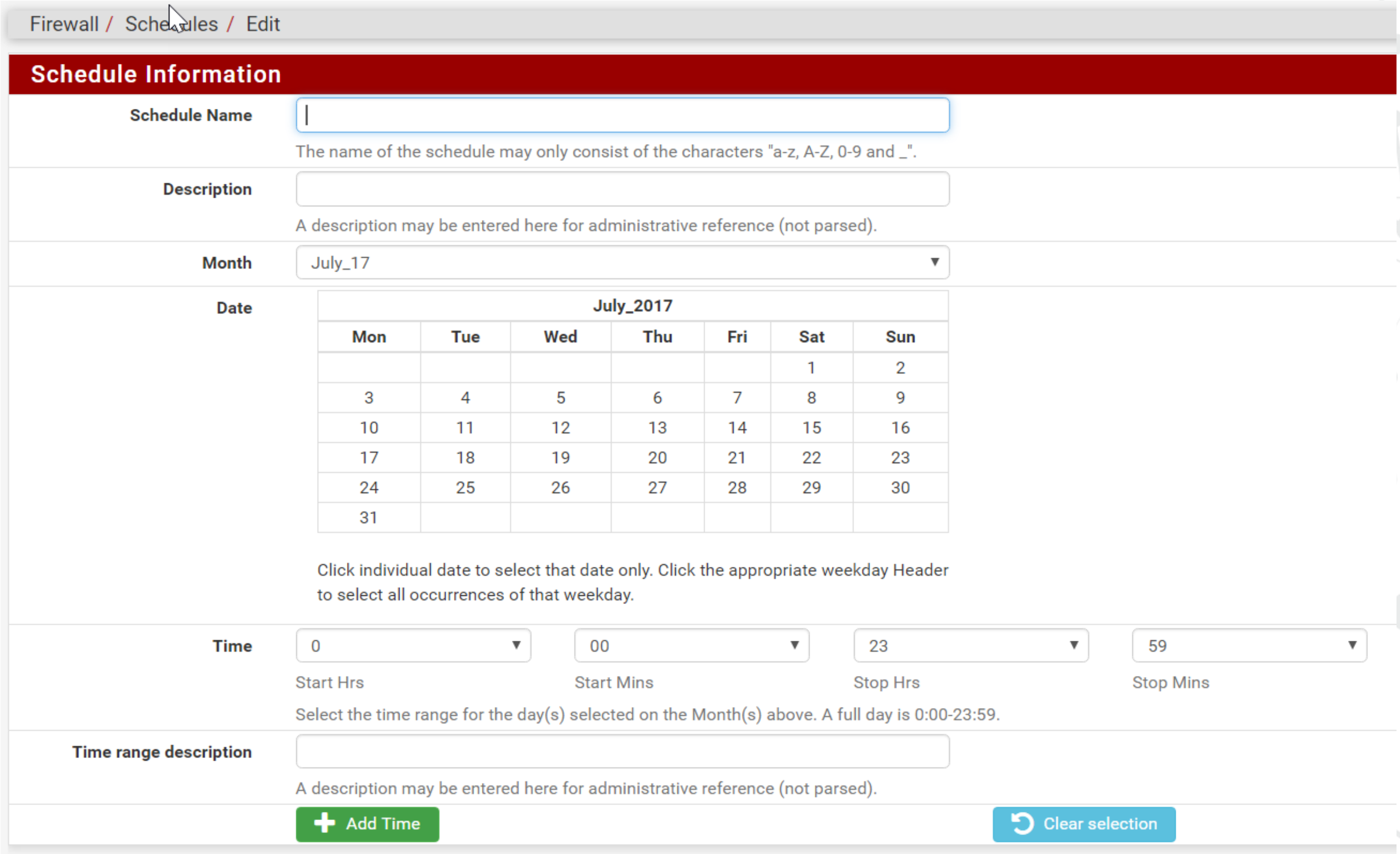


Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✖	0/0 B	IPv4 *	*	*	10.0.64.255	*	*	none		Don't log broadcast traffic on the WAN interface bro	

Schedules

Schedules can be created which are applied to rules causing that rule to only be active during the schedule window of time. Schedules can be created/edited by navigating to **Firewall→ Schedules**



Firewall / Schedules / Edit

Schedule Information

Schedule Name	The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	A description may be entered here for administrative reference (not parsed).
Month	July_17
Date	

July_2017

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time: Start Hrs 0, Start Mins 00, Stop Hrs 23, Stop Mins 59

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time range description

A description may be entered here for administrative reference (not parsed).

VLANS

Virtual LANs (VLANs) allow network administrators to subdivide a physical network into separate logical broadcast domains.

On a standard Layer 2 network, all hosts connected to a switch are members of the same broadcast domain; and broadcast domains can only be physically separated across different switches by routers.

As networks scale, it becomes necessary to introduce multiple broadcast domains to segment traffic for performance, security or logistics reasons. Without the use of VLANs, this would typically require each network segment to have its own separate switch infrastructure, with one or more routers managing communication between each switch segment.

A VLAN represents a broadcast domain. VLANs are identified by a VLAN ID (a number between 0 – 4095), with the default VLAN on any network being VLAN 1. Each port on a switch or router can be assigned to be a member of a VLAN (i.e., to allow receiving and sending traffic on that VLAN).

A guide to understanding Virtual LANS

VLAN Trunking

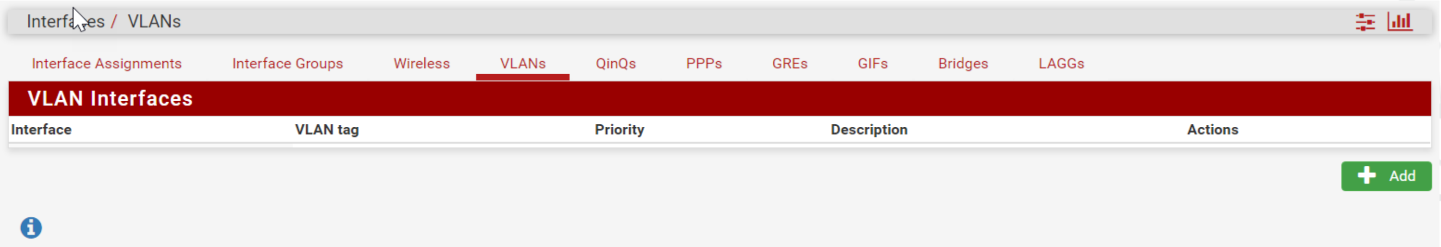
A trunk is a point-to-point link between two network devices that carries more than one VLAN. With VLAN trunking, you can extend your configured VLAN across the entire network.

Default VLAN1

Switches and networking devices that support VLANs generally default to VLAN 1 as the native VLAN. Because it's commonly the default in many devices, it's highly recommended that VLAN configurations do not use VLAN 1. There are many issues which can arise from using VLAN 1 so it's best to avoid it if possible.

Creating a VLAN

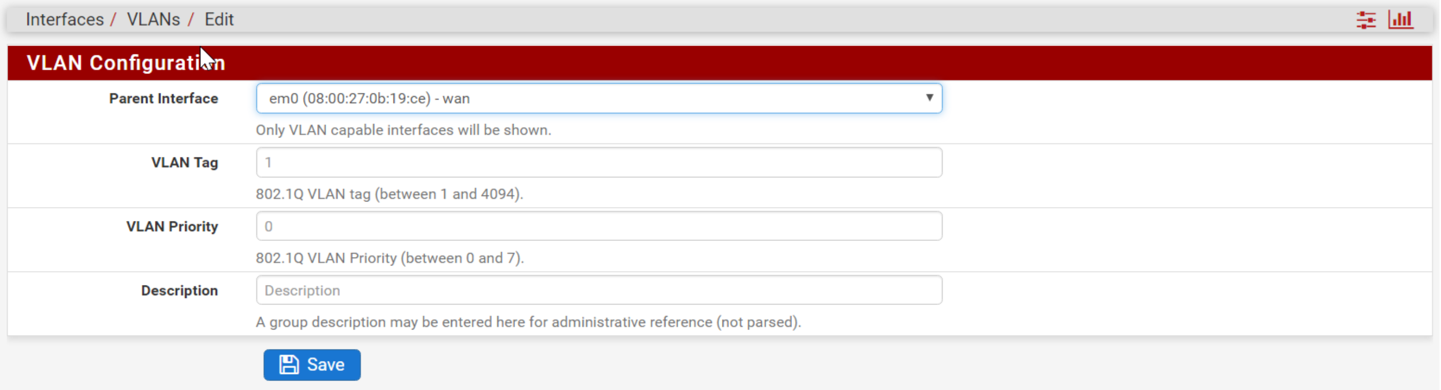
Navigate to **Interfaces→ Assign→VLAN Tab**.



VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions

Click ➕ Add to begin adding a VLAN.



VLAN Configuration

Parent Interface	em0 (08:00:27:0b:19:ce) - wan Only VLAN capable interfaces will be shown.
VLAN Tag	1 802.1Q VLAN tag (between 1 and 4094).
VLAN Priority	0 802.1Q VLAN Priority (between 0 and 7).
Description	Description A group description may be entered here for administrative reference (not parsed).

Parent Interface: The interface that the VLAN will be assigned to. This can be physical or virtual interfaces.

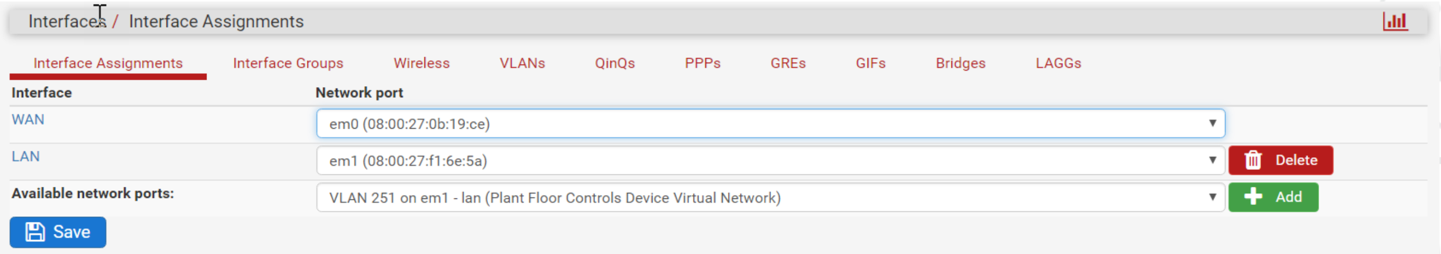
VLAN Tag: This is the VLAN ID which will be used to identify this virtual LAN. Avoid using VLAN 1.

VLAN Priority: Defaults to 0. These values can be used to prioritize traffic such as voice, video, controls etc. If unsure, the default value of zero should be used.

Description (Optional): A description of the VLAN for documentation and administrative purposes. For example, if this VLAN will be the virtual network to hold the plant floor controls traffic, a description of "Plant Floor Controls Device Virtual Network" may be useful.

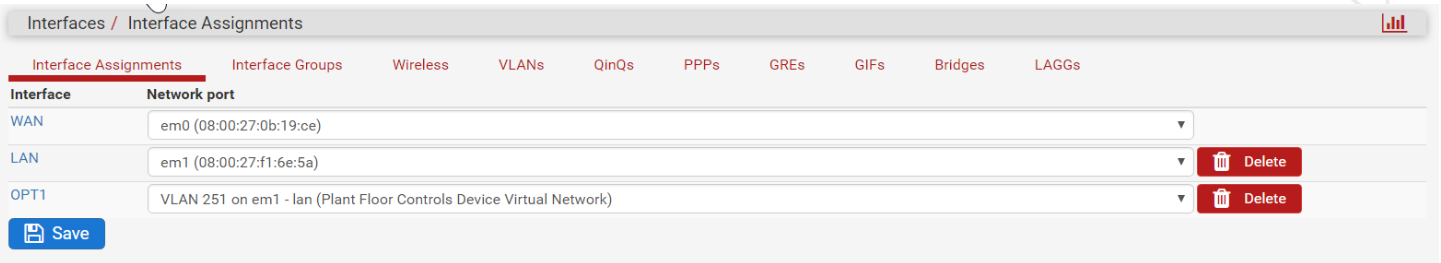
Creating an Interface with the new VLAN

Returning to the Interface Assignments Tab, the newly created VLAN is available for use but has not been assigned an interface name.



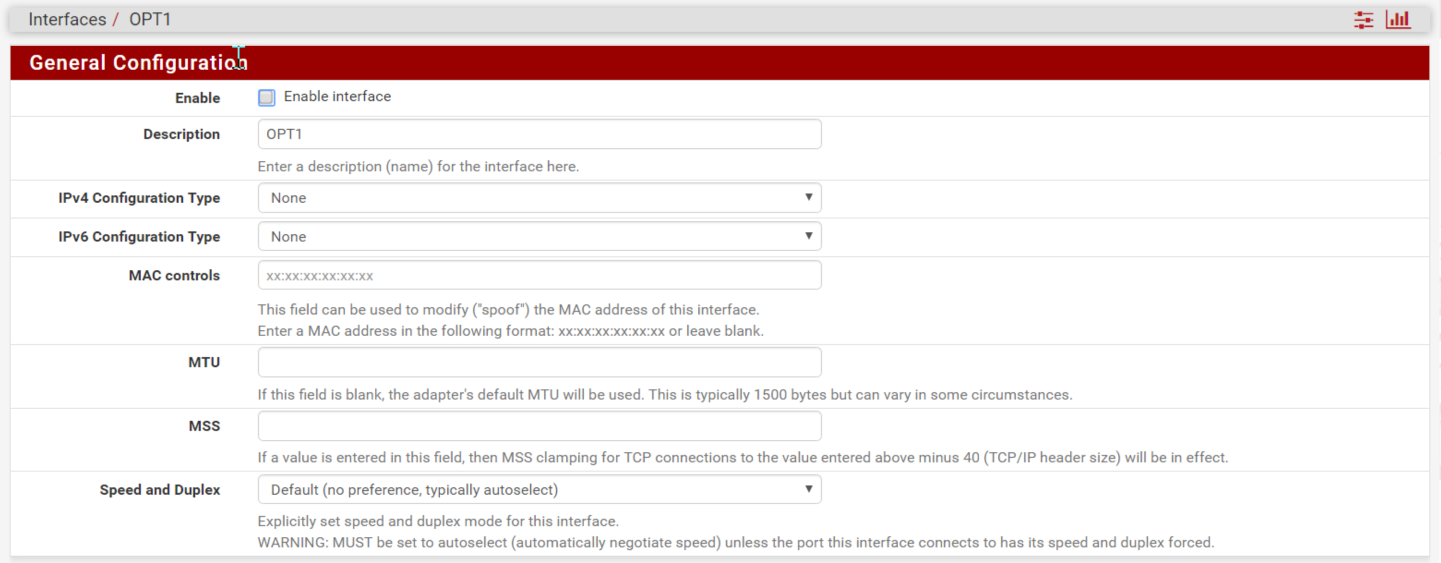
Interface	Network port
WAN	em0 (08:00:27:0b:19:ce)
LAN	em1 (08:00:27:f1:6e:5a)
Available network ports:	VLAN 251 on em1 - lan (Plant Floor Controls Device Virtual Network)

Click ➕ Add to create a usable interface with VLAN 251.



Interface	Network port
WAN	em0 (08:00:27:0b:19:ce)
LAN	em1 (08:00:27:f1:6e:5a)
OPT1	VLAN 251 on em1 - lan (Plant Floor Controls Device Virtual Network)

OPT1 is now available on physical NIC em1, participating in Virtual LAN 251, and can be configured as an interface in ICS-Defender.



General Configuration

Enable	□ Enable interface
Description	OPT1 Enter a description (name) for the interface here.
IPv4 Configuration Type	None
IPv6 Configuration Type	None
MAC controls	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 (TCP/IP 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.

Double Tagged/Stacked VLANS (IEEE 802.1ad)

For any needs regarding this feature-set, please contact Dynics.

Virtual Private Networks (VPN)

ICS-Defender Pro supports SSL, IPsec, and L2TP. There are several uses for VPN functionality as described in the following sections.

Line to Line Connectivity (Site to Site)

Connecting one manufacturing area or line to another when a dedicated always on connection is required. Often, situations arise where data needs to be exchanged between two or more manufacturing systems and sending raw controls or plant floor traffic through typical IT networks isn't desired for both reasons of management and security.

ICS-Defender allows this type of connectivity greatly improving upon the security and reliability of the data being moved. This approach also precludes the need to physically, directly connect large controls systems together which would yield issues with network size and reliability.

Remote Access

Remote access for users and applications to securely connect to a manufacturing system. This allows remote troubleshooting and access by associates and potentially suppliers. **See the section on Captive Portal for supplier access control.**

Unattended Applications

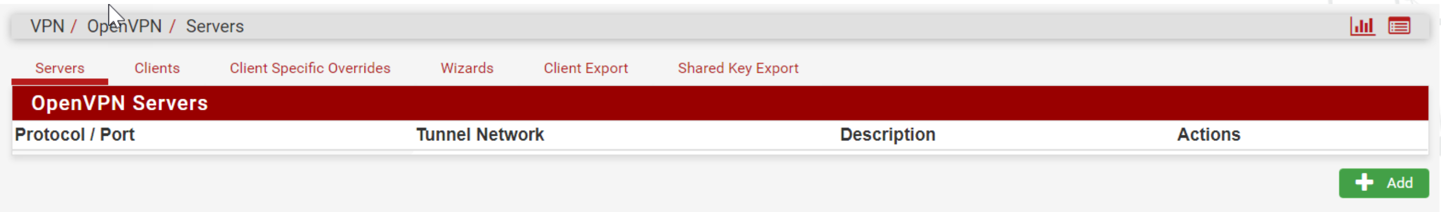
Separation of PC assets from controls networks prevents malware and other attacks from being introduced to more vulnerable control systems. Applications residing on a PC outside of the control system can securely access only those PLCs or devices to which they are expressly required to access.

SSL VPN

OpenVPN, the SSL VPN supported by ICS-Defender, can connect a site to site tunnel to either an IPv4 address or an IPv6 address and both traffic types may be passed inside the SSL VPN tunnel simultaneously.

Manual SSL VPN Server Creation

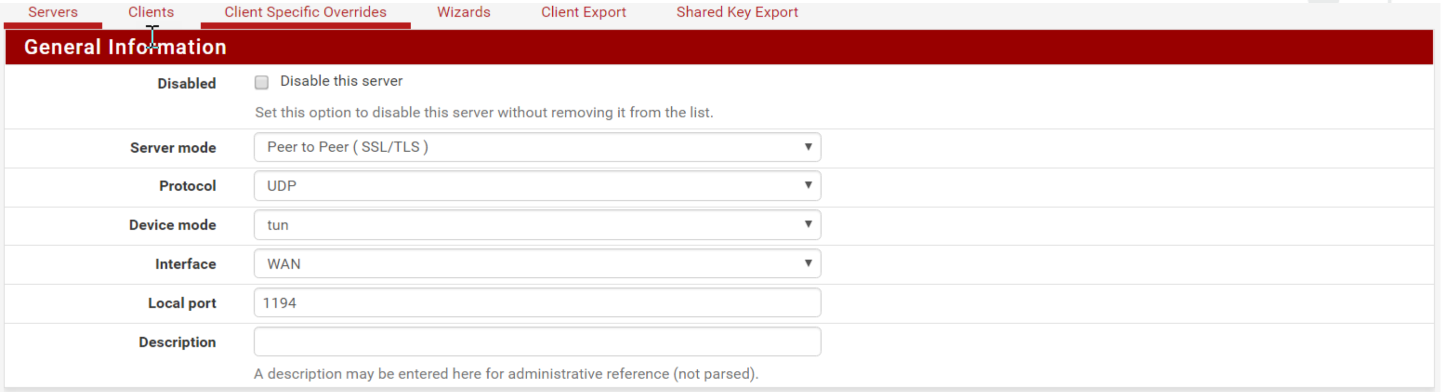
It's recommended to use the VPN Wizard to create a VPN. To manually create, or edit, navigate to **VPN→ Open VPN→ Server Tag** to create a VPN Server.



OpenVPN Servers

Protocol / Port	Tunnel Network	Description	Actions

Click Add to create a VPN Server



General Information

Disabled	□ Disable this server Set this option to disable this server without removing it from the list.
Server mode	Peer to Peer (SSL/TLS)
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	1194
Description	 A description may be entered here for administrative reference (not parsed).

Disabled: Enables or disabled the VPN Server.

Server Mode:

- Peer to Peer (SSL/TLS) – A connection between local and remote networks secured by SSL/TLS. This method offers increased security and the ability to push configuration commands to clients.
- Peer to Peer (Shared Key) – A connection between local and remote networks that is secured by a single Shared Key, configured on both nodes.
- Remote Access (SSL/TLS) – A mobile client setup with per-user X.509 certificates. Similar to peer-to-peer SSL/TLS connections, this method offers increased security and the ability to push configuration commands to clients.
- Remote Access (User Auth.) – A client access server that does not use certificates, however, does require the end user to supply a username and password when connecting. This is not recommended unless authentication is handled externally by LDAP or RADIUS.
- Remote Access (SSL/TLS + User Auth.) – ***The most secure and recommended method***. This method uses SSL/TLS and requires username and password when connecting. Client access can be disabled by revoking the certificate as well as changing the password. It is unlikely that an attacker would have both the compromised security key as well as the username and password.

Protocol: TCP or UDP for IPv4 or IPv6 can be selected. An OpenVPN server instance can bind to IPv4 or IPv6, but not both simultaneously. UDP, a connectionless protocol, is the fastest and the most reliable. It is the recommended method.

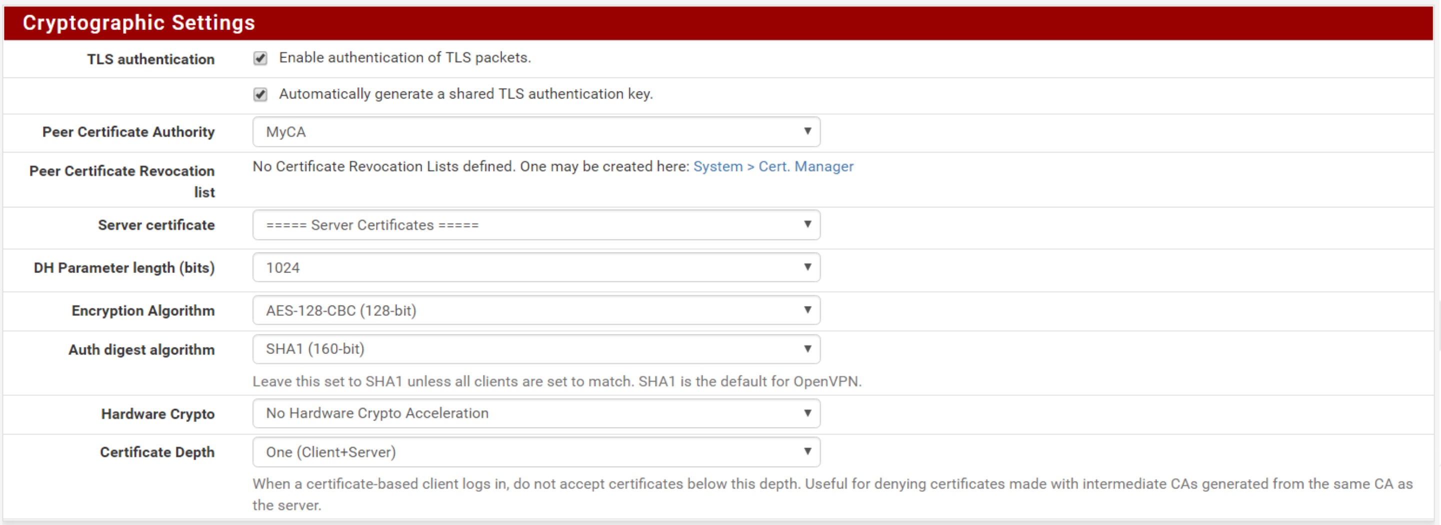
Device Mode: OpenVPN operates with one of two different modes:

- **tun**: Operates on OSI Layer 3 and performs routing on point-to-point basis. **tun** is more stable and more widely supported. In addition, Android and iOS only support **tun** mode unless the device is rooted or jailbroken.
- **tap**: Operates on OSI Layer 2 and performs both routing and bridging as needed.

Interface: The interface, physical or virtual, virtual IP or failover group that the OpenVPN server will listen on for incoming connections. The selected interface is also where traffic from the server will exit. Generally, the WAN interface is used.

Local Port: The local port is the port number that the OpenVPN server will listen on at the selected interface. Firewall rules must allow traffic to this port and it is specified in the client configuration. Each server must have unique port on each interface.

Description: A description for the VPN server. For example, "Asset Management VPN Server".



Cryptographic Settings

TLS authentication	☑ Enable authentication of TLS packets.
	☑ Automatically generate a shared TLS authentication key.
Peer Certificate Authority	MyCA ▾
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
Server certificate	===== Server Certificates ===== ▾
DH Parameter length (bits)	1024 ▾
Encryption Algorithm	AES-128-CBC (128-bit) ▾
Auth digest algorithm	SHA1 (160-bit) ▾ Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	No Hardware Crypto Acceleration ▾
Certificate Depth	One (Client+Server) ▾ When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

TLS Authentication: Checking the box enables authentication of TLS packets. If there is an existing TLS key, disable "automatically generate a shared TLS authentication key". If a key already exists, paste it into the box that appears when unchecking auto-generation.

Peer Certificate Authority: A certificate authority is required. Select the appropriate certificate authority, if none have been created or assigned, it must be done prior to setting this option.

Peer Certificate Revocation List: The certificate revocation list used by this tunnel.

Server Certificate: Each OpenVPN server instance requires a server certificate. If none are present in this list, refer to User and Server Certificates to create one.

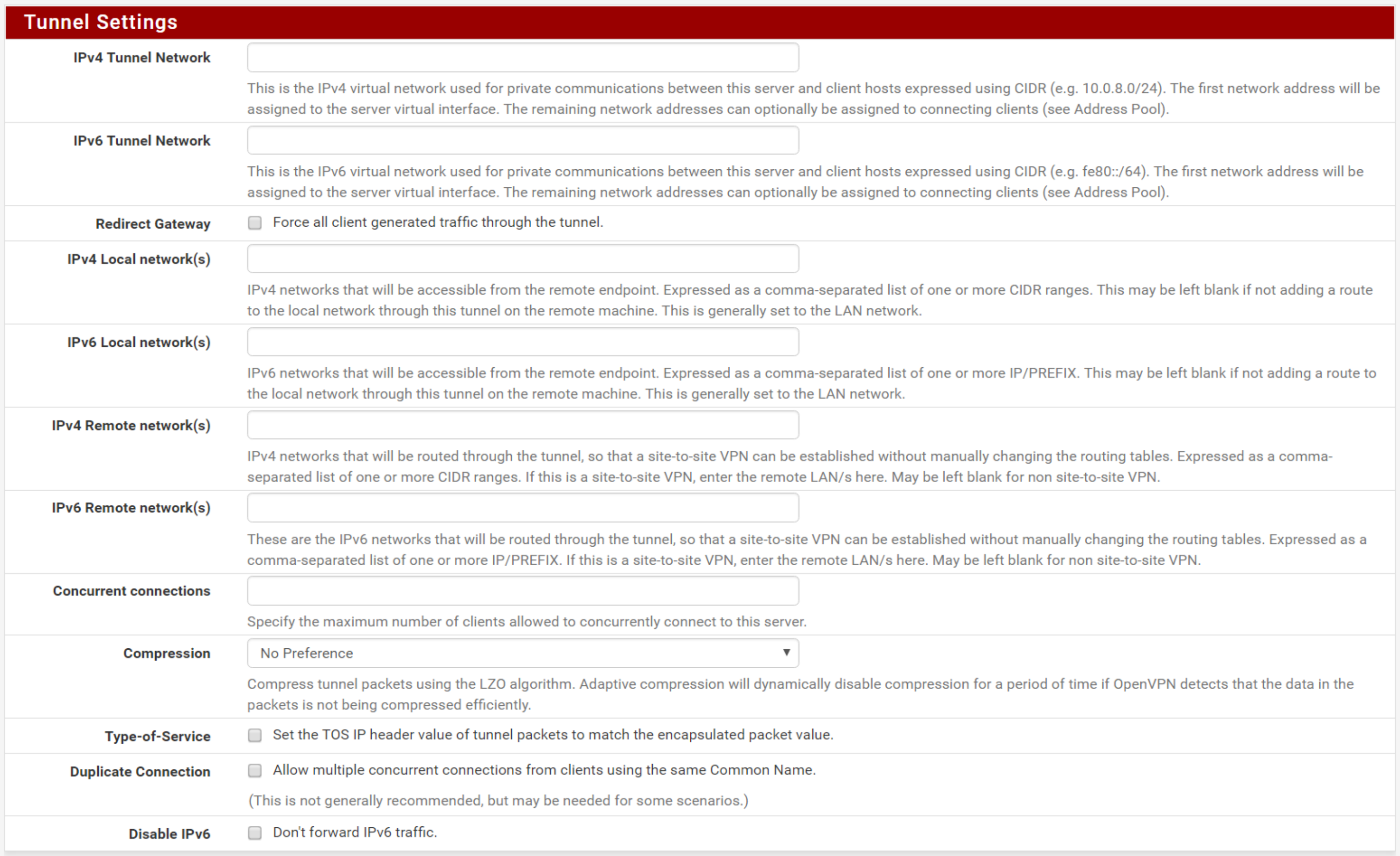
DH Parameter Length (bits): Used in establishing a secure communications channel. Generally, there is no reason to change this from the default settings.

Encryption Algorithm: The encryption algorithm used for this connection. Generally, there is no reason to change from the default.

Auth. Digest Algorithm: OpenVPN defaults to SHA1. Do not change this setting without reason.

Hardware Crytpo: If available, a hardware cryptography engine can be selected.

Certificate Depth: This option limits the length of a certificate chain before it fails validation. The default value is One (Client + Server) which in the event an unauthorized intermediate CA is generated by an attacker, certificates signed by the rogue intermediate would fail validation. Generally, there is no reason to change from the default.



Tunnel Settings

IPv4 Tunnel Network	This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).
IPv6 Tunnel Network	This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).
Redirect Gateway	□ Force all client generated traffic through the tunnel.
IPv4 Local network(s)	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local network(s)	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv4 Remote network(s)	IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.
IPv6 Remote network(s)	These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.
Concurrent connections	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	No Preference ▾ Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	□ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Duplicate Connection	□ Allow multiple concurrent connections from clients using the same Common Name. (This is not generally recommended, but may be needed for some scenarios.)
Disable IPv6	□ Don't forward IPv6 traffic.

IPv4 Tunnel Network: Pool of addresses which are assigned to clients upon connection. The server will use the first address of the pool for internal use and subsequent addresses in the pool are assigned to clients that connect. These addresses are used for communication between tunnel endpoints. Any subnet can be used provided that the subnet is not in use locally or at the remote site.

IPv6 Tunnel Network: See IPv4 Tunnel Network above.

Redirect Gateway: When this option is selected, the server will push a message to clients instructing them to forward all traffic over the VPN tunnel.

IPv4 Local Networks: Specifies which local networks are reachable by VPN clients. A route for these networks is pushed to clients connecting to this server. If multiple routes for subnets are needed, enter the subnets separated by a comma. Example: 192.168.2.0/24, 192.168.56.0/24.

IPv6 Local Networks: See IPv4 Local Networks above.

IPv4 Remote Networks: This option applies to Peer-to-Peer connections. When subnets are specified in this field, routes are added to the firewall. The routes point traffic destined for these networks to the other end of the OpenVPN tunnel. If more than one remote network subnet is needed, enter the subnets separated by a comma. Example: 192.168.2.0/24, 192.168.56.0/24.

IPv6 Remote Networks: See IPv4 Remote Networks above.

Concurrent Connections: The maximum number of clients that may simultaneously connect to the OpenVPN Server.

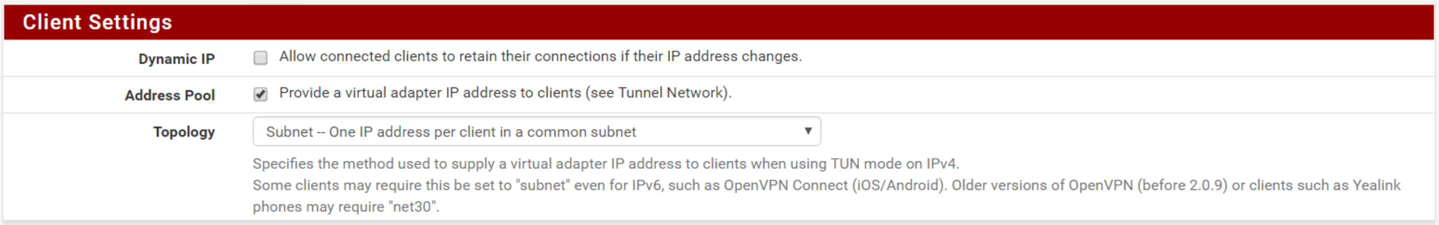
Compression: When compressions is enabled, any traffic crossing the VPN tunnel will be compressed prior to being encrypted. Compression decreases bandwidth utilization for many types of traffic. This improvement will cause increased CPU usage on both the server and client side though the impact is general minimal.

- No Preference – Omits compression directives from the OpenVPN configuration meaning no compression will be performed.
- Disabled – Explicitly disabled compression.
- Enabled with Adaptive Compression – Enabled compression with a periodic test to verify that the traffic is capable of being compressed. If compression is not optimal, compress is disabled until the next successful test. This option offers the best balance as it will compress when advantageous to do so and no compress when it makes no sense to do so.
- Enabled without Adaptive Compression – Explicitly enable compression at all times.

Type-of-Service: When enabled, OpenVPN will set the TOS IP header value of tunnel packets to match the encapsulated packet value. This may assist high priority or important traffic to be handled faster through the tunnel. A common example is VoIP or video traffic.

Duplicate Connection: A default behavior of OpenVPN is to associate an IP address from its tunnel network with a certificate or username for a given session. If the same certificate connects again, it is assigned the same IP address and either disconnect the first client session or cause an IP conflict between the two client connections. The purpose behind this is to prevent the same certificate being used by multiple clients simultaneously. It is recommended to use a unique certificate each connection client. If multiple clients will use the same certificate, enable duplicate connections.

Disable IPv6: When checked, IPv6 traffic forwarding is disabled.



Client Settings

Dynamic IP ☐ Allow connected clients to retain their connections if their IP address changes.

Address Pool ☑ Provide a virtual adapter IP address to clients (see Tunnel Network).

Topology: Subnet -- One IP address per client in a common subnet

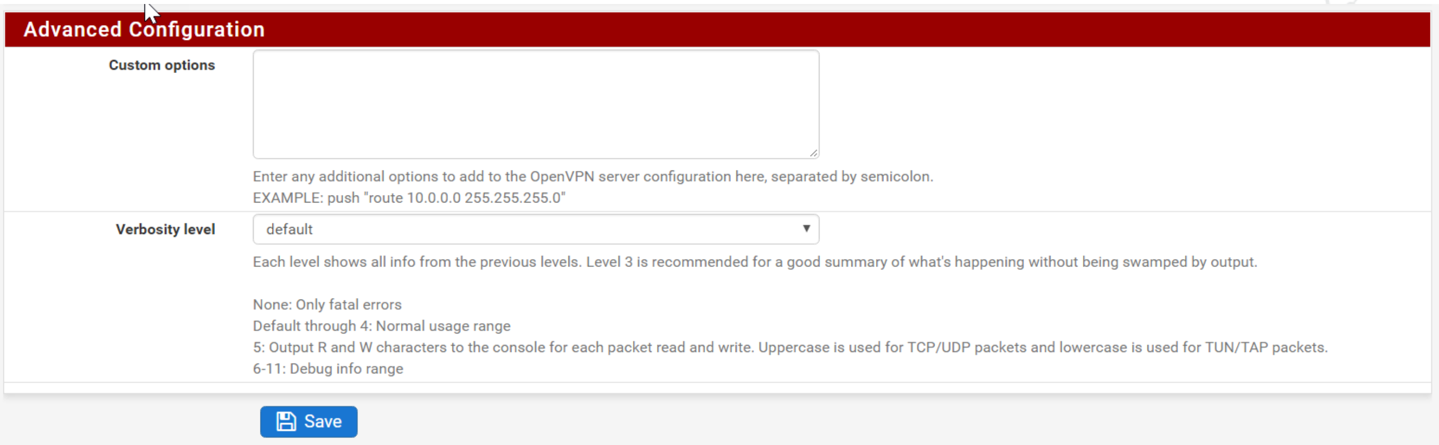
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Dynamic IP: Checking this option allows OpenVPN clients retain their connection if their IP address changes.

Address Pool: When enabled, the VPN server will assign virtual adapter IP addresses to clients from the subnet specified in the Tunnel Network option. When unchecked, clients will have to set their own static IP addresses manually in their client configuration files. This option should remain checked except for very rare cases.

Topology: By default, OpenVPN utilizes a topology style of subnet when Device Mode is set to “tun”. In this manner, there is only one IP address per client as opposed to an isolated subnet per client. This is the only available method when using the “tap” Device Mode. If the older style net30 topology for “tun” is selected, OpenVPN allocates a /30 CIDR network which consists of four IP addresses, two of which are usable, to each connecting client.

Note: The default is subnet because the net30 style has been deprecated by the OpenVPN project indicating it will be removed at some point in the future.



Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Verbosity level: default

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

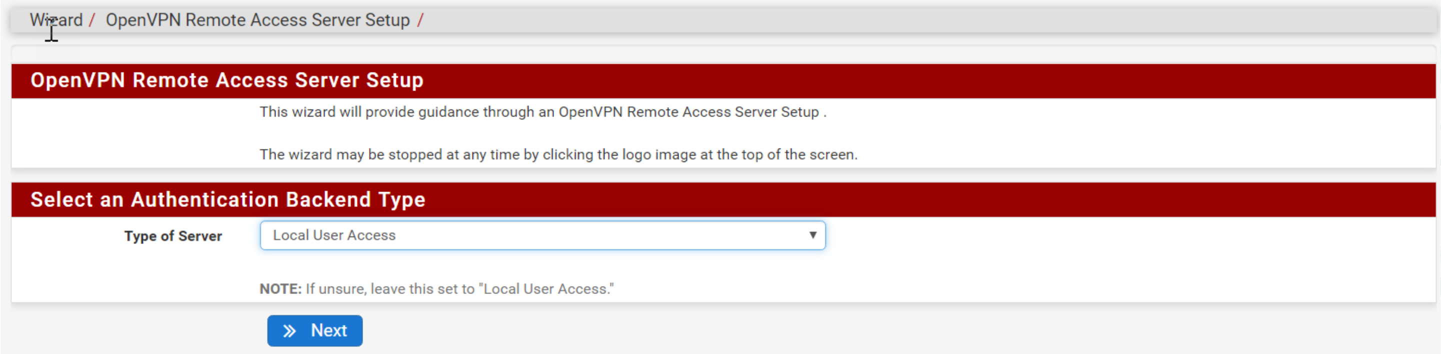
Custom Options: The ICS-Defender WebGUI allows configuration and control of most OpenVPN features, however, there are several options that are unavailable in the WebGUI. This box allows an unlimited use of custom configuration options for this VPN server.

A comprehensive list is beyond the scope of this document but the available options can be found at the OpenVPN documentation site. Care should be taken when using custom options as there is no validation of the options to ensure they are correct. If an incorrect option is entered, the OpenVPN client or server may not start. Review the logs at **Status→System Logs→OpenVPN** to look for error message such as “Options Error: Unrecognized or missing parameters”

Verbosity Level: Sets the level of verbosity used in the logs captured by ICS-Defender for this VPN server.

SSL VPN Remote Access Server Wizard (Recommended)

Navigate to VPN→OpenVPN→Wizards Tab to start the wizard. This wizard is specific to **Remote Access** functionality and will also create client specific overrides/settings used in remote access configurations.



OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

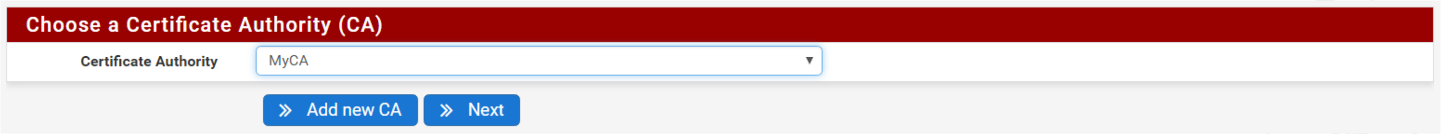
Select an Authentication Backend Type

Type of Server: Local User Access

NOTE: If unsure, leave this set to "Local User Access."

Type of Server: Local User access, LDAP, or RADIUS. For this example, Local User Access is used.

After selecting the type of server, click » Next to continue.

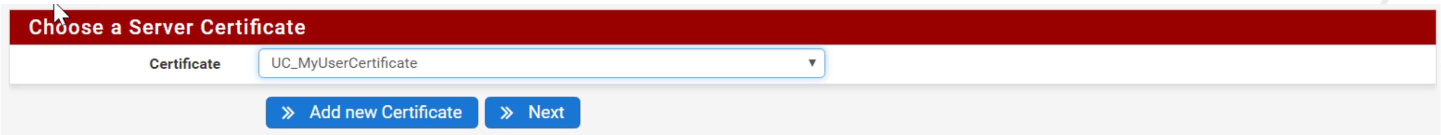


Choose a Certificate Authority (CA)

Certificate Authority: MyCA

Certificate Authority: Choose a certificate authority from the available list or add a new certificate authority. Creating a certificate authority is covered here.

After adding or selecting an existing CA, click » Next to continue.

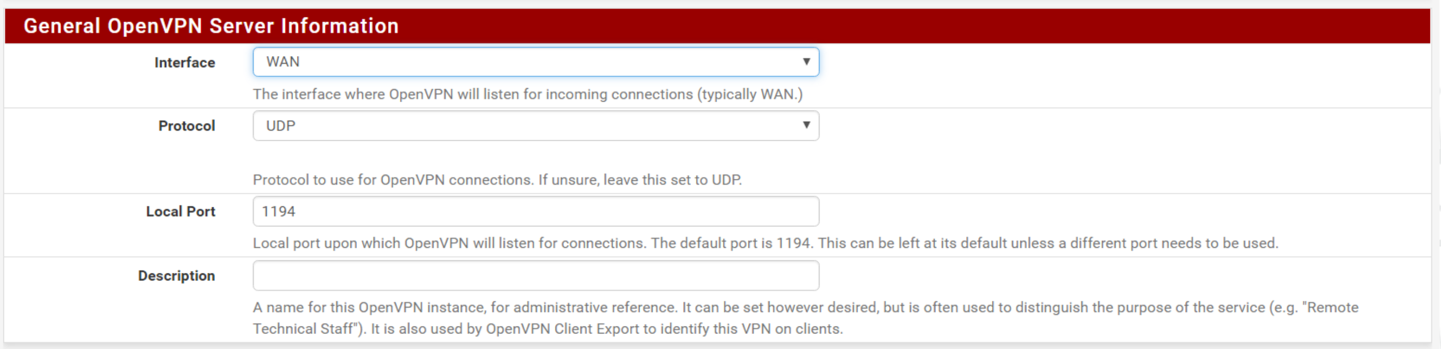


Choose a Server Certificate

Certificate: UC_MyUserCertificate

Certificate: Select or add a server certificate. Adding server certificates is discussed here.

After adding or selecting an existing server certificate, click » Next to continue to the next screen of the wizard.



General OpenVPN Server Information

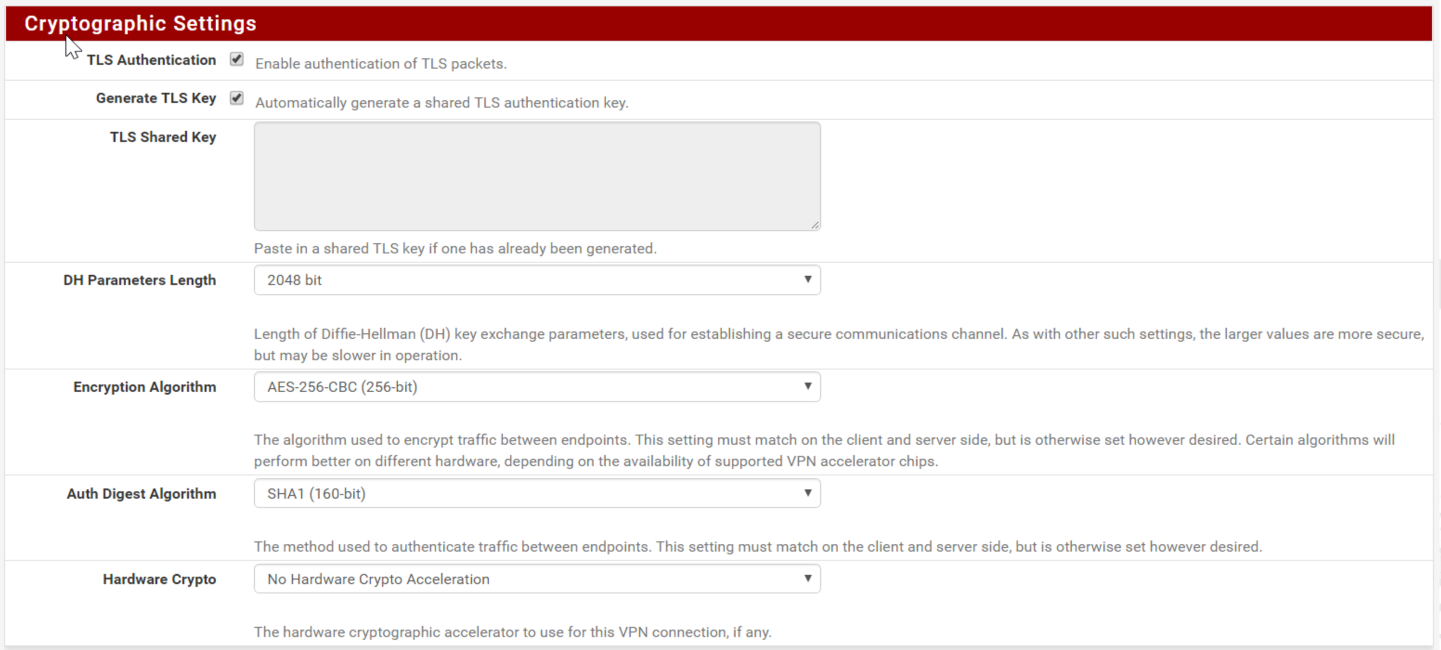
Interface	WAN ▾ The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	UDP ▾ Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	 A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Interface: Select the interface that the VPN Server will be available on.

Protocol: Select the protocol that the VPN Server will utilize.

Local Port: This is the port on ICS-Defender that will be used to listen for incoming connections/vpn traffic.

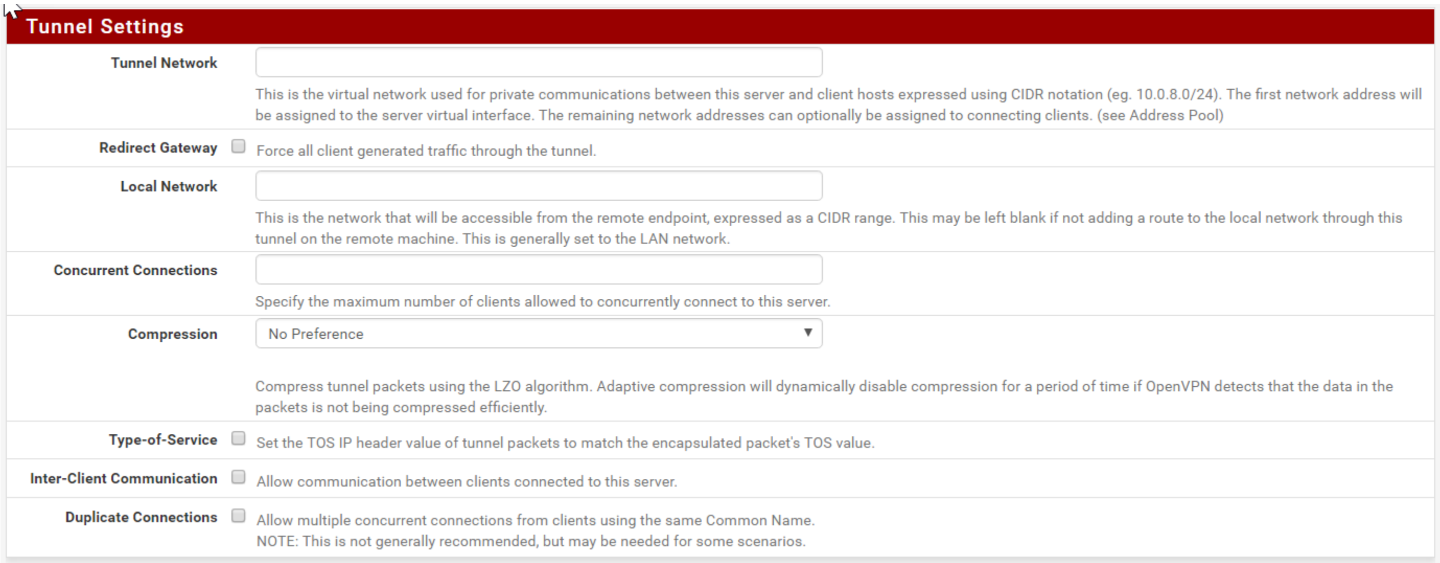
Description: An optional description used to describe the use of the VPN Sever. For example, “Asset Management VPN Server”



Cryptographic Settings

TLS Authentication	☑ Enable authentication of TLS packets.
Generate TLS Key	☑ Automatically generate a shared TLS authentication key.
TLS Shared Key	 Paste in a shared TLS key if one has already been generated.
DH Parameters Length	2048 bit ▾ Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.
Encryption Algorithm	AES-256-CBC (256-bit) ▾ The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.
Auth Digest Algorithm	SHA1 (160-bit) ▾ The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	No Hardware Crypto Acceleration ▾ The hardware cryptographic accelerator to use for this VPN connection, if any.

No changes are necessary to Cryptographic settings. For any needs regarding this feature-set, please contact Dynics.



Tunnel Settings

Tunnel Network	This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway	□ Force all client generated traffic through the tunnel.
Local Network	This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	No Preference ▼ Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	□ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	□ Allow communication between clients connected to this server.
Duplicate Connections	□ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

Tunnel Network: ICS-Defender uses an internal network for communications between a VPN connection and the local network. This network is not generally accessible outside of ICS-Defender and should not use addresses assigned to any interface.

Example: If the WAN interface is 10.0.5.1 and the LAN interface is 192.168.200.1, an entry of 172.19.0.0/24 would provide a tunnel network of 255 addresses.

**Note that the IP address range ends in a zero.*

Redirect Gateway: No change is necessary.

Local Network: The local network is the network on the LAN interface that is to be reached from the VPN Connection when initiated. For example, if PLCs on the LAN are at 192.168.200.12 and 192.168.200.21, with a subnet mask of /24 (255.255.255.0), then the local network should be set to 192.168.200.0/24.

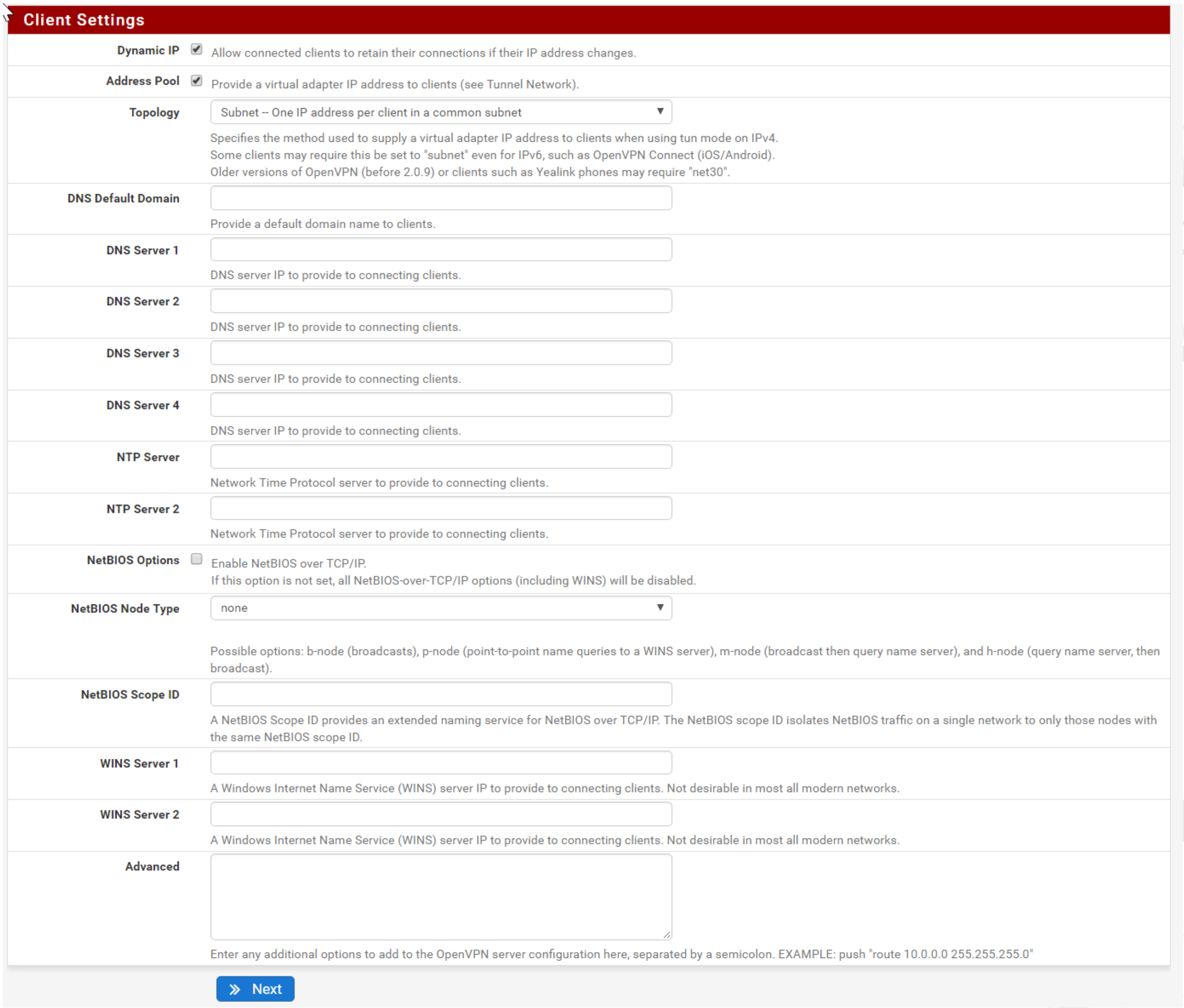
**Note that the IP address range ends in a zero.*

Concurrent Connections: This value determines how many concurrent VPN connections the server will allow. It is recommended to set this number to a value which represents what expected connections will be.

Type of Service: No change is necessary to this default setting of unchecked.

Inter-Client Communication: No change is necessary to this default setting of unchecked.

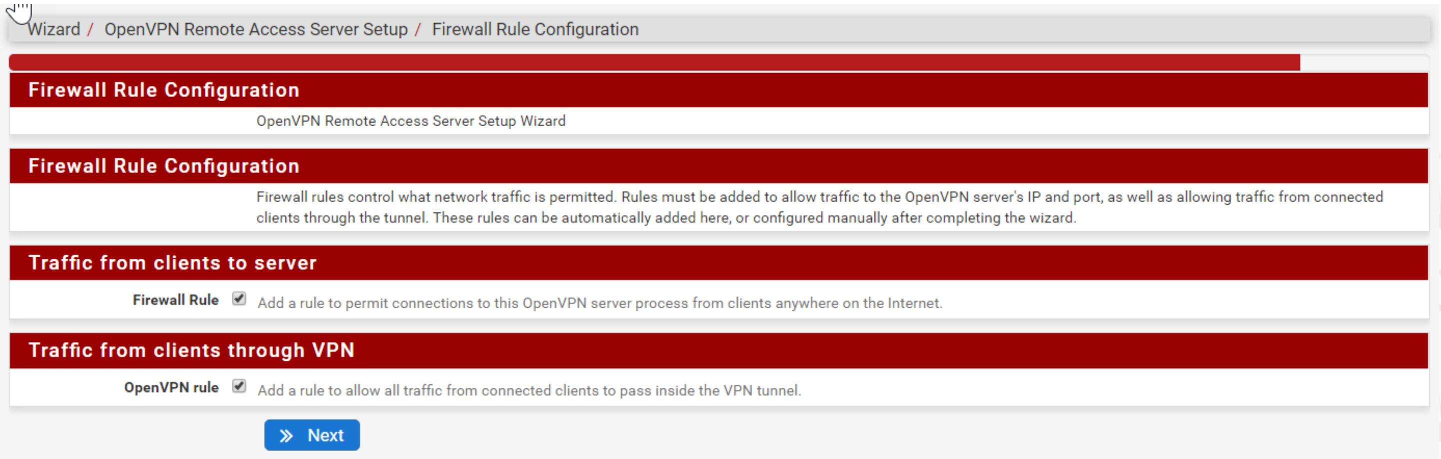
Duplicate Connections: If multiple clients will connect using the same user/client certificate then this setting must be enabled/checked. Using the same certificate for different originating connections (PCs) is not recommended from a security perspective.



Client Settings

Dynamic IP	☑ Allow connected clients to retain their connections if their IP address changes.
Address Pool	☑ Provide a virtual adapter IP address to clients (see Tunnel Network).
Topology	Subnet -- One IP address per client in a common subnet ▼ Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
DNS Default Domain	Provide a default domain name to clients.
DNS Server 1	DNS server IP to provide to connecting clients.
DNS Server 2	DNS server IP to provide to connecting clients.
DNS Server 3	DNS server IP to provide to connecting clients.
DNS Server 4	DNS server IP to provide to connecting clients.
NTP Server	Network Time Protocol server to provide to connecting clients.
NTP Server 2	Network Time Protocol server to provide to connecting clients.
NetBIOS Options	□ Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	none ▼ Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced	Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"

All Settings under Client Settings: No changes are necessary to the default settings unless specific functionality is required and the reason for making the change is understood.


Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

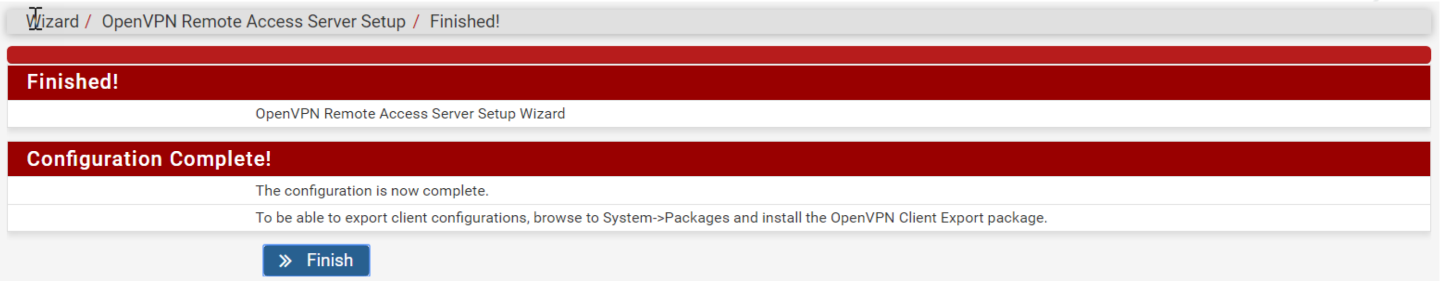
Traffic from clients to server

Firewall Rule ☑ Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule ☑ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

To have the VPN wizard create the necessary firewall rules to allow VPN connections to the VPN server and throug h ICS-Defender to the target LAN network, check both boxes and click “Next”.



Finished!

OpenVPN Remote Access Server Setup Wizard

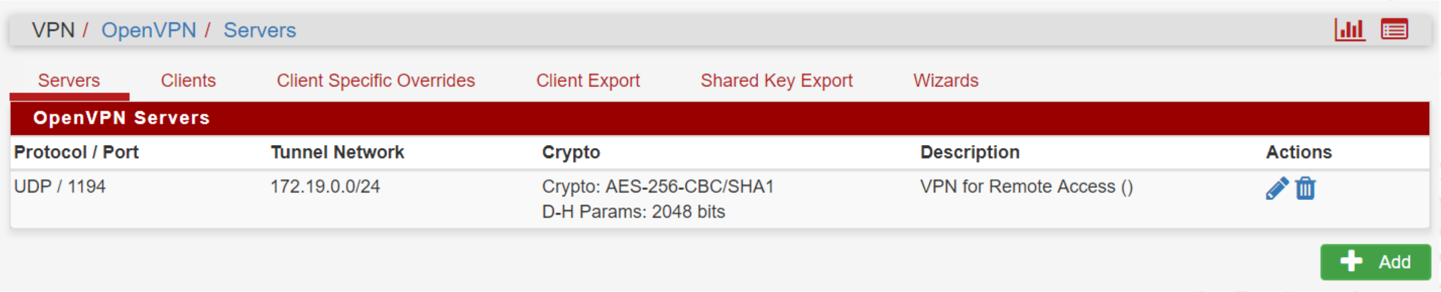
Configuration Complete!

The configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

Click “Finish” to exit the wizard.

The newly created OpenVPN Server is listed under **VPN→OpenVPN→Servers**.



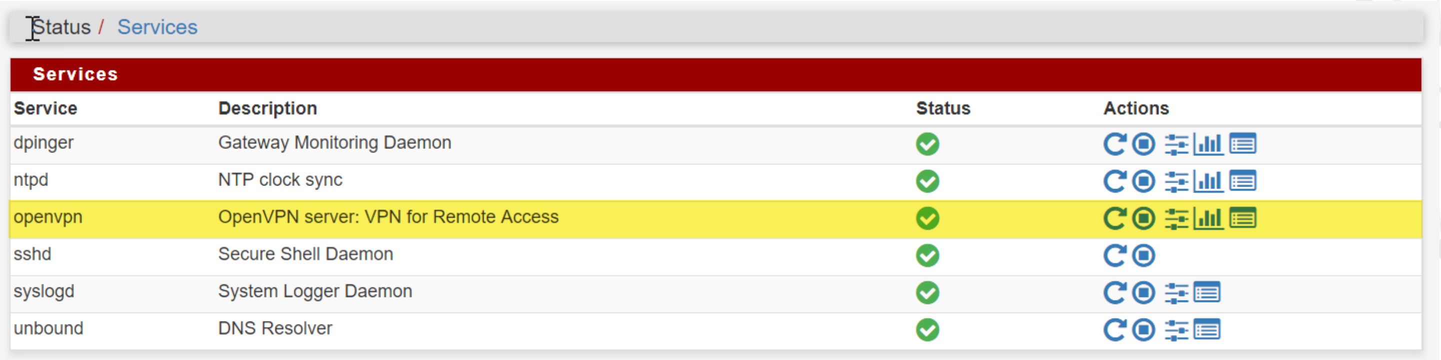
OpenVPN Servers

Protocol / Port	Tunnel Network	Crypto	Description	Actions
UDP / 1194	172.19.0.0/24	Crypto: AES-256-CBC/SHA1 D-H Params: 2048 bits	VPN for Remote Access ()	✎ 🗑

Verify OpenVPN Service

Navigate to **Status→ Services** and verify that the OpenVPN service is running. If not, check Status→System Logs→OpenVPN for entries describing the issue preventing the service from starting.

Running

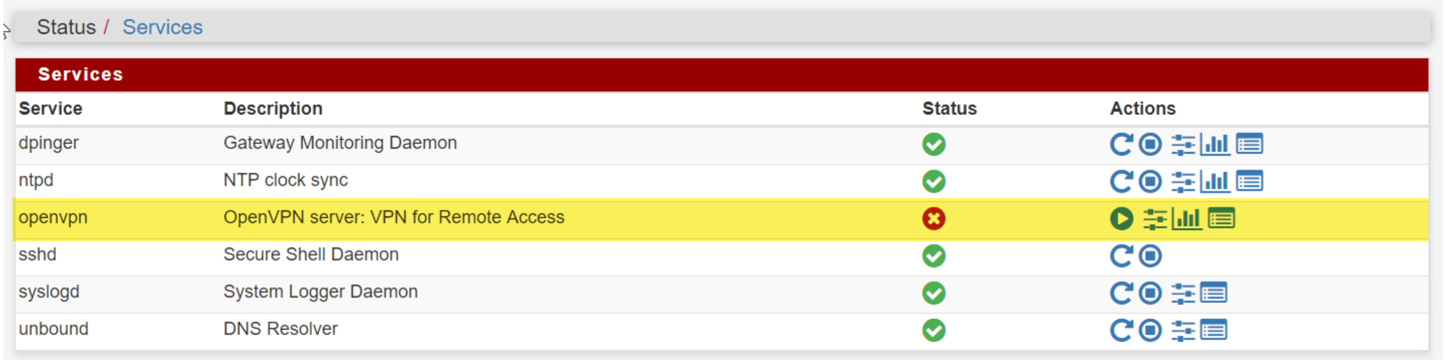


Status / Services

Services

Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	↻ ◉ ☰ 📊 ▤
ntpd	NTP clock sync	✓	↻ ◉ ☰ 📊 ▤
openvpn	OpenVPN server: VPN for Remote Access	✓	↻ ◉ ☰ 📊 ▤
sshd	Secure Shell Daemon	✓	↻ ◉
syslogd	System Logger Daemon	✓	↻ ◉ ☰ ▤
unbound	DNS Resolver	✓	↻ ◉ ☰ ▤

Issue / Not Running

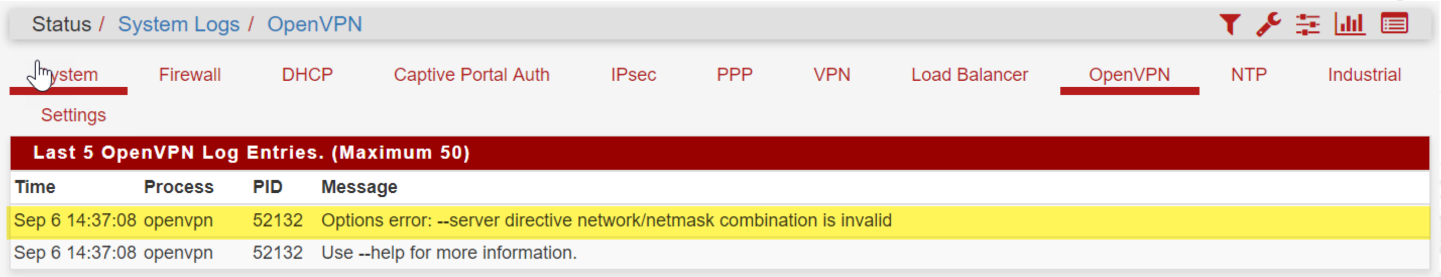


Status / Services

Services

Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	↻ ◉ ☰ 📊 ▤
ntpd	NTP clock sync	✓	↻ ◉ ☰ 📊 ▤
openvpn	OpenVPN server: VPN for Remote Access	✗	▶ ☰ 📊 ▤
sshd	Secure Shell Daemon	✓	↻ ◉
syslogd	System Logger Daemon	✓	↻ ◉ ☰ ▤
unbound	DNS Resolver	✓	↻ ◉ ☰ ▤

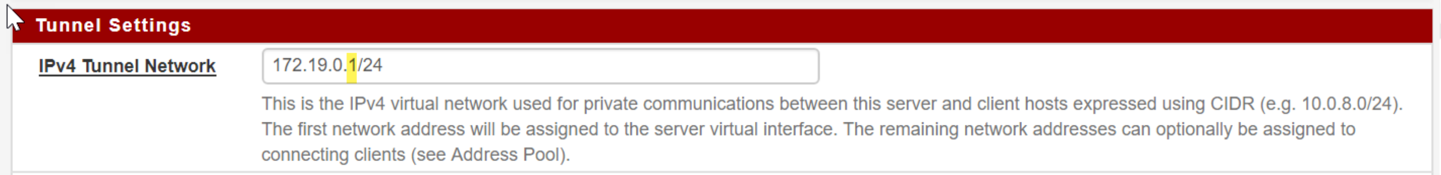
A log entry indicates an error in the OpenVPN Configuration.



Last 5 OpenVPN Log Entries. (Maximum 50)

Time	Process	PID	Message
Sep 6 14:37:08	openvpn	52132	Options error: --server directive network/netmask combination is invalid
Sep 6 14:37:08	openvpn	52132	Use --help for more information.

In this case, and it's a common error, in the OpenVPN server configuration, the tunnel network configuration doesn't end in a 0. The correct value should be 172.19.0.0/24.



Tunnel Settings

IPv4 Tunnel Network: 172.19.0.1/24

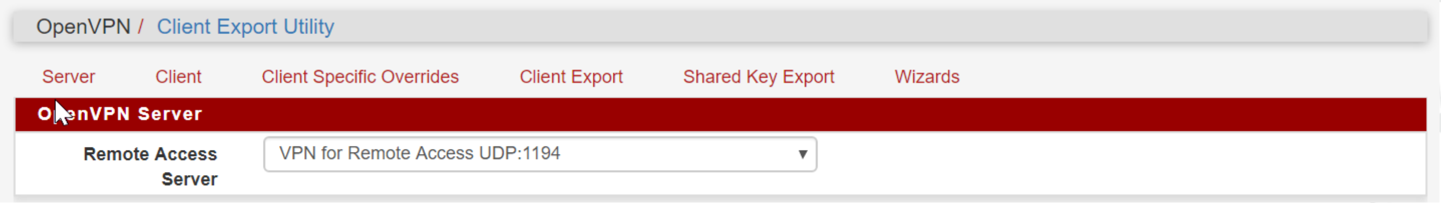
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).

Exporting VPN Configurations and OpenVPN Client Software

Once a VPN Server has been created, both the certificate, OpenVPN configuration, and OpenVPN client can be exported from ICS-Defender. Navigate to **VPN→OpenVPN→Client Export Utility**.

None of the default settings need to be changed for full functionality. Changes should only be made to the settings on the Client Export page by knowledgeable users.

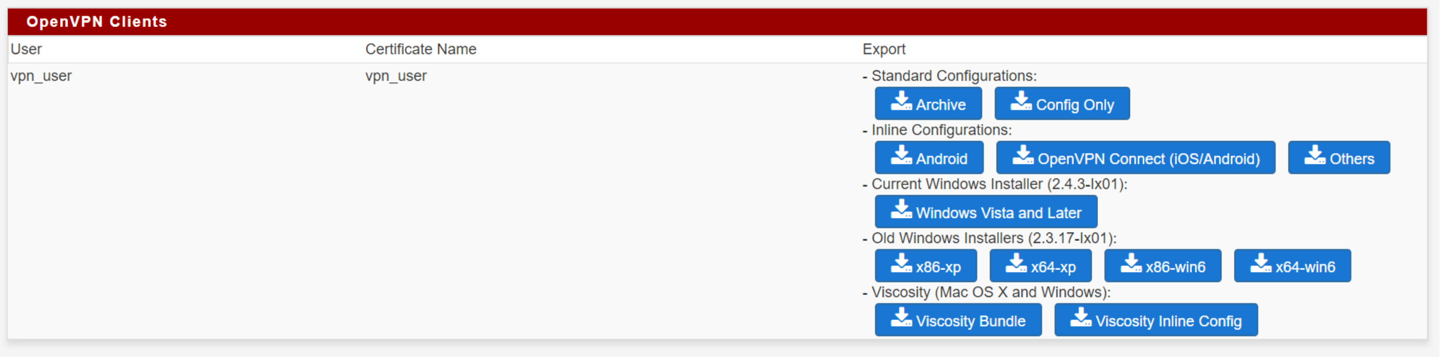
Select the VPN for which to export a configuration.



OpenVPN Server

Remote Access Server: VPN for Remote Access UDP:1194

Scroll down the page to the OpenVPN Clients.



OpenVPN Clients

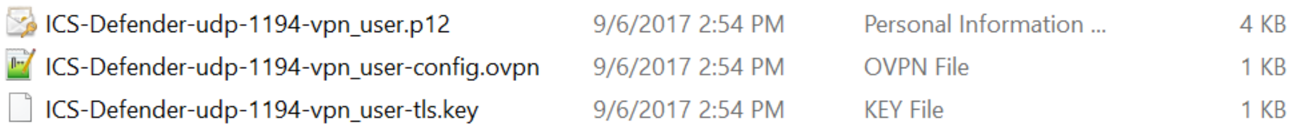
User	Certificate Name	Export
vpn_user	vpn_user	- Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Current Windows Installer (2.4.3-Ix01): Windows Vista and Later - Old Windows Installers (2.3.17-Ix01): x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Note: If the above option is not shown it generally means that there are no users or user certificates created. When more than one user certificate is created, they will all be listed here.

To export only the configuration (for use in an existing OpenVPN client installation) download using the "Standard Configurations", for Android or mobile configurations, use Inline Configurations.

If the OpenVPN client isn't installed on the PC that will be connecting to the VPN server, download the appropriate installer. The installer will come bundled with the necessary configuration already included and in the appropriate configuration folder after installation.

The files that are included in the configuration should be located in the "Program Files→OpenVPN→config" folder on the PC. There are three files, note that the name included in the file name matches the user in the above image.



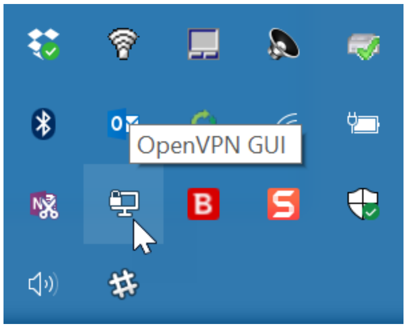
ICS-Defender-udp-1194-vpn_user.p12	9/6/2017 2:54 PM	Personal Information ...	4 KB
ICS-Defender-udp-1194-vpn_user-config.ovpn	9/6/2017 2:54 PM	OVPN File	1 KB
ICS-Defender-udp-1194-vpn_user-tls.key	9/6/2017 2:54 PM	KEY File	1 KB

The .OVPN file is the only editable file but should not be edited unless done so by a knowledgeable user.

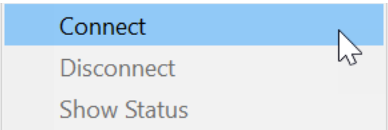
Connecting with OpenVPN

Once the OpenVPN configuration is installed in the OpenVPN→config folder, the OpenVPN client can be launched from the Windows Start menu.

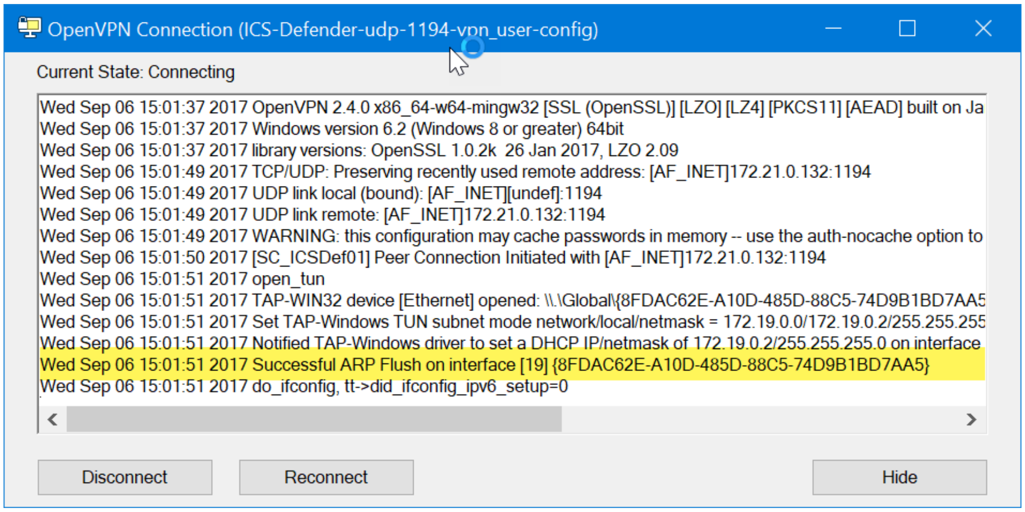
Once started, an icon should appear in the task bar or tool tray (depending upon the OS of the PC).



Right clicking the OpenVPN icon will present a "Connect" option. Note that if there is more than one OpenVPN configuration present, a list of the available configurations and connect buttons will be displayed.



Click connect to connect to the VPN server.



Current State: Connecting

```
Wed Sep 06 15:01:37 2017 OpenVPN 2.4.0 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AEAD] built on Ja
Wed Sep 06 15:01:37 2017 Windows version 6.2 (Windows 8 or greater) 64bit
Wed Sep 06 15:01:37 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.09
Wed Sep 06 15:01:49 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]172.21.0.132:1194
Wed Sep 06 15:01:49 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Sep 06 15:01:49 2017 UDP link remote: [AF_INET]172.21.0.132:1194
Wed Sep 06 15:01:49 2017 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to
Wed Sep 06 15:01:50 2017 [SC_ICSDef01] Peer Connection Initiated with [AF_INET]172.21.0.132:1194
Wed Sep 06 15:01:51 2017 open_tun
Wed Sep 06 15:01:51 2017 TAP-WIN32 device [Ethernet] opened: \\.\Global\{8FDAC62E-A10D-485D-88C5-74D9B1BD7AA5
Wed Sep 06 15:01:51 2017 Set TAP-Windows TUN subnet mode network/local/netmask = 172.19.0.0/172.19.0.2/255.255.255
Wed Sep 06 15:01:51 2017 Notified TAP-Windows driver to set a DHCP IP/netmask of 172.19.0.2/255.255.255.0 on interface
Wed Sep 06 15:01:51 2017 Successful ARP Flush on interface [19] {8FDAC62E-A10D-485D-88C5-74D9B1BD7AA5}
Wed Sep 06 15:01:51 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
```

To determine if the connection is successful, look for an entry near the bottom indicating a "Successful ARP Flush…"

Also note, for understanding the correlation between the tunnel network the VPN server is configured to use and connections to the VPN server, that an address from the VPN server tunnel network was used in making this connection. In the above example, the fourth line from the bottom indicates "Set TAP-Windows driver to set a DHCP IP/netmask of 172.19.0.2/255.255.255.0". Recall that the tunnel network, in the VPN server configuration as 172.19.0.0/24.

Status

The status menu in ICS-Defender provides information about a wide variety of systems and services within the appliance. Not all items on the status menu are discussed here, only those which are commonly used.

Captive Portal

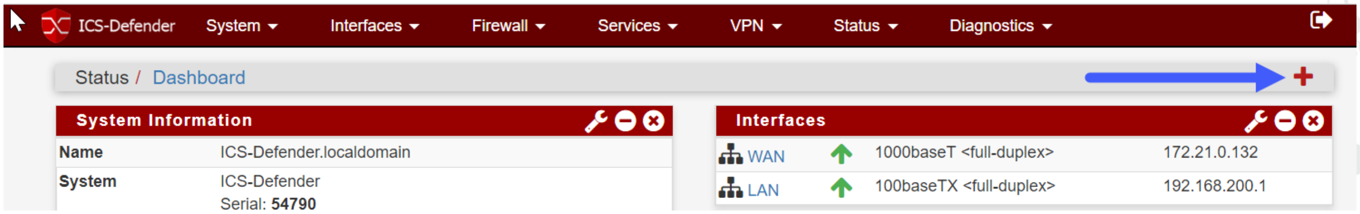
A captive portal is a web page which is displayed to newly connected users before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, acceptance of EULA/accepted use policies, or other valid credentials that both the host and user agree to adhere by. A captive portal can also be used to provide access to enterprise or residential wired networks, such as apartment houses, hotel rooms, and business centers. An example of use in an industrial environment would be to require suppliers to log into a control system either remotely or locally using a voucher provided by the plant engineering team.

If no captive portals are in use, this status menu will direct the user to the Captive Portal setup page.

Dashboard

The dashboard is the "home" page of ICS-Defender. It can be reached by either selecting this entry on the Status page or by clicking the ICS-Defender logo in the upper left corner.

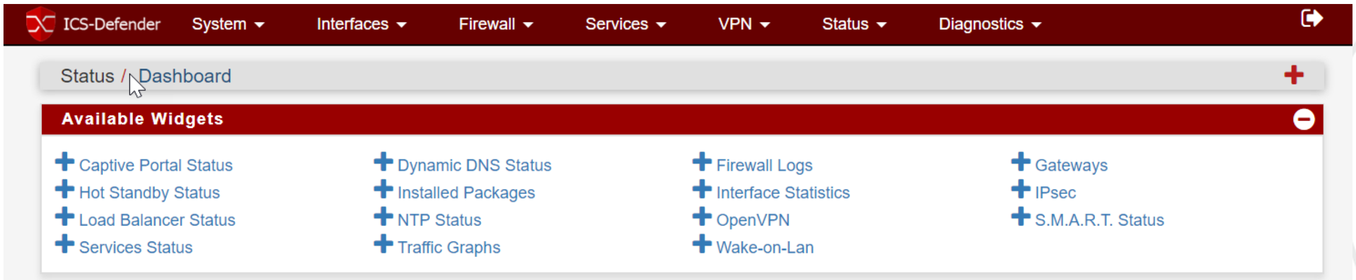
The dashboard content can be edited/customized to the users liking by editing the layout via the + at the top right of the dashboard screen.



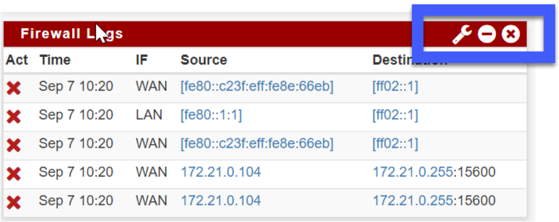
Name	ICS-Defender.localdomain
System	ICS-Defender Serial: **54790**

WAN	↑	1000baseT <full-duplex>	172.21.0.132
LAN	↑	100baseTX <full-duplex>	192.168.200.1

Clicking the + sign next to any of the widgets will add it to the dashboard.



Once added to the dashboard, many widgets offer customization options via the tool icon in their upper right corner.



Act	Time	IF	Source	Destination
✗	Sep 7 10:20	WAN	[fe80::c23f:eff:fe8e:66eb]	[ff02::1]
✗	Sep 7 10:20	LAN	[fe80::1:1]	[ff02::1]
✗	Sep 7 10:20	WAN	[fe80::c23f:eff:fe8e:66eb]	[ff02::1]
✗	Sep 7 10:20	WAN	172.21.0.104	172.21.0.255:15600
✗	Sep 7 10:20	WAN	172.21.0.104	172.21.0.255:15600

DHCP Leases

One of the features of DHCP is that it provides IP addresses that "expire." When DHCP assigns an IP address, it leases that connection identifier to the user's computer for a specific amount of time. The default lease is five days. Any current leases will be displayed on this status page.

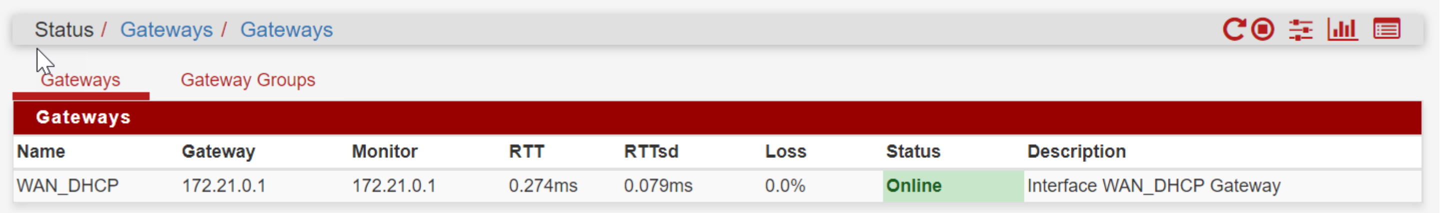
Filter Reload

Filter reload causes ICS-Defender to reload all rules and firewall filter settings. Note that there may be an impact to traffic while this reload is occurring so use only when appropriate and by knowledgeable personnel.

Gateways

A gateway is a node (router) in a computer network, a key stopping point for data on its way to or from other networks. Thanks to gateways, communication across the network is possible with data being sent back and forth. In ICS-Defender, the gateways monitored by this status page are typically those Enterprise gateways on the corporate network side of the WAN interface.

In this example, the WAN Interface is configured by DHCP, and the gateway is online and healthy.

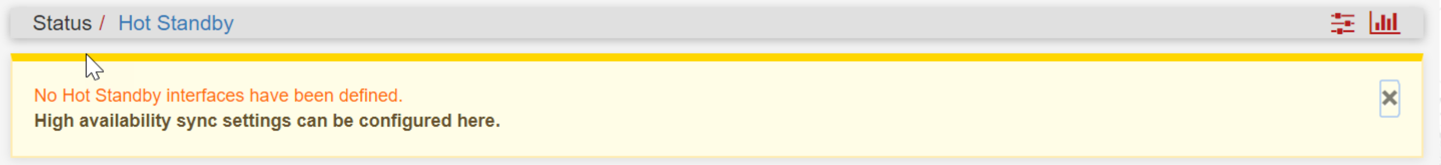


Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
WAN_DHCP	172.21.0.1	172.21.0.1	0.274ms	0.079ms	0.0%	Online	Interface WAN_DHCP Gateway

Hot Standby (Failover)

Hot standby is a redundant method in which one ICS-Defender is the primary system and a second (or more) ICS-Defenders act as hot standbys. Upon failure of the primary ICS-Defender, the hot standby ICS-Defender immediately takes over, replacing the primary ICS-Defender. This allows for bumpless transition and no interruption in the flow of data through the system.

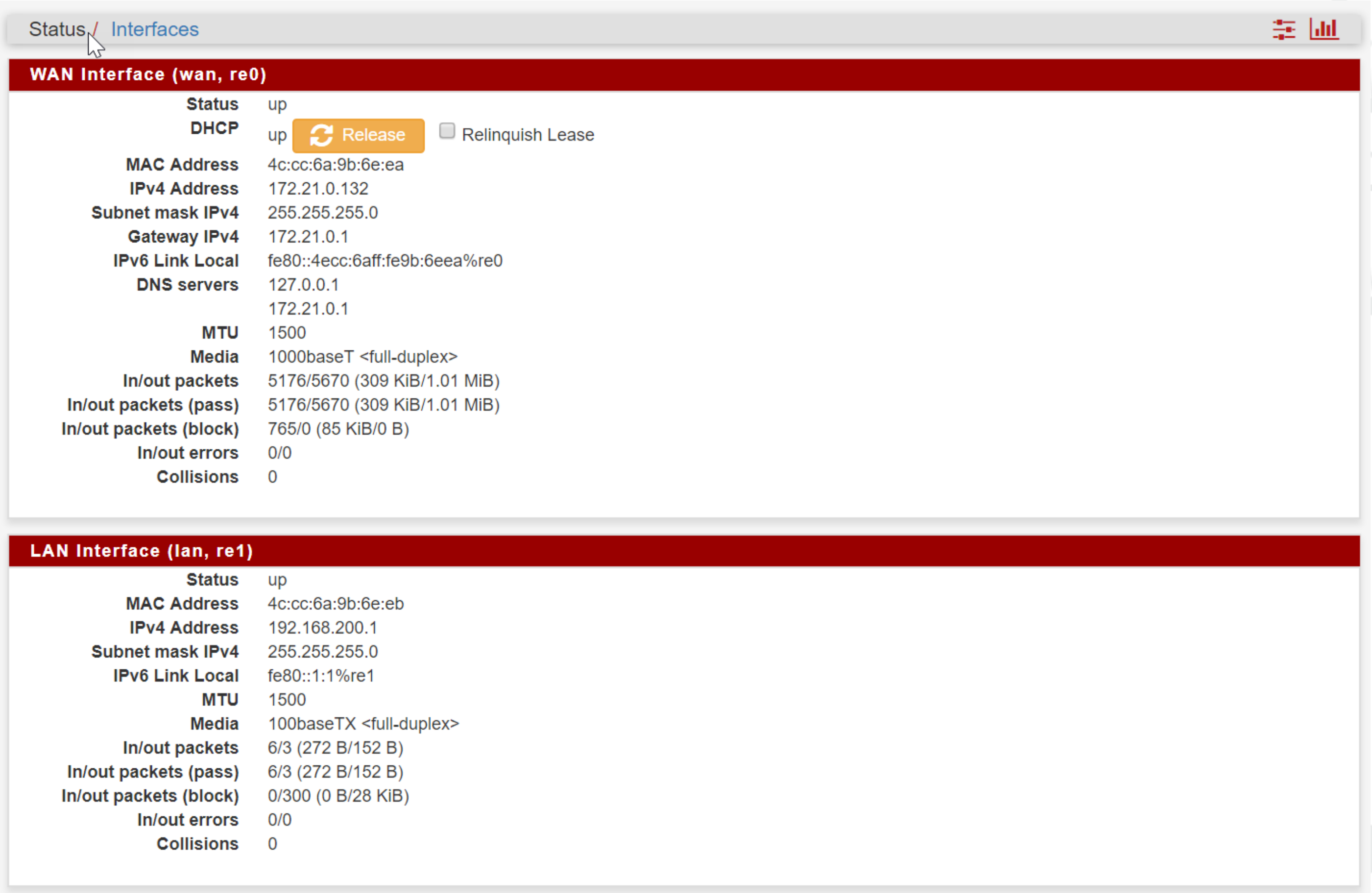
If there are no hot-standbys configured, there is no status information available.



No Hot Standby interfaces have been defined.
High availability sync settings can be configured here.

Interfaces

Interface status provides detailed information on the state and connection of the configured interfaces in the system.



WAN Interface (wan, re0)

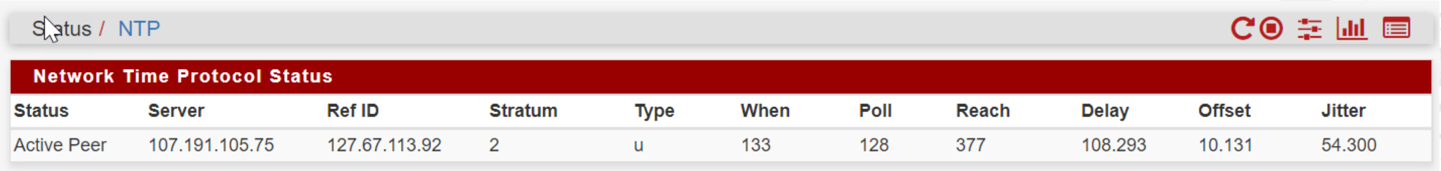
Status	up
DHCP	up
MAC Address	4c:cc:6a:9b:6e:ea
IPv4 Address	172.21.0.132
Subnet mask IPv4	255.255.255.0
Gateway IPv4	172.21.0.1
IPv6 Link Local	fe80::4ecc:6aff:fe9b:6eea%re0
DNS servers	127.0.0.1 172.21.0.1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	5176/5670 (309 KiB/1.01 MiB)
In/out packets (pass)	5176/5670 (309 KiB/1.01 MiB)
In/out packets (block)	765/0 (85 KiB/0 B)
In/out errors	0/0
Collisions	0

LAN Interface (lan, re1)

Status	up
MAC Address	4c:cc:6a:9b:6e:eb
IPv4 Address	192.168.200.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::1:1%re1
MTU	1500
Media	100baseTX <full-duplex>
In/out packets	6/3 (272 B/152 B)
In/out packets (pass)	6/3 (272 B/152 B)
In/out packets (block)	0/300 (0 B/28 KiB)
In/out errors	0/0
Collisions	0

NTP

ICS-Defender can synchronize it's time with an NTP Server (Network Time Protocol). The status of that synchronization is shown in the status page. Time servers can be configured in **System→General Setup→Localization**.

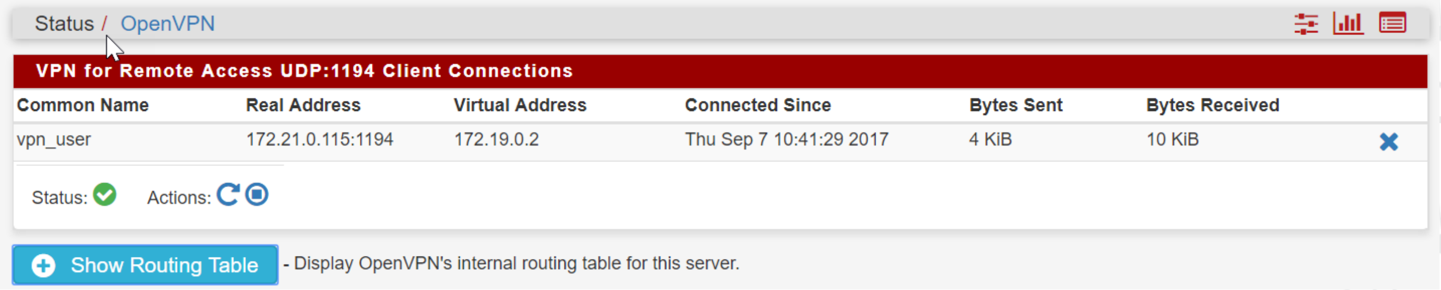


Network Time Protocol Status

Status	Server	Ref ID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
Active Peer	107.191.105.75	127.67.113.92	2	u	133	128	377	108.293	10.131	54.300

OpenVPN

The status of the OpenVPN servers and clients are shown on this page. If connections are made through the OpenVPN servers configured the details are displayed here as well. Actions of restarting or stopping the VPN Server or Client are available.



Status / OpenVPN

VPN for Remote Access UDP:1194 Client Connections

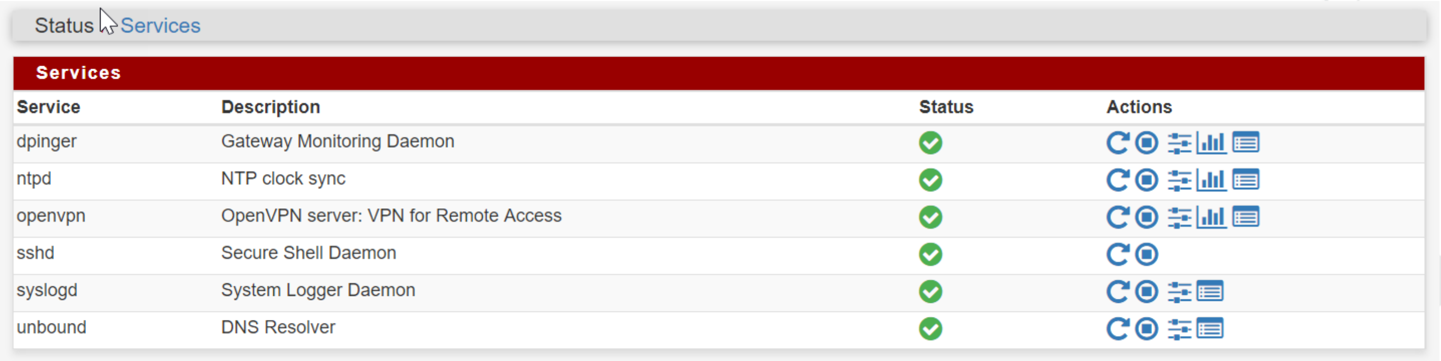
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	
vpn_user	172.21.0.115:1194	172.19.0.2	Thu Sep 7 10:41:29 2017	4 KiB	10 KiB	✖

Status: ✓ Actions: ↻ ◉

- Display OpenVPN's internal routing table for this server.

Services

Services are "workers" in ICS-Defender. There are several services that are enabled/visible based on the current ICS-Defender configuration. Controls are available to restart and stop the services from here. Caution should be taken before doing so in a production environment as stopping or restarted a service can impact the flow of data through ICS-Defender.



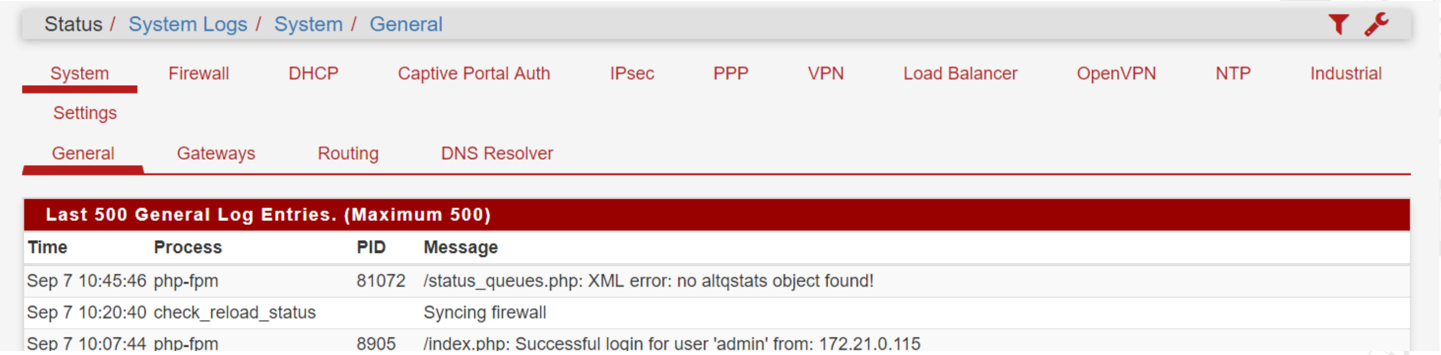
Status / Services

Services

Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	↻ ◉ ☰ 📊 ☰
ntpd	NTP clock sync	✓	↻ ◉ ☰ 📊 ☰
openvpn	OpenVPN server: VPN for Remote Access	✓	↻ ◉ ☰ 📊 ☰
sshd	Secure Shell Daemon	✓	↻ ◉
syslogd	System Logger Daemon	✓	↻ ◉ ☰ ☰
unbound	DNS Resolver	✓	↻ ◉ ☰ ☰

System Logs

Logs are available for most sub-systems in ICS-Defender.



Status / System Logs / System / General

Last 500 General Log Entries. (Maximum 500)

Time	Process	PID	Message
Sep 7 10:45:46	php-fpm	81072	/status_queues.php: XML error: no altqstats object found!
Sep 7 10:20:40	check_reload_status		Syncing firewall
Sep 7 10:07:44	php-fpm	8905	/index.php: Successful login for user 'admin' from: 172.21.0.115

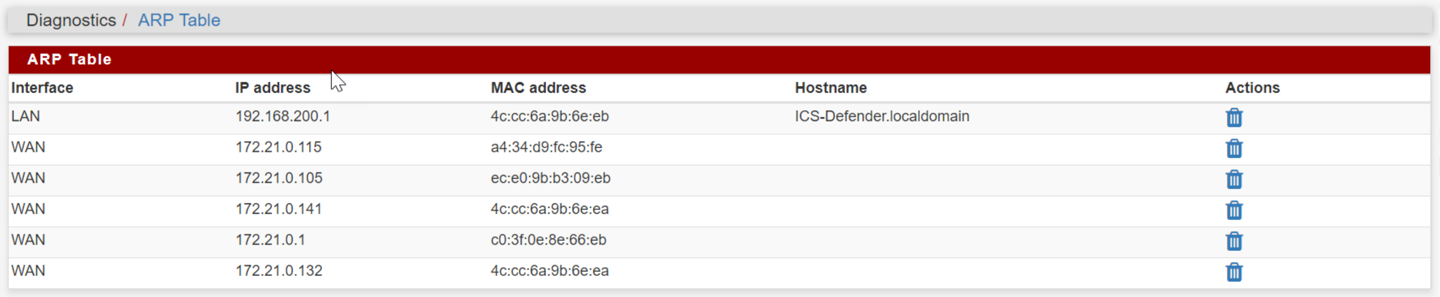
Log file sizes and details can be configured via the Status→System Logs→Settings.

Diagnostics

Diagnostic information is available from ICS-Defender for use in troubleshooting both external systems on either side of the appliance or settings within the appliance.

ARP Table

The ARP table shows the devices on the network of a particular interface as well as MAC address for the device.



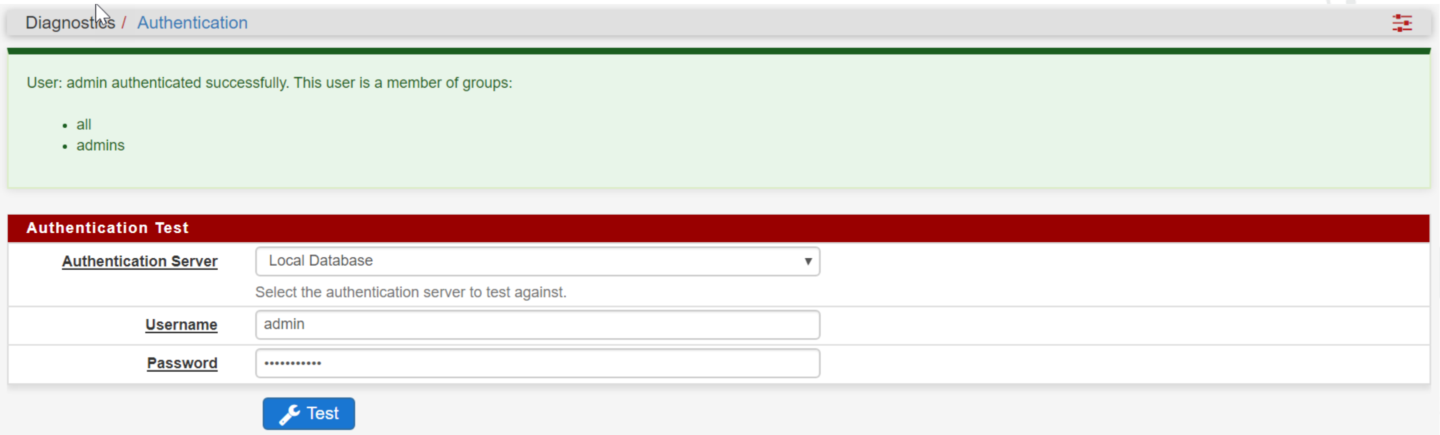
Diagnostics / ARP Table

ARP Table

Interface	IP address	MAC address	Hostname	Actions
LAN	192.168.200.1	4c:cc:6a:9b:6e:eb	ICS-Defender.localdomain	🗑
WAN	172.21.0.115	a4:34:d9:fc:95:fe		🗑
WAN	172.21.0.105	ec:e0:9b:b3:09:eb		🗑
WAN	172.21.0.141	4c:cc:6a:9b:6e:ea		🗑
WAN	172.21.0.1	c0:3f:0e:8e:66:eb		🗑
WAN	172.21.0.132	4c:cc:6a:9b:6e:ea		🗑

Authentication

This option allows testing user credentials, whether using internal users or LDAP/Active Directory credentials. This is particularly useful to test a username and password against an active directory.



Diagnostics / Authentication

User: admin authenticated successfully. This user is a member of groups:

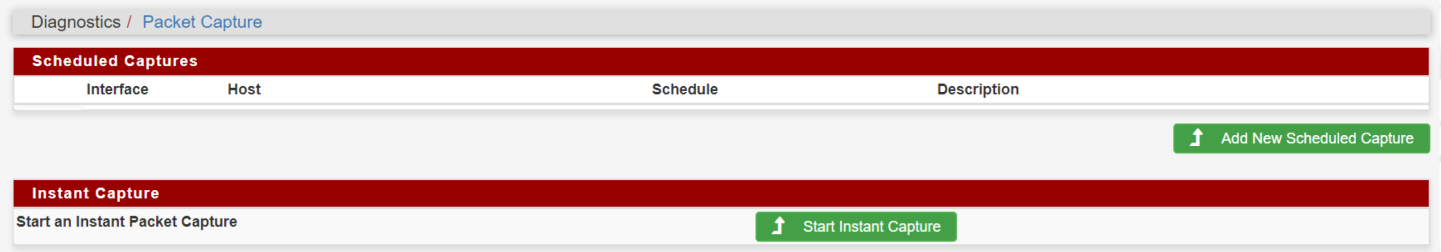
- all
- admins

Authentication Test

Authentication Server	Local Database Select the authentication server to test against.
Username	admin
Password	•••••••••••

Packet Capture

Packet captures allow capturing of network packets for debug or creating industrial protocol rules via analysis. Captures can be done immediately, or if a schedule is created, they can be executed on a schedule.



Diagnostics / Packet Capture

Scheduled Captures

Interface	Host	Schedule	Description

Add New Scheduled Capture

Instant Capture

Start an Instant Packet Capture

Start Instant Capture

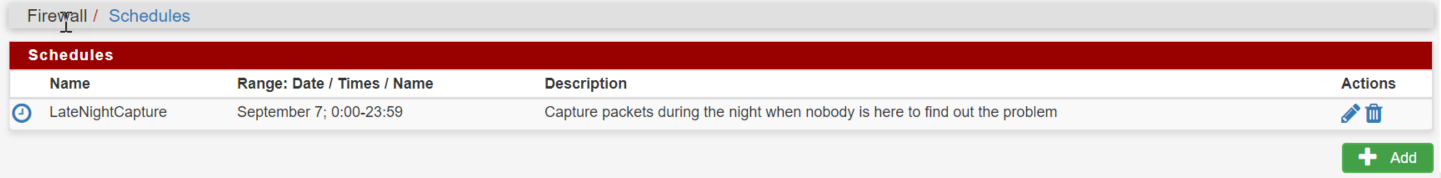
Immediate

Immediate packet capture is just as it sounds, the ability to capture traffic on any interface defined in ICS-Defender.

Scheduled

Scheduled packet captures are particularly useful for logging traffic at odd hours when unusual or undesirable network events are occurring and there is nobody around to manually capture traffic.

To create a schedule, navigate to **Firewall→Schedules**. The only difference in creating a scheduled capture versus an immediate capture is in a scheduled capture a schedule is chosen versus immediately starting a capture. Note schedules can also be used to enable/disable firewall rules automatically.



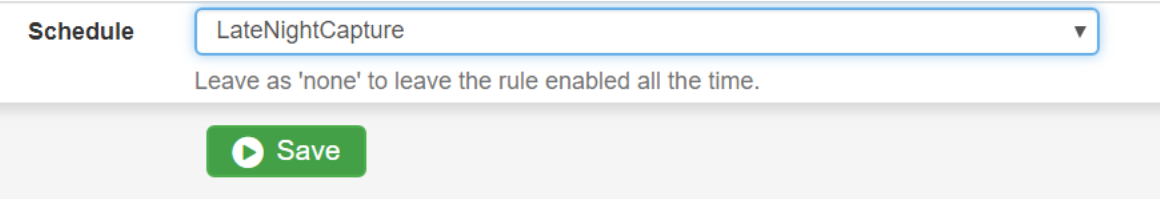
Firewall / Schedules

Schedules

	Name	Range: Date / Times / Name	Description	Actions
🕒	LateNightCapture	September 7; 0:00-23:59	Capture packets during the night when nobody is here to find out the problem	✎ 🗑

Add

Add a New Scheduled Capture and assign it to the desired schedule.

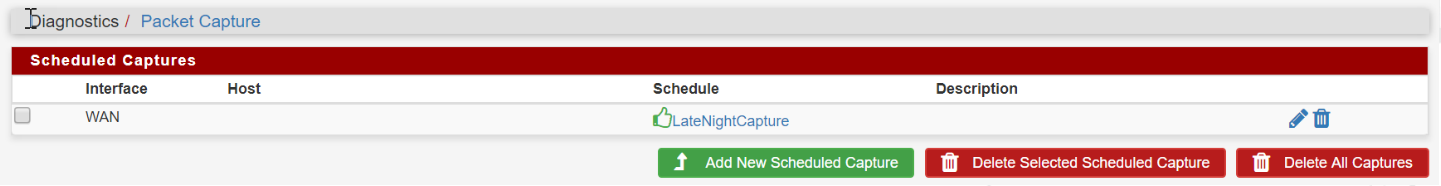


Schedule LateNightCapture ▾

Leave as 'none' to leave the rule enabled all the time.

Save

Once scheduled, the thumbs down icon indicates the packet capture isn't running, a thumbs up icon indicates the capture is actively running. Once a capture is complete, to the left of the delete icon (garbage can on the left) a download icon will appear allowing the capture to be downloaded.

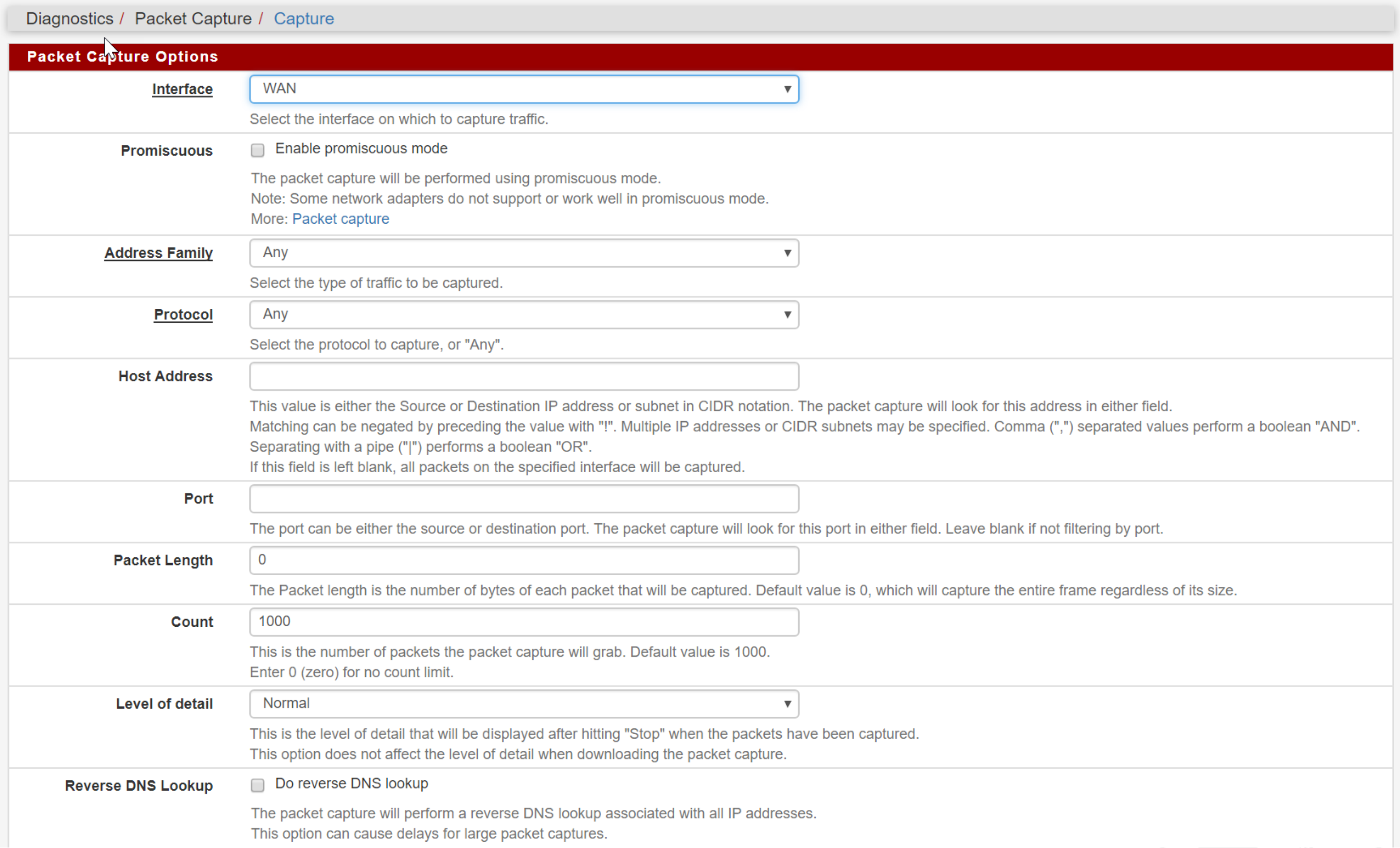


Diagnostics / Packet Capture

Scheduled Captures

	Interface	Host	Schedule	Description	
□	WAN		👍LateNightCapture		✎ 🗑

Add New Scheduled Capture | Delete Selected Scheduled Capture | Delete All Captures



Diagnostics / Packet Capture / Capture

Packet Capture Options

Interface	WAN ▾ Select the interface on which to capture traffic.
Promiscuous	□ Enable promiscuous mode The packet capture will be performed using promiscuous mode. Note: Some network adapters do not support or work well in promiscuous mode. More: Packet capture
Address Family	Any ▾ Select the type of traffic to be captured.
Protocol	Any ▾ Select the protocol to capture, or "Any".
Host Address	 This value is either the Source or Destination IP address or subnet in CIDR notation. The packet capture will look for this address in either field. Matching can be negated by preceding the value with "!". Multiple IP addresses or CIDR subnets may be specified. Comma (",") separated values perform a boolean "AND". Separating with a pipe ("|") performs a boolean "OR". If this field is left blank, all packets on the specified interface will be captured.
Port	 The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if not filtering by port.
Packet Length	0 The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.
Count	1000 This is the number of packets the packet capture will grab. Default value is 1000. Enter 0 (zero) for no count limit.
Level of detail	Normal ▾ This is the level of detail that will be displayed after hitting "Stop" when the packets have been captured. This option does not affect the level of detail when downloading the packet capture.
Reverse DNS Lookup	□ Do reverse DNS lookup The packet capture will perform a reverse DNS lookup associated with all IP addresses. This option can cause delays for large packet captures.

Interface: Which interface on ICS-Defender from which to capture network traffic/packets.

Promiscuous: Leave disabled by default.

Address Family: Specifying an address family from the drop down can narrow the traffic in the capture. Unless capturing on an interface with both IPv4 and IPv6, leaving it at the default setting is fine.

Protocol: Generally left at the default unless a particular protocol is to be captured.

Host Address: Any IP address entered in this field will force the capture to only include those packets with that IP in the source or destination field. Leave blank by default.

Port: Specify a unique port for network traffic. For example, to capture only CIP traffic, use port 44818.

Packet Length: Leave at the default setting of 0 to allow any length into the capture.

Count: By default the value is 1000 packets. Setting this to 0 will capture all packets as long as the capture is enabled. Setting this to a value other than 0 is generally used to limit the size of the capture when performing a scheduled capture.

Level of Detail: Leave at the default. This does not change the detail of the capture, only what is displayed on screen.

Reverse DNS Lookup: Leave at the default of unchecked unless this is specifically needed.

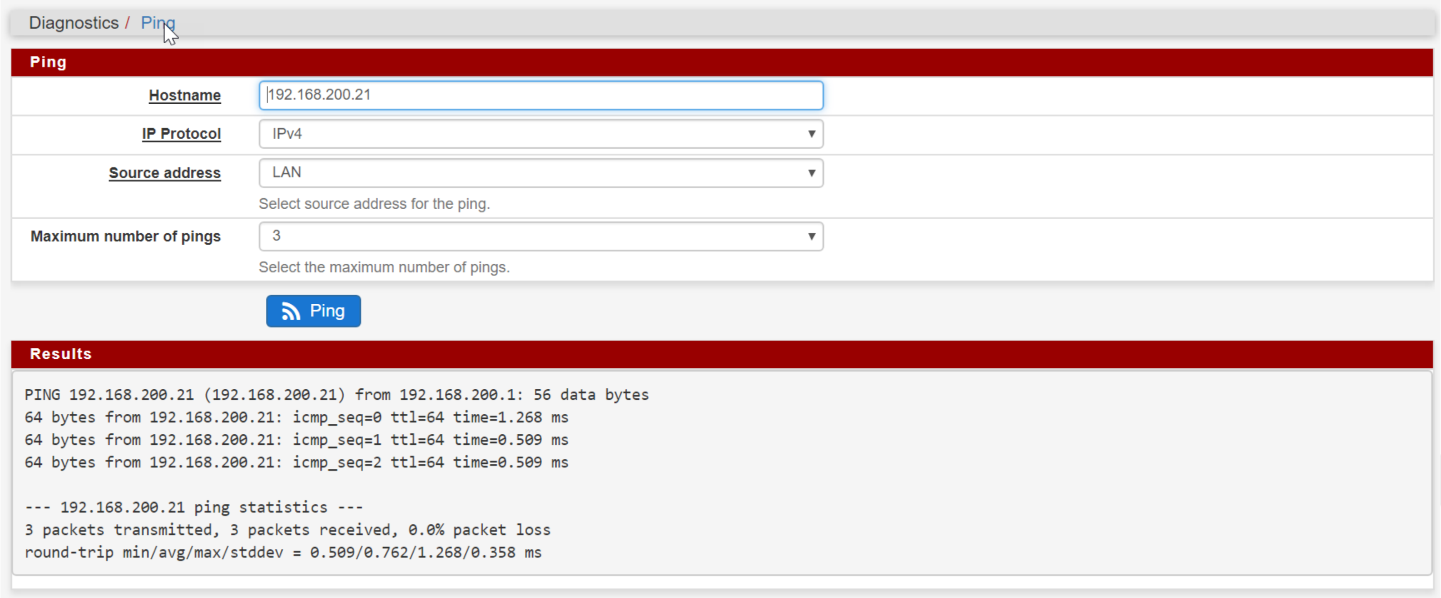
Ping

Ping is an ICMP protocol tool used to check for a connection from a PC/device to another IP device.

Note that firewall rules typically must be added to ICS-Defender to allow devices on any interface to get a response from ICS-Defender when a ping (echo request) is done. An example of setting up a rule to allow ICS-Defender to respond to pings can be found here.

It's also important to note that devices which communicate via industrial protocol may respond to a PING request but may not be able to connect via programming software etc. Often an IT department will allow ICPM traffic (pings) on a network but won't allow non-traditional IT traffic such as CIP/EtherNet/IP.

In the below example, a PLC at 192.168.200.21 is successfully pinged on the LAN interface. Pinging that PLC with the 192.168.200.21 IP Address on the WAN interface will fail as the PLC is part of a controls network connected to the LAN interface side of ICS-Defender.



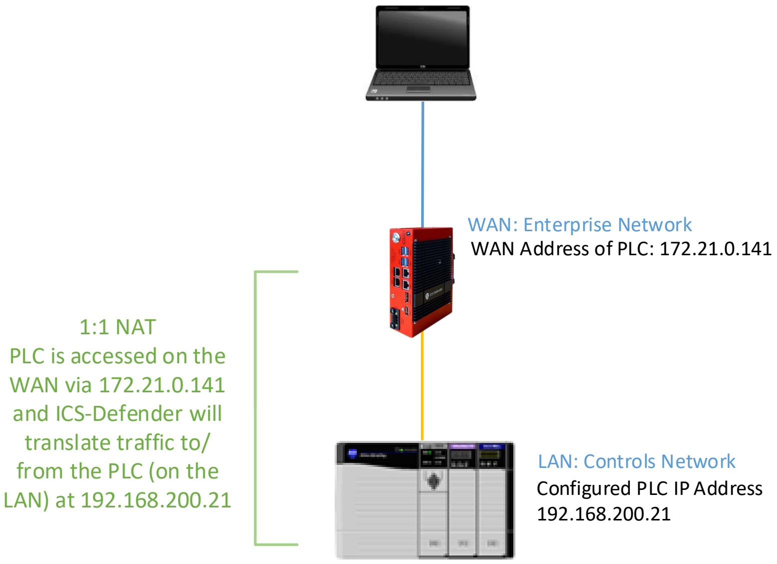
Hostname	192.168.200.21
IP Protocol	IPv4
Source address	LAN Select source address for the ping.
Maximum number of pings	3 Select the maximum number of pings.

```
PING 192.168.200.21 (192.168.200.21) from 192.168.200.1: 56 data bytes
64 bytes from 192.168.200.21: icmp_seq=0 ttl=64 time=1.268 ms
64 bytes from 192.168.200.21: icmp_seq=1 ttl=64 time=0.509 ms
64 bytes from 192.168.200.21: icmp_seq=2 ttl=64 time=0.509 ms

--- 192.168.200.21 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.509/0.762/1.268/0.358 ms
```

Pinging & 1:1 NAT

Important Note: *When pinging the WAN IP of a device that is using 1:1 NAT to allow reaching that device from the WAN to the LAN, the ping response comes from the WAN IP, not necessarily the device on the LAN network. Pinging the PLC at its NAT WAN address of 172.21.0.141* ***could*** *result in a positive response, even though the PLC isn't physically connected to the network.*


WAN: Enterprise Network
WAN Address of PLC: 172.21.0.141
1:1 NAT
PLC is accessed on the WAN via 172.21.0.141 and ICS-Defender will translate traffic to/ from the PLC (on the LAN) at 192.168.200.21
LAN: Controls Network
Configured PLC IP Address
192.168.200.21

Backup & Recovery

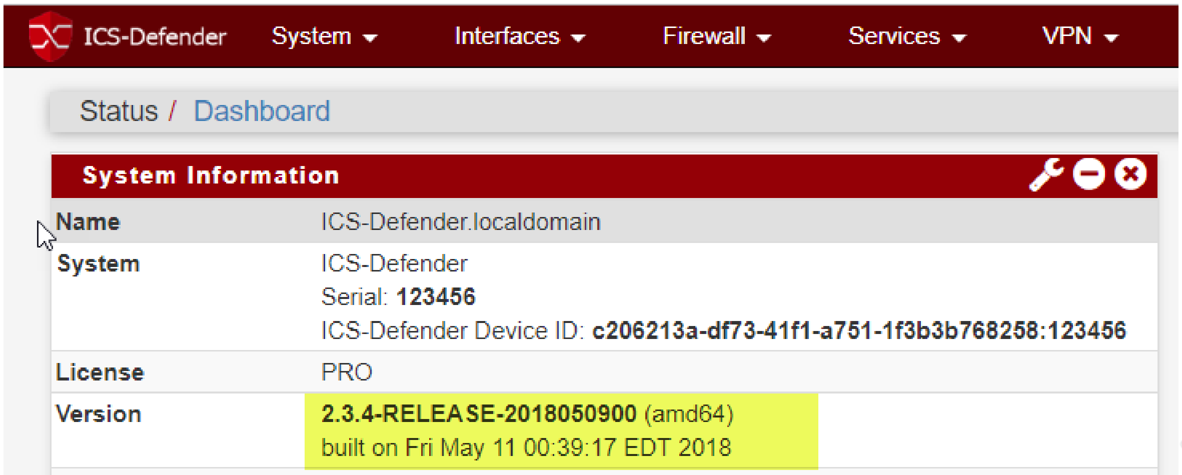
System Update

System update options can be found at **System→Update→System Update Tab** in the menu. There are several ways to update the system firmware which include connection via internet to the ICS-Defender automatic update site as well as updating via USB memory stick.

It is highly recommended that the running configuration be backed up. ICS-Defender should flash and restart with the currently running configuration, but care should be taken to avoid unexpected issues with a backup.

IMPORTANT: Any firmware update will cause the system to restart upon completion. Make sure the environment / production is such that a restart will not negatively affect the system being protected by ICS-Defender.

It is recommended that the person performing the update make a note of the existing version prior to update for a visual confirmation that the update completed.



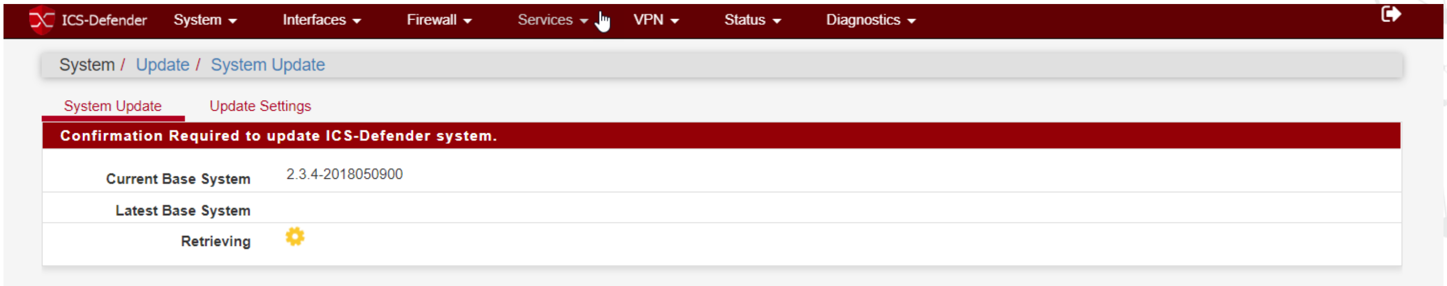
System Information

Name	ICS-Defender.localdomain
System	ICS-Defender Serial: **123456** ICS-Defender Device ID: **c206213a-df73-41f1-a751-1f3b3b768258:123456**
License	PRO
Version	**2.3.4-RELEASE-2018050900** (amd64) built on Fri May 11 00:39:17 EDT 2018

Update Portal (Via Internet)

To update via the internet, upon navigating to the update page, the system will attempt to reach our update portal and check the running version of the firmware against the most recent version.

It requires a support and maintenance agreement to update firmware.



Confirmation Required to update ICS-Defender system.

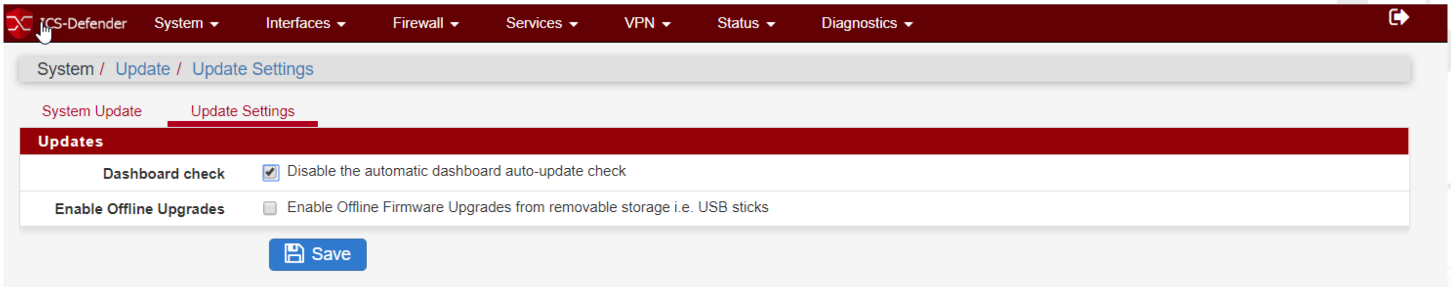
Current Base System	2.3.4-2018050900
Latest Base System	
Retrieving	

If a new version is detected, the system will prompt the user to update. If the update is started, the system will download the updated firmware, flash the system and automatically reboot. It will return to a running state with the previous configuration.

USB Update

USB updates are performed using a memory stick flashed with firmware from Dynics. The firmware is secure, the system securely checked by the ICS-Defender prior to allowing the update to begin.

To set the system to USB Update mode, insert a properly created USB stick in any of the four USB ports on the ICS-Defender. Once that step is complete, navigate to the **System→ Update→Update Settings Tab.**



Updates

Dashboard check	☑ Disable the automatic dashboard auto-update check
Enable Offline Upgrades	□ Enable Offline Firmware Upgrades from removable storage i.e. USB sticks

Check the box for "Enable Offline Upgrades" and the USB stick will be accessed and checked. Once confirmed that the update is from Dynics and safe, the necessary files will be transferred to the ICS-Defender. Wait 45 seconds, then click back to the System Update tab and the ICS-Defender should recheck the current against the new (the new from the USB stick) and prompt for an update if available.

Note: if the files haven't completed copying in the time before clicking System Update again, refresh the screen by clicking the System Update Tab.

The update should complete, and the ICS-Defender will restart. Check the new version from the dashboard against the previous version to visually confirm the update completed.