CHECK POINT™

R82 TLS Inspection Enhancements

HTTP/3 INSPECTION

Hadi Frohar

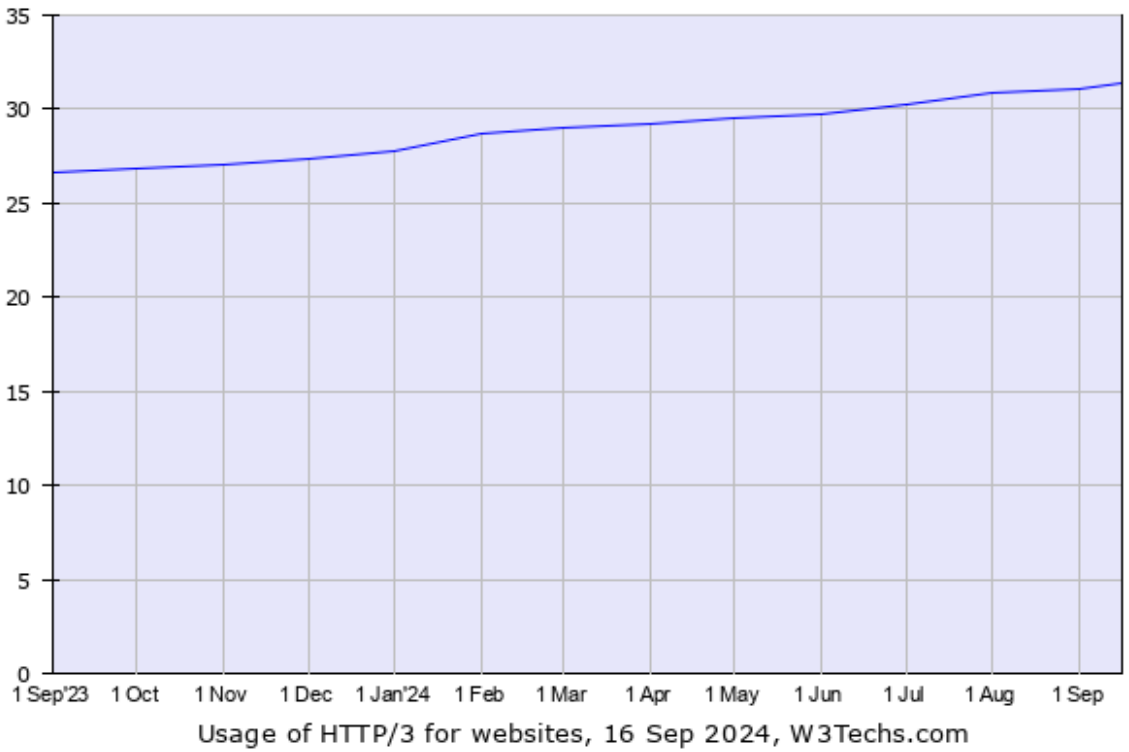
17/09/2024

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

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

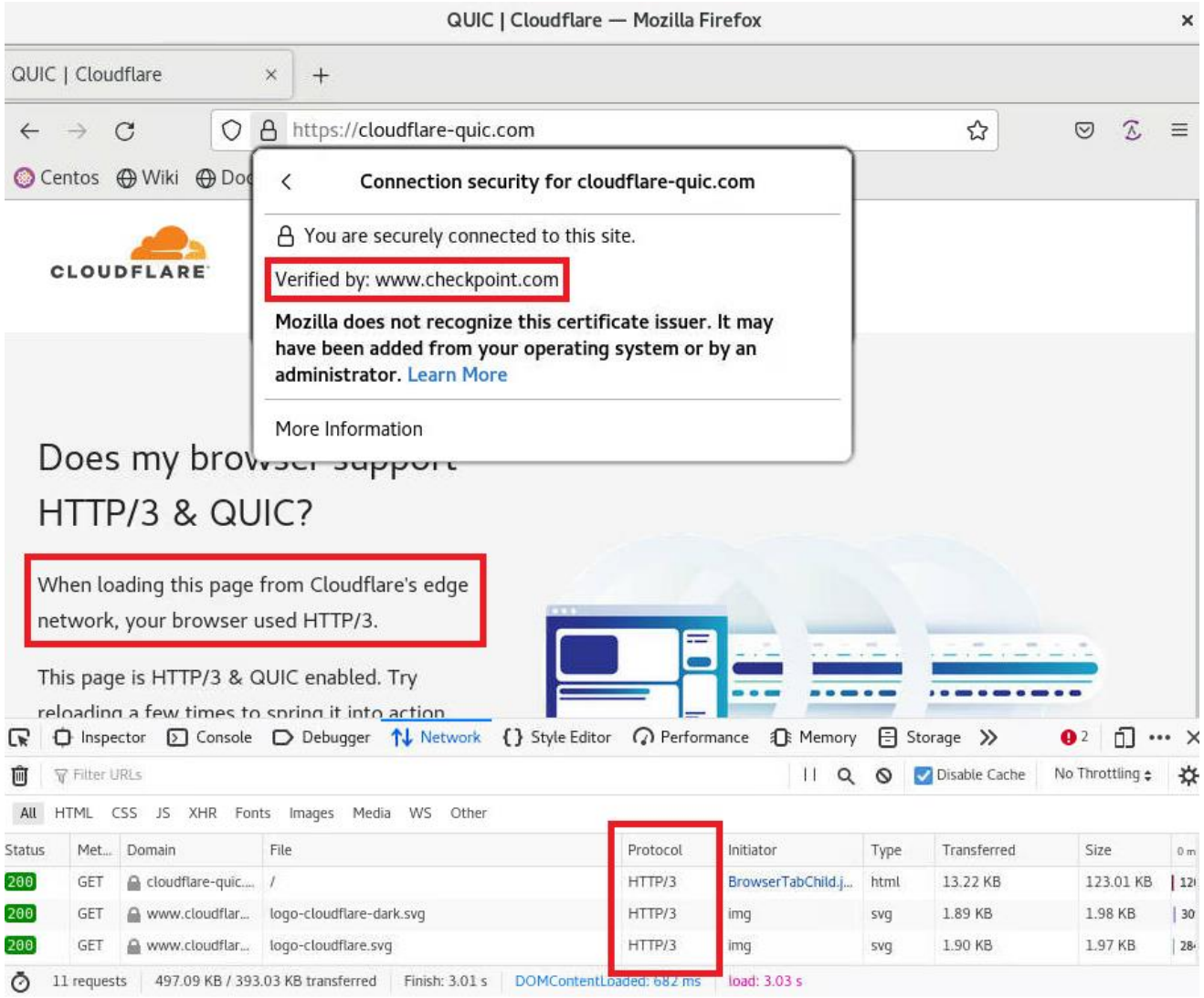
HTTPS outbound policy

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.

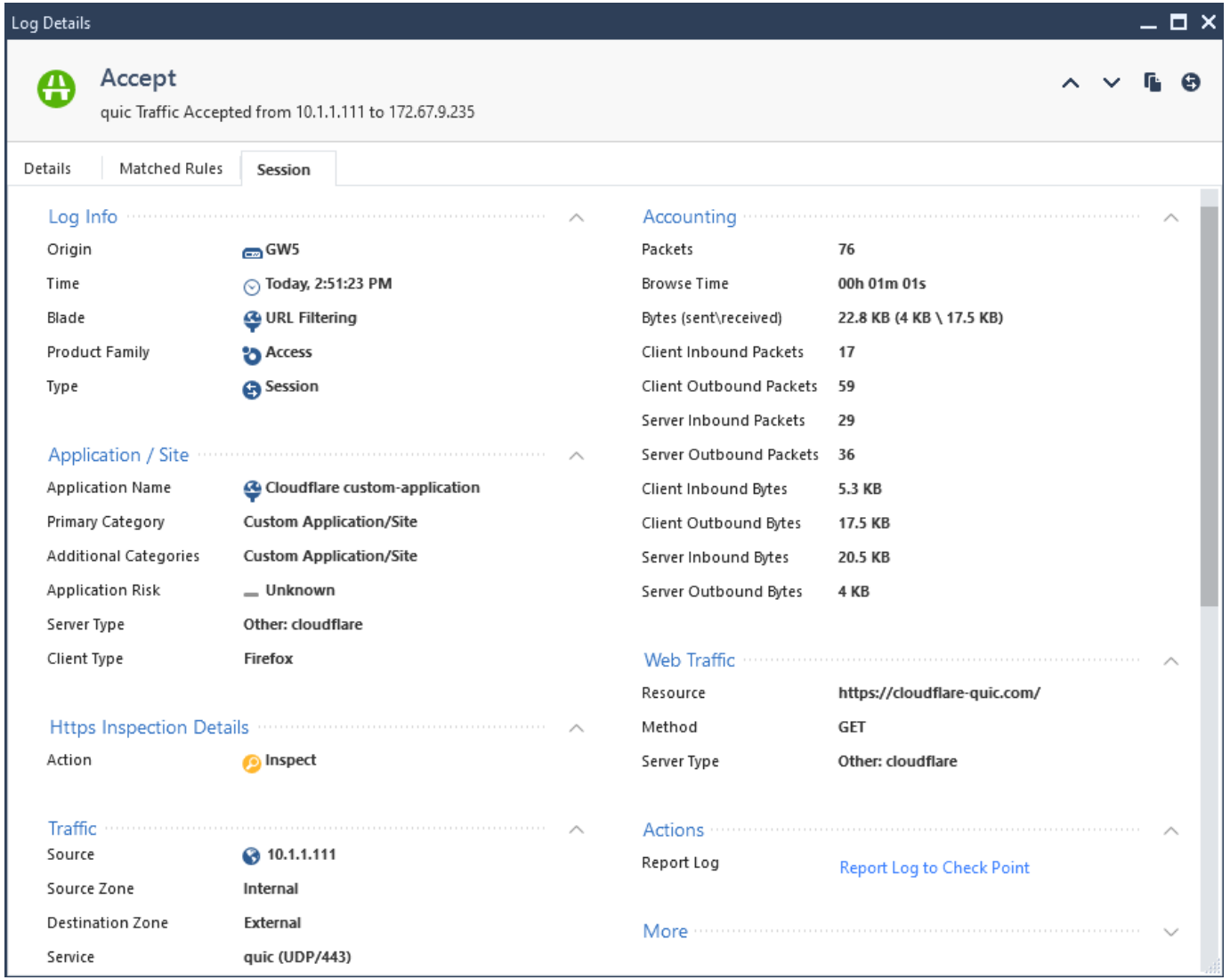
HTTP/3 inspection – example

Inspected HTTP/3 connection with HTTPS inspection certificate



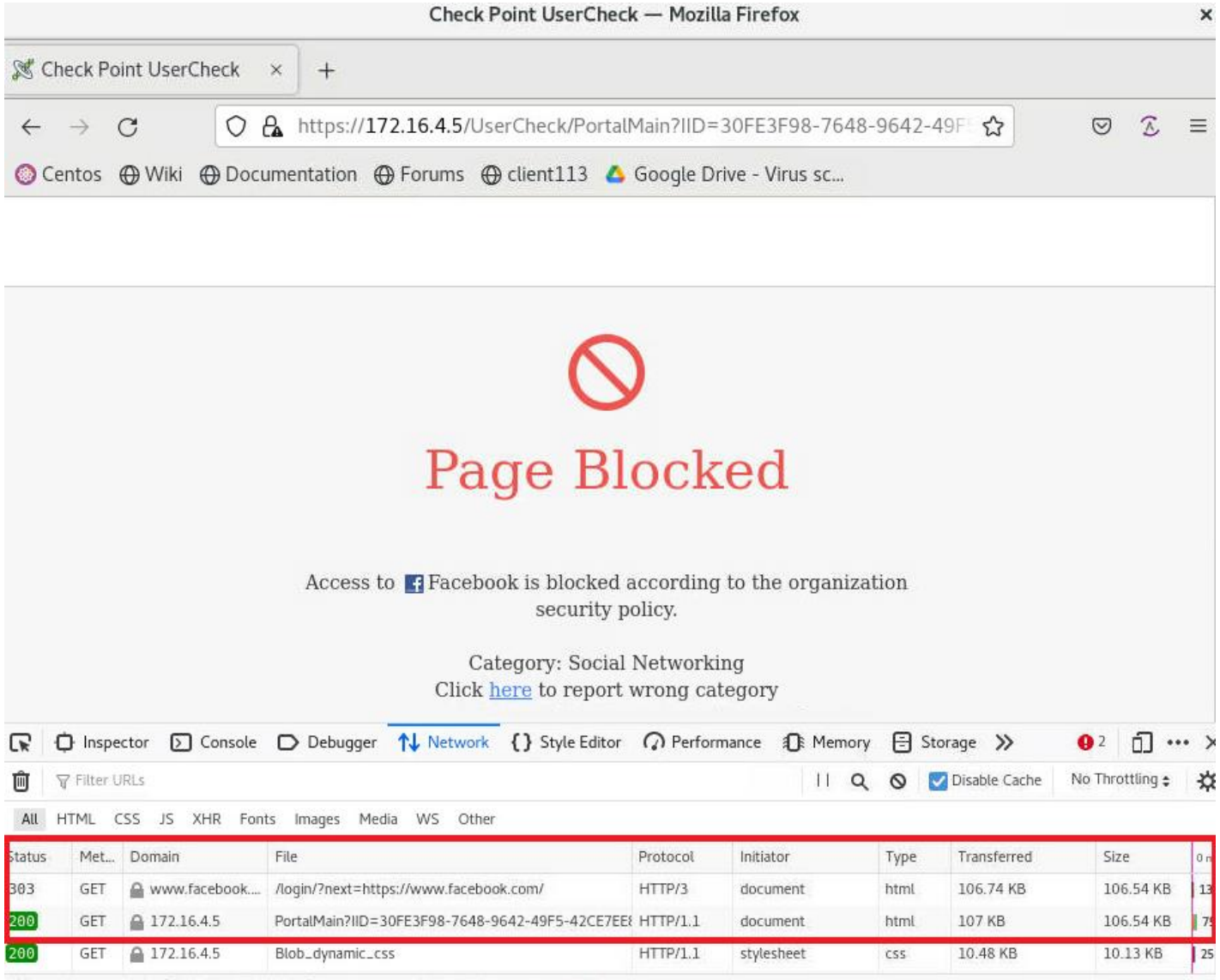
HTTP/3 inspection – example

Inspected HTTP/3 connection matched on custom application



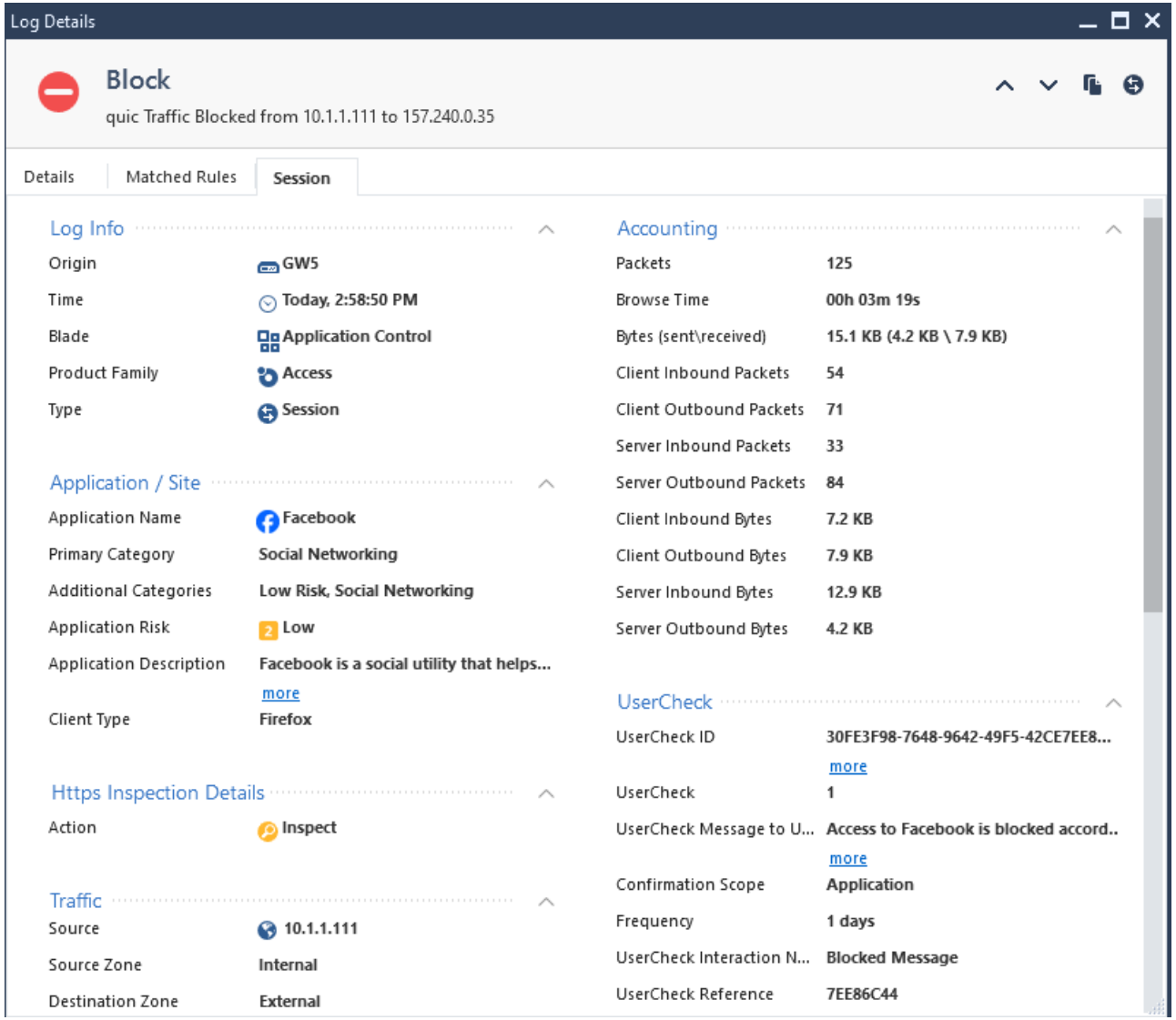
HTTP/3 inspection – example

Inspected HTTP/3 connection redirected to block page



HTTP/3 inspection – example

Inspected HTTP/3 connection redirected to block page



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

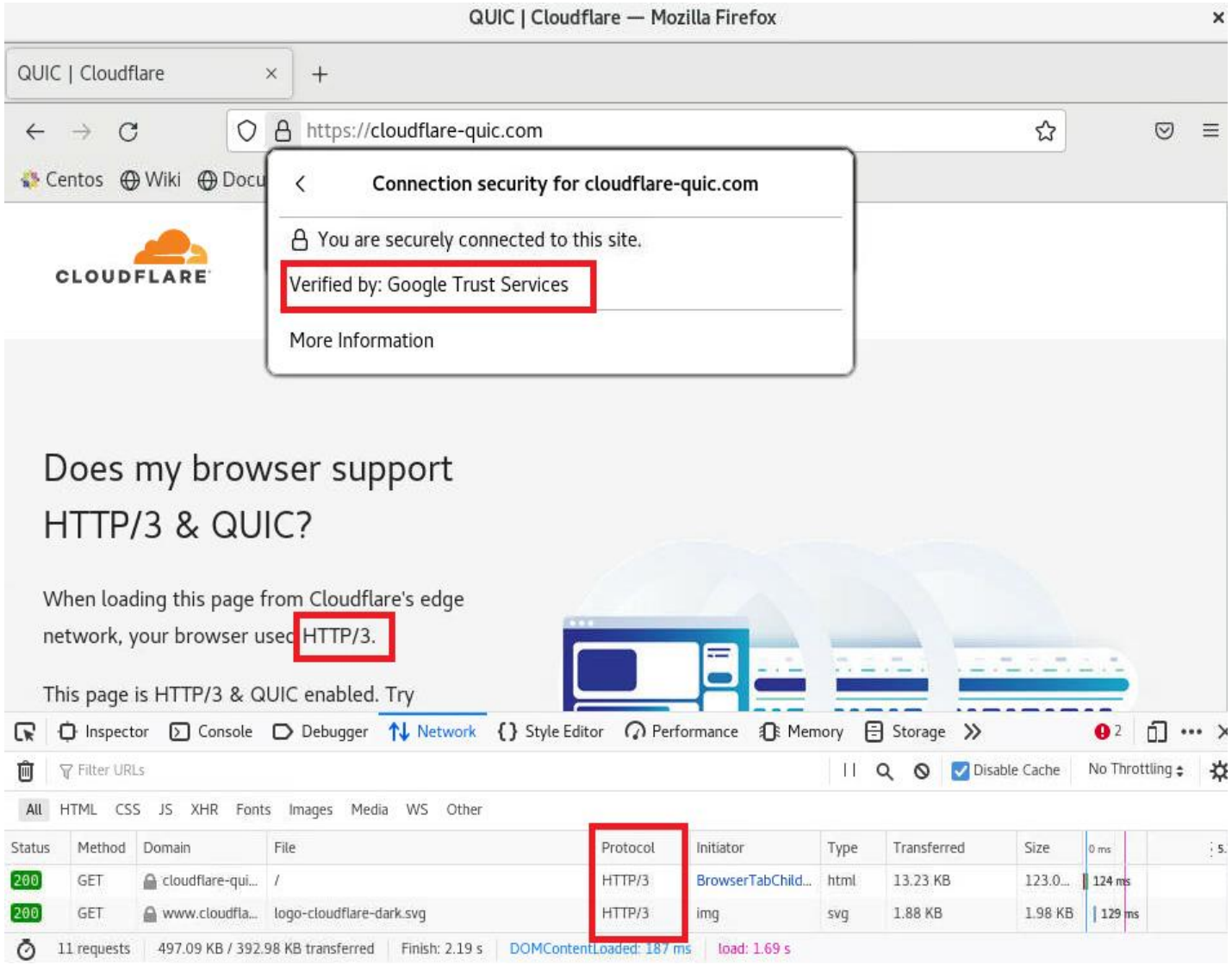
HTTPS outbound policy

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.

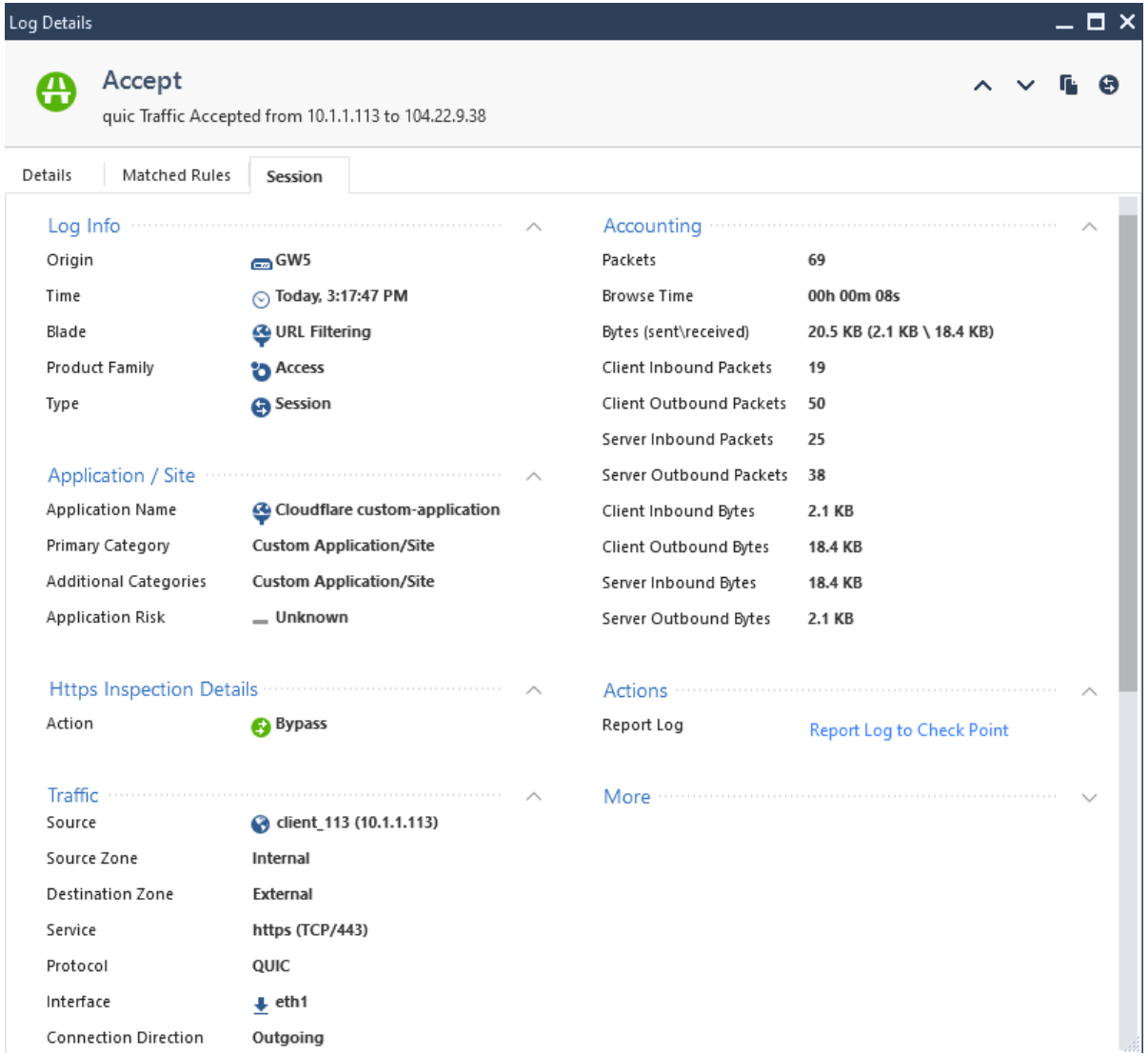
HTTP/3 inspection – example

Bypassed HTTP/3 connection with server certificate



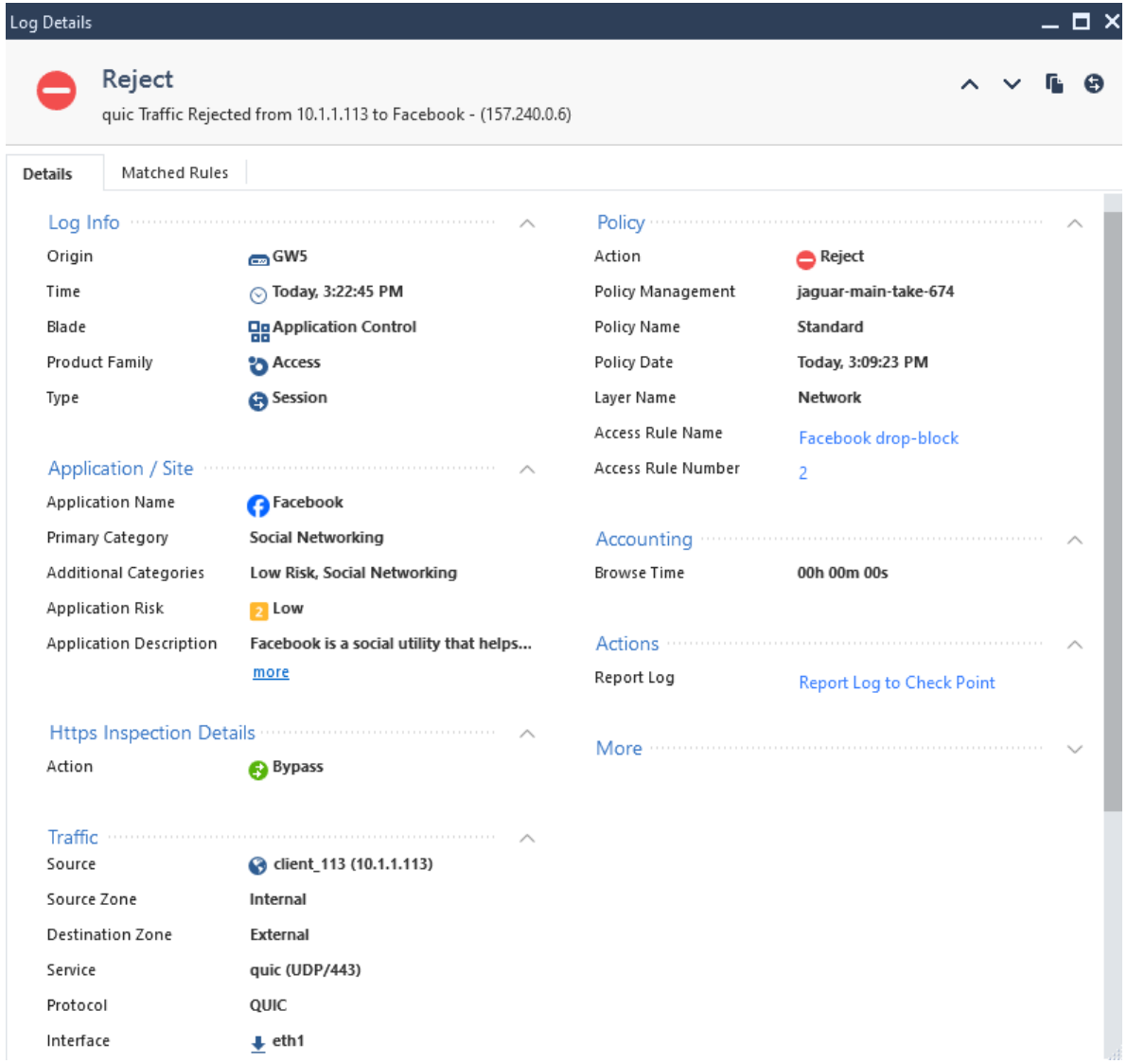
HTTP/3 inspection – example

Bypassed HTTP/3 connection matched on custom application



HTTP/3 inspection – example

Bypassed HTTP/3 connection matched on drop rule



CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY