Palo Alto PA-220 URL Filtering Lab

Andrew Pai

Period 5 Cybersecurity

Purpose:

The purpose of this lab was to set up URL filtering on our Palo Alto PA-220 firewall. After having reset and configured the PA-220 for a SOHO network, this next step ensures that our firewall can filter and block various web traffics based on the URL. This will help protect our network and clients from malicious or harmful web threats, even if they're unknown.

Background Information:

This lab focuses on implementing URL filtering for our SOHO network that we set up in our last lab. URL filtering is essentially a method of web protection that can help network administrators prevent their network hosts from performing malicious activity or exposing the network to malware, either purposefully or accidentally. When done correctly, URL filtering can be as specialized as allowing network hosts onto certain websites but preventing actions that may lead to a breach of network security, such as downloading files or entering personal and corporate information into websites. However, the goal for this lab is much broader than that and will focus on preventing users from accessing specific categories of websites.

The form of URL filtering that this lab will focus on is restricting access to certain content groups and websites on the Internet based on the URL. This will be done through utilizing various preset categories that Palo Alto has set up, such as groups like "abused-drugs," "adult," "malware," "nudity," and "weapons." By creating a URL filtering profile on the Palo Alto PA-220, network administrators will be able to stop all URL traffic from websites that fall under the categories they choose. This is useful in helping prevent network hosts from accessing sites that may contain any malware or simply preventing them from accessing sites detrimental to their work or education, a tool crucial to small school labs like ours. However, by setting up an override, network administrators will still be able to access these sites themselves if they ever need to.

In order to set up URL filtering through the Palo Alto PA-220 GUI, we should first understand how URL filtering works. As mentioned before, Palo Alto has predefined URL filtering categories, which plays into how the PA-220 filters URLs. The first step of URL filtering is for the PA-220 to inspect web traffic from when users try to access websites. The firewall will take the URL or the domain name, and using that, it'll look through the Palo Alto database of

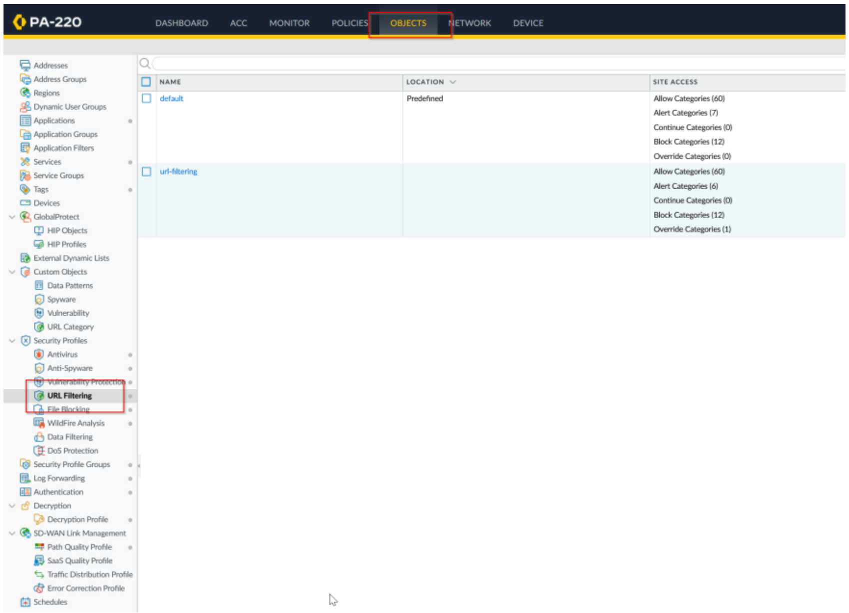
URLs, using the categorizations there to determine whether or not to filter the traffic.

However, for HTTPS sites that have encryption and don't allow the firewall to look at the URL or domain name, the PA-220 will use SSL decryption to gain access to the website information. It does this by using Man in the Middle Decryption, where it establishes a connection with the client to intercept SSL handshakes, decrypting the data to inspect it, and re-encrypting the data when it sends it back out. This then allows the firewall to do the same thing it does with HTTP sites, comparing the URL to the Palo Alto database of categories and carrying out proper filtering. One important thing to note about setting up HTTPS filtering is that the SSL decryption requires a certificate for the firewall to be able to establish a connection with clients from the web.

Overall, this lab is designed to give a comprehensive overview of how to set up both HTTP and HTTPS URL filtering on a Palo Alto PA-220. Not only does this lab familiarize the users with setting up URL filtering on the PA-220 GUI, it gives an understanding of what's actually happening to the traffic passed in and out of the firewall.

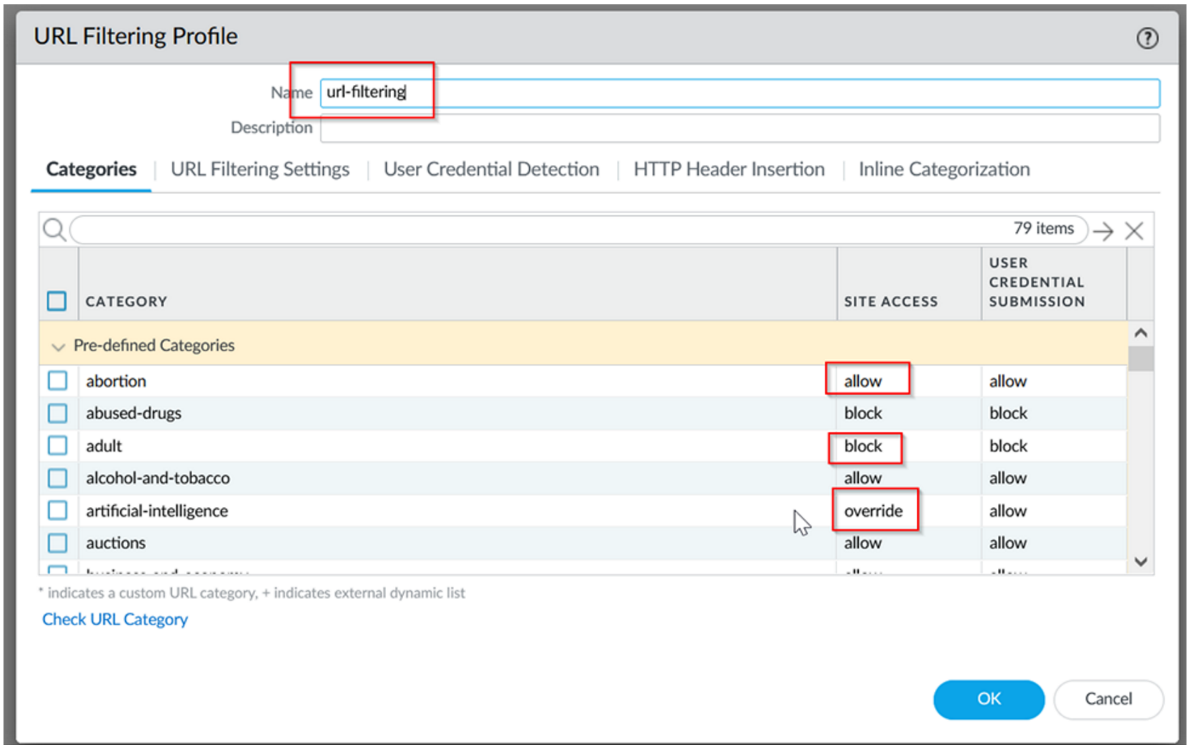
Lab Summary:

Navigate to "Objects" on the upper taskbar and then to "URL Filtering" under "Security Profiles" on the left taskbar. Once there, press "Add" on the bottom left to create a new URL Filtering profile.



□	NAME	LOCATION	SITE ACCESS
□	default	Predefined	Allow Categories (60) Alert Categories (7) Continue Categories (0) Block Categories (12) Override Categories (0)
□	url-filtering		Allow Categories (60) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (1)

In the URL Filtering profile, create a name and change the access responses to Palo Alto filtering categories. To allow a website means traffic will go through, to block a website means traffic isn’t allowed, and to override a category means that a password must be provided.



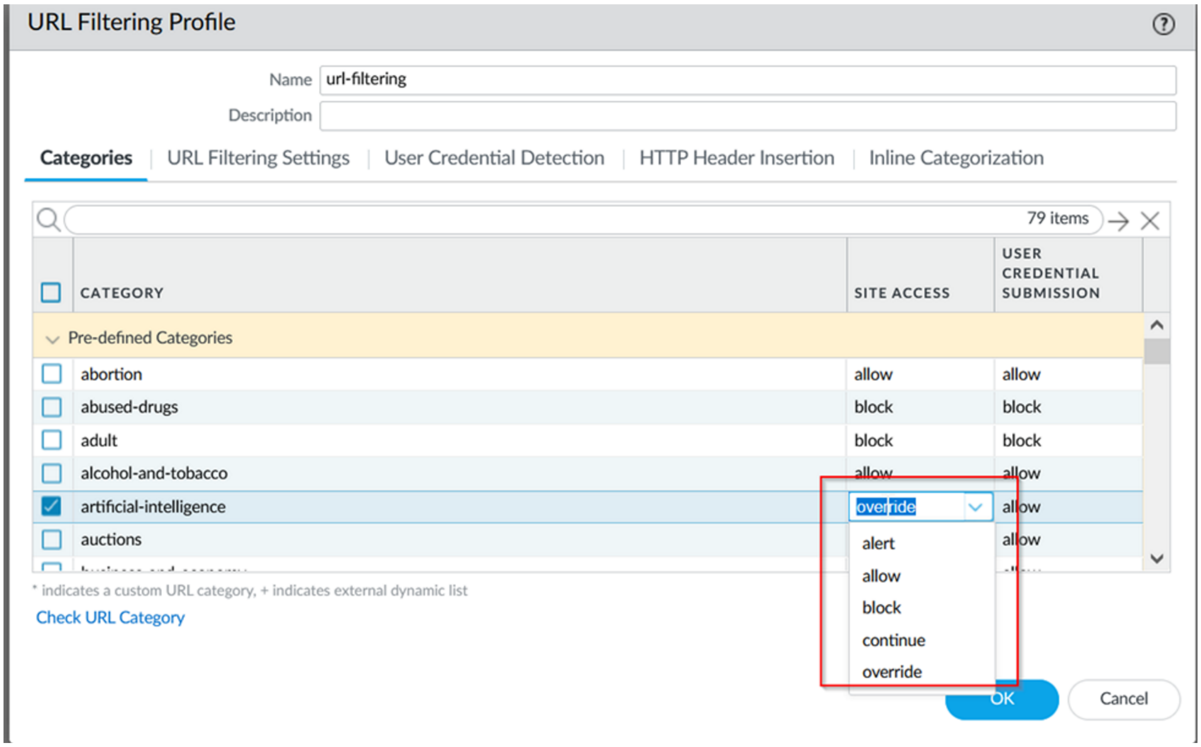
URL Filtering Profile

Name: url-filtering

Description:

☐ CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Pre-defined Categories		
☐ abortion	allow	allow
☐ abused-drugs	block	block
☐ adult	block	block
☐ alcohol-and-tobacco	allow	allow
☐ artificial-intelligence	override	allow
☐ auctions	allow	allow

* indicates a custom URL category, + indicates external dynamic list



URL Filtering Profile

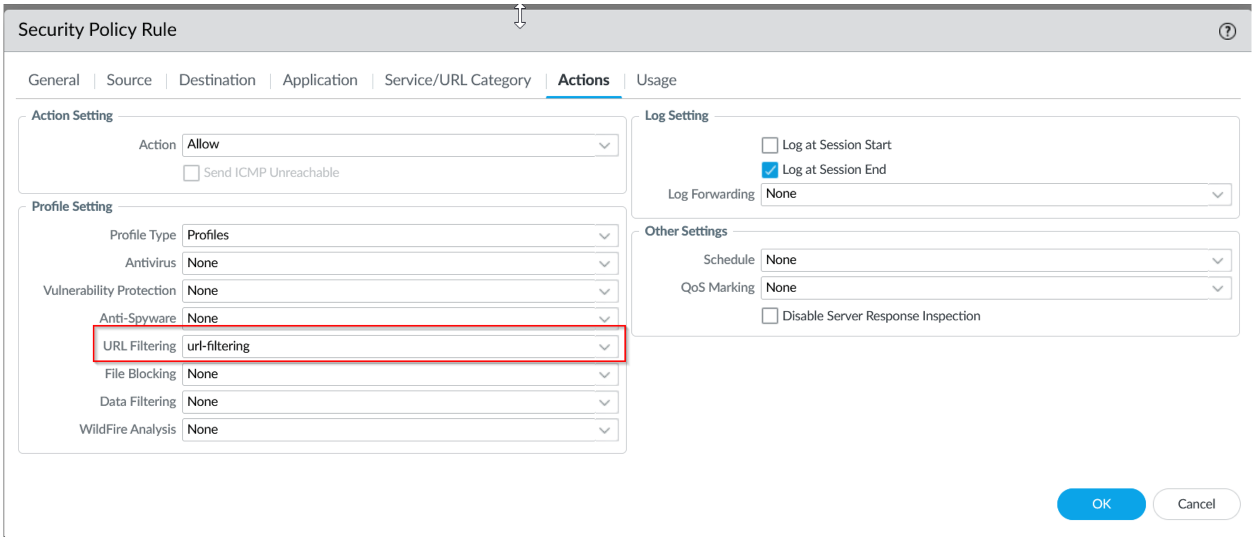
Name: url-filtering

Description:

☐ CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Pre-defined Categories		
☐ abortion	allow	allow
☐ abused-drugs	block	block
☐ adult	block	block
☐ alcohol-and-tobacco	allow	allow
☑ artificial-intelligence	override	allow
☐ auctions	allow	allow

* indicates a custom URL category, + indicates external dynamic list

Once you've created your URL filtering profile, navigate to "Policies" on the upper taskbar of the GUI and then to "Security" on the left taskbar. Select the outgoing security policy, navigate to "Actions" and then select your newly created URL filtering profile under the URL filtering section.



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: url-filtering

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

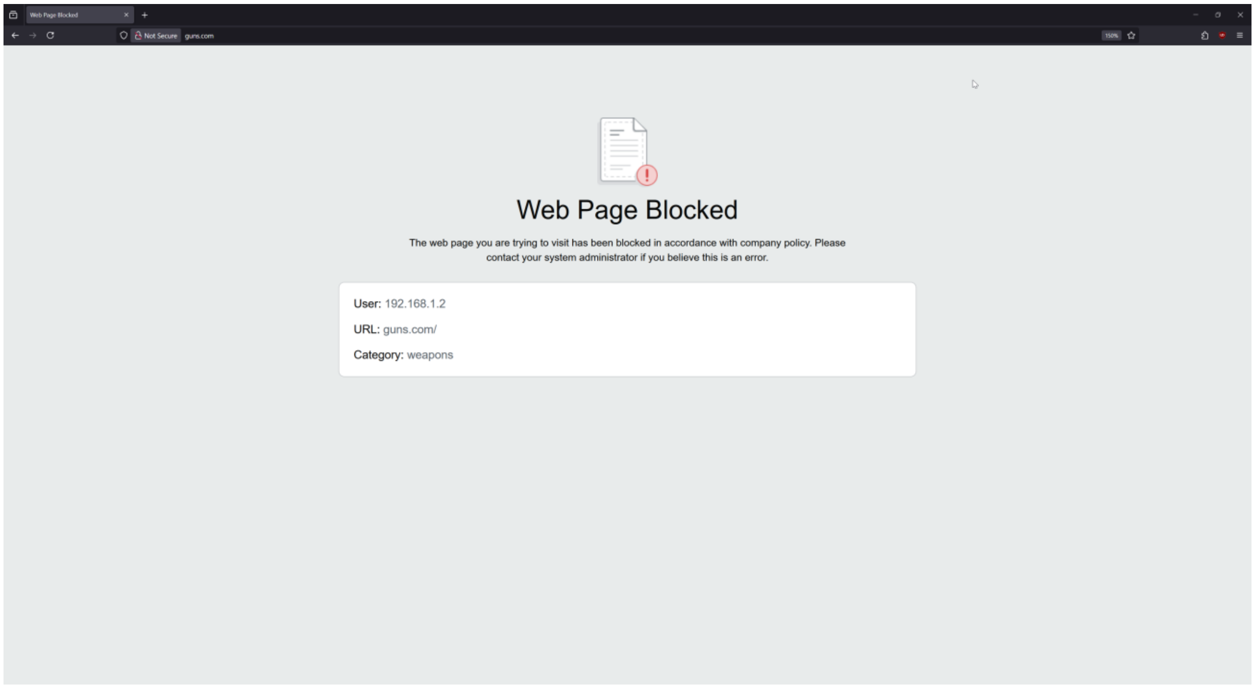
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Press "Ok" to save this security policy and commit changes to the firewall. Once these changes to your URL filtering profile and security profile have been saved and committed, your firewall will now block the websites in the categories specified. This will only work for HTTP sites, but check with a website blocked by a category you specified.



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.1.2

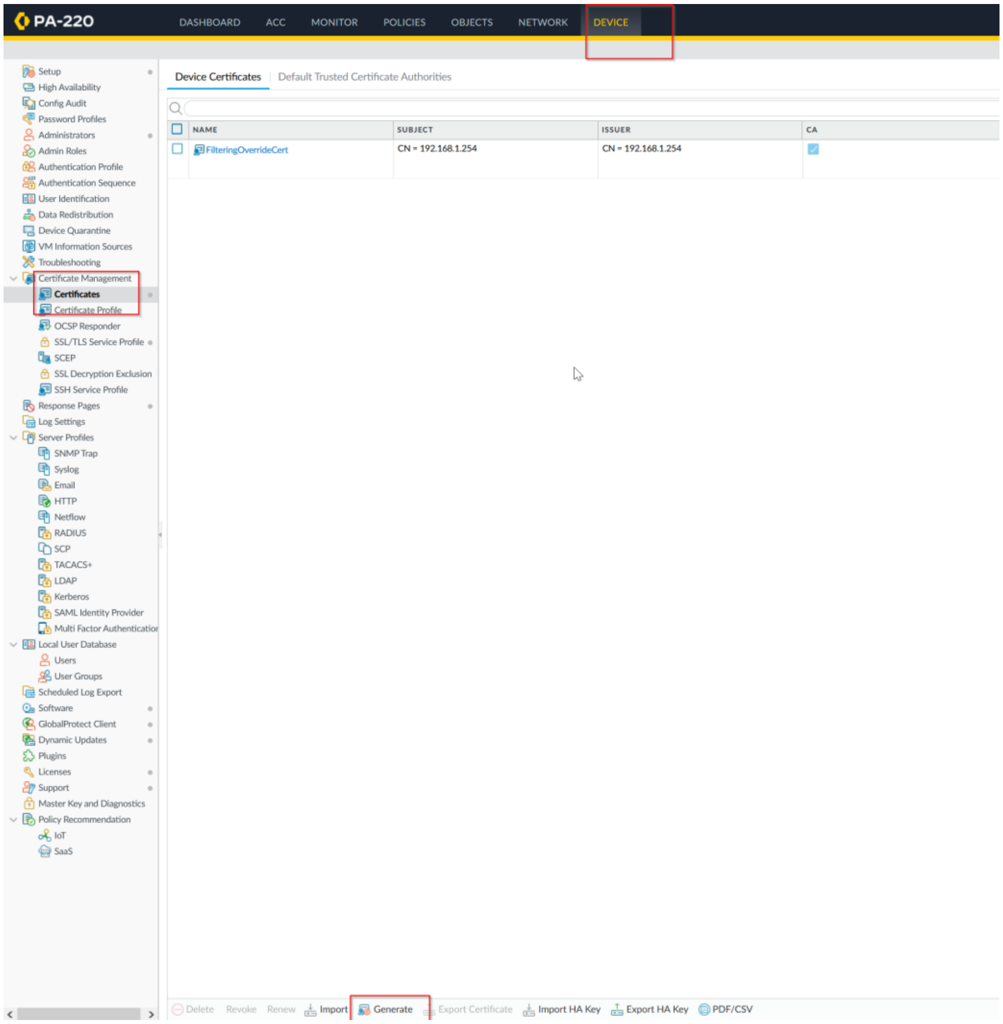
URL: guns.com/

Category: weapons

In order to set up HTTPS filtering instead of just HTTP, we should configure certificates as well. Console into the firewall and enter the below command to allow the PA-220 to inject URL filtering pages to an HTTPS session.

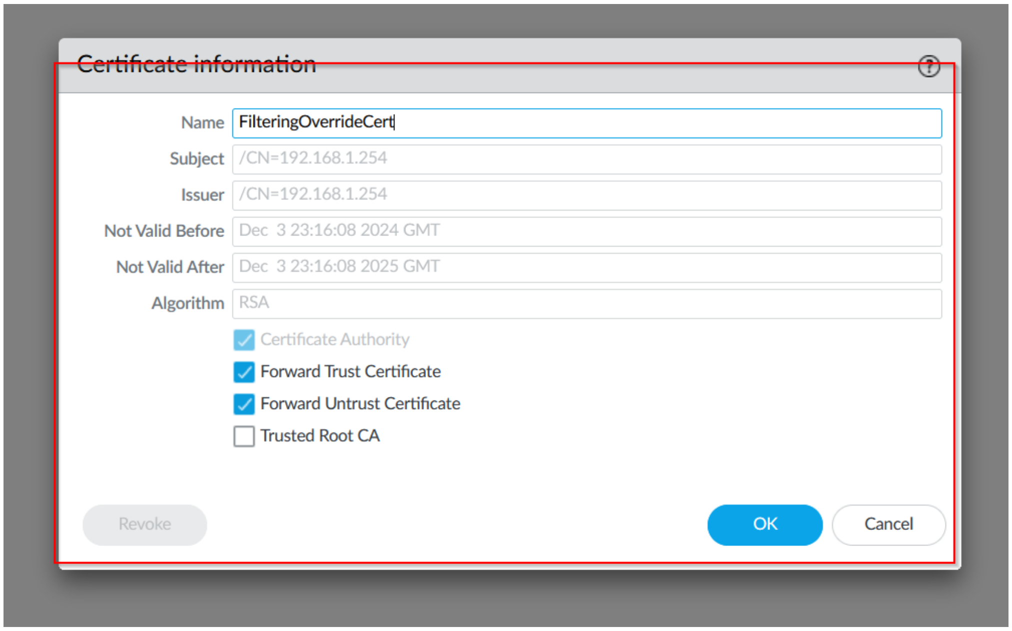
```
# set deviceconfig setting ssl-decrypt url-proxy yes
```

Once your command has been entered, navigate to "Device" on the upper taskbar and then "Certificates" on the left taskbar. Click "Generate" on the bottom to create a new certificate.



□	NAME	SUBJECT	ISSUER	CA
□	FilteringOverrideCert	CN = 192.168.1.254	CN = 192.168.1.254	☑

Create a name for your certificate and enter the following information in below. Make sure that Forward Trust and Untrust Certificates are checked off.



Name: FilteringOverrideCert

Subject: /CN=192.168.1.254

Issuer: /CN=192.168.1.254

Not Valid Before: Dec 3 23:16:08 2024 GMT

Not Valid After: Dec 3 23:16:08 2025 GMT

Algorithm: RSA

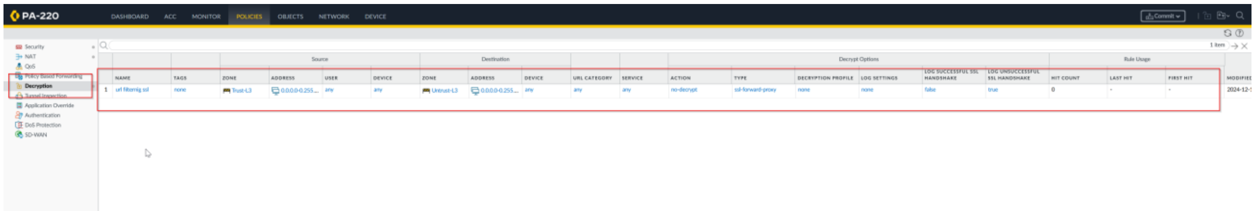
☑ Certificate Authority

☑ Forward Trust Certificate

☑ Forward Untrust Certificate

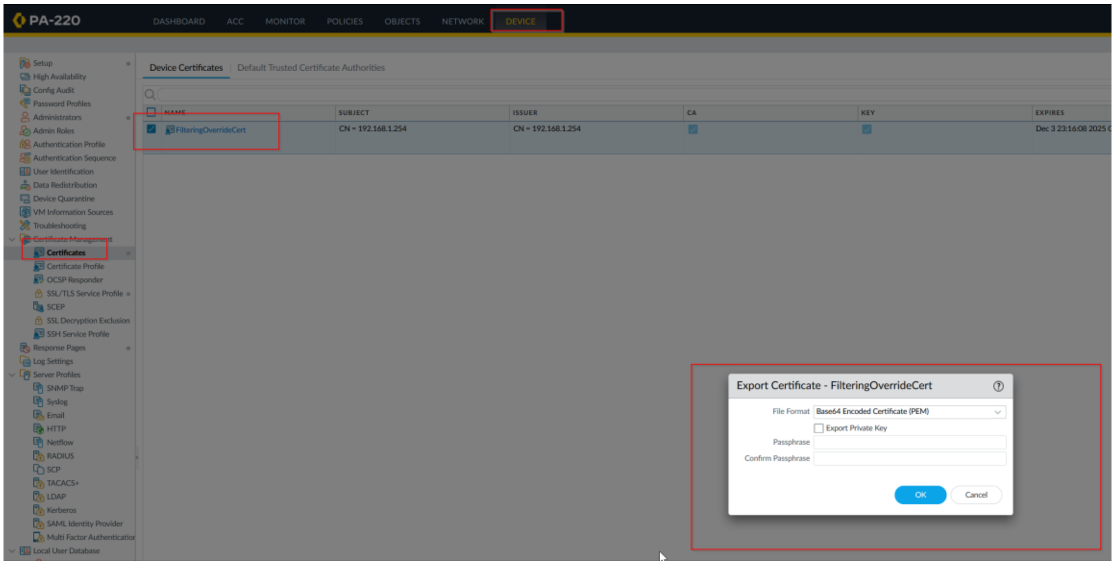
□ Trusted Root CA

In “Policies” on the top taskbar and “Description” on the left, create a new policy for inbound and outbound traffic, with the type ssl-decrypt-proxy.



			Source				Destination					Decrypt Options						Rule Usage			
	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE	HIT COUNT	LAST HIT	FIRST HIT	MODIFIED
1	url filtering ssl	none	Trust-L3	0.0.0.0-0.255...	any	any	Untrust-L3	0.0.0.0-0.255...	any	any	any	no-decrypt	ssl-forward-proxy	none	none	false	true	0	-	-	2024-12-

Navigate back to “Device” and “Certificates” to export the certificate to your computer.



	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES
☑	FilteringOverrideCert	CN = 192.168.1.254	CN = 192.168.1.254	☑	☑	Dec 3 23:16:08 2025

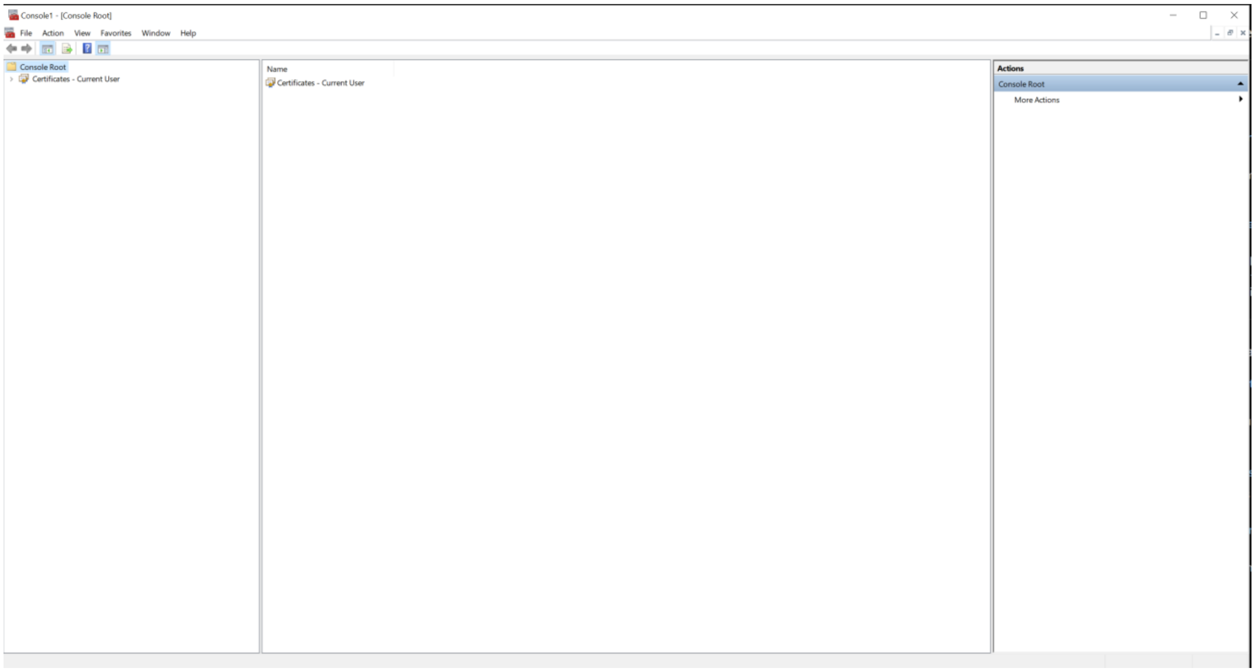
File Format: Base64 Encoded Certificate (PEM)

□ Export Private Key

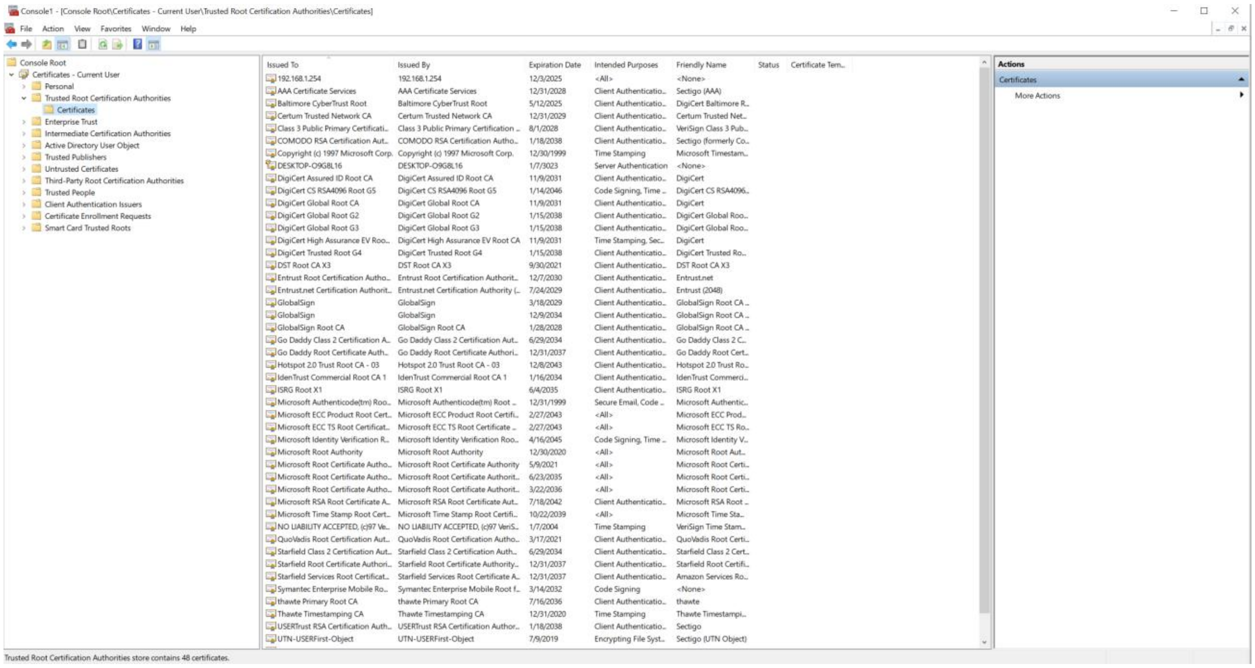
Passphrase:

Confirm Passphrase:

After downloading the root certificate, install it into your computer. For a Windows computer, you’ll need to press “Windows + r” to launch the Windows management console. From there, you can add the certificate to the menu.



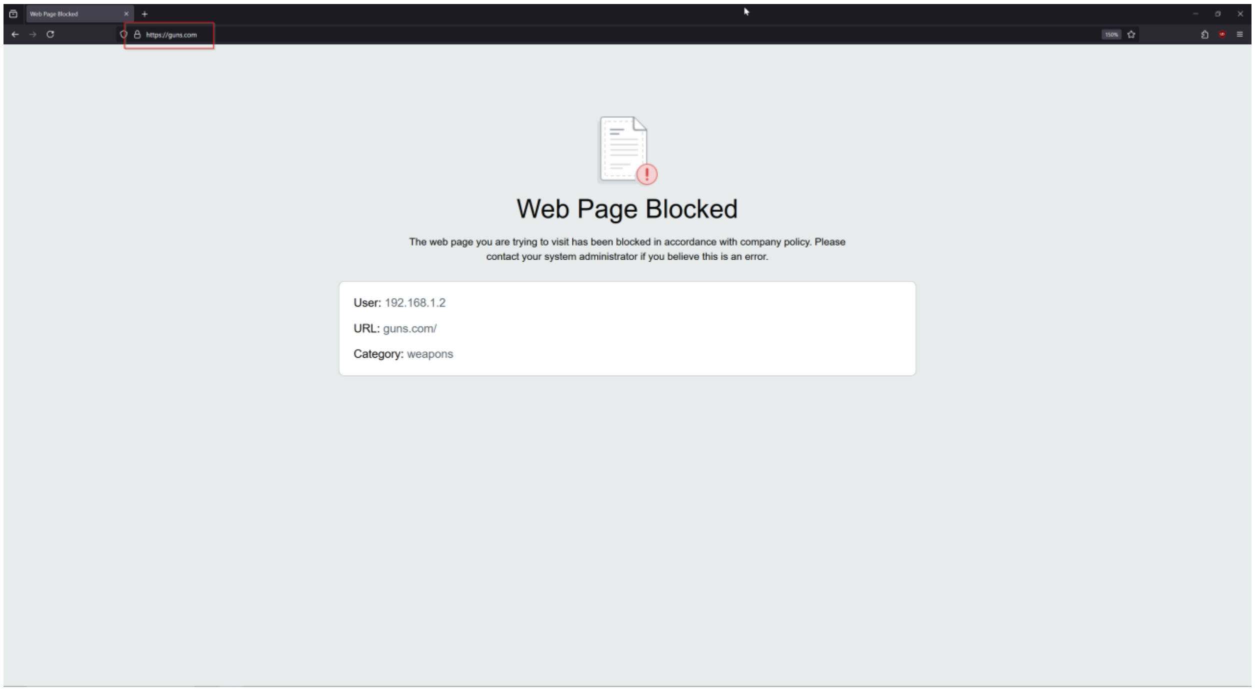
Navigate to “Certificates – Current User,” “Trusted Root Certification Authorities,” and then to “Certificates.” Right click to add a new certificate and add the certificate from where you downloaded it to.


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem…
192.168.1.254	192.168.1.254	12/3/2025	<All>	<None>		
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticatio…	Sectigo (AAA)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticatio…	DigiCert Baltimore R…		
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authenticatio…	Certum Trusted Net…		
Class 3 Public Primary Certificati…	Class 3 Public Primary Certification …	8/1/2028	Client Authenticatio…	VeriSign Class 3 Pub…		
COMODO RSA Certification Aut…	COMODO RSA Certification Autho…	1/18/2038	Client Authenticatio…	Sectigo (formerly Co…		
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestam…		
DESKTOP-O9G8L16	DESKTOP-O9G8L16	1/7/3023	Server Authentication	<None>		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticatio…	DigiCert		
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time …	DigiCert CS RSA4096…		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticatio…	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticatio…	DigiCert Global Roo…		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticatio…	DigiCert Global Roo…		
DigiCert High Assurance EV Roo…	DigiCert High Assurance EV Root CA	11/9/2031	Time Stamping, Sec…	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticatio…	DigiCert Trusted Ro…		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticatio…	DST Root CA X3		
Entrust Root Certification Autho…	Entrust Root Certification Authorit…	12/7/2030	Client Authenticatio…	Entrust.net		
Entrust.net Certification Authorit…	Entrust.net Certification Authority (…	7/24/2029	Client Authenticatio…	Entrust (2048)		
GlobalSign	GlobalSign	3/18/2029	Client Authenticatio…	GlobalSign Root CA …		
GlobalSign	GlobalSign	12/9/2034	Client Authenticatio…	GlobalSign Root CA …		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticatio…	GlobalSign Root CA …		
Go Daddy Class 2 Certification A…	Go Daddy Class 2 Certification Aut…	6/29/2034	Client Authenticatio…	Go Daddy Class 2 C…		
Go Daddy Root Certificate Auth…	Go Daddy Root Certificate Authori…	12/31/2037	Client Authenticatio…	Go Daddy Root Cert…		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticatio…	Hotspot 2.0 Trust Ro…		
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	1/16/2034	Client Authenticatio…	IdenTrust Commerci…		
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticatio…	ISRG Root X1		
Microsoft Authenticode(tm) Roo…	Microsoft Authenticode(tm) Root …	12/31/1999	Secure Email, Code …	Microsoft Authentic…		
Microsoft ECC Product Root Cert…	Microsoft ECC Product Root Certifi…	2/27/2043	<All>	Microsoft ECC Prod…		
Microsoft ECC TS Root Certificat…	Microsoft ECC TS Root Certificate …	2/27/2043	<All>	Microsoft ECC TS Ro…		
Microsoft Identity Verification R…	Microsoft Identity Verification Roo…	4/16/2045	Code Signing, Time …	Microsoft Identity V…		
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>	Microsoft Root Aut…		
Microsoft Root Certificate Autho…	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi…		
Microsoft Root Certificate Autho…	Microsoft Root Certificate Authorit…	6/23/2035	<All>	Microsoft Root Certi…		
Microsoft Root Certificate Autho…	Microsoft Root Certificate Authorit…	3/22/2036	<All>	Microsoft Root Certi…		
Microsoft RSA Root Certificate A…	Microsoft RSA Root Certificate Aut…	7/18/2042	Client Authenticatio…	Microsoft RSA Root …		
Microsoft Time Stamp Root Cert…	Microsoft Time Stamp Root Certifi…	10/22/2039	<All>	Microsoft Time Sta…		
NO LIABILITY ACCEPTED, (c)97 Ve…	NO LIABILITY ACCEPTED, (c)97 VeriS…	1/7/2004	Time Stamping	VeriSign Time Stam…		
QuoVadis Root Certification Aut…	QuoVadis Root Certification Autho…	3/17/2021	Client Authenticatio…	QuoVadis Root Certi…		
Starfield Class 2 Certification Aut…	Starfield Class 2 Certification Auth…	6/29/2034	Client Authenticatio…	Starfield Class 2 Cert…		
Starfield Root Certificate Authori…	Starfield Root Certificate Authority…	12/31/2037	Client Authenticatio…	Starfield Root Certifi…		
Starfield Services Root Certificat…	Starfield Services Root Certificate A…	12/31/2037	Client Authenticatio…	Amazon Services Ro…		
Symantec Enterprise Mobile Ro…	Symantec Enterprise Mobile Root f…	3/14/2032	Code Signing	<None>		
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Client Authenticatio…	thawte		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi…		
USERTrust RSA Certification Auth…	USERTrust RSA Certification Author…	1/18/2038	Client Authenticatio…	Sectigo		
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst…	Sectigo (UTN Object)		

Trusted Root Certification Authorities store contains 48 certificates.

Now that the certificate is installed, your URL filtering should work for HTTPS websites as well.



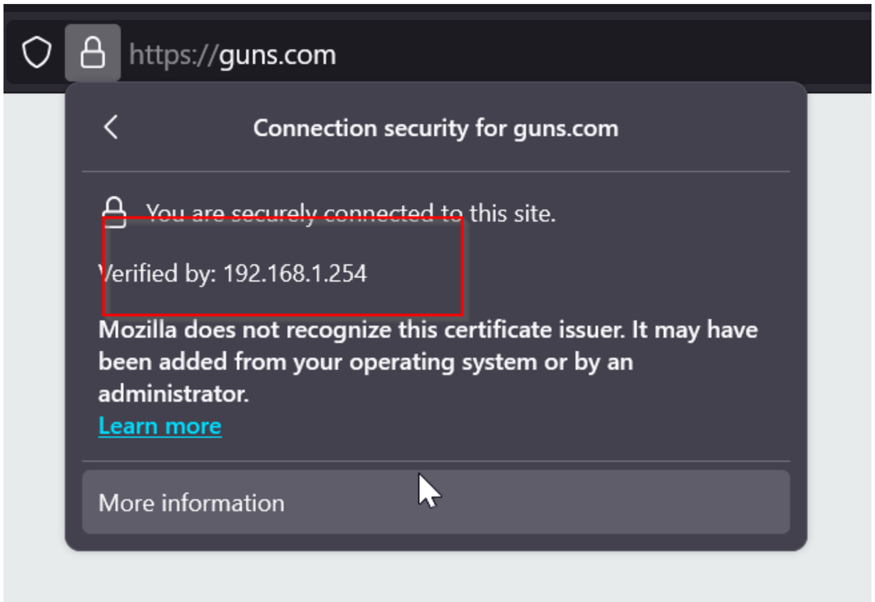
Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.1.2

URL: guns.com/

Category: weapons



Connection security for guns.com

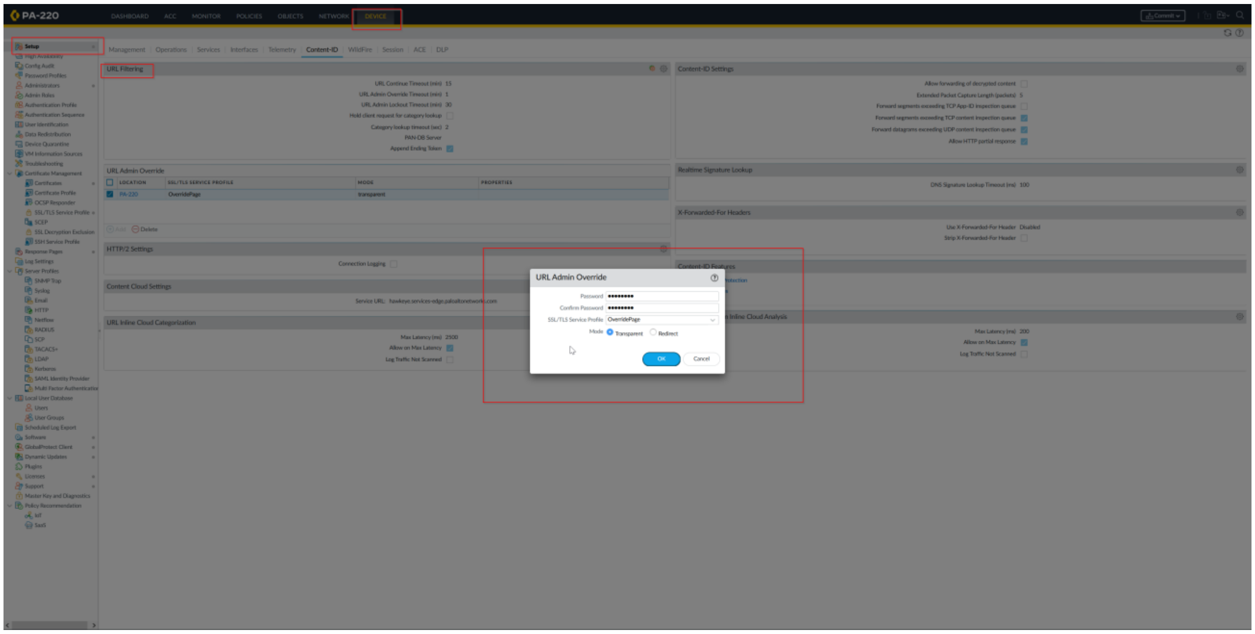
You are securely connected to this site.

Verified by: 192.168.1.254

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator.

Learn more

Since we have both HTTP and HTTPS URL filtering, we can add in the “override” settings for admins. In the Palo Alto PA-220 GUI, navigate to “Device” in the top taskbar, and then “Setup” and “URL Filtering.” Add a new URL Admin Override profile.



URL Filtering

URL Continue Timeout (min) 15
URL Admin Override Timeout (min) 1
URL Admin Lockout Timeout (min) 30
Hold client request for category lookup □
Category lookup timeout (sec) 2
PAN-DB Server
Append Ending Token ☑

URL Admin Override

LOCATION	SSL/TLS SERVICE PROFILE	MODE	PROPERTIES
PA-220	OverridePage	transparent	

HTTP/2 Settings

Connection Logging □

Content Cloud Settings

Service URL: hawkeye.services-edge.paloaltonetworks.com

URL Inline Cloud Categorization

Max Latency (ms) 2500

URL Admin Override

Password ••••••••

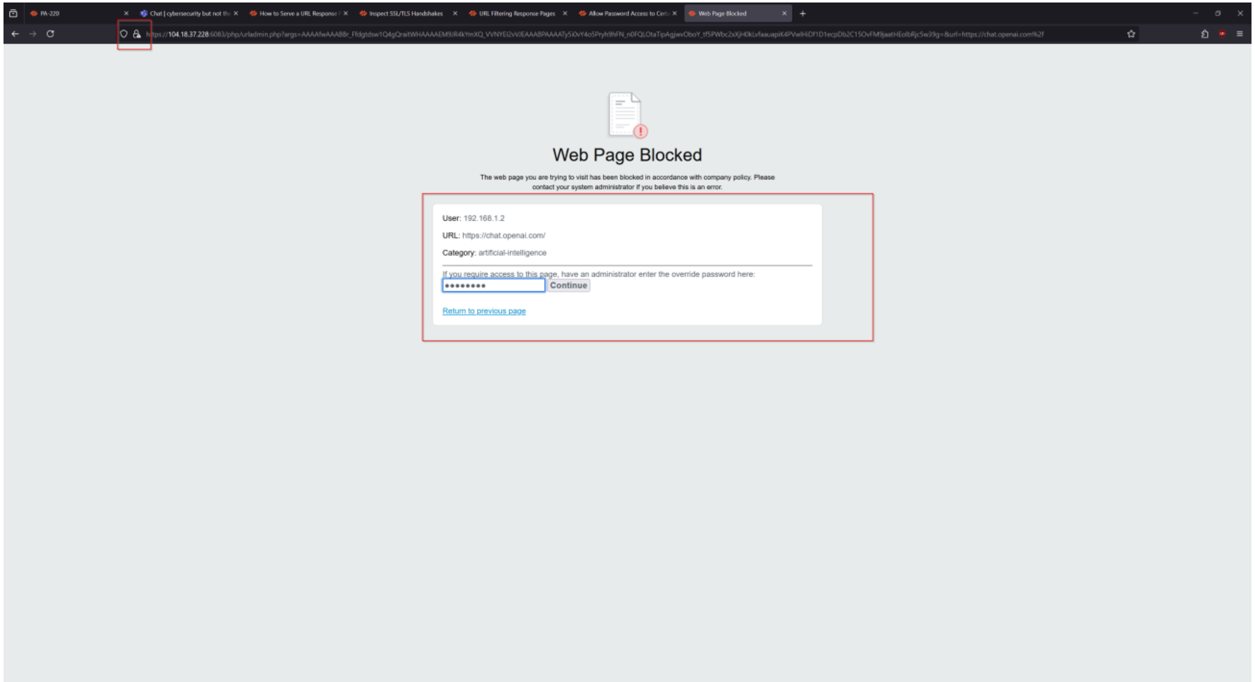
Confirm Password ••••••••

SSL/TLS Service Profile OverridePage

Mode ● Transparent ○ Redirect

OK Cancel

Verify that override works by entering your admin password into a website configured as override.



Web Page Blocked

The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.1.2

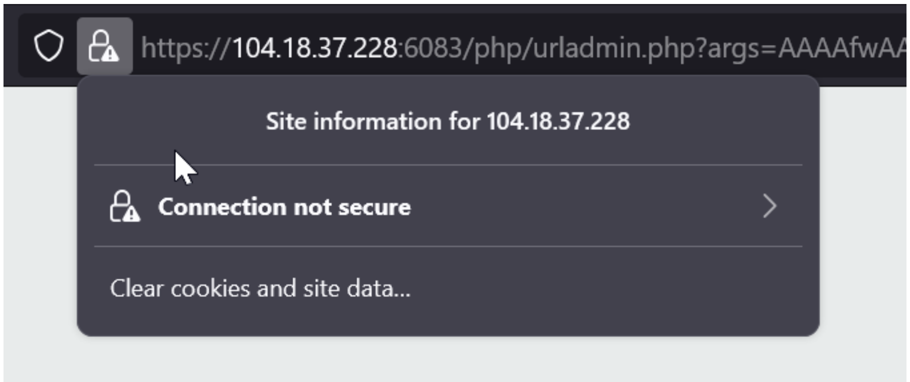
URL: https://chat.openai.com/

Category: artificial-intelligence

If you require access to this page, have an administrator enter the override password here:

•••••••• Continue

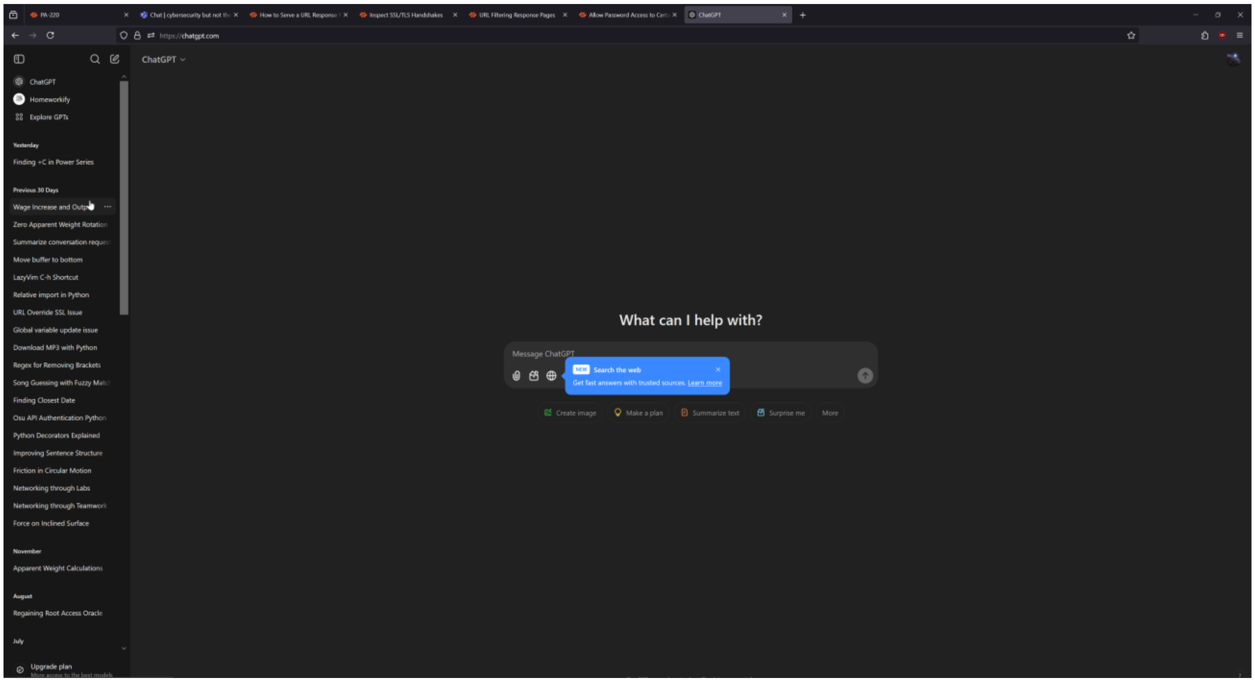
Return to previous page



https://104.18.37.228:6083/php/urladmin.php?args=AAAAfwAA

Site information for 104.18.37.228

Connection not secure



https://chatgpt.com
ChatGPT
Homeworkify
Explore GPTs
Yesterday
Finding +C in Power Series
Previous 30 Days
Wage Increase and Output
Zero Apparent Weight Rotation
Move buffer to bottom
LazyVim C-h Shortcut
Relative import in Python
URL Override SSL Issue
Global variable update issue
Download MP3 with Python
Regex for Removing Brackets
Finding Closest Date
Osu API Authentication Python
Python Decorators Explained
Improving Sentence Structure
Friction in Circular Motion
Networking through Labs
Networking through Teamwork
Force on Inclined Surface
November
Apparent Weight Calculations
August
Regaining Root Access Oracle
July
Upgrade plan
What can I help with?
Message ChatGPT
Search the web
Get fast answers with trusted sources. Learn more
Create image
Make a plan
Summarize text
Surprise me
More

If override succeeds, URL filtering is now set up properly on your Palo Alto PA-220.

Lab Commands:

The only new command used in this lab was one used to allow our PA-220 to insert the URL block page into HTTPS sessions as shown below.

```
    # set deviceconfig setting ssl-decrypt url-proxy yes
```

This command essentially allows the firewall to decrypt SSL traffic so that it can check for security threats and to see if the traffic falls under one of the blocked filtering categories on the PA-220. Without this, our URL filtering policy wouldn’t be able to work on HTTPS, meaning that a large range of websites would slip out from under our control.

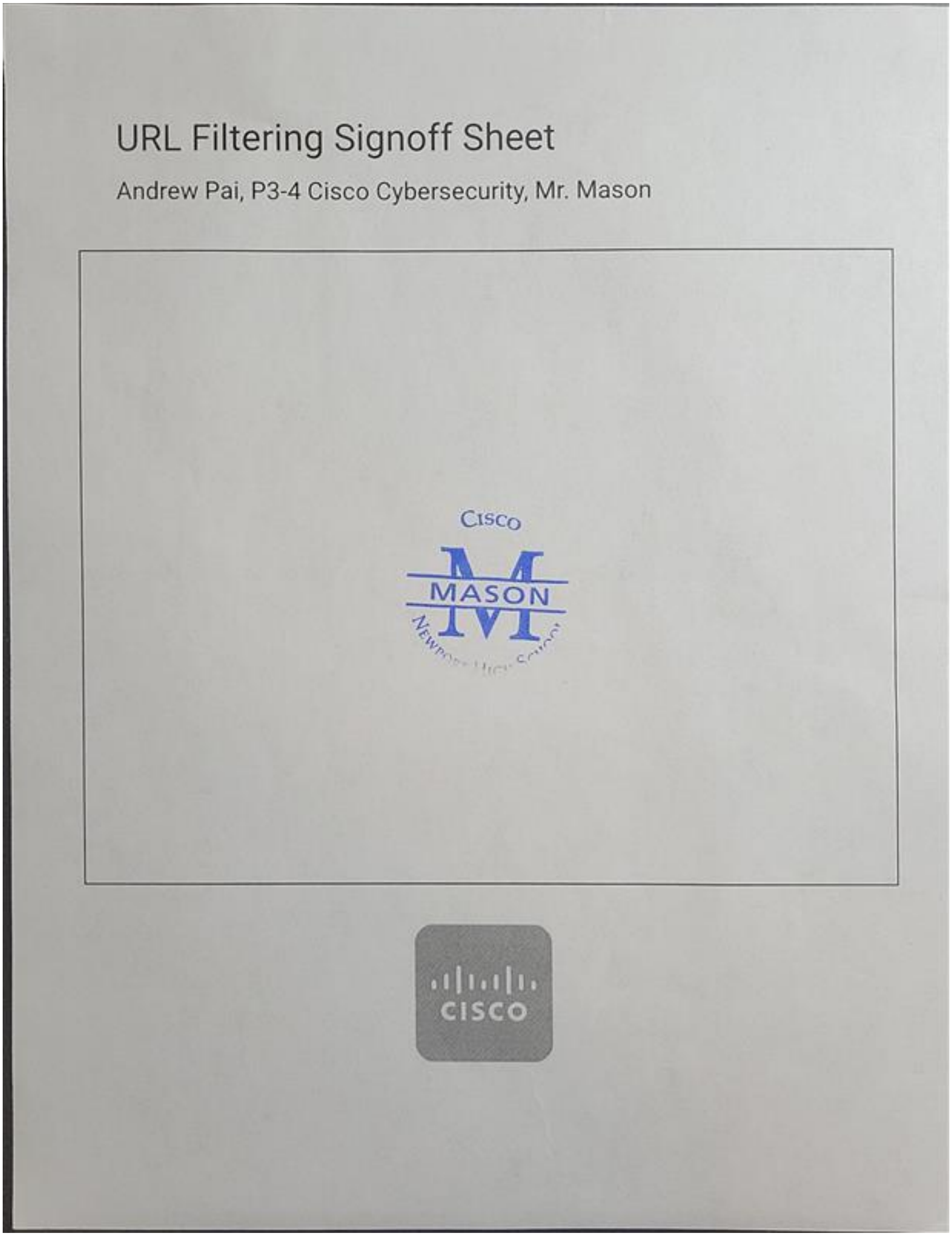
Problems:

The biggest problem that our group had with this lab was with our HTTPS filtering and lack of a CA Certificate. Since HTTPS traffic is encrypted, our group couldn’t figure out how to use the PA-220 to stop and filter URLs the same way that we could with HTTP traffic. This caused us to be stuck on HTTPS filtering for quite a while before figuring out that we needed to actually decrypt the HTTPS traffic by using SSL decryption. SSL decryption allowed us to decrypt, analyze, and stop web traffic just like we did with HTTP, but we needed a CA Certificate in order to implement the connection between firewall and client. Therefore, before moving on with any HTTPS filtering, our group had to go through the process of getting a CA Certificate and installing it. After the certificate was installed and SSL decryption was allowed on our firewall though, HTTPS filtering worked perfectly and allowed us to move onto the override aspect of the lab.

Conclusion:

In conclusion, URL filtering is a critical way to maintain network security and ensure that all network hosts have a safe environment to work in. The URL filtering setup in this lab is applicable to various types of networks, from corporate to educational to personal. This lab was meant to setup URL filtering for both HTTP and HTTPS sites, blocking harmful categories but still allowing admins with an override password to access this traffic. To do this, we used the Palo Alto GUI and had to install a certificate for HTTPS traffic.

Lab Signoff:



URL Filtering Signoff Sheet

Andrew Pai, P3-4 Cisco Cybersecurity, Mr. Mason

Cisco
MASON
Newport High School

CISCO