Application Control & URL Filtering

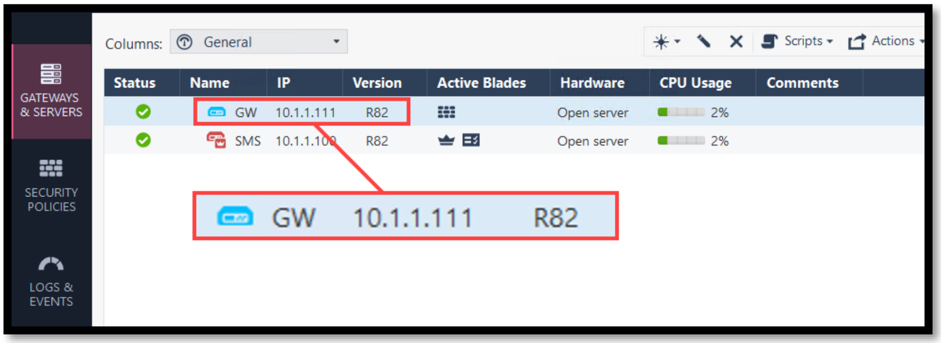
Introduction

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***.

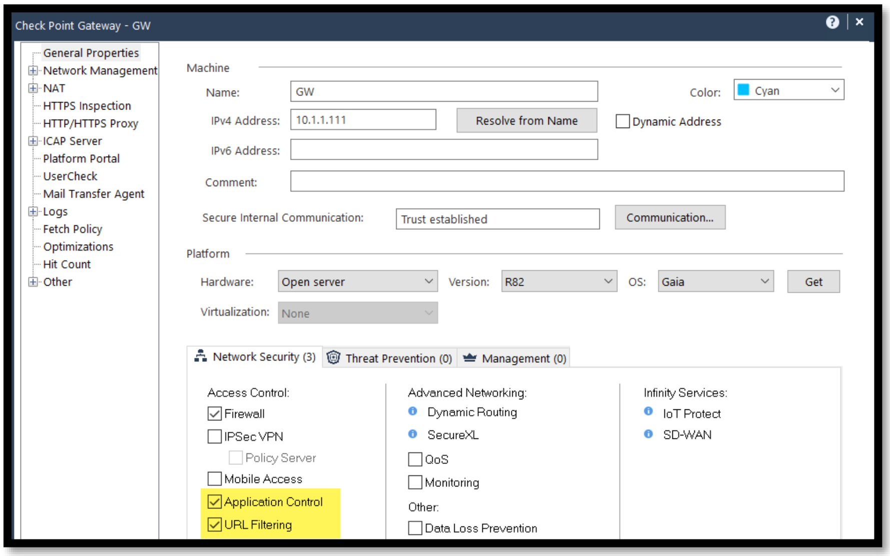
1. While connecting to the jump server, use SmartConsole to login to the Management server ***SMS***. Use the address 10.0.1.100 "***admin/Cpwins!1***" and edit the gateway object ***GW***.



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Comments
✓	GW	10.1.1.111	R82		Open server	2%	
✓	SMS	10.1.1.100	R82		Open server	2%	

GW 10.1.1.111 R82

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



Machine

Name: GW

Color: Cyan

IPv4 Address: 10.1.1.111

☐ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server Version: R82 OS: Gaia

Virtualization: None

Access Control:
☑ Firewall
☐ IPSec VPN
☐ Policy Server
☐ Mobile Access
☑ Application Control
☑ URL Filtering

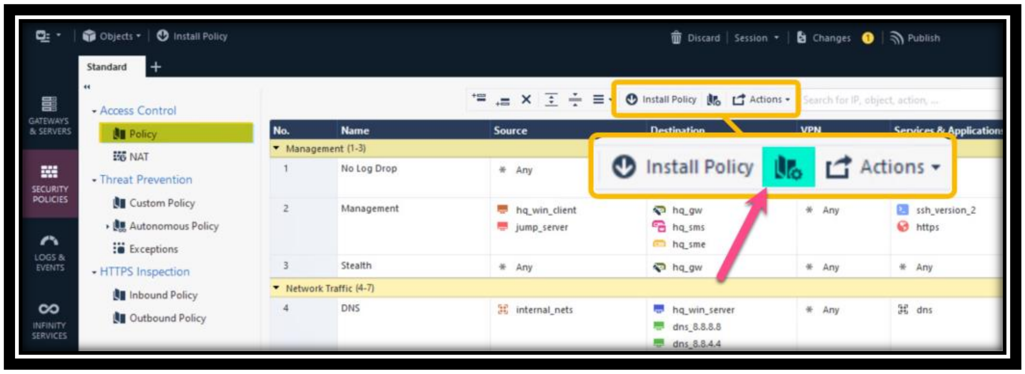
Advanced Networking:
Dynamic Routing
SecureXL
☐ QoS
☐ Monitoring

Other:
☐ Data Loss Prevention

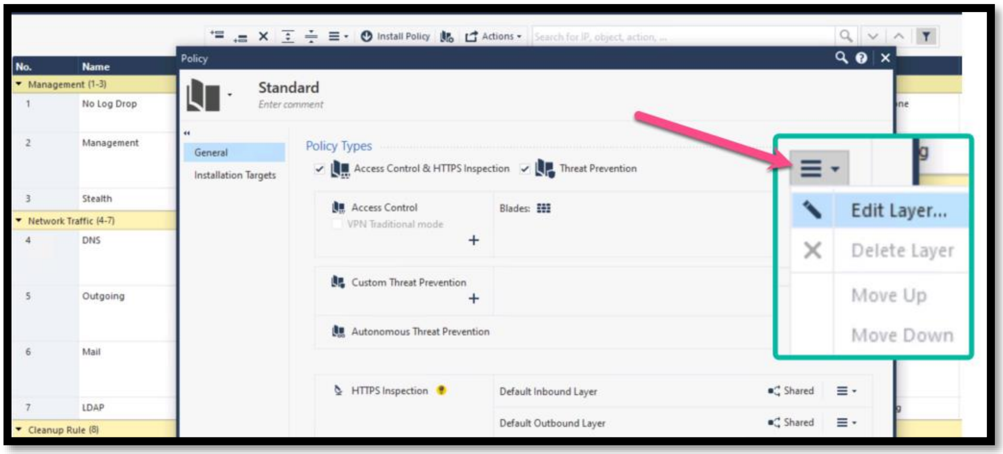
Infinity Services:
IoT Protect
SD-WAN

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

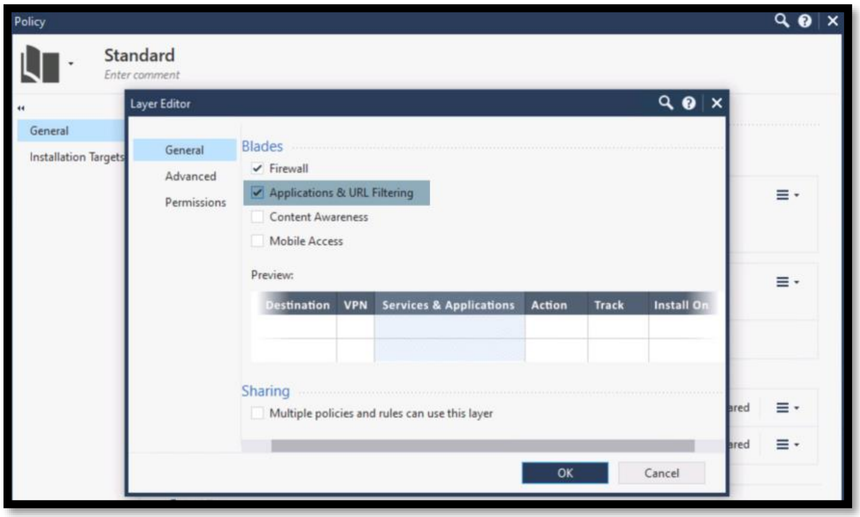
3. Navigate to the ***Policy*** tab. Click the icon to edit the ***Policy Package***.



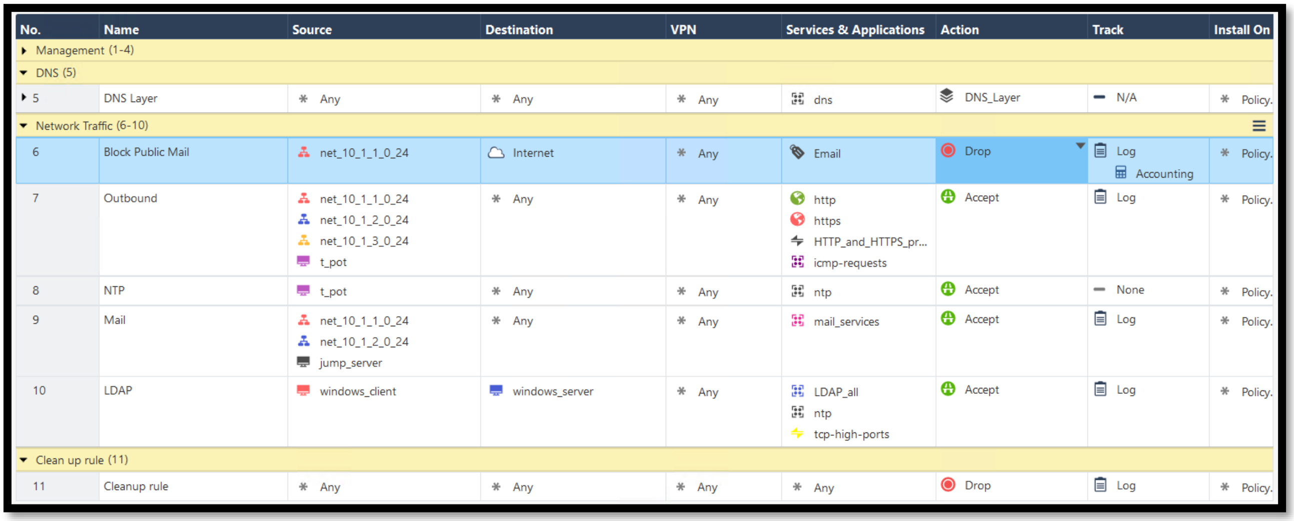
4. The Current default policy package has a single layer with only Firewall rules activated. Edit the layer as shown below.



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



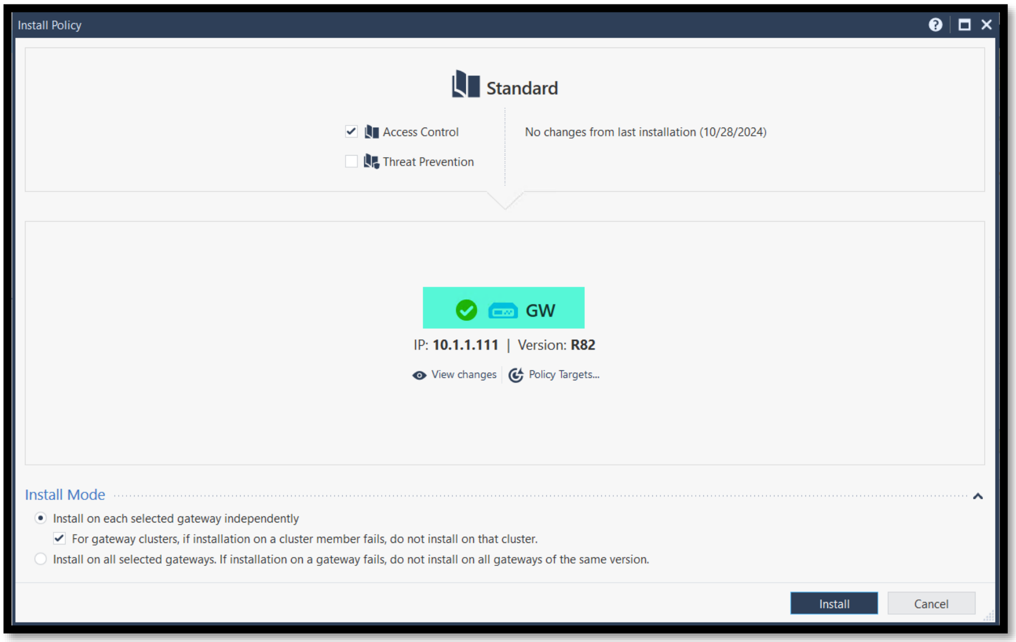
6. Create a new rule on top of the outbound rule. Use this rule to blocking hosts on the internal subnet **10.1.1.0/24** public Email web sites. Use the category ***Email***.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-4)								
DNS (5)								
5	DNS Layer	Any	Any	Any	dns	DNS_Layer	N/A	Policy.
Network Traffic (6-10)								
6	Block Public Mail	net_10_1_1_0_24	Internet	Any	Email	Drop	Log Accounting	Policy.
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_pr... icmp-requests	Accept	Log	Policy.
8	NTP	t_pot	Any	Any	ntp	Accept	None	Policy.
9	Mail	net_10_1_1_0_24 net_10_1_2_0_24 jump_server	Any	Any	mail_services	Accept	Log	Policy.
10	LDAP	windows_client	windows_server	Any	LDAP_all ntp tcp-high-ports	Accept	Log	Policy.
Clean up rule (11)								
11	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy.

- Two of the fields are containing 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.



Install Policy

Standard

☑ Access Control — No changes from last installation (10/28/2024)

☐ Threat Prevention

GW

IP: **10.1.1.111** | Version: **R82**

View changes | Policy Targets...

Install Mode

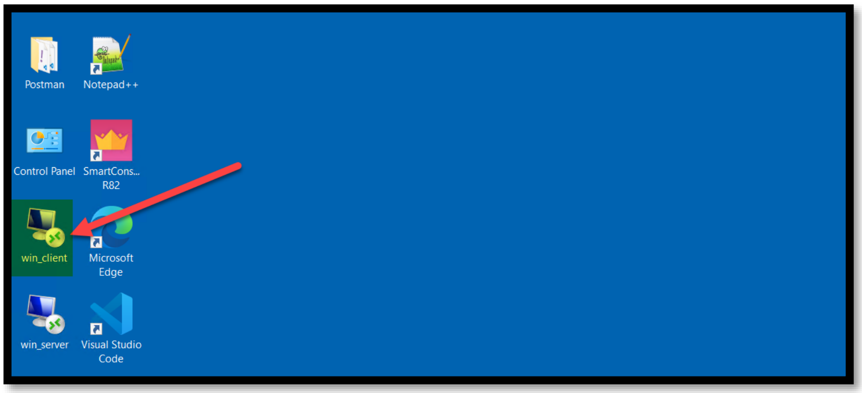
● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

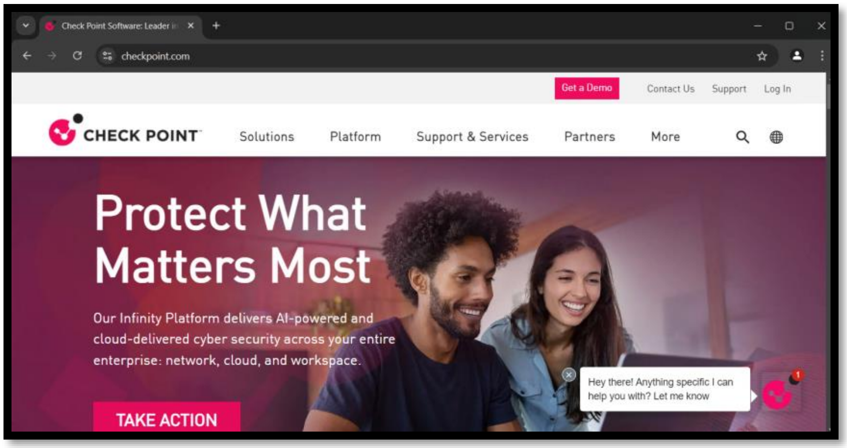
○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

Install | Cancel

8. Use the saved RDP to login to the ***win_client*** machine **10.0.1.222**. Use the account "***admin/Cpwins!1***"



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

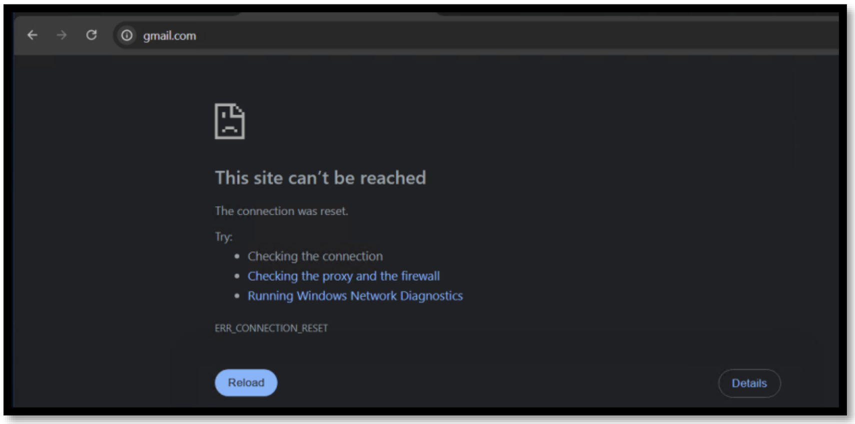


Protect What Matters Most

Our Infinity Platform delivers AI-powered and cloud-delivered cyber security across your entire enterprise: network, cloud, and workspace.

Hey there! Anything specific I can help you with? Let me know

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



This site can't be reached

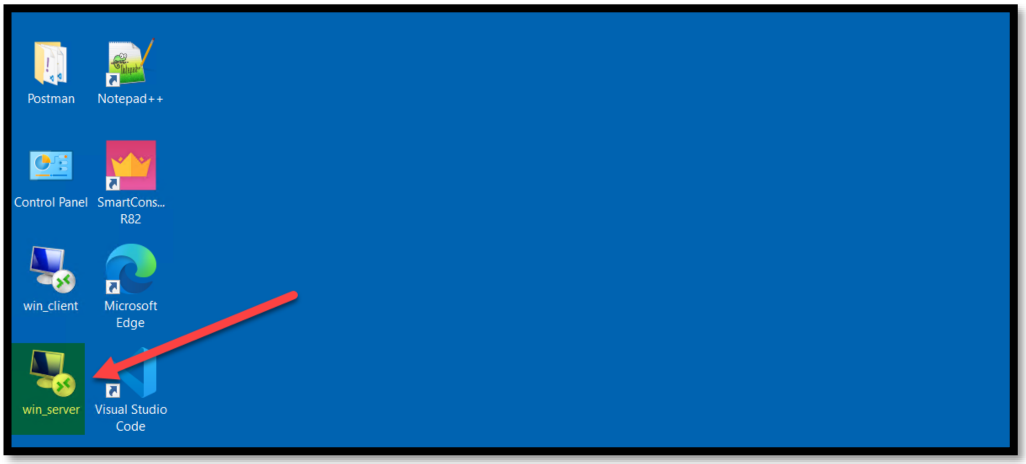
The connection was reset.

Try:

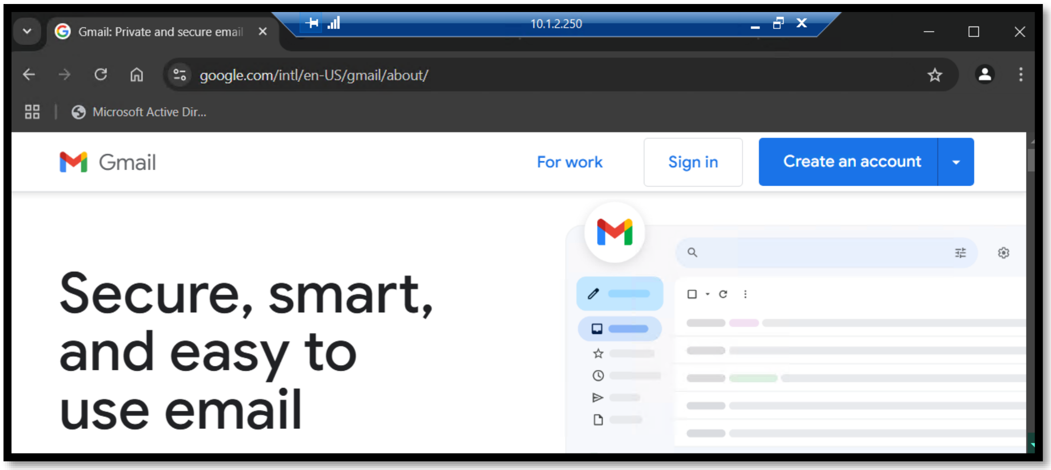
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

11. Connect to the domain controller (win-server) using the session on desktop.

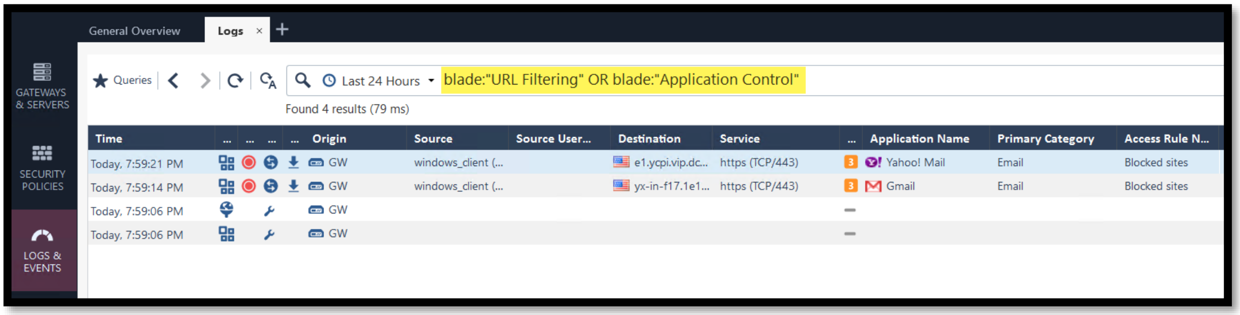


12. Try accessing Gmail or any other public Email service. Notice that this subnet is still able to access Gamil successfully according to the policy.


Gmail: Private and secure email
10.1.2.250
google.com/intl/en-US/gmail/about/
Microsoft Active Dir...
Gmail
For work
Sign in
Create an account
Secure, smart, and easy to use email

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"



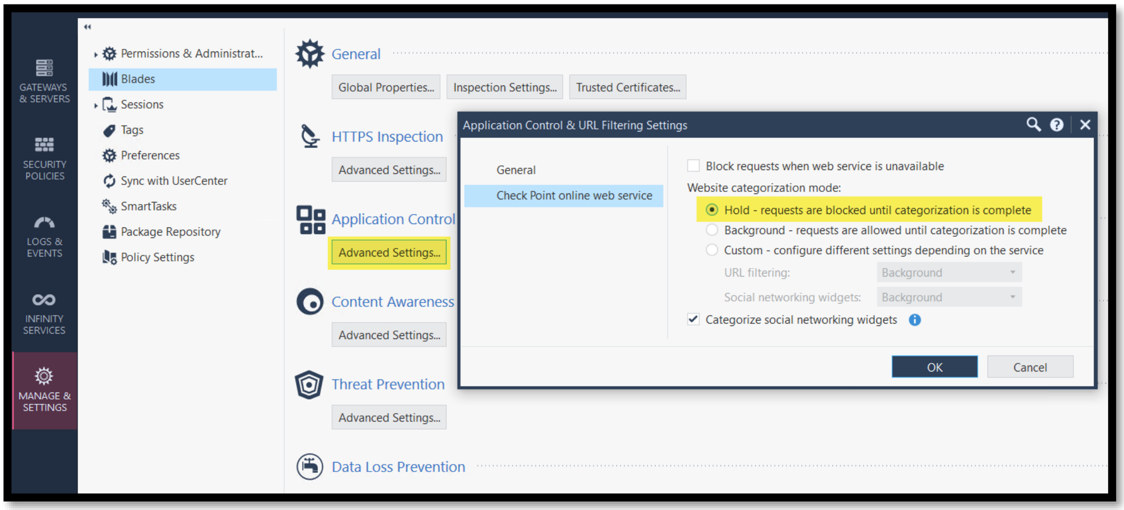
blade:"URL Filtering" OR blade:"Application Control"

Found 4 results (79 ms)

Time	...	...	...	...	Origin	Source	Source User...	Destination	Service	...	Application Name	Primary Category	Access Rule N...
Today, 7:59:21 PM					GW	windows_client (...		e1.ycpi.vip.dc...	https (TCP/443)	3	Yahoo! Mail	Email	Blocked sites
Today, 7:59:14 PM					GW	windows_client (...		yx-in-f17.1e1...	https (TCP/443)	3	Gmail	Email	Blocked sites
Today, 7:59:06 PM					GW					—			
Today, 7:59:06 PM					GW					—			

In case the website categorization is unknown to the Gateway, the resource adviser daemon (RAD) sends a request to 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**.



Application Control & URL Filtering Settings

General
Check Point online web service

□ Block requests when web service is unavailable

Website categorization mode:

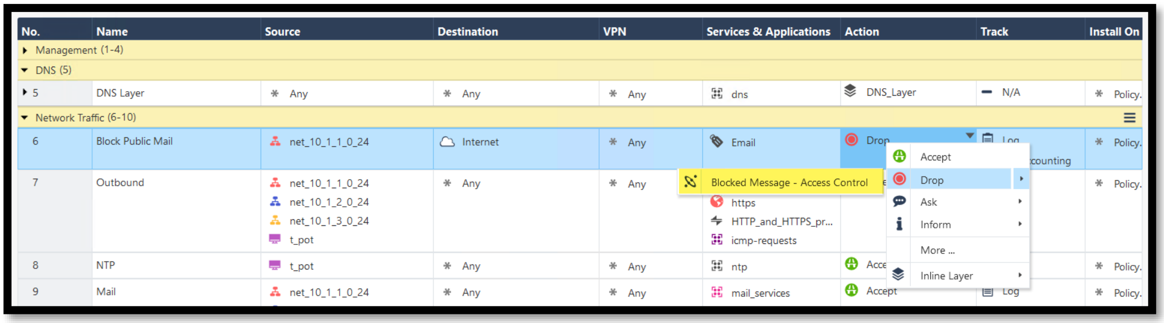
● Hold - requests are blocked until categorization is complete
○ Background - requests are allowed until categorization is complete
○ Custom - configure different settings depending on the service

URL filtering: Background
Social networking widgets: Background

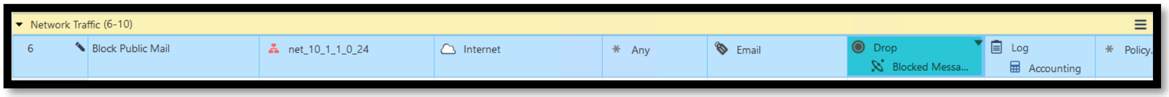
☑ Categorize social networking widgets

OK Cancel

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



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Management (1-4)								
DNS (5)								
5	DNS Layer	Any	Any	Any	dns	DNS_Layer	N/A	Policy.
Network Traffic (6-10)								
6	Block Public Mail	net_10_1_1_0_24	Internet	Any	Email	Drop	Log counting	Policy.
7	Outbound	net_10_1_1_0_24 net_10_1_2_0_24 net_10_1_3_0_24 t_pot	Any	Any	https HTTP_and_HTTPS_pr... icmp-requests			Policy.
8	NTP	t_pot	Any	Any	ntp	Acce		Policy.
9	Mail	net_10_1_1_0_24	Any	Any	mail_services	Accept	Log	Policy.

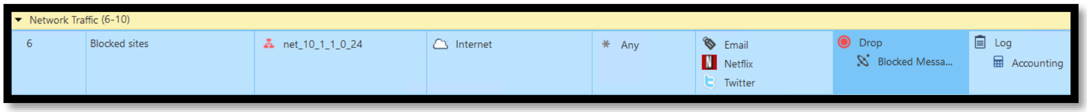


Network Traffic (6-10)								
6	Block Public Mail	net_10_1_1_0_24	Internet	Any	Email	Drop Blocked Messa...	Log Accounting	Policy.

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.

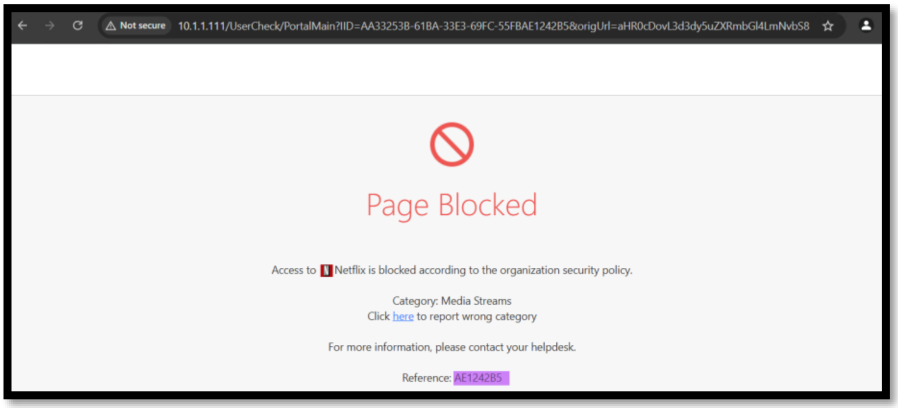
15. Edit the rule and add two more applications to be blocked, Netflix and Twitter. Install the access policy.



Network Traffic (6-10)

6	Blocked sites	net_10_1_1_0_24	Internet	Any	Email Netflix Twitter	Drop Blocked Messa...	Log Accounting

16. Notice that a block message is now returned.



Not secure 10.1.1.111/UserCheck/PortalMain?IID=AA33253B-61BA-33E3-69FC-55FBAE1242B5&origUrl=aHR0cDovL3d3dy5uZXRmbGl4LmNvbS8

Page Blocked

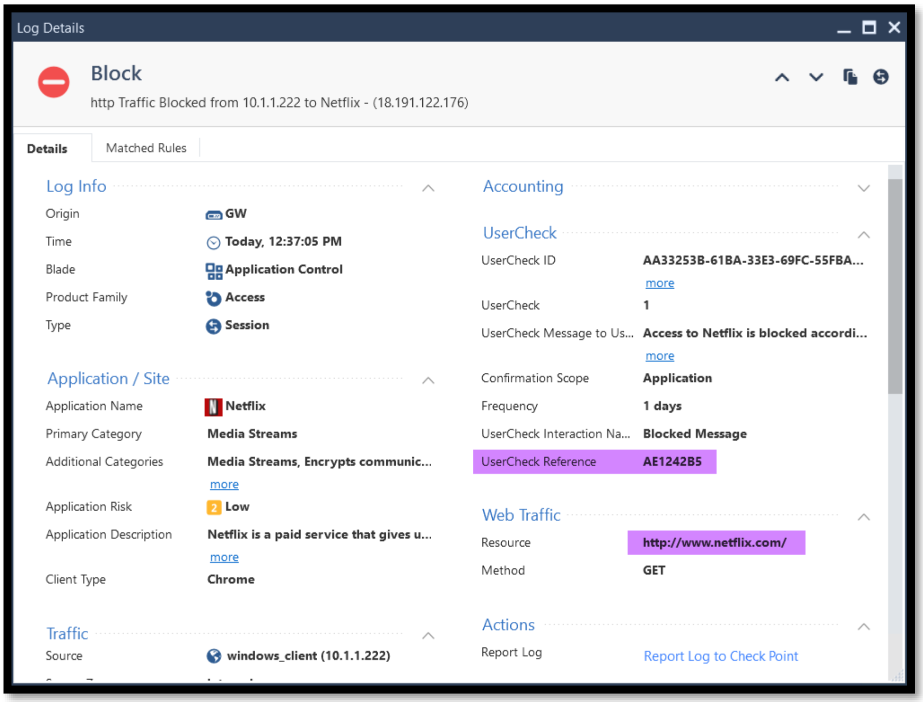
Access to Netflix is blocked according to the organization security policy.

Category: Media Streams
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: AE1242B5

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.



Log Details

Block
http Traffic Blocked from 10.1.1.222 to Netflix - (18.191.122.176)

Log Info
Origin: GW
Time: Today, 12:37:05 PM
Blade: Application Control
Product Family: Access
Type: Session

Application / Site
Application Name: Netflix
Primary Category: Media Streams
Additional Categories: Media Streams, Encrypts communic... more
Application Risk: 2 Low
Application Description: Netflix is a paid service that gives u... more
Client Type: Chrome

Traffic
Source: windows_client (10.1.1.222)

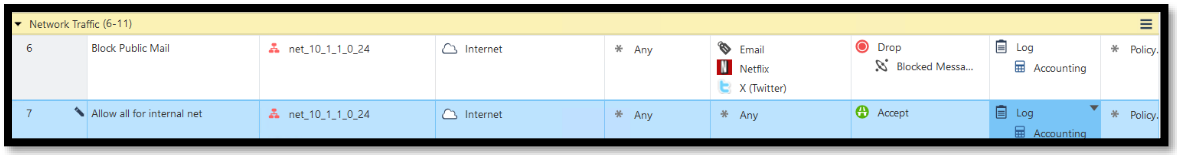
Accounting

UserCheck
UserCheck ID: AA33253B-61BA-33E3-69FC-55FBA... more
UserCheck: 1
UserCheck Message to Us...: Access to Netflix is blocked accordi... more
Confirmation Scope: Application
Frequency: 1 days
UserCheck Interaction Na...: Blocked Message
UserCheck Reference: AE1242B5

Web Traffic
Resource: http://www.netflix.com/
Method: GET

Actions
Report Log: Report Log to Check Point

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**.

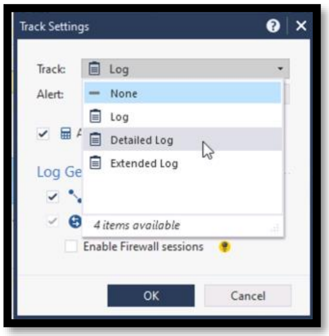


Network Traffic (6-11)

6	Block Public Mail	net_10_1_1_0_24	Internet	Any	Email Netflix X (Twitter)	Drop Blocked Messa...	Log Accounting	Policy.
7	Allow all for internal net	net_10_1_1_0_24	Internet	Any	Any	Accept	Log Accounting	Policy.

19. 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 category or Application in the rule we created.
    - The log field is set to the default "Log"
    - We need to use a different log option to be able to see the application names in the logs.

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



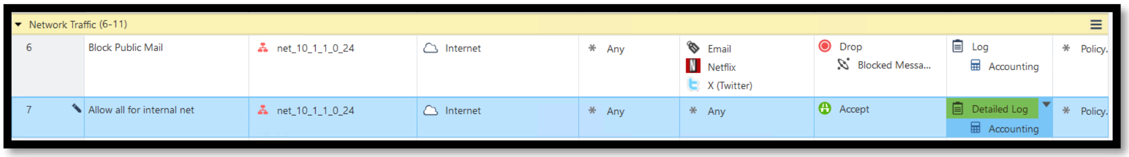
Track Settings

Track: Log

Alert:

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***.

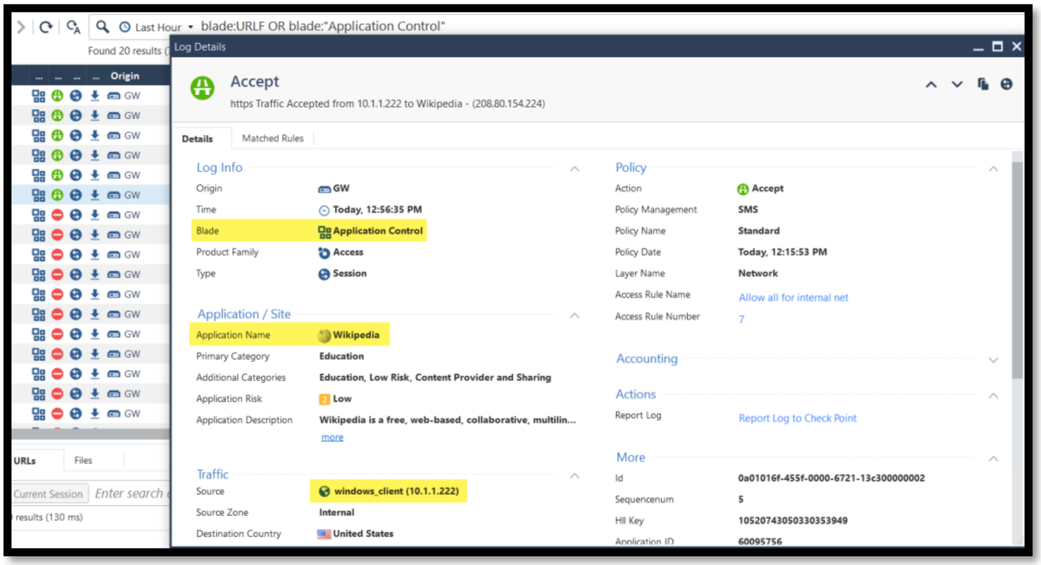
21. The rule base should have **Detailed Log** selected in the ***Track*** column. Install the access policy.



Network Traffic (6-11)

6	Block Public Mail	net_10_1_1_0_24	Internet	Any	Email Netflix X (Twitter)	Drop Blocked Messa...	Log Accounting	Policy.
7	Allow all for internal net	net_10_1_1_0_24	Internet	Any	Any	Accept	Detailed Log Accounting	Policy.

22. 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.



blade:URLF OR blade:"Application Control"

Accept
https Traffic Accepted from 10.1.1.222 to Wikipedia - (208.80.154.224)

Log Info

Origin	GW
Time	Today, 12:56:35 PM
Blade	Application Control
Product Family	Access
Type	Session

Application / Site

Application Name	Wikipedia
Primary Category	Education
Additional Categories	Education, Low Risk, Content Provider and Sharing
Application Risk	2 Low
Application Description	Wikipedia is a free, web-based, collaborative, multilin...

Traffic

Source	windows_client (10.1.1.222)
Source Zone	Internal
Destination Country	United States

Policy

Action	Accept
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 12:15:53 PM
Layer Name	Network
Access Rule Name	Allow all for internal net
Access Rule Number	7

Accounting

Actions

Report Log	Report Log to Check Point

More

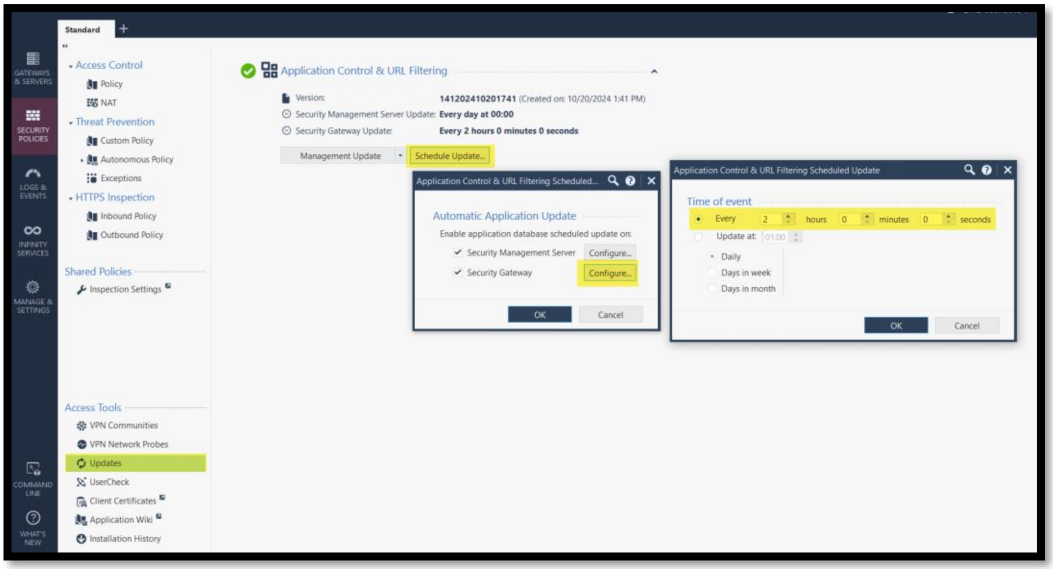
Id	0a01016f-455f-0000-6721-13c300000002
Sequencenum	5
Hll Key	10520743050330353949
Application ID	60095756

Exercise 2: Engine Updates

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

1. Navigate to the update section and review the default "Schedule Update" settings for both GW and the SMS.

    - Notice that the management servers check for updates every day at midnight while the GW fetches update every 2 hours.



Application Control & URL Filtering

Version:	141202410201741 (Created on: 10/20/2024 1:41 PM)
Security Management Server Update:	Every day at 00:00
Security Gateway Update:	Every 2 hours 0 minutes 0 seconds

Application Control & URL Filtering Scheduled...

Automatic Application Update

Enable application database scheduled update on:

☑ Security Management Server

☑ Security Gateway

Application Control & URL Filtering Scheduled Update

Time of event

● Every 2 hours 0 minutes 0 seconds

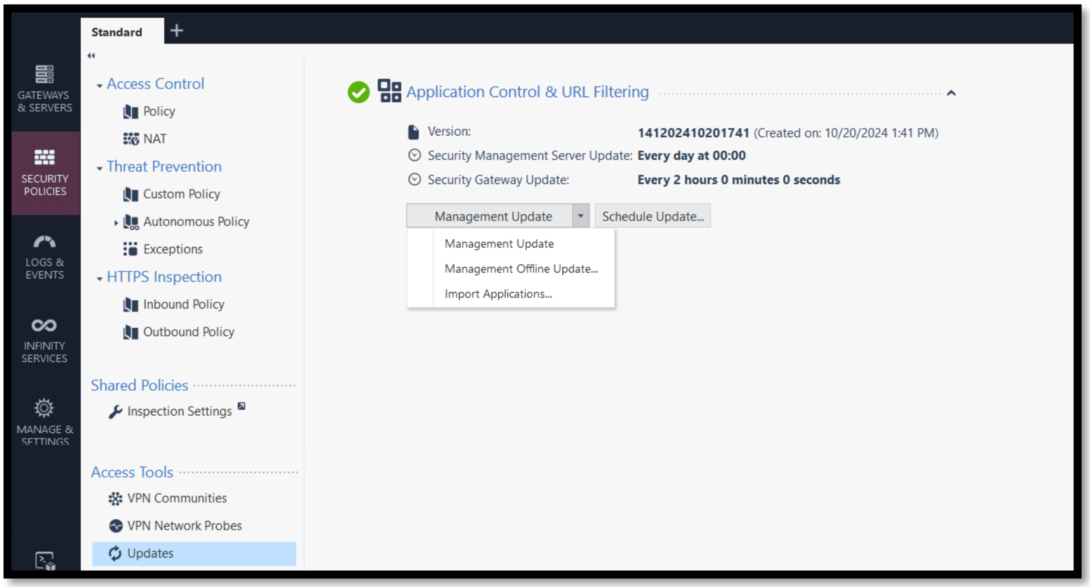
○ Update at: 01:00

● Daily

○ Days in week

○ Days in month

2. Click the dropdown menu next to "Management Update" and check the available option to update the URLF and Application control database on the management server.



Version: 141202410201741 (Created on: 10/20/2024 1:41 PM)

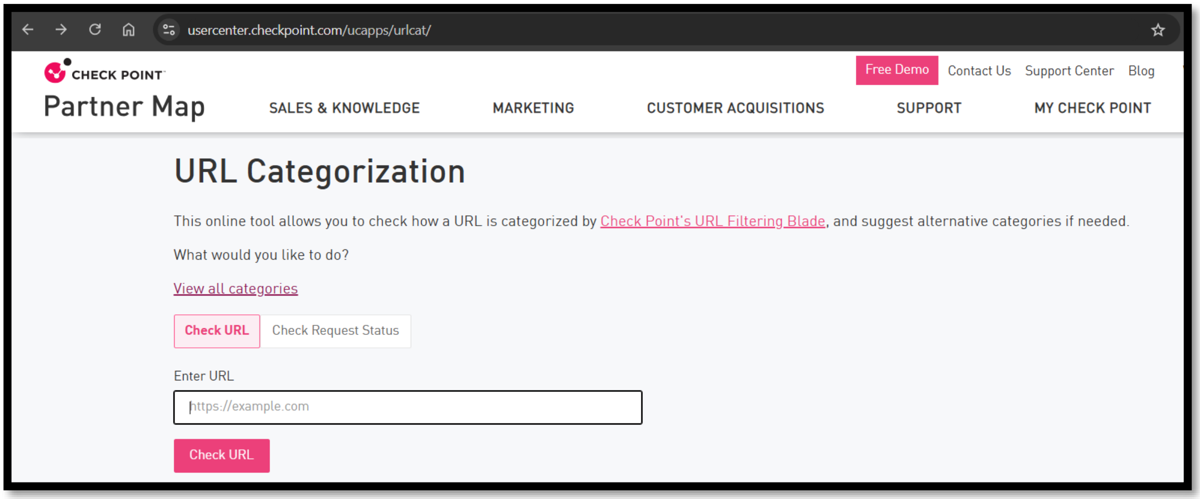
Security Management Server Update: Every day at 00:00

Security Gateway Update: Every 2 hours 0 minutes 0 seconds

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).

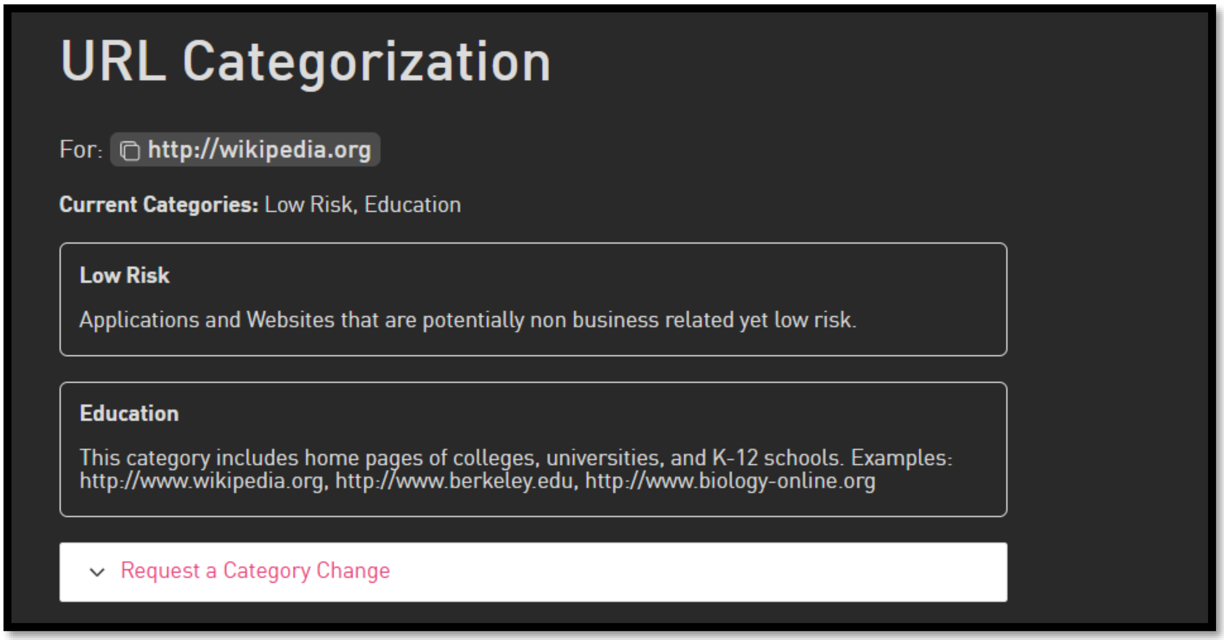


URL Categorization

This online tool allows you to check how a URL is categorized by Check Point's URL Filtering Blade, and suggest alternative categories if needed.

What would you like to do?

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



URL Categorization

For: http://wikipedia.org

Current Categories: Low Risk, Education

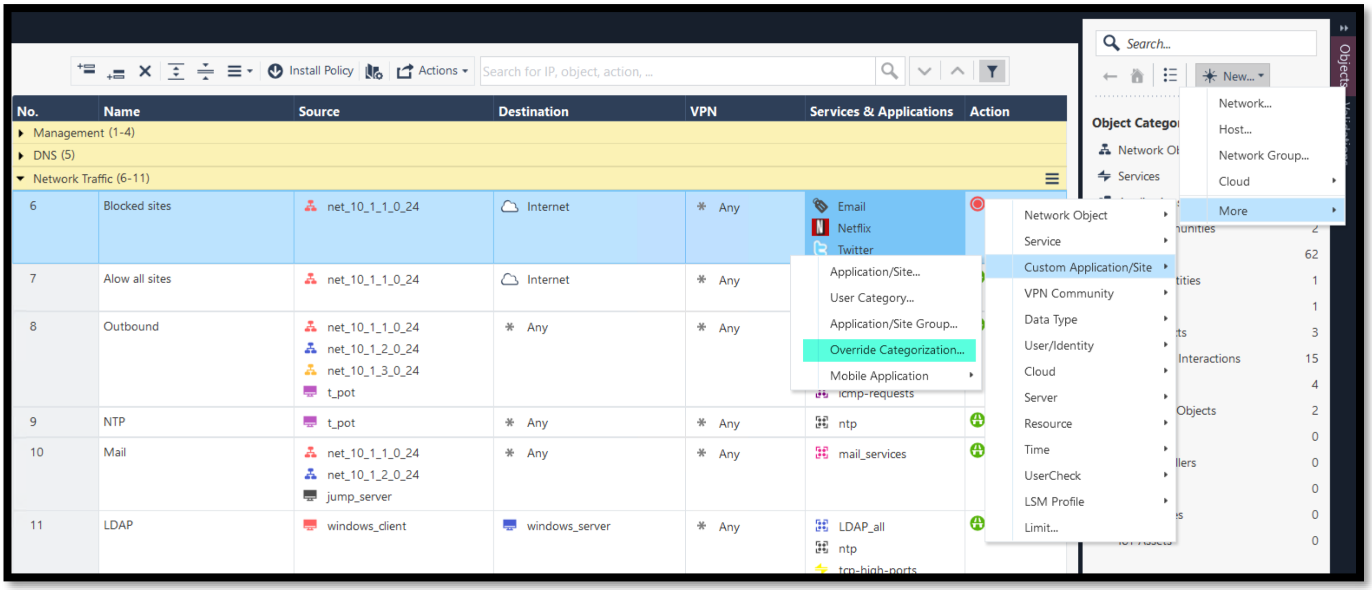
Low Risk

Applications and Websites that are potentially non business related yet low risk.

Education

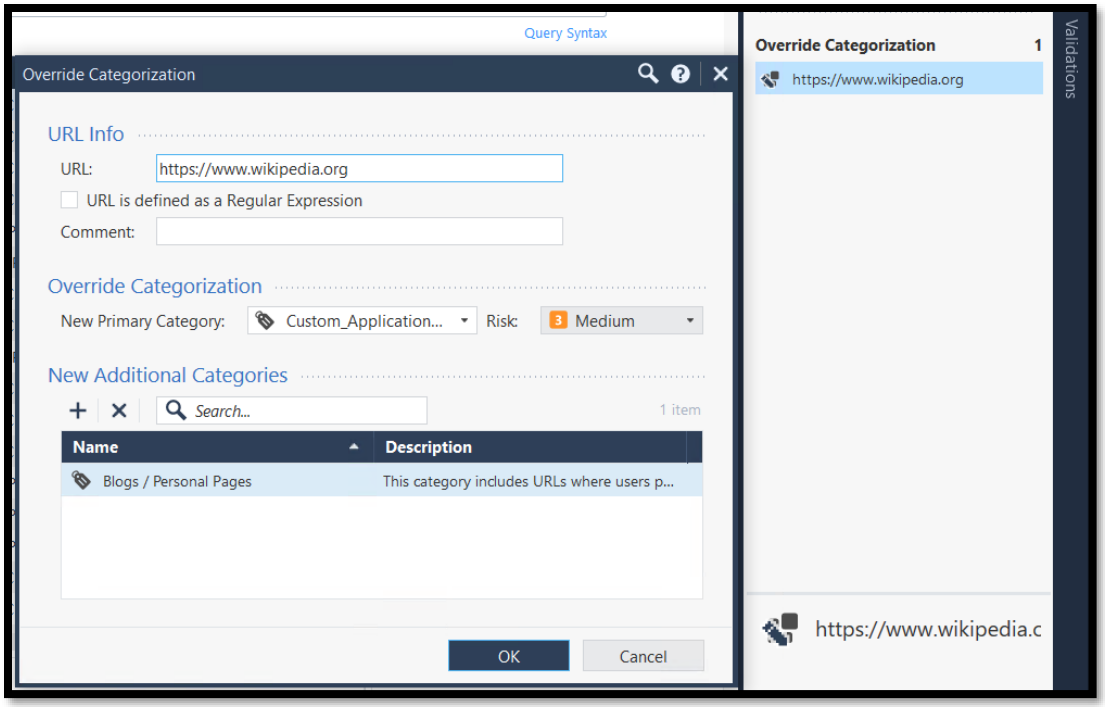
This category includes home pages of colleges, universities, and K-12 schools. Examples: http://www.wikipedia.org, http://www.berkeley.edu, http://www.biology-online.org

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".



No.	Name	Source	Destination	VPN	Services & Applications	Action
Management (1-4)						
DNS (5)						
Network Traffic (6-11)						
6	Blocked sites	net_10_1_1_0_24	Internet	Any	Email Netflix Twitter	
7	Alow all sites	net_10_1_1_0_24	Internet	Any		
8	Outbound	net_10_1_1_0_24 net_10_1_2_0_24 net_10_1_3_0_24 t_pot	Any	Any	icmp-requests	
9	NTP	t_pot	Any	Any	ntp	
10	Mail	net_10_1_1_0_24 net_10_1_2_0_24 jump_server	Any	Any	mail_services	
11	LDAP	windows_client	windows_server	Any	LDAP_all ntp tcp-high-ports	

4. 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"



URL Info

URL: https://www.wikipedia.org

□ URL is defined as a Regular Expression

Comment:

Override Categorization

New Primary Category: Custom_Application... Risk: 3 Medium

New Additional Categories

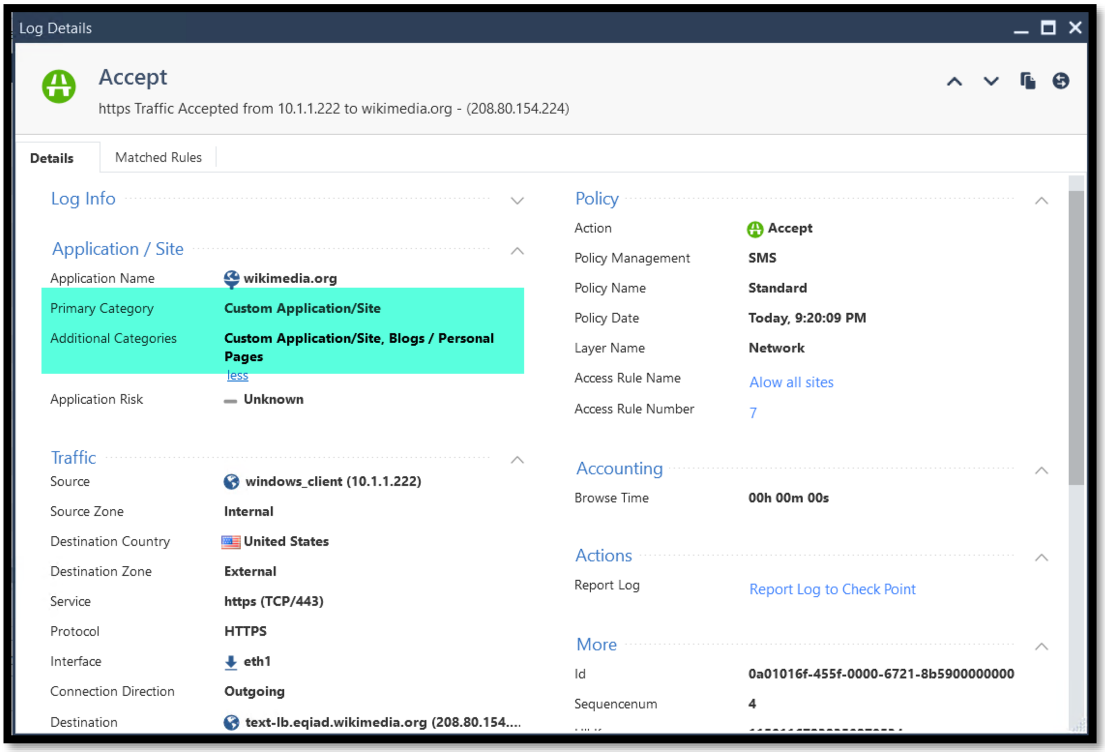
Search... 1 item

Name	Description
Blogs / Personal Pages	This category includes URLs where users p...

Override Categorization 1
https://www.wikipedia.org

https://www.wikipedia.c

5. Try to access the site from win_client and review the log.
    - Note that we can use any of the categories in the security policy



Accept

https Traffic Accepted from 10.1.1.222 to wikimedia.org - (208.80.154.224)

Log Info

Application / Site

Application Name	wikimedia.org
Primary Category	Custom Application/Site
Additional Categories	Custom Application/Site, Blogs / Personal Pages less
Application Risk	Unknown

Traffic

Source	windows_client (10.1.1.222)
Source Zone	Internal
Destination Country	United States
Destination Zone	External
Service	https (TCP/443)
Protocol	HTTPS
Interface	eth1
Connection Direction	Outgoing
Destination	text-lb.eqiad.wikimedia.org (208.80.154....

Policy

Action	Accept
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 9:20:09 PM
Layer Name	Network
Access Rule Name	Allow all sites
Access Rule Number	7

Accounting

Browse Time	00h 00m 00s

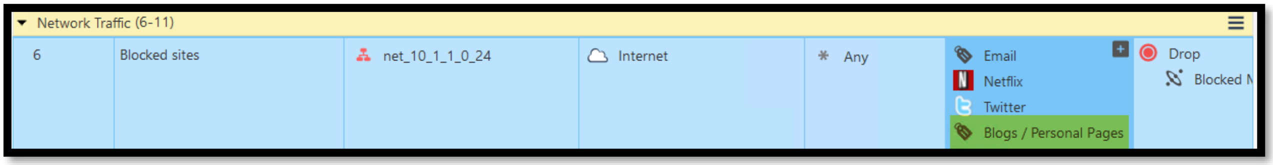
Actions

Report Log	Report Log to Check Point

More

Id	0a01016f-455f-0000-6721-8b5900000000
Sequencenum	4

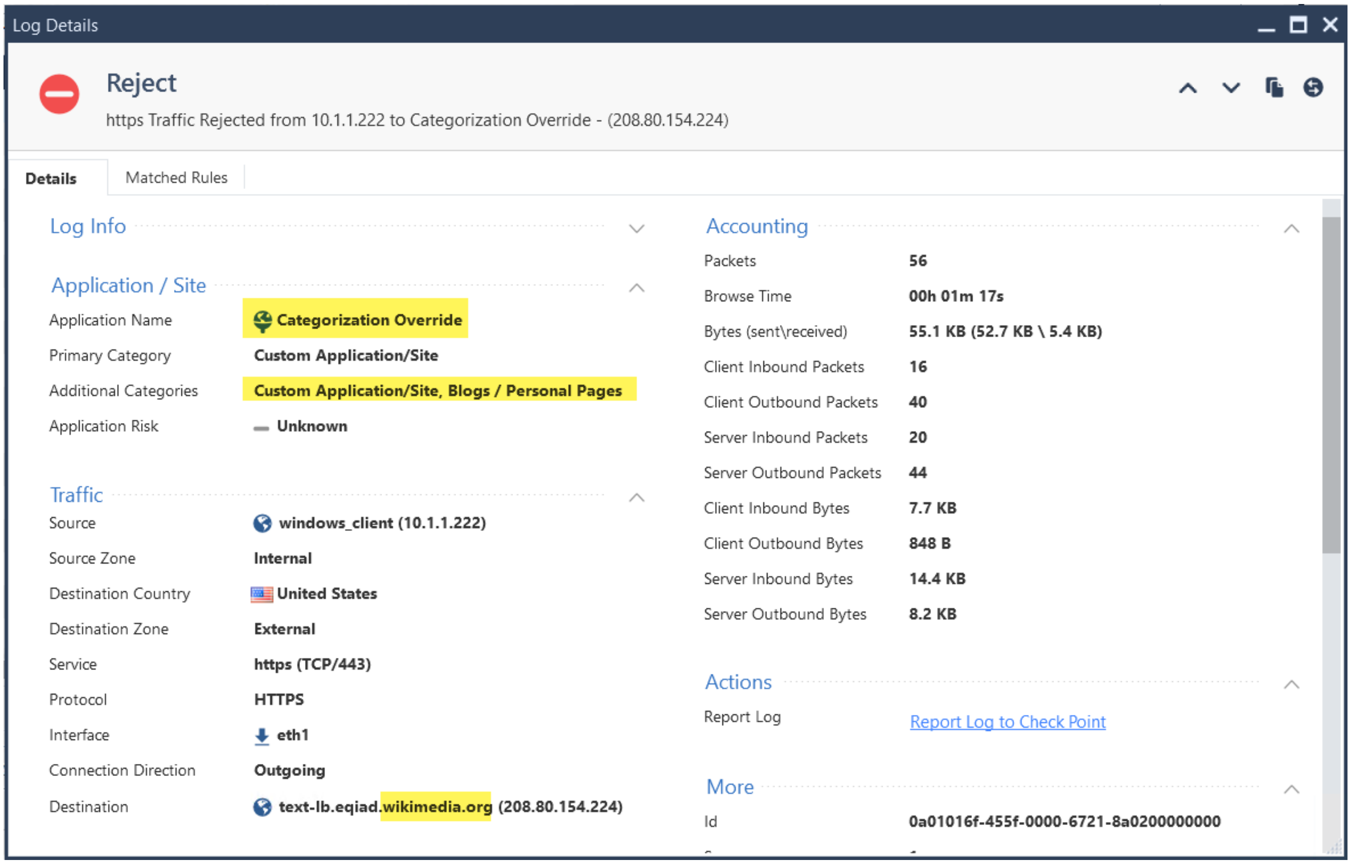
6. Edit the existing block rule and add the additional category we used in the override categorization object we created in the previous step and install the Access Policy.



Network Traffic (6-11)

6	Blocked sites	net_10_1_1_0_24	Internet	Any	Email Netflix Twitter Blogs / Personal Pages	Drop Blocked M

7. Try to access Wikipedia.org from win_client. Review the logs and make sure we are seeing the expected category.



Log Details

Reject

https Traffic Rejected from 10.1.1.222 to Categorization Override - (208.80.154.224)

Details | Matched Rules

Log Info

Application / Site

Application Name	Categorization Override
Primary Category	Custom Application/Site
Additional Categories	Custom Application/Site, Blogs / Personal Pages
Application Risk	Unknown

Traffic

Source	windows_client (10.1.1.222)
Source Zone	Internal
Destination Country	United States
Destination Zone	External
Service	https (TCP/443)
Protocol	HTTPS
Interface	eth1
Connection Direction	Outgoing
Destination	text-lb.eqiad.wikimedia.org (208.80.154.224)

Accounting

Packets	56
Browse Time	00h 01m 17s
Bytes (sent\received)	55.1 KB (52.7 KB \ 5.4 KB)
Client Inbound Packets	16
Client Outbound Packets	40
Server Inbound Packets	20
Server Outbound Packets	44
Client Inbound Bytes	7.7 KB
Client Outbound Bytes	848 B
Server Inbound Bytes	14.4 KB
Server Outbound Bytes	8.2 KB

Actions

Report Log	Report Log to Check Point

More

Id	0a01016f-455f-0000-6721-8a0200000000

End of Lab 1