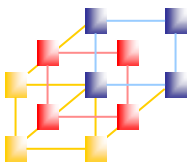


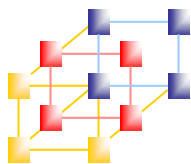
Unit 4

Firewall



廠商眼中的防火牆

- 先看廠商自吹自擂
- <https://www.youtube.com/watch?v=I9vNNNoCYiJk>
- 看看老王怎麼賣瓜
 - 怎麼利用一個領域的優勢攻佔其他領域
 - 了解防火牆是怎麼一回事
 - 反思，真的有他說的這麼好嗎？！那不就天下太平了？！

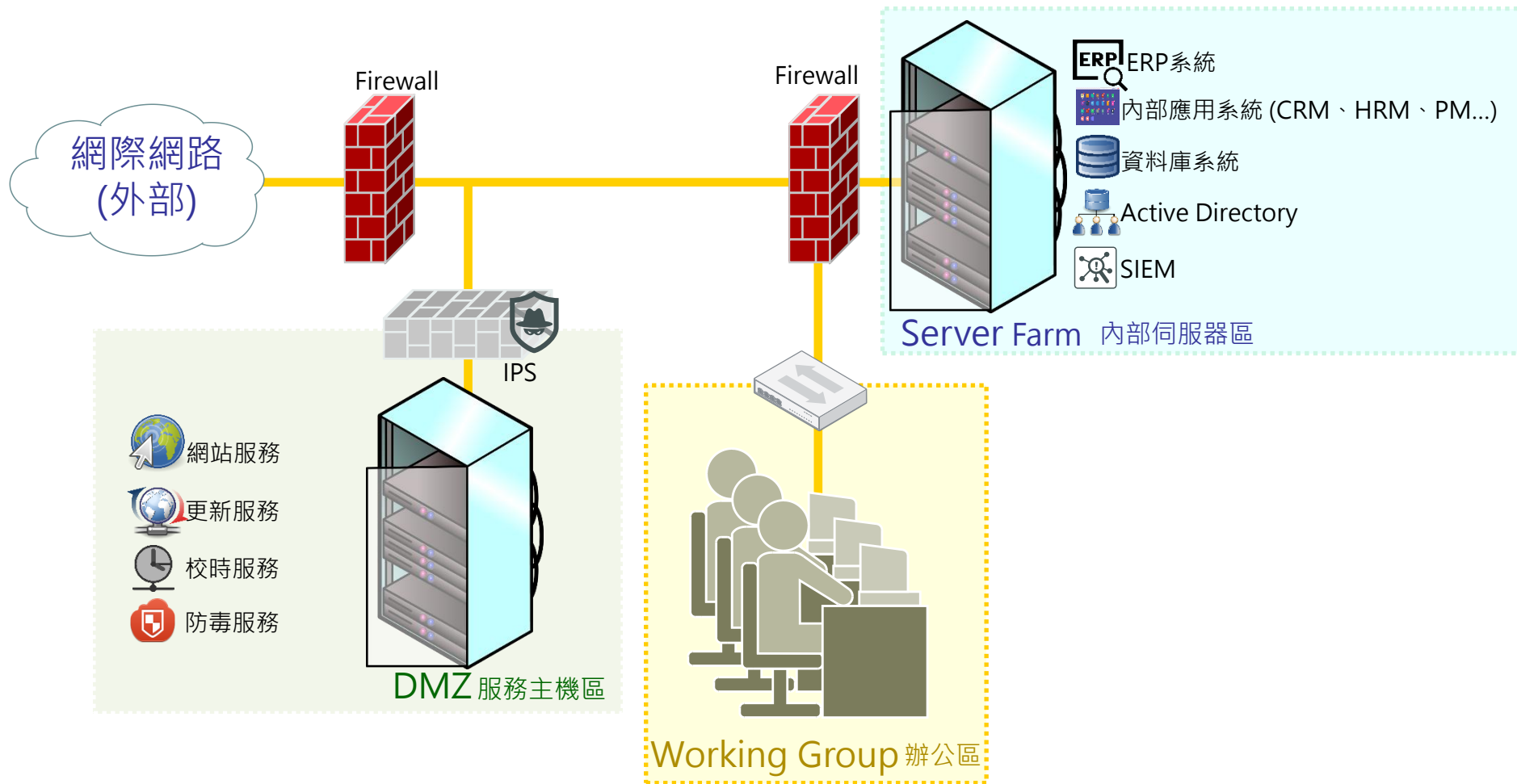


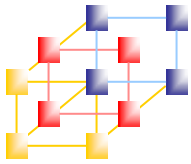
Quiz 9



- 從這個自吹自擂的影片看到什麼？
 - 該產品的優勢？
 - 該產品的隱憂？
- 請將答案寫在紙條上，下課收來講桌。
- ((請記得寫上班級姓名學號

常見的網路架構示意

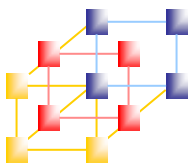




先來看影片

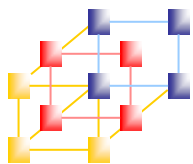


- 什麼是防火牆？
 - <https://youtu.be/kDEX1HXybrU>

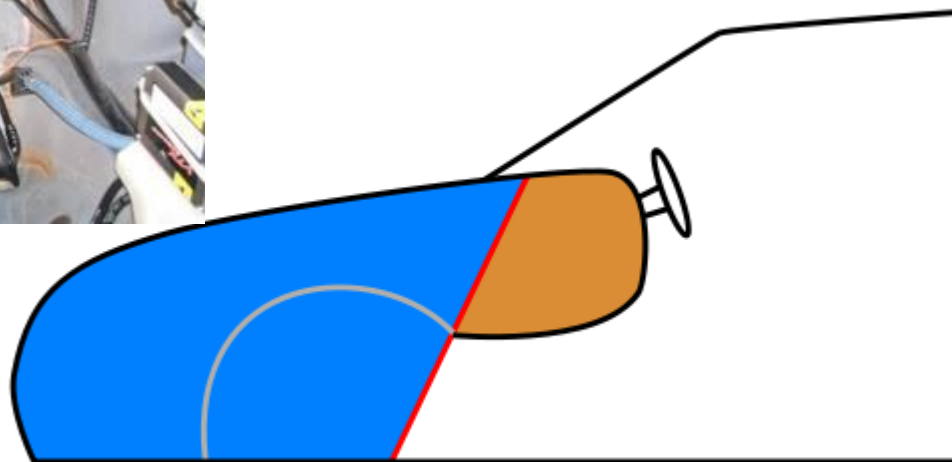


防火牆是怎麼一回事？

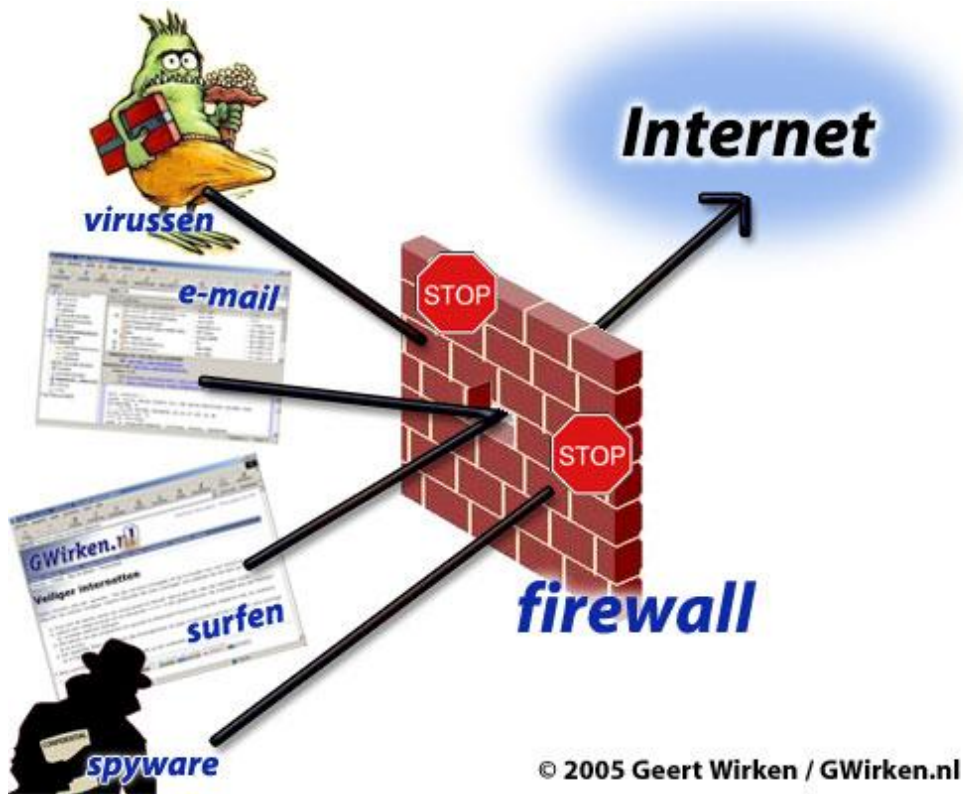


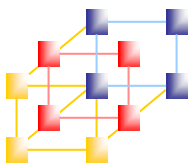


這也是防火牆



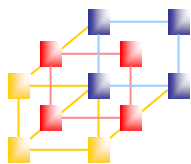
這還是防火牆





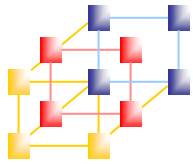
實際上防火牆長怎樣？

- <https://youtu.be/MFavkeIrVfc>
- (上次影片太虛無飄渺了，換一個)
- <https://youtu.be/OREhXPi2op0>
- 一堆防火牆的比較



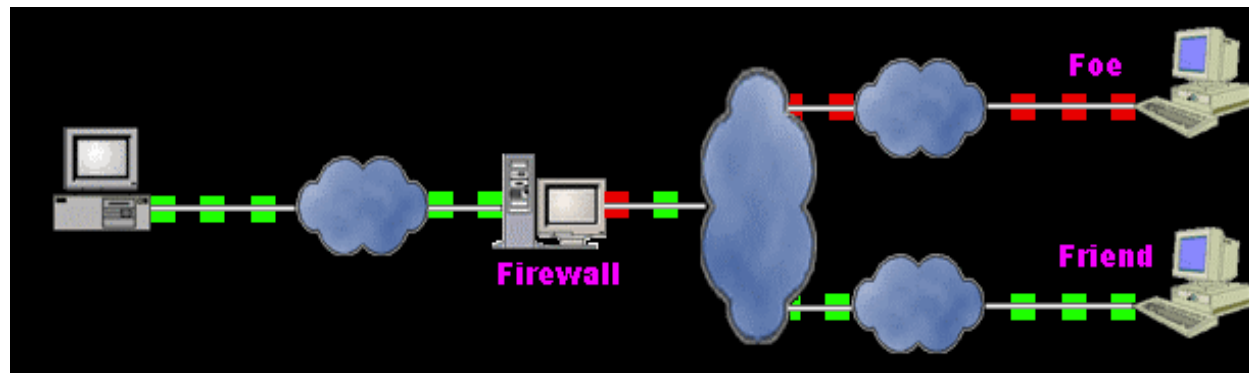
軟體解決方案

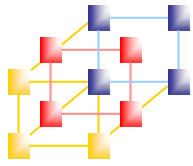
- <https://youtu.be/zOg-EYDaHX8?t=396>
- 軟體好用就會想要賺更多錢！！
- <https://www.netgate.com/pfsense-plus-software/how-to-buy>



Firewall introduction

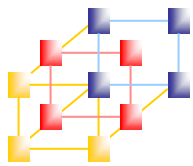
- Firewalls control the flow of network traffic
- Interconnect networks with differing trust
 - Imposes restrictions on network services
 - Only authorized traffic is allowed
- Auditing and controlling access
 - Can implement alarms for abnormal behavior





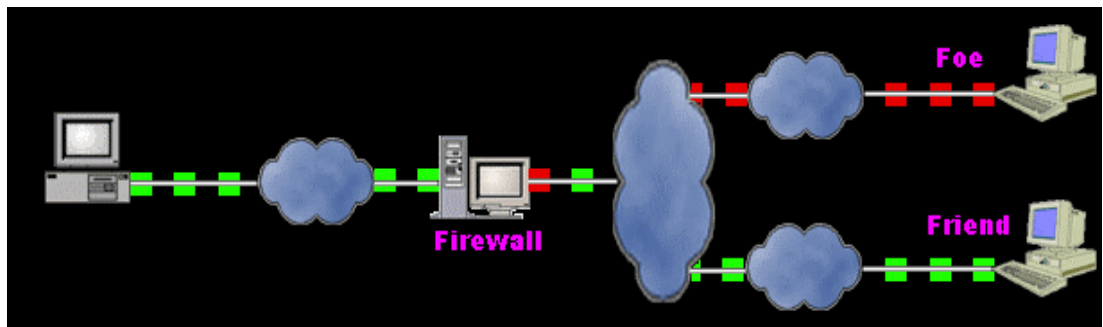
Firewall functions

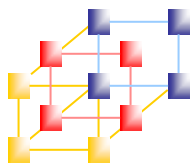
- Service control
 - Determine the type of Internet services that can be accessed, inbound or outbound
- Direction control
 - Determine the direction in which particular service requests may be initiated and allowed to flow through the firewall
- User control
 - Control access to a service according to which user is attempting to access it
- Behavior control
 - Control how particular services are used



防火牆做什麼事？

- 控制封包與資料流
- 信任的才通過
- 不信任的不通過
- 封包轉送
- 存取控制與稽核
 - 異常流量警示





防火牆怎麼分區？

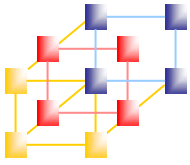


- WAN (Wide area network)
- LAN (Local area network)
- DMZ (Demilitarized zone)

原指南北韓停戰協定中，南北雙方沿著北緯38度線各自向後撤退2公里，而形成的一種避免衝突的非軍事區。

- 介於WAN與LAN之間
- WAN、LAN均可存取
- 放置對外服務之伺服器 (HTTP、DNS、SMTP...)

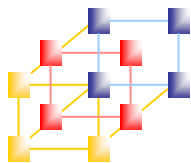




再來看影片

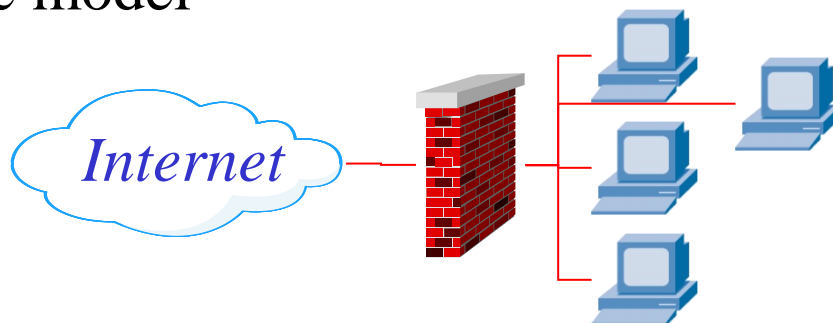


- 什麼是DMZ？
 - <https://youtu.be/dqlzQXo1wqo>

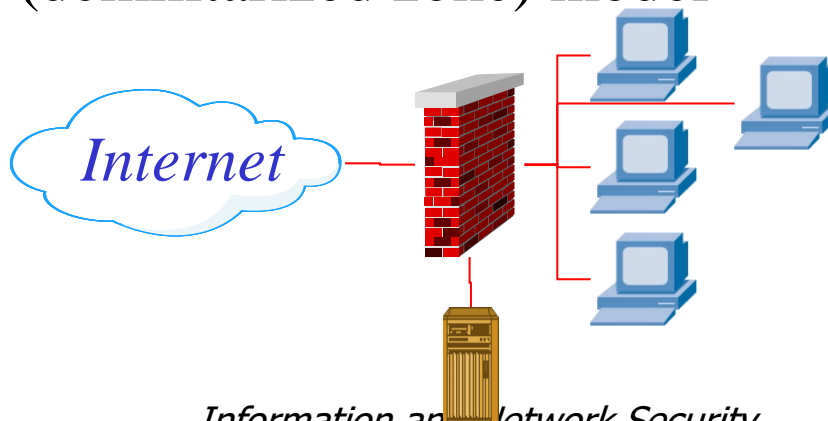


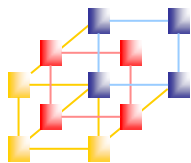
Firewall architecture (1/3)

- Single firewall
 - Basic model



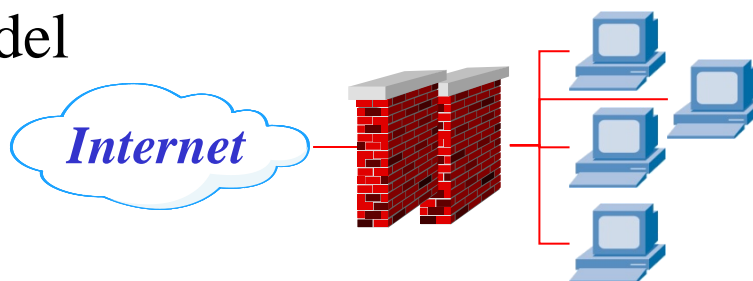
- DMZ (demilitarized zone) model



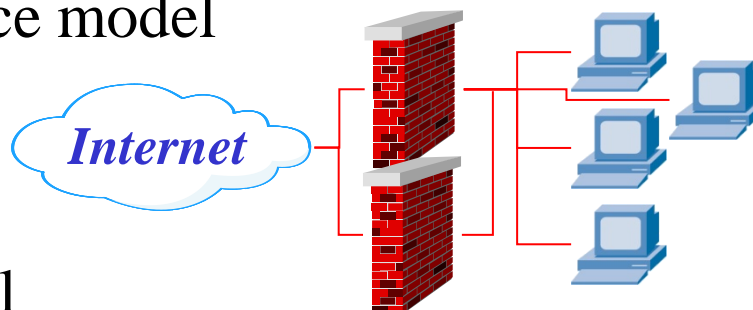


Firewall architecture (2/3)

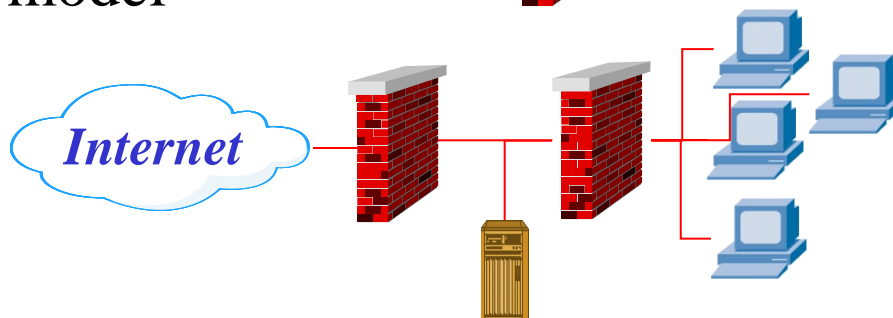
- Dual firewall
 - Backup model

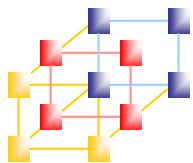


- Load balance model



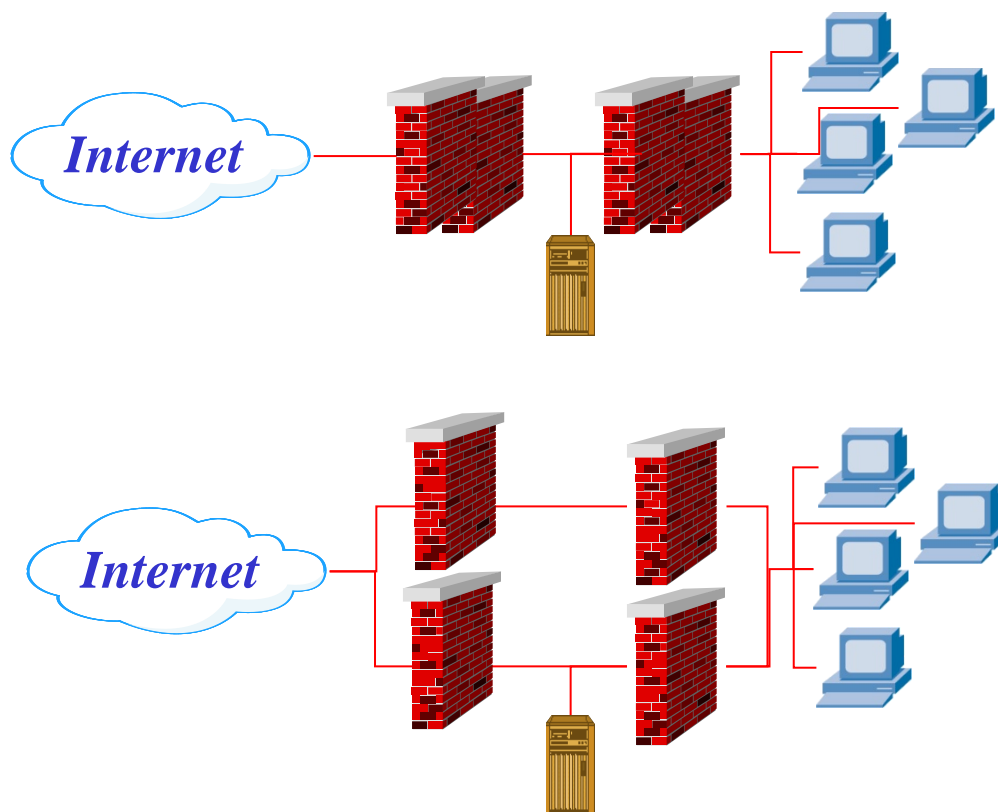
- DMZ model

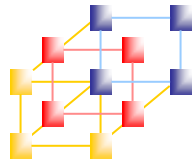




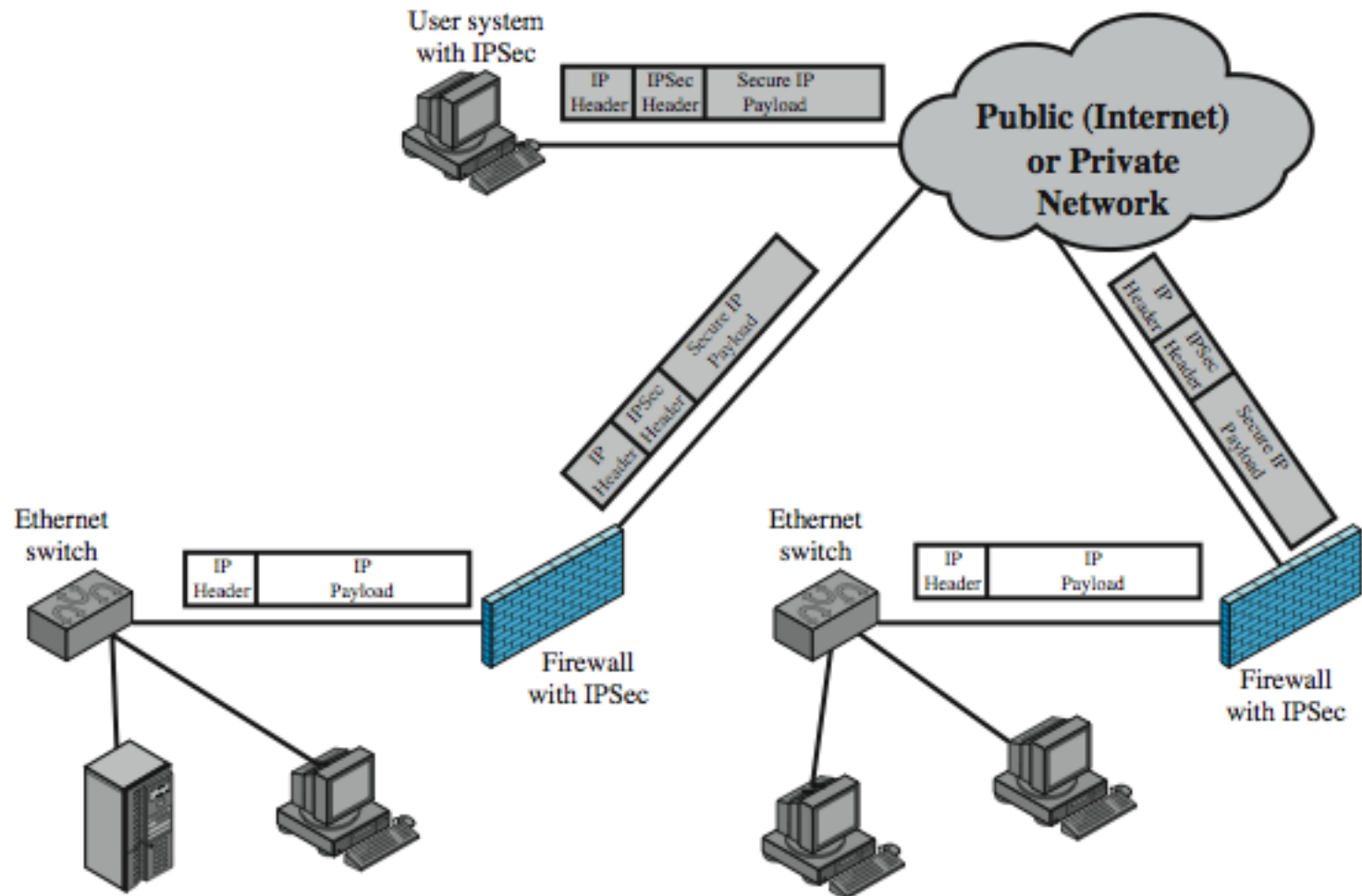
Firewall architecture (3/3)

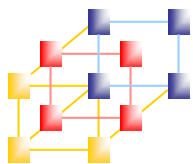
- Multi-firewall





Virtual private networks

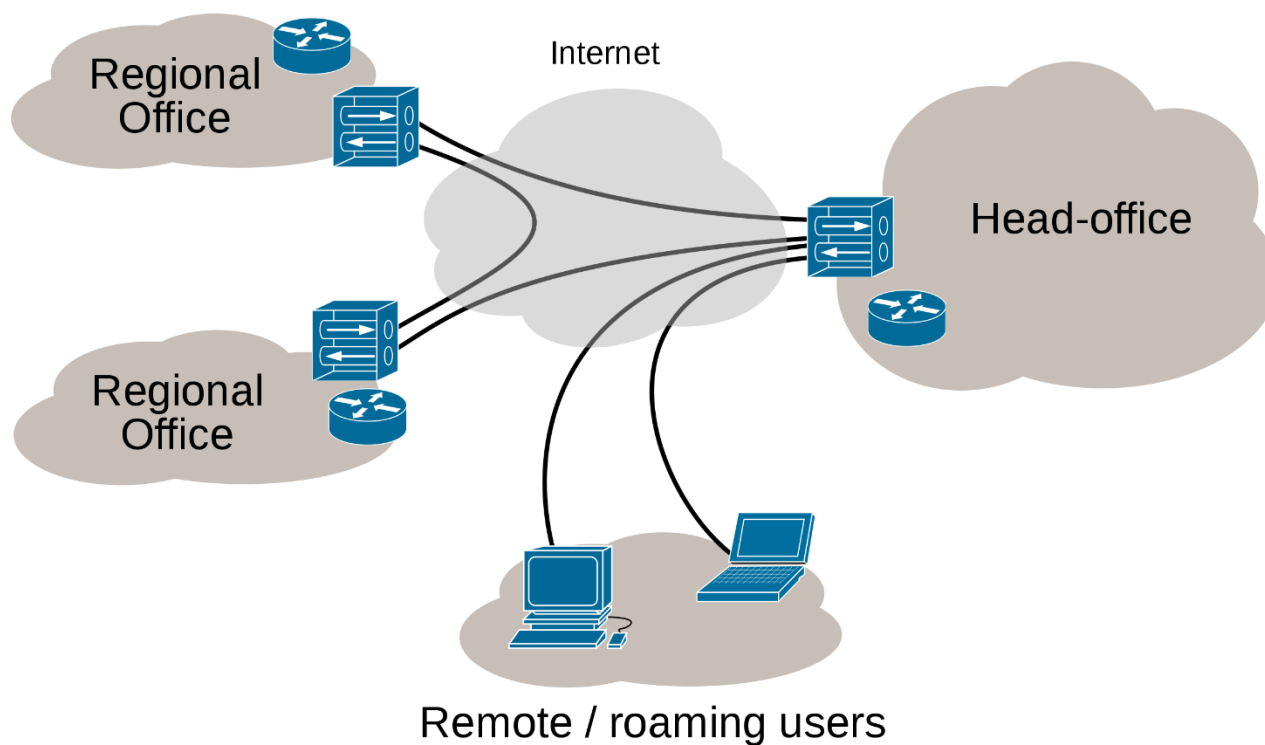




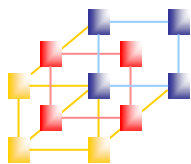
VPN是什麼？



Internet VPN



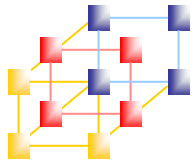
Source: <https://zh.wikipedia.org/>



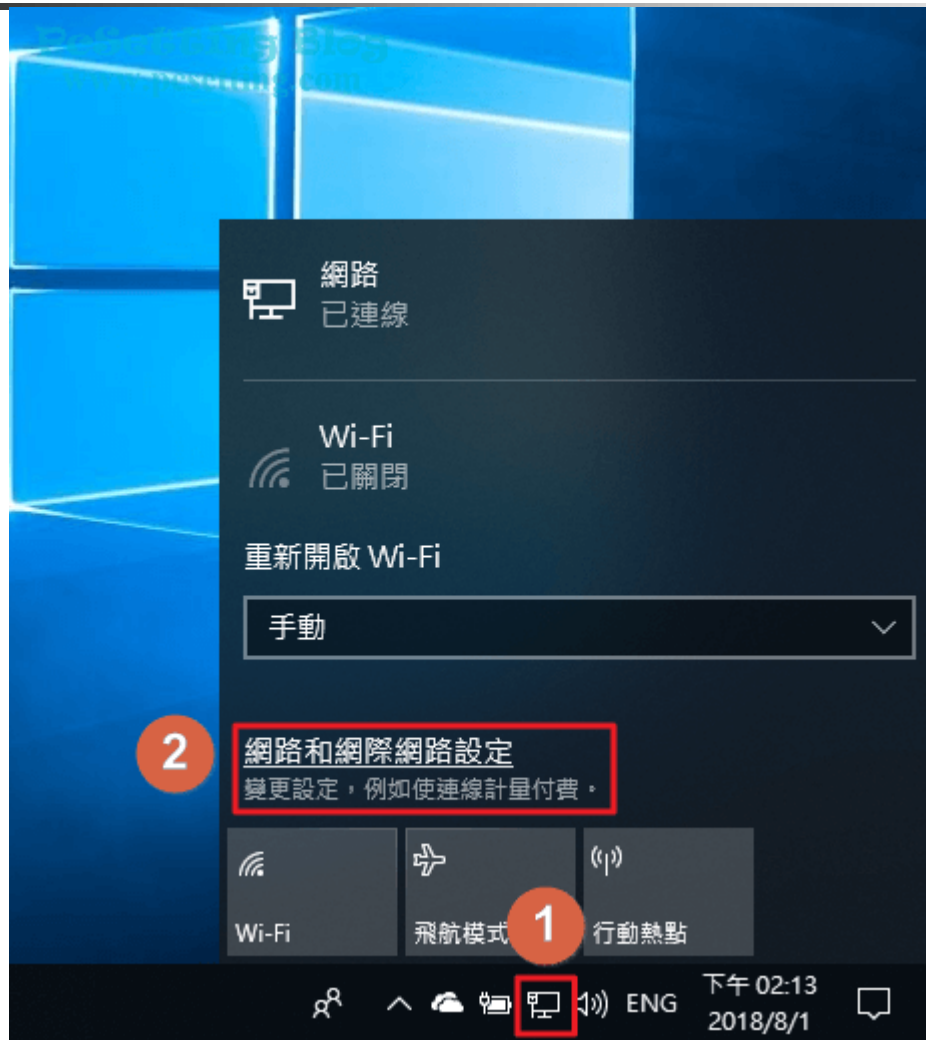
VPN

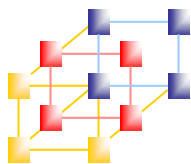


- 在公開網路上建立加密的虛擬通道
 - Point-to-Site VPN
 - 出外辦公用
 - Site-to-Site VPN
 - 外點區網連線至內部
 - SSH Tunnel (?)
 - 翻牆用(? !)



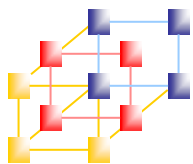
Point-to-Site VPN使用教學





Point-to-Site VPN使用教學





Point-to-Site VPN使用教學

設定

新增 VPN 連線

VPN 提供者

連線名稱

伺服器名稱或位址

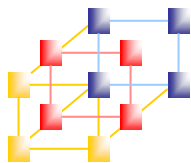
登入資訊的類型

使用者名稱 (選擇性)

密碼 (選擇性)

儲存 取消

PcSetting Blog
www.pcsetting.com



Point-to-Site VPN使用教學

VPN Gate: 公共 VPN 中繼 x

安全 | <https://www.vpngate.net/cn/>

一个学术实验
@日本国立筑波大学研究生院
www.tsukuba.ac.jp/chinese/

防火墙
因不明原因
发生故障

VPN Gate Client
国内互联网

VPN Gate
一个学术实验
公共 VPN 中继服务器
由志愿者托管

自由!!

目标服务器
海外互联网

辛苦! 欢迎来到西方世界的“真正的”互联网。

你的 IP: 125-227-... .HINET-IP.hinet.net (125.227. ...)

你的国家或地区: Taiwan

通过使用 VPN Gate 来更改你的 IP 地址!

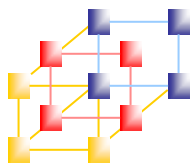
如果在未来贵国政府的防火墙由于故障 www.vpngate.net 网站变得无法访问, 建议记住 镜像站点 URL 列表。

镜像站点的最新列表: <https://www.vpngate.net/cn/sites.aspx>

你自己应定期执行复制操作。在未来, 当 www.vpngate.net 无法访问时, 你可以尝试访问镜像站点列表的 URL 之一。

如果你是一个国家的公民由于政府防火墙的未知错误, 防止从国内互联网访问 www.vpngate.net, 请访问 镜像站点列表页面, 复制 URL 列表, 并将其粘贴到你们国家的 SNS, 博客或社区论坛, 以帮助你们国家的 VPN 用户, 以帮助你周围的人。我们爱互联网用户在你的国家。我们想帮助他们。

PCSetting Blog
www.pcsetting.com



Point-to-Site VPN使用教學

設定

新增 VPN 連線

1 VPN 提供者

Windows (內建)

連線名稱

伺服器名稱或位址

2 VPN 類型

自動

點對點通道通訊協定 (PPTP)

L2TP/IPsec (使用憑證)

L2TP/IPsec (使用預先共用金鑰)

安全通訊端通道通訊協定 (SSTP)

IKEv2

儲存 取消

PeSetting Blog
www.pesetting.com

Point-to-Site VPN使用教學

VPN Gate: 公共 VPN 中繼 x



安全 | https://www.vpngate.net/cn/

1 世界各地有 5062 个公共 VPN 中繼服务器。
您可以连接到任何以下 VPN 服务器与参数: 用户名: 'vpn', 密码: 'vpn'.

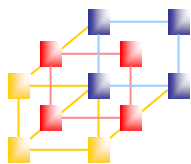
应用过滤器: ☐ SoftEther VPN (SSL-VPN) ☒ L2TP/IPsec ☐ OpenVPN ☐ MS-SSTP 更新服务器列表 2

在某些国家, 你必须指定的目标 VPN 服务器的 IP 地址, 而不是 DDNS 主机名。

Do you want to parse the below HTML table? Instead you can use [CSV List](#) to make your own VPN Gate client app.

国家 / 地区 (物理位置)	DDNS 主机名 IP 地址 (ISP 主机名)	VPN 会话数 运行时间 累计用户数	线路质量 吞吐量和 Ping 累积转移 日志策略	SSL-VPN Windows (合适的)	L2TP/IPsec Windows, Mac, iPhone, Android 无需 VPN 客户端	OpenVPN Windows, Mac, iPhone, Android
 Japan	118.4.78.152 (p209152-ipngn200407niho.hiroshima.ocn.ne.jp)	129 会话 14 天 累计 426,738 用户	219.09 Mbps Ping: 10 ms 118,646.07 GB 日志策略: 两周	✓ SSL-VPN 连接指南 TCP: 1760 UDP: 支持		
 Japan	153.209.208.113 (p2871113-ipngn22801marunouchi.tokyo.ocn.ne.jp)	83 会话 13 天 累计 465,379 用户	47.98 Mbps Ping: 27 ms 72,496.14 GB 日志策略: 两周	✓ SSL-VPN 连接指南 TCP: 1957 UDP: 支持		

PCSetting Blog
www.pcsetting.com



Point-to-Site VPN使用教學

VPN Gate: 公共VPN中... x
www.pcsetting.com

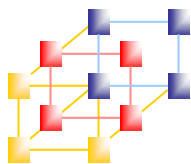
安全 | https://www.vpngate.net/cn/

应用过滤器: ☐ SoftEther VPN (SSL-VPN) ☒ L2TP/IPsec ☐ OpenVPN ☐ MS-SSTP [更新服务器列表](#)

在某些国家, 你必须指定的目标 VPN 服务器的 IP 地址, 而不是 DDNS 主机名。

Do you want to parse the below HTML table? Instead you can use [CSV List](#) to make your own VPN Gate client app.

国家 / 地区 (物理位置)	DDNS 主机名 IP 地址 (ISP 主机名)	VPN 会话数 运行时间 累计用户数	线路质量 吞吐量 Ping 累积转移 日志策略	SSL-VPN Windows (合适的)	L2TP/IPsec Windows, Mac, iPhone, Android 无需 VPN 客户端	OpenVPN Windows, Mac, Phone, Android	M...
 Korea Republic of	121.168.45.38	0 会话 10 天 累计 0 用户	0.02 Mbps Ping: 32 ms 0.00 GB 日志策略: 两周	✓ SSL-VPN 连接指南 TCP: 443	✓ L2TP/IPsec 连接指南	✓ OpenVPN 配置文件 TCP: 443 UDP: 1194	SS st w
 Japan	110.163.134.17 (mo110-163-134-17.fix.mopera.net)	195 会话 1 天 累计 615,302 用户	61.29 Mbps Ping: 8 ms 34,500.26 GB 日志策略: 两周	✓ SSL-VPN 连接指南 TCP: 992 UDP: 支持	✓ L2TP/IPsec 连接指南	✓ OpenVPN 配置文件 TCP: 992 UDP: 1194	SS m er
 United States	75.118.202.212 (d118-75-212-202.nap.wideopenwest.com)	62 会话 22 小时 累计 20,154 用户	11.66 Mbps Ping: 37 ms 938.95 GB 日志策略:	✓ SSL-VPN 连接指南 TCP: 905	✓ L2TP/IPsec 连接指南	✓ OpenVPN 配置文件 TCP: 905	



Point-to-Site VPN使用教學

設定

新增 VPN 連線

VPN 提供者
Windows (內建)

1 連線名稱
vpn-jp

2 伺服器名稱或位址
mo110-163-134-17.fix.mopera.net

3 VPN 類型
L2TP/IPsec (使用預先共用金鑰)

預先共用金鑰

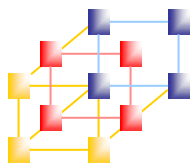
登入資訊的類型

VPN Gate: 公共 VPN 中心

安全 | <https://www.vpngate.net/cn/>

国家 / 地区 (物理位置)	DDNS 主机名 IP 地址 (ISP 主机名)	VPN 会话数 运行时间 累计用户数
Korea Republic of	121.168.45.38	0 会话 10 天 累计 0 用户
Japan	110.163.134.17 (mo110-163-134-17.fix.mopera.net)	195 会话 1 天 累计 615,302 用户
United States	75.118.202.212 (d118-75-212-202.nap.wideopenwest.com)	62 会话 22 小时 累计 20,154 用户
United States	108.230.228.94	5 会话

PcSetting Blog
www.pcsetting.com



Point-to-Site VPN使用教學

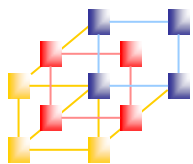
Setting Blog
www.pcsetting.com

新增 VPN 連線

L2TP/IPsec (使用預先共用金鑰) ▼

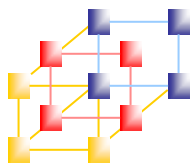
- 1 預先共用金鑰
...
- 2 登入資訊的類型
使用者名稱與密碼 ▼
- 3 使用者名稱 (選擇性)
vpn
- 4 密碼 (選擇性)
...
- 5 ☒ 記住我的登入資訊

6 儲存 取消



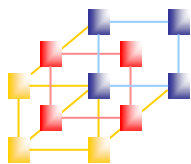
Point-to-Site VPN使用教學





Point-to-Site VPN使用教學





Point-to-Site VPN使用教學

VPN Gate: 公共 VPN 中繼服務器

安全 | <https://www.vpngate.net/cn/>

一个学术实验
@日本国立筑波大学研究生院
www.tsukuba.ac.jp/chinese/

VPN Gate
一个学术实验
公共 VPN 中繼服務器
由志愿者托管

VPN

自由!!

VPN Gate Client
国内互联网

目标服务器
海外互联网

www.vpngate.net

辛苦了! 欢迎来到西方世界的“真正的”互联网。

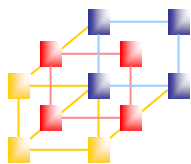
你的 IP: mo110-163-134-17.fix.mopera.net (110.163.134.17)

你的国家或地区: Japan

通过使用 VPN Gate 来更改你的 IP 地址!

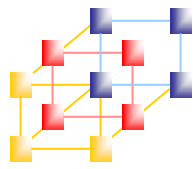
如果在未来贵国政府的防火墙由于故障 www.vpngate.net 网站变得无法访问, 建议记住 镜像站点 URL 列表。
镜像站点的最新列表: <https://www.vpngate.net/cn/sites.aspx>
你自己应定期执行复制操作。在未来, 当 www.vpngate.net 无法访问时, 你可以尝试访问镜像站点列表的 URL 之一。
如果你是一个国家的公民由于政府防火墙的未知错误, 防止从国内互联网访问 www.vpngate.net, 请访问 镜像站点列表页面,
复制 URL 列表, 并将其粘贴到你们国家的 SNS, 博客或社区论坛, 以帮助你们国家的 VPN 用户,
以帮助你周围的人。我们爱互联网用户在你的国家。我们想帮助他们。

PcSetting Blog
www.pcsetting.com

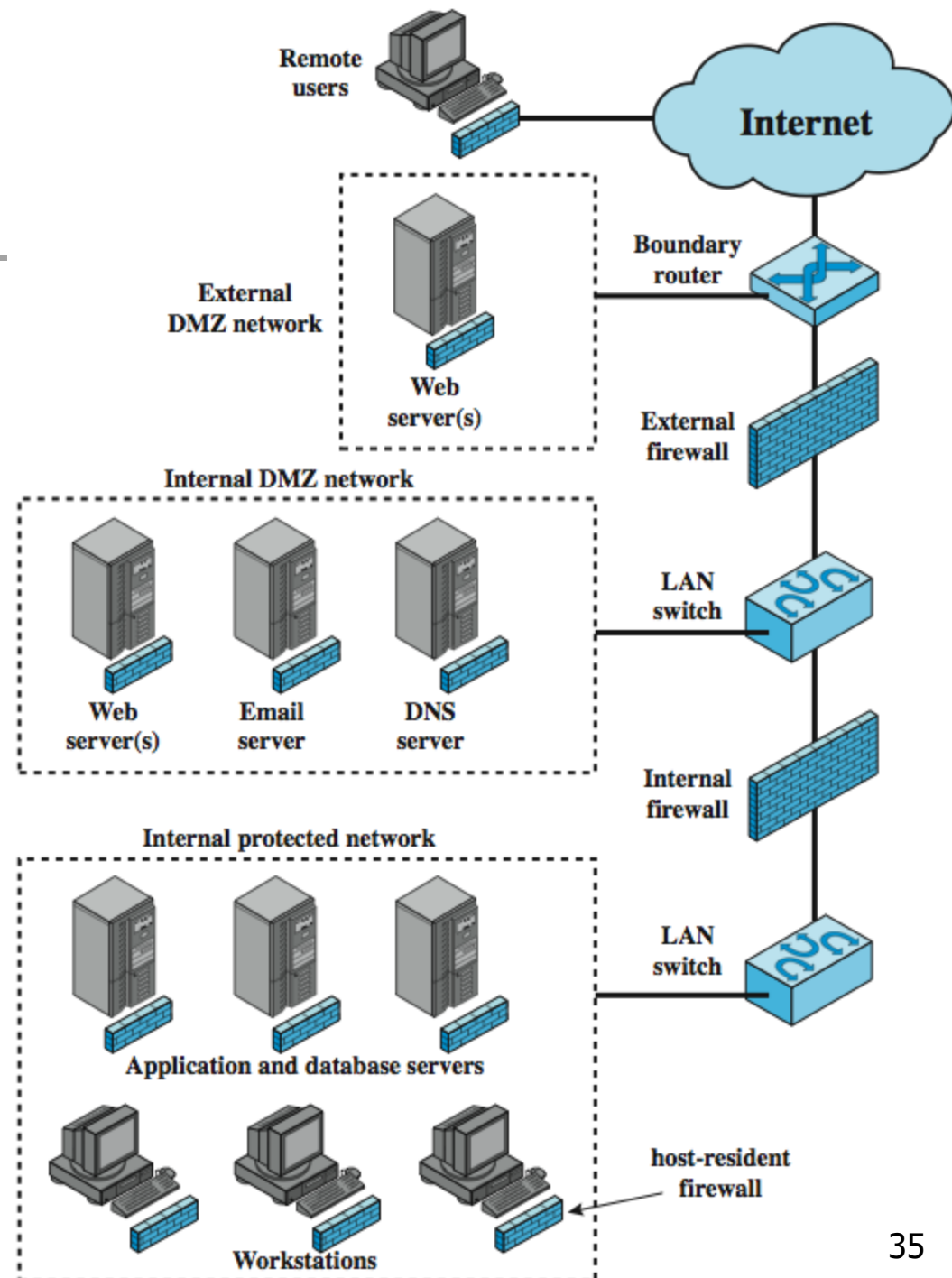


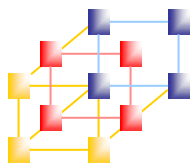
何時使用VPN？

- 在家辦公
- 翻牆
- 跨區買東西
- ...



Distributed Firewalls

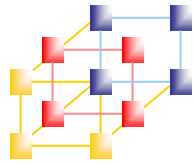




SD-***



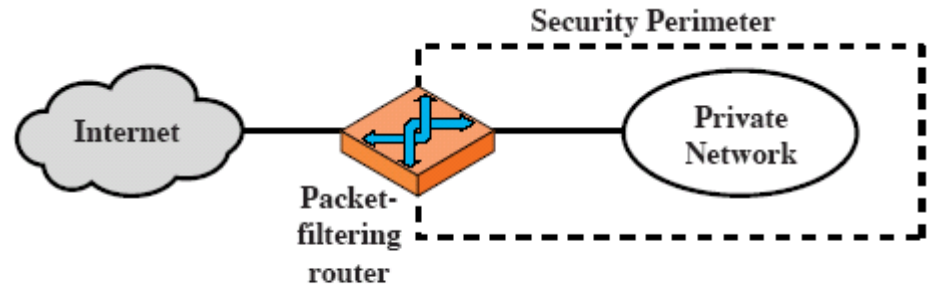
- Software-Defined ***
- 合久必分，分久必合



Types of firewall

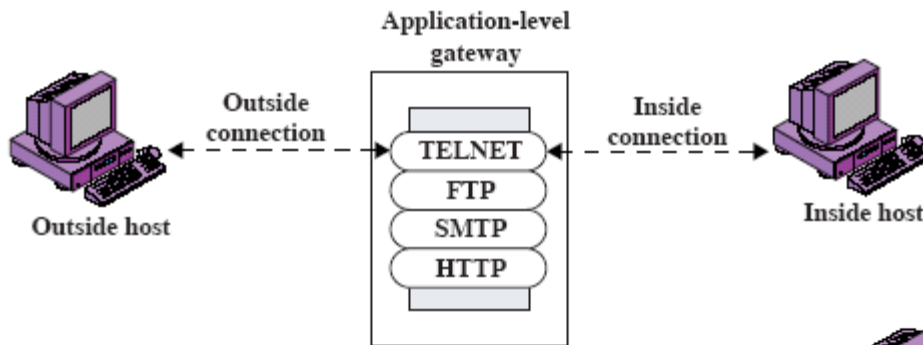
Packet-filtering router

- Stateful inspection firewalls



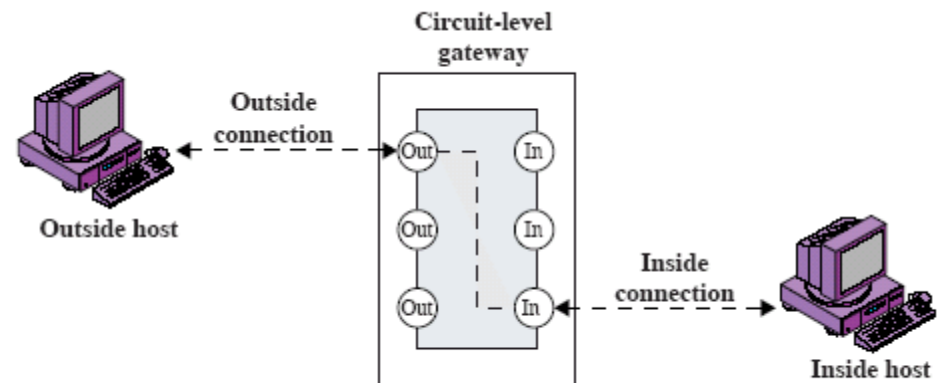
(a) Packet-filtering router

Application-level gateway

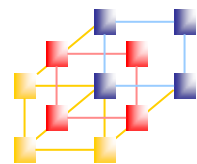


(b) Application-level gateway

Circuit-level gateway

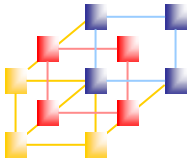


(c) Circuit-level gateway



Packet-filtering router

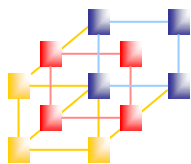
- Simplest
- Foundation of any firewall system
- Examine each IP packet
- Possible default policies
 - Everything not specifically permitted is **denied**.
 - Everything not specifically denied is **permitted**.



Packet-filtering router

■ 封包過濾器

- 簡單
- 常見於所有防火牆
- 分析通過封包
- 可能的預設政策
 - Everything not specifically permitted is denied.
所有沒定義允許的-丟掉：白名單
 - Everything not specifically denied is permitted.
所有沒定義丟掉的-允許：黑名單



Quiz 10



- 以下環境適合白名單還是黑名單，為什麼？
 1. 銀行單位的ATM系統機房端閘道防火牆
 2. 學生宿舍對外防火牆
 3. 上市公司進銷存系統前的防火牆
 4. TANET骨幹防火牆
 5. 機房DMZ區閘道防火牆