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:

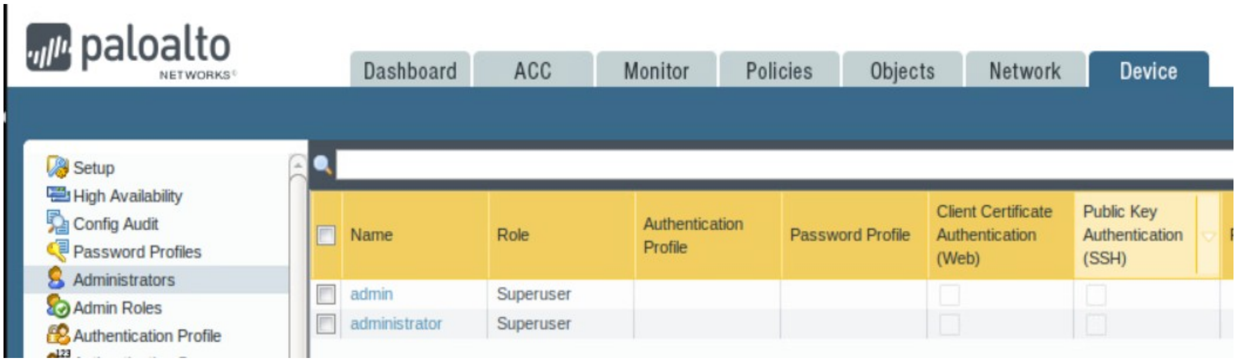
COMMIT / Save settings after every step

No access on Windows 10 Box. 172.20.242.150

admin changeme123 WakeParkHilt333

FIRST LOGIN:

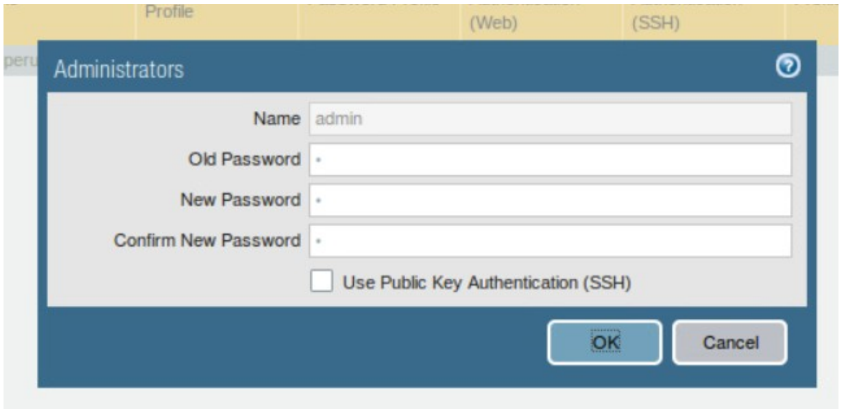
Device > Administrators



☐	Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)
☐	admin	Superuser			☐	☐
☐	administrator	Superuser			☐	☐

REMOVE any that aren't admin

Click admin to change password



Name: admin
Old Password: •
New Password: •
Confirm New Password: •
☐ Use Public Key Authentication (SSH)

(save current named state, export named state)

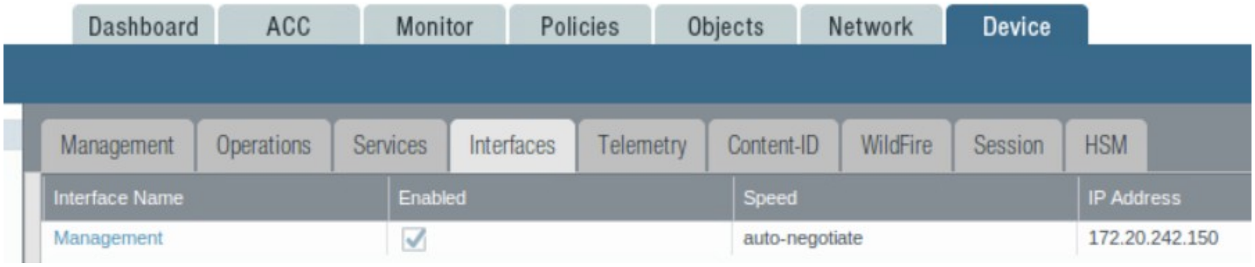
Delete any existing named saves

Move/delete any existing downloaded saves as well

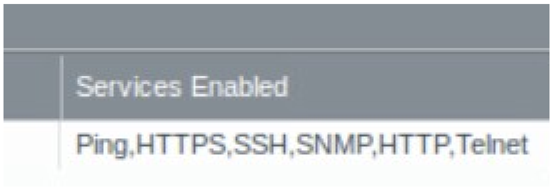
Export XML current config state to desktop (name="badconf_23.xml")

Configure Interface

Device > Setup > interfaces

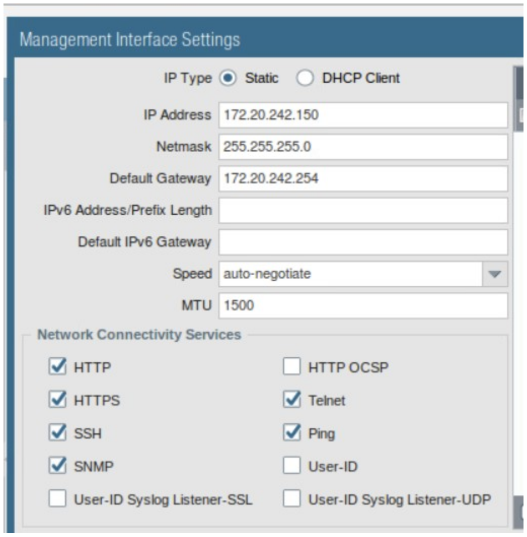


Interface Name	Enabled	Speed	IP Address
Management	☑	auto-negotiate	172.20.242.150



Services Enabled
Ping,HTTPS,SSH,SNMP,HTTP,Telnet

MUST DISABLE: SSH – telnet – ping – SNMP



Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address 172.20.242.150

Netmask 255.255.255.0

Default Gateway 172.20.242.254

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed auto-negotiate

MTU 1500

Network Connectivity Services

☑ HTTP	□ HTTP OCSP
☑ HTTPS	☑ Telnet
☑ SSH	☑ Ping
☑ SNMP	□ User-ID
□ User-ID Syslog Listener-SSL	□ User-ID Syslog Listener-UDP

Configure Devices

Objects > Addresses

2012
IP:____

Debian

IP:____

Fedora

IP:____

Splunk

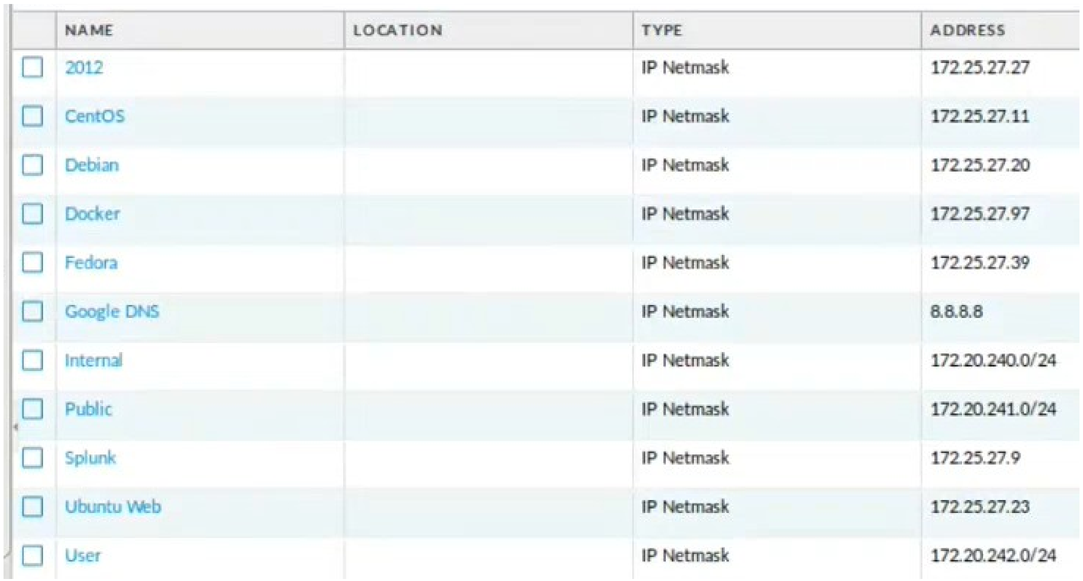
IP:____

CentOS

IP:____

Objects > Services

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



	NAME	LOCATION	TYPE	ADDRESS
□	2012		IP Netmask	172.25.27.27
□	CentOS		IP Netmask	172.25.27.11
□	Debian		IP Netmask	172.25.27.20
□	Docker		IP Netmask	172.25.27.97
□	Fedora		IP Netmask	172.25.27.39
□	Google DNS		IP Netmask	8.8.8.8
□	Internal		IP Netmask	172.20.240.0/24
□	Public		IP Netmask	172.20.241.0/24
□	Splunk		IP Netmask	172.25.27.9
□	Ubuntu Web		IP Netmask	172.25.27.23
□	User		IP Netmask	172.20.242.0/24

Configure Networking Rules

Policies > Security

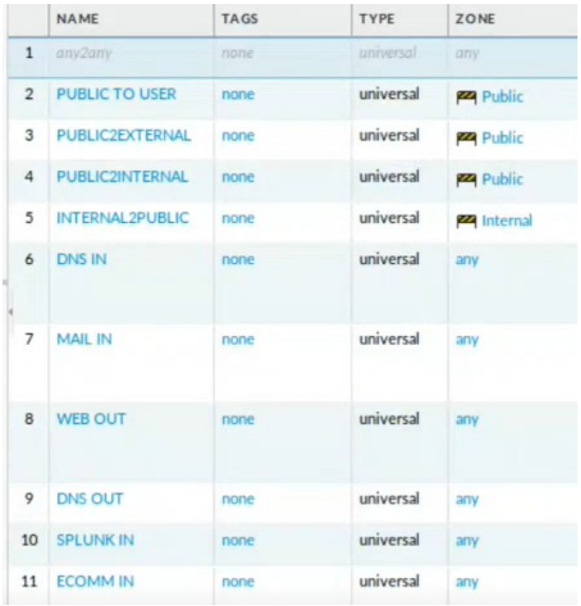
Name	Source	Destination	Application	Service
PUBLIC2USER	ZONE: Public	ZONE: User	any	any
PUBLIC2EXTERNAL	ZONE: Public	ZONE: External	any	any
PUBLIC2INTERNAL	ZONE: Public	ZONE: Internal	any	any
INTERNAL2PUBLIC	ZONE: Internal	ZONE: Public	any	any
DNS IN*	any	2012*, Debian*	dns	application-default
DNS OUT*	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 ***

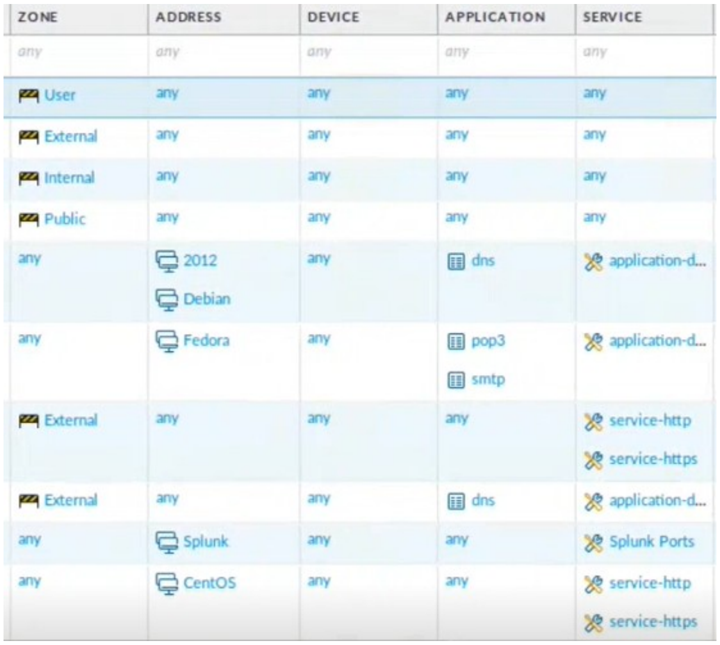
*** COMMIT AND REBOOT AFTER EVERYTHING IS GOOD ***

Drop Traffic on other connections.

Source Destination



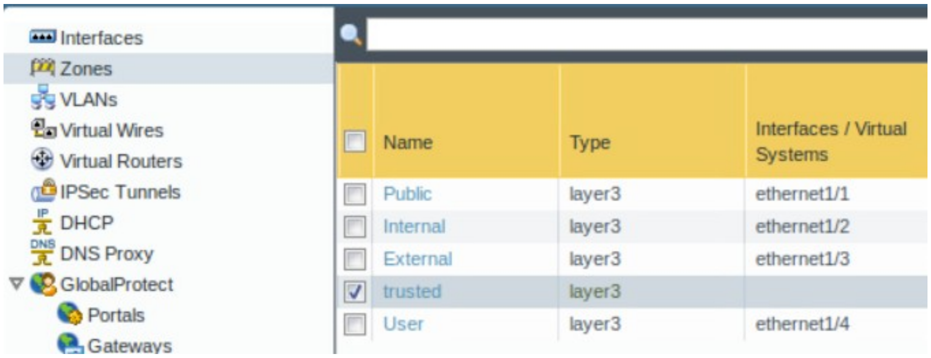
	NAME	TAGS	TYPE	ZONE
1	any2any	none	universal	any
2	PUBLIC TO USER	none	universal	Public
3	PUBLIC2EXTERNAL	none	universal	Public
4	PUBLIC2INTERNAL	none	universal	Public
5	INTERNAL2PUBLIC	none	universal	Internal
6	DNS IN	none	universal	any
7	MAIL IN	none	universal	any
8	WEB OUT	none	universal	any
9	DNS OUT	none	universal	any
10	SPLUNK IN	none	universal	any
11	ECOMM IN	none	universal	any



ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
any	any	any	any	any
User	any	any	any	any
External	any	any	any	any
Internal	any	any	any	any
Public	any	any	any	any
any	2012 Debian	any	dns	application-d...
any	Fedora	any	pop3 smtp	application-d...
External	any	any	any	service-http service-https
External	any	any	dns	application-d...
any	Splunk	any	any	Splunk Ports
any	CentOS	any	any	service-http service-https

Hidden Garbage to Remove

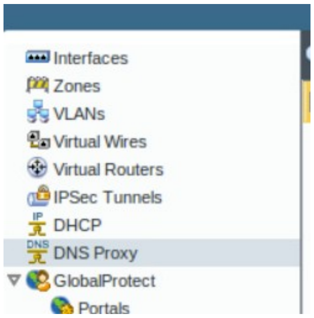
Network > Zones



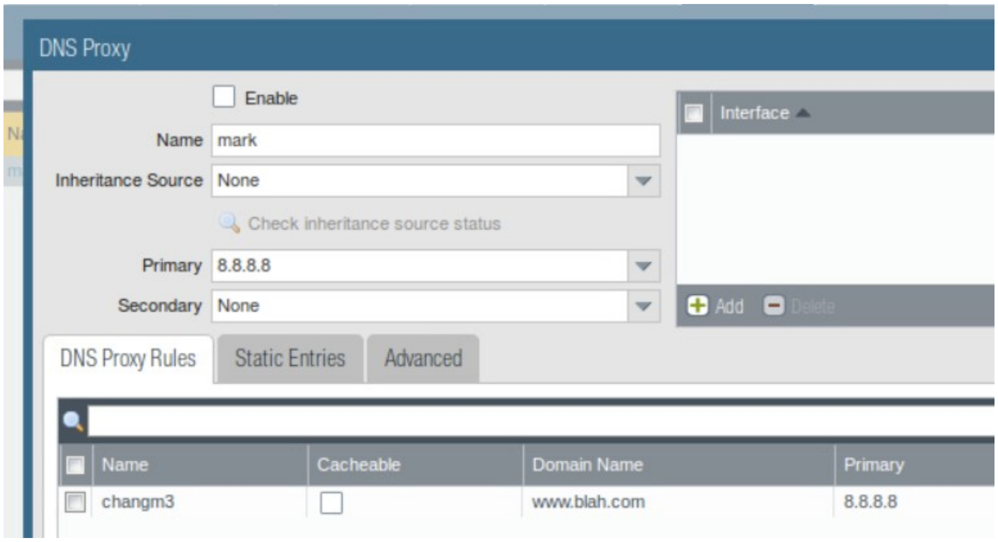
☐	Name	Type	Interfaces / Virtual Systems
☐	Public	layer3	ethernet1/1
☐	Internal	layer3	ethernet1/2
☐	External	layer3	ethernet1/3
☑	trusted	layer3	
☐	User	layer3	ethernet1/4

REMOVE TRUSTED

Network > DNS Proxy



REMOVE MARK



DNS Proxy

□ Enable

Name: mark

Inheritance Source: None

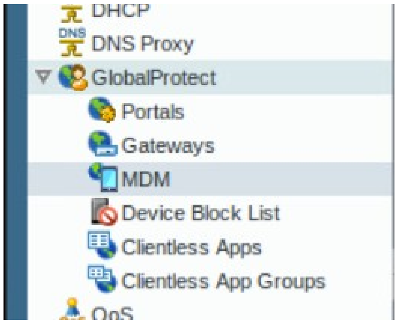
Check inheritance source status

Primary: 8.8.8.8

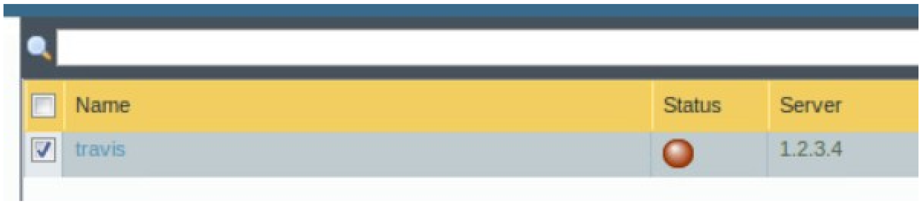
Secondary: None

□	Name	Cacheable	Domain Name	Primary
□	changm3	□	www.blah.com	8.8.8.8

Network > GlobalProtect > MDM

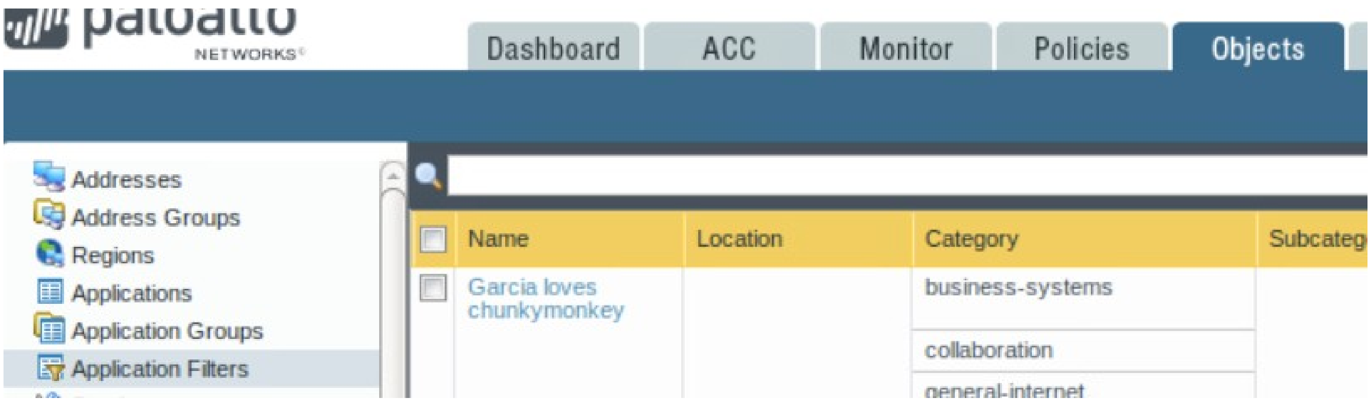


REMOVE travis



□	Name	Status	Server
☑	travis	●	1.2.3.4

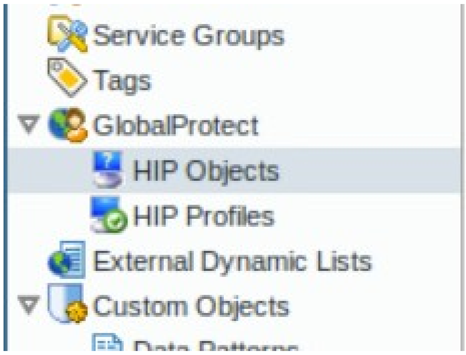
Objects > Application Filters



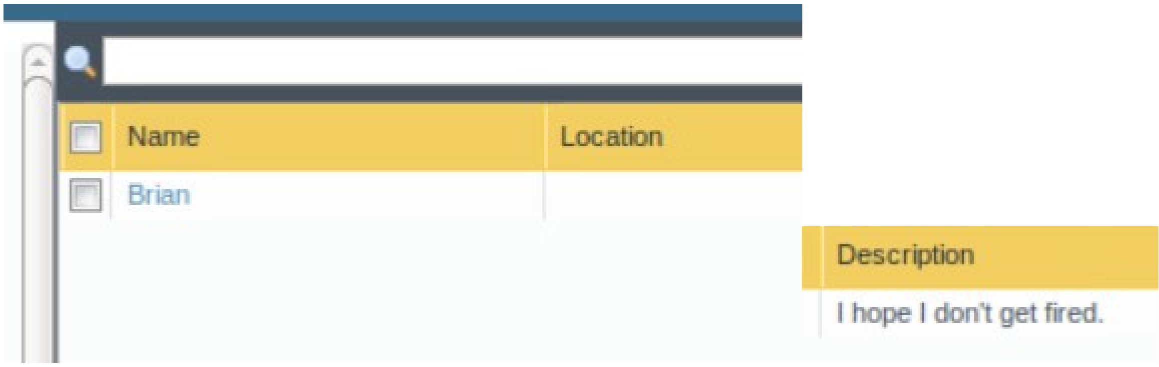
☐	Name	Location	Category	Subcateg
☐	Garcia loves chunkymonkey		business-systems collaboration general-internet	

REMOVE ALL FILTERS

Objects > GlobalProtect > HIP Objects

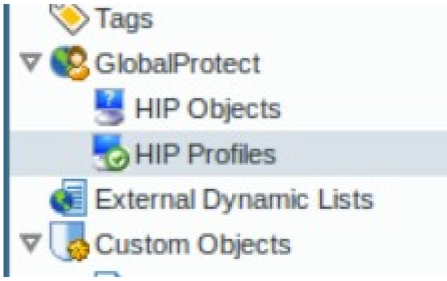


REMOVE brian

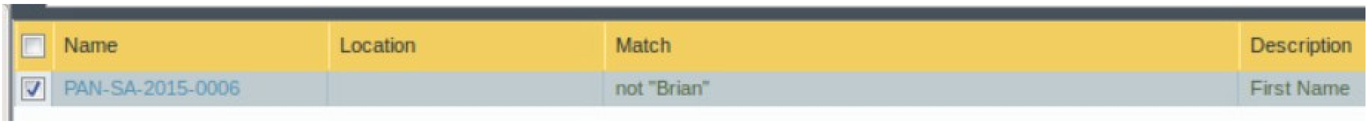


☐	Name	Location	Description
☐	Brian		I hope I don't get fired.

Objects > GlobalProtect > HIP Profiles



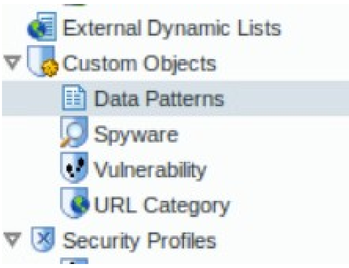
REMOVE PAN-SA



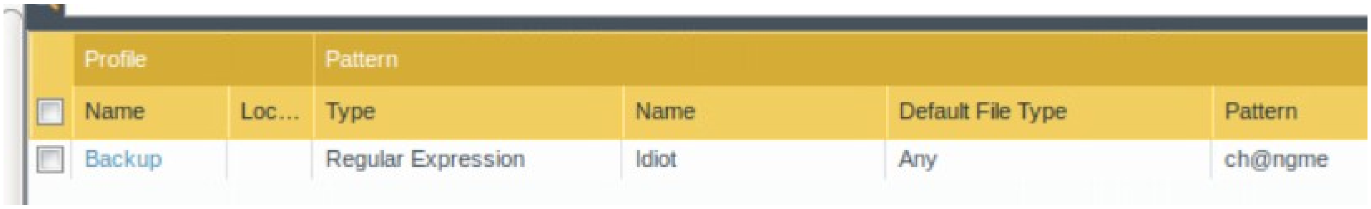
□	Name	Location	Match	Description
☑	PAN-SA-2015-0006		not "Brian"	First Name

PAN-SA-2015-0006

Objects > Custom Objects > Data Patterns

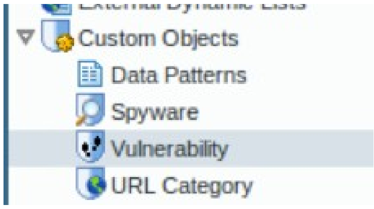


REMOVE backup

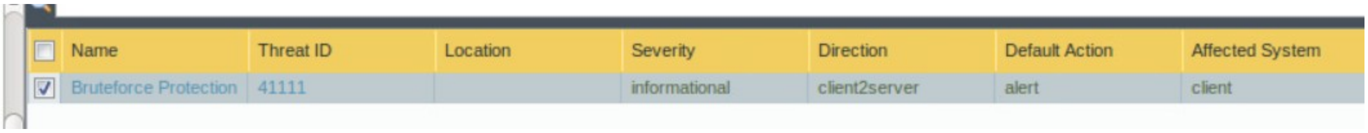


	Profile		Pattern			
□	Name	Loc…	Type	Name	Default File Type	Pattern
□	Backup		Regular Expression	Idiot	Any	ch@ngme

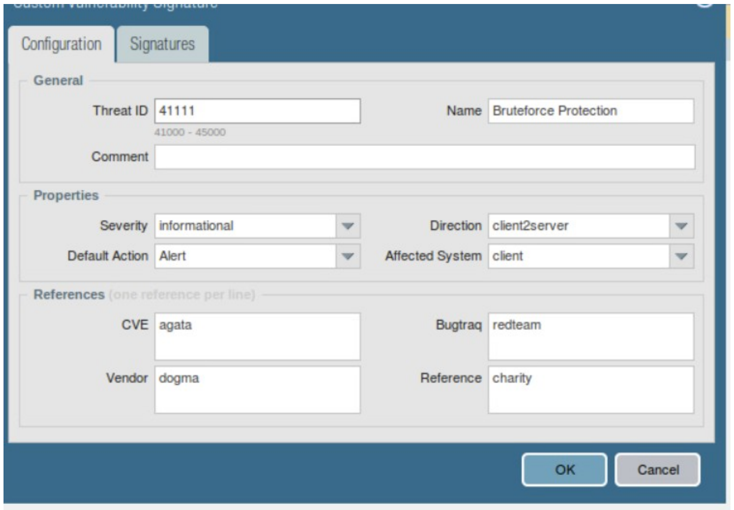
Objects > Custom Objects > Vulnerability



Remove Bruteforce



□	Name	Threat ID	Location	Severity	Direction	Default Action	Affected System
☑	Bruteforce Protection	41111		informational	client2server	alert	client



General

Threat ID: 41111 (41000 - 45000)

Name: Bruteforce Protection

Comment:

Properties

Severity: informational

Direction: client2server

Default Action: Alert

Affected System: client

References (one reference per line)

CVE: agata

Bugtraq: redteam

Vendor: dogma

Reference: charity

Objects > Schedules

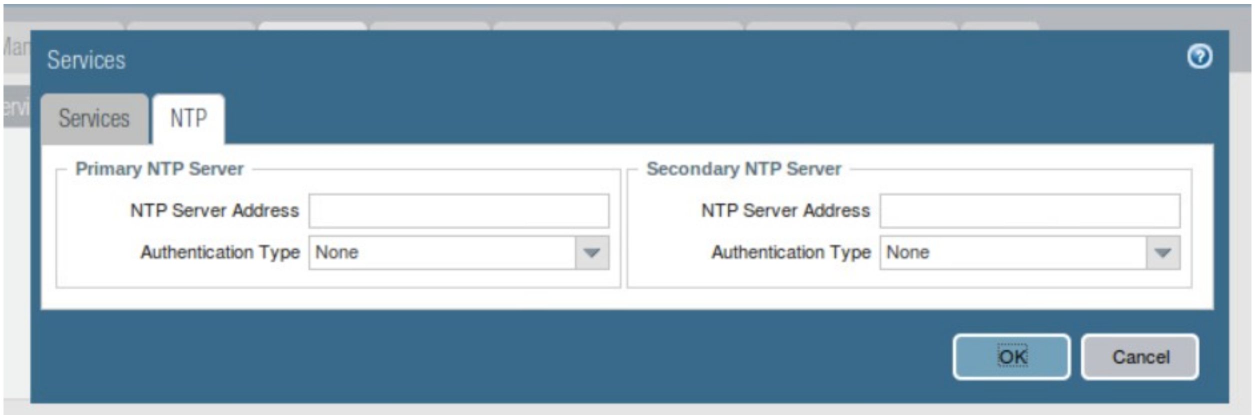
check for schedules, disable?

Possibly check for updates (Devices > Software)

OPTIONAL

Setting an NTP server:

Devices > Services



Primary NTP Server

NTP Server Address:

Authentication Type: None

Secondary NTP Server

NTP Server Address:

Authentication Type: None

Viewing Logs:

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

Configure QOS:

Select Policies®QoS and Add a new policy rule.

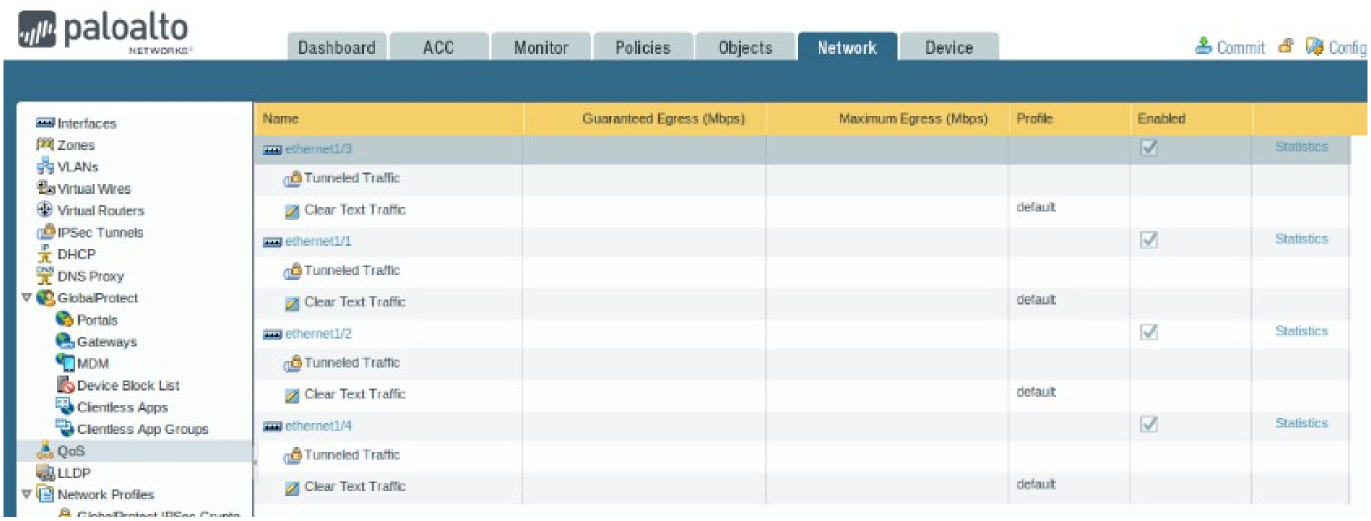
General tab, Name policy

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)



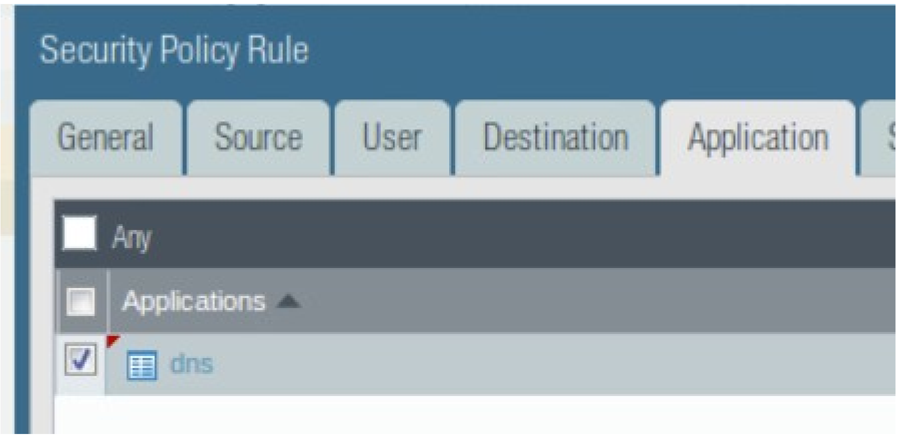
Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/3				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			default		
ethernet1/1				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			default		
ethernet1/2				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			default		
ethernet1/4				✓	Statistics
Tunneled Traffic					
Clear Text Traffic			default		

POLICY NOTES

Policies > Security

+ to add:

Under Application:

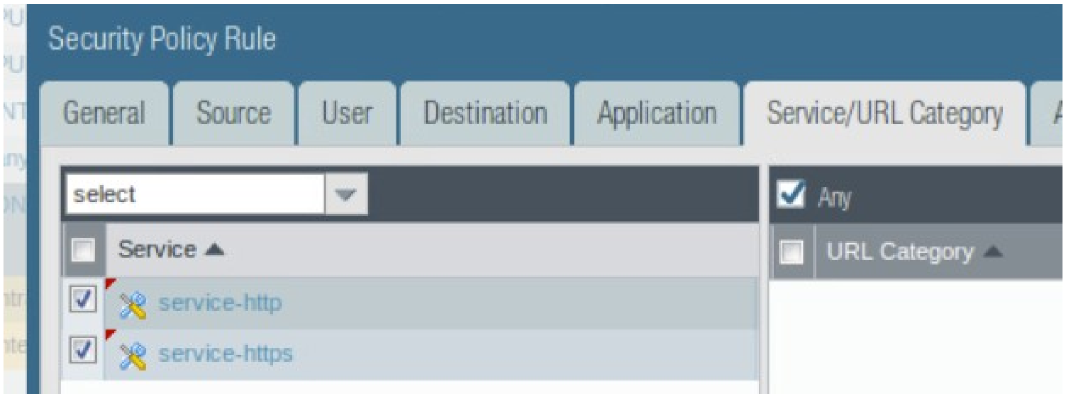


□ Any

□ Applications ▲

☑ dns

Setting HTTP:



☐ Service ▲

☑ service-http

☑ service-https

☑ Any

☐ URL Category ▲

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