# Palo Alto Initial Script

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClaCCAS

To create a new security policy from the CLI: (Do not type < or >)

> configure

# set rulebase security rules <**InboundBlock**> from <**External**> to <**Any**> action <**deny**>

# set rulebase security rules <**Outbound**> from <**Any**> to <**External**> application <**dns**>   
 service <**application-default**> action <**allow**>

# set rulebase security rules <**Outbound**> from <**Any**> to <**External**> service <service-**http**>   
 action <**allow**>

# set rulebase security rules <**Outbound**> from <**Any**> to <**External**> service <service-**https**>   
 action <**allow**>

# set rulebase security rules <**Outbound**> from <**Any**> to <**External**> service <service-**ntp**>   
 action <**allow**>

# move rulebase security rules <**InboundBlock**> top

# move rulebase security rules <**Outbound**> top

# exit

# Palo Alto Box Steps:

**COMMIT / Save settings after every step**

No access on Windows 10 Box. 172.20.242.150

admin changeme123 WakeParkHilt333

## FIRST LOGIN:

Device > Administrators

Table

Description automatically generated with medium confidence

REMOVE any that aren’t admin

Click admin to change password

Graphical user interface, text, application, website

Description automatically generated

(save current named state, export named state)

**Delete any existing named saves**

**Move/delete any existing downloaded saves as well**

Export XML current config state to desktop (name="badconf\_23.xml")

## Configure Interface

Device > Setup > interfaces

Graphical user interface, application, website

Description automatically generated

Graphical user interface, text, application

Description automatically generated

MUST DISABLE: SSH – telnet – ping - SNMP

Graphical user interface, application

Description automatically generated

Configure Devices

Objects > Addresses

2012 IP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Debian IP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fedora IP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Splunk IP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CentOS IP:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Objects > Services

Splunk Ports Ports: **8000, 8008?, 8089** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table

Description automatically generated

Configure Networking Rules

Policies > Security

Name Source Destination Application Service

PUBLIC2USER ZONE: Public ZONE: User any any

PUBLIC2EXTERNAL ZONE: Public ZONE: External any any

PUBLIC2INTERNAL ZONE: Public ZONE: Internal any any

INTERNAL2PUBLIC ZONE: Internal ZONE: Public any any

DNS IN\* any 2012\*, Debian\* dns application-default

DNS OUT\* any ZONE: External dns application-default

MAIL IN\* any Fedora\* pop3, smtp application-default

WEB OUT\* any ZONE: External any service-http, -https

SPLUNK IN\* any Splunk\* any Splunk Ports\*

ECOMM IN\* any CentOS\* any service-http, -https

\*\*\* DOUBLE CHECK EVERYTHING \*\*\*

\*\*\* COMMIT AND REBOOT AFTER EVERYTHING IS GOOD \*\*\*

**Drop Traffic on other connections.**

Graphical user interface, application

Description automatically generated **Source Destination**

Table

Description automatically generated with medium confidence

Hidden Garbage to Remove

**Network > Zones**

Graphical user interface

Description automatically generated

REMOVE TRUSTED

**Network > DNS Proxy**

Graphical user interface, text, application

Description automatically generated REMOVE MARK

Graphical user interface

Description automatically generated

**Network > GlobalProtect > MDM**

Graphical user interface, text, application, chat or text message

Description automatically generated REMOVE travis

Background pattern

Description automatically generated

**Objects > Application Filters**

Timeline

Description automatically generated with low confidence

REMOVE ALL FILTERS

**Objects > GlobalProtect > HIP Objects**

Graphical user interface, text, application, chat or text message

Description automatically generated REMOVE brian

Graphical user interface

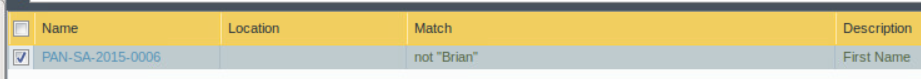
Description automatically generated with low confidenceA picture containing text, orange, screenshot

Description automatically generated

**Objects > GlobalProtect > HIP Profiles**

Graphical user interface, text, application, chat or text message

Description automatically generated REMOVE PAN-SA





**Objects > Custom Objects > Data Patterns**

Graphical user interface, text, application, chat or text message

Description automatically generated REMOVE backup

A picture containing chart

Description automatically generated

**Objects > Custom Objects > Vulnerability**

Graphical user interface, text, application, chat or text message

Description automatically generated Remove Bruteforce



Graphical user interface

Description automatically generated

**Objects > Schedules**

**check for schedules, disable?**

**Possibly check for updates (Devices > Software)**

## OPTIONAL

**Setting an NTP server:**

Devices > Services

Graphical user interface, application

Description automatically generated

**Viewing Logs:**

Select Monitor®Logs®Traffic to view the Traffic logs.

**Configure QOS:**

Select Policies®QoS and Add a new policy rule.

General tab, Name policy

Specify traffic to receive QoS treatment based on Source, Destination, Application, Service/URL Category,

and DSCP/ToS (Unlikely to need this)

For example, select the Application, click Add, and select web-browsing to apply QoS to web browsing traffic.

(Query all traffic for every service)

Table

Description automatically generated

## POLICY NOTES

Policies > Security

+ to add:

Under Application:

Graphical user interface, text, application

Description automatically generated

Setting HTTP:

Graphical user interface

Description automatically generated with medium confidence

config can clear admin accts, disable services, do objects > addresses

suspect we'll need to leave SSH alone until upload confirmed good, then disable manually

does splunk need inbound/outbound/both? TCP/UDP/both?

policy > security: intrazones?

export