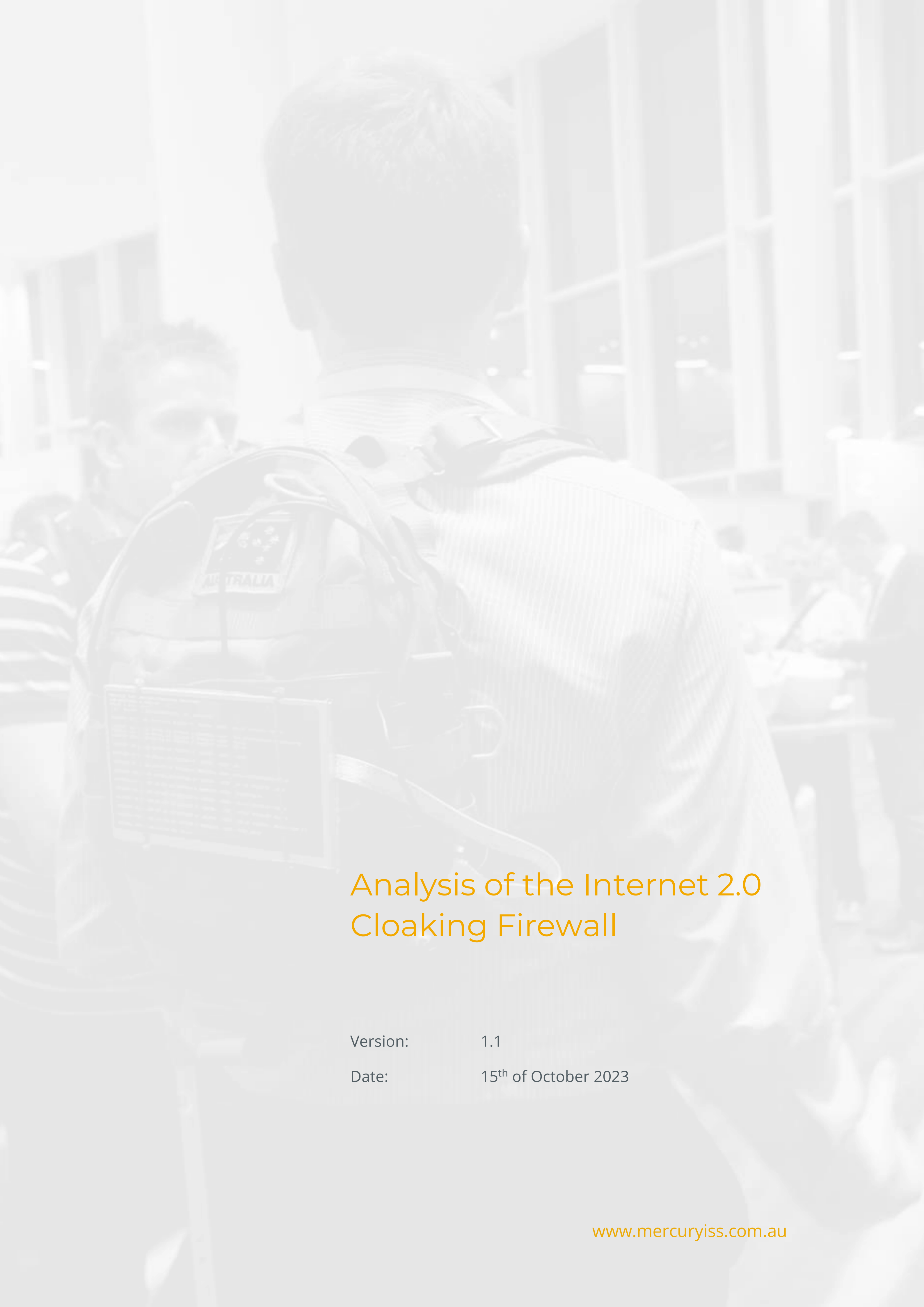


Analysis of the Internet 2.0 Cloaking Firewall

Version: 1.1

Date: 15th of October 2023

www.mercuryiss.com.au

Table of Contents

Document Control

Version	Date	Author	Comments
0.1	20 AUG 2023	Caleb House, Edward Farrell,	Originated
0.2	18 SEP 2023	Sick Codes, Oliver Judson	Technical QA and further research
0.3	21 SEP 2023	Edward Farrell	Internal release
0.4	26 SEP 2023	Edward Farrell	v2 Internal release
0.5	30 SEP 2023	Sick Codes, Edward Farrell	CVEs issued by MITRE Advisory released to vendor
0.6	7 OCT 2023	Edward Farrell	Report updated with Vendor Feedback. Internal and partner release.
1.0	11 OCT 2023	Caleb House, Edward Farrell	Appendices B3-B6 added based on internal feedback. Report approved for public release.
1.1	15 OCT 2023	Edward Farrell	Minor update- broken URL. Added additional URL to illustrate how far behind patching is. Removed AWS/OPNSense observation from Azure related finding.

Executive Summary

Internet 2.0 is a joint US and Australia cyber security organisation whose stated mission is to defend clients and partners from the most advanced threats. Internet 2.0's core products include the Internet 2.0 Cloaking Firewall, Malcore and 5th Column. In July of 2023 Internet 2.0 published an update to content relating to their Cloaking Firewall. The firewall has been a flagship of the organisations product suite and advertises itself as a unique, patented innovation within the cyber security ecosystem *"through our state of the art Obfuscation 2.0 technology".*[1]

Mercury Information Security Services (Mercury) conducted independent analysis of the Internet 2.0 Cloaking Firewall to assess the products security claims, security controls and innovation, the findings of which are system detailed below. This assessment incorporated an analysis of backups generated by Mercury in concert with open-source information.

Key findings

Mercury's assessment of the Cloaking Firewall identified two separate products that appeared to be made up entirely of existing software solutions with limited configuration changes. The presence of default credentials, an unmaintainable application, alongside the absence of hardening guidance for consumers or documentation increased the overall risk profile. A more configurable, easy to use system with lower operational costs and risks could be achieved if consumers employ the technologies on which both products are based on.

Internet 2.0 provided a response to our vulnerability disclosure which was inconsistent with our observations of the systems and Internet 2.0s marketing. As the issue is unlikely to be remediated and our current observations with the vendors approach to vulnerability disclosure, Mercury has published its analysis.

Key observations include:

1. **Azure instance**- Mercury's analysis of the Cloaking Firewall identified that the product in Azure is based largely on an unlicenced version of pfSense Plus, with no additional software, code or unique packages beyond changes to its web interface. Further to this a lack of updates applied over the past 2 years, the existing left over SSH keys, root passwords and information disclosure raised the systems overall risk profile. As patching and configuration is not possible in the current state, a number of these issues may prove challenging to remediate. 4 CVEs have been identified in this product.
2. **AWS Instance**- The AWS instance appears to be an up to date and hardened instance of OPNSense. Having stated this, the absence of stated features such as machine learning as well as another Internet 2.0 product (Malcore) was observed. It may be possible to enumerate AWS instances through the products use of a static OpenVPN port.
3. **Patent Claim**- During our analysis of the Azure instance of the Cloaking Firewall, no unique innovations, code, binaries or innovations were observed. The Internet 2.0 patent application has lapsed and may not be applicable.

Conclusion & recommendations

Whilst both offerings employ existing software solutions and perform firewall related functions, end users may wish to consider the intent of their use as well as greater support and value for money though the existing products on which both solutions are based.

[1] https://web.archive.org/web/20200916122330/https://www.internet2-0.com/

Cloaking Firewall (Azure instance)

Summary

The Internet 2.0 Cloaking Firewall has been advertised as a hardened system that *"disappears your servers and cloud infrastructure from the internet. It no longer appears too [sic] aggressive, deep scanning bots or those running frequent mass port scans".*[2] *The* product is advertised as a significantly hardened pfSense with additional security measures implemented. Mercury backed up the Azure instance of the firewall and conducted its analysis below.

Method of backing up the firewall

To back up the firewalls hard drive, Mercury instantiated a version in Azure from the following link: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001?tab=overview

Mercury backed this system up employing the following steps:

1. Backup the entire VHD following Microsoft's advice.
2. Convert the VHD into a VMDK using the following command
   a. `qemu-img convert -f vpc -O vmdk source.vhd destination.vmdk`
3. Instantiate a new virtual machine with the same hard drive size as the VHD
4. Replace the virtual machines VMDK with the VMDK generated in step 2
5. Launch the virtual machine.

This action took place on the 1st of August 2023 and again on the 7th of September to verify if credentials and other parameters were hardcoded or set as part of instantiation.

Analysis of hard drive artefacts

During our analysis of our backup, Mercury observed the following:

1. The Operating system is FreeBSD Version 12.2-STABLE. Mercury notes this OS is out of date and, in comparison with the dates with which content was generated, appears to have been built whist 3 months out of date.
2. pfSense version 21.05.2 is the primary application running on the Internet 2.0 Cloaking Firewall. This appears to be a version of pfSense Plus, however it is several versions behind. Other applications and software were identified and detailed in the Bill of materials below.
3. The version of Suricata installed is 6.0.4. This application is also several iterations behind and missing critical patches.
4. Historical files from development (Approved SSH key in developers home directory) were also observed.

Beyond images, CSS and HTML referencing Internet 2.0 or the individual artefacts stipulated above, no unique software, applications or proprietary material was identified on the hard drive. Several IP's appear to be automatically denied, however, these appear to come from a set of publicly available lists as well and do not contain any unique insights. The contents of the system are largely open-source packages and software that have been provided in the bill of materials below.

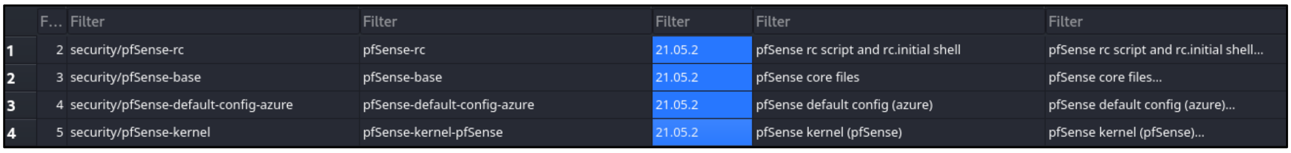
[2] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001?tab=overview

Software Bill of Materials (high level)

As part of Mercury's analysis, the following Bill of Materials was generated from the installed packages via package management. During this generation we identified the following key components were observed to be out of date including:

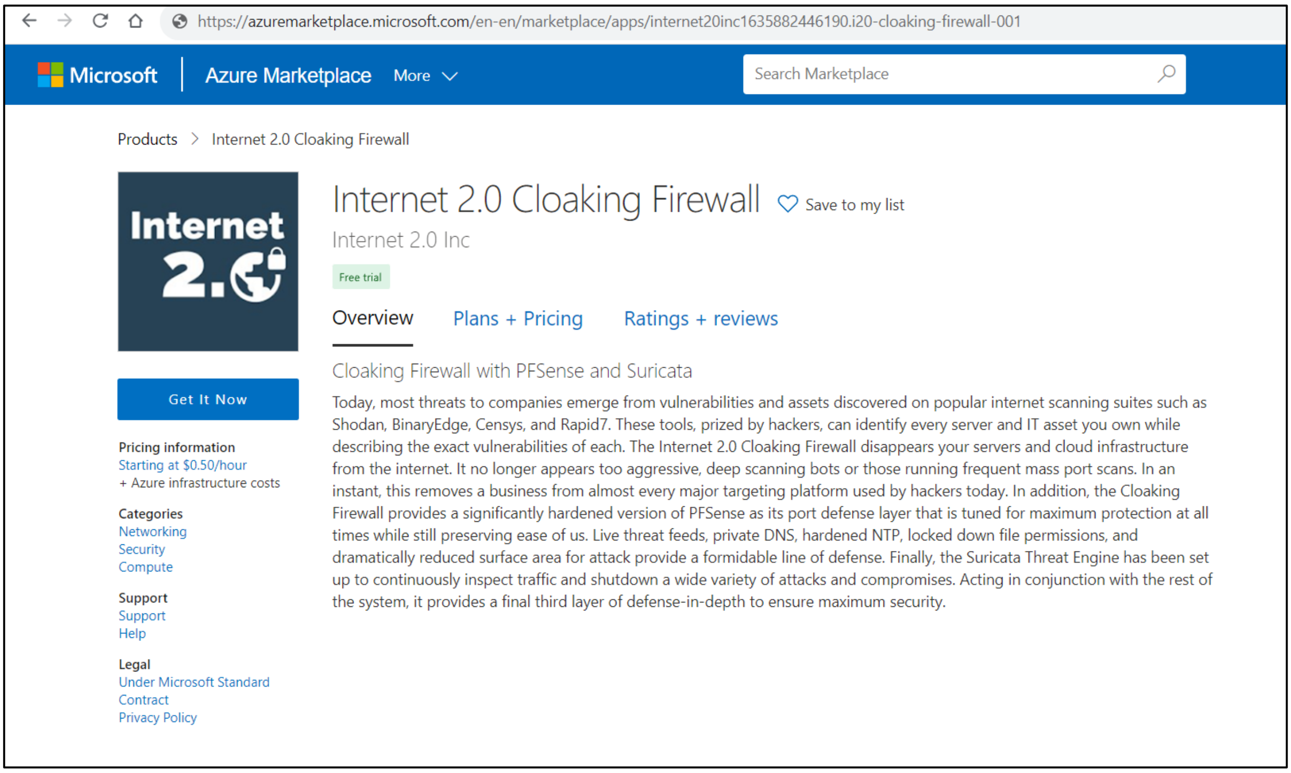
- FreeBSD Version: 12.2-STABLE
- pfSense Plus Version: 21.05.2
- Suricata 6.0.4
- Python Version: 3.8

While it is possible to update pfSense Plus using the command line interface or the web portal, this only updates pfSense Plus and not FreeBSD, Suricata or Python. A more expansive bill of materials has been provided in the appendices however an exhaustive assessment of risk against these items has not taken place.



	F...	Filter	Filter	Filter	Filter	Filter
1	2	security/pfSense-rc	pfSense-rc	21.05.2	pfSense rc script and rc.initial shell	pfSense rc script and rc.initial shell...
2	3	security/pfSense-base	pfSense-base	21.05.2	pfSense core files	pfSense core files...
3	4	security/pfSense-default-config-azure	pfSense-default-config-azure	21.05.2	pfSense default config (azure)	pfSense default config (azure)...
4	5	security/pfSense-kernel	pfSense-kernel-pfSense	21.05.2	pfSense kernel (pfSense)	pfSense kernel (pfSense)...

Figure: Identified pfSense files



https://azuremarketplace.microsoft.com/en-en/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001
Microsoft
Azure Marketplace
More
Search Marketplace
Products > Internet 2.0 Cloaking Firewall
Internet 2.0
Save to my list
Free trial
Overview
Plans + Pricing
Ratings + reviews
Get It Now

Internet 2.0 Cloaking Firewall

Internet 2.0 Inc

Pricing information
Starting at $0.50/hour
+ Azure infrastructure costs

Categories
Networking
Security
Compute

Support
Support
Help

Legal
Under Microsoft Standard Contract
Privacy Policy

Cloaking Firewall with PFSense and Suricata

Today, most threats to companies emerge from vulnerabilities and assets discovered on popular internet scanning suites such as Shodan, BinaryEdge, Censys, and Rapid7. These tools, prized by hackers, can identify every server and IT asset you own while describing the exact vulnerabilities of each. The Internet 2.0 Cloaking Firewall disappears your servers and cloud infrastructure from the internet. It no longer appears too aggressive, deep scanning bots or those running frequent mass port scans. In an instant, this removes a business from almost every major targeting platform used by hackers today. In addition, the Cloaking Firewall provides a significantly hardened version of PFSense as its port defense layer that is tuned for maximum protection at all times while still preserving ease of us. Live threat feeds, private DNS, hardened NTP, locked down file permissions, and dramatically reduced surface area for attack provide a formidable line of defense. Finally, the Suricata Threat Engine has been set up to continuously inspect traffic and shutdown a wide variety of attacks and compromises. Acting in conjunction with the rest of the system, it provides a final third layer of defense-in-depth to ensure maximum security.

Figure: Marketplace offering as it appeared on the 7th of October 2023

Reinforcing the absence of patching has been the presence of the following artefacts in `/root/.cache/pip/selfcheck/0a10f0265722f9a57bbf905d8bf4f3733fa9a7c3e4d8a80438e0686e` illustrated below.

{"key":"/root/lib/azure-cli","last_check":"2021-12-08T00:14:25Z","pypi_version":"21.3.1"}

Vulnerabilities

Proprietary software being used without licence (CVE-2023-44051)

CWE: CWE-1329

The Azure version of the Cloaking Firewall appears to be using pfSense Plus, which requires a licence. pfSense Plus is Netgate's commercial fork of the pfSense project. The version used in the Cloaking Firewall is out of date, and there does not appear to be any indication that the product is licenced or supported by the vendor. As the admin panel was inaccessible, Mercury has only been able to qualify this through its analysis of the file system. Our analysis has identified that:

1. The Netgate Device ID stored in `/var/db/uniqueid` is consistent across both instances acquired from Azure (ID is `61fc9a3274fa10b0aa3c`). This is required for unique device enrolment. Mercury understands a unique key is meant to be generated on instantiation, based on a unique MAC address, this may suggest that the disk image has been cloned.
2. The log at `/cf/conf/upgrade_log.txt` provided an error of “unable to compare version of pfSense-repo” which indicates an error with patching. Our analysis of the help forums indicates that as a result of this message, the system can only be updated by getting the software licenced through the web console.

As pfSense Plus has not been updated since 2021 and does not appear to be maintainable without a software licence. This limits sustained support, enhancements, and updates for the product. Of note, several security patches were released and cannot be applied:

- https://docs.netgate.com/pfsense/en/latest/releases/22-01_2-6-0.html
- https://docs.netgate.com/pfsense/en/latest/releases/versions.html#x

As licencing the product requires a login which is not a default credential or available to the end user to access the admin interface, and factoring in the device ID issue, it is likely that in the normal course of operation of the system the Cloaking Firewall will not be maintainable by the end user.

Public vulnerabilities in Suricata (CVE-2023-44052)

CWE: CWE-1395

A vulnerable instance of In Suricata was observed on the Azure instances of the Cloaking Firewall. before version 6.0.13 of Suricata, a vulnerability is present that may allow an adversary who controls an external source of Lua rules may be able to execute Lua code. This is addressed in 6.0.13 by disabling Lua unless allow-rules are true in the security Lua configuration section (CVE-2023-35853)[3].

Lua rules are disabled in the default state of the provided instance and do not pose an immediate risk. Should Lua rules be enabled this could be exploited as part of 3rd party attacks against supporting infrastructure.

SSH key left in place (CVE-2023-44049)

CWE: CWE-798

User Dan Ehrlich, who left Internet 2.0 in February of 2021 according to LinkedIn, has two authorised SSH keys present for the `danehrlich` and `azureuser` accounts. These keys have been in place for nearly 2 years. As the associated key is also used in a generic account, this key erodes positive assurance that unauthorised access has not taken place against any azure based instances of the system. Both keys have been illustrated below and were observed on both created systems.

[3] https://nvd.nist.gov/vuln/detail/CVE-2023-35853

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDHR51CNyqXShD9zJpEIo73ZUQJ8ZDlvPjFg0BZd6f3X
oD5q39gzxPEiiCSJgYyQ5yyDWiVM838a4dE0Q3C6Ys+dugjGk61pogphQ8kH/oBJtdKDsbksPSU6
4pQ1BAVFdlaDpe4vjukV4lJXN65xg5naA0BtTFUXkxfAl00afdkCD501byoJCDhdiTKeQA+wukPun
YfsQcp+lyoVbPi06MlYNyP7G0rnMftRi9sdV6rzY8hLEn6xcbME2XTPItAXr+GjdB1eGSTnRQnkMD8
vF3dDnsT5qW6HdLDUiJkz9hJ4JHm9UvDaAsh3UO9O5RCEgAet5NbXKT9B8jUSVTtW5bTeh7FO
tNWrgzXJuFx7mR9ZsZFKq0sDocR4gq58GRkfE7lr5h7tyIJu3CNfDQQkeaSZYXIV4qD7GmFx2iZu
RzsgILr+AaXmn7YLETD8L1DRca17pphf8aAbHog/5fNm7QTPxQ66s9wPalUOklfW1o9QE1G6clL5B
MV8D3iKw9MDZE=
```

Figure: output from /home/danehrlich/.ssh/publickeys (last modified 8th of December 2021)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQD45FUqetjc5AXPx4+YKgGBlhfVzx4O7k9e7gHcTsb7ge
Csw0k6Pchn65d/JmcJ97q5ZbwequSPZrWOehbnYp3xma56zeCt5FELrej5z7Sjr9bWFOM5q7OLZ
pn75SiYjW3w609w0+cKeCaVedU68KHcOf4tt9wXBZYPCtWXrUcFhPKFY8bFhpqpLblt1jXfxy2l0o
iPDRJlErOlqaHNCDmeFVwC7dZWhSbgf74lAaiF0nFtTNgHxUjtlR8liH9DGyFtUxiFtO4
M0YoMR5S9Zap5r94e2SDjkHp6glvwaTJkoTAzWJOKOLAtJI1ucCPA/
bONFmOEk5Dby7m95GnBgQZWPiN0kMGElloQcdVWl138Eu4cz4BGyACE6lJG14DYtoK0iD
ery1ebY7qJiQQ2ZZHKeMWUXA4Xfv8Y7MHBmI+IHcWoW7ooBo7Sxf0tc89etdE2Rny/e/
wr+YkphLC0cEFDl4B5wkjvyPnZaUGeGrM5BirlG/2AtQY5h9VdipGWajs=
danehrlich@ntwindows5.local
```

Figure: output from /home/azureuser/.ssh/publickeys. This key is also base64 encoded in the config.xml file (last modified on system creation, indicating key still in use)

Enabled root password account (CVE-2023-44050)

CWE: CWE-798

An administrator account and a root account which make up part of pfSense were observed to have had the default password (*pfSense*) changed to one chosen by Internet 2.0. were both observed as being active within the system and it appears that login is still enabled. These accounts and their `/etc/shadow` parameters have been detailed below and were consistent across 2x separate instances of the firewall extracted from Azure downloaded on separate months. The extract from each file has been illustrated below.

```
root:$2y$10$O/JvoZLcvhTukFtQBlUP3eplIZcawF897JmRVAz94STUfOTkPSvzG:0:0::0:0:Charlie
&:/root:/bin/sh
```

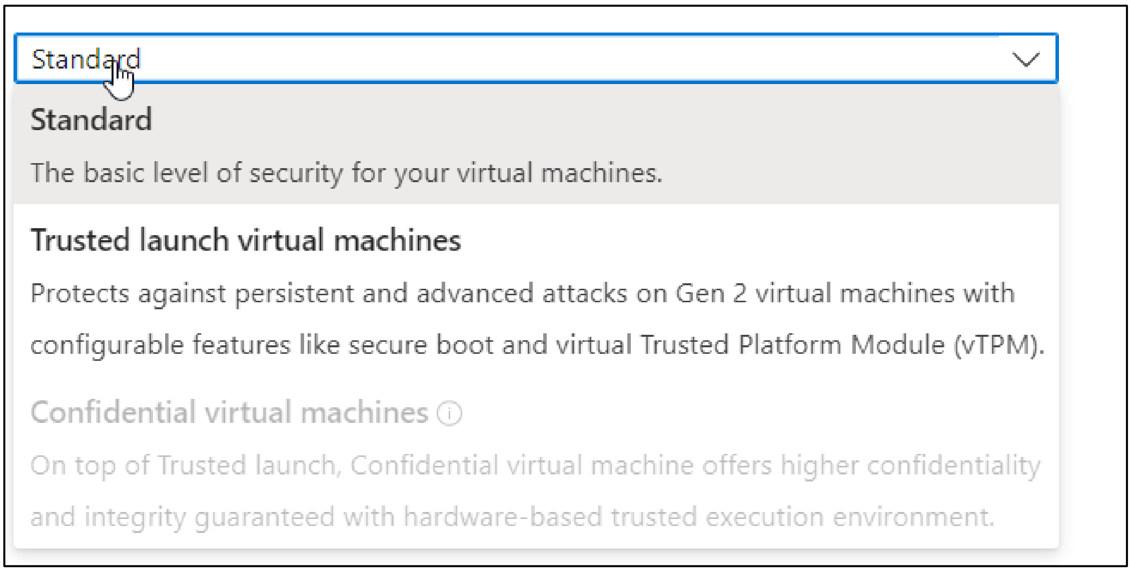
```
admin:$2y$10$O/JvoZLcvhTukFtQBlUP3eplIZcawF897JmRVAz94STUfOTkPSvzG:0:0::0:0:System
Administrator:/root:/etc/rc.initial
```

Figure: enabled root account and admin account. The password on both accounts is shared.

Other observations

Azure security controls cannot be implemented

When creating the system in Azure, it is not possible to select a security type above Standard, which impacts the risk profile for certain users.



Standard

Standard

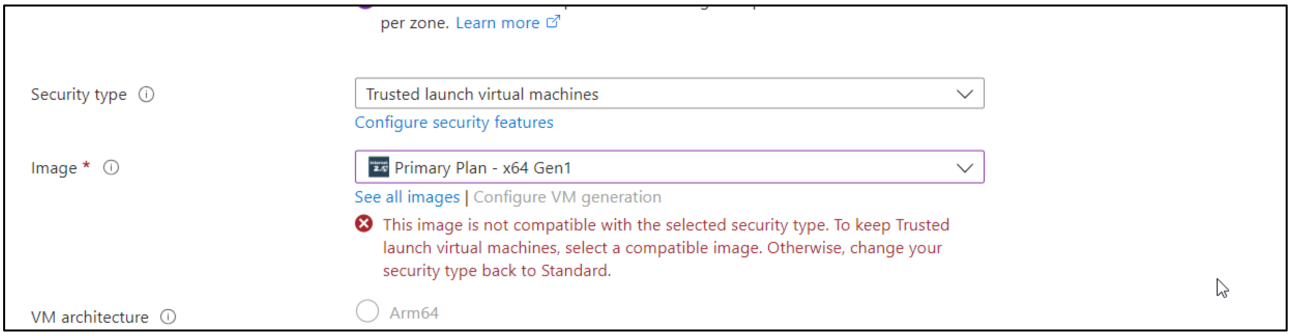
The basic level of security for your virtual machines.

Trusted launch virtual machines

Protects against persistent and advanced attacks on Gen 2 virtual machines with configurable features like secure boot and virtual Trusted Platform Module (vTPM).

Confidential virtual machines ⓘ

On top of Trusted launch, Confidential virtual machine offers higher confidentiality and integrity guaranteed with hardware-based trusted execution environment.



per zone. Learn more

Security type ⓘ: Trusted launch virtual machines

Configure security features

Image * ⓘ: Primary Plan - x64 Gen1

See all images | Configure VM generation

This image is not compatible with the selected security type. To keep Trusted launch virtual machines, select a compatible image. Otherwise, change your security type back to Standard.

VM architecture ⓘ: ○ Arm64

Figure: Azure security controls for trusted/confidential launch cannot be set

Expired/Default Certificates & Keys

Certificates on both the instantiated Azure systems appeared to be the same for the web interface and VPN server. These certificates were self-signed and expired. No documentation on replacing certificates was observed. Similarly, SSH keys were also default and not updated. As the private keys of both can be extracted, these could be used as part of phishing attacks under specific requirements. Awareness of their contents enabled enumeration of systems on the internet has been illustrated in OSINT analysis of public exposure.

IP address disclosure

The contents of /cf/conf/backup/backup.cache identified a login from IP address 203.220.177.89, using the administrator account during the month of January 2022. This IP address was observed throughout the downloaded instances. The IP address is located in Brisbane.

Version control

In the process of documenting the CVEs above, Mercury attempted to ascertain a unique version number of the product which was not available in the information available. As such, we have documented this as v2023 to support vulnerability identification.

Cloaking Firewall (AWS instance)

Summary

The Cloaking Firewall is advertised on AWS as a hardened repackaged version of the OPNSense Firewall. Internet 2.0 have advertised that:

1. *This firewall presents an innovative and more cost-effective cybersecurity solution, as it eliminates the potential for an attack on your network in the first place.*
2. *As a highlight, Machine learning and Malcore analysis [are present] to process threats at the edge and deliver insights and alerts before any other security technology.*
3. *Cloaking technology to disappear from all internet-based scanners*[4].

Mercury backed up the AWS instance of the firewall and conducted its analysis below.

Method of backing up the firewall

Mercury backed up the AWS firewall with the following method:

1. Instantiate an AWS instance of the Internet 2.0 Cloaking Firewall
2. Take a volume snapshot of the firewall
3. Create an instance of OPNSense with 43GB
4. Restore the volume snapshot as a new drive and attach to OPNSense instance.
5. Back up `/dev/nvd1p1` to `./i20_AWS.iso`
6. download `i20_AWS.iso`

This process took place on the 8th of September 2023.

Software Bill of Materials (high level)

As part of Mercury's analysis, the following Bill of Materials was generated from the installed packages via package management. During this generation we identified the key components of OPNSense were present and, whilst some patches were missing, these did not present a security risk. It appears that the OPNSense instance was created during August of 2023 and configured throughout the month. A more expansive bill of materials has been provided in Appendix B6: Software Bill of Materials. Initial analysis suggests multiple packages in excess of what is required remain on the system however this will be the subject of future review.

[4] https://aws.amazon.com/marketplace/pp/prodview-a6g5edkhv3kuo

Observations & configuration analysis

Positive observations

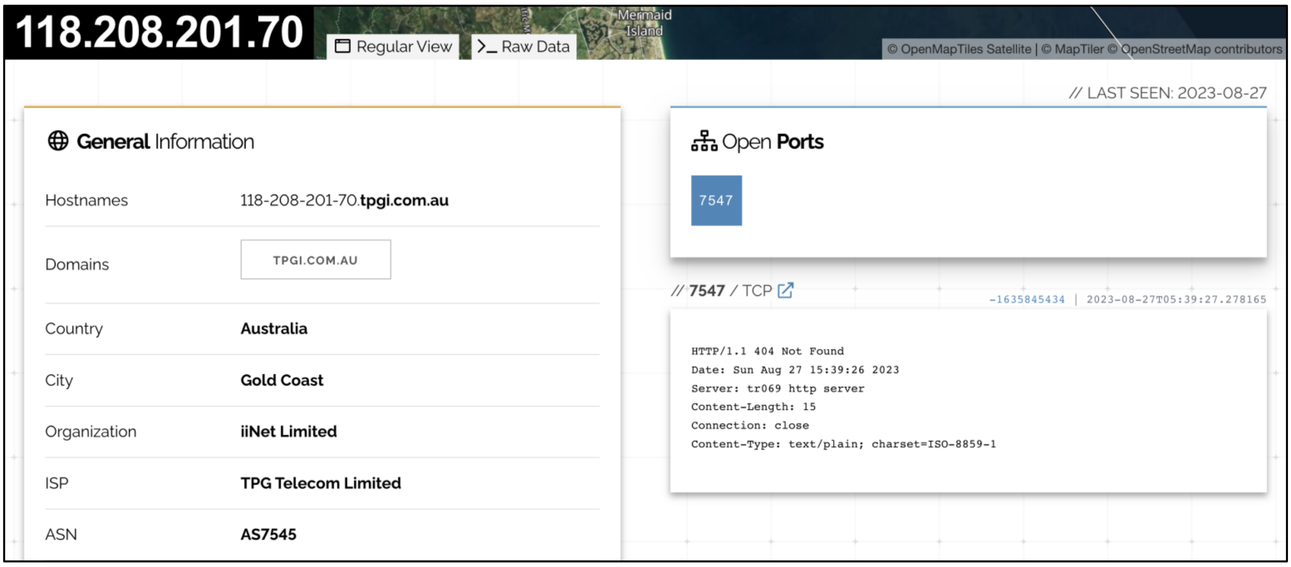
The root account appeared to be disabled and existing keys were removed. The system, which appears to have been published in the past 4 weeks, is largely up to date. However, several release increments (not relating to security vulnerabilities) were published during the time of analysis.

Information disclosure- origin IP addresses

The configuration logs identified a root login during August 2023 from the following IP addresses:

- `118.208.201.70`- TPG Gold Coast IP address (see below)
- `1.146.104.143`- Telstra IP address in Brisbane.
- `103.109.113.14`- Sovereign Cloud Canberra

The address on the Gold Coast did have an exposed service as illustrated below.



Regular View
Raw Data
Mermaid Island
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors

118.208.201.70

// LAST SEEN: 2023-08-27

General Information

Hostnames	118-208-201-70.**tpgi.com.au**
Domains	TPGI.COM.AU
Country	**Australia**
City	**Gold Coast**
Organization	**iiNet Limited**
ISP	**TPG Telecom Limited**
ASN	**AS7545**

Open **Ports**

7547

// **7547** / TCP

-1635845434 | 2023-08-27T05:39:27.278165

```
HTTP/1.1 404 Not Found
Date: Sun Aug 27 15:39:26 2023
Server: tr069 http server
Content-Length: 15
Connection: close
Content-Type: text/plain; charset=ISO-8859-1
```

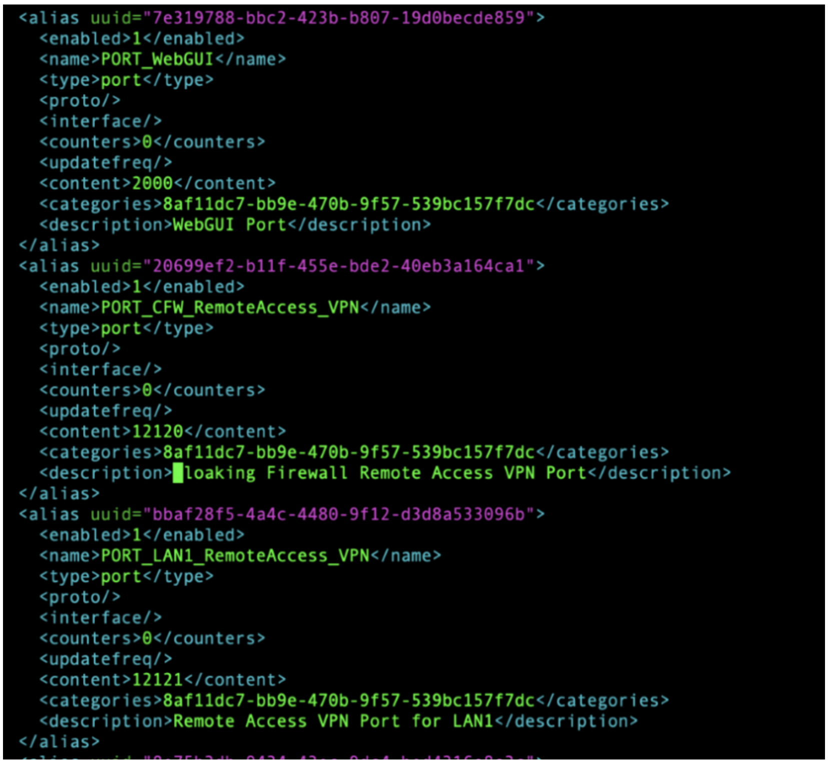
Figure: shodan output for 118.208.201.70

Default Keys & Certificates

The default OpenVPN certificates, SSH Keys and private keys for HTTPS are still in place. This does not present an immediate risk however these should be changed should a user employ the Cloaking Firewall.

Unique UDP port for OpenVPN

During our analysis Mercury identified the default OpenVPN UDP port at 12120. Compared to the usual port of 1194 for OpenVPN. This port is expected to be static across all new instances of the AWS Cloaking Firewall. The use of a static port that cannot be hidden amongst other OpenVPN servers may facilitate the identification of instances of the Cloaking Firewall, as well as enable the identification of end users should traffic be intercepted, and default keys reused to target end users. These rules have been illustrated below:



```
<alias uuid="7e319788-bbc2-423b-b807-19d0becde859">
  <enabled>1</enabled>
  <name>PORT_WebGUI</name>
  <type>port</type>
  <proto/>
  <interface/>
  <counters>0</counters>
  <updatefreq/>
  <content>2000</content>
  <categories>8af11dc7-bb9e-470b-9f57-539bc157f7dc</categories>
  <description>WebGUI Port</description>
</alias>
<alias uuid="20699ef2-b11f-455e-bde2-40eb3a164ca1">
  <enabled>1</enabled>
  <name>PORT_CFW_RemoteAccess_VPN</name>
  <type>port</type>
  <proto/>
  <interface/>
  <counters>0</counters>
  <updatefreq/>
  <content>12120</content>
  <categories>8af11dc7-bb9e-470b-9f57-539bc157f7dc</categories>
  <description>█loaking Firewall Remote Access VPN Port</description>
</alias>
<alias uuid="bbaf28f5-4a4c-4480-9f12-d3d8a533096b">
  <enabled>1</enabled>
  <name>PORT_LAN1_RemoteAccess_VPN</name>
  <type>port</type>
  <proto/>
  <interface/>
  <counters>0</counters>
  <updatefreq/>
  <content>12121</content>
  <categories>8af11dc7-bb9e-470b-9f57-539bc157f7dc</categories>
  <description>Remote Access VPN Port for LAN1</description>
</alias>
```

Figure: Firewall rules

Analysis of other file artefacts

A number of other analysis activities took place, the evidence for which has been provided in Appendices B2 to B6. Key observations include:

1. Mercury did not observe any indication that Malcore or machine learning were present on the system. Of note, an API call to api.Malcore.io was not observed in the provided system similar to what is present in the Malcore client applications.
2. Bash History does not indicate any exhaustive configuration activities have taken place.
3. Initial analysis of the start-up scripts and cron jobs do not indicate any custom software or code that would indicate unique innovation are present.

These observations reinforce our deduction that the firewall appears to be a hardened instance of OPNSense.

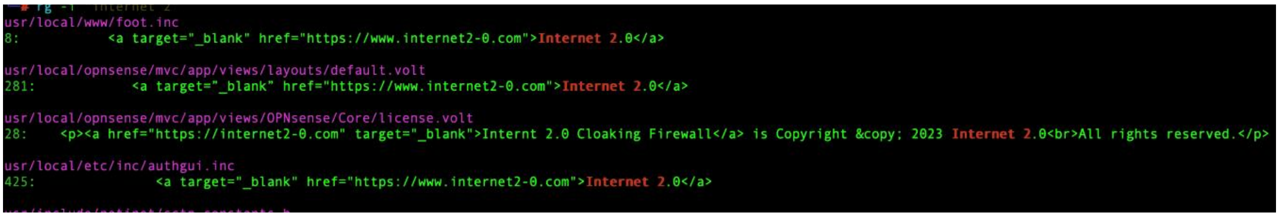
General observations

Difference and Innovation

Within the Azure instance, the only substantiated difference between the Internet 2.0 Cloaking Firewall and pfSense as a standalone system has been the addition of Suricata, the process of which is detailed in the documentation provided by Netgate:

- https://docs.netgate.com/pfSense/en/latest/packages/snort/index.html

As the AWS instance was based on the OPNSense instance provided in the same marketplace, a comparison against file changes identified that additional packages were installed on the Internet 2.0 Cloaking Firewall. No custom or unknown applications were present at the time of writing that would indicate new or innovative products in the AWS instance. Of note, the marketplace description of Internet 2.0s offering discusses the use of Malcore in its defensive posture, however, its presence was not observed during our analysis of the file system, the method for searching for this has been discussed in the Appendices below.



```
└─# rg -i  Internet 2
usr/local/www/foot.inc
8:          <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>

usr/local/opnsense/mvc/app/views/layouts/default.volt
281:           <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>

usr/local/opnsense/mvc/app/views/OPNsense/Core/license.volt
28:    <p><a href="https://internet2-0.com" target="_blank">Internt 2.0 Cloaking Firewall</a> is Copyright &copy; 2023 Internet 2.0<br>All rights reserved.</p>

usr/local/etc/inc/authgui.inc
425:                <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>
```

Figure: only variations observed were within the interface and licence agreement

Governance & Service Level Agreements

Internet 2.0 does not provide service level agreements or support options in comparable detail to the other offerings. Of note, pfSense & OPNSense advertise their support functions and pricing, and in the case of pfSense have prescribed service level agreements. Internet 2.0 does not provide any indication of support mechanisms beyond a contact email and a Jira ticketing system, or any indication of cost. Both products also offer ongoing patching which does not appear to be present with Internet 2.0's operating model.

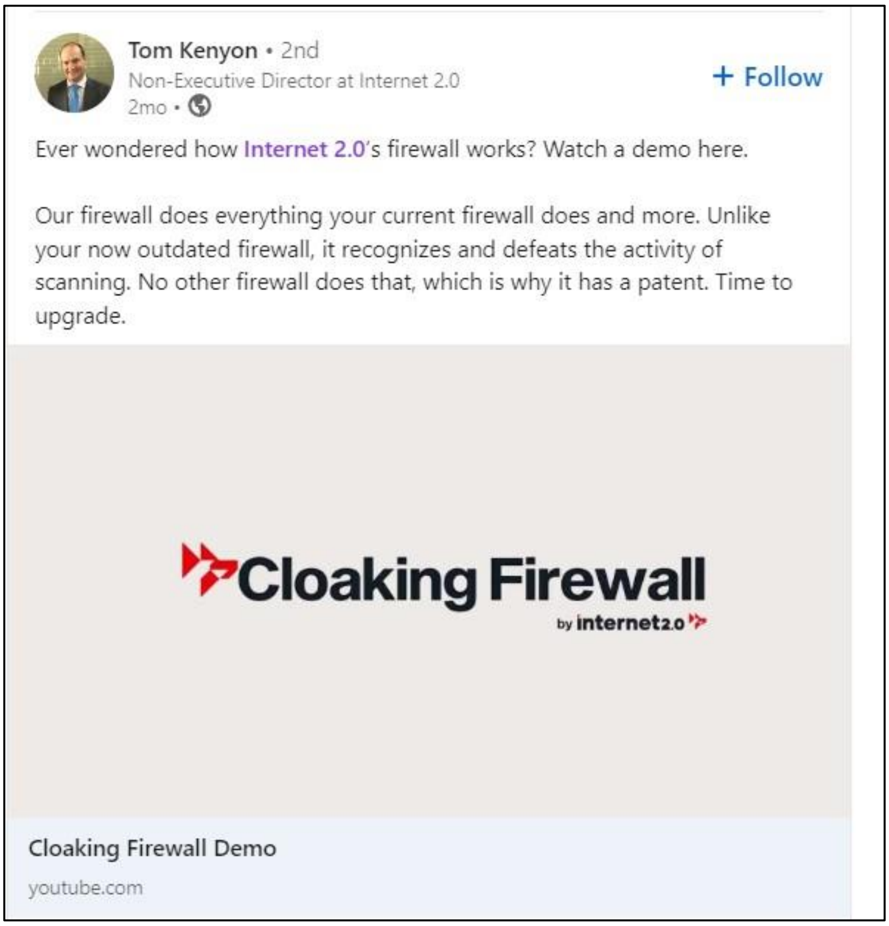
Help manuals and secure configuration guidance

Guidance in securing and maintaining was absent compared to other offerings. pfSense Plus and OPNSense provide support documentation and guidance within their websites.

1. https://docs.netgate.com/pfSense/en/latest/solutions/azure-appliance/index.html
2. https://docs.opnsense.org/manual/how-tos/installaws.html

Patented technology

Internet 2.0 has continued to advertise as of the 7th of September 2023 that the Cloaking Firewall contains patented technology. No unique technology has been found in the drives analysed. This has been a critical component of the marketing materials, the video outlining the firewall and LinkedIn posts. An example of this is illustrated below:



Tom Kenyon • 2nd
Non-Executive Director at Internet 2.0
2mo •

Ever wondered how Internet 2.0's firewall works? Watch a demo here.

Our firewall does everything your current firewall does and more. Unlike your now outdated firewall, it recognizes and defeats the activity of scanning. No other firewall does that, which is why it has a patent. Time to upgrade.

Cloaking Firewall Demo
youtube.com

Figure: screenshot of LinkedIn post taken 5th of October 2023

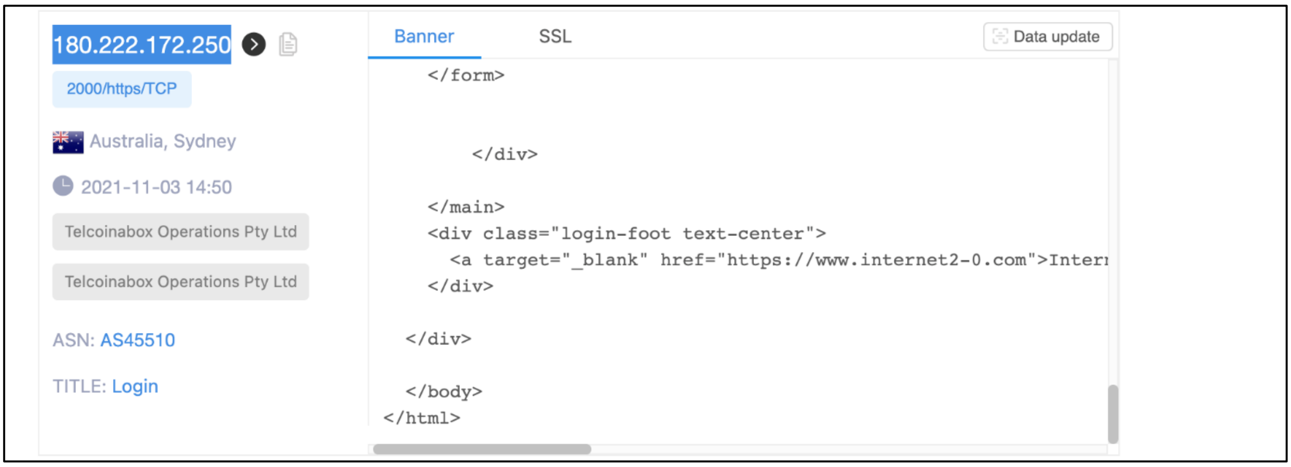
Internet 2.0 filed a provisional patent application in June of 2021 which has since lapsed. Whilst we have not been able to access the patent details, the patent title is "*Systems, methods and devices for secure communication*" However as illustrated above, no innovative or unique software was observed during our analysis, with most of the systems and methods leveraging existing open-source software. Details on the patent application are available at the following URL:

- http://pericles.ipaustralia.gov.au/ols/auspat/applicationDetails.do?applicationNo=2021901725

The OPNSense version discusses the presence of cloaking technologies as well as the presence of Malcore and machine learning, none of which were observed during our analysis.

OSINT analysis of public exposure

Mercury sought to enumerate internet facing instances of the Internet 2.0 Cloaking Firewall. The firewall itself explicitly blocks known scanning engines and malicious sites. It is possible for the firewall to be identified by originating from a location not part of these lists. Mercury did identify instances of the system in the Chinese scanning engine zoomeye, as illustrated below.



180.222.172.250

2000/https/TCP

Australia, Sydney

2021-11-03 14:50

Telcoinabox Operations Pty Ltd

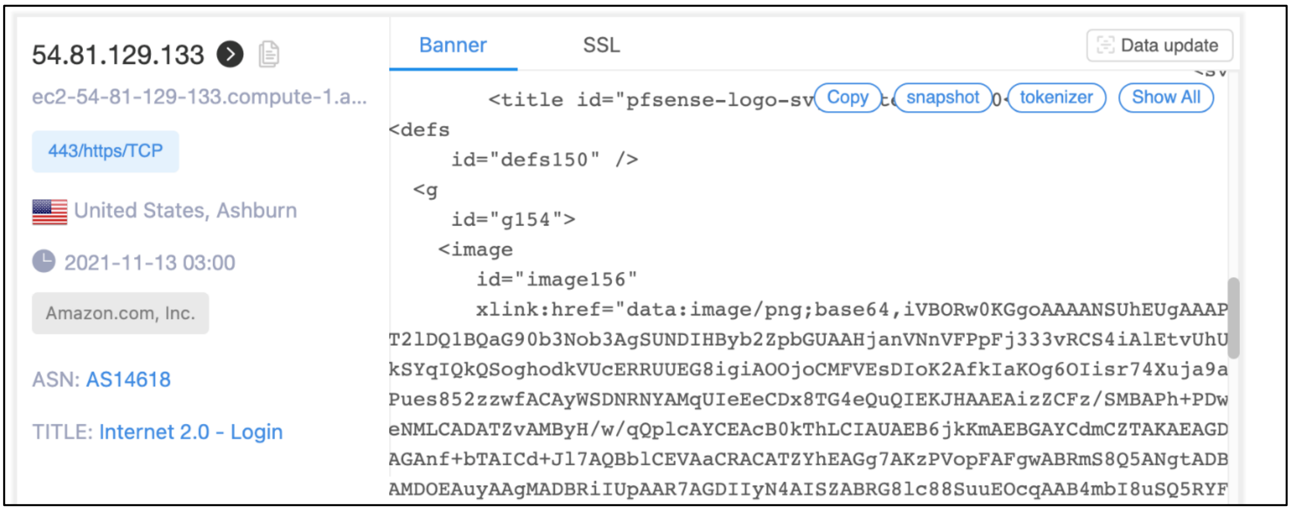
Telcoinabox Operations Pty Ltd

ASN: AS45510

TITLE: Login

```
    </form>


        </div>

    </main>
    <div class="login-foot text-center">
      <a target="_blank" href="https://www.internet2-0.com">Intern
    </div>

  </div>

  </body>
</html>
```

Figure: public instance of Internet 2.0 Cloaking Firewall identified (since removed from the internet)



54.81.129.133

ec2-54-81-129-133.compute-1.a...

443/https/TCP

United States, Ashburn

2021-11-13 03:00

Amazon.com, Inc.

ASN: AS14618

TITLE: Internet 2.0 - Login

```
        <title id="pfsense-logo-sv
<defs
     id="defs150" />
  <g
     id="g154">
    <image
       id="image156"
       xlink:href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAP
```

T2lDQ1BQaG90b3Nob3AgSUNDIHByb2ZpbGUAAHjanVNnVFPpFj333vRCS4iAlEtvUhU
kSYqIQkQSoghodkVUcERRUUEG8igiAOOjoCMFVEsDIoK2AfkIaKOg6OIisr74Xuja9a
Pues852zzwfACAyWSDNRNYAMqUIeEeCDx8TG4eQuQIEKJHAAEAizZCFz/SMBAPh+PDw
eNMLCADATZvAMByH/w/qQplcAYCEAcB0kThLCIAUAEB6jkKmAEBGAYCdmCZTAKAEAGD
AGAnf+bTAICd+Jl7AQBblCEVAaCRACATZYhEAGg7AKzPVopFAFgwABRmS8Q5ANgtADB
AMDOEAuyAAgMADBRiIUpAAR7AGDIIyN4AISZABRG8lc88SuuEOcqAAB4mbI8uSQ5RYF

Figure: public instance of Internet 2.0 Cloaking Firewall identified (since removed from the internet)

Cost analysis (Azure)

Calculating the cost per hour on Azure vs the cost of instantiating a separate pfSense firewall, the following annualised costs and observations have been made (not including traffic costs). As illustrated below, Azures in built systems are financially more cost effective to achieve the same solution from a firewall and reporting standpoint, and as discussed above. Additionally, the support mechanisms within Azure and pfSense are far more detailed and provide prescriptive documentation represents value for money.

	Internet 2.0	pfSense+ on Azure	Azure firewall
Min Hourly Cost	50c/hour	8c/hour	39.5c/hour
Min Annualised cost	$4380 a year	$700 a year	$3460.20 a year
Additional support costs	Unknown, assumed to be integrated.	$399 (pro) to $799 (Enterprise)	NIL, although additional paid likely to be needed.
Total annual cost	**$4380**	**$700 to $1499** depending on licencing.	**$3460.20**
Support options	Via Jira ticketing system	Email/portal, or telephone for enterprise support	NIL- support likely to come from a system integrator.
SLA	SLAs not publicly available	24 to 4 hours engineering support depending on support option selected	Uptime SLA only. Support available from integrators.
Patching and systems maintenance	Cannot be maintained	Manual updates	Automatic updates

Cost analysis (AWS)

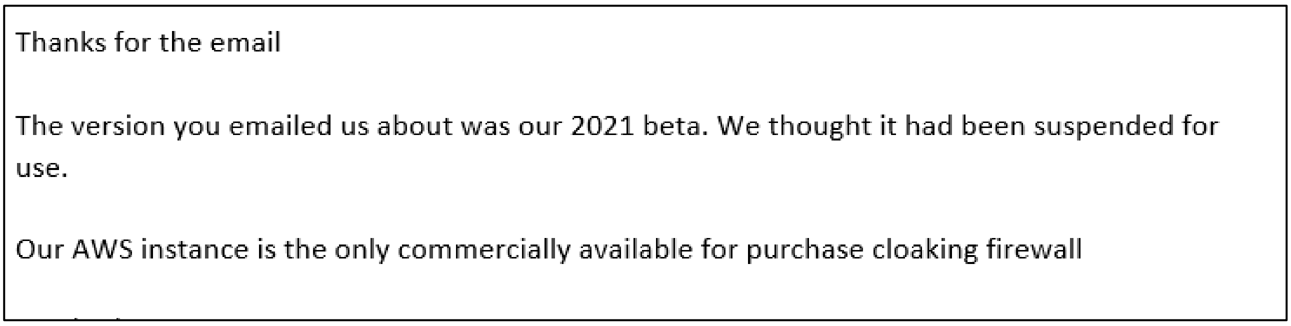
A cost analysis on AWS was slightly more comparable given the greater similarity between both products. Analysis of AWS Marketplace identified that between recommended versions, the OPNSense product is far more configurable and nearly half the price if an annual subscription is made.

	Internet 2.0	OPNSense on AWS
Estimated hourly cost	$0.332/hr (including $0.16 an hour for SW) Total pricing per instance for services hosted on m5a.xlarge in US East (N. Virginia).	USD $0.22/hr (including $0.12 an hour for SW) Total pricing per instance for services hosted on m4.large in US East (N. Virginia). (Source: AWS)
Estimated annual cost	**$3293.76**	***$1844*** *Including savings from annualised purchase.*
Support costs and options	Unknown	Support and professional services available here: https://shop.opnsense.com/product-categorie/support/
SLA	SLAs not publicly available	Support available during enteral European time.
Patching and systems maintenance	Manual updates	Manual updates

Vulnerability disclosure, vendor feedback and response

A vulnerability disclosure was released to the vendor on the 30th of September 2023 featuring our observations in the Azure & AWS instances of the system, however our release to the vendor did not include the executive summary, general observations made above or all our appendices that appear in this document. We have also made modifications following disclosure and expanded our analysis.

A follow up contact was made with the vendor on the 5th of October. The following response was received on the 5th of October:



Thanks for the email

The version you emailed us about was our 2021 beta. We thought it had been suspended for use.

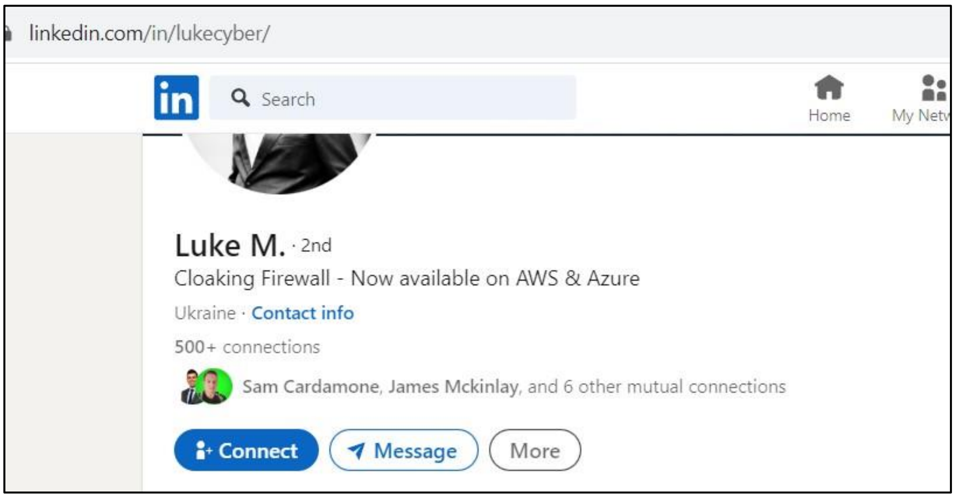
Our AWS instance is the only commercially available for purchase cloaking firewall

Figure: email response from vendor 5th of October 2023

Noting the comment that this as a 2021 Beta, Mercury made following observations between the 5th of October and 7th of October 2023:

1. The white paper was updated on the 2nd of October since its original update on the 5th of October. This can be observed at the archived pages. The white paper itself is not available from July 2023, and cannot be used to qualify if the AWS instance was or was not the only commercially available instance:
    a. 26th of September 2023 archive (white paper updated 5th of July 2023): https://web.archive.org/web/20230926144306/https://internet2-0.com/
    b. 7th of October 2023 archive (white paper updated 2nd of October 2023): https://web.archive.org/web/20231007033710/https://internet2-0.com/
2. The Azure marketplace advertises that the Cloaking Firewall was formally released in February of 2022. This is inconsistent with the observation that this was a 2021 product and much less a beta release. This would also imply that the product was released on the marketplace with the known vulnerabilities released between the 28th of October and the 25th of January 2022, over which period 4 security advisories were released:
    a. Microsoft publication Feb 2022: https://techcommunity.microsoft.com/t5/marketplace-blog-for-partners/azure-marketplace-new-offers-february-24-2022/ba-p/3032248
    b. Security advisories published by Netgate, noting that 21.05.2 was released October 2021: https://docs.netgate.com/advisories/index.html

3. The Azure marketplace instance was still actively advertised on a separate URL on the Internet 2.0 website in August of 2022. https://web.archive.org/web/20220813010502/https://internet2-0.com/solutions/azure-cloaking-firewall/. The Internet 2.0 website links to the instance of the Cloaking Firewall on the Azure marketplace that was the subject of our analysis and is illustrated below. Its presence and active marketing in August 2022 as well as ongoing availability as of October 2023 is inconsistent with the comment that this was a beta version limited to 2021.
    a. Original URL: https://azuremarketplace.microsoft.com/en-en/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001?tab=overview
    b. Archived URL: https://web.archive.org/web/20231007033734/https://azuremarketplace.microsoft.com/en-en/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001
    c. Supporting Media Release: https://web.archive.org/web/20230331031758/https://internet2-0.com/media-release-internet-2-0-partners-with-another-cloud-giant-to-offer-next-generation-firewall-services/
4. An employee of the company was still advertising the Cloaking Firewall as being available on Azure in October 2023, which is also inconsistent with the above statement.



linkedin.com/in/lukecyber/

Luke M. · 2nd

Cloaking Firewall - Now available on AWS & Azure

Ukraine · Contact info

500+ connections

Sam Cardamone, James Mckinlay, and 6 other mutual connections

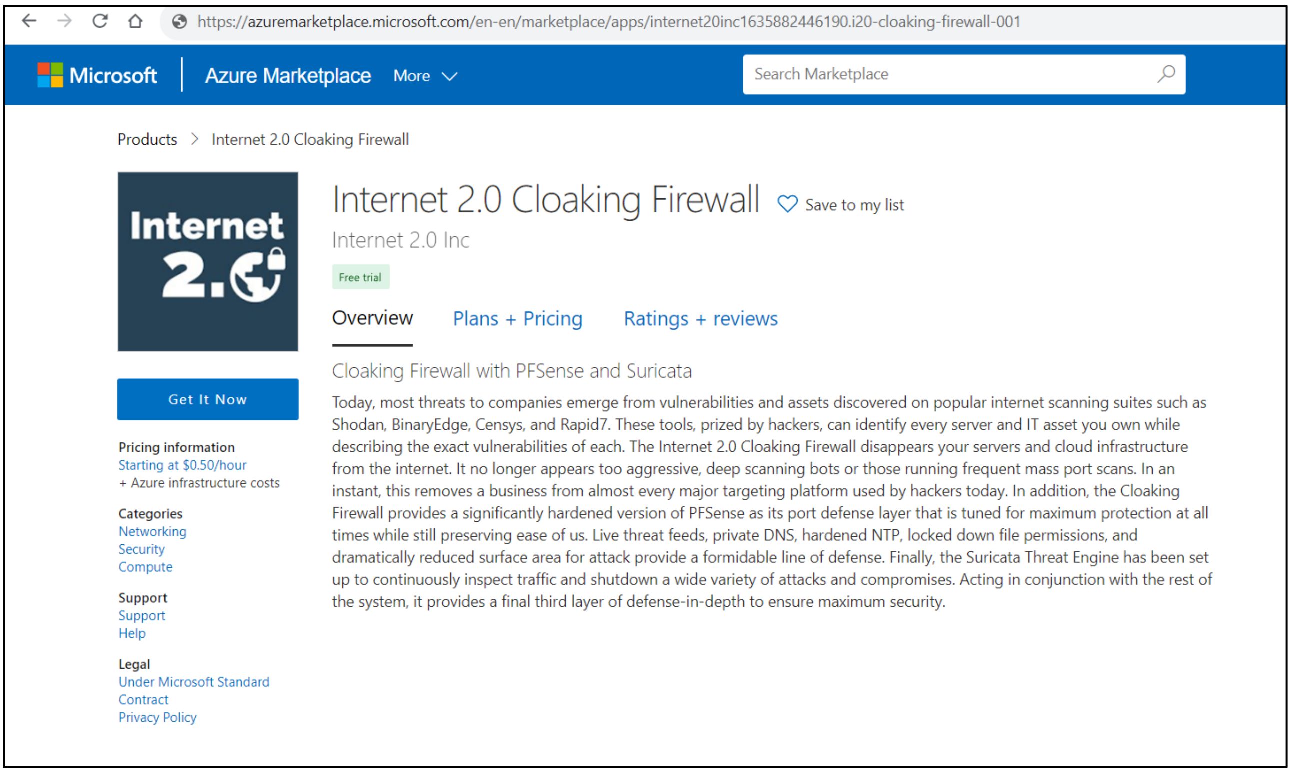
Figure: screenshot of vendor employee profile 5th of October 2023

No contest as to our findings was made around the absence of Malcore, machine learning or the presence of a static port.

It is our assessment that the issue itself is unlikely to be remediated given its claimed state as a beta release, the inconsistencies we have observed and the close ended approach to vulnerability disclosure by the vendor. As a result, we have published these findings ahead of normal disclosure timeframes.

Appendix A: Technical details (Azure)

Appendix A1: Screenshot of marketplace offering


https://azuremarketplace.microsoft.com/en-en/marketplace/apps/internet20inc1635882446190.i20-cloaking-firewall-001
Microsoft
Azure Marketplace
More
Search Marketplace
Products > Internet 2.0 Cloaking Firewall
Internet 2.0
Save to my list
Free trial
Overview
Plans + Pricing
Ratings + reviews
Get It Now

Internet 2.0 Cloaking Firewall

Internet 2.0 Inc

Pricing information
Starting at $0.50/hour
+ Azure infrastructure costs

Categories
Networking
Security
Compute

Support
Support
Help

Legal
Under Microsoft Standard Contract
Privacy Policy

Cloaking Firewall with PFSense and Suricata

Today, most threats to companies emerge from vulnerabilities and assets discovered on popular internet scanning suites such as Shodan, BinaryEdge, Censys, and Rapid7. These tools, prized by hackers, can identify every server and IT asset you own while describing the exact vulnerabilities of each. The Internet 2.0 Cloaking Firewall disappears your servers and cloud infrastructure from the internet. It no longer appears too aggressive, deep scanning bots or those running frequent mass port scans. In an instant, this removes a business from almost every major targeting platform used by hackers today. In addition, the Cloaking Firewall provides a significantly hardened version of PFSense as its port defense layer that is tuned for maximum protection at all times while still preserving ease of us. Live threat feeds, private DNS, hardened NTP, locked down file permissions, and dramatically reduced surface area for attack provide a formidable line of defense. Finally, the Suricata Threat Engine has been set up to continuously inspect traffic and shutdown a wide variety of attacks and compromises. Acting in conjunction with the rest of the system, it provides a final third layer of defense-in-depth to ensure maximum security.

Marketplace offering as it appeared on the 7th of October 2023

Appendix A2: Software Bill of Materials

The following software packages were enumerated on the Azure instance of the Cloaking Firewall.

NAME	VERSION	TYPE
Babel	2.9.1	python
Jinja2	3.0.1	python
MarkupSafe	2.0.1	python
OpenVPN-Installer	1.0.0	dotnet
PyGithub	1.54	python
PyJWT	1.7.1	python
PyNaCl	1.4.0	python
PySocks	1.7.1	python
PyYAML	5.4.1	python
Pygments	2.7.2	python
WALinuxAgent	2.2.54.2	python
adal	1.2.7	python
aiohttp	3.7.4.post0	python
antlr4-python3-runtime	4.9	python
applicationinsights	0.11.10	python

NAME	VERSION	TYPE
argcomplete	1.12.3	python
async-timeout	3.0.1	python
attrs	21.2.0	python
azure-appconfiguration	1.1.1	python
azure-batch	11.0.0	python
azure-cli	2.29.2	python
azure-cli-core	2.29.2	python
azure-cli-telemetry	1.0.6	python
azure-common	1.1.25	python
azure-core	1.20.1	python
azure-cosmos	3.2.0	python
azure-datalake-store	0.0.49	python
azure-functions-devops-build	0.0.22	python
azure-graphrbac	0.61.1	python
azure-identity	1.5.0	python
azure-keyvault	1.1.0	python
azure-keyvault-administration	4.0.0b3	python
azure-keyvault-keys	4.4.0	python
azure-loganalytics	0.1.0	python
azure-mgmt-advisor	9.0.0	python
azure-mgmt-apimanagement	0.2.0	python
azure-mgmt-appconfiguration	2.0.0	python
azure-mgmt-applicationinsights	1.0.0	python
azure-mgmt-authorization	0.61.0	python
azure-mgmt-batch	16.0.0	python
azure-mgmt-batchai	7.0.0b1	python
azure-mgmt-billing	6.0.0	python
azure-mgmt-botservice	0.3.0	python
azure-mgmt-cdn	11.0.0	python
azure-mgmt-cognitiveservices	12.0.0	python
azure-mgmt-compute	23.0.0	python
azure-mgmt-consumption	3.0.0	python
azure-mgmt-containerinstance	9.0.0	python
azure-mgmt-containerregistry	8.1.0	python
azure-mgmt-containerservice	16.1.0	python
azure-mgmt-core	1.2.1	python
azure-mgmt-cosmosdb	6.4.0	python
azure-mgmt-databoxedge	1.0.0	python
azure-mgmt-datalake-analytics	0.6.0	python
azure-mgmt-datalake-store	0.5.0	python
azure-mgmt-datamigration	9.0.0	python
azure-mgmt-deploymentmanager	0.2.0	python
azure-mgmt-devtestlabs	4.0.0	python
azure-mgmt-dns	8.0.0	python

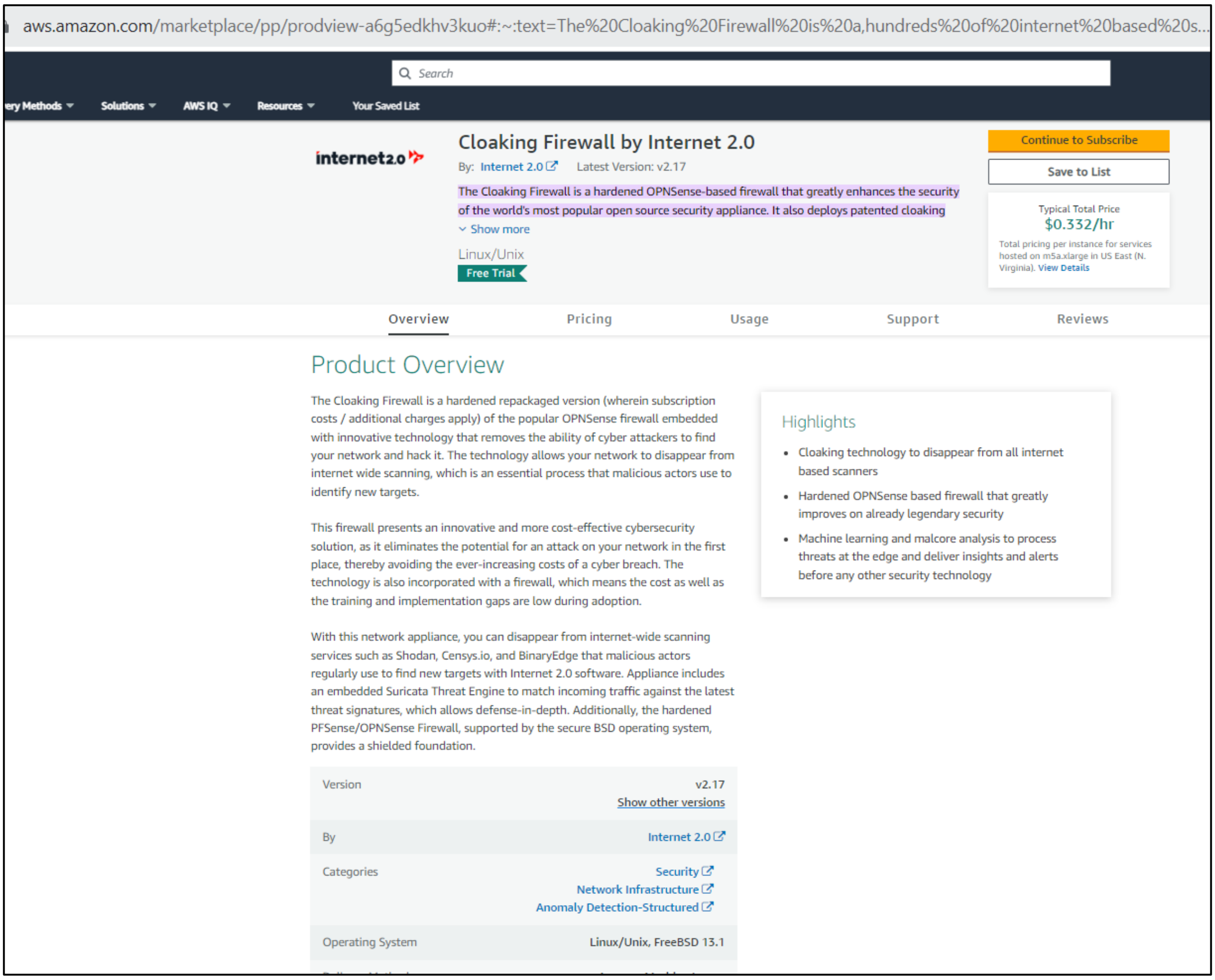
NAME	VERSION	TYPE
azure-mgmt-eventgrid	9.0.0	python
azure-mgmt-eventhub	9.1.0	python
azure-mgmt-extendedlocation	1.0.0b2	python
azure-mgmt-hdinsight	8.0.0	python
azure-mgmt-imagebuilder	0.4.0	python
azure-mgmt-iotcentral	9.0.0b1	python
azure-mgmt-iothub	2.1.0	python
azure-mgmt-iothubprovisioningservices	0.3.0	python
azure-mgmt-keyvault	9.1.0	python
azure-mgmt-kusto	0.5.0	python
azure-mgmt-loganalytics	11.0.0	python
azure-mgmt-managedservices	1.0.0	python
azure-mgmt-managementgroups	0.2.0	python
azure-mgmt-maps	2.0.0	python
azure-mgmt-marketplaceordering	1.1.0	python
azure-mgmt-media	7.0.0	python
azure-mgmt-monitor	2.0.0	python
azure-mgmt-msi	1.0.0	python
azure-mgmt-netapp	4.0.0	python
azure-mgmt-network	19.0.0	python
azure-mgmt-policyinsights	1.0.0	python
azure-mgmt-privatedns	1.0.0	python
azure-mgmt-rdbms	9.1.0b1	python
azure-mgmt-recoveryservices	2.0.0	python
azure-mgmt-recoveryservicesbackup	0.15.0	python
azure-mgmt-redhatopenshift	1.0.0	python
azure-mgmt-redis	13.0.0	python
azure-mgmt-relay	0.2.0	python
azure-mgmt-reservations	0.7.0	python
azure-mgmt-resource	19.0.0	python
azure-mgmt-search	8.0.0	python
azure-mgmt-security	2.0.0b1	python
azure-mgmt-servicebus	6.0.0	python
azure-mgmt-servicefabric	1.0.0	python
azure-mgmt-servicefabricmanagedclusters	1.0.0	python
azure-mgmt-signalr	1.0.0b2	python
azure-mgmt-sql	3.0.1	python
azure-mgmt-sqlvirtualmachine	1.0.0b1	python
azure-mgmt-storage	19.0.0	python
azure-mgmt-synapse	2.0.0	python
azure-mgmt-trafficmanager	0.51.0	python
azure-mgmt-web	4.0.0	python

NAME	VERSION	TYPE
azure-multiapi-storage	0.6.2	python
azure-storage-common	2.1.0	python
azure-synapse-accesscontrol	0.5.0	python
azure-synapse-artifacts	0.8.0	python
azure-synapse-managedprivateendpoints	0.3.0	python
azure-synapse-spark	0.2.0	python
bash	5.1.8	binary
bcrypt	3.2.0	python
blinker	1.4	python
certifi	2021.10.8	python
cffi	1.15.0	python
chardet	4.0.0	python
chunky_png	1.3.8	gem
colorama	0.4.4	python
cryptography	3.3.2	python
fabric	2.5.0	python
humanfriendly	10	python
idna	2.1	python
invoke	1.6.0	python
isc	2	python
isodate	0.6.0	python
javaproperties	0.5.2	python
jmespath	0.10.0	python
jsondiff	1.3.0	python
knack	0.8.2	python
libphp	7.4.20	binary
maxminddb	2.0.3	python
msal	1.10.0	python
msal-extensions	0.3.0	python
msrest	0.6.21	python
msrestazure	0.6.3	python
multidict	5.2.0	python
nginx	1.20.1	binary
oauthlib	1.1.2	python
packaging	21.3	python
paramiko	2.7.2	python
php-cli	7.4.20	binary
php-fpm	7.4.20	binary
pip	20.3.4	python
pip	21.3.1	python
pkginfo	1.8.2	python

NAME	VERSION	TYPE
ply	3.11	python
portalocker	1.7.1	python
psutil	5.8.0	python
pyOpenSSL	20.0.1	python
pyasn1	0.4.7	python
pycparser	2.21	python
pyparsing	3.0.6	python
python	3.8.10	binary
python-dateutil	2.8.1	python
pytz	2021.3	python
requests	2.25.1	python
requests-oauthlib	0.6.2	python
scp	0.13.3	python
semver	2.13.0	python
setuptools	57.0.0	python
setuptools	59.5.0	python
six	1.16.0	python
sqlite3	0.0.0	python
sshtunnel	0.1.5	python
suricata	6.0.4	python
suricata-update	1.2.3	python
tabulate	0.8.6	python
typing-extensions	3.10.0.2	python
urllib3	1.26.7	python
vsts	0.1.25	python
websocket-client	0.58.0	python
wheel	0.36.2	python
wheel	0.37.0	python
xmltodict	0.12.0	python
yarl	1.7.2	python

Appendix B: Technical details (AWS)

Appendix B1: Screenshot of marketplace offering



aws.amazon.com/marketplace/pp/prodview-a6g5edkhv3kuo#:~:text=The%20Cloaking%20Firewall%20is%20a,hundreds%20of%20internet%20based%20s...
Search
ery Methods
Solutions
AWS IQ
Resources
Your Saved List
internet2.0
Continue to Subscribe
Save to List
Overview
Pricing
Usage
Support
Reviews

Cloaking Firewall by Internet 2.0

By: Internet 2.0 Latest Version: v2.17

The Cloaking Firewall is a hardened OPNSense-based firewall that greatly enhances the security of the world's most popular open source security appliance. It also deploys patented cloaking

Show more

Linux/Unix

Free Trial

Typical Total Price
$0.332/hr
Total pricing per instance for services hosted on m5a.xlarge in US East (N. Virginia). View Details

Product Overview

The Cloaking Firewall is a hardened repackaged version (wherein subscription costs / additional charges apply) of the popular OPNSense firewall embedded with innovative technology that removes the ability of cyber attackers to find your network and hack it. The technology allows your network to disappear from internet wide scanning, which is an essential process that malicious actors use to identify new targets.

This firewall presents an innovative and more cost-effective cybersecurity solution, as it eliminates the potential for an attack on your network in the first place, thereby avoiding the ever-increasing costs of a cyber breach. The technology is also incorporated with a firewall, which means the cost as well as the training and implementation gaps are low during adoption.

With this network appliance, you can disappear from internet-wide scanning services such as Shodan, Censys.io, and BinaryEdge that malicious actors regularly use to find new targets with Internet 2.0 software. Appliance includes an embedded Suricata Threat Engine to match incoming traffic against the latest threat signatures, which allows defense-in-depth. Additionally, the hardened PFSense/OPNSense Firewall, supported by the secure BSD operating system, provides a shielded foundation.

Version	v2.17 Show other versions
By	Internet 2.0
Categories	Security Network Infrastructure Anomaly Detection-Structured
Operating System	Linux/Unix, FreeBSD 13.1

Highlights

- Cloaking technology to disappear from all internet based scanners
- Hardened OPNSense based firewall that greatly improves on already legendary security
- Machine learning and malcore analysis to process threats at the edge and deliver insights and alerts before any other security technology

Marketplace offering as it appeared on the 7th of October 2023

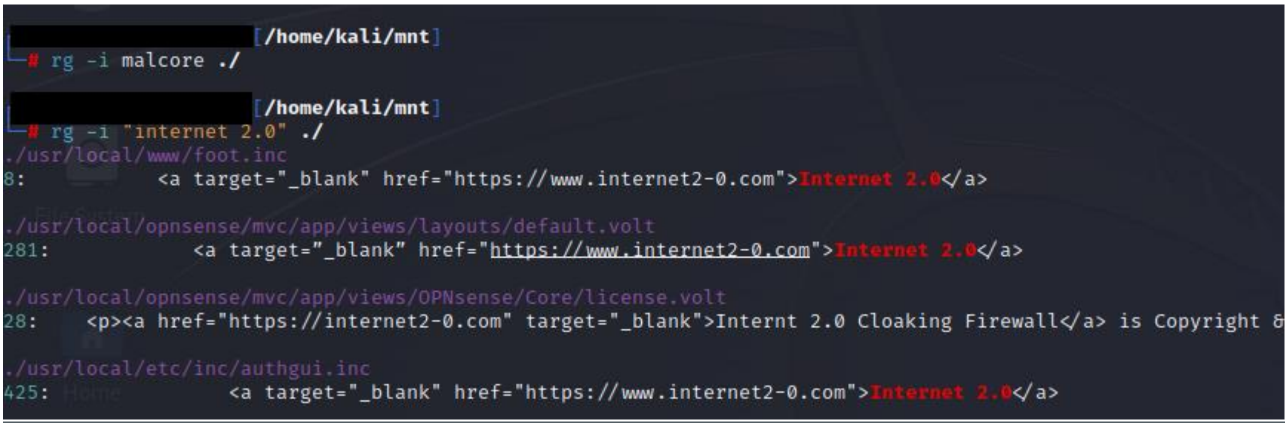
Appendix B2: test case- presence (or absence) of Malcore

Aim: to verify if Malcore was present Malcore analysis to *"process threats at the edge"* in line with the product statement made on AWS marketplace.

Rationale: Malcore is an Internet 2.0 product that is advertised as *"…the fastest commercial sandbox built with a reverse engineering platform at its core.*[5]*"* Any indicator that Malcore is in use as advertised on the marketplace offering would be indicated by the presence of Malcore as a string. This rationale has been deducted from the Malcore agent where a call is made to api.Malcore.io and no local analysis appears to be conducted.

Method: run ripgrep over AWS disk instance to search for any strings containing the string (all cases) "Malcore"

Observation:



```
┌[redacted][/home/kali/mnt]
└─# rg -i malcore ./

┌[redacted][/home/kali/mnt]
└─# rg -i "internet 2.0" ./
./usr/local/www/foot.inc
8:          <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>

./usr/local/opnsense/mvc/app/views/layouts/default.volt
281:            <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>

./usr/local/opnsense/mvc/app/views/OPNsense/Core/license.volt
28:     <p><a href="https://internet2-0.com" target="_blank">Internt 2.0 Cloaking Firewall</a> is Copyright &

./usr/local/etc/inc/authgui.inc
425:             <a target="_blank" href="https://www.internet2-0.com">Internet 2.0</a>
```

Figure- search for Malcore. In its absence, another search for Internet 2.0 was made to verify the same disk was being analysed.

Conclusion: Malcore was not observed on disk and has been assessed as not being present.

[5] https://malcore.io/

Appendix B3: Bash history

The following contents below is the output of the bash history for the ec2-user on the AWS instance of the Cloaking Firewall. SSH Keys were removed frequently and crontab updated. Crontabs have been provided in Appendix B4: Crontab.

```
#+1643190757
su -
#+1643190773
sudo /bin/sh
#+1643200242
sudo sh
#+1643874864
sudo sh
#+1643875783
sudo sh
#+1643876725
joe /conf/config.xml
#+1643876733
joe /conf/config.xml
#+1643876771
cd /usr/local/opnsense/scripts/aws/
#+1643876776
ls
#+1643876780
./init.sh
#+1643876782
ls -asl
#+1643876789
sudo sh
#+1643877391
sudo sh
#+1643878528
sudo sh
#+1643878878
sudo sh
#+1643880286
sudo sh
#+1643881482
sudo sh
#+1684727378
exit
#+1687842290
ls
#+1687842319
su root
#+1687842326
sudo su root
#+1691276334
opnsense-opnsense-shell password
#+1691276338
opnsense-shell password
#+1691276380
sudo opnsense-shell password
#+1691276391
```

```
sudo su -
#+1691706215
opnsense-shell
#+1691706219
sudo opnsense-shell
#+1691706246
ls
#+1691706248
pwd
#+1691706252
crontab -e
#+1691706256
sudo su -
#+1691995821
crontab -e
#+1691995834
crontab -e
#+1691995895
rm -rf ~/.ssh/authorized_keys
#+1691995900
cat ~/.ssh/authorized_keys
#+1691995902
sudo shutdown -h now
#+1692241492
sudo su -
#+1692243032
cat ~/.ssh/authorized_keys
#+1692243035
crontab -e
#+1692243080
exit
#+1692243109
rm -f ~/.ssh/authorized_keys
#+1692243111
ls
#+1692243114
ls -la .ssh
#+1692243117
ls -la .ssh
#+1692243118
ls -la .ssh
#+1692243120
ls -la .ssh
#+1692243152
ls -la .ssh
#+1692243156
ls -la .ssh
#+1692243159
ls -la .ssh
#+1692243237
crontab -e
#+1692676224
sudo ls
#+1692676233
cat ~/.ssh/authorized_keys
#+1692676246
```

```
rm -f ~/.ssh/authorized_keys
#+1692676247
rm -f ~/.ssh/authorized_keys
#+1692676247
sudo shutdown -h now
#+1693236088
crontab -e
#+1693236138
crontab -e
#+1693236151
ls -la ~/.ssj
#+1693236153
ls -la ~/.ssh
#+1693236179
cd ~/ssh
#+1693236183
cd ~/.ssh
#+1693236184
cat authorized_keys
#+1693236257
crontab -e
#+1693236263
rm -f ~/.ssh/authorized_keys && sudo shutdown -h now
```

Appendix B4: Crontab

Crontabs appeared to be regularly modified on the AWS instance of the Cloaking Firewall. These did not appear to be modified in a way that would imply additional jobs or software were applied.

```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.GEcSlETcdu installed on Mon Aug 28 15:22:14 2023)
# (Cron version -- $FreeBSD$)
* * * * * /usr/local/bin/curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key >
~/.ssh/authorized_keys
```

Crontab: ec2-user

```
# DO NOT EDIT THIS FILE -- OPNsense auto-generated file
#
# User-defined crontab files can be loaded via /etc/cron.d
# or /usr/local/etc/cron.d and follow the same format as
# /etc/crontab, see the crontab(5) manual page.
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
#minute     hour    mday    month   wday    command
# Origin/Description: IDS/ids rule updates
22      2       *       *       *       /usr/local/sbin/configctl -d 'ids update'
```

Crontab: nobody

```
# DO NOT EDIT THIS FILE -- OPNsense auto-generated file
#
# User-defined crontab files can be loaded via /etc/cron.d
# or /usr/local/etc/cron.d and follow the same format as
# /etc/crontab, see the crontab(5) manual page.
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
REQUESTS_CA_BUNDLE=/etc/ssl/cert.pem
#minute     hour    mday    month   wday    command
1       *       *       *       *       (/usr/local/sbin/configctl -d syslog archive) > /dev/null
2       *       *       *       *       (/usr/local/sbin/expiretable -v -t 3600 sshlockout) > /dev/null
3       *       *       *       *       (/usr/local/sbin/expiretable -v -t 3600 virusprot) > /dev/null
4       *       *       *       *       (/usr/local/etc/rc.expireaccounts) > /dev/null
*/4     *       *       *       *       (/usr/local/sbin/ping_hosts.sh) > /dev/null
0       22      *       *       *       (/usr/local/sbin/configctl -d firmware changelog cron) >
/dev/null
0       */8     *       *       *       (/usr/local/etc/rc.syshook.d/backup/20-dhcpleases) >
/dev/null
0       */8     *       *       *       (/usr/local/etc/rc.syshook.d/backup/20-captiveportal) >
/dev/null
1       3       *       *       0       (/usr/local/sbin/configctl -d filter schedule bogons) > /dev/null
*       *       *       *       *       (/usr/local/bin/flock -n -E 0 -o /tmp/filter_update_tables.lock
/usr/local/opnsense/scripts/filter/update_tables.py) > /dev/null
```

Crontab: root

Appendix B5: Directory index of /usr/local/etc/rc.d

The directory index of /usr/local/etc/rc.d is illustrated in below. Our current assessment of the files located in this directory have not identified any contents that would suggest custom software or applications as part of the instantiation of the AWS instance of the Cloaking Firewall. Similar analysis of /etc/rc.d identified that the scripts were being executed appear to all be part of OPNSense.

```
-rwxr-xr-x 1 root root  2733 Jul 28 09:32 dnsmasq
-rwxr-xr-x 1 root root  3992 Jul 28 09:33 unbound
-rwxr-xr-x 1 root root   495 Jul 28 11:01 kpropd
-rwxr-xr-x 1 root root   667 Jul 28 11:13 choparp
-rwxr-xr-x 1 root root   721 Jul 28 11:25 uuidd
lrwxr-xr-x 1 root root    12 Jul 28 11:53 isc-dhcrelay6 -> isc-dhcrelay
-rwxr-xr-x 1 root root  1814 Jul 28 11:53 isc-dhcrelay
lrwxr-xr-x 1 root root     9 Jul 28 11:54 isc-dhcpd6 -> isc-dhcpd
-rwxr-xr-x 1 root root 12252 Jul 28 11:54 isc-dhcpd
-rwxr-xr-x 1 root root   774 Jul 28 12:09 mpd5
-rwxr-xr-x 1 root root   444 Jul 28 12:16 radvd
-rwxr-xr-x 1 root root  1922 Jul 28 12:17 samplicator
-rwxr-xr-x 1 root root  1741 Jul 28 12:20 wireguard
-rwxr-xr-x 1 root root  1005 Jul 28 12:24 dhcp6c
-rwxr-xr-x 1 root root   714 Jul 28 12:24 flowd
-rwxr-xr-x 1 root root  5558 Jul 28 12:30 openssh
-rwxr-xr-x 1 root root   404 Jul 28 12:36 expiretable
-rwxr-xr-x 1 root root  4374 Jul 28 12:42 openvpn
-rwxr-xr-x 1 root root  1300 Jul 28 12:45 stunnel
-rwxr-xr-x 1 root root  2036 Jul 28 12:46 suricata
-rwxr-xr-x 1 root root   863 Jul 28 13:07 monit
-rwxr-xr-x 1 root root  3315 Jul 28 13:21 lighttpd
-rwxr-xr-x 1 root root  1212 Aug  8 08:16 php-fpm
-rwxr-xr-x 1 root root   970 Aug  8 08:57 rrdcached
-rwxr-xr-x 1 root root  1885 Aug  8 10:30 telegraf
-rwxr-xr-x 1 root root  2097 Aug  8 12:46 strongswan
-rwxr-xr-x 1 root root  1148 Aug  8 13:19 syslog-ng
-rwxr-xr-x 1 root root  4705 Aug  8 13:35 squid
-rwxr-xr-x 1 root root  6990 Aug  9 15:38 netflow
-rwxr-xr-x 1 root root  1143 Aug  9 15:38 flowd_aggregate
-rwxr-xr-x 1 root root  1713 Aug  9 15:38 configd
-rwxr-xr-x 1 root root  5723 Aug  9 15:38 captiveportal
```

Appendix B6: Software Bill of Materials

The following software packages were enumerated on the AWS instance of the Cloaking Firewall.

NAME	VERSION	TYPE
Babel	2.12.1	python
Bottleneck	1.3.7	python
Cython	0.29.36	python
Jinja2	3.1.2	python
MarkupSafe	1.1.1	python
MarkupSafe	2.1.3	python
PySocks	1.7.1	python
PyYAML	6	python
aioquic	0.9.21	python
anyio	3.7.1	python
async-generator	1.1	python
attrs	23.1.0	python
bash	5.2.15	binary
certifi	2023.5.7	python
cffi	1.15.1	python
charset-normalizer	3.2.0	python
cloud.google.com/go	v0.110.1	go-module
cloud.google.com/go/bigquery	v1.51.1	go-module
cloud.google.com/go/compute/metadata	v0.2.3	go-module
cloud.google.com/go/iam	v1.0.0	go-module
cloud.google.com/go/monitoring	v1.14.0	go-module
cloud.google.com/go/pubsub	v1.30.1	go-module
cloud.google.com/go/storage	v1.29.0	go-module
code.cloudfoundry.org/clock	v1.0.0	go-module
collectd.org	v0.5.0	go-module
cryptography	3.4.8	python
dnspython	2.4.1	python
duckdb	0.8.1	python
exceptiongroup	1.1.2	python
firebase/php-jwt	v5.0.0	php-composer
github.com/99designs/keyring	v1.2.2	go-module
github.com/Azure/azure-amqp-common-go/v4	v4.1.0	go-module
github.com/Azure/azure-event-hubs-go/v3	v3.5.0	go-module
github.com/Azure/azure-kusto-go	v0.8.0	go-module
github.com/Azure/azure-pipeline-go	v0.2.3	go-module
github.com/Azure/azure-sdk-for-go	v65.0.0+incompatible	go-module
github.com/Azure/azure-sdk-for-go/sdk/azcore	v0.21.1	go-module
github.com/Azure/azure-sdk-for-go/sdk/azidentity	v0.13.2	go-module
github.com/Azure/azure-sdk-for-go/sdk/internal	v0.9.1	go-module

NAME	VERSION	TYPE
github.com/Azure/azure-sdk-for-go/sdk/resourcemanager/monitor/armmonitor	v0.4.1	go-module
github.com/Azure/azure-sdk-for-go/sdk/resourcemanager/resources/armresources	v0.3.1	go-module
github.com/Azure/azure-sdk-for-go/sdk/storage/azblob	v0.3.0	go-module
github.com/Azure/azure-storage-blob-go	v0.15.0	go-module
github.com/Azure/azure-storage-queue-go	v0.0.0-20191125232315-636801874cdd	go-module
github.com/Azure/go-amqp	v0.19.1	go-module
github.com/Azure/go-autorest/autorest	v0.11.29	go-module
github.com/Azure/go-autorest/autorest/adal	v0.9.23	go-module
github.com/Azure/go-autorest/autorest/azure/auth	v0.5.12	go-module
github.com/Azure/go-autorest/autorest/azure/cli	v0.4.5	go-module
github.com/Azure/go-autorest/autorest/date	v0.3.0	go-module
github.com/Azure/go-autorest/autorest/to	v0.4.0	go-module
github.com/Azure/go-autorest/autorest/validation	v0.3.1	go-module
github.com/Azure/go-autorest/logger	v0.2.1	go-module
github.com/Azure/go-autorest/tracing	v0.6.0	go-module
github.com/Azure/go-ntlmssp	v0.0.0-20220621081337-cb9428e4ac1e	go-module
github.com/AzureAD/microsoft-authentication-library-for-go	v0.4.0	go-module
github.com/ClickHouse/clickhouse-go	v1.5.4	go-module
github.com/Masterminds/goutils	v1.1.1	go-module
github.com/Masterminds/semver	v1.5.0	go-module
github.com/Masterminds/sprig	v2.22.0+incompatible	go-module
github.com/Shopify/sarama	v1.38.1	go-module
github.com/aerospike/aerospike-client-go/v5	v5.11.0	go-module
github.com/alecthomas/participle	v0.4.1	go-module
github.com/alecthomas/units	v0.0.0-20211218093645-b94a6e3cc137	go-module
github.com/aliyun/alibaba-cloud-sdk-go	v1.62.337	go-module
github.com/amir/raidman	v0.0.0-20170415203553-1ccc43bfb9c9	go-module
github.com/andybalholm/brotli	v1.0.5	go-module
github.com/antchfx/jsonquery	v1.3.1	go-module
github.com/antchfx/xmlquery	v1.3.15	go-module
github.com/antchfx/xpath	v1.2.4	go-module
github.com/antlr/antlr4/runtime/Go/antlr/v4	v4.0.0-20230305170008-8188dc5388df	go-module

NAME	VERSION	TYPE
github.com/apache/arrow/go/arrow	v0.0.0-20211112161151-bc219186db40	go-module
github.com/apache/arrow/go/v12	v12.0.0	go-module
github.com/apache/arrow/go/v13	v13.0.0-20230505140406-c2f7d13e16c4	go-module
github.com/apache/iotdb-client-go	v0.12.2-0.20220722111104-cd17da295b46	go-module
github.com/apache/thrift	v0.18.1	go-module
github.com/aristanetworks/glog	v0.0.0-20191112221043-67e8567f59f3	go-module
github.com/aristanetworks/goarista	v0.0.0-20190325233358-a123909ec740	go-module
github.com/armon/go-metrics	v0.4.1	go-module
github.com/awnumar/memcall	v0.1.2	go-module
github.com/awnumar/memguard	v0.22.3	go-module
github.com/aws/aws-sdk-go-v2	v1.18.1	go-module
github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream	v1.4.10	go-module
github.com/aws/aws-sdk-go-v2/config	v1.18.8	go-module
github.com/aws/aws-sdk-go-v2/credentials	v1.13.26	go-module
github.com/aws/aws-sdk-go-v2/feature/dynamodb/attributevalue	v1.2.0	go-module
github.com/aws/aws-sdk-go-v2/feature/ec2/imds	v1.13.4	go-module
github.com/aws/aws-sdk-go-v2/feature/s3/manager	v1.7.1	go-module
github.com/aws/aws-sdk-go-v2/internal/configsources	v1.1.34	go-module
github.com/aws/aws-sdk-go-v2/internal/endpoints/v2	v2.4.28	go-module
github.com/aws/aws-sdk-go-v2/internal/ini	v1.3.28	go-module
github.com/aws/aws-sdk-go-v2/service/cloudwatch	v1.26.2	go-module
github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs	v1.20.9	go-module
github.com/aws/aws-sdk-go-v2/service/dynamodb	v1.17.3	go-module
github.com/aws/aws-sdk-go-v2/service/dynamodbstreams	v1.4.0	go-module
github.com/aws/aws-sdk-go-v2/service/ec2	v1.80.1	go-module
github.com/aws/aws-sdk-go-v2/service/internal/accept-encoding	v1.9.10	go-module
github.com/aws/aws-sdk-go-v2/service/internal/endpoint-discovery	v1.7.28	go-module
github.com/aws/aws-sdk-go-v2/service/internal/presigned-url	v1.9.28	go-module

NAME	VERSION	TYPE
github.com/aws/aws-sdk-go-v2/service/internal/s3shared	v1.9.0	go-module
github.com/aws/aws-sdk-go-v2/service/kinesis	v1.17.8	go-module
github.com/aws/aws-sdk-go-v2/service/s3	v1.19.0	go-module
github.com/aws/aws-sdk-go-v2/service/sso	v1.12.12	go-module
github.com/aws/aws-sdk-go-v2/service/ssooidc	v1.14.12	go-module
github.com/aws/aws-sdk-go-v2/service/sts	v1.19.2	go-module
github.com/aws/aws-sdk-go-v2/service/timestreamwrite	v1.17.2	go-module
github.com/aws/smithy-go	v1.13.5	go-module
github.com/awslabs/kinesis-aggregation/go	v0.0.0-20210630091500-54e17340d32f	go-module
github.com/benbjohnson/clock	v1.3.3	go-module
github.com/beorn7/perks	v1.0.1	go-module
github.com/blues/jsonata-go	v1.5.4	go-module
github.com/bmatcuk/doublestar/v3	v3.0.0	go-module
github.com/boschrexroth/ctrlx-datalayer-golang	v1.3.0	go-module
github.com/bufbuild/protocompile	v0.4.0	go-module
github.com/caio/go-tdigest	v3.1.0+incompatible	go-module
github.com/cenkalti/backoff	v2.2.1+incompatible	go-module
github.com/cenkalti/backoff/v4	v4.2.1	go-module
github.com/cespare/xxhash/v2	v2.2.0	go-module
github.com/cisco-ie/nx-telemetry-proto	v0.0.0-20230117155933-f64c045c77df	go-module
github.com/clarify/clarify-go	v0.2.4	go-module
github.com/cloudevents/sdk-go/v2	v2.14.0	go-module
github.com/compose-spec/compose-go	v1.15.0	go-module
github.com/coocood/freecache	v1.2.3	go-module
github.com/coreos/go-semver	v0.3.1	go-module
github.com/coreos/go-systemd	v0.0.0-20190719114852-fd7a80b32e1f	go-module
github.com/couchbase/go-couchbase	v0.1.1	go-module
github.com/couchbase/gomemcached	v0.1.3	go-module
github.com/couchbase/goutils	v0.1.0	go-module
github.com/cpuguy83/go-md2man/v2	v2.0.2	go-module
github.com/davecgh/go-spew	v1.1.1	go-module
github.com/denisenkom/go-mssqldb	v0.12.3	go-module
github.com/devigned/tab	v0.1.1	go-module
github.com/dgryski/go-rendezvous	v0.0.0-20200823014737-9f7001d12a5f	go-module

NAME	VERSION	TYPE
github.com/digitalocean/go-libvirt	v0.0.0-20220811165305-15feff002086	go-module
github.com/dimchansky/utfbom	v1.1.1	go-module
github.com/djherbis/times	v1.5.0	go-module
github.com/docker/distribution	v2.8.2+incompatible	go-module
github.com/docker/docker	v23.0.4+incompatible	go-module
github.com/docker/go-connections	v0.4.0	go-module
github.com/docker/go-units	v0.5.0	go-module
github.com/doclambda/protobufquery	v0.0.0-20220727165953-0da287796ee9	go-module
github.com/dvsekhvalnov/jose2go	v1.5.0	go-module
github.com/dynatrace-oss/dynatrace-metric-utils-go	v0.5.0	go-module
github.com/eapache/go-resiliency	v1.3.0	go-module
github.com/eapache/go-xerial-snappy	v0.0.0-20230111030713-bf00bc1b83b6	go-module
github.com/eapache/queue	v1.1.0	go-module
github.com/eclipse/paho.golang	v0.10.0	go-module
github.com/eclipse/paho.mqtt.golang	v1.4.2	go-module
github.com/emicklei/go-restful/v3	v3.10.1	go-module
github.com/fatih/color	v1.15.0	go-module
github.com/form3tech-oss/jwt-go	v3.2.5+incompatible	go-module
github.com/gabriel-vasile/mimetype	v1.4.0	go-module
github.com/go-asn1-ber/asn1-ber	v1.5.4	go-module
github.com/go-ldap/ldap/v3	v3.4.4	go-module
github.com/go-logfmt/logfmt	v0.6.0	go-module
github.com/go-logr/logr	v1.2.4	go-module
github.com/go-openapi/jsonpointer	v0.19.6	go-module
github.com/go-openapi/jsonreference	v0.20.2	go-module
github.com/go-openapi/swag	v0.22.3	go-module
github.com/go-redis/redis/v7	v7.4.1	go-module
github.com/go-redis/redis/v8	v8.11.5	go-module
github.com/go-sql-driver/mysql	v1.7.1	go-module
github.com/go-stack/stack	v1.8.1	go-module
github.com/go-stomp/stomp	v2.1.4+incompatible	go-module
github.com/gobwas/glob	v0.2.3	go-module
github.com/goccy/go-json	v0.10.2	go-module
github.com/gofrs/uuid	v4.2.0+incompatible	go-module
github.com/gofrs/uuid/v5	v5.0.0	go-module
github.com/gogo/protobuf	v1.3.2	go-module
github.com/golang-jwt/jwt	v3.2.1+incompatible	go-module
github.com/golang-jwt/jwt/v4	v4.5.0	go-module

NAME	VERSION	TYPE
github.com/golang-sql/civil	v0.0.0-20190719163853-cb61b32ac6fe	go-module
github.com/golang-sql/sqlexp	v0.1.0	go-module
github.com/golang/geo	v0.0.0-20190916061304-5b978397cfec	go-module
github.com/golang/groupcache	v0.0.0-20210331224755-41bb18bfe9da	go-module
github.com/golang/protobuf	v1.5.3	go-module
github.com/golang/snappy	v0.0.4	go-module
github.com/google/cel-go	v0.14.1-0.20230424164844-d39523c445fc	go-module
github.com/google/flatbuffers	v23.3.3+incompatible	go-module
github.com/google/gnostic	v0.6.9	go-module
github.com/google/gnxi	v0.0.0-20221016143401-2aeceb5a2901	go-module
github.com/google/go-cmp	v0.5.9	go-module
github.com/google/go-github/v32	v32.1.0	go-module
github.com/google/go-querystring	v1.1.0	go-module
github.com/google/gofuzz	v1.2.0	go-module
github.com/google/gopacket	v1.1.19	go-module
github.com/google/s2a-go	v0.1.3	go-module
github.com/google/uuid	v1.3.0	go-module
github.com/googleapis/enterprise-certificate-proxy	v0.2.3	go-module
github.com/googleapis/gax-go/v2	v2.8.0	go-module
github.com/gopcua/opcua	v0.3.7	go-module
github.com/gophercloud/gophercloud	v1.2.0	go-module
github.com/gorilla/mux	v1.8.0	go-module
github.com/gorilla/websocket	v1.5.0	go-module
github.com/gosnmp/gosnmp	v1.35.0	go-module
github.com/grid-x/modbus	v0.0.0-20211113184042-7f2251c342c9	go-module
github.com/grid-x/serial	v0.0.0-20211107191517-583c7356b3aa	go-module
github.com/gwos/tcg/sdk	v0.0.0-20220621192633-df0eac0a1a4c	go-module
github.com/hailocab/go-hostpool	v0.0.0-20160125115350-e80d13ce29ed	go-module

NAME	VERSION	TYPE
github.com/harlow/kinesis-consumer	v0.3.6-0.20211204214318-c2b9f79d7ab6	go-module
github.com/hashicorp/consul/api	v1.20.0	go-module
github.com/hashicorp/errwrap	v1.1.0	go-module
github.com/hashicorp/go-cleanhttp	v0.5.2	go-module
github.com/hashicorp/go-hclog	v1.4.0	go-module
github.com/hashicorp/go-immutable-radix	v1.3.1	go-module
github.com/hashicorp/go-multierror	v1.1.1	go-module
github.com/hashicorp/go-rootcerts	v1.0.2	go-module
github.com/hashicorp/go-uuid	v1.0.3	go-module
github.com/hashicorp/golang-lru	v0.6.0	go-module
github.com/hashicorp/packer-plugin-sdk	v0.3.1	go-module
github.com/hashicorp/serf	v0.10.1	go-module
github.com/huandu/xstrings	v1.3.2	go-module
github.com/imdario/mergo	v0.3.16	go-module
github.com/influxdata/go-syslog/v3	v3.0.0	go-module
github.com/influxdata/influxdb-observability/common	v0.5.0	go-module
github.com/influxdata/influxdb-observability/influx2otel	v0.5.0	go-module
github.com/influxdata/influxdb-observability/otel2influx	v0.5.0	go-module
github.com/influxdata/line-protocol/v2	v2.2.1	go-module
github.com/influxdata/tail	v1.0.1-0.20210707231403-b283181d1fa7	go-module
github.com/influxdata/telegraf	(devel)	go-module
github.com/influxdata/toml	v0.0.0-20190415235208-270119a8ce65	go-module
github.com/influxdata/wlog	v0.0.0-20160411224016-7c63b0a71ef8	go-module
github.com/jackc/chunkreader/v2	v2.0.1	go-module
github.com/jackc/pgconn	v1.14.0	go-module
github.com/jackc/pgio	v1.0.0	go-module
github.com/jackc/pgpassfile	v1.0.0	go-module
github.com/jackc/pgproto3/v2	v2.3.2	go-module
github.com/jackc/pgservicefile	v0.0.0-20221227161230-091c0ba34f0a	go-module
github.com/jackc/pgtype	v1.14.0	go-module
github.com/jackc/pgx/v4	v4.18.1	go-module
github.com/jackc/puddle	v1.3.0	go-module
github.com/jaegertracing/jaeger	v1.38.0	go-module

NAME	VERSION	TYPE
github.com/james4k/rcon	v0.0.0-20120923215419-8fbb8268b60a	go-module
github.com/jcmturner/aescts/v2	v2.0.0	go-module
github.com/jcmturner/dnsutils/v2	v2.0.0	go-module
github.com/jcmturner/gofork	v1.7.6	go-module
github.com/jcmturner/gokrb5/v8	v8.4.3	go-module
github.com/jcmturner/rpc/v2	v2.0.3	go-module
github.com/jeremywohl/flatten/v2	v2.0.0-20211013061545-07e4a09fb8e4	go-module
github.com/jhump/protoreflect	v1.15.1	go-module
github.com/jmespath/go-jmespath	v0.4.0	go-module
github.com/josharian/intern	v1.0.0	go-module
github.com/jpillora/backoff	v1.0.0	go-module
github.com/json-iterator/go	v1.1.12	go-module
github.com/karrick/godirwalk	v1.16.2	go-module
github.com/kballard/go-shellquote	v0.0.0-20180428030007-95032a82bc51	go-module
github.com/klauspost/compress	v1.16.5	go-module
github.com/klauspost/cpuid/v2	v2.2.4	go-module
github.com/klauspost/pgzip	v1.2.6	go-module
github.com/kolo/xmlrpc	v0.0.0-20220921171641-a4b6fa1dd06b	go-module
github.com/kylelemons/godebug	v1.1.0	go-module
github.com/leodido/ragel-machinery	v0.0.0-20181214104525-299bdde78165	go-module
github.com/linkedin/goavro/v2	v2.12.0	go-module
github.com/logzio/azure-monitor-metrics-receiver	v1.0.0	go-module
github.com/mailru/easyjson	v0.7.7	go-module
github.com/mattn/go-colorable	v0.1.13	go-module
github.com/mattn/go-ieproxy	v0.0.1	go-module
github.com/mattn/go-isatty	v0.0.19	go-module
github.com/matttproud/golang_protobuf_extensions	v1.0.4	go-module
github.com/mdlayher/apcupsd	v0.0.0-20220319200143-473c7b5f3c6a	go-module
github.com/microsoft/ApplicationInsights-Go	v0.4.4	go-module
github.com/miekg/dns	v1.1.51	go-module
github.com/minio/highwayhash	v1.0.2	go-module
github.com/mitchellh/copystructure	v1.2.0	go-module
github.com/mitchellh/go-homedir	v1.1.0	go-module
github.com/mitchellh/mapstructure	v1.5.0	go-module

NAME	VERSION	TYPE
github.com/mitchellh/reflectwalk	v1.0.2	go-module
github.com/modern-go/concurrent	v0.0.0-20180306012644-bacd9c7ef1dd	go-module
github.com/modern-go/reflect2	v1.0.2	go-module
github.com/montanaflynn/stats	v0.6.6	go-module
github.com/mtibben/percent	v0.2.1	go-module
github.com/multiplay/go-ts3	v1.1.0	go-module
github.com/munnerz/goautoneg	v0.0.0-20191010083416-a7dc8b61c822	go-module
github.com/naoina/go-stringutil	v0.1.0	go-module
github.com/nats-io/jwt/v2	v2.3.0	go-module
github.com/nats-io/nats-server/v2	v2.9.9	go-module
github.com/nats-io/nats.go	v1.27.0	go-module
github.com/nats-io/nkeys	v0.4.4	go-module
github.com/nats-io/nuid	v1.0.1	go-module
github.com/netsampler/goflow2	v1.3.3	go-module
github.com/newrelic/newrelic-telemetry-sdk-go	v0.8.1	go-module
github.com/nsqio/go-nsq	v1.1.0	go-module
github.com/olivere/elastic	v6.2.37+incompatible	go-module
github.com/open-telemetry/opentelemetry-collector-contrib/pkg/pdatautil	v0.79.0	go-module
github.com/openconfig/gnmi	v0.9.1	go-module
github.com/opencontainers/go-digest	v1.0.0	go-module
github.com/opencontainers/image-spec	v1.1.0-rc2	go-module
github.com/opensearch-project/opensearch-go/v2	v2.2.0	go-module
github.com/opentracing/opentracing-go	v1.2.1-0.20220228012449-10b1cf09e00b	go-module
github.com/p4lang/p4runtime	v1.3.0	go-module
github.com/pborman/ansi	v1.0.0	go-module
github.com/philhofer/fwd	v1.1.2	go-module
github.com/pierrec/lz4/v4	v4.1.17	go-module
github.com/pion/dtls/v2	v2.2.7	go-module
github.com/pion/logging	v0.2.2	go-module
github.com/pion/transport/v2	v2.2.1	go-module
github.com/pkg/browser	v0.0.0-20210911075715-681adbf594b8	go-module
github.com/pkg/errors	v0.9.1	go-module
github.com/pmezard/go-difflib	v1.0.0	go-module
github.com/prometheus-community/pro-bing	v0.2.0	go-module
github.com/prometheus/client_golang	v1.15.1	go-module
github.com/prometheus/client_model	v0.4.0	go-module
github.com/prometheus/common	v0.44.0	go-module

NAME	VERSION	TYPE
github.com/prometheus/procfs	v0.9.0	go-module
github.com/prometheus/prometheus	v0.42.0	go-module
github.com/rabbitmq/amqp091-go	v1.8.1	go-module
github.com/rcrowley/go-metrics	v0.0.0-20201227073835-cf1acfcdf475	go-module
github.com/riemann/riemann-go-client	v0.5.1-0.20211206220514-f58f10cdce16	go-module
github.com/robbiet480/go.nut	v0.0.0-20220219091450-bd8f121e1fa1	go-module
github.com/russross/blackfriday/v2	v2.1.0	go-module
github.com/samuel/go-zookeeper	v0.0.0-20200724154423-2164a8ac840e	go-module
github.com/shirou/gopsutil/v3	v3.23.5	go-module
github.com/showwin/speedtest-go	v1.6.2	go-module
github.com/signalfx/com_signalfx_metrics_protobuf	v0.0.3	go-module
github.com/signalfx/gohistogram	v0.0.0-20160107210732-1ccfd2ff5083	go-module
github.com/signalfx/golib/v3	v3.3.50	go-module
github.com/signalfx/sapm-proto	v0.12.0	go-module
github.com/sirupsen/logrus	v1.9.0	go-module
github.com/sleepinggenius2/gosmi	v0.4.4	go-module
github.com/snowflakedb/gosnowflake	v1.6.13	go-module
github.com/spf13/pflag	v1.0.5	go-module
github.com/stoewer/go-strcase	v1.2.0	go-module
github.com/stretchr/objx	v0.5.0	go-module
github.com/stretchr/testify	v1.8.4	go-module
github.com/thomasklein94/packer-plugin-libvirt	v0.3.4	go-module
github.com/tidwall/gjson	v1.14.4	go-module
github.com/tidwall/match	v1.1.1	go-module
github.com/tidwall/pretty	v1.2.0	go-module
github.com/tinylib/msgp	v1.1.8	go-module
github.com/tklauser/go-sysconf	v0.3.11	go-module
github.com/uber/jaeger-client-go	v2.30.0+incompatible	go-module
github.com/uber/jaeger-lib	v2.4.1+incompatible	go-module
github.com/urfave/cli/v2	v2.25.5	go-module
github.com/vapourismo/knx-go	v0.0.0-20220829185957-fb5458a5389d	go-module
github.com/vjeantet/grok	v1.0.1	go-module

NAME	VERSION	TYPE
github.com/vmware/govmomi	v0.28.1-0.20220921224932-b4b508abf208	go-module
github.com/wavefronthq/wavefront-sdk-go	v0.13.0	go-module
github.com/wvanbergen/kafka	v0.0.0-20171203153745-e2edea948ddf	go-module
github.com/wvanbergen/kazoo-go	v0.0.0-20180202103751-f72d8611297a	go-module
github.com/x448/float16	v0.8.4	go-module
github.com/xdg-go/pbkdf2	v1.0.0	go-module
github.com/xdg-go/scram	v1.1.2	go-module
github.com/xdg-go/stringprep	v1.0.4	go-module
github.com/xdg/scram	v1.0.5	go-module
github.com/xdg/stringprep	v1.0.3	go-module
github.com/xrash/smetrics	v0.0.0-20201216005158-039620a65673	go-module
github.com/youmark/pkcs8	v0.0.0-20201027041543-1326539a0a0a	go-module
github.com/yuin/gopher-lua	v0.0.0-20200816102855-ee81675732da	go-module
github.com/zeebo/xxh3	v1.0.2	go-module
go.mongodb.org/mongo-driver	v1.11.2	go-module
go.opencensus.io	v0.24.0	go-module
go.opentelemetry.io/collector/consumer	v0.79.0	go-module
go.opentelemetry.io/collector/pdata	v1.0.0-rcv0012	go-module
go.opentelemetry.io/collector/semconv	v0.79.0	go-module
go.starlark.net	v0.0.0-20220328144851-d1966c6b9fcd	go-module
go.uber.org/atomic	v1.11.0	go-module
go.uber.org/multierr	v1.11.0	go-module
go.uber.org/zap	v1.24.0	go-module
golang.org/x/crypto	v0.9.0	go-module
golang.org/x/exp	v0.0.0-20230522175609-2e198f4a06a1	go-module
golang.org/x/net	v0.10.0	go-module
golang.org/x/oauth2	v0.8.0	go-module
golang.org/x/sync	v0.3.0	go-module
golang.org/x/sys	v0.9.0	go-module
golang.org/x/term	v0.9.0	go-module
golang.org/x/text	v0.9.0	go-module

NAME	VERSION	TYPE
golang.org/x/time	v0.3.0	go-module
golang.org/x/xerrors	v0.0.0-20220907171357-04be3eba64a2	go-module
golang.zx2c4.com/wireguard/wgctrl	v0.0.0-20211230205640-daad0b7ba671	go-module
gonum.org/v1/gonum	v0.13.0	go-module
google.golang.org/api	v0.121.0	go-module
google.golang.org/appengine	v1.6.7	go-module
google.golang.org/genproto	v0.0.0-20230530153820-e85fd2cbaebc	go-module
google.golang.org/genproto/googleapis/api	v0.0.0-20230530153820-e85fd2cbaebc	go-module
google.golang.org/genproto/googleapis/rpc	v0.0.0-20230530153820-e85fd2cbaebc	go-module
google.golang.org/grpc	v1.55.0	go-module
google.golang.org/protobuf	v1.30.0	go-module
google/apiclient-services	v0.113	php-composer
google/auth	v1.5.2	php-composer
gopkg.in/fatih/pool.v2	v2.0.0	go-module
gopkg.in/fsnotify.v1	v1.4.7	go-module
gopkg.in/gorethink/gorethink.v3	v3.0.5	go-module
gopkg.in/inf.v0	v0.9.1	go-module
gopkg.in/ini.v1	v1.67.0	go-module
gopkg.in/olivere/elastic.v5	v5.0.86	go-module
gopkg.in/tomb.v1	v1.0.0-20141024135613-dd632973f1e7	go-module
gopkg.in/tomb.v2	v2.0.0-20161208151619-d5d1b5820637	go-module
gopkg.in/yaml.v2	v2.4.0	go-module
gopkg.in/yaml.v3	v3.0.1	go-module
guzzlehttp/guzzle	6.3.3	php-composer
guzzlehttp/promises	v1.3.1	php-composer
guzzlehttp/psr7	1.6.1	php-composer
h11	0.14.0	python
h2	4.0.0	python

NAME	VERSION	TYPE
hpack	4.0.0	python
httpcore	0.17.3	python
httpx	0.24.1	python
hyperframe	6.0.0	python
idna	3.4	python
k8s.io/api	v0.27.2	go-module
k8s.io/apimachinery	v0.27.2	go-module
k8s.io/client-go	v0.27.2	go-module
k8s.io/klog/v2	v2.90.1	go-module
k8s.io/kube-openapi	v0.0.0-20230501164219-8b0f38b5fd1f	go-module
k8s.io/utils	v0.0.0-20230308161112-d77c459e9343	go-module
layeh.com/radius	v0.0.0-20221205141417-e7fbddd11d68	go-module
libphp	8.2.8	binary
monolog/monolog	2.0.0	php-composer
netaddr	0.8.0	python
numexpr	2.8.4	python
numpy	1.25.0	python
outcome	1.2.0	python
pandas	2.0.3	python
php-cli	8.2.8	binary
php-fpm	8.2.8	binary
phpseclib/phpseclib	2.0.21	php-composer
psr/cache	1.0.1	php-composer
psr/http-message	1.0.1	php-composer
psr/log	1.1.0	php-composer
pyOpenSSL	21.0.0	python
pycparser	2.21	python
pylsqpack	0.3.17	python
python	3.9.17	binary
python-dateutil	2.8.2	python
pytz	2023.3	python
ralouphie/getallheaders	3.0.3	php-composer
requests	2.31.0	python

NAME	VERSION	TYPE
setuptools	63.1.0	python
sigs.k8s.io/json	v0.0.0-20221116044647-bc3834ca7abd	go-module
sigs.k8s.io/structured-merge-diff/v4	v4.2.3	go-module
sigs.k8s.io/yaml	v1.3.0	go-module
six	1.16.0	python
sniffio	1.3.0	python
sortedcontainers	2.4.0	python
sqlite3	0.0.0	python
trio	0.22.2	python
tzdata	2023.3	python
ujson	5.8.0	python
urllib3	1.26.16	python
vici	5.9.11	python

About Mercury

Mercury Information Security Services is a leading provider of information security services, advice and consulting in Australia.

Founded in 2015, Mercury provides cyber security assessment, assurance and research services.

For more information, visit their website or get in contact:

Website:	www.mercuryiss.com.au
Twitter:	twitter.com/mercuryiss
Email:	info@mercuryiss.com.au