

Application Control & URL Filtering

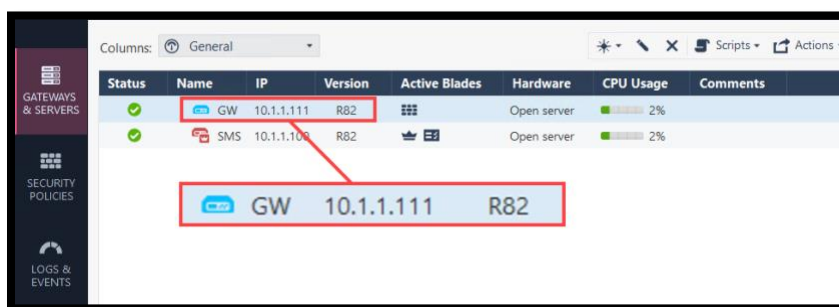
Introduction

In this lab, we will enable the Application Control and URL filtering blades.

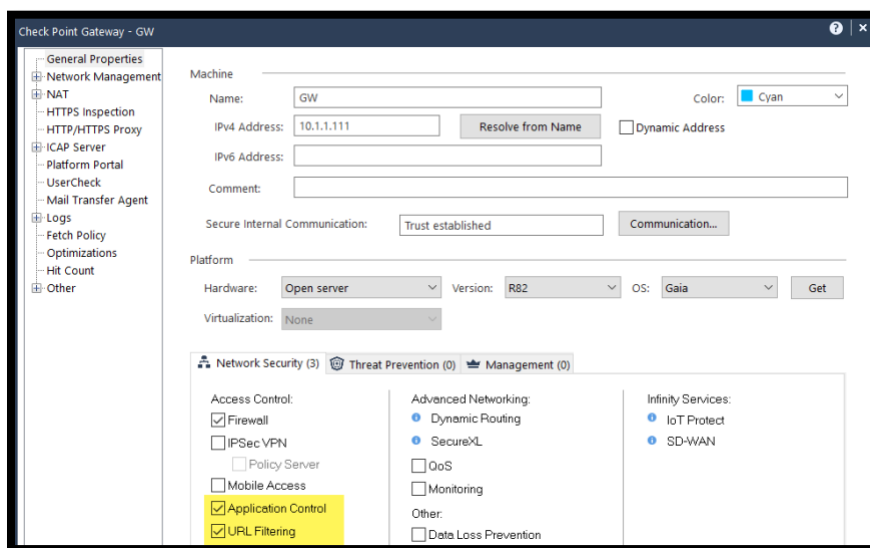
Exercise 1: Onboarding

In this exercise, we will enable the Application control and URLF blades on the central gateway object **GW**.

1. While connecting to the jump server, use SmartConsole to login to the Management server **SMS**. Use the IP address **10.1.1.100** **admin/Cpwins!1** and edit the gateway object **GW**.

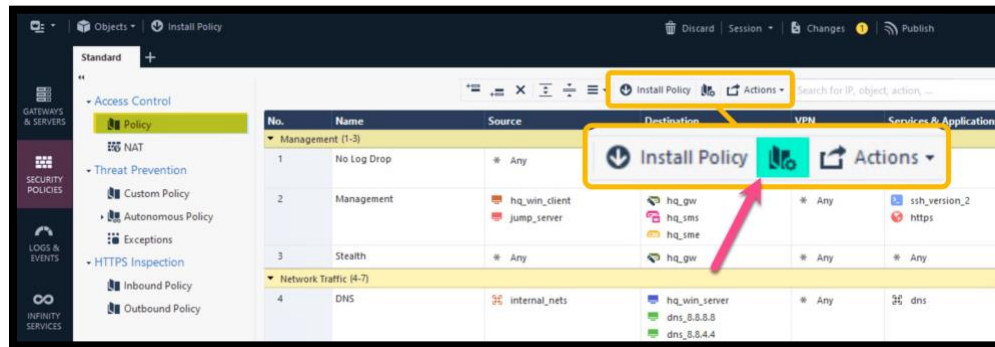


2. Enable the **Application Control** and **URL Filtering** blades. Click **OK** to close the gateway editor.

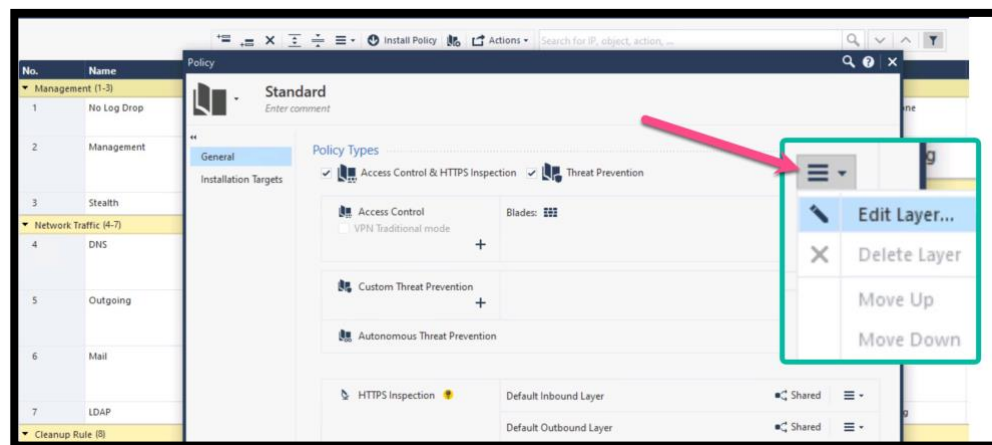


Notice that a new tab is now visible under **Global Properties** -> **UserCheck**.

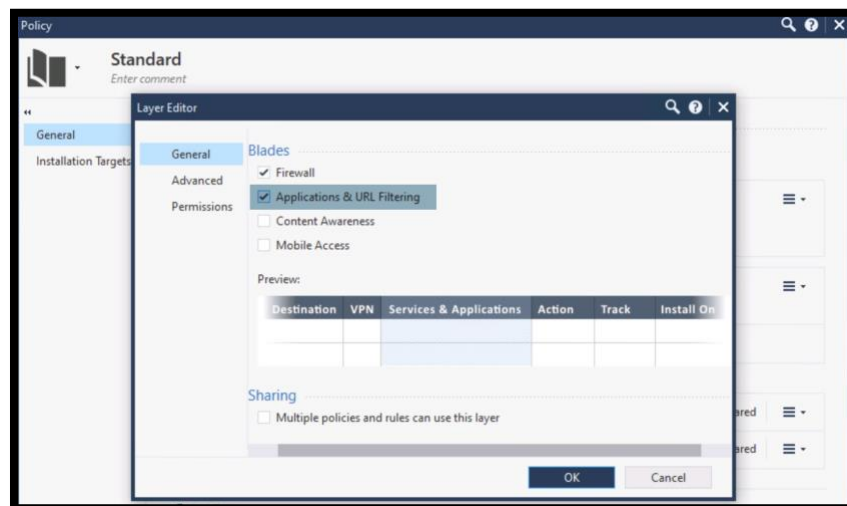
3. Navigate to the **Policy** tab. Click the icon to edit the **Policy Package**.



4. The Current default policy package has a single layer with only **Firewall** rules activated. Edit the layer as shown below.



5. Make sure **Applications & URL Filtering** is checked and click OK to close the editor.

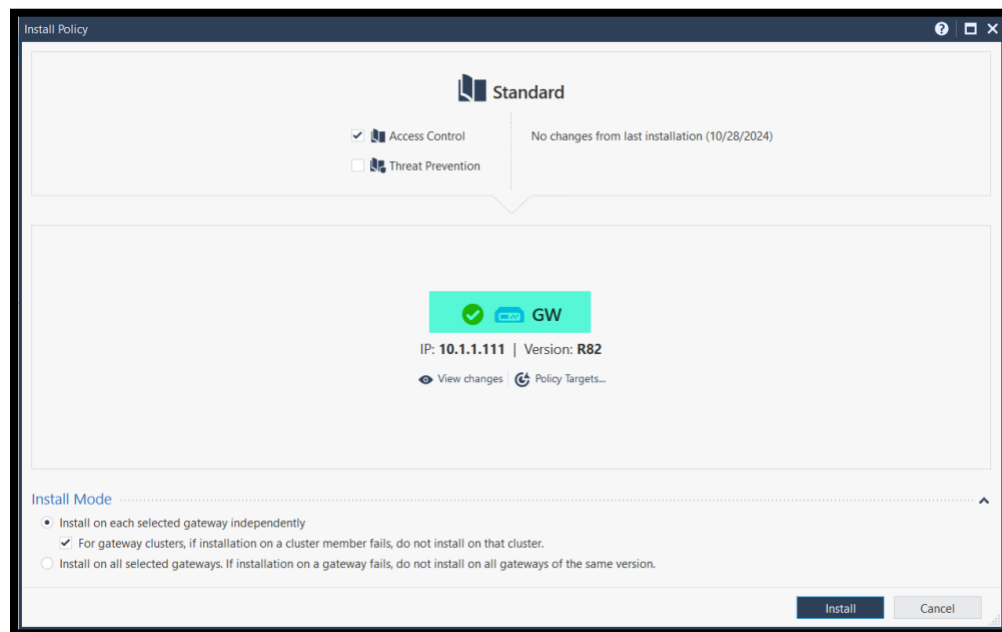


6. Create a new rule on top of the outbound rule. Use this rule to blocking hosts in the internal subnet **10.1.1.0/24** from accessing public Email web sites. Use the category **Email**.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-4)								
DNS (5)								
Network Traffic (6-10)								
6	Block Public Mail	net_10_1_1_0_24	Internet	* Any	Email	Drop	Log Accounting	* Policy Ta...
7	Outbound	net_10_1_1_0_24 net_10_1_2_0_24 net_10_1_3_0_24 t_pot	* Any	* Any	http https HTTP_and_HTTPS_p... icmp-requests quic	Accept	Log	* Policy Ta...
8	NTP	t_pot	* Any	* Any	ntp	Accept	None	* Policy Ta...
9	Mail	net_10_1_1_0_24 net_10_1_2_0_24 jump_server	* Any	* Any	mail_services	Accept	Log	* Policy Ta...
10	LDAP	windows_client SMS	windows_server	* Any	LDAP_all ntp tcp-high-ports	Accept	Log	* Policy Ta...
DMZ (11)								
Clean up rule (12)								

- Two of the fields contain **URLF** and **Application Control** objects.
 - The destination is set to Internet. This object is supported when the application control and URL filtering blades are enabled on the Layer (Step 5 above).
 - The service field is a URLF category.
 - Only rules with URLF and Application control objects are processed by the blades and related logs will be generated.

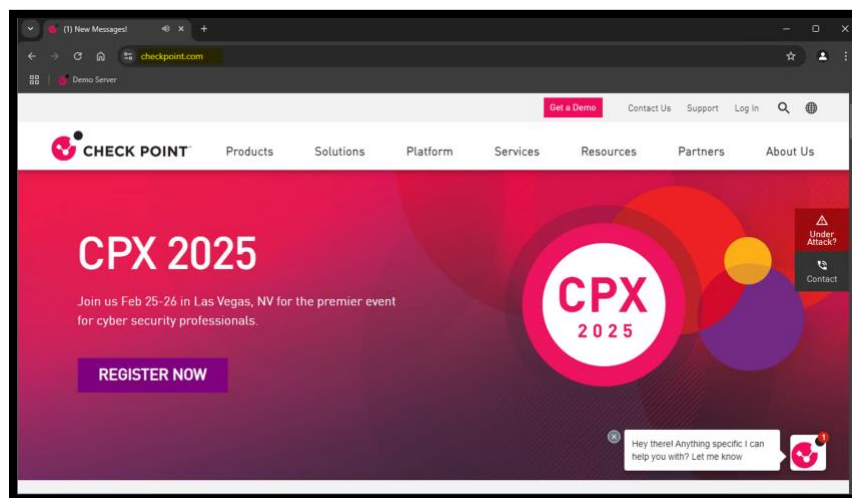
7. **Publish** the changes and Install the **Access Control** Policy.



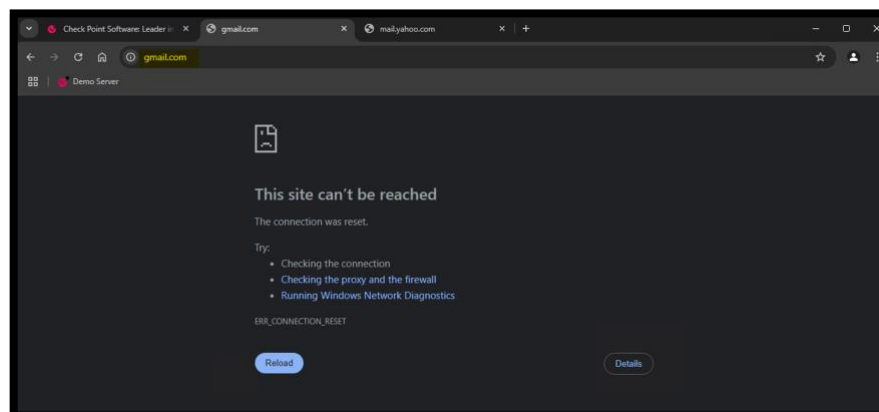
8. From the Jump server Desktop, use the saved **RDP** to login to the **win_client** host, the IP address is **10.1.1.222**. Use the account **admin/Cpwins!1**.



9. Launch chrome and navigate to <https://checkpoint.com> and confirm it works successfully.



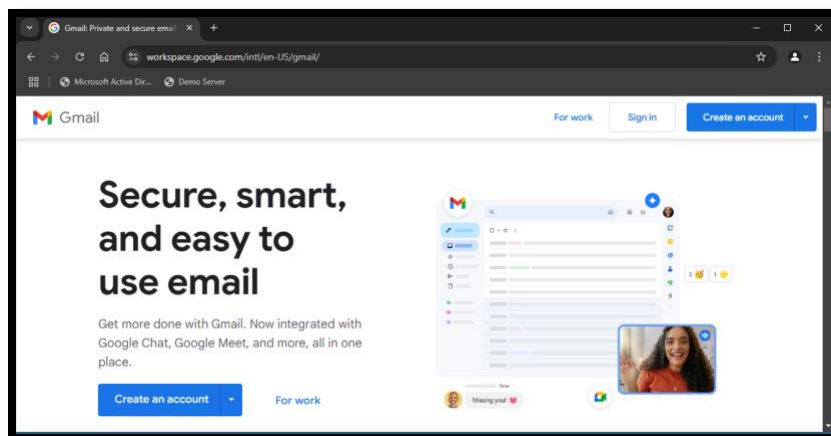
10. Test the new block rule by navigating to <https://gmail.com> and any other Email websites. E.g. <https://mail.yahoo.com>. Are you able to access the Email sites?



11. From the Jump server Desktop, use the saved **RDP** to login to the **win_server** host, the IP address is **10.1.2.250**. Use the account **administrator/Cpwins!1**.

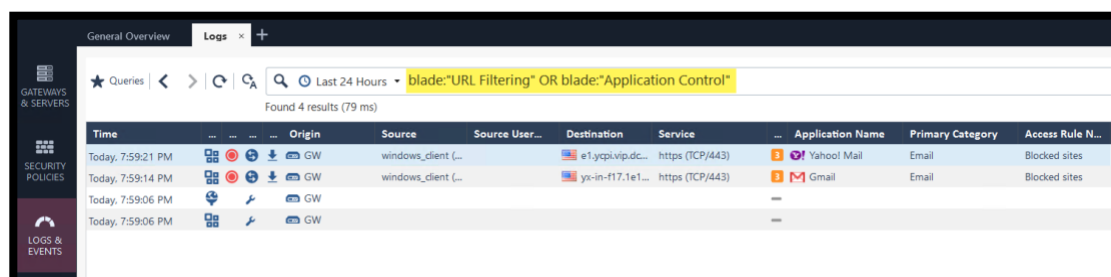


12. Try accessing Gmail or any other public Email service. Notice that this subnet is still able to access Gmail successfully according to the policy.



13. From the **Jump Server**, open SmartConsole and navigate to **Logs and Events** tab. Filter the logs to show URLF and Application control blades only. Use the filter:

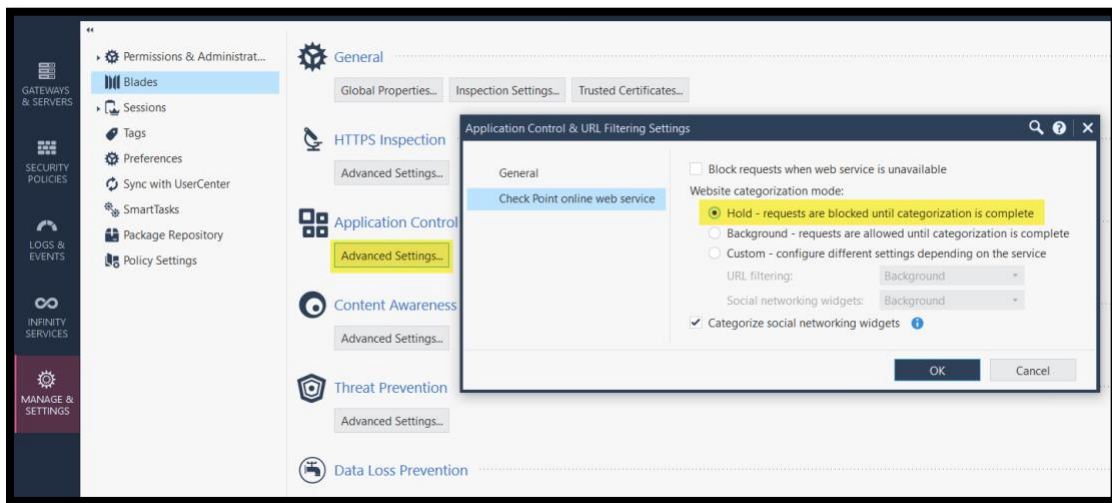
blade:"URL Filtering" OR blade:"Application Control"



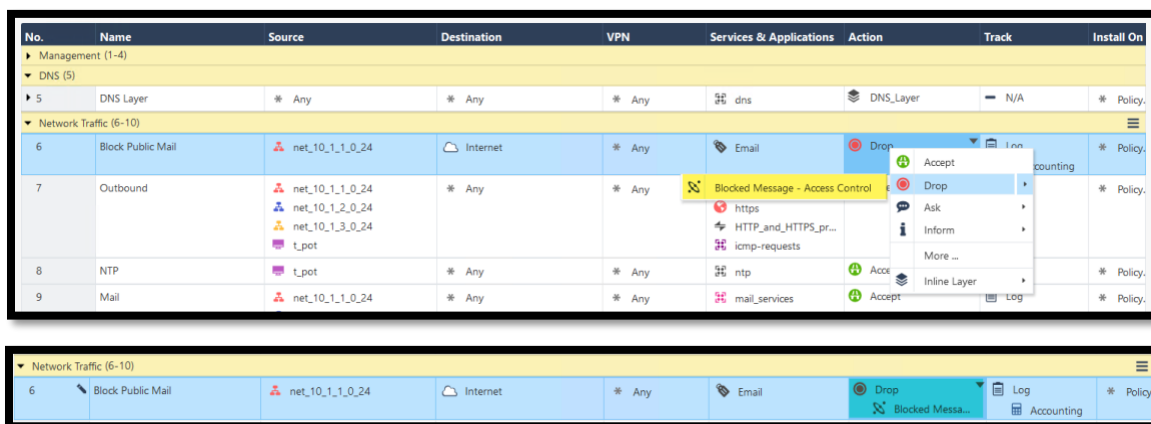


In case the website categorization is unknown to the Gateway, the resource adviser daemon (**RAD**) sends a request to the Check Point Cloud. The connection is handled in the background. Meaning, the gateway will not hold the connection until the categorization is done.

12. To change the behavior above, navigate to the Application Control & URL Filtering Advanced Settings and change the Website Categorization Mode to **Hold**.



13. Modify the **Action** Column and select the **Blocked Message** under the **Drop** option.



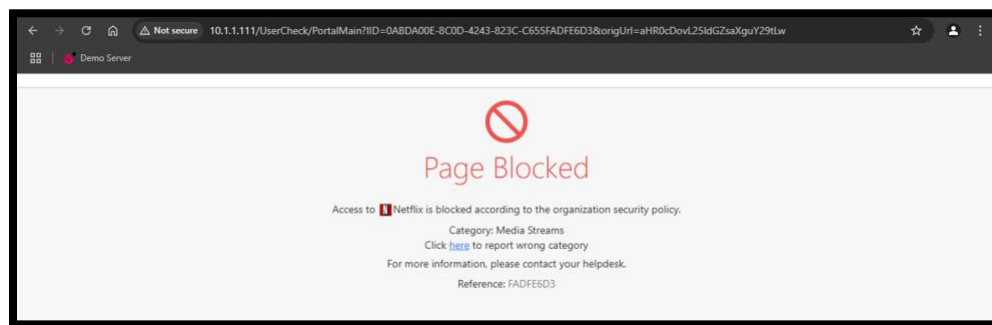
14. Install the Access Policy and try to any news website. Did you receive a block message? Why?

- Notice that the GW can **categorize HTTPS sites** and enforce the policy correctly (Certificate-Based categorization). However, because traffic is encrypted, the GW will not be able to redirect the user to a block message presented by the **UserCheck** blade.
- For full functionalities, **HTTPS inspection** is required. Refer to [SK108840](#) for more details.

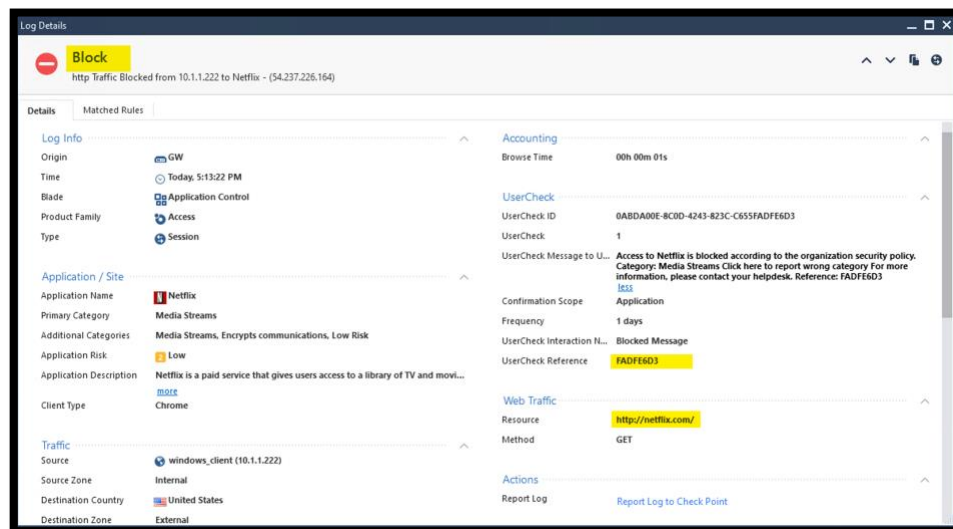
15. Edit the same rule, change the rule name to **blocked Sites**, and add two more applications to be blocked, for example, block **Netflix** and **X(Twitter)**. Install the **Access Policy**.



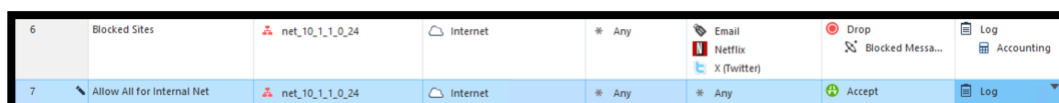
16. Try to access Netflix from the **win_client** host and notice that a block message is now returned when a site is blocked by the rule above.



17. Review the log and notice that we can see the resource as HTTP, hence we were able to redirect the user to a UserCheck block message.



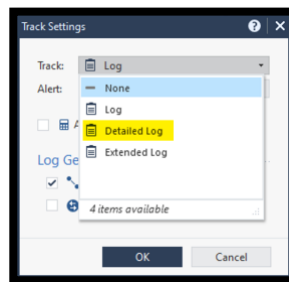
18. Add a new rule below the block rule and allow all traffic to the Internet from the internal subnet **10.1.1.0/24**.



19. Install the Access Control Policy. Try accessing multiple web sites, e.g. **Wikipedia.com**. Review the log and check if any URLF or application control **logs** are present.

- Notice that we have not specified any **Site categories** or **Applications** in the rule we created above.
- The log field is set to the default **Log** option.
- We need to use a different log option to be able to see the application names in the logs. We can use **Detailed Log** or **Extended Log**.

20. Edit the log field, select **Detailed Log** and click OK to close the editor.



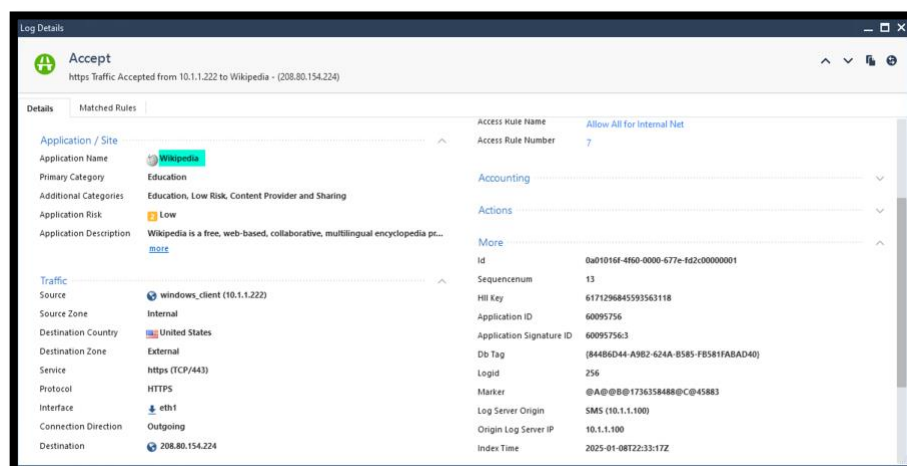
Detailed Log is equivalent to the Log option, but also shows the application that matched the connections, *even if the rule does not specify an application*.

21. The rule base should have **Detailed Log** selected in the **Track** column.

6	Blocked Sites	net_10_1_1_0_24	Internet	* Any	Email Netflix X (Twitter)	Drop Blocked Messa...	Log Accounting
7	Allow All for Internal Net	net_10_1_1_0_24	Internet	* Any	* Any	Accept	Detailed Log Accounting

12. Install the access policy.

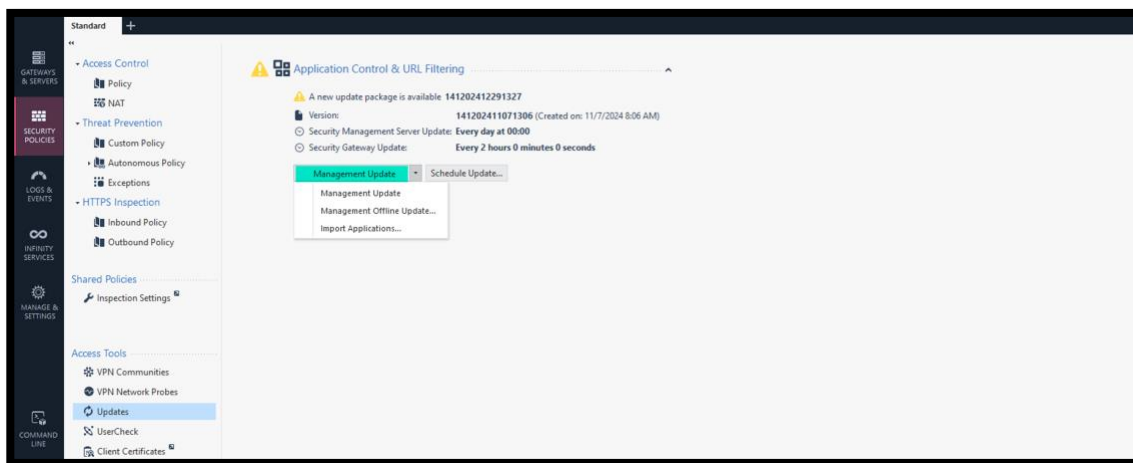
13. Access **Wikipedia** or any other sites you tested earlier and noticed that we can now see the accept log in the Application Control and URLF blades.



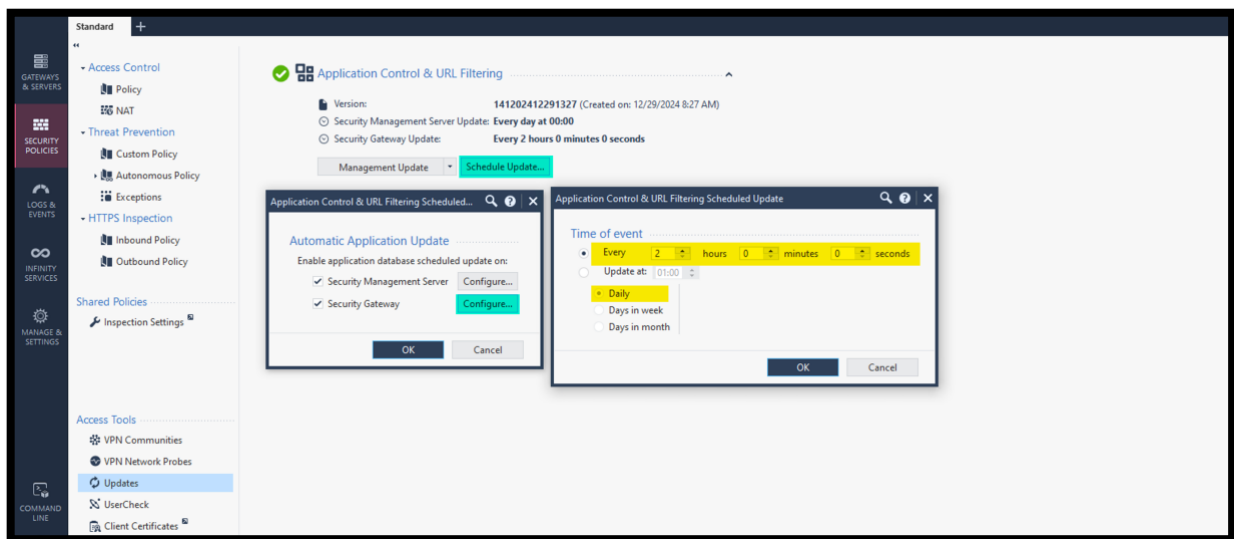
Exercise 2: Engine Updates

In this exercise, we will review the default automatic and manual options for URLF and Application control engines.

1. Check if any updates are available under Updates as you can see below. If there is a new version, select **Management Updates**.



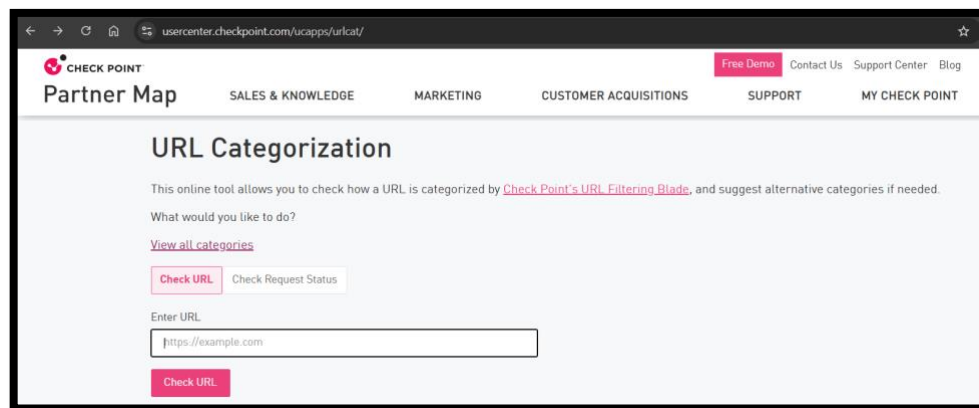
2. Navigate to the update section and review the default **Schedule Update** settings for the **GW** and the **SMS** objects.
 - Notice that the management server checks for updates every day at midnight while the GW fetches the updates every 2 hours.



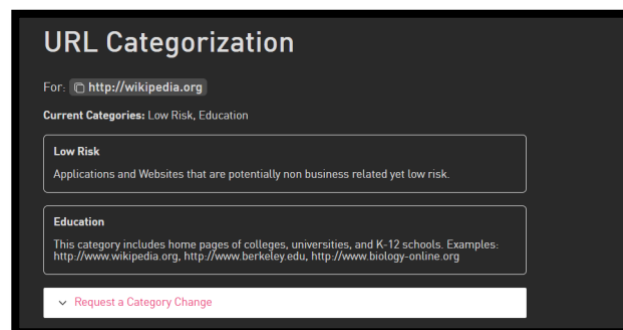
Exercise 3: URL Categorization

In this exercise, we will use the Check Point categorization portal to review categories and override default categories.

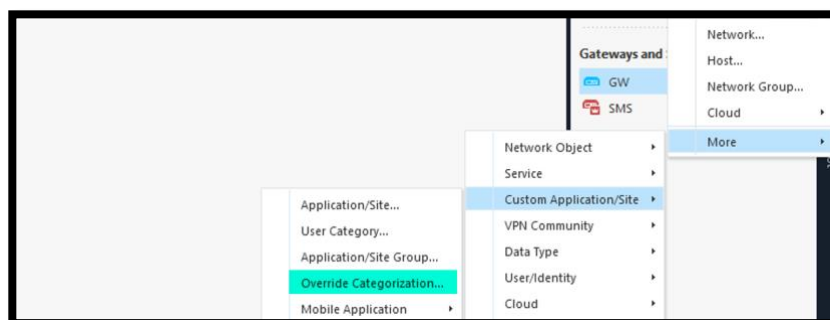
1. Open the Check Point URL categorization portal at <https://usercenter.checkpoint.com/ucapps/urlcat/> (login required).



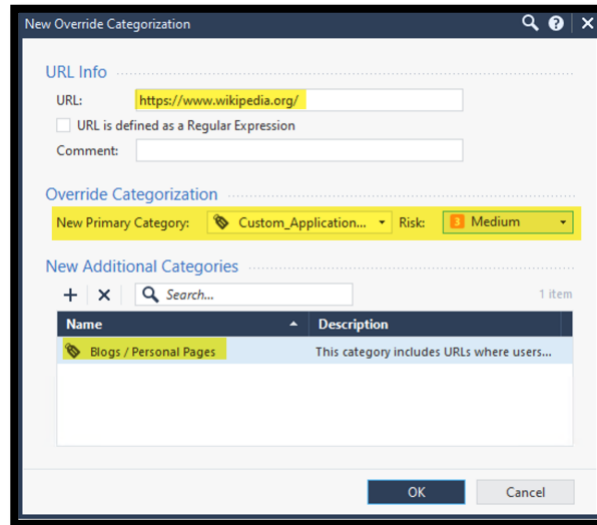
2. Enter the URL for any sites to test. try Wikipedia.org.



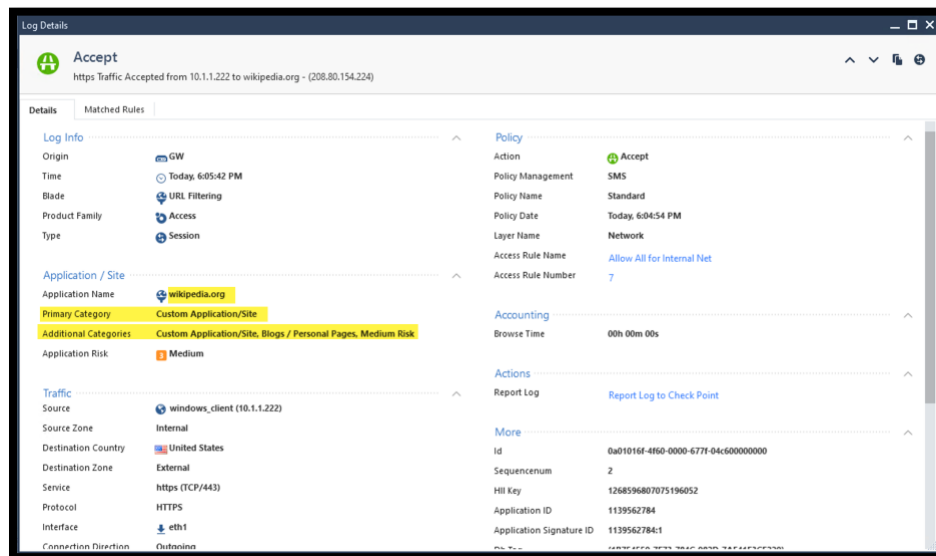
3. To override the default category, you can create a change request through the portal above. We can also override the default category using the "Override Categorization".



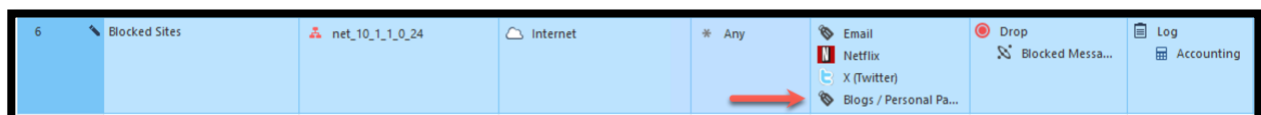
- The default category is **Custom_Application_Site** is set as the new primary category by default. Add an additional category and select **Blogs / Personal Pages**



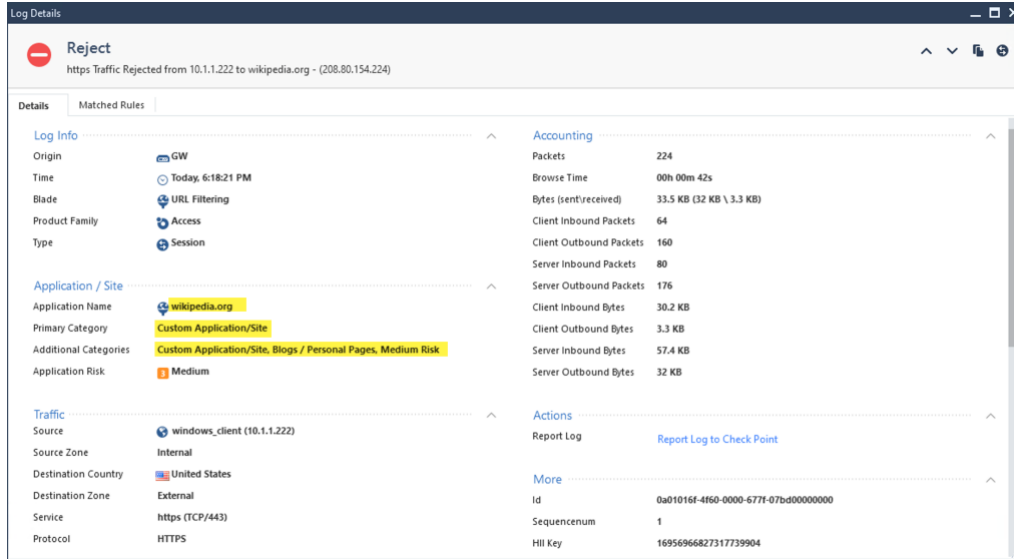
- Install the Access Control Policy.
- Try to access the site from **win_client** and review the log.



- Edit the existing **blocked Sites** rule and add the category **Blogs / Personal Pages**



8. Install the Access Policy.
9. Try to access **Wikipedia.org** from the **win_client** host. Review the logs and make sure we are seeing the expected category.



Log Details

Reject
https Traffic Rejected from 10.1.1.222 to wikipedia.org - (208.80.154.224)

Details | **Matched Rules**

Log Info

- Origin: GW
- Time: Today, 6:18:21 PM
- Blade: URL Filtering
- Product Family: Access
- Type: Session

Application / Site

- Application Name: wikipedia.org
- Primary Category: Custom Application/Site
- Additional Categories: Custom Application/Site, Blogs / Personal Pages, Medium Risk
- Application Risk: Medium

Traffic

- Source: windows_client (10.1.1.222)
- Source Zone: Internal
- Destination Country: United States
- Destination Zone: External
- Service: https (TCP/443)
- Protocol: HTTPS

Accounting

- Packets: 224
- Browse Time: 00h 00m 42s
- Bytes (sent/received): 33.5 KB (32 KB \ 3.3 KB)
- Client Inbound Packets: 64
- Client Outbound Packets: 160
- Server Inbound Packets: 80
- Server Outbound Packets: 176
- Client Inbound Bytes: 30.2 KB
- Client Outbound Bytes: 3.3 KB
- Server Inbound Bytes: 57.4 KB
- Server Outbound Bytes: 32 KB

Actions

- Report Log: [Report Log to Check Point](#)

More

- Id: 0a01016f-4f60-0000-677f-07bd00000000
- Sequencenum: 1
- Hll Key: 16956966827317739904

End of Lab 1