



Networking and Security

Kars Ohrenberg
DESY, IT

What I will not talk about ...



- Networking in general
 - Bandwidth, nowadays its just there ;-)
 - Delays, Jitter, ...
 - Quality of Service, ...
 - Reliability, Redundancy, ...
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)

Addresses, Networks and Ports



- What's an IP-address?
 - Identifies a single system attached to the network, e.g. 131.169.40.200
- What's a network address
 - Identifies a range of IP-addresses, e.g. 131.169.0.0/16
 - Networks are interconnected via routers
- What's a TCP/UDP port
 - Identifies a service running on a network connected system, e.g. 80 = http, 22 = ssh, ...

Network Security

- Per default a system on a network can reach any other system without any restriction
- Software is never bug free, thus there are possible threats which disturb operations:
 - Denial of Service Attack (DoS), Worms, Hacker, Viruses,
- Nowadays an unprotected and unpatched systems sees the first attacks from the Internet within minutes and might be infected in less then 15 minutes!

Host Based Security



- Beside implementing security mechanisms within the network there are various ways to improve the security on the end systems themselves
 - Patches
 - Personal Firewall
 - Virus Scanner
 - ...

Problems with Host Based Security



- You have to modify your system frequently which is not always adequate
- Hard to implement a central management especially taking into account systems from various institutes
- Mobile systems are usually very personalized with lots of individual setups and components

Security Mechanisms within Networks



■ Packetfilter

- Router can filter traffic based on IP-addresses, network addresses or protocol ports
- Cheap and easy to implement (comes with the router) but stateless filtering

■ Firewalls

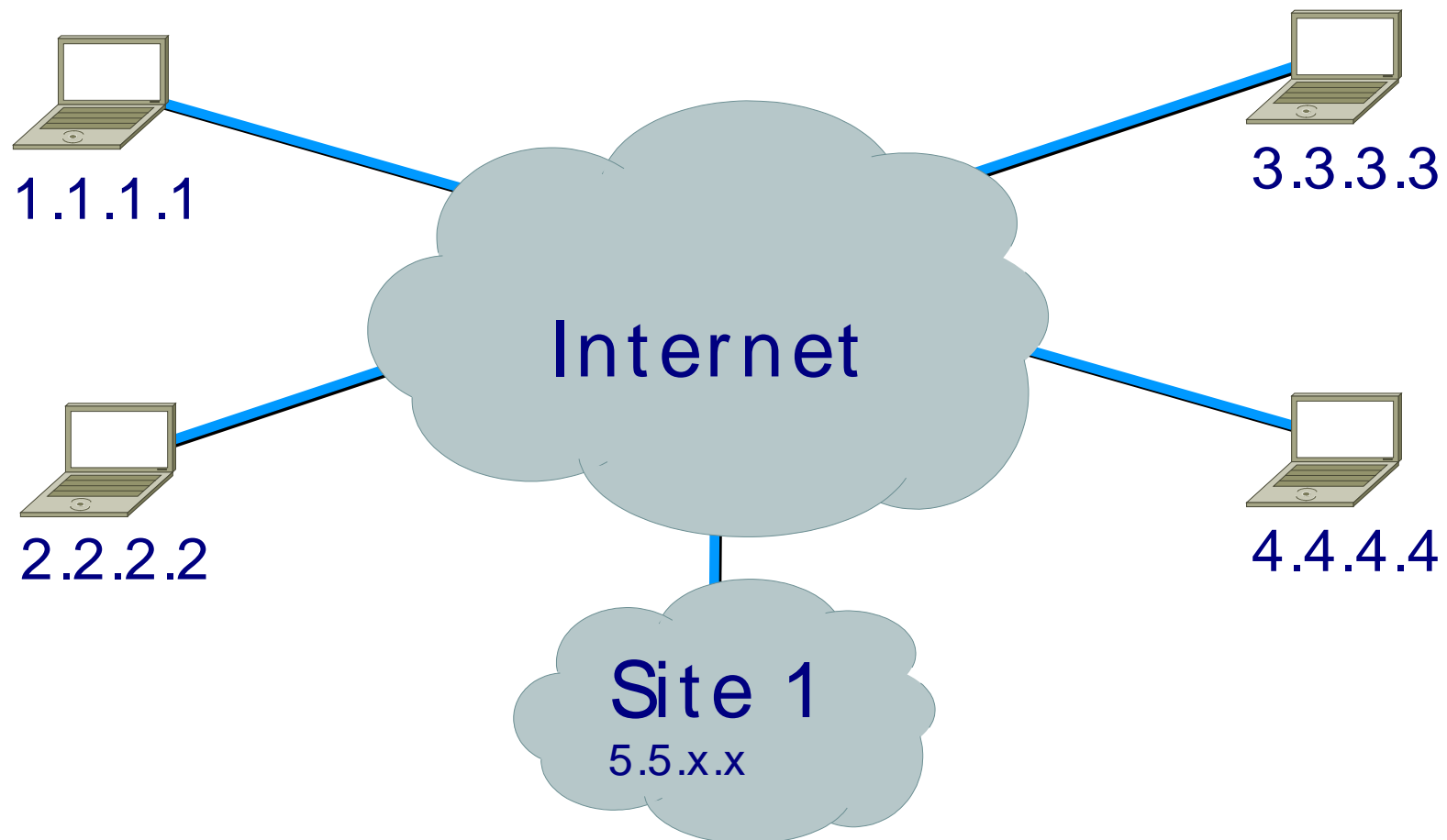
- More advanced and statefull filtering
- Protocol based filtering, ports are opened on demand by listening on the communication stream of the application (e.g. H.323, FTP, ...)

Virtual Private Networks (VPNs)

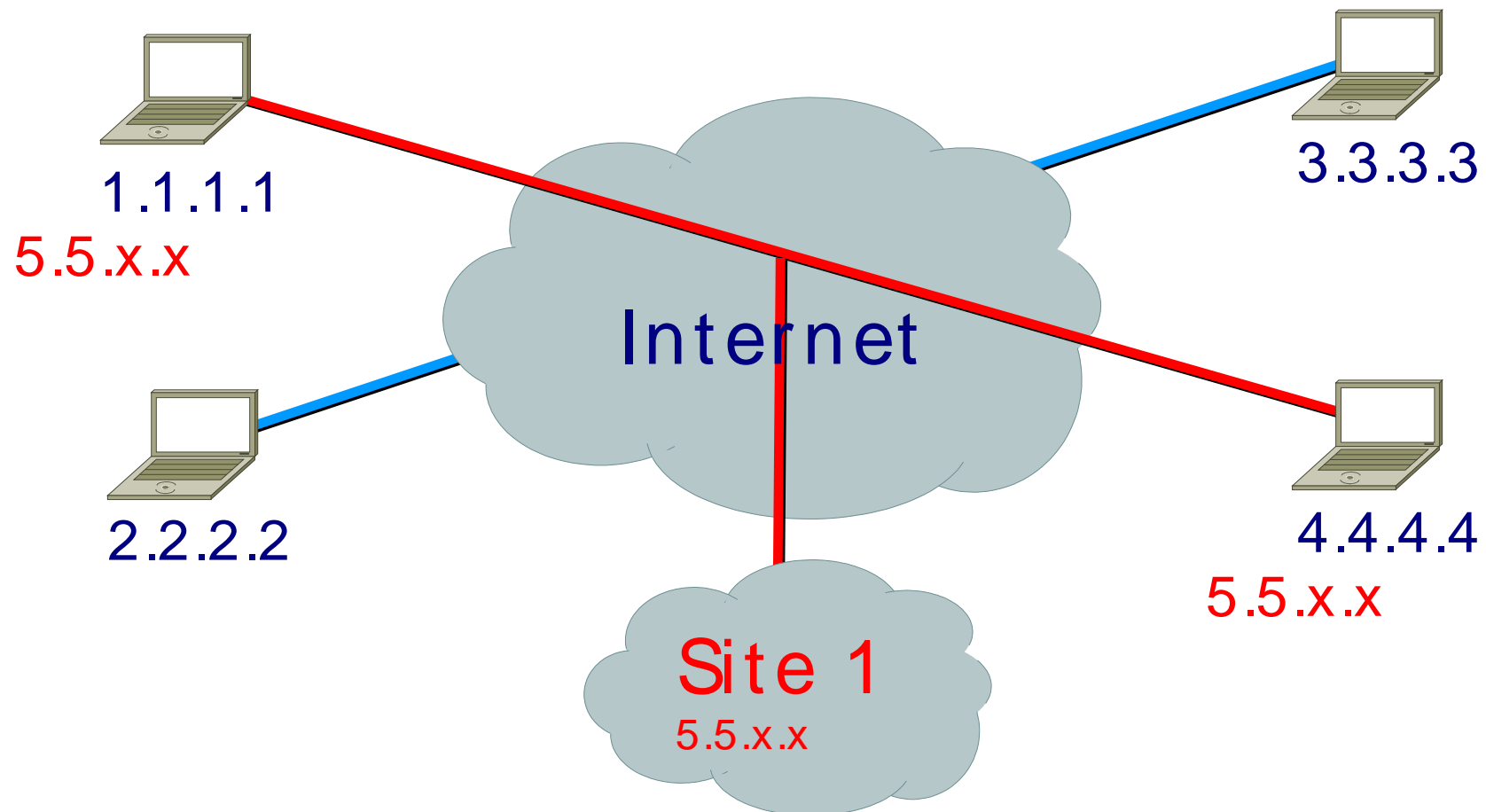


- Firewalls are a good solution for on-site systems but are a nightmare for mobile systems
 - External access to the Intranet usually blocked
- A common solution are VPNs
 - Site-to-Site
 - routers authenticate each other and pass traffic between their networks encrypted across the internet
 - Client-Server
 - The PC starts a client SW and builds a secure tunnel

VPNs (2)



VPNs (2)



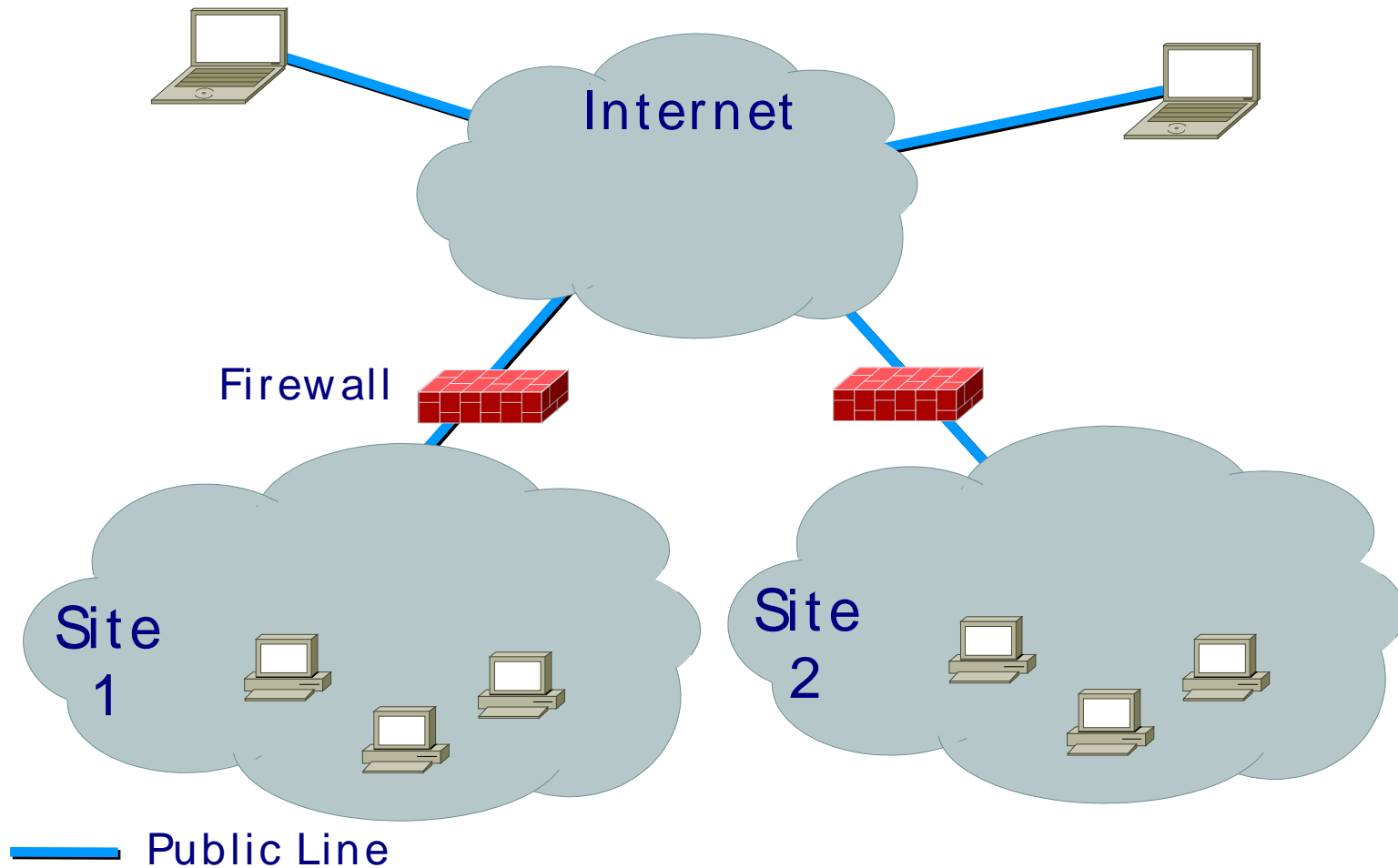
VPN Security

- Privacy is ensured as all traffic is encrypted (e.g. 3DES, AES, ...)
- User-authentication can be based on various available methods (Active Directory, Kerberos, Radius,)
- VPN requires one software to be installed on the client systems
 - Usually available for all common platforms (Win XP, Linux, MAC, ...)
 - Web-VPNs are coming up

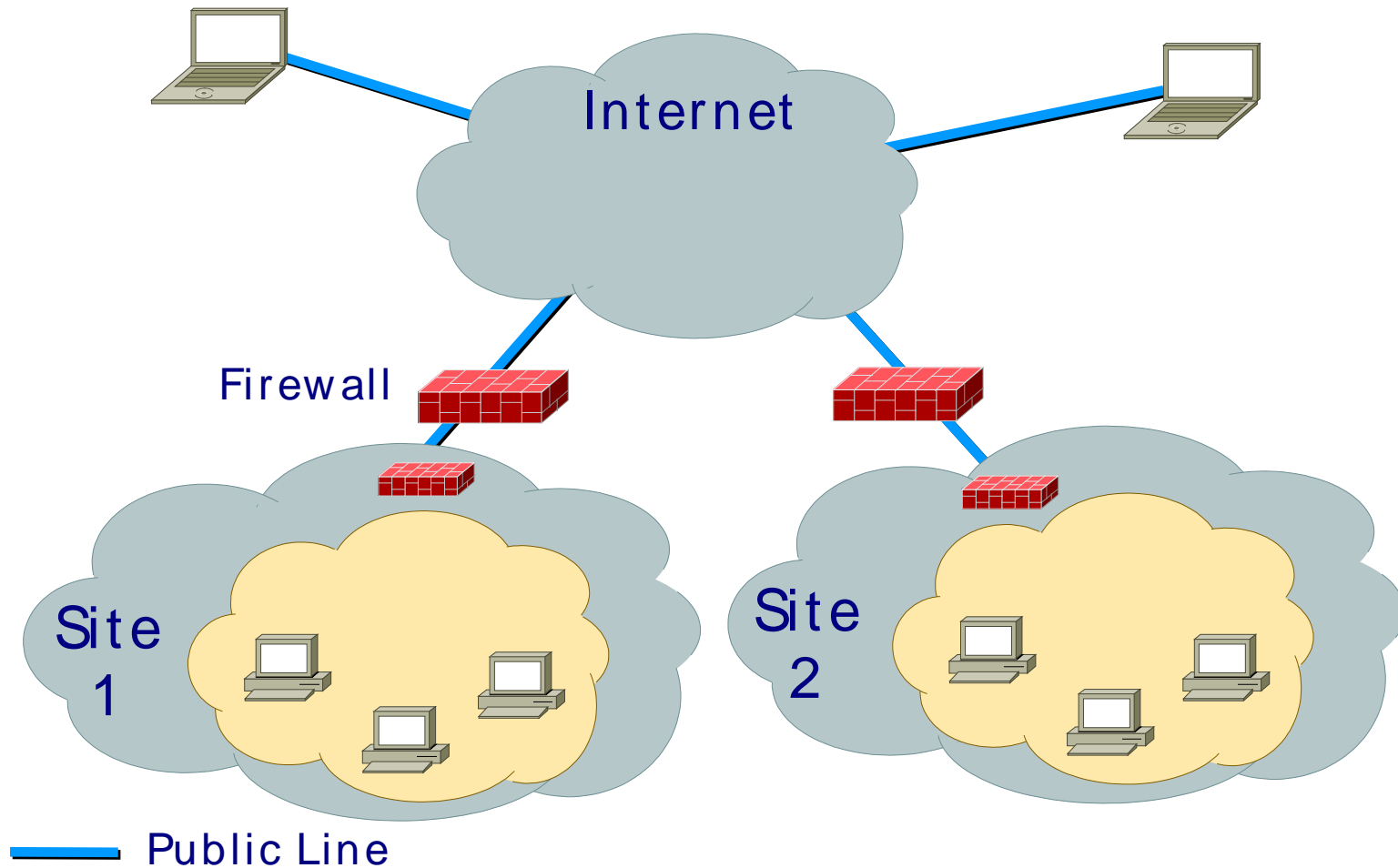
VPN Security

- VPN Access Policies can be defined and be central managed
- Policies are defined per user or group and can include
 - Access Rights, Access Hours, ...
 - Type of Encryption
 - Authentication Method
 - Can require that certain software is installed on the client system (virus scanner, ...)
 - ...

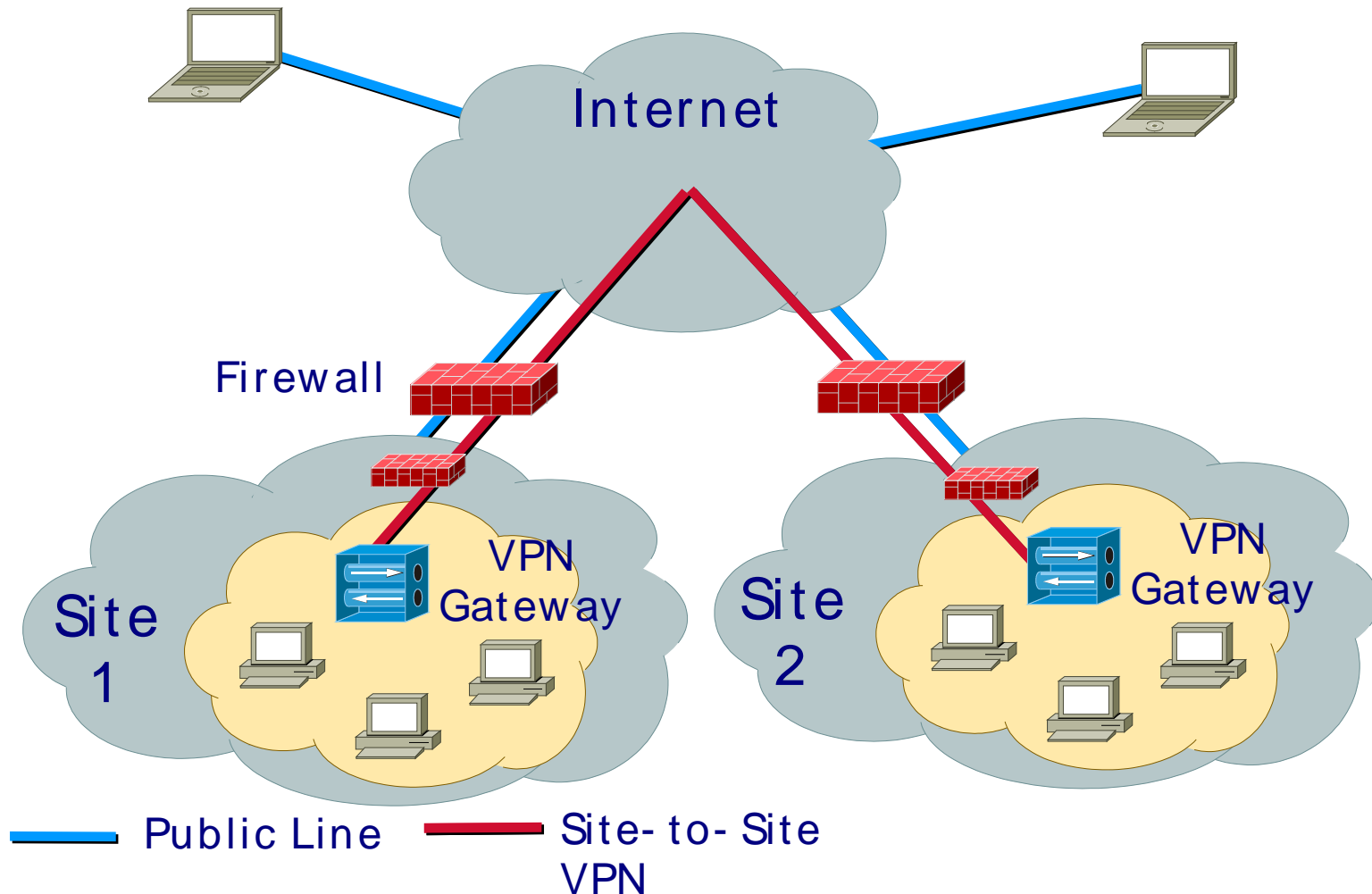
A VPN and Firewall based Network Design



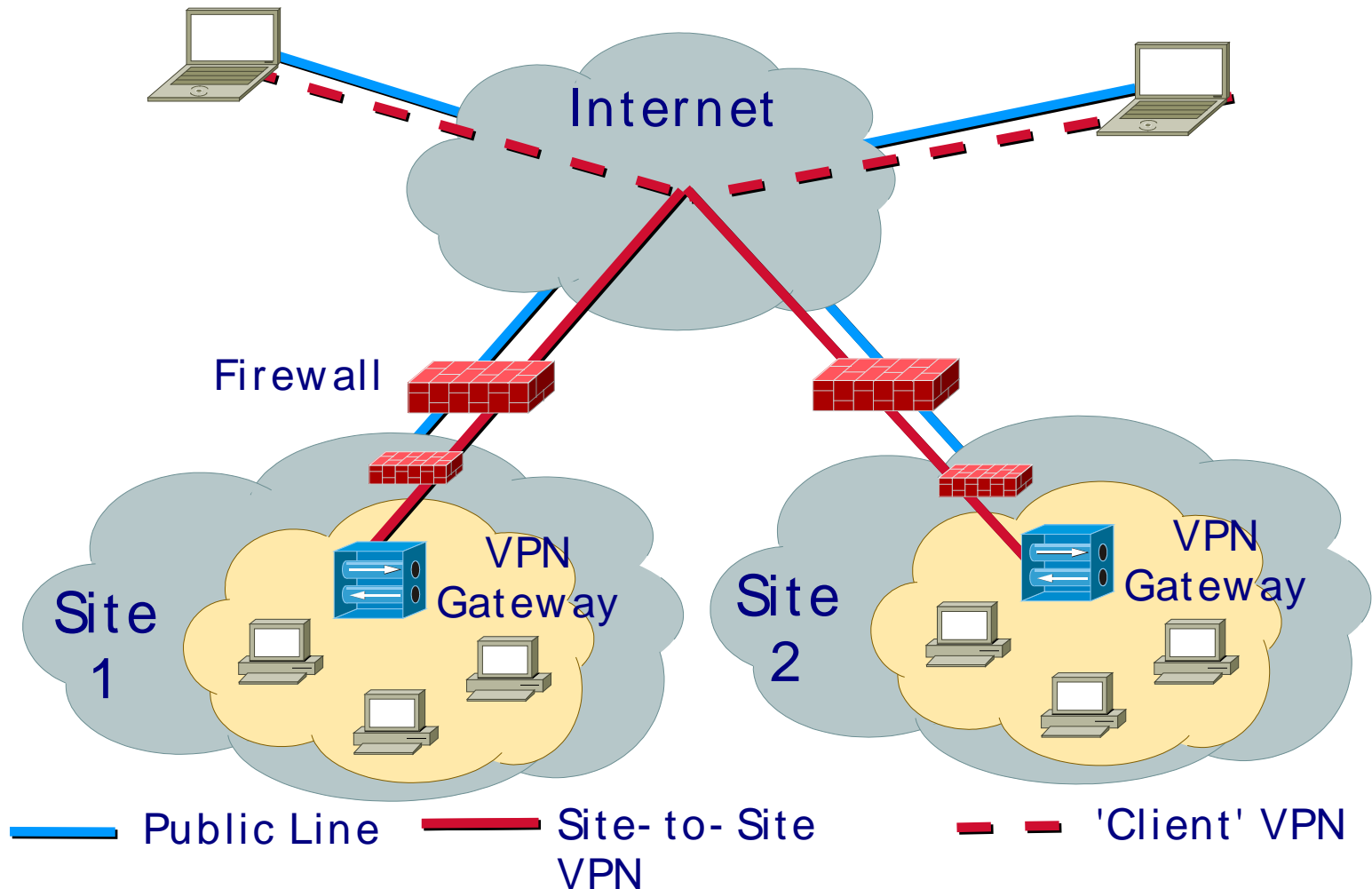
A VPN and Firewall based Network Design



A VPN and Firewall based Network Design



A VPN and Firewall based Network Design



Summary

- Host based security is the best solution if you are able to modify and patch your systems frequently
- Network based security (Firewalls, etc.) can protect insecure systems efficiently
- You can open a single port in the firewall for your application but you have to implement encryption, authentication yourself
- VPN comes with encryption, authentication out of the box but requires additional SW

Security makes network access more complicated and you have to find the right balance