



R82 TLS Inspection Enhancements

HTTP/3 INSPECTION

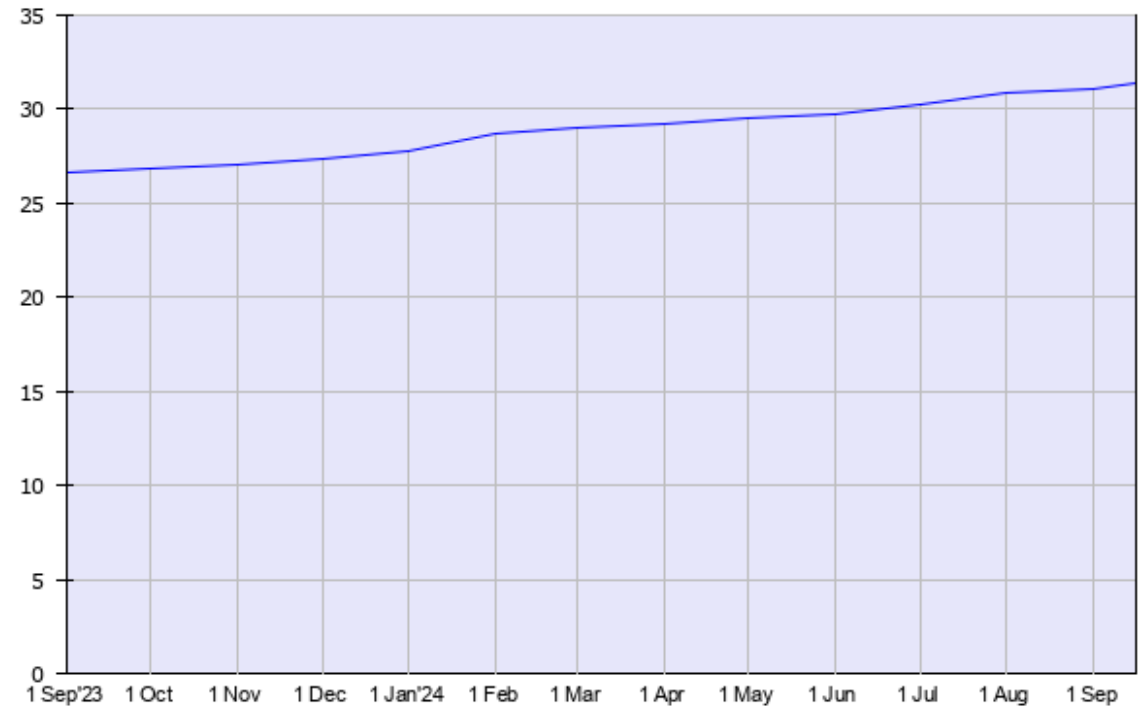
Hadi Frohar

17/09/2024

YOU DESERVE THE BEST SECURITY

HTTP/3 Overview

- HTTP/3: Built on QUIC for Faster and More Secure Connections
 - Faster Connections
 - Enhanced Congestion Control
 - Multiplexed
 - Header compression
- As of September 2024
31.3% of all websites use HTTP/3



Usage of HTTP/3 for websites, 16 Sep 2024, W3Techs.com

HTTP/3 Inspection

- HTTP/3 inspection is enabled by default
 - QUIC service is part of HTTPS default services
- Categorize HTTPS websites is enabled by default
 - For bypassed traffic
- Outbound/inbound inspection
- Same functionalities as in HTTP/2



Supported Versions and Limitations

- **Supported versions:** R82 and above
- **Supported architectures:** security gateway, cluster, VSX
- **Limitations**
 - USFW mode only: HTTP/3 inspection is not supported in kernel mode
 - Deep-inspection is not supported yet
 - Content awareness blade is not supported yet



Quantum

HTTP/3 inspection – example

Access policy

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Cloudflare accept	* Any	* Any	Cloudflare custom-...	Accept	Log Accounting	* Policy Targets
2	Facebook drop-block	* Any	* Any	Facebook	Drop Blocked Messa...	Log Accounting	* Policy Targets
3	Any-any-accept	* Any	* Any	* Any	Accept	None	* Policy Targets

HTTPS outbound policy

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate
1	Client 113 bypass	client_113	Internet	HTTPS default s...	* Any	Bypass	Log	* Policy H...	Outbound Certi...
2	Predefined Rule	* Any	Internet	HTTPS default s...	* Any	Inspect	Log	* Policy H...	Outbound Certi...

Unmatched traffic will be bypassed.

HTTP/3 inspection – example

Inspected HTTP/3 connection
with HTTPS inspection certificate

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `https://cloudflare-quick.com`. A security warning dialog is open, stating: "Connection security for cloudflare-quick.com. You are securely connected to this site. Verified by: www.checkpoint.com. Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More." Below the dialog, the page content includes the Cloudflare logo and the heading "Does my browser support HTTP/3 & QUIC?". A red box highlights a paragraph: "When loading this page from Cloudflare's edge network, your browser used HTTP/3." Below this, it says "This page is HTTP/3 & QUIC enabled. Try reloading a few times to spring it into action." At the bottom, the Network Inspector is open, showing a table of requests. A red box highlights the "Protocol" column, which shows "HTTP/3" for the first three requests.

Status	Met...	Domain	File	Protocol	Initiator	Type	Transferred	Size	0 m
200	GET	cloudflare-quick.com	/	HTTP/3	BrowserTabChild.j...	html	13.22 KB	123.01 KB	12
200	GET	www.cloudflar...	logo-cloudflare-dark.svg	HTTP/3	img	svg	1.89 KB	1.98 KB	30
200	GET	www.cloudflar...	logo-cloudflare.svg	HTTP/3	img	svg	1.90 KB	1.97 KB	28

HTTP/3 inspection – example

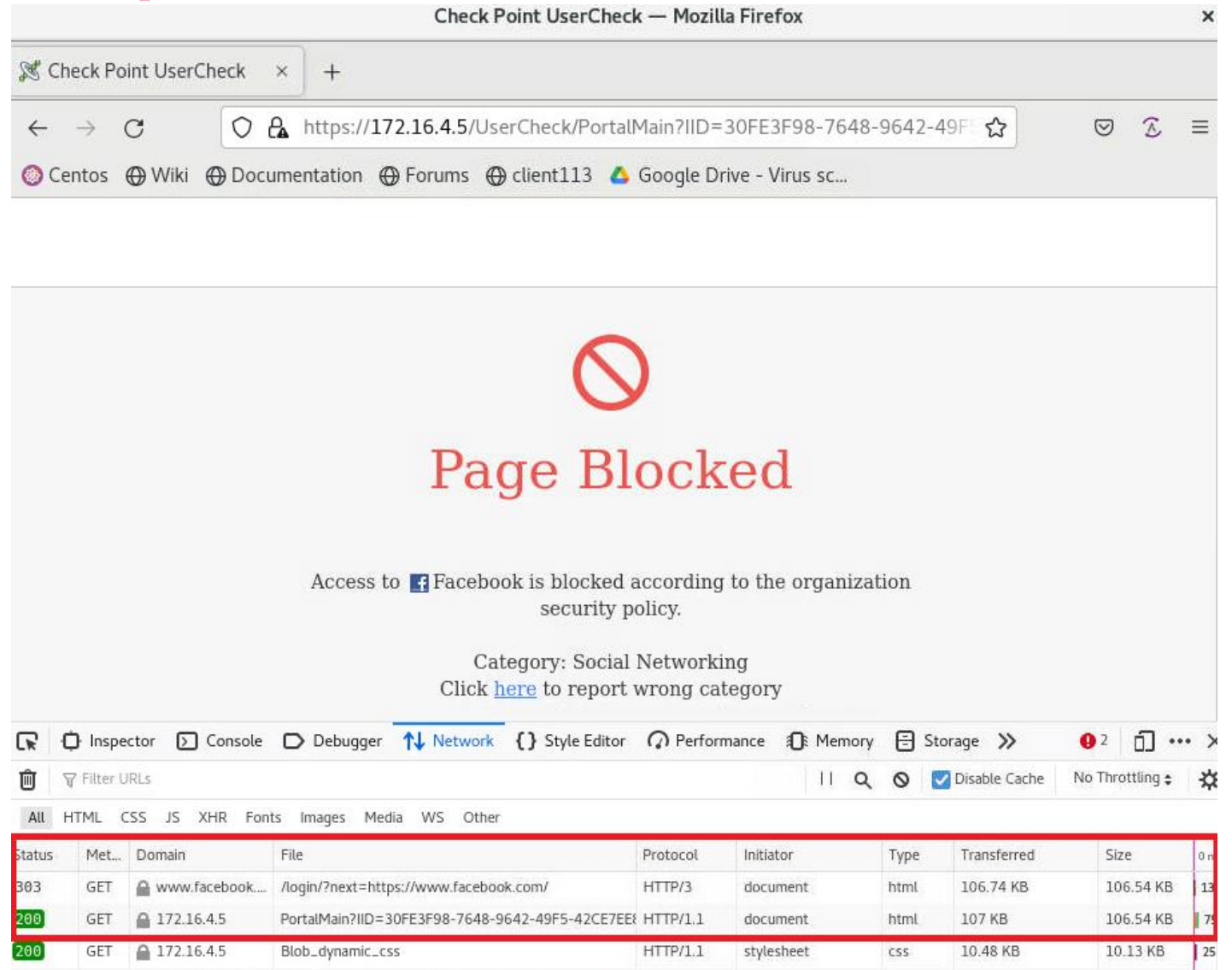
Inspected HTTP/3 connection
matched on custom application

The screenshot displays the 'Log Details' window for an 'Accept' event. The event description is 'quic Traffic Accepted from 10.1.1.111 to 172.67.9.235'. The 'Session' tab is selected, showing various details:

- Log Info:** Origin (GW5), Time (Today, 2:51:23 PM), Blade (URL Filtering), Product Family (Access), Type (Session).
- Application / Site:** Application Name (Cloudflare custom-application), Primary Category (Custom Application/Site), Additional Categories (Custom Application/Site), Application Risk (Unknown), Server Type (Other: cloudflare), Client Type (Firefox).
- Https Inspection Details:** Action (Inspect).
- Traffic:** Source (10.1.1.111), Source Zone (Internal), Destination Zone (External), Service (quic (UDP/443)).
- Accounting:** Packets (76), Browse Time (00h 01m 01s), Bytes (sent\received) (22.8 KB (4 KB \ 17.5 KB)), Client Inbound Packets (17), Client Outbound Packets (59), Server Inbound Packets (29), Server Outbound Packets (36), Client Inbound Bytes (5.3 KB), Client Outbound Bytes (17.5 KB), Server Inbound Bytes (20.5 KB), Server Outbound Bytes (4 KB).
- Web Traffic:** Resource (https://cloudflare-quic.com/), Method (GET), Server Type (Other: cloudflare).
- Actions:** Report Log (Report Log to Check Point).
- More:** (expandable section).

HTTP/3 inspection – example

Inspected HTTP/3 connection redirected to block page




Check Point UserCheck — Mozilla Firefox

Check Point UserCheck x +

https://172.16.4.5/UserCheck/PortalMain?IID=30FE3F98-7648-9642-49F5-42CE7EE... ☆

Centos Wiki Documentation Forums client113 Google Drive - Virus sc...

Page Blocked

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

Category: Social Networking
Click [here](#) to report wrong category

Inspector Console Debugger Network Style Editor Performance Memory Storage 2

Filter URLs Disable Cache No Throttling

Status	Met...	Domain	File	Protocol	Initiator	Type	Transferred	Size	0 r
303	GET	www.facebook...	/login/?next=https://www.facebook.com/	HTTP/3	document	html	106.74 KB	106.54 KB	13
200	GET	172.16.4.5	PortalMain?IID=30FE3F98-7648-9642-49F5-42CE7EE...	HTTP/1.1	document	html	107 KB	106.54 KB	75
200	GET	172.16.4.5	Blob_dynamic.css	HTTP/1.1	stylesheet	css	10.48 KB	10.13 KB	25

HTTP/3 inspection – example

Inspected HTTP/3 connection
redirected to block page

The screenshot shows a 'Log Details' window with a 'Block' status. The main header indicates 'quic Traffic Blocked from 10.1.1.111 to 157.240.0.35'. The 'Session' tab is active, displaying various details:

- Log Info:** Origin: GW5, Time: Today, 2:58:50 PM, Blade: Application Control, Product Family: Access, Type: Session.
- Application / Site:** Application Name: Facebook, Primary Category: Social Networking, Additional Categories: Low Risk, Social Networking, Application Risk: Low, Application Description: Facebook is a social utility that helps..., Client Type: Firefox.
- Https Inspection Details:** Action: Inspect.
- Traffic:** Source: 10.1.1.111, Source Zone: Internal, Destination Zone: External.
- Accounting:** Packets: 125, Browse Time: 00h 03m 19s, Bytes (sent\received): 15.1 KB (4.2 KB \ 7.9 KB), Client Inbound Packets: 54, Client Outbound Packets: 71, Server Inbound Packets: 33, Server Outbound Packets: 84, Client Inbound Bytes: 7.2 KB, Client Outbound Bytes: 7.9 KB, Server Inbound Bytes: 12.9 KB, Server Outbound Bytes: 4.2 KB.
- UserCheck:** UserCheck ID: 30FE3F98-7648-9642-49F5-42CE7EE8..., UserCheck: 1, UserCheck Message to U...: Access to Facebook is blocked accord..., Confirmation Scope: Application, Frequency: 1 days, UserCheck Interaction N...: Blocked Message, UserCheck Reference: 7EE86C44.

HTTP/3 inspection – example

Access policy

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Cloudflare accept	* Any	* Any	Cloudflare custom-...	Accept	Log Accounting	* Policy Targets
2	Facebook drop-block	* Any	* Any	Facebook	Drop Blocked Messa...	Log Accounting	* Policy Targets
3	Any-any-accept	* Any	* Any	* Any	Accept	None	* Policy Targets

HTTPS outbound policy

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Install On	Certificate
1	Client 113 bypass	client_113	Internet	HTTPS default s...	* Any	Bypass	Log	* Policy H...	Outbound Certi...
2	Predefined Rule	* Any	Internet	HTTPS default s...	* Any	Inspect	Log	* Policy H...	Outbound Certi...

Unmatched traffic will be bypassed.

HTTP/3 inspection – example

Bypassed HTTP/3 connection
with server certificate

QUIC | Cloudflare — Mozilla Firefox

QUIC | Cloudflare x +

← → ↻ 🔒 https://cloudflare-quic.com ☆ 🔒 ☰

Centos Wiki Docu

🔒 Connection security for cloudflare-quic.com

🔒 You are securely connected to this site.

Verified by: Google Trust Services

More Information

CLOUDFLARE

Does my browser support HTTP/3 & QUIC?

When loading this page from Cloudflare's edge network, your browser used HTTP/3.

This page is HTTP/3 & QUIC enabled. Try

Inspector Console Debugger Network Style Editor Performance Memory Storage

Filter URLs Disable Cache No Throttling

Status	Method	Domain	File	Protocol	Initiator	Type	Transferred	Size	0 ms	: 5
200	GET	cloudflare-qui...	/	HTTP/3	BrowserTabChild...	html	13.23 KB	123.0...	124 ms	
200	GET	www.cloudfla...	logo-cloudflare-dark.svg	HTTP/3	img	svg	1.88 KB	1.98 KB	129 ms	

11 requests 497.09 KB / 392.98 KB transferred Finish: 2.19 s DOMContentLoaded: 187 ms load: 1.69 s

HTTP/3 inspection – example

Bypassed HTTP/3 connection
matched on custom application

Log Details

Accept
quic Traffic Accepted from 10.1.1.113 to 104.22.9.38

Details | Matched Rules | **Session**

Log Info

Origin	GW5
Time	Today, 3:17:47 PM
Blade	URL Filtering
Product Family	Access
Type	Session

Application / Site

Application Name	Cloudflare custom-application
Primary Category	Custom Application/Site
Additional Categories	Custom Application/Site
Application Risk	Unknown

Https Inspection Details

Action	Bypass
--------	--------

Traffic

Source	client_113 (10.1.1.113)
Source Zone	Internal
Destination Zone	External
Service	https (TCP/443)
Protocol	QUIC
Interface	eth1
Connection Direction	Outgoing

Accounting

Packets	69
Browse Time	00h 00m 08s
Bytes (sent/received)	20.5 KB (2.1 KB \ 18.4 KB)
Client Inbound Packets	19
Client Outbound Packets	50
Server Inbound Packets	25
Server Outbound Packets	38
Client Inbound Bytes	2.1 KB
Client Outbound Bytes	18.4 KB
Server Inbound Bytes	18.4 KB
Server Outbound Bytes	2.1 KB

Actions

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

More

HTTP/3 inspection – example

Bypassed HTTP/3 connection
matched on drop rule

The screenshot displays a 'Log Details' window for a rejected connection. The main header shows a red 'Reject' icon and the text 'quic Traffic Rejected from 10.1.1.113 to Facebook - (157.240.0.6)'. Below this, there are two tabs: 'Details' and 'Matched Rules'. The 'Details' tab is active and shows the following information:

- Log Info**
 - Origin: GW5
 - Time: Today, 3:22:45 PM
 - Blade: Application Control
 - Product Family: Access
 - Type: Session
- Application / Site**
 - Application Name: Facebook
 - Primary Category: Social Networking
 - Additional Categories: Low Risk, Social Networking
 - Application Risk: Low
 - Application Description: Facebook is a social utility that helps... [more](#)
- Https Inspection Details**
 - Action: Bypass
- Traffic**
 - Source: client_113 (10.1.1.113)
 - Source Zone: Internal
 - Destination Zone: External
 - Service: quic (UDP/443)
 - Protocol: QUIC
 - Interface: eth1
- Policy**
 - Action: Reject
 - Policy Management: jaguar-main-take-674
 - Policy Name: Standard
 - Policy Date: Today, 3:09:23 PM
 - Layer Name: Network
 - Access Rule Name: Facebook drop-block
 - Access Rule Number: 2
- Accounting**
 - Browse Time: 00h 00m 00s
- Actions**
 - Report Log: Report Log to Check Point
- More** (dropdown menu)



Thank You!

YOU DESERVE THE BEST SECURITY