HTTPS Inspection

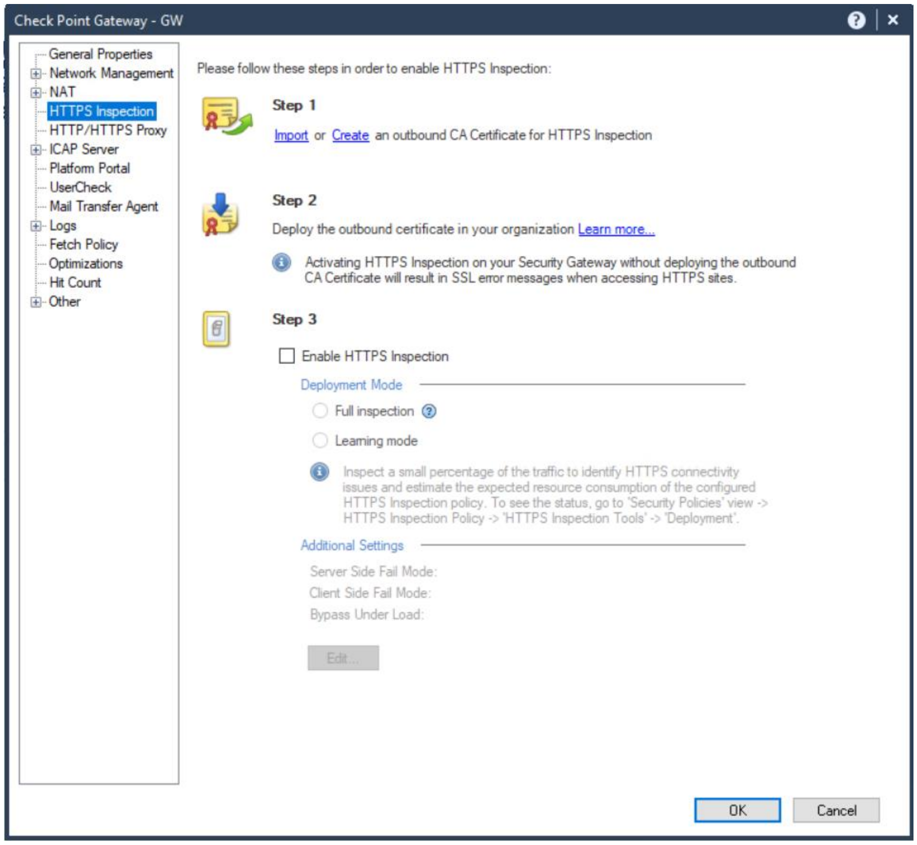
Introduction

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 "***admin/Cpwins!1***" and edit the gateway object ***GW***. From the Global Properties menu, select ***HTTPS Inspection***.



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

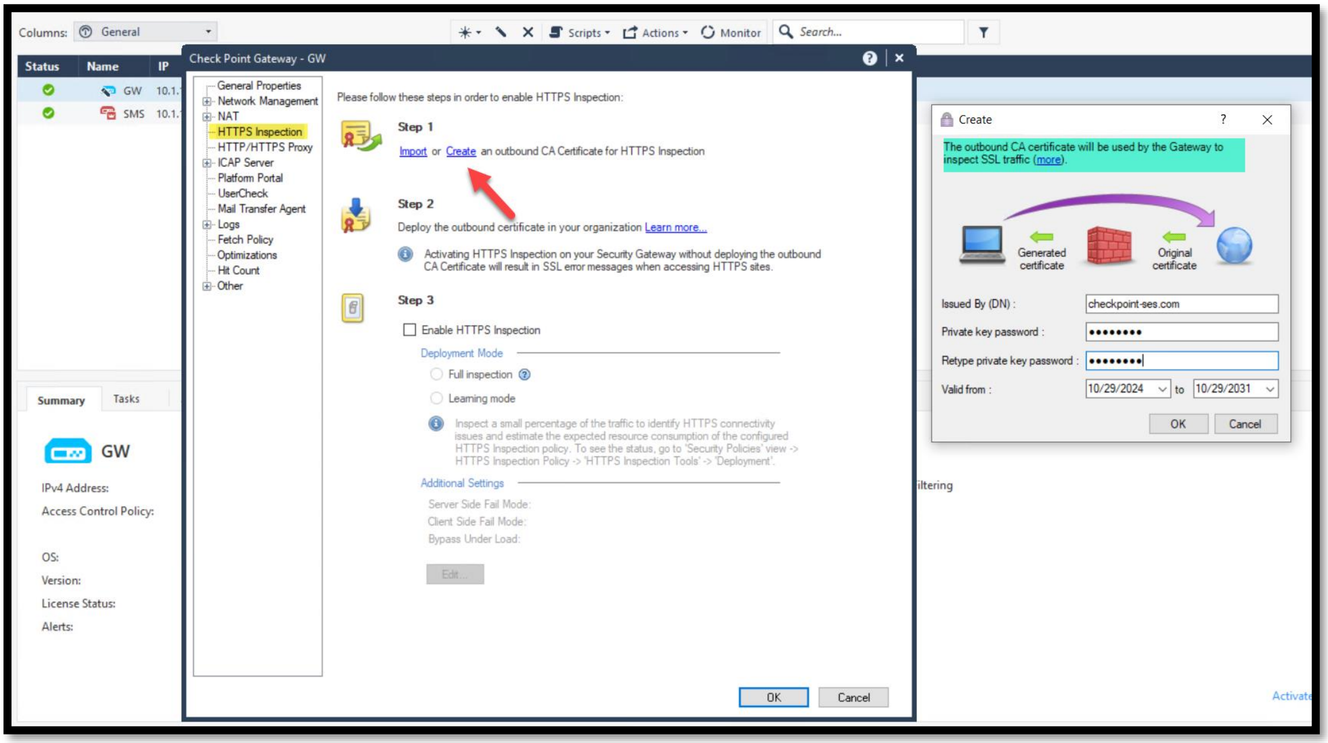
Inspect a small percentage of the traffic to identify HTTPS connectivity issues and estimate the expected resource consumption of the configured HTTPS Inspection policy. To see the status, go to 'Security Policies' view -> HTTPS Inspection Policy -> 'HTTPS Inspection Tools' -> 'Deployment'.

Additional Settings

Server Side Fail Mode:
Client Side Fail Mode:
Bypass Under Load:

Edit...

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



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:

Edit...

OK Cancel

Create

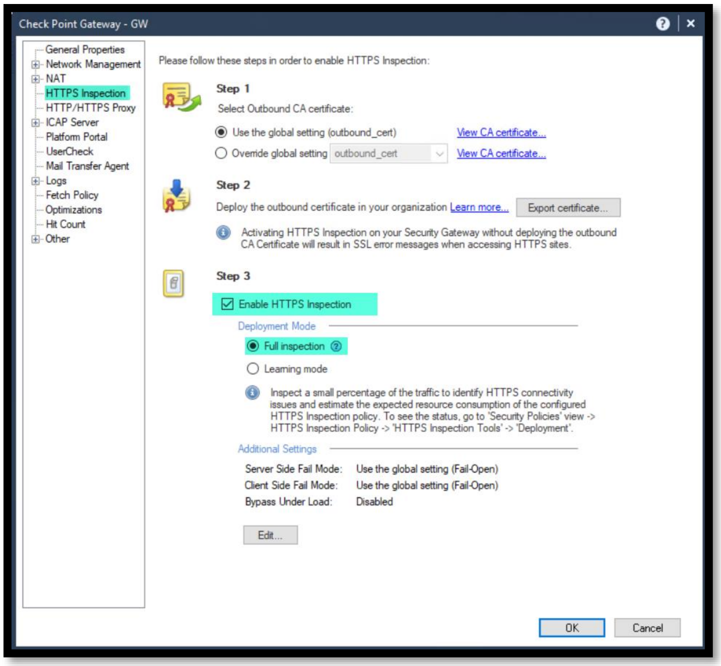
The outbound CA certificate will be used by the Gateway to inspect SSL traffic (more).

Issued By (DN): checkpoint-ses.com
Private key password: ••••••••
Retype private key password: ••••••••
Valid from: 10/29/2024 to 10/29/2031

OK Cancel

Note that this certificate will be used by the GW to inspect HTTPS traffic.

3. Skip step number 2, we will export the certificate in a later step. Under **Step 3** check the option **Enable HTTPS Inspection** and select **Full Inspection.**



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

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'.

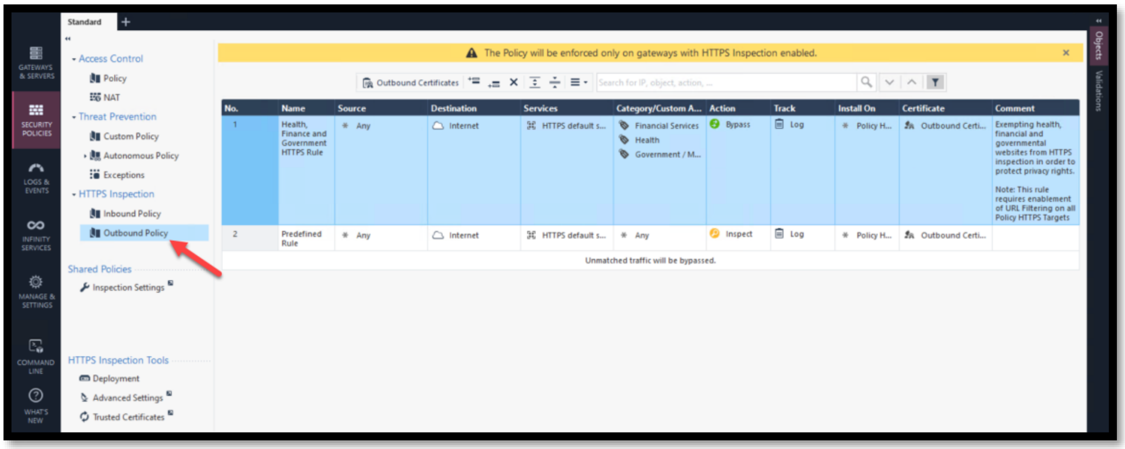
Additional Settings

Server Side Fail Mode: Use the global setting (Fail-Open)
Client Side Fail Mode: Use the global setting (Fail-Open)
Bypass Under Load: Disabled

Edit...

OK Cancel

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.

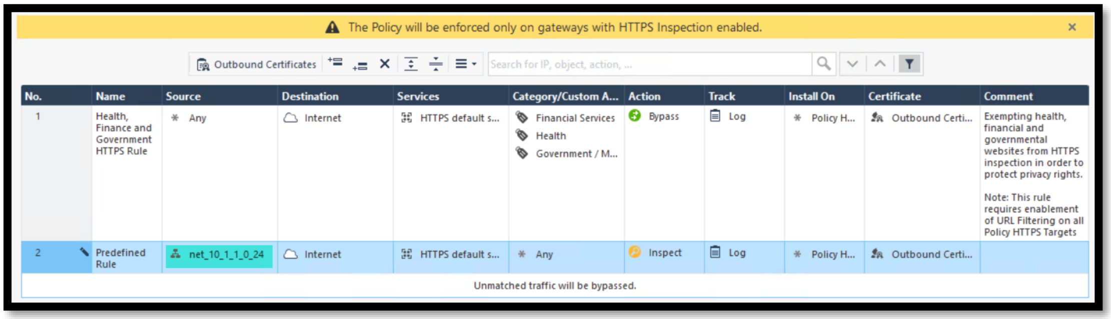


The Policy will be enforced only on gateways with HTTPS Inspection enabled.

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. Install the Access Policy.

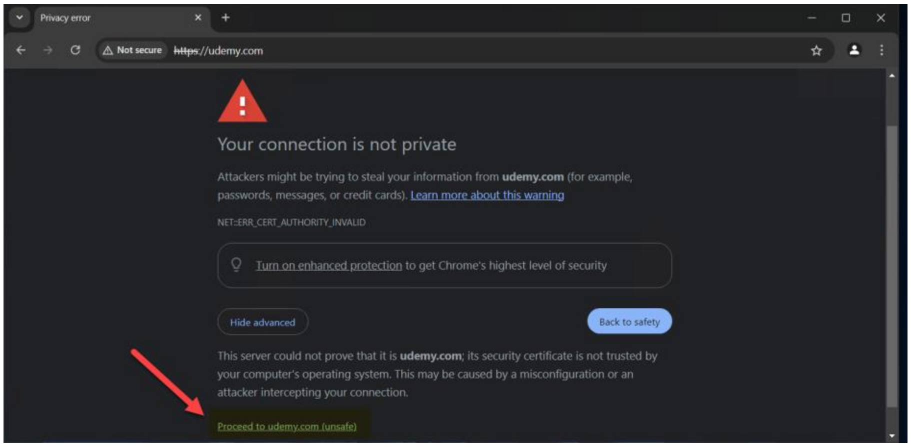


The Policy will be enforced only on gateways with HTTPS Inspection enabled.

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. From win-client, open chrome and try to access a website. E.g. https://www.wikipedia.org. Notice that we are presented with a certificate trust warning.



Your connection is not private

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

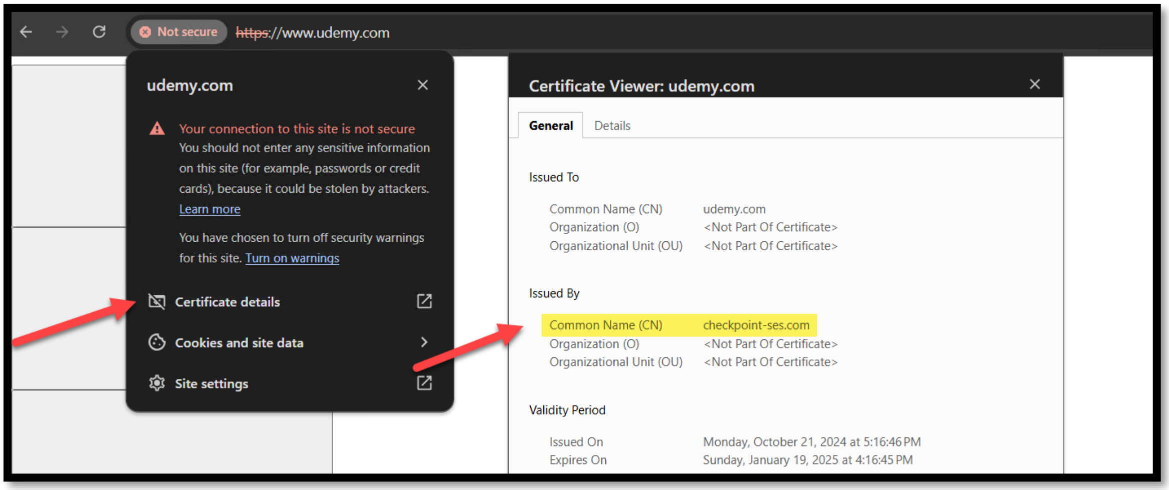
NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

This server could not prove that it is **udemy.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 udemy.com (unsafe)

7. Bypass the security warning by clicking “Proceed to …” (if missing type *thisisunsafe* to bypass the warning). 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.



~~https~~://www.udemy.com

udemy.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

You have chosen to turn off security warnings for this site. Turn on warnings

Certificate details
Cookies and site data
Site settings

Certificate Viewer: udemy.com

General | Details

Issued To

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

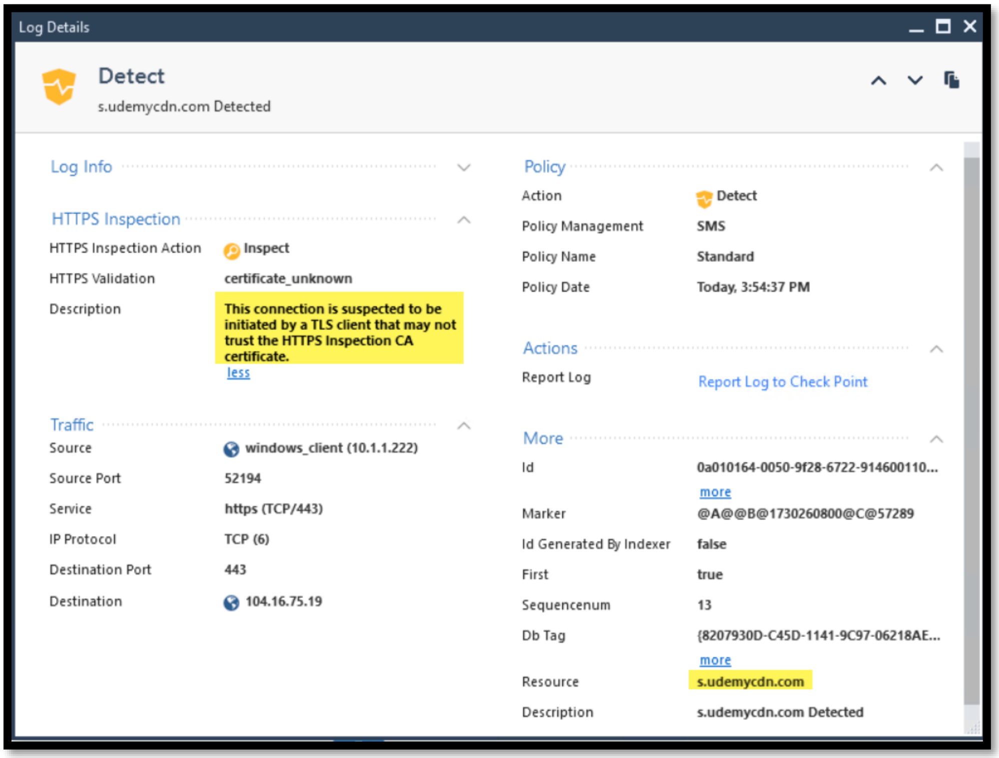
Issued By

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

Validity Period

Issued On	Monday, October 21, 2024 at 5:16:46 PM
Expires On	Sunday, January 19, 2025 at 4:16:45 PM

8. Review the related HTTP Inspection log and notice that the GW logged a warning related to the certificate being untrusted by the client.



Log Details

Detect
s.udemycdn.com Detected

Log Info

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

Source	windows_client (10.1.1.222)
Source Port	52194
Service	https (TCP/443)
IP Protocol	TCP (6)
Destination Port	443
Destination	104.16.75.19

Policy

Action	Detect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 3:54:37 PM

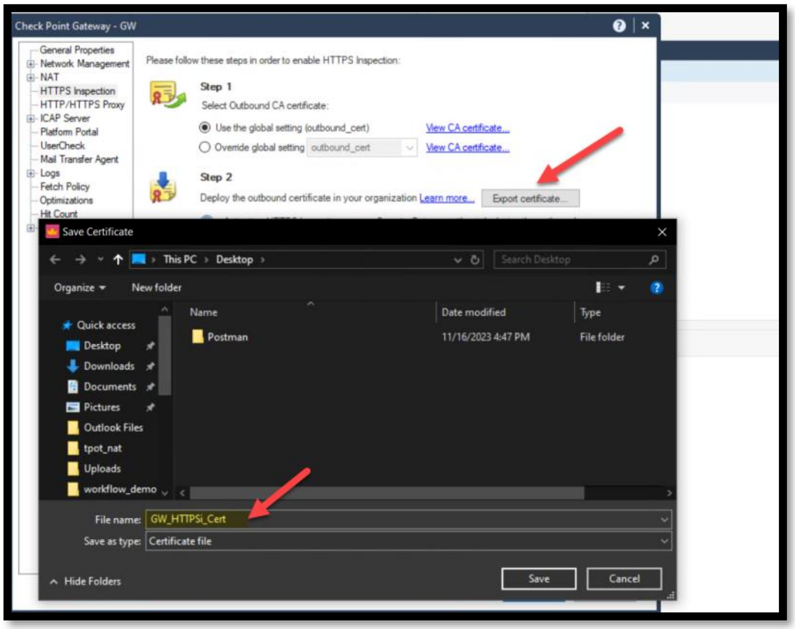
Actions

Report Log	Report Log to Check Point

More

Id	0a010164-0050-9f28-6722-914600110... more
Marker	@A@@B@1730260800@C@57289
Id Generated By Indexer	false
First	true
Sequencenum	13
Db Tag	{8207930D-C45D-1141-9C97-06218AE... more
Resource	s.udemycdn.com
Description	s.udemycdn.com Detected

9. 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...

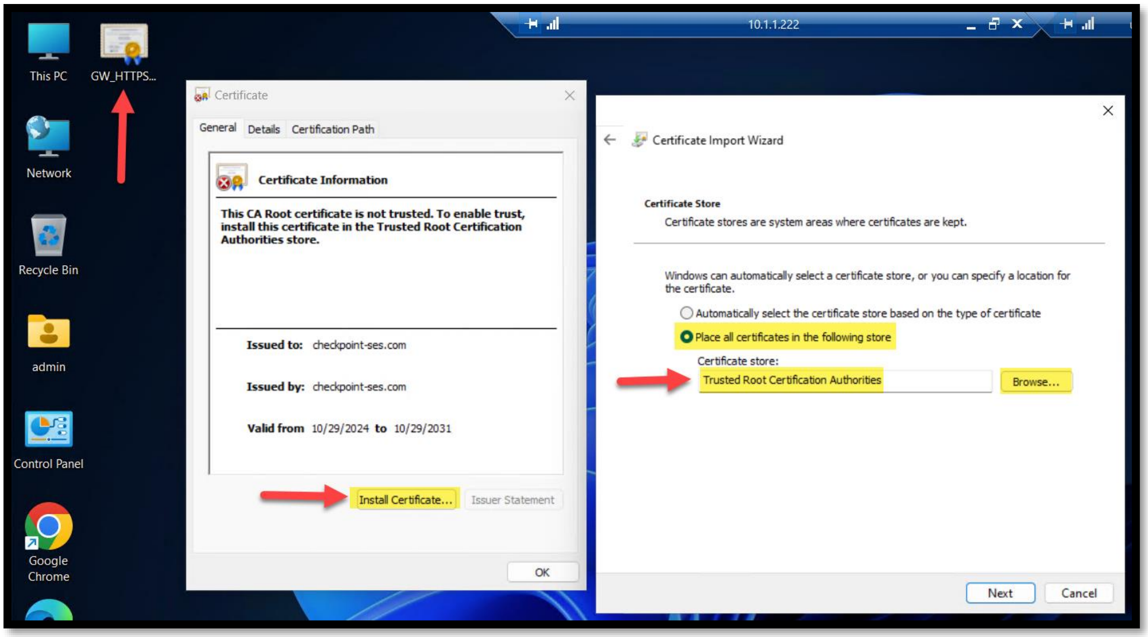
Step 2
Deploy the outbound certificate in your organization Learn more... Export certificate...

Save Certificate

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

File name: GW_HTTPSi_Cert
Save as type: Certificate file

10. Copy the certificate to the win-client machine and install (for store location select local machine) it as a Trusted Root Certification Authorities path. 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 10/29/2024 **to** 10/29/2031

Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

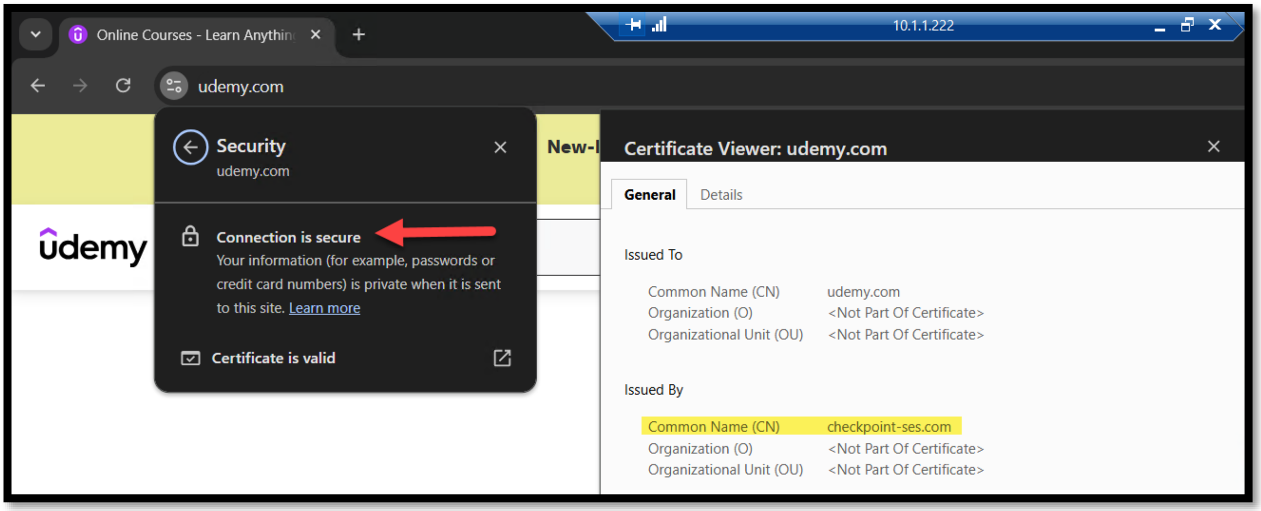
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ 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 you can use GPO in a domain controller environment to deploy the certificate.
- Customer can import their own trusted certificate instead of creating a certificate as we did in the previous steps.
- Chrome uses the windows certificate trust store while Firefox has its own certificate authority store that the CA key must be imported into.

11. Close and reopen chrome and try reaching the website again. Notice that the certificate warning is no longer present.



Security
udemy.com

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: udemy.com

General | Details

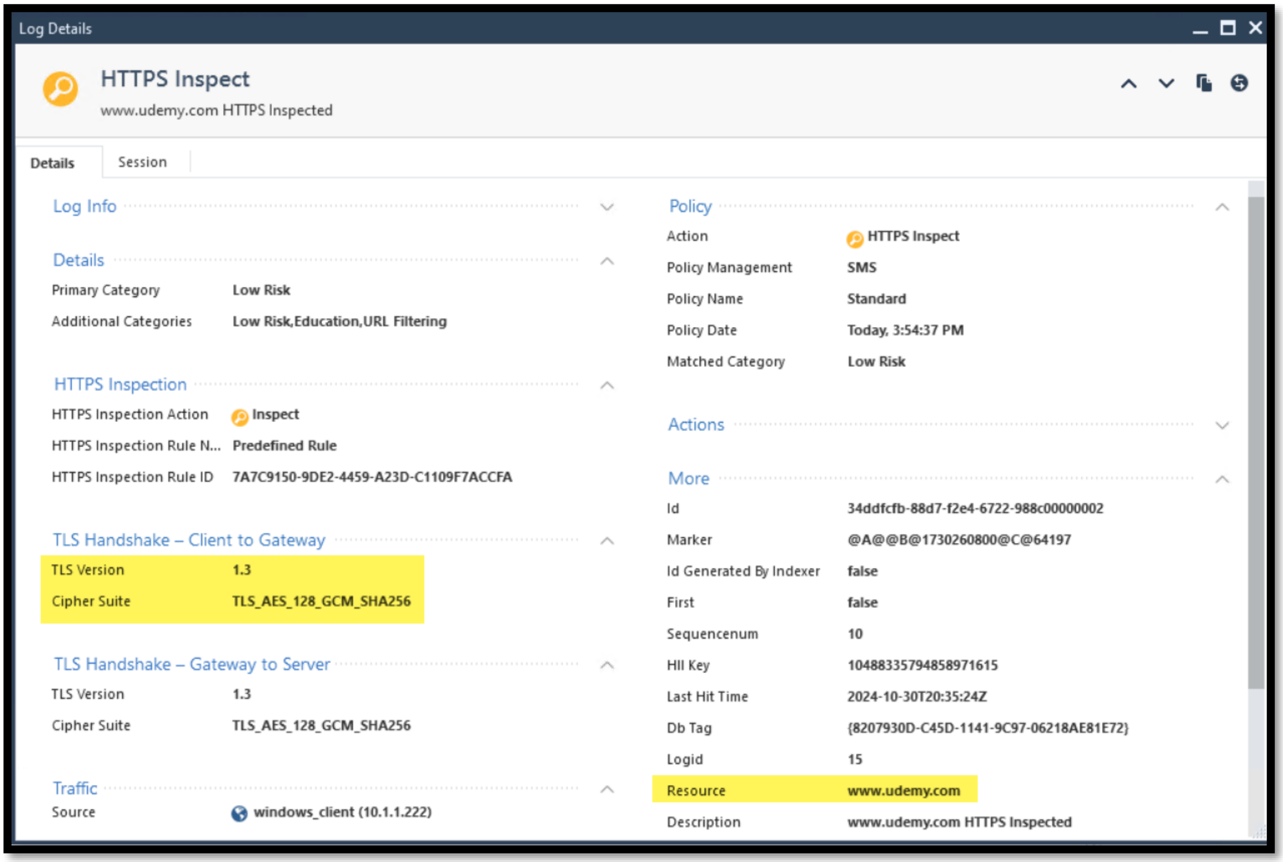
Issued To

Common Name (CN)	udemy.com
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>

12. 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.



HTTPS Inspect
www.udemy.com HTTPS Inspected

Log Info

Details

Primary Category	Low Risk
Additional Categories	Low Risk,Education,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)

Policy

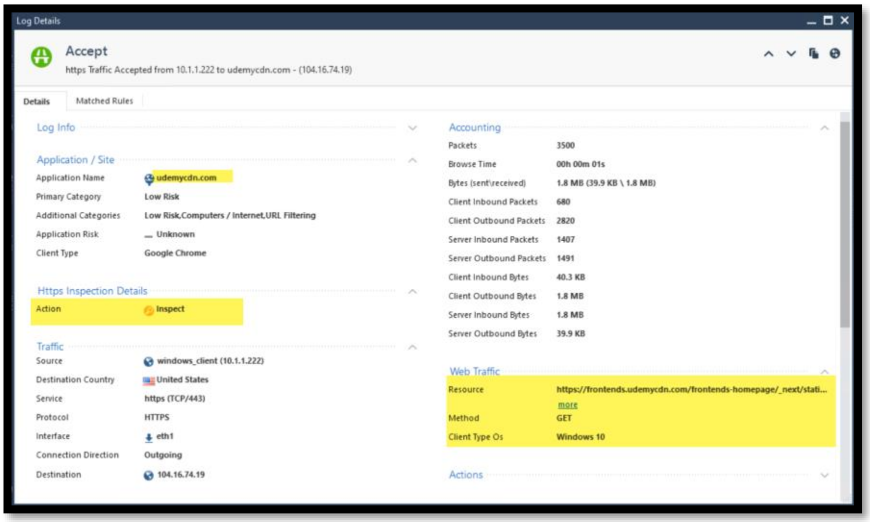
Action	HTTPS Inspect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 3:54:37 PM
Matched Category	Low Risk

Actions

More

Id	34ddfcfb-88d7-f2e4-6722-988c00000002
Marker	@A@@B@1730260800@C@64197
Id Generated By Indexer	false
First	false
Sequencenum	10
Hll Key	10488335794858971615
Last Hit Time	2024-10-30T20:35:24Z
Db Tag	{8207930D-C45D-1141-9C97-06218AE81E72}
Logid	15
Resource	www.udemy.com
Description	www.udemy.com HTTPS Inspected

13. Review the Application Control / URL Filtering log, notice that it is now enhanced with the HTTPS Inspection field.



Accept
https Traffic Accepted from 10.1.1.222 to udemycdn.com - (104.16.74.19)

Log Info

Application / Site

Application Name	udemycdn.com
Primary Category	Low Risk
Additional Categories	Low Risk,Computers / Internet,URL Filtering
Application Risk	Unknown
Client Type	Google Chrome

Https Inspection Details

Action	Inspect

Traffic

Source	windows_client (10.1.1.222)
Destination Country	United States
Service	https (TCP/443)
Protocol	HTTPS
Interface	eth1
Connection Direction	Outgoing
Destination	104.16.74.19

Accounting

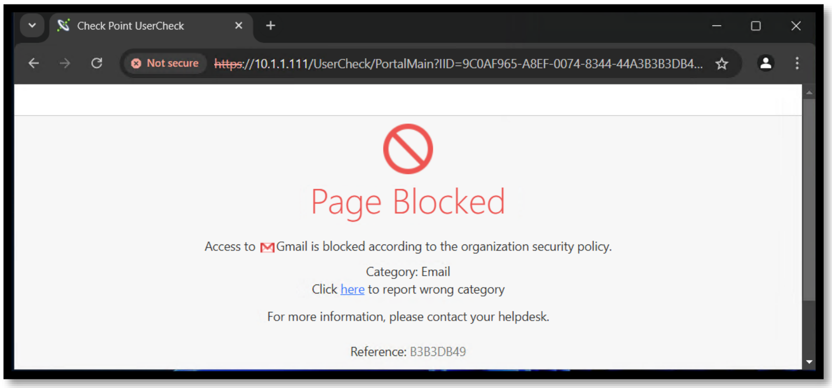
Packets	3500
Browse Time	00h 00m 01s
Bytes (sent\received)	1.8 MB (39.9 KB \ 1.8 MB)
Client Inbound Packets	680
Client Outbound Packets	2820
Server Inbound Packets	1407
Server Outbound Packets	1491
Client Inbound Bytes	40.3 KB
Client Outbound Bytes	1.8 MB
Server Inbound Bytes	1.8 MB
Server Outbound Bytes	39.9 KB

Web Traffic

Resource	https://frontends.udemycdn.com/frontends-homepage/_next/stati... more
Method	GET
Client Type Os	Windows 10

Actions

14. In the previous lab, we blocked access to public Email server, however, we were not returning a block message because of the inability to redirect HTTPS inspection traffic. Try to reach Gmail or any public Email server and notice that block message is now returned successfully.


Check Point UserCheck
Not secure
https://10.1.1.111/UserCheck/PortalMain?IID=9C0AF965-A8EF-0074-8344-44A3B3B3DB4...

Page Blocked

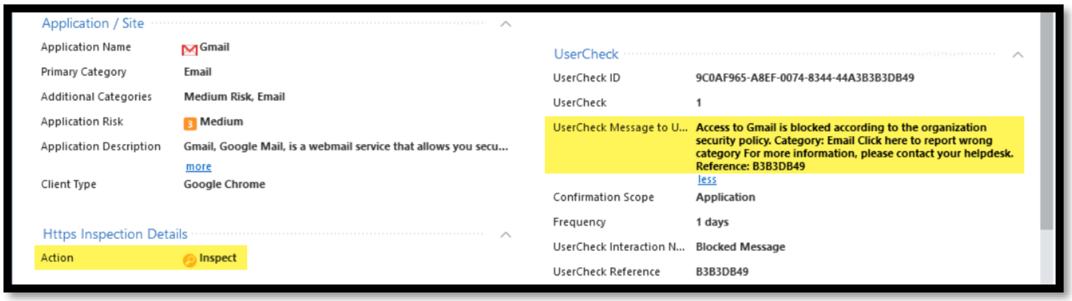
Access to Gmail is blocked according to the organization security policy.

Category: Email
Click here to report wrong category

For more information, please contact your helpdesk.

Reference: B3B3DB49

15. Review the related log.



Application / Site

Application Name	Gmail
Primary Category	Email
Additional Categories	Medium Risk, Email
Application Risk	3 Medium
Application Description	Gmail, Google Mail, is a webmail service that allows you secu... more
Client Type	Google Chrome

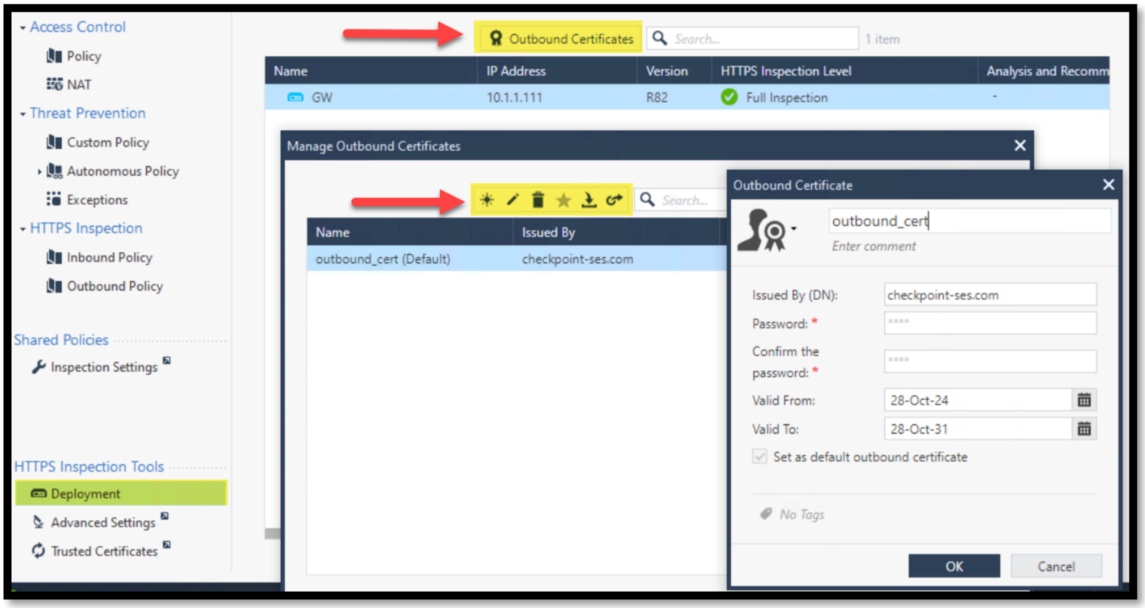
Https Inspection Details

Action	Inspect

UserCheck

UserCheck ID	9C0AF965-A8EF-0074-8344-44A3B3B3DB49
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: B3B3DB49 less
Confirmation Scope	Application
Frequency	1 days
UserCheck Interaction N...	Blocked Message
UserCheck Reference	B3B3DB49

- It is possible to edit, delete and perform multiple operations related to the outbound certificates under the **Deployment** settings.



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

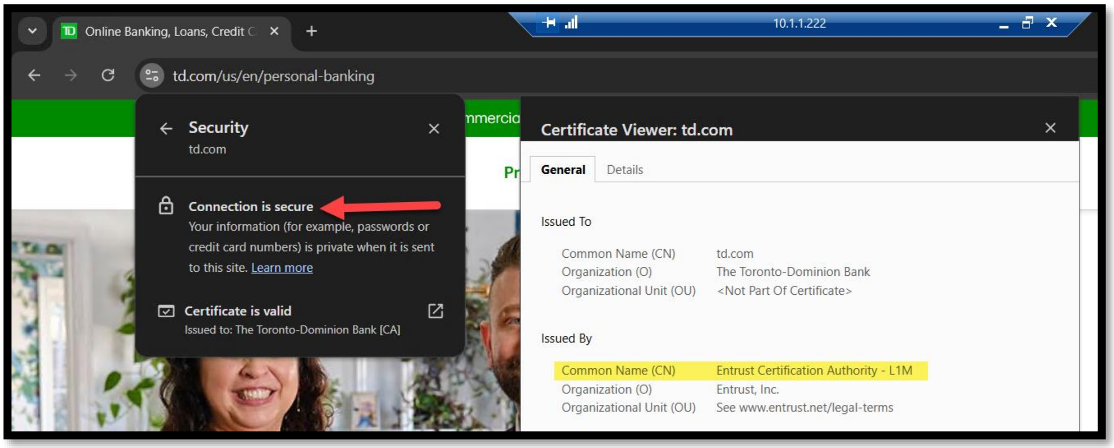
Name	Issued By
outbound_cert (Default)	checkpoint-ses.com

outbound_cert
Enter comment
Issued By (DN): checkpoint-ses.com
Password: * ****
Confirm the password: * ****
Valid From: 28-Oct-24
Valid To: 28-Oct-31
☑ 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), 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 open a financial institution website. For example, https://www.td.com. Review the issuer of the certificate.


Online Banking, Loans, Credit C
10.1.1.222
td.com/us/en/personal-banking
Security
td.com
Certificate Viewer: td.com
General
Details

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
Issued to: The Toronto-Dominion Bank [CA]

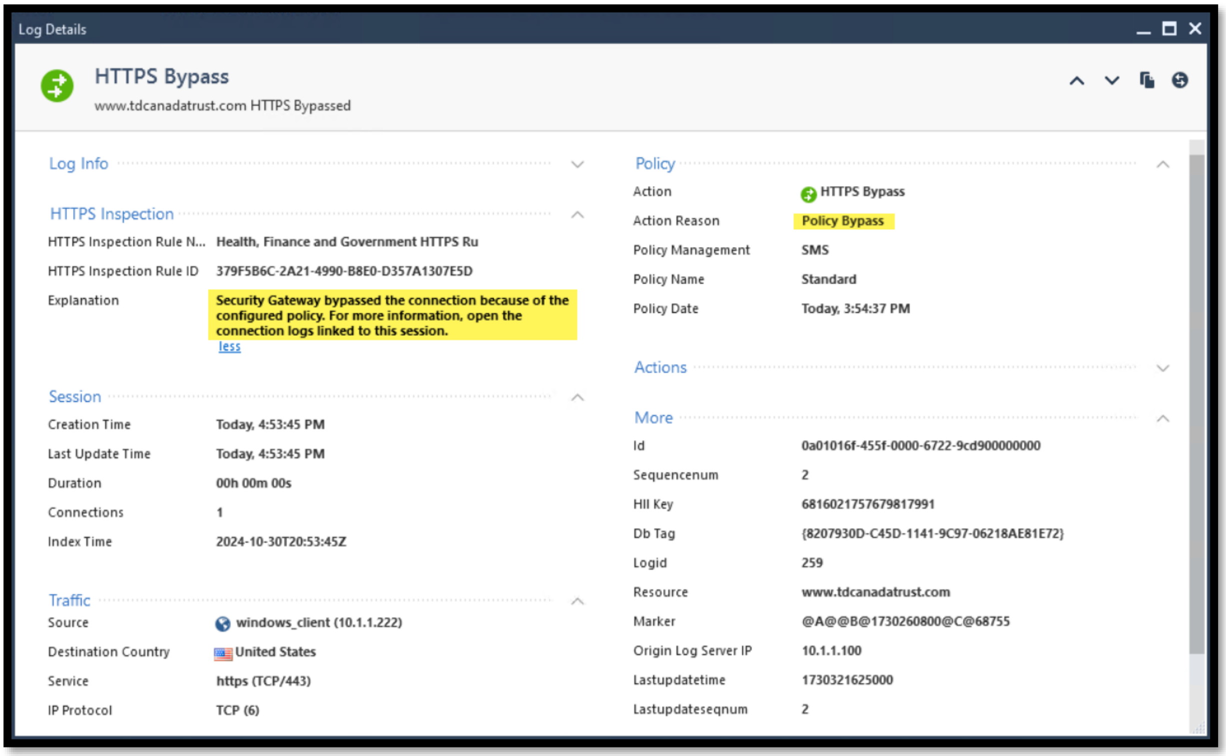
Issued To

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.



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, 4:53:45 PM
Last Update Time	Today, 4:53:45 PM
Duration	00h 00m 00s
Connections	1
Index Time	2024-10-30T20:53:45Z

Traffic

Source	windows_client (10.1.1.222)
Destination Country	United States
Service	https (TCP/443)
IP Protocol	TCP (6)

Policy

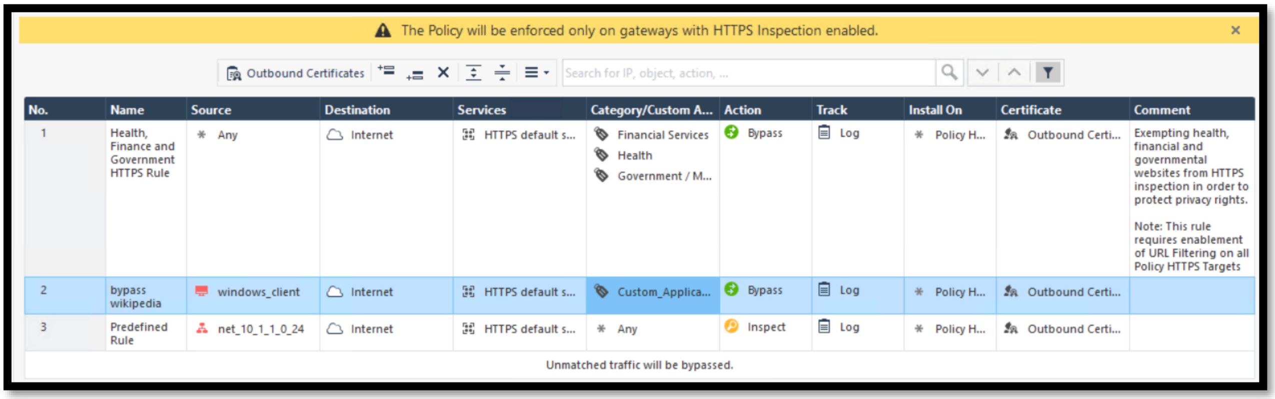
Action	HTTPS Bypass
Action Reason	Policy Bypass
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 3:54:37 PM

Actions

More

Id	0a01016f-455f-0000-6722-9cd900000000
Sequencenum	2
Hll Key	6816021757679817991
Db Tag	{8207930D-C45D-1141-9C97-06218AE81E72}
Logid	259
Resource	www.tdcanadatrust.com
Marker	@A@@B@1730260800@C@68755
Origin Log Server IP	10.1.1.100
Lastupdatetime	1730321625000
Lastupdateseqnum	2

3. Create a new rule below the existing bypass rule, use the custom application object. We created override categorization object in a previous lab. We will use the same object to bypass inspecting traffic to Wikipedia.org.



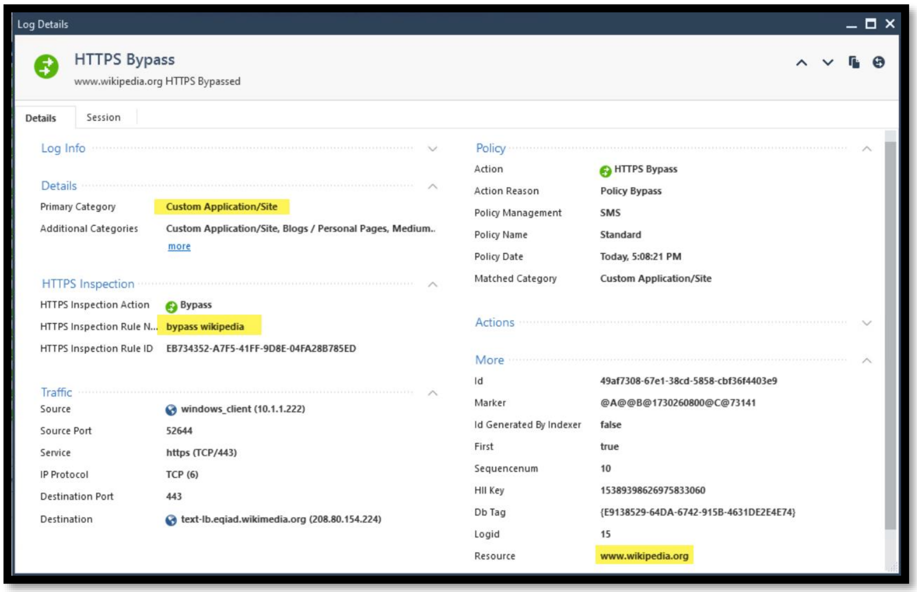
The Policy will be enforced only on gateways with HTTPS Inspection enabled.

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	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 windows-client try to reach Wikipedia.org.
    - Notice that we are no longer presented with a block message since the connection is not inspected by HTTPS Inspection and we are no longer able to redirect HTTPS sites.

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

Log Info

Details

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

HTTPS Inspection

HTTPS Inspection Action	Bypass
HTTPS Inspection Rule N...	bypass wikipedia
HTTPS Inspection Rule ID	EB734352-A7F5-41FF-9D8E-04FA28B785ED

Traffic

Source	windows_client (10.1.1.222)
Source Port	52644
Service	https (TCP/443)
IP Protocol	TCP (6)
Destination Port	443
Destination	text-lb.eqiad.wikimedia.org (208.80.154.224)

Policy

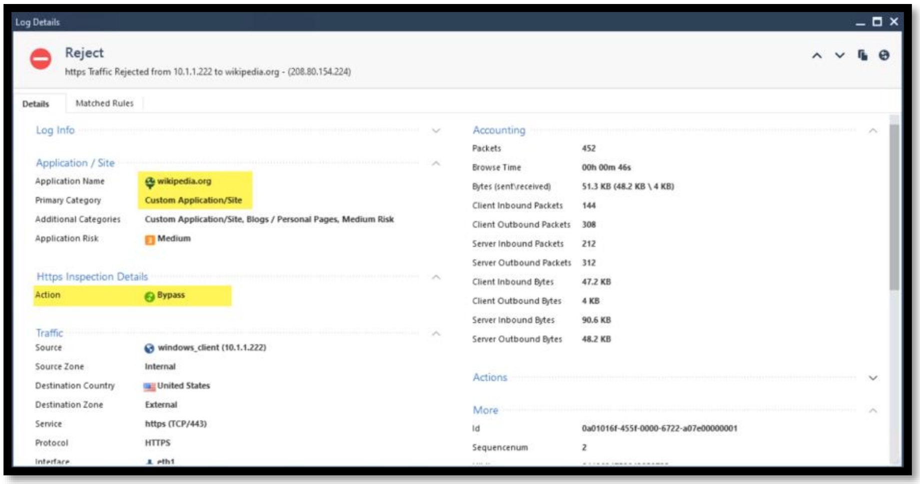
Action	HTTPS Bypass
Action Reason	Policy Bypass
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 5:08:21 PM
Matched Category	Custom Application/Site

Actions

More

Id	49af7308-67e1-38cd-5858-cbf36f4403e9
Marker	@A@@B@1730260800@C@73141
Id Generated By Indexer	false
First	true
Sequencenum	10
Hll Key	15389398626975833060
Db Tag	{E9138529-64DA-6742-915B-4631DE2E4E74}
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)

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	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

Accounting

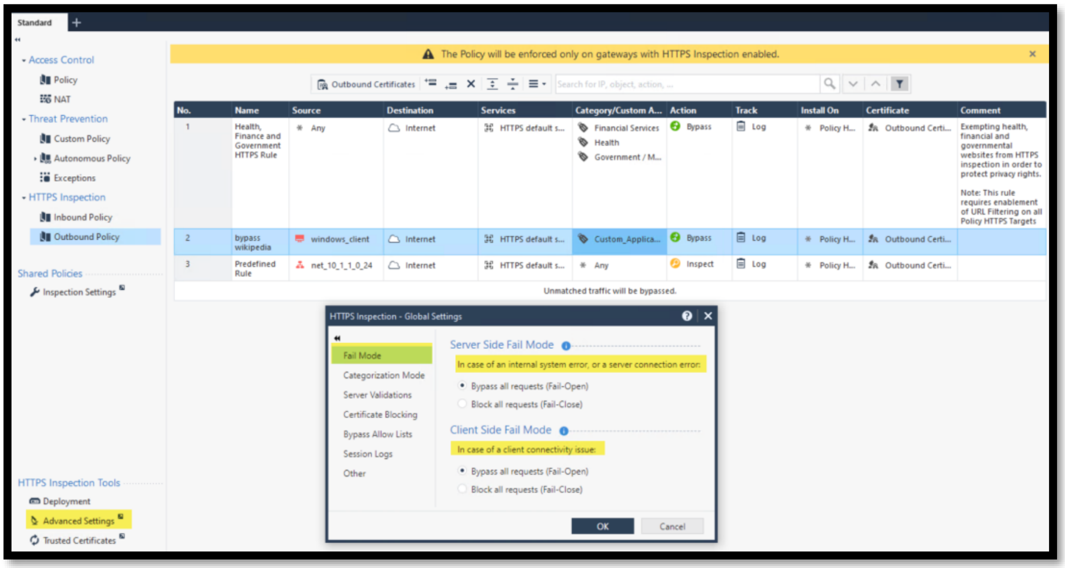
Packets	452
Browse Time	00h 00m 46s
Bytes (sent\received)	51.3 KB (48.2 KB \ 4 KB)
Client Inbound Packets	144
Client Outbound Packets	308
Server Inbound Packets	212
Server Outbound Packets	312
Client Inbound Bytes	47.2 KB
Client Outbound Bytes	4 KB
Server Inbound Bytes	90.6 KB
Server Outbound Bytes	48.2 KB

Actions

More

Id	0a01016f-455f-0000-6722-a07e00000001
Sequencenum	2

7. Open the Advanced Settings and review the default fail modes.
    a. The client side fail mode controls issues on the client side
    b. The server side fail mode controls:
        i. Engine failures
        ii. Server issues.



Standard

- Access Control
  - Policy
  - NAT
- Threat Prevention
  - Custom Policy
  - Autonomous Policy
  - Exceptions
- HTTPS Inspection
  - Inbound Policy
  - Outbound Policy

Shared Policies
- Inspection Settings

HTTPS Inspection Tools
- Deployment
- Advanced Settings
- Trusted Certificates

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.

HTTPS Inspection - Global Settings

- Fail Mode
- Categorization Mode
- Server Validations
- Certificate Blocking
- Bypass Allow Lists
- Session Logs
- Other

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

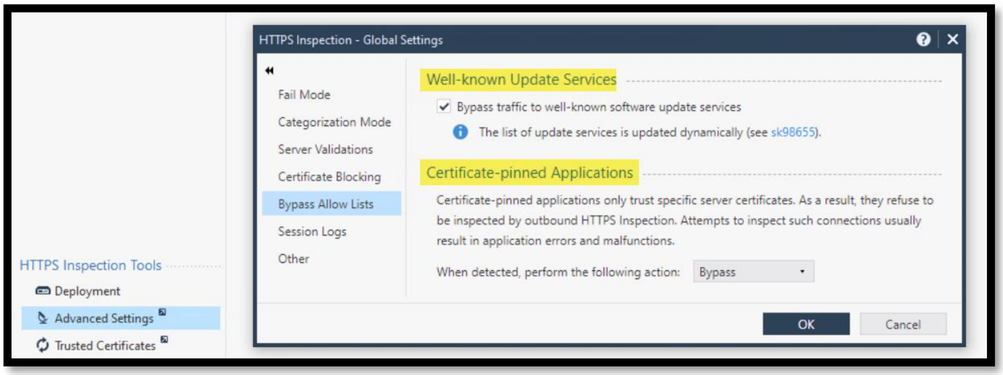
In case of a client connectivity issue:

● Bypass all requests (Fail-Open)

○ Block all requests (Fail-Close)

OK | Cancel

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



HTTPS Inspection Tools
- Deployment
- Advanced Settings
- Trusted Certificates

HTTPS Inspection - Global Settings

- Fail Mode
- Categorization Mode
- Server Validations
- Certificate Blocking
- Bypass Allow Lists
- Session Logs
- Other

Well-known Update Services

☑ Bypass traffic to well-known software update services

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

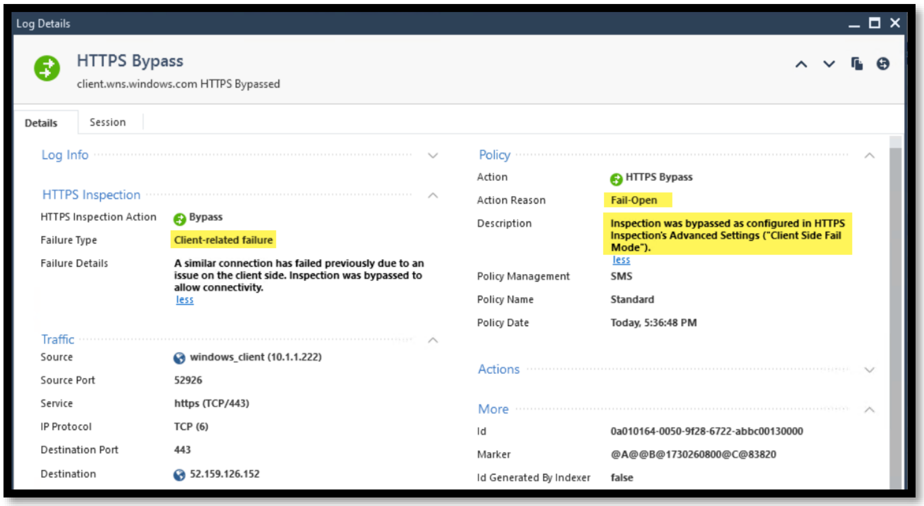
Certificate-pinned Applications

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

OK | Cancel

9. Review the HTTPS Inspection bypass logs. Find logs related to bypass based on the advanced settings.



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

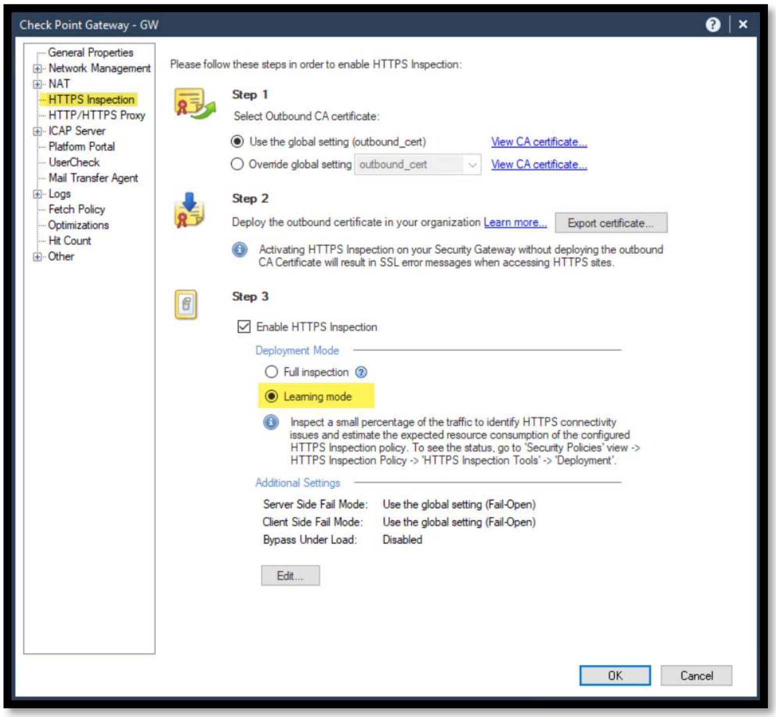
More

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" and install the access policy.



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

Deployment Mode

○ Full inspection

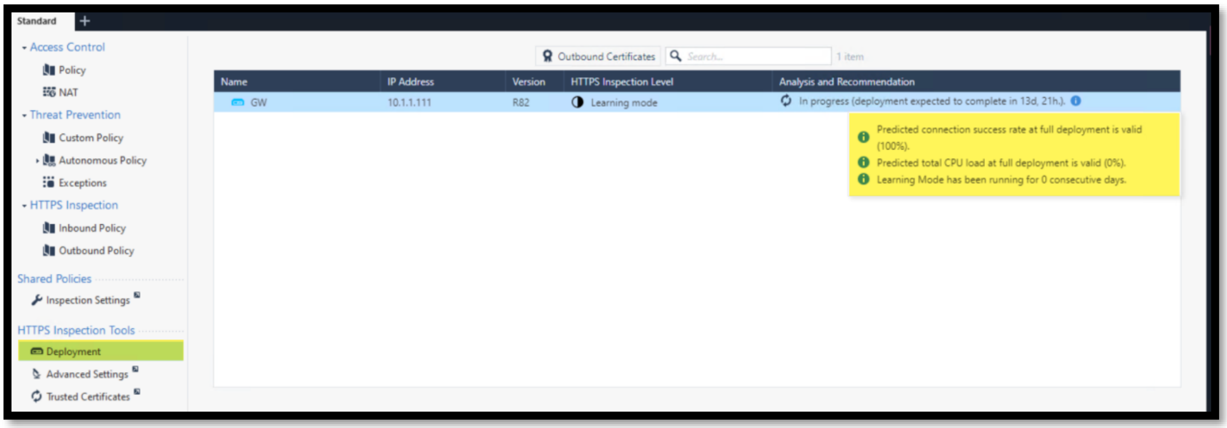
● Learning mode

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

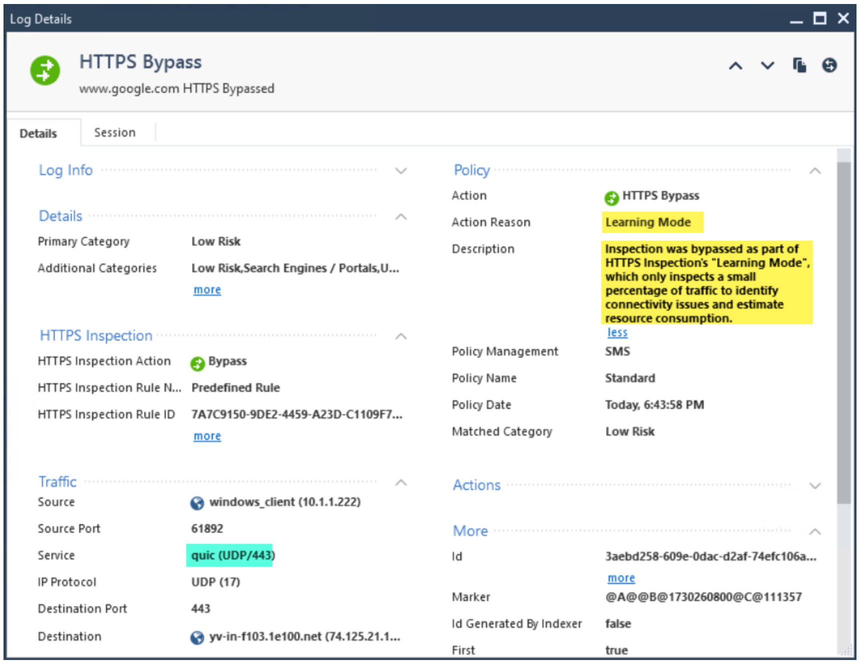
2. Review the GW status under Deployment



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.

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



Log Details

HTTPS Bypass
www.google.com HTTPS Bypassed

Details | Session

Log Info

Details

Primary Category	Low Risk
Additional Categories	Low Risk,Search Engines / Portals,U... more

HTTPS Inspection

HTTPS Inspection Action	Bypass
HTTPS Inspection Rule N...	Predefined Rule
HTTPS Inspection Rule ID	7A7C9150-9DE2-4459-A23D-C1109F7... more

Traffic

Source	windows_client (10.1.1.222)
Source Port	61892
Service	quic (UDP/443)
IP Protocol	UDP (17)
Destination Port	443
Destination	yv-in-f103.1e100.net (74.125.21.1...

Policy

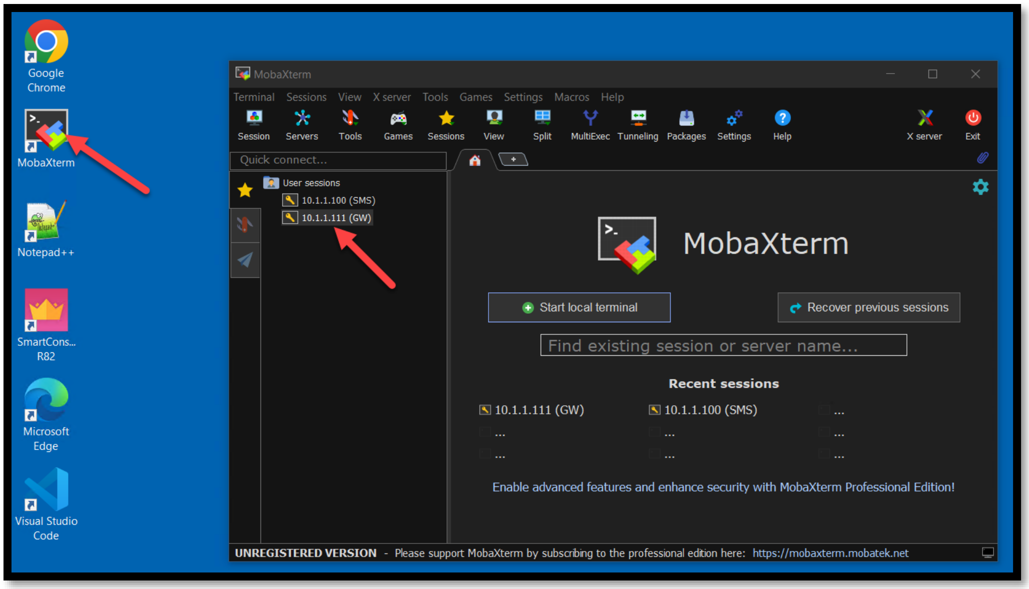
Action	HTTPS Bypass
Action Reason	Learning Mode
Description	Inspection was bypassed as part of HTTPS Inspection's "Learning Mode", which only inspects a small percentage of traffic to identify connectivity issues and estimate resource consumption. less
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 6:43:58 PM
Matched Category	Low Risk

Actions

More

Id	3aebd258-609e-0dac-d2af-74efc106a... more
Marker	@A@@B@1730260800@C@111357
Id Generated By Indexer	false
First	true

4. To see more details, use the SSH client MobaXterm, and open the GW saved session.

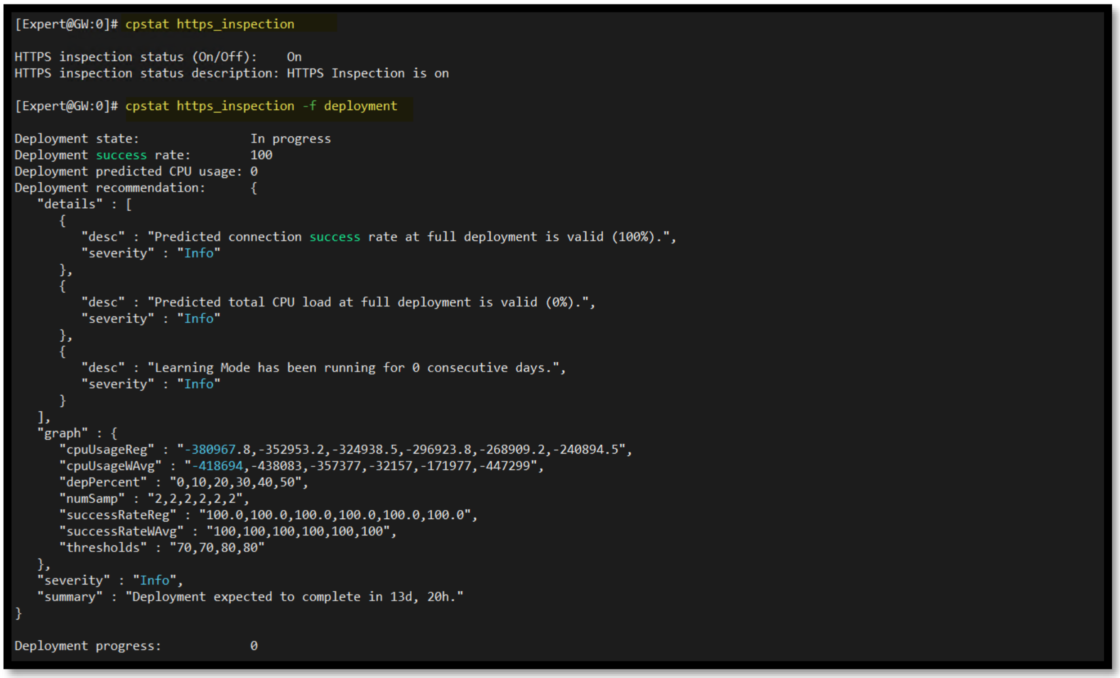

Google Chrome
MobaXterm
Notepad++
SmartCons... R82
Microsoft Edge
Visual Studio Code
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
User sessions
10.1.1.100 (SMS)
10.1.1.111 (GW)
MobaXterm
Start local terminal
Recover previous sessions
Find existing session or server name...
Recent sessions
10.1.1.111 (GW)
10.1.1.100 (SMS)

Enable advanced features and enhance security with MobaXterm Professional Edition!

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

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

```
cpstat https_inspection -f deployment
```

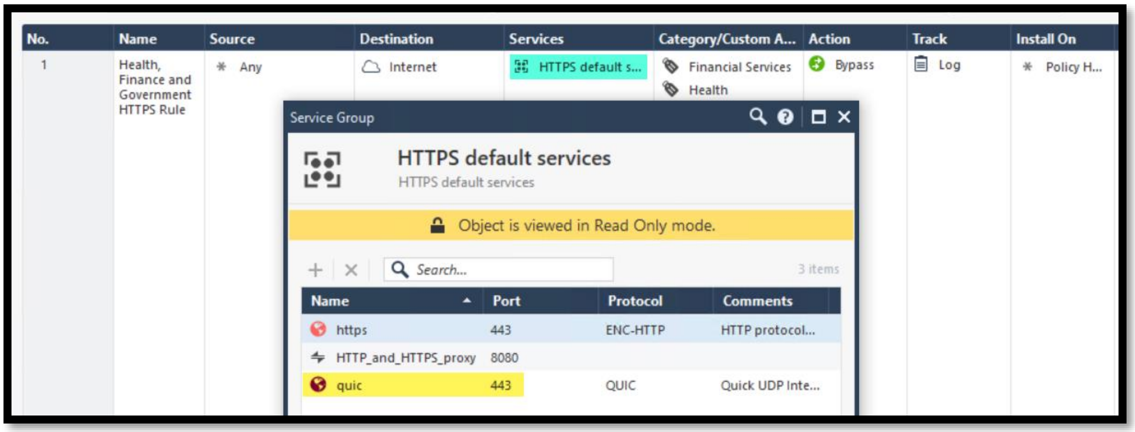


```
[Expert@GW:0]# cpstat https_inspection

HTTPS inspection status (On/Off):    On
HTTPS inspection status description: HTTPS Inspection is on

[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" : "-380967.8,-352953.2,-324938.5,-296923.8,-268909.2,-240894.5",
      "cpuUsageWAvg" : "-418694,-438083,-357377,-32157,-171977,-447299",
      "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. 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.



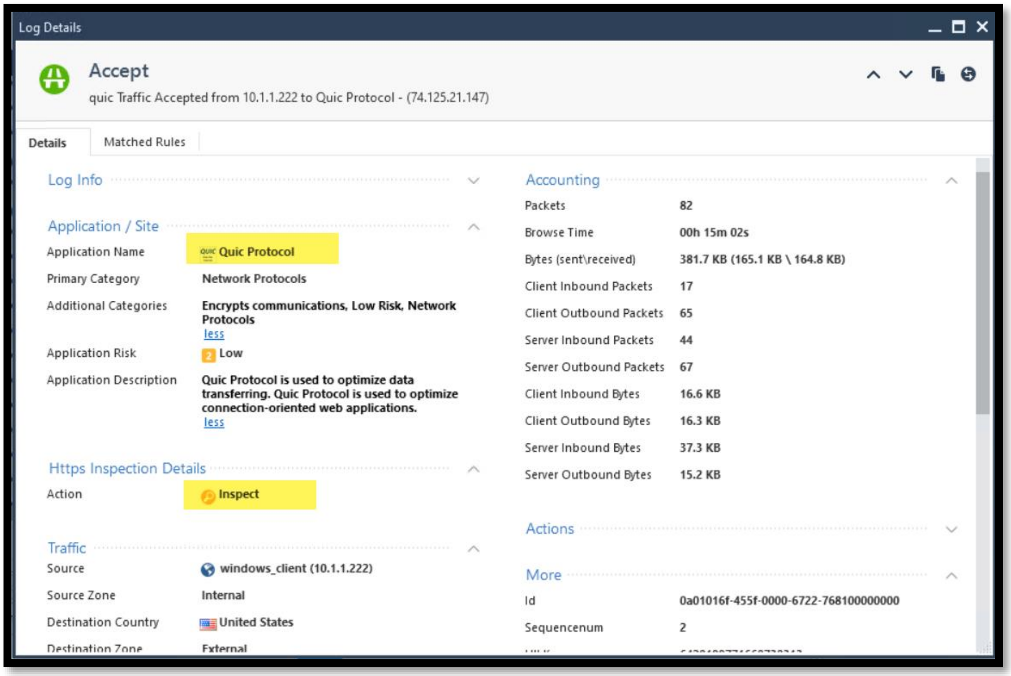
No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On
1	Health, Finance and Government HTTPS Rule	Any	Internet	HTTPS default s...	Financial Services Health	Bypass	Log	Policy H...

HTTPS default services
HTTPS default services

Object is viewed in Read Only mode.

Name	Port	Protocol	Comments
https	443	ENC-HTTP	HTTP protocol...
HTTP_and_HTTPS_proxy	8080		
quic	443	QUIC	Quick UDP Inte...

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

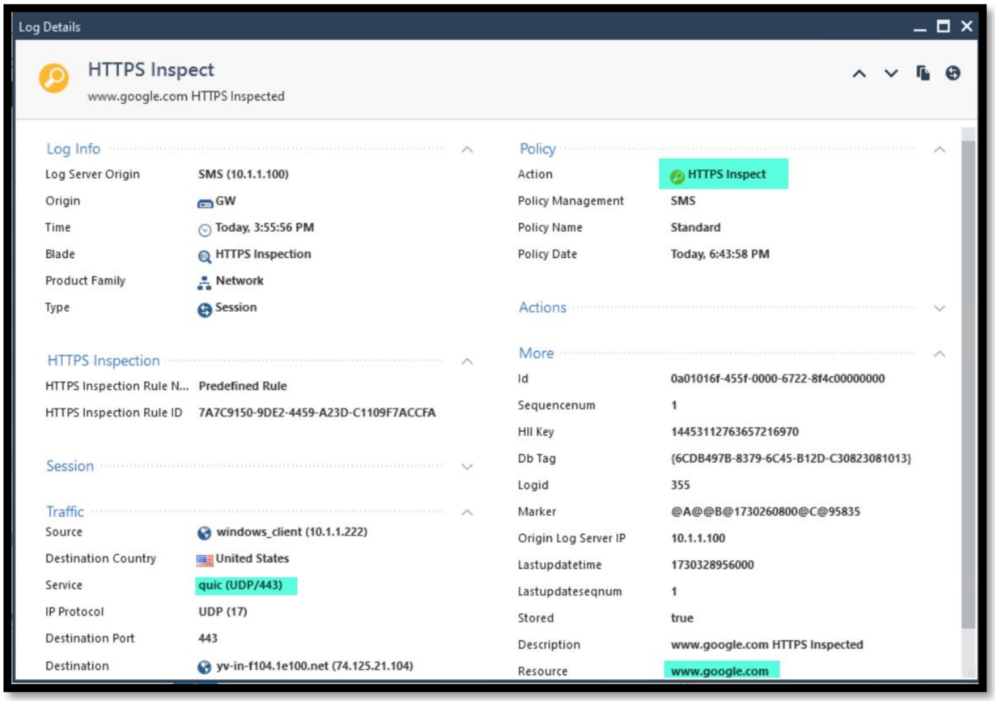
Packets	82
Browse Time	00h 15m 02s
Bytes (sent\received)	381.7 KB (165.1 KB \ 164.8 KB)
Client Inbound Packets	17
Client Outbound Packets	65
Server Inbound Packets	44
Server Outbound Packets	67
Client Inbound Bytes	16.6 KB
Client Outbound Bytes	16.3 KB
Server Inbound Bytes	37.3 KB
Server Outbound Bytes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

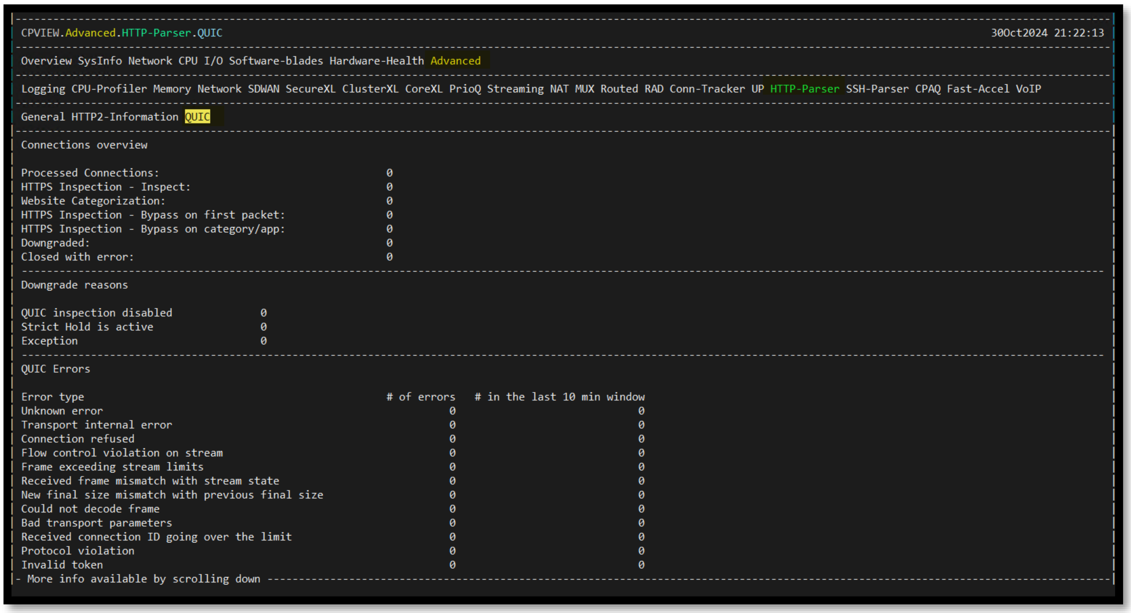
Action	HTTPS Inspect
Policy Management	SMS
Policy Name	Standard
Policy Date	Today, 6:43:58 PM

Actions

More

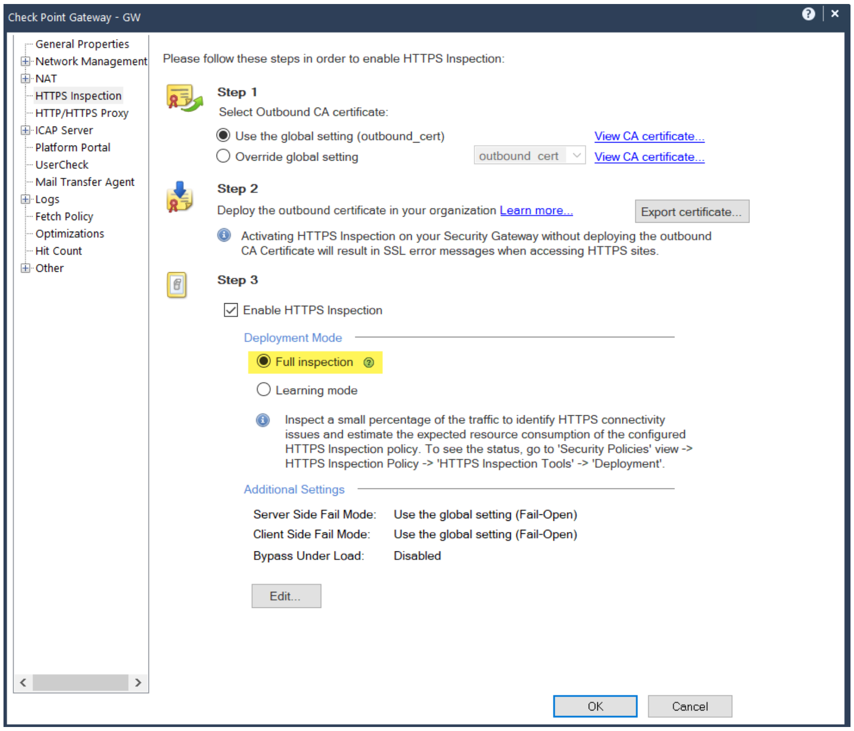
Id	0a01016f-455f-0000-6722-8f4c00000000
Sequencenum	1
Hll Key	14453112763657216970
Db Tag	{6CDB497B-8379-6C45-B12D-C30823081013}
Logid	355
Marker	@A@@B@1730260800@C@95835
Origin Log Server IP	10.1.1.100
Lastupdatetime	1730328956000
Lastupdateseqnum	1
Stored	true
Description	www.google.com HTTPS Inspected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



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

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

End of Lab 2