HTTPS Inspection

Expected Time: 50 Minutes

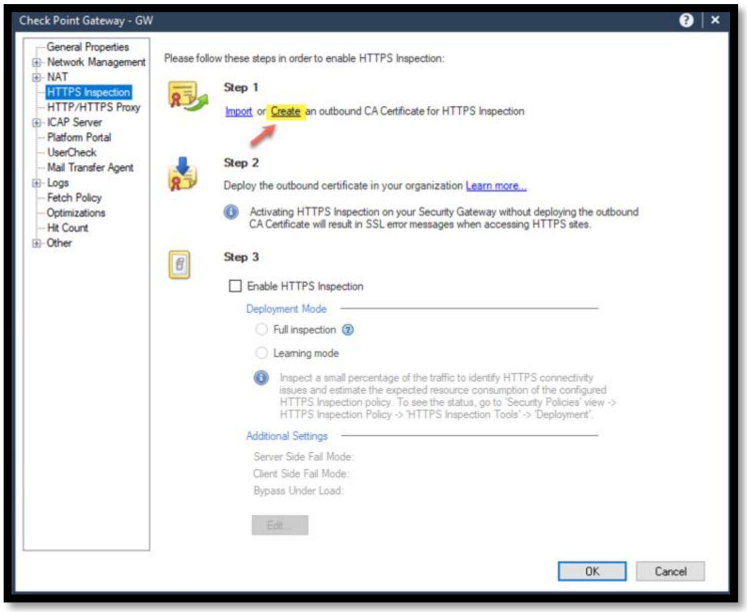
Introduction

In this lab, we will enable the HTTPS Inspection blades. HTTPS Inspection adds the capabilities to decrypt and inspect encrypted HTTPS sites.

Exercise 1: Onboarding

In this exercise, we will enable the HTTPS Inspection 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 **10.1.1.100** and the credentials ***admin/Cpwins!1*** and edit the gateway object **GW**. From the Global Properties menu, select **HTTPS Inspection**.



Check Point Gateway - GW

Please follow these steps in order to enable HTTPS Inspection:

Step 1

Import or Create an outbound CA Certificate for HTTPS Inspection

Step 2

Deploy the outbound certificate in your organization Learn more...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

☐ Enable HTTPS Inspection

Deployment Mode

○ Full inspection

○ Learning mode

Inspect a small percentage of the traffic to identify HTTPS connectivity issues and estimate the expected resource consumption of the configured HTTPS Inspection policy. To see the status, go to 'Security Policies' view -> HTTPS Inspection Policy -> 'HTTPS Inspection Tools' -> 'Deployment'.

Additional Settings

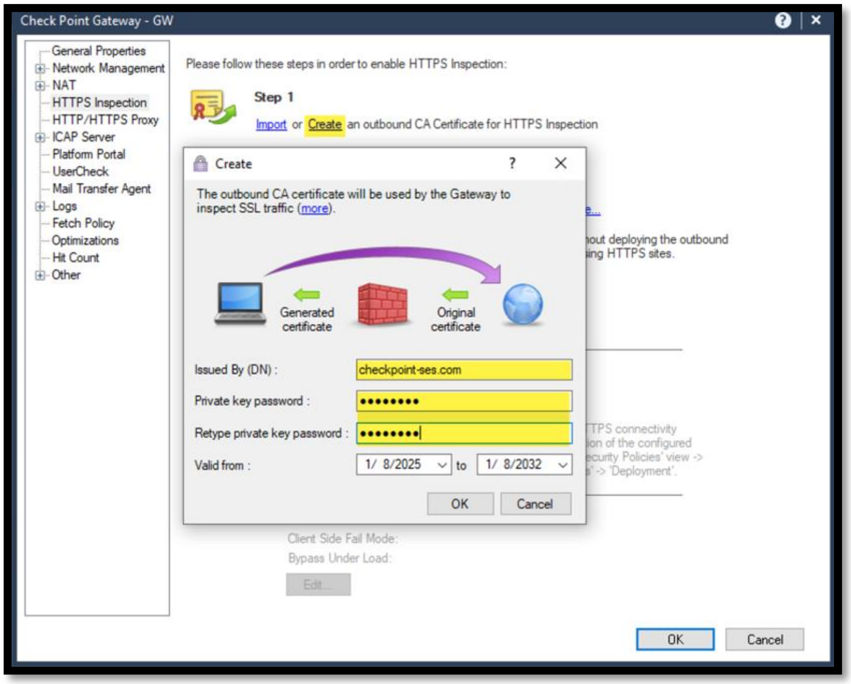
Server Side Fail Mode:

Client Side Fail Mode:

Bypass Under Load:

2. Under **Step 1,** click **Create** and fill in the details for the root certificate and click OK to create the certificate.

   a. Note that this certificate is a self-signed CA. This certificate is untrusted publicly by default.
   b. Generally, public vendors will not be able to provide their own trusted Certificate Authority certificate.
   c. It is common to import a trusted CA from an internal CA. for example, in an AD environment, the trusted CA from the domain controller is imported to issue certificates. The issued certificate will be trusted by all hosts that are part of this AD domain.



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Import or Create an outbound CA Certificate for HTTPS Inspection

The outbound CA certificate will be used by the Gateway to inspect SSL traffic (more).

Issued By (DN) : checkpoint-ses.com

Private key password : ••••••••

Retype private key password : ••••••••

Valid from : 1/ 8/2025 to 1/ 8/2032

...out deploying the outbound ...ing HTTPS sites.

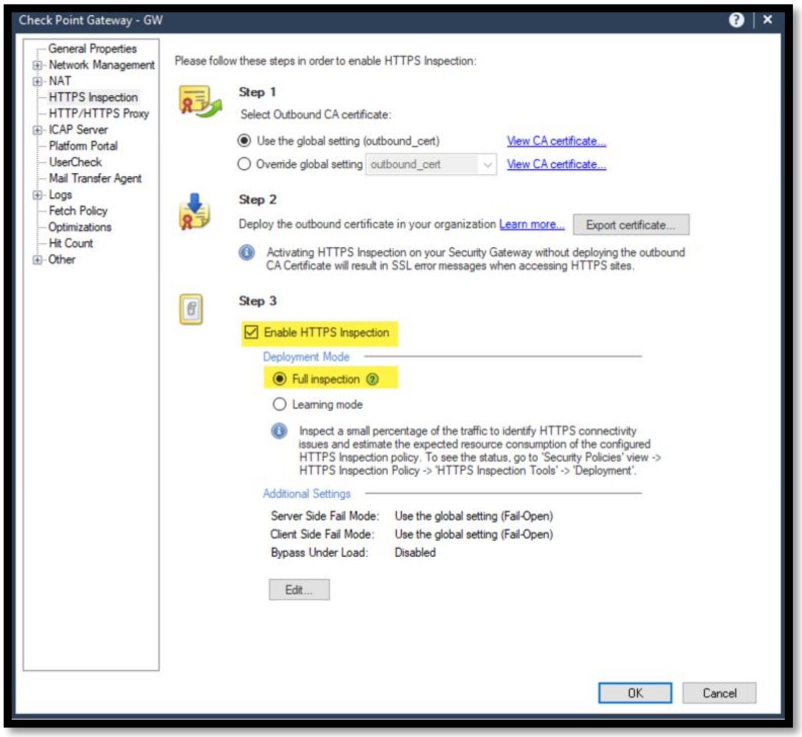
...TTPS connectivity ...ion of the configured ...ecurity Policies' view -> ...' -> 'Deployment'.

Client Side Fail Mode:

Bypass Under Load:

Note that this certificate will be used by the GW to issue certificate mimicking the server certificate while inspect HTTPS traffic.

3. Skip **Step 2** for now, we will export the certificate in a later step. Under **Step 3** check the option **Enable HTTPS Inspection** and select **Full Inspection.** click **OK** to close the object.



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Select Outbound CA certificate:

● Use the global setting (outbound_cert)

○ Override global setting outbound_cert

Step 2

Deploy the outbound certificate in your organization

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

☑ Enable HTTPS Inspection

Deployment Mode

● Full inspection

○ Learning mode

Inspect a small percentage of the traffic to identify HTTPS connectivity issues and estimate the expected resource consumption of the configured HTTPS Inspection policy. To see the status, go to 'Security Policies' view -> HTTPS Inspection Policy -> 'HTTPS Inspection Tools' -> 'Deployment'.

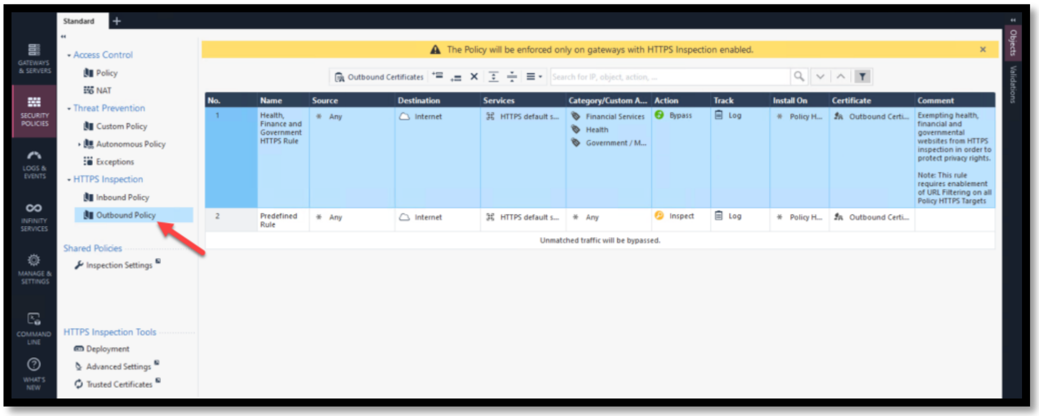
Additional Settings

Server Side Fail Mode: Use the global setting (Fail-Open)

Client Side Fail Mode: Use the global setting (Fail-Open)

Bypass Under Load: Disabled

4. Under **HTTPS Inspection**, review the default **Outbound Policy**. Notice the categories bypassed by the first rule. The second rule **inspect** all outbound web traffic by default.

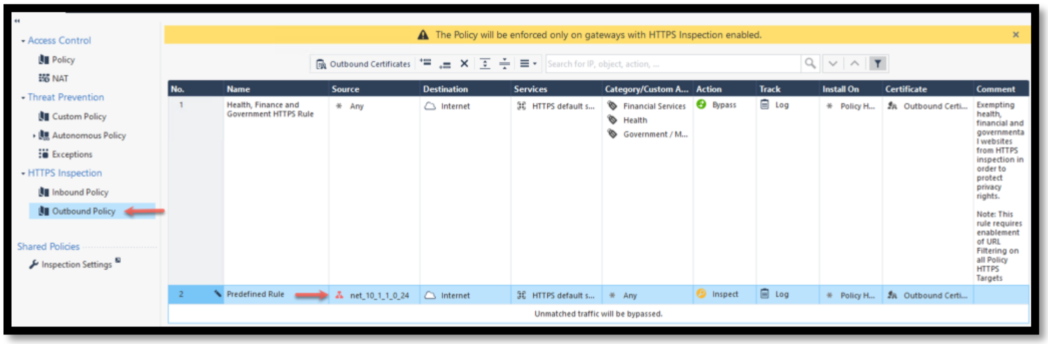


The Policy will be enforced only on gateways with HTTPS Inspection enabled.

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate	Comment
1	Health, Finance and Government HTTPS Rule	Any	Internet	HTTPS default s...	Financial Services Health Government / M...	Bypass	Log	Policy H...	Outbound Certi...	Exempting health, financial and governmental websites from HTTPS inspection in order to protect privacy rights. Note: This rule requires enablement of URL Filtering on all Policy HTTPS Targets
2	Predefined Rule	Any	Internet	HTTPS default s...	Any	Inspect	Log	Policy H...	Outbound Certi...	

Unmatched traffic will be bypassed.

5. We will enable HTTPS inspection for the internal subnet **10.1.1.0/24** only. Modify the second rule and add **net_10_1_1_0_24** as the source of the rule.

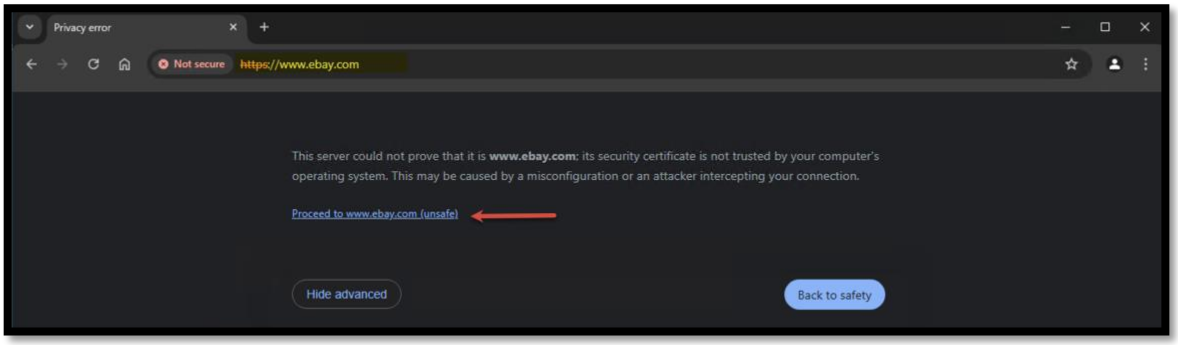


The Policy will be enforced only on gateways with HTTPS Inspection enabled.

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate	Comment
1	Health, Finance and Government HTTPS Rule	Any	Internet	HTTPS default s...	Financial Services Health Government / M...	Bypass	Log	Policy H...	Outbound Certi...	Exempting health, financial and governmental websites from HTTPS inspection in order to protect privacy rights. Note: This rule requires enablement of URL Filtering on all Policy HTTPS Targets
2	Predefined Rule	net_10_1_1_0_24	Internet	HTTPS default s...	Any	Inspect	Log	Policy H...	Outbound Certi...	

Unmatched traffic will be bypassed.

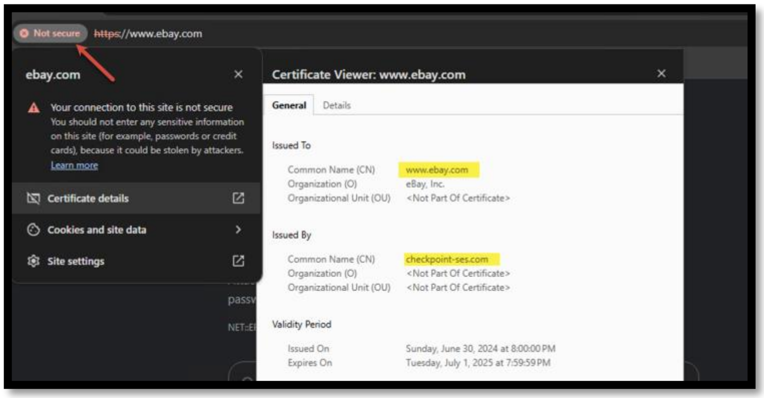
6. Install the Access Control Policy.
7. From **win_client**, open a web browser and try to access any allowed website. E.g. http://www.ebay.com. Notice that we are presented with a certificate trust warning.
8. Bypass the security warning by clicking Proceed to www.ebay.com (unsafe) (if missing type *thisisunsafe* to bypass the warning).



This server could not prove that it is **www.ebay.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to www.ebay.com (unsafe)

9. Open the certificate and notice that the certificate presented is a certificate issued by the GW using the certificate we created in the steps above.



ebay.com

Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Learn more

Certificate Viewer: www.ebay.com

Issued To

Common Name (CN)	www.ebay.com
Organization (O)	eBay, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

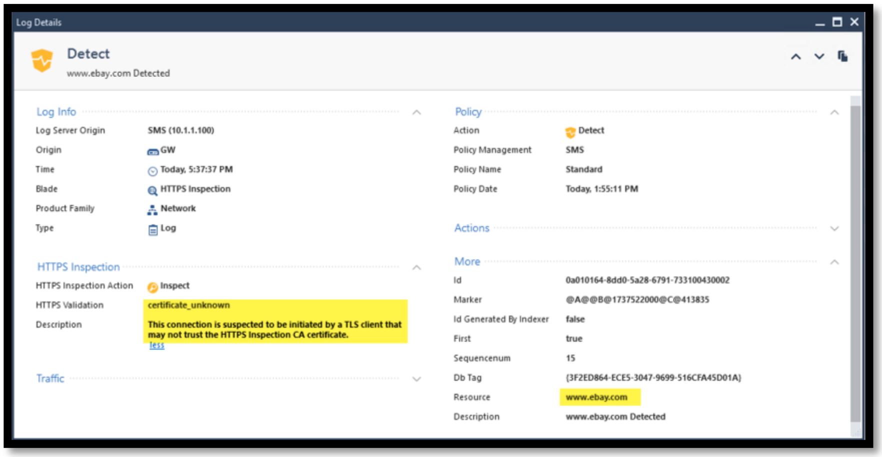
Issued By

Common Name (CN)	checkpoint-ses.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Sunday, June 30, 2024 at 8:00:00 PM
Expires On	Tuesday, July 1, 2025 at 7:59:59 PM

10. From **SmartConsole**, filter the logs to show logs related to HTTPS Inspection **blade: "HTTPS Inspection"**. Or simply search for www.ebay.com in the log view.



Detect
www.ebay.com Detected

Log Info

Log Server Origin	SMS (10.1.1.100)
Origin	GW
Time	Today, 5:37:37 PM
Blade	HTTPS Inspection
Product Family	Network
Type	Log

HTTPS Inspection

HTTPS Inspection Action	Inspect
HTTPS Validation	certificate_unknown
Description	This connection is suspected to be initiated by a TLS client that may not trust the HTTPS Inspection CA certificate. less

Traffic

Policy

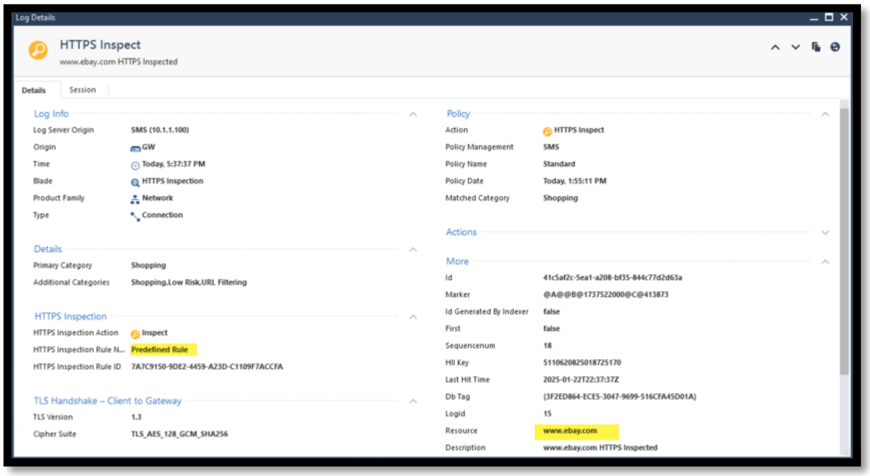
Action	Detect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 1:55:11 PM

Actions

More

Id	0a010164-8dd0-5a28-6791-733100430002
Marker	@A@@B@1737522000@C@413835
Id Generated By Indexer	false
First	true
Sequencenum	15
Db Tag	{3F2ED864-ECE5-3047-9699-516CFA45D01A}
Resource	www.ebay.com
Description	www.ebay.com Detected

11. Review other security log related to the site we tested. https://www.ebay.com in the example above. Notice that the traffic was inspected successfully.



HTTPS Inspect
www.ebay.com HTTPS Inspected

Log Info

Log Server Origin	SMS (10.1.1.100)
Origin	GW
Time	Today, 5:37:37 PM
Blade	HTTPS Inspection
Product Family	Network
Type	Connection

Details

Primary Category	Shopping
Additional Categories	Shopping,Low Risk,URL Filtering

HTTPS Inspection

HTTPS Inspection Action	Inspect
HTTPS Inspection Rule N...	Predefined Rule
HTTPS Inspection Rule ID	7A7C9150-9DE2-4459-A23D-C1109F7ACCFA

TLS Handshake – Client to Gateway

TLS Version	1.3
Cipher Suite	TLS_AES_128_GCM_SHA256

Policy

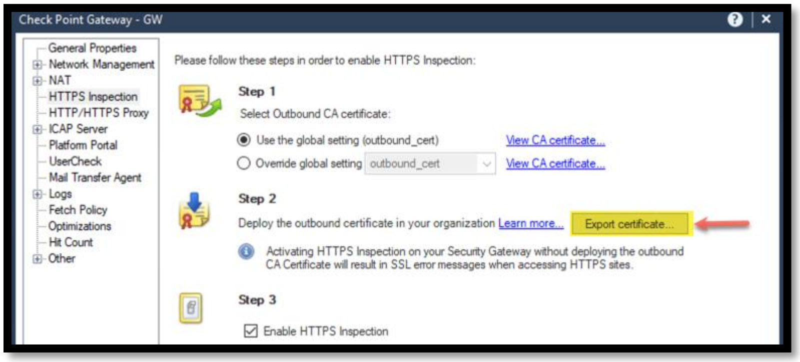
Action	HTTPS Inspect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 1:55:11 PM
Matched Category	Shopping

Actions

More

Id	41c5af2c-5ea1-a208-bf35-844c77d2d63a
Marker	@A@@B@1737522000@C@413873
Id Generated By Indexer	false
First	false
Sequencenum	18
Hll Key	5110620825018725170
Last Hit Time	2025-01-22T22:37:37Z
Db Tag	{3F2ED864-ECE5-3047-9699-516CFA45D01A}
Logid	15
Resource	www.ebay.com
Description	www.ebay.com HTTPS Inspected

12. To avoid getting the certificate warning, open the GW object and export the HTTPS inspection certificate.



Check Point Gateway - GW

Please follow these steps in order to enable HTTPS Inspection:

Step 1

Select Outbound CA certificate:

● Use the global setting (outbound_cert) View CA certificate...

○ Override global setting outbound_cert View CA certificate...

Step 2

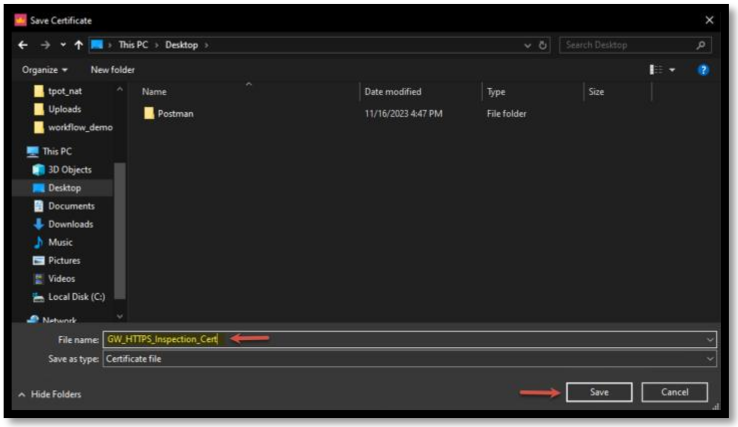
Deploy the outbound certificate in your organization Learn more... Export certificate...

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

☑ Enable HTTPS Inspection

13. Give the certificate a proper name and save it to the Desktop of the Jump Server.



Save Certificate

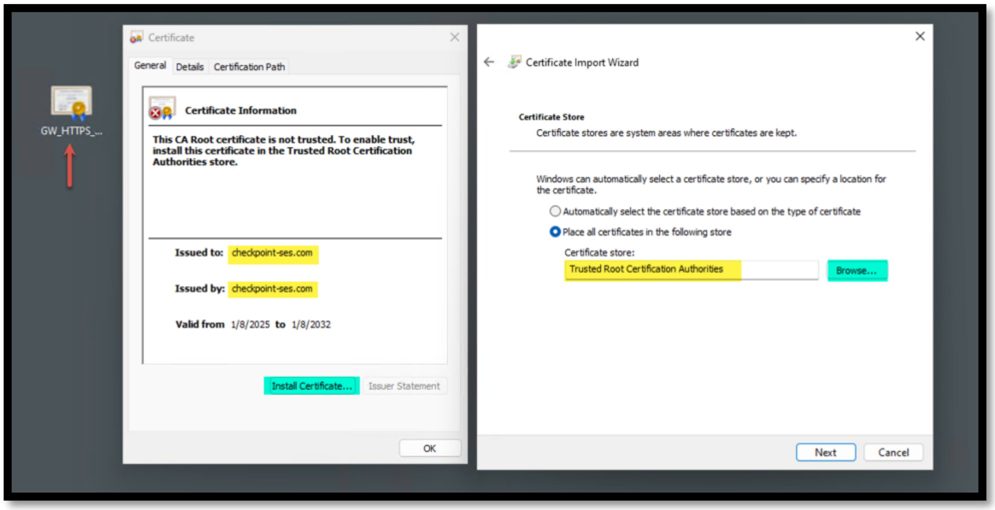
This PC › Desktop ›

Name	Date modified	Type	Size
Postman	11/16/2023 4:47 PM	File folder	

File name: GW_HTTPS_Inspection_Cert

Save as type: Certificate file

14. Copy the certificate file to the **win_client** host (over RDP) and install it as a Trusted Root Certification Authority. Make sure the certificate is installed successfully.



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: checkpoint-ses.com

Issued by: checkpoint-ses.com

Valid from 1/8/2025 **to** 1/8/2032

Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

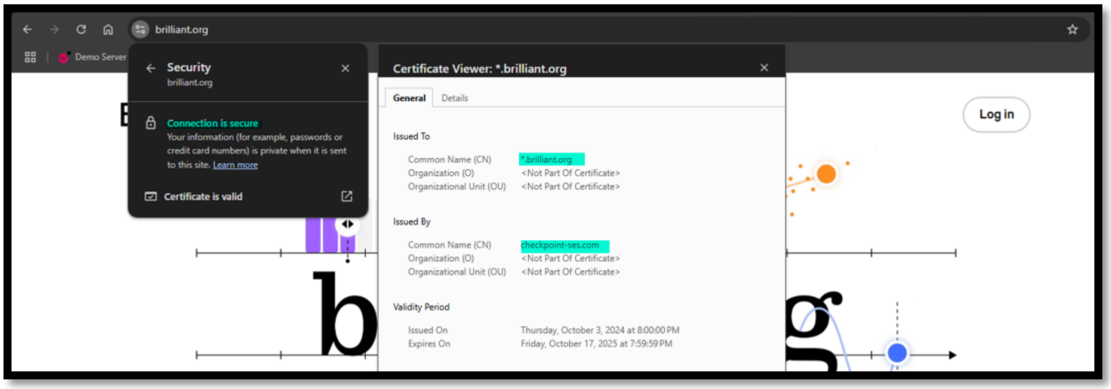
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

- Note that Chrome uses the Windows Certificate Trust Store while **Firefox** has its own certificate authority store that the CA key must be imported into.

15. Use any web browser like chrome and try reaching any allowed website again, e.g. https://briliant.org. Notice that the certificate warning is no longer present and the Connection is considered secure by the browser.



Security
brilliant.org

Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Certificate Viewer: *.brilliant.org

General | Details

Issued To

Common Name (CN)	*.brilliant.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

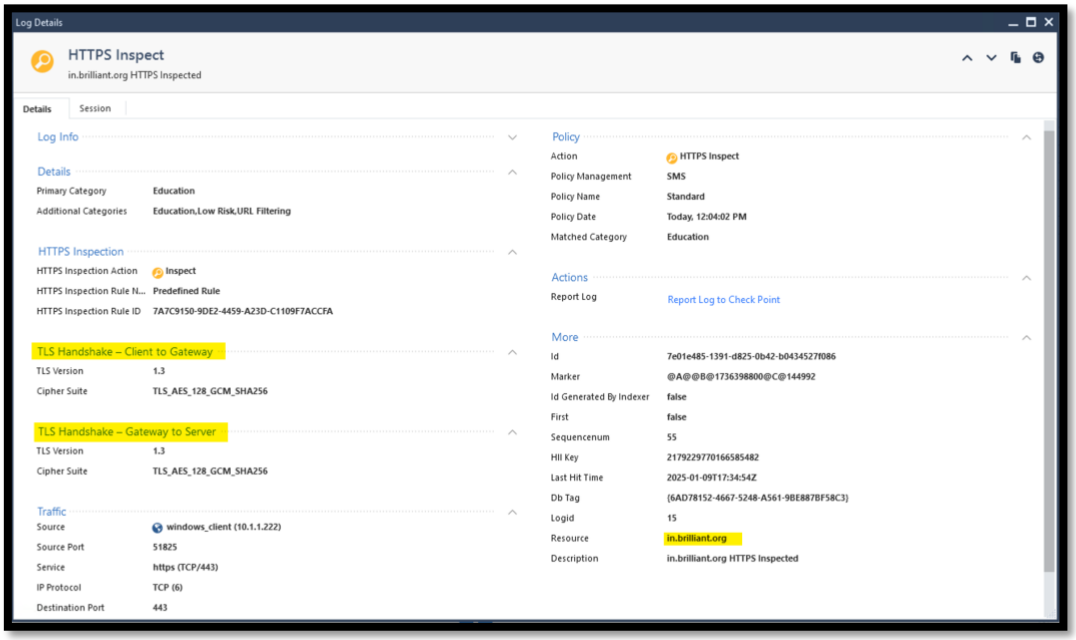
Issued By

Common Name (CN)	checkpoint-ses.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, October 3, 2024 at 8:00:00 PM
Expires On	Friday, October 17, 2025 at 7:59:59 PM

16. Review the HTTPS Inspection log. Notice that we can see details related to the TLS version and the cipher used on the client and the GW side.


Log Details

HTTPS Inspect
in.brilliant.org HTTPS Inspected

Details | Session

Log Info

Details

Primary Category	Education
Additional Categories	Education,Low Risk,URL Filtering

HTTPS Inspection

HTTPS Inspection Action	Inspect
HTTPS Inspection Rule N...	Predefined Rule
HTTPS Inspection Rule ID	7A7C9150-9DE2-4459-A23D-C1109F7ACCFA

TLS Handshake – Client to Gateway

TLS Version	1.3
Cipher Suite	TLS_AES_128_GCM_SHA256

TLS Handshake – Gateway to Server

TLS Version	1.3
Cipher Suite	TLS_AES_128_GCM_SHA256

Traffic

Source	windows_client (10.1.1.222)
Source Port	51825
Service	https (TCP/443)
IP Protocol	TCP (6)
Destination Port	443

Policy

Action	HTTPS Inspect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 12:04:02 PM
Matched Category	Education

Actions

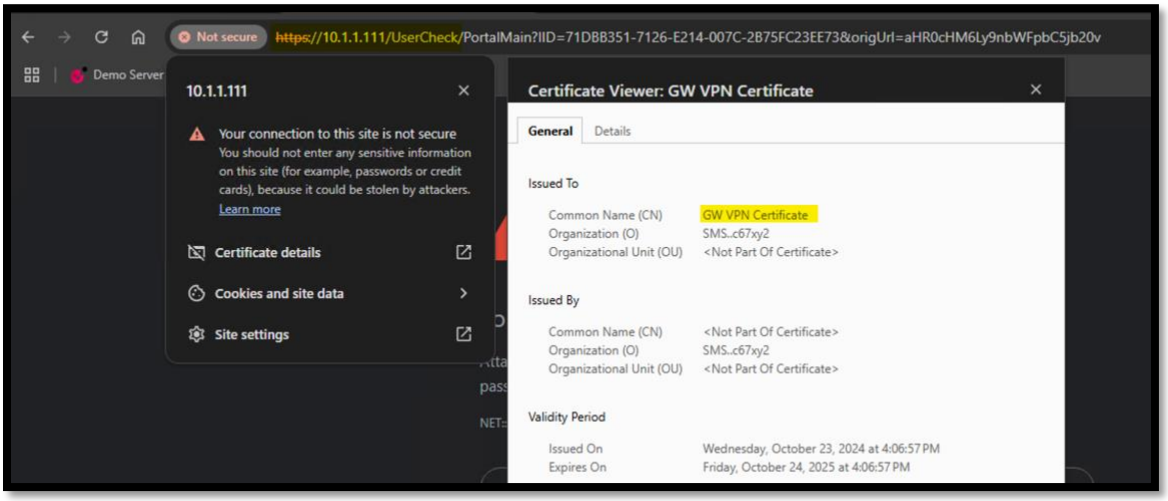
Report Log	Report Log to Check Point

More

Id	7e01e485-1391-d825-0b42-b04345271086
Marker	@A@@B@1736398800@C@144992
Id Generated By Indexer	false
First	false
Sequencenum	55
Hll Key	2179229770166585482
Last Hit Time	2025-01-09T17:34:54Z
Db Tag	{6AD78152-4667-5248-A561-9BE887BF58C3}
Logid	15
Resource	in.brilliant.org
Description	in.brilliant.org HTTPS Inspected

- In the previous lab, we blocked access to public Email server, however, we were not getting a block message because of the inability to redirect HTTPS inspection traffic. This issue should be resolved with HTTPS Inspection enabled.

17. From the **win_client** host, try to reach **Gmail**.com or any public Email server. Note that the UserCheck blade is using the default GW VPN Certificate. This is a self-signed internal cert that is not trusted by default. This is separate from the HTTPS Inspection, and it is presented to the user because we are accessing the **UserCheck** portal.



Not secure https://10.1.1.111/UserCheck/PortalMain?IID=71DBB351-7126-E214-007C-2B75FC23EE73&origUrl=aHR0cHM6Ly9nbWFpbC5jb20v

Demo Server

10.1.1.111

Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Learn more

Certificate Viewer: GW VPN Certificate

Issued To

Common Name (CN)	GW VPN Certificate
Organization (O)	SMS..c67xy2
Organizational Unit (OU)	<Not Part Of Certificate>

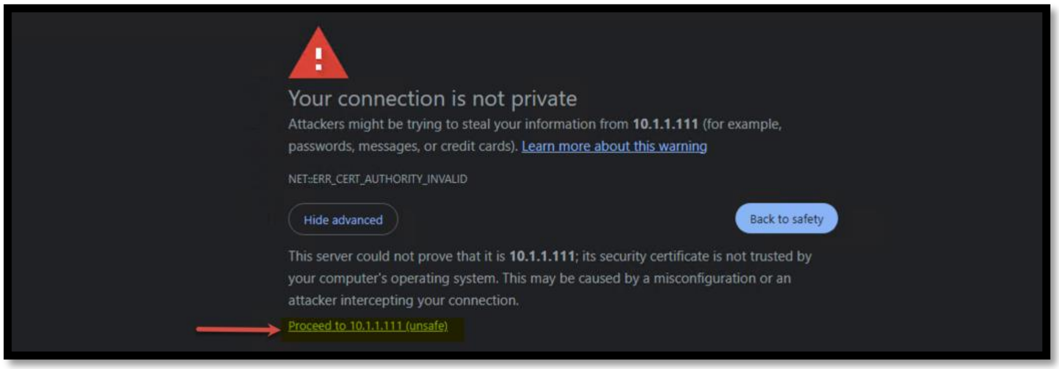
Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	SMS..c67xy2
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Wednesday, October 23, 2024 at 4:06:57 PM
Expires On	Friday, October 24, 2025 at 4:06:57 PM

18. Bypass the security warning related to the UserCheck certificate.



Your connection is not private

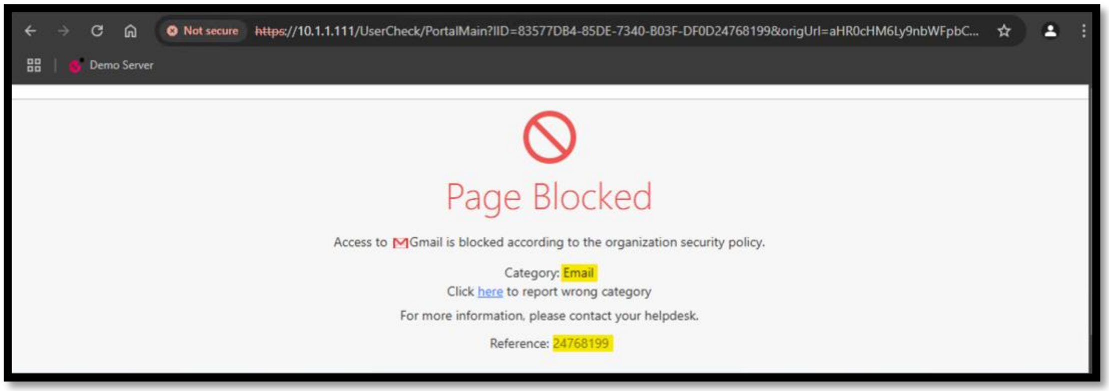
Attackers might be trying to steal your information from **10.1.1.111** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **10.1.1.111**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.1.1.111 (unsafe)

19. notice that block message is now returned successfully.



Not secure https://10.1.1.111/UserCheck/PortalMain?IID=83577DB4-85DE-7340-B03F-DF0D24768199&origUrl=aHR0cHM6Ly9nbWFpbC...

Demo Server

Page Blocked

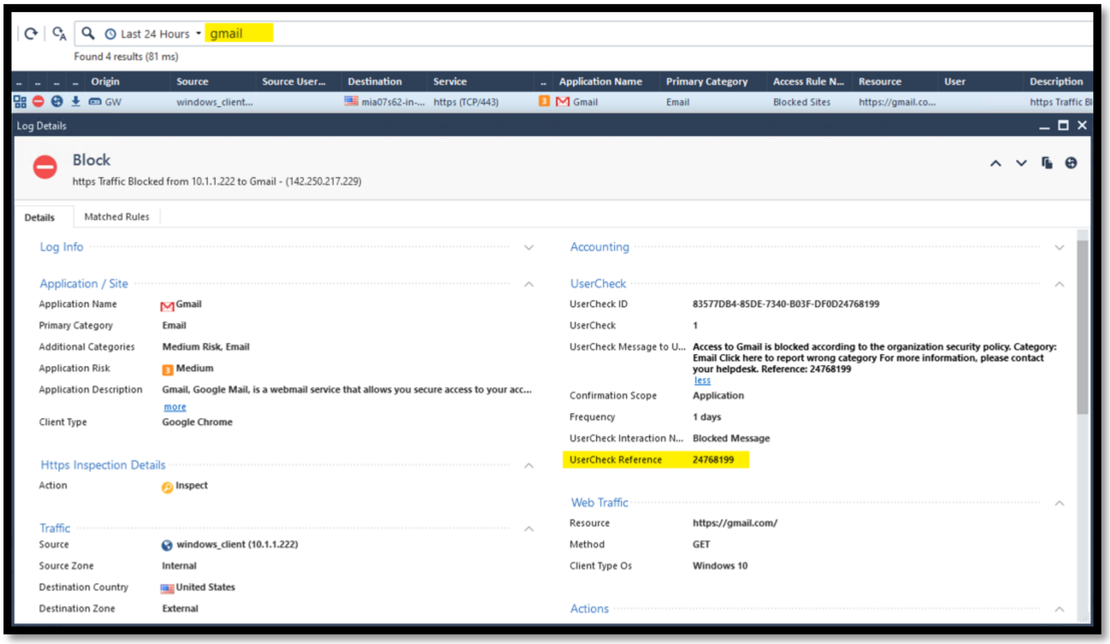
Access to Gmail is blocked according to the organization security policy.

Category: Email
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: 24768199

20. Review the related log, you can filter logs related to Gmail or you can use the UserCheck Reference.



Found 4 results (81 ms)

Origin	Source	Source User...	Destination	Service	Application Name	Primary Category	Access Rule N...	Resource	User	Description
GW	windows_client...		mia07s62-in-...	https (TCP/443)	Gmail	Email	Blocked Sites	https://gmail.co...		https Traffic Bl

Log Details

Block
https Traffic Blocked from 10.1.1.222 to Gmail - (142.250.217.229)

Application / Site

Application Name	Gmail
Primary Category	Email
Additional Categories	Medium Risk, Email
Application Risk	Medium
Application Description	Gmail, Google Mail, is a webmail service that allows you secure access to your acc... more
Client Type	Google Chrome

Https Inspection Details

Action	Inspect

Traffic

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

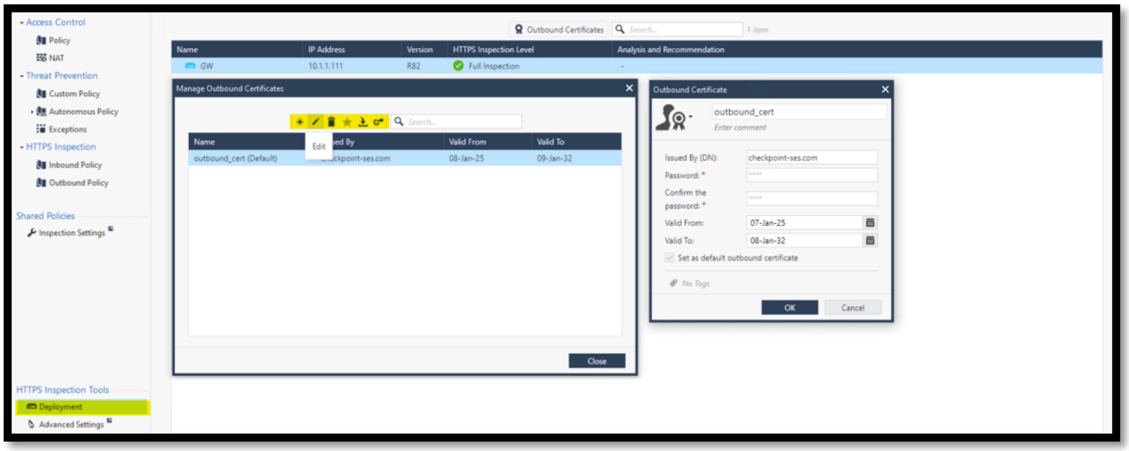
UserCheck

UserCheck ID	83577DB4-85DE-7340-B03F-DF0D24768199
UserCheck	1
UserCheck Message to U...	Access to Gmail is blocked according to the organization security policy. Category: Email Click here to report wrong category For more information, please contact your helpdesk. Reference: 24768199 less
Confirmation Scope	Application
Frequency	1 days
UserCheck Interaction N...	Blocked Message
UserCheck Reference	24768199

Web Traffic

Resource	https://gmail.com/
Method	GET
Client Type Os	Windows 10

- Note that starting R82, it is possible to **add**, **edit**, **delete** and perform other operations related to the outbound certificates under the **Deployment** settings.



Name	IP Address	Version	HTTPS Inspection Level	Analysis and Recommendation
GW	10.1.1.111	R82	Full Inspection	-

Manage Outbound Certificates

Name	...ed By	Valid From	Valid To
outbound_cert (Default)	...ckpoint-ses.com	08-Jan-25	09-Jan-32

Outbound Certificate

outbound_cert
Enter comment

Issued By (DN):	checkpoint-ses.com
Password: *	****
Confirm the password: *	****
Valid From:	07-Jan-25
Valid To:	08-Jan-32

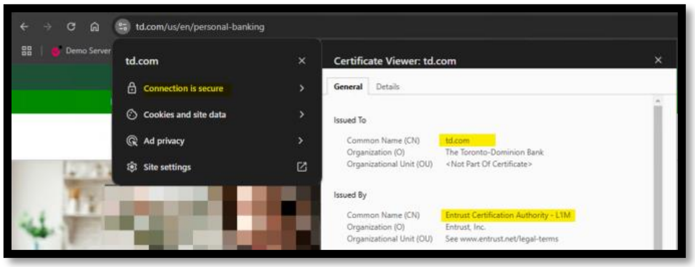
☑ Set as default outbound certificate

No Tags

Exercise 2: Bypass Behaviors

There are cases when some websites are not inspected by HTTPS inspection. For example, some servers will not allow the GW to reach the server on behalf of the client (certificate pinning to prevent **MITM** attacks), or servers that do not follow the protocol standards.
There are other scenarios where we bypass due to **regulation** such as in financial and health web sites.

1. From **win_client**, use chrome to browse to a financial institution website. For example, https://www.td.com. Review the issuer of the certificate.



td.com/us/en/personal-banking

Demo Server

td.com

- Connection is secure
- Cookies and site data
- Ad privacy
- Site settings

Certificate Viewer: td.com

General | Details

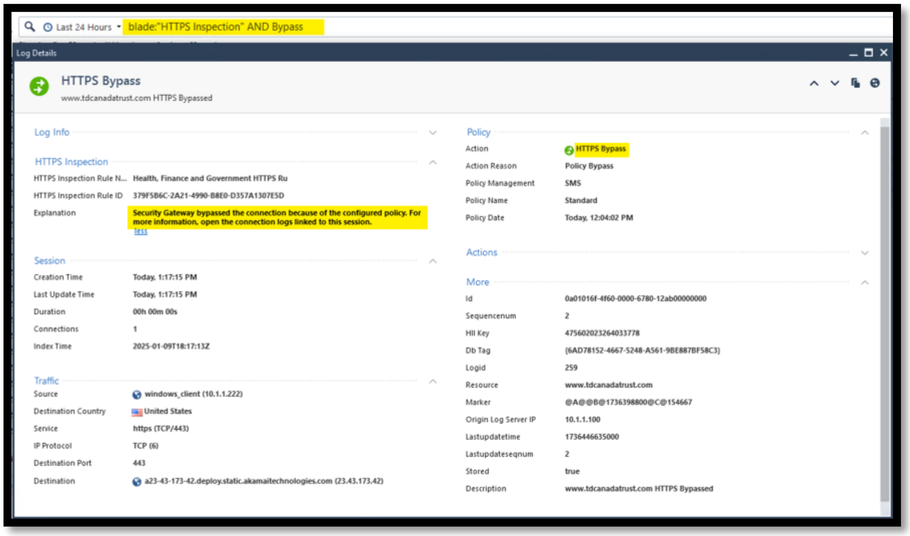
Issued To

Common Name (CN) td.com
Organization (O) The Toronto-Dominion Bank
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) Entrust Certification Authority - L1M
Organization (O) Entrust, Inc.
Organizational Unit (OU) See www.entrust.net/legal-terms

2. Review the HTTPS Inspection bypass log. Notice that this was bypassed as configured in the first rule of the outbound policy.



Last 24 Hours blade:"HTTPS Inspection" AND Bypass

Log Details

HTTPS Bypass
www.tdcanadatrust.com HTTPS Bypassed

Log Info

HTTPS Inspection

HTTPS Inspection Rule N... Health, Finance and Government HTTPS Ru
HTTPS Inspection Rule ID 379F5B6C-2A21-4990-B8E0-D357A1307E5D
Explanation Security Gateway bypassed the connection because of the configured policy. For more information, open the connection logs linked to this session.
less

Session

Creation Time Today, 1:17:15 PM
Last Update Time Today, 1:17:15 PM
Duration 00h 00m 00s
Connections 1
Index Time 2025-01-09T18:17:13Z

Traffic

Source windows_client (10.1.1.222)
Destination Country United States
Service https (TCP/443)
IP Protocol TCP (6)
Destination Port 443
Destination a23-43-173-42.deploy.static.akamaitechnologies.com (23.43.173.42)

Policy

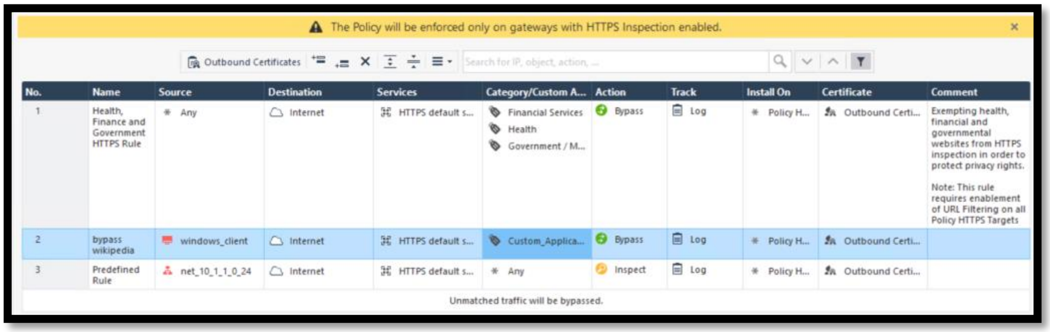
Action HTTPS Bypass
Action Reason Policy Bypass
Policy Management SMS
Policy Name Standard
Policy Date Today, 12:04:02 PM

Actions

More

Id 0a01016f-4f60-0000-6780-12ab00000000
Sequencenum 2
Hll Key 475602023264033778
Db Tag {6AD78152-4667-5248-A561-9BE887BF58C3}
Logid 259
Resource www.tdcanadatrust.com
Marker @A@@B@1736398800@C@154667
Origin Log Server IP 10.1.1.100
Lastupdatetime 1736446635000
Lastupdateseqnum 2
Stored true
Description www.tdcanadatrust.com HTTPS Bypassed

3. In the previous lab, we created the override categorization object to recategorize https://www.wikipedia.org. Create a new rule below the existing bypass rule, use the **Custom Application** object to bypass inspecting traffic to Wikipedia.org from the **win_client** host.
   - Name the Rule "Bypass Wikipedia" and set the Source to **win_client**
   - Set the destination is set to "Internet"
   - Category/Custom Application column to **Custom_application_site**
   - Action should be **Bypass**



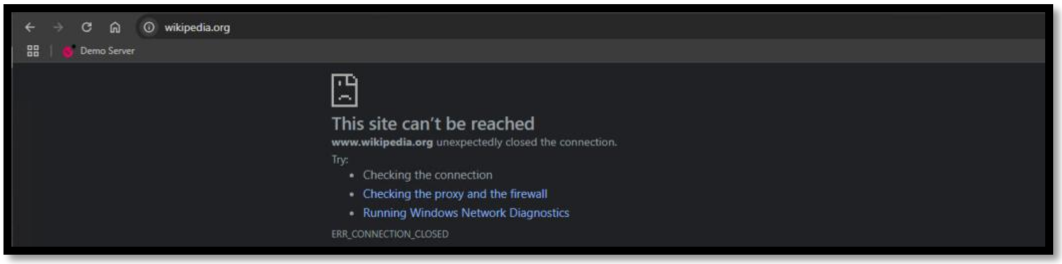
The Policy will be enforced only on gateways with HTTPS Inspection enabled.

Outbound Certificates | Search for IP, object, action, ...

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate	Comment
1	Health, Finance and Government HTTPS Rule	Any	Internet	HTTPS default s...	Financial Services Health Government / M...	Bypass	Log	Policy H...	Outbound Certi...	Exempting health, financial and governmental websites from HTTPS inspection in order to protect privacy rights. Note: This rule requires enablement of URL Filtering on all Policy HTTPS Targets
2	bypass wikipedia	windows_client	Internet	HTTPS default s...	Custom_Applica...	Bypass	Log	Policy H...	Outbound Certi...	
3	Predefined Rule	net_10_1_1_0_24	Internet	HTTPS default s...	Any	Inspect	Log	Policy H...	Outbound Certi...	

Unmatched traffic will be bypassed.

4. From **win_client** try to reach https://www.wikipedia.org.



wikipedia.org

Demo Server

This site can't be reached

www.wikipedia.org unexpectedly closed the connection.

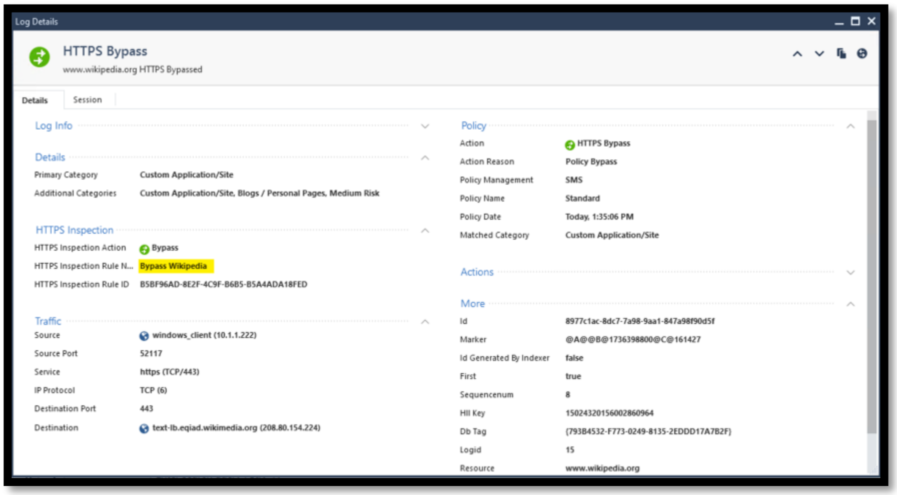
Try:

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

ERR_CONNECTION_CLOSED

- Notice that once the site is bypassed, the HTTPS inspection blade will not handle the traffic. Hence, the block message will not be presented to the user since redirecting HTTPS sites requires the HTTPS inspection blade to be active for the connection as demonstrated in the previous steps.

5. Review the HTTPS inspection log and notice the details related to the user related settings.



Log Details

HTTPS Bypass

www.wikipedia.org HTTPS Bypassed

Details | Session

Log Info

Details

Primary Category	Custom Application/Site
Additional Categories	Custom Application/Site, Blogs / Personal Pages, Medium Risk

HTTPS Inspection

HTTPS Inspection Action	Bypass
HTTPS Inspection Rule N...	Bypass Wikipedia
HTTPS Inspection Rule ID	B5BF96AD-8E2F-4C9F-B6B5-B5A4ADA18FED

Traffic

Source	windows_client (10.1.1.222)
Source Port	52117
Service	https (TCP/443)
IP Protocol	TCP (6)
Destination Port	443
Destination	text-lb.eqiad.wikimedia.org (208.80.154.224)

Policy

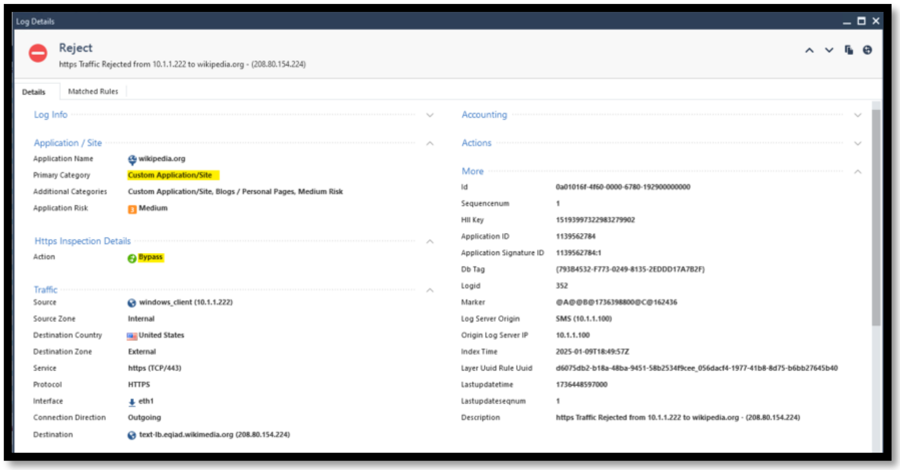
Action	HTTPS Bypass
Action Reason	Policy Bypass
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 1:35:06 PM
Matched Category	Custom Application/Site

Actions

More

Id	8977c1ac-8dc7-7a98-9aa1-847a98f90d5f
Marker	@A@@B@1736398800@C@161427
Id Generated By Indexer	false
First	true
Sequencenum	8
Hll Key	15024320156002860964
Db Tag	{793B4532-F773-0249-8135-2EDDD17A7B2F}
Logid	15
Resource	www.wikipedia.org

6. Review the URLF log and review the related HTTPS inspection field indicating a bypass.



Log Details

Reject

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

Details | Matched Rules

Log Info

Application / Site

Application Name	wikipedia.org
Primary Category	Custom Application/Site
Additional Categories	Custom Application/Site, Blogs / Personal Pages, Medium Risk
Application Risk	3 Medium

Https Inspection Details

Action	Bypass

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

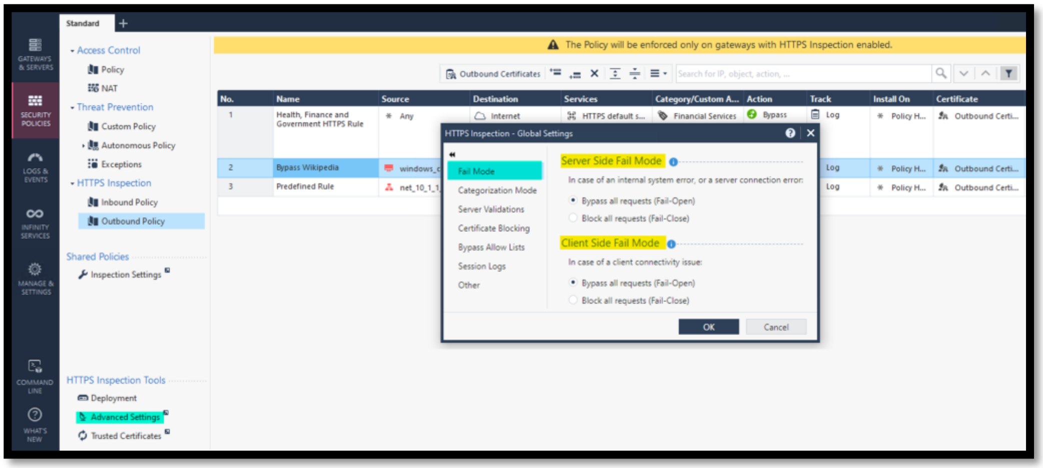
Actions

More

Id	0a01016f-4f60-0000-6780-192900000000
Sequencenum	1
Hll Key	15193997322983279902
Application ID	1139562784
Application Signature ID	1139562784:1
Db Tag	{793B4532-F773-0249-8135-2EDDD17A7B2F}
Logid	352
Marker	@A@@B@1736398800@C@162436
Log Server Origin	SMS (10.1.1.100)
Origin Log Server IP	10.1.1.100
Index Time	2025-01-09T18:49:57Z
Layer Uuid Rule Uuid	d6075db2-b18a-48ba-9451-58b2534f9cee_056dacf4-1977-41b8-8d75-b6bb27645b40
Lastupdatetime	1736448597000
Lastupdateseqnum	1
Description	https Traffic Rejected from 10.1.1.222 to wikipedia.org - (208.80.154.224)

7. From **SmartConsole**, click on HTTPs inspection Outbound policy and then you will see the HTTPS Inspection tools below and to the left of the screen, Open **Advanced Settings** and review the default Fail Modes.

    - The **Client Side Fail Mode** controls issues on the client side
    - The **Server Side Fail Mode** controls:
        - Engine failures
        - Server issues.



The Policy will be enforced only on gateways with HTTPS Inspection enabled.

HTTPS Inspection - Global Settings

Server Side Fail Mode

In case of an internal system error, or a server connection error:

● Bypass all requests (Fail-Open)

○ Block all requests (Fail-Close)

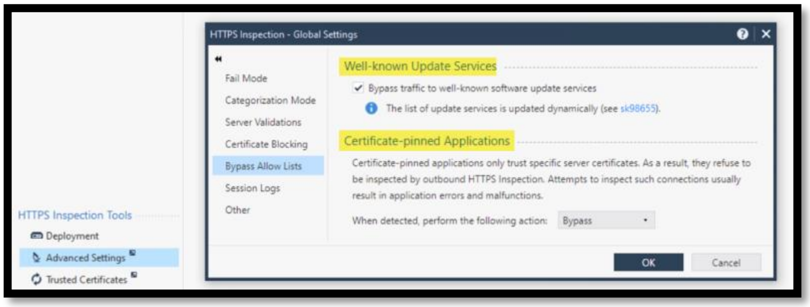
Client Side Fail Mode

In case of a client connectivity issue:

● Bypass all requests (Fail-Open)

○ Block all requests (Fail-Close)

8. Review the Bypass Allow Lists. Review the list in SK98655.



HTTPS Inspection - Global Settings

Well-known Update Services

☑ Bypass traffic to well-known software update services

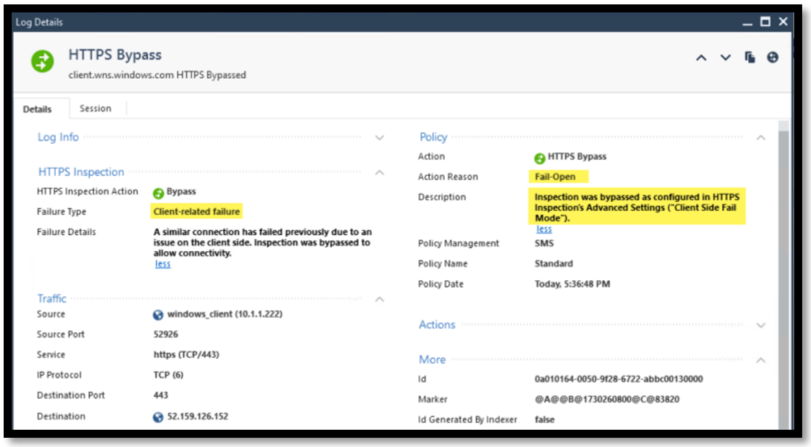
The list of update services is updated dynamically (see sk98655).

Certificate-pinned Applications

Certificate-pinned applications only trust specific server certificates. As a result, they refuse to be inspected by outbound HTTPS Inspection. Attempts to inspect such connections usually result in application errors and malfunctions.

When detected, perform the following action: Bypass

- Note that the log below shows a bypass action related to the fail-mode.



Log Details

HTTPS Bypass

client.wns.windows.com HTTPS Bypassed

Details | Session

Log Info

HTTPS Inspection

HTTPS Inspection Action	Bypass
Failure Type	Client-related failure
Failure Details	A similar connection has failed previously due to an issue on the client side. Inspection was bypassed to allow connectivity. less

Traffic

Source	windows_client (10.1.1.222)
Source Port	52926
Service	https (TCP/443)
IP Protocol	TCP (6)
Destination Port	443
Destination	52.159.126.152

Policy

Action	HTTPS Bypass
Action Reason	Fail-Open
Description	Inspection was bypassed as configured in HTTPS Inspection's Advanced Settings ("Client Side Fail Mode"). less
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 5:36:48 PM

Actions

More

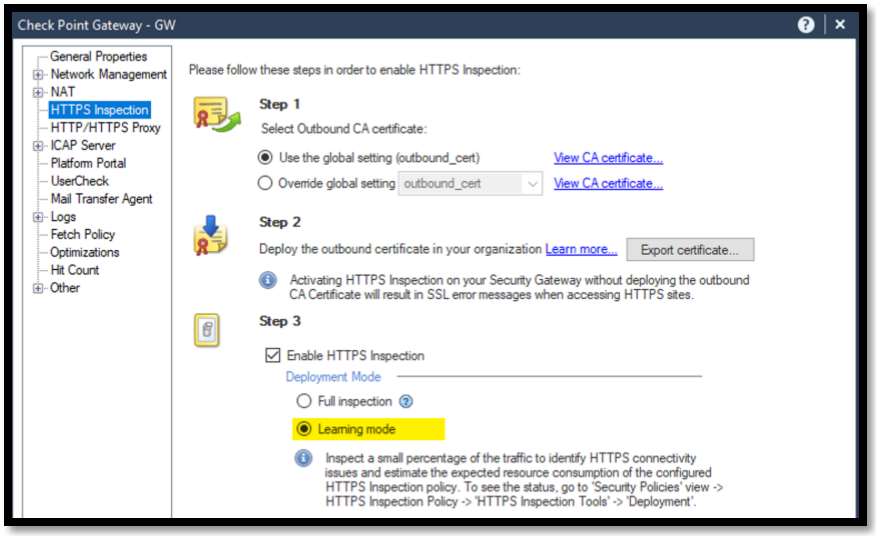
Id	0a010164-0050-9f28-6722-abbc00130000
Marker	@A@@B@1730260800@C@83820
Id Generated By Indexer	false

Exercise 3: Deployment Assessment

In the previous exercises, we configured the HTTPS Inspection outbound policy to inspect traffic from one network **10.1.1.0/24** while all HTTPS traffic from other network will be bypassed by default. This can be a good deployment strategy to deploy HTTPS inspection gradually.

R82 brings a new deployment assessment feature to monitor the traffic and provide recommendations.

1. Edit the GW object and change the HTTPS Inspection **Deployment mode** to **Learning Mode**.



Please follow these steps in order to enable HTTPS Inspection:

Step 1

Select Outbound CA certificate:

● Use the global setting (outbound_cert)

○ Override global setting outbound_cert

Step 2

Deploy the outbound certificate in your organization

Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.

Step 3

☑ Enable HTTPS Inspection

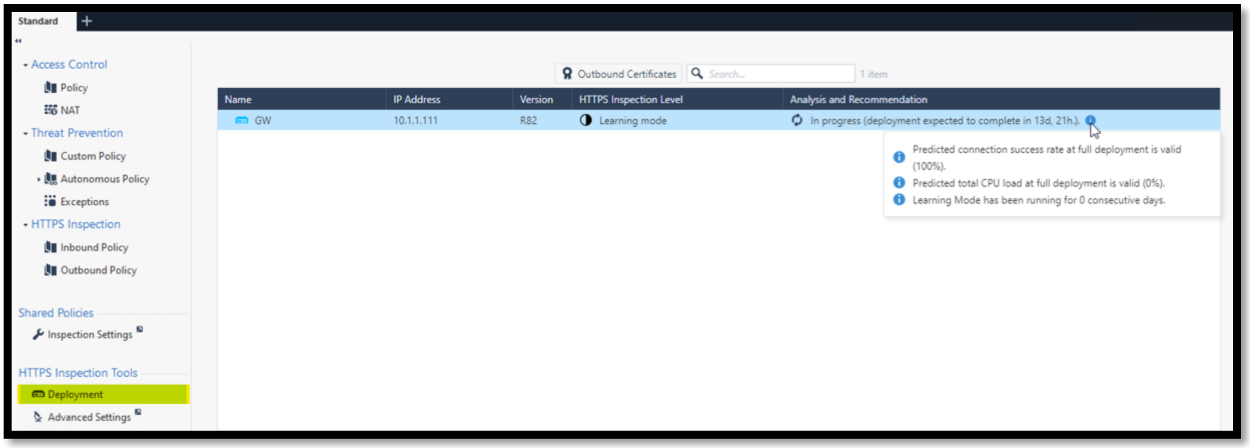
Deployment Mode

○ Full inspection

● Learning mode

Inspect a small percentage of the traffic to identify HTTPS connectivity issues and estimate the expected resource consumption of the configured HTTPS Inspection policy. To see the status, go to 'Security Policies' view -> HTTPS Inspection Policy -> 'HTTPS Inspection Tools' -> 'Deployment'.

2. Install the Access Policy.
3. Review the **GW** status under Deployment.



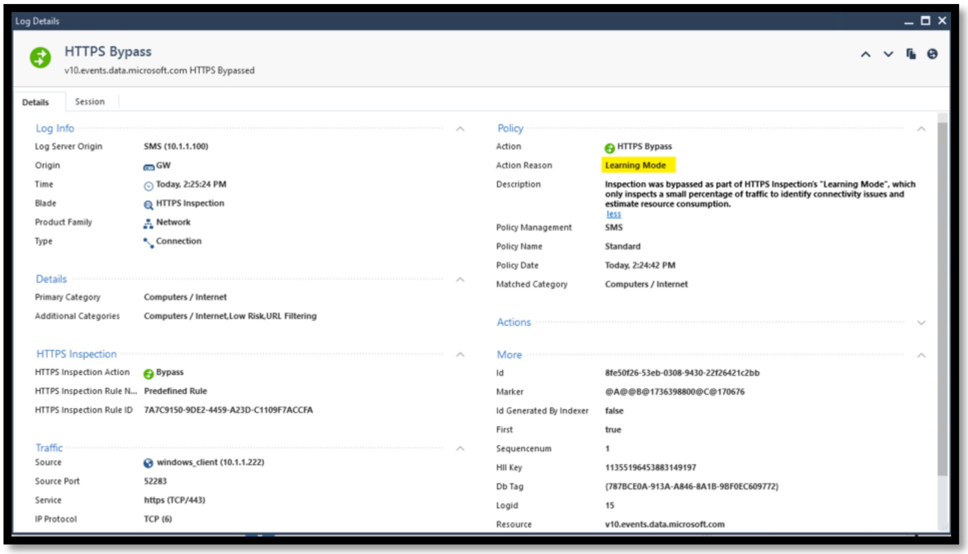
Name	IP Address	Version	HTTPS Inspection Level	Analysis and Recommendation
GW	10.1.1.111	R82	Learning mode	In progress (deployment expected to complete in 13d, 21h.).

Predicted connection success rate at full deployment is valid (100%).

Predicted total CPU load at full deployment is valid (0%).

Learning Mode has been running for 0 consecutive days.

4. Review the HTTPS inspection logs and notice that the traffic is bypassed.



Log Details

HTTPS Bypass
v10.events.data.microsoft.com HTTPS Bypassed

Details | Session

Log Info

Log Server Origin	SMS (10.1.1.100)
Origin	GW
Time	Today, 2:25:24 PM
Blade	HTTPS Inspection
Product Family	Network
Type	Connection

Details

Primary Category	Computers / Internet
Additional Categories	Computers / Internet,Low Risk,URL Filtering

HTTPS Inspection

HTTPS Inspection Action	Bypass
HTTPS Inspection Rule N...	Predefined Rule
HTTPS Inspection Rule ID	7A7C9150-9DE2-4459-A23D-C1109F7ACCFA

Traffic

Source	windows_client (10.1.1.222)
Source Port	52283
Service	https (TCP/443)
IP Protocol	TCP (6)

Policy

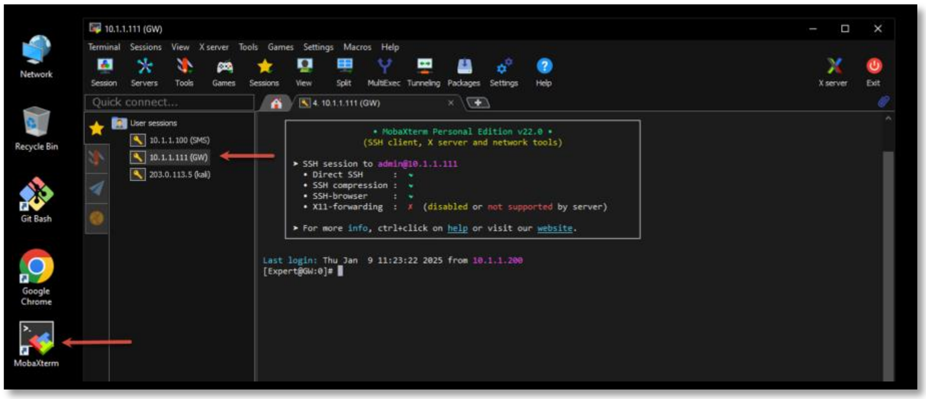
Action	HTTPS Bypass
Action Reason	Learning Mode
Description	Inspection was bypassed as part of HTTPS Inspection's "Learning Mode", which only inspects a small percentage of traffic to identify connectivity issues and estimate resource consumption. less
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 2:24:42 PM
Matched Category	Computers / Internet

Actions

More

Id	8fe50f26-53eb-0308-9430-22f26421c2bb
Marker	@A@@B@1736398800@C@170676
Id Generated By Indexer	false
First	true
Sequencenum	1
Hll Key	11355196453883149197
Db Tag	{787BCE0A-913A-A846-8A1B-9BF0EC609772}
Logid	15
Resource	v10.events.data.microsoft.com

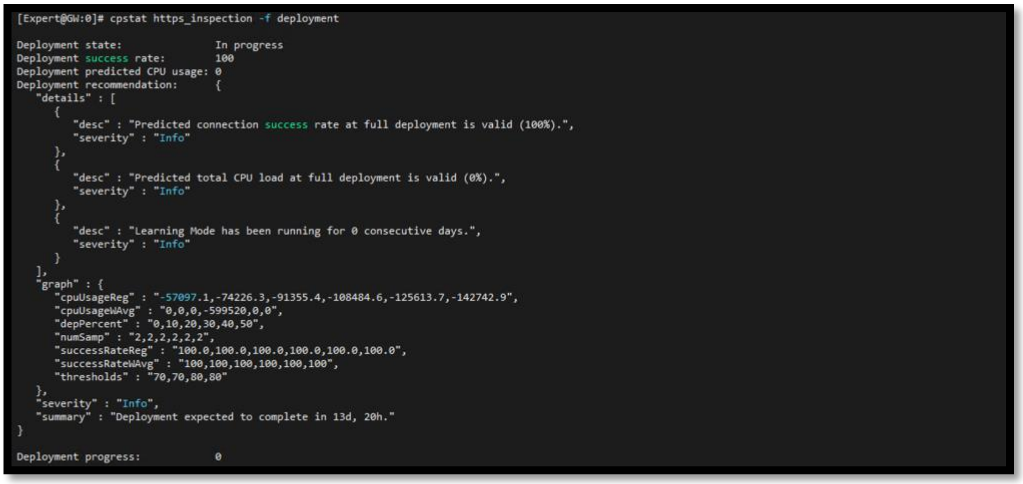
5. To get more details, use the SSH client **MobaXterm**, and open the **GW** saved session.



```
              • MobaXterm Personal Edition v22.0 •
            (SSH client, X server and network tools)

 ➤ SSH session to admin@10.1.1.111
   • Direct SSH      :  ✓
   • SSH compression :  ✓
   • SSH-browser     :  ✓
   • X11-forwarding  :  ✗  (disabled or not supported by server)

 ➤ For more info, ctrl+click on help or visit our website.

Last login: Thu Jan  9 11:23:22 2025 from 10.1.1.200
[Expert@GW:0]#
```

6. Run the command below to see get the status of the deployment assessment.

```
cpstat https_inspection -f deployment
```

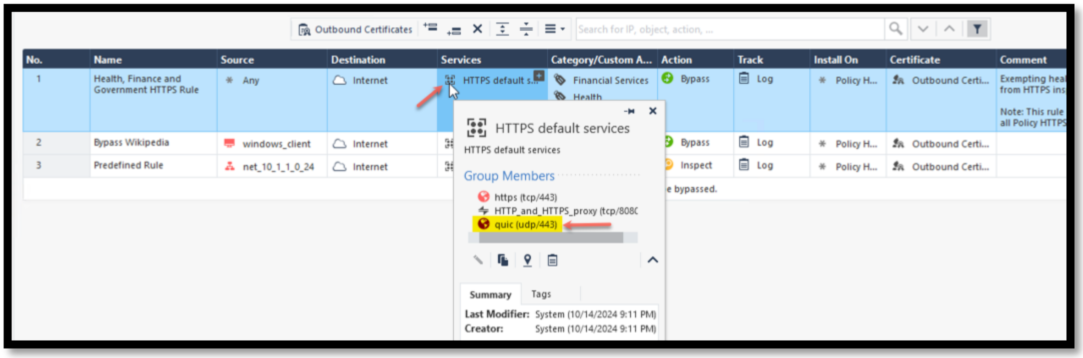


```
[Expert@GW:0]# cpstat https_inspection -f deployment

Deployment state:               In progress
Deployment success rate:        100
Deployment predicted CPU usage: 0
Deployment recommendation:      {
   "details" : [
      {
         "desc" : "Predicted connection success rate at full deployment is valid (100%).",
         "severity" : "Info"
      },
      {
         "desc" : "Predicted total CPU load at full deployment is valid (0%).",
         "severity" : "Info"
      },
      {
         "desc" : "Learning Mode has been running for 0 consecutive days.",
         "severity" : "Info"
      }
   ],
   "graph" : {
      "cpuUsageReg" : "-57097.1,-74226.3,-91355.4,-108484.6,-125613.7,-142742.9",
      "cpuUsageWAvg" : "0,0,0,-599520,0,0",
      "depPercent" : "0,10,20,30,40,50",
      "numSamp" : "2,2,2,2,2,2",
      "successRateReg" : "100.0,100.0,100.0,100.0,100.0,100.0",
      "successRateWAvg" : "100,100,100,100,100,100",
      "thresholds" : "70,70,80,80"
   },
   "severity" : "Info",
   "summary" : "Deployment expected to complete in 13d, 20h."
}

Deployment progress:            0
```

Exercise 4: HTTP3 Protocol over QUIC

Starting **R82**, the Check Point **GW** is capable of inspecting **HTTP3/QUIC** traffic. In this exercise, we will review the logs and changes related to this feature.

1. Open the service group used in the HTTPS Inspection Policy **HTTPS Default services**. Notice that **QUIC** is now inspected by default.



No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate	Comment
1	Health, Finance and Government HTTPS Rule	Any	Internet	HTTPS default s...	Financial Services Health	Bypass	Log	Policy H...	Outbound Certi...	Exempting hea from HTTPS ins Note: This rule all Policy HTTPS
2	Bypass Wikipedia	windows_client	Internet			Bypass	Log	Policy H...	Outbound Certi...	
3	Predefined Rule	net_10_1_1_0_24	Internet			Inspect	Log	Policy H...	Outbound Certi...	

e bypassed.

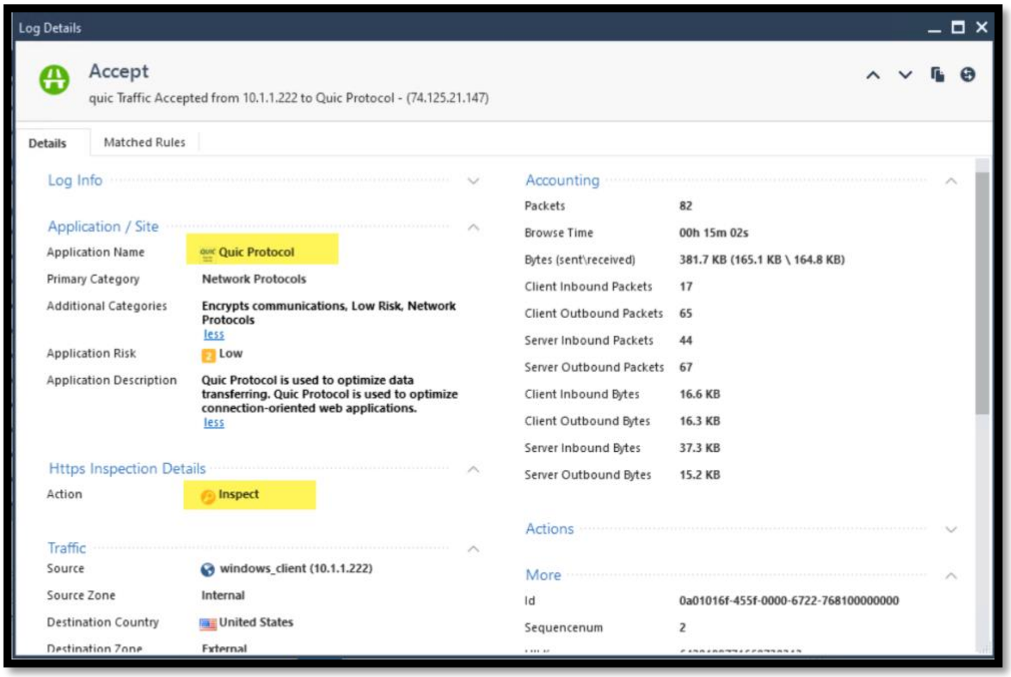
HTTPS default services
HTTPS default services

Group Members
- https (tcp/443)
- HTTP_and_HTTPS_proxy (tcp/808(
- quic (udp/443)

Summary | Tags

Last Modifier: System (10/14/2024 9:11 PM)
Creator: System (10/14/2024 9:11 PM)

2. Filter the logs to find **QUIC** related logs. Notice that we can see logs from the Application control inspecting **QUIC**.



Log Details

Accept
quic Traffic Accepted from 10.1.1.222 to Quic Protocol - (74.125.21.147)

Details | Matched Rules

Log Info

Application / Site

Application Name	Quic Protocol
Primary Category	Network Protocols
Additional Categories	Encrypts communications, Low Risk, Network Protocols less
Application Risk	2 Low
Application Description	Quic Protocol is used to optimize data transferring. Quic Protocol is used to optimize connection-oriented web applications. less

Https Inspection Details

Action	Inspect

Traffic

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

Accounting

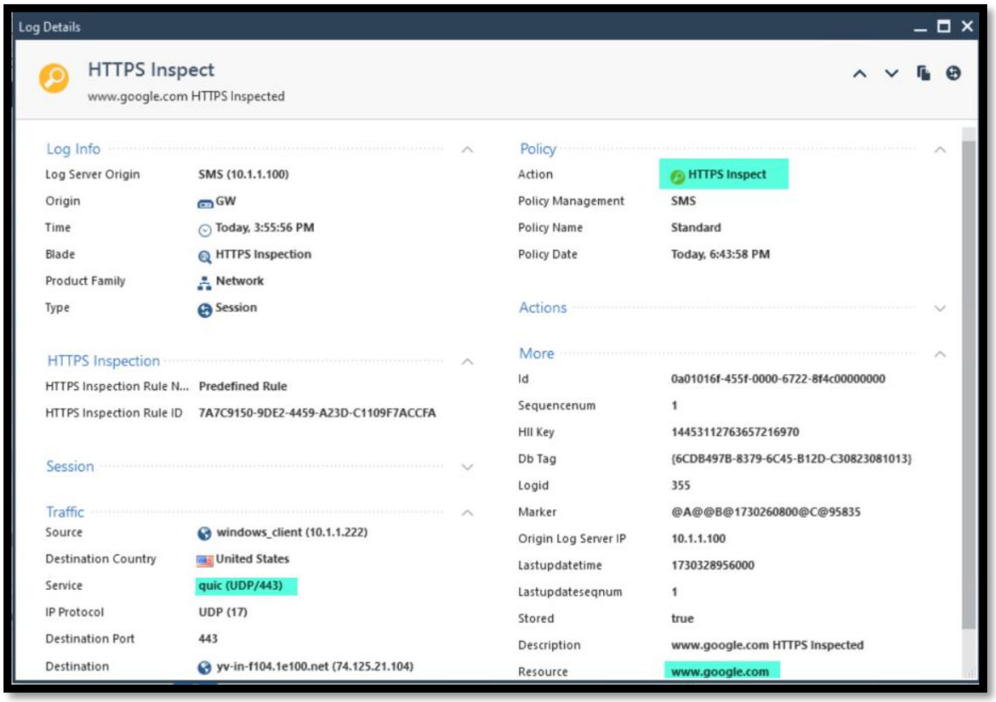
Packets	82
Browse Time	00h 15m 02s
Bytes (sent\received)	381.7 KB (165.1 KB \ 164.8 KB)
Client Inbound Packets	17
Client Outbound Packets	65
Server Inbound Packets	44
Server Outbound Packets	67
Client Inbound Bytes	16.6 KB
Client Outbound Bytes	16.3 KB
Server Inbound Bytes	37.3 KB
Server Outbound Bytes	15.2 KB

Actions

More

Id	0a01016f-455f-0000-6722-768100000000
Sequencenum	2

3. Review the HTTPS inspection logs, notice that the **QUIC** traffic is being inspected like how HTTPS traffic is logged.



Log Details

HTTPS Inspect
www.google.com HTTPS Inspected

Log Info

Log Server Origin	SMS (10.1.1.100)
Origin	GW
Time	Today, 3:55:56 PM
Blade	HTTPS Inspection
Product Family	Network
Type	Session

HTTPS Inspection

HTTPS Inspection Rule N...	Predefined Rule
HTTPS Inspection Rule ID	7A7C9150-9DE2-4459-A23D-C1109F7ACCFA

Session

Traffic

Source	windows_client (10.1.1.222)
Destination Country	United States
Service	quic (UDP/443)
IP Protocol	UDP (17)
Destination Port	443
Destination	yv-in-f104.1e100.net (74.125.21.104)

Policy

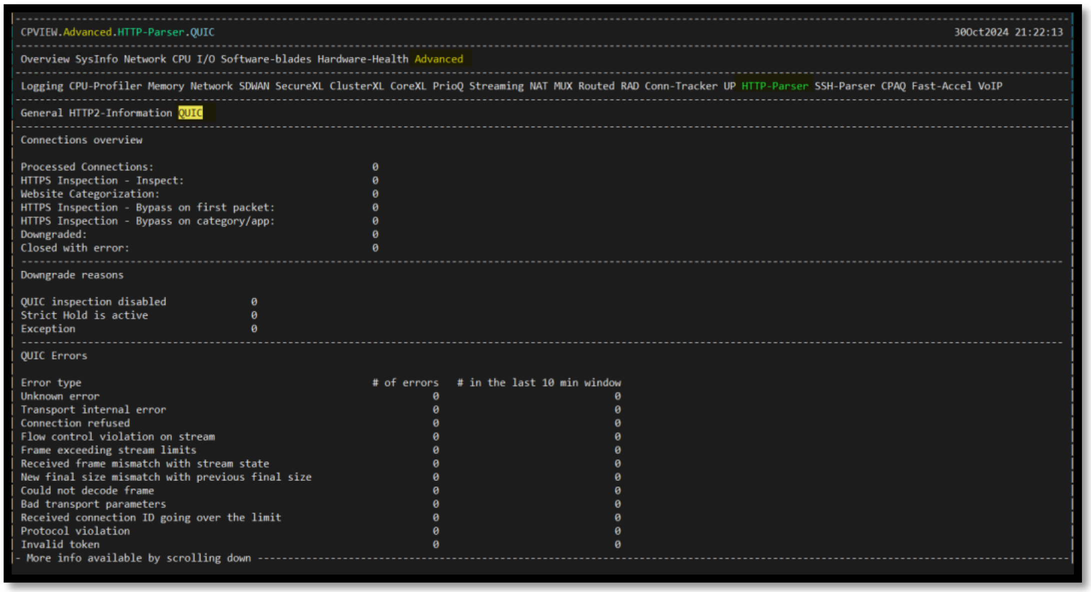
Action	HTTPS Inspect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 6:43:58 PM

Actions

More

Id	0a01016f-455f-0000-6722-8f4c00000000
Sequencenum	1
Hll Key	14453112763657216970
Db Tag	{6CDB497B-8379-6C45-B12D-C30823081013}
Logid	355
Marker	@A@@B@1730260800@C@95835
Origin Log Server IP	10.1.1.100
Lastupdatetime	1730328956000
Lastupdateseqnum	1
Stored	true
Description	www.google.com HTTPS Inspected
Resource	www.google.com

4. Login to the GW over SSH and use CPVIEW to see more details regarding **QUIC** protocol inspection.



```
CPVIEW.Advanced.HTTP-Parser.QUIC                                                                                    30Oct2024 21:22:13
Overview SysInfo Network CPU I/O Software-blades Hardware-Health Advanced
Logging CPU-Profiler Memory Network SDWAN SecureXL ClusterXL CoreXL PrioQ Streaming NAT MUX Routed RAD Conn-Tracker UP HTTP-Parser SSH-Parser CPAQ Fast-Accel VoIP
General HTTP2-Information QUIC
Connections overview

Processed Connections:                              0
HTTPS Inspection - Inspect:                         0
Website Categorization:                             0
HTTPS Inspection - Bypass on first packet:          0
HTTPS Inspection - Bypass on category/app:          0
Downgraded:                                         0
Closed with error:                                  0
Downgrade reasons

QUIC inspection disabled            0
Strict Hold is active               0
Exception                           0
QUIC Errors

Error type                                          # of errors   # in the last 10 min window
Unknown error                                                 0                             0
Transport internal error                                      0                             0
Connection refused                                            0                             0
Flow control violation on stream                              0                             0
Frame exceeding stream limits                                 0                             0
Received frame mismatch with stream state                     0                             0
New final size mismatch with previous final size              0                             0
Could not decode frame                                        0                             0
Bad transport parameters                                      0                             0
Received connection ID going over the limit                   0                             0
Protocol violation                                            0                             0
Invalid token                                                 0                             0
- More info available by scrolling down
```

5. Edit the GW object and change the deployment mode for HTTTPS Inspection to **Full Inspection**.
6. Install the Access Policy.

End of Lab 2