Securing the Modern Web with QUIC Inspection

WHITEPAPER

Table of Contents

Introduction to QUIC: The Next-Generation Transport Protocol 4

- What is QUIC? 4
- How QUIC Operates 4
- The Value of QUIC 4

How QUIC Enables Threat Actors to Elude Detection 5

1. Exploiting Mandatory Encryption (The “Blind Spot”) 5
2. Connection Migration (Evading “5-tuple” Tracking) 5
3. DPI Desynchronization 5
4. UDP “Hole Punching” 6

- How to Mitigate These Risks 6

Zscaler’s QUIC Inspection: Security Without Compromise 6

- The Challenge of the QUIC “Blind Spot” 6
- Zscaler’s Technical Approach 7
- Derived Security Value 7

Ecosystem Considerations 8

Conclusion 8

Executive Summary

As the internet transitions from the decades-old TCP/IP stack to more modern protocols, QUIC has emerged as the new standard for high-performance web traffic. While QUIC offers significant improvements in speed, efficiency, and built-in security, it also introduces a "blind spot" for traditional security architectures that rely on TCP-based inspection. This white paper explores the mechanics of the QUIC protocol (RFC 9000) and details how Zscaler's QUIC Inspection capability enables organizations to maintain full visibility and security posture without sacrificing the performance benefits of the modern web.

Introduction to QUIC: The Next-Generation Transport Protocol

For over thirty years, the Transmission Control Protocol (TCP) coupled with Transport Layer Security (TLS) has been the backbone of web communication. However, as web applications become more complex and mobile-centric, the limitations of TCP—such as legacy congestion and flow control as well as outdated window scaling mechanism and multi-step handshakes—have become performance bottlenecks.

What is QUIC?

QUIC (RFC 9000) is a UDP-based, multiplexed, and secure transport layer protocol. Originally developed by Google and later standardized by the IETF, it serves as the foundation for HTTP/3. Unlike its predecessors, QUIC integrates encryption (TLS 1.3) directly into the transport layer, rather than layering it on top of a stream.

How QUIC Operates

QUIC achieves its performance gains through several architectural innovations:

- **Low-Latency Handshakes:** Traditional TCP+TLS requires multiple round trips (2—3 RTTs) to establish a secure connection. QUIC combines transport and cryptographic negotiations into a single exchange (1-RTT). For returning users, QUIC supports 0-RTT, allowing data to be sent immediately with the first packet.

- **Eliminating Head-of-Line Blocking:** In multiplexed TCP, if a single packet is lost, all subsequent packets must wait for its retransmission, stalling the entire stream. QUIC supports multiple independent streams within a single connection. A lost packet in one stream does not affect the delivery of packets in other streams, ensuring smoother performance for complex web pages.

- **Connection Migration:** Traditional connections are tied to a 4-tuple (source/destination IP and port). QUIC uses unique Connection IDs (CIDs). This allows a session to survive a network change—for example, when a mobile user moves from a Wi-Fi network to a cellular data network—without dropping the connection.

The Value of QUIC

From a networking perspective, QUIC provides a more resilient and efficient transport mechanism for lossy or high-latency environments. From an application perspective, it enables faster page loads, smoother video streaming, and more responsive interactive services.

How QUIC Enables Threat Actors to Elude Detection

Hackers and malicious actors can exploit the QUIC protocol to bypass traditional inline security controls. While QUIC is designed for performance and privacy, security stakeholders and practitioners should inspect traffic where QUIC is applied just as they would inspect TLS-encrypted traffic to maximize visibility and detect and block potential threats.

Here are the primary ways attackers get around inline inspection when QUIC is in use:

1. Exploiting Mandatory Encryption (The "Blind Spot")

Unlike TCP, where the transport headers are sent in the clear, QUIC partially encrypts the initial pre-handshake packets and everything after the initial handshake. This means inspection tools are required to perform significant work to ascertain the contents of SNI and other parameters from TLS handshake that is normally sent in the clear.

Traditional Deep Packet Inspection (DPI) tools may not be optimized for TCP/TLS 1.2 and cannot always "see" adequately inside the QUIC data stream.

- **The Hack:** Attackers deliver malware or exfiltrate data over UDP port 443 (HTTP/3). Without decrypting QUIC or blocking it to force a TCP fallback, the malicious payload passes through completely uninspected.

2. Connection Migration (Evading "5-tuple" Tracking)

Traditional firewalls track sessions using a "5-tuple" (Source IP, Source Port, Destination IP, Destination Port, and Protocol). QUIC uses a Connection ID (CID) instead.

- **The Hack:** QUIC allows a session to stay active even if the user's IP address or port changes (e.g., switching from Wi-Fi to 5G). Attackers can use "IP hopping" or "port hopping" to stay ahead of automated blocking rules. A firewall may block an IP, but the attacker simply "migrates" the active malicious QUIC session to a new IP, and the CID allows it to continue without interruption.

3. DPI Desynchronization

Since QUIC runs over UDP, it is "stateless" at the network layer compared to TCP.

- **The Hack:** Attackers can perform DPI Desynchronization by injecting "junk" or malformed UDP packets at the start of a stream. Many stateful inspection engines will give up trying to parse the stream if the first few packets look like noise, effectively "tuning out" while the actual malicious QUIC traffic follows immediately after.

4. UDP “Hole Punching”

Because UDP does not have explicit “FIN” or “RST” flags to close a connection, firewalls must rely on inactivity timers to close a session.

- **The Hack:** Attackers use low-volume “keep-alive” traffic to keep a “hole” open in the firewall indefinitely. This allows them to maintain a long-term, uninspected back-door for data exfiltration that stays under the radar of volume-based anomaly detection.

How to Mitigate These Risks

To counter these techniques, organizations typically employ two methods:

1. **QUIC Blocking:** Forcing a fallback to TCP/TLS (HTTP/2) so that legacy inspection tools can see the traffic.

2. **Native QUIC Inspection:** Using a modern platform like Zscaler that can natively decrypt and inspect QUIC/HTTP/3 traffic, ensuring that 0-RTT data, migrated connections, and encrypted payloads are subjected to the same security policies as traditional web traffic. For more on how Zscaler delivers this, read on.

Zscaler’s QUIC Inspection: Security Without Compromise

As HTTP/3 and QUIC adoption surpasses 25-30% of global web traffic, security teams face a dilemma: block QUIC to force a fallback to TCP for inspection (degrading performance) or allow it to pass through a network uninspected (creating a massive security gap). Zscaler’s QUIC Inspection provides a third path: native, high-performance inspection of HTTP/3 traffic.

The Challenge of the QUIC “Blind Spot”

Attackers are increasingly leveraging the “opaque” nature of encrypted UDP traffic to bypass legacy firewalls. Without the ability to decrypt and inspect QUIC, organizations are blind to:

- Malware delivered via high-speed UDP streams.
- Data exfiltration (DLP) hidden within encrypted QUIC sessions.
- Unauthorized use of AI tools and SaaS applications that default to QUIC.

Zscaler's Technical Approach

ZIA (Zscaler Internet Access) brings HTTP/3 traffic under the same rigorous inspection posture as legacy HTTP/1 and HTTP/2. By intercepting QUIC flows, Zscaler provides:

- **Native Inspection (No Fallback Required):** Unlike solutions that block UDP port 443 to force a TCP fallback, Zscaler can inspect the QUIC streams directly. This preserves the user experience and the speed benefits of the protocol.

- **Transparent Redirection:** QUIC inspection is supported through Zscaler's most advanced redirection modes, including Zscaler Client Connector (ZCC), Zero Trust Branch, Tunnel 2.0, GRE, and IPsec. This ensures that mobile and remote workers are protected regardless of their location.

- **SSL Configuration Integration:** Admins can easily enable QUIC (HTTP/3) inspection within the standard SSL Configuration policies, treating it as a first-class citizen alongside traditional web protocols.

Derived Security Value

By enabling QUIC inspection, security personas gain several critical advantages:

1. **Advanced Threat Protection (ATP):** Zscaler's security engines scan decrypted QUIC traffic for known and unknown malware, preventing attackers from using modern protocols as a "path of least resistance."

2. **Data Loss Prevention (DLP):** Full visibility into QUIC payloads allows the DLP engine to identify and block the unauthorized movement of sensitive data across modern web applications.

3. **Secure AI Adoption:** Modern AI applications are moving to QUIC to optimize the massive throughput required for LLM interactions. Zscaler ensures these AI-driven flows are governed, preventing "Shadow AI" risks.

4. **Operational Consistency:** QUIC traffic is integrated into Zscaler's unified logging and reporting framework. This provides security analysts with the granular data needed for audits, incident investigations, and compliance reporting.

Ecosystem Considerations

While Zscaler provides robust inspection for browsers like Firefox, there are currently ecosystem-wide limitations for Chromium-based browsers (Chrome/Edge) due to specific browser-level restrictions on Man-in-the-Middle (MITM) inspection for QUIC. Zscaler continues to work closely with browser vendors to expand support as the standards evolve.

Conclusion

The shift to QUIC is an inevitable and positive step for the performance of the internet. However, they require a modernized security architecture that can "speak" UDP-based protocols natively and perform deep packet inspection on QUIC traffic: Zscaler's QUIC Inspection allows network and security staff in any organization to embrace the future of the web—leveraging the speed of RFC 9000—while maintaining the deep visibility and threat prevention necessary to protect the modern enterprise.

Zscaler provides comprehensive visibility and security for QUIC traffic by treating it with the same rigor as standard web traffic. By eliminating the QUIC blind spots, organizations can ensure that their security posture evolves at the same pace as their network and application performance.

Learn more about how Zscaler enables secure access by scheduling a meeting with our security experts today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.