NIAGARA NETWORKS

ePACKETRON

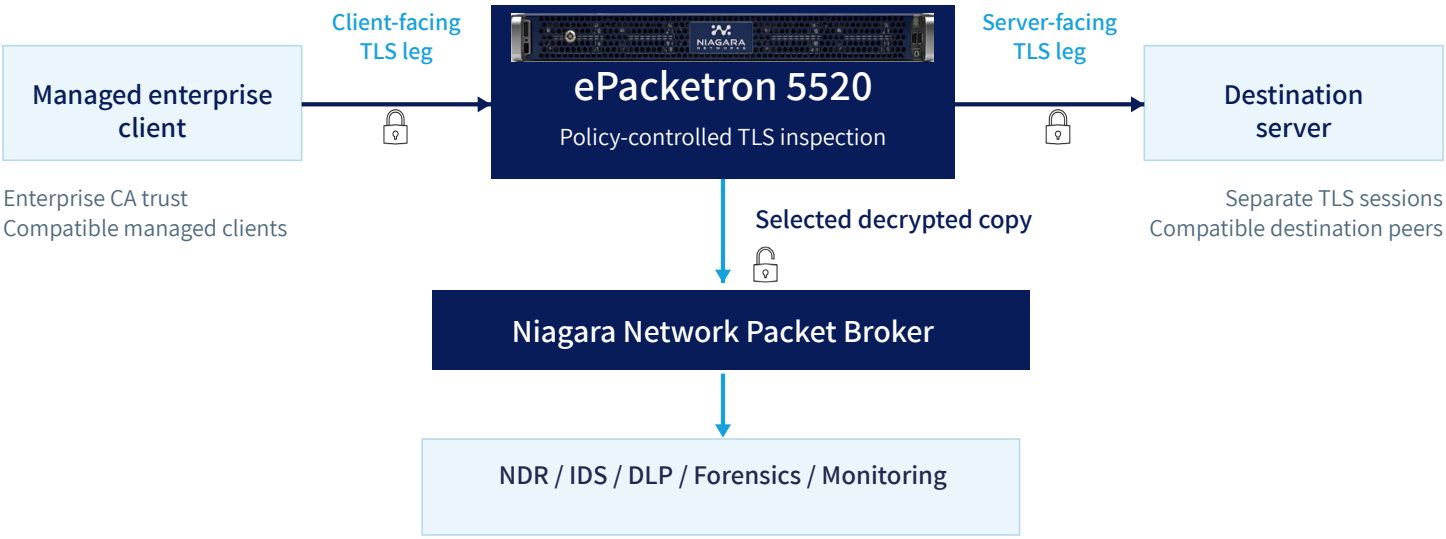
ECH-Aware TLS 1.3 Selective Decryption

Intelligent encrypted traffic visibility for SOC & NOC teams

TLS 1.3 encrypts application traffic; Encrypted Client Hello (ECH) also conceals the real destination hostname used by conventional passive SNI monitoring. ePacketron brings authorized active inspection to supported enterprise-managed connections, applying destination intelligence and configured policies to inspect eligible traffic while keeping designated sensitive communications encrypted.

Decrypt What Matters. Bypass What Is Private.

Active inline inspection. Selected decrypted copies for existing tools.



Conceptual workflow: interception is active and inline; approved monitoring tools receive copies out of band.

Restore inspection context

Inspect eligible ECH sessions without stripping or downgrading ECH.

Respect privacy policies

Keep designated categories encrypted; mask approved monitoring feeds.

Offload security tools

Decrypt once, then distribute relevant traffic to multiple approved tools.

Classify by destination, category & reputation | Decrypt, bypass, block or log

FABRICFLOW 12.14 / TECHNICAL HIGHLIGHTS

High performance. Selective control.

90+ Gbps	110,000	1 million	Up to 600
TLS decrypted throughput	New decrypted TLS sessions per second	Concurrent decrypted TLS sessions	Gbps overall packet processing capacity

Reported Niagara Networks TLS benchmark includes mirroring every decrypted byte to an out-of-band tool.
Results vary with traffic, cipher suites, session mix and enabled functions; do not assume identical performance for every ECH/PQ configuration.
The 600 Gbps packet-processing figure is distinct from TLS throughput.

Post-quantum key exchange

PQ groups are enabled by default on both TLS legs, with hybrid X25519MLKEM768 preferred. Standalone ML-KEM-1024 is also supported. Each leg negotiates independently with its compatible peer.

Policy that evolves with traffic

Destination categories, supported reputation intelligence and customer rules guide handshake-time handling: none (encrypted bypass), log, drop or decrypt. Hot-reloadable category data supports updates without a maintenance window or dropped active sessions.

Deploy with control. Deliver with confidence.

Active inspection & optimized delivery

ePacketron terminates and re-establishes authorized TLS connections, re-encrypting production traffic. Selected decrypted copies reach out-of-band tools through the packet broker. Apply supported filtering, deduplication, slicing, masking and load balancing. A passive TAP copy alone is insufficient. Enterprise CA trust and validated client/server compatibility are required; pinned applications may need bypass.

Availability & deployment planning

The ePacketron 5520 can be paired with a Niagara Networks inline physical bypass switch for high-availability protection, maintaining network connectivity by bypassing the appliance if it becomes unavailable. This physical bypass differs from policy-based privacy bypass and does not maintain decryption during failover. Validate hardware compatibility, health checks, fail-open/fail-closed policy, TLS session recovery & fail-back.

Talk to a Visibility Specialist

Plan ECH-aware inspection, privacy policies, post-quantum support and delivery to your existing security tools.

Explore ePacketron | niagaranetworks.com/epacketron

