TVA
:A DoS-limiting Network Architecture*

Xiaowei Yang, David Wetherall, and Tom Anderson
In IEEE/ACM Transactions on Networking (ToN), vol 16, no. 6, Dec. 2008.

Presented by
Soonho Kong
soonhok@cs.cmu.edu

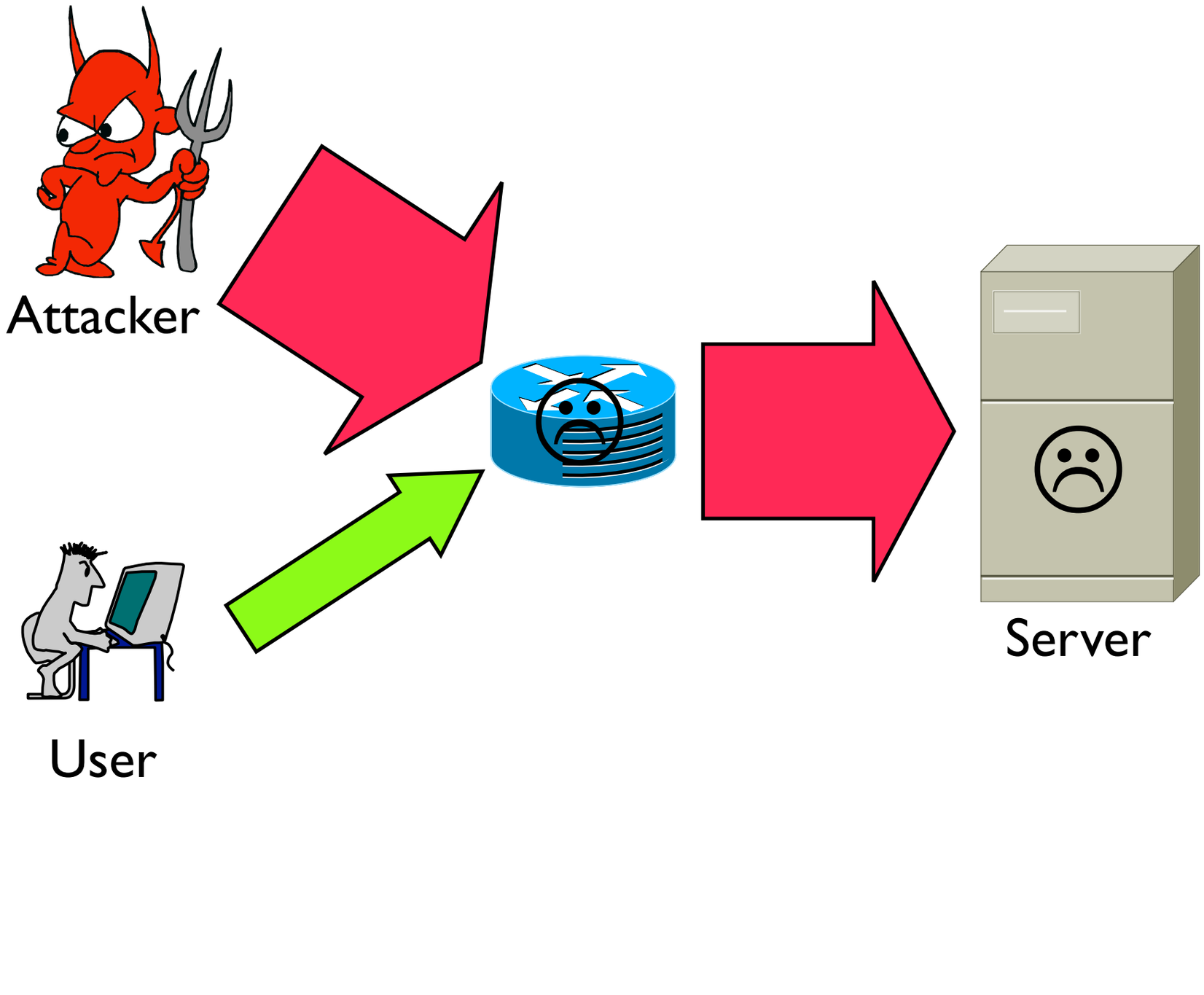
10 November 2010

1

Problem, Goal, and Key Idea

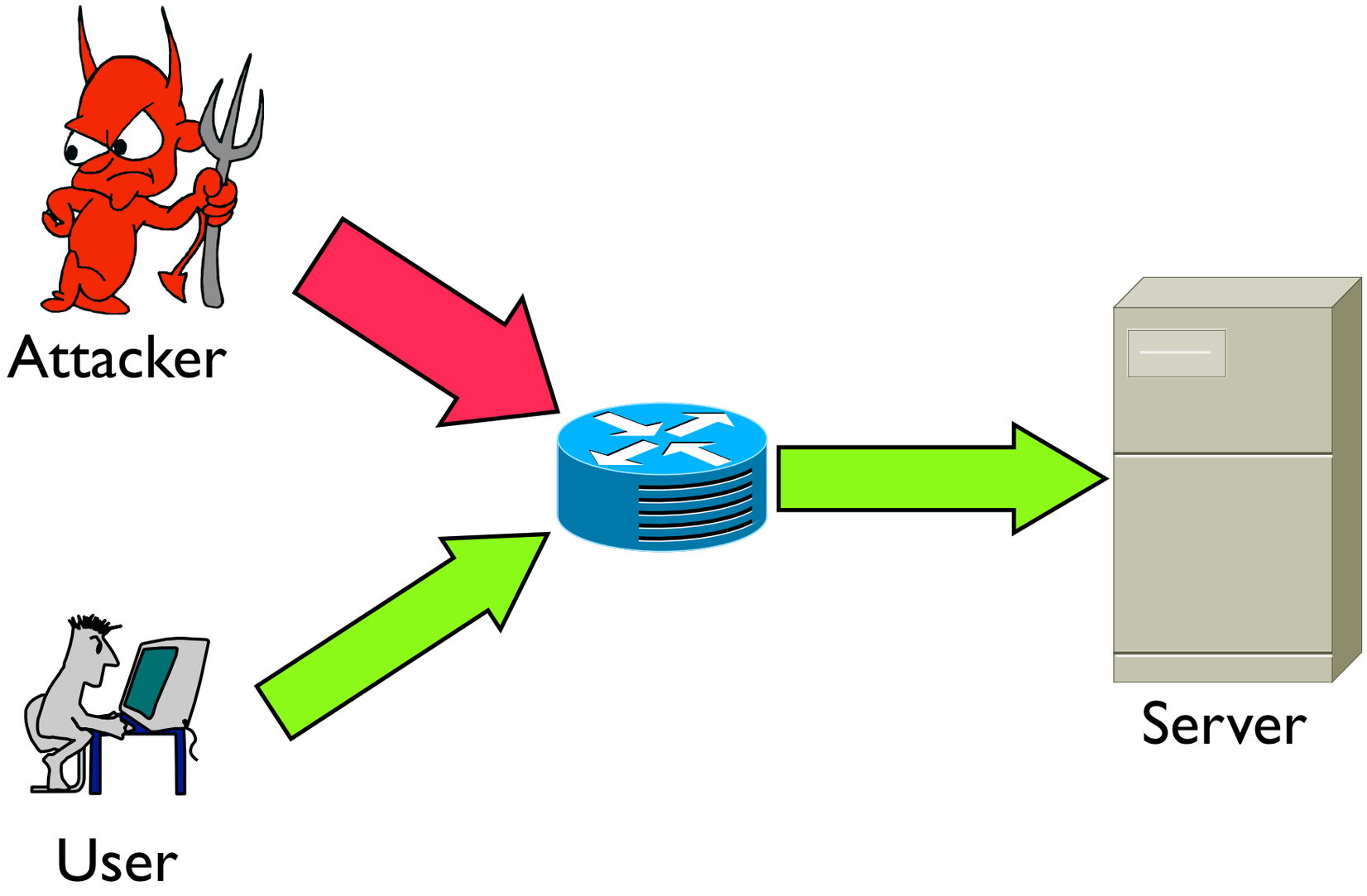
Problem:

DoS(Denial of Service) Attack



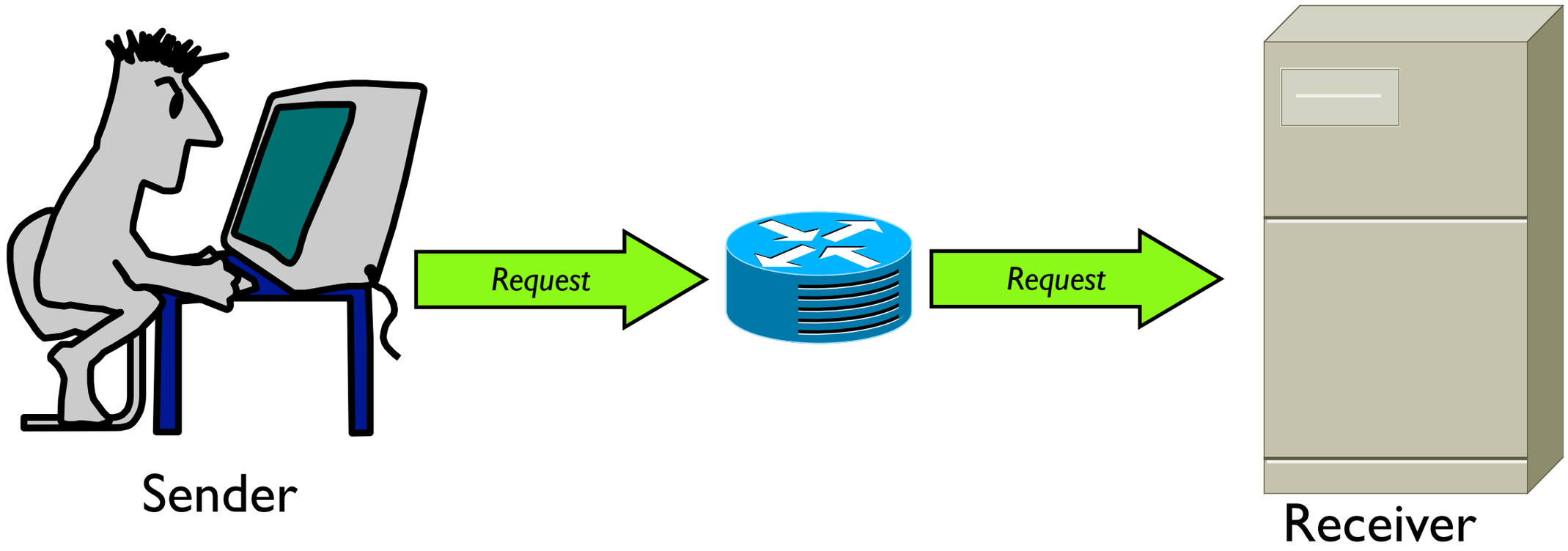
Goal:

Effectively Communicate!



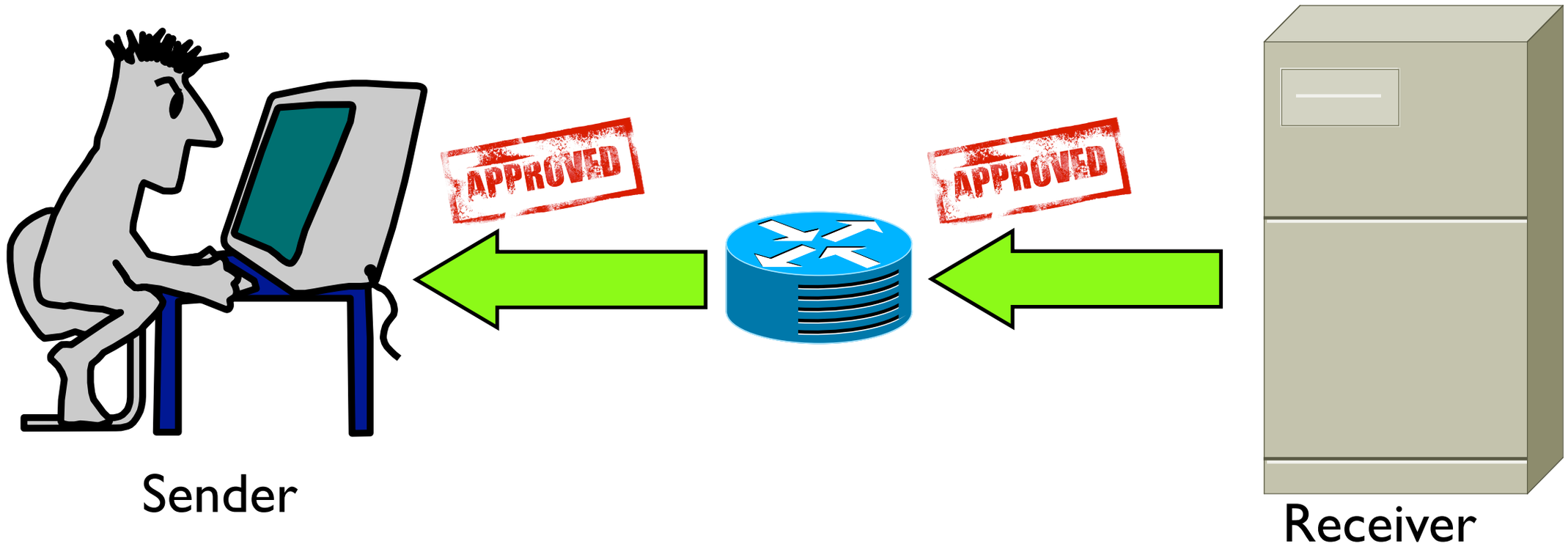
Idea: Capability

Idea: Capability



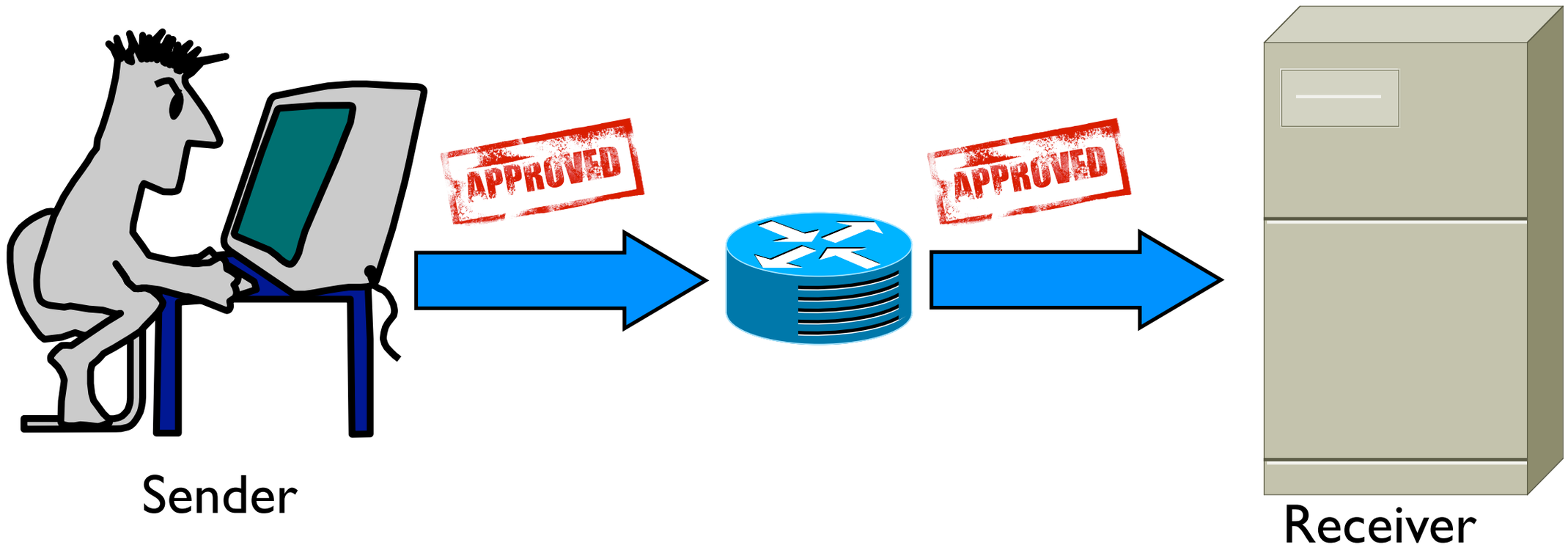
1 Request Capabilities

Idea: Capability



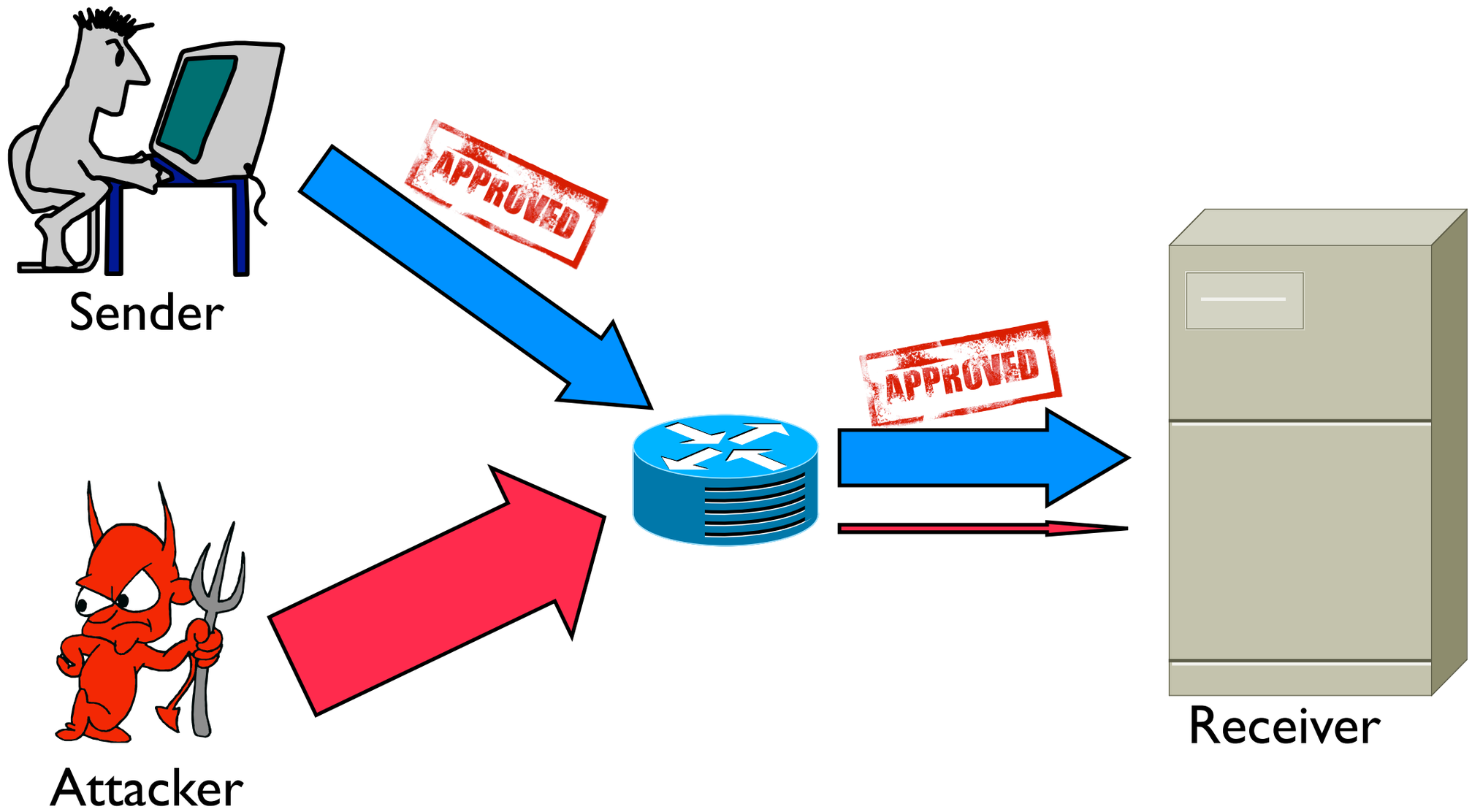
2 Send Capabilities

Idea: Capability



3 Send Packets with Capabilities

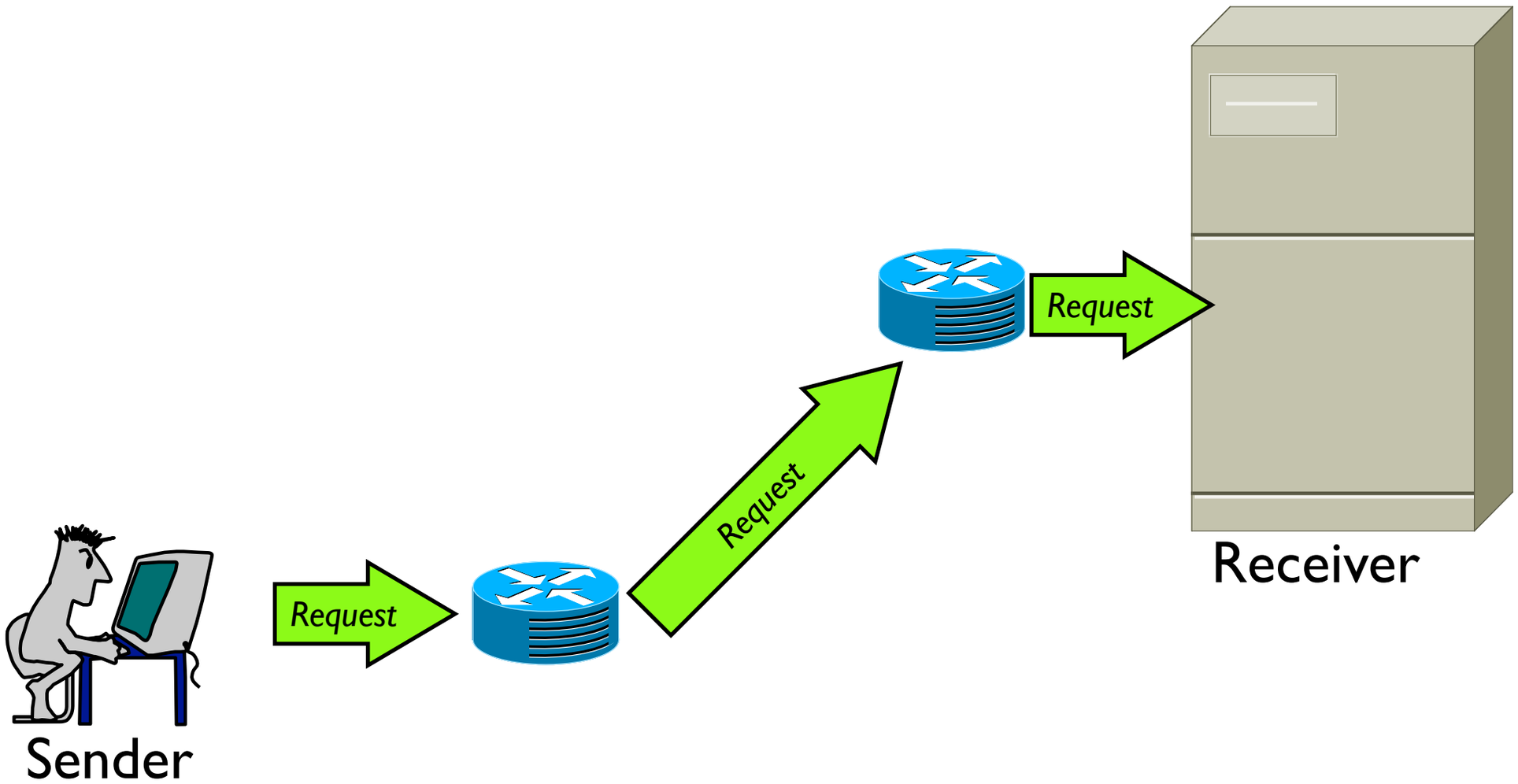
Idea: Capability



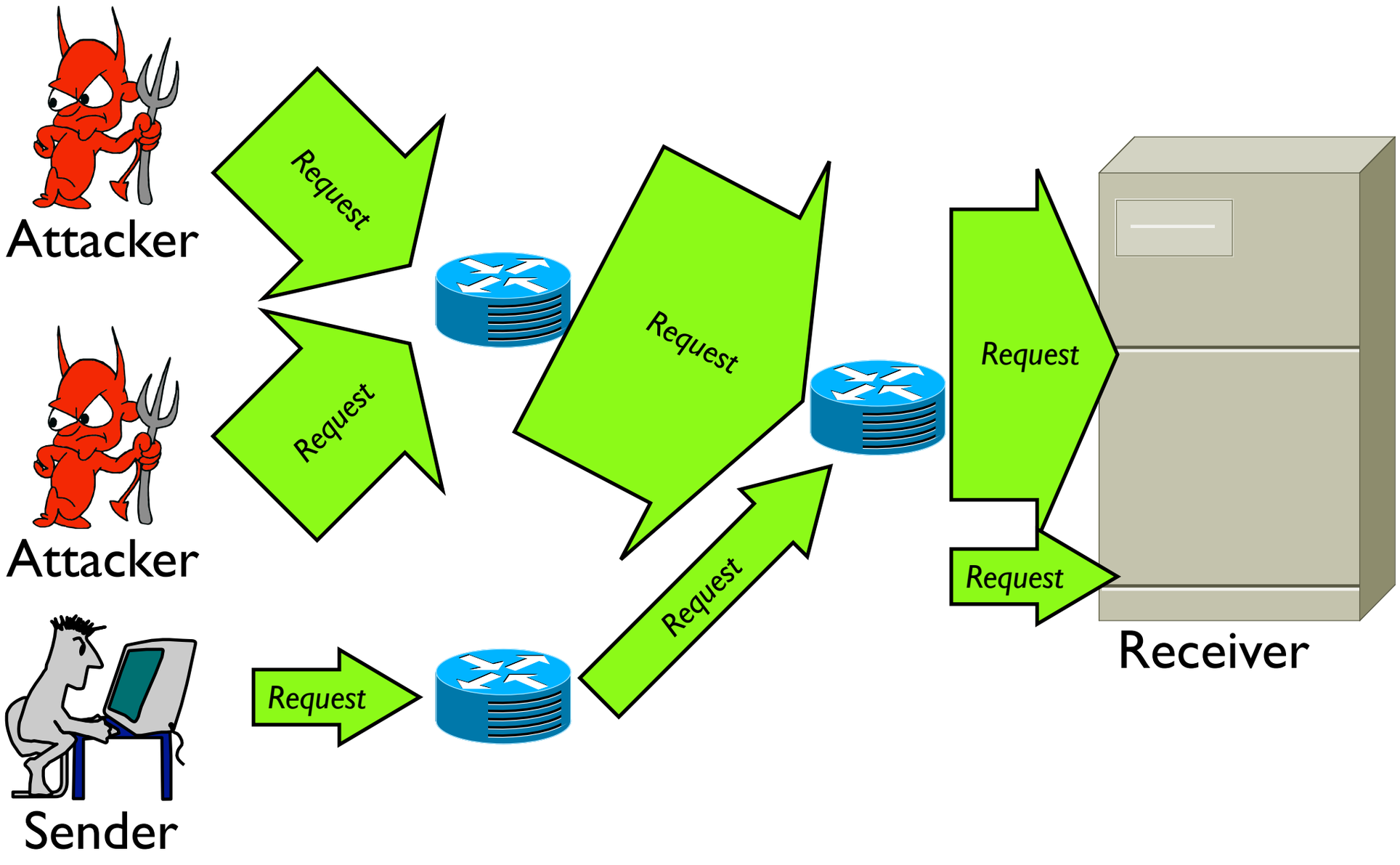
2

Key Challenges and Their Solutions

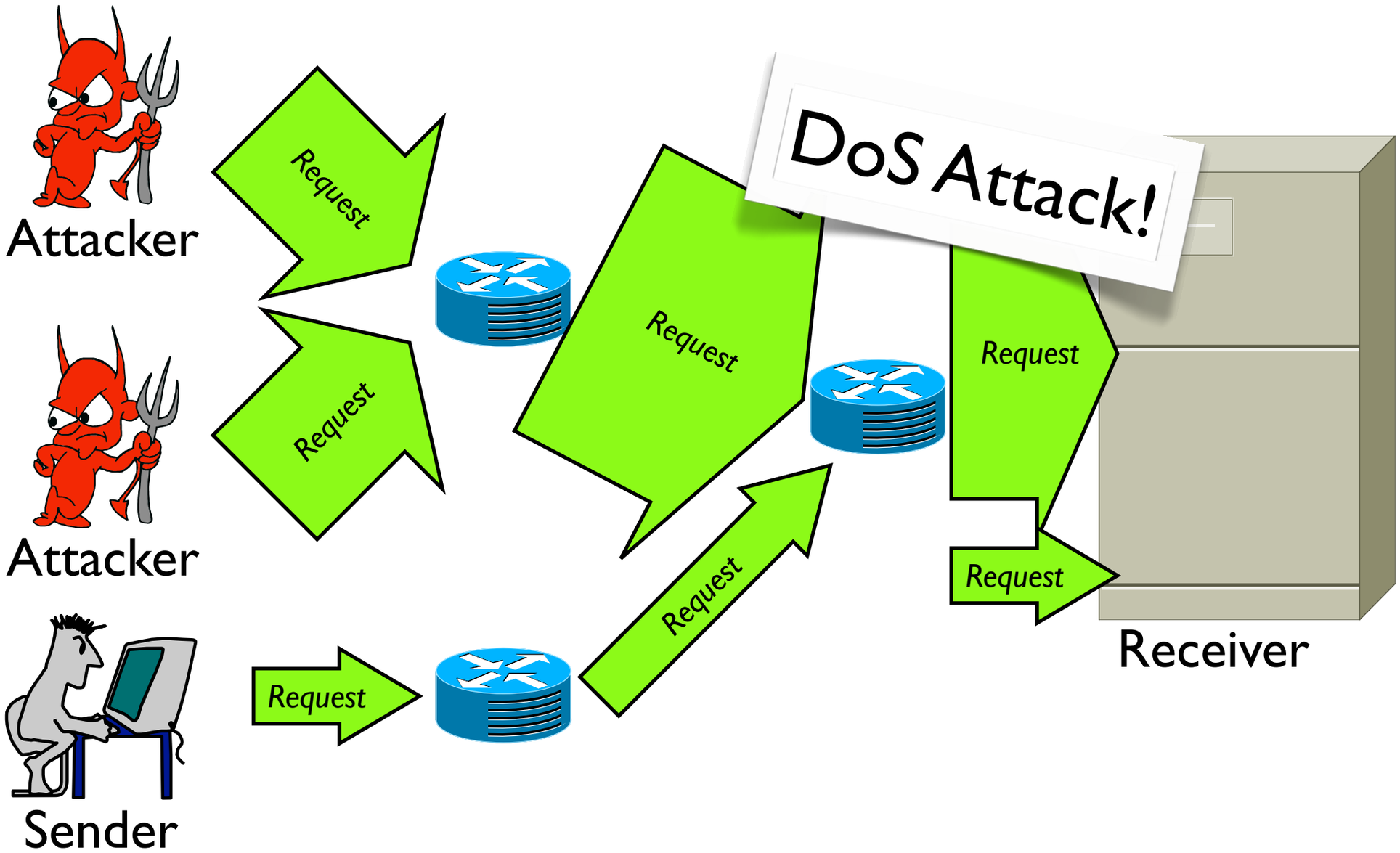
Challenge:
Request Flood



Challenge:
Request Flood

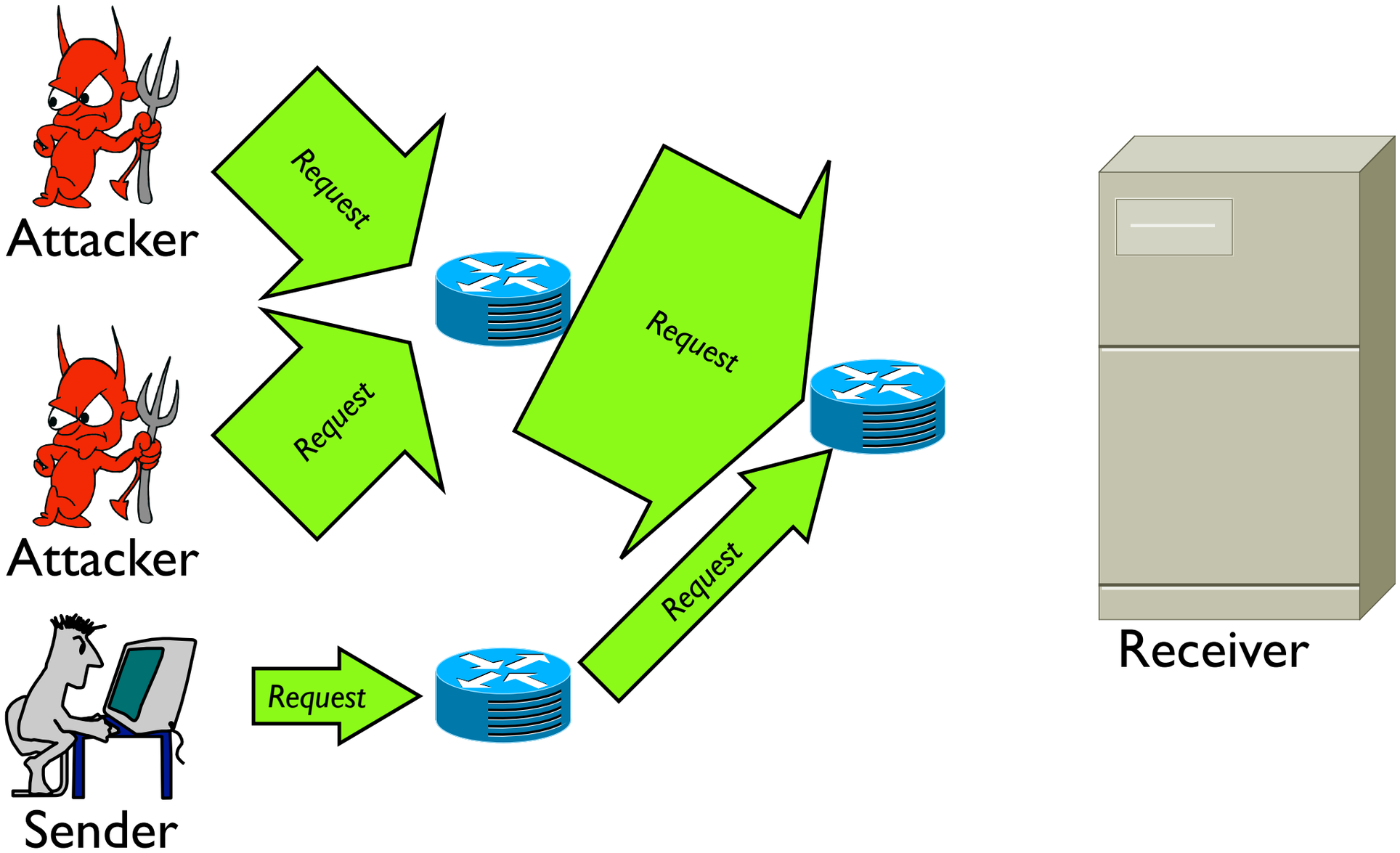


Challenge:
Request Flood



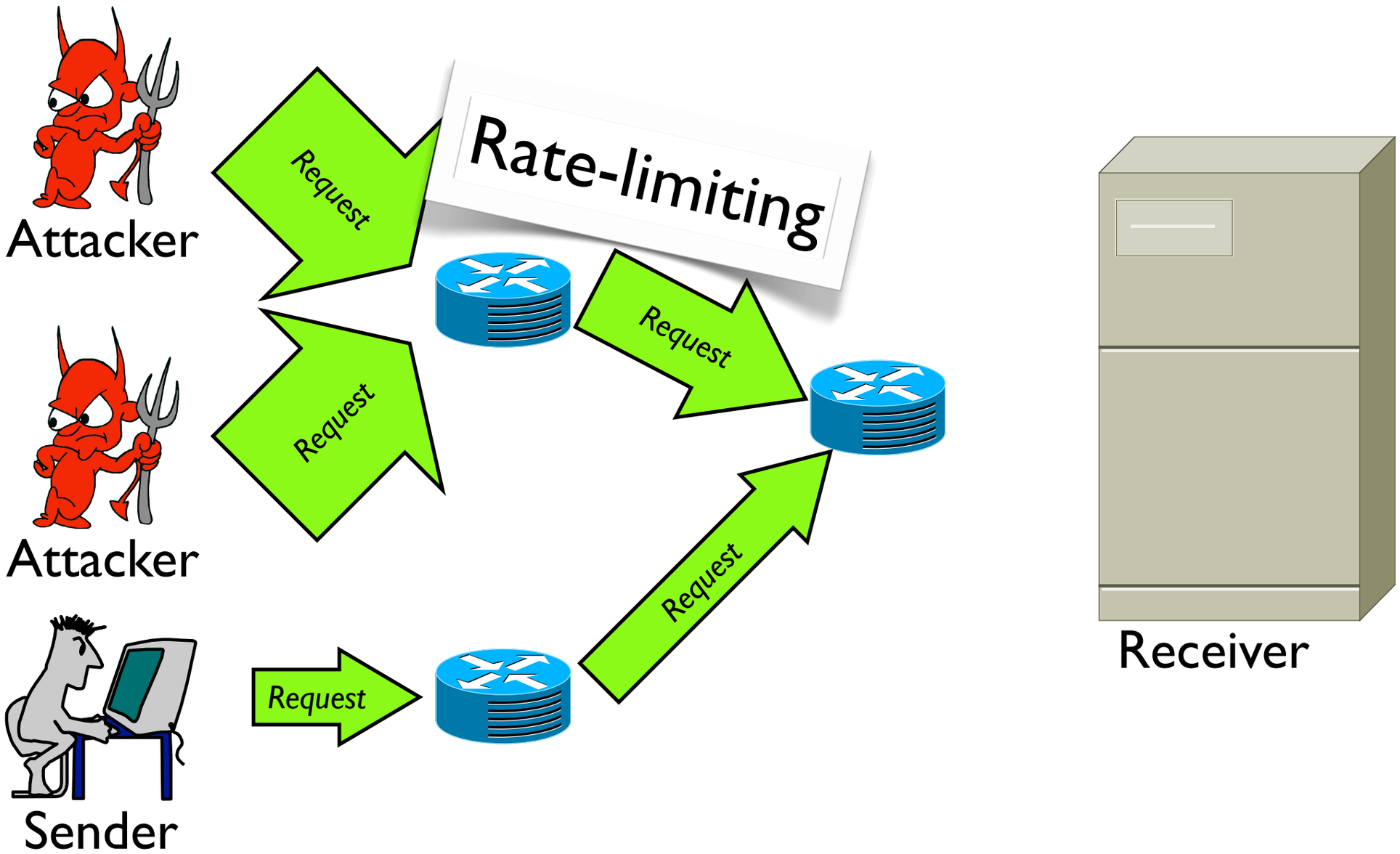
Solution:

Rate-limiting Request + per-identifier Fair-Queuing



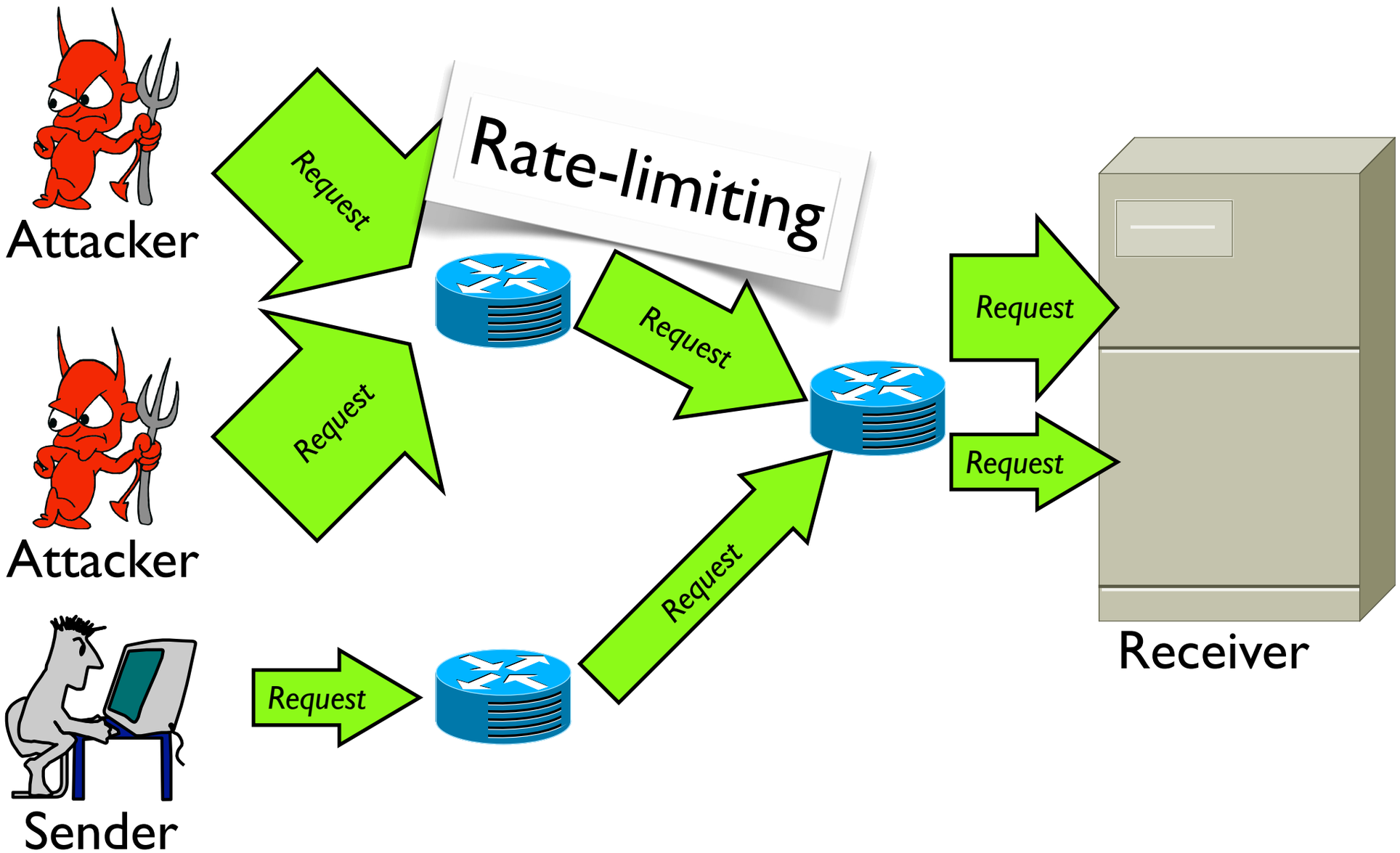
Solution:

Rate-limiting Request + per-identifier Fair-Queuing



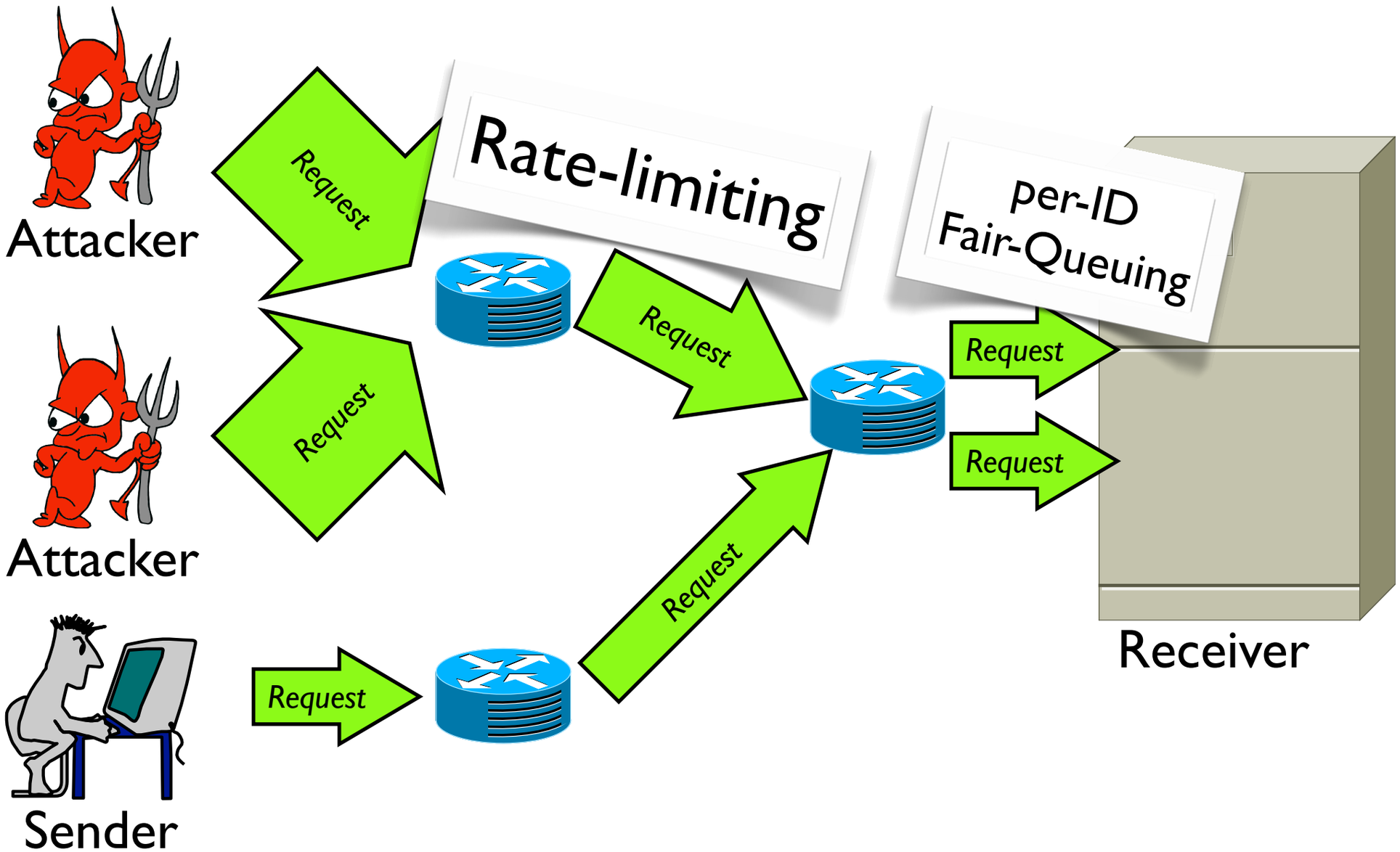
Solution:

Rate-limiting Request + per-identifier Fair-Queuing

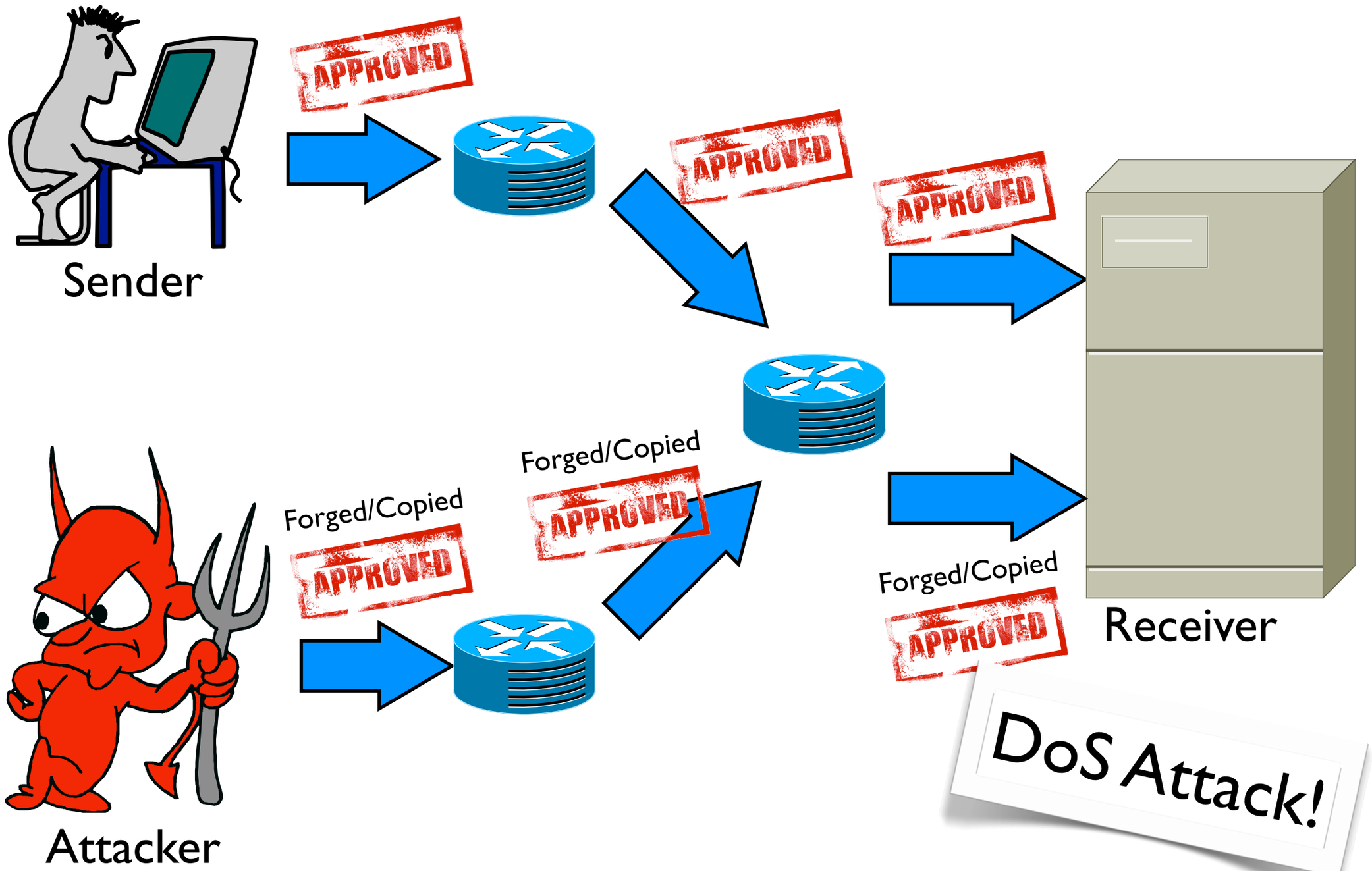


Solution:

Rate-limiting Request + per-identifier Fair-Queuing

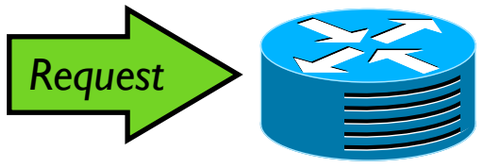


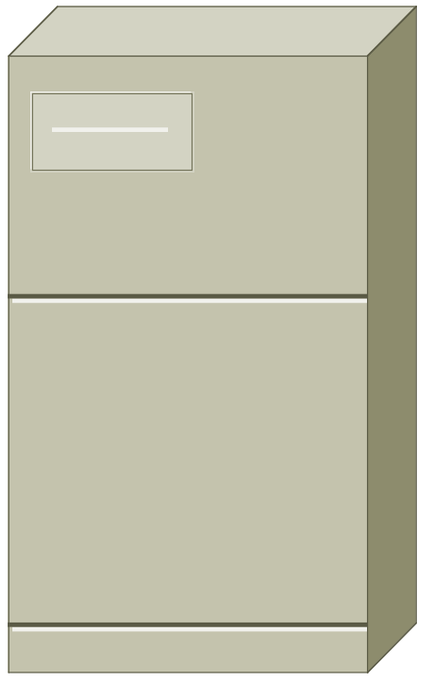
Challenge:
Secure Capabilities



Solution:
Cryptographic Hash

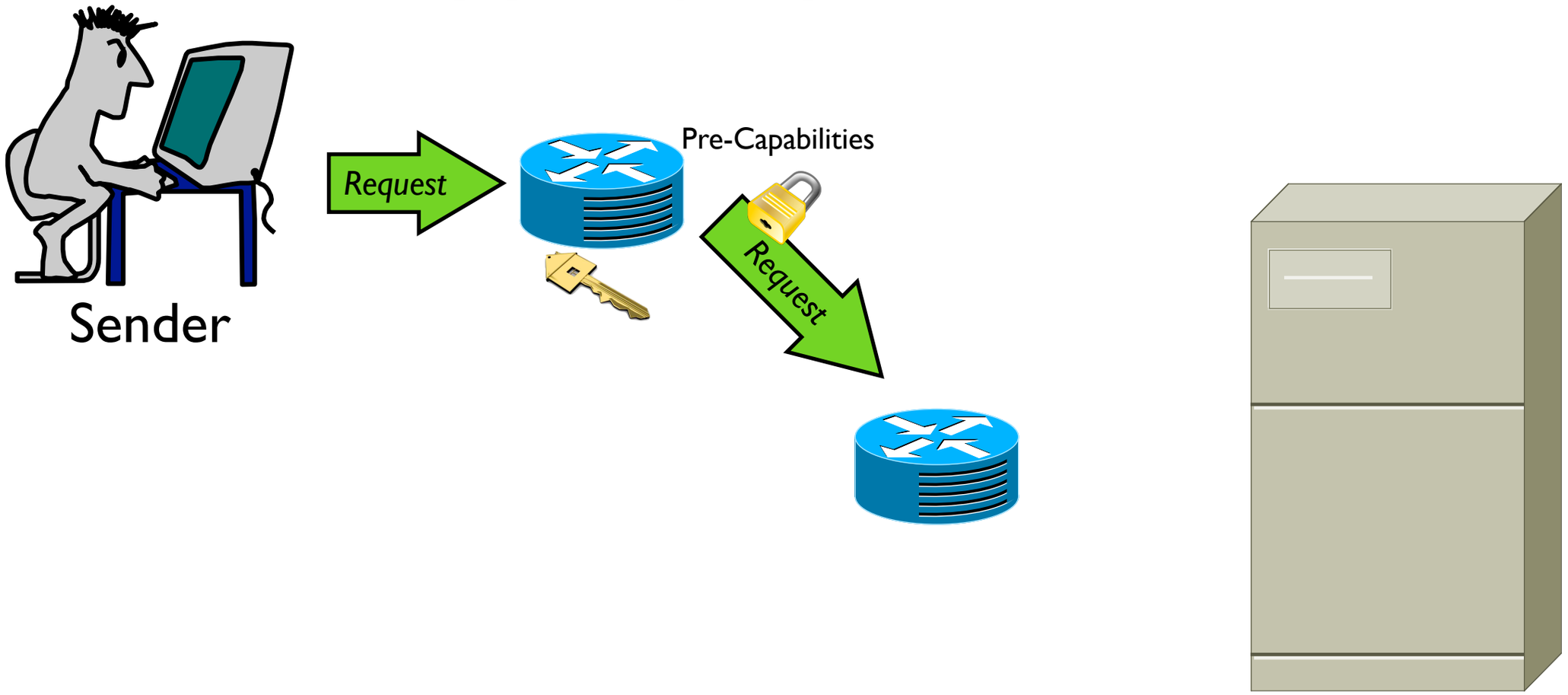
Sender





Receiver

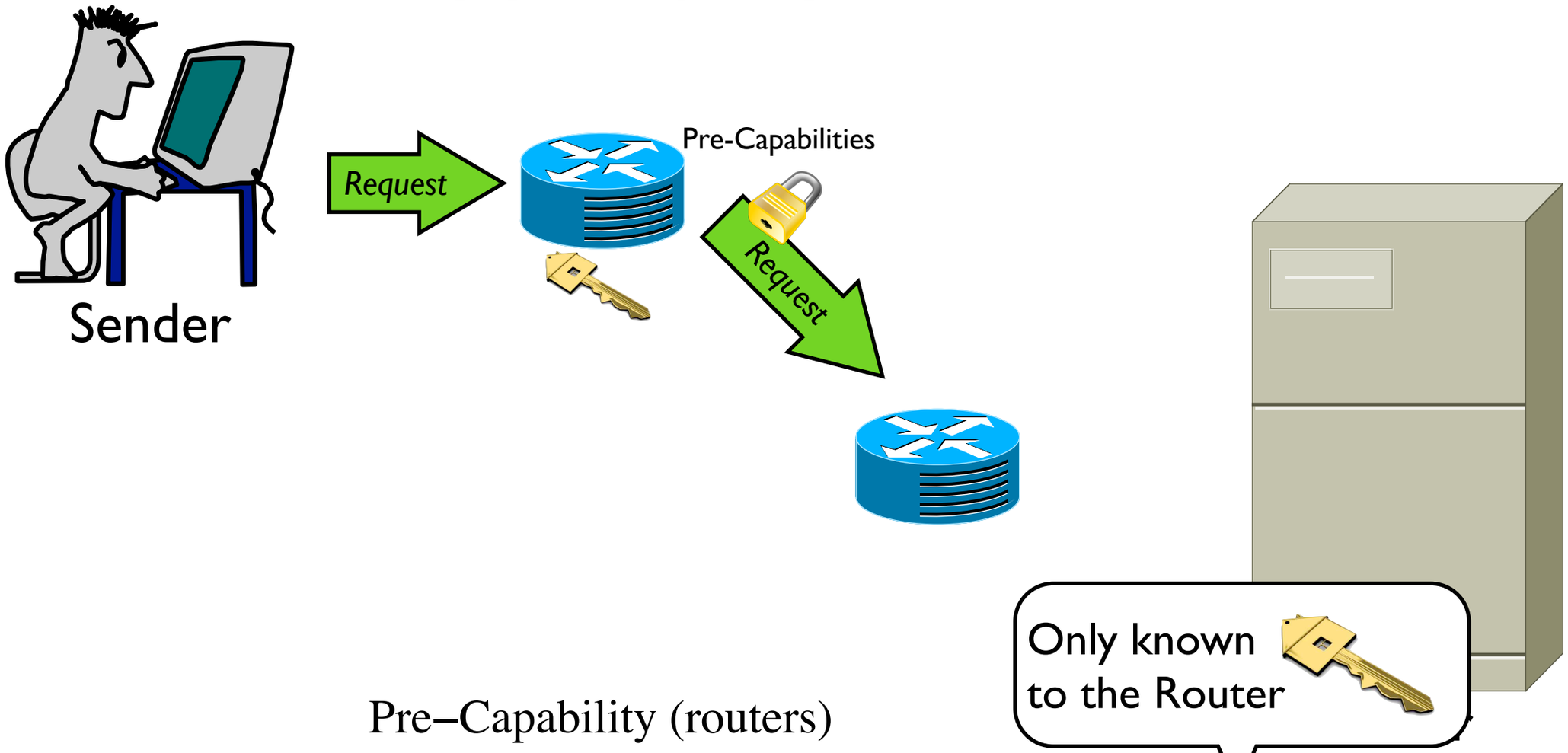
Solution:
Cryptographic Hash



Pre–Capability (routers)

timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

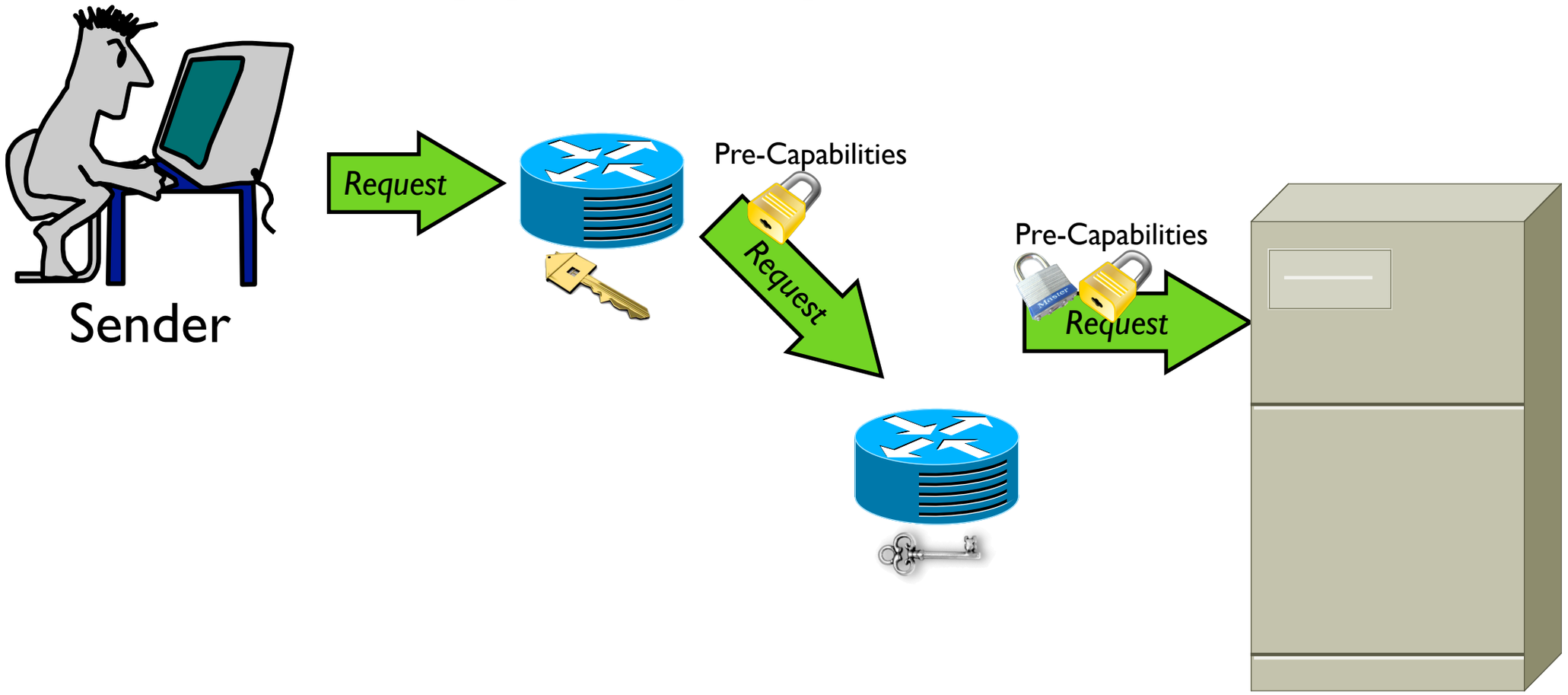
Solution:
Cryptographic Hash



Pre–Capability (routers)

timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Solution:
Cryptographic Hash

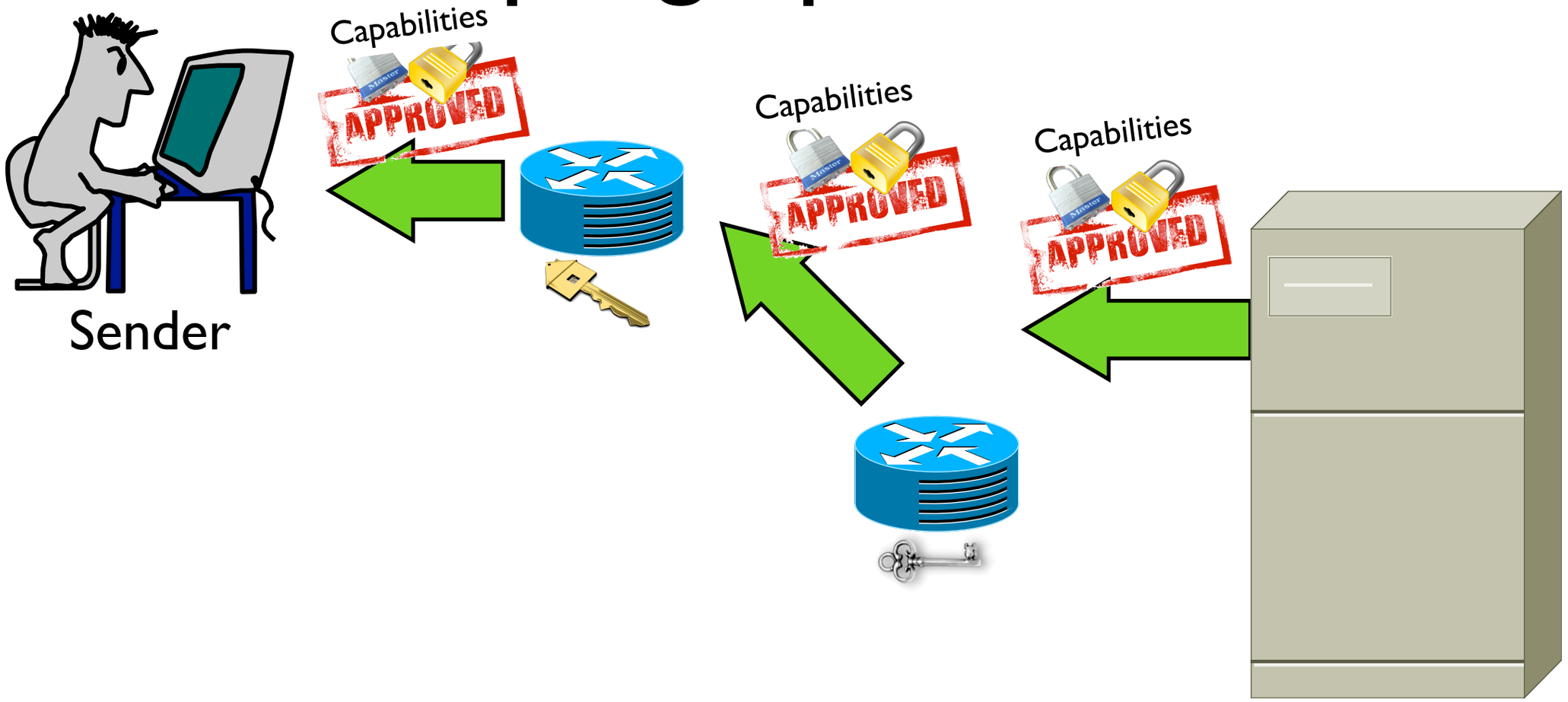


Pre–Capability (routers)

timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Solution:

Cryptographic Hash



Pre–Capability (routers)

timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

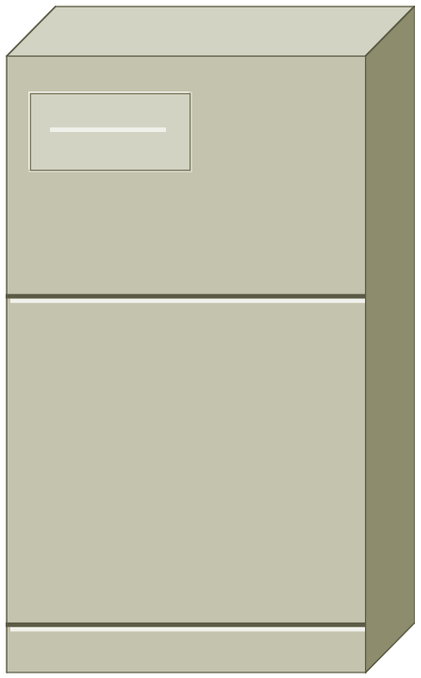
Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash

Sender



Receiver

Pre–Capability (routers)

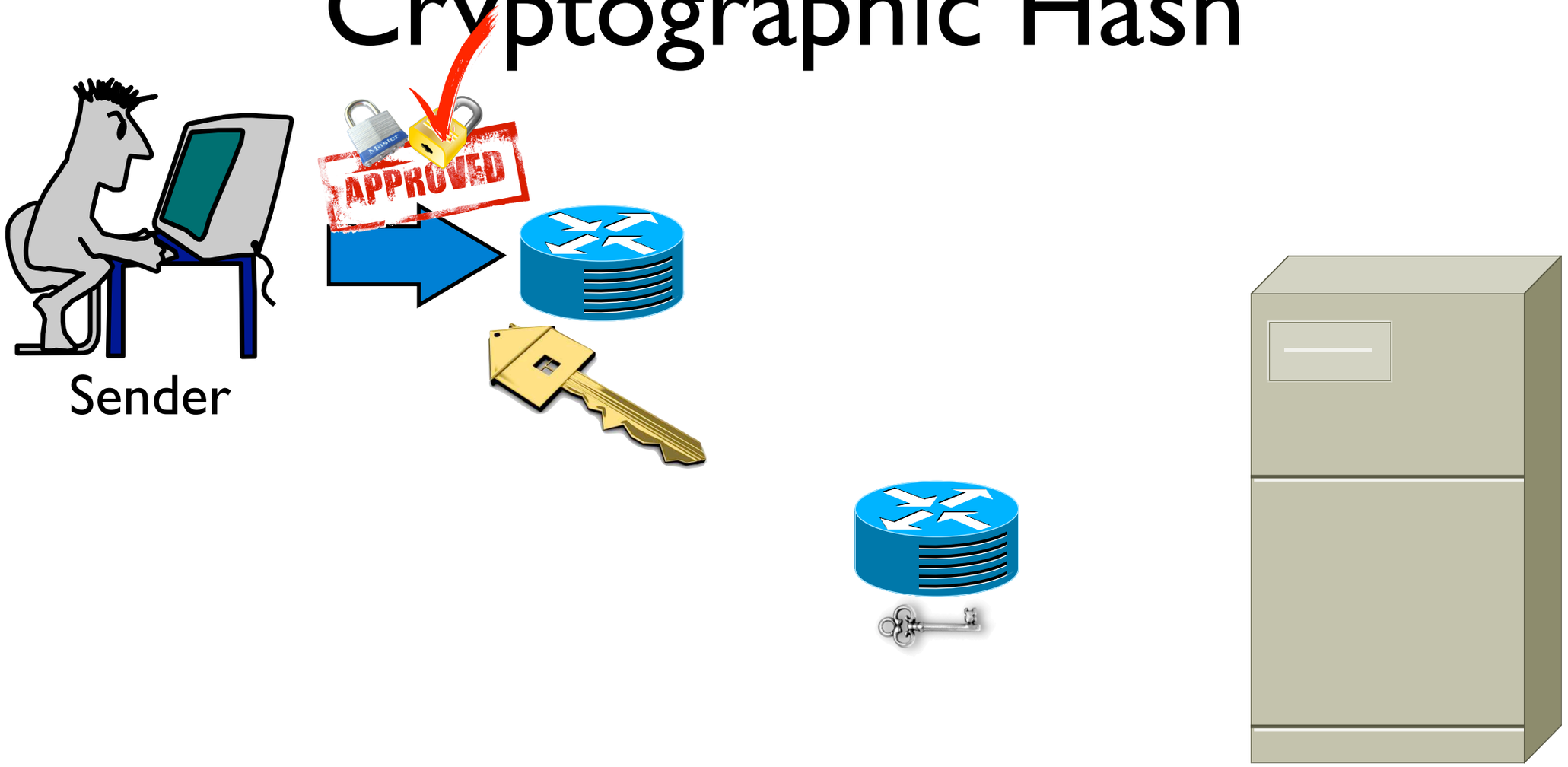
timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash



Pre–Capability (routers)

timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash

Pre–Capability (routers)

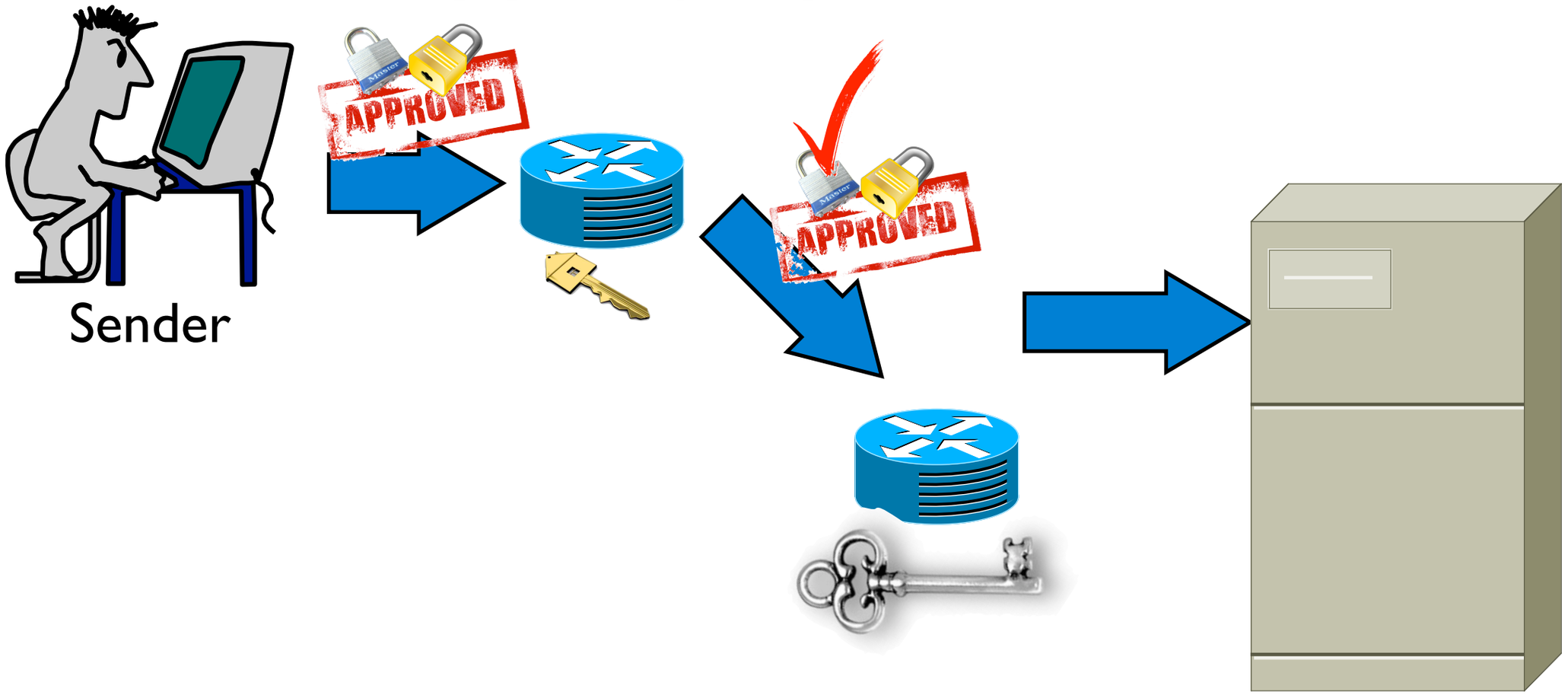
timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash



Pre–Capability (routers)

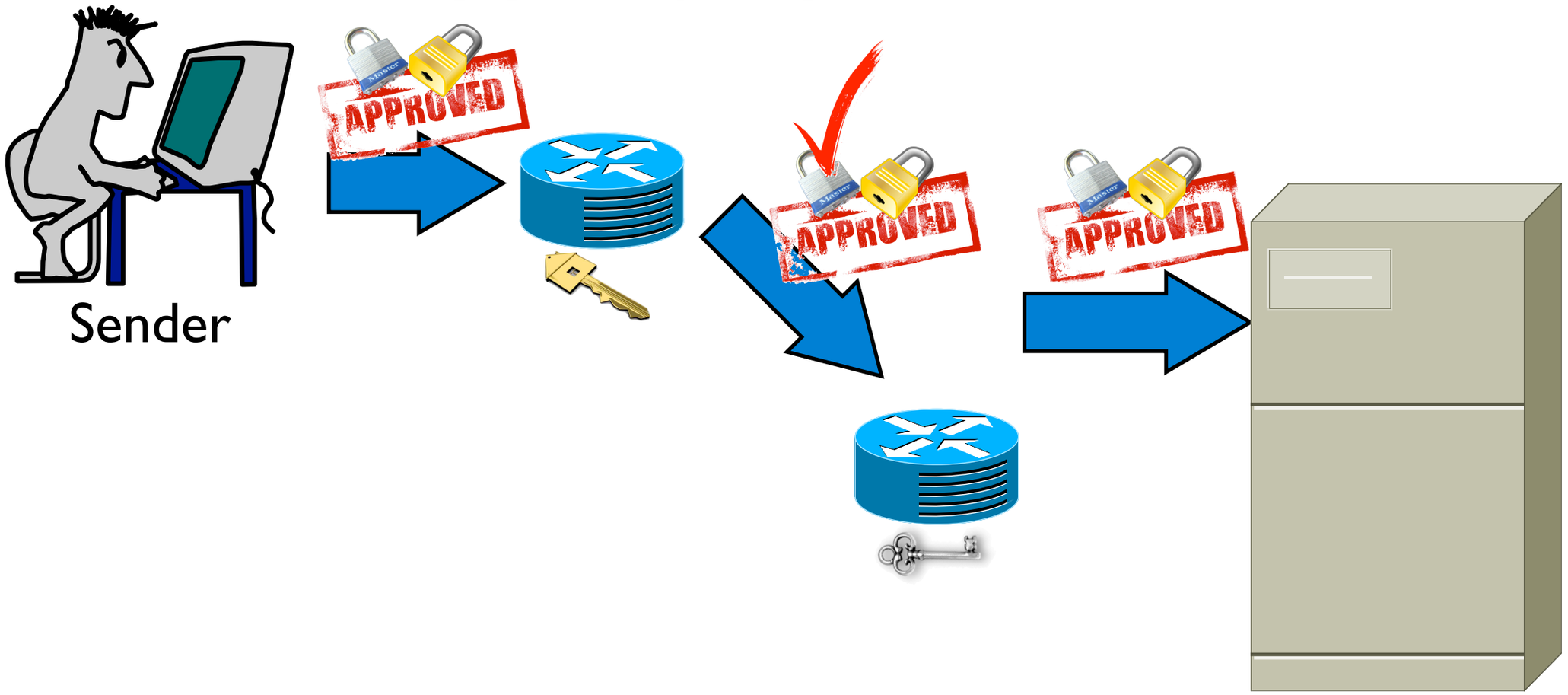
timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash



Pre–Capability (routers)

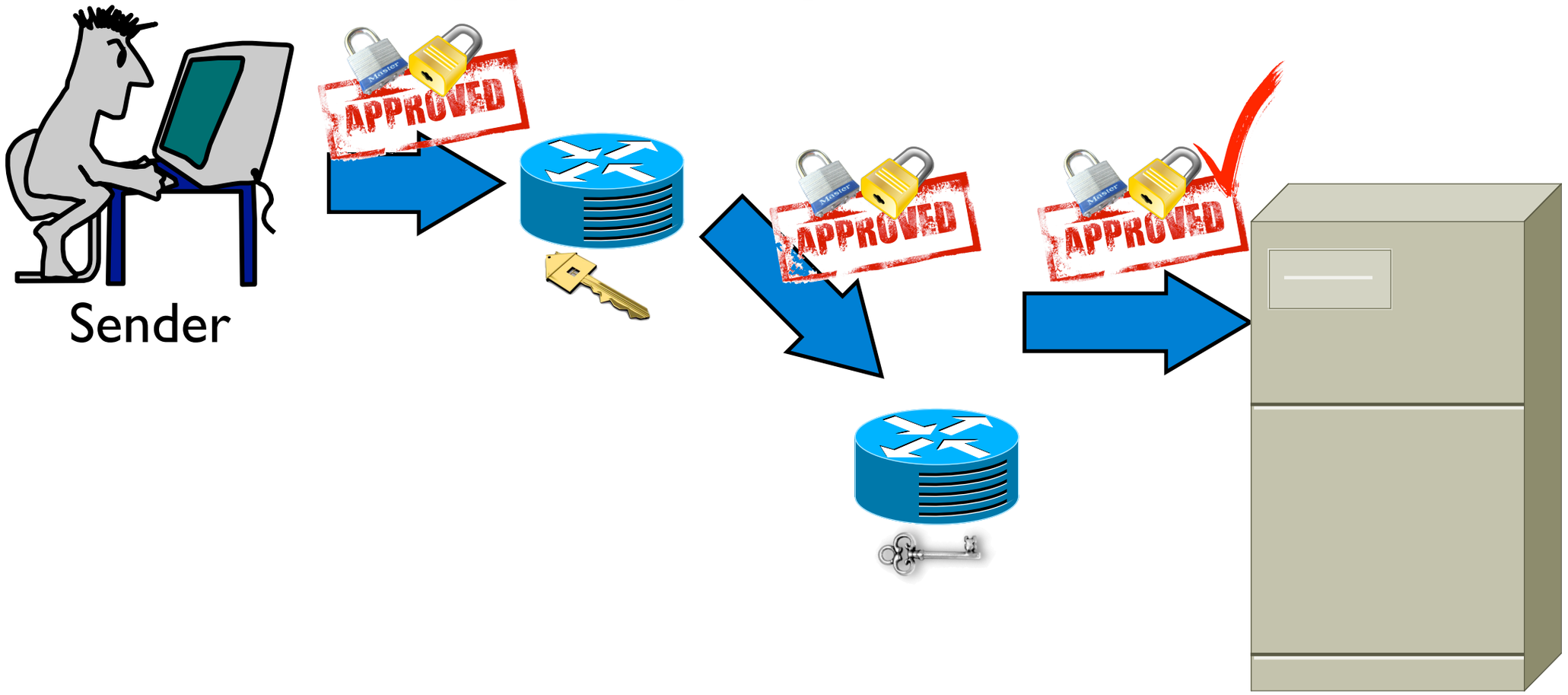
timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Cryptographic Hash



Pre–Capability (routers)

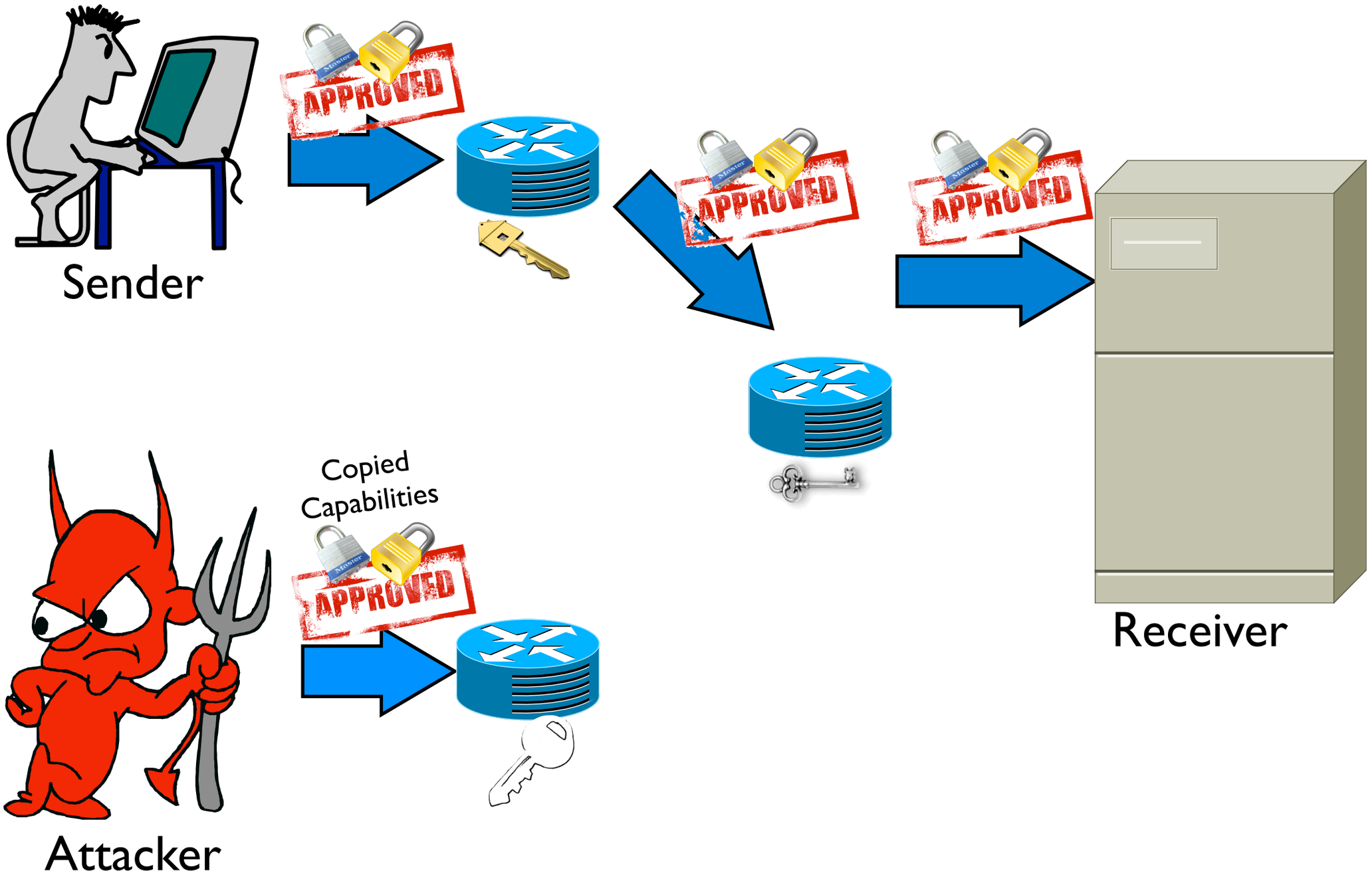
timestamp (8 bits)	hash(src IP, dest IP, in iface, out iface,time, secret) (56 bits)

Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

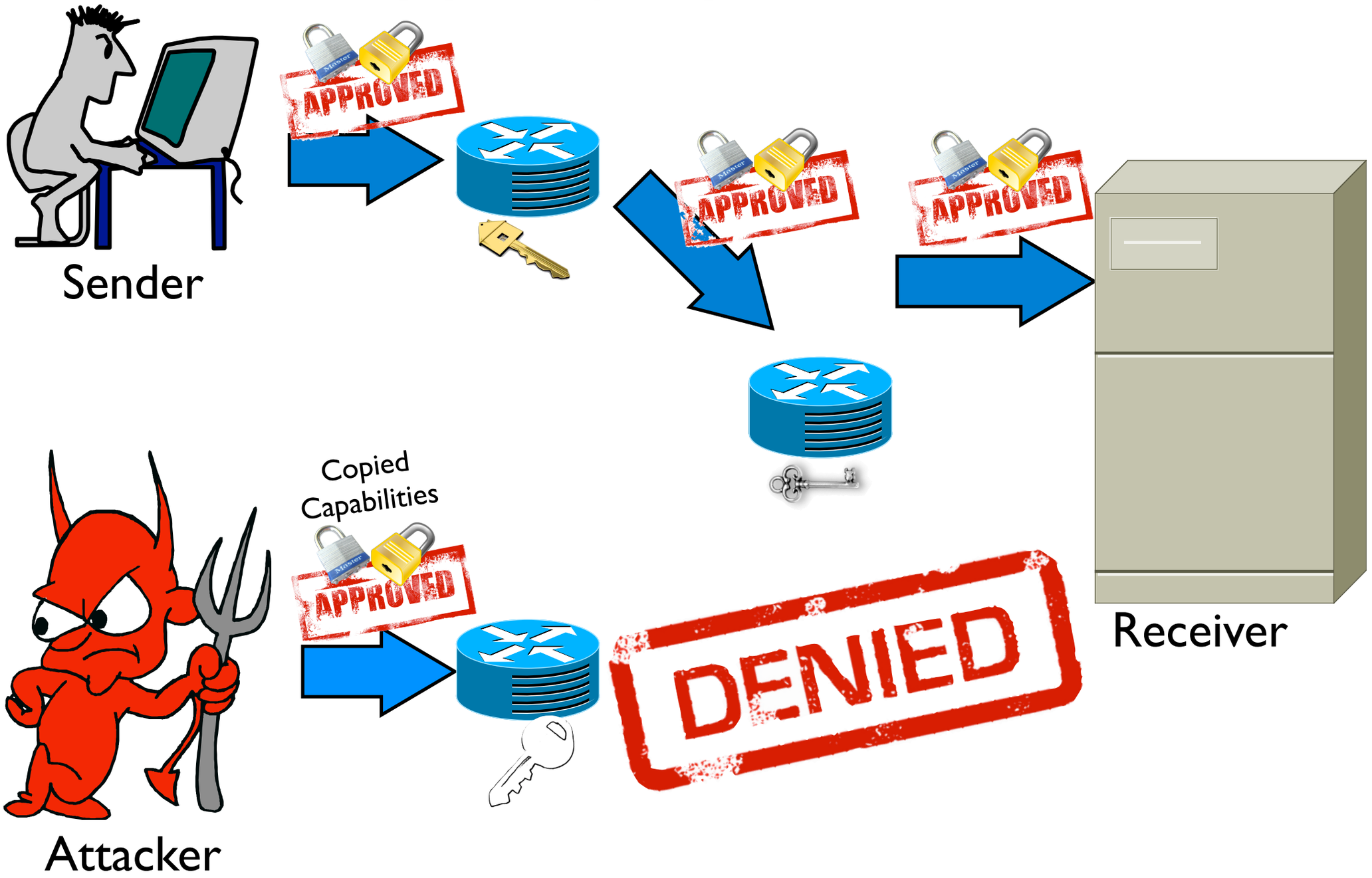
Solution:

Cryptographic Hash

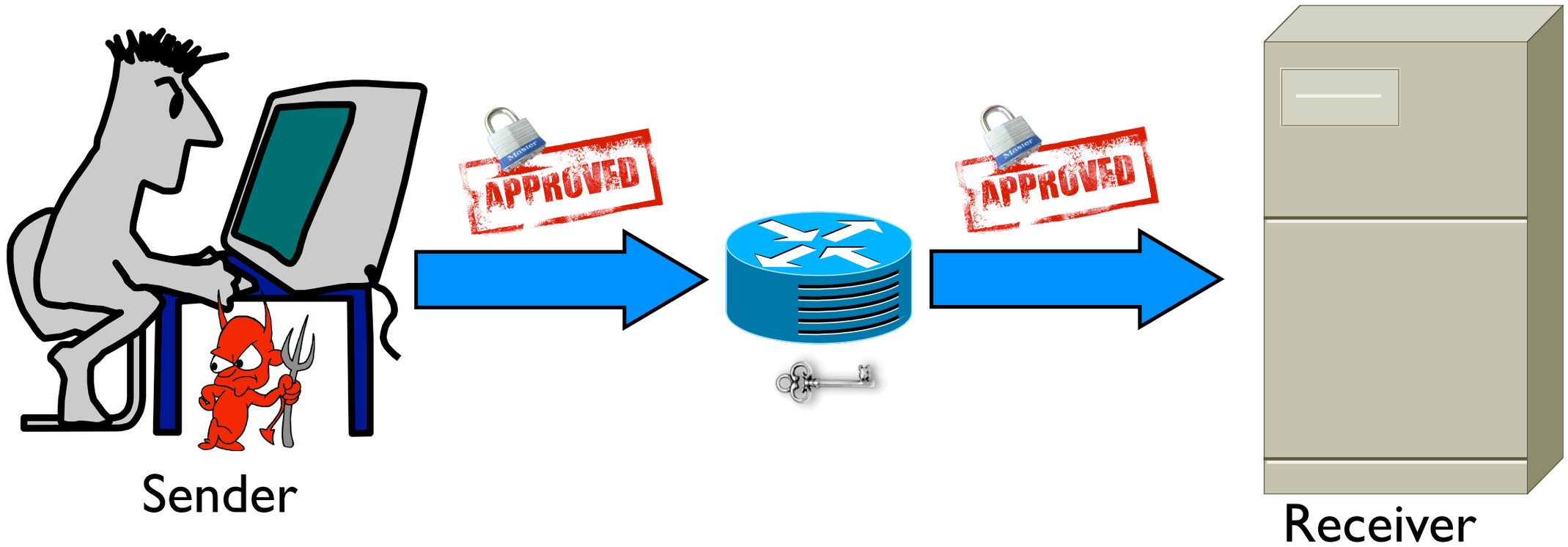


Solution:

Cryptographic Hash

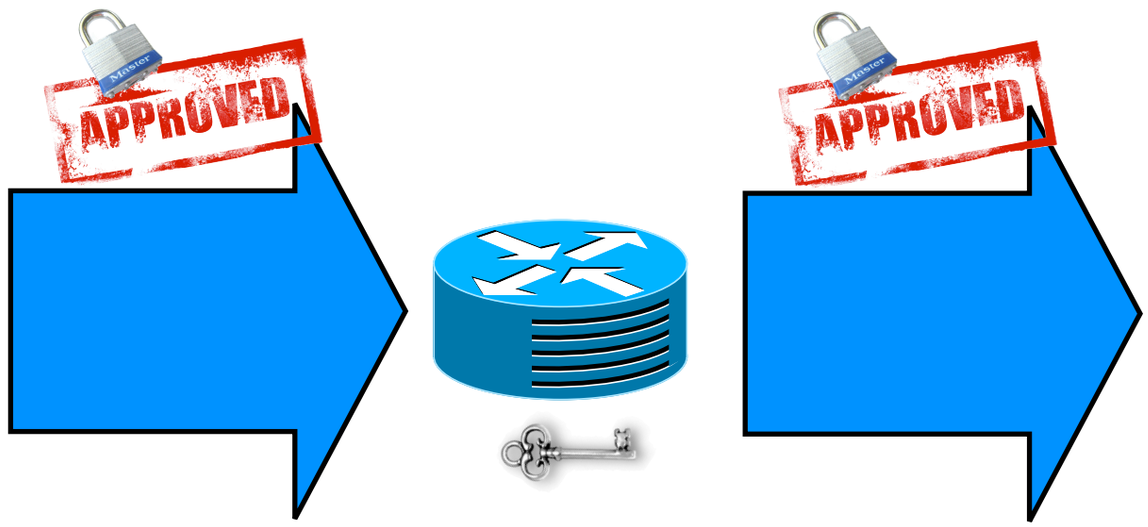


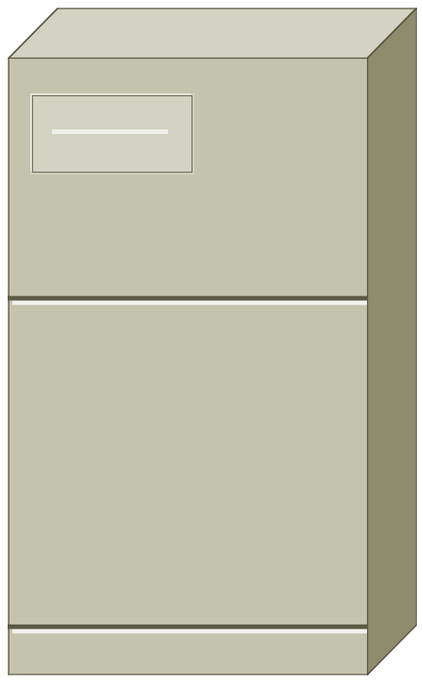
Challenge:
Abuse Capabilities



Challenge:
Abuse Capabilities

Attacker



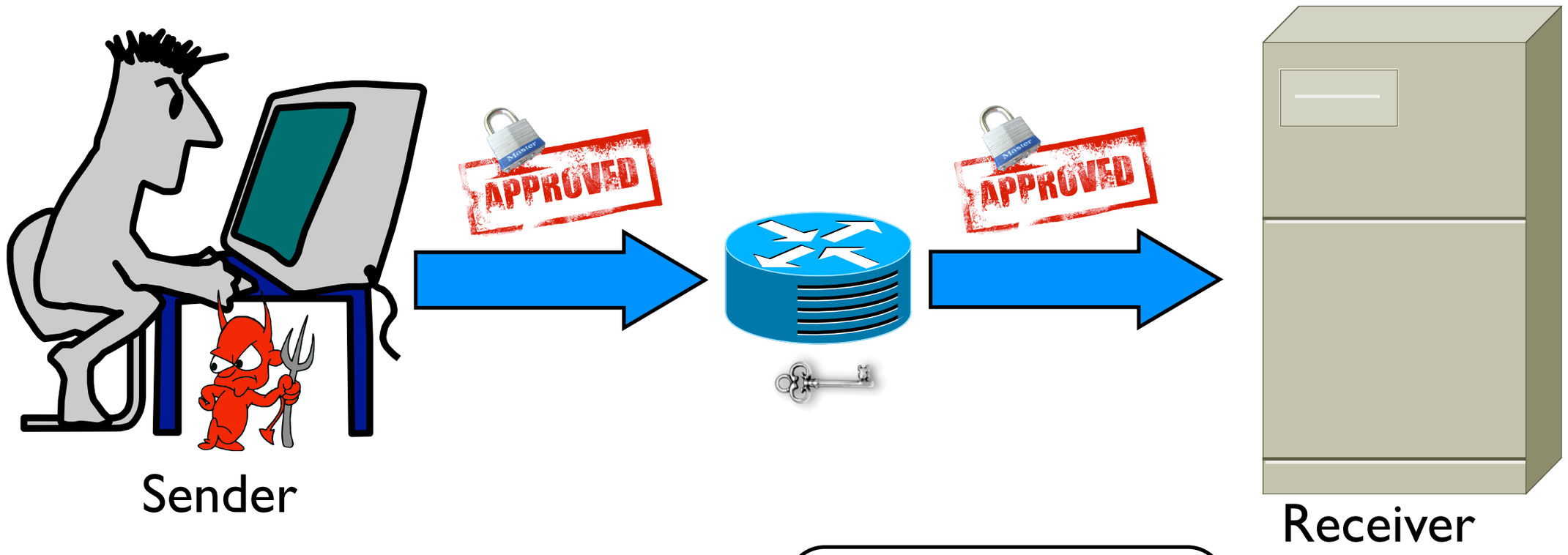


Receiver

DoS Attack!

Solution:

Limit the Amount of Data & Period of Validity



Capability (hosts)

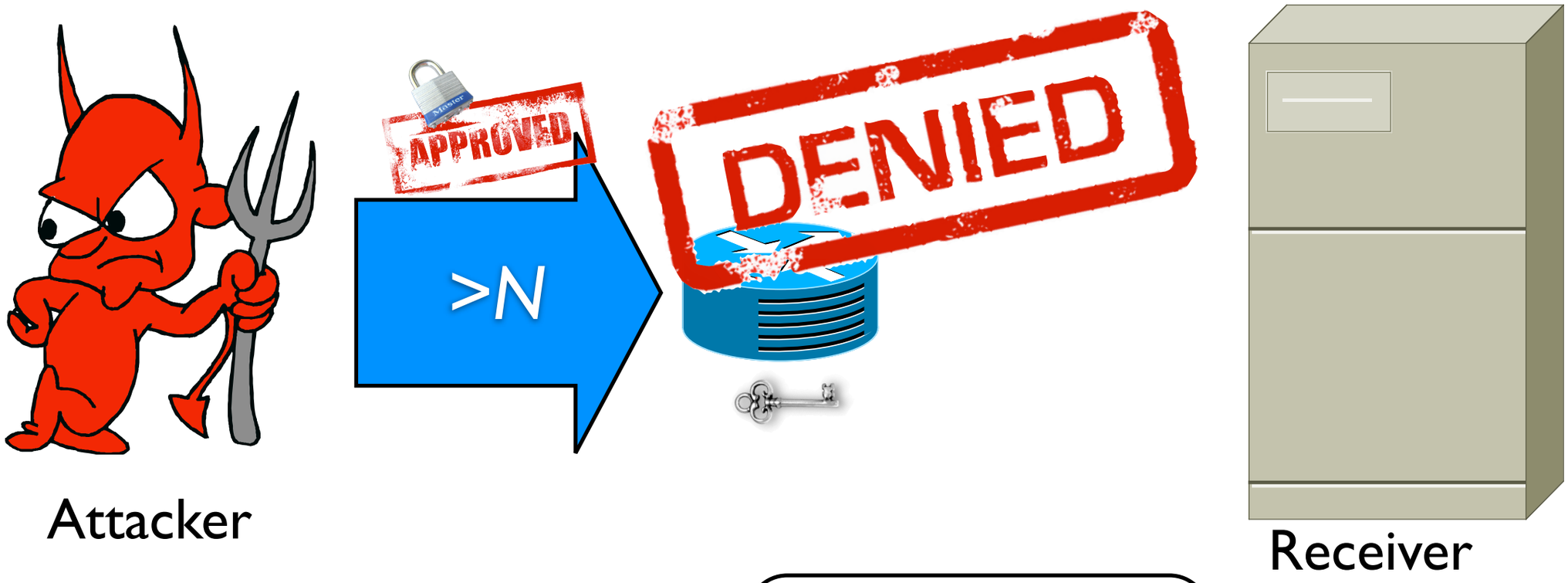
the Amount of Data

timestamp (8 bits)	hash(pre−capability, N, T) (56 bits)

the Period of Validity

Solution:

Limit the Amount of Data & Period of Validity



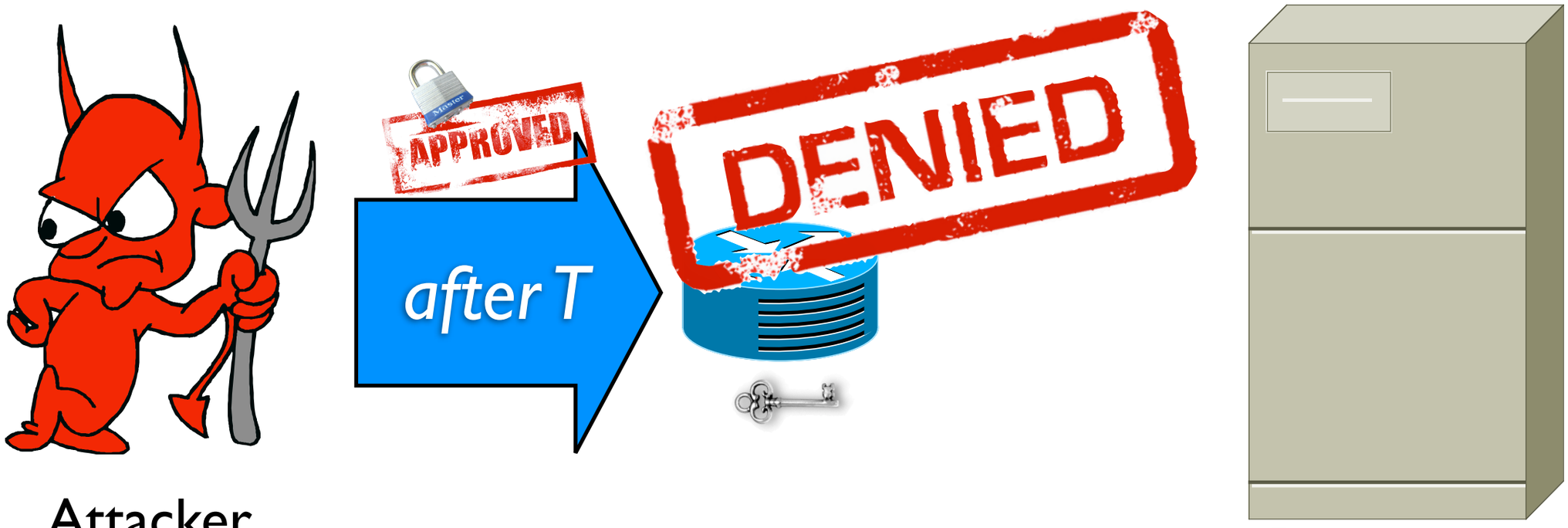
Capability (hosts)

the Amount of Data

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

Solution:

Limit the Amount of Data & Period of Validity

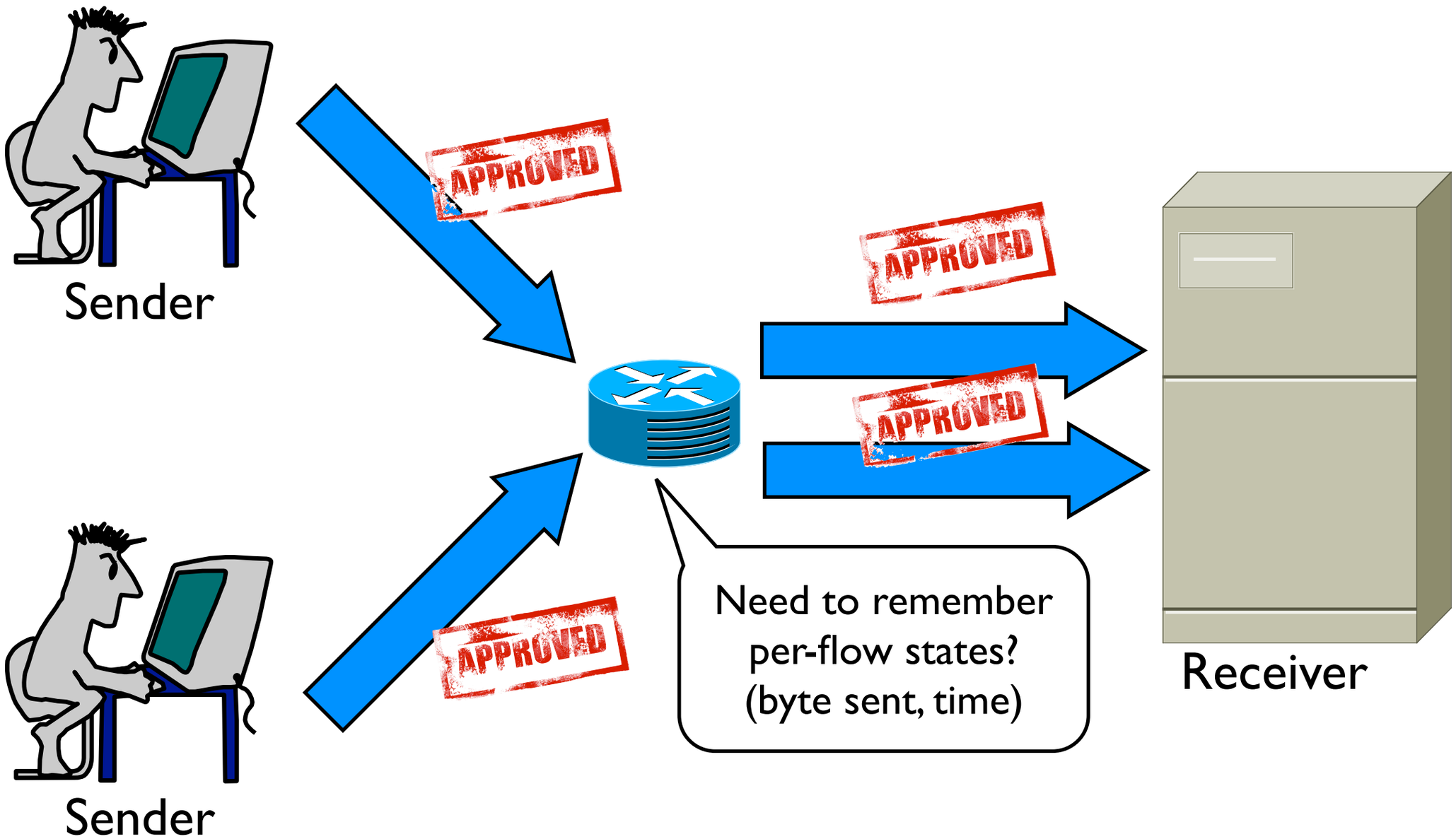


Capability (hosts)

timestamp (8 bits)	hash(pre–capability, N, T) (56 bits)

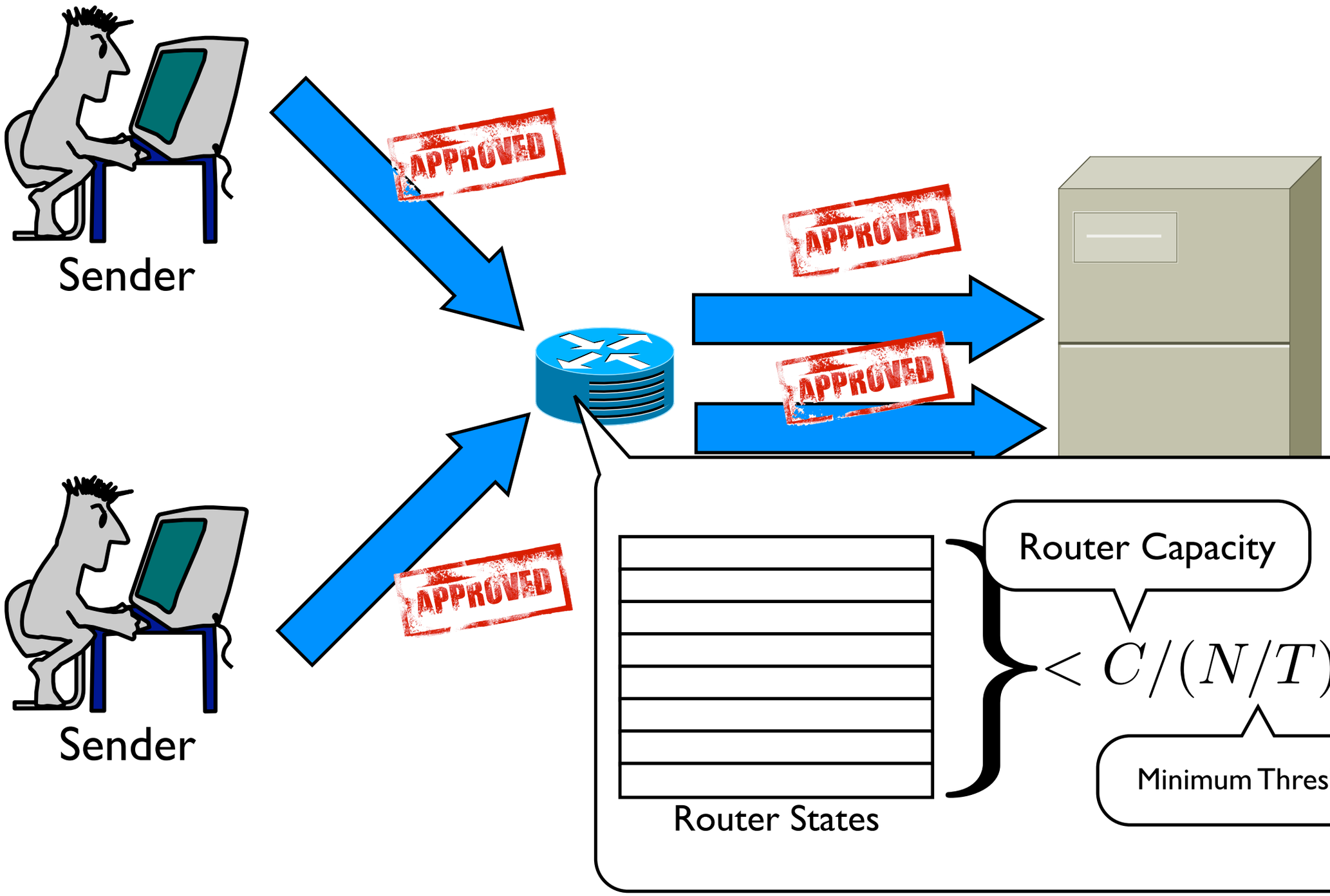
the Period of Validity

Challenge:
Router States



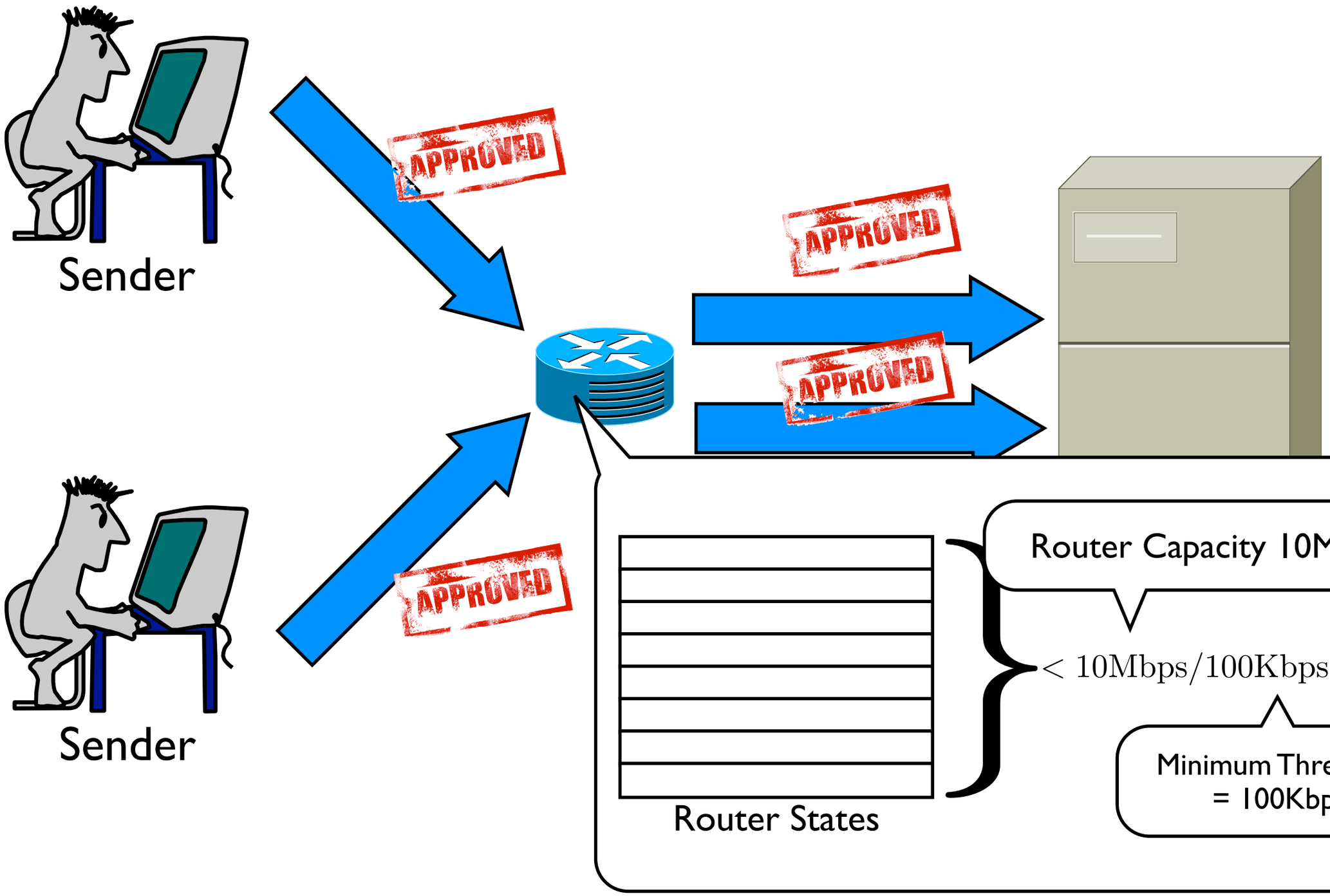
Solution:

Keep state only for flows that send >N/T

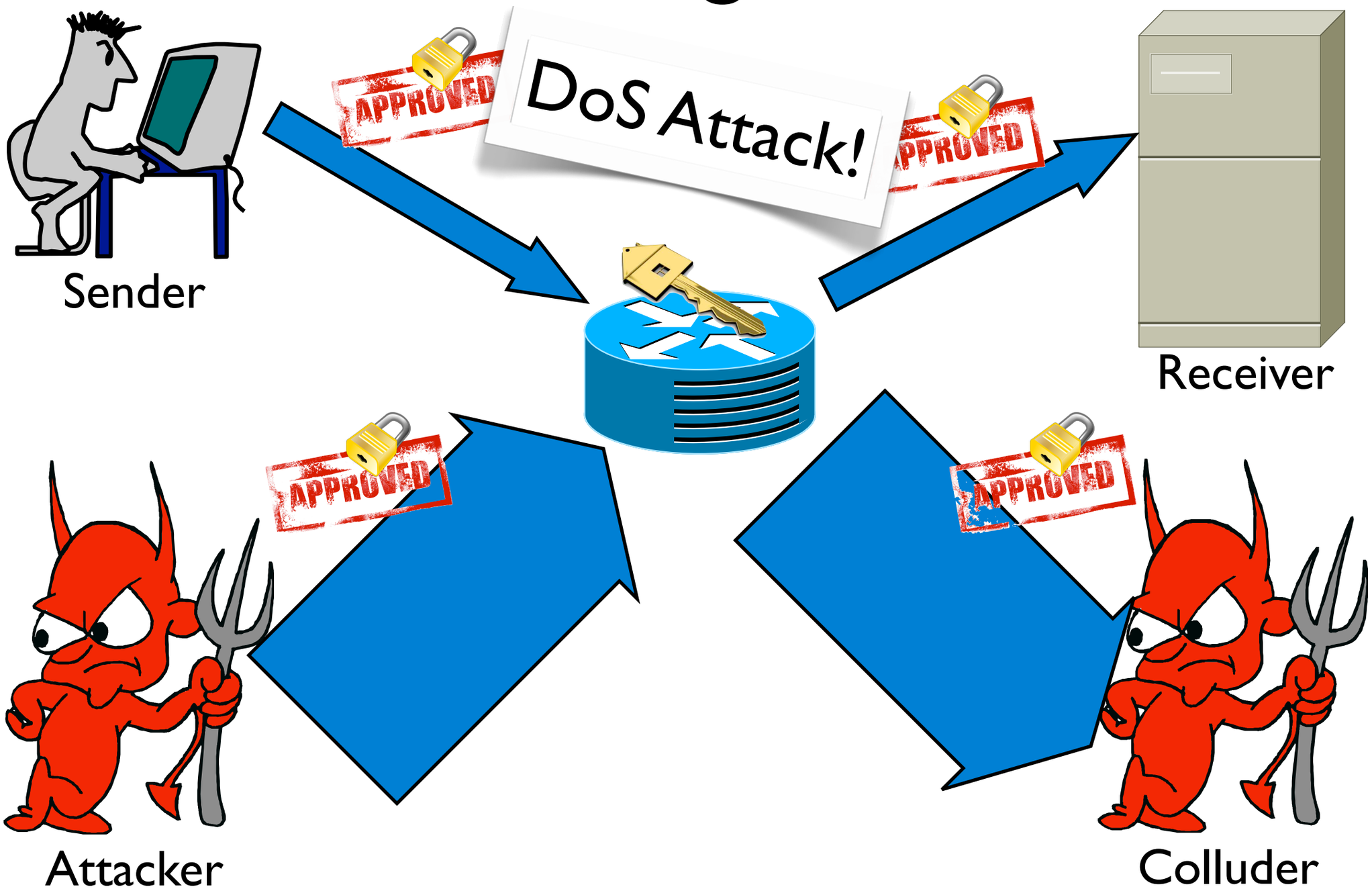


Solution:

Keep state only for flows that send >N/T

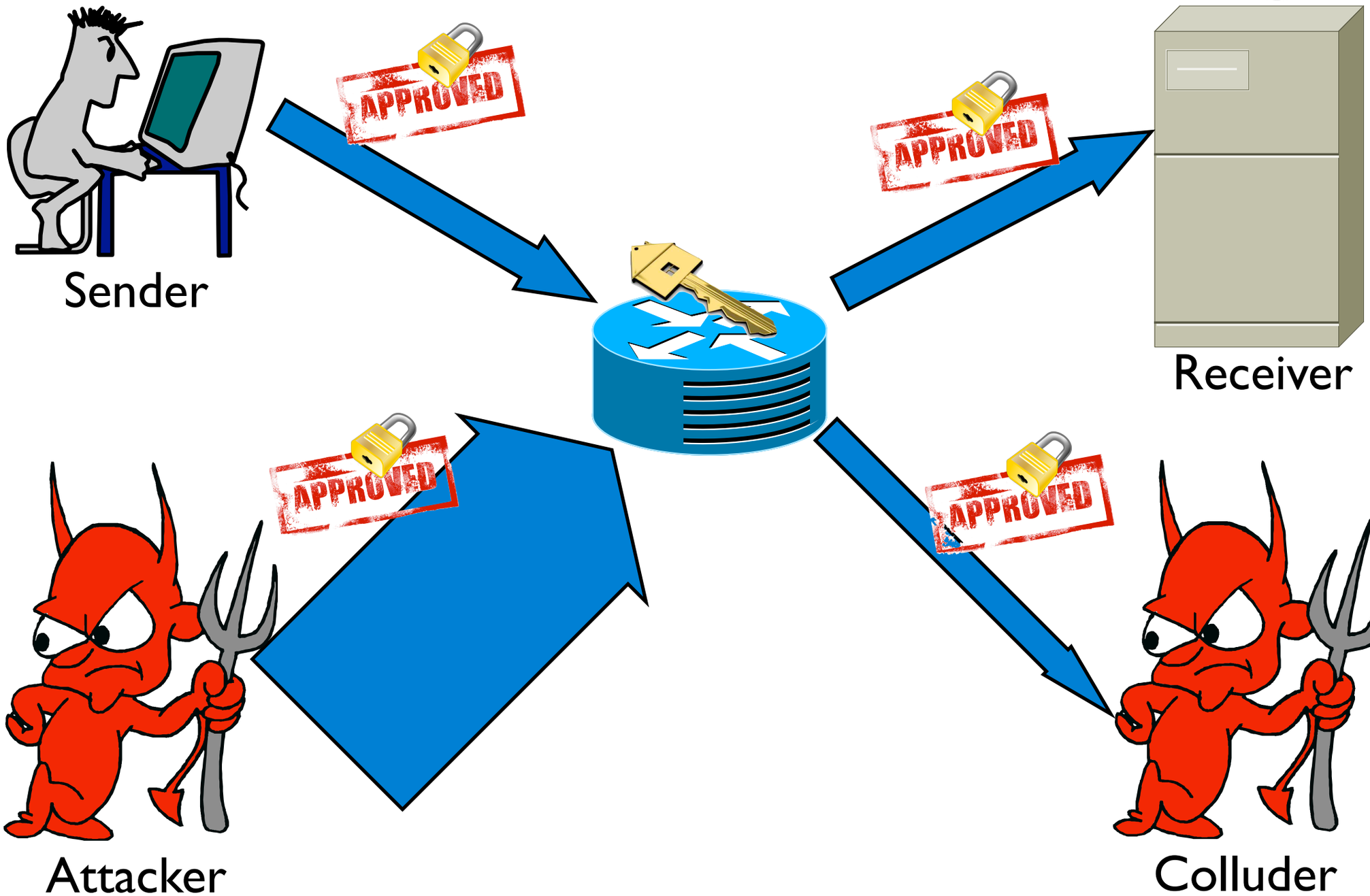


Challenge:
Colluding Attack



Solution:

Per-Destination Fair-Queuing



Summary:
Fair-Queuing of TVA Router

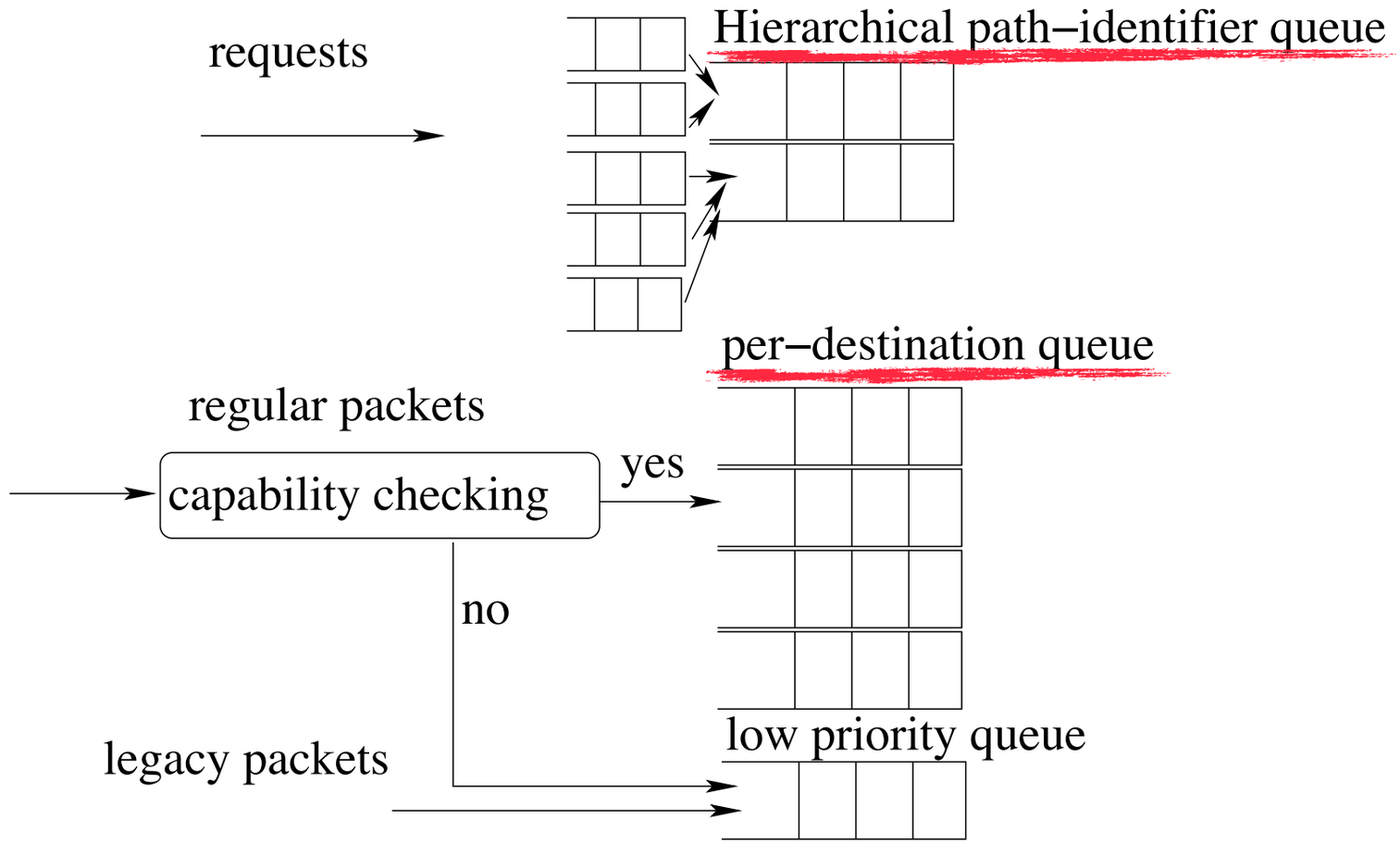


Fig. 2. **Queue management at a capability router. There are three types of traffic: requests that are rate-limited; regular packets with associated capabilities that receive preferential forwarding; and legacy traffic that competes for any remaining bandwidth.**

3

Discussions

Discussion

- Possible alternative End-to-End solutions?
- Incremental deployment issue when considering legacy internet traffic as low-priority?
- Work for DDoS attacks as well?
- Work well in the Internet-scale topology?