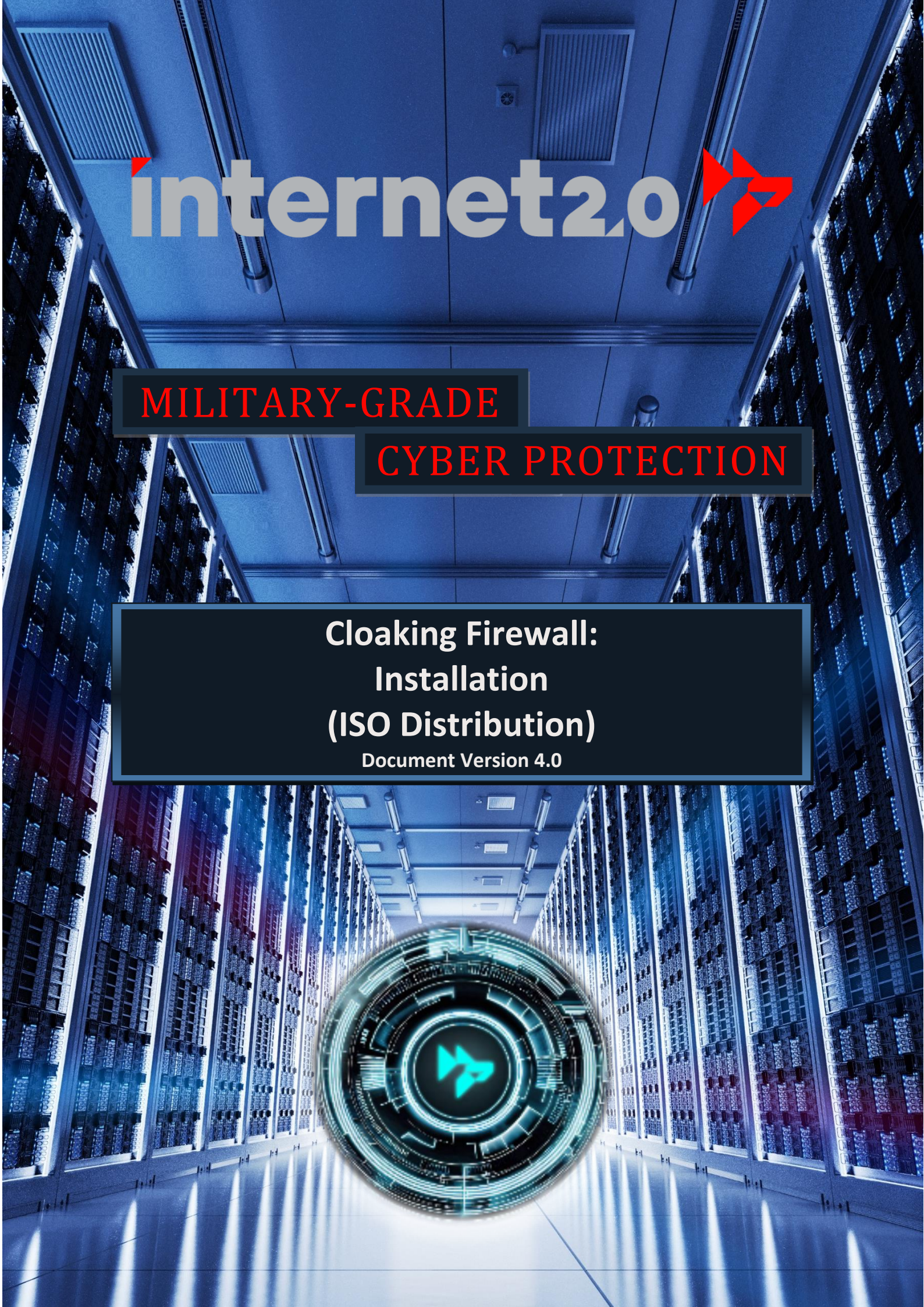

internet2.0
MILITARY-GRADE
CYBER PROTECTION
Cloaking Firewall:
Installation
(ISO Distribution)
Document Version 4.0

DISCLAIMER

This document is to allow Internet 2.0 to preconfigure and deploy a Cloaking Firewall (referred to as "Security Systems") to a client's ("Client") site/network, with minimal configuration required upon installation. Internet 2.0 will make every attempt to ensure the accuracy and reliability of the installation process based on the information provided by the Client. However, the information provided by the Client must be as accurate and detailed as possible. Internet 2.0 does not accept any responsibility or liability for the accuracy, content, completeness, legality, or reliability of the information provided by the Client.

Internet 2.0's Security Systems are designed to allow for customization; however, not all network configurations or systems may be supported, which may then require the Client to reconfigure their network/system to enable the successful operation and functionality of the Security Systems.

The Client understands and agrees that the use of Internet 2.0 is entirely at the Client's own risk and that Internet 2.0's services, appliances, and systems are provided "As Is" and "As Available." Internet 2.0 does not make any express or implied warranties, endorsements, or representations whatsoever as to the operation of the Internet 2.0 security services, appliances, systems, website, information, content, materials, or products. This includes, but is not limited to, implied warranties of merchantability, fitness for a particular purpose, non-infringement, and warranties that access to or use of the service will be uninterrupted or error-free or that defects in the service will be corrected.

The Client understands and agrees that Internet 2.0 and any of its subsidiaries or affiliates shall in no event be liable for any direct, indirect, incidental, consequential, or exemplary damages. This includes, but is not limited to, damages for loss of profits, business interruption, business reputation or goodwill, loss of programs or information, or other intangible losses arising out of the use of or the inability to use the service, information, or any permanent or temporary cessation of such service or access to information, or the deletion or corruption of any content or information, or the failure to store any content or information. The above limitation shall apply whether or not Internet 2.0 has been advised of or should have been aware of the possibility of such damages. In jurisdictions where the exclusion or limitation of liability for consequential or incidental damages is not allowed, the liability of Internet 2.0 is limited to the greatest extent permitted by law.

Licensing:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Internet 2.0 Cloaking Firewall and OPNsense include various freely available software packages and ports. The incorporated third-party tools are listed in Appendix E.

Contents

DISCLAIMER i
Overview of the Cloaking Firewall Installation 1
Navigating the Guide 1
Purpose and Benefits 1
Cloaking Firewall Specifications 2
Hardware Specifications 2
Additional Considerations 2
Prerequisites for Installing Cloaking Firewall 3
Install Cloaking Firewall from ISO 4
Initial Login with the Cloaking Firewall 15
Quick overview of the Dashboard 17
Menu 17
Header 17
Picture 18
System Information 18
Services 19
Firewall Log 19
Gateways 19
Network Time 19
Interfaces 19
Traffic Graph 20
Quick Setup with Provided Configuration File 21
Configure Gateway and WAN Interface 22
Configure Interfaces and Gateway (Default Configuration) 26
Perform Updates 30
Configuring the Systems of the Cloaking Firewall 32
Reporting Settings 32
Create Server Certificate Authorities and Certificates (SSL) 33
User Accounts: Change Passwords 36
User Groups 37
Administration Settings 38
Cron Tasks 39
General Settings 40
Logging Settings 40
Miscellaneous Settings 41
Services: Network Timing 42
Services: Unbound DNS 42
Services: Monit Settings 43

IDS (Suricata) Configuration 45
Enable Rules for Suricata 45
Enable and Configure OpenVPN 47
Create Remote Access for Firewall Administration 47
Download VPN Client 49
Perform Reboot if OpenVPN Server(s) are Enabled 49
Optional: Implement a VPN Interface 49
Firewall Configuration 50
Firewall Rules, Precedence/Priority 50
Firewall and Asymmetric Routing 51
Advanced Firewall Settings 52
Firewall NAT Port Forward 53
Firewall NAT Outbound 55
Firewall Rules 56
Disable the Anti-Lockout Rule 59
Configure RAIDEN 60
Tunable Settings: 62
Download Site Configuration File 65
Perform Reboot and System Checks 65
Troubleshooting 66
Disable the Firewall in case of Lockout 66
Resetting to Default Configuration 67
Errata 69
Performing Additional Updates 69
Appendix A: Improve IDPS Performance 70
Appendix B: Implement Multi-Factor Authentication 71
Add in MFA for Administrative WebGUI Logins 71
Appendix C: Monit - Email Notifications for MS Office 72
Microsoft Azure 72
Create User Account 72
Set Usage Location 72
Assign License 72
Exclude Multi-Factor Authentication (MFA) 72
Microsoft Office Admin Console 73
Enable SMTP for User's Mailbox 73
Microsoft Exchange 73
Add SMTP Email Address 73
Microsoft Online 73
Log in with the New Account 73
Setup Email Forwarding 74

Cloaking Firewall Monit Settings 74
Appendix D: Cloaking Nginx (Reverse Proxy) from Scans 76
Install Nginx Plugin 76
Configure IDPS 76
Configure Virtual IP 76
Configure Nginx 77
Configure Firewall 81
Appendix E: Systems and Versions 83

Overview of the Cloaking Firewall Installation

Welcome to the Cloaking Firewall Installation Guide. This comprehensive document is designed to assist you throughout the entire process of setting up and configuring your Cloaking Firewall system, ensuring optimal performance and robust security for your network infrastructure. From initial installation to advanced configurations, this guide provides detailed instructions and insights to help IT professionals efficiently deploy and manage the Cloaking Firewall.

Navigating the Guide

This guide is structured to take you step-by-step through the various stages of installation and configuration:

- **Prerequisites & Specifications:** Start by reviewing the necessary prerequisites and detailed specifications of Cloaking Firewall to ensure compatibility and readiness for installation.
- **Installation Process:** Follow detailed steps to install the Cloaking Firewall system, including adding and adjusting network interfaces and setting up routing tables for specific subnets.
- **Initial Configuration:** Perform initial setup procedures such as executing the bootup script, configuring interfaces and gateways, and establishing logging settings.
- **Advanced Settings and Customization:** Get guidance on performing updates, installing plugins, and transferring support files. This section also covers configuring cron jobs, monitoring, reporting, and IP blocker settings.
- **Security Enhancements:** Learn how to create VPN user groups, configure network timing, manage DNS settings, and set up server certificates. Administrative security measures like lockdowns and secure web browser connections are also detailed.
- **Operational Management:** Manage firewall configurations, including rules, NAT settings, and advanced firewall settings. Additionally, this section explains how to set up IDS, IPS, and manage OpenVPN setups.
- **Maintenance and Troubleshooting:** Find guidance on routine maintenance tasks, implementing multi-factor authentication, and troubleshooting common issues such as IP blocker failures and firewall lockouts.
- **System Customization and Finalization:** Customize your system to meet specific needs, perform final updates, and prepare the system for operational deployment. This includes creating and managing access for remote firewall administration.

Purpose and Benefits

The Cloaking Firewall Installation Guide is intended to provide a clear and systematic approach to setting up your firewall, from basic configurations to advanced security and operational settings. Whether you are an experienced network administrator or new to firewall configurations, this guide is crafted to provide all the information you need to successfully deploy and manage your Cloaking Firewall.

By following this guide, you will ensure that your network is protected with a high level of security while optimizing network performance and resource utilization. We encourage you to follow the steps closely and refer to the specific sections as needed to fully leverage the capabilities of the Cloaking Firewall in your network environment.

Cloaking Firewall Specifications

When planning the installation of Cloaking Firewall, it is essential to consider the hardware specifications to ensure compatibility and optimal performance. The hardware chosen should have sufficient processing power, memory, and storage to handle the demands of network traffic and security processes without bottlenecks. Here are the detailed hardware requirements and recommendations, including considerations for virtual environments and cloud deployments:

Hardware Specifications

- **Processor (CPU):**
  - **Minimum:** 2 cores
  - **Recommended:** 4 cores or more; Intel® based
    A multi-core processor is recommended to efficiently handle concurrent processes and high network traffic. Higher core counts can significantly improve performance, especially in environments with heavy usage or multiple security tasks.
- **Memory (RAM):**
  - **Minimum:** 2 GB
  - **Recommended:** 8 GB or more
    Adequate RAM is crucial for the smooth operation of security functions, handling multiple user connections, and running additional services. More memory ensures better performance and stability under load.
- **Storage (DISK):**
  - **Minimum:** 30 GB SSD
  - **Recommended:** 50 to 150 GB SSD
    Solid-state drives (SSDs) are preferred for their faster data access speeds and improved system responsiveness. Larger SSDs provide additional space for logs, updates, and other critical data, enhancing overall system performance.
- **Network Interfaces (NICs):**
  - **Minimum:** 2 (One WAN and One LAN)
  - **Recommended:** 4 (Two WANs and Two LANs) Intel® based
    Multiple network interfaces are necessary to separate different types of traffic and management tasks. This setup helps with better traffic management, redundancy, and increased security through segmentation.

Additional Considerations

- **Network Throughput:** Ensure that the chosen hardware or cloud instance can support the expected network throughput. Higher throughput capabilities are necessary for large or high-traffic environments to prevent bottlenecks and maintain performance.
- **Power Supply:** For physical deployments, a reliable power supply unit (PSU) with sufficient capacity to handle all hardware components is essential. Consider a redundant PSU for critical deployments to ensure continuous operation.
- **Cooling:** Proper cooling mechanisms should be in place to prevent overheating, especially in high-performance setups. Consider using hardware with efficient cooling solutions or placing the system in a well-ventilated area.
- **Form Factor:** Depending on the deployment environment, choose an appropriate form factor such as rack-mounted or tower servers. Rack-mounted servers are ideal for data centers, while tower servers may be suitable for smaller setups.

Prerequisites for Installing Cloaking Firewall

Before proceeding with the installation of Cloaking Firewall, it is important to ensure that all prerequisites are met to facilitate a smooth and successful setup. Below are the key requirements that need to be addressed:

1. **Hardware Requirements:**
   - Ensure the hardware meets or exceeds the minimum specifications outlined for the Cloaking Firewall. This includes a compatible processor, sufficient RAM, adequate storage capacity with SSDs recommended, and necessary network interface cards.
   - Ensure that access is possible to the firewall:
     i. If a physical appliance, then a keyboard and monitor are needed to access the console.
     ii. If it is a virtual machine, then the console can be accessed through the hypervisor manager.
2. **Network Connectivity:**
   - Reliable network connectivity is crucial. Ensure that all networking equipment (such as routers, switches) and cabling are in good working order. The network should be stable to avoid disruptions during the firewall installation and configuration.
3. **ISO Media Preparation:**
   - Download the latest version of the Cloaking Firewall ISO from the official website. Verify the integrity of the download with checksums to ensure the file is not corrupted. Prepare a bootable USB drive or DVD with the ISO image, depending on the installation method preferred or the capabilities of the hardware. Also, the ISO can be used within a virtual environment.
4. **Backup Existing Data:**
   - Before installing the new firewall system, back up all existing data and configurations from the current system. This precaution will prevent data loss and provide a recovery point in case the installation does not go as planned.
5. **Access Credentials:**
   - Have all necessary access credentials ready. This includes admin credentials for existing network devices and systems that might need to be configured or turned off during the firewall installation.
6. **Installation Documentation:**
   - Familiarize yourself with the installation guide and any specific vendor documentation. Having a clear understanding of the installation steps, configurations, and settings will help avoid common pitfalls.
7. **Legal and Compliance Checks:**
   - Verify that the installation and use of Cloaking Firewall complies with local and international laws and regulations concerning data protection and network security.
8. **Plan for Network Downtime:**
   - Schedule a maintenance window during which the installation will take place. Inform all stakeholders of potential network downtime to minimize disruption to business operations.

By ensuring these prerequisites are met, you can proceed with the installation of Cloaking Firewall confidently, knowing that you have prepared the environment for a successful deployment. This preparation will help avoid technical issues during the installation process and ensure that the firewall integrates smoothly into your existing network infrastructure.

Install Cloaking Firewall from ISO

To begin the installation process of the Cloaking Firewall, with the ISO made into a bootable media (DVD, USB, etc), insert the prepared bootable device containing the Cloaking Firewall ISO into the designated server and power on the system. Ensure that the BIOS/UEFI settings are configured to prioritize booting from the USB/DVD drive. Once the system boots from the correct media, follow the on-screen instructions to commence the installation setup, selecting the appropriate options for your network environment.

For best performance and security is to use UEFI (or sometimes referred to as EFI).

This installation guide assumes that IPv4 Addresses will be used.

1. When the system powers on, it will begin the booting process from the ISO media.
    a. The bootup process will take some time as the WAN interface is not configured.

2. Let the Cloaking Firewall complete the bootup process until the Login prompt:

3. To log in, type:
    Login: root
    Password: internet2-0.com

4. The console menu will appear.

```
*** Internet 2.0 Cloaking Firewall: cloakingfw.internet2-0.soc ***

 01_WAN1 (vmx1)  ->
 10_LAN1 (vmx0)  -> v4: 192.168.0.1/24

 HTTPS: SHA256 D7 A6 BD A8 B2 FB 6D 35 D9 A1 63 43 BC 56 B3 FD
               A8 EB F6 FF 72 5C B0 F9 07 E2 CB 59 51 C3 50 6A

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

5. The interfaces will need to be configured first.
6. Enter “1” and then press “Enter” to assign the interfaces:
    a. LAGGs: N (and then press “Enter”)
    b. VLANs: N (and then press “Enter”)
    c. There will be a listing of interfaces with their MAC physical addresses listed. Identify which interface will be used for the WAN and LAN.

```
Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

vmx0            00:50:56:01:16:0d VMware VMXNET3 Ethernet Adapter
vmx1            00:50:56:01:16:0e VMware VMXNET3 Ethernet Adapter

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection:
```

Shown above are two interfaces, this for with use in Vmware.
The WAN will be using vmx0, while the LAN will use vmx1.

    d. For the WAN (which is normally the Internet facing interface), type in the interface identifier, then press “Enter” to continue.
    e. For the LAN (which would be for the private local network), type in the interface identifier, then press “Enter” to continue.
    f. The Optional interfaces can be skipped for now. Press “Enter” to continue.

```
The interfaces will be assigned as follows:

WAN  -> vmx0
LAN  -> vmx1

Do you want to proceed? [y/N]: y
```

Above is an example of assigning the interfaces.

    g. If there are no typos, type in “y” and then press “Enter” to proceed.
        i. If there has been a mistake, hit CTRL-C to start again.

7. When the assignments have been completed, to set the IP addresses of the LAN press “2” and then “Enter”.
   Note: If the Default IP Address of 192.168.0.1 is the correct IP for the LAN, then can skip to Step 8.
   a. Press “2” for LAN and then press “Enter”.
   b. DHCP setup: N (and then press “Enter”)
   c. IPv4 Address:
      i. Enter the IP address in IPv4 format.
   d. Subnet:
      i. Enter the Subnet, which is typically 24.
   e. Upstream Server: Leave blank and press “Enter”
   f. Configure for DHCP6: N (and then press “Enter”)
   g. IPv6 Address:
      i. Leave blank and press “Enter” unless using IPv6, then enter the IP address in IPv6 format.
   h. Enable DHCP server on LAN: N (and then press “Enter”)
   i. Change web GUI from HTTPS to HTTP: N (and then press “Enter”)
   j. Generate New Self-Signed Certificate: N (and then press “Enter”)
   k. Restore web GUI access defaults: N (and then press “Enter”)

```
Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.20.10

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
Do you want to generate a new self-signed web GUI certificate? [y/N] n
Restore web GUI access defaults? [y/N] n
```

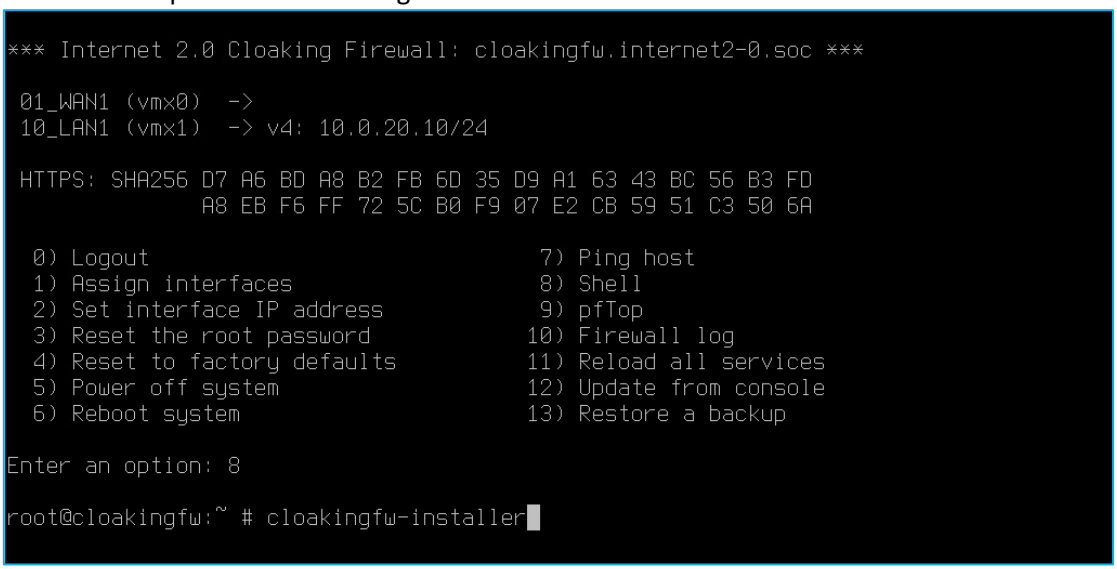
An example of configuring the LAN interface.

```
*** Internet 2.0 Cloaking Firewall: cloakingfw.internet2-0.soc ***

 01_WAN1 (vmx0)  ->
 10_LAN1 (vmx1)  -> v4: 10.0.20.10/24

 HTTPS: SHA256 D7 A6 BD A8 B2 FB 6D 35 D9 A1 63 43 BC 56 B3 FD
               A8 EB F6 FF 72 5C B0 F9 07 E2 CB 59 51 C3 50 6A

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

An example of completing the initial configuration.

8. When the configuration of the LAN interface is completed, go to the Shell (command line), by pressing “8” and then press “Enter”.

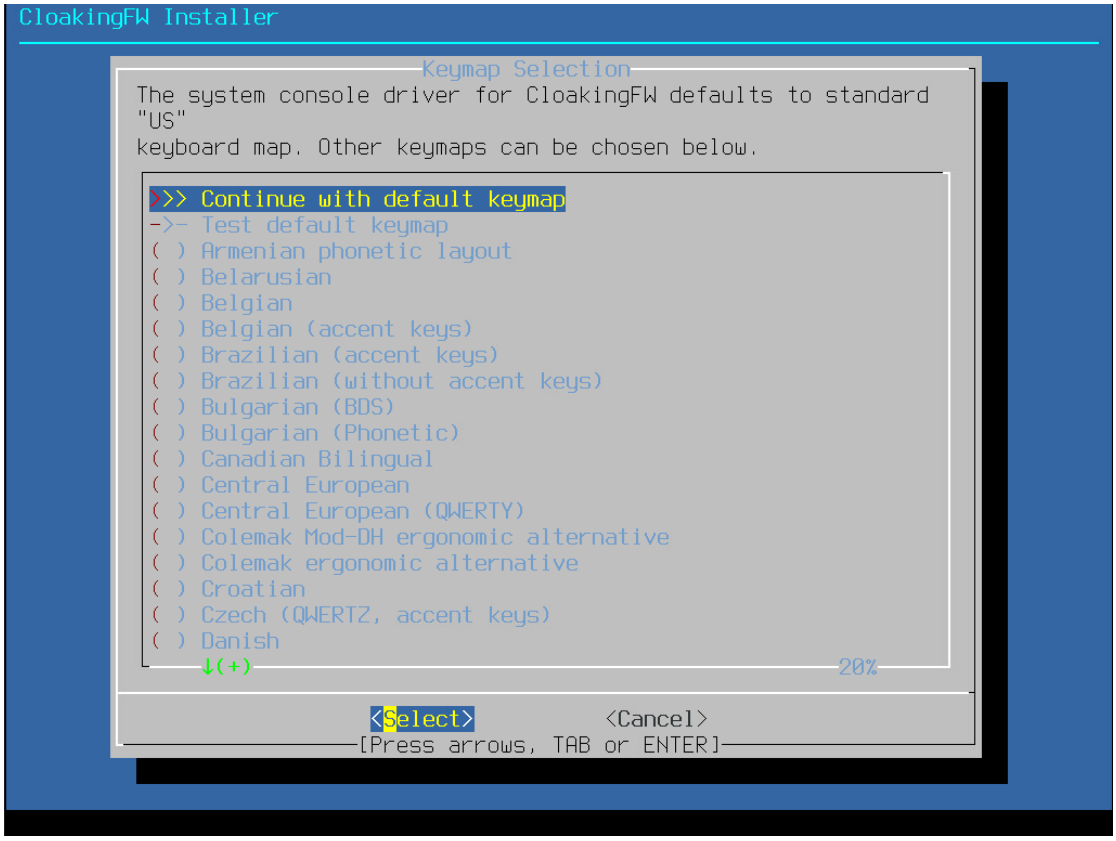
9. At the prompt, type:
   `cloakingfw-installer`
   And then press “Enter” to begin.



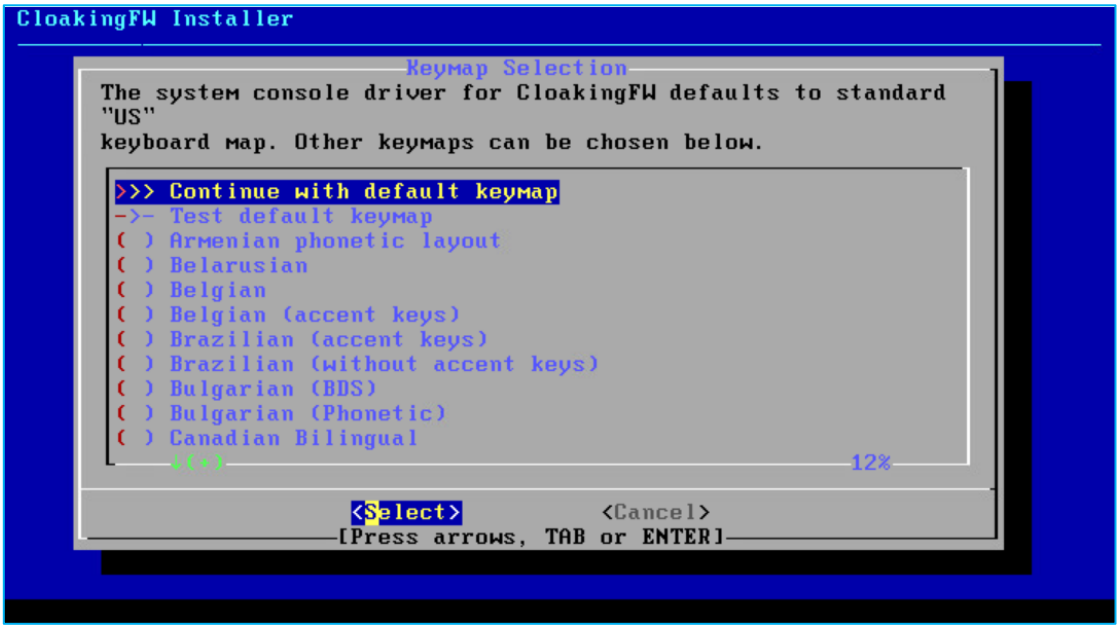
During the installation process, there will be slight differences between UEFI and BIOS installations.

10. At the Keymap Selection, select the keyboard mapping to use, otherwise leave as default and hit Enter.

UEFI Installation:

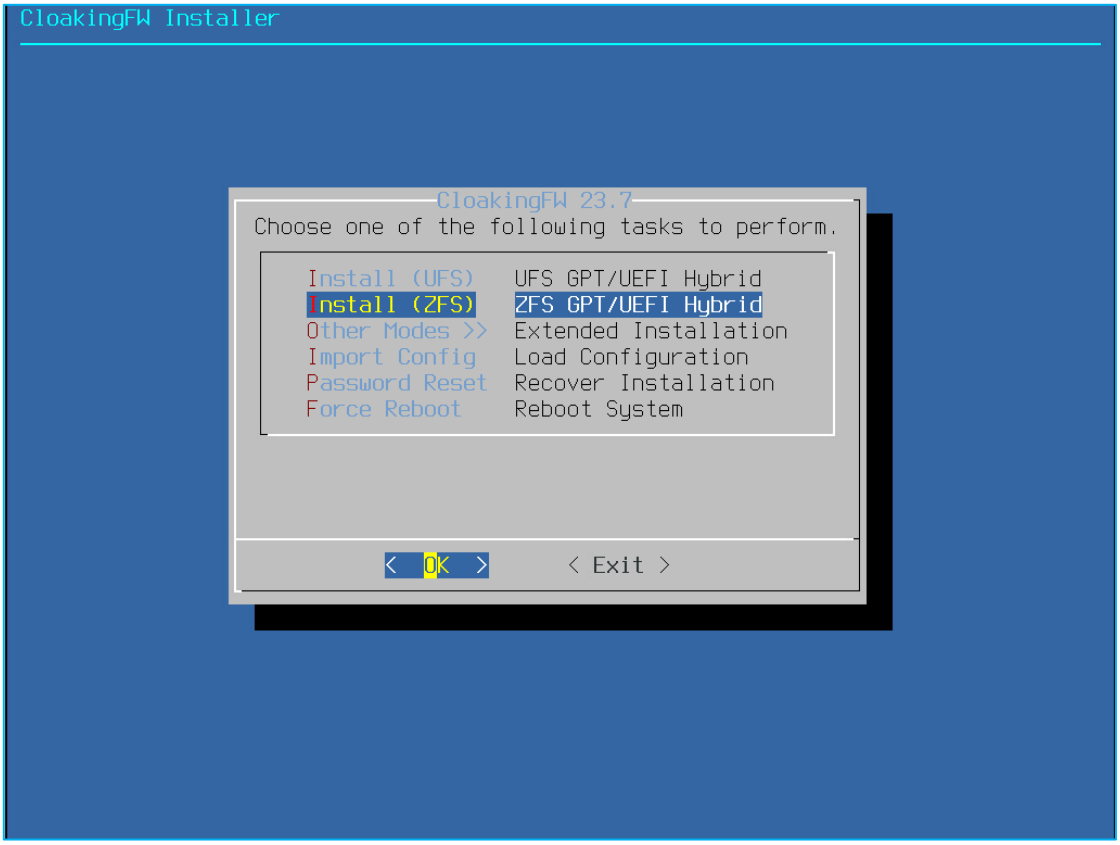


BIOS Installation:

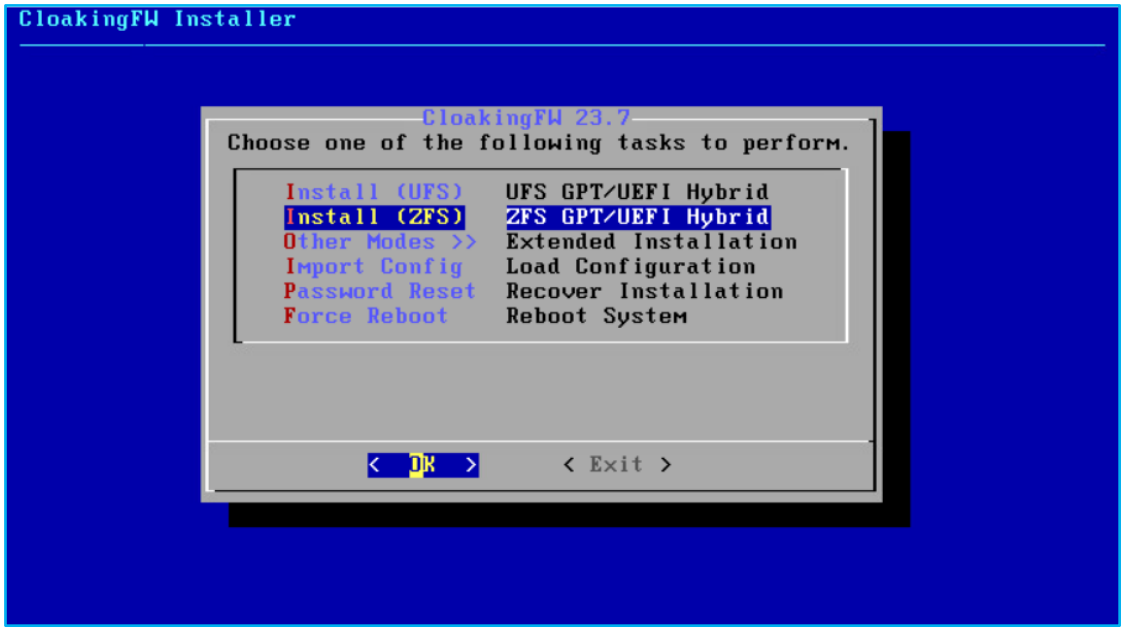


11. At the Task Window, it is best to select “ZFS” if listed, otherwise select “UFS”.
    a. To select “ZFS”, use the down arrow key to highlight it and then hit Enter.
    Note: Some system may not be able to support ZFS. Should an error occur when using ZFS, then select UFS instead.

UEFI Installation:

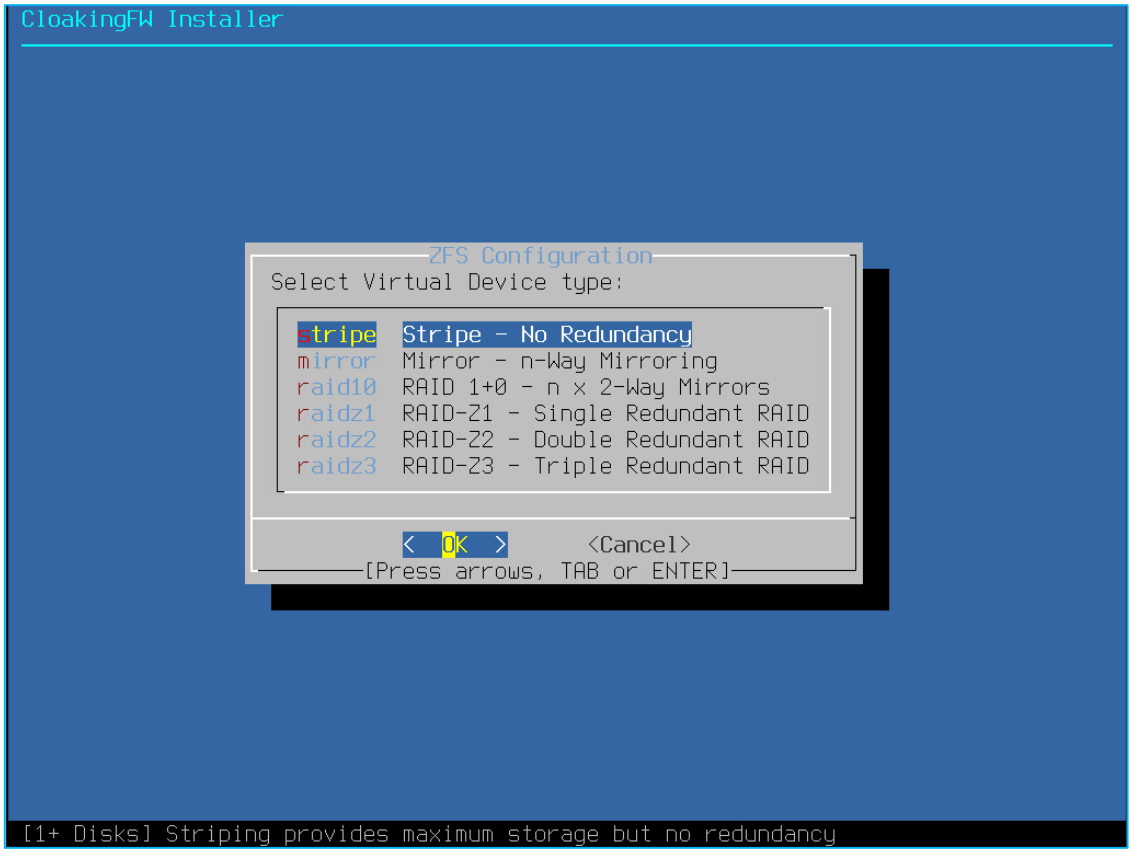


BIOS Installation:

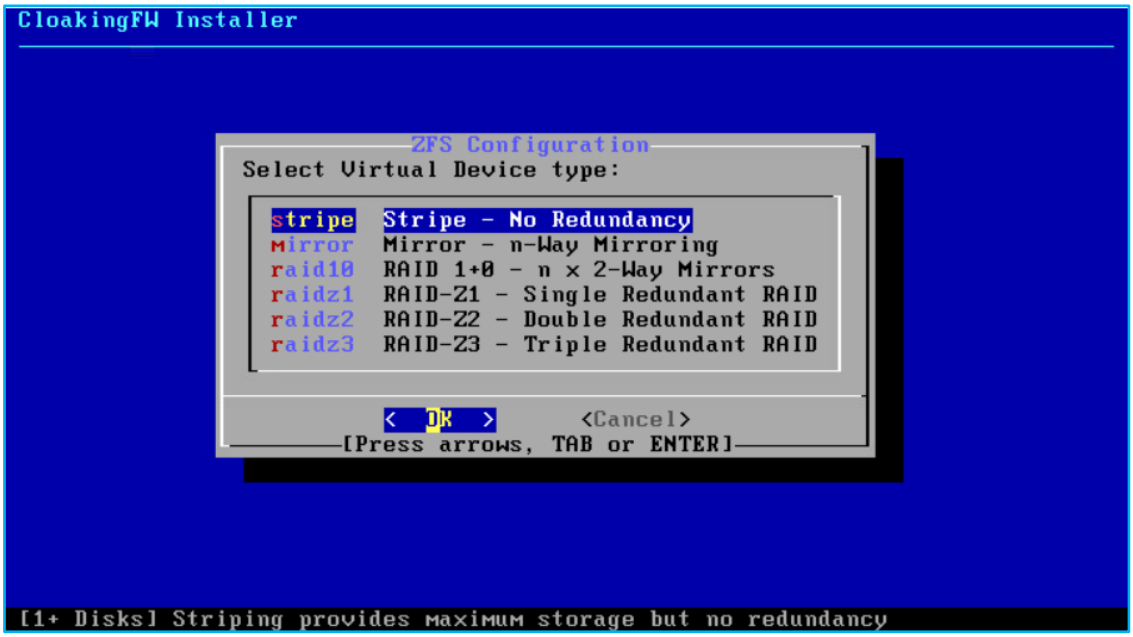


b. At the Disk RAID window, select the correct RAID if to use one. Otherwise, leave as Stripe. Hit enter to continue.

UEFI Installation:

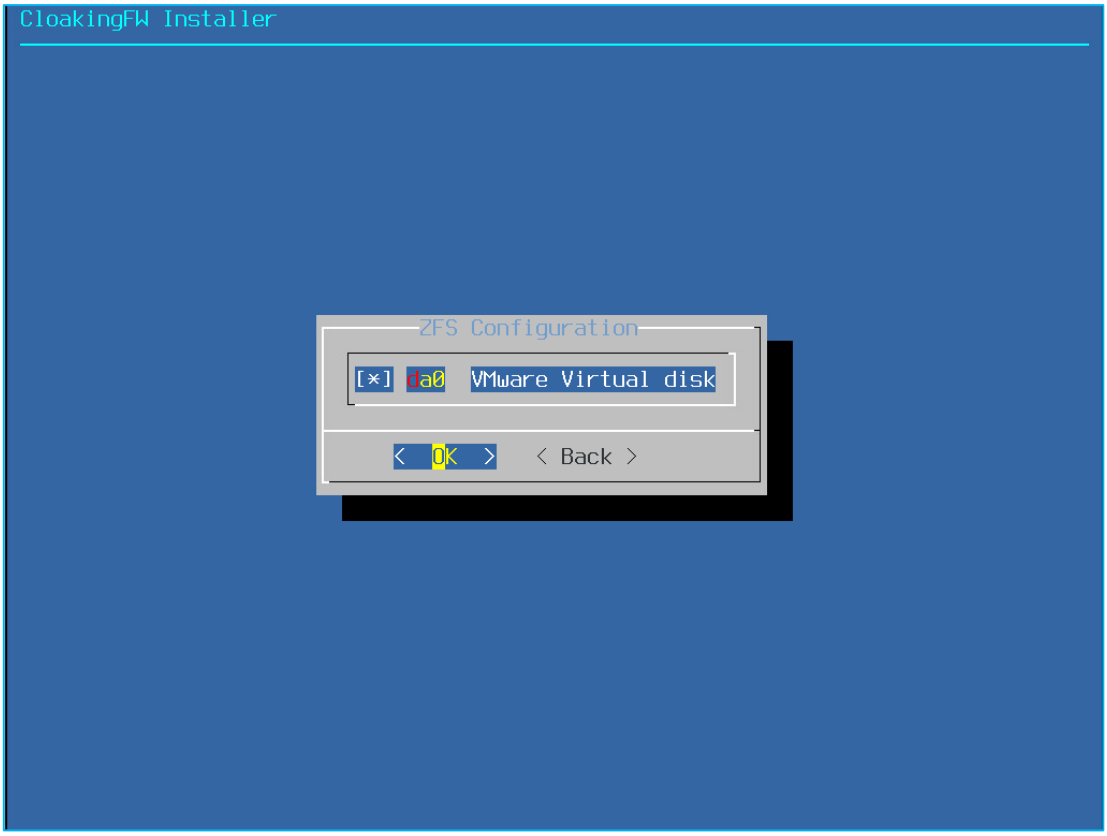


BIOS Installation:

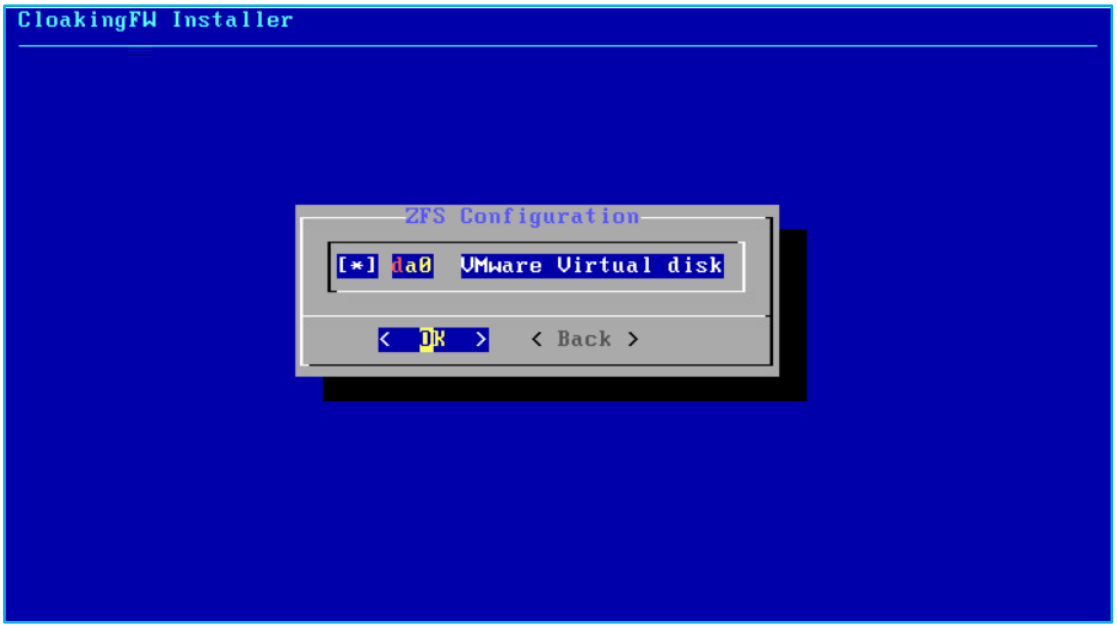


c. At the Drive Device window, select the designated drive to use. If needed, use the arrow keys to highlight the drive. Hit the spacebar to select the drive. Then hit Enter to continue.

UEFI Installation:

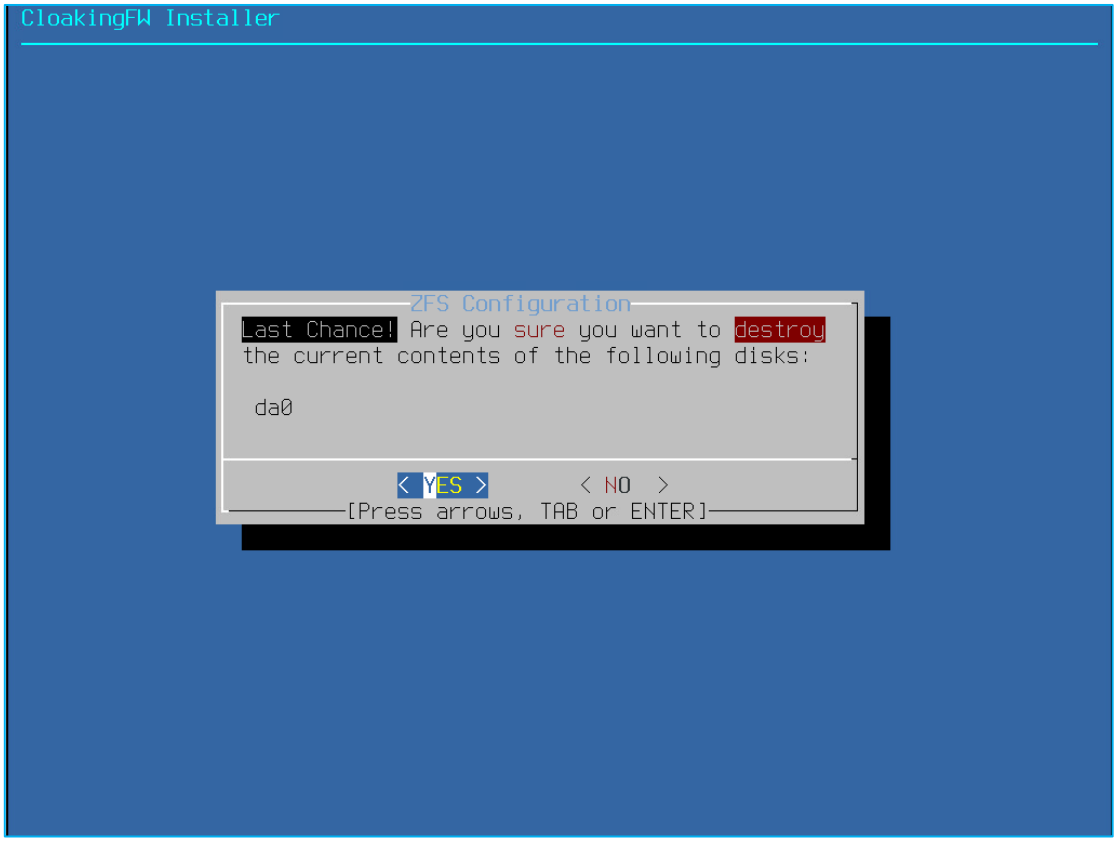


BIOS Installation:

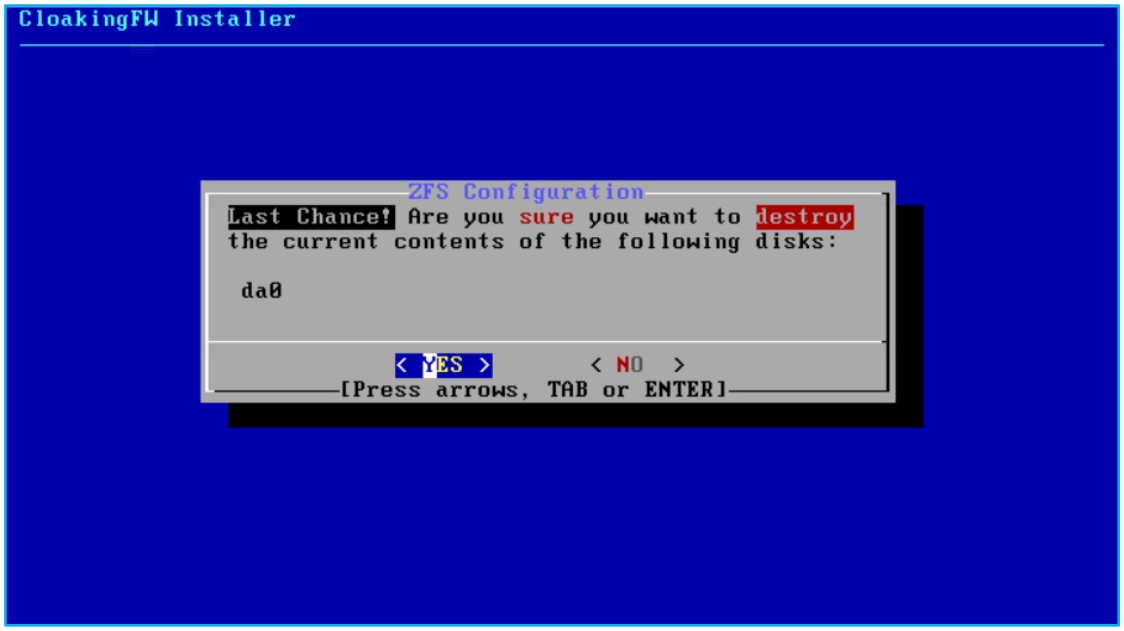


d. The Confirmation Window will appear, confirm this is the drive to use. If so, then use the left arrow key to select “YES” and then hit Enter to proceed.
    i. Otherwise leave at “NO” and hit Enter to redo the drive settings.

UEFI Installation:

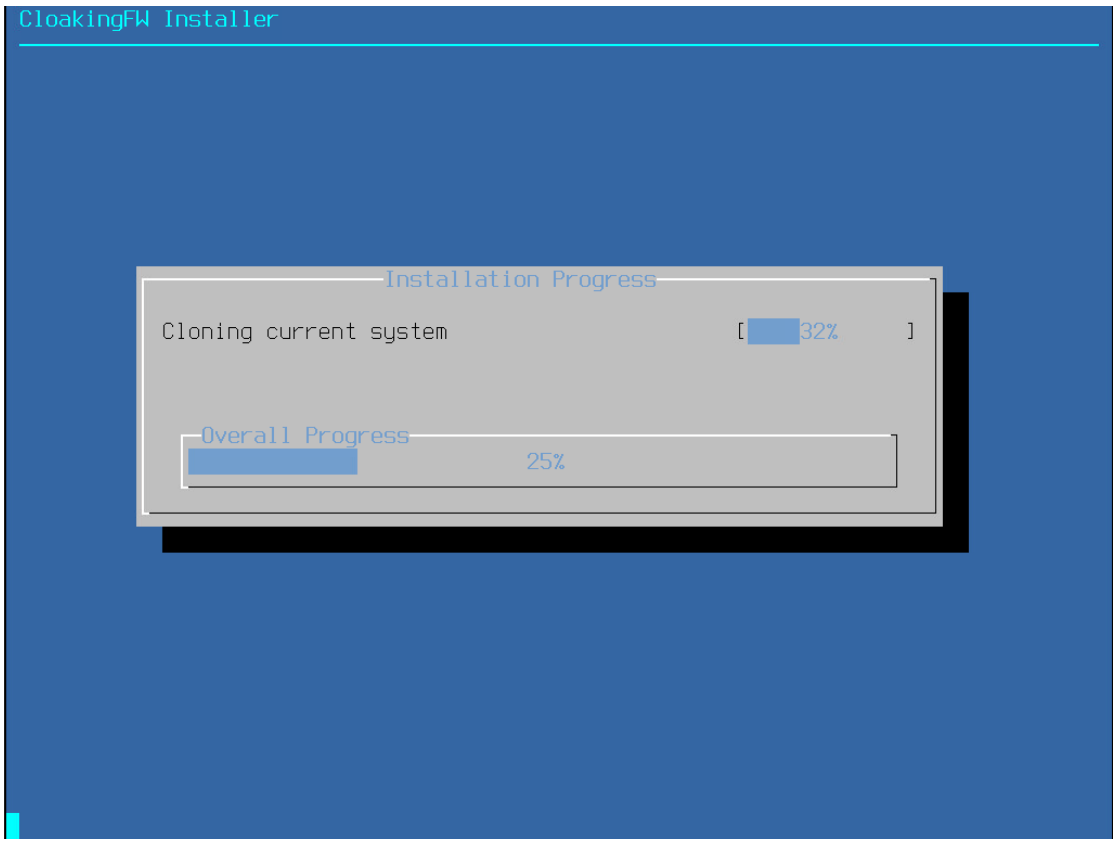


BIOS Installation:

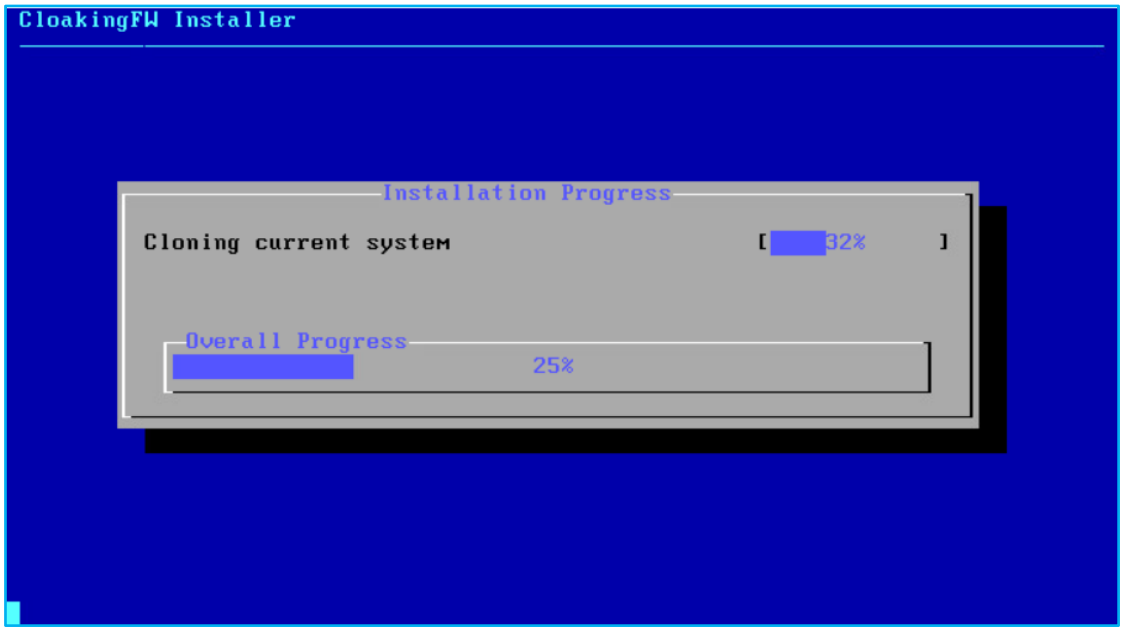


e. The installation will begin.

UEFI Installation:

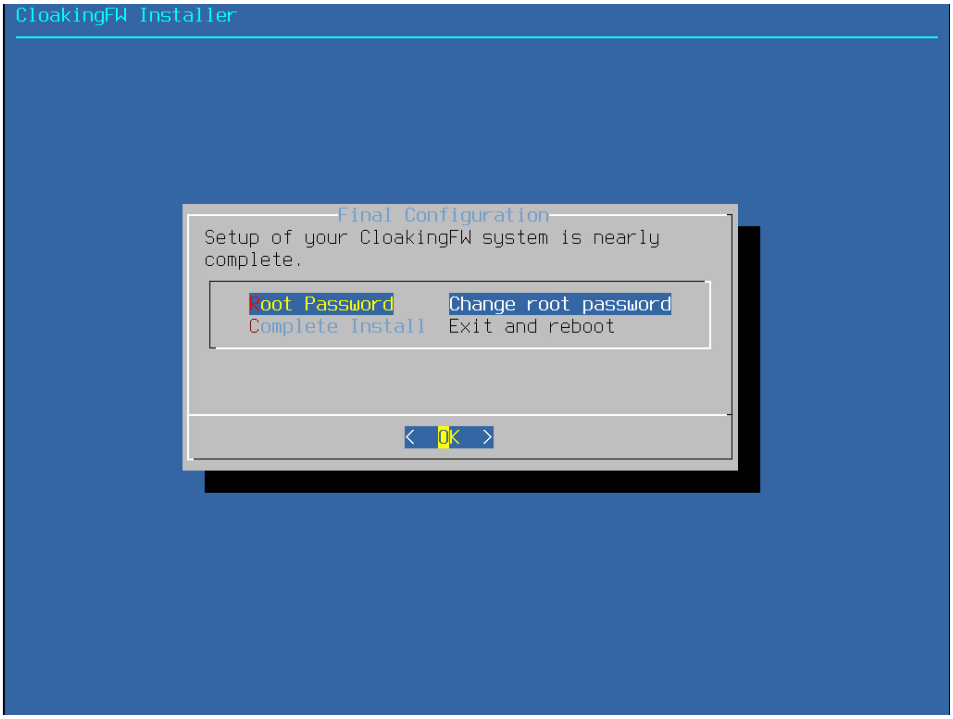


BIOS Installation:

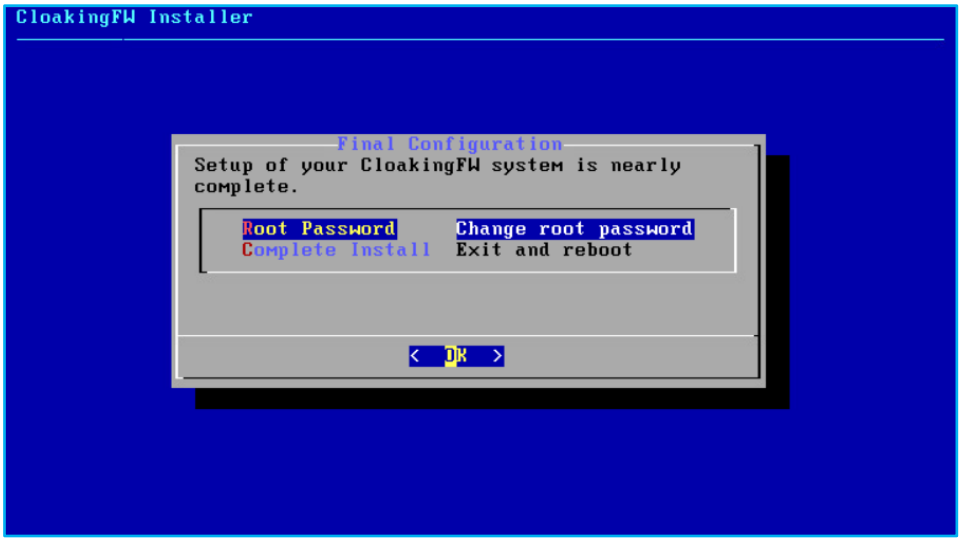


f. At the Final Configuration window, ignore changing the Root Password at this time.

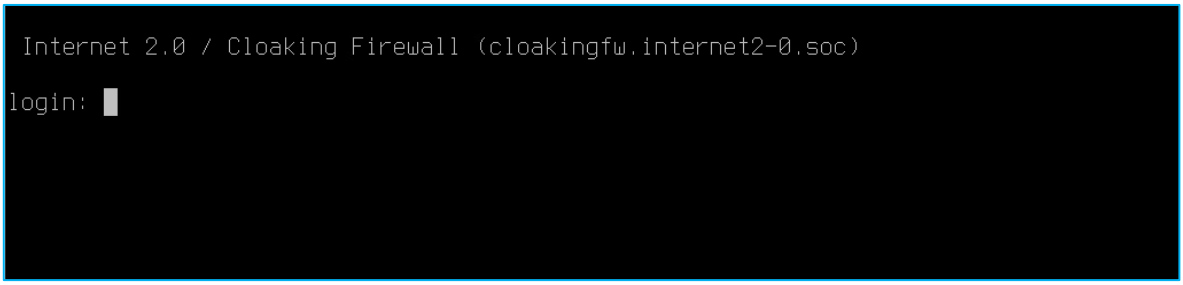
UEFI Installation:



BIOS Installation:



g. To complete the installation, use the down arrow key to select “Complete Install” and then hit enter.
h. The system will reboot.
i. When the system reboots, the bootable media needs to be prevented booting. Check with the BIOS to ensure that the installed drive will be used. Also, will need to eject the Cloaking Firewall ISO media. Some systems will automatically boot to the correct drive.
j. When the bootup has completed, the login prompt will be displayed.

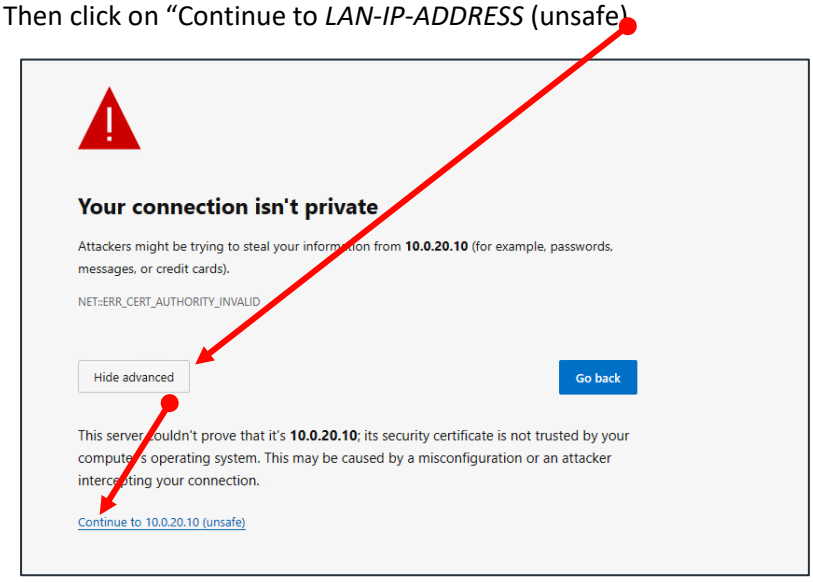


Initial Login with the Cloaking Firewall

Upon initial login to the firewall, users must navigate to the specified management IP address and access the interface through port 2000. This custom port ensures an added layer of security by deviating from the default ports commonly used by other systems.

Note: By Default, the Cloaking Firewall WebGUI uses Port 2000.

1. Using a computer that is on the LAN, open a browser and go to:
    a. https://LAN-IP-ADDRESS:2000
        Where “LAN-IP-ADDRESS” is the IP Address that was used for the LAN.
        Ensure that “:2000” is added to the end of the IP Address.
        For example: https://10.0.20.10:2000
2. The Cloaking Firewall uses a Self-Signed Certificate, so an Exception needs to be made.
    a. For example, if using Microsoft Edge:
        i. Click on Advanced
        ii. Then click on “Continue to *LAN-IP-ADDRESS* (unsafe)



3. The Clocking Firewall WebGUI will be presented.

4. To login:

   Username: root
   Password: internet2-0.com
   Or the Password that was provided during the installation process.

The Initial Dashboard of the Cloaking Firewall

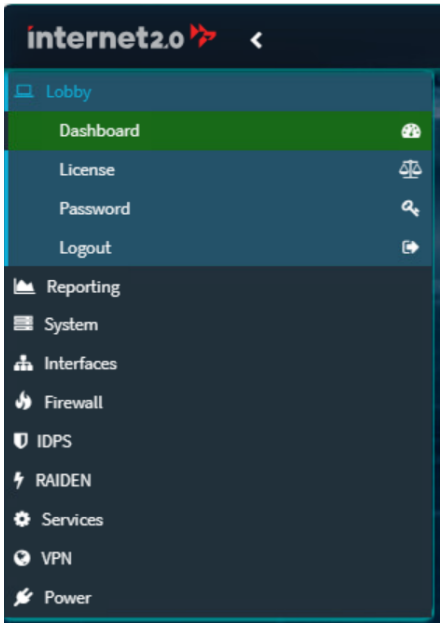
Quick overview of the Dashboard

The Dashboard of the Cloaking Firewall

Menu

The menu on the left hand side allows for the selection of the WebGUI for navigation. Each of the sections of the menu has additional subsections.

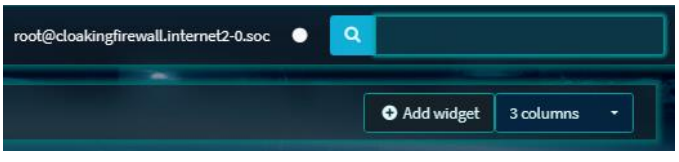
Also, the menu can be minimized by clicking on the white left pointing arrow next to the Internet 2.0 Logo.



Header

The Header contains information of the user account that is logged in along with the hostname and domain of the firewall.

The Search Field allows for quick navigation if to look for certain items.



There are also two buttons to allow for additional dashboard widgets and for less or more columns.

Picture

The picture widget allows for a picture or logo to be applied with the default set for Internet 2.0's logo. Clicking on the pencil icon button will allow for a new picture to be uploaded.

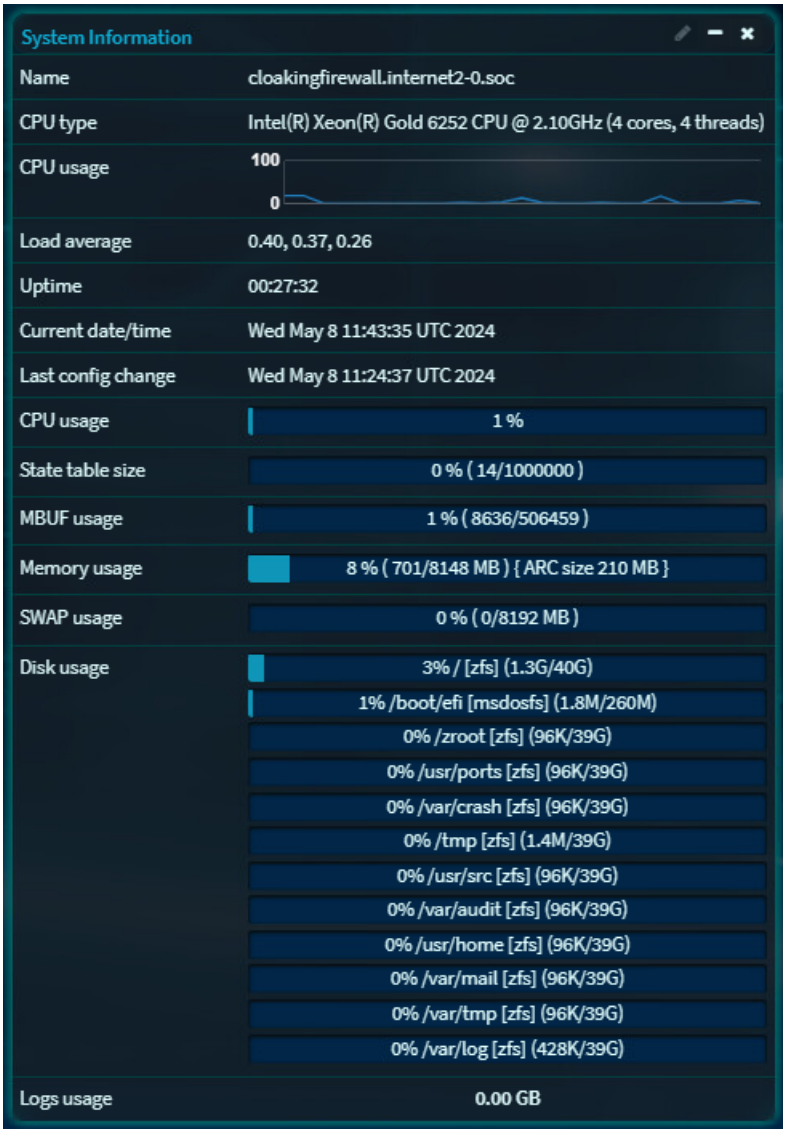
System Information

The System Information widget provides information of the system in terms of the CPU, Uptime, Firewall Tables, Memory, and Storage.

For the Load Average, these are listed in three time sets: of 1 minute, 5 minutes and 15 minutes. Each Whole Number (1.0, 2.0, 3.0, etc) represents a thread of a CPU being used. Load Averages should be less than 80% of all of the CPU threads. For example, in this image of an Intel® Xeon® processor has Four Cores and Four Threads. Therefore, Loading Averages should remain below 3.2. When the CPU is maximized, this will impact the throughput of the firewall, making the experience of the network appear to be running slow. CPU is impacted by the amount of bandwidth and systems, such as the Intrusion Detection Prevention System in use.

Memory is related to the number of rules and systems being put to use. Keep the amount of RAM utilization under 80%.

Disk Usage list the amount of used storage of the disks and partitions. Best to keep the storage under 80%. Should the storage reach 100%, then the firewall will be impacted. There is an automatic module to allow for monitoring and keeping the disk from reach 100% but does so by deleting or purging the logs. This is explained in the Monit section.



To note, that the Dashboard does take up some load of the CPU, especially with the Traffic Graph in use. If there is heavy loading of the CPU, consider relying on use with a System Event & Information Management (SIEM) or a custom dashboard.

Services

This widget displays the listing of services in use and the ability to Start, Restart and Stop.

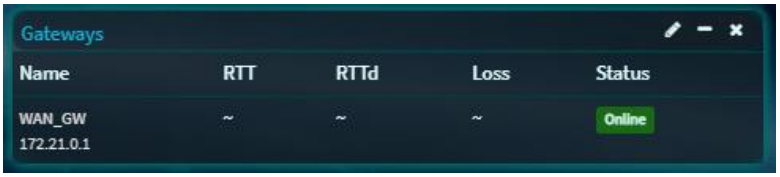
Note: The RAIDEN (raidend) plugin module is currently halted as it is shown with a red Stop. This will be enabled later on during the configuration process.

Firewall Log

This widget displays the events that are occurring with the firewall in terms of traffic being allowed or denied. This can be edited by the pencil icon for preferences. Currently it is set for the WAN interface only for denied events.

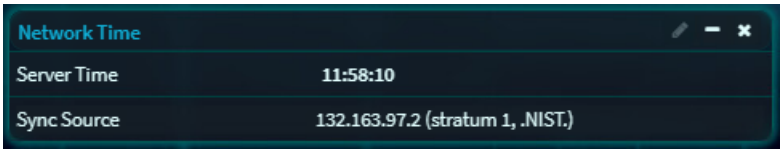
Gateways

This widget shows the statuses of the gateways in use, which is primarily with the WAN interface.



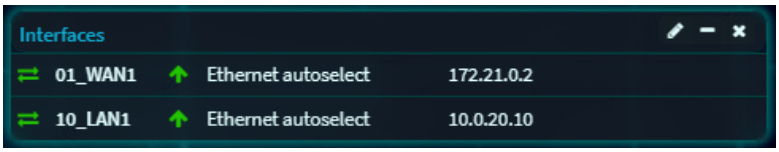
Network Time

The Network Time is useful is providing if the firewall is receiving timing telemetry in order to avoid any potential problems. It is currently set to receive the timing for the US NIST Atomic Clock located at Fort Collins, CO USA. The source of the timing can be changed in Services > Network Time.



Interfaces

This provides the status of the interfaces if running (Up) or Off (Down) and of the IP addresses.



Traffic Graph

The Traffic Graph shows the traffic flowing through the firewall. By default, both the WAN and LAN are displayed with their Inbound and Outbound traffic. This can be useful to see if there is congestion or a lack of traffic.

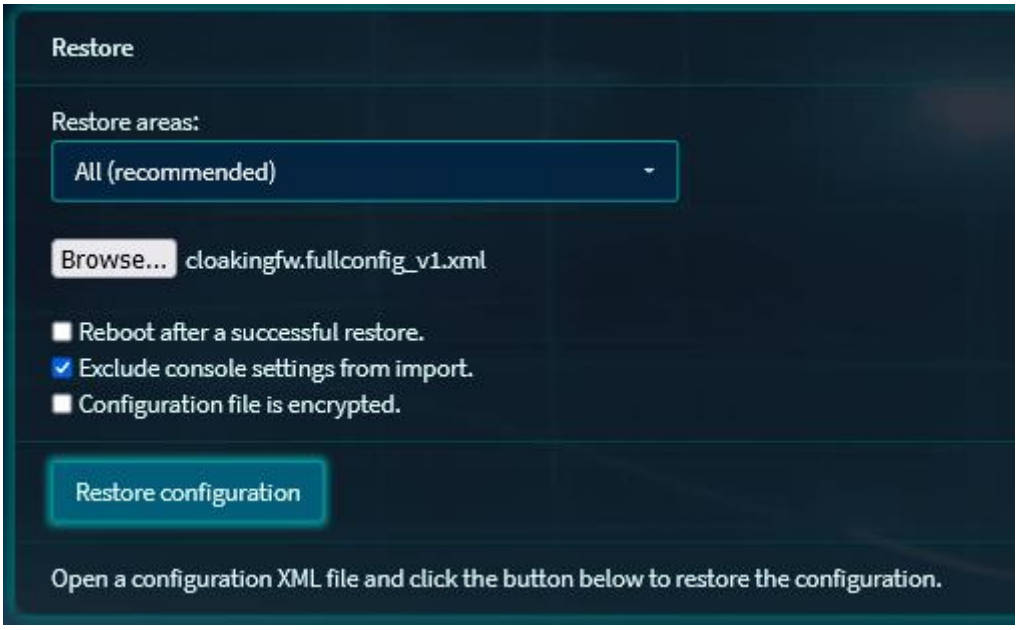
Quick Setup with Provided Configuration File

There is a quick setup process by uploading a provided configuration file (cloakingfw.fullconfig_v1.xml) to provide a streamlined process designed to save significant time in implementation and setup. By utilizing this pre-configured file, administrators can quickly apply all necessary settings, including network interfaces, security policies, and custom configurations, without the need to manually input each parameter. This approach ensures consistency and accuracy, reducing the risk of configuration errors and accelerating the deployment process. The XML file acts as a blueprint, enabling the firewall to be operational with minimal manual intervention, thereby enhancing efficiency and allowing IT professionals to focus on other critical tasks.

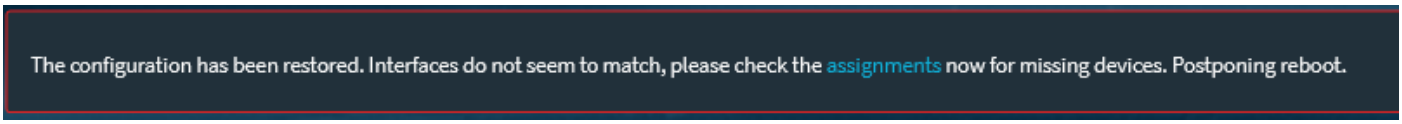
Use these Steps to import the provided configuration file (cloakingfw.fullconfig_v1.xml).

Otherwise if to use the default configuration from the installation, skip to "*Configure Interfaces and Gateway (Default Configuration)*".

1. Go to System > Configuration > Backups
2. At the Restore Section, click on the Browse button.
3. At the popup window, navigate and open the cloakingfw.fullconfig_v1.xml file.
4. Click on Restore configuration button.



5. An error will appear as this is due to having interfaces which are not part of the configuration file. As shown below:



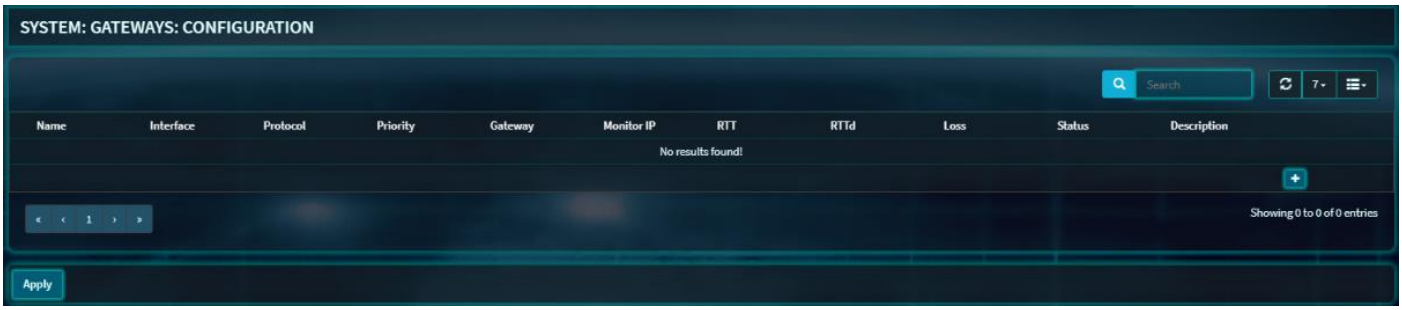
6. Click on the word "assignments" in the error section or Go to Interfaces > Assignments.
7. As was done through the terminal previously, set both the WAN and LAN to the correct Interfaces.

8. Then click on Save

9. Due to the importing of the configuration file, the LAN Interface needs to be reconfigured.
10. Go to Interfaces > 10_LAN1
    a. Lock: Checked
        a. This helps to prevent an accidental removing of the interface.
    b. Description: This can be changed to another term, such as LAN.
    c. Block Private Networks Unchecked (Default)
    d. Block Bogons Checked
    e. IPv4 Configuration: Static IPv4
    f. IPv6 Configuration: None (Default)
    g. IPv4 Address: Enter in the IP and Subnet that was used at the Terminal.
    h. IPv4 Upstream Gateway: Normally is not needed for a LAN.
    i. Click on Save
    j. Click on the Apply Changes button at the top right.

Configure Gateway and WAN Interface

Configuring the interfaces and gateway in the Cloaking Firewall is a foundational step in setting up the system's network structure. This process involves assigning IP addresses to each network interface and defining the default gateway, which directs outbound traffic to the appropriate external network. Proper configuration ensures efficient and secure routing of both inbound and outbound network traffic, aligning with specific network policies and security protocols.



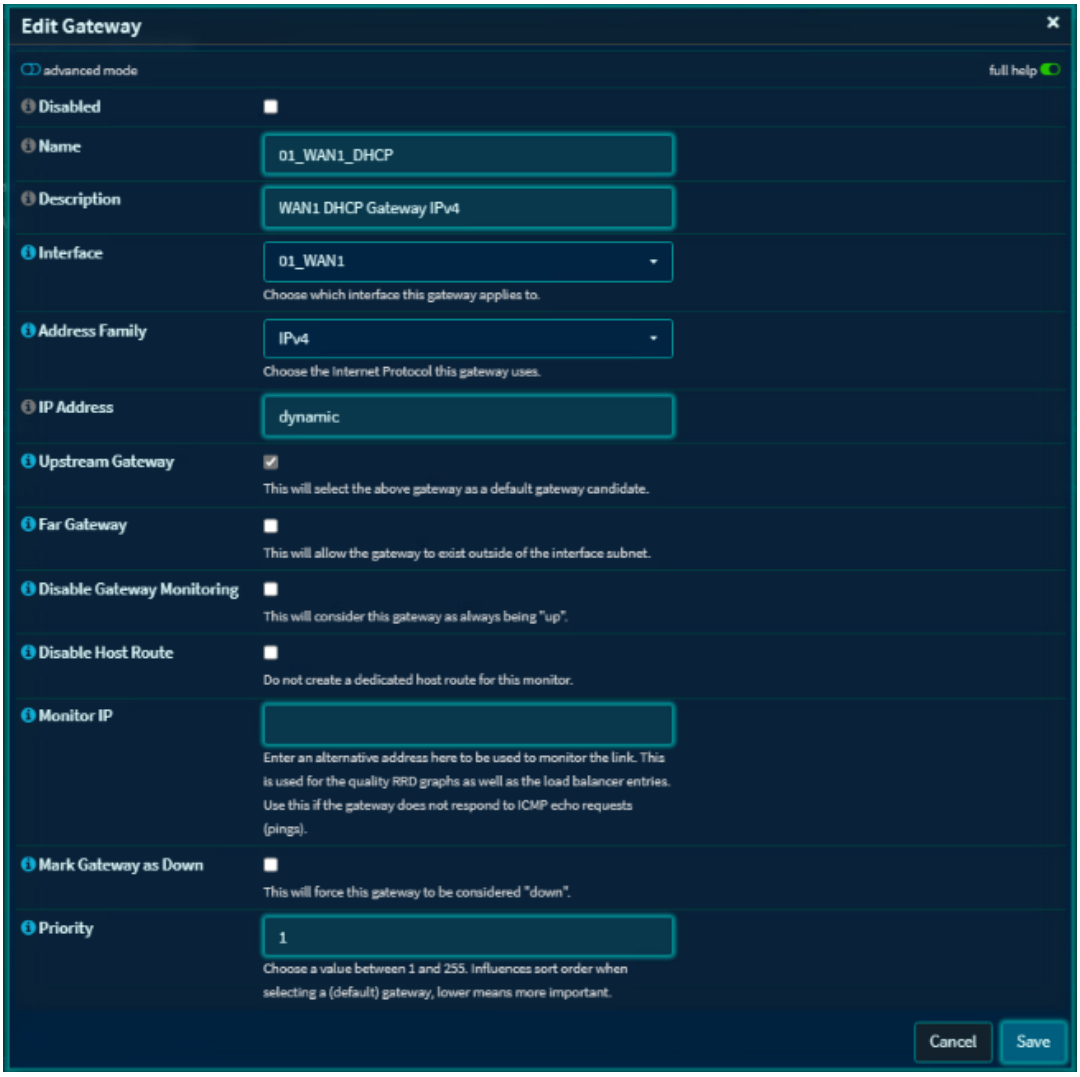
1. Go to System > Gateways > Configuration
2. If DHCP (IPv4) is to be used, proceed with the following steps, otherwise skip to Step 3:
    a. Click the Plus “+” to add a new WAN Gateway.
        i. Name: 01_WAN1_DHCP
        ii. Description: WAN1 DHCP Gateway IPv4
        iii. Interface: 01_WAN1
        iv. Address Family: IPv4
        v. IP Address: The IP Address of the Gateway
        vi. Upstream Gateway: Checked
        vii. To enable Monitoring of the Gateway:

1. Disable Gateway Monitoring: Unchecked
2. Monitor IP if left blank will check with the Gateway's IP be default. If another source is to be used, then enter it here.

viii. Set the Priority to the Highest, this being 1 (255 is the lowest).
1. Priority: 1

ix. Click on Save

b. Click on Apply



3. If using a Static IP Address, then:

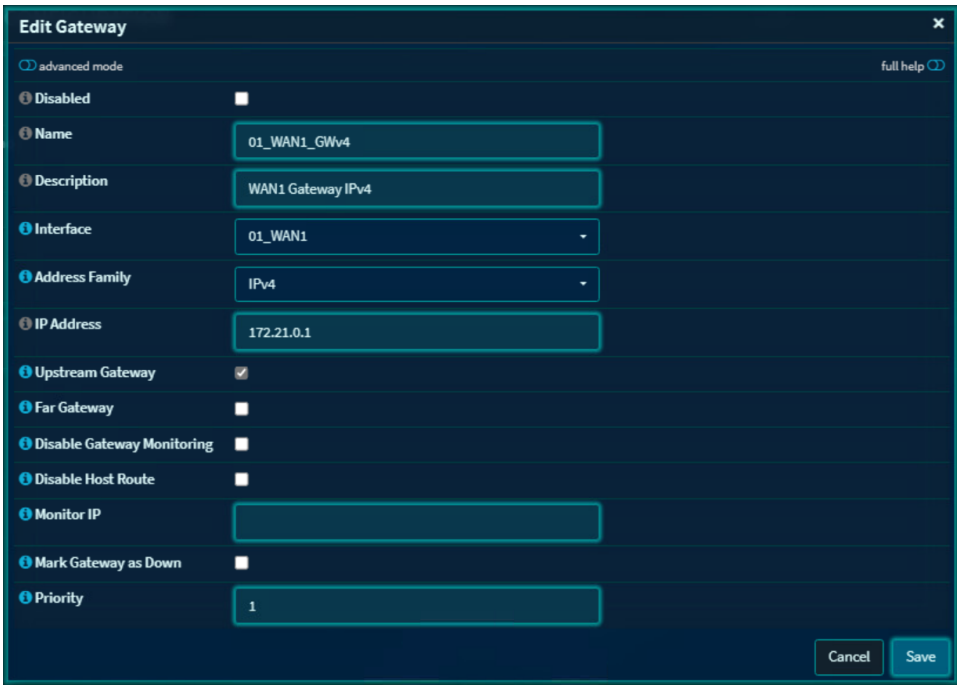
c. Add a New Gateway, by clicking on the Plus "+" button.

i. Name: 01_WAN1_GWv4
ii. Description: WAN1 Gateway IPv4
iii. Interface: 01_WAN1
iv. Address Family: IPv4
v. IP Address: The IP Address of the Gateway
vi. Upstream Gateway: Checked
vii. Disable Gateway Monitoring: Unchecked
1. Monitor IP if left blank will check with the Gateway's IP be default. If another source is to be used, then enter it here.

viii. Set the Priority to the Highest, this being 1 (255 is the lowest).
1. Priority: 1

ix. Click on Save

d. Click on Apply



e. To refresh the page, click on the two circling circles at the top right section.

f. There will be two Gateways shown at this time.

4. Go to Interfaces > 01_WAN1

a. Lock: Checked
   a. This helps to prevent an accidental removing of the interface.

b. Description: This can be changed to another term, such as WAN.

c. Block Private Networks Checked (Default)

d. Block Bogons Checked (Default)

e. IPv4 Configuration:

f. If to use DHCP: DHCP
   a. If to use a static IP Address: Static IPv4
   b. IPv6 Configuration: None (Default)

g. If using a Static IP Address:
   a. IPv4 Address: Enter in a new IP Address and Subnet if Static IP is used.
   b. IPv4 Upstream Gateway: Change to the DHCP or to 01_WAN1_GWv4.

h. Click on Save if any changes were made, such as checking for Lock.

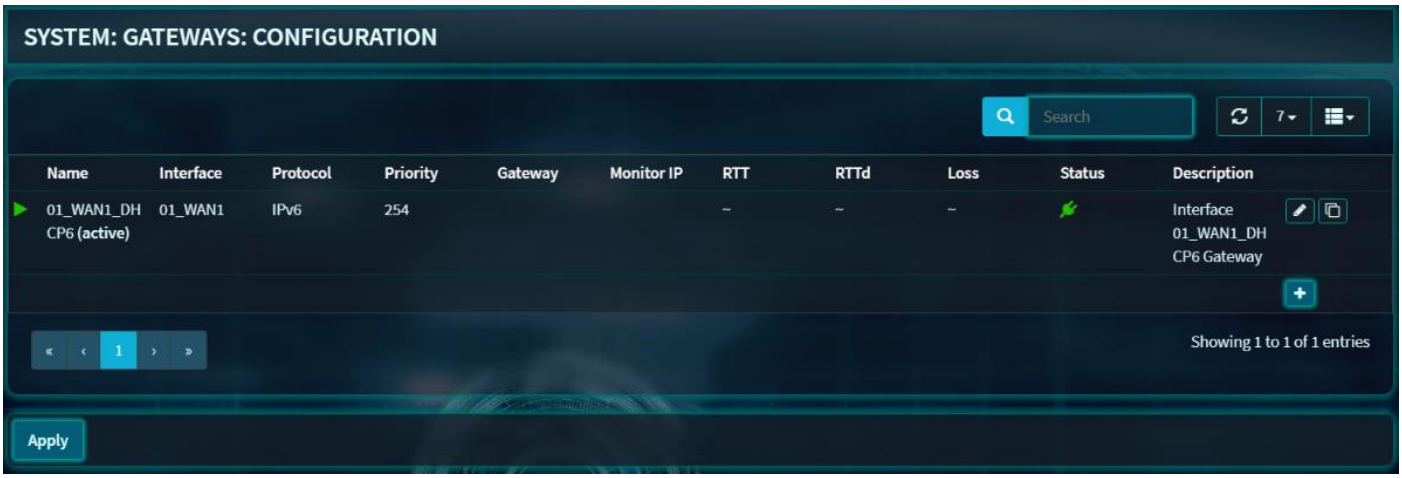
i. Click on the Apply Changes button at the top right corner.
   a. Note, there may be a delay as the WAN is changed.

5. Reboot the Cloaking Firewall, by going to Power > Reboot
6. Click on Yes to proceed with the Reboot

Log into the Cloaking Firewall and proceed to, "*Perform Updates*".

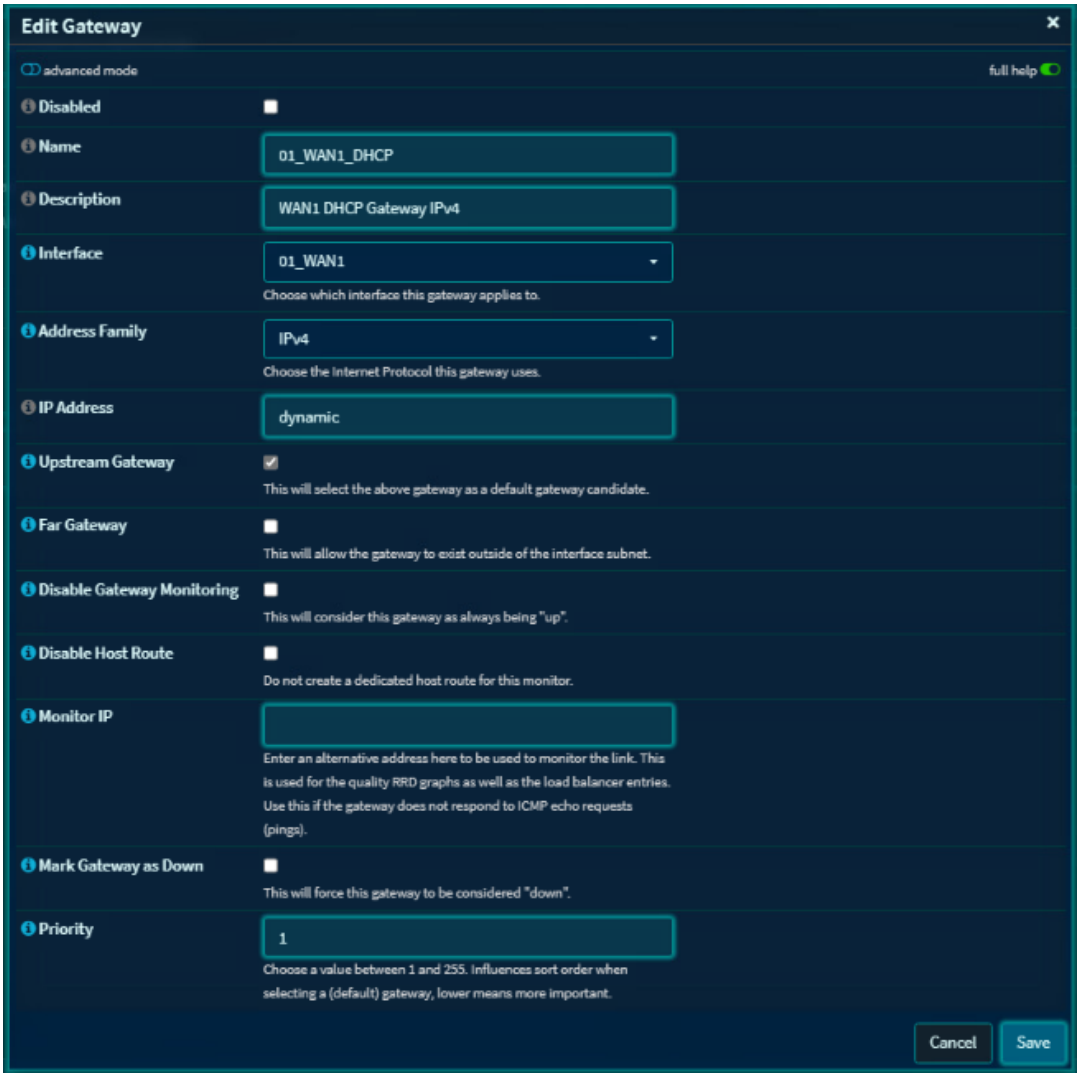
Configure Interfaces and Gateway (Default Configuration)

Configuring the interfaces and gateway in the Cloaking Firewall is a foundational step in setting up the system's network structure. This process involves assigning IP addresses to each network interface and defining the default gateway, which directs outbound traffic to the appropriate external network. Proper configuration ensures efficient and secure routing of both inbound and outbound network traffic, aligning with specific network policies and security protocols.

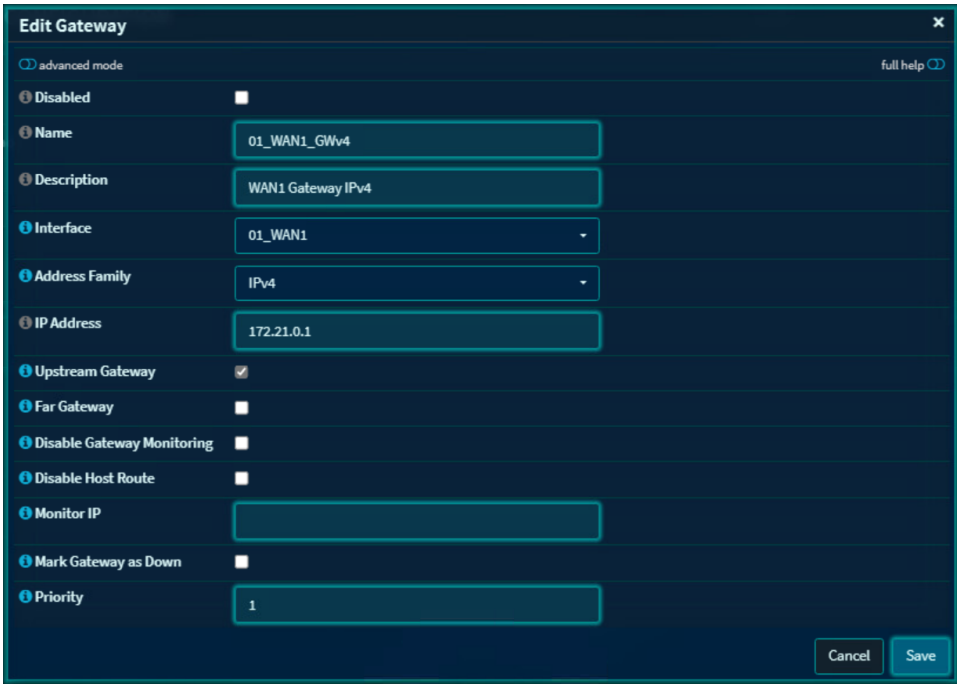


7. Go to System > Gateways > Configuration
8. If DHCP6 is being used and no IPv4 (or DHCP), then perform the following steps, otherwise skip to Step 3:
    g. Click to edit the WAN Gateway (01WAN1_DHCP6) by clicking on the pencil icon.
        i. Upstream Gateway: Checked
        ii. To enable Monitoring of the Gateway:
            1. Disable Gateway Monitoring: Unchecked
            2. Monitor IP if left blank will check with the Gateway's IP be default. If another source is to be used, then enter it here.
        iii. Set the Priority to the Highest, this being 1 (255 is the lowest).
            1. Priority: 1
        iv. Click on Save
    h. Click on Apply

9. If DHCP (IPv4) is to be used (with no DHCP6), proceed with the following steps, otherwise skip to Step 4:
    i. Click the Plus "+" to add a new WAN Gateway.
        i. Name: 01_WAN1_GWv4
        ii. Description: WAN1 DHCP Gateway IPv4
        iii. Interface: 01_WAN1
        iv. Address Family: IPv4
        v. IP Address: The IP Address of the Gateway
        vi. Upstream Gateway: Checked
        vii.
        viii. To enable Monitoring of the Gateway:
            1. Disable Gateway Monitoring: Unchecked
            2. Monitor IP if left blank will check with the Gateway's IP be default. If another source is to be used, then enter it here.
        ix. Set the Priority to the Highest, this being 1 (255 is the lowest).
            1. Priority: 1
        x. Click on Save
    j. Click on Apply



10. If using a Static IP Address, then:
    k. Add a New Gateway, by clicking on the Plus “+” button.
        i. Name: 01_WAN1_GWv4
        ii. Description: WAN1 Gateway IPv4
        iii. Interface: 01_WAN1
        iv. Address Family: IPv4
        v. IP Address: The IP Address of the Gateway
        vi. Upstream Gateway: Checked
        vii. Disable Gateway Monitoring: Unchecked
            1. Monitor IP if left blank will check with the Gateway’s IP be default. If another source is to be used, then enter it here.
        viii. Set the Priority to the Highest, this being 1 (255 is the lowest).
            1. Priority: 1
        ix. Click on Save
    l. Click on Apply



m. To refresh the page, click on the two circling circles at the top right section.

n. There will be two Gateways shown at this time.

11. Go to Interfaces > 01_WAN1

j. Lock: Checked
   a. This helps to prevent an accidental removing of the interface.

k. Description: This can be changed to another term, such as WAN.

l. Block Private Networks Checked (Default)

m. Block Bogons Checked (Default)

n. IPv4 Configuration: DHCP (Default)
   a. If to use a static IP Address: Static IPv4

o. IPv6 Configuration: DHCPv6 (Default)
   a. If not to use DHCPv6: None

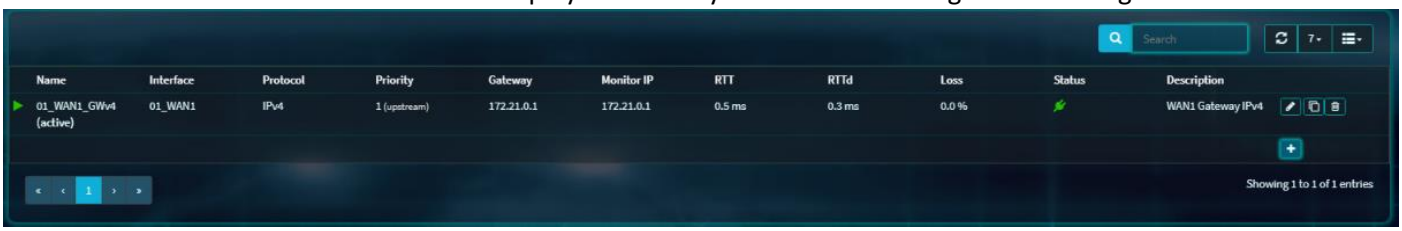
p. If using a Static IP Address:
   a. IPv4 Address: Enter in a new IP Address and Subnet if Static IP is used.
   b. IPv4 Upstream Gateway: Change to the DHCP or to 01_WAN1_GWv4.

q. Click on Save if any changes were made, such as checking for Lock.
r. Click on the Apply Changes button at the top right corner.
    a. Note, there may be a delay as the WAN is changed.

12. Go to Interfaces > 10_LAN1
    k. Lock: Checked
        a. This helps to prevent an accidental removing of the interface.
    l. Description: This can be changed to another term, such as LAN.
    m. Block Private Networks Unchecked (Default)
    n. Block Bogons Checked (Default)
    o. IPv4 Configuration: Static IPv4 (Default)
    p. IPv6 Configuration: None (Default)
    q. IPv4 Address: Enter in a new IP Address and Subnet if needed.
    r. IPv4 Upstream Gateway: Normally is not needed for a LAN.
    s. Click on Save if any changes were made, such as checking for Lock.
    t. Click on the Apply Changes button at the top right.

Verify the Gateways

13. Go to System > Gateways > Configuration
14. There should now be the correct display of Gateways and also indicating of monitoring.

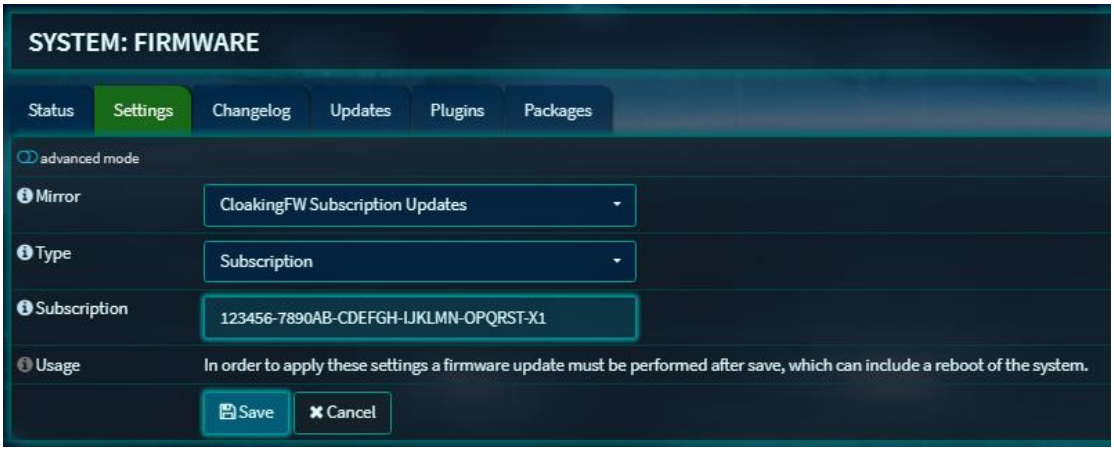


Perform Updates

To access the latest updates and additional configurations for the Cloaking Firewall, users must first enter their subscription key. This key unlocks the ability to download and install updates and plugins that enhance the firewall's functionality and security features.

Regularly performing updates and installing plugins on the Cloaking Firewall is essential to maintain its effectiveness and security. Updates ensure that the firewall is equipped with the latest security patches, performance improvements, and bug fixes, minimizing vulnerabilities and enhancing overall stability. Additionally, plugins extend the functionality of the firewall, allowing for customized features such as advanced reporting, additional security protocols, or enhanced network management tools. This process typically involves accessing the firewall's management interface, selecting available updates or desired plugins, and applying them with minimal downtime. Keeping the firewall updated and utilizing relevant plugins helps in adapting to evolving security threats and meeting the specific needs of the network environment

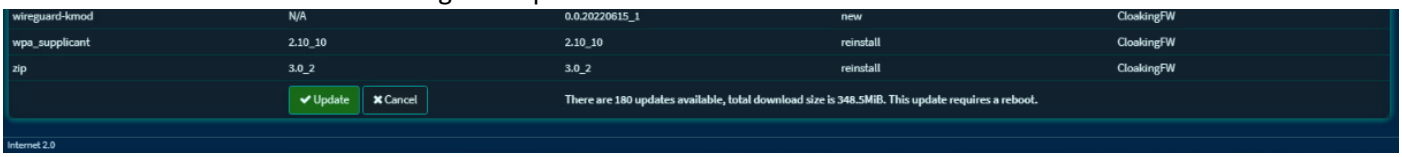
1. Go to System > Firmware > Status
2. Click on the Settings Tab
3. Make the following changes:
    a. Mirror: CloakingFWSubscription Updates
    b. Type: Subscription
    c. Subscription: Type or paste in the Subscription License.
4. Click on Save



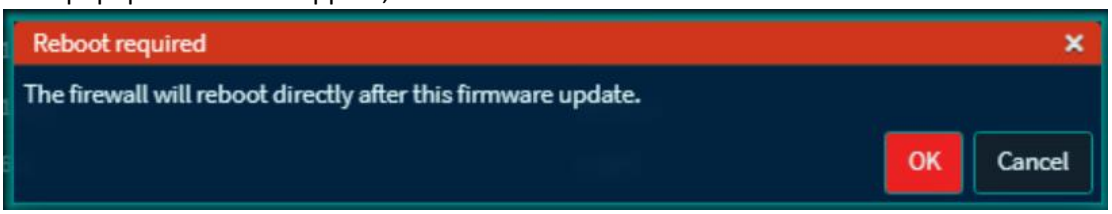
5. Click on the Status Tab

6. Check for Updates by clicking on Check for Updates
7. There will be a listing of the systems that will be updated:

8. Scroll down and click on the green Update Button



9. A reboot popup window will appear, click on OK



10. When the update has finished, there will be another popup window indicating that the firewall will be rebooting. You may observe the boot up process from the existing terminal or wait until the WebGUI Login Screen appears.

11. There is no need to repeat the update process.

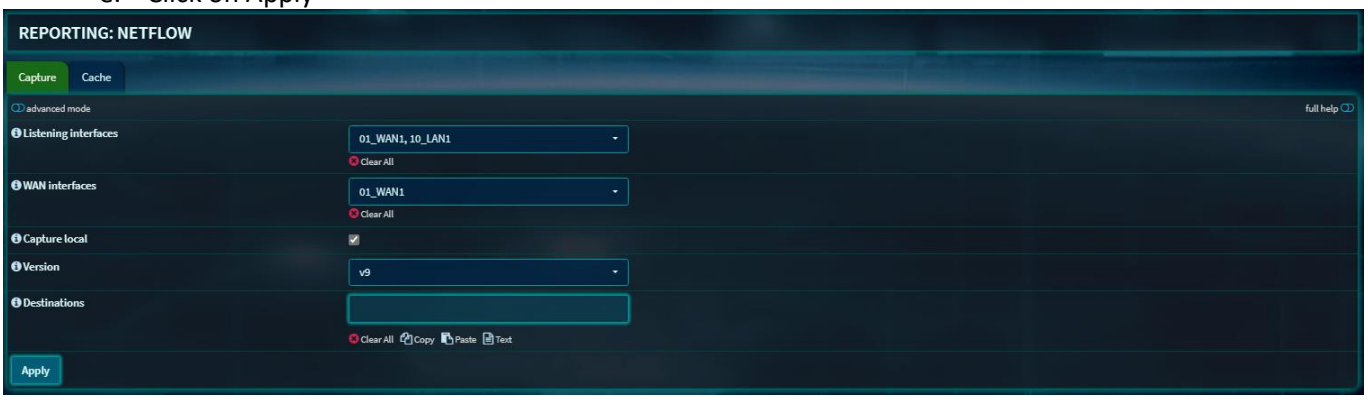
Configuring the Systems of the Cloaking Firewall

Configuring the Cloaking Firewall involves a comprehensive setup process that ensures all components are tailored to meet the specific security needs of the network. After the basic installation and initial bootup, administrators are guided through a series of steps to configure network interfaces, set routing tables, and establish core settings such as IP blocking and firewall rules. Advanced configurations involve setting up Intrusion Detection and Prevention Systems (IDPS) like Suricata, optimizing network performance through tunables, and implementing robust security measures including VPN setups and multi-factor authentication. Each step is crucial in reinforcing the firewall's capabilities to not only manage and monitor traffic efficiently but also to actively prevent unauthorized access and mitigate potential threats. The process is meticulous to ensure that the firewall operates as a dynamic shield, enhancing overall network security while maintaining optimal performance.

Reporting Settings

The Reporting section of the firewall provides a comprehensive suite of tools for monitoring and analyzing network performance and security. The Health module offers real-time statistics and historical data on system performance, including CPU usage, memory utilization, and interface traffic. Insight delivers detailed visibility into traffic patterns and bandwidth usage, helping administrators identify trends and potential issues. Netflow provides granular analysis of network flows, enabling the tracking of individual connections and the detection of anomalies. Additionally, the Unbound DNS monitoring tool ensures that DNS queries and responses are functioning optimally, providing critical insights into DNS performance and potential security threats. These tools collectively enhance the ability to maintain a robust and secure network environment.

1. Netflow Reporting Settings:
    a. Go to Reporting > Netflow
    b. Listening Devices: 01_WAN1, 11_LAN1
    c. WAN Interfaces: 01_WAN1
    d. Capture Local: Checked
    e. Click on Apply



2. After any installation, it is best to reset the RND and Reporting Database. Also, this is good to do so after performing updates.
    a. Go to Reporting > Settings
    b. Unbound DNS Reporting:
        i. Click on Reset DNS data button
        ii. Click on Yes from the popup window.
    c. Reporting Database Options:
        i. Click on Rest RRD Data button
        ii. Click on Yes from the popup window.
        iii. Click on Reset Netflow Data button
        iv. Click on Yes from the popup window.

Create Server Certificate Authorities and Certificates (SSL)

Although purchasing certificates from certified Certificate Authorities (CA) is preferred, this is not always the case, and Self-Signed Certificates are still possible to use, such as within private and trusted networks. This process is to create two sets of internal Certificate Authorities, one for private use and another for public use if there are webservers to protect with Nginx.

1. Go to System > Trust > Authorities

Internal Private CA

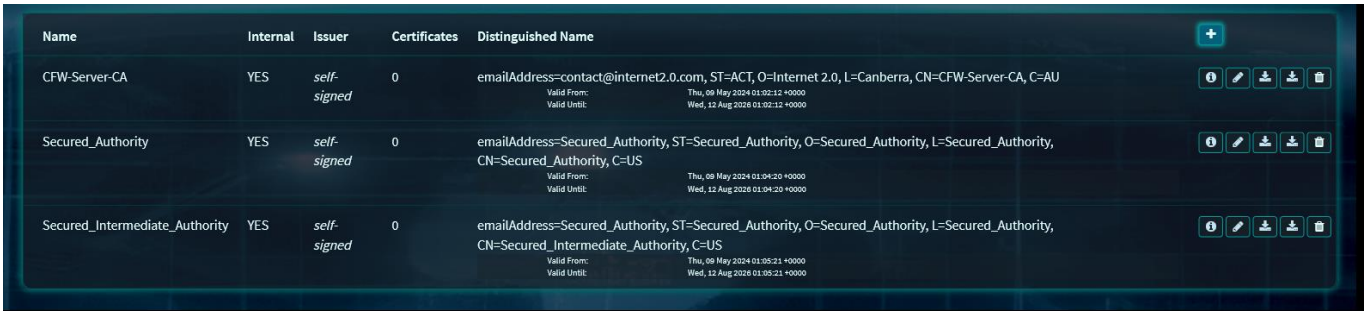
2. Create a Private Certificate Authority
   a. Click on the Add Button
   b. Descriptive Name: CFW-Server-CA
   c. Method: Create an internal Certificate Authority
   d. Key Type: RSA
   e. Key Lengths: 4096
   f. Digest Algo: SHA512
   g. Lifetime (days): 825
   h. Country Code: Select the country (Ex: Australia)
   i. State: Type in the State (Ex: ACT)
   j. City: Type in the City (Ex: Canberra)
   k. Organization: The name of the organization (Ex: Internet 2.0)
   l. Email Address: Type in the Email Address (Ex: contact@internet2-0.com
   m. Common Name: CFW-Server-CA
   n. Click on Save

Public CAs

3. Create a Public Certificate Authority
   a. Click on the Add Button
   b. Descriptive Name: Secured_Authority
   c. Method: Create an internal Certificate Authority
   d. Key Type: RSA
   e. Key Lengths: 4096
   f. Digest Algo: SHA512
   g. Lifetime (days): 825
   h. Country Code: Select a Country
   i. State: Secured_Authority
   j. City: Secured_Authority
   k. Organization: Secured_Authority
   l. Email Address: Secured_Authority
   m. Common Name: Secured_Authority
   n. Click on Save

4. Create a Public Intermediate Certificate Authority
   o. Click on the Add Button
   p. Descriptive Name: Secured_Intermediate_Authority
   q. Method: Create an intermediate Certificate Authority
   r. Key Type: RSA
   s. Key Lengths: 4096

t. Digest Algo: SHA512
u. Lifetime (days): 825
v. Country Code: US
w. State: Secured_Authority
x. City: Secured_Authority
y. Organization: Secured_Authority
z. Email Address: Secured_Authority
aa. Common Name: Secured_Intermediate_Authority
bb. Click on Save



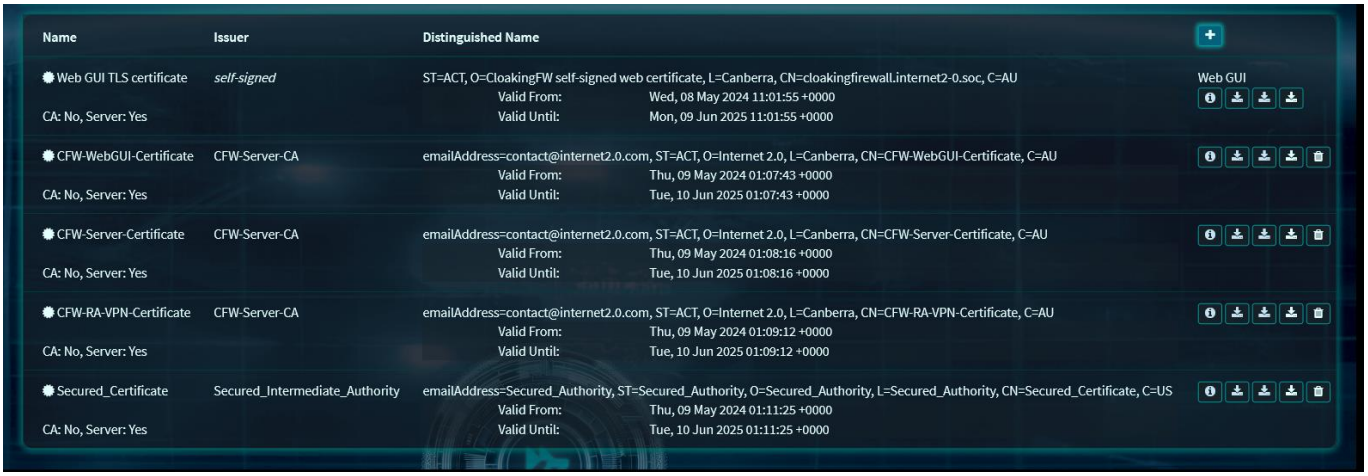
Create Certificates

1. Create a Certificate for the WebGUI
   a. Go to System > Trust > Certificates
   b. Click on the Add button
   c. Method: Create an internal Certificate
   d. Descriptive Name: CFW-WebGUI-Certificate
   e. Certificate Authority: CFW-Server-CA
   f. Type: Server Certificate
   g. Key Type: RSA
   h. Key Length: 4096
   i. Digest Algo: SHA512
   j. Lifetime: 397
   k. Private key location: Save on this firewall
   l. Common Name: CFW-WebGUI-Certificate
   m. Click on Save

2. Create a Certificate for General Server connections:
   a. Click on the Add button
   b. Method: Create an internal Certificate
   c. Descriptive Name: CFW-Server-Certificate
   d. Certificate Authority: CFW-Server-CA
   e. Type: Server Certificate
   f. Key Type: RSA
   g. Key Length: 4096
   h. Digest Algo: SHA512
   i. Lifetime: 397
   j. Private key location: Save on this firewall
   k. Common Name: i20-Server-Certificate
   l. Click on Save

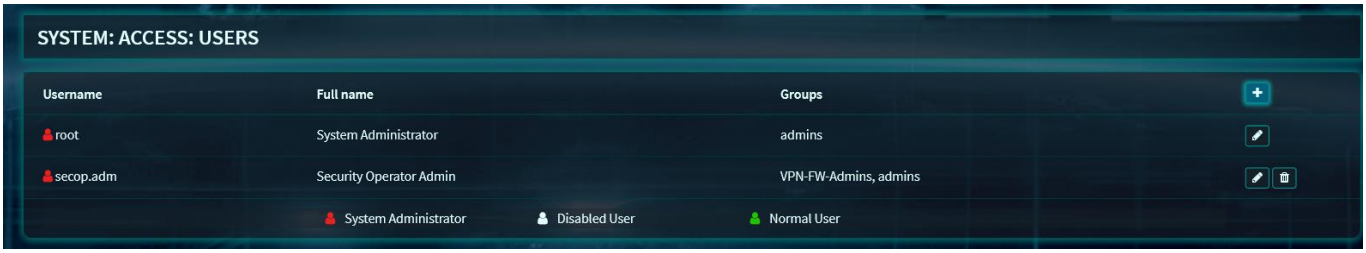
3. Create a Certificate for Remote Access to the Server (for use with VPNs)
   a. Click on the Add button
   b. Method: Create an internal Certificate
   c. Descriptive Name: CFW-RA-VPN-Certificate
   d. Certificate Authority: CFW-Server-CA
   e. Type: Server Certificate
   f. Key Type: RSA
   g. Key Length: 4096
   h. Digest Algo: SHA512
   i. Lifetime: 397
   j. Private key location: Save on this firewall
   k. Common Name: CFW-RA-VPN-Certificate
   l. Click on Save

4. Create a Certificate for Public Access:
   This is only needed if remote systems are to be accessible by external parties. Such as a Webserver that allows access from the Internet.
   a. Click on the Add button
   b. Method: Create an internal Certificate
   c. Descriptive Name: Secured_Certificate
   d. Certificate Authority: Secured_Intermediate_Authority
   e. Type: Server Certificate
   f. Key Type: RSA
   g. Key Length: 4096
   h. Digest Algo: SHA512
   i. Lifetime: 397
   j. Private key location: Save on this firewall
   k. Common Name: Secured_Certificate
   l. Click on Save



User Accounts: Change Passwords

1. Go to System > Access > Users



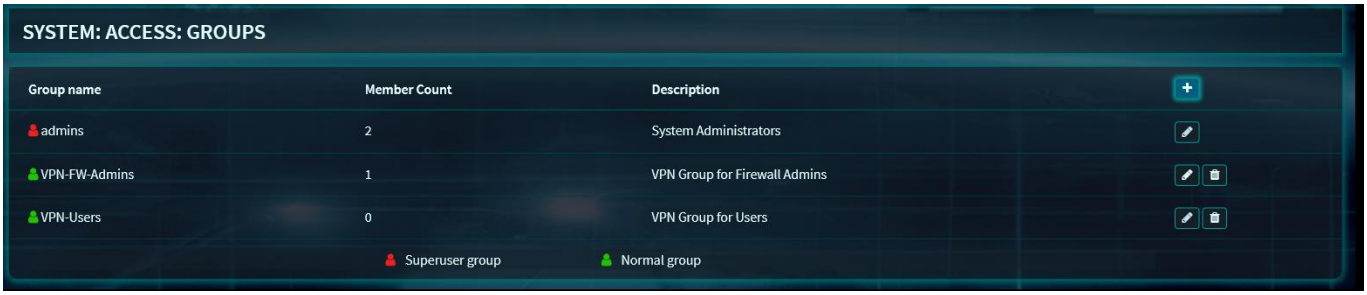
There are two user accounts, but with Administrative Privileges:

- Root: This account has full access to the WebGUI, SSH (by Default) and the Terminal. The Root account should be used sparingly, with the Secop.adm account to be preferred for use. By default, the Roo account is only in the Admin group.
- Secop.adm: Similar to the Root Account but does not have access to the Terminal. This account is to be used for remote access as it is part of the VPN-FW-Admins group.

2. Changing of Passwords for the accounts. Skip this step for Root if the password has already been changed.
3. Click on the pencil to Edit the Root account.
    a. Password: Set password to given standards (x2)
    b. E-Mail: Type in the email to use as a reference.
    c. Comment: Enter in a comment such as:
    This is the Root Account that has full access to the Firewall, including via Terminal. Please use another administrator account.
4. Click on Save and go back
5. Click on the pencil to Edit the Secop.adm account.
    a. Password: Set password to given standards (x2)
    b. E-Mail: Type in the email to use as a reference.
    c. Comment: Enter in a comment such as:
    This is the Root Account that has full access to the Firewall and to be used for Remote Access via VPN.
6. Scroll down and click on Save.
7. Then go to the User Certificates section.
8. Click to Add a User Certificate
    a. Method: Create an internal Certificate
    b. Descriptive Name: secop.adm
    The Descriptive Name must be the same as the Username
    c. Certificate Authority: CFW-Server-CA
    d. Type: Client Certificate
    e. Key Type: RSA
    f. Key Length: 4096
    g. Digest Algorithm: SHA512
    h. Lifetime: 397
    i. Private key location: Save on this firewall
    j. Common Name: secop.adm
    k. Click on Save
9. Click on Save and go back

User Groups

1. Go to System > Access > Groups

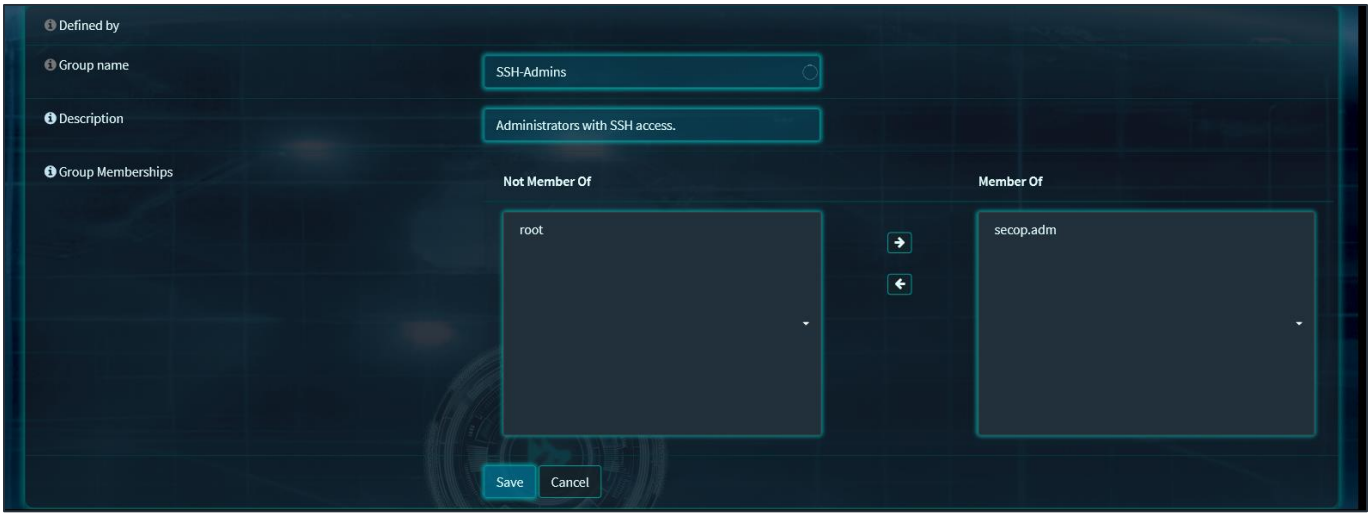


There are three User Groups by default and are to be used for the following purposes:

- Admins: User accounts within this group have full administration capabilities with the firewall. By default, Root and Secop.adm are in this group.
- VPN-FW-Admins: This group is for user accounts to allow for remote administration access when using the VPN.
- VPN-Users: This group is similar to the one above but is for regular users to access the local networks and systems, not the firewall. Thus, a user in this group can use the VPN to access a database server that is in the LAN.

2. There is no group for SSH specifically, so instead of allowing only Admins to access SSH, a group can be used to limit which accounts can use SSH to access the firewall. This will be useful for not allowing Root to use SSH, thus providing better restrictions. These steps will help to create a group and to assign a user account to it, this being for Secop.adm.

3. Click on the Add "+" button to create a new group
   a. Group Name: Type in a name, such as SSH-Admins
   b. Description: Type in a Description, for example, Administrators with SSH access.
   c. Add "secop.adm" to the Member Of section:
      i. By selecting secop.adm, and then click on the Right Arrow
   d. Click on Save



Administration Settings

The Administration settings of the firewall allow users to manage access controls and system preferences. This includes configuring administrative access, setting up multi-factor authentication for enhanced security and these settings also provide options for customizing the web interface and setting up secure connections for remote management.

1. Go to System > Settings > Administration
2. Make the changes to the following settings:
    a. SSL Certificate: CFW-WebGUI-Certificate
    b. HTTP Strict Transport Security: Checked (By Default)
    c. TCP Port: 2000 (By Default)
    This can be changed but recommend avoiding using common ports such as 443.
    d. HTTP Redirect: Checked (By Default)
    e. Session Timeout: 15 (By Default)
    f. Listen Interfaces: All (By Default)
    Recommend changing this to 11_LAN1 interface to avoid exposing access to the WAN. This is set to Any only for the purpose of installation to avoid potential lockouts. If to use the VPN, then set this to the LAN interface.
    g. HTTP_REFERER Enforcement: Checked (By Default)
    This is only needed to access the Firewall if there is another device or system that is in between the remote accessing machine and the firewall. For example, if the Cloaking Firewall is installed in a cloud environment and is to be accessed from its WAN, then this setting will need to be Checked.
    If accessing this firewall from the LAN or by the VPN (which connects to the LAN interface) then this setting can be unchecked.
    h. Secure Shell section:
        i. Secure Shell Server: Unchecked (By Default)
        If SSH is to be used, then this is to Checked.
        Firewall Rules can be used to allow for restrictions with if SSH is to be enabled.
        ii. Login Group: wheel, admins (By Default)
        Change to the new SSH Admin group that was created.
        Ex: wheel, SSH-Admins
        iii. Root Login: Checked (By Default)
        Recommend unchecking to prevent the Root account being used from SSH access, as there is the Secop.adm account available.
        iv. Authentication Method: Checked (By Default)
        v. Listen Interfaces: All (By Default)
        Recommend changing this to 11_LAN1 interface to avoid exposing access to the WAN. This is set to Any only for the purpose of installation to avoid potential lockouts. If to use the VPN, then set this to the LAN interface.

i. Shell section:
    i. Inactivity Timeout: 15 (By Default)
2. Click on Save
3. Open up a new tab (or click on the link) to go the IP and Port (2000 or a new one if used) address.

Delete the original WebGUI Certificate.

4. Go to System > Trust > Certificates
    a. Delete the default Web GUI TLS certificate(s)
    b. Click on the Yes button in the pop-up window.

Cron Tasks

The term Cron refers to time in Greek and as such, is used to schedule tasks. For here, is to set the scheduling for the firewall to check for connectivity with the WAN interface. These tasks will check for a connection, and if there is no connection within a given time frame, will reset the WAN interface in an attempt to restore the connection.

These tasks require connectivity to the Internet, particularly with Google DNS and Cloudflare DNS servers. If there is no internet connection or that such a connection is not to be used (example: isolated networks or organizational policies) then do not enable these tasks.

Set CRON Jobs for the WAN to conduct PING Checks, and if there is a failure, attempts will be made by resetting the WAN interface to make a new connection.

1. Go to System > Settings > Cron
2. If using DHCP, then click on the empty box in the Enabled column. Then click on Apply.
3. If using a static IP address, then click on the empty box in the Enabled column. Then click on Apply. Note, only use one of the two and not both.
4. The tasks can be edited, by clicking on the pencil button of the particular task, such as for DHCP:
    a. Enter in the following information (run every 2 minutes):

Enabled:	**Checked**
Minutes:	*/2
Hours:	*
Days of Month:	*
Months:	*
Days of Week:	*
Command:	w1dhcp_check
Parameters:	Leave Blank
Description:	WAN1 DHCP Ping Check

    b. Click on Save
5. For Static IP Address, Click on the copy button of the above CRON Job

Enabled:	**Checked**
Minutes:	*/2
Hours:	*
Days of Month:	*
Months:	*
Days of Week:	*
Command:	w1ping_check
Parameters:	Leave Blank
Description:	WAN1 Static Ping Check

    a. Click on Save
6. Click on Apply

General Settings

The General Settings contains the basic information for the Cloaking Firewall such as the Hostname, Domain, and other forms.

1. Go to System > Settings > General
    a. Hostname: Change the name of the firewall to your organization's naming convention or designated system name.
    b. Domain: Change the domain name of the firewall to the organization's domain.
    c. Time zone: ETC/UTC (By Default)
    d. Language: English (By Default)
    e. Prefer IPv4 over IPv6: Checked
    f. DNS Entries: If the Cloaking Firewall is not to provide DNS services, but act as a client, then enter in the IP Address of the DNS server.
    If the Cloaking Firewall is to be a DNS server, then leave all Blank.
    If the gateway is listed here, clear the field.
    g. DNS server options: Checked
    h. Click on Save

Logging Settings

These settings help to reduce the amount of storage that will be consumed by logs. This depends on the storage size in use, particularly small storages such as 30GB and under.

1. Go to System > Settings > Logging
    a. Maximum Preserve Logs: 31
        i. This is the number of days to retain the logs, unless there is a maximum file size in Megabytes set in the following field. In this case, the days become the number of logs to maintain.
    b. Maximum file size (MB): 50 (or blank)
        i. By setting it to 50 MB per log and with 31 logs, this would be 153MB per system log.
    c. Click on Apply

To clear the logs, this is done by clicking on the Reset Log files button. Useful if to start at a clean baseline or to free up disk space quickly.

Miscellaneous Settings

1. Go to System > Settings > Miscellaneous
2. Hardware Acceleration:
    a. Check the Processor being used (at the Dashboard)
    b. If the Processor is an Intel Xeon, it is likely to support encryption acceleration other than AES-NI.
        i. Examples:
            Intel Xeon Platinum 8124M
            Intel Xeon Silver 4314
    c. If the Processor is supported:
        i. Hardware Acceleration: Intel QuickAssist Technology (qat)
    d. Or, set to None (AES-NI acceleration is built into the kernel)
3. Periodic Backups:
    a. Periodic RRD Backup: 8 hours (Recommended)
    b. Periodic Netflow: 8 hours (Recommended)
4. Click on Save

Services: Network Timing

The Cloaking Firewall ISO is initially configured to synch with the US NIST Atomic Clock at Ft. Collins, CO USA. If to change this to an internal timing server, then perform the following steps.

1. Set Network Time, go to Services > Network Time > General
    a. Time Servers:
        i. Replace the existing ones with the preferred one
        ii. Check the Prefer box for the primary server.
        Note for reference:

time-b-wwv.nist.gov	USA
time1.est.int	Europe
ntp.nict.jp	Japan
132.163.97.2	This IP is with NIST (time-a-g.nist.gov) base at Gaithersburg, Maryland, USA. This has been provided in case there is no DNS capability.

    b. Interfaces: Set to the LAN interface
    c. Click on Save
2. Restart the service by clicking on the Restart button at the top right corner.

Services: Unbound DNS

The Cloaking Firewall provides DNS service, which is enabled by default and pulls from the Not-for-profit organization Quad 9. Quad9 is a DNS service that emphasizes security and privacy as its core features, distinguishing it from other popular DNS providers like Google DNS or Cloudflare. By automatically blocking access to known malicious domains, Quad9 helps prevent users from connecting to sites that are likely to include malware, phishing attacks, and other cyber threats. This proactive security measure is backed by real-time threat intelligence from multiple sources, enhancing overall network security without sacrificing performance. Unlike some other DNS services, Quad9 also prioritizes user privacy by not using DNS query data for advertising or tracking purposes, making it an appealing choice for users and organizations that are particularly sensitive about their internet privacy and security.

If there is another server to be used or if the Cloaking Firewall is not to provide DNS service then proceed with the following process.

1. Go to Services > Unbound DNS > General
2. To Disable DNS:
    a. Enable Unbound: Unchecked
    b. Click on Apply
3. Or to modify, then:
    a. Enable Unbound: Checked (By Default)
    b. Network Interfaces: LAN interface (By Default for clients)
    c. DNSSEC: Checked (By Default)
    d. Click on the Advanced Mode slider at the top left area.
    e. Advanced:
        i. Outgoing Network Int: WAN interface (By Default)
    f. Click on Apply if any changes are made.
    g. Go to Services > Unbound DNS > Advanced
    h. Hide Identity Checked (By Default)
    i. Hide Version Checked (By Default)
    j. Hardened DNSSEC data: Checked (By Default)
    k. Aggressive NSEC: Checked (By Default)

l. Click on Apply if any changes are made.

4. Go to Services > Unbound DNS > DNS over TLS

   These are the Primary and Secondary DNS servers of Quad 9 in both IPv4 and IPv6 addresses. These can be disabled or edited for other servers, but public and private.

   a. If to add:
      i. Click the Add button
         1. Enabled: Checked
         2. Domain: The domain of the network.
         3. Server IP: The IP Address (either IPv4 or IPv6) of the DNS Server.
         4. Server Port: 853 for secured communications. 53 for normal.
         5. Verify CN: The common name of the server is listed in its certificate.
      ii. Click on Save
5. Click on Apply

DNS Blocklists

Using the DNS Blocklists is only really needed If there are users who will be using the firewall to surf the web. If the local environment is for only servers, then the Blocklists is likely to not be used, or can be customized to allow for Whitelisting for better security.

As an example, to implement DNS Blocklists:

6. Got to Services > Unbound DNS > Blocklist
   a. Enabled: Checked
   b. Type of DNSBL: Abuse.ch – Threatfox IOC database
   c. Click Apply
7. Restart the service.

Services: Monit Settings

Monit serves as a robust tool for managing and monitoring system processes, files, directories, and devices. It is particularly valuable for ensuring the high availability and proper operation of network services. Monit constantly checks and manages system criteria, such as daemon processes and the usage of file systems and can automatically restart services if it detects a failure or unresponsiveness. This capability significantly enhances the resilience and stability of the Cloaking Firewall by allowing administrators to proactively address issues before they escalate into more significant problems.

1. Go to Services > Monit > Settings > General Settings
   a. Click on the Advance mode slider at the top left area.
   b. Enable Monit: Checked
   c. Polling: 60 (By Default in seconds)
   d. Start Delay: 60 (By Default in seconds)
   e. For enabling alerts to be sent via Email, the following can be done.
      i. Mail Server Port 25 (By Default), 587 is used as a secured port.
      ii. Mail Server Username: Type in the username credential.
      iii. Mail Server Password: Type in the password credential.
      iv. Mail Server SSL Connection: Check if required
   f. Click on Save
2. Click on Apply
3. May need to click on Apply one more time.

An example of how to send email alerts to Microsoft Office is provided in the Appendix.

To generate Alerts:

1. Go to Alert Settings
    a. Copy the Monit Event Template
    b. Enable Alert: Checked
    c. Recipient: Use the Email or SMTP Address
    d. Events: Select the Event or Events
    e. Mail Format: Modify where needed.
    f. Description: Set a description of the Alert
    g. Click on Save
2. Click on Apply

To Enable WAN Interface Checks

1. Go to Service Settings Tab
2. If to enable the connectivity checks with the WAN interface, then check the Enable box to the respective addressing of the WAN interface (DHCP or STATIC).
3. Click on Apply

To Enable Storage Checking with Automatic Deletion/Purge of Logs

This service runs a script that will routinely check the storage utilization. It is to safeguard the storage from filling up to full capacity, which can greatly impact the firewall. This service also acts as a safeguard against Denial of Service (DoS) attacks which seek to generate events for the logs to fill up the storage.

If enabled, then have a remote SIEM or syslog server available to store the logs.

These are the thresholds and actions the service will execute:

- At 78% utilization. it will generate an alert.
- At 90% utilization, it will begin deleting log files (oldest first) until reduced to 80%.
- At 98% utilization, it will purge the logs.

1. Go to Service Settings Tab
2. If to enable the Check Log Storage service, click on the box in the Enabled column.
3. Click on Apply

Check Status

1. Go to Services > Monit > Status
2. This will provide a listing of the services in use and their statuses.

IDS (Suricata) Configuration

Suricata serves as a powerful Intrusion Detection and Prevention System (IDPS) within the Cloaking Firewall, designed to monitor network traffic in real-time to detect and prevent malicious activity. It operates by analyzing traffic patterns based on a comprehensive set of rules that describe known threats, such as malware, exploits, and unauthorized access attempts. When a potential threat is identified, Suricata can generate alerts for system administrators, offering detailed information about the intrusion attempt. More actively, Suricata can be configured to block packets that match these threat signatures, effectively stopping malicious traffic before it can reach networked resources. This capability is particularly useful in mitigating the risk posed by network scans, as Suricata can recognize the signatures of common scanning techniques and automatically block or alert administrators about these unauthorized reconnaissance activities.

1. Go to Services > Intrusion Detection > Administration
2. Click on the small "advanced mode" slider to enable advanced settings
    a. Enabled: Checked
    b. IPS Mode: Checked
    c. Promiscuous mode: Unchecked
    d. Enabled syslog alerts: Checked (By Default)
    e. Enable eve syslog output: Checked (By Default)
    f. Pattern matcher: Hyperscan (Default for 4GB+ RAM)
    Aho-Corasick (Recommended for 2CPU and 2GB RAM)
3. Detect Profile: Medium (By Default)
4. Interfaces: 11_LAN1 (By Default)
    Avoid using the WAN for the IDS, as the IDS takes precedence over Firewall Rules, and thus impacts performance.
5. Home Networks: Delete the existing Private IP Networks
    Add in the IP Addresses of the devices.
    For example, 172.24.10.10
6. Rotate log: Weekly (By Default)
7. Save Logs: 4 (By Default)
8. Click on Apply

Enable Rules for Suricata

Note if an Emerging Threats Professional License has been purchased, then please install the Emerging Threats Professional Rules Plugin by going to Settings > Firmware > Plugins and click on the plus button (+) for “cfw-intrusion-detection-content-et-pro”.

1. Click on the Download tab
    a. Click on Download & Update Rules button
        This will download the preconfigured rules:
            ET open/emerging_attack_response
            ET open/emerging_attack_coinminer (in case of compromised systems)
            ET open/emerging-exploit
            ET open/emerging-exploit_kit
            ET open/emerging-hunting
            ET open/emerging-ja3 (helps with encrypted packets)
            ET open/emerging-malware (may contain false positives)
            ET open/emerging-phishing (contains signatures for Log4J)
            ET open/emerging-scan
            ET open/emerging-shellcode (may contain false positives)

ET open/emerging-webserver (this can be disabled if there are no webservers in use)

ET open/emerging-worm
Internet_20-IDS/Cloaking

b. Additional rule can be enabled. Do understand that as more rules are applied, will begin to impact the performance of the firewall. Therefore, monitor performance after enabling additional rules.
    i. Click on the Enable selected
    ii. Click on Download & Update Rules
    iii. Click on Save
c. When the download is finished, click on the Rules tab to verify the rules downloaded.
d. Click on the Schedule Tab

    By Default, the rules are downloaded everyday at 02:22am UTC)

Enabled:	Checked	
Minutes:	22	(By Default)
Hours:	2	(By Default)
Day:	*	(By Default)
Months:	*	(By Default)
Days:	*	(By Default)
Command:	Update and reload intrusion detection rules	

e. Click on Save

Enable and Configure OpenVPN

Create Remote Access for Firewall Administration

There are two types of OpenVPN servers available for use and both can be running at the same time if needed, but the preference is to use only one or the other. Both VPNs are set to use the UDP protocol of Ports 12120 (Full Tunnel) and 12121 (Half Tunnel) for better performance and reduce risk of successful scans.

- VPN Full Tunnel: This VPN runs as an Instances in which the entire traffic of the remote user goes to the firewall. That is, the Cloaking Firewall acts as a gateway or proxy for remote users. This means that even to "surf the web" the Cloaking Firewalls acts as the source for the user. This provides more security as the entire traffic of the user is secured and protected by the firewall.
- VPN Split Tunnel: This VPN runs as a server in which only the traffic of the user that is accessing the Firewall, LAN or the protected systems is using the VPN. All other traffic, both at the local site and the Internet is not passed through the VPN. While not as secure as a Full Tunnel, this does provide less use of the firewall's bandwidth. For example, if a user was to be streaming videos from a commercial site, and remoting into the Firewall's network, then the bandwidth of the VPN would not be consumed with the video streaming.

To Enable and Configure VPN Full Tunnel

1. Go to VPN > OpenVPN > Instances
2. Click on the pencil button to edit.
3. Click on the Advanced mode slider at the top left area.
4. General Information:
    a. Role: Server (By Default)
    b. Description: FW Remote Admin Access VPN Server (Full Tunnel) (By Default)
    c. Enabled: Checked
    d. Protocol: UDP (By Default)
    e. Local Port: 12120 (By Default)
    f. Bind Address: Set this to the LAN interface's IP Address
    g. Type: tun (By Default)
    h. Verbose: 3 (By Default)
    i. Concurrent Connections 10 (By Default)
    The maximum number of clients to connect at any one time.
    j. Keep Alive 60 (By Default)
    k. Keep Alive Timeout 300 (By Default)
    l. Server (IPv4): 172.20.1.0/24 (By Default)
        i. Choose any Private IP Address CIDR that does not conflict with any existing networks.
        ii. The server will automatically take the IP Address ending with .1
    m. Server (IPv6): Blank (By Default)
        i. Choose any Private IP Address set that does not conflict with any existing networks.
    n. Topology net30 (By Default)
    o. Certificate: Select the CFW-RA-VPN-Certificate
    p. Certificate Authority: - Use from certificate (By Default)
    q. Verify Client Certificate: required (By Default)

r. Certificate Depth: One (Client+Server) (By Default)
s. Auth: SHA512 (512-bit) (By Default)
t. Data Ciphers: AES-256-GCM (By Default)
u. Authentication: Local Database (By Default)
v. Enforce local group: VPN-FW-Admins (By Default)
w. Strict User/CN Matching: Checked (By Default)
x. Local Network: Type in the IP Address CIDR of the LAN (Ex: 10.0.20.0/24)
y. Redirect Gateway: Block local (By Default)
z. Default Domain: Type in the domain to use

5. Click on Save

To Enable and Configure VPN Split Tunnel

1. Go to VPN > OpenVPN > Servers (legacy)
2. Click on the pencil button to edit.
3. General Information:
   a. Disabled: Unchecked
   b. Description: FW Remote Admin Access VPN Server (Split-Tunnel) (By Default)
   c. Server Mode: Remote Access (SSL/TLS + User Auth) (By Default)
   d. Backend for Auth: Local Database (By Default)
   e. Enforce local group: VPN-FW-Admins (By Default)
   f. Protocol: UDP (By Default)
   g. Device mode: tun (By Default)
   h. Interface: 10_LAN1 (By Default)
   i. Local Port: 12121 (By Default)
4. Cryptographic Settings:
   a. TLS Auth: Enabled – Authentication & encryption
   b. Generate TLS Shared Key: Checked (By Default)
   c. Peer Certificate Authority: CFW-Server-CA
   d. Server Certificate: CFW-RA-VPN-Certificate
   e. Encryption Algo: AES-256-GCM (256 bit key, 128 bit block (By Default)
   f. Auth Digest Algo: SHA512 (By Default)
   g. Certificate Depth: One (Client+Server) (By Default)
   h. Strict User/CN Matching: Checked (By Default)
5. Tunnel Settings:
   a. Tunnel Network: 172.20.2.0/24 (By Default)
      i. Choose any Private IP Address CIDR that does not conflict with any existing networks.
      ii. This is the VPN Tunnel Network, the actual IP CIDR is dependent on the client net schema.
   b. Redirect Gateway: Unchecked (By Default)
      i. NOTE: What the Redirect Gateway does is when enabled, force all clients to use the server's gateway for traffic. This is useful for some situations, such as having all work related traffic from corporate machines or hosting a VPN service.
      ii. If Redirect Gateway is checked:
         1. May need to enter for IPv4 Remote Network: 0.0.0.0/0
            This is to allow for access to the Internet, but please verify with testing.
   c. Local Network:
      i. The LAN IP Address can be of just the Firewall or of all of the LAN.
      ii. For just to access the Firewall, then enter as a /32 (example: 10.0.20.10/32)

iii. For the whole LAN1 network, then use /24 (example: 10.0.20.0/24)
iv. The actual IP CIDR is dependent on the client networking schema. In this case, the VPN is being used to access the LAN.
v. To add in multiple LAN's, use a comma (,) followed by a space to separate.
1. Example: 10.100.100.0/29, 192.168.1.0/24

d. Concurrent Connections: 10 (By Default)
The maximum number of clients to connect at any one time.
e. Compression: [No preference] (By Default)
f. Type of Service: Unchecked (By Default)
g. Inter-Client Comms: Unchecked (By Default)
h. Duplicate Comms: Unchecked (By Default)

6. Client Settings:
a. Dynamic IP: Unchecked (By Default)
b. Topology: Checked (By Default)
c. DNS Default Domain: Checked (By Default) (Type in the domain to use)
7. Advanced configuration:
a. Verbosity level: 3 (recommended) (By Default)
8. Click on Save

Download VPN Client

To download the certificate to use for a given user,

1. Go to VPN > OpenVPN > Client Export
a. Remote Access Server: Select which of the two VPNs, Full Tunnel or Split Tunnel
b. Set Export Type to: File Only
c. Set Hostname to: If connected to the Internet, then change to the Public IP
If for isolated or internal networks, then the Private IP of the WAN.
d. Port: Select 12120 (Full Tunnel) or 12121 (Half Tunnel)
2. Scroll down to the Accounts/Certificates section.
3. Download the Secop.adm certificate.

Perform Reboot if OpenVPN Server(s) are Enabled

If either or both of the OpenVPN servers are enabled, then for best performance and to unlock the Firewall OpenVPN Rules is to conduct a reboot.

1. Go to Power > Reboot
2. Click on Yes to Reboot
3. Log in and continue with the steps.

Optional: Implement a VPN Interface

Having a VPN Interface helps to provide for better control.

1. Go to Interfaces > Assignments
2. At the Assign a new Interface section, select the given ovpns (1 or 2) interface.
a. OVPNS1 Full Tunnel VPN
b. OVPNS2 Split Tunnel VPN
3. Description:
a. OVPNS1: 30_OVPN1
b. OVPNS2: 30_OVPN2
4. Click on Save

Firewall Configuration

Firewall Rules, Precedence/Priority

There is an ordering of the firewall rules of which rules take precedence over others. The firewall rules come in two primary types, followed by sub-types. Firewall rules are done in a prioritizing of a Top Down Approach, in which the rules are the top have “first match” and take immediate effect if the given situation matches the rules. It is possible to set rules as a “Last Match”, which would work as a “catch-all” kind of rule.

The two main types of Rules, Networking and Filter rules. Of these, Networking Rules have higher priority over Filter Rules. Therefore, added caution must be used when implementing Networking Rules as they could cause a by-pass of the conventional filter rules in blocking malicious threats.

For example, a NAT Port Forwarding Rule was created to allow for HTTPS based traffic (TCP Port 443) to be redirected to a web server on LAN1. There is a Filter Rule that has blacklisted all of the IPv4’s of Russia from accessing any ports. However, with how the two types of rules work, the Port Forwarded Rule will allow for the IPv4’s of Russia to by-pass the Filter Rules, thus allowing anyone in Russia to access the webserver.

To prevent this, NAT Port Forwarding rules can be created to Deny the capability to have network routing. This is achieved by using the “No RDR (ReDiRect) NOT” rule to be checked.

Also, a Filter Rule, known as Floating, can be used to block IPs to multiple interfaces, such as the WAN and LAN, without the need to create duplicated rules. With the example above, a Floating Rule can be created to have Russian based IPv4’s to be blocked at the WAN and also from accessing the LAN.

- Networking Rules: These firewall rules are associated with networking and comprise of the NAT Port Forwarding, NAT Outbound, One-to-One and NPTv6. These rules have precedence over the Filter Rules.
- Filter Rules: Filter Rules come in four types of precedence:
    1. IP Blocker Rule: This rule sets nearly at the top (Number 4) and takes priority over the following other rules. Only the defaults rules, such as “Deny All” has a higher priority. IP’s that are blacklisted in the IP Blocker lists, will be blocked at any given interface and of the direction of traffic. Therefore, whitelisting of the trusted and/or Administrative IP’s are crucial to prevent being locked out.
       While IP Blocker is a Filter Rule and has less priority with Networking Rules, the IP Blocker will take effect when the second interface is accessed.
       For example, with the Russian example of Port Forwarding, although the WAN Filter rules have no effect, the routed traffic must enter the LAN interface, before exiting the LAN interface. As the Russian based traffic is entering the LAN interface, the IP Blocker rule takes effect, thereby blocking offending IP’s if they had triggered an event.
    2. Special Rules: These rules are the automatic generated rules that are not normally visible, such as the “Default Deny All” rule.
    3. Floating Rules: These rules can be used to cover multiple interfaces and therefore have precedence with the rest of the Specific Interfaces Rules. Additionally, Floating Rules can cover both directions (In, Out) with a single rule, while Specific Interface rules can only cover one direction and therefore would need two rules.
    4. Specific Interface Rules: These are the most common of the firewall rules, which help to allow or to deny traffic through the firewall.

Firewall and Asymmetric Routing

In technical terms, when two machines in the same LAN communicate via a Firewall (or any gateway), asymmetric routing happens if the request from Machine A to Machine B takes a different network path than the response from Machine B back to Machine A. This can cause issues, especially when a Firewall is involved, because the Firewall might only see one side of the conversation. This can lead to dropped packets, failed connections, or other unpredictable behavior since the Firewall might think the incoming traffic from Bob (in our analogy below) is unsolicited, as it didn't see the initial letter from Alice.

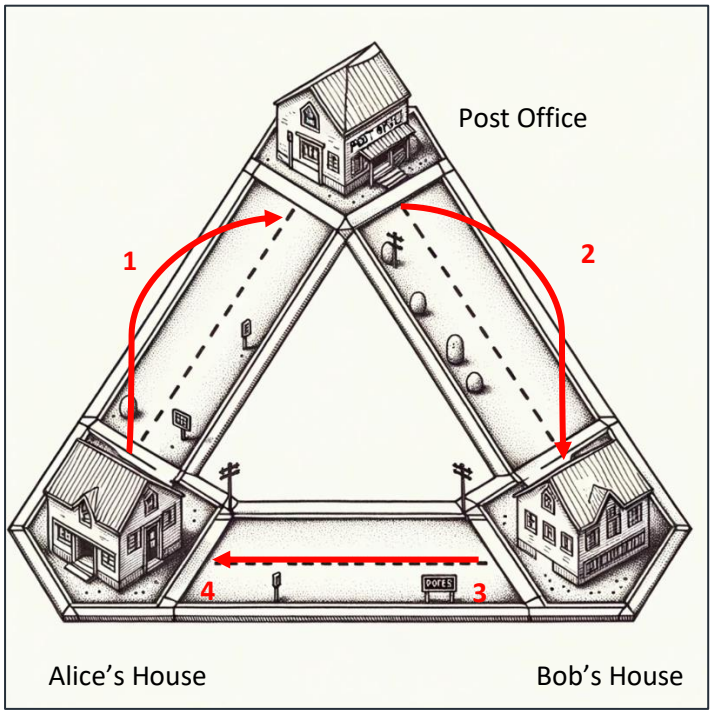
Asymmetric Routing only occurs with TCP based traffic and when there is a Firewall in place acting as the Gateway. Asymmetric Routing is normally not encountered in most networks as the Gateway is either a Router or a Server (example DHCP/DNS) and no governing Firewall rules are in place.

Asymmetric Routing analogy:

Imagine a town with two roads leading from Alice's house to Bob's house. Alice and Bob want to send letters to each other. The town's post office (which acts like the Firewall in our analogy) sits on one of these roads and checks every letter that goes through it to ensure it's safe and doesn't contain anything harmful.

Alice sends her letter to Bob using the road that passes through the post office (Firewall).

Bob receives the letter and decides to reply. However, instead of using the same road that Alice used (which goes through the post office), he uses the other road that goes directly to Alice's house, bypassing the post office entirely.



1. Alices sends a secured letter to the Post Office to go to Bob.

2. Post Offices sends the letter to Bob's House.

3. Rather than using the same envelop and mail a reply to the Post Office, Bob decides to use a new letter envelop and goes over to Alice's house, dropping it off.

4. Alice picks up the letter from Bob, but it has no posting, with a different envelop and therefore confuses Alice if this is a

Setting Firewall Rules to deal with TCP Asymmetric Routing

To rectify this should there be machines that need to communicate with each other, and the Firewall is acting as the Gateway, use the following measures when implementing Filter Based Firewall Rules. UDP base rules are not impacted by Asymmetric Routing due to the fact that UDP is a connectionless protocol.

1. When a TCP based rule has been mostly finished, scroll down to the bottom to Advanced features, and click on the "Show/Hide" button.

2. Scroll down to TCP flags and check the box for “Any flags.”
3. Change State Type to “Sloppy State”.
4. Then save the rule.

Advanced Firewall Settings

1. Go to Firewall > Settings > Advanced
   a. Bogon Networks: Update Frequency: Weekly (By Default)
   b. Gateway Monitoring Skip rules: Checked (By Default)
   c. Set Firewall Optimization to: Normal (By Default)

   For the following settings when dealing with Firewall States, depends on the amount of available RAM, and of use of the number of rules for the IDPS and endpoints. By Default, 10% of the RAM is set aside for the number of States.

   States is the number of connections that are allowed with the firewall. However, this does include connections to and from the Firewall. Thus, a user or server, that accesses the Internet will be actually of 2 Connections (1 Connection with the Server to the Firewall, and 1 Connection with the Firewall to the Internet), this number should be considered as halved for the actual connections to be used. However, some users and systems are likely to have more than 1 connection. An assumption should be that 10 connections may be used per user or systems.

   For example, with a system that has 8GB RAM, 789,000 single connections would be allowed (or 394,500 connections through the firewall). Assuming that 10 full connections (passing through the firewall) are used per user or device, the actual number of connected users or devices would be 39,400.

   For most purposes, this the default setting is sufficient, but high volume sites may want to have more.

   If the firewall has a large amount of RAM to work with, then these settings could be increased.

   To determine the number of states allocated, go to “Firewall Maximum States”, and click on the Circled “I” to see the help. The number of states provided will be shown.

   For example: “Note: Leave this blank for the default. On your system the default size is: 789000”

   To make an adjustment, or even to indicate using the default settings, this is how it is done.

   Note, if to use Default Settings, leave these entries blank.

   d. Firewall Adaptive Timeouts:
      i. Start (by default, 60% of Maximum States): 600000
      ii. End (by default, 120% of Maximum States): 1200000
   e. Maximum Firewall States (by default, 10% of RAM): 1000000

   Normally 1,000,000 Table Entries is sufficient. Table Entries are the number of firewall rules and Aliases that are to be used. If a large amount of firewall rules or threat feeds are to be used, then this may need to be increased. To ensure there are no errors and for best performance, ensure that no more than 80% of the Maximum Table Entries are in used.

   f. Firewall Maximum Table Entries = 1500000
   g. Click Save

Firewall NAT Port Forward

NAT Port Forwarding, also known as port mapping, is a network address translation technique used to redirect communication requests from one address and port number combination to another. This method allows external devices to access services on a private network by mapping a specific external port to an internal IP address and port. Commonly utilized in scenarios where a device on a local network needs to be accessible from outside the network, such as hosting a web server, gaming server, or remote desktop service, NAT Port Forwarding enhances connectivity while maintaining the security of the internal network by not exposing the entire network infrastructure.

1. Go to Firewall > NAT > Port Forward

By Default, there Eight Rules that are used for Port Forwarding, most of which are disabled. Three rules that are enabled are to prevent a lookout of the WebGUI (“Anti-Lockout Rule”) the two Denal rules for Suspected Bad Sites and Recon Intel Scanners. These two help to prevent unauthorized access via the NAT rules. If there are no port forwarding to be done, then these rules can be disabled.

The Rules:

- Anti-Lockout Rule:
  To prevent being locked out from the Cloaking Firewall’s WebGUI. Once the initial configuration has been completed and has tested the connections, then this rule can be disabled.
- Inbound - Allow Forward: Trusted Sites VPN for LAN1 Remote Access:
  This rule is to allow only VPN Full Tunnel connections from Whitelisted Trusted Sites.
- Inbound - Allow Forward: Trusted Countries VPN for LAN1 Remote Access:
  Similar to the above rule, but instead of Trusted Sites, this is dealing with Whitelisted Countries. This would be for example having remote employes to access the LAN from their homes. Since home based networks typically have dynamic IP Addressing, Whitelisted Trusted Sites normally cannot be used effectively.
- Inbound - Allow Forward: From Any Where Full Tunnel VPN for LAN1 Remote Access
  Should there be remote users from many parts of the world, or perhaps as travelling (i.e.: Road Warriors), then this rule allows for any location.
- Inbound - Allow Forward: From Any Where Split Tunnel VPN for LAN1 Remote Access
  This is similar to the above rule but is for the Split-Tunnel VPN.
- Deny - Inbound: Blacklist of Sanctioned Countries
  This rule is to deny any IPs that are listed in the Blacklist of Sanctioned Countries Alias.
- Deny - Inbound: Blacklist of Suspected Bad sites IPv4
  This rule is to deny any IPs that are listed in the Blacklist of suspected malicious sites.

- Deny - Inbound: Blacklist of Recon Intel Scanners
  This rule is to deny any IPs that are listed in the Blacklist of sites that perform Internet scans.

Initially the Blacklist Rules have the lower precedence to avoid potential blocks from the initial installation. When the connections for remote access are working, then these blacklists can be moved upwards.

Enable a Rule

To enable a Rule, such as the Split-Tunnel rule, click on the grayed out Left-Right Arrow at the left hand side. Then click on the Apply Changes button.

Disable a Rule

To disable a Rule, such as the now enabled Split-Tunnel rule, click on the Green Left-Right Arrow at the left hand side. Then click on the Apply Changes button.

Create a Split Tunnell Rule for Whitelisted Sites

This is to allow for the VPN Split Tunnel to be forwarded to the LAN Interface from and not used at the WAN Interface.

2. Click on the Add button for a new rule
   a. Disabled: Unchecked
   b. No RDR (NOT) Unchecked
      NOTE: By checking this box, any IP that matches this rule is blocked from Port Forwarding
   c. Interface: 01_WAN1
   d. TCP/IP Version: IPv4
   e. Protocol: UDP
   f. Source: WHITELISTED_Trusted_Sites_IPv4
   g. Destination: 01_WAN1 address
   h. Destination Port: PORT_CFW_RemoteAccess_VPN
   i. Redirect Target IP: INTERFACE_01_LAN1
   j. Redirect Target Port: PORT_CFW_RemoteAccess_VPN
   k. Log: Checked
   l. Category: VPN
   m. Description: Inbound - Allow Forward: Trusted Sites VPN for LAN1 Remote Access
   n. Click on Save
3. Click on the Add button for a new rule
   a. No RDR (NOT) **Checked**
      NOTE: By checking this box, any IP that matches this rule is blocked from Port Forwarding
   b. Interface: 01_WAN1
   c. TCP/IP Version: IPv4
   d. Protocol: TCP/UDP
   e. Source: BLACKLIST_Sanctioned_Countries
   f. Destination: 01_WAN1 address
   g. Destination Port: PORTS_Protected_Exposed_Ports
   h. Log: Unchecked
   i. Category: Blacklist
   j. Description: Deny - Inbound: Blacklist of Sanctioned Countries
   k. Click on Save

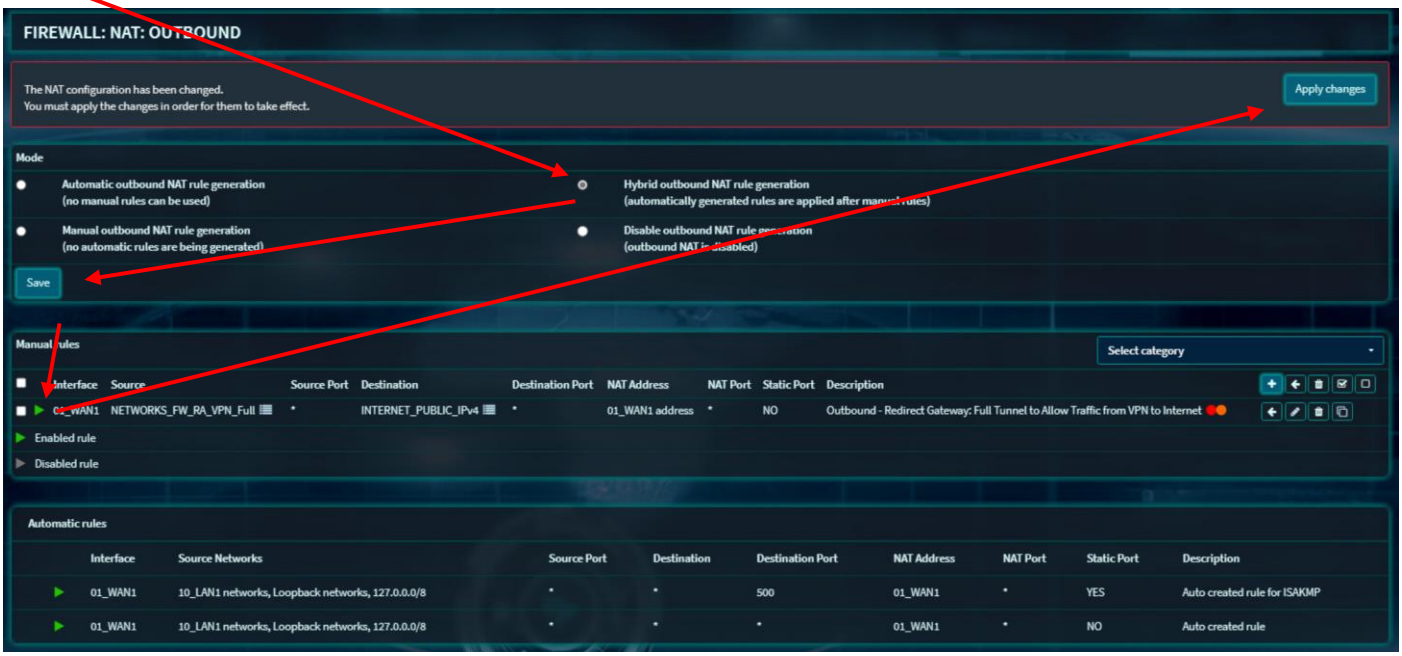
4. Copy the above rule
    a. Source: BLACKLIST_Recon_Scanners_IPv4
    b. Description: Deny - Inbound: Blacklist of Recon Intel Scanners
    c. Click on Save
5. Copy the above rule
    a. Source: BLACKLIST_Bad_IPv4_CIDR_High
    b. Description: Deny - Inbound: Blacklist of Suspected Bad sites IPv4
    c. Click on Save
6. Copy the above rule
    a. Source: BLACKLIST_Suspected_IPv4
    b. Description: Deny - Inbound: Blacklist of Suspected IPs from IDPS IPv4
    c. Click on Save
7. Click on the Add button for a new rule
    a. No RDR (NOT) **Unchecked**
    b. Interface: 01_WAN1
    c. TCP/IP Version: IPv4
    d. Protocol: UDP
    e. Source: Any
    f. Destination: 01_WAN1 address
    g. Destination Port: PORT_CFW_RemoteAccess_VPN
    h. Redirect target IP: Interface_11_LAN1_IP
    i. Redirect Target Port: PORT_CFW_RemoteAccess_VPN
    j. Log: Checked
    k. Category: VPN
    l. Description: Inbound - Allow Forward: Roadwarrior VPN for LAN1 Remote Access
    m. Click on Save
8. Click on Apply Changes

Firewall NAT Outbound

NAT Outbound Rules, also known as Source NAT (SNAT), are network address translation configurations that control how internal IP addresses are translated when they access external networks. These rules modify the source address of outbound traffic, typically changing private IP addresses to a public IP address, allowing devices within a private network to communicate with external networks, such as the internet. This process is crucial for managing multiple internal devices that share a single public IP address and helps in preserving the limited number of public IP addresses. NAT Outbound Rules enhance security by hiding internal IP addresses and enable proper routing of return traffic back to the originating internal device.

NAT Outbound rules can be skipped, unless to implement VPN Full Tunnel. If to enable VPN Full Tunnel, then the following steps are required. VPN Split-Tunnel does not require this.

1. Set Mode to Hybrid
2. Click on Save
3. At the Manual Rules section:
    a. Click the Grayed out Arrow (pointing right) to enable the rule.
4. Click on Apply Changes



Firewall Rules

Firewall rules are essential components of network security configurations that define how traffic is managed and controlled within a network. These rules specify which types of traffic are allowed or denied based on various criteria such as IP addresses, port numbers, and protocols. By establishing these rules, administrators can control the flow of incoming and outgoing traffic, ensuring that only authorized connections are permitted while blocking potentially harmful or unauthorized access. Firewall rules are crucial for protecting network resources, preventing unauthorized access, mitigating threats, and maintaining the overall security and integrity of the network infrastructure.

Floating Rules

Floating firewall rules are advanced configurations that apply to multiple interfaces, overriding standard interface-based rules. These rules provide flexible and powerful control over network traffic, allowing administrators to enforce consistent policies across different network segments.

The Rules:

- Deny – ICMP: Prevent possible DoS Attack by PING Events to Logs:
  This rule helps to prevent in the possible attempt to perform a Denial of Service (DoS) from ICMP PING packets. While the rule is set to Deny incoming packets to avoid detection, this rule further avoids logging the events. PING based attacks attempt to flood the logs causing tremendous number of Writes and Reads to the storage drives. The performance of the firewall may become sluggish, even when there is little amount of bandwidth in use. This is set to the WAN interface.
- Deny - Inbound: Blacklist of Sanctioned Countries
  This rule is to deny any IPs that are listed in the Blacklist of Sanctioned Countries Alias that are incoming to the firewall. This is set to disabled, until a source for GeoIP can be implemented. This is set to both the WAN and LAN interfaces.
- Deny - Inbound: Blacklist of Suspected Bad sites IPv4
  This rule is to deny any IPs that are listed in the Blacklist of suspected malicious sites that are incoming to the firewall. This is set to both the WAN and LAN interfaces.
- Deny - Inbound: Blacklist of Recon Intel Scanners
  This rule is to deny any IPs that are listed in the Blacklist of sites that perform Internet scans that are incoming to the firewall. This is set to both the WAN and LAN interfaces.

- Deny - Outbound: Blacklist of Sanctioned Countries

  This rule is to deny any IPs that are listed in the Blacklist of Sanctioned Countries Alias from leaving the firewall. This is set to disabled, until a source for GeoIP can be implemented. This is set to the WAN interface.
- Deny - Inbound: Blacklist of Suspected Bad sites IPv4

  This rule is to deny any IPs that are listed in the Blacklist of suspected malicious sites from leaving the firewall. This is set to the WAN interface.

01_WAN1 Rules

WAN-based firewall rules control the traffic entering and exiting a network through the Wide Area Network (WAN) interface. These rules are designed to manage and secure external connections, protecting the internal network from unauthorized access and potential threats from the internet.

1. Go to Firewall > Rules > 01_WAN1

As of this time, there is no need for any additional WAN base rules. The four that are listed are associated with the previous NAT Port Forwarding rules.

10_LAN1 Rules

LAN-based firewall rules regulate the traffic within the Local Area Network (LAN), managing communication between internal devices and ensuring secure and efficient data flow. These rules help to control access to network resources, enforce internal security policies, and segment the network for improved performance and protection.

1. Go to Firewall > Rules > 11_WAN1

The Rules:

- Allow – MAINT: Inbound – Allow: Any LAN1 IPv4 Endpoint to Access CFW WebGUI:

  This rule is a Maintenance Rule, indicating that it should only be enabled when performing maintenance and disabled when no longer needed.

  This rule allows for any device on the LAN to be able to access the Cloaking Firewall WebGUI. For best practice, the Cloaking Firewall WebGUI should be accessible by a designated Endpoint (specific IP Address) and/or VPN.
- Allow – MAINT: Inbound – Allow: Any LAN1 IPv4 Endpoint to Access CFW SSH:

  This rule is a Maintenance Rule, indicating that it should only be enabled when performing maintenance and disabled when no longer needed.

  This rule allows for any device with an IPv4 Address on the LAN to be able to access to any other endpoint on the LAN and the Internet, essentially Anywhere. For best practice, devices on the LAN should not be allowed to communicate to Anywhere. This rule is useful when installing new endpoints and need to check for connectivity before locking down the rules.
- Allow – MAINT: Inbound - Allow: All LAN1 IPv6 Net Traffic to Any

  This rule is a Maintenance Rule, indicating that it should only be enabled when performing] maintenance and disabled when no longer needed.

  This rule allows for any device with an IPv6 Address on the LAN to be able to access to any other endpoint on the LAN and the Internet, essentially Anywhere. For best practice, devices on the LAN should not be allowed to communicate to Anywhere. This rule is useful when installing new endpoints and need to check for connectivity before locking down the rules.

- Allow - Internal: ICMP IPv4 Traffic within LAN1 Net
  This rule allows for any endpoint to PING to any other device within the LAN. This rule is useful for checking on the internal communications capability of the LAN. However, this rule should be disabled or modified to only allow designated endpoints to perform PING's to specified IP addresses.
- Allow - Internal: TCP Any IPv4 Traffic within LAN1 Net (Asyn Traffic)
  This rule allows for TCP based traffic from any endpoint to communicate to any other endpoint within the LAN. The reason for the Asynchronous Traffic, is that all TCP based traffic must flow through the firewall's LAN interface and not directly to another device.
- Allow - Internal: UDP Any IPv4 Traffic within LAN1 Net
  This rule is similar to the above TCP rule in allowing for UDP based traffic from any endpoint to communicate to any other endpoint within the LAN. Due to the properties of UDP, Asynchronous Traffic control is not needed.
- Allow - External: ICMP IPv4 Traffic from LAN1 Net to Internet
  This allows for LAN based endpoints to perform PINGs to the Internet. Should this not be required, this rule can then be disabled or modified as a Maintenance Rule.
- Allow - External: TCP/UDP IPv4 Traffic from LAN1 Net to Internet
  This rule allows for LAN based endpoints to communicate out to the Internet.

OpenVPN Rules

OpenVPN firewall rules manage the traffic associated with OpenVPN connections, ensuring secure and controlled access for remote users. These rules regulate which types of traffic can pass through the VPN, providing protection and secure communication between remote clients and the internal network.

Note:
All of the VPN Rules are disabled by Default, to enable the click on the grayed out arrow(s) of the rule(s) to toggle to be Enabled (turns to Green). Once all of the rule or rules have been enabled, then click on Apply Changes.

1. Go to Firewall > Rules > OpenVPN

The Rules:

- Allow - MAINT: Allow - Inbound: All VPN Traffic to Anywhere
  This rule is a Maintenance Rule, indicating that it should only be enabled when performing] maintenance and disabled when no longer needed.
  This rule allows for any connection on the Full Tunnel VPN to be able to access to any other endpoint Any Where. For best practice, this rule should be disabled after installation and connectivity checks.
- Allow - MAINT: Allow - Inbound: All VPN Traffic to Internet (Full Tunnel)
  This rule is a Maintenance Rule, indicating that it should only be enabled when performing] maintenance and disabled when no longer needed.
  This rule allows for any connection on the Full Tunnel VPN to be able to access the Internet. This rule can be modified as a standard rule if the intent is to allow for users on the Full Tunnel VPN to access the Internet.
- Allow - MAINT: Allow - Inbound: All VPN Traffic to Anywhere (Split Tunnel)
  This rule is a Maintenance Rule, indicating that it should only be enabled when performing] maintenance and disabled when no longer needed.
  This rule allows for any connection on the Split Tunnel VPN to be able to access to any other endpoint Any Where. For best practice, this rule should be disabled after installation and connectivity checks.

- Allow - MAINT: Allow - Inbound: All VPN Traffic to Internet (Split Tunnel)
  This rule is a Maintenance Rule, indicating that it should only be enabled when performing] maintenance and disabled when no longer needed.
  This rule allows for any connection on the Split Tunnel VPN to be able to access the Internet. This is normally not possible as Split Tunnel VPNs generally only have access to the designated networks.
  This rule is included if there are modifications to the Split Tunnel to make it into a Full Tunnel.
- Allow – Inbound: ICMP PING from VPN Net to LAN1 Net (Not Logged):
  This rule helps to prevent in the possible attempt to perform a Denial of Service (DoS) from ICMP PING packets within the Full Tunnel VPN, hence the PING events are not logged.
- Allow – Inbound: TCP from VPN Net to access WebGUI:
  This rule allows for any connection on the Full Tunnel VPN to be able to access the Cloaking Firewall WebGUI.
- Allow – Inbound: TCP from VPN Net to access SSH:
  This rule allows for any connection on the Full Tunnel VPN to be able to access the Cloaking Firewall via SSH.
- Allow – Inbound: ICMP PING from VPN Net to LAN1 Net (Not Logged) (Split Tunnel):
  This rule helps to prevent in the possible attempt to perform a Denial of Service (DoS) from ICMP PING packets within the Split Tunnel VPN, hence the PING events are not logged.
- Allow – Inbound: TCP from VPN Net to access WebGUI (Split Tunnel):
  This rule allows for any connection on the Split Tunnel VPN to be able to access the Cloaking Firewall WebGUI.
- Allow – Inbound: TCP from VPN Net to access SSH (Split Tunnel):
  This rule allows for any connection on the Split Tunnel VPN to be able to access the Cloaking Firewall via SSH.

Disable the Anti-Lockout Rule

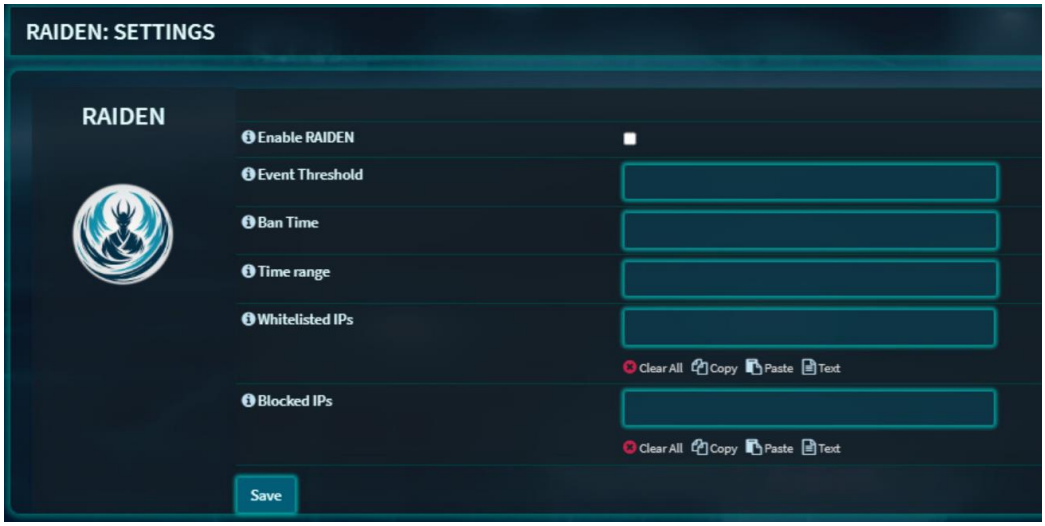
When all of the Firewall Rules have been completed, the Anti-Lockout Rule can be disabled.

1. Go to Firewall > Settings > Advanced
   c. Scroll down towards the bottom.
   d. Set Disable anti-lockout: Checked (To disable)
   e. Click on Save

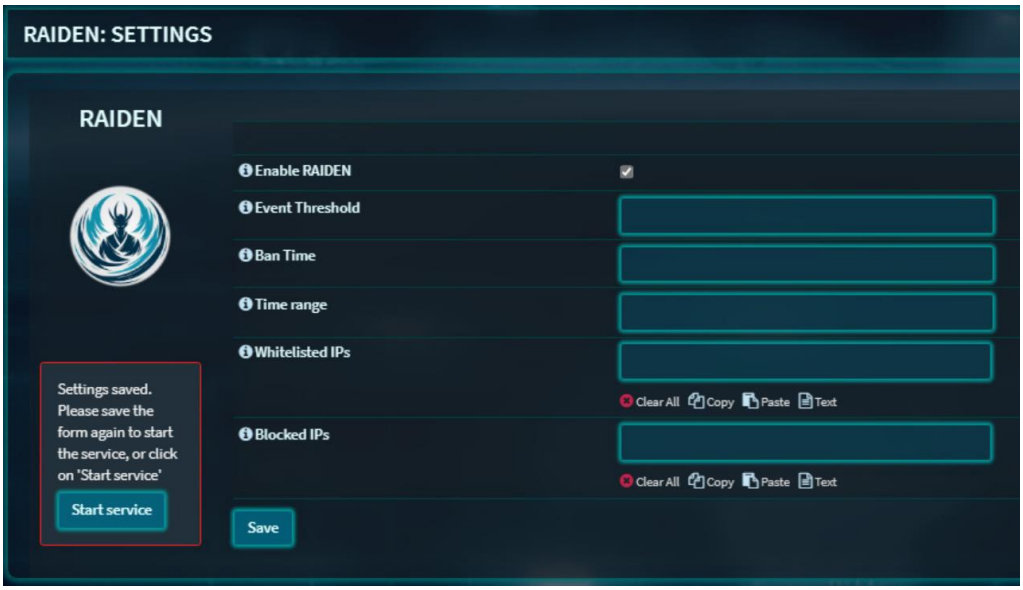
Configure RAIDEN

RAIDEN is an autoblocking module that whenever a triggered event occurs, via Firewall Rules or IDPS, RAIDEN swings into action, barring the offending IP address for a specified duration. This mechanism imparts a "memory" to the system, logging IP addresses associated with nefarious activities. RAIDEN essentially enforces a period of exclusion for these malicious IPs, preventing them from interacting with the network during that time. This mechanism not only provides immediate remediation by stopping ongoing malicious activity but also serves as a deterrent, making the network a less appealing target for repeated malicious attempts.

1. Go to RAIDEN > Settings



2. At first, the RAIDEN GUI will appear with emptied fields. For now, click on the checkbox to Enable RAIDEN.
3. Then click on Save.
4. A new window will appear on the lefthand side, indicating to start the service. Click on the Start Service button.

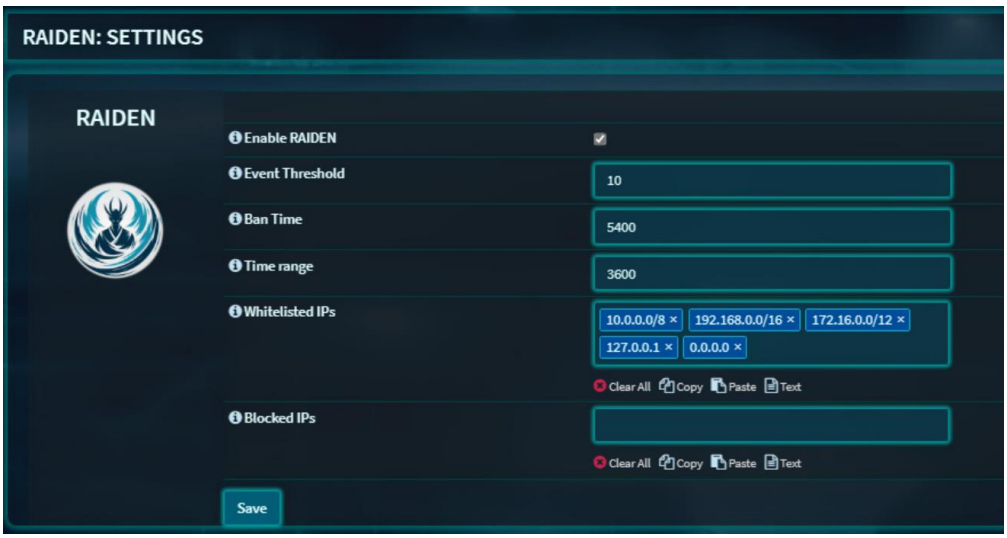


5. RAIDEN will now have settings with the following values:
    a. Event Threshold: 10 Number of bandable events before IP Address is banned.
    b. Ban Time: 5400 Number of seconds to ban IP address

c. Time Range: 3600 Number of seconds to evaluate banned events for. For example, if set to (default) 600, raiden will look at the last 10 minutes for the number of banable events.

d. Whitelisted IPs: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, 127.0.0.1. 0.0.0.0
These are IP Addresses or IP Ranges to be excluded from being blocked by RAIDEN. By Default, all Private IPs, Local Host, and Broadcast are exempted. If accessing the firewall remotely, then type in the Remote IPs and VPN IP Ranges. This will help prevent accidental lockouts. The whitelist can be modified to reduce the Private IP addresses, which can then allow for internal systems to be blocked.
For example, if only having a single server behind the firewall, then that server's IP can be whitelisted (ex: 192.168.10.10). Also include the firewall's LAN IP (ex: 192.168.10.1), so that if any other unauthorized device is installed, it will be blocked.

e. Blacklist IPs: [Blank] This will be the list of IPs that have been banned for violating a Firewall or IDPS rule. These IPs can be individually removed or all at once.
To remove a single IP from the Blacklist, click on the respective "X" and then click on Save.



By Default settings, an IP Address will be banned if it is not part of the Private IPs (local host and Broadcast) and has triggered 10 more events within 3600 seconds (1 hour). If so, this IP address will be on the Blacklist for 90 minutes. If this IP continues to trigger events within the 1 hour time range, its ban time will be reset to 90 minutes again.

6. For restrictive measures in stopping scans, these are the recommended settings to use:
   a. Event Threshold: 1
   b. Ban Time: 600 (10 minutes)
   c. Time Range: 600 (10 minutes)
   d. Whitelisted IPs: Include the IPs for the following:
      Public or Private DNS servers (8.8.8.8, 9.9.9.9, 1.1.1.1)
      Partner or Vendor IPs
      Network Timing Service Sites
      VPN Tunnel IP Ranges

Tunable Settings:

Tunables form the basis for specialized network capabilities. They are parameters that can be adjusted to modify the system's kernel behavior at runtime. These parameters provide administrators with the flexibility to optimize system performance, manage resource allocation, and enhance security settings according to specific network requirements and hardware capabilities. Tunables are instrumental in fine-tuning a system to achieve desired performance metrics, especially in environments where network traffic and security are critical concerns.

By adjusting tunables, system administrators can significantly impact how the system handles network connections, memory management, process scheduling, and more. For instance, network-related tunables can dictate how much memory is allocated to network buffers, or how the TCP/IP stack should handle packet processing and traffic prioritization. This ability to configure and optimize settings at such a granular level makes tunables a powerful tool in tailoring system operations to align perfectly with the operational demands and performance targets of enterprise-level networks and services.

In sense, the ability to “go under the hood” and make performance adjustments.

Due to the importance of Tuning the System for Optimal Performance, this section is dedicated to it. This is much like tuning up a car for best performance and speed. Also, some of these settings are based on the number of CPUs, RAM, and Bandwidth, and therefore adjustments may be needed.

1. Go to System > Settings > Tunables

The following setting is set for up to 10 Gbps throughput, which should satisfy most systems. If higher bandwidth is needed, such as 25Gbps or to go lower, the values are listed. Edit the value as needed.

Tunable	Value	Description
kern.ipc.maxsockbuf	16777216	Improved Performance: Maximum socket buffer size. Default: 10 Gbps – 16777216 (16 MB) 1 Gbps – 2097152 (2 MB) 2 Gbps – 4262144 (4 MB) 5 Gbps – 8388608 (8 MB) 25 Gbps – 33554432 (32 MB)

The following Tunables have been able to be configured if the provided Configuration File was imported.

Otherwise, if using the default configuration from the installation, the following tunables are recommended to be added to improve network and IDPS performance.

Tunable	Value	Description
dev.netmap.buf_num	327680	For use with the IDS set to IDPS Mode.
dev.netmap.buf_size	4096	For use with the IDS set to IPS Mode. For Default, use 1024. For 4GB or Higher RAM, use 4096
kern.ipc.nmbclusters	1000000	Maximum number of mbuf clusters allowed
kern.random.fortuna.minpoolsize	128	Improved Performance: Improves the RNG entropy pool for VPNs.
kern.random.harvest.mask	351	Entropy harvesting mask
net.inet.carp.senderr_demotion_factor	0	Send error demotion factor adjustment
net.inet.ip.check_interface	1	DoS mitigation: verify packet arrives on correct interface (default 0)
net.inet.ip.process_options	0	DoS mitigation: ignore IP options in the incoming packets (default 1)
net.inet.raw.recvspace	131072	Maximum space for incoming raw IP datagrams
net.inet.raw.maxdgram	131072	Maximum outgoing raw IP datagram size
net.inet.tcp.abc_l_var	52	Improved Performance: Improves efficiency while processing IP fragments.
net.inet.tcp.minmss	536	Improved Performance: Configures the minimum segment size, or smallest payload of data which a single IPv4 TCP segment will agree to transmit.

net.inet.tcp.msl	5000	DoS mitigation: Maximum Segment Lifetime is the time a TCP segment can exist on the network and is used to determine the TIME_WAIT interval, 2*MSL (default 30000 which is 60 seconds)
net.inet.tcp.mssdflt	1240	Improved Performance: Improves efficiency while processing IP fragments.
net.inet.tcp.path_mtu_discovery	0	DoS mitigation: Disable MTU discovery since most ICMP type 3 packets are dropped by others (default 1) Set to 0 (Disable) for mtu=1500 as most paths drop ICMP type 3 packets Set to 1 (Enable) for mtu=9000
net.inet.tcp.recvbuf_max	4194304	Improved Performance: TCP Buffers: Larger buffers and TCP Large Window Extensions (RFC1323) can help alleviate the long fat network (LFN) problem caused by insufficient window size. Default - For environments that are to support a large number of connections with low RAM should use: 4194304 For environments that are for performance, have high RAM, then can use this setting: 16777216
net.inet.tcp.rfc1323	1	Enables TCP extensions for high performance, such as window scaling and timestamps, which are essential for managing large TCP window sizes and improving throughput.
net.inet.tcp.sendbuf_max	4194304	Improved Performance: TCP Buffers: Larger buffers and TCP Large Window Extensions (RFC1323) can help alleviate the long fat network (LFN) problem caused by insufficient window size. Default - For environments that are to support a large number of connections with low RAM should use: 4194304 For environments that are for performance, have high RAM, then can use this setting: 16777216
net.inet.tcp.sendbuf_inc	65536	Improved Performance: TCP Buffers: Larger buffers and TCP Large Window Extensions (RFC1323) can help alleviate the long fat network (LFN) problem caused by insufficient window size. Default - For environments that are to support a large number of connections with low RAM should use: 65536 For environments that are for performance, have high RAM, then can use this setting: 524288
net.inet.tcp.soreceive_stream	1	Using soreceive_stream for TCP sockets
net.inet.tcp.syncache.rexmtlimit	0	Reduce the amount of SYN/ACKs the server will re-transmit to an ip address who did not respond to the first SYN/ACK. (Default 3)
net.pf.source_nodes_hashsize	1048576	Improved Performance: Increases the packet filter hash table size to allow more connections in the table before performance deteriorates.
net.pfsync.carp_demotion_factor	0	pfsync's CARP demotion factor adjustment
net.raw.recvspace	65536	Default raw socket receive space
net.raw.sendspace	65536	Default raw socket send space
net.route.netisr_maxqlen	1024	Maximum routing socket dispatch queue length

Security related and optional settings, there are recommended to be left with the default settings:

Tunable	Value	Description
hw.ibrs_disable	0	Disable Indirect Branch Restricted Speculation (Specter V2 mitigation). 0 (Default) is Disabled, 1 is Enabled Intel Chips are likely to require this, however, depends on the environment. Performance may or may not be impacted if enabled.
vm.pmap.pti	0	Page Table Isolation (Meltdown mitigation, requires reboot.) For Intel based CPUs, such as Xeons, this can be disabled as they are not vulnerable.
net.inet.tcp.recvbuf_inc	524288	Optional: Governs the receive window autotuning step size but may not be needed.

IF any additions or changes are made, then click on the Apply Change button.

NOTE: A reboot is required for the settings to take effect.

To Reboot, go to Power > Reboot, and click on Yes.

Download Site Configuration File

Downloading the configuration file from this firewall involves accessing its administrative interface and navigating to the backup or export settings section. Here, users can find an option to download the current configuration file, which includes all the settings, rules, and policies configured on the firewall. This file is crucial for creating backups, performing migrations, or restoring settings in case of a system failure. The configuration file is downloaded in in XML format and should be stored securely to prevent unauthorized access. Proper management and safeguarding of this file ensure that critical network settings can be easily restored or transferred as needed..

1. Go to System > Configuration > Backups
2. Click on Download Configuration
3. Save the Configuration to the same location of the Backup Site Files

Perform Reboot and System Checks

4. Go to Power > Reboot
5. Click on Yes to Reboot
6. Log in and review that the Cloaking Firewall is functioning properly.

Congratulations on completing the installation of your Cloaking Firewall! With the setup now finished, your network is equipped with enhanced security measures to protect against unauthorized access and potential threats. It is important to regularly update your firewall software, review and adjust your security policies, and monitor network traffic to maintain optimal performance and security. Additionally, consider creating regular backups of your configuration settings to ensure you can quickly restore your firewall in case of any issues. Your network is now more secure, and you can confidently manage and protect your digital assets.

Troubleshooting

Disable the Firewall in case of Lockout

Should a lockout occur, the following command may help in regaining access.

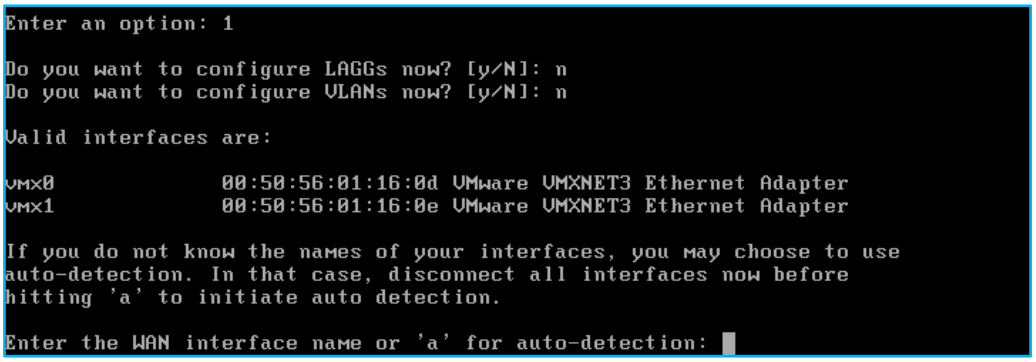
1. In AWS, go to the EC2 Serial Console of the Cloaking Firewall.
2. Log in as root.
3. Hit 8 and enter, to access the Shell.
4. To disable the firewall, type:
   ```
   sysctl -d
   ```
5. Attempt to access the firewall and perform troubleshooting procedures to determine the cause of the incident.
6. A possible temporary fix is to enable a Maintenance rule that enables WebGUI access, such as with the WAN.
7. Every time Apply Changes are made, the lockout may continue. Go back to the console and run the command again to disable the firewall rules.
8. After changes are made and a lockout still seems in effect, try a reboot with the firewall.

Resetting to Default Configuration

To implement the Default Configuration (also known as Factory Reset) is done through the terminal as the only means of performing the reset to defaults as this is not possible through the WebGUI.

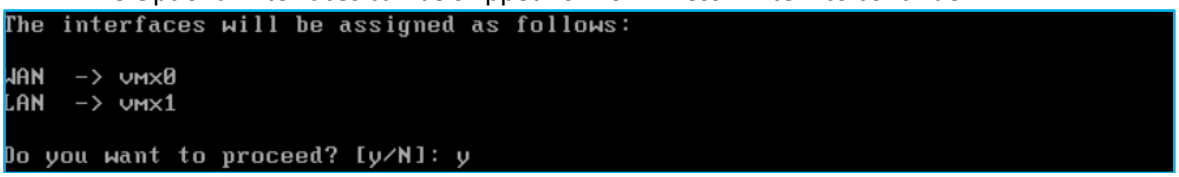
1. At the terminal, if not already logged in, please log in.
2. At the terminal menu, type “4” and press “Enter” to “Reset to factory defaults.”
3. At the confirmation warning, type “y” and press “Enter”.
4. The machine may power down, if so, go to physical device and power back on. If using a virtualized environment, then perform a power on for the virtual machine.
5. At the terminal log in screen, log in.
6. Let the Cloaking Firewall complete the bootup process until the Login prompt:
7. To log in, type:
   Login: root
   Password: internet2-0.com
8. The console menu will appear. Note that the interfaces have to be redone as the WAN has no field listed and the LAN has a 192.168.0.1/24 IP Address.

9. If the default LAN (10_LAN1) interface IP Address is the correct address to be used, then please skip the following terminal steps and log into the WebGUI.
10. Otherwise, the interfaces will need to be configured first.
11. Enter “1” and then press “Enter” to assign the interfaces:
    a. LAGGs: N (and then press “Enter”)
    b. VLANs: N (and then press “Enter”)
    c. There will be a listing of interfaces with their MAC physical addresses listed. Identify which interface will be used for the WAN and LAN.



Shown above are two interfaces, this for with use in Vmware.
The WAN will be using vmx0, while the LAN will use vmx1.

d. For the WAN (which is normally the Internet facing interface), type in the interface identifier, then press “Enter” to continue.
e. For the LAN (which would be for the private local network), type in the interface identifier, then press “Enter” to continue.
f. The Optional interfaces can be skipped for now. Press “Enter” to continue.



Above is an example of assigning the interfaces.

g. If there are no typos, type in “y” and then press “Enter” to proceed.
    i. If there has been a mistake, hit CTRL-C to start again.

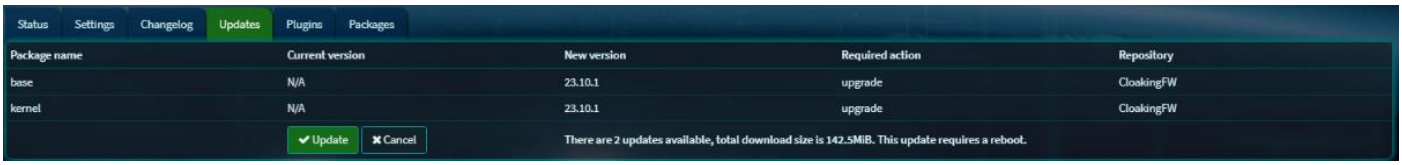
12. When the assignments have been completed, to set IP addresses of the 10_LAN1, press “2” and then “Enter”.

At this time, log back into the WebGUI.

Errata

Performing Additional Updates

There is currently a software bug from performing updates, in which there will be showing of just the Base and Kernal with versions 23.10.1. There is no need to perform a second update due to these artifacts. If another update is performed, there is no effect, other than for a reboot.



Appendix A: Improve IDPS Performance

The bandwidth throughput performance of the IDPS can be greatly improved by applying the following tunable settings.

These settings make use of Receive Side Scaling (RSS), which not all Network Interfaces support. However, these settings are very likely to improve throughput considerably when using the IDPS in Protection mode. There have been problems with DNS not working properly with pulling Updates. If such problems occur, then remove or disable these settings, or during performing updates.

1. Go to System > Settings > Tunables
2. Add the following Tunables and click Apply Changes. Reboot when completed.

Tunable	Value	Description
net.isr.bindthreads	1	Improved Performance. Binds each of the ISR threads to 1 CPU core
net.isr.dispatch	deferred	Improved Performance. To "deferred" or "hybrid" is required to make the other net.isr tunables
net.isr.maxthreads	-1	Improve performance. Uncaps the amount of CPU's which can be used for netisr processing.
net.inet.rss.bits	**2**	Improved Performance. Receive Side Scaling, this RSS value is based on the number of CPU cores of the virtual machine. 1 - for 2-core systems, 2 - for 4-core systems, 3 - for 8-core systems, 4 - for 16-core systems
net.inet.rss.enabled	**1**	Improved Performance. Receive Side Scaling, this RSS setting improves parallel processing of network traffic on multi-core systems.

Notes about the settings:

- **net.isr.bindthreads: 1**
  - **Effect**: Binds interrupt service routines (ISRs) to specific threads, which can improve CPU affinity and cache utilization.
  - **Impact**: This can enhance performance on multi-core systems by reducing context switches and keeping ISR handling on the same CPU core.

- **net.isr.dispatch: deferred**
  - **Effect**: Defers the handling of ISRs to a later time, reducing the immediate processing burden.
  - **Impact**: This can help in scenarios with high packet rates by spreading out the processing load, leading to better throughput.

- **net.isr.maxthreads: -1**
  - **Effect**: Allows the system to use as many threads as there are CPU cores.
  - **Impact**: This can maximize parallelism, especially on multi-core systems, leading to improved performance.

- **net.inet.rss.bits: #**
  - **#**: Set this number to the number of available cores as listed in the table. For cores that are not listed, then use the next level higher. For example, a 6 core CPU will have a value of 3.
  - **Effect**: Sets the number of bits used for Receive Side Scaling (RSS), which helps distribute incoming network traffic across multiple CPU cores.
  - **Impact**: Enhances parallel processing of network packets, which can improve throughput.

- **net.inet.rss.enabled: 1**
  - **Effect**: Enables RSS, which distributes network traffic to different CPU cores.
  - **Impact**: Improves load balancing and parallel processing, leading to better performance.

Appendix B: Implement Multi-Factor Authentication

NOTE: Requires the use of Google or Microsoft Authenticators.

For use of Multi-Factor Authentication (MFA), a TOTP (Time-based One Time Password) server is enabled. An MFA TOTP Server will be set up for the use of logging in locally as a Firewall Administrator and for VPN Access (example: VPN Users).

To login (either for the VPN or WebGUI) for the password, the user will enter/paste the Password and then enter in the MFA Code from the Authenticator, using no spaces.

For example:

Password is:	internet2-0.com
MFA Code at the give time is:	123123
Thus, the user will enter:	internet2-0.com123123

Implementing the TOTP (Time-based One Time Password) server for access:

1. Go to System > Access > Servers
2. Click on the Add button
    a. Descriptive Name: MFA TOTP Server
    a. Type: Local + Timebased One Time Password
    b. Reverse token order: Checked
    This allows for the password to be typed/pasted first, then enter in the MFA number.
    c. Leave all other settings as Defaults
    d. Click on Save

Add in MFA for Administrative WebGUI Logins

1. Go to System > Settings > Administration
2. Scroll down to the Authentication section.
3. Change Server to: MFA TOTP Server, Local Database
    This will be changed after the installation and added by other users.
4. Click on Save

Appendix C: Monit - Email Notifications for MS Office

Microsoft Azure

Create User Account

1. Go to: https://portal.azure.com
2. Log in with an Admin Account
3. Go to Users
4. Click to Add New User
    a. User Principle Name: *emailname@domain.ext*
    Example: alerts@example.com
    b. Mail Nickname: Leave as default
    c. Display Name: System Alerts
    d. Password: Password for the Email Address
    e. Account Enabled: Checked
5. Click on Next: Properties
    a. First Name: System
    b. Last Name: Alerts
    c. User Type: Member
6. Click on Next: Assignments:
    a. Ensure there are no Administrator Roles
    b. Add groups if by organizational policies
7. Click on Next: Review and Create
8. After Reviewing, click on Create

Set Usage Location

1. Scroll down and click on the newly created user account (System Alerts)
    a. May need to refresh and/or wait
2. Click on Settings tab
    a. Usage location: Country of the Organization
3. Click on Save

Assign License

1. Click on Licenses (left side menu)
2. Add a new Assignment
3. Check the license to use (ex: Microsoft 365 Business Standard)
4. Select the license options allowed
    a. Examples: Exchange Online (Plan 1)
5. Click on Save

Exclude Multi-Factor Authentication (MFA)

1. Go to Home
2. Search for, or click on “Microsoft Entra ID”
3. Click on Security (Left side menu)
4. Click on Conditional Access (Left side menu)
5. Click on Policies (Left side menu)

6. Search for “CA004: Require multifactor authentication for all users”
7. Click on “CA004: Require multifactor authentication for all users”
8. At left side, click on Users: “All users included, and specific users excluded”
9. Click on the Exclude tab
10. Under “Select excluded users and groups”, click on the link that shows “# users”
11. Search for the new user account “System Alerts”
12. Check the box for “System Alerts”
13. Click on Select
14. Click on Save (Lower left corner)
15. Verify that the user account has been excluded.

Microsoft Office Admin Console

Enable SMTP for User’s Mailbox

1. Go to: https://admin.microsoft.com
2. Expand Users (Left side menu)
3. Click on Active Users
4. Scroll down and click on the new user account “System Alerts”
    a. At the flyout (right side), click on the Mail tab
    b. Click on Manage email apps
    c. Check “Authenticated SMTP”
5. Click on Save Changes

Microsoft Exchange

Add SMTP Email Address

1. Go to: https://admin.exchange.microsoft.com
2. Expand the Recipients menu (Left side menu)
3. Click on Mailboxes
4. Scroll down and click on the new user account (System Alerts)
5. At the flyout (right side), click on “Manage email address types”
6. Click on “Add email address type”
    a. SMTP: Selected
    b. Email Address: *emailname*@*domain*.onmicrosoft.com
        i. Example: *alerts*@*example*.onmicrosoft.com
    c. Click on Save

Microsoft Online

Log in with the New Account

1. Go to: https://login.microsoftonline.com
2. Enter in the login ID: *emailname@domain.ext*
   alerts@example.com
3. Enter in the Password:
4. More information required window:
    a. Click on Next
5. Pick an Account

a. The new account
6. Microsoft Authenticator window, click on Skip setup
7. Stayed signed in window, click on No
8. At the Splash screen, go through the Welcoming
9. Click on the Outlook icon (Left side menu)
10. Go through the process of logging into Outlook
    a. Skip the Authenticator
    b. Click on “No” to stay logged in.

Setup Email Forwarding

1. Click on Settings (Gear icon, top right corner)
2. Click on Rules
3. Click on Add New Rule
    a. Name: Alert Email Forwarding
    b. Add a Condition:
    c. From: New User Address (*emailname@domain.ext*)
       Example: alerts@example.com
        i. To: New User Address (*emailname@domain.ext*)
           Example: alerts@example.com
        ii. Subject Includes: [ALERT]
        iii. Message Body includes: Monit Alert Notification
    d. Add an Action:
        i. Forward to: Add in the email addresses
        ii. Marked as Read
        iii. Move to: New Folder, Processed_Alerts
        iv. Marked with Importance: High
    e. Stop process more rules: Checked
4. Click on Save
5. Close the Rules window
6. Log out of Outlook

Cloaking Firewall Monit Settings

3. Log into the Cloaking Firewall
4. Go to Services > Monit > Settings
5. Set, “Advanced Mode” to Enable
    a. Mail Server Address: smtp.office365.com
    b. Mail Server Port: 587
    c. Mail Server Username: *emailname@domain.ext*
       Example: alerts@example.com
    d. Mail Server Password: The password for the service account
    e. Mail Server SSL Connection: Checked
    f. SSL Version: TLSV12
    g. Verify SSL Certificates: Checked
    h. Click on Save
6. Go to Alert Settings
    a. Copy the Monit Event Template

b. Enable Alert: Checked
c. Recipient: Use the SMTP Address with .onmicrosoft
emailname@*domain*.onmicrosoft.com
Example: alerts@example.onmicrosoft.com
d. Events: Select the Event or Events
e. Mail Format: Modify where needed.
f. Description: Set a description of the Alert
g. Click on Save

7. Click on Apply

Example to Send Alerts based on Status Failure (for failure with Hard Drive Storage)

a. Copy the Monit Event Template
b. Enable Alert: Checked
c. Recipient: *emailname*@*domain*.onmicrosoft.com
Example: alerts@example.onmicrosoft.com
d. Events: Status Failure
e. Mail Format:

From: *emailname@domain.ext*
Reply-To: *support@domain.ext*
Subject: [ALERT] Instance Changed
Message: Monit Alert Notification:
Event: $EVENT Service $SERVICE
Date: $DATE
Action: $ACTION
Host: $HOST
Description: $DESCRIPTION

Respectfully,
Internet 2.0 CFW Notification Service Alert

f. Description: Status Failure

Appendix D: Cloaking Nginx (Reverse Proxy) from Scans

Nginx, when used as a reverse proxy, acts as an intermediary between clients and backend servers, effectively protecting and optimizing websites. By routing client requests to the appropriate server, Nginx enhances security by masking the backend infrastructure and providing an additional layer of defense against attacks. It can also manage SSL/TLS encryption, ensuring secure communication, and distribute the load among multiple servers to improve performance and reliability. Utilizing Nginx as a reverse proxy helps safeguard websites from threats such as DDoS attacks, improves response times, and ensures seamless access to web applications.

These steps will allow for the Nginx Reverse Proxy to be protected by the IDPS. This will help to prevent its certificates, as the Secured_Certificate from being discovered. Nginx will now only listen to an assigned Virtual IP on the Local Network(s). Traffic that comes the Internet is Port Forwarded to the new Nginx VIP.

Install Nginx Plugin

1. Log into the Cloaking Firewall
2. Install Nginx, by going to System > Firmware > Plugins
3. Search for “cfw-nginx” and click on the Plus “+” to install Nginx.
4. The Updates tab will be shown and wait until the plugin has completed the installation.

Configure IDPS

1. When the plugin has been installed, verify IDPS has the VIP protected by going to IDPS > Administration > Settings
    a. Click on the Advance Mode slider
    b. Verify that the Nginx VIP is in the Home Networks or as part of the LAN CIDR.
        i. If not, add in the Nginx VIP into the Home Networks and click on Apply

Configure Virtual IP

1. Create a new Virtual IP (VIP) Address for Nginx to respond to.
    a. Go to Interfaces > Virtual IPs > Settings
    b. Click to add a new VIP
        i. Mode: IP Alias
        ii. Interface: 11_LAN1
        iii. Network/Address: 172.24.10.253/32 (Example)
        iv. Deny Service binding: Unchecked
        v. VHID Group: Blank
        vi. Description: Nginx VIP
    c. Click on Save
2. Create a Firewall Alias:
    a. Go to Firewall > Aliases
    b. Click to add a new Alias
        i. Enabled: Checked
        ii. Name: HOST_Nginx_VIP
        iii. Type: Host(s)
        iv. Categories: CloakingFW
        v. Content: The Nginx VIP (ex: 172.24.10.253)
        vi. Statistics: Unchecked
        vii. Description: The Virtual IP of Nginx Reverse Proxy
    c. Click on Save
    d. Click on Apply

Configure Nginx

1. Configure Nginx Service, by going to Services > Nginx > Configuration
2. General Settings:
    a. Click on the Advanced Mode slider
    b. Enable nginx: Checked
    c. Autoblock TTL (minutes): 60
3. Click on the General Settings dropdown menu and select Global HTTP Settings
    a. Worker Processes 1
    b. Worker Connections 1024
    c. Enable sendfile Unchecked
    d. Keepalive Timeout 60
    e. Reset Timed Out Connections Unchecked
    f. Default MIME-Type Blank
    g. Hash Bucket Size Blank
    h. Server Names Hash Max Size Blank
    i. Autoban Response Code Blank
    j. Enable Headers More module 403 Forbidden
4. Click on Apply

Download NAXSI WAF Rules

5. Go to the HTTP(s) dropdown tab and select NAXSI WAF Policy
    a. Click on the Download button to download the rules
    b. Click on Accept and Download button

Set up Server

6. Go to the Upstream dropdown tab and select Upstream Server
    a. Click on the Plus “+” button to add a new Server.
    b. Description: A description or name of the server. Ex: Windows_Webserver
    c. Server: The Private IP Address of the server. Ex: 10.0.20.100
    d. Port: The port used for the server. Ex: 80
    e. Server Priority: 1
    f. Maximum Connections: Blank or set limit. Generally, 1 user is roughly equal to 4 connections
    g. Maximum Failures: Blank or set a limit of failed attempts
    h. Fail Timeout: Blank or set a time limit.
7. Click on Save

Set up Server Group

8. Go to the Upstream dropdown tab and select Upstream
    a. Click on the Plus “+” button to add a new Group.
    b. Click on the Advanced mode slider
    c. Description: Description or name of the server. Ex: Windows_Webserver_Group
    d. Server Entries Select the server (Ex: Windows_Webserver)
    e. Load Balancing Algorithm Weighted Round Robin
    f. PROXY Protocol Unchecked
    g. Host header port Blank
    h. XFH: Use original Host header Unchecked
    i. Enable TLS (HTTPS) Checked
    j. TLS: Client Certificate Secured_Certificate
    k. TLS: Servername override Secured_Certificate
    l. TLS: Supported Versions TLSv1.2, TLSv1.3

m. TLS: Session Reuse — Checked
n. TLS: Trusted Certificate — Nothing Selected
o. TLS: Verify Certificate — Checked
p. TLS: Verify Depth — 2
q. Store — Unchecked

9. Click on Save

Set up Locations

10. Go to the HTTP(s) dropdown tab and select Location
    a. Click on the Plus "+" button to add a new location.
    b. Description: — Provide description, such as "Windows_Webserver_Location"
    c. URL Pattern: — /
    d. Match Type: — None
    e. URL Rewriting: — Nothing Selected
    f. Enable Security Rules: — Checked
    g. Learning Mode: — Unchecked (unless want to observe of what would be banned before implementing banning capability)
    h. Violate Error Page: — None
    i. Block XSS Score: — 4
    j. Block SQL Injection Score: — 4
    k. Customer Security Policy: — Select All Policies (unless to choose certain ones)
    l. Upstream Servers: — The Group that was created (Ex: Windows_Webserver_Group)
    m. Path Prefix: — Blank
    n. Cache Directory: — None
    o. Cache: Use Stale: — Nothing Selected
    p. Cache: Minimum Uses: — 1
    q. Cache: Background Update — Unchecked
    r. Cache: Lock Backend on Update — Unchecked
    s. Cache: Revalidate — Unchecked
    t. Cache: HTTP Verbs — Nothing Selected
    u. Limit Requests — Nothing Selected
    v. File System Root — Blank
    w. Maximum Body Size — Blank
    x. Body Buffer Size — Blank
    y. Index File — Blank
    z. Automatic Index — Unchecked
    aa. Basic Authentication — Blank
    bb. Basic Credentials List — None
    cc. Enable Advanced ACLs — Unchecked
    dd. IP ACL — None
    ee. Satisfy — None
    ff. Force HTTPS — Checked
    gg. Enable HTTP/2 Preloading — Unchecked
    hh. Pass Request To Local PHP Interpreter / Threat Upstream As FastCGI — Unchecked
    ii. (PHP) Router Script — Blank
    jj. Honeypot — Unchecked

    Advanced Proxy Options

    kk. WebSocket Support — Unchecked

ll. Proxy Read Timeout 180
mm. TLS SNI Forwarding Unchecked
nn. Proxy Buffer Size (kB) 128
oo. Proxy Buffers: Count 4
pp. Proxy Buffers: Size (kB) 256
qq. Proxy Busy Buffers Size (kB) 356
rr. Proxy Send Timeout Blank
ss. Response Buffering Checked
tt. Request Buffering Checked
uu. Maximum Temporary File Size Blank
vv. Ignore Client Abort Unchecked
ww. Error Pages Nothing Selected

11. Click on Save

Set up HTTP Server

12. Go to the HTTP(s) dropdown tab and select HTTP Server
13. Click on the Plus "+" button to add a HTTP Server
    a. Click on the Advanced Mode slider
    b. HTTP Listen Address: Provide the port to listen for HTTP
       Example: 80 or 8080
       If using IPv6, then use [::]: before the port
       Example: [::]:80 [::]:8080
    c. HTTPS Listen Address: Provide the port to listen for HTTPS
       Example: 443 or 4443
       If using IPv6, then use [::]: before the port
       Example: [::]:443 [::]:4443
    d. Default Server: Checked
    e. Reject SSL Handshake Unchecked
    f. SYSLOG targets Nothing selected
    g. PROXY Protocol Unchecked
    h. Trusted Proxies Blank
    i. Trusted Proxies (Firewall Alias) None
    j. Real IP Source None
    k. Server Name: Add in the new Nginx VIP (Ex: 172.24.10.253)
    l. Locations Add in the Location (Ex: Windows_Webserver_Location)
    m. URL Rewriting Nothing selected
    n. File System Root Blank
    o. Maximum Body Size Blank
    p. Body Buffer Size Blank
    q. TLS Certificate Secured_Certificate
    r. Client CA Certificate None
    s. Verify Client Certificate Off
    t. Zero RTT Unchecked
    u. Access Log Format Default
    v. Error Log Level Error (default)
    w. Enable Checked
       Let's Encrypt Plugin Support
    x. Charset utf-8
    y. HTTPS Only Checked

z. TLS Protocols — TLSv1.2, TLSv1.3

aa. TLS Ciphers — ECDHE-ECDSA-CAMELLIA256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CAMELLIA256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-CAMELLIA128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CAMELLIA128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-AES128-SHA256

bb. ECDH curve — Blank

cc. Prefer server ciphers — Checked

dd. OCSP Stapling — Unchecked

ee. OCSP Verify — Unchecked

ff. Block Configuration Files — Unchecked

gg. Disable Bot Protection — Unchecked

hh. IP ACL — None

ii. Advanced ACL Authentication Backend — Local Database

jj. Satisfy — None

kk. Naxsi Trusted Source IPs — Blank

ll. Extensive Naxsi Log — Unchecked

mm. Enable Sendfile — Checked

nn. Header Buffer Size (kB) — 1

oo. Count Of Large Header Buffers — 4

pp. Size Of Large Header Buffers (kB) — 8

qq. Security Header — None

rr. Limit Requests — Nothing Selected

ss. Error Pages — Nothing Selected

14. Click on Save

Set DDoS and Scan Limits

15. Go to the Access dropdown tab and select Limit Zone
16. Click on the Plus “+” button to add a new Zone
    a. Description — Description or name of the Zone Ex: DDoS_Limit_Rate_Requests_Timing
    b. Key — Remote IP Address
    c. Size (MB) — 20
    d. Rate — 30
    e. Rate Unit — Request Per Minute
17. Click on Save
18. Click on the Plus “+” button to add a new Zone
    f. Description: — Description or name of the Zone Ex: Scan_Limit_Rate_Requests_Timing
    g. Key — Remote IP Address
    h. Size (MB) — 20
    i. Rate — 10
    j. Rate Unit — Request Per Second
19. Click on Save
20. Go to the Access dropdown tab and select Connection Limits

21. Click on the Plus "+" button to add a new Limit
    k. Description: Description or name of the Limit
       Ex: DDoS_Limit_Rate_Requests_Connections
    l. Limit Zone: DDoS_Limit_Rate_Requests_Timing
    m. Connection Count (Streams Only): 10
    n. Burst (HTTP Only): 20
    o. No Delay (HTTP Only): 1
22. Click on Save
23. Go to the General Settings tab
24. Click on Apply

Configure Firewall

Create Port Forwarding

3. Create Firewall Rules (Port Forwarding):
    a. Go to Firewall > NAT > Port Forward
    b. Click to add a new Port Forwarding Rule
        i. No RDR (NOT): Unchecked
        ii. Interface: 01_WAN1
        iii. TCP/IP: IPv4
        iv. Protocol: TCP/UDP
        v. Source: Any
        vi. Destination: 01_WAN1 Address
        vii. Destination Port: PORTS_NGINX_Protected
        viii. Redirect Target IP: HOST_Nginx_VIP
        ix. Redirect Target Port: PORTS_NGINX_Protected
        x. Log: Checked:
        xi. Category: Infrastructure
        xii. Description: Inbound - Allow - Nginx: Internet Access to Nginx Reverse Proxy
        xiii. Click on Save
    c. Move the Port Forward Rule where needed if at current location is not acceptable.
    d. Click on Apply Changes
    e. Go to Firewall > Rules > 01_WAN1
        i. Verify that the position of the Firewall Rule of the Port Forwarding Rule is satisfactory.
            1. If not, move to the acceptable position and click Apply Changes

Create Floating Rule Forwarding

1. Go to Firewall > Rules > Floating
2. Click to add a new Port Forwarding Rule
    a. Action: Block
    b. Interface: 01_WAN1, 10_LAN1
    c. Direction: In
    d. TCP/IP Version: IPv4+IPv6
    e. Protocol: any
    f. Source: nginx_autoblock
    g. Destination: any
    h. Destination Port: any
    i. Log: Checked
    j. Category: Blacklist
    k. Description: Deny - Inbound: Blacklist from Nginx Banned List

l. Click on Save

3. Click on Apply Changes

Add TLS/SSL Certificate to Endpoint

If an endpoint does not have a TSL/SSL certificate than the Security_Authority certificate can be used.

Please refer to the endpoint system of how to install the certificate.

SYN Based Scan Limitation and Mitigation

However, SYN based Scans will still be capable of detecting that the port is opened and using Nginx, just like a TCP Connect scan would, but still will not be able to gain information of the service and certificate.

To ensure that SYN based scans and perhaps others, will not work, then the 01_WAN1 IP address needs to be included with the IDPS. Note, that this can impact performance as the IDPS is scanning two interfaces. To help with performance, if using a cloud provider Firewall, limit the number of opened ports.

Perform the following steps to allow for the IDPS to protect the WAN and thereby defeat SYN scans:

1. Go to IDPS > Administration > Settings
    a. Click on the Advance Mode slider
    b. Interfaces, add: 01_WAN1
    c. Home networks, add: Add WAN1's IP (ex: 172.24.0.254)
    d. Click on Apply

Appendix E: Systems and Versions

Name	Version	License	Comment
base	23.10.1	BSD2CLAUSE	FreeBSD userland set
beep	1.0_2	BSD4CLAUSE	Beeps a certain duration and pitch out of the PC Speaker
Boost-libs	1,84.0	BSL	Free portable C++ libraries (without Boost.Python)
ca_root_nss	3.93	MPL20	Root certificate bundle from the Mozilla Project
cfw-raiden	0.1.1.0	BSD2CLAUSE	Internet 2.0's RAIDEN
cfw-telegraf	1.12.10	BSD2CLAUSE	Agent for collecting metrics and data
cfw-wireguard	2.6	BSD2CLAUSE	Wireguard VPN service kernel implementation
choparp	20150613_1	BSD3CLAUSE	Simple proxy arp daemon
cloakingfw-business	23.10.1_1063	BSD2CLAUSE	CloakingFW business release
cloakingfw	23.7.0_1464	BSD2CLAUSE	CloakingFW community release
cloakingfw-installer	23.7	BSD2CLAUSE	CloakingFW installer scripts
cpdup	1.22_1	BSD2CLAUSE	Comprehensive filesystem mirroring and backup program
curl	8.6.0	MIT	Command line tool and library for transferring data with URLs
cyrus-sasl	2.1.28_4	BSD4CLAUSE	RFC 2222 SASL (Simple Authentication and Security Layer)
cyrus-sasl-gssapi	2.1.28	BSD4CLAUSE	SASL GSSAPI authentication plugin
dhcp6c	20230530	BSD3CLAUSE	OPNsense WIDE-DHCPv6 client
dhcprelay	0.3	BSD3CLAUSE	OpenBSD dhcprelay daemons
dnsmasq	2.90_1,1	GPLv2	Lightweight DNS forwarder, DHCP, and TFTP server
dpinger	3.3	BSD2CLAUSE	IP device monitoring tool
e2fsprogs-libuuid	1.47.0	BSD3CLAUSE	UUID library from e2fsprogs package
easy-rsa	3.1.7	GPLv2	Small RSA key management package based on openssl
expat	2.6.2	MIT	XML 1.0 parser written in C
filterlog	0.7_1	BSD3CLAUSE	Parse pflog(4) output
flock	2.37.2_1	GPLv2	Manage locks from shell scripts
flowd	0.9.1_5	BSD2CLAUSE	Small, fast, and secure NetFlow collector
gettext-runtime	0.22_5	GPLv3+	GNU gettext runtime libraries and programs
glib	2.80.0,2	LGPL20	Some useful routines of C programming (current stable version)
gmp	6.3.0	LGPL3	Free library for arbitrary precision arithmetic
hostapd	2.10_10	BSD3CLAUSE	IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator
hyperscan	5.4.0	BSD3CLAUSE	High-performance multiple regex matching library
icu	74.2_1,1	ICU	International Components for Unicode (from IBM)
ifinfo	13.0_1	MIT	Interface statistics reader
iftop	1.0.p4_1	GPLv2	Display bandwidth usage on an interface by host
indexinfo	0.3.1	BSD2CLAUSE	Utility to regenerate the GNU info page index
isc-dhcp44-server	4.4.3P1_1	MPL20	ISC Dynamic Host Configuration Protocol server
ivykis	0.43_1	LGPL21	Asynchronous I/O readiness notification library
jansson	2.14	MIT	C library for encoding, decoding, and manipulating JSON data
json-c	0.17	MIT	JSON (JavaScript Object Notation) implementation in C
kea	2.4.1_2	MPL20	Alternative DHCP implantation by ISC
kernel	23.10.1	BSD3CLAUSE	FreeBSD kernel set
krb5	1.21.2_3	MIT	MIT implementation of RFC 4120 network authentication service
ldns	1.8.3_!	BSD3CLAUSE	Library for programs conforming to DNS RFCs and drafts
libargon2	20190702_1	CC0-1.0	Memory hard password hashing program and library
libcbor	0.11.0	MIT	CBOR protocol implementation for C and others
libcjson	1.7.17	MIT	Ultralightweight JSON parser in ANSI C
libedit	3.1.20230828_1,1	BSD2CLAUSE	Command line editor library
libevent	2.1.12	BSD3CLAUSE	API for executing callback functions on events or timeouts

libffi	3.4.4_1	MIT	Foreign Function Interface
libfido2	1.14.0	BSD2CLAUSE	Provides library functionality for FIDO 2.0
libiconv	1.17_1	GPLv3	Character set conversion library
libidn2	2.3.7	GPLv3	Implementation of IDNA2008 internationalized domain names
libinotify	20211018_1	MIT	Kevent based inotify compatible library
libltdl	2.4.7	LGPL21	System independent dlopen wrapper
liblz4	1.9.4_1,1	BSD2CLAUSE	LZ4 compression library, lossless and very fast
libmcrypt	2.5.8_4	LGPL21+	Multi-cipher cryptographic library (used in PHP)
libnet	1.3,1	BSD2CLAUSE	C library for creating IP packets
libnghttp2	1.60.0	MIT	HTTP/2.0 C Library
libpfctl	0.10	BSD2CLAUSE	Library for interaction with pf(4)
libpsl	0.21.5	MIT	C library to handle the Public Suffix List
libsodium	1.0.18	ISCL	Library to build higher-level cryptographic tools
libucl	0.9.1	BSD2CLAUSE	Universal configuration library parser
libunistring	1.2	GFDL	Unicode string library
libxml2	2.11.7	MIT	XML parser library for GNOME
libyaml	0.2.5	MIT	YAML 1.1 parser and emitter written in C
lighttpd	1.4.75	BSD3CLAUSE	Secure, fast, compliant, and flexible Web Server
Log4cplus	2.1.1	APACHE20	Logging library for C++
lzo2	2.10_1	GPLv2	Portable speedy, lossless data compression library
monit	5.33.0_1	AGPLv3	Unix system management and proactive monitoring
mpd5	5.9_18	BSD3CLAUSE	Multi-link PPP daemon based on netgraph(4)
mpdecimal	4.0.0	BSD2CLAUSE	C/C++ arbitrary precision decimal floating point libraries
nettle	3.9.1	GPLv2+	Low-level cryptographic library
nspr	4.35	MPL20	Platform-neutral API for system level and libc like functions
nss	3.98	MPL20	Libraries to support development of security-enabled applications
oniguruma	6.9.9	BSD2CLAUSE	Regular expressions library compatible with POSIX/GNU/Perl
openldap26-client	2.6.7	OPENLDAP	Open-source LDAP client implementation
openssh-portable	9.7.p_1,1	OPENSSH	The portable version of OpenBSD's OpenSSH
openssl	3.0.13_1,1	OpenSSL	TLSv1.3 capable SSL and crypto library
openvpn	2.6.9	GPLv2	Secure IP/Ethernet tunnel daemon
opnsense-installer	23.7	BSD2CLAUSE	CloakingFW installer scripts
opnsense-lang	23.7.11	BSD2CLAUSE	OPNsense translations
opnsense-update	23.10.1	BSD2CLAUSE	CloakingFW update utilities
pam_opnsense	24.1	BSD2CLAUSE	OPNsense shared authentication system using PAM
pcre	8.45_3	BSD3CLAUSE	Perl Compatible Regular Expressions library
pcre2	10.43	BSD3CLAUSE	Perl Compatible Regular Expressions library, version 2
perl5	5.34.3_3	ART10	Practical Extraction and Report Language
pftop	0.10_1	BSD2CLAUSE	Utility for real-time display of statistics for pf
php82	8.2.17	PHP301	PHP Scripting Language (8.2.X branch)
php82-ctype	8.2.17	PHP301	The ctype shared extension for php
php82-curl	8.2.17	PHP301	The curl shared extension for php
php82-dom	8.2.17	PHP301	The dom shared extension for php
php82-filter	8.2.17	PHP301	The filter shared extension for php
php82-gettext	8.2.17	PHP301	The gettext shared extension for php
php82-google-api-php-client	2.4.0	APACHE20	Google APIs Client Library for PHP
php82-ldap	8.2.17	PHP301	The ldap shared extension for php
php82-mbstring	8.2.17	PHP301	The mbstring shared extension for php
php82-pcntl	8.2.17	PHP301	The pcntl shared extension for php
php82-pdo	8.2.17	PHP301	The pdo shared extension for php
php82-pear	1.10.13	PHP301	PEAR framework for PHP
php82-pecl-mcrypt	1.0.6	PHP301	PHP extension for mcrypt, removed in PHP 7.2

php82-pecl-radius	1.4.0b1_2	BSD3CLAUSE	Radius client library for PHP
php82-phalcon	5.6.2	BSD3CLAUSE	Phalcon PHP Framework written in C-language
php82-phpseclib	3.0.36	MIT	PHP Secure Communications Library
php82-session	8.2.17	PHP301	The session shared extension for php
php82-simplexml	8.2.17	PHP301	The simplexml shared extension for php
php82-sockets	8.2.17	PHP301	The sockets shared extension for php
php82-sqlite3	8.2.17	PHP301	The sqlite3 shared extension for php
php82-xml	8.2.17	PHP301	The xml shared extension for php
php82-zlib	8.2.17	PHP301	The zlib shared extension for php
pkcs11-helper	1.29.0_3	BSD3CLAUSE	Helper library for multiple PKCS#11 providers
pkg	1.19.2_1	BSD2CLAUSE	Package manager
py39-aioquic	0.9.25	BSD3CLAUSE	Implementation of QUIC and HTTP/3
py39-anyio3	4.3.0	MIT	High level compatibility layer for multiple asynchronous event loop implementations
py39-async_generator	1.10	APACHE20	Tiny library to add async generators to Python 3.5
py39-attrs	23.2.0	MIT	Python attributes without boilerplate
py39-Babel	2.14.1	BSD3CLAUSE	Collection of tools for internationalizing Python applications
py39-bottleneck	1.3.8	BSD2CLAUSE	Collection of fast NumPy array functions written in Cython
py39-certifi	2024.2.2	MPL20	Mozilla SSL certificates
py39-cffi	1.16.1	MIT	Foreign Function Interface for Python calling C code
py39-charset-normalizer	3.3.2	MIT	Real First Universal Charset Detector
py39-cryptography	42.0.5_1,1	APACHE20	Cryptographic recipes and primitives for Python developers
py39-dateutil	2.9.0	BSD3CLAUSE	Extensions to the standard Python datetime module
py39-dnspython	2.6.1,1	ISCL	DNS toolkit for Python
py39-duckdb	0.10.1	MIT	In-process SQL OLAP database management system
py39-exceptiongroup	1.2.0	MIT	Backport of PEP 654 (exception groups)
py39-fail2ban	1.0.2_1	GPLv2	Scans log files and bans IP that makes too many password failures
py39-h2	4.1.0	MIT	HTTP/2 State-Machine based protocol implementation
py39-h11	0.14.0	MIT	Pure-Python, bring-your-own-I/O implementation of HTTP/1.1
py39-hpack	4.0.0	MIT	HTTP/2 header encoding (HPACK) logic implementation
py39-httpcore	1.0.4_1	BSD3CLAUSE	Minimal low-level HTTP client
py39-httpx	0.27.0	BSD3CLAUSE	Next generation HTTP client
py39-hyperframe	6.0.0	MIT	Python module that decodes binary streams into HTTP/2 frames
py39-idna	3.6	BSD3CLAUSE	Internationalized Domain Names in Applications (IDNA)
py39-Jinja2	3.1.3	BSD3CLAUSE	Fast and easy to use stand-alone template engine
py39-markupsafe	2.1.5	BSD3CLAUSE	Implements XML/HTML/XHTML Markup safe string for Python
py39-netaddr	0.10.1	BSD3CLAUSE	Manipulation of IPv4, IPv6, CIDR, EUI and MAC network addresses
py39-numexpr	2.9.0	MIT	Fast numerical array expression evaluator for Python and NumPy
py39-numpy	1.25._6,1	BSD3CLAUSE	The New Numeric Extension to Python
py39-openssl	23.2.0,1	APACHE20	Python interface to the OpenSSL library
py39-outcome	1.3.0	APACHE20	Capture the outcome of Python function calls
Py3-packaging	23.2	APACHE20	Core utilities for Python packages
py39-pandas	2.0.3_1,1	BSD3CLAUSE	Flexible, high-performance data analysis in Python
Py39-pyasn1	0.5.0	BSD3CLAUSE	ASN.1 toolkit for Python
Py39-pyasn1-modules	0.3.0	BSD3CLAUSE	Collection of ASN.1 data structures for py-pyasn1
py39-pycparser	2.21	BSD3CLAUSE	C parser in Python
py39-pyinotify	0.9.6	MIT	Python interface to (lib)inotify
py39-pysocks	1.7.1	BSD3CLAUSE	Python SOCKS module
py39-pytz	2024.1,1	MIT	World Timezone Definitions for Python
py39-requests	2.31.0	APACHE20	Python HTTP for Humans
py39-service-identity	2.31.0	MIT	Service identity verification for pyOpenSSL & cryptography
py39-setuptools	63.1.0_1	MIT	Python packages installer
py39-six	1.16.0	MIT	Python 2 and 3 compatibility utilities
py39-sniffio	1.3.1	APACHE20	Sniff out which async library your code is running under
py39-sortedcontainers	2.4.0	APACHE20	Python Sorted Container Types: SortedList, SortedDict, and SortedSet
py39-sqlite3	3.9.18_7	PSFL	Standard Python binding to the SQLite3 library (Python 3.9)
py39-trio	0.25.0	APACHE20	Library for async concurrency and I/O
Py29-typing-extensions	4.10.0	PSFL	Backported and Experimental Type Hints for Python 3.5+

py39-tzdata	2024.1	APACHE20	Provider of IANA time zone data
py39-ujson	5.9.0	BSD3CLAUSE	Ultra-fast JSON encoder and decoder for Python
py39-urllib3	1.26.18,1	MIT	HTTP library with thread-safe connection pooling, file post, and more
py39-vici	5.9.11	MIT	Native Python interface for strongSwan's VICI protocol
py39-yaml	6.0.1	MIT	Python YAML parser
python39	3.9.18_2	PSFL	Interpreted object-oriented programming language
radvd	2.19_3	RADVD	Linux/BSD IPv6 router advertisement daemon
readline	8.2.10	GPLv3	Library for editing command lines as they are typed
rrdtool	1.8.0_4	GPLv2	Round Robin Database Tools
samplicator	1.3.8.r1_1	GPLv2	Receives UDP datagrams and redistributes them to a set of receivers
sqlite3	3.45.0,1	PD	SQL database engine in a C library
squid	6.8	GPLv2	HTTP Caching Proxy
strongswan	5.9.13_2	GPLv2	Open Source IKEv2 IPsec-based VPN solution
sudo	1.9.15p5_4	sudo	Allow others to run commands as root
suricata	7.0.4	GPLv2	High Performance Network IDS, IPS and Security Monitoring engine
syslog-ng	4.6.0_2	GPLv2+	Powerful syslogd replacement
telegraf	1.30.0	MIT	Time-series data collection
unbound	1.19.3	BSD3CLAUSE	Validating, recursive, and caching DNS resolver
wireguard-kmod	0.0.20220615_1	MIT	WireGuard implementation for the FreeBSD kernel
wpa_supplicant	2.10_10	BSD3CLAUSE	Supplicant (client) for WPA/802.1x protocols
zip	3.0_2	BSD3CLAUSE	Create/update ZIP files compatible with PKZIP