

Security in Digital Age

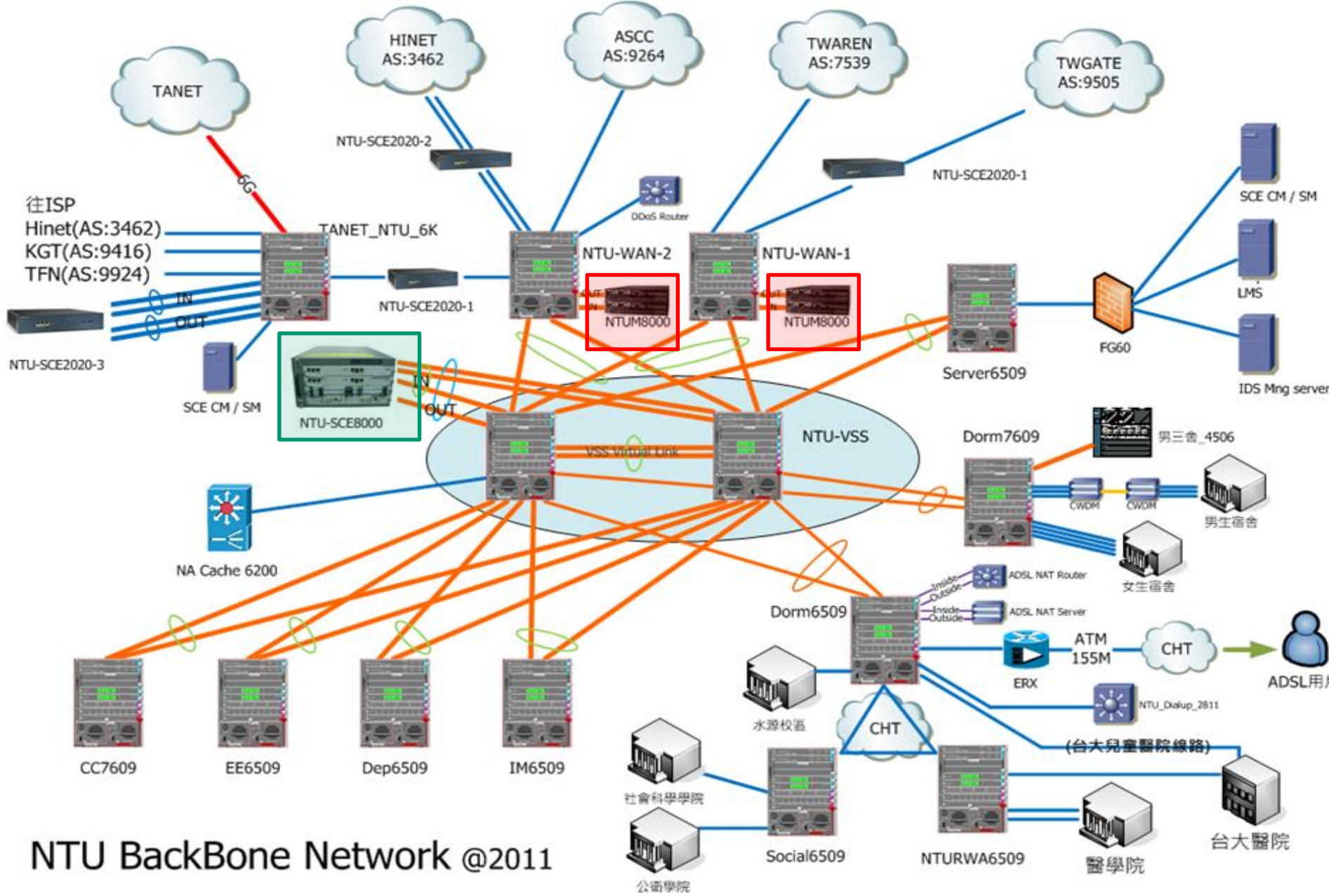


孫雅麗

國立臺灣大學

December 2016

Network Intrusion Prevention System (IPS)



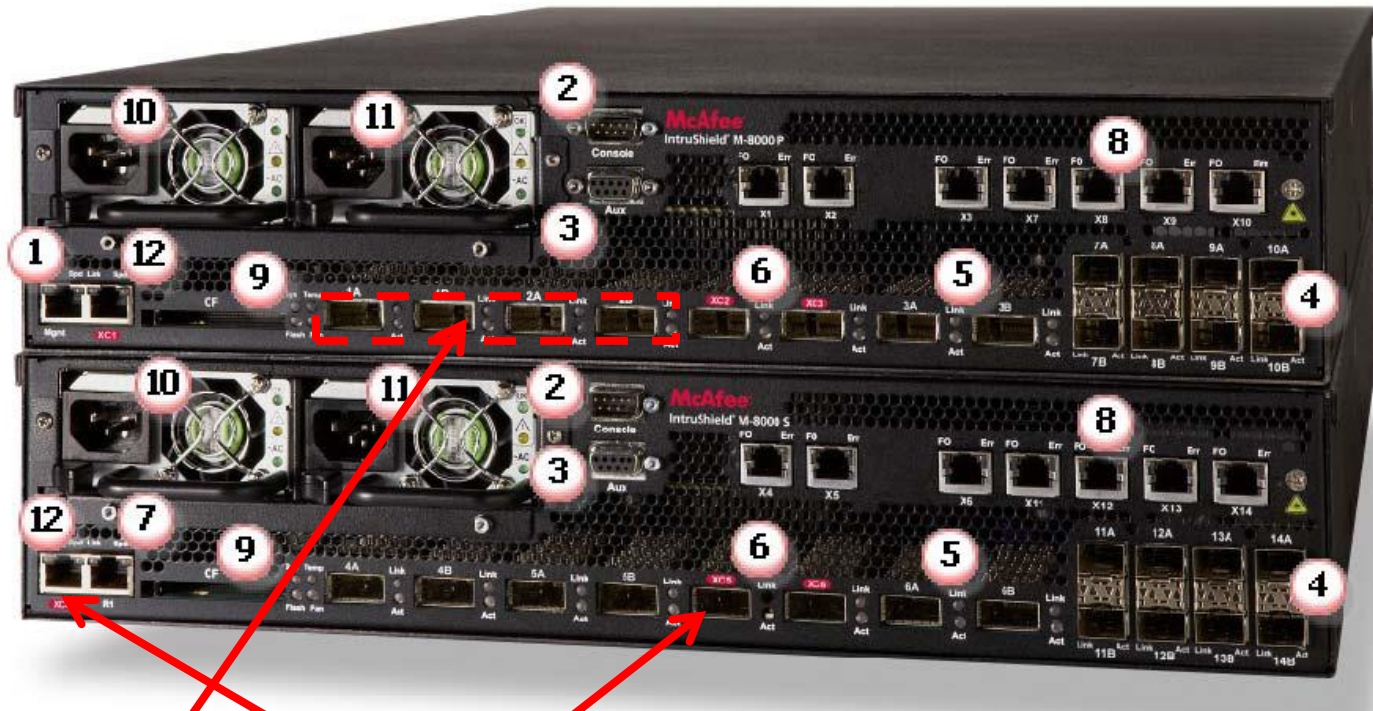
NTU BackBone Network @2011

transmitted in any form, or by any means without the prior written permission of the author.

Cisco SCE 8000

- NTU wants to have visibility into **application and subscriber usage patterns**, and the **capability to manage network bandwidth** and to **differentiate service offerings**.
- The Cisco SCE (Service Control Engine) 8000 is designed for high-capacity (10Gbps) **stateful application and session-based classification and management of all IP network traffic**.
- It is based on a patented architecture that employs **hardware acceleration with multiple high-speed RISC processors**.
- It can track and manage up to 32M concurrent **unidirectional application sessions over an IP network**.

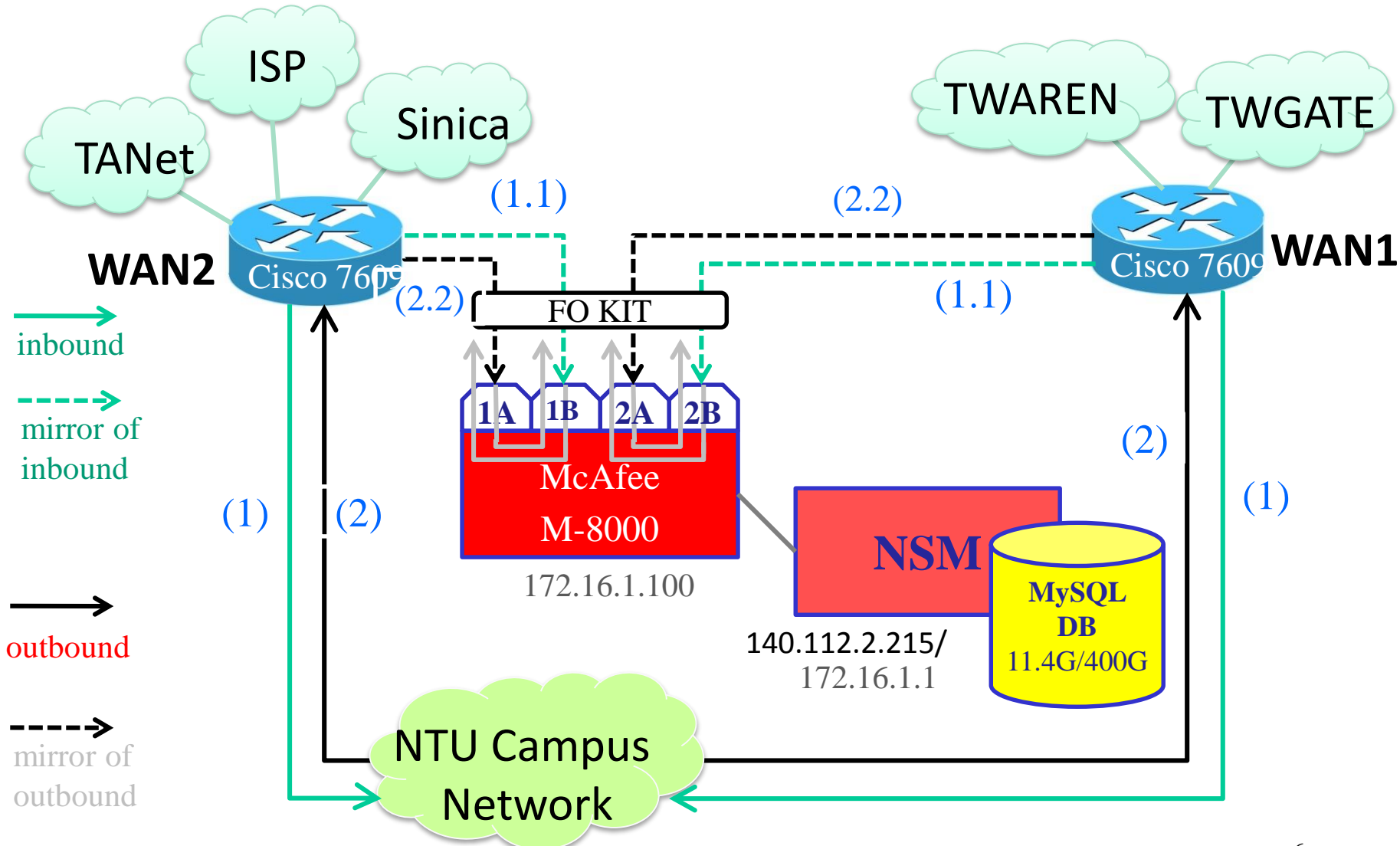
McAfee M-8000 (outer)



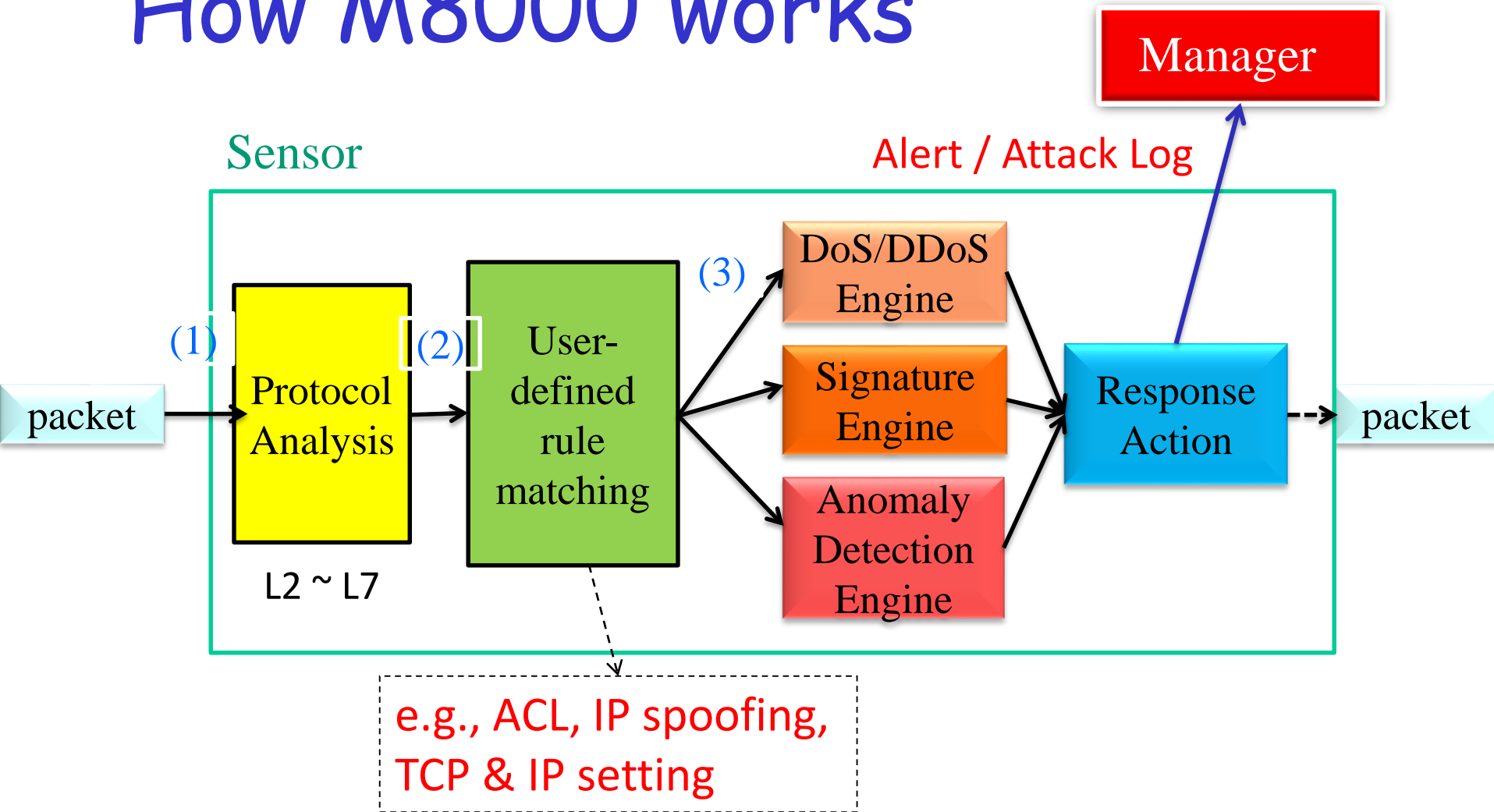
1. Management port (on M-8000 P only)
2. Console port
3. Auxiliary port
4. SFP Gigabit Ethernet Monitoring ports
5. XFP Gigabit Ethernet Monitoring ports
6. XFP Interconnect ports

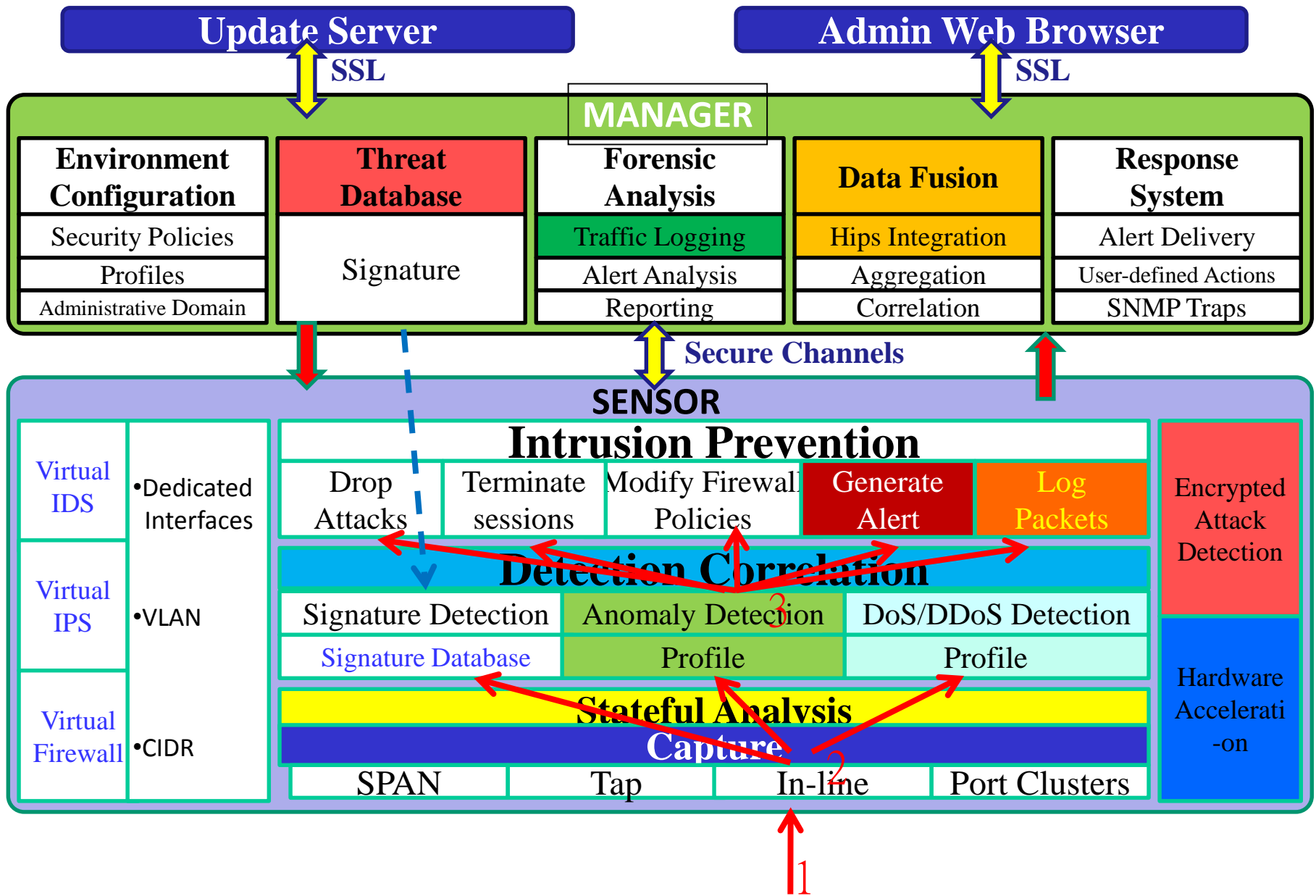
7. Response port (on M-8000 S only)
8. Fail-Open Control ports
9. External Compact Flash port
10. Power Supply A
11. Power Supply B
12. 10/100/1000 Interconnect ports

NSP deployment in NTU



How M8000 works





Security Operations Center (SOC)

Network Security Management

Intrusion Detection

Attack Analysis

Network Forensics

Notification


Recovery

TANET 北區A-SOC

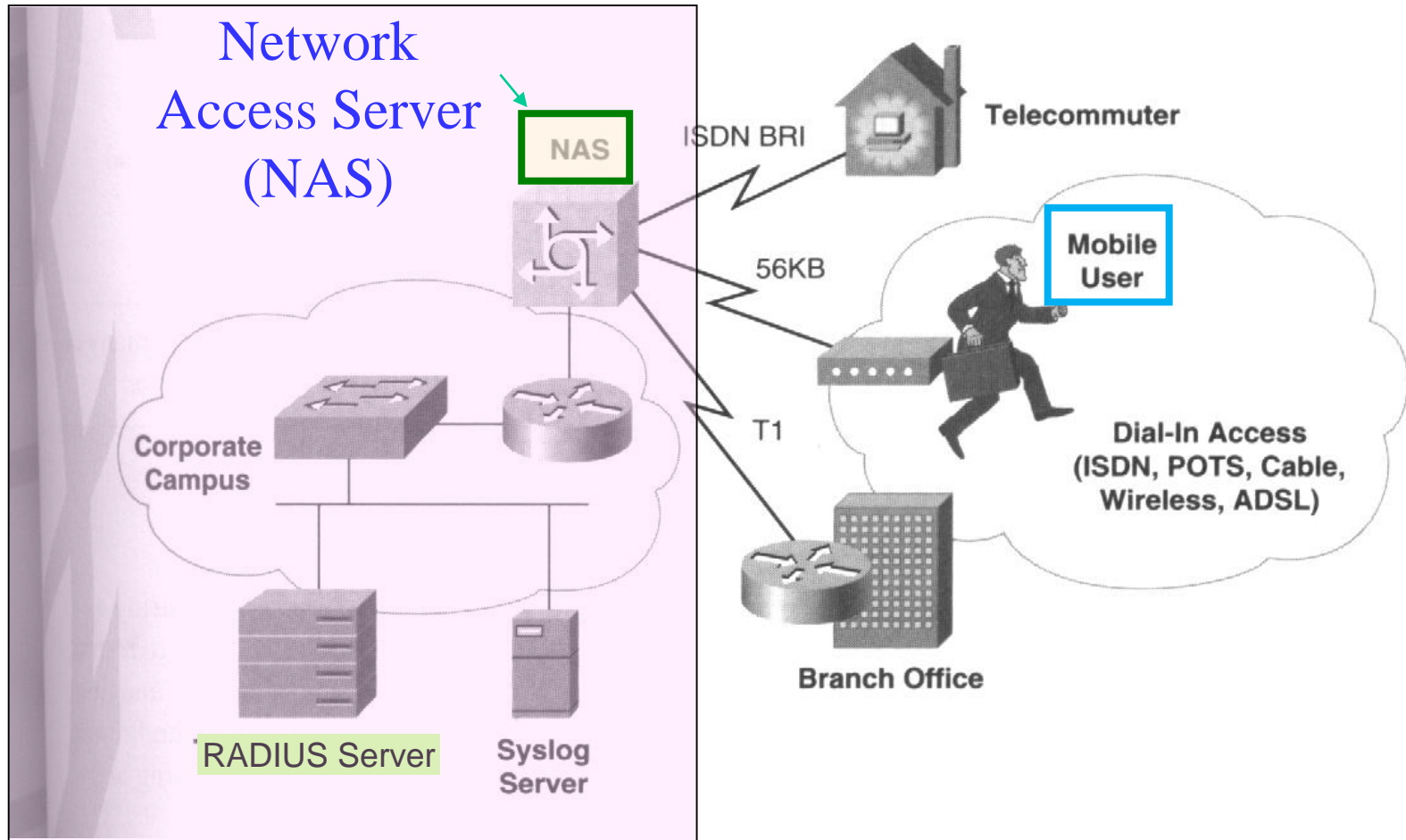
Comparisons

Firewall Capability	Packet filters	Application-level gateway	Stateful inspection
Communication Information	Partial	Partial	Yes
Communication-derived State	No	Partial	Yes
Application-derived State	No	Yes	Yes
Information Manipulation	Partial	Yes	Yes

Proxy Server with User Authentication

- Proxy server *challenges* a user initially at the application layer.
- May integrate with an industry-standard user authentication database, e.g.,
 - Terminal Access Controller Access Control System (TACACS)+
 - Remote Authentication Dial-In User Service (*RADIUS*) 
- Once passed, the firewall *shifts the session flow*, and all traffic thereafter flows directly between the two parties while maintaining session state, e.g., VPN.

Access from the Internet



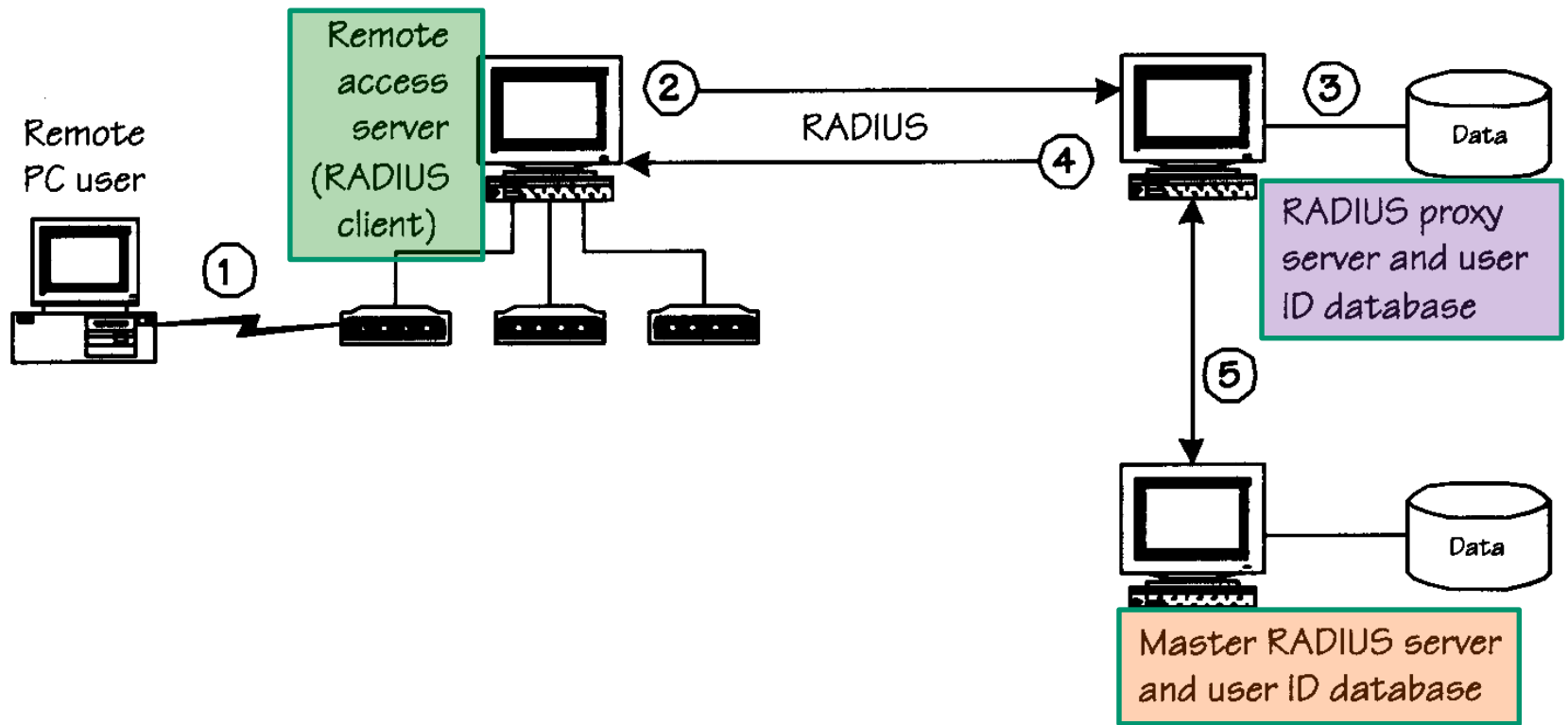
Remote Address Dial-In User Service (RADIUS)

RADIUS

- Remote Address Dial-In User Service (RADIUS)
- An access server authentication and accounting protocol
- RFC2058 (protocol specification) and RFC 2059 (accounting)
- Use UDP protocol
 - RADIUS implementation provides the functions of server availability, retransmission and timeouts

RADIUS (cont'd)

- A **client/server protocol**
 - client: Network Access Server (NAS)
 - server: a daemon process running on some UNIX or Windows machine
- Server can **act as a proxy** to RADIUS server



① User dials in to remote access server.

② Using the RADIUS protocol, the remote access server, a RADIUS client, sends requests for authentication/authorization to the proxy server.

③ The authentication server checks request against its user ID database.

④ Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access.

⑤ The Master RADIUS server periodically updates the user database in the proxy server as needed.



[Back](#)

FIGURE 6.6 Interactions among a RADIUS server, proxy server, and clients.

Bastion Host

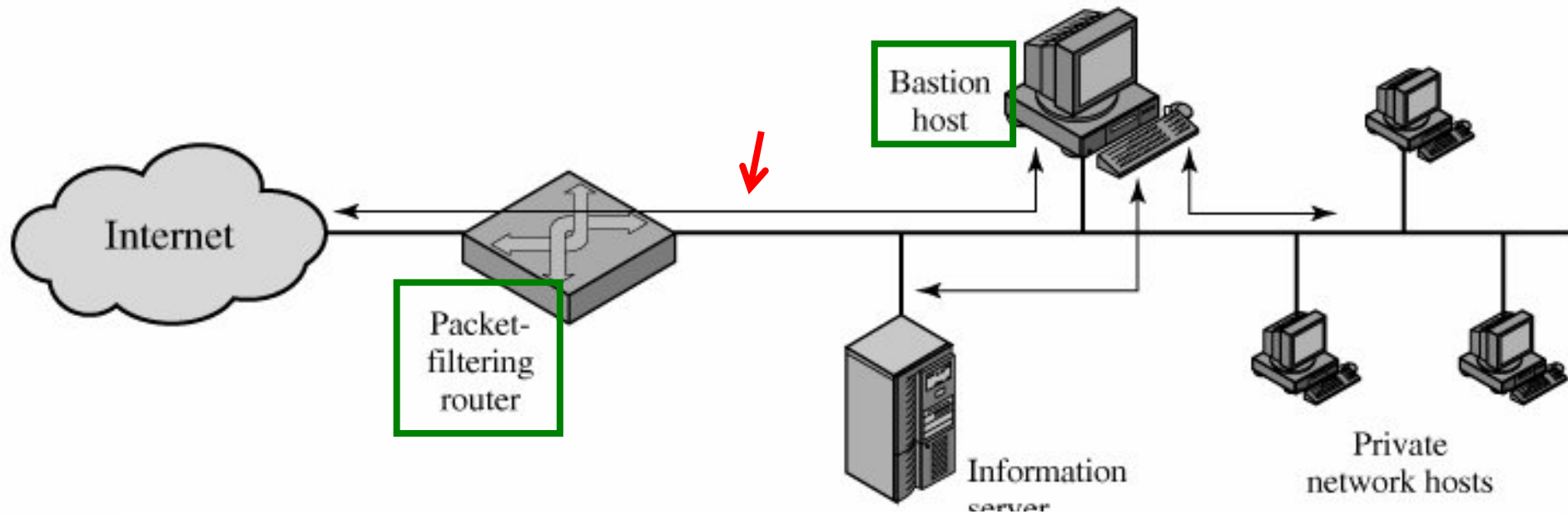
Bastion Host

- It is a system identified by the firewall administrator as a critical strong point in the network's security.
- It is suitable to serve as *application level gateways*

Bastion Host: Characteristics

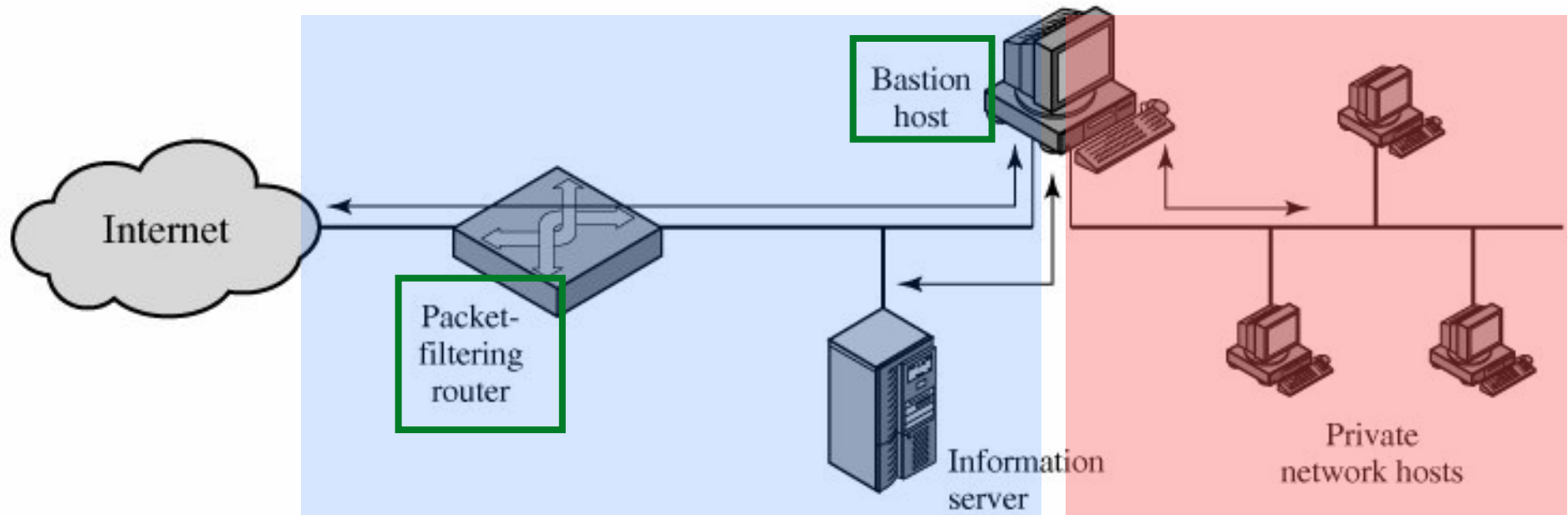
- Secure version of operating system
- Only the services that the network administrator considers essential are installed
- May require *user authentication* before a user is allowed to access to the proxy services.
- Maintains **detailed *audit*** info by logging all traffic, each connection and its duration.
 - **Audit log is important to discover and terminate intruder attacks.**
- Each proxy module is independent and separately managed.

Single-homed bastion host



- The router
 - for inbound traffic, only allows IP packets destined for the bastion host.
 - for outbound traffic, only allows IP packets sent from the bastion host.
- Bastion host: Authentication and proxy functions.
- They are on the same network
- If router is comprised, door is opened up.

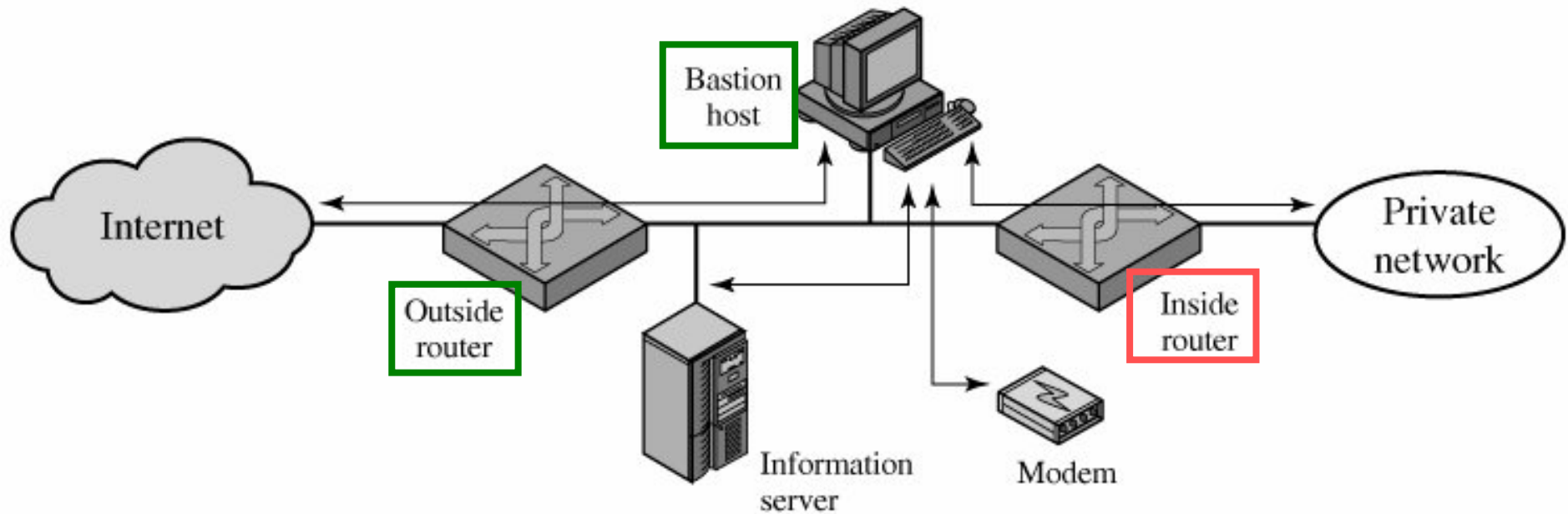
Dual-homed bastion system



(b) Screened host firewall system (dual-homed bastion host)

- Two physically separate networks
- Bastion host serves as a gateway

Screened subnet firewall



(c) Screened-subnet firewall system

- Two packet-filtering routers and a bastion host.

網路管理

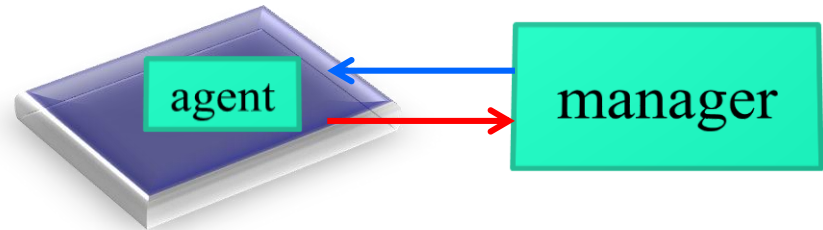
- **現今企業組織所面臨的問題:**
- 區域網路眾多節點中內，若懷疑某網段有異常情形時，多用「猜測」及「換換看」的除錯方式，完全無法達到網管效率
- 無線網路的架設，因無實體線路存在，若某網段有異常情形時，不知從何查起
- 無法即時針對網路流量進行分析，即時除錯

網路管理 (cont'd)

- 網路分析儀(Protocol Analyzer)
 - 網管模組及網路連接器
 - 當網管人員發現或懷疑某區段網路有異常時，
 - 可將Protocol Analyzer接上網路，
 - 即時的分析該網段的流量及資料封包，
 - 並藉由”專家系統”快速的找出網路問題所在，並獲得可能解決方法的提示
- Wireshark

網路管理 (cont'd)

■ RMON2的Agent



- 利用 **management station** 連接遠端的 **management agent** 進行跨網際的網路分析及除錯
- **MIB (Management Information Base)**
- 利用RMON作網路的使用分析，對於網路的長期使用規劃可以提供正確而有效的分析數據

Denial of Service (DoS) Attacks

Introduction

- Motivated by the widely known February 2000 distributed attacks on Yahoo!, Amazon.com, CNN.com, and other major Web sites.
- A denial of service is characterized by an explicit attempt by an attacker to **prevent legitimate users from using resources**.
- Even though denial of service attacks have existed for some time, their recent **distributed formats** have made these attacks *more difficult to prevent*.

Characteristics of DoS Attacks

- Examples of denial of service attacks include:
 - Attempts to “**flood**” a network, thereby preventing legitimate network traffic.
 - Attempts to disrupt connections between two machines thereby preventing access to a service.
 - Attempts to prevent a particular individual from accessing a service (consuming server's resources).
 - Attempts to disrupt service to a specific system or person.

Attacks that Exploit Vulnerability of TCP and IP Protocols!

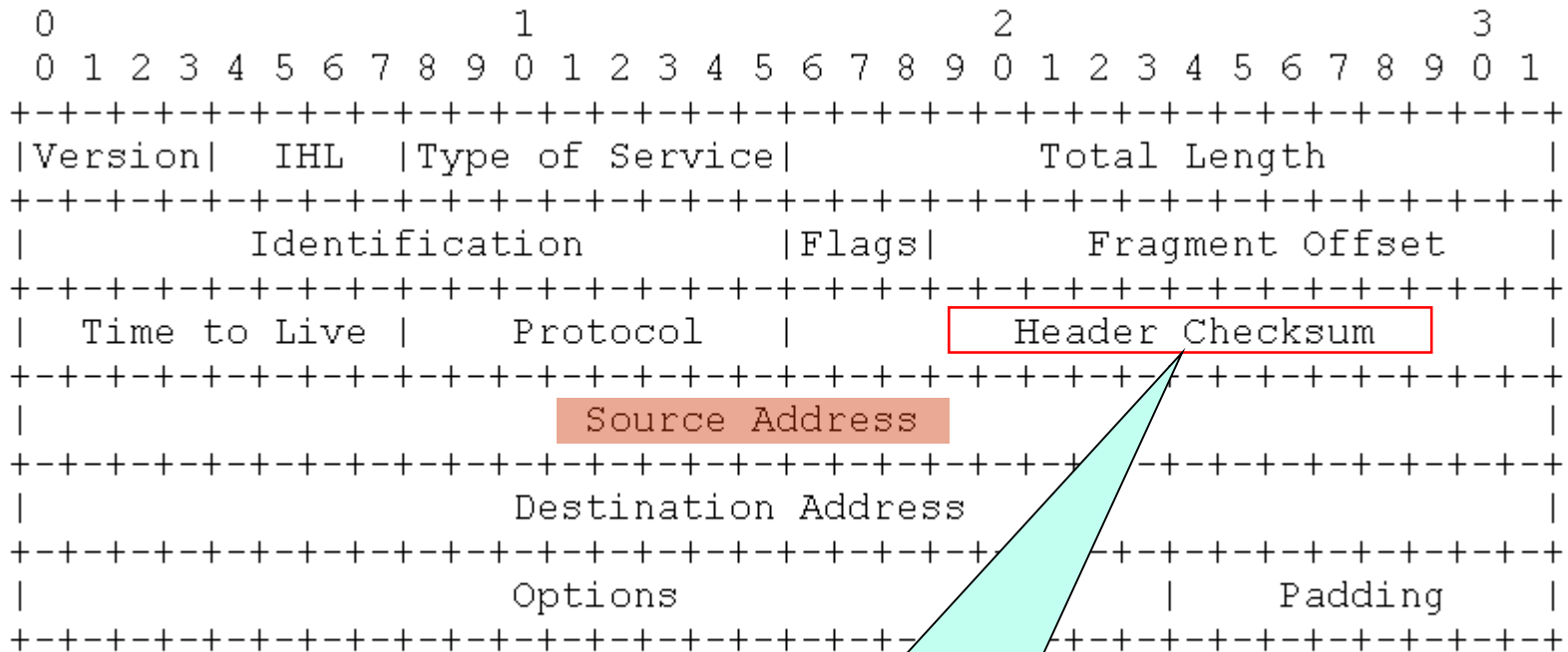
Example Attacks

- IP Spoofing Attacks
- Source Routing Attacks
- Tiny Fragments Attacks
- Stateful inspection
- Sequence number prediction
- TCP SYN flooding
- The Land Attack - IP DOS
- Snipping

Example #1: IP Spoofing Attack

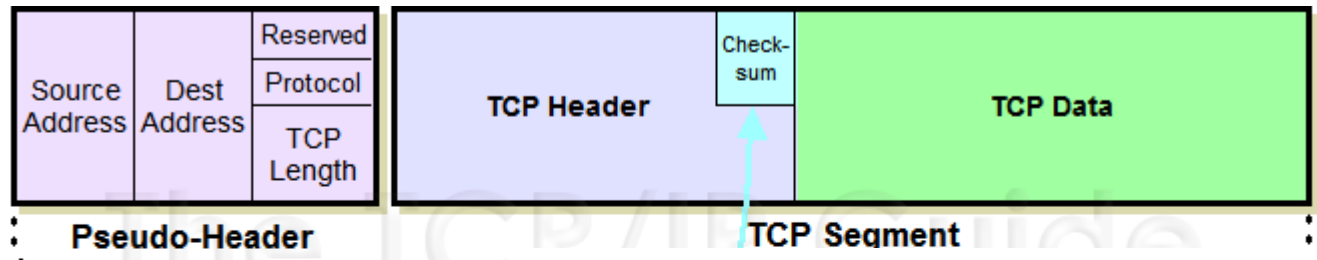
- Attacker 可以自行填寫送出的 IP packet 中 source address 的欄位。
- Victim 無法知道真正的攻擊來源。
- How to do IP spoofing?
 - Use raw socket
 - 自行算出該 raw packet 的 checksum，以避免被當成有問題的封包，而被 drop。

Example #1: IP Spoofing Attack - IP Header



Hacker 可自行
算出 checksum

Example #1: IP Spoofing Attack - TCP Header

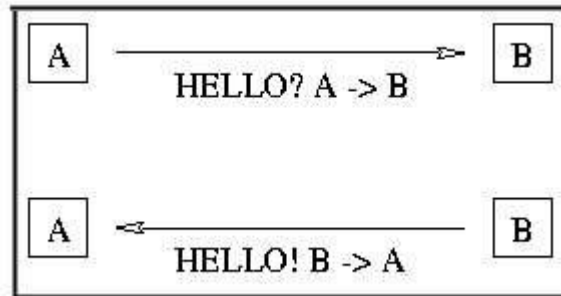


Checksum Calculated

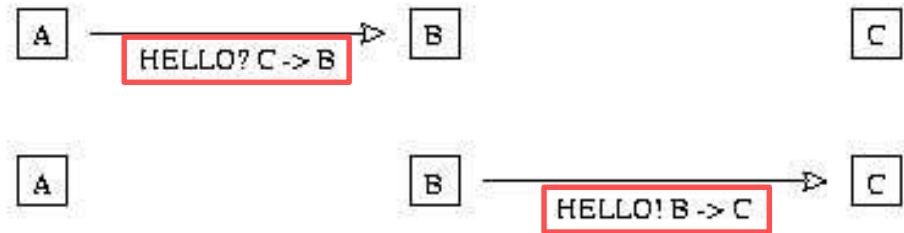
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
Source Port				Destination Port				Sequence Number				Acknowledgment Number			
Data Offset		Reserved		U A P R S F		Window		Checksum		Urgent Pointer		Options		Padding	
data															

Hacker 可自行算出 checksum

Example #1: IP Spoofed Denial-of-Service Attack - "Smurf" (1/4)

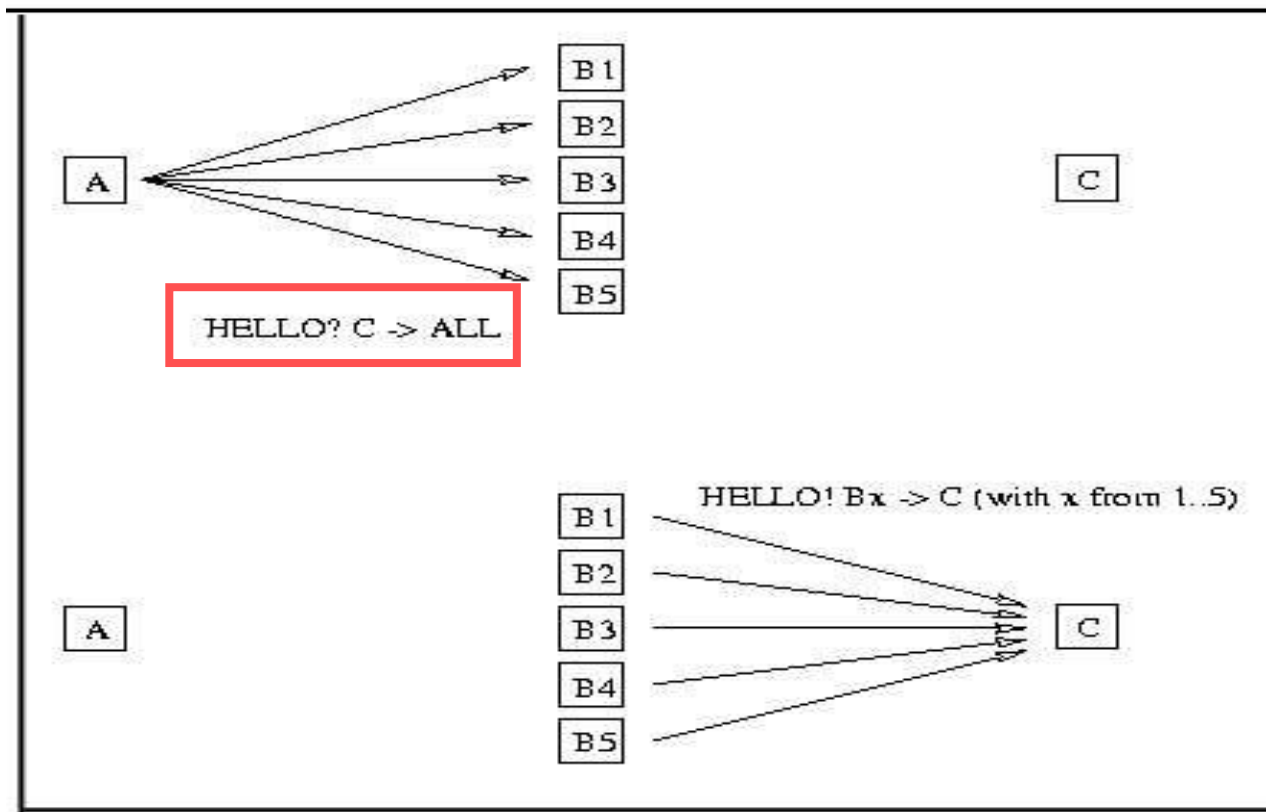


- Use forged ICMP echo request packets sent to IP broadcast addresses.
- The victim source is flooded with simultaneous replies (1998).



Example #1: IP Spoofed Denial-of-Service Attack - "Smurf" (2/4)

- Sending a large amount of ICMP echo traffic to a set of IP broadcast address with a specified spoofing source address.



Example #1: IP Spoofed Denial-of-Service Attack - auto tools (3/4)

- Automated tools are used to send attacks to multiple intermediaries (e.g., bots) at the same time.
- Causing all of the intermediaries to **direct their responses** to the *same victim*.
- Tools looking for potential intermediaries in attacks
 - *Routers* that do not filter broadcast traffic (broadcast/multicast storming) and *networks* where multiple hosts respond.

Example #1: IP Spoofed Denial-of-Service Attack - performance degradation (4/4)

- Both the **intermediary** and **victim** of the attack may suffer degraded network performance - **both on their internal networks or on their connection to the Internet**.
- Performance may be degraded to the point that the **network cannot be used, i.e. *denial of service***.

Example Attacks

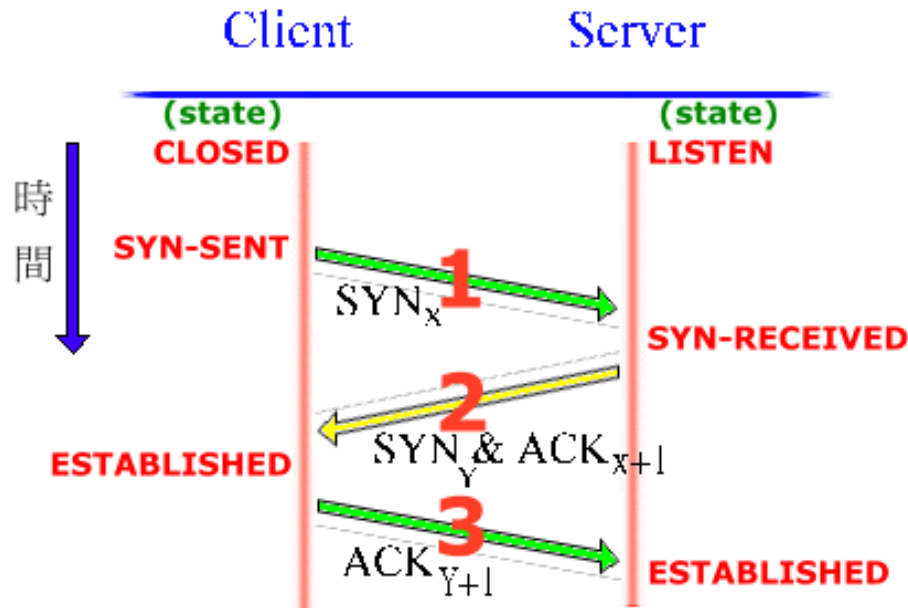
- IP Spoofing Attacks
- Source Routing Attacks
- Tiny Fragments Attacks
- Stateful inspection
- Sequence number prediction
- TCP SYN flooding
- The Land Attack - IP DOS
- Snipping

Example #2: IP-spoofed TCP SYN Flooding Attack

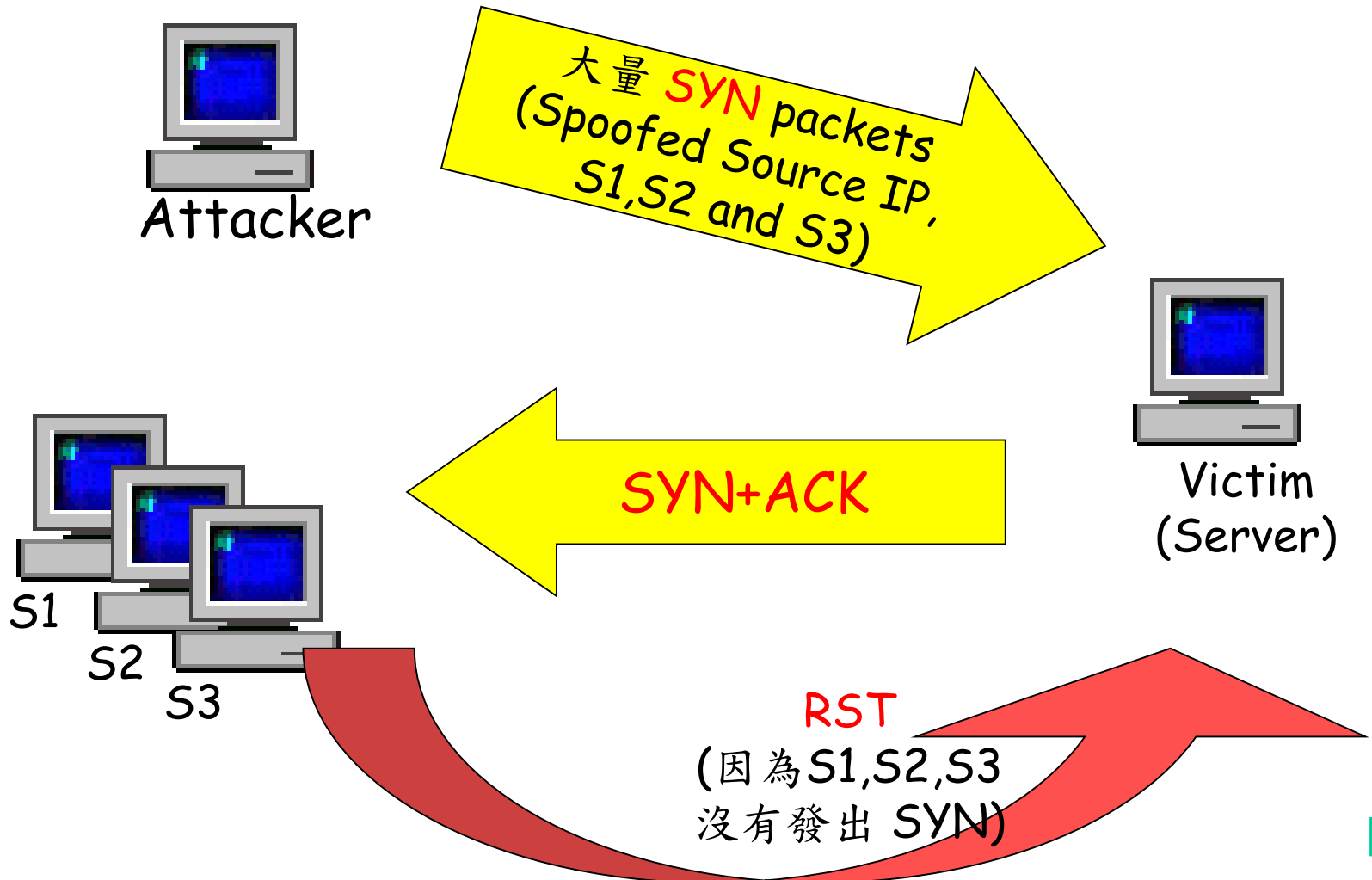
- **Any system** connected to the Internet and providing **TCP-based network services** (such as a Web server, FTP server, or mail server) is potentially subject to this attack.
- The attack itself is fundamental to the TCP protocol used by all systems.

Example #2: IP-spoofed TCP SYN Flooding Attack

TCP connection establishment



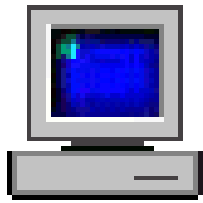
Example #2: IP-spoofed TCP SYN Flooding Attack - case 1



Example #2: IP-spoofed TCP SYN Flooding Attack - case 2



大量 **SYN** packets
(Spoofed Source IP,
V1, V2 and V3)



不在使用的IP



SYN+ACK

S1, S2, S3
此時不存在
Internet 上

持續等待
S1, S2, S3的
RST or ACK

Example #2: IP-spoofed TCP SYN Flooding Attack

- 大量的 SYN packet 送往攻擊主機
- 被攻擊主機通常會保留 SYN 5~15個連線
- 連線通常會被保留在系統的queue中，等待連線成功，或者等到timeout時間到達（一般為75秒）
- 假如系統接收 connection 的 buffer 滿了，則新進來的 SYN 會被 drop 掉

Example #2: IP-spoofed TCP SYN Flooding Attack

- Attacker 要在送出的 SYN packet 上 spoof 來源 IP，而且這個 IP 要是當時沒有機器使用的 IP。
 - Victim 會對 spoofed source IP 回 SYN+ACK。
 - 如果 spoofing 的 IP 存在，則會回 RST。Victim 收到 RST 會將 queue 中的 SYN 清除 ([example 1](#))。
 - 如果 spoofing 的 IP 不存在，則 victim 則會等候，造成 DoS ([example 2](#))。
- 因此，選擇當時沒有機器在使用的 IP，可以讓 victim 收不到 RST，而持續等待正常的 ACK，造成 victim 資源浪費。



Example Attacks

- IP Spoofing Attacks
- Source Routing Attacks
- Tiny Fragments Attacks
- Stateful inspection
- Sequence number prediction
- SYN flooding
- The Land Attack - IP DOS
- Snipping

Example #3: The Land/ Latierra Attack

- **Attacker** sends a packet to a **victim machine** with the **source host/port the same as the destination host/port (IP Spoofing)**.
- Victim 收到此來源與目的位址相同的封包時，會無法正常處理。
- 因為各家作業系統對於這個部分的 implementation 不同，造成不同結果：
 - Crash/hang
 - Slow down
- 防止方法：安裝各系統提供的修正更新檔案。

Example Attacks

- IP Spoofing Attacks
- Source Routing Attacks
- Tiny Fragments Attacks
- Stateful inspection
- Sequence number prediction
- SYN flooding
- The Land Attack - IP DOS
- Snipping

Example #4: Snipping

- 假設在同一網路上， X 與 Y 透過網路在通訊，同時 A 正在竊聽之間的訊息
- A 可以得到 X 或 Y 的 TCP sequence number
- 接著 A 送出含有正確的 TCP sequence number 的 **RST packet** 到 X 或 Y
(spoofed IP packet with X or Y)
- 將導致原本 X 與 Y 之間的連線中斷 – **cut off (snip) an on-going TCP connection**

Denial of Service

依照攻擊模式分類：

■ 頻寬阻絕

- UDP Flood Attack
- ICMP Flood Attack
- ICMP Smurf Flood Attack

■ 伺服器癱瘓

- TCP SYN Attack
- File/Socket Descriptor, CPU, Disk, Process
使用過量

■ 這些攻擊，通常都會將自己的來源 IP 隱藏 (IP Spoofing)。

Distributed Denial of Service Attacks

DoS and DDoS

■ Denial of Service (DoS) :

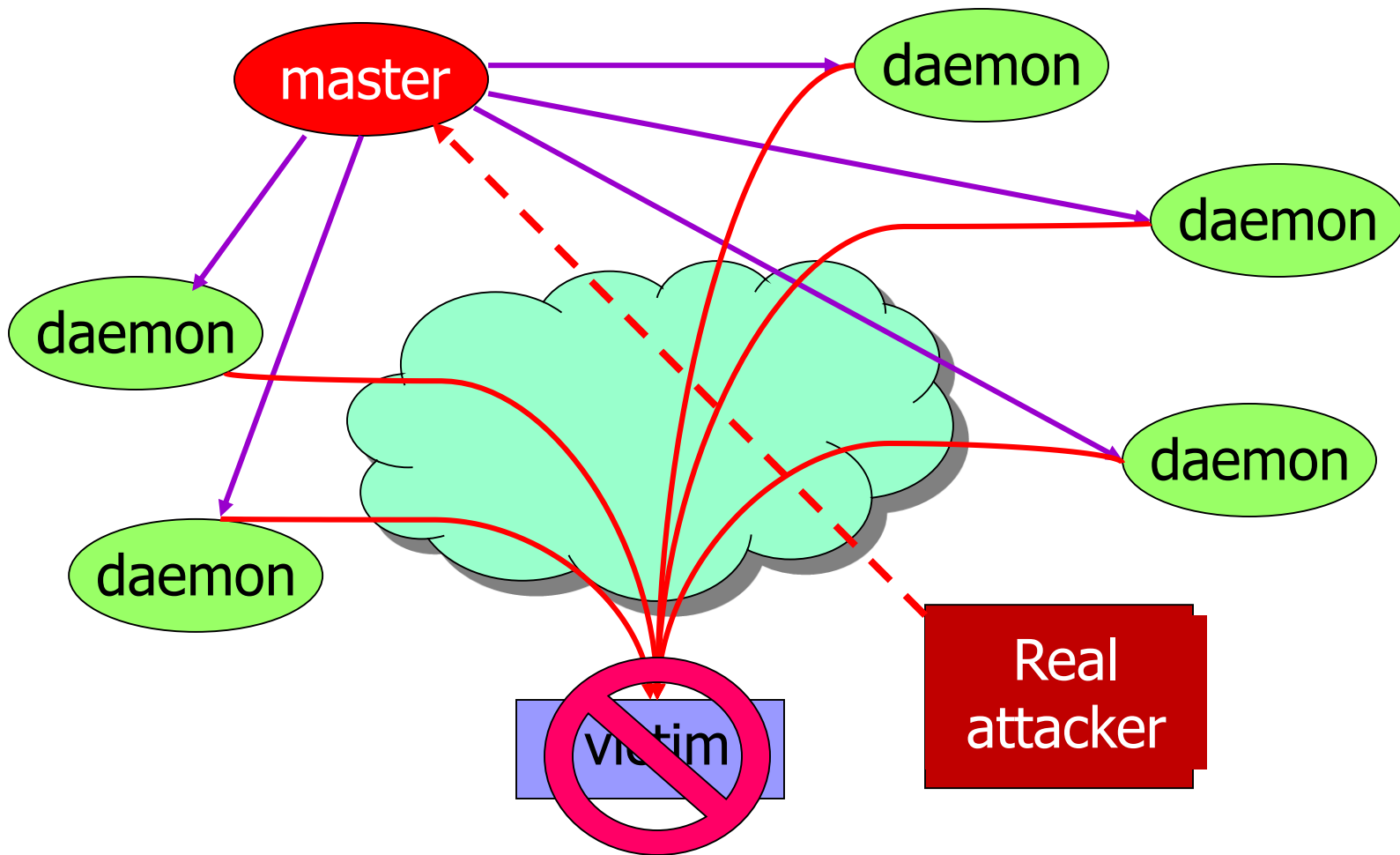
- 這種情形就如同某公司電話總機**同一時間被一個人**，不停的撥進電話，佔據有限的線路，導致其他正常使用者沒辦法接通。

■ Distributed DoS (**分散式阻絕服務**) :

- 這種情形就如同某公司電話總機**同一時間被一群人**，**從各地**不停的撥進電話，佔據有限的線路，導致其他正常使用者沒辦法。

Distributed Denial of Service (DDoS)

- Tools utilize distributed technology to *create large networks of hosts* capable of launching *large coordinated packet flooding* denial of service attacks.
- Examples
 - Trinoo
 - Tribe flood network (TFN)
 - Stacheldraht
 - Shaft
 - TFN2K
 - etc.



The *four* components of a distributed denial of service attack: a real attacker, a control master program, attack daemon and the **victim**

A DDoS attack is composed of four elements ...

■ Victim

- The **target host** that has been chosen to receive the brunt of the attack.

■ Attack daemon agents

- These are agent programs that **actually conduct the attack** on the target victim.
- Deploying these attack daemons requires the attacker to *gain access* and infiltrate (break through secretly) the host computer.

■ Control master program

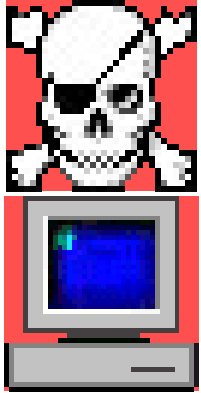
- Its task is to **coordinate the attack**.

■ Real attacker

- By using a control master program, the real attacker can stay behind the scenes of the attack.

DDoS Attack (1/4)

Hacker



Master Server



Agents

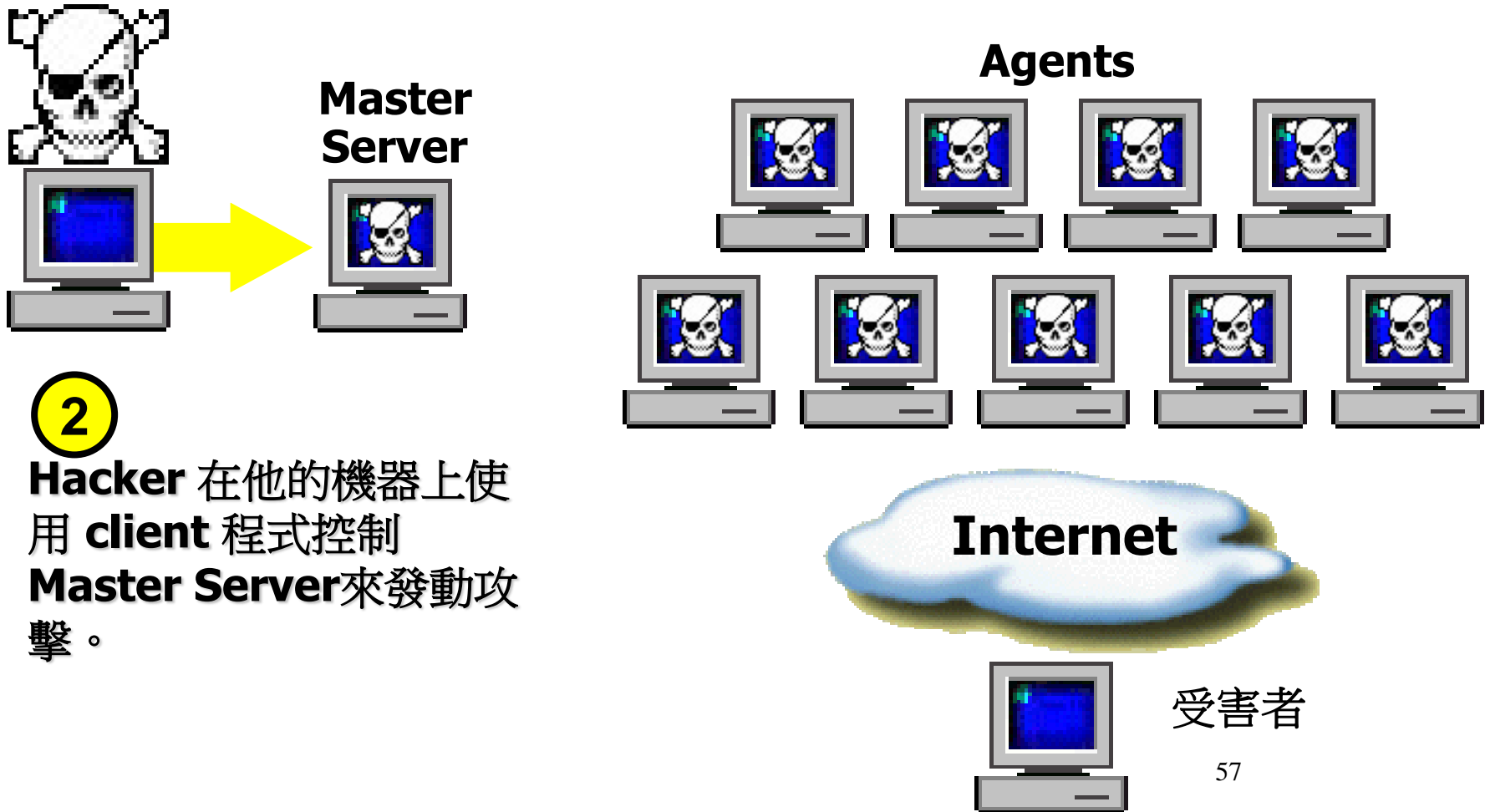


1

Hacker 選定一台 **Master Server** 來對 **Agents** 下達攻擊指令，以發動攻擊。

其中 **Agents** 與 **Master Server** 是預先透過入侵主機方式取得非法使用權限。並且置入相關攻擊程式。用來接受攻擊指令。

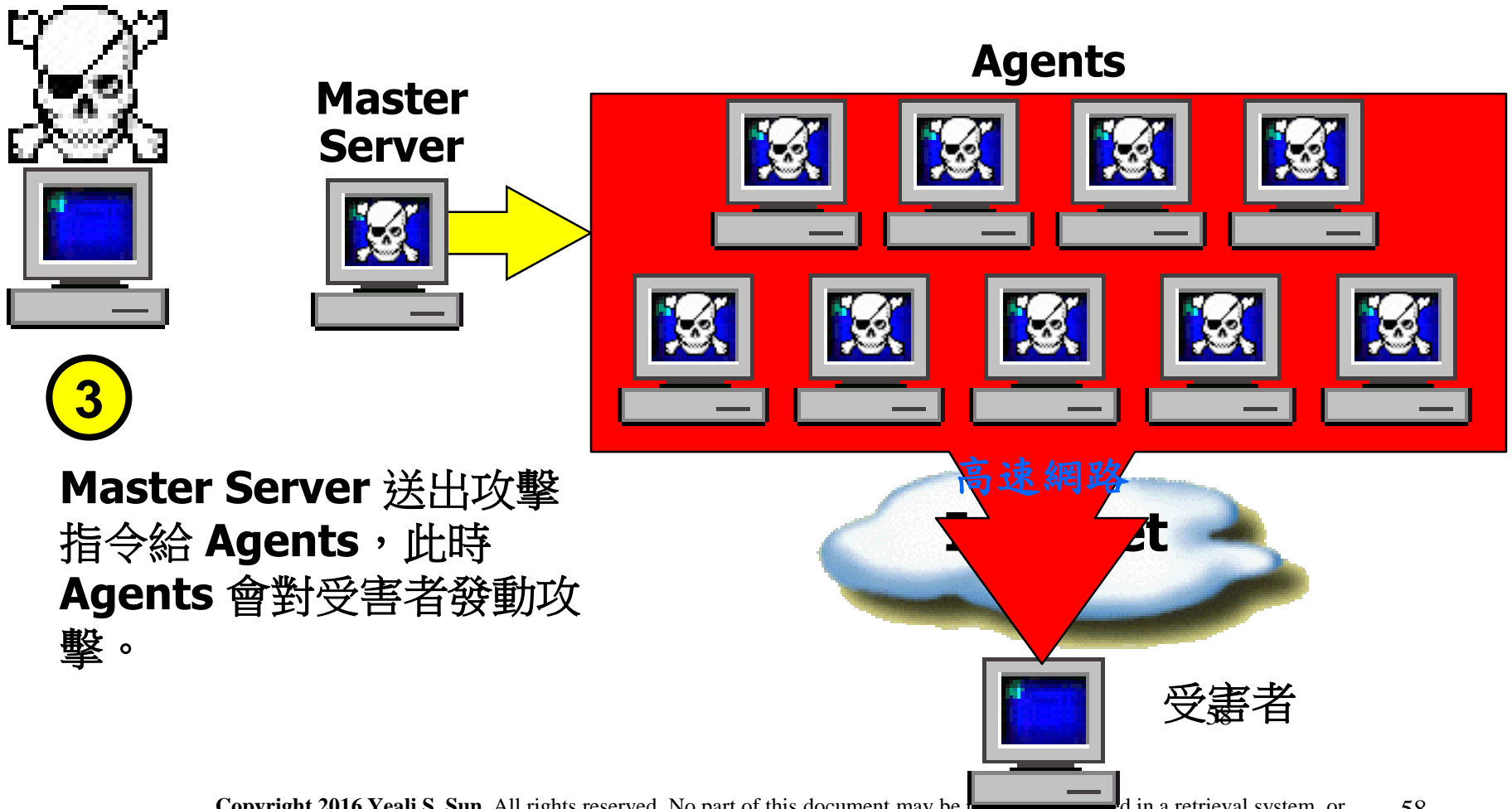
DDoS Attack (2/4)



2

Hacker 在他的機器上使用 **client** 程式控制 **Master Server** 來發動攻擊。

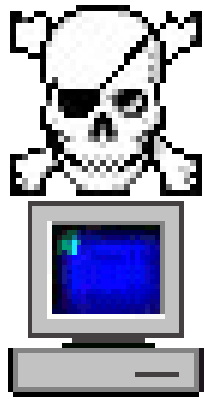
DDoS Attack (3/4)



3

Master Server 送出攻擊指令給 **Agents**，此時 **Agents** 會對受害者發動攻擊。

DDoS Attack (4/4)



Master Server



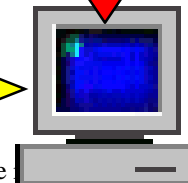
Agents



4 受害者此時無法對正常使用者提供任何的服務。



Request Denied



受害者

正常使用者

Copyright 2016 Yeali S. Sun. All rights reserved. No part of this document may be reproduced in any form, or by any means without the prior written permission of the author.

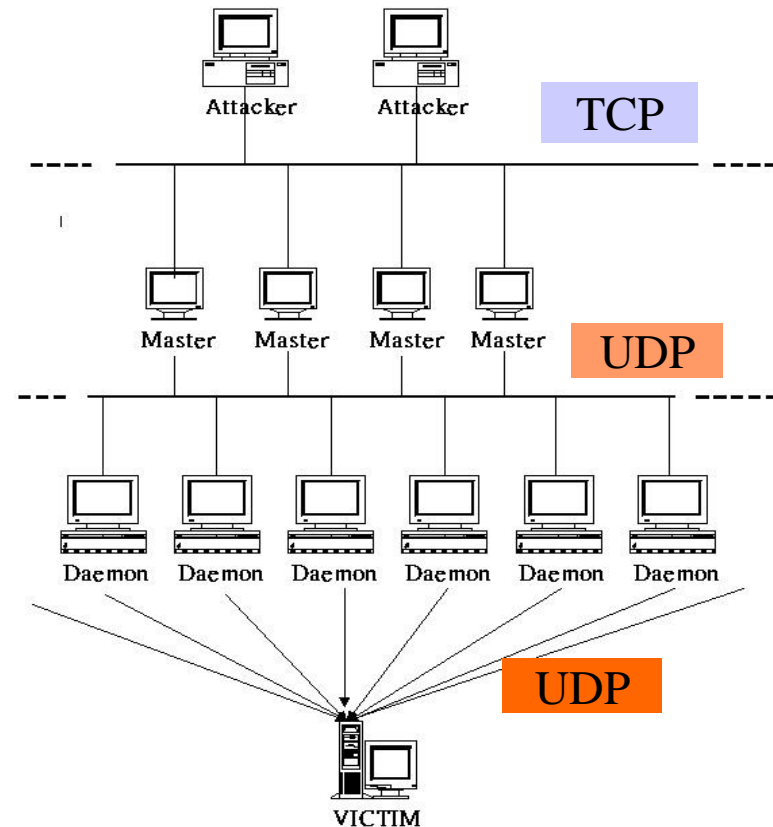
Attack scenario

- **Attacker -> Master** : “execute” message
 - **Master -> Daemons** : command
 - **Daemons -> Victim** : attack
-
- The attacker must study the **target’s network topology** and search for *bottlenecks* and *vulnerabilities* that can be exploited during the attack.

Trinoo: UDP DDoS

Scenario

- An intruder connects to a trinoo master and instructs that master to launch a denial of service attack against one or more IP addresses.
- The trinoo master communicates with the daemons giving instructions to attack one or more *IP addresses* for a specified *period of time*.
- intruder --> master; destination port 27665/tcp
- master ---> daemons; destination port 27444/udp
- daemons ---> UDP flood to target with randomized destination ports



DDoS Attacks (1/2)

■ TFN:

A $\xrightarrow{\text{TCP, UDP, ICMP}}$ M $\xrightarrow{\text{ICMP echo reply}}$ D \Rightarrow

UDP Flood

SYN Flood

Smurf

ICMP Flood

■ Stacheldraht:

A $\xrightarrow{\text{TCP (encrypted)}}$ M $\xrightarrow{\text{TCP, ICMP}}$ D \Rightarrow UDP Flood, SYN Flood
ICMP Flood, Smurf

DDoS Attacks (2/2)

- Shaft:

$A \xrightarrow{\text{TCP}} M \xrightarrow{\text{UDP}} D \Rightarrow \text{UDP Flood} \cdot \text{SYN Flood}$
 $\text{ICMP Flood} \cdot \text{Smurf}$

- It has the ability to switch control master servers and ports in real time.

- TFN2K:

$A \xrightarrow{\text{TCP} \cdot \text{UDP} \cdot \text{ICMP}} M \xrightarrow{\text{TCP} \cdot \text{UDP} \cdot \text{ICMP}} D \Rightarrow \text{Smurf}$
(encrypted by a key-based CAST-256)

UDP Flood
SYN Flood
ICMP Flood

Case Study: Attack on Router

Distributed Denial of Service (DDoS)

Google: Project Shield

How can Google's infrastructure support free expression?

Project Shield

Motivation

- Every day, independent news, human rights, and election monitoring sites around the world are taken offline and silenced by attacks on their servers.
- Google offers free DDoS mitigation services to protect websites at risk and keep them online.

Google: Project Shield



Products

Our Users

Vision

We build products to help people
under digital attack

Explore **Project Shield**



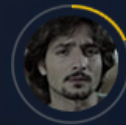
Mariam Memarsadeghi

SOCIAL ENTREPRENEUR



We build products to help people defend against hackers

Discover **Password Alert**



Dishad Othman

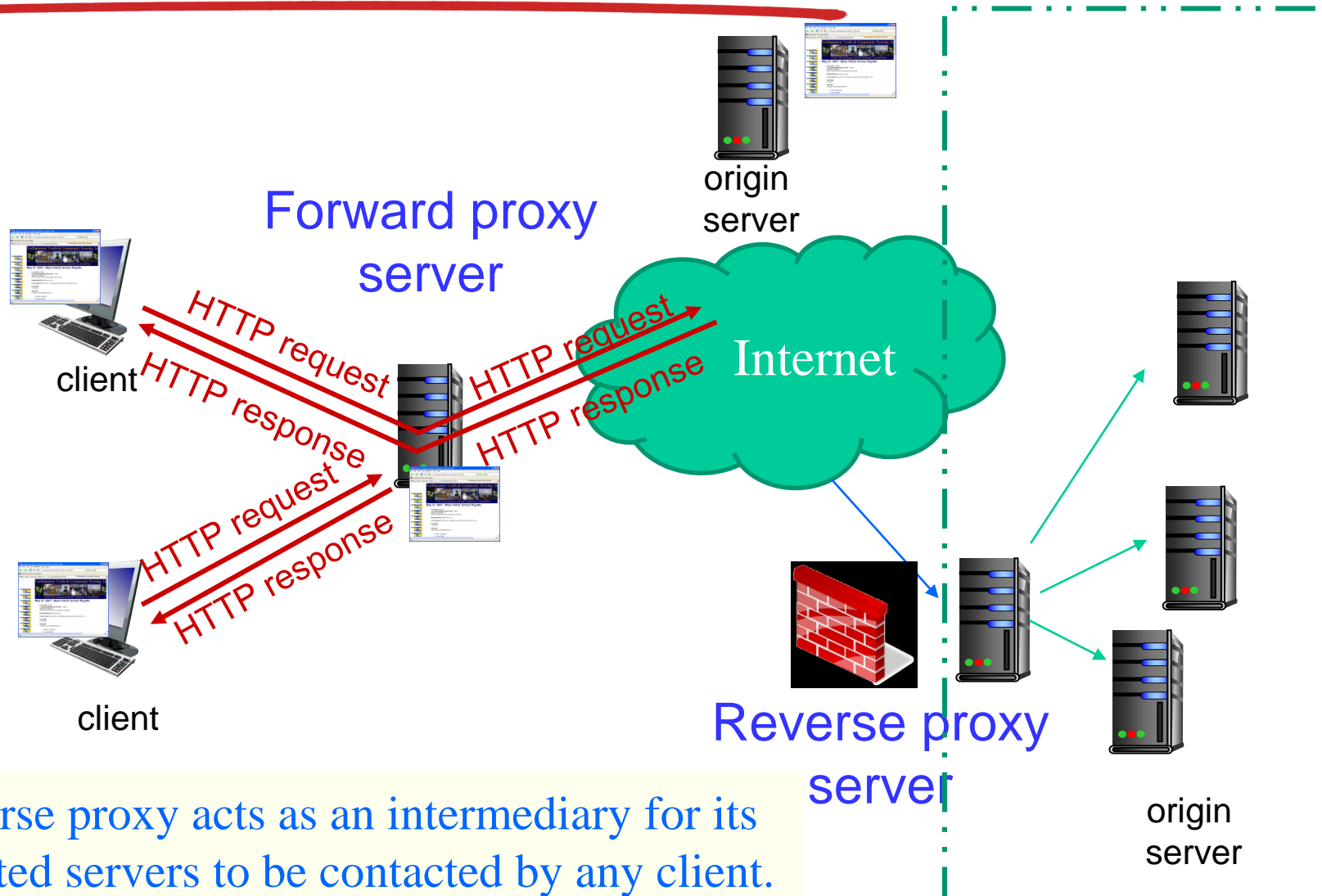
INFORMATION SECURITY EXPERT



Google Shield

- Using **reverse proxy** technology.
- It allows a **webmaster** to serve their site **through Google infrastructure** for free, providing a “**shield**” against would-be attackers.

Reverse Proxy Servers



✓ A reverse proxy acts as an intermediary for its associated servers to be contacted by any client.

Project Shield: Anti-DDoS Services

Built on Google's PageSpeed service, a frontend tool that offers developers faster loading times (CDN-like service)



- Sites hosted by Project Shield would *sit behind PageSpeed's infrastructure*, allowing Google to pool resources if any one site fell, victim to an attack.
- **Unless an attack were strong enough to bring down all the PageSpeed sites, it wouldn't be able to bring down any of them.**
- **Cloudflare** - Offers CDN, DNS, DDoS protection and security.

BUYING ATTACKS

香港公投網站DDoS攻擊內幕大公開，連Google、亞馬遜都擋不住

According to **TrendMicro Research** you can buy a week-long DDoS attack on the black market for \$150. And it's only getting cheaper.

2014.6.22 香港民間全民投票 (622公投)

- 讓愛與和平佔領中環（「和平佔中」）
- 促進真普選，委託香港大學民意研究計畫舉辦一次民間全民投票，選出一個行政長官選舉方案。

香港公投防禦DDoS攻擊: Project Galileo (1/3)

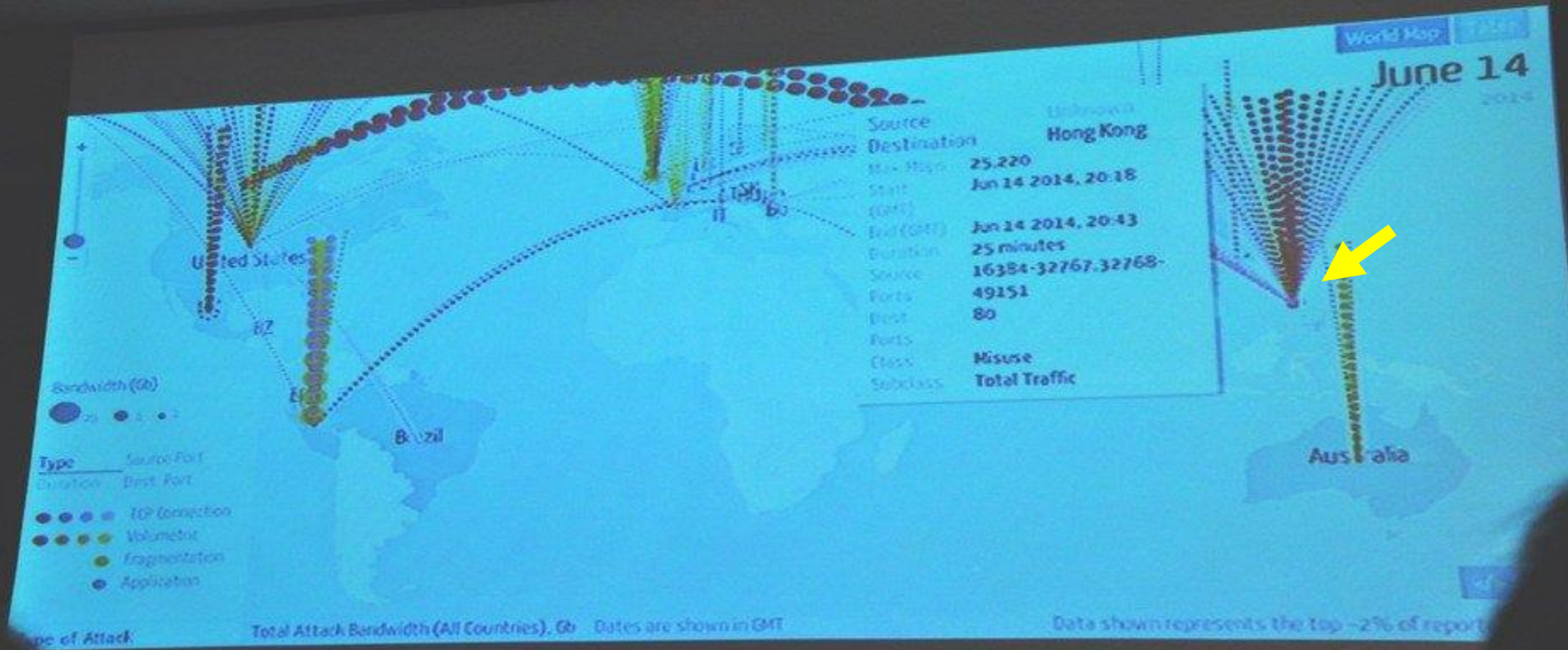
- 2014年六月二十日香港公投投票第一日。
- 投票一開始，PopVote 投票網站（popvote.hk）就遭遇到了**超大規模的DDoS攻擊**，攻擊流量達網路史上第二高。
- 早在投票前幾天，PopVote就遭受到**一波大規模DDoS攻擊**，為了避免影響為期多日的正式投票過程，負責提供線上投票系統的PopVote網站向**Cloudflare**團隊求助。

香港公投防禦DDoS攻擊: Project Galileo (2/3)

- Cloudflare使用亞馬遜的AWS雲端服務，加入抵禦攻擊的行列
- 但此時PopVote網站已遭受到大量DDoS攻擊，包括出現DNS及NTP（Network Time Protocol）[reflection attacks](#)。
- 在6月17日甚至出現網路攻擊流量最高峰，一度達到**每秒150Gb**。最後，AWS服務也因無法應付大量攻擊流量而終止提供服務。

香港公投防禦DDoS攻擊： Project Galileo (3/3)

- Cloudflare 找Google。
- Google的工程團隊以自家的Project Shield 攻擊防禦解決方案，作為PopVote網站第二層的DDoS防禦機制。
- 但，最後，因為網路攻擊流量過於龐大而影響Google其他服務，以致於最後不得不宣布退出。
- Cloudflare 最後靠著全球網路服務業者聯手，才撐過了這10天投票過程。



根據Google 2014/6/14 偵測到的全球網路總攻擊頻寬顯示，鎖定PopVote網站的網路攻擊活動，遍及世界各地，以各種DDoS攻擊手法，如DNS、NTP進行大規模網路流量的癱瘓攻擊。



DNS Reflection Attack (1/4)

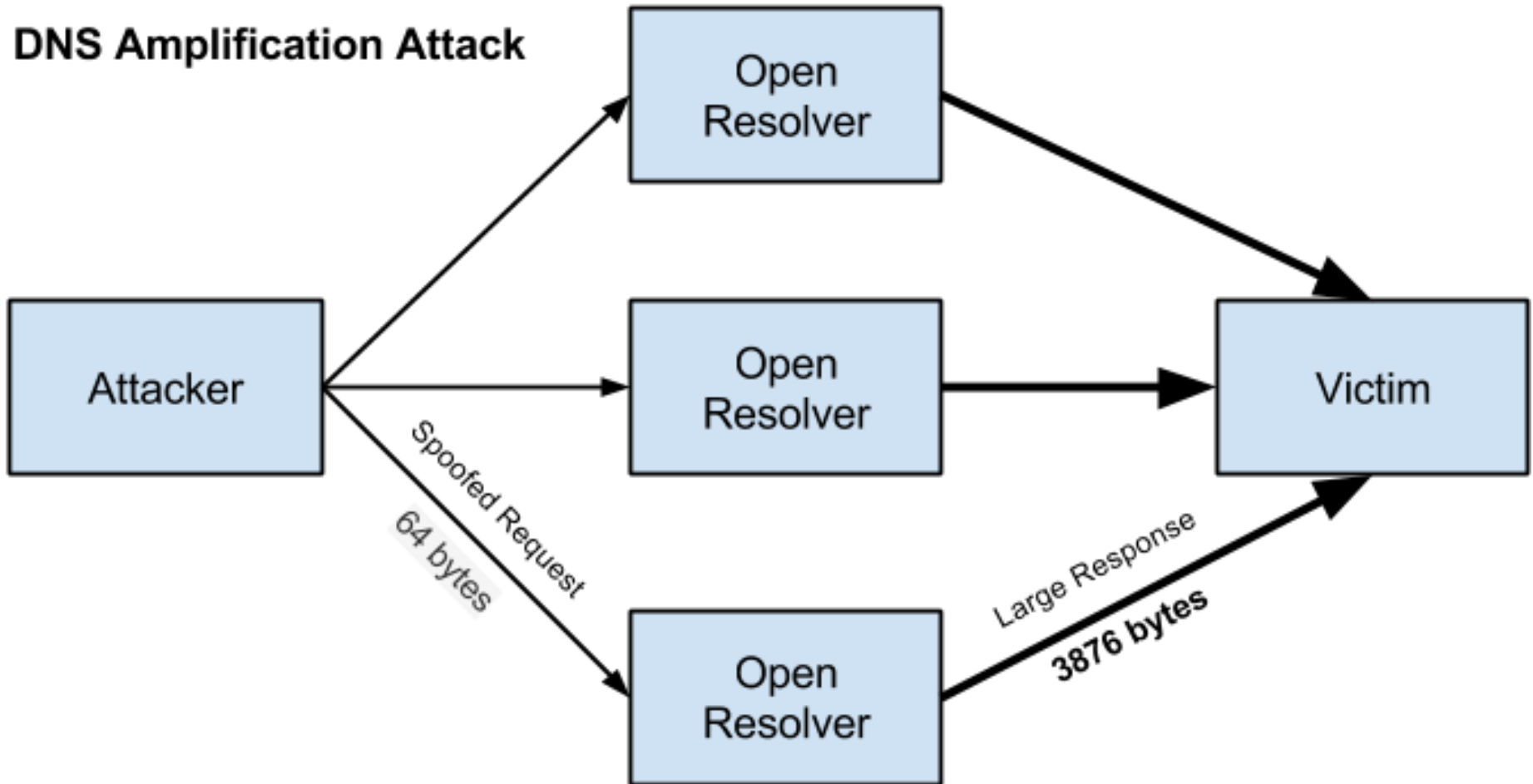
How DNS works?

- Two categories of name server: the **authoritative name server** and the **recursive name server**.
- An *open resolver* is a category of resolver that will answer recursive queries from any client, not just those local to them.
- UDP packets

DNS Reflection Attack (2/4)

- To conduct an attack:
 1. An adversary sends a set of spoofed DNS queries to open resolvers with **forged source address (some chosen targets)**.
 2. The requests are designed to have **much larger responses** (e.g., using an ANY request, a 64 byte request yields a 512-byte response), thus resulting in the **recursive name servers sending about 8 times as much traffic** at the **target**. (DNS amplification attacks)

DNS Amplification Attack



DNS Reflection Attack: ANY Request (3/4)

- Attackers often issue a special type of DNS request called an ANY request.
- ANY requests ask the DNS resolver for **ALL information that it currently knows about the domain** which may include where the mail servers are (MX records), what the IP addresses are (A records) and so on.

DNS records

DNS: distributed db storing resource records (RR)

RR format: (name, value, type, ttl)

type=A

- **name** is hostname
- **value** is IP address
- `dns1.networkutopia.com,`
`212.212.212.1, A)`

type=NS

- **name** is domain (e.g.,
foo.com)
- **value** is hostname of
authoritative name server
for this domain

type=CNAME

- **name** is alias name for some
“canonical” (the real) name
- `www.ibm.com` is really
`servereast.backup2.ibm.com`
- **value** is canonical name

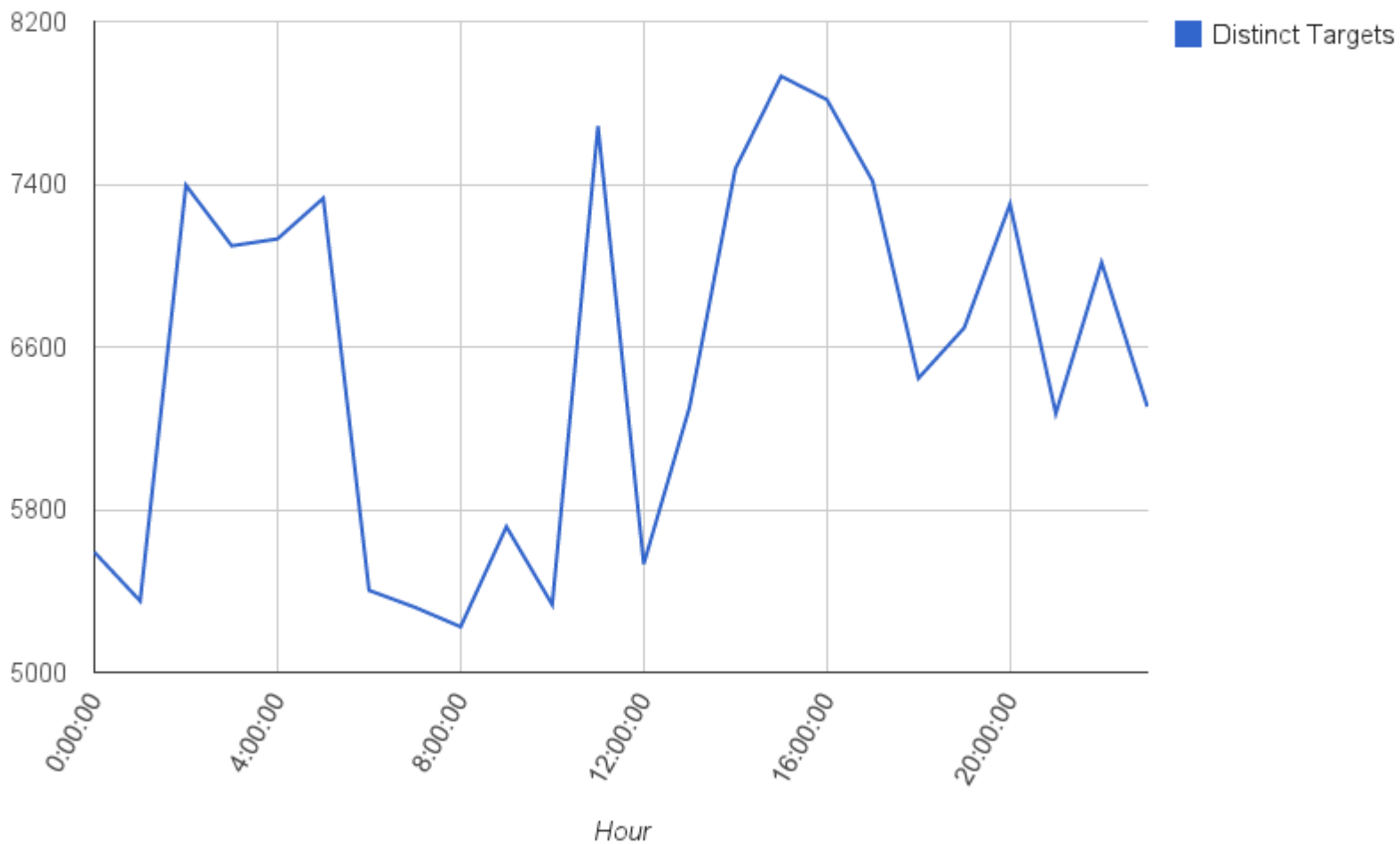
type=MX

- **value** is name of mailserver
associated with **name**

DNS Reflection Attack (4/4)

- Take advantage of three things:
 - the **forgeability** of UDP **source addresses**
 - the availability of **open resolvers**, and
 - the **asymmetry** of DNS requests and responses.

Amplification Attacks Over 24 Hours



DDoS Attack Analytics (1/2)

- For example, Cisco is one of the world's largest open DNS resolvers.
- They are constantly on the lookout for abuse of their service, especially when it means they would be taking part in an attack against other networks.
- Using their analytics platform, they can outline the
 - exact domains used in these attacks,
 - how long the attack lasted,
 - who the intended victims were and
 - the intended size of the attack.

DDoS Attack Analytics (2/2)

- They also estimate the approximate source location of the attacks even though the packets are spoofed.
- They use Anycast, a networking technology, to route customer requests to the nearest **OpenDNS resolver** in one of Cisco's datacenters around the globe.
- They use this metric to estimate how distributed the attack is.

- See more at: <https://blog.opendns.com/2014/03/17/dns-amplificationattacks/#sthash.tqMl2N2V.dpuf>

DNS Amplification Attacks

- How these attacks work?
- How to protect from these attacks as a website operator?
- How to avoid taking part in such attacks as a DNS server administrator or network administrator

See more at: <https://blog.opendns.com/2014/03/17/dns-amplification-attacks/#sthash.tqMl2N2V.dpuf>

Defense (1/2)

- As a Website Operator, one may want to use a DDOS protection service such as those offered by Cloudflare, Verisign, and Arbor Networks.
- As a DNS or NTP Server Administrator, one should make sure your resolver is not open to the internet.

Defense (2/2)

Q: How to protect my network from participating in such attacks?

- Ensure to perform egress filtering on your edge devices which prevents spoofed packets from leaving your network, thereby preventing malicious devices in your network participating in attacks relying on the ability to send spoofed packets to the internet.



Defenses Against Attacks

- (1) Filtering Routers:
 - Filtering all packets entering and leaving the network protects the network from attacks.
 - The measure requires installing **ingress** and **egress** packet filters on **all** routers.
 - IP Traceback

Akamai's State of the Internet / Security Q2 2015 report:

"The second quarter of 2015 set a record for the number of DDoS attacks recorded... more than double what was reported in Q2 2014."

Mitigating DDoS attacks by using a CBSP

- Erring on the side of caution, many businesses contract with a **Cloud Based Security Provider (CBSP)** that offer security services such as **DDoS mitigation**.



Image: Courtesy of the ACM and Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis

- One simple way to quench DDoS attacks is to divert internet traffic destined for the client's network through the CBSP's security infrastructure

Routing Redirection

■ DNS rerouting:

- The client configures the company website domain name to resolve to an IP address belonging to the CBSP.

■ BGP rerouting:

- In the case that the client manages an entire /24 IP block.
- The client can withdraw the BGP announcements for that block from the company routers.
- Then, the CBSP will begin BGP announcements for that same range.
- That will send all traffic to the CBSP.



DNS rerouting: It does not eliminate the possibility of DDoS attacks.

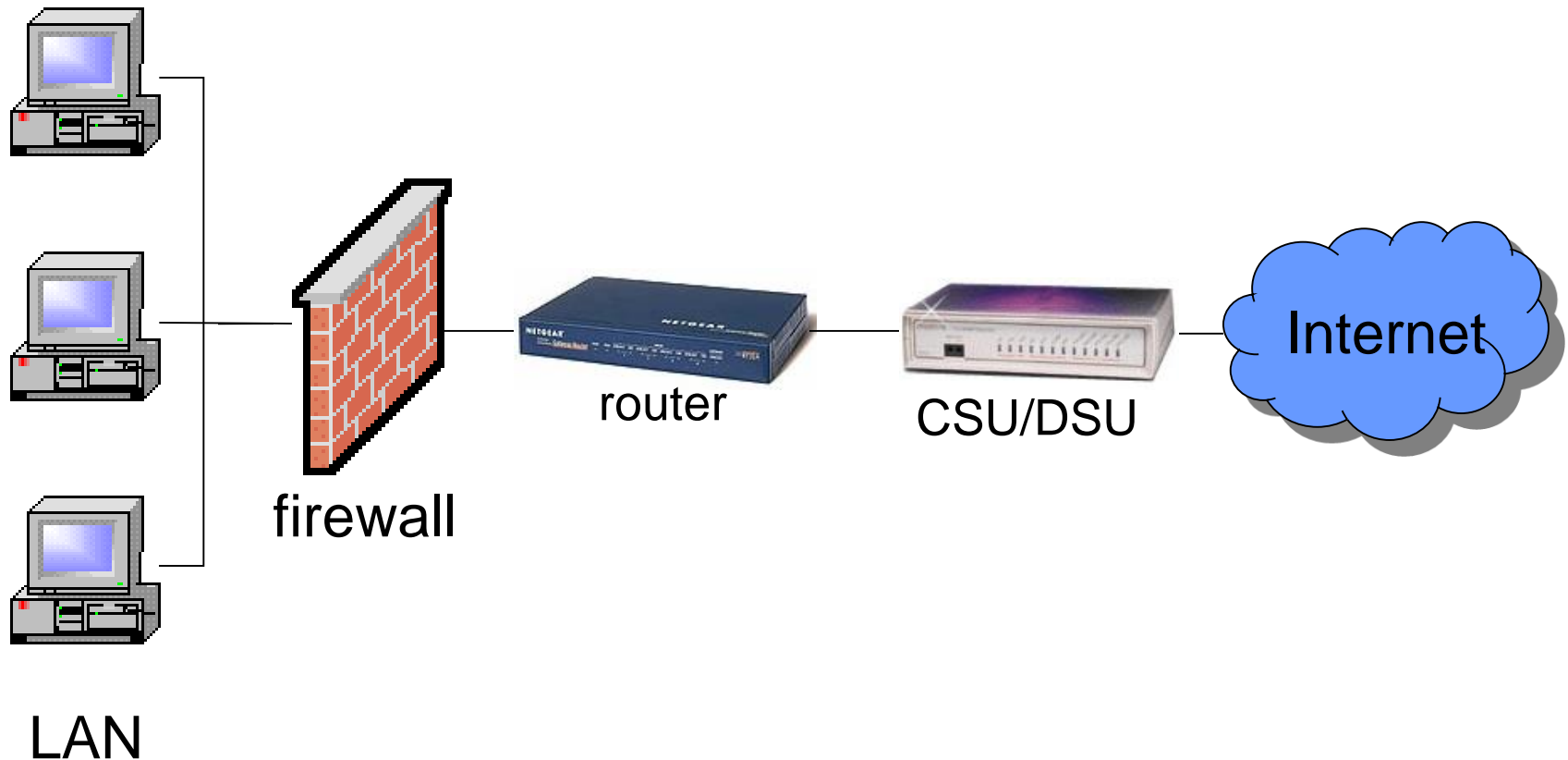
- This can be completely circumvented by directly attacking the website's hosting IP address.
- Therefore, it is crucial that their real IP address remains hidden from potential attackers.



BGP rerouting

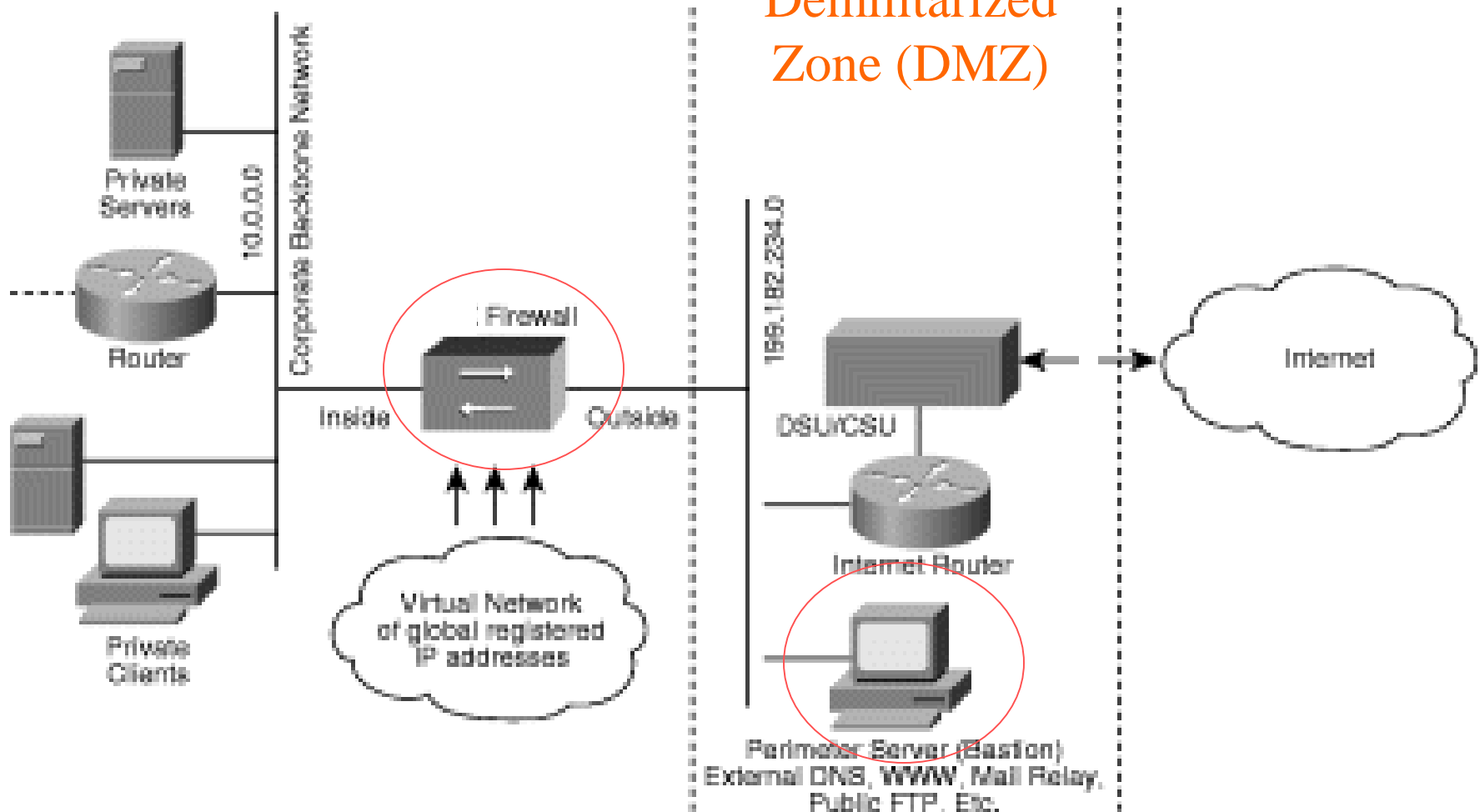
- At the CBSP, the client's traffic passes through a scrubbing center.
- If the traffic is legitimate, it will be forwarded to the client's web servers for processing; otherwise, the traffic will be silently discarded.

Packet-Filtering in a Stand-alone Firewall



Two-tiered approach to network security

Demilitarized Zone (DMZ)



Defenses Against Attacks

- Many observers have stated that **there are currently no successful defenses against a fully distributed denial of service attack.**
- Nevertheless, there are numerous safety measures to make the network more secure.

Defenses Against Attacks

- (2) Disabling IP Broadcasts:
 - By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attack.
 - “Traceroute”
 - “Ping”

Defenses Against Attacks

- (3) Applying Security Patches:
 - Hosts must be updated with the latest security patches and techniques.
 - Example: Program bugs
 - Web program -- escape code.
 - Buffer overflow

Defenses Against Attacks

- (4) Disable Unused Services:
 - If network services are unneeded or unused, the service should be disabled to prevent tampering and attacks.

Defenses Against Attacks

- (5) Performing Intrusion detection
 - Network *monitoring* is a very good preventive way of guarding against denial of service attacks.
 - By *monitoring* traffic patterns, a network can determine when it is under attack, and take the required step to defend itself.
 - Passive, off-line

Defenses Against Attacks

- (6) IETF's IP Security Authentication Header/ Encapsulating Security Payload (AH /ESP) protocols/algorithms to authentication and encrypt data packets.
 - Allows companies to create a virtual private network (VPN) across the Internet or any other packet network.

Conclusion

- Hackers/Intruders will keep hacking and intruding.
- Administrators should keep systems/networks working.
- Firewall and Intrusion Detection/Prevention Systems serves as the first-line protection.
- Firewall and Intrusion Detection/Prevention Systems products mainly differ in their performances and functionalities.

The end. 😊