



mistborn 

   + 13 more











Mistborn is your own virtual private cloud platform and WebUI that manages self hosted services, and secures them with firewall, Wireguard VPN w/ PiHole-DNSCrypt, and IP filtering. Optional SIEM+IDS. Supports 2FA, Nextcloud, Jitsi, Home Assistant, +


[Project badge](#)



**Merge branch '188-elasticsearch' into 'master'**

[Steven Foerster](#) authored 1 week ago

Name	Last commit	Last update
 <a href="#">compose/production</a>	<a href="#">Resolve "Bug: Tor unable to start after Jitsi starts"</a>	6 months ago
 <a href="#">dev</a>	<a href="#">Resolve "Raspbian"</a>	1 year ago
 <a href="#">extra</a>	<a href="#">Resolve "Wazuh is not Starting"</a>	1 month ago
 <a href="#">modules</a>	<a href="#">Resolve "DNS issue on Ubuntu 20.04"</a>	1 year ago
 <a href="#">scripts</a>	<a href="#">elasticsearch credentials</a>	1 week ago
 <a href="#">.gitignore</a>	<a href="#">Resolve "README: troubleshooting extra services"</a>	1 year ago
 <a href="#">.gitlab-ci.yml</a>	<a href="#">Resolve "Jitsi - "You have beend disconnected" - Only..."</a>	5 months ago
 <a href="#">.gitmodules</a>	<a href="#">Resolve "DNS issue on Ubuntu 20.04"</a>	1 year ago
 <a href="#">LICENSE</a>	<a href="#">Docker</a>	1 year ago
 <a href="#">README.md</a>	<a href="#">Resolve "Update README"</a>	3 weeks ago

Name	Last commit	Last update
 <a href="#">base.yml</a>	<a href="#">pihole v5.7</a>	2 months ago

 [README.md](#)

# Mistborn

---

A secure platform for easily standing up and managing your own cloud services: including firewall, ad-blocking, and multi-factor Wireguard VPN access

# Wireguard Profiles

Mistborn Users

## Manage Users & Wireguard Profiles

Create User

Gateways

admin (S)

Natalia (S)

Olivia

Steven (S)

### New Wireguard Client

Name\*

Profile type\*

Wireguard Only

Select Gateway

DEFAULT

Select Endpoint IP Address

204.48.18.234 (public)

Create

### System76



10.21.176.34  
DEFAULT

Server: 204.48.18.234:56059

Profile Type: Multi Factor  
Authentication

View Config

### HP Envy



10.21.176.26  
DEFAULT

Server: 204.48.18.234:48881

Profile Type: Multi Factor  
Authentication

View Config

Remove

### Samsung Galaxy S



10.21.176.22

### Dell



10.21.176.18  
DEFAULT

Server: 204.48.18.234:33491

Profile Type: Wireguard Only

View Config

### default



10.21.176.6  
DEFAULT

Server: 204.48.18.234:36325

Remove

Server: 204.48.18.234:36407

View Config

Profile Type: Wireguard Only

View Config

Remove

Remove

Copyright © 2019-2020 Cyber5K. All rights reserved.

Mistborn by Steven Foerster

Wireguard Management in Mistborn

As featured in [Linux Magazine](#) (Linux Pro Magazine in North America) in November 2020



# Table of Contents

---

- [Mistborn](#)
- [Table of Contents](#)
- [What is Mistborn](#)
- [Quickstart](#)
- [Network Diagram](#)
- [Security Information & Event Management \(SIEM\)](#)
- [Coppercloud](#)
- [Gateways](#)
- [Remote Desktop](#)
- [Client to client communication](#)
- [Installation](#)
- [Non-Interactive Installation](#)
  - [Environment Variables](#)
  - [Example Noninteractive Install](#)
- [Post-Installation](#)
  - [Login via Wireguard](#)
  - [Wireguard Management](#)
  - [Extra Services](#)
  - [Mistborn Firewall Metrics](#)
- [Authentication](#)
  - [Profile: Wireguard Authentication](#)
  - [Profile: Multi Factor Authentication \(MFA\)](#)
    - [MFA Internet Access](#)
    - [MFA Mistborn Service Access - Fixed on 4 December 2020](#)
    - [Notes](#)
- [Mistborn Subdomains](#)
- [Default Credentials](#)
- [Gateway Setup](#)
  - [Gateway Requirements](#)
  - [Install Gateway Wireguard config file](#)
- [Phones and Mobile Devices](#)
  - [App Links](#)
  - [TLS Certificate](#)
- [FAQ](#)
  - [Where is My Data?](#)
  - [How do I SSH into Mistborn?](#)
  - [How do I change the upstream DNSCrypt servers?](#)
- [Troubleshooting](#)
  - [Troubleshooting Wireguard](#)
  - [Troubleshooting Extra Services](#)
  - [Troubleshooting Docker](#)
  - [Troubleshooting Upgrade from Ubuntu 18.04 to 20.04](#)
  - [Troubleshooting Raspberry Pi OS \(Raspbian\)](#)

- [Troubleshooting Debian 10](#)
- [Technical and Security Insights](#)
  - [Attack Surface](#)
  - [Firewall](#)
  - [Additional Notes](#)
- [Roadmap \(not necessarily in order\)](#)
- [Featured In](#)
- [Follow](#)
- [Contact](#)
- [Support Mistborn](#)

# What is Mistborn

---

The term [Mistborn](#) is inspired by a type of powerful Allomancer in Brandon Sanderson's Cosmere.

Mistborn started as a passion project for a husband and father protecting his family. Certain family members insisted on connecting their devices to free public WiFi networks. We needed a way to secure all family devices with a solid VPN (Wireguard). Once we had that we wanted to control DNS to block ads to all devices and block malicious websites across all family devices. Then we wanted chat, file-sharing, and webchat services that we could use for ourselves without entrusting our data to some big tech company. And then... home automation. I know I'll be adding more services so I made that easy to do.

As an [Offensive Security Certified Professional \(OSCP\)](#), I designed Mistborn thinking about how it would be attacked by both external and internal threats. In making design trade-off decisions I tend to the paranoid. See [Technical and Security Insights](#).

Ideal for teams who:

- hate internet ads
- need to be protected from malicious internet domains
- need to collaborate securely
- need multi-factor authentication for Wireguard
- want to retain sole ownership of their data
- want to easily grant and revoke access to people and devices via a simple web interface
- want secure internet access wherever they are
- want to limit or stop data collecting services
- want to prevent being detected/blocked for using a proxy or VPN service

See the [Mistborn Network Security](#) wiki page to see the network scan results for Mistborn.

Mistborn depends on these core open source technologies:

- [Docker](#): containerization
- [Wireguard](#): secure VPN access
- [SSH](#): secure remote management

These tools are not vital to Mistborn itself but are integrated to enhance security, ease, and features:

- [iptables](#): The powerful Linux netfilter firewall tool
- [cockpit](#): A Graphical User Interface for system management, including container management
- [Pi-hole](#): A DNS server for network-wide ad blocking, etc
- [DNSCrypt](#): prevents DNS spoofing via cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered
- [Traefik](#): A modern, efficient reverse-proxy

These tools can be turned on from the Mistborn Security Operations Center:

- [Wazuh](#): Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.
- [Suricata](#): Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.

Within Mistborn is a panel to enable and manage these free extra services (off by default), locally hosted in Docker containers:

- [Home Assistant](#): Open source home automation that puts local control and privacy first
- [Nextcloud](#): Nextcloud offers the industry-leading, on-premises content collaboration platform. It combines the convenience and ease of use of consumer-grade solutions like Dropbox and Google Drive with the security, privacy and control business needs.
- [BitWarden](#): Password manager. The easiest and safest way for individuals, teams, and business organizations to store, share, and sync sensitive data.
- [Syncthing](#): Syncthing is a continuous file synchronization program. It synchronizes files between two or more computers in real time, safely protected from prying eyes.
- [OnlyOffice](#): Cloud office suite. ONLYOFFICE provides you with the most secure way to create, edit and collaborate on business documents online.
- [Rocket.Chat](#): Free, Open Source, Enterprise Team Chat.
- [Jellyfin](#): The Free Media Software System.
- [Tor](#): The Onion Router. One tool in the arsenal of online security and privacy.
- [Jitsi](#): Multi-platform open-source video conferencing
- [Guacamole](#): A clientless remote desktop gateway that supports standard protocols like VNC, RDP, and SSH.
- [RaspAP](#): The easiest, full-featured wireless router setup for Debian-based devices. Period. (Mistborn integration in alpha testing).

## Quickstart

---

Tested Operating Systems (in order of thoroughness):

- Ubuntu 20.04 LTS
- Ubuntu 18.04 LTS
- Debian 10 (Buster)
- Raspberry Pi OS (formerly Raspbian) Buster

**Note:** Install operating system updates and restart. Raspberry Pi OS particularly needs to be restarted after kernel updates (kernel modules for the currently running kernel may be missing).

Tested Browsers:

- Firefox

The default tests are run on DigitalOcean Droplets: 2GB RAM, 1 CPU, 50GB hard disk.

The Mistborn docker images exist for these architectures:

Mistborn Docker Images (hub.docker.com)	Architectures
mistborn (django, celery{worker,beat})	amd64, arm64, arm/v7
dnscrypt-proxy	amd64, arm64, arm/v7

Recommended System Specifications:

Use Case	Description	RAM	Hard Disk
Bare bones	Wireguard, Pihole (no Cockpit, no extra services)	2 GB	15 GB
Default	Bare bones + Cockpit	2 GB+	15 GB
Low-resource services	Default + Bitwarden, Tor, Syncthing	4 GB	20 GB
High-resource services	Default + Jitsi, Nextcloud, Jellyfin, Rocket.Chat, Home Assistant, OnlyOffice	6 GB+	25 GB+
SIEM	Default + Wazuh + Extras	16 GB+	100 GB+

Starting from base installation

```
git clone https://gitlab.com/cyber5k/mistborn.git
sudo -E bash ./mistborn/scripts/install.sh
```

Get default admin Wireguard profile *wait 1 minute after "Mistborn Installed" message*

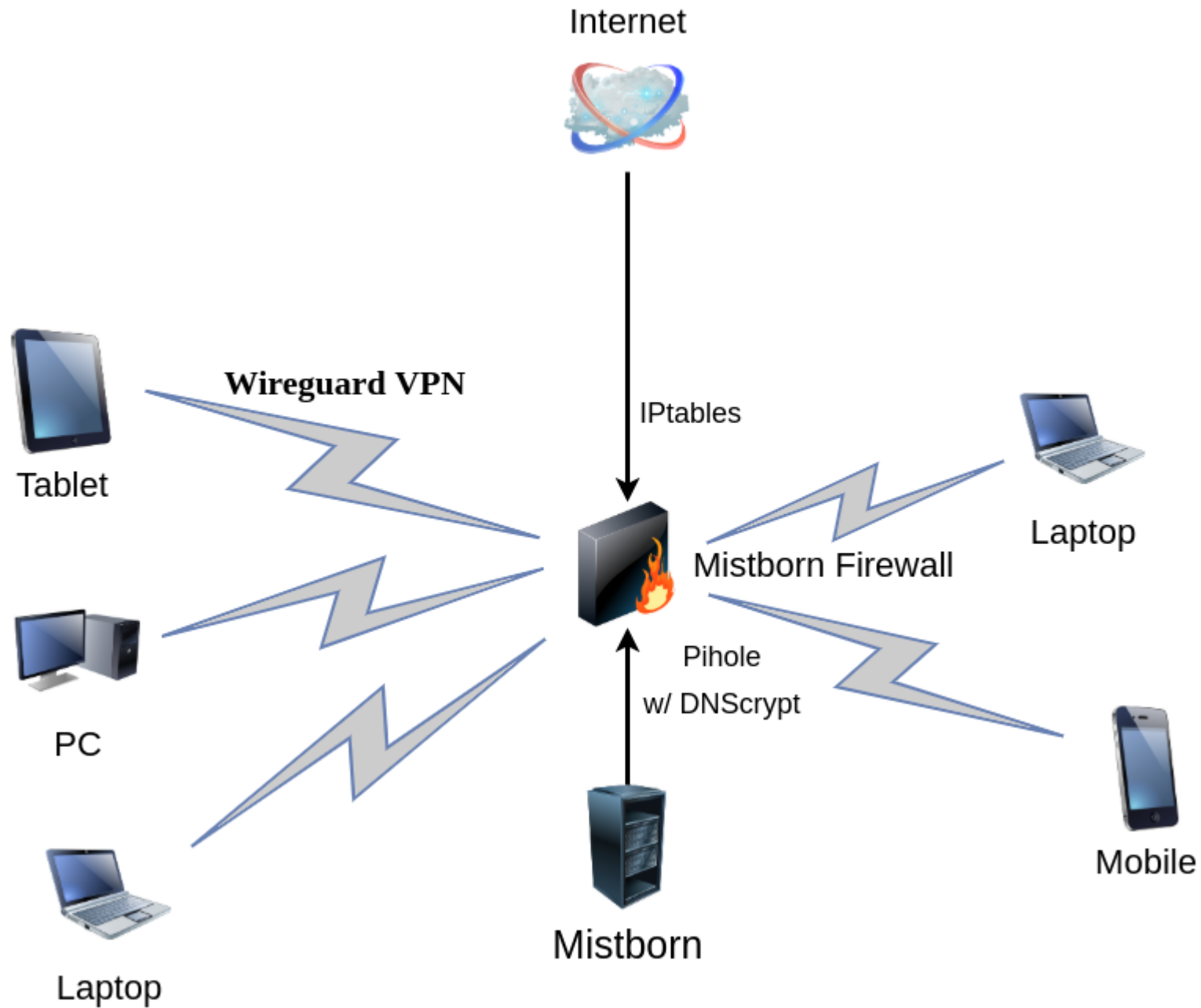
```
sudo mistborn-cli getconf
```

Connect via Wireguard then visit `http://home.mistborn`

For more information, see the [Installation](#) section below.



# Network Diagram



Mistborn protects your data in a variety of ways:

- All of your devices are protected wherever they go with the Wireguard VPN protocol

- The Mistborn firewall blocks unsolicited incoming internet packets
- Pi-hole running on Mistborn blocks outgoing internet requests to configurable blocked domains (ads, malicious/phishing domains, etc.)

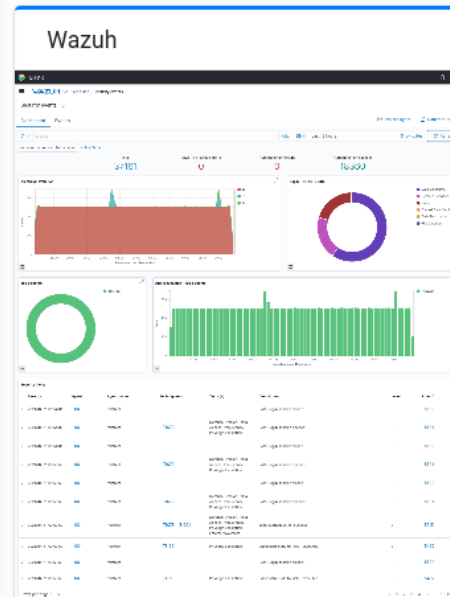
See the [Mistborn Network Security](#) wiki page to see more network diagrams and the network scan results for Mistborn.

## Security Information & Event Management (SIEM)

---

## SIEM: Security Information & Event Management

The Security Information & Events Manager (SIEM) requires an Elasticsearch (or Open Distro for Elasticsearch) backend to store, process, and audit security logs from your devices connected to Mistborn.



### Wazuh

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.

Status: running

Stop

Open Wazuh

### Local Elasticsearch



### Local Elasticsearch

Elasticsearch is a distributed, RESTful search and analytics engine capable of addressing a growing number of use cases. As the heart of the Elastic Stack, it centrally stores your data for lightning fast search, fine-tuned relevancy, and powerful analytics that scale with ease.

This local Elasticsearch feature is provided so that Mistborn can remain entirely standalone. But it should be treated as a non-production environment (no backups, no redundancy, etc) and the Mistborn host should have **at least 8 GB RAM**. Do not try to run this on a Raspberry Pi (though it will not stop you).

Status: running

Stop

### Wazuh Endpoint Agents



### Wazuh Endpoint Agents

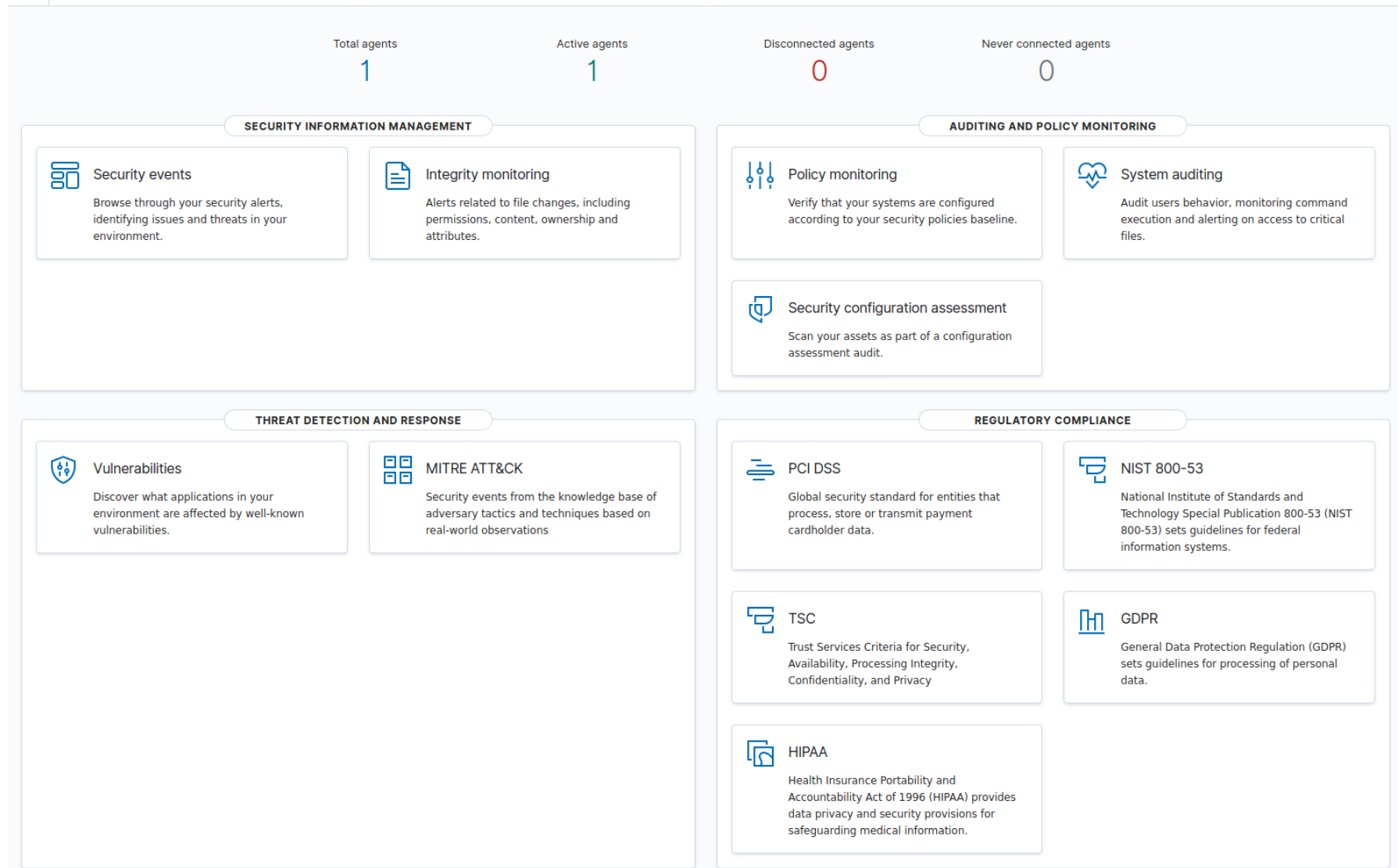
The Wazuh agent is multi-platform and runs on the hosts that the user wants to monitor. It provides the following capabilities:

- Log and data collection
- File integrity monitoring
- Rootkit and malware detection
- Security policy monitoring
- Configuration assessments
- Software inventory

Wazuh Agent Downloads

The Mistborn Security Operations Center provides SIEM services with Wazuh. The Wazuh Manager requires an Open Distro for Elasticsearch backend. When the Mistborn host has >8 GB RAM the provided Elasticsearch backend can be used. Just click "Start Wazuh" on the [Security Center](#) page and enjoy your Enterprise-grade SIEM. Wazuh agents can be installed on just about any OS and all Wazuh agent traffic is communicated over the Wireguard connections. Instructions for adding endpoint agents can be found within Wazuh itself.

Mistborn's Wazuh installs and integrates with Suricata running on Mistborn with logs ingested into Wazuh.



The Wazuh Kibana plugin leverages the power of Elasticsearch:

Security events

Dashboard Events

Explore agent Generate report

Search KQL Last 12 hours Show dates Refresh

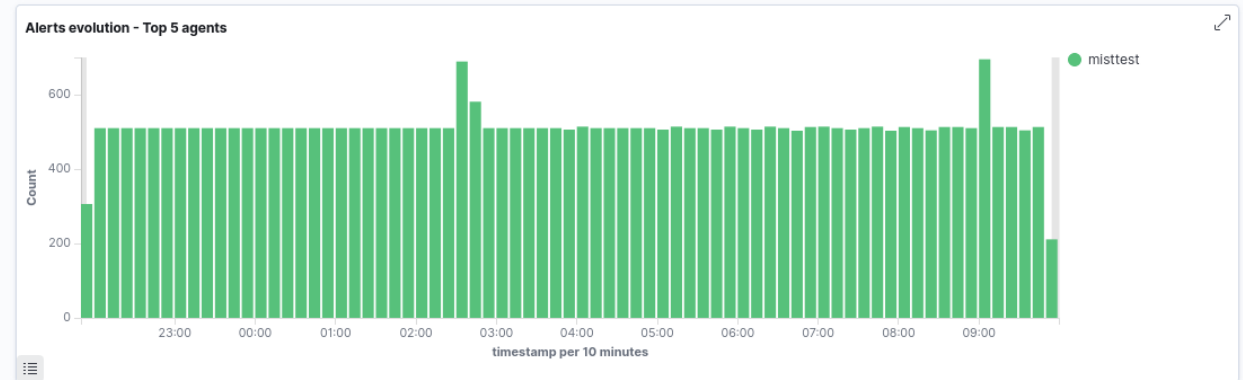
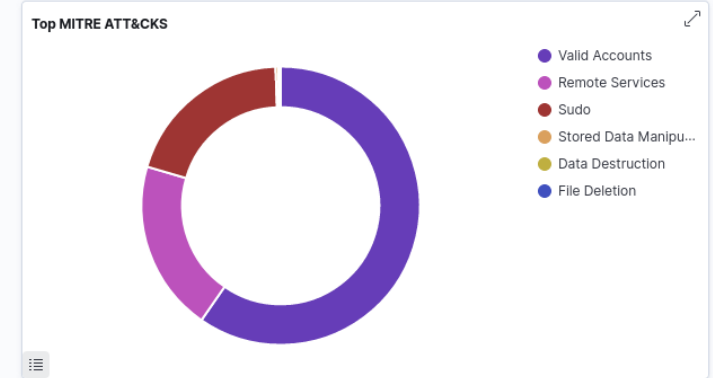
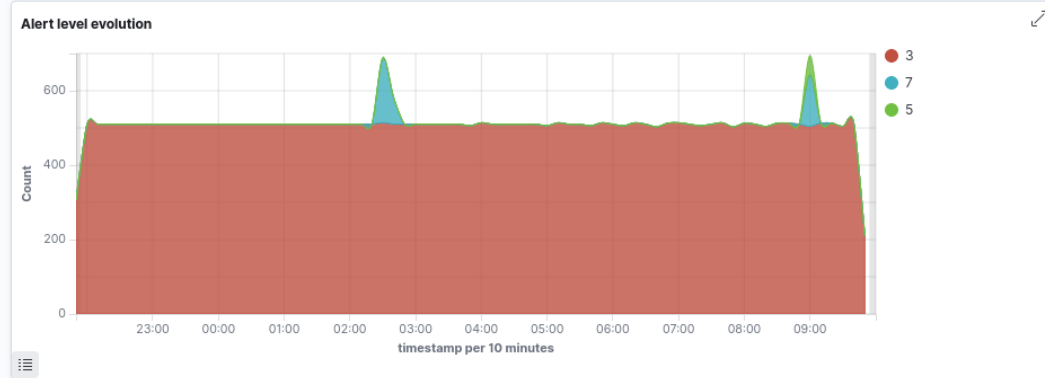
manager.name: wazuh-manager + Add filter

Total  
37161

Level 12 or above alerts  
0

Authentication failure  
0

Authentication success  
18360



**Security Alerts**

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> 2021/04/21 09:54:01	001	misttest			PAM: Login session closed.	3	5502
> 2021/04/21 09:54:01	001	misttest	T1078	Defense Evasion, Initial Access, Persistence, Privilege Escalation	PAM: Login session opened.	3	5501
> 2021/04/21 09:54:01	001	misttest			PAM: Login session closed.	3	5502
> 2021/04/21 09:53:59	001	misttest	T1078	Defense Evasion, Initial Access, Persistence,	PAM: Login session opened.	3	5501

>	2021/04/21 09:53:59	001	misttest			PAM: Login session closed.	3	5502	
>	2021/04/21 09:53:59	001	misttest	T1078		Defense Evasion, Initial Access, Persistence, Privilege Escalation	PAM: Login session opened.	3	5501
>	2021/04/21 09:53:59	001	misttest	T1078	T1021	Defense Evasion, Initial Access, Persistence, Privilege Escalation, Lateral Movement	sshd: authentication success.	3	5715
>	2021/04/21 09:53:59	001	misttest	T1169		Privilege Escalation	Successful sudo to ROOT executed.	3	5402
>	2021/04/21 09:53:59	001	misttest				PAM: Login session closed.	3	5502
>	2021/04/21 09:53:59	001	misttest	T1169		Privilege Escalation	Successful sudo to ROOT executed.	3	5402

Rows per page: 10 < 1 2 3 4 5 ... 1000 >

## Coppercloud

Pihole provides a way to block outgoing DNS requests for given lists of blocked domains. Coppercloud provides a way to block outgoing network calls of all types to given lists of IP addresses (IPv4 only for now). This is especially useful for blocking outgoing telemetry (data and state sharing) to owners of software running on all of your devices.

- System
- Firewall
- PiHole
- Coppercloud
- Metrics
- Wireguard Logged In
- Manage Extra Services
- Tests

## Mistborn IP Filtering

### Manage IP Lists: Blacklists & Whitelists

Create IP List

Windows Telemetry (BLACKLIST)

Add IP Address to Windows Telemetry

Ip\*

Add

Delete IP List: Windows Telemetry

Delete IP List

#### IP List: Windows Telemetry

IP Address	Action
134.170.30.202	Remove
137.116.81.24	Remove
157.56.106.189	Remove
184.86.53.99	Remove
2.22.61.43	Remove
2.22.61.66	Remove
204.79.197.200	Remove
23.218.212.69	Remove
65.39.117.230	Remove
65.55.108.23	Remove
64.4.54.254	Remove
IP Address	Action



This example shows Coppercloud blocking a list of Microsoft IP addresses on a network with Windows 10 clients.

## Gateways

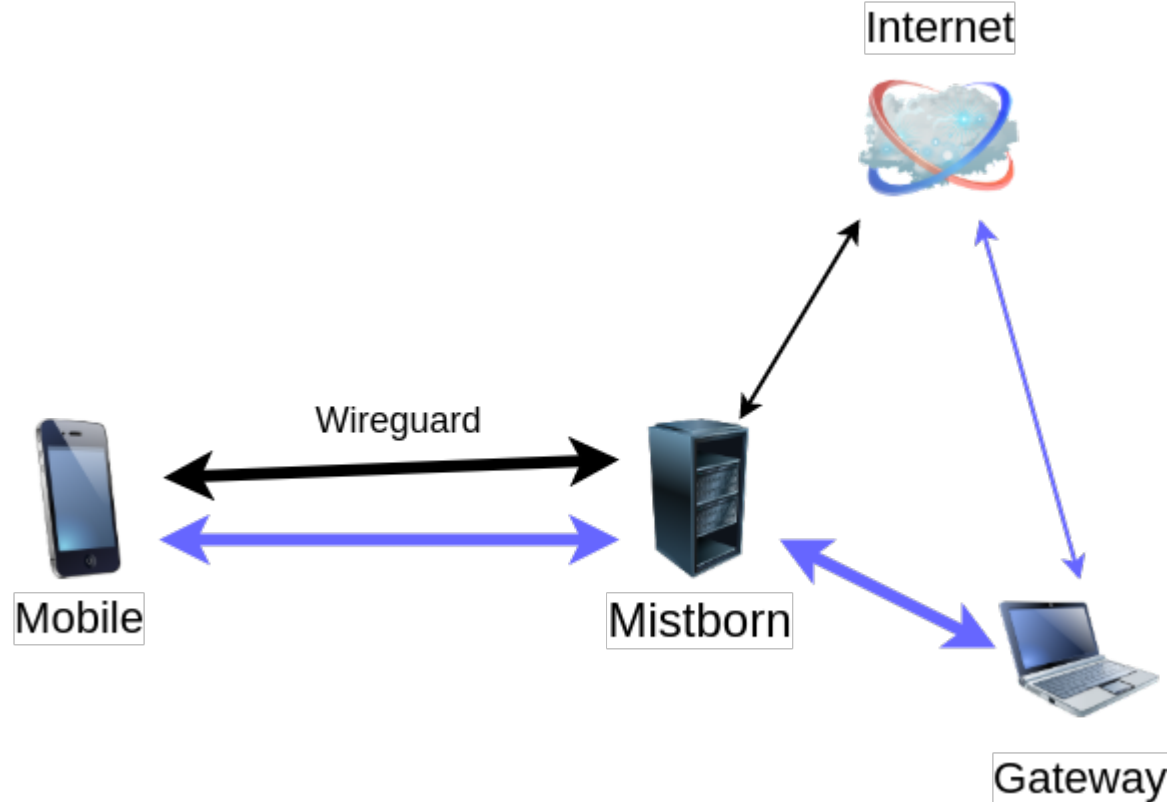
---

We were getting frustrated at being forced to choose between being connected to our VPN and using streaming services that we have paid for.



*Netflix blocking my connections that it sees coming from a DigitalOcean droplet*

In Mistborn, Gateways are upstream from the VPN server so connections to third-party services (e.g. Netflix, Hulu, etc.) will appear to be coming from the public IP address of the Gateway. I setup a Gateway at home (Raspberry Pi with `wireguard` and `openresolv` installed) and with our Mistborn on DigitalOcean, all Wireguard profiles created with this Gateway will appear to be coming from my house and are not blocked. No port-forwarding required (assuming Mistborn is publicly accessible).



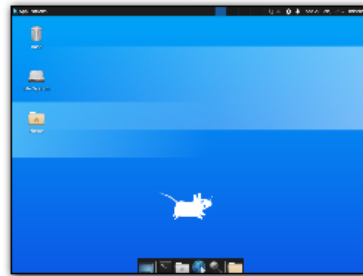
The Gateway adds an extra network hop. DNS is still resolved in Mistborn so pihole is still blocking ads.

## Remote Desktop

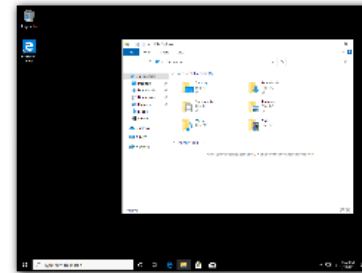
Remote desktops enable multiple users to share desktop resources and data. Remote desktops also enable groups to prevent sensitive data from ever entering an endpoint devices such as a smartphone. For reference, some United States Government regulations require controls to protect Controlled Unclassified Information (CUI) that are not feasible to implement on all endpoint devices and remote desktops prevent the data from entering the device (see NIST SP 800-171 3.1.19, CMMC AC.3.022).

Mistborn enables remote desktop access via the Apache Guacamole extra service, which supports VNC, RDP, SSH, and other protocols.

Mistborn Apache Guacamole  
guac.mistborn/#/ RECENT CONNECTIONS mistborn



XFCE4



Win10

ALL CONNECTIONS

Filter

- Win10
- XFCE4

Currently in use by 1 user.

Currently in use by 1 user.

Guacamole implements its own users and groups access controls to manage access to individual desktops. All Mistborn users must be authenticated with Mistborn (via Wireguard only or MFA) to access the Guacamole interface.

## Client to client communication

By default direct communication between network clients is blocked. Mistborn clients can all talk to Mistborn and communicate via shared services (Jitsi, Nextcloud, etc). Direct client to client communication can be enabled via the "client-to-client" toggle.

Server Settings

off Client-to-client

Update Restart

# Installation

---

Mistborn is regularly tested on Ubuntu 20.04 LTS (DigitalOcean droplet with 2 GB RAM). It has also been successfully used on Debian Buster and Raspbian Buster systems (though not regularly tested). Make sure to install OS updates and restart before installing Mistborn (Wireguard installs differently on recent kernels).

Clone the git repository and run the install script:

```
git clone https://gitlab.com/cyber5k/mistborn.git
sudo -E bash ./mistborn/scripts/install.sh
```

Running `install.sh` will do the following:

- create a `mistborn` system user
- clone the mistborn repo to `/opt/mistborn`
- setup iptables and ip6tables rules and chains
- install iptables-persistent
- install Docker
- install OpenSSH
- install Wireguard
- install Cockpit (optional)
- create a `cockpit` system user (if Cockpit is installed)
- configure unattended-upgrades
- generate a self-signed TLS certificate/key (WebRTC functionality requires TLS)
- create and populate `traefik.toml`
- create `/opt/mistborn_volumes` and setup folders for services that will be mounted within
- backup original contents of `/opt/mistborn_volumes` in `/opt/mistborn_backup`
- Pull docker images for `base.yml`
- Build docker images for `base.yml`
- Disable competing DNS services (`systemd-resolved` and `dnsmasq`)
- copy Mistborn `systemd` service files to `/etc/systemd/system`
- start and enable `Mistborn-base`

## Non-Interactive Installation

---

In order to install without interaction some environment variables need to be pre-set.

### Environment Variables

---

See the environment variables needed in `./scripts/noninteractive/.install_barebones`

# Example Noninteractive Install

---

This will perform a noninteractive install with the default environment variables set in `.install_barebones`.

```
git clone https://gitlab.com/cyber5k/mistborn.git
sudo -E bash -c "source ./mistborn/scripts/noninteractive/.install_barebones && ./mistborn/scripts/install.sh"
```

## Post-Installation

---

When Mistborn-base starts up it will create volumes, initialize the PostgreSQL database, start pihole, run Django migrations and then check to see if a Mistborn superuser named `admin` exists yet. If not, it will create the superuser `admin` along with an accompanying default Wireguard configuration file and start the Wireguard service.

You can watch all of this happen with:

```
sudo journalctl -xfu Mistborn-base
```

The default Wireguard configuration file for `admin` may be obtained via:

```
sudo mistborn-cli getconf
```

Please notice that the following lines are **NOT** part of the Wireguard config:

```
Starting mistborn_production_postgres ... done
Starting mistborn_production_redis    ... done
PostgreSQL is available
```

The Wireguard config will look like this:

```
# "10.15.91.2" - WireGuard Client Profile
[Interface]
Address = 10.15.91.2/32
# The use of DNS below effectively expands to:
#   PostUp = echo nameserver 10.15.91.1 | resolvconf -a tun.%i -m 0 -x
#   PostDown = resolvconf -d tun.%i
# If the use of resolvconf is not desirable, simply remove the DNS line
# and use a variant of the PostUp/PostDown lines above.
```

```
# The IP address of the DNS server that is available via the encrypted
# WireGuard interface is 10.15.91.1.
DNS = 10.15.91.1
PrivateKey = cPPflVGsxVFW2/lMmhiFTXMmH345bGqoqArD/NgjiXU=

[Peer]
PublicKey = DfIV1urYZXqXKiU4r0Sf00Iu589pE0+59dHV5w5N0mU=
PresharedKey = Z1S05NuAnZ7JhzVCuUnYOQLW0QYmMoqG0pG1SNXUlh0=
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = <Mistborn public IP address>:39207
```

## Login via Wireguard

---

[Install wireguard](#) on your computer. If you get a `resolvconf: command not found` error when starting Wireguard then install openresolv: `sudo apt-get install -y openresolv`

- Copy the text of the default admin Wireguard config to `/etc/wireguard/wg_admin.conf` on your computer
- Run `sudo systemctl start wg-quick@wg_admin`
- Run `sudo systemctl enable wg-quick@wg_admin`
- Open your browser and go to "<http://home.mistborn>"
- Browse your Mistborn system! **Note:** The home.mistborn server takes a minute to come up after Mistborn is up (collectstatic on all that frontend JavaScript and CSS)

## Wireguard Management

---

Mistborn users can be added (non-privileged or superuser) and removed by superusers. Multiple Wireguard profiles can be created for each user. A non-privileged user can create profiles for themselves.

# Wireguard Profiles

Mistborn Users

## Manage Users & Wireguard Profiles

Create User

Gateways

admin (S)

Natalia (S)

Olivia

Steven (S)

### New Wireguard Client

Name\*

Profile type\*

Wireguard Only

Select Gateway

DEFAULT

Select Endpoint IP Address

204.48.18.234 (public)

Create

### System76



10.21.176.34  
DEFAULT

Server: 204.48.18.234:56059

Profile Type: Multi Factor Authentication

View Config

### HP Envy



10.21.176.26  
DEFAULT

Server: 204.48.18.234:48881

Profile Type: Multi Factor Authentication

View Config

Remove

### Samsung Galaxy S



10.21.176.22

### Dell



10.21.176.18  
DEFAULT

Server: 204.48.18.234:33491

Profile Type: Wireguard Only

View Config

### default



10.21.176.6  
DEFAULT

Server: 204.48.18.234:36325

- System
- Firewall
- Wireguard **Logged in**
- Manage Extra Services
- Tests

Remove

Server: 204.48.18.234:36407

View Config

Profile Type: Wireguard Only

View Config

Remove

Remove

Copyright © 2019-2020 [Cyber5K](#). All rights reserved.

Mistborn by Steven Foerster

*Wireguard Management in Mistborn*

## Extra Services

---

Mistborn makes extra services available.



# Manage Extra Mistborn Services

- System
- Firewall
- Wireguard **Logged In**
- Manage Extra Services
- Tests



**Mistborn-bitwarden**  
 Bitwarden is a free and open-source password management service that stores sensitive information such as website credentials in an encrypted vault. The Bitwarden platform offers a variety of client applications including a web interface, desktop applications, browser extensions, mobile apps, and a CLI.

Status: stopped

[Start](#) [Open Mistborn-bitwarden](#)



**Mistborn-jellyfin**  
 The Free Software Media System. Jellyfin is the volunteer-built media solution that puts you in control of your media. Stream to any device from your own server, with no strings attached.

Status: stopped

[Start](#) [Open Mistborn-jellyfin](#)



**Mistborn-raspap**  
 The easiest, full-featured wireless router setup for Debian-based devices. Period. (Mistborn integration in alpha testing)

Status: stopped

[Start](#) [Open Mistborn-raspap](#)



**Mistborn-guacamole**  
 Apache Guacamole is a clientless remote desktop



**Mistborn-jitsi**  
 Jitsi is a collection of free and open-source multiplatform voice, videoconferencing and instant messaging applications for the web platform, Windows, Linux, Mac OS X and Android



**Mistborn-rocketchat**  
 Rocket.Chat is the leading open source team chat software solution.

Status: stopped

[Start](#) [Open Mistborn-rocketchat](#)



RDP, and SSH.

Status: stopped

[Start](#) [Open Mistborn-guacamole](#)



#### Mistborn-homeassistant

Home Assistant is an Open source home automation software that puts local control and privacy first.

Status: stopped

[Start](#) [Open Mistborn-homeassistant](#)

Status: stopped

[Start](#) [Open Mistborn-jitsi](#)

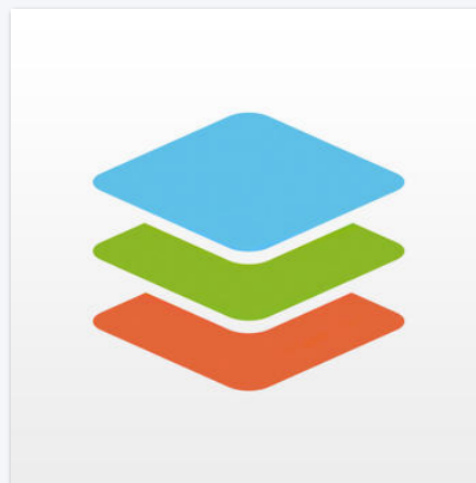


#### Mistborn-nextcloud

Nextcloud is a suite of client-server software for creating and using file hosting services. Nextcloud application functionally is similar to Dropbox.

Status: stopped

[Start](#) [Open Mistborn-nextcloud](#)



#### Mistborn-onlyoffice

An open source office suite featuring online document editors, platform for document management, corporate communication, mail and project management tools.

Status: stopped

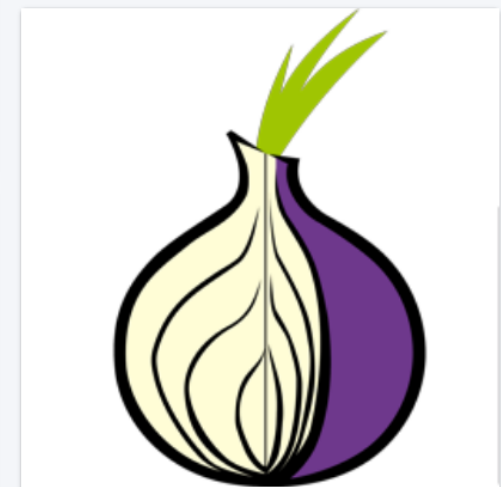


#### Mistborn-syncthing

Syncthing is a free, open-source peer-to-peer file synchronization application available for Windows, Mac, Linux, Android, Solaris, Darwin, and BSD. It can sync files between devices on a local network, or between remote devices over the Internet. Data security and data safety are built into the design of the software.

Status: stopped

[Start](#) [Open Mistborn-syncthing](#)



#### Mistborn-tor

Tor is free and open-source software for enabling anonymous communication.

Status: stopped

[Start](#) [Open Mistborn-tor](#)

*Mistborn Extra Services Available*

## Mistborn Firewall Metrics

---

Mistborn functions as a network firewall and provides metrics on blocked probes from the internet.

# Mistborn Metrics: Firewall

- System
- Firewall**
- PIHole
- Coppercloud
- Metrics
- Wireguard Logged In
- Manage Extra Services
- Tests

**6068**  
Internet Probes Blocked

[More info](#)

**3408**  
Unique IP Addresses Blocked

[More info](#)

**1921**  
Unique Ports Probed

[More info](#)

**5.6 (limit: 6)**  
Avg Probes Per Minute (last 24 hrs)

[More info](#)

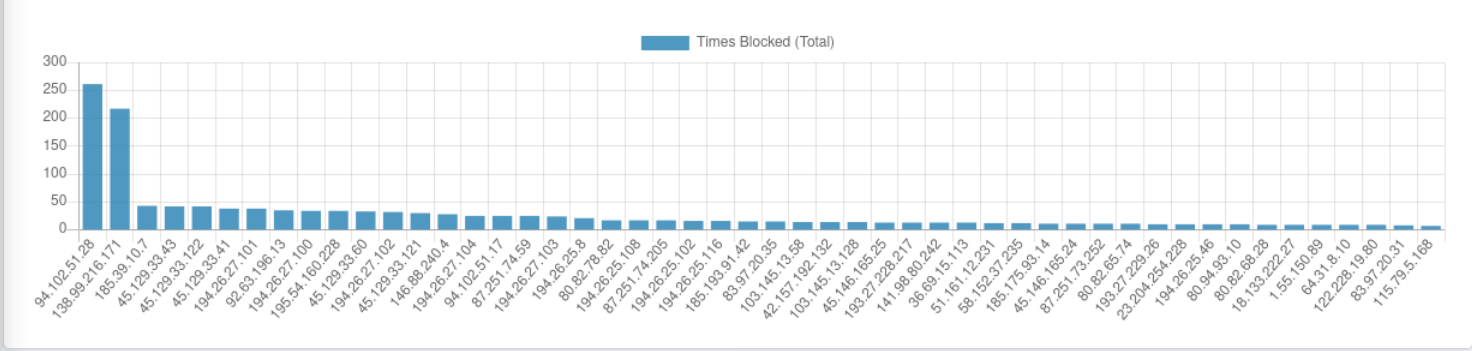
**Nov. 9, 2020, 11:23 p.m.**  
Time of First Logged Probe Attempt (UTC)

[More info](#)

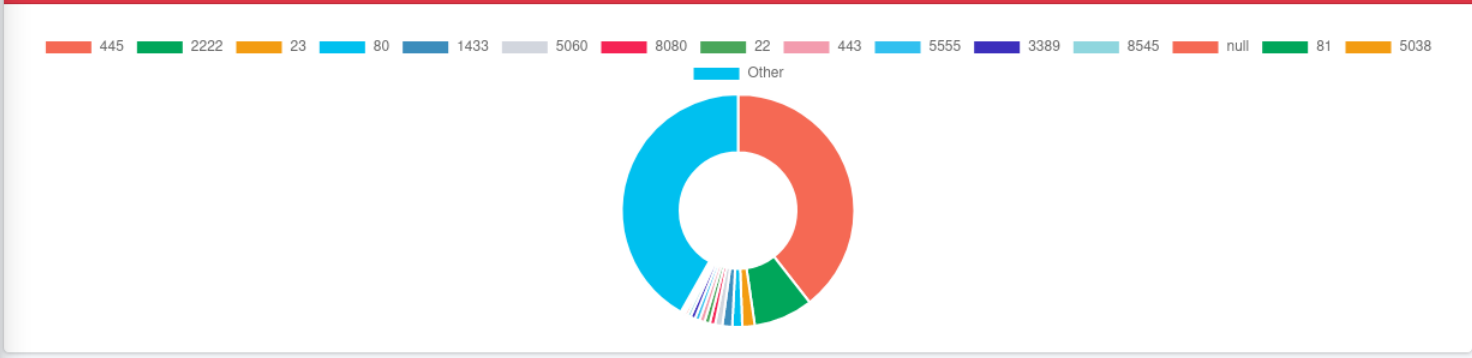
**Nov. 10, 2020, 5:33 p.m.**  
Time of Last Logged Probe Attempt (UTC)

[More info](#)

## Top Count of Blocked Probes by IP Address



## Top Count of Blocked Probes by Port



## Count of Internet Probes by Unique IP Address Blocked by Mistborn

Show:

Search:

entries

94.102.51.28	261
138.99.216.171	217
185.39.10.7	43
45.129.33.43	42
45.129.33.122	42
45.129.33.41	38
194.26.27.101	38
92.63.196.13	35
194.26.27.100	34
195.54.160.228	34
<b>Source IP Address</b>	<b>Count of times blocked</b>

Showing 1 to 10 of 3,408 entries

List of Internet Probes Blocked by Mistborn (last 24 hours) - x

Show

10

Search:

entries

Source IP Address	When Probe was Blocked (UTC)	Protocol	Destination Port
87.251.74.200	Nov. 10, 2020, 5:33 p.m.	TCP	4894
168.119.161.159	Nov. 10, 2020, 5:33 p.m.	TCP	20945
46.234.125.89	Nov. 10, 2020, 5:33 p.m.	ICMP	None
192.35.169.31	Nov. 10, 2020, 5:33 p.m.	TCP	88
125.166.187.162	Nov. 10, 2020, 5:33 p.m.	TCP	445
125.166.187.162	Nov. 10, 2020, 5:32 p.m.	TCP	445
125.166.187.162	Nov. 10, 2020, 5:32 p.m.	TCP	445
187.252.195.119	Nov. 10, 2020, 5:32 p.m.	TCP	445
194.26.27.101	Nov. 10, 2020, 5:32 p.m.	TCP	54332
139.59.215.171	Nov. 10, 2020, 5:32 p.m.	TCP	2222
Source IP Address	When Probe was Blocked (UTC)	Protocol	Destination Port

Showing 1 to 10 of 6,068 entries

# Authentication

There are multiple ways to authenticate and use the system.

The screenshot shows a web interface for 'Mistborn'. On the left is a dark sidebar with a 'Mistborn' logo at the top, a user profile for 'Steven', and a menu with items: System, Firewall, Wireguard (with a 'Logged in' badge), Manage Extra Services, and Tests. The main content area has a top navigation bar with 'Home', 'About', and 'Server Settings'. Below this is a 'Multi Factor Authentication' section with a large heading 'Enable Two-Factor Authentication'. The text below the heading explains that a smartphone should be used to scan a QR code and then enter the generated token. A QR code is displayed in the center. Below the QR code is a 'Token:' input field with a dropdown arrow. At the bottom of the form are three buttons: 'Cancel', 'Back', and 'Next'. The footer contains copyright information for Cyber5K and the text 'Mistborn by Steven Foerster'.

# Profile: Wireguard Authentication

Mistborn always authenticates with Wireguard. You must have a valid Wireguard configuration file associated with the correct internal IP address. A classic Mistborn profile (Wireguard Only) will allow you to access the internet and all services hosted by Mistborn once you have connected via Wireguard. Note: individual services may require passwords or additional authentication.

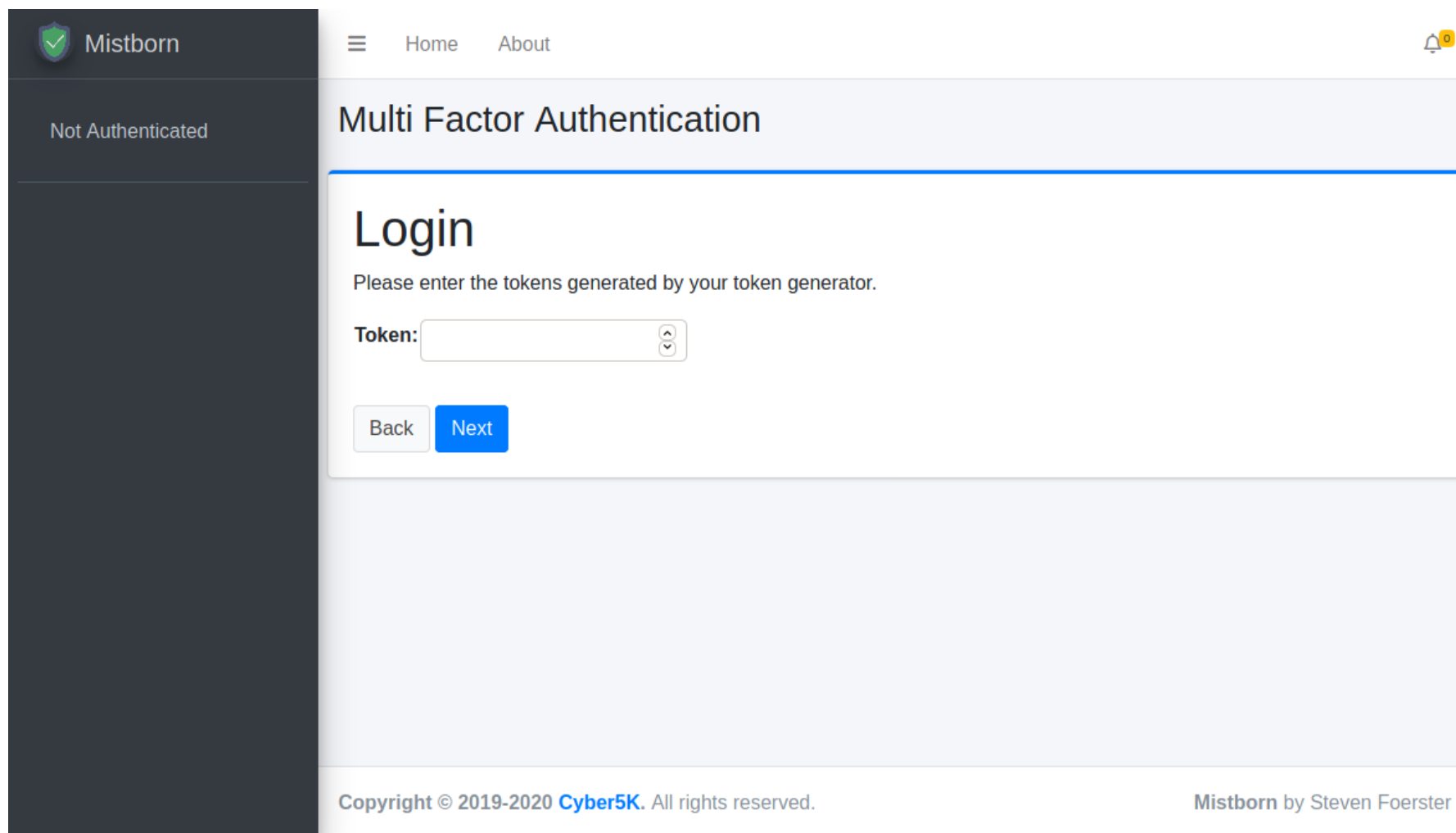
# Profile: Multi Factor Authentication (MFA)

In addition to Wireguard, you may create a Mistborn profile enabling multi-factor authentication (MFA). You must first connect to Mistborn via Wireguard. Then all internet traffic will route you to the Mistborn webserver where you must first setup and thereafter authenticate with an app (Google Authenticator, Authy, etc.). You must go to <http://home.mistborn> to complete the authentication process.

The screenshot shows the Mistborn web interface. On the left is a dark sidebar with the Mistborn logo (a shield with a checkmark) and the text "Mistborn". Below the logo, it says "Not Authenticated". The main content area has a light blue header with a hamburger menu icon, "Home", and "About" links, and a notification bell icon in the top right. The main heading is "Multi Factor Authentication". Below this is a white box with a blue border containing the "Login" section. The text "Enter your credentials." is followed by three input fields: "Username:" with the value "Steven", "IP Address:" with the value "10.21.176.34", and "Profile:" with the value "System76". At the bottom of the login box are two buttons: "Back" and "Next". The footer contains the copyright notice "Copyright © 2019-2020 Cyber5K. All rights reserved." and the text "Mistborn by Steven Foerster".

## MFA Internet Access

Internet access is blocked via iptables until authentication is completed for an MFA profile. You must go to <http://home.mistborn> to complete the authentication process. Click "Sign Out" to re-block internet access until authentication completes again.



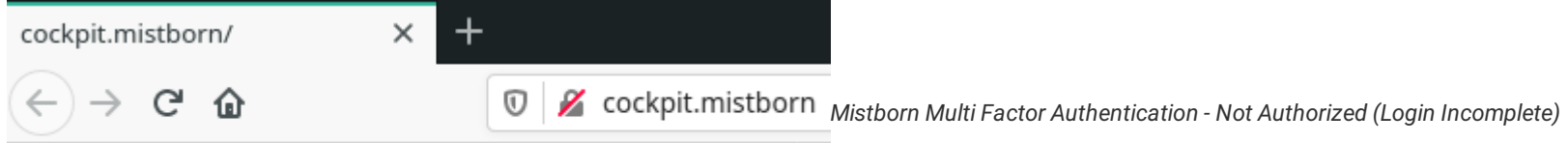
The screenshot shows a web interface for Multi Factor Authentication. On the left is a dark sidebar with the Mistborn logo (a shield with a checkmark) and the text "Mistborn". Below the logo, it says "Not Authenticated". The main content area has a navigation bar with "Home" and "About" links, and a notification bell icon. The main heading is "Multi Factor Authentication". Below this is a "Login" section with the instruction "Please enter the tokens generated by your token generator." There is a "Token:" label followed by a text input field with a dropdown arrow. At the bottom of the login section are two buttons: "Back" and "Next". The footer contains the copyright notice "Copyright © 2019-2020 Cyber5K. All rights reserved." and the text "Mistborn by Steven Foerster".

*Mistborn Multi Factor Authentication - Token Prompt*

## MFA Mistborn Service Access - Fixed on 4 December 2020

Mistborn service access is blocked via traefik until Mistborn authentication is complete. You will not be able to access the web pages for pihole, cockpit, or any extra services until authentication is complete for an MFA profile. Attempting to visit one of these pages will produce a "Mistborn: Not authorized" HTTP 403. Click "Sign Out" to re-block access until authentication completes again.





Mistborn: Not authorized

## Notes

- **Sessions:** Traefik checks the authenticated sessions on the server side to determine whether to allow access to the Mistborn service web pages. If an open session exists for your Mistborn IP address then access will be granted. You may close all sessions by clicking "Sign Out" on the Mistborn home page. Expired sessions are regularly cleaned by the Mistborn system (celery periodic task).

## Mistborn Subdomains

---

Mistborn uses the following domains (that can be reached by all Wireguard clients):

Service	Domain	Default Status
Home	home.mistborn	On
Pihole	pihole.mistborn	On
Cockpit	cockpit.mistborn	On
Nextcloud	nextcloud.mistborn	Off
Rocket.Chat	chat.mistborn	Off
Home Assistant	homeassistant.mistborn	Off
Bitwarden	bitwarden.mistborn	Off
Jellyfin	jellyfin.mistborn	Off
Syncthing	syncthing.mistborn	Off
OnlyOffice	onlyoffice.mistborn	Off

Service	Domain	Default Status
Jitsi	jitsi.mistborn	Off
Guacamole	guac.mistborn	Off
RaspAP	raspap.mistborn	Off
Wazuh	wazuh.mistborn	Off

## Default Credentials

---

These are the default credentials to use in the services you choose to use:

Service	Username	Password
Pihole		{{default mistborn password}}
Cockpit	cockpit	{{default mistborn password}}
Wazuh	mistborn	{{default mistborn password}}
Nextcloud	mistborn	{{default mistborn password}}
Guacamole	mistborn	{{default mistborn password}}
RaspAP	mistborn	{{default mistborn password}}

You can find the credentials sent to the Docker containers in: `/opt/mistborn/.envs/.production/`

## Gateway Setup

---

Mistborn will generate the Wireguard configuration script for the Gateway. From a base Ubuntu/Debian/Raspbian operating system the following packages are recommended to be installed beforehand:

# Gateway Requirements

---

- Wireguard (you can consult the Mistborn Wireguard installer: `mistborn/scripts/subinstallers/wireguard.sh`)
- Openresolv (a Wireguard dependency that is also installed via the Mistborn Wireguard installer)
- Fail2ban

## Install Gateway Wireguard config file

---

On Mistborn:

- Click `View Config` on the Gateways tab in Mistborn
- Highlight the config
- Copy (Ctrl-C)

On Gateway:

- Paste the config to `/etc/wireguard/gateway.conf`
- Run `sudo systemctl start wg-quick@gateway`
- Run `sudo systemctl enable wg-quick@gateway`

## Phones and Mobile Devices

---

All your devices can be connected to Mistborn as Wireguard clients.

First steps:

1. Device: Download the Wireguard app on your device. Links: [Android](#) [Apple](#)
2. Mistborn: Create a Wireguard profile for the device.
3. Device: Scan Wireguard client QR code in Wireguard app.
4. Device: Enable Wireguard connection.

All of you device network traffic is now being routed through Wireguard. Ads and malicious sites are blocked by pihole. DNS queries are verified via DNSCrypt.

But wait, there's more! You can:

- visit the [Mistborn web interface](#) through your phone's browser.
- download the apps for any extra services you have running and connect them to your Mistborn using the Mistborn domains.

## App Links

---

	<b>Android</b>	<b>Apple</b>
--	----------------	--------------

	Android	Apple
Nextcloud	<a href="#">Nextcloud</a>	<a href="#">Nextcloud</a>
Syncthing	<a href="#">Syncthing</a>	
Jitsi Meet	<a href="#">Jitsi Meet</a>	<a href="#">Jitsi Meet</a>
Bitwarden	<a href="#">Bitwarden</a>	<a href="#">Bitwarden</a>
Jellyfin	<a href="#">Jellyfin</a>	<a href="#">Jellyfin</a>
Home Assistant	<a href="#">Home Assistant</a>	<a href="#">Home Assistant</a>
Rocket.Chat	<a href="#">Rocket.Chat</a>	<a href="#">Rocket.Chat</a>

## TLS Certificate

---

Some apps require TLS (HTTPS). All traffic to Mistborn domains already occurs over Wireguard but to keep apps running, a TLS certificate exists for Mistborn and can be imported into your device's trusted credentials in the security settings. This certificate is checked every day and will be re-generated when expiration is less than 30 days away.

The TLS certificate can be found here:

```
/opt/mistborn_volumes/base/tls/cert.crt
```

## FAQ

---

Frequently Asked Questions

## Where is My Data?

---

The Docker services mount volumes located in:

```
/opt/mistborn_volumes
```

The core Mistborn services have volumes mounted in `/opt/mistborn_volumes/base` . These should not be modified. The extra services' volumes are mounted in:

```
/opt/mistborn_volumes/extra
```

Your data from Nextcloud, Syncthing, Bitwarden, etc. will be located there.

## How do I SSH into Mistborn?

---

If Mistborn is installed via SSH then an iptables rule is added allowing external SSH connections from the same source IP address only. If Mistborn was installed locally then no external SSH is permitted.

SSH is permitted from any device connected to Mistborn by Wireguard.

Password authentication is enabled. Fail2ban blocks IPs with excessive failed login attempts.

You can SSH using the Mistborn domain when connected by Wireguard:

```
ssh user@home.mistborn
```

## How do I change the upstream DNSCrypt servers?

---

The upstream servers used by dnscrypt-proxy are set in:

`base.yml` :

```
services:
  ...
  dnscrypt-proxy:
    ...
    environment:
      ...
      - DNSCRYPT_SERVER_NAMES=[...]
```

The available options are here: <https://download.dnscrypt.info/dnscrypt-resolvers/v2/public-resolvers.md>

## Troubleshooting

---

Once you're connected to Wireguard you should see `.mistborn` domains and the internet should work as expected. Be sure to use http (<http://home.mistborn>). Wireguard

is the encrypted channel so there's usually no need to bother with TLS certs (WebRTC functionality and some mobile apps require TLS so it is available). Here are some things to check if you have issues:

Check if you can ping an external IP address:

```
ping 1.1.1.1
```

Check if you can resolve local DNS queries:

```
dig home.mistborn
```

Check if you can resolve external DNS queries:

```
dig cyber5k.com
```

See if any docker containers are stopped:

```
sudo docker container ls -a
```

Check the running log for Mistborn-base:

```
sudo journalctl -xfu Mistborn-base
```

Mistborn-base is a systemd process and at any time restarting it should get you to a working state:

```
sudo systemctl restart Mistborn-base
```

The Wireguard processes run independently of Mistborn and will still be up if Mistborn is down. You can check running Wireguard interfaces with:

```
sudo wg show
```

Note the Mistborn naming convention for Wireguard interfaces on the server is wg. So if the particular Wireguard process is listening on UDP port 56392 then the interface will be named wg56392 and the config will be in `/etc/wireguard/wg56392.conf`

The `dev/` folder contains a script for completing a hard reset: destroying and rebuilding the system from the original backup:

```
sudo ./dev/rebuild.sh
```

## Troubleshooting Wireguard

---

Ensure that your public IP address in your client profile (e.g. `Endpoint = <Mistborn public IP address>:<random port>`) is actually publicly available (not in 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) if you are attempting to access Mistborn across the internet.

## Troubleshooting Extra Services

---

Each extra service has its own systemd process which can be monitored:

```
sudo journalctl -xfu Mistborn-homeassistant
sudo journalctl -xfu Mistborn-bitwarden
sudo journalctl -xfu Mistborn-syncthing
sudo journalctl -xfu Mistborn-jellyfin
sudo journalctl -xfu Mistborn-nextcloud
sudo journalctl -xfu Mistborn-jitsi
sudo journalctl -xfu Mistborn-guacamole
sudo journalctl -xfu Mistborn-rocketchat
sudo journalctl -xfu Mistborn-onlyoffice
sudo journalctl -xfu Mistborn-tor
sudo journalctl -xfu Mistborn-raspap
sudo journalctl -xfu Mistborn-wazuh
```

## Troubleshooting Docker

---

Instead of defaulting to a system DNS server, Docker will try to use a public DNS server (e.g. 8.8.8.8). If you're having issues pulling or building Docker containers with "failure to connect" errors, this is the likely problem. You can manually set the DNS server Docker should use with the `DOCKER_OPTS` field in `/etc/default/docker`. Example:

```
DOCKER_OPTS="--dns 192.168.50.1 --dns 1.1.1.1"
```

Be sure to restart Docker afterward:

```
sudo systemctl restart docker
```

## Troubleshooting Upgrade from Ubuntu 18.04 to 20.04

---

New installations of 18.04 and 20.04 after 25 April 2020 don't seem to be having issues. If you installed Mistborn on Ubuntu 18.04 prior to 25 April 2020 and then upgrade to 20.04 you may have one minor issue described below.

Owing to changes in docker NAT rules and container DNS resolution, some Wireguard client configurations generated with Mistborn before 25 April 2020 (be sure to update Mistborn) may experience issues after upgrading to Ubuntu 20.04 LTS. Symptoms: can ping but can't resolve DNS.

Solution: Edit the Wireguard client config and set the DNS directive as follows:

```
DNS = 10.2.3.1
```

Close the config and restart the client Wireguard process.

## Troubleshooting Raspberry Pi OS (Raspbian)

---

Be sure to always reboot after updating the kernel. When the kernel is updated the kernel modules are deleted (for the currently running kernel) and you will have issues with any function requiring kernel modules (e.g. `iptables` or `wireguard`).

**Note:** The Raspberry Pi OS 64-bit BETA (versions from May 2020 and prior) have a bug where the `os-release` info indicates that it is Debian. Mistborn proceeds to install as though it were Debian. Since it's not Debian there are errors.

## Troubleshooting Debian 10

---

Run updates and restart before installing Mistborn (`sudo apt-get update && sudo apt-get -y dist-upgrade && sudo shutdown -r now`). Some older Linux kernels will prevent newer Wireguard versions from installing.

## Technical and Security Insights

---

These are some notes regarding the technical design and implementations of Mistborn. Feel free to contact me for additional details.

### Attack Surface

---

See the [Mistborn Network Security](#) wiki entry.

- **Wireguard:** Wireguard is the only way in to Mistborn. When new Wireguard profiles are generated they are attached to a random UDP port. Wireguard does not respond to unauthenticated traffic. External probes on the active Wireguard listening ports are not logged and do not appear on the Metrics page.
- **SSH:** If Mistborn is installed over SSH (most common) then an `iptables` rule is added allowing future SSH connections from the same source IP address. All other external SSH is blocked. Internal SSH (over the Wireguard tunnels) is allowed. Password authentication is allowed. The SSH key for the `mistborn` user is only accepted from internal source IP addresses. `Fail2ban` is also installed.
- **Traefik:** `iptables` closes web ports (TCP 80 and 443) from external access and additionally all web interfaces are behind the Traefik reverse-proxy. All web requests (e.g. `home.mistborn`) must be resolved by Mistborn DNS (Pi-hole/dnsmasq) and originate from a Wireguard tunnel.



- **Docker:** When Docker exposes a port it creates a PREROUTING rule in the NAT table to catch eligible network requests. This means that even if your INPUT chain policy is DROP, your docker containers with exposed ports can receive and respond to traffic. Whenever Mistborn brings up a docker container with an exposed port it creates an iptables rule to block external traffic to that service.

## Firewall

---

- **IPtables:** Iptables rules and chains are manipulated directly. If UFW is present it is disabled. IPtables-persistent is used to save a simple set of secure default rules (most importantly setting the INPUT and FORWARD policies to DROP and allowing ESTABLISHED and RELATED traffic) that will be effective immediately upon system startup. Additional rules and chains are created by Docker on startup. Mistborn also creates some iptables chains during installation that are saved in the persistent rules. Mistborn iptables chains and rules are designed to work with Docker's with logic that is easy to follow. A power cycle will always result in a working state.
- **PostUp/PostDown:** Wireguard configuration files on Mistborn include PostUp and PostDown directives that set routes and iptables rules for each Wireguard client individually.
- **Wireguard:** There is a one-to-one mapping between each Wireguard client and server instance listening on Mistborn. By default Wireguard clients cannot talk directly to each other but can use shared services and resources on Mistborn (e.g. Syncthing, Nextcloud, Jitisi, etc). Toggling the "client-to-client" option will enable direct client-to-client communication.
- **Metrics:** In addition to the iptables INPUT policy set to DROP, an iptables chain exists that logs the packet meta data before dropping it. Mistborn redirects packets that will be dropped to this chain instead. A summary of the data about these dropped packets (unsolicited network traffic) can be found on the Metrics page.
- **Coppercloud:** Coppercloud works by populating ipsets with the ipset module in iptables to DROP (blacklist) or ACCEPT (whitelist) a given set of IP addresses. Upon system startup a celery task will compile the IP addresses, create the ipsets, and iptables rules.

## Additional Notes

---

- Interface names are not hardcoded anywhere in Mistborn. Two commands that are used in different circumstances to determine the default network interface and the interface that would route a public IP address are: `ip -o -4 route show to default` and `ip -o -4 route get 1.1.1.1`.
- The "Update" button will pull updated Docker images for mistborn, postgresql, redis, pihole, and dnscrypt. Those services will then be restarted.
- The generated TLS certificate has an RSA modulus of 4096 bits, is signed with SHA-256, and is good for 397 days. The certificate is checked daily and will regenerate when expiration is within 30 days.
- Outbound UDP on port 53 is blocked. All DNS requests should be handled by the dnscrypt\_proxy service and if any client, service, etc. tries to circumvent that it is blocked.
- Unattended upgrades are set to automatically install operating system security updates.
- Ownership of mistborn files is set to the system mistborn user and access to environment variables is disabled for users other than the owner.

## Roadmap (not necessarily in order)

---

Many features and refinements are in the works at various stages including:

- Plugins for Extra Services (enabling third-party development)
- Plugin repository
- IPv6 support
- Anomaly detection in network traffic

# Featured In

---

- [Linux Magazine](#) November 2020 (featuring Mistborn version from early May 2020)
- [Awesome Open Source](#) July 2020
- [DB Tech](#) May 2021

# Follow

---

You can find recent bugfixes, functional additions, some extra documentation and more at the Cyber5K Patreon page: <https://www.patreon.com/cyber5k>

# Contact

---

Contact me at [steven@cyber5k.com](mailto:steven@cyber5k.com)

# Support Mistborn

---

Please consider supporting the project via:

- [Paypal.me](#)
- [Buy me a drink](#)
- [Patreon](#)