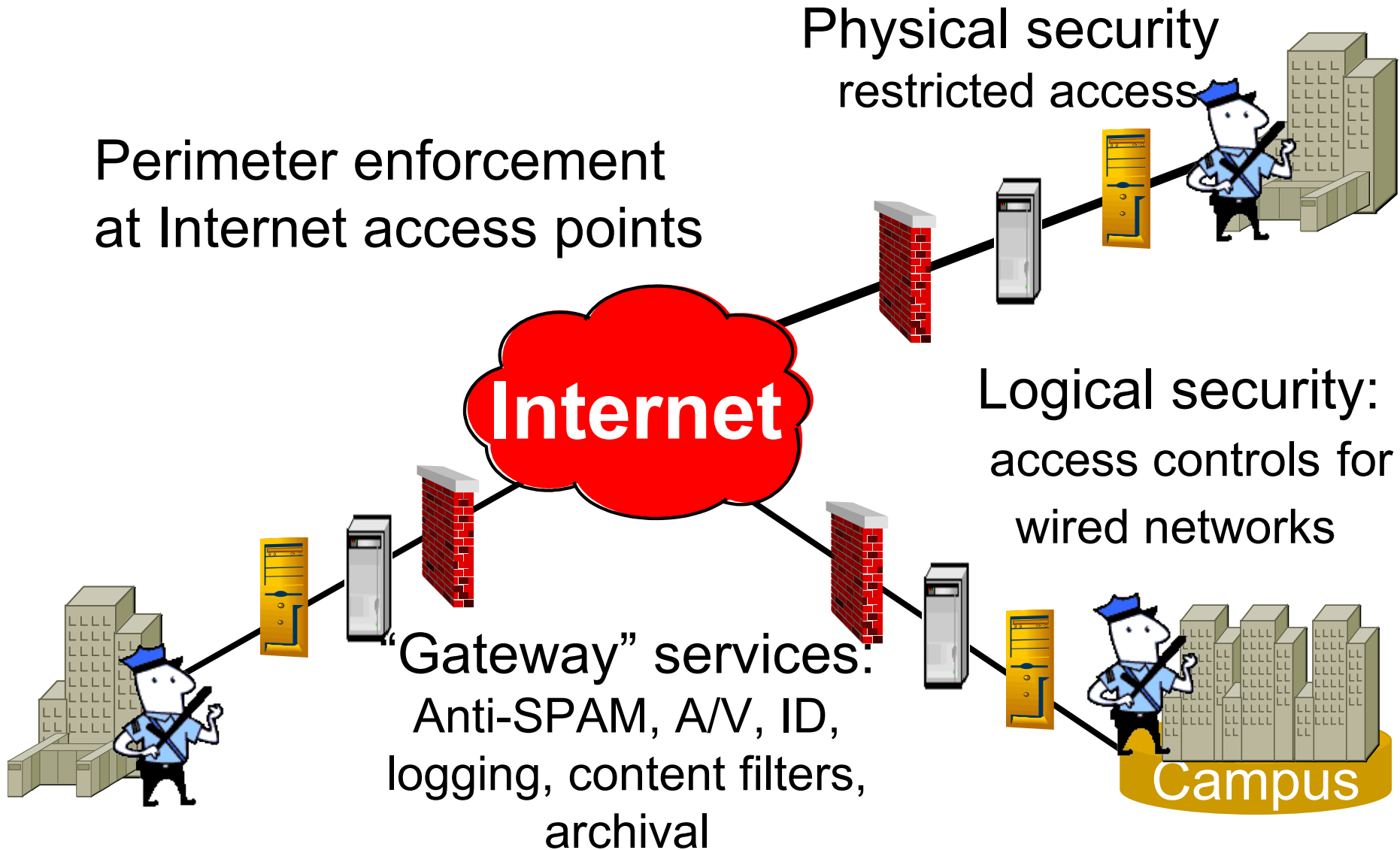


When Perimeters Dissolve: Security for a Mobile Enterprise

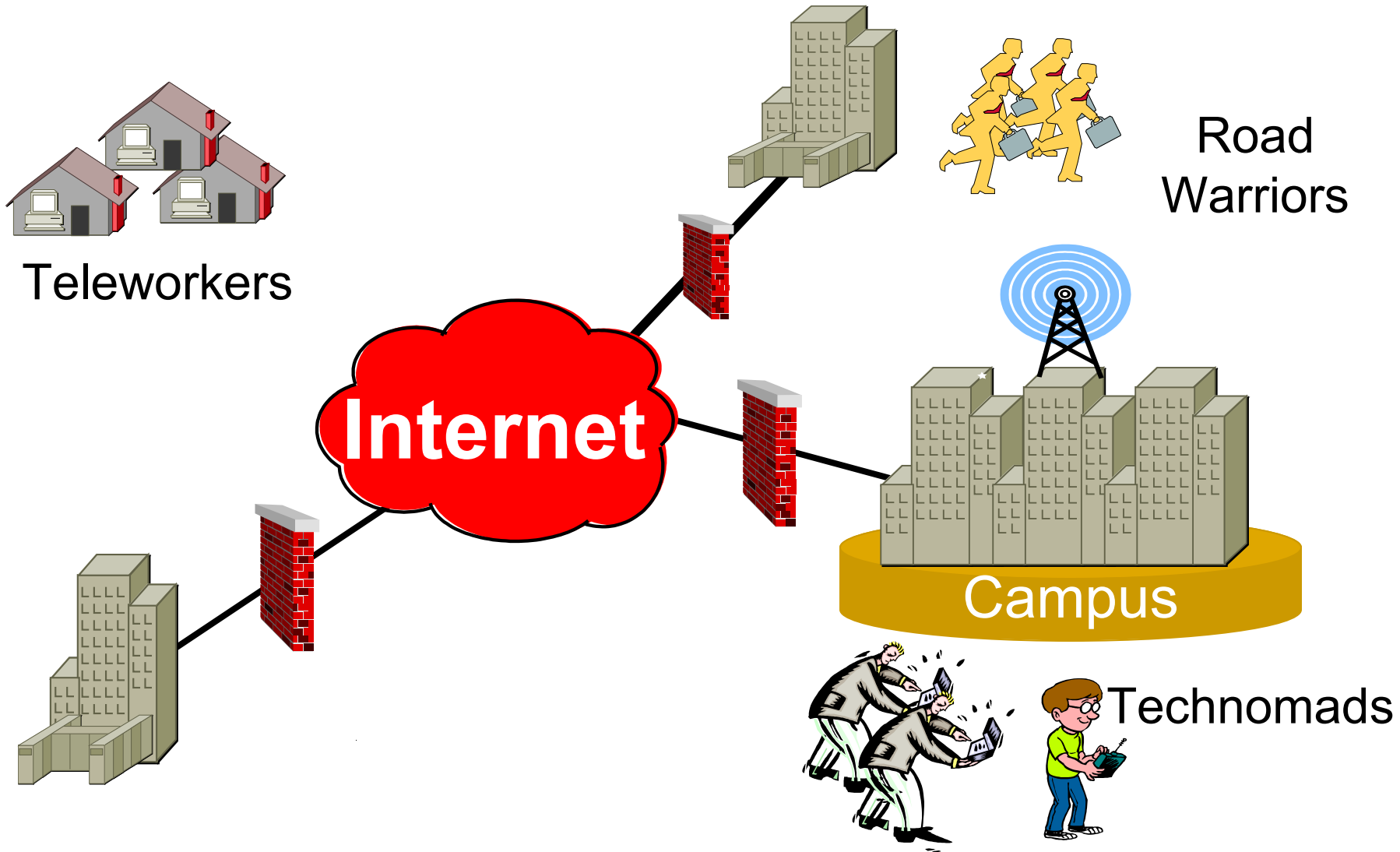
David M. Piscitello
Core Competence, Inc.
dave@corecom.com

September 11, 2002

Traditional Internet Security Paradigm



Today's Workforce Spends More Time Outside Defenses Than *Behind* Them



Exposures

- Physical security
 - Increased susceptibility to theft on road, at home
 - What's stolen is neither archived nor encrypted
 - Wired LANs in home shared with non-employees
 - Wireless LANs are commonly wide open
- Perimeter
 - Client hosts don't run firewalls, or
 - use ad hoc FW policy, inconsistent with corporate FW
- Anti-virus, Anti-SPAM, Content filtering
 - Client hosts lag in virus definition updates
 - Email and web AV gateways circumvented
 - Clients hosts don't run "enterprise" content filtering, AUP difficult to enforce

More Exposures

- Auditing
 - Clients either don't use logging or fail to preserve, forward, or protect logs
 - Client software policy configuration altered to meet an immediate need
 - Incidents emanating from client hosts hard to analyze
- Access control
 - Residential LANs and WLANs undermine VPN, increased vulnerability to illegal entry via authenticated (and encrypted) path
- Software control (A previously unsolved problem)
 - Illegal copies of registered software,
 - Software from suspect sources
 - Poor patch/upgrade practices



History Repeats Itself?

- Network security is often compared to castles
 - Layers of physical security (moats, walls, parapets)
 - Access Controls and Intrusion Detection (Bastion hosts, Man Traps, Check points)
 - **Nobility by and large remained protected in the Keep**
- Siege engines, tunneling, artillery threatened castles
 - Over time, countermeasures EVOLVED
 - and the castle (mostly) endured
- BUT
 - **Nobles and merchants began to travel**

Security for Mobile Clients Has Roots in Norman England!

- While they did not abandon castles, the Normans did not rely exclusively on them to protect occupants!
- As nobles increased travel
 - Entourage was accompanied by knights and yeoman
- Security was then, and remains, an exercise in layering...



Clients must be protected with comparable security measures to those provided at corporate facilities, irrespective of how they connect...

One F100 Enterprise Admin's Wish List

“I want to verify that every client host

- Runs personal firewall software
- Runs desktop antivirus software
- Is current with OS and application software versions and patches
- Uses a browser configuration consistent with our Acceptable Use Policy
- Uses authenticated, encrypted tunnels (VPN)



Irrespective of user and client host ‘location’” and

BEFORE I allow that client on my network

How it might work...

- Client host connects to corporate network
- User authenticates via VPN Tunnel
- Agent on client host identifies
 - PFW version, policy
 - A/V version, configuration, policy
 - Desktop antivirus use, definition update, and policy
 - OS and application software versions and patches installed
 - Browser configuration (enterprise grade “net nanny”...)
 - VPN version, policy
 - Appropriate authentication credentials presented
- Administrative software admits client only if all these defenses are current and functional
- Agent disconnects if any defense is disabled

-
- Is this admin's wish list out of reach?
 - How real are the threats?
 - Can we satisfy some of these today?
 - How close to real is this?