



บทที่ 5 : การประยุกต์ใช้คริปโตกราฟฟี Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- Web Security
 - S-HTTP
 - HTTPS
 - SSL/TLS
- Remote Login Security
 - SSH
- Network Security
 - VPN



Web Security

- ▶ โดยปกติการสื่อสารของ WWW จะใช้โปรโตคอล HTTP (Hyper Text Transfer Protocol) โดยใช้พอร์ต 80 เป็นการสื่อสารระหว่างเว็บเซิร์ฟเวอร์และไคลเอนต์
- ▶ ปกติโปรโตคอล HTTP จะไม่มีการเข้ารหัสข้อมูล เพราะฉะนั้นใครก็ตามที่ดักจับข้อมูลระหว่างเส้นทางการสื่อสารได้จะสามารถอ่านข้อมูลนั้นได้ทันที

Web Security : S-HTTP

- S-HTTP (Secure HTTP) หลักการคือสร้างโปรโตคอล HTTP ที่มีความสามารถในการเข้ารหัสและถอดรหัสอยู่ภายในตัวเอง โดยตรง
- ใช้เทคนิคการเข้ารหัสของ RSA ซึ่งเป็นการเข้ารหัสแบบพับลิคคีย์
- ปัจจุบันโปรโตคอล S-HTTP ไม่เป็นที่นิยมเท่าที่ควร

Web Security : HTTPS



- HTTPS (HTTP over SSL) เป็นโพรโตคอลที่พัฒนาโดย Netscape
- ใช้เข้ารหัสข้อมูลที่รับส่งระหว่างเซิร์ฟเวอร์และบราวเซอร์
- ปกติจะใช้พอร์ต 443 แทนที่พอร์ต 80
- เวอร์ชันแรกใช้การเข้ารหัสแบบ RC4 คีย์ 40 บิต ต่อมานิยมใช้ RSA 2048 bit

Web Security : SSL/TLS

- ▶ SSL พัฒนาโดย Netscape เป็นโปรโตคอลที่ใช้บริการเข้ารหัสและพิสูจน์ตัวตนระหว่างเว็บเซิร์ฟเวอร์กับไคลเอนต์
- ▶ เริ่มต้นจะมีการตกลงกันก่อนว่าจะใช้อัลกอริทึมและคีย์ใดในการเข้ารหัสและการพิสูจน์ตัวตน
- ▶ จากนั้นเริ่มสื่อสารโดยข้อมูลที่รับส่งมีการเข้ารหัสด้วยเซสชันคีย์
- ▶ เว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ส่วนใหญ่จะรองรับโปรโตคอลนี้อยู่แล้ว

Web Security : SSL/TLS [2]

- ▶ TLS ได้มีการพัฒนาต่อมาจาก SSL ซึ่งได้ขยายการรองรับ
ลายเซ็นดิจิทัล



การทำงานของ SSL เทียบกับ HTTP ปกติ

วิธีการส่งข้อมูลแบบปกติ



วิธีการส่งข้อมูลด้วย SSL



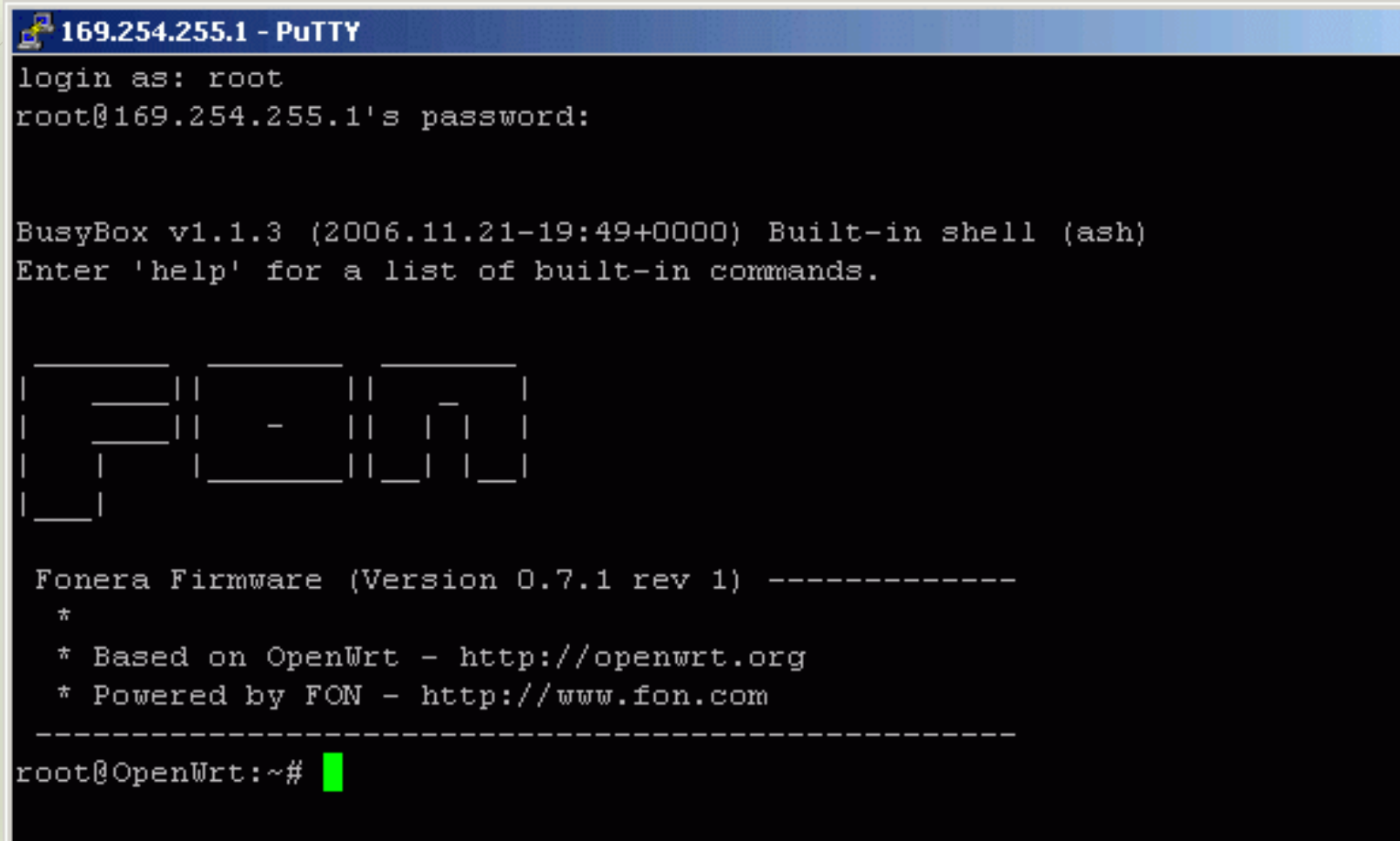
Remote Login & File Transfer Security

- การใช้งานรีโมทล็อกอินจำเป็นอย่างยิ่งที่จะต้องมีการเข้ารหัสข้อมูล เพื่อป้องกันการแอบดูข้อมูลที่สื่อสารกัน
- โพรโตคอลที่ใช้ในการรีโมทล็อกอินทั่วไปคือ TELNET ซึ่งได้มีการพัฒนาเป็นโปรโตคอล **SSH** เพื่อเข้ารหัสระหว่างการสื่อสาร
- โพรโตคอลที่ใช้ในการดาวน์โหลด-อัปโหลดไฟล์ คือ **FTP** ปกติจะไม่มีมีการเข้ารหัส จึงได้พัฒนาโปรโตคอล **SFTP** ขึ้นมาเพื่อเข้ารหัสข้อมูล

Remote Login & File Transfer Security: SSH

- SSH (Secure Shell) เป็นรูปแบบการรีโมทล็อกอินและ FTP ที่นิยมมากที่สุด ใช้สำหรับเข้ารหัสข้อมูลที่รับ-ส่งระหว่างไคลเอนต์และเซิร์ฟเวอร์
- ใช้พอร์ต 22 แทนพอร์ต 23 (TELNET) และ 21 (FTP)
- หลักการคือไคลเอนต์จะเชื่อมต่อไปยังเซิร์ฟเวอร์ เพื่อสร้าง Public Key สำหรับการเชื่อมต่อ ปัจจุบันใช้ RSA ร่วมกับ SHA-256 ในการเข้ารหัสข้อมูลและทำ Digital Signature
- โปรแกรม SSH ที่นิยม เช่น Putty, OpenTerm, OpenSSH

โปรแกรม Putty



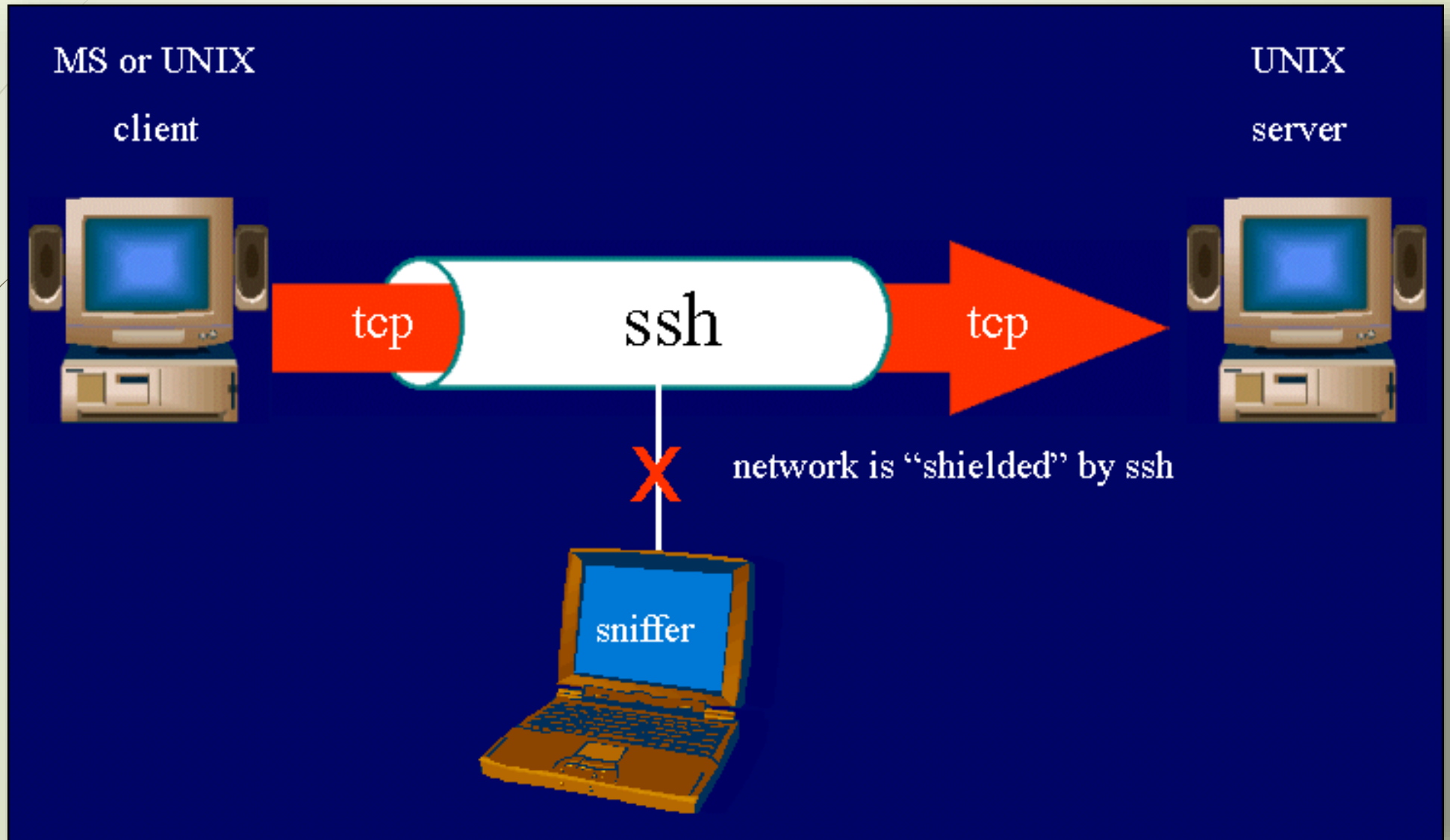
```
169.254.255.1 - PuTTY
login as: root
root@169.254.255.1's password:

BusyBox v1.1.3 (2006.11.21-19:49+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _____
 |   _   | |   _   | |   _   | | | | | | |
 |  _ |  | |  _ |  | |  _ |  |
 | |_) | | | |_) | | | |_) | |
 |  __/  | |  __/  | |  __/  |
 |_____||_____||_____||

Fonera Firmware (Version 0.7.1 rev 1) -----
*
* Based on OpenWrt - http://openwrt.org
* Powered by FON - http://www.fon.com
-----
root@OpenWrt:~# █
```

แบบจำลองการทำงานของ SSH

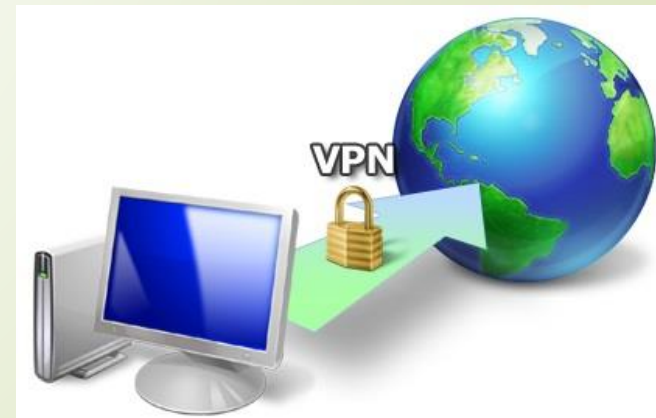


Network Security

- ▶ โพรโตคอลที่กล่าวมาข้างต้นทั้งหมดเป็นการเข้ารหัสข้อมูลในเลเยอร์ที่เหนือกว่าชั้นเน็ตเวิร์ค ส่วนใหญ่จะเป็นแอปพลิเคชันที่พัฒนาขึ้นเป็นพิเศษ
- ▶ แต่ถ้ามีการรักษาความปลอดภัยในระดับที่ต่ำลงมา เช่น ในระดับเน็ตเวิร์ค จะต้องใช้โปรโตคอลที่ทำงานในระดับเน็ตเวิร์ค
- ▶ โพรโตคอลที่มีการรักษาความปลอดภัยระดับเน็ตเวิร์ค เช่น VPN ส่วนโปรโตคอลย่อยที่นิยมคือ IPsec

Network Security : VPN

- เครือข่ายส่วนบุคคลเสมือน หรือ VPN (Virtual Private Network) หมายถึงระบบเครือข่ายส่วนบุคคลที่สร้างโดยแชร์ลิงก์ (เช่น อินเทอร์เน็ต)
- ช่วยให้ผู้ใช้สามารถแชร์ข้อมูลผ่านเครือข่ายสาธารณะโดยมีการเข้ารหัสไว้ ทำให้ดูเหมือนว่าเป็นการสื่อสารกันภายในเครือข่ายส่วนบุคคล
- ข้อดีคือทำให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเชื่อมต่อเข้ามายังเครือข่ายขององค์กรได้อย่างปลอดภัย

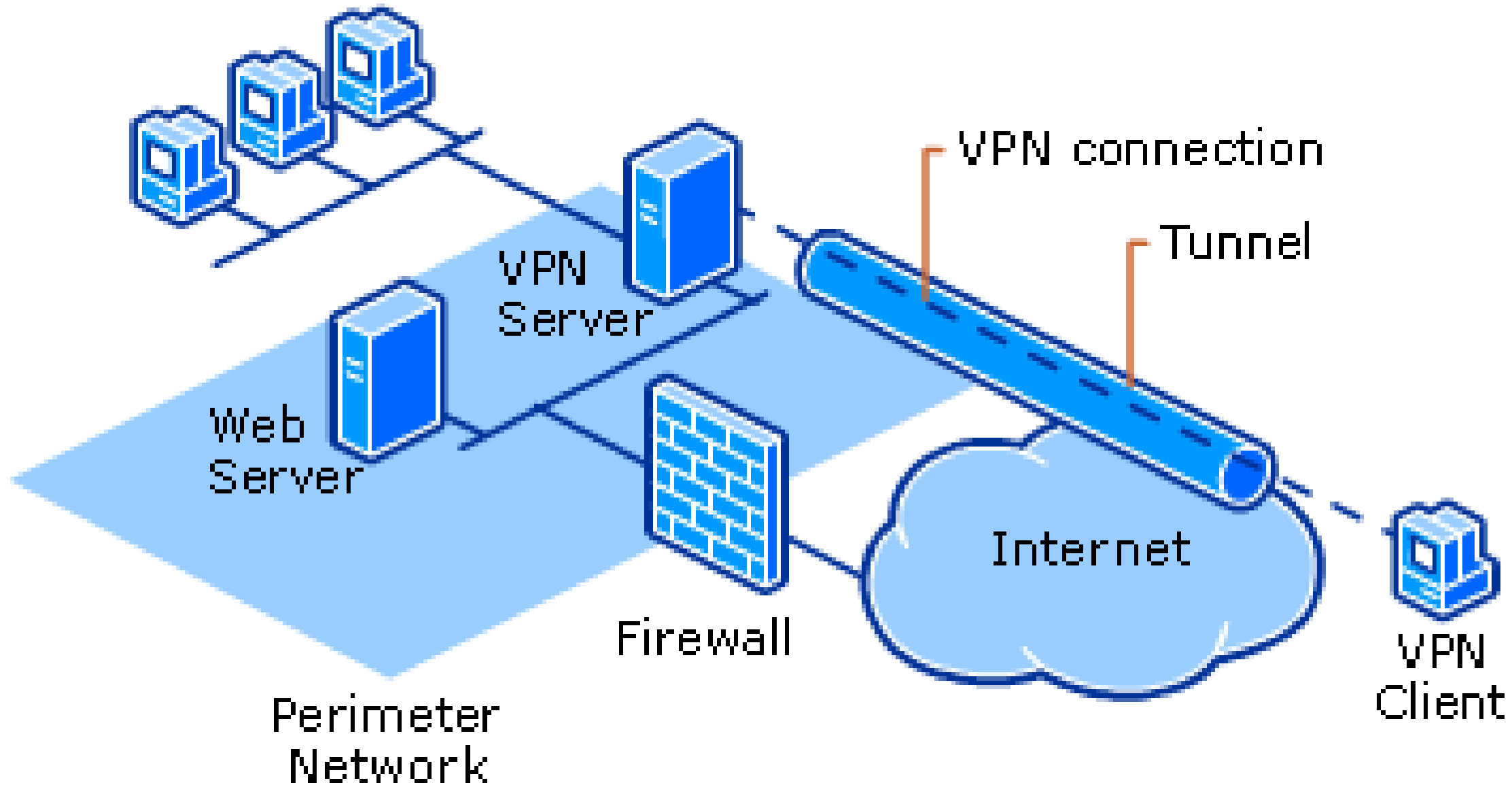


Network Security : VPN [2]

VPN แบ่งเป็น 3 ประเภท ขึ้นอยู่กับลักษณะการใช้งาน

- **Access VPN** : ใช้เชื่อมต่อผู้ใช้ระยะไกล เช่นพนักงานที่ต้องเดินทางบ่อยๆ
- **Intranet VPN** : เชื่อมต่อกับเครือข่ายย่อยขององค์กร ผ่านเครือข่ายอินเทอร์เน็ต เช่น สาขาย่อยของบริษัท
- **Extranet VPN** : ใช้เชื่อมต่อระหว่างองค์กร

แบบจำลองการทำงานของ VPN



Network Security : VPN [3]

โพรโตคอลที่ใช้สร้าง VPN มี 4 โพรโตคอล คือ

- ▶ PPTP (Point-to-Point Tunneling Protocol)
- ▶ L2F (Layer-2 Forwarding)
- ▶ L2TP (Layer-2 Tunneling Protocol)
- ▶ *IPSec (IP Security Protocol)
- ▶ SSL VPN (Secure Sockets Layer)

Network Security : VPN -> IPSec

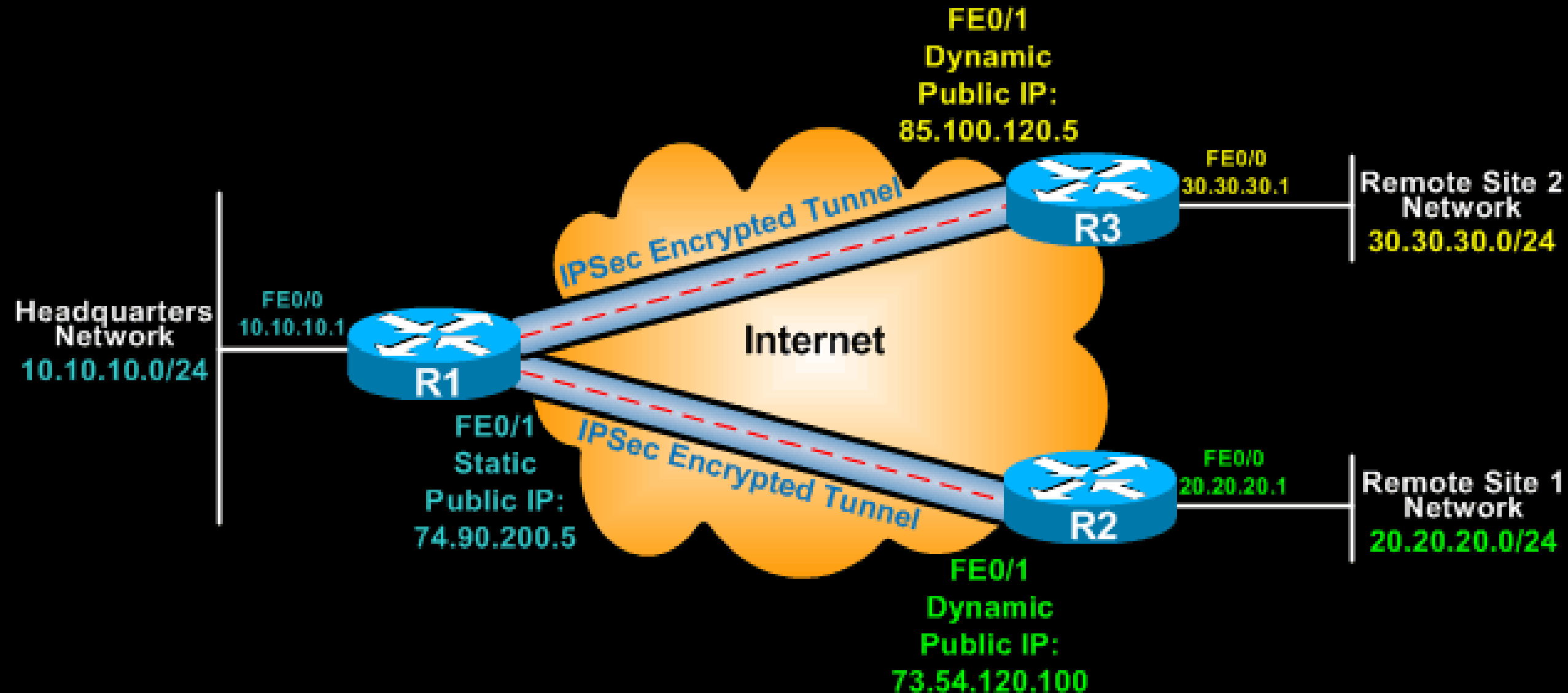
- เป็นโปรโตคอลที่รักษาความปลอดภัยข้อมูลในระดับเน็ตเวิร์กเลเยอร์
- ถือเป็นโปรโตคอลที่เหมาะสมที่สุดสำหรับการสร้าง VPN
- ออกแบบมาสำหรับการเข้ารหัสข้อมูลแพ็กเก็ตของโปรโตคอล IP
- รับรองความลับของข้อมูล (Confidentiality), ความคงสภาพของข้อมูล (Integrity) และการพิสูจน์ตัวตนของฝ่ายส่ง (Authentication)

Network Security : VPN -> IPSec [2]

อัลกอริทึมที่ IPSec ใช้เข้ารหัสข้อมูล คือ

- ➡ ใช้ Diffie-Hellman ในการแลกเปลี่ยนเซสชันคีย์ผ่านเครือข่ายสาธารณะ
- ➡ AES-GCM : สำหรับการเข้ารหัสข้อมูลและยืนยันตัวตน
- ➡ SHA2-256: ใช้ในการตรวจสอบความคงสภาพ
- ➡ Digital Certificate : สำหรับตรวจสอบเจ้าของพับลิคคีย์

IPSec VPN Architecture



การใช้งาน VPN ของมหาวิทยาลัยแม่โจ้ เพื่อสืบค้นข้อมูลจากภายนอกเครือข่ายมหาวิทยาลัย



The screenshot shows the website for the Central Library of Maejo University. The header includes the university logo and the text 'สำนักหอสมุด มหาวิทยาลัยแม่โจ้ CENTRAL LIBRARY MAEJO UNIVERSITY'. Below the header, there are navigation links: 'หน้าแรก', '+ สืบค้นทรัพยากร', '+ ข้อมูลองค์กร', 'VIDEO ON DEMAND', 'สายตรงผู้อำนวยการ', and a language selection button 'Select Language'. The main content area is titled 'การสืบค้นข้อมูลนอกเครือข่ายมหาวิทยาลัย' and contains a paragraph explaining that faculty and students can access external resources using VPN technology. It lists various types of resources available, such as online journals, e-books, and ThaiLIS (TDC). A section titled 'รายละเอียดเพิ่มเติม' provides instructions for different user groups: faculty and staff (username and password same as library system), students (username and password same as university system), and those without credentials (contact IT support at 0 5387 8505 or www.it.mju.ac.th).

หน้าแรก + สืบค้นทรัพยากร + ข้อมูลองค์กร VIDEO ON DEMAND สายตรงผู้อำนวยการ

การสืบค้นข้อมูลนอกเครือข่ายมหาวิทยาลัย

อาจารย์ บุคลากร นักศึกษา มหาวิทยาลัยแม่โจ้ สามารถสืบค้นข้อมูลจากภายนอกเครือข่ายมหาวิทยาลัยได้โดยใช้เทคโนโลยีระบบเครือข่ายเสมือนส่วนตัว หรือ Virtual Private Network (VPN) โดยสามารถสืบค้น และดาวน์โหลดข้อมูล จากฐานข้อมูลออนไลน์ ฐานข้อมูลหนังสือ/วารสารอิเล็กทรอนิกส์ ฐานข้อมูลวิทยานิพนธ์/วิจัย ฐานข้อมูลเอกสารอิเล็กทรอนิกส์โครงการ ThaiLIS (TDC) หรือการใช้งานระบบอื่นๆ ที่จำเป็นต้องใช้ IP Address ของมหาวิทยาลัยแม่โจ้

รายละเอียดเพิ่มเติม
คลิกที่นี่

- สำหรับอาจารย์และบุคลากร
username และ password เดียวกันกับการเข้าใช้งานระบบหนังสือเวียนอิเล็กทรอนิกส์
- สำหรับนักศึกษา
username และ password เดียวกันกับการเข้าใช้งานอินเทอร์เน็ตของมหาวิทยาลัย
- กรณีไม่มี username และ password สามารถติดต่อลงกะเบ็ญนี้ได้
ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ โทร. 0 5387 8505 เบอร์ภายใน 4040 www.it.mju.ac.th

<https://library.mju.ac.th/content.php?page=data&id=102:VPN>