University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

PSIT302 & PSIT3P2 – Information Security Management (ISM)

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

Firewall

A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.

A firewall can block an unauthorized access to network (E.g. A watchman standing at gate can block a thief)

A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)

Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)

No man-power is required to manage a firewall.

Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)

IDS

An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network.

An IDS can only report an intrusion; it cannot block it (E.g. A CCTV camera which can alert about a thief but cannot stop it)

IDS is fully capable of internal security by collecting information from a variety of system and network resources and analyzing the symptoms of security problems

IDS keeps a check of overall network

An administrator (man-power) is required to respond to threats issued by IDS

IDS are very difficult to be spotted in a network (especially stealth mode of IDS).

Unit II – Security Management of IT Systems

- Network Security Management

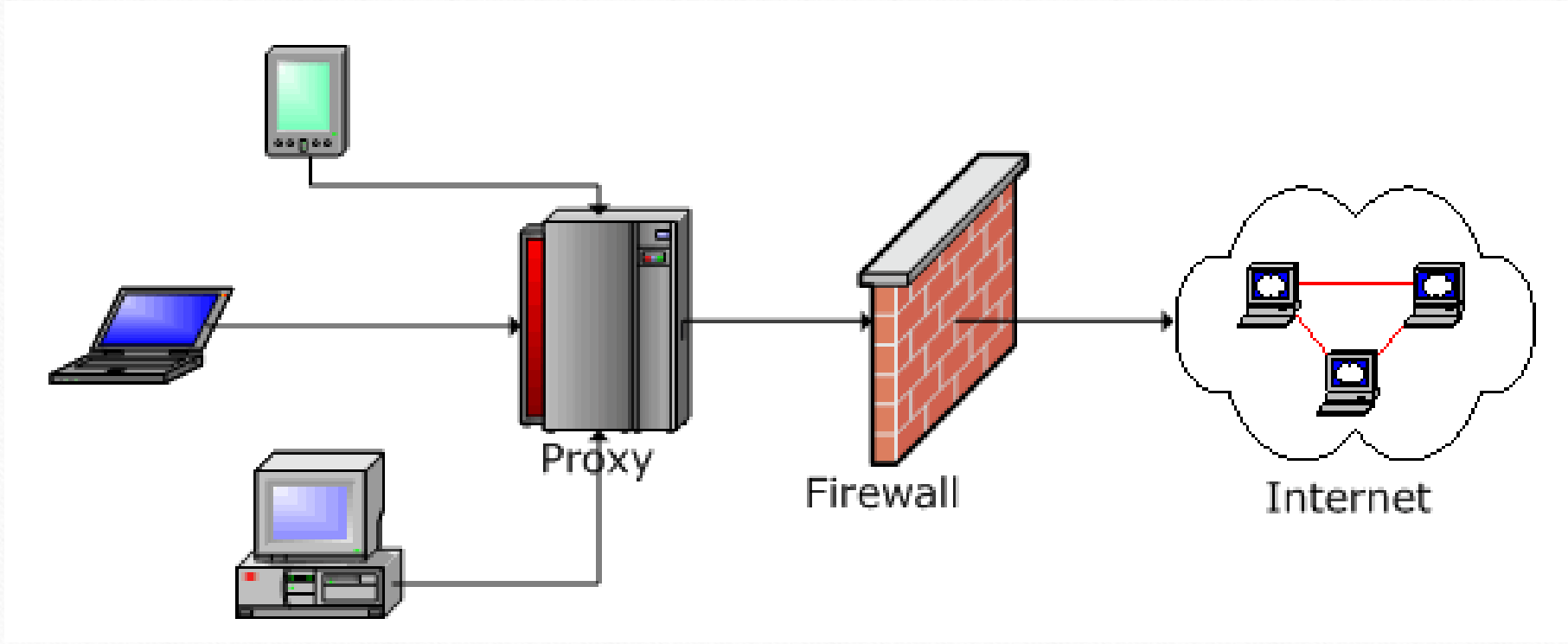
- **Firewalls**, IDS and IPS Configuration Management
- **Web and Wireless Security Management**
- General Server Configuration guidelines and maintenance
- ISM Classification
- Access control Models
- Linux and Windows Case Study
- Technical Controls
- Password Management and Key Management for USers

Firewall

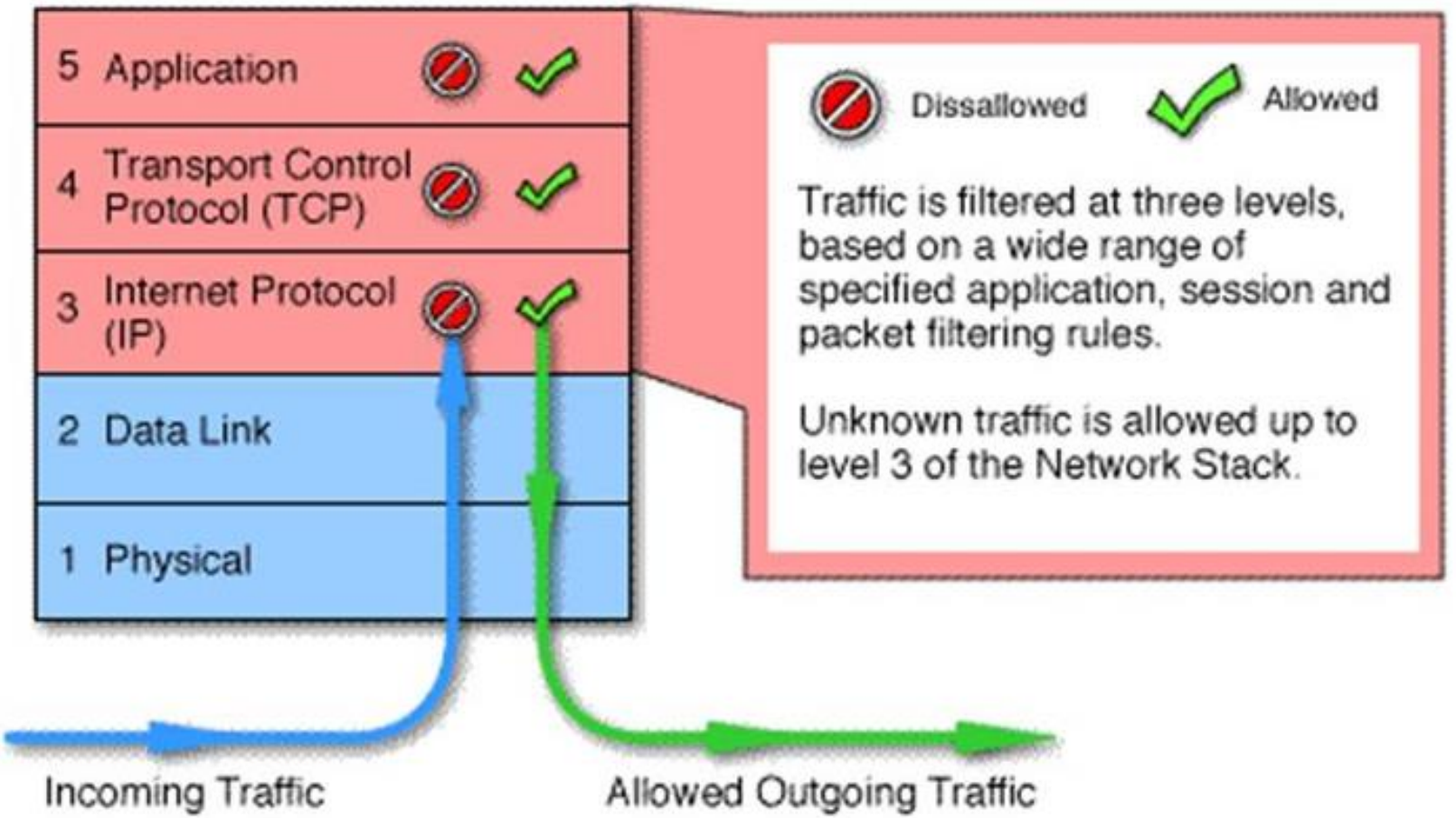
- A *firewall* is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A *firewall* typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Types of firewalls

- **Proxy firewall**
  - An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application.
  - Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.
- **Stateful inspection firewall**
  - Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol.
  - It monitors all activity from the opening of a connection until it is closed.
  - Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

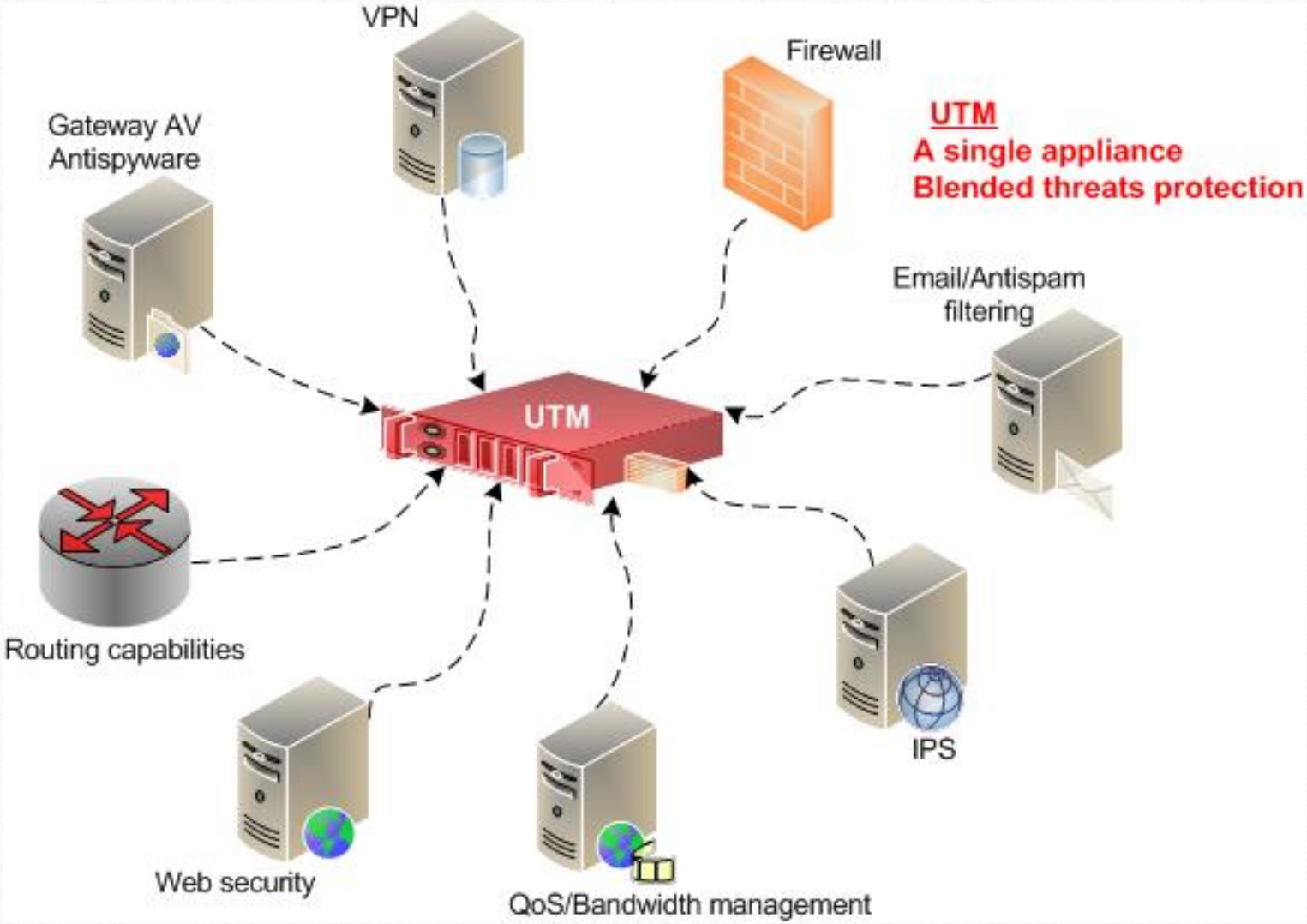


Proxy Server



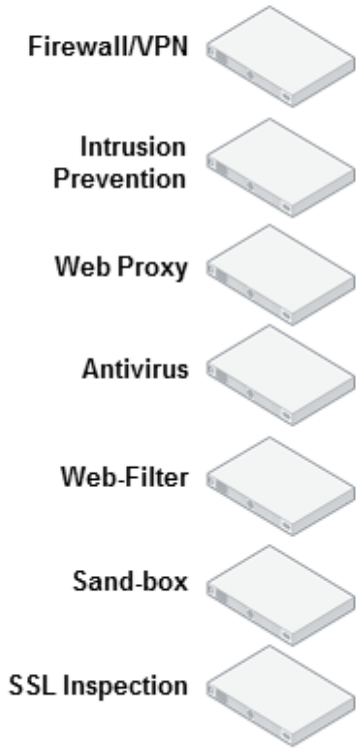
Stateful Inspection Firewall

- **Unified threat management (UTM) firewall**
  - A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.
- **Next-generation firewall (NGFW)**
  - Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.
- According to Gartner, Inc.'s definition, a next-generation firewall must include:
  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

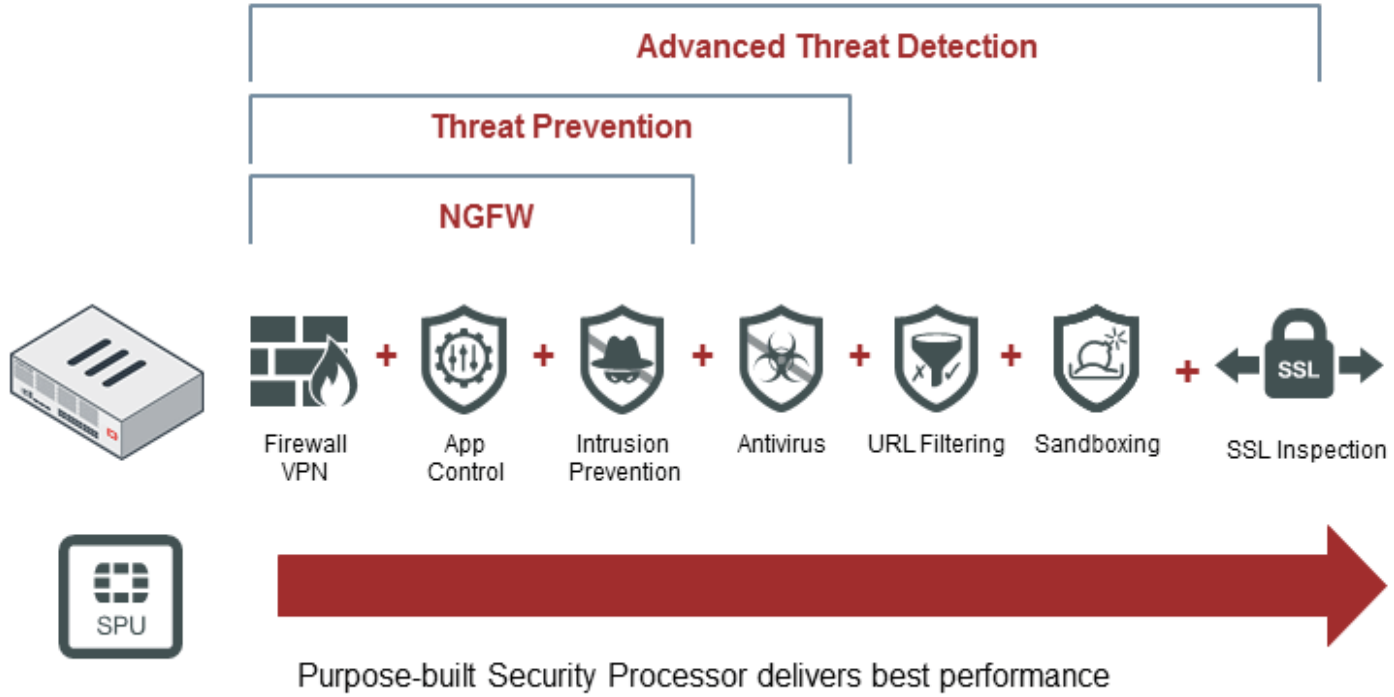

VPN
Firewall
UTM
A single appliance
Blended threats protection
Gateway AV
Antispyware
Email/Antispam
filtering
UTM
Routing capabilities
IPS
Web security
QoS/Bandwidth management

Next Generation Firewall

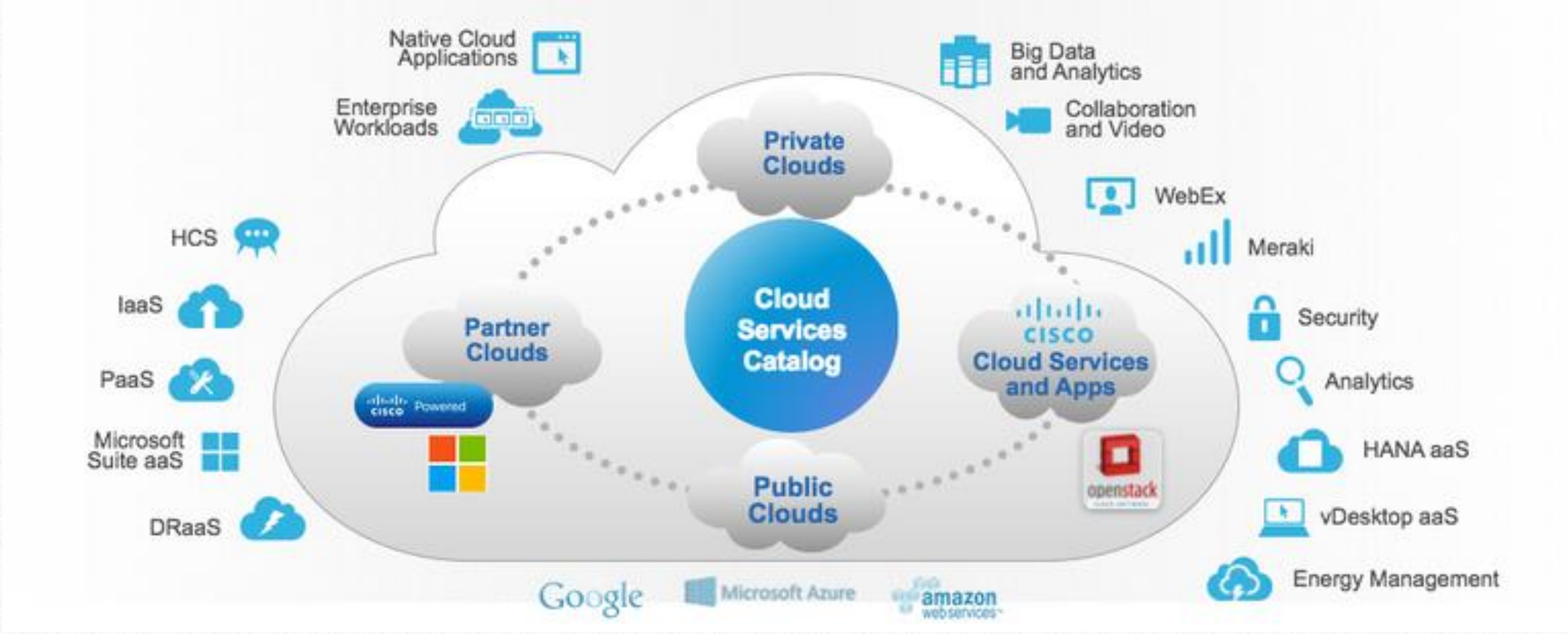
Standalone



FortiGate Next Generation Firewalls

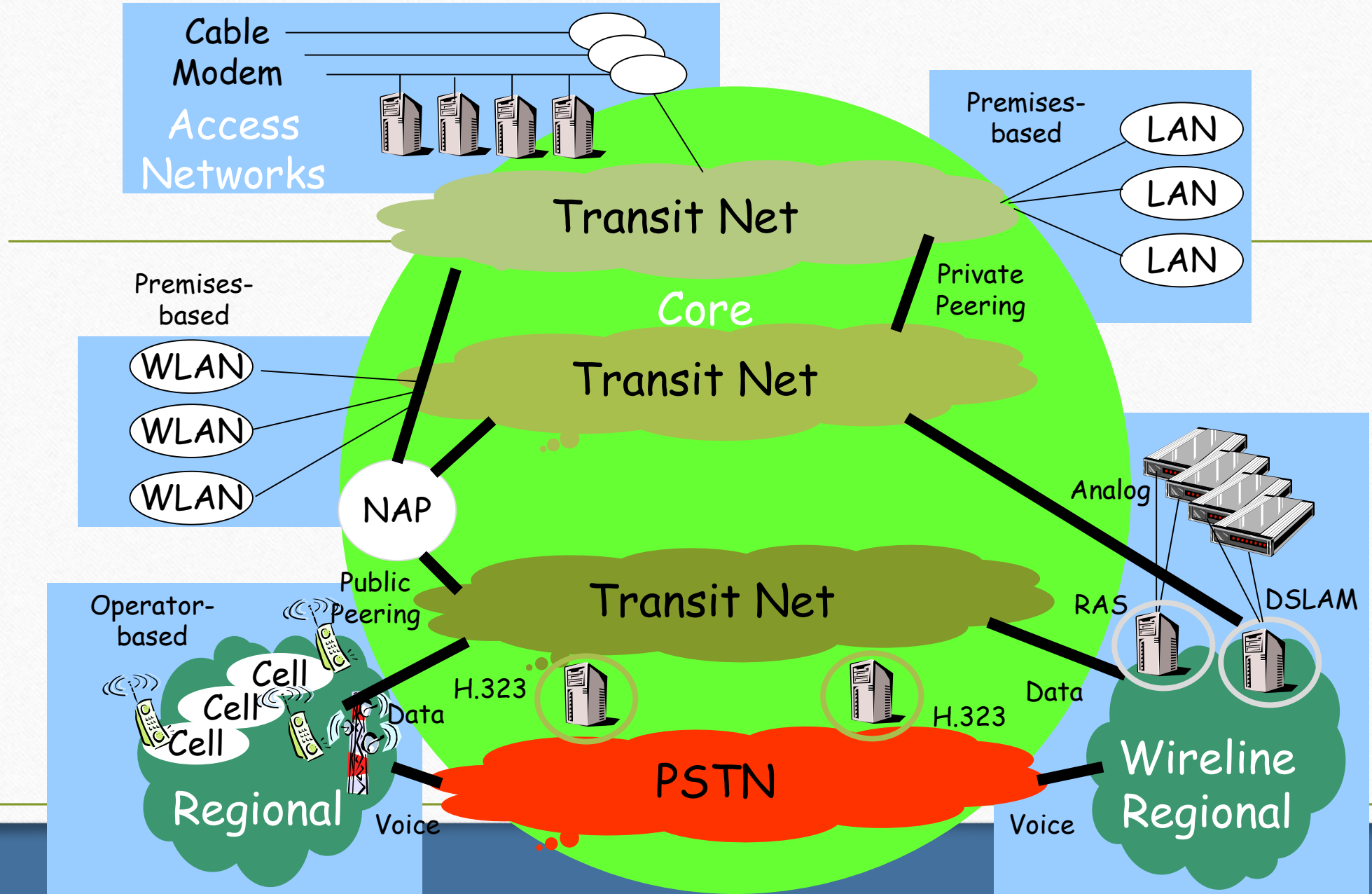


- **Threat-focused NGFW**
  - These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:
  - **Know which assets are most at risk** with complete context awareness
  - **Quickly react to attacks** with intelligent security automation that sets policies and hardens your defenses dynamically
  - **Better detect evasive or suspicious activity** with network and endpoint event correlation
  - **Greatly decrease the time from detection to cleanup** with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
  - **Ease administration and reduce complexity** with unified policies that protect across the entire attack continuum


Native Cloud Applications
Enterprise Workloads
Big Data and Analytics
Collaboration and Video
WebEx
Meraki
Security
Analytics
HANA aaS
vDesktop aaS
Energy Management
HCS
IaaS
PaaS
Microsoft Suite aaS
DRaaS
Private Clouds
Partner Clouds
Public Clouds
Cloud Services Catalog
CISCO Cloud Services and Apps
Powered
openstack
Google
Microsoft Azure
amazon web services

Wireless Security Management

The Current Internet: Connectivity and Processing



How can it affect cell phones?

- Cabir worm can infect a cell phone
  - Infect phones running Symbian OS
  - Started in Philippines at the end of 2004, surfaced in Asia, Latin America, Europe, and later in US
  - Posing as a security management utility
  - Once infected, propagate itself to other phones via Bluetooth wireless connections
  - Symbian officials said security was a high priority of the latest software, Symbian OS Version 9.
- With ubiquitous Internet connections, more severe viruses/worms for mobile devices have appeared and will continue to strive …

Outlines

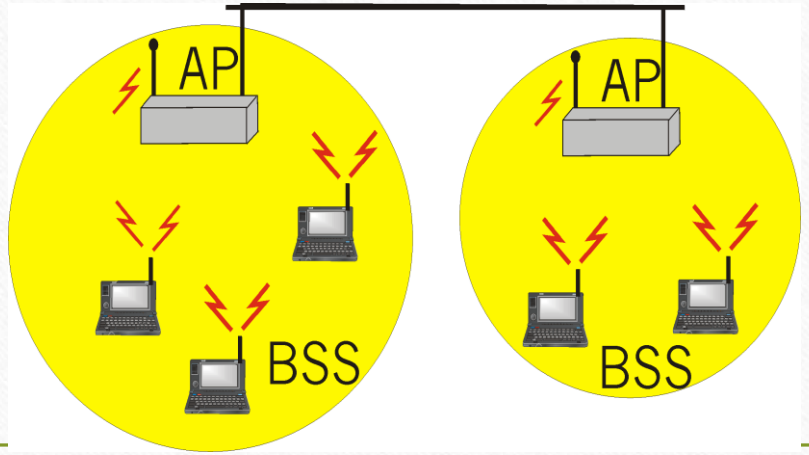
- 802.11 Basics
- Security in 802.11b: WEP
- WPA and WPA2

IEEE 802.11 Wireless LAN

- 802.11b
  - up to 11 Mbps
- 802.11a
  - up to 54 Mbps
- 802.11g
  - up to 54 Mbps
- 802.11n
  - up to 150 ~ 600 Mbps
- All have base-station and ad-hoc network versions

Base station approach

- Wireless host communicates with a base station
  - base station = access point (AP)
- Basic Service Set (BSS) (a.k.a. "cell") contains:
  - wireless hosts
  - access point (AP): base station
- BSS's combined to form distribution system (DS)

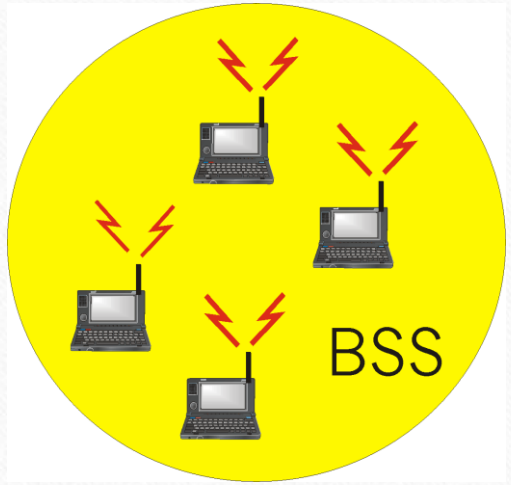


Ad Hoc Network approach

- No AP (i.e., base station)
- wireless hosts communicate with each other

  - to get packet from wireless host A to B may need to route through wireless hosts X,Y,Z

- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield



Outlines

- 802.11 Basics
- Security in 802.11b
- WEP
- WPA and WPA2

802.11b: Built in Security Features

- Service Set Identifier (SSID)

- Differentiates one access point from another
- SSID is cast in ‘beacon frames’ every few seconds.
- Beacon frames are in plain text!

Associating with the AP

- Access points have two ways of initiating communication with a client

---

- Shared Key or Open System authentication
- Open System: need to supply the correct SSID
  - Allow anyone to start a conversation with the AP
- Shared Key is supposed to add an extra layer of security by requiring authentication info as soon as one associates

How Shared Key Auth. works

- Client begins by sending an association request to the AP
- AP responds with a challenge text (unencrypted)
- Client, using the proper WEP key, encrypts text and sends it back to the AP
- If properly encrypted, AP allows communication with the client

Wired Equivalent Protocol (WEP)

- Primary built security for 802.11 protocol
- Uses 40bit RC4 encryption
- Intended to make wireless as secure as a wired network
- Unfortunately, since ratification of the 802.11 standard, RC4 has been proven insecure, leaving the 802.11 protocol wide open for attack

Wi-Fi Protected Access (WPA)

- Flaws in WEP known since January 2001 - flaws include weak encryption (keys no longer than 40 bits), static encryption keys, lack of key distribution method.
- In April 2003, the Wi-Fi Alliance introduced an interoperable security protocol known as WiFi Protected Access (WPA).
- WPA was designed to be a replacement for WEP networks without requiring hardware replacements.
- WPA provides stronger data encryption (weak in WEP) and user authentication (largely missing in WEP).

WPA Security Enhancements

- WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms.
- The combination of these two mechanisms provides dynamic key encryption and mutual authentication
- TKIP adds the following strengths to WEP:
  - Per-packet key construction and distribution:

WPA automatically generates a new unique encryption key periodically for each client. This avoids the same key staying in use for weeks or months as they do with WEP.

  - Message integrity code: guard against forgery attacks.
  - 48-bit initialization vectors, use one-way hash function instead of XOR

WPA2

- In July 2004, the IEEE approved the full IEEE 802.11i specification, which was quickly followed by a new interoperability testing certification from the WiFi Alliance known as WPA2.

- Strong encryption and authentication for infrastructure and ad-hoc networks (WPA1 is limited to infrastructure networks)
  - Use AES instead of RC4 for encryption
- WPA2 certification has become mandatory for all new equipment certified by the Wi-Fi Alliance, ensuring that any reasonably modern hardware will support both WPA1 and WPA2.