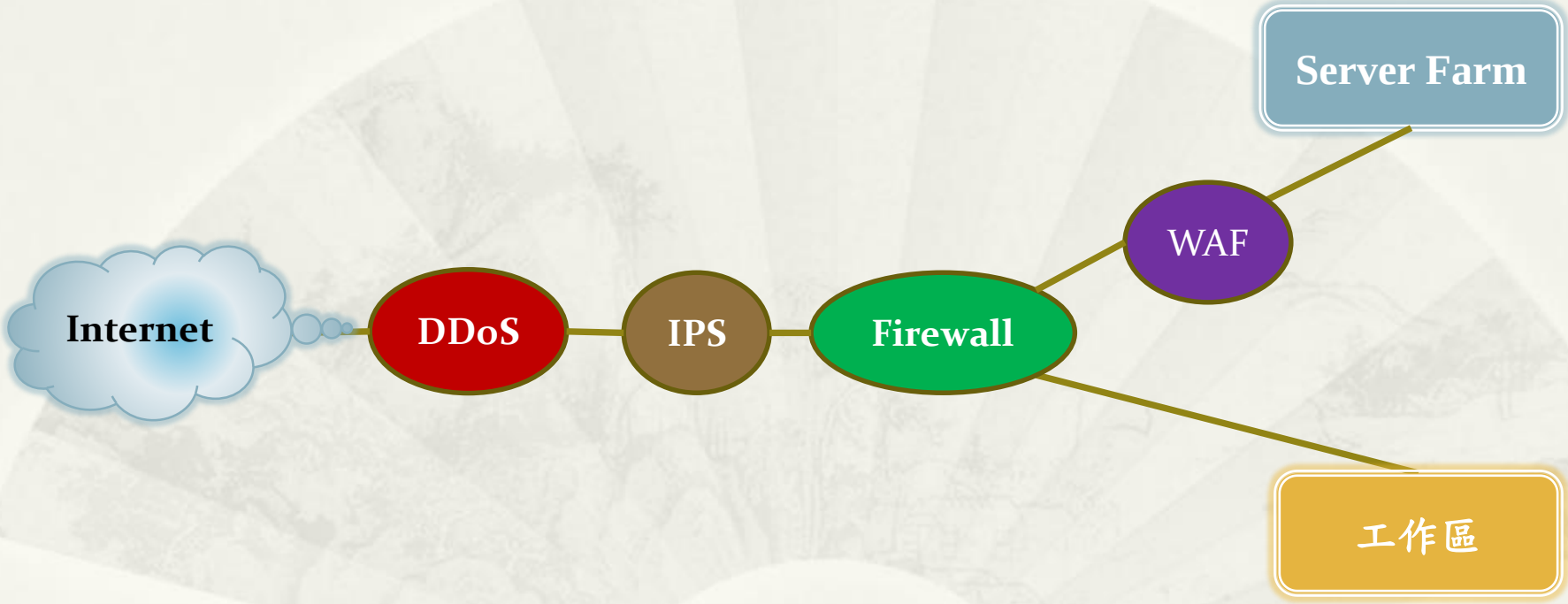
教育體系資安檢核

臺灣大學計資中心網路組
游子興
davisyou@ntu.edu.tw
02-33665008

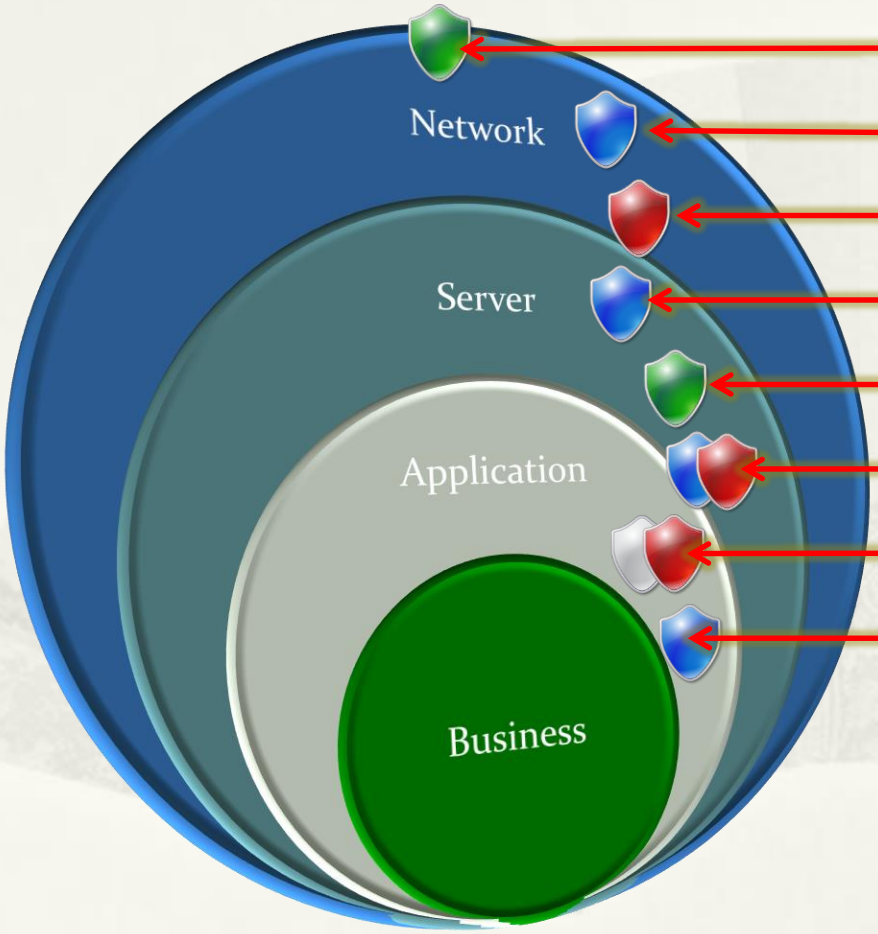
網路架構檢核

網路架構

* 各式資安設備部署位置參考



Mapping Security Protection Tools



Large volume network flood attacks

Network scan

Intrusion

Port scan

SYN flood attack

"Low & Slow" DoS attacks (e.g.Sockstress)

Application vulnerability, malware

High and slow Application DoS attacks

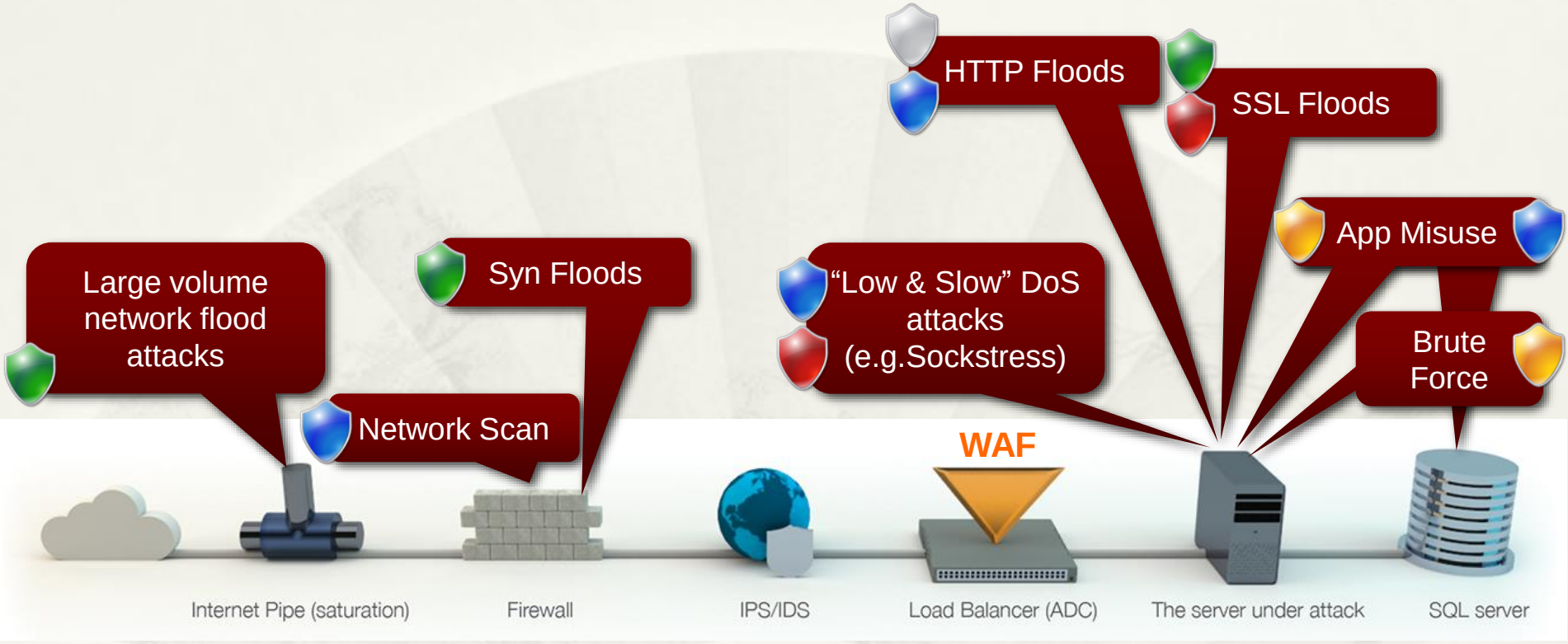
DDoS Protection

Behavioral Analysis

IPS

IP Reputation

DDoS Attack Vectors



DDoS Protection

Behavioral Analysis

IPS

IP Reputation

Ref. Radware Training and Education

Firewall Policy
IP 網段

	IP 網段	內對外	外對內	內對內 ACL 存取控制
工作區	Private IP	Dest IP: 黑名單	reject all	Permit Private IP
Server Farm	Private IP + Public IP	Dest IP: 白名單 (Zero Trust)	80/443: permit all 22: Src IP 白名單 3389:Src IP 白名單 …	跳板機/VPN
網路設備/ IOT 設備	Private IP	reject all	reject all	Permit Private IP

Firewall Policy vs. Router ACL

- Session-based vs. Non Session-based
- Stateful vs. Stateless
- Session-based/Stateful
  - 使用記憶體記錄 Sessions，易受 SYN Flood 攻擊

Case1. 某PC
外對內: 僅允許 Src IP: 140.112.3.0/24

* Router ACL

* 方法1: 設定於介面 Out 方向

```
ipv4 access-list acl_out
  permit ipv4 140.112.3.0 0.0.0.255 any
int Gio/9/1/7
  ipv4 access-group acl_out egress
```

* 方法2: 設定於介面 In 方向

```
ipv4 access-list acl_in
  permit ipv4 any 140.112.3.0 0.0.0.255
int Gio/9/1/7
  ipv4 access-group acl_in ingress
```

設定於介面 In/Out 差異

* 設定於 Out 方向
  * 外對內: Permit Source IP: 140.112.3.0/24
  * 內對外: 不限制.
* 設定於 In 方向
  * 外對內: 不限制.
  * 內對外: Permit Dest IP: 140.112.3.0/24
* 嚴謹設定: In + Out 皆設定

```
int Gio/9/1/7
  ipv4 access-group acl_in ingress
  ipv4 access-group acl_out egress
```

Case1. 某PC
外對內: 僅允許 Src IP: 140.112.3.0/24

- Firewall Policy
  - Allow Rules 僅需設定在連線發起之方向(Initial session)，另一方向不需設定。
  - 等同 ACL 嚴謹設定

Floating WAN LAN

允許 **Src IP: 140.112.3.0/24**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Gateway	Queue	Schedule	Description	Actions
☐	✔ 0 /0 B	IPv4 *	ACL_1	*	*	none			

Alias details

Value
140.112.3.0/24

Floating WAN LAN

內對外: 全部拒絕

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

Case2. 某PC
內對外: 全部開放 外對內: 全部拒絕

- Router ACL
  - Non Session-based 無法設定

Case2. 某PC
內對外: 全部開放 外對內: 全部拒絕

- Firewall Policy
  - Allow Rules 僅需設定在連線發起之方向(Initial session)，另一方向不需設定。

Floating WAN LAN

外對內: 全部拒絕

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

Floating WAN LAN

內對外: 全部開放

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	6 /1.55 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
✔	14 /4.50 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑

Firewall Logs Review

- Deny Rules Logs
  - 預設開啟
  - 幫助有限, 因為已經被 Deny 無資安風險.
- Allow Rules Logs
  - 預設未開啟, 建議開啟, 才能分析是否異常.
  - 個人電腦連線分析
    - 外對內連線: 不應有.
    - 內對外連線
      - 使用 GEOIP 進行 Country & ASN 分析, 針對冷門之 Country & ASN 應特別留意是否可能是後門程式在運作.
      - Review 所有 Dest Port != 80, 443, 53 連線
      - 搭配 Snort/Layer7 分析
        - Dest Port 80 但非 http protocol
        - Dest Port 443 但非 https protocol
        - Dest Port 53 但非 DNS protocol

Firewall Logs Review

* Server farm 連線分析
  * 外對內連線:
    * Web Server: 歷史記錄之平均頻率與次數
    * 可用 Size & 頻率 看出是否進行 SQL Injection & try 密碼攻擊
  * 內對外
    * ☆☆☆應僅有 Window Update, Linux OS Update 等系統更新連線記錄, 不應有主動內對外連線行為.

使用 Snort 偵測異常

* 內對外攻擊
  * 所有 Snort Rules 反方向
* 內對外 Reverse Shell 連線

網路政策

* 跳板機連線政策
* VPN 連線政策
* 備援機制
  * 網路備援
  * 主機/服務備援

簡報完畢
謝謝