

# De-perimeterization of Networks

Tomas Olovsson, CTO



# AppGate Company Introduction

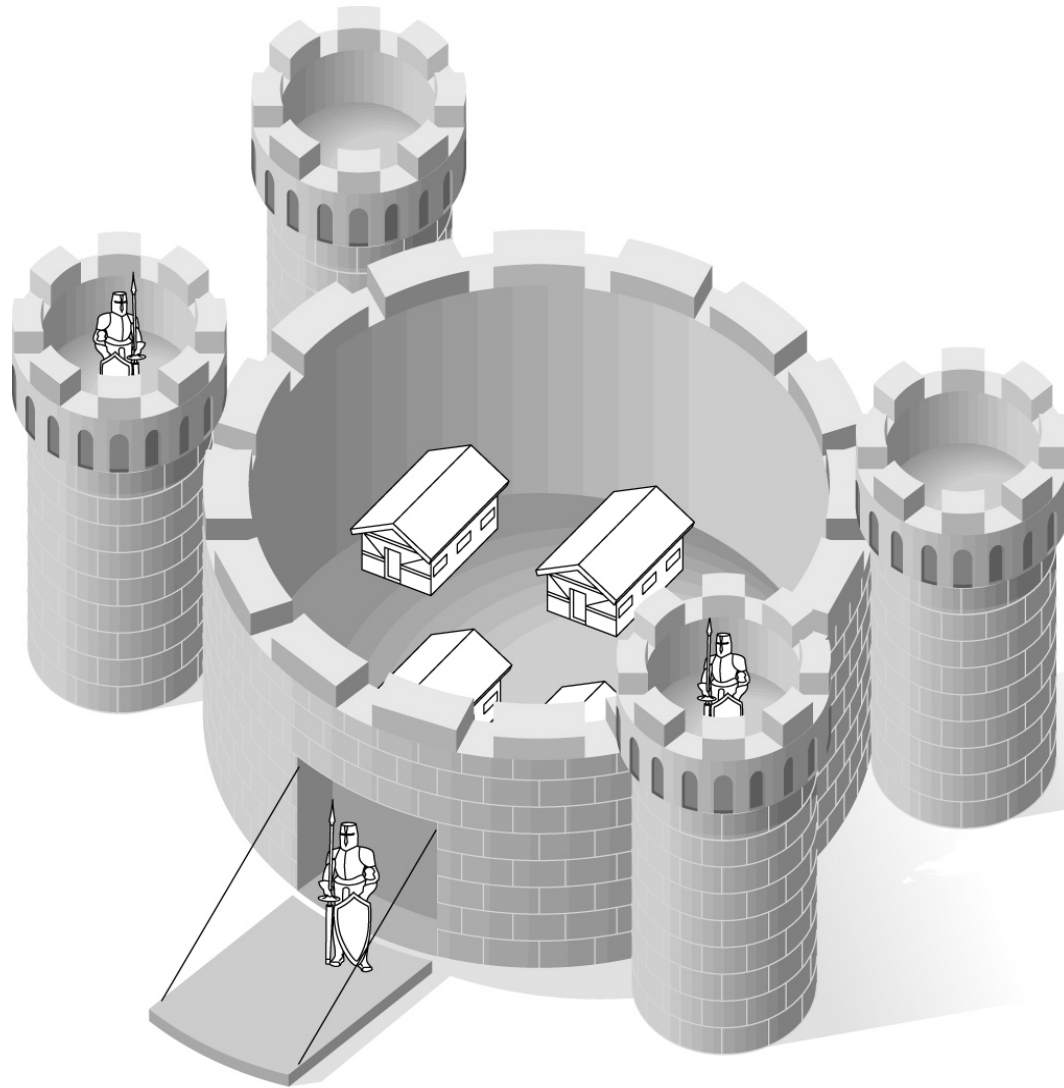
- AppGate is a Swedish company with sales and support offices in the U.K and the U.S.
- AppGate support customers worldwide
- AppGate's first installation was made in 1997 in the defense industry
- AppGate has customers in all verticals, all with one thing in common: the need to give access to resources in a secure way
- AppGate has been recognized for its leadership in technology and support many times over the years
- AppGate has shown a stable growth since 1997

# Example of customer types

- Defence
- Defence industry
- Government organizations
- Banking
- Pharmaceutical
- Hospitals, healthcare
- Telecommunications
- Aerospace and avionics
- *Most customers are large corporations and organisations*

# The current network architecture

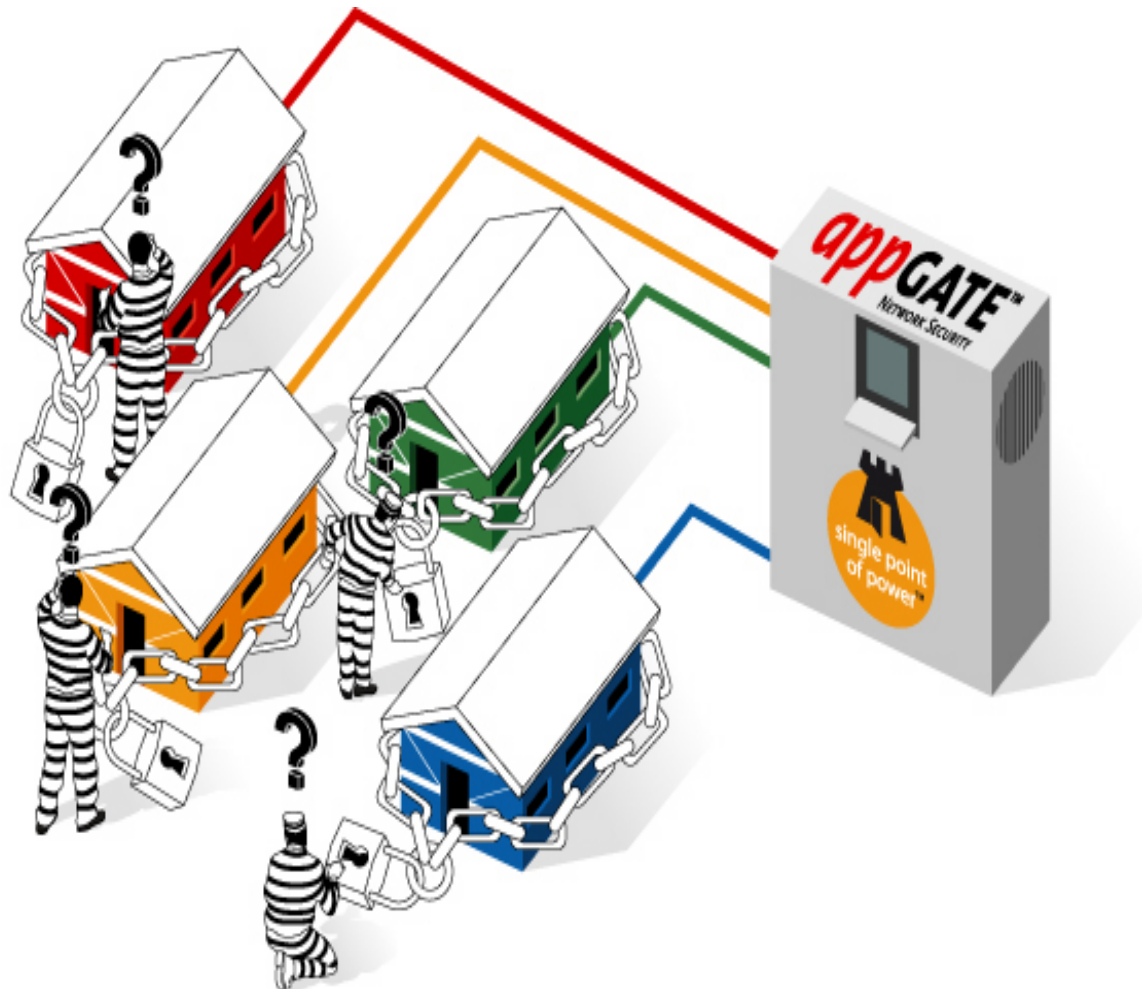
# A false sense of security



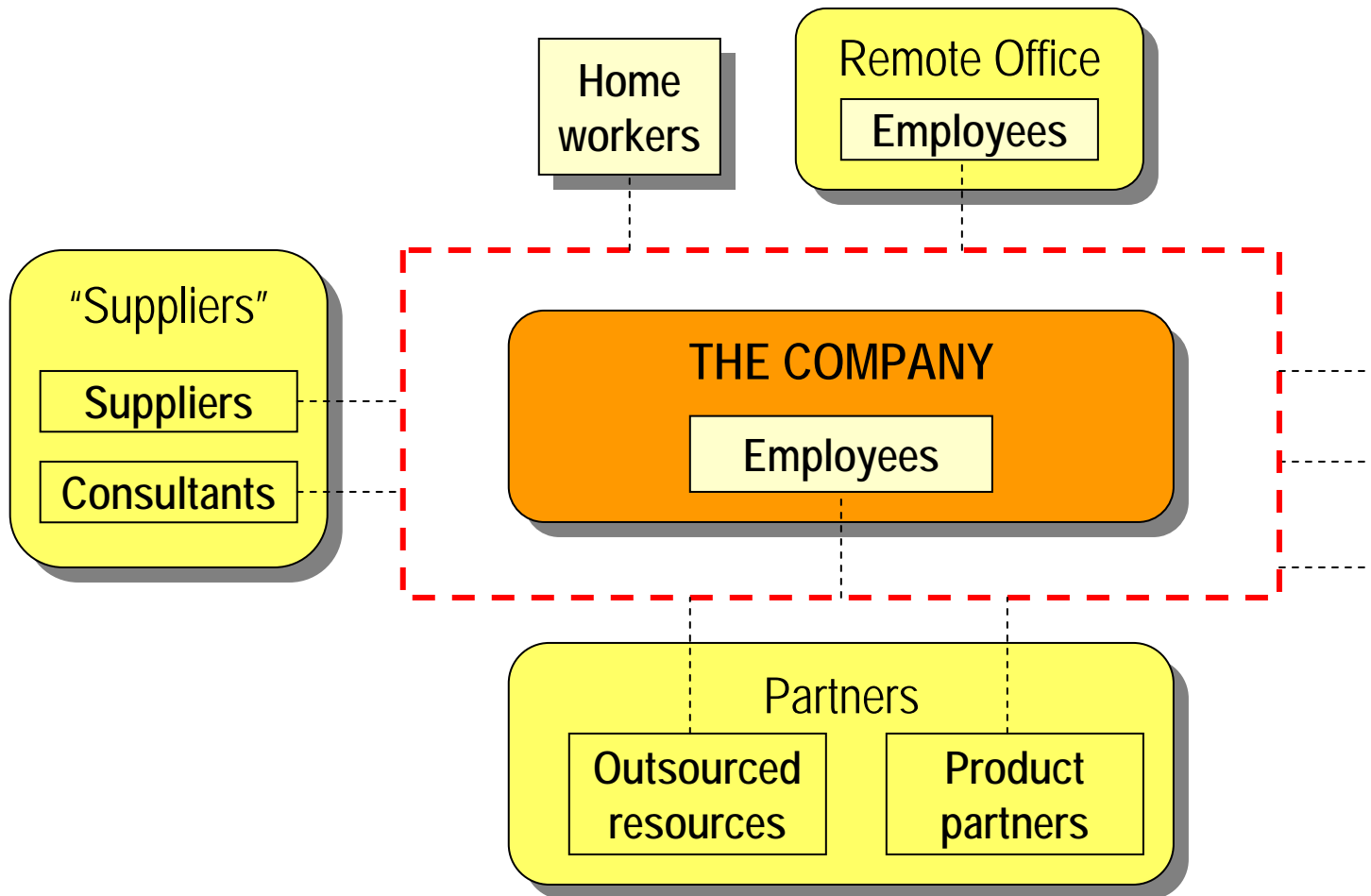
# Reality is different



# Information needs to be protected at the source and access managed centrally

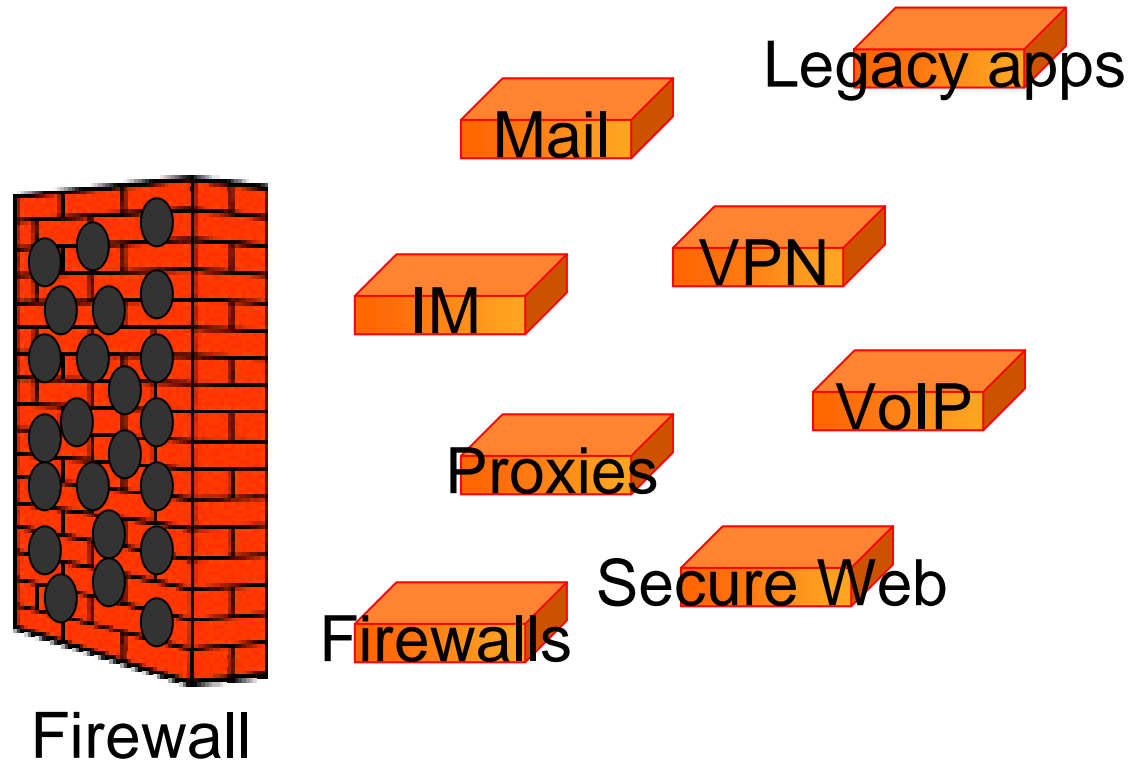


# We can no longer hide behind a wall

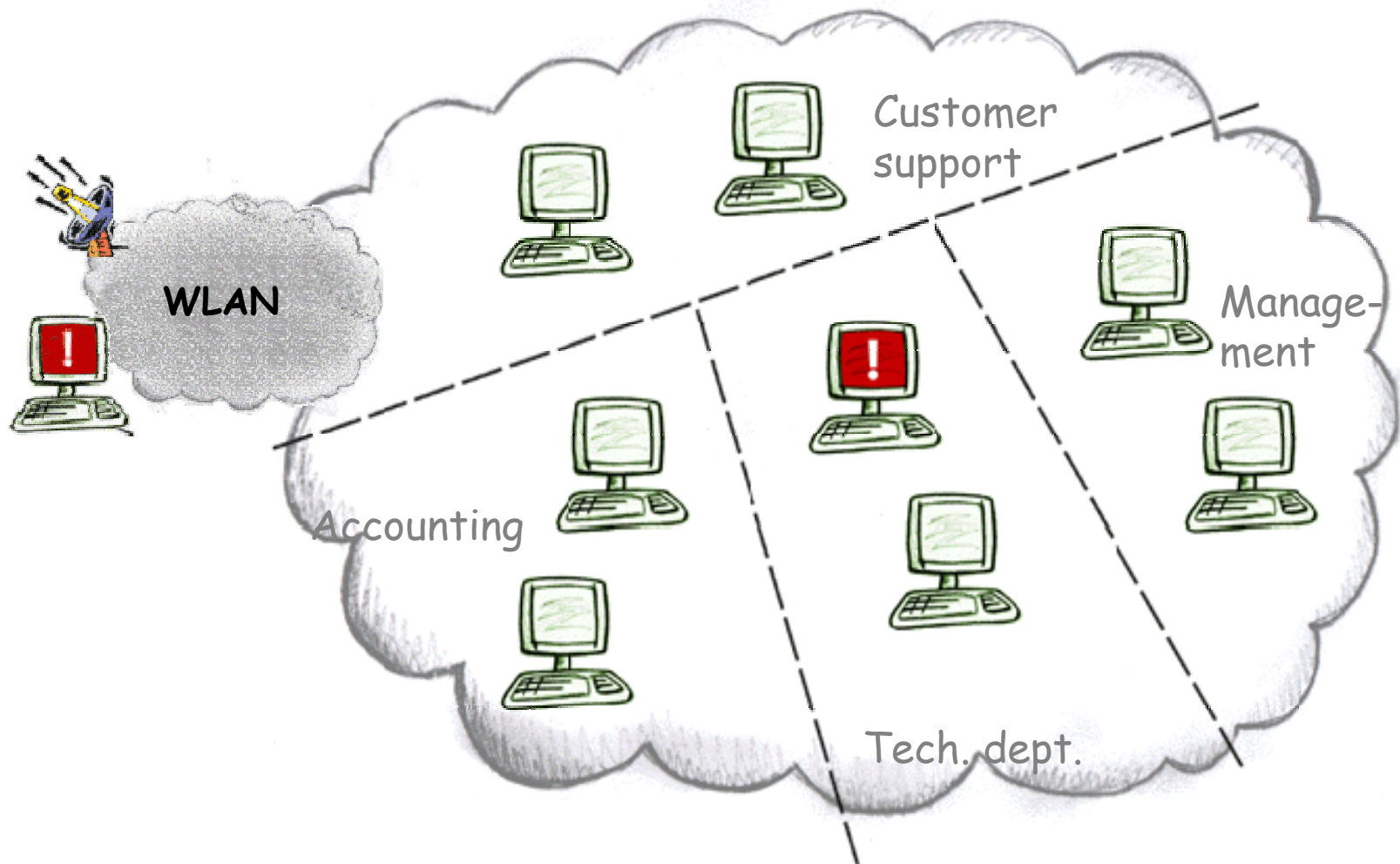




# The Firewall-centric view...



# Another observation: Large networks must be partitioned



# The de-perimeterization approach

# Jericho Forum

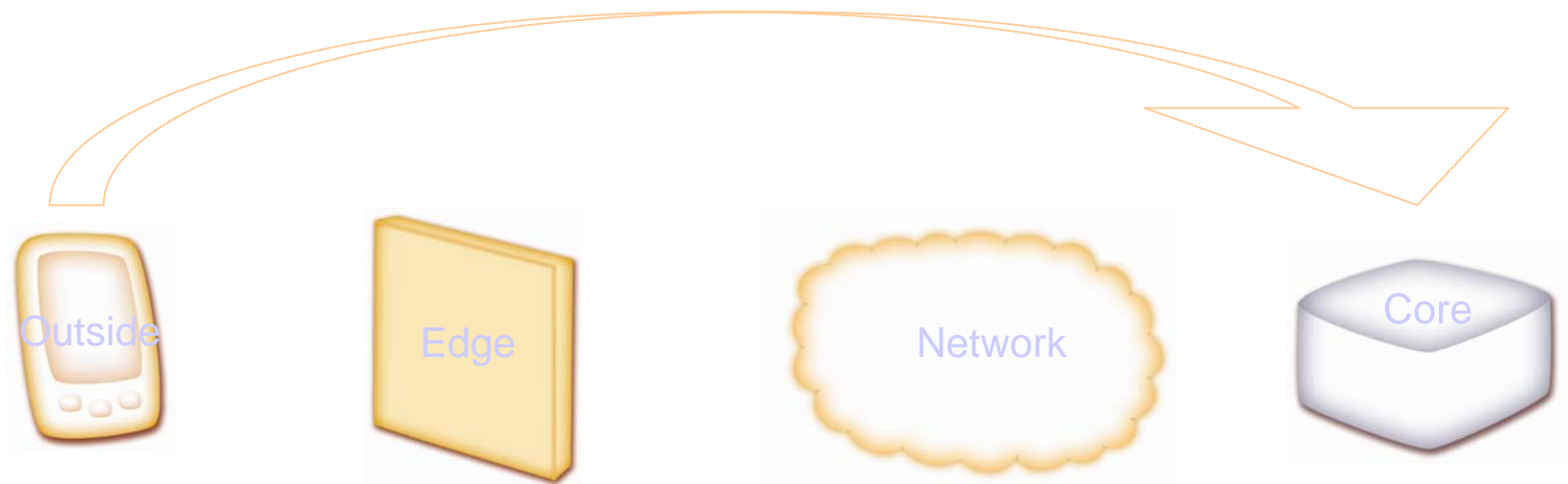
- The Jericho Forum is an international forum of IT customer and vendor organizations: [www.opengroup.org/jericho](http://www.opengroup.org/jericho)
- Made up of security officers within corporations like the Royal Mail, Standard Chartered Bank and the BBC.
- **“Perimeter security has become obsolete”**
- **“The old hard-shell model of security isn't sustainable** in light of the need for businesses to open up their networks to partners, consultants and clients”
- **Deperimeterization doesn't mean discarding the firewall.**



# Is this a problem?

- Secure and boundaryless information flows across organisations...

...Simple then; we just want to connect a specific user to the app server securely....**so why should this be so difficult?**



# It is really simple, if...

- Each application server is able to protect itself
- And each client system can protect itself
- Central authentication system(s) for all users exist
  - In reality, delegation is needed
  - But applications should not have to deal with authentication
- A distributed authorisation system exists
  - E.g. project leaders can decide who can do what
  - Applications should only deal with user roles, not with assigning users to roles
  - A user role may depend on authorisation method, end point device, time of day, location, etc.
- Applications only visible to authorised users
  - Type of service must depend on users role
  - Some services may require encrypted communication
- Then:
  - No central firewall would be needed (in reality, we would probably still keep it)
  - No difference between local access and remote access
  - It may not even be necessary to define what is the home/internal network!

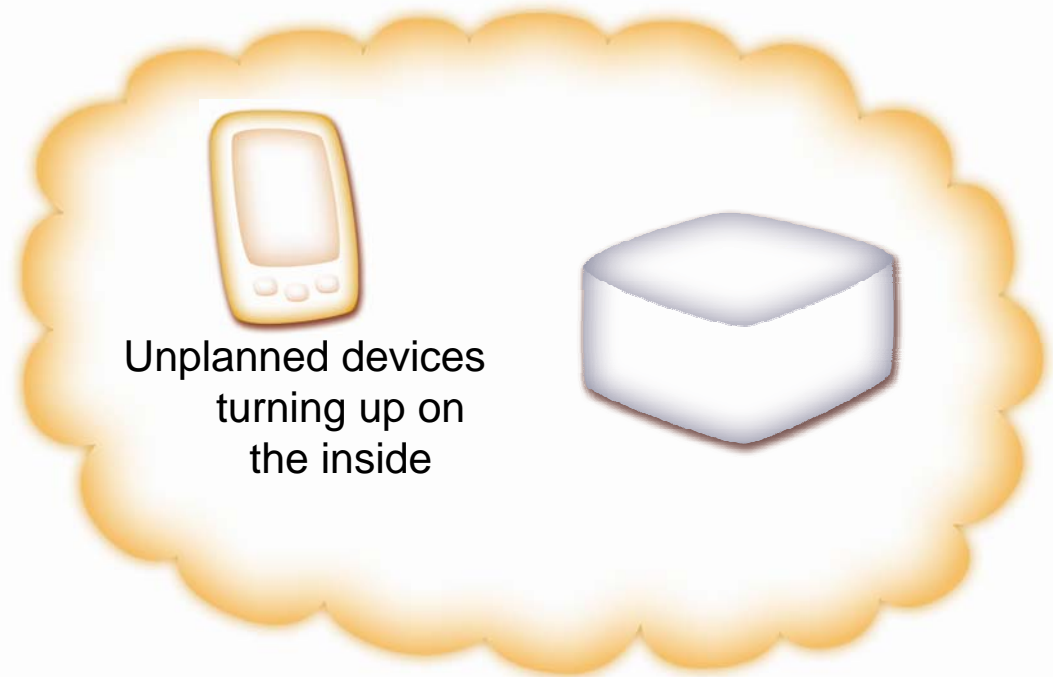
# Physical Boundaries

So the network model needs to evolve...

...and having security control just the physical boundary *is being slowly eroded away...*



Unknown, un-trusted  
devices coming in  
from the outside



# Examples

- Cisco
  - Laptops all have full admin rights and are not locked down. They rely on end point security tools like PFW, IPS, AV, etc AND on personal responsibility.
  
- BP
  - Have ejected 18,000 of their laptops from the network. Even if they come into the office they are only have internet access.
  
- AppGate
  - Laptops are privately owned and run Windows, open BSD, Linux and Mac OSx. When non-office based staff come into the office they only have Internet access.





An architecture for the future

# 1 - End-Points



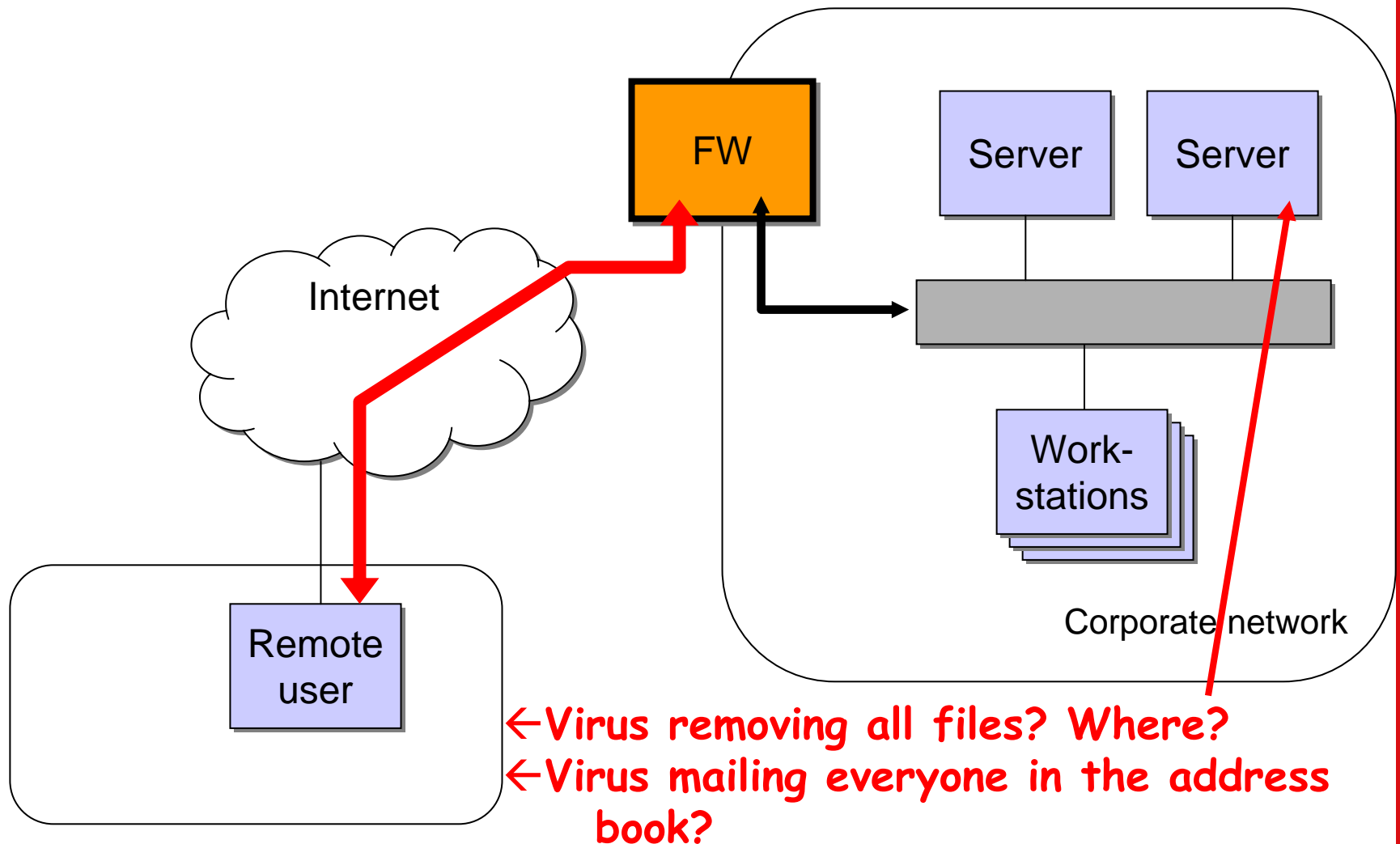
# Multiple Platforms



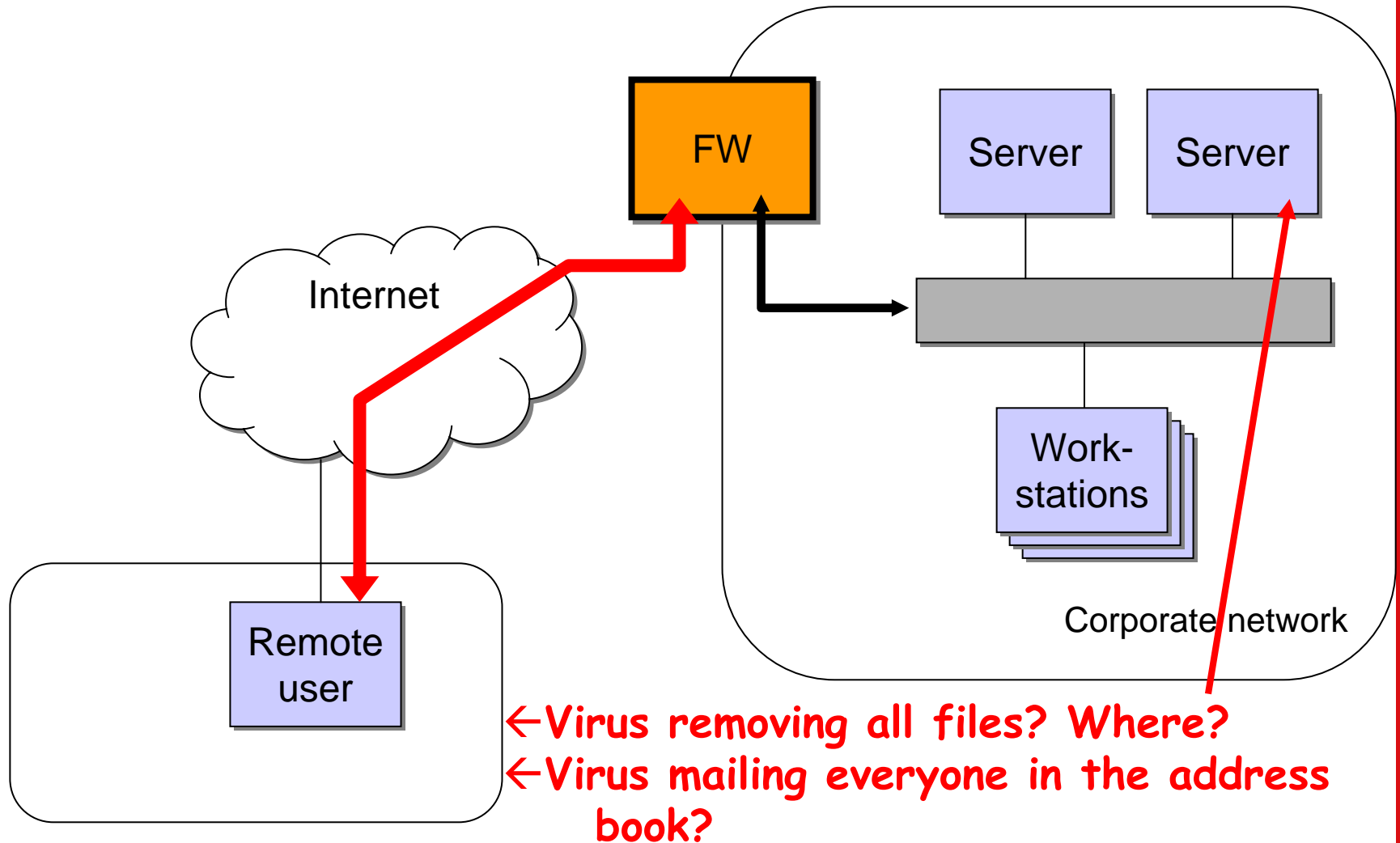
The AppGate solution supports numerous different operating systems making it possible to support most end-point types.



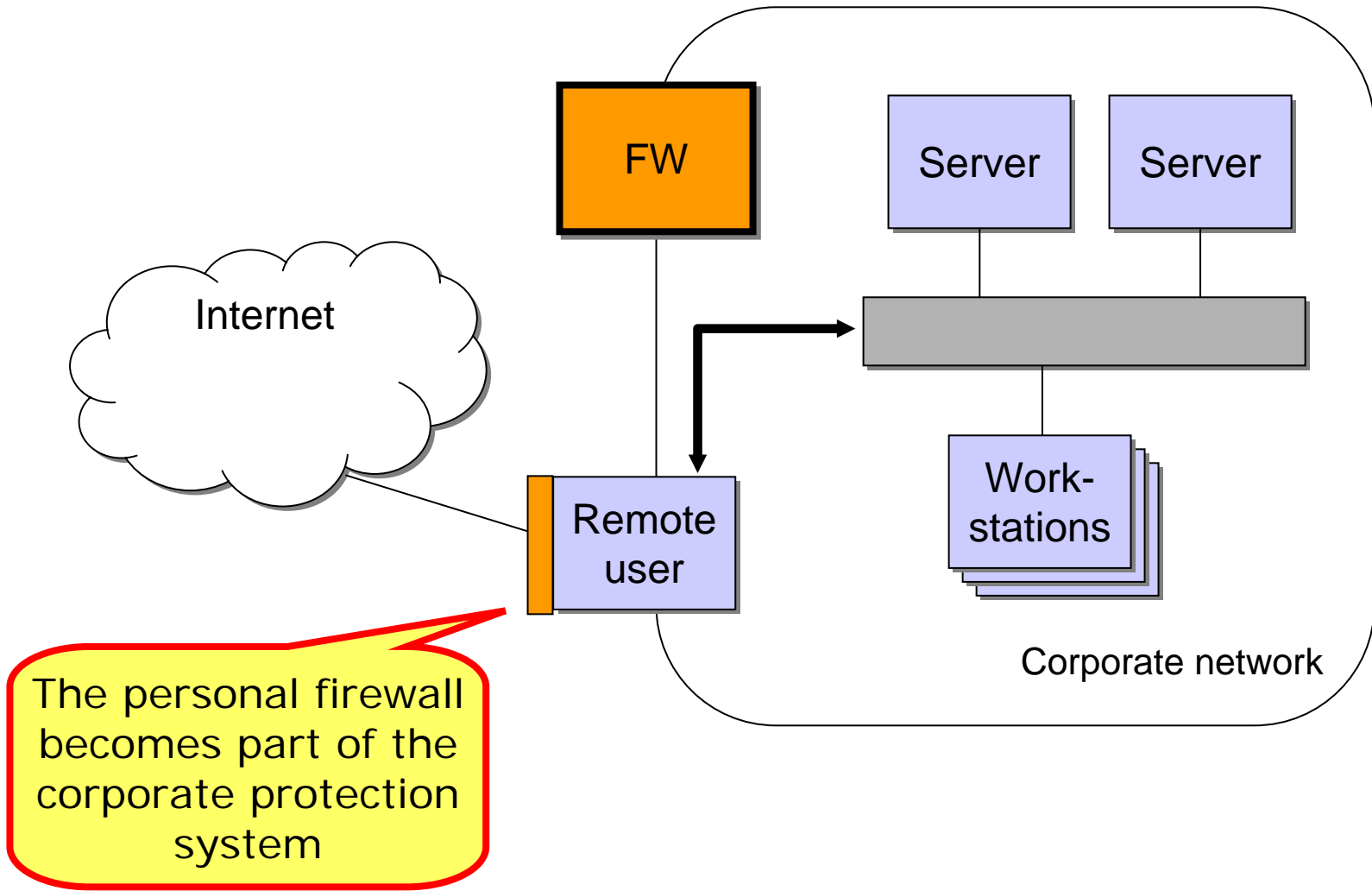
# Remote connections can be a problem



# Remote connections can be a problem



# This is the same picture



# Personal Firewall



- It is important that each client system can protect itself
  - Firewall functionality is required
  
- The AppGate solution includes an enterprise PFW
  - Acts as an extension of the 'network firewall'.
  - Users cannot change any of the rule sets.
  - Works in conjunction with other firewalls.
  - The Firewall can have different rule sets depending on location:
    - Remote ,connected to the Internet
    - Remote, connected to the office through a VPN
    - Office

# Client Check



The AppGate system can perform checks to verify/improve the security of the end-point device.

- Checks standard parameters – i.e. OS, IP address, AG client, etc
  - Checks files/dates/versions
  - Checks processes
  - Checks registry
  - Checks system info
- 
- Checks can be a user written .bat, .exe, etc
  - All checks are done by OS and OS version

**check.exe**



# Client Command

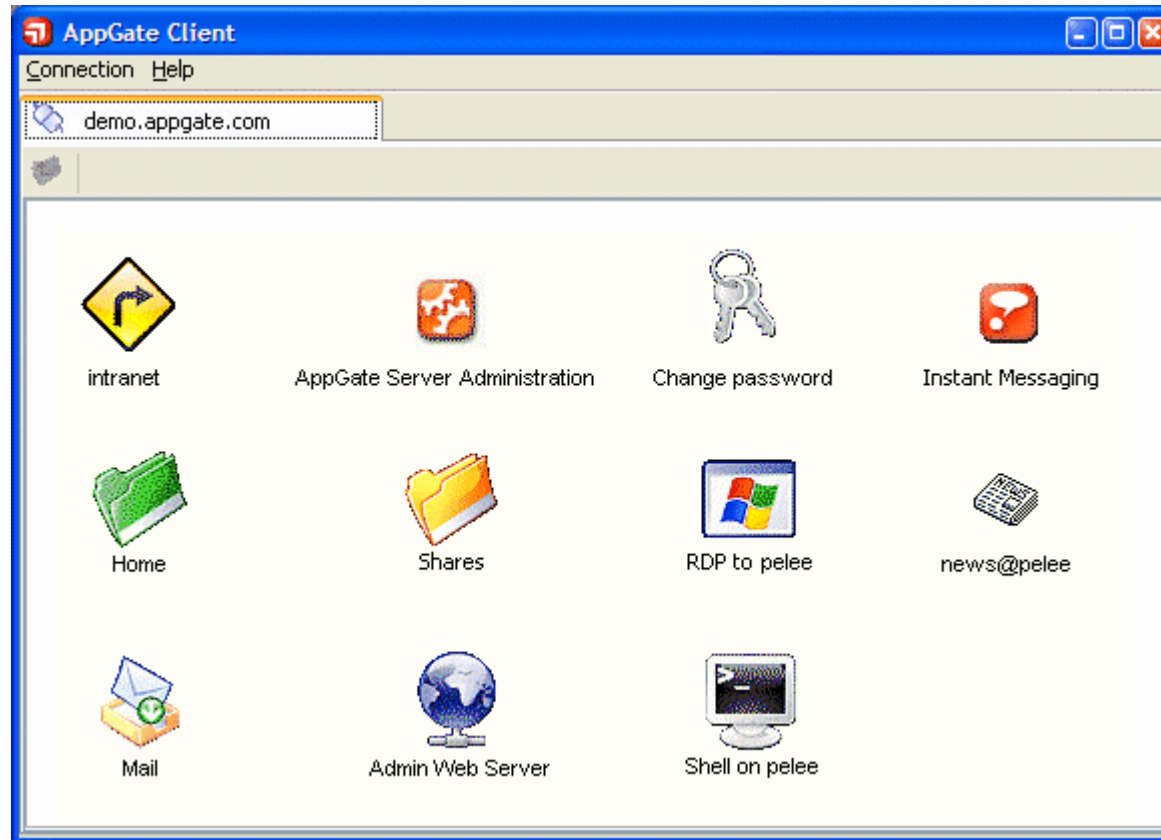


The AppGate solution can force the end-point to perform tasks that improve both the usability and security.

- Upload executables
- Start programmes/executables
- Configuration of the end-point
- Cleaning the cache

**agexec.exe**

# Users can see all services available from the system

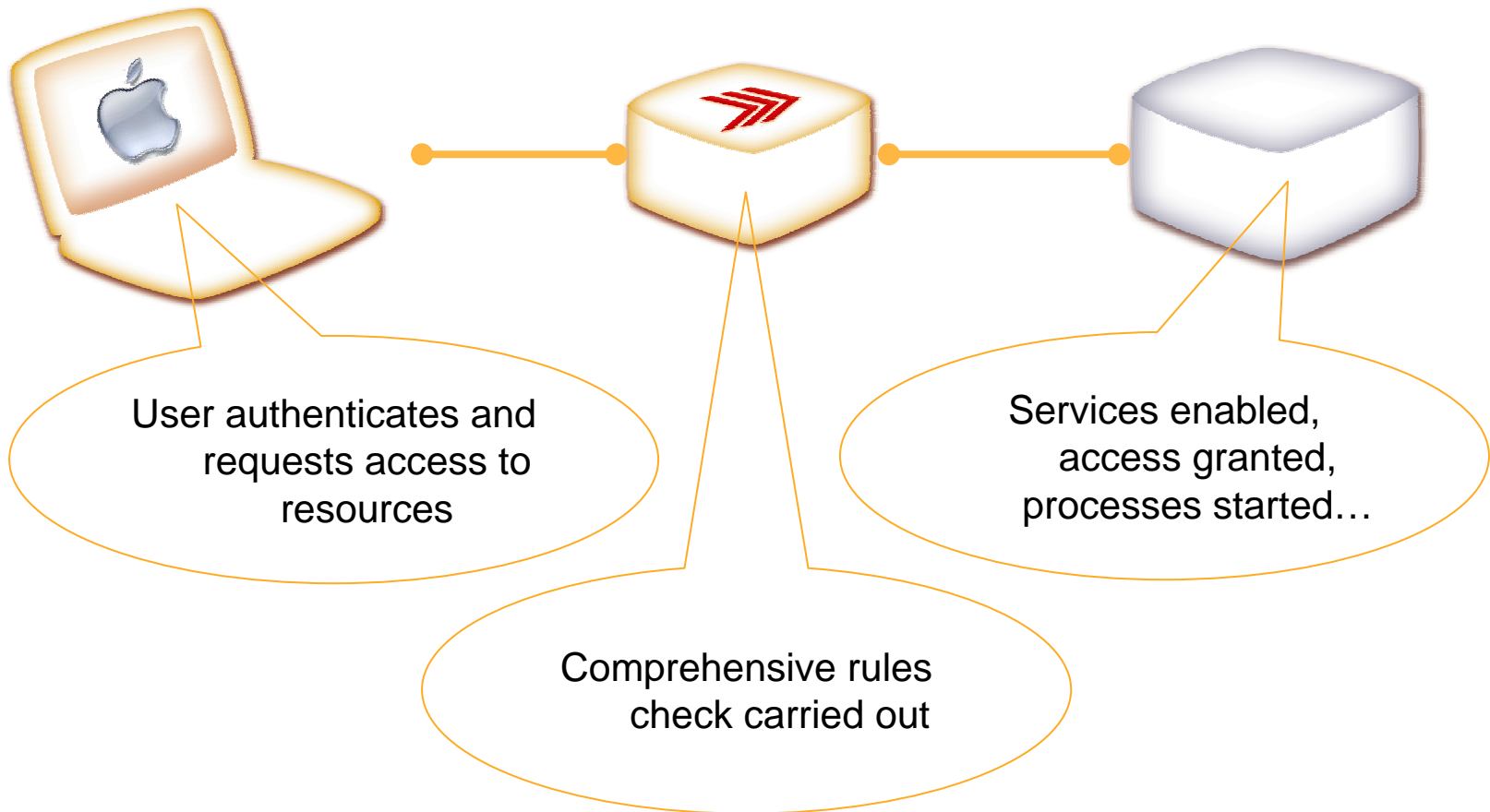


## 2a - Networks

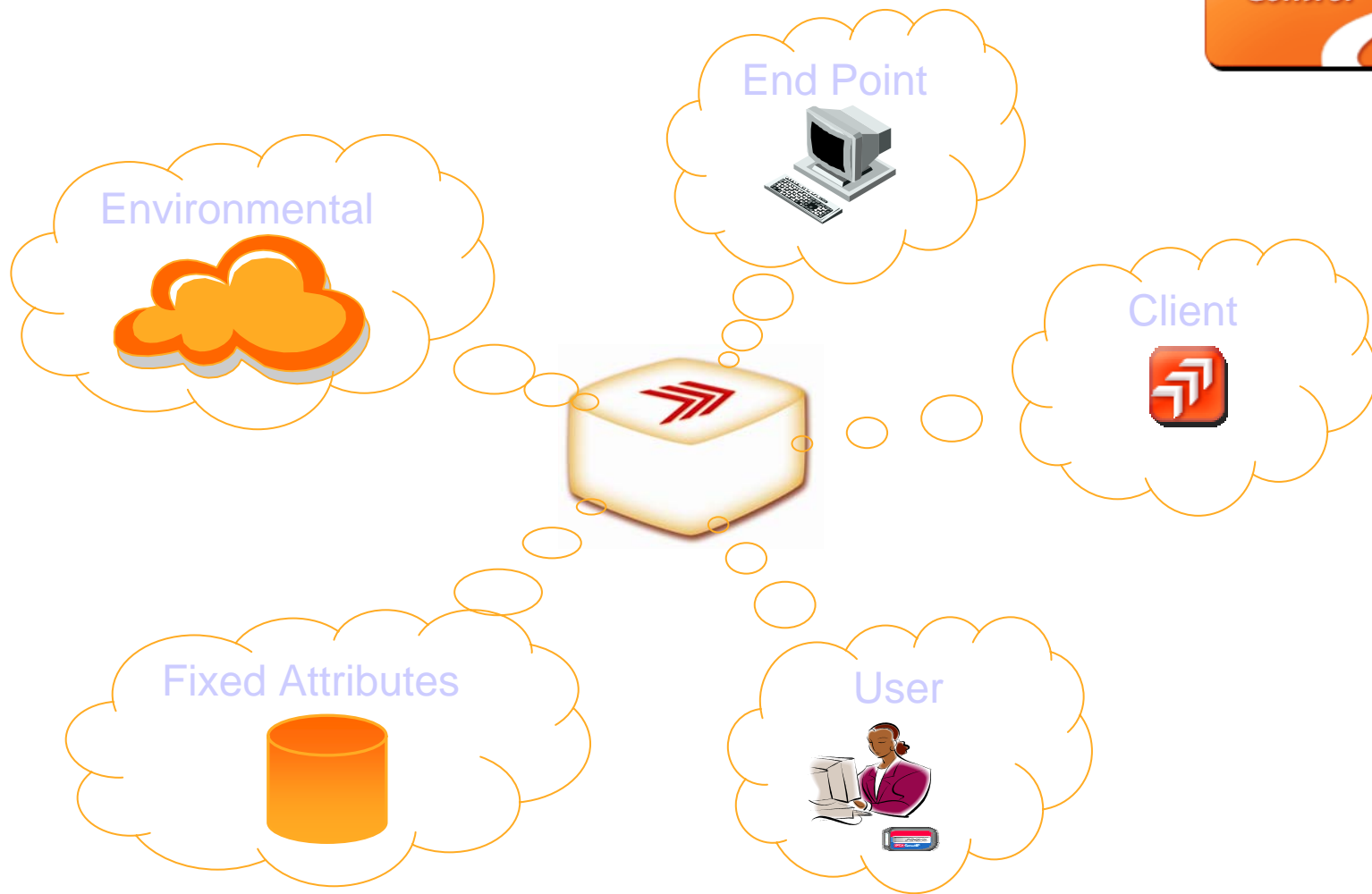


# Network Admission Control

Network  
Admission  
Control



# Flexible Rules



# More than just Network Admission Control

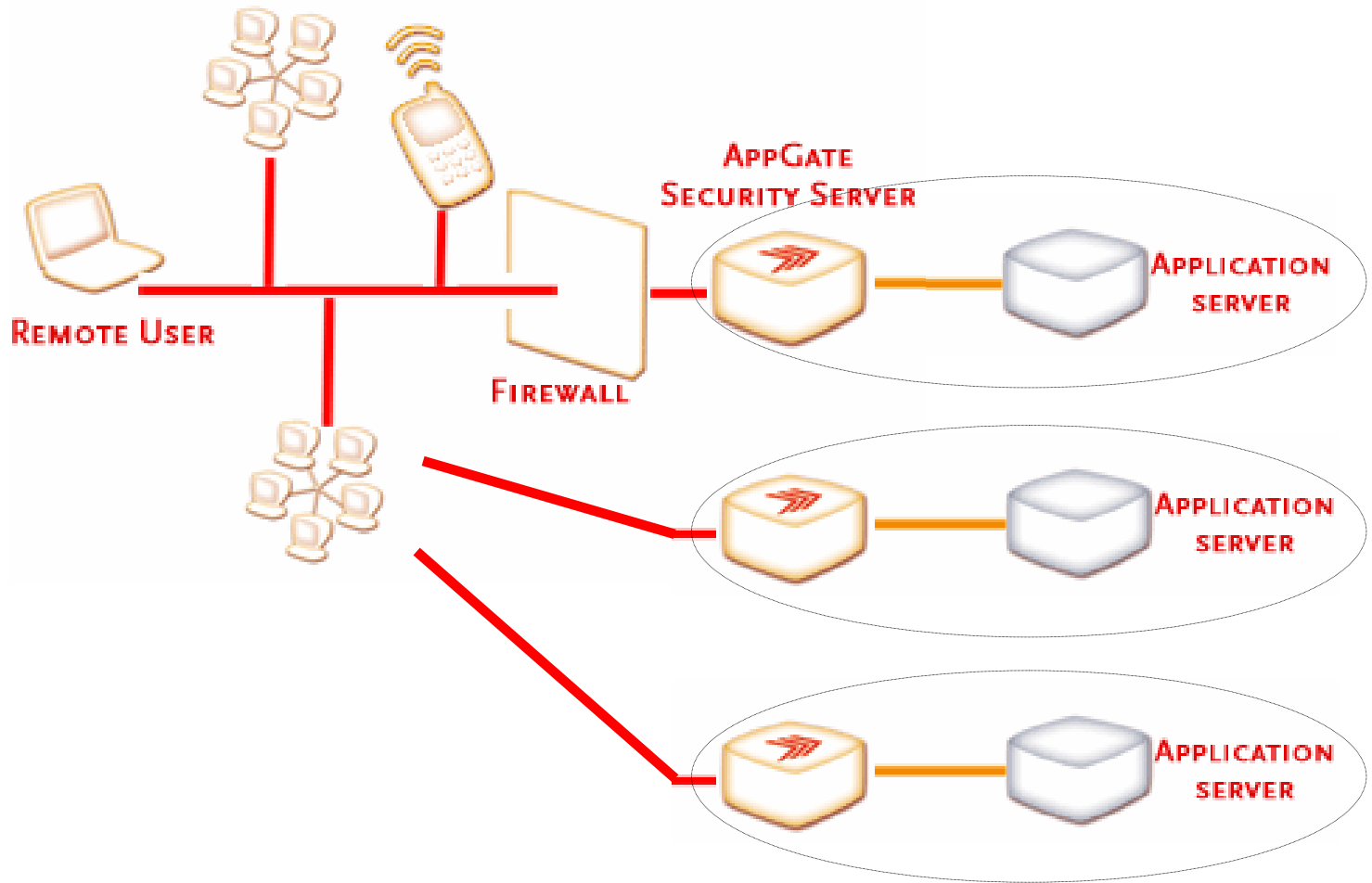


IP Access  
Reverse IP access  
ICMP access  
Admin access  
Log access  
Client command  
Server command  
Message  
Web proxy  
Shares proxy  
FTP proxy  
RDP proxy

## 2b - Networks



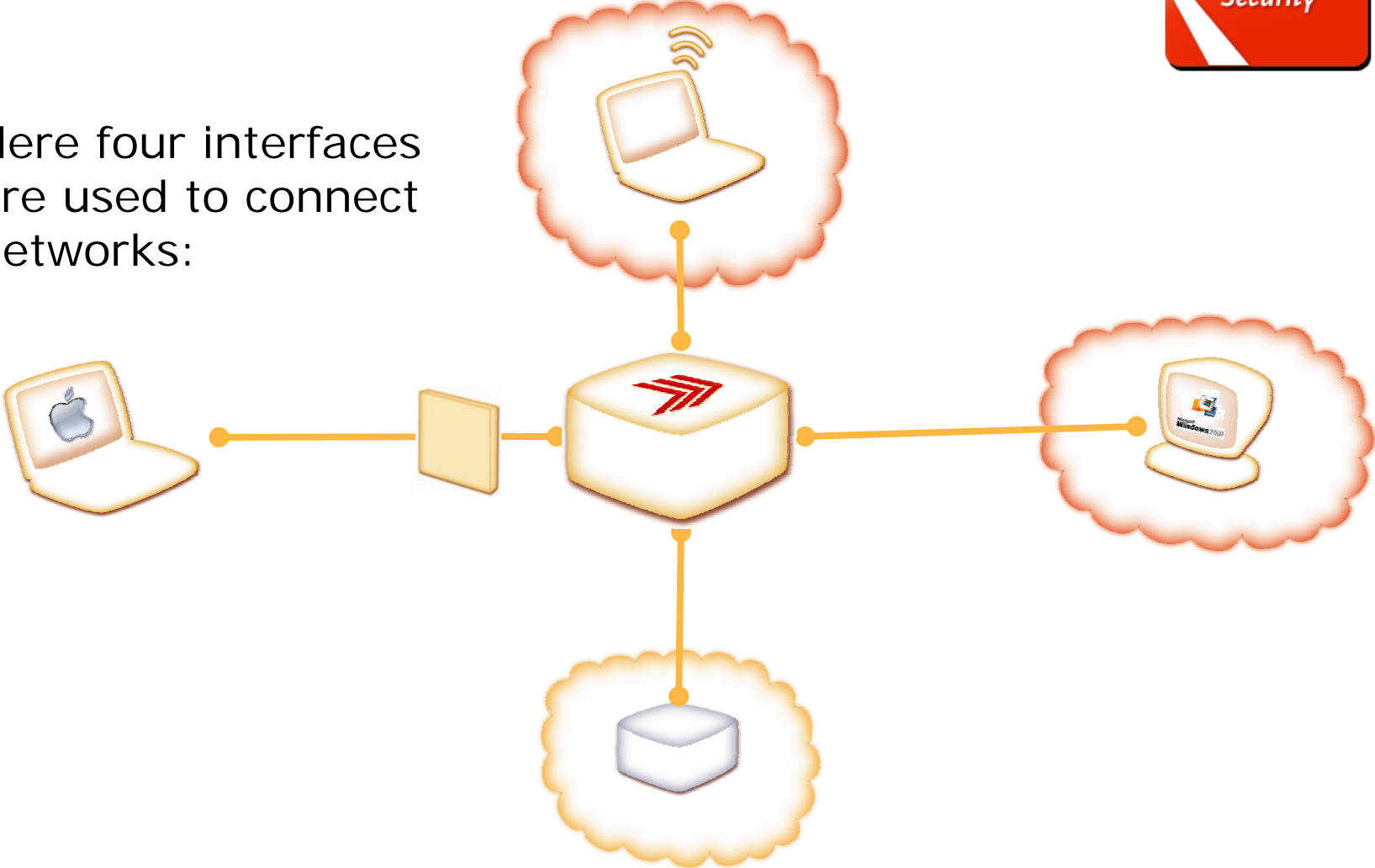
# Many servers can cooperate





# Not just an “inside” and an “outside”

Here four interfaces are used to connect networks:



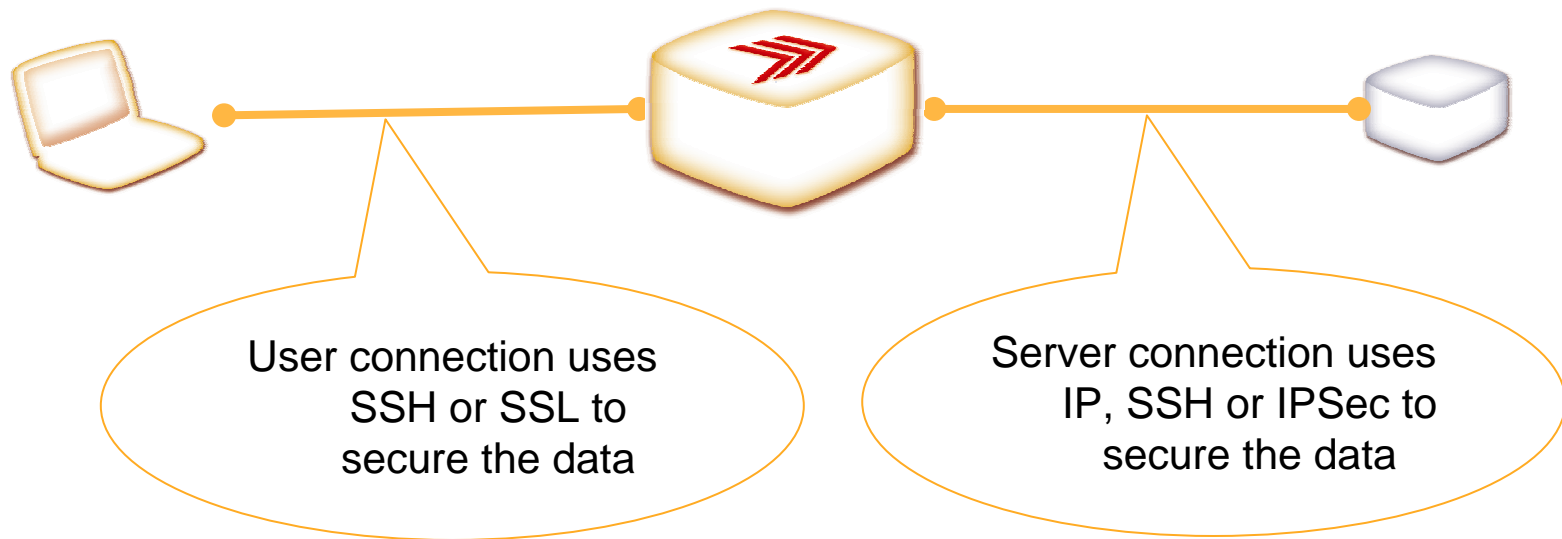
# 3 - Data



# Securing the data

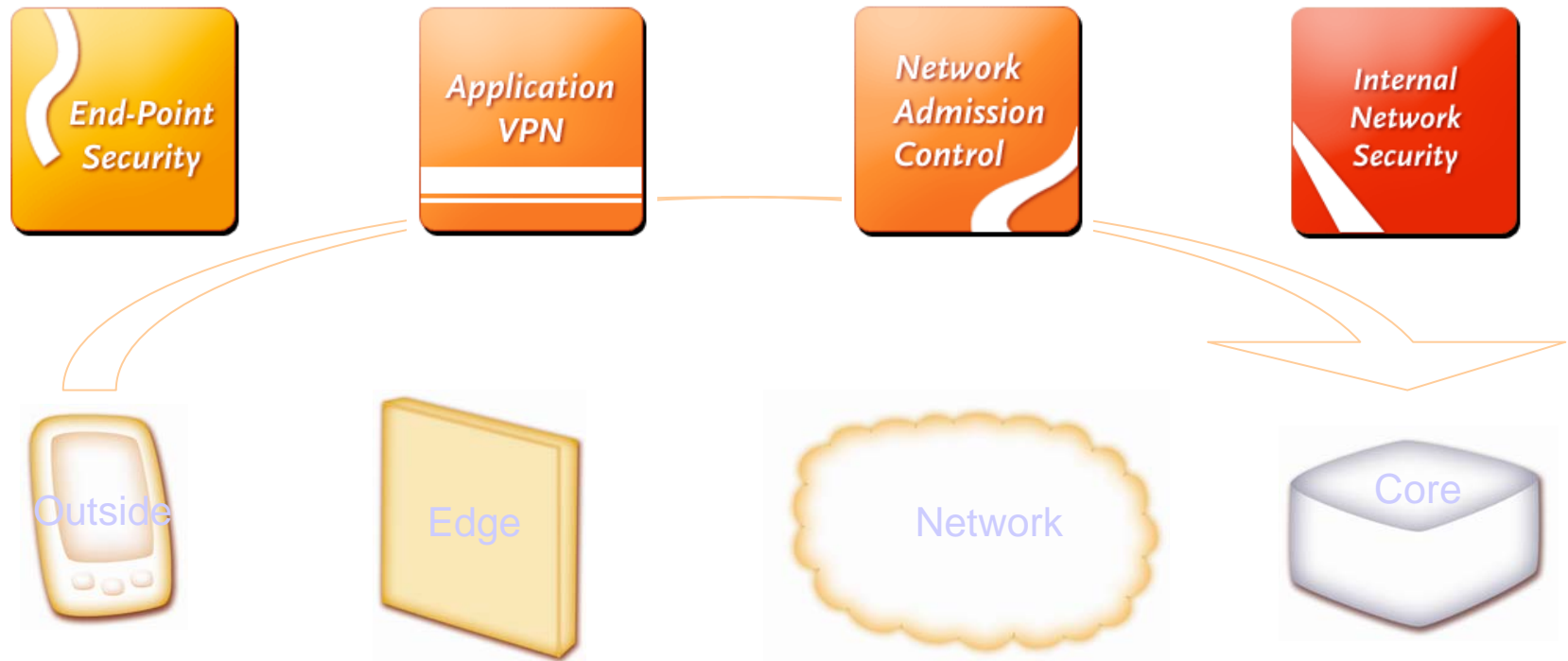


The AppGate solution uses different protocols according to the type of traffic being secured.



# The total solution....

By crossing all the barriers the AppGate solution is able to offer a Jericho style solution for secure information flows



# AppGate Quadrants of Security

## - Summary -

### Network Admission Control:

- Rights Management
- Client Check
- Distributed
- Personal Firewall



### Application VPN:

- Authentication & Encryption
- Roles & Rights Management
- Client Independence
- Full Application Support
- Secure Print
- Mobile VPN Roaming

### Balancing the Equation

### End-Point Security:

- Personal Firewall
- Cache Cleaning
- Client Check



### Internal Network Security:

- Authentication & Encryption
- Roles & Rights Management
- Single Sign On
- Full Application Support
- The server acts as a Firewall
- Instant Messaging

# The AppGate solution

- Supports secure connection regardless of device, transmission type (wired or wireless) or application
- Gives access to all important business information whenever it's needed, through one security system



- One system to administer, increased security at lower cost
- Delivered as an appliance on a **Sun Solaris** box

# Questions?

