SSL Offload Presentation

For more information, visit our website at

http://www.mooreperformance.net

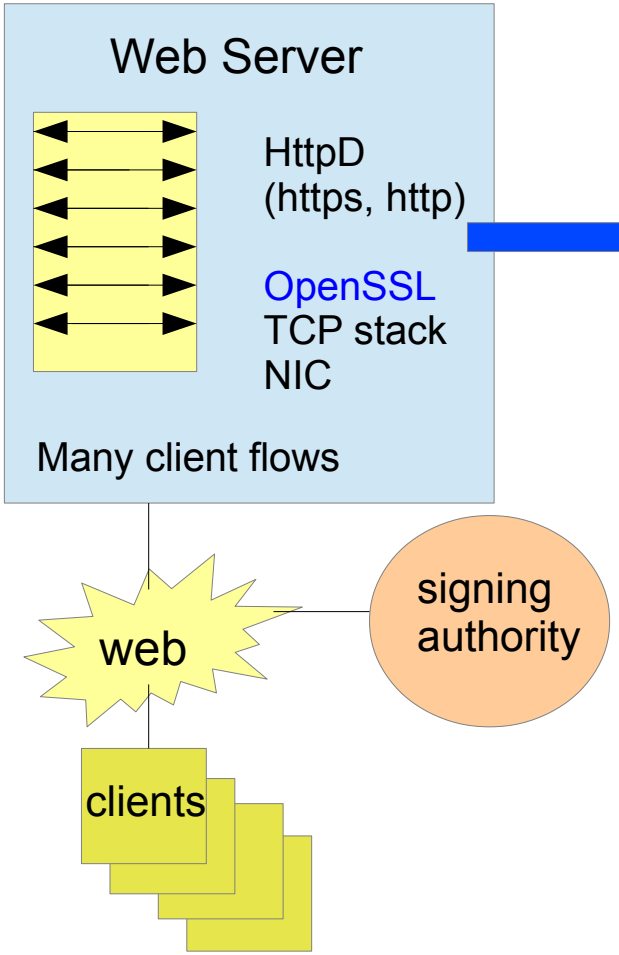
Or contact us at

(408)779-7772 | pete@mooreperformance.net

Contents:

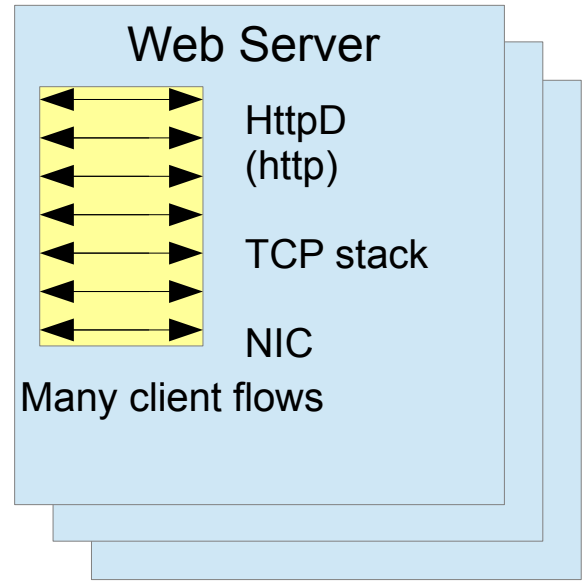
- SSL Monitoring vs. SSL Termination
- SSL Monitoring models: “Enterprise In” and “Enterprise Out”
- SSL Acceleration, connection, & bulk crypto
- Inline vs. Parallel SSL Hardware Acceleration
- Inline solutions & features for SSL monitoring solutions

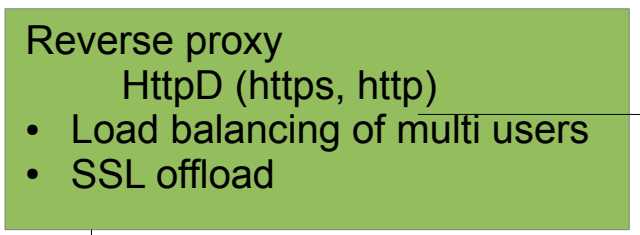
Termination – Standard Web Server Deployment

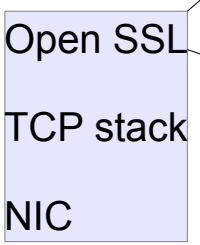


- Connection & crypto overhead for each https client flow.
- Server private key & certificate installed.

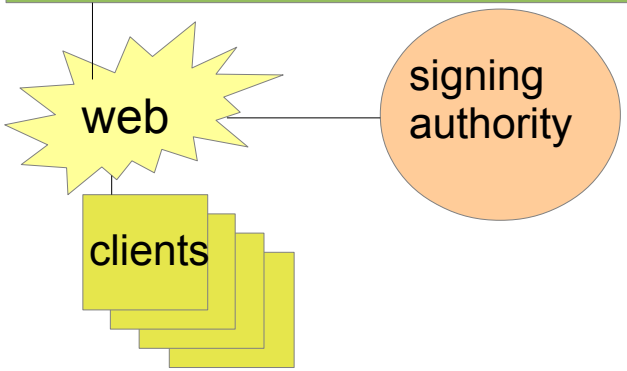
Web Server Deployment with Reverse Proxy



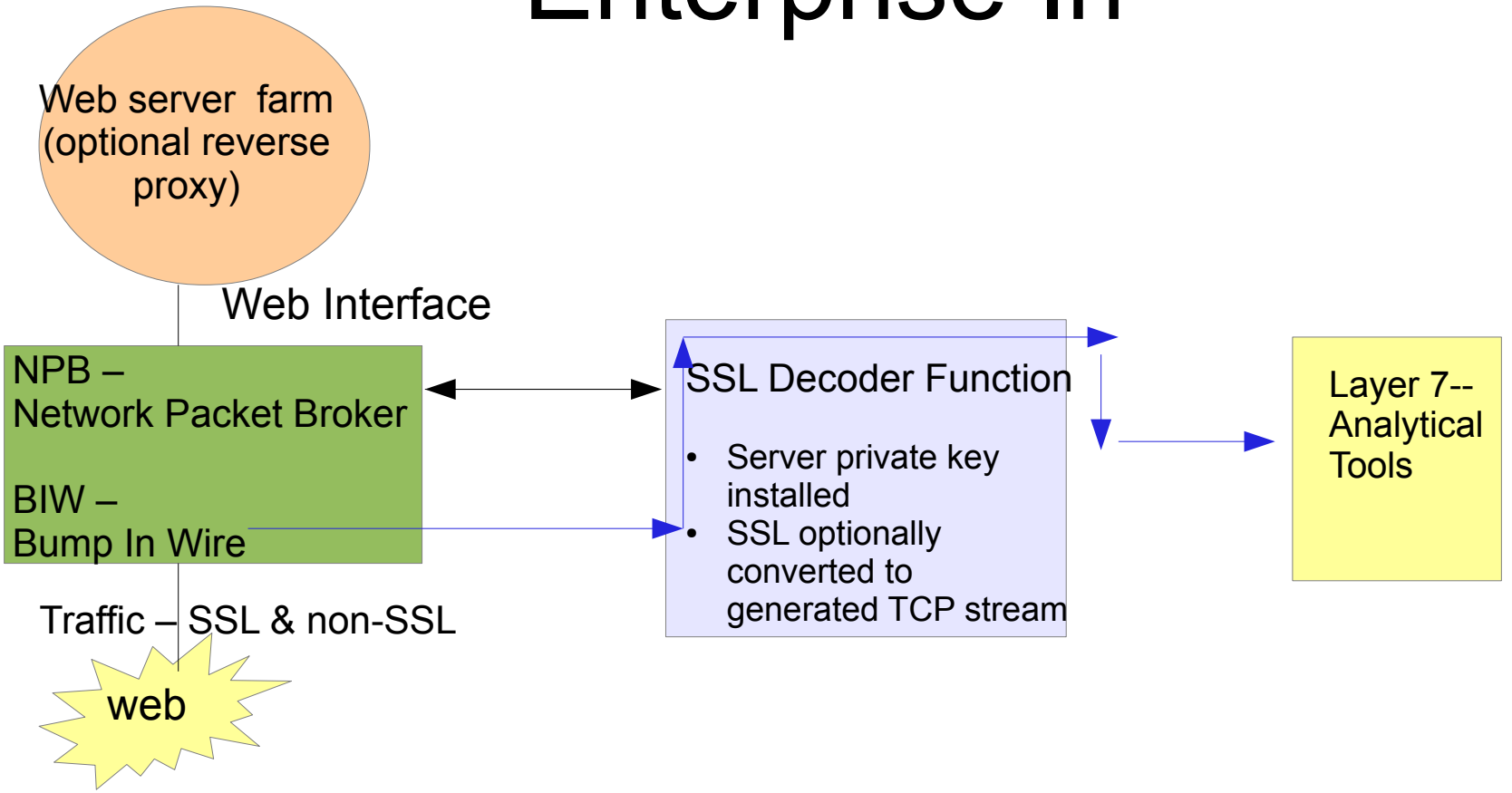




- Connection & crypto overhead for each https client flow.
- Server private key & certificate installed.

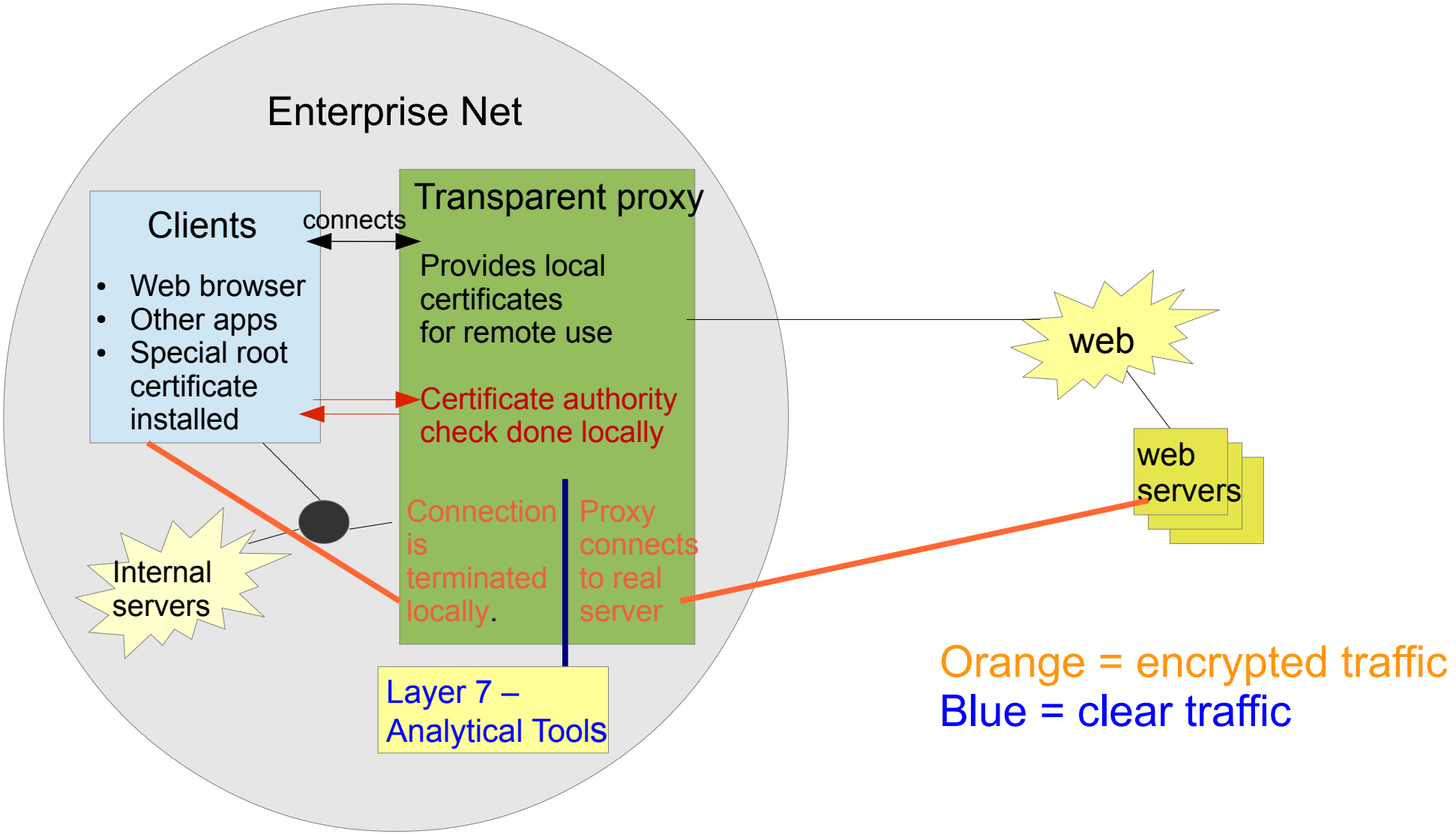


SSL Monitoring Models: "Enterprise In"

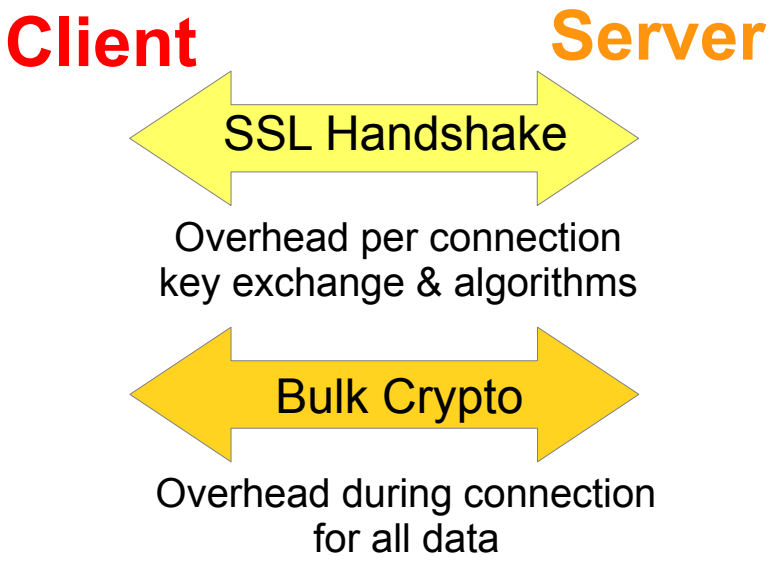


SSL Decoder Function could optionally be integrated into the NPB or Analytical Tools units.

SSL Monitoring Models: “Enterprise Out”



SSL Acceleration: connection, & bulk crypto



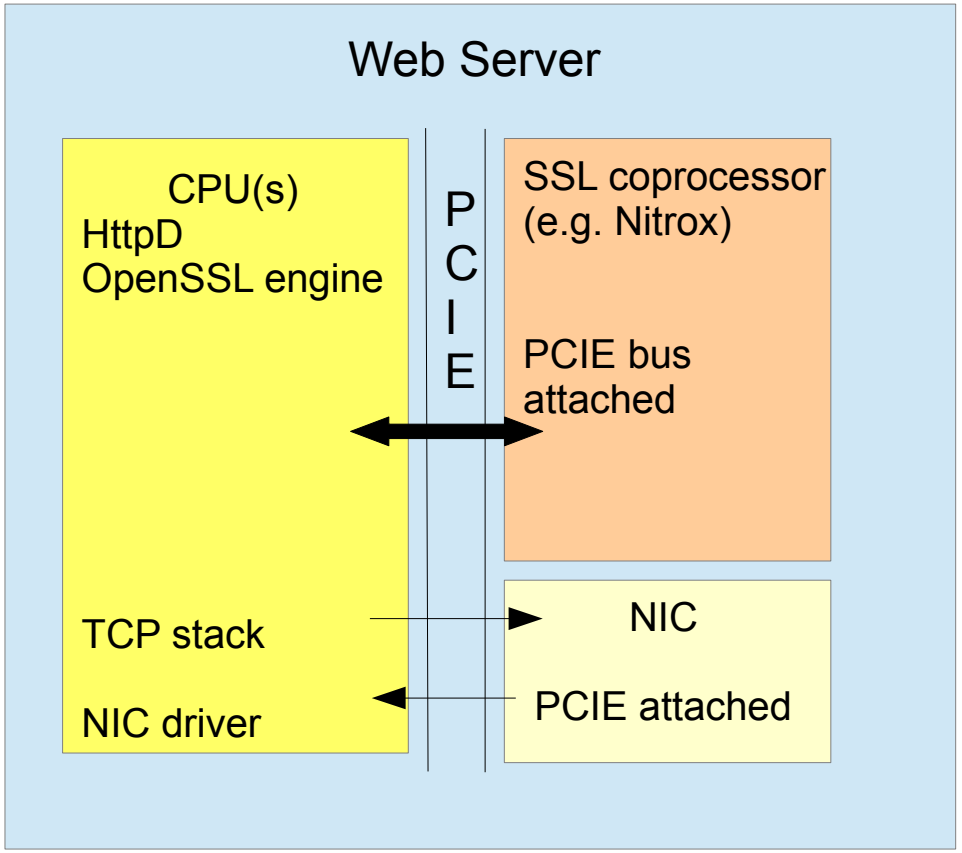
SSL Acceleration

- Connection
  - High software overhead
  - Significant software overhead even with hardware acceleration on some algorithms
- Bulk crypto
  - High software overhead
  - Hardware accelerators significantly help

Hardware Acceleration solutions may accelerate connection, bulk crypto, or both.

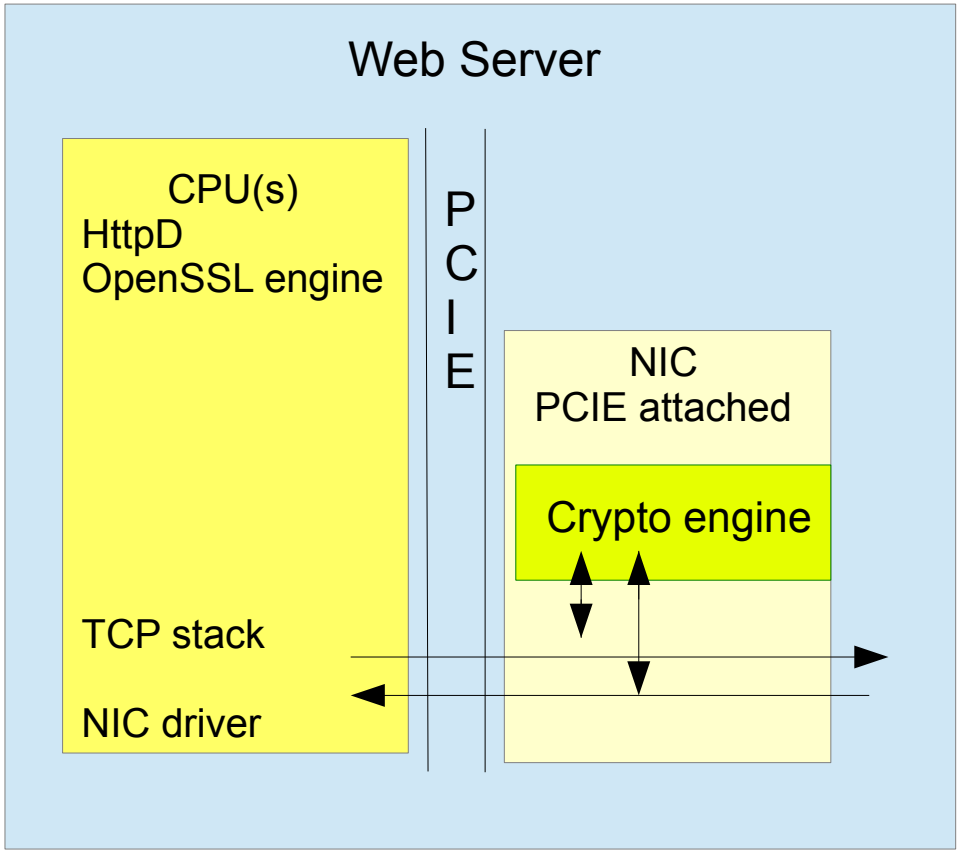
Many hardware solutions let software process connections while hardware accelerates bulk crypto.

Parallel or Co-processor Hardware Acceleration Model



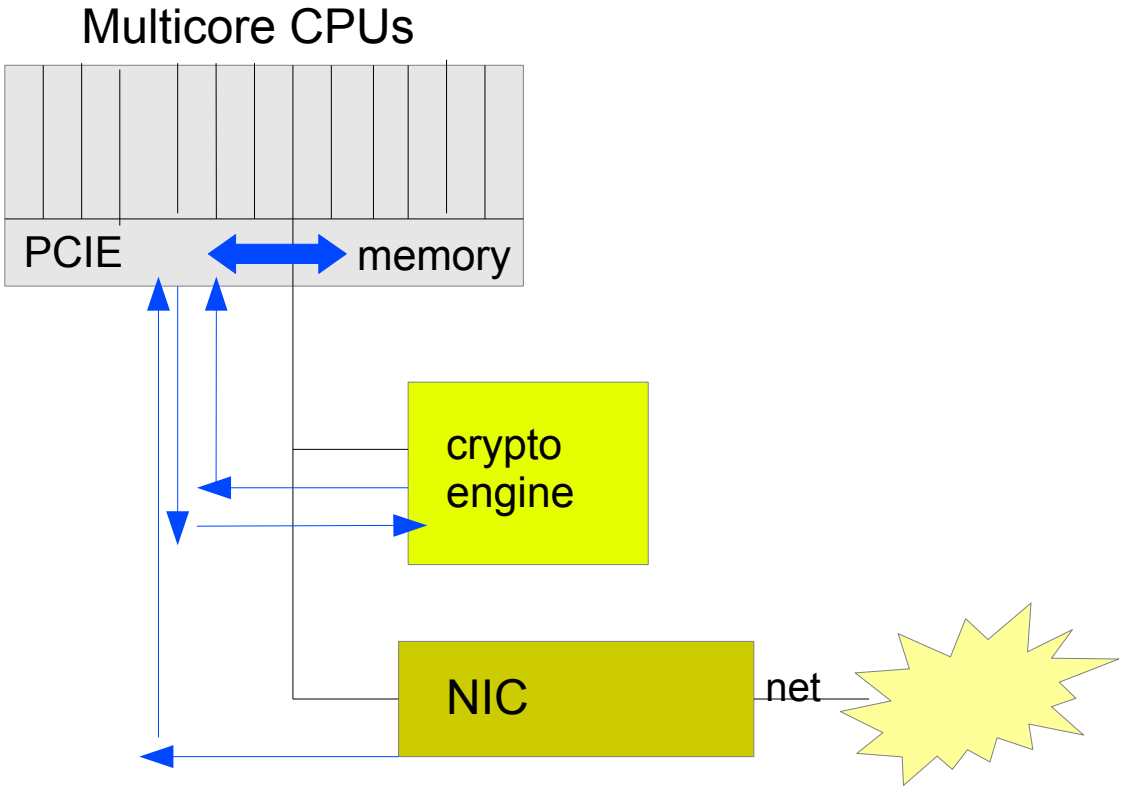
Typical Hardware SSL Acceleration in use Today

Inline Hardware Accleration Model



Inline Solution offers advantages for some applications.

Inline vs. Parallel SSL Offload: Parallel PCIE Attached Coprocessors



For each direction:

- Data crosses PCIE 2x (crypto engine), NIC 1x.
  - Significant bus & memory overhead with extra I/O operations.
- Still significant software/CPU overhead processing connections and interacting with crypto engine.

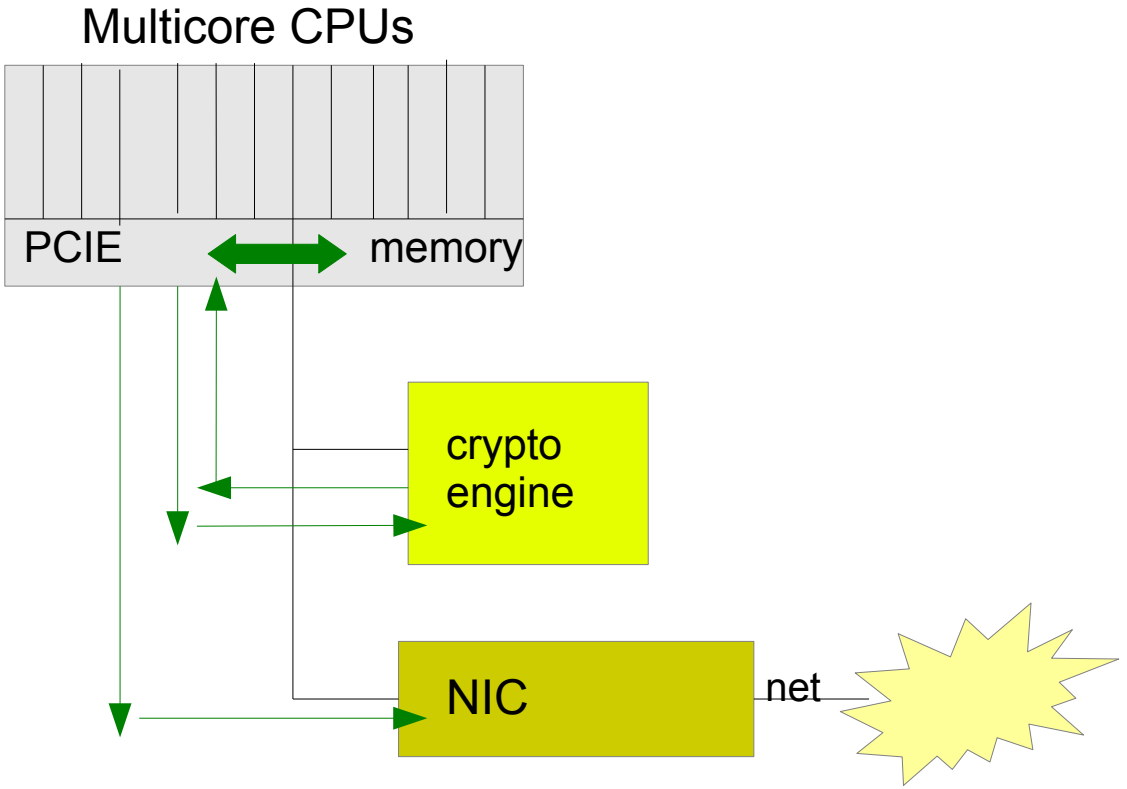
Recieve:

- 1) Load balance to a CPU
- 2) TCP stack
- 3) Open SSL
- a) To crypto engine
- b) Back from crypto engine
- 4) Application delivery and processing

Transmit:

- 1) App to open SSL
- 2) Open SSL
- 2a) To crypto engine
- 2b) Back to Open SSL
- 3) TCP stack
- 4) Out to NIC

Inline vs. Parallel SSL Offload: Parallel PCIE Attached Coprocessors



For each direction:

- Data crosses PCIE 2x (crypto engine), NIC 1x.
  - Significant bus & memory overhead with extra I/O operations.
- Still significant software/CPU overhead processing connections and interacting with crypto engine.

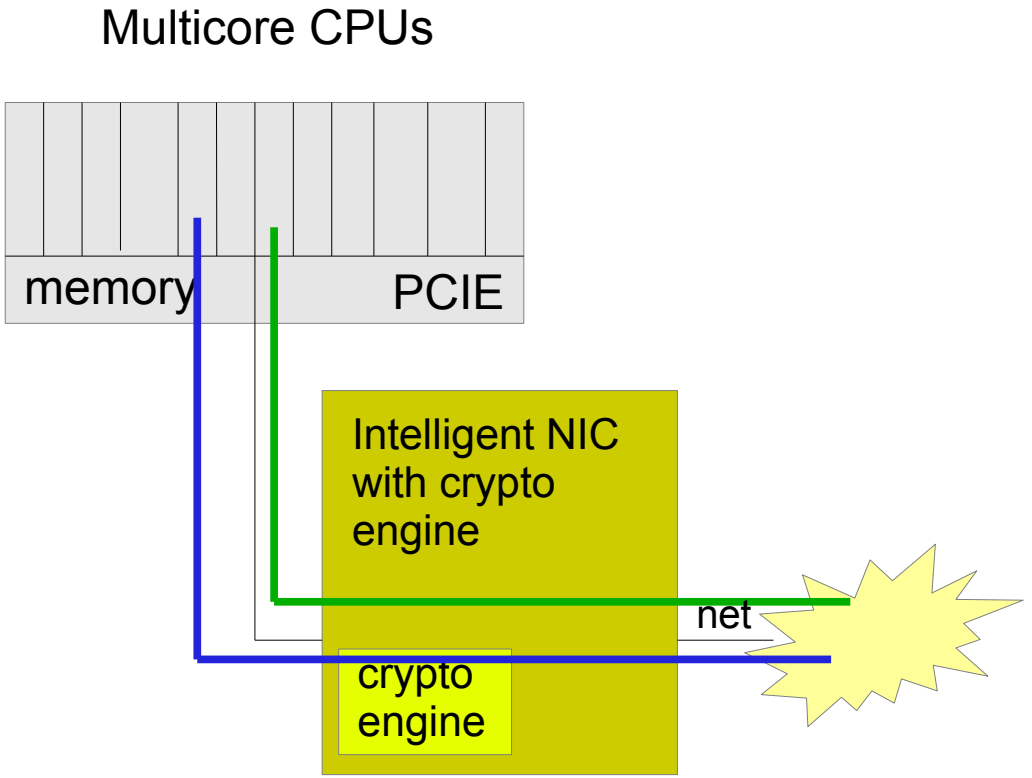
Recieve:

- 1) Load balance to a CPU
- 2) TCP stack
- 3) Open SSL
- a) To crypto engine
- b) Back from crypto engine
- 4) Application delivery and processing

Transmit:

- 1) App to open SSL
- 2) Open SSL
- 2a) To crypto engine
- 2b) Back to Open SSL
- 3) TCP stack
- 4) Out to NIC

Inline vs. Parallel SSL Offload: Inline Solution



Recieve:

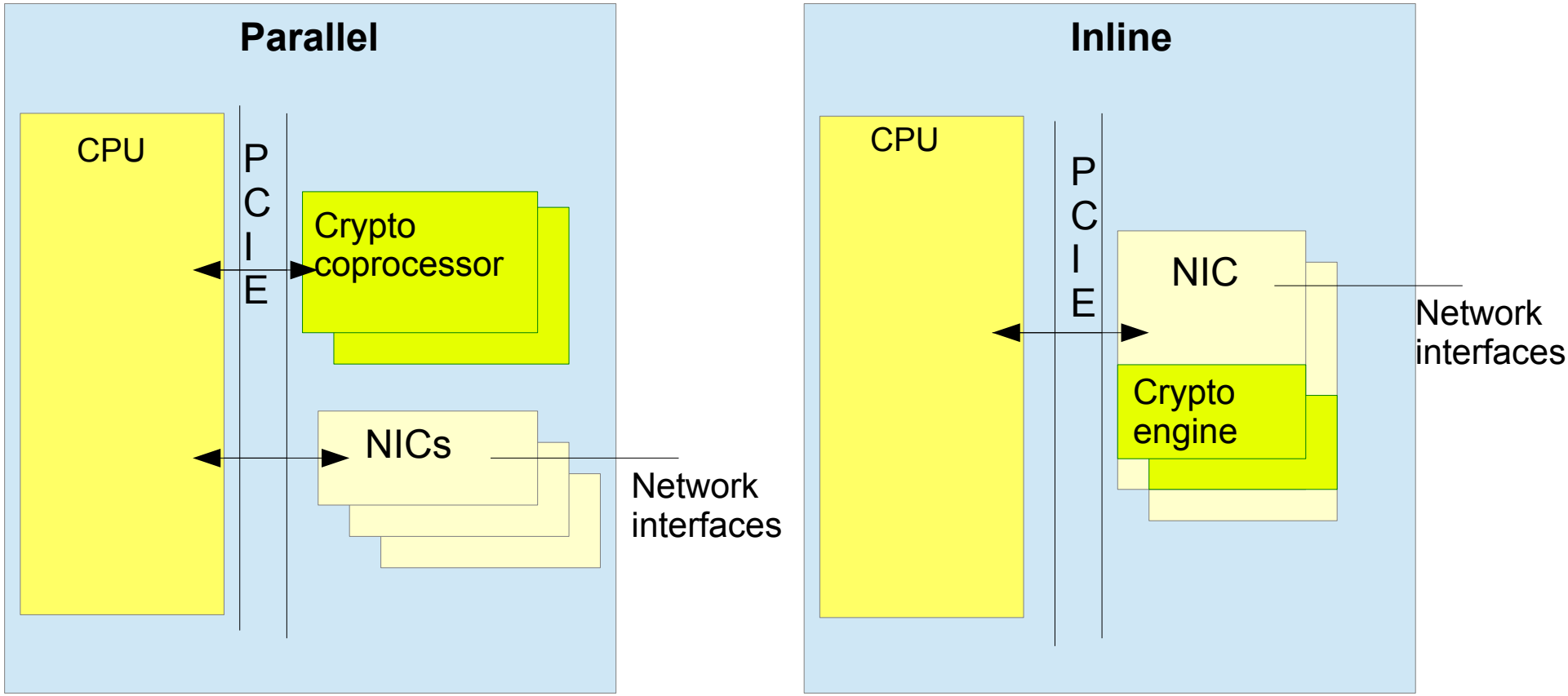
- 1) Load balance to a CPU
- 2) TCP stack
- 3) Application delivery and processing

Transmit:

- 1) App to TCP stack
- 3) TCP stack
- 4) Out to NIC

Extra bus transfers removed. All SSL software/CPU overhead offloaded to NIC

Parallel vs. Inline Scalability



- Coprocessors are a global resource.
- Multiple can be installed but require a software load balance implementation.
- Inline crypto acceleration is per NIC.
- Multiple can be installed with load balance across interfaces.

Inline Solutions & Features for SSL Monitoring Solutions

Monitoring solution desired features:

1. Option to “cut-through” non-SSL traffic.
   - Out BIW port
   - To host for normal analytics
2. 2-way NPB (Network Packet Broker) interface for host to decide to forward or drop a packet (as opposed to a simple Tap interface).
3. Option for SSL traffic to be delivered as “payload-only” or “generated TCP streams”.
4. Support for multiple Tap ports to prevent oversubscription.

Additional MPS Inline SSL Monitoring Features:

1. Traffic can be delivered with zero-copy, kernel bypass drivers, directly to user-space applications.
2. Host application interface can be customized to meet customer requirements.
3. “Cut-through” options can be configurable.

MPS Inline SSL Monitoring Solution can provide these features to meet customer requirements.

For more information on our consulting services or products, visit our website at

http://www.mooreperformance.net

Or contact us at

(408)779-7772 | pete@mooreperformance.net