Trust in Networking

Mario Baldi

Politecnico di Torino

(Technical University of Turin)

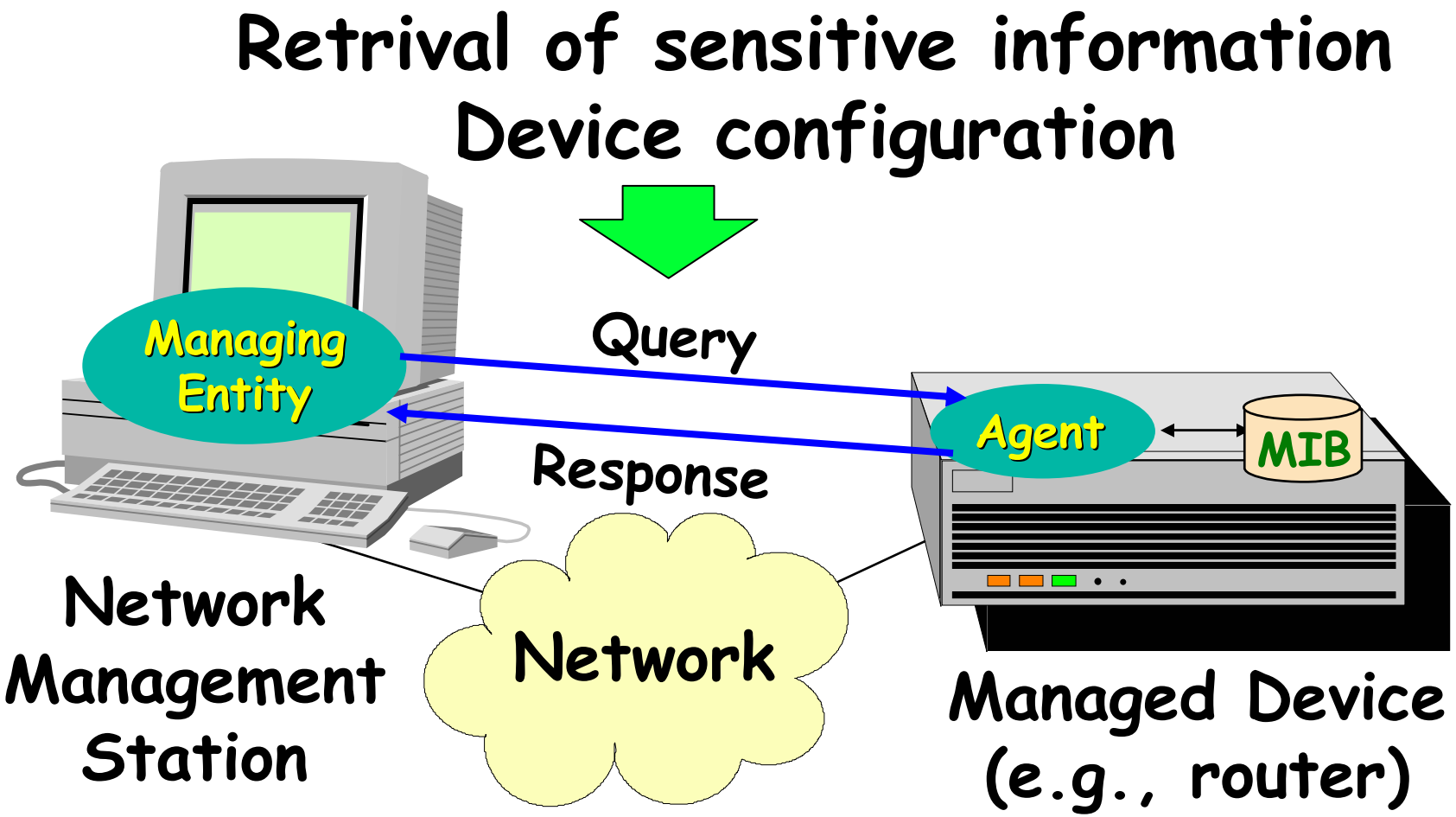
mario.baldi@polito.it

http://staff.polito.it/mario.baldi

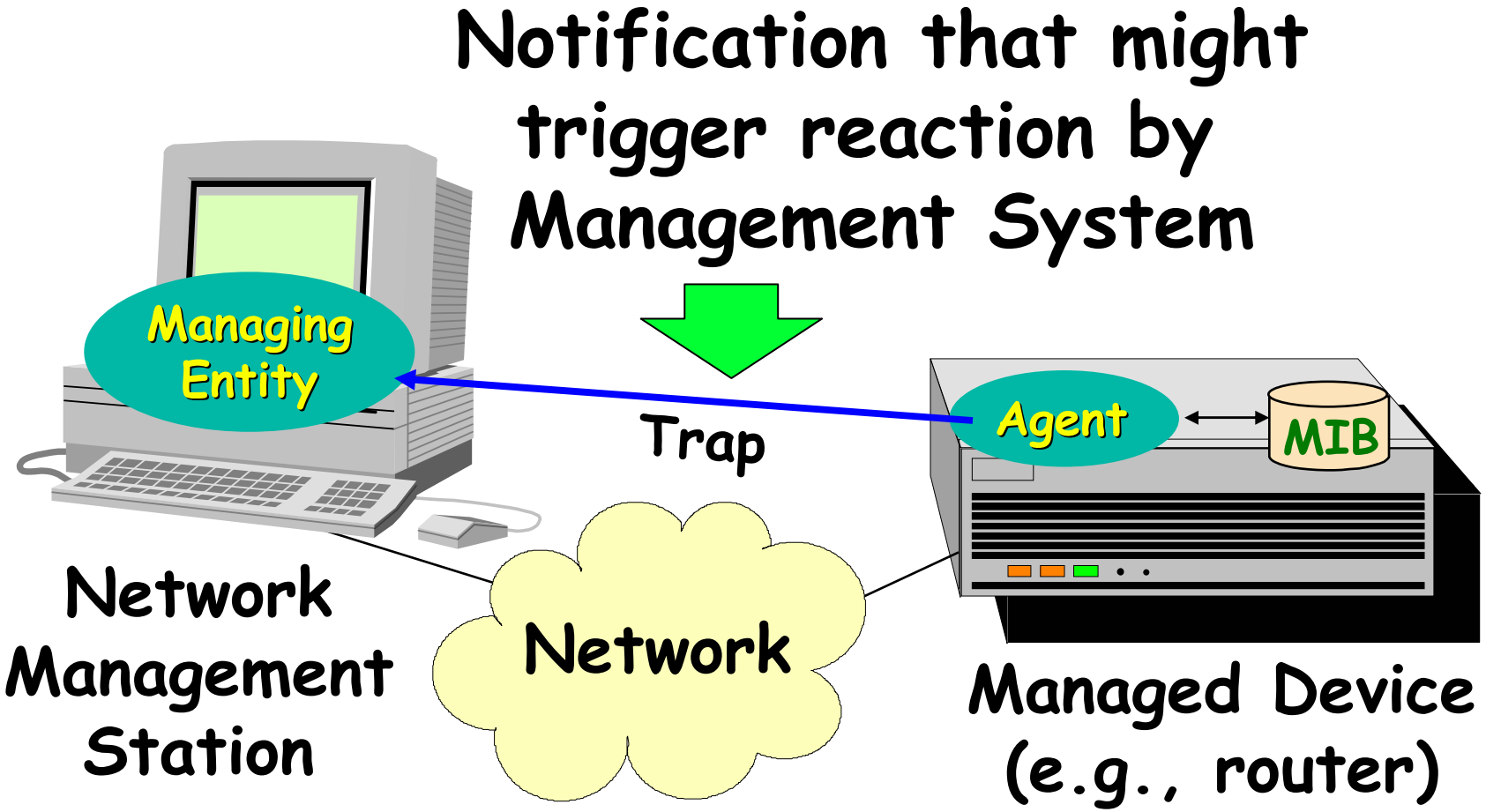
Where in Networking can Trust be Useful/Fundamental?

- Network management
- Virtual Private Network: VPN
- Access control (policing)
- TCP threat prevention
- Denial of service prevention
- Intrusion prevention
- Distributed Firewalling

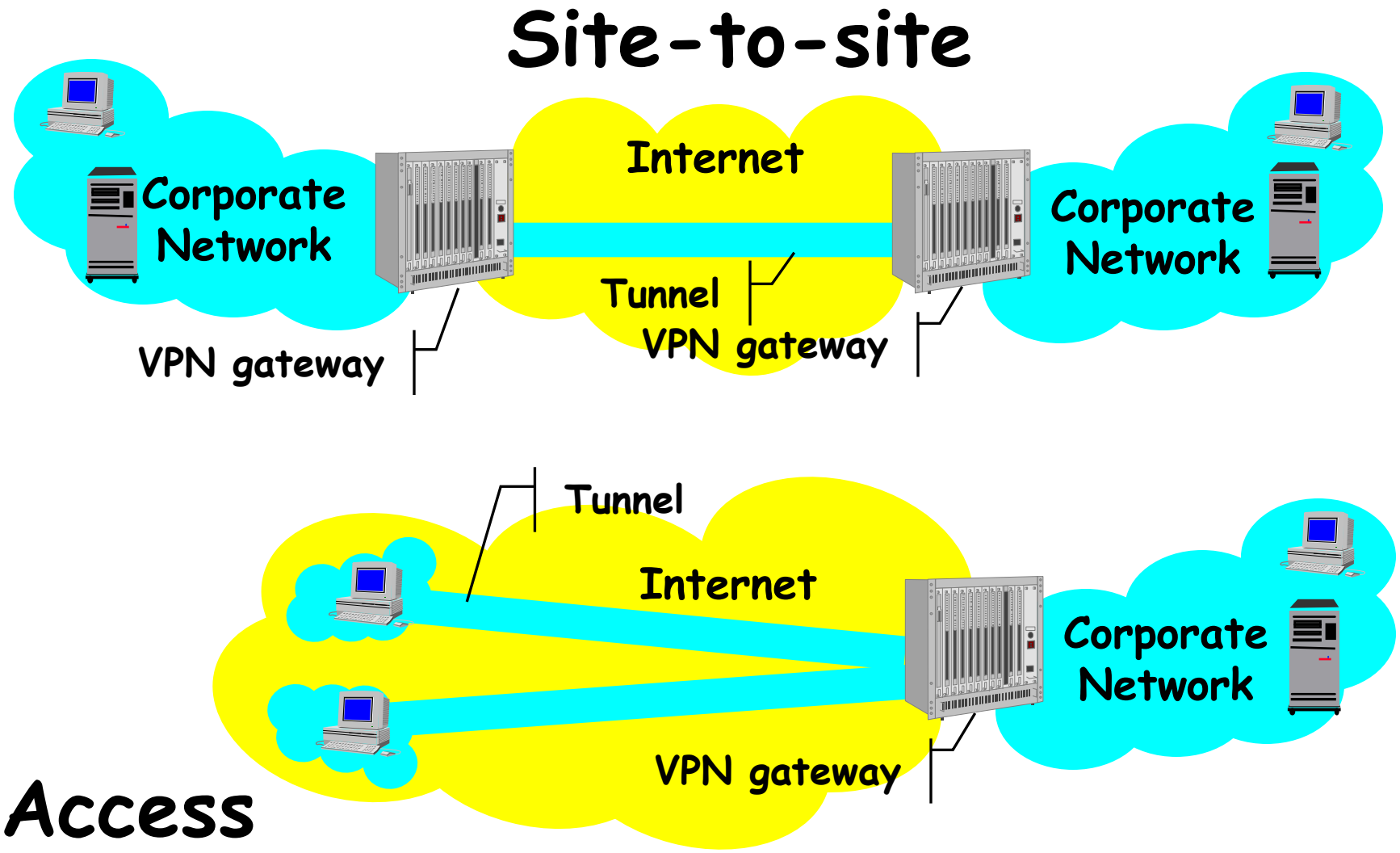
Network Management



Network Management



Virtual Private Network



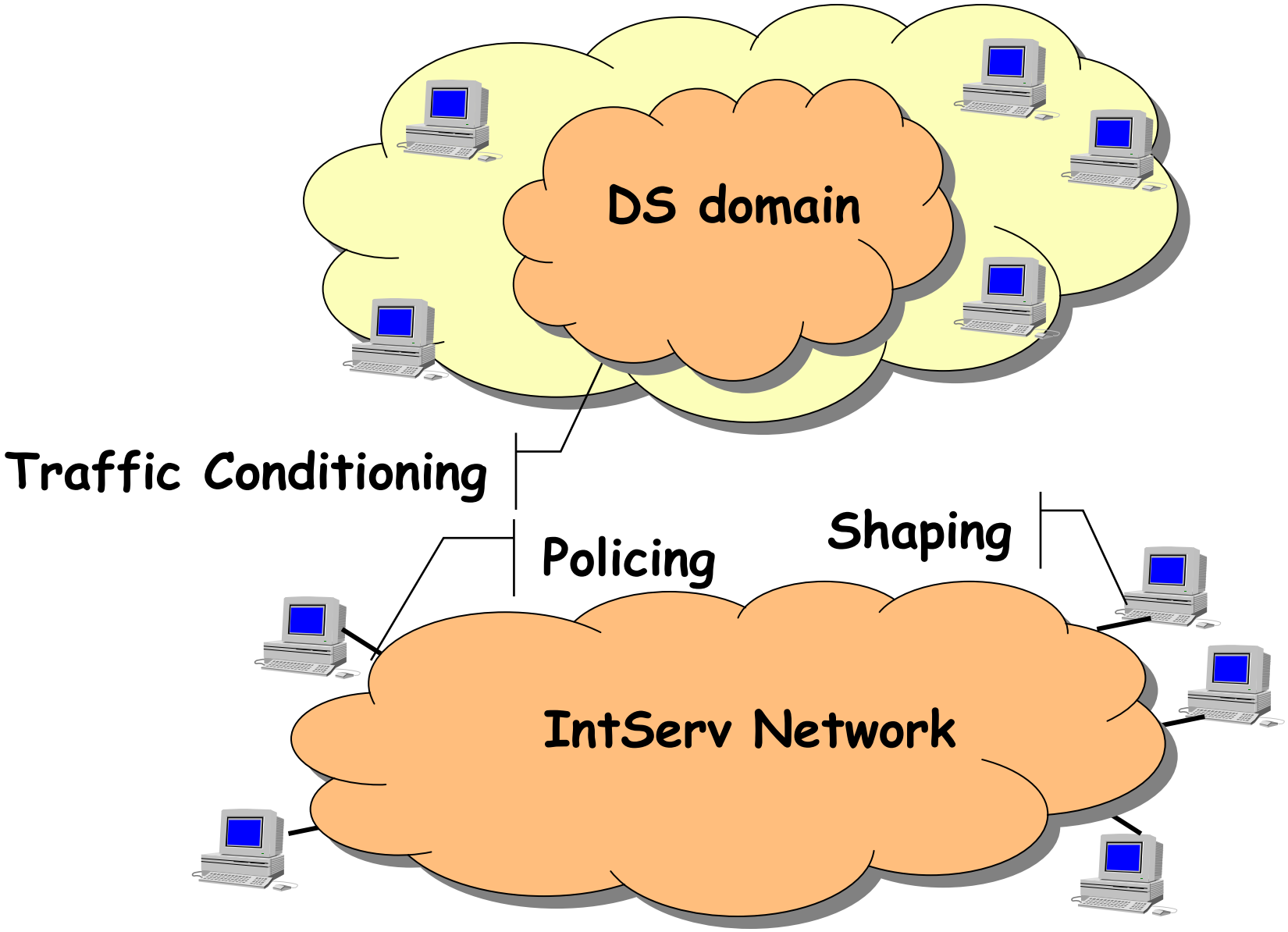
Existing solutions suffice (?)

- Authentication
- Encryption
- Cryptographic techniques
- Authentication services

Access Control

- Key to a better-than-best-effort service
- Guaranteed quality of service
  - Integrated Services (IntServ)
  - Shaper/Policer
- Classes of service
  - Differentiated Services (DiffServ)
  - Traffic conditioners

Current Solution

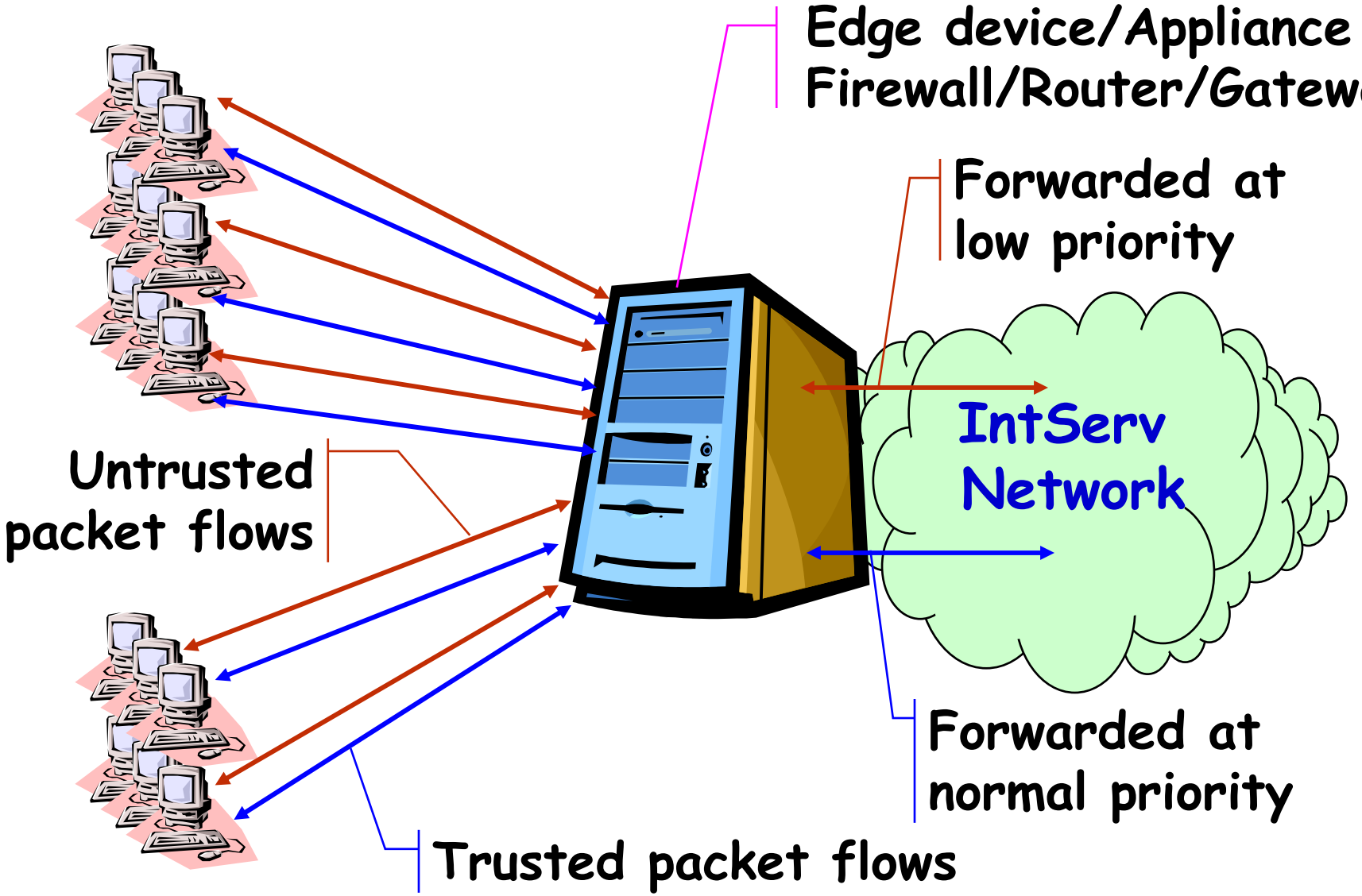


Problem

Edge device might have to support a large number of traffic conditioners policers

- One per flow with the IntServ model

Alternative Solution



Necessary Condition

Implementing trust must be simpler than current traffic conditioning and policing algorithms

- E.g., leaky bucket

TCP Error Control

- Go-back-N
  - If a packet is lost retransmit it together with all the subsequent ones
  - i.e., if the network is congested congest it even more
- In 1986 the Internet got completely stuck
  - Packets dropped due to congestion
  - Retransmissions maintain congestion

Introducing TCP Congestion Control

- Triggered by packet loss
- When there is congestion transmit less
  - Resize transmission window
- Increase transmission gradually
  - Slow start
- Avoid congestion

Everyone must do the same!

Where is the threat?

Global distributed

denial of service

Recreating the 1986 preconditions

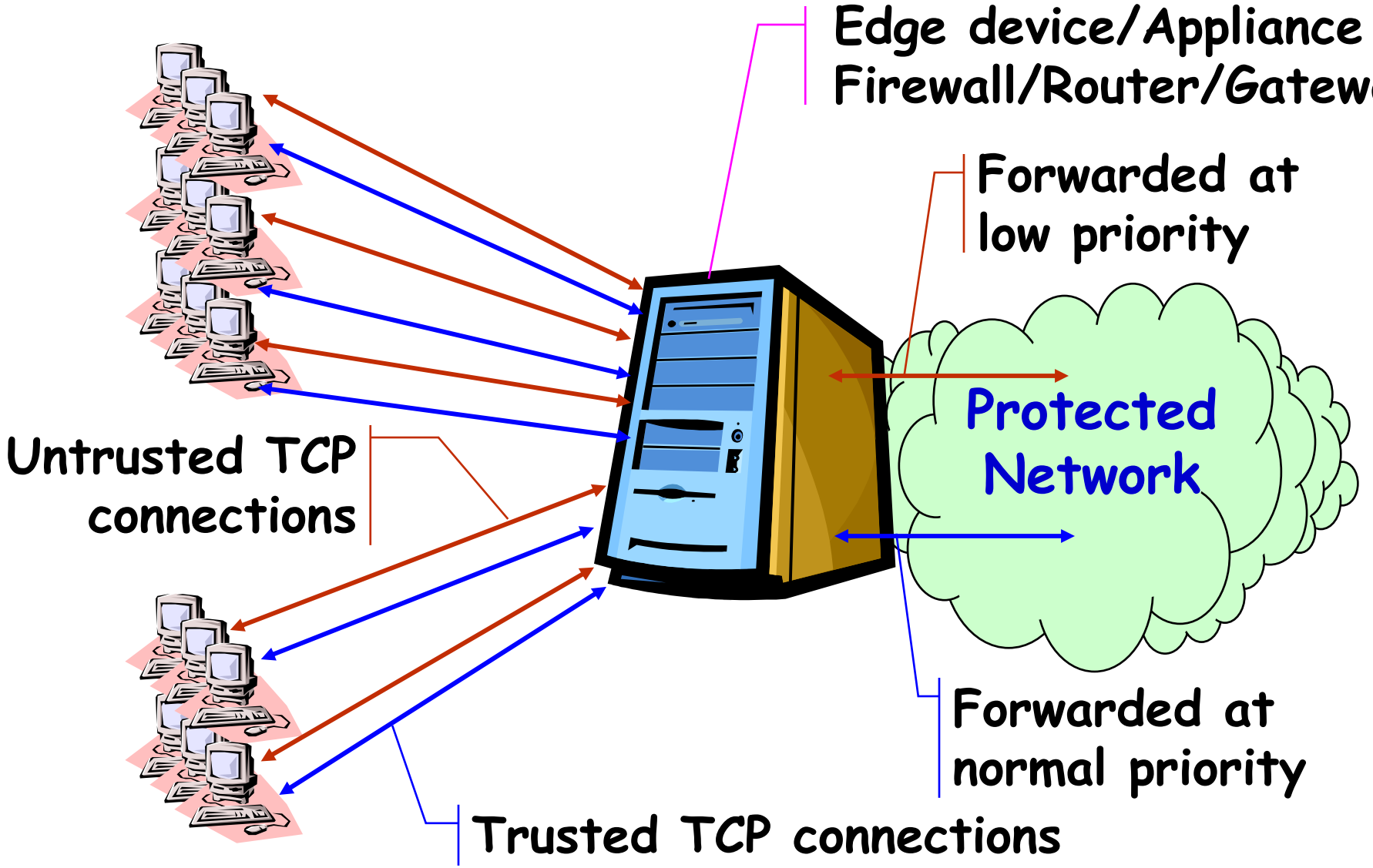
How?

Click here
to download

Boost your data transfers!

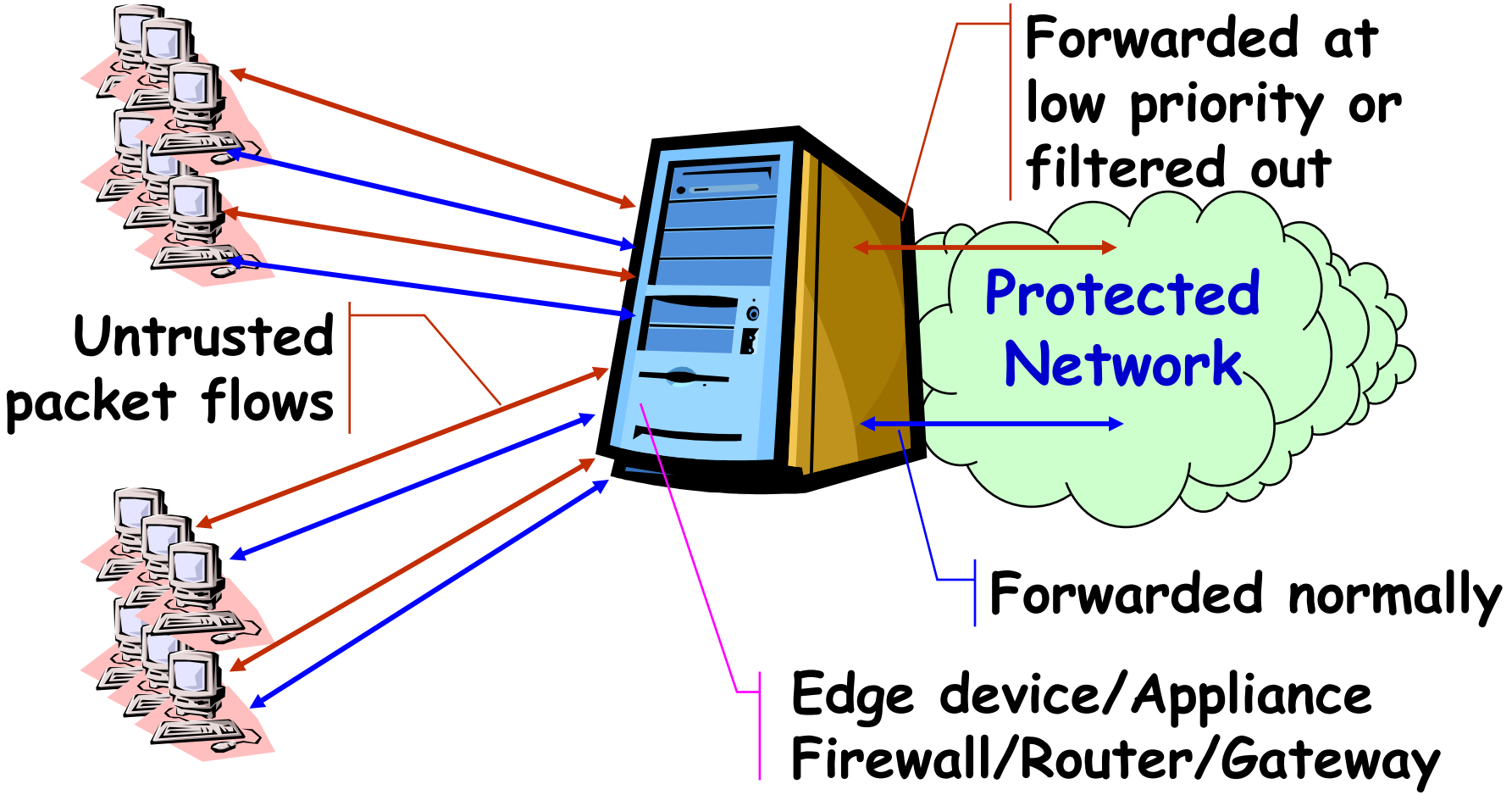
Try it for free

Architecture



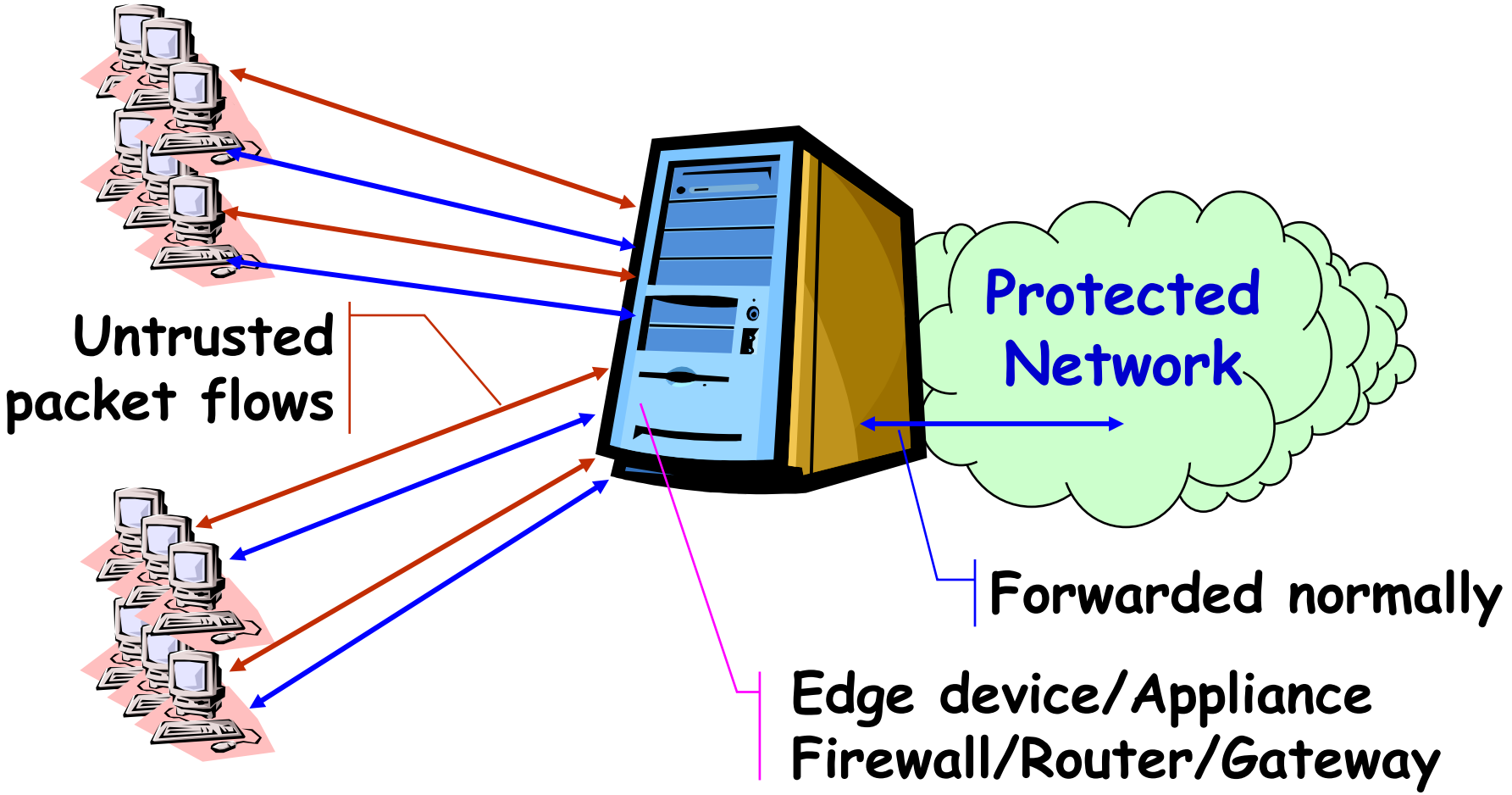
Denial of Service Prevention

Traffic generated by malicious software (untrusted) is segregated



Intrusion Prevention

Traffic generated by malicious software (untrusted) is filtered out



Distributed Firewalling

Firewall function is distributed across end-systems