

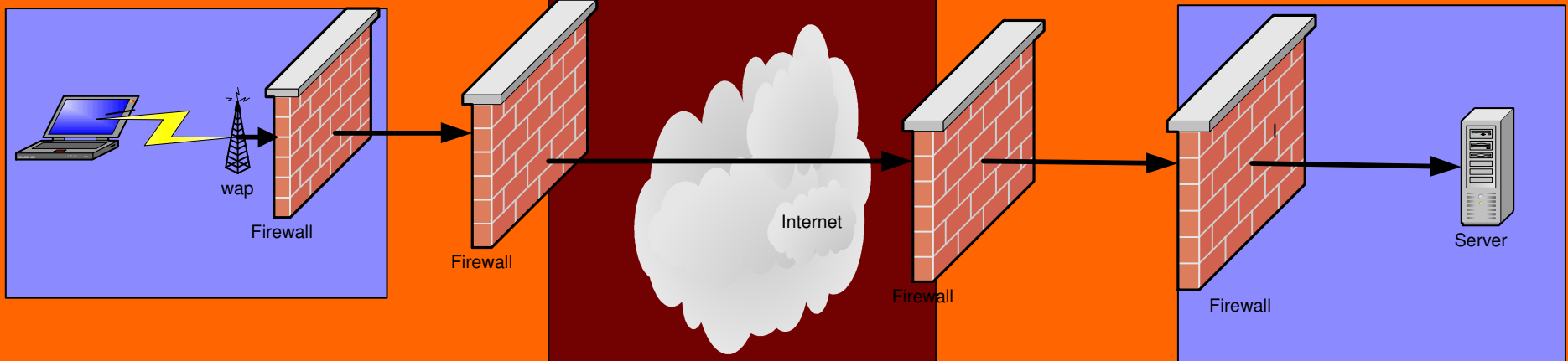
Authenticated Traversal

Contessa Project Review

April 1, 2003

Carl Gunter, Michael McDougall,
and Alwyn Goodloe

Motivating Example



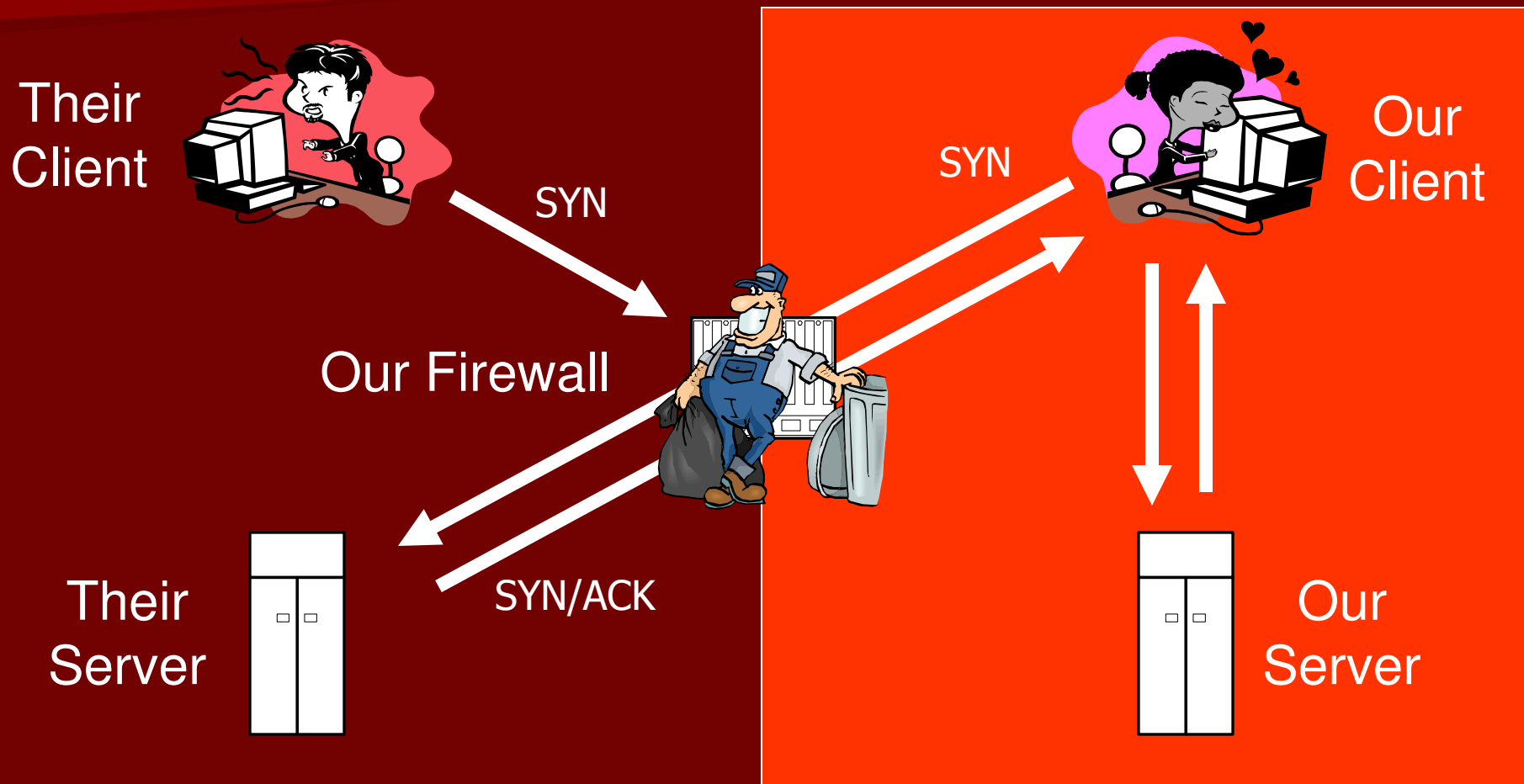
Authorization Model

- We distinguish between *authenticated* traffic and *authorized* traffic
- Authenticated traffic is authorized based on its origin and shape
- Unauthenticated traffic is authorized based on its shape alone
- Shape filtering enables “pass-through” for negotiations and optimizations

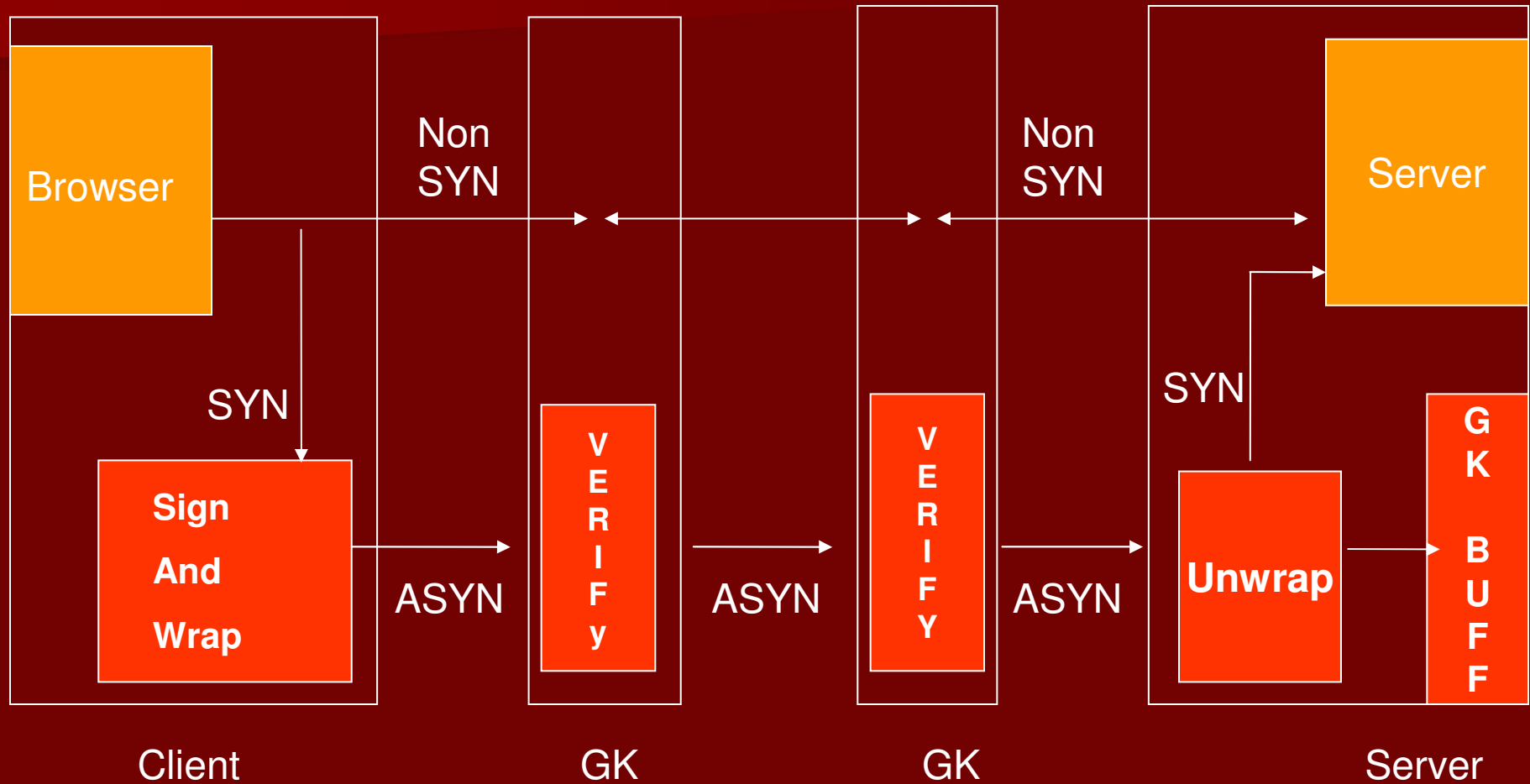
Initiation VS Response Traffic

- Initiation traffic sets up connections.
 - TCP handshake.
 - ping
- Response traffic is processed only in established connections.
- Filtering initiation traffic is sufficient.
 - If initiation traffic is blocked, then no connection is established.
 - We have experimented with a scheme that required tcp syn packets to be authenticated.

Example: SYN Filtering



AST Protocol



AST vs. IPSec

■ AST

- Low bandwidth overhead not affected by number of security gateways
- Works well with header compression and NATs
- Limits on implementation
- Subject to denial of service
- Simple

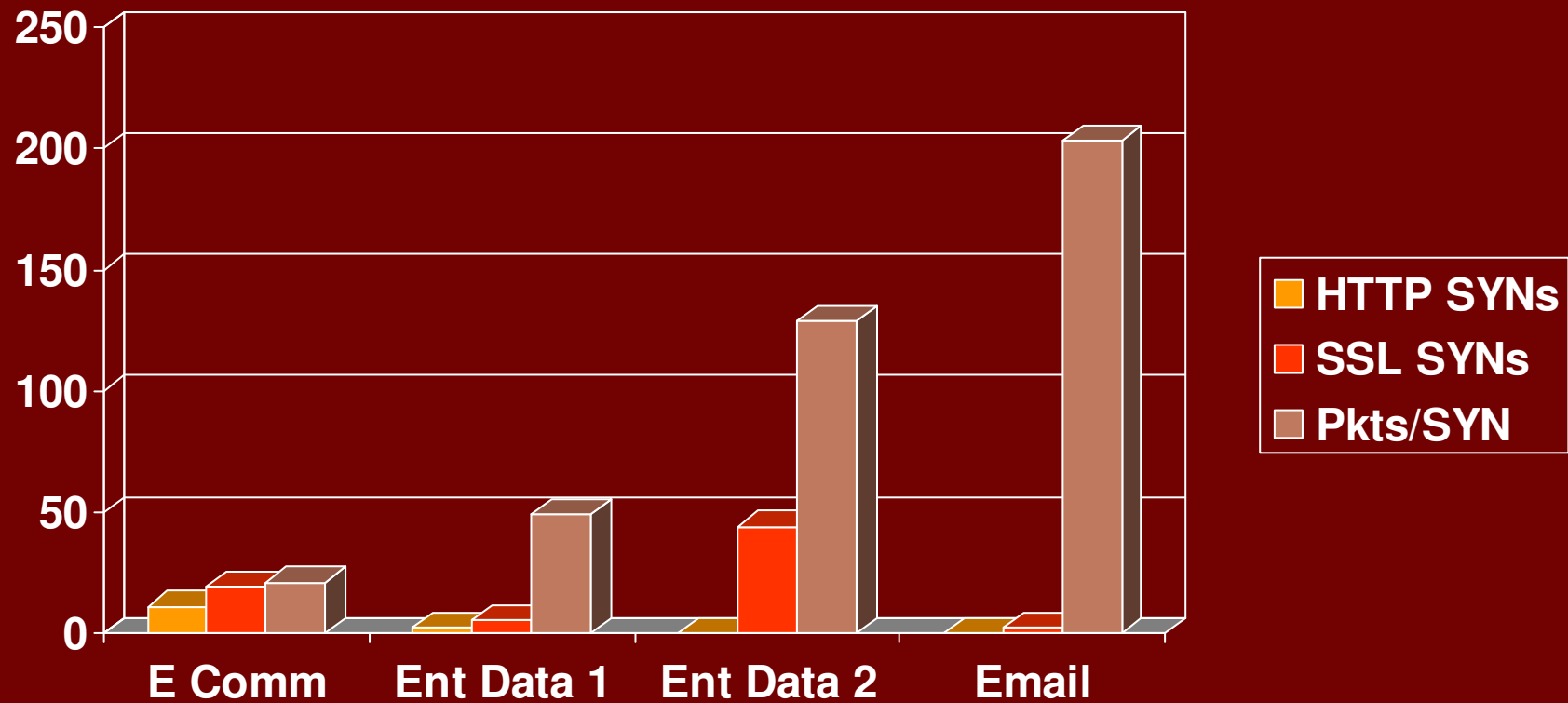
■ IPSec

- More General
 - Handles UDP
 - Tunneling
- Better resistance to denial of service
- Amortizes cost of multiple connections
- Implementations are not mature
- Complex configuration process

Cryptographic Cost

Crypto Operations	Operating Time
Sign(3)	4920 μ s
Verify(3)	86.8 μ s
Sign(65,537)	5100 μ s
Verify(65,537)	240 μ s
Hash(1460)	13.3 μ s
Hash(10)	1.57 μ s

Some Connection Statistics



Experimental Testbed

Client

Router

Router

Server

Plain IP

Concatenated with 3DES encryption

Concatenated with null encryption

Nested with 3DES

Nested with 3DES/null

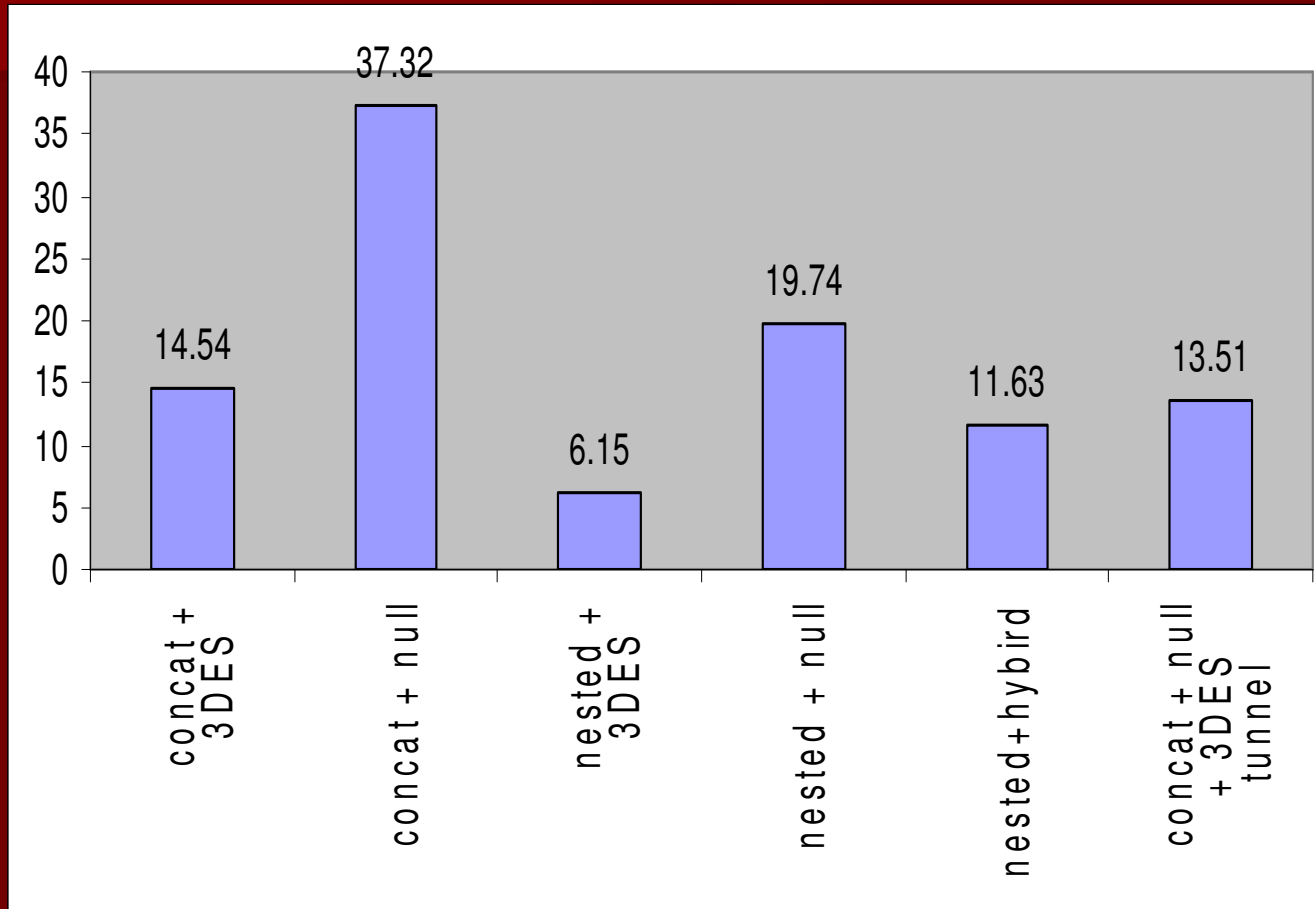
Null concatenated with 3DES tunnel

Nested with null encryption

Benchmarks

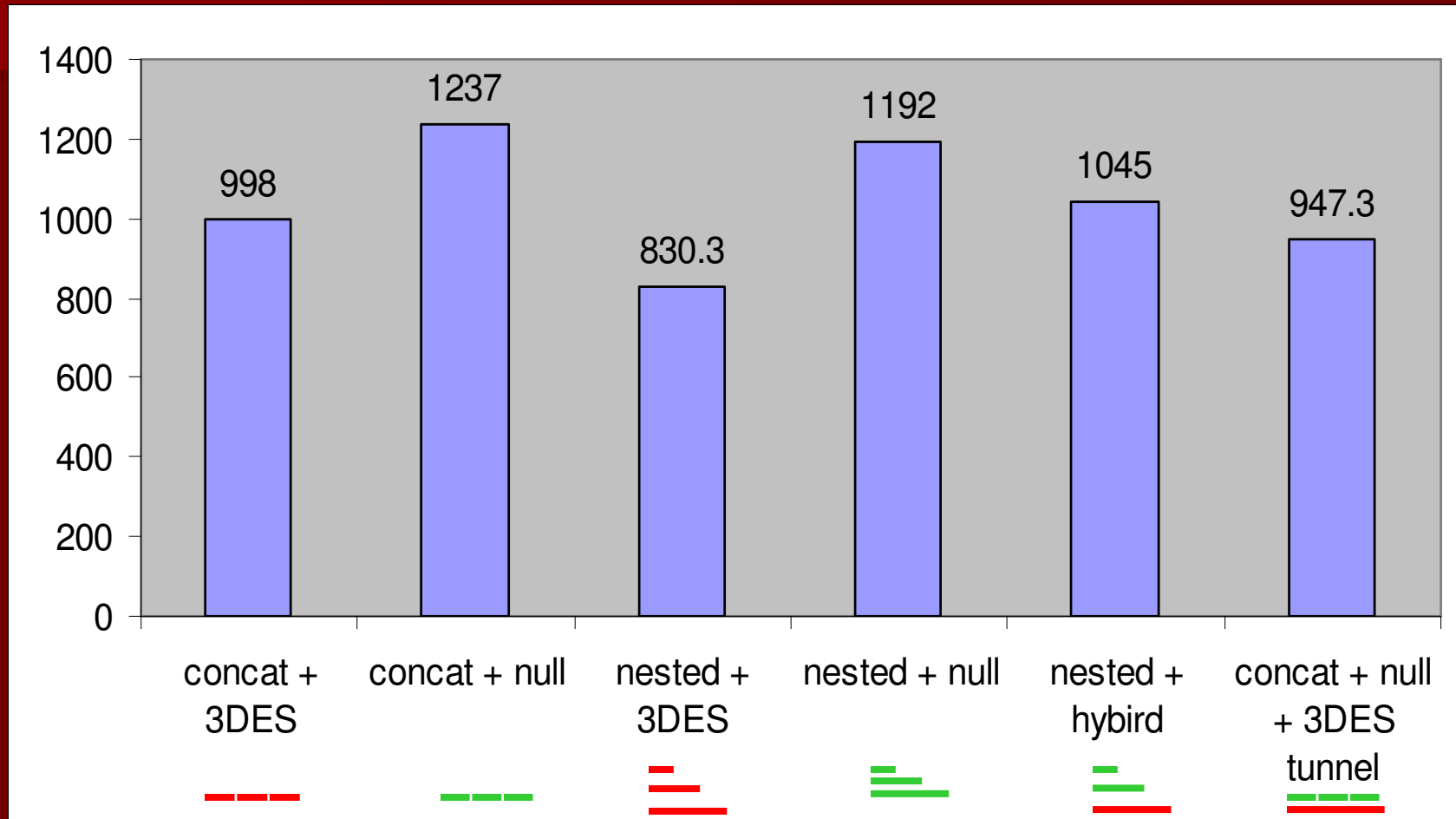
- Performed on a network of four machines running FreeBSD 4.7
 - FreeBSD IPsec implementation was used
 - Neither IKE nor JFK is mature enough to use for setting up such complex security associations.
- Raw TCP: Netperf
 - Throughput
 - Transactions per second

TCP Throughput - Mbits per second



Using netperf.

TCP Transactions per second



Using netperf.
Transactions of 1
byte going both
directions

Nesting VS Concatenation

- Concatenated tunnels do better when the issue is bandwidth, but worse when issue is latency.
- Neither is particularly worse than the other.
- Better to avoid encryption when possible due to the computational costs.
- We can do the authentication only on initiation traffic. Experiments on this case hampered by immaturity of IPSEC.