Firewall

MS1 Thanin Muangpool

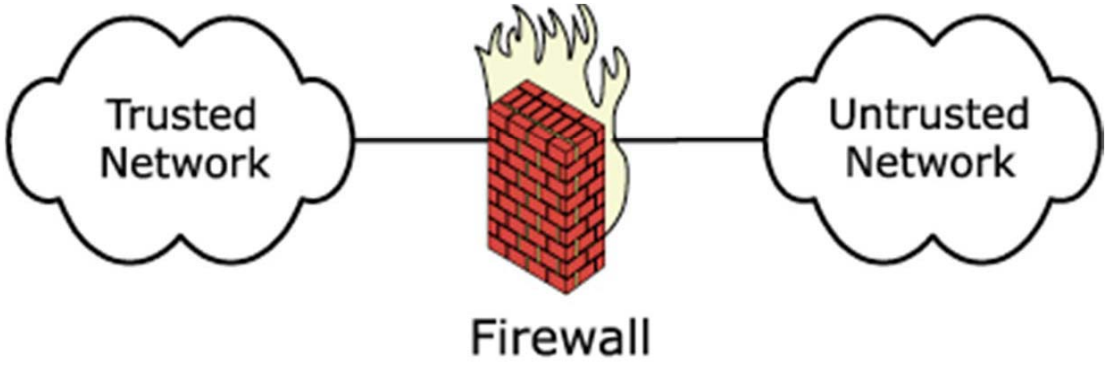
What is a Firewall ?

Firewall คือ ระบบที่ใช้ในการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และใช้ในการป้องกันการบุกรุกในระบบเครือข่ายคอมพิวเตอร์จากผู้ที่ไม่ได้ รับอนุญาตให้ใช้งานระบบดังกล่าว โดย Firewall จะถูกใช้เป็นตัวกำหนดกฎเกณฑ์ในการควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ระหว่างระบบเครือข่ายภายใน (Internal Private Network) กับเครือข่ายภายนอก (External Public Network) ให้เป็นไปตามนโยบายขององค์กร

Type of Firewall

Firewall จำแนกได้เป็น 2 กลุ่ม ดังนี้

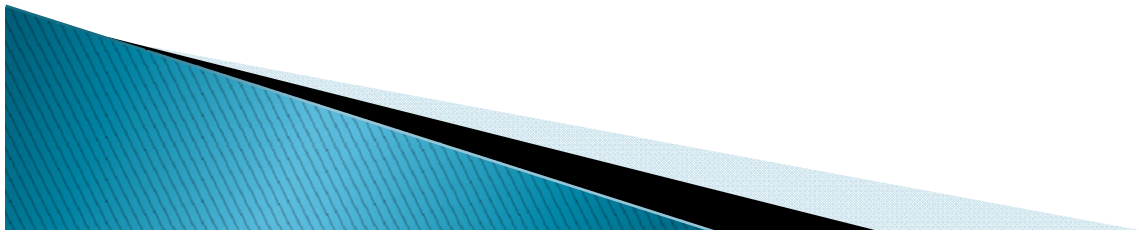
1. Processing Mode
2. Development Generation



Type of Firewall →Processing Mode

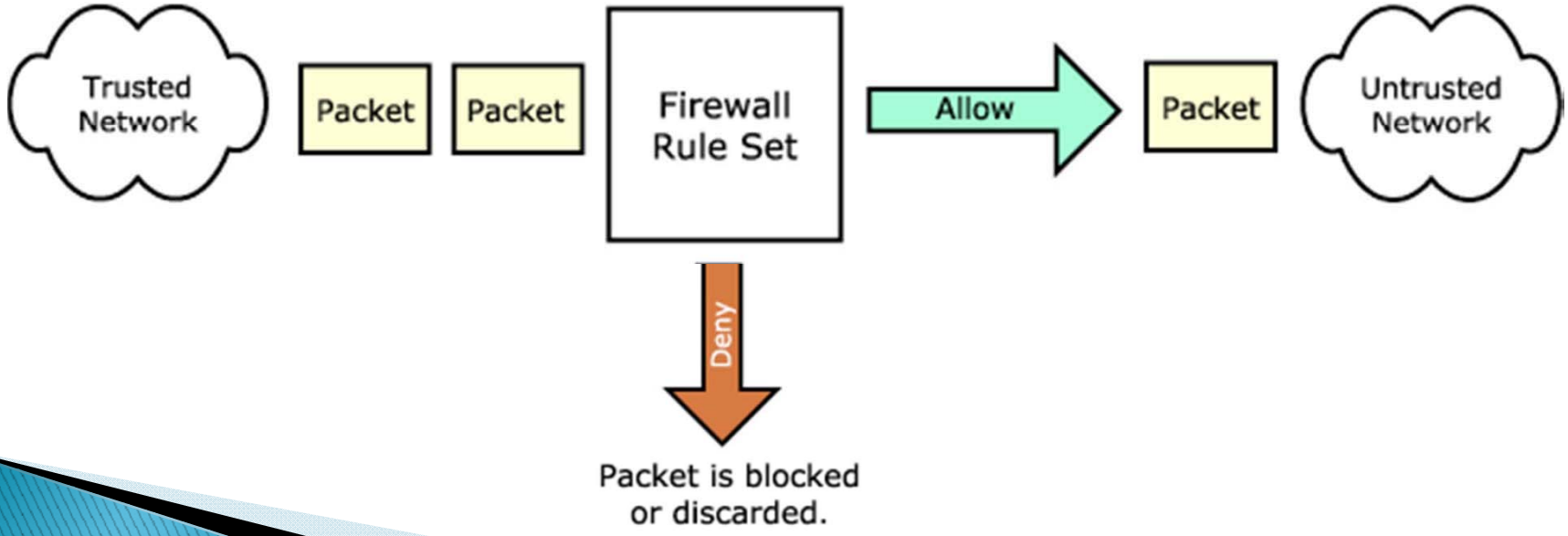
Processing Mode แบ่งออกเป็น 5 ประเภท ดังนี้

1. Packet Filtering
2. Application Firewall
3. Circuit Gateways
4. MAC Layer
5. Hybrid Firewall

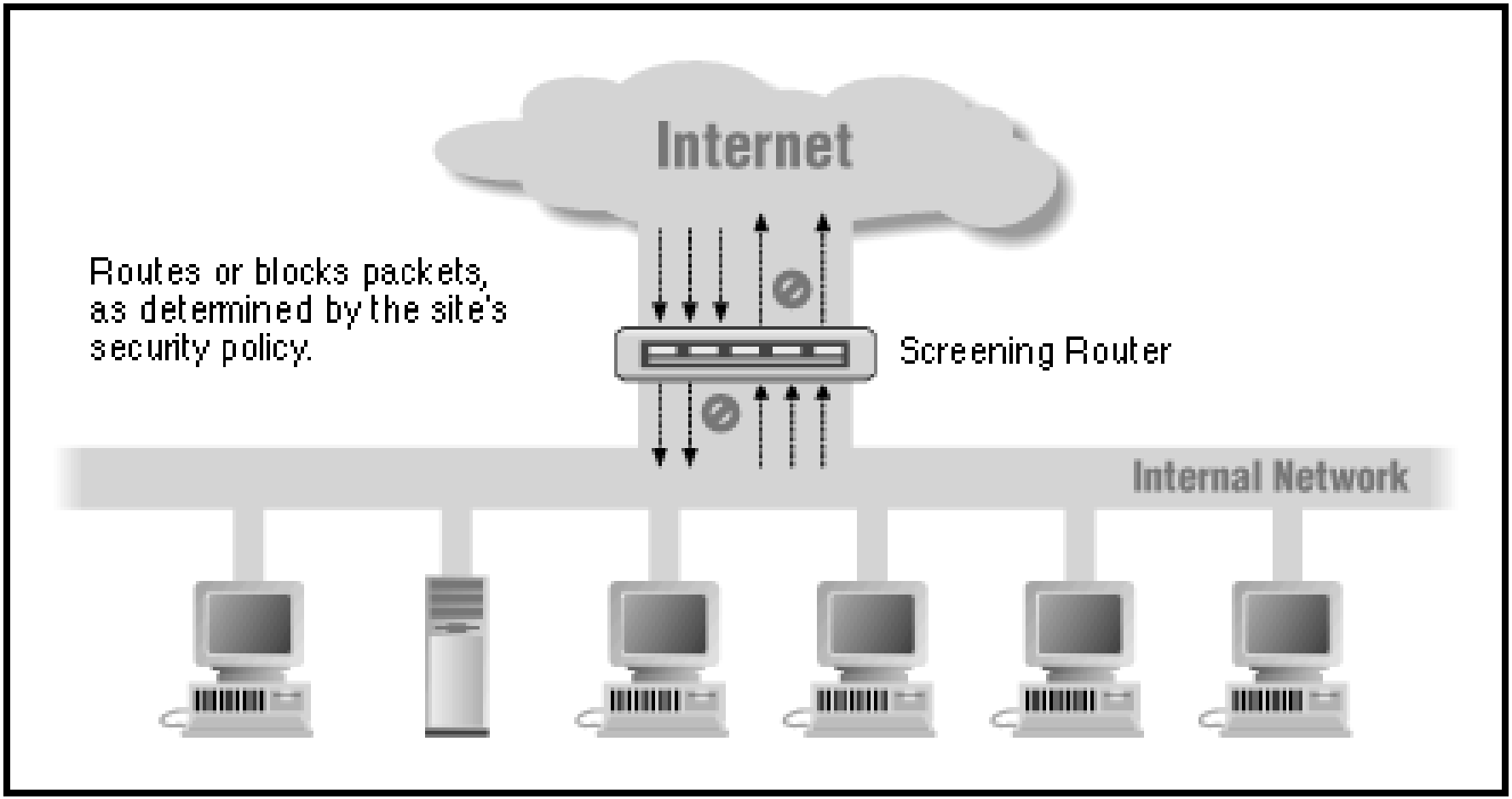


Processing Mode → Packet Filtering

Packet Filter ทำงานโดยทำการหาเส้นทางและส่งต่ออย่างมีเงื่อนไข (Screening Router) โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ใน header ของ Packet ที่ผ่านเข้ามา เทียบกับกฎ (Rules) ที่กำหนดไว้ และตัดสินว่าควรจะทิ้ง (Drop) หรือว่าจะยอม (Accept) Packet



Processing Mode → Packet Filtering

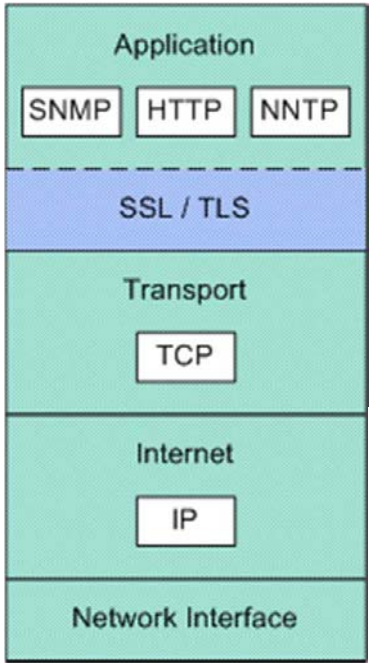


Processing Mode → Packet Filtering

Packet Filter จะทำงานที่ Internet Layer and Transport Layer ใน Internet Model

ใน Internet Layer จะมี Attribute ที่สำคัญต่อ Packet Filtering ดังนี้

- Source Port
- Destination Port
- Type of Protocol (TCP UDP และ ICMP)



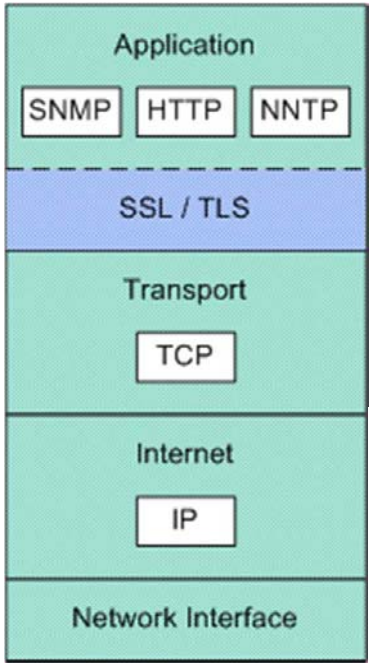
Processing Mode → Packet Filtering

ใน Transport Layer จะมี Attribute ที่สำคัญต่อ Packet Filtering ดังนี้

- Source Port
- Destination Port
- Flag (TCP)
- ICMP Massage (ICMP)

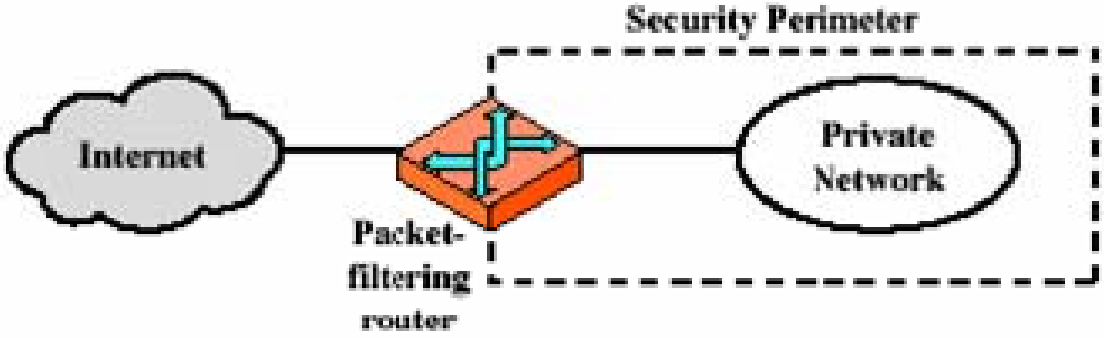
Port ของ Transport Layer ทั้ง TCP และ UDP จะเป็นสิ่งที่บอกถึง Application ที่ Packet ต้องการติดต่อ เช่น Port 80 หมายถึง HTTP

Port 21 หมายถึง FTP เป็นต้น

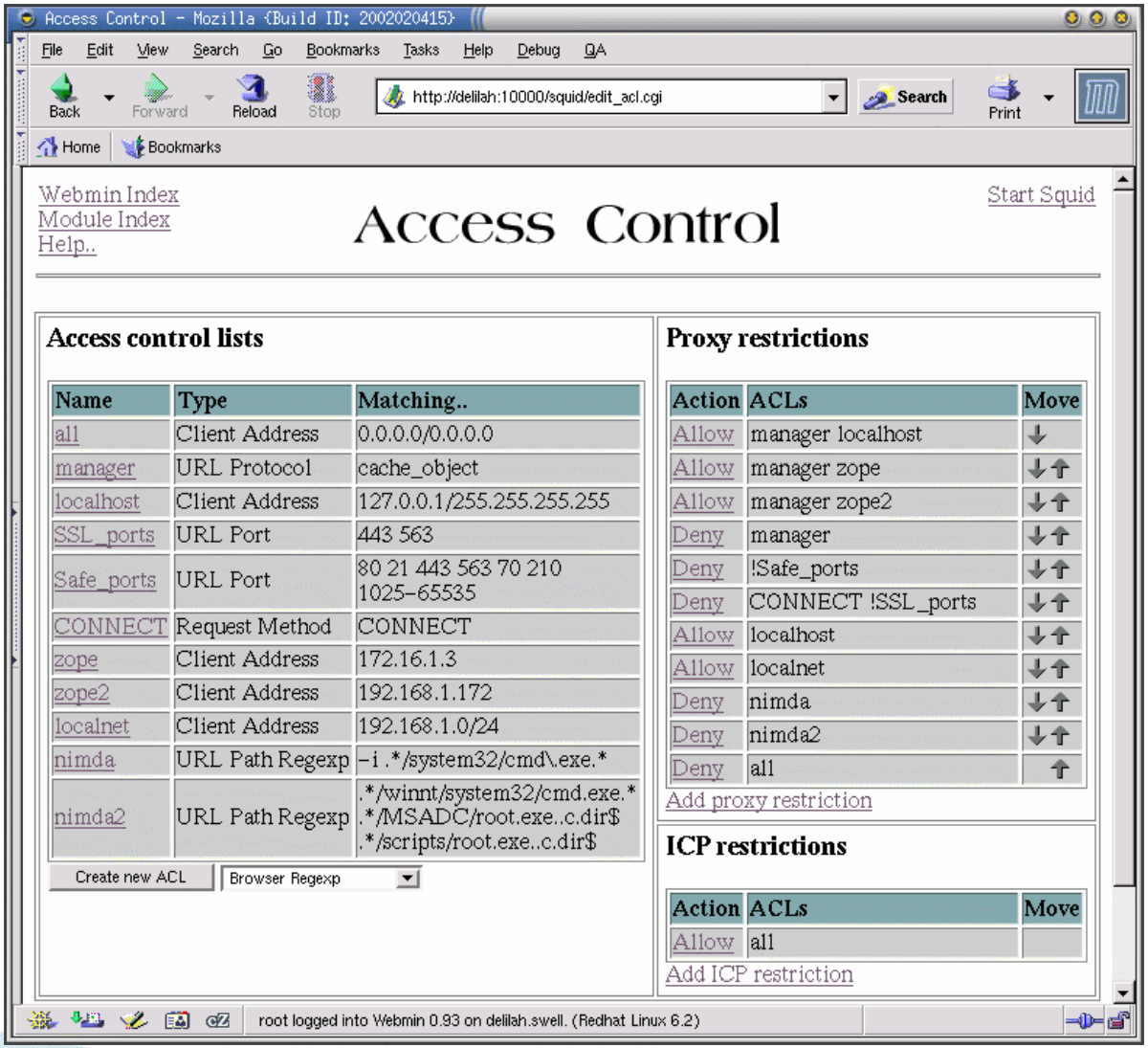


Processing Mode → Packet Filtering

Address Restriction Rule เป็นกฎการตรวจสอบ Data Packet ซึ่งจะทำการติดตั้งไว้ที่อุปกรณ์เครือข่าย เช่น Router โดยจะกำหนด Rule ไว้ในตาราง Access Control List : ACL เพื่อเก็บไว้เปรียบเทียบกับ Data Packet ที่เข้ามาว่าจะยอมรับหรือปฏิเสธ ตัวอย่างเช่น



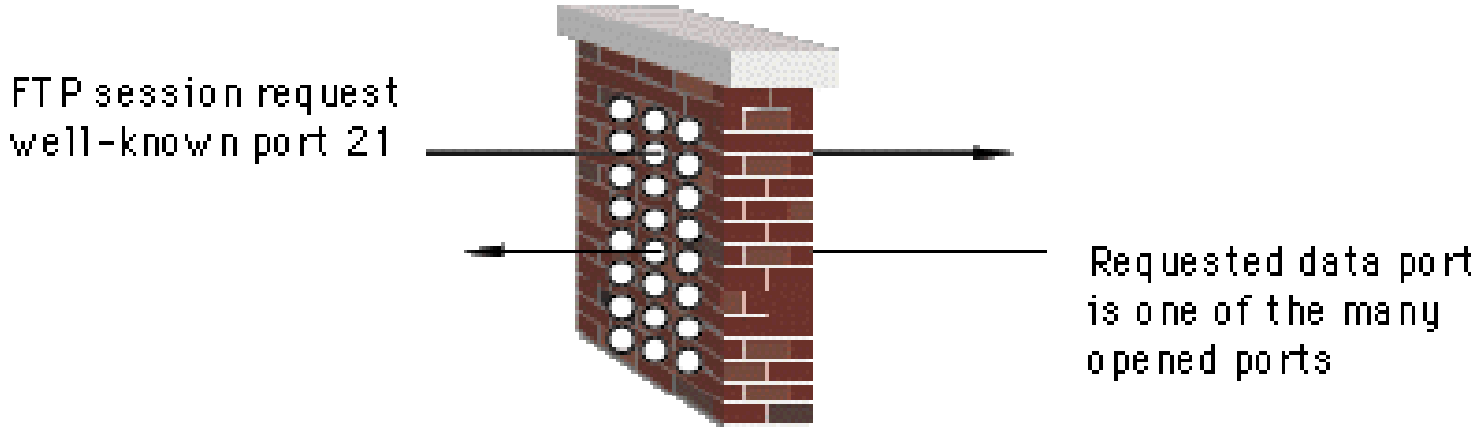
Processing Mode → Packet Filtering



Processing Mode → Packet Filtering

Packet Filtering Firewall แบ่งชนิดย่อยออกเป็น 3 ชนิด คือ

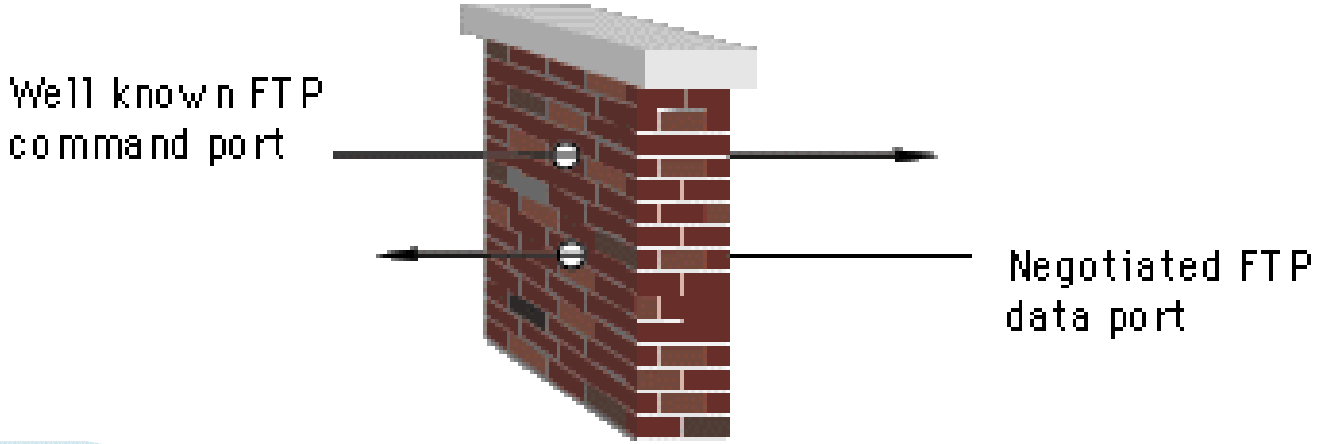
1. Static Filtering or Constant or Unchanging Filtering เป็นการตรวจสอบว่าอนุญาตหรือปฏิเสธ Data Packet พร้อมกับเลือกว่าจะเปิดหรือปิด Port ที่ถูกร้องขอจากการเชื่อมต่อภายนอก ถ้าเปิดก็เปิดทั้งหมด ถ้าปิดก็ปิดทั้งหมด จึงเป็นช่องโหว่ให้ถูกโจมตีได้ง่ายจากผู้ไม่หวังดี



Processing Mode → Packet Filtering

Packet Filtering Firewall แบ่งชนิดย่อยออกเป็น 3 ชนิด คือ

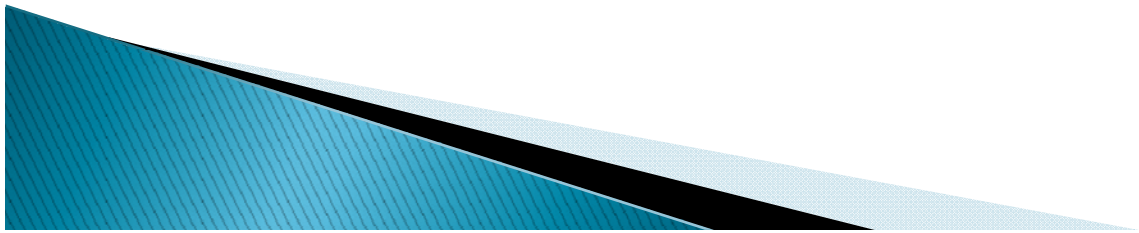
2. Dynamic Filtering เป็นกลไกที่ยืดหยุ่นกว่าแบบ Static Filtering เพราะสามารถที่จะเลือกเปิด Port ที่ต้องการได้ ซึ่งจะทำการตรวจสอบจาก Request ที่มาพร้อมกับ Packet ที่ต้องการให้เปิด Port และจะเปิดจนกว่าจะจบ Session ของการทำงาน



Processing Mode → Packet Filtering

Packet Filtering Firewall แบ่งชนิดย่อยออกเป็น 3 ชนิด คือ

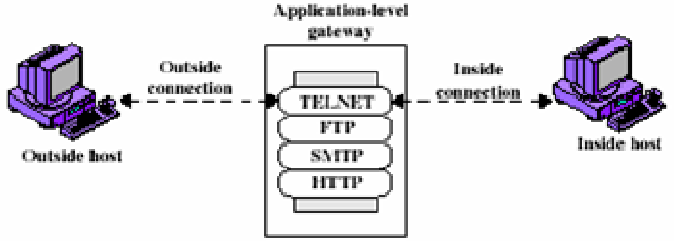
3. Stateful Inspection or Stateful Firewall เป็นกลไกที่รวมทั้ง Static and Dynamic Filtering เข้าด้วยกัน แต่จะมีเพิ่มการกำหนดระยะเวลา เมื่อ Packet ใดไม่มีการตอบรับภายในระยะเวลาที่กำหนด Firewall จะตัดการเชื่อมต่อ เพื่อสร้างการเชื่อมต่อกับ Request ใหม่ทันที



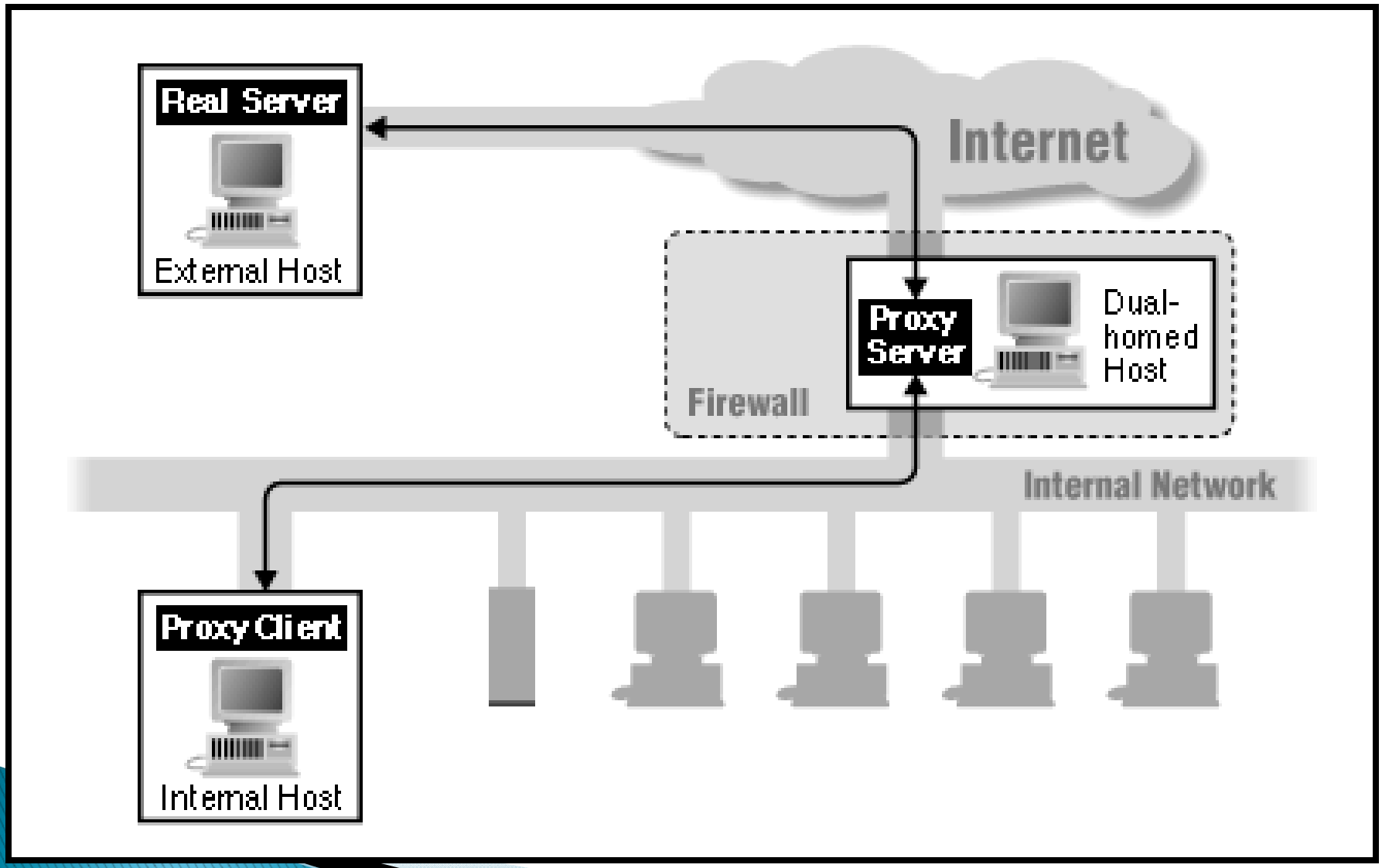
Processing Mode → Application Firewall

Application Firewall or Application-Level Firewall or Application Gateway ทำหน้าที่เพิ่มความปลอดภัยของ Network System โดยการควบคุมการเชื่อมต่อระหว่าง Network ภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของ Application Layer

เมื่อ Client ต้องการใช้เซอร์วิสภายนอก Client จะทำการติดต่อไปยัง Proxy ก่อน Client จะเจรจา กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ 2 การเชื่อมต่อ คือ Client กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่



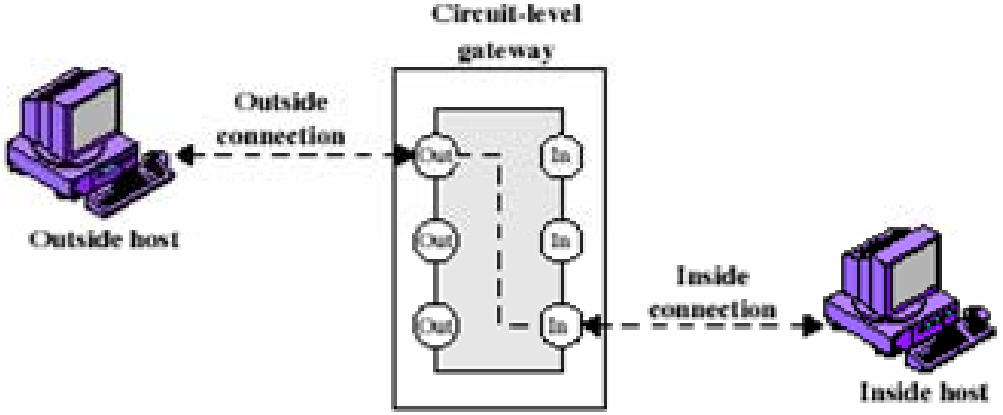
Processing Mode → Application Firewall



Processing Mode → Circuit Gateway Firewall

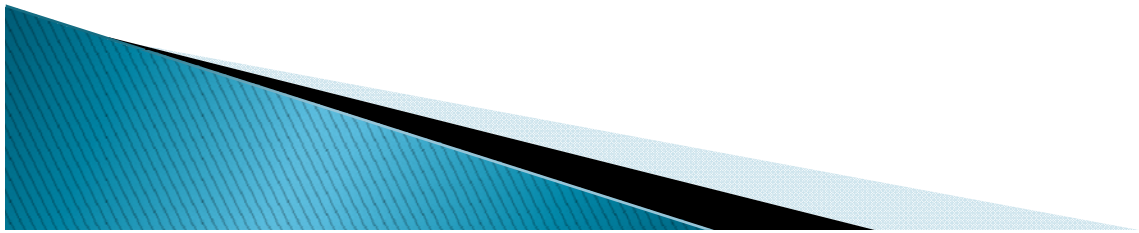
เป็น Firewall ที่ทำงานบน Transport Layer ของ OSI Model ซึ่งจะไม่ตรวจสอบข้อมูลใน Packet แต่จะตรวจสอบ Connection ระหว่าง User กับ Network ภายนอก และป้องกันการเชื่อมต่อโดยตรงระหว่าง User กับเครื่องอื่นๆ ภายนอกเครือข่าย

Circuit Gateway Firewall จะสร้าง Virtual Circuit ขึ้นมาจาก Library เพื่อจัดการการเชื่อมต่อโดยที่ User ไม่ทราบ ถ้าเส้นทางใดไม่ตรงตามกฎ ก็จะปฏิเสธการเชื่อมต่อ ซึ่งการสร้าง Virtual Circuit สามารถที่จะให้บริการ User ได้หลายคน สามารถติดต่อกับ Network ภายนอกได้หลาย Network



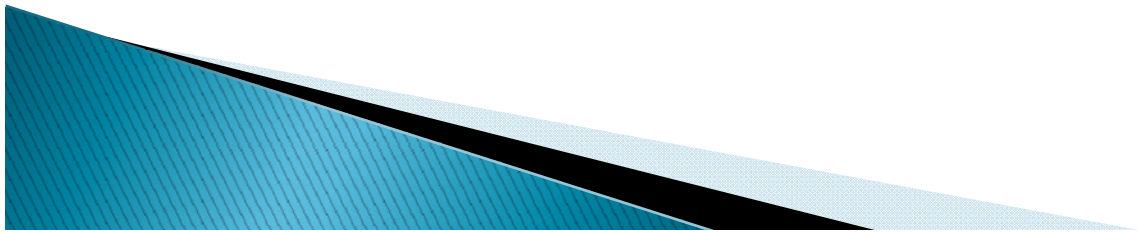
Processing Mode → MAC Layer Firewall

เป็น Firewall ที่ทำงานบน Data Link Layer ของ OSI Model ซึ่งสามารถระบุ Host Computer ได้ในขณะการกลั่นกรอง Packet โดยดูจาก MAC Address ที่เชื่อมโยงกับตาราง ACL เพื่อการตรวจสอบ Packet ที่มาพร้อมกับ Host Computer



Processing Mode → Hybrid Firewall

เป็น Firewall ที่รวมเอาความสามารถของ Firewall ชนิดอื่น ๆ เข้าด้วยกัน ซึ่งจะทำให้องค์กรสามารถเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของระบบได้มากยิ่งขึ้น



Type of Firewall →Development Generation

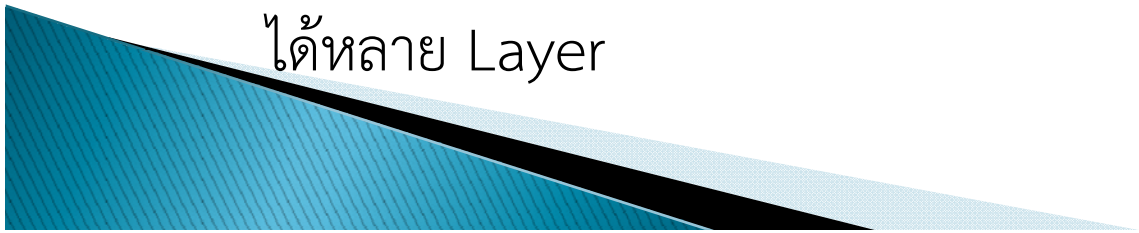
First Generation Firewall ส่วนใหญ่จะเป็นแบบ Static Packet Filtering Firewall

Second Generation Firewall จะเป็นแบบ Application Firewall

Third Generation Firewall จะเป็นแบบ Stateful Inspection Firewall

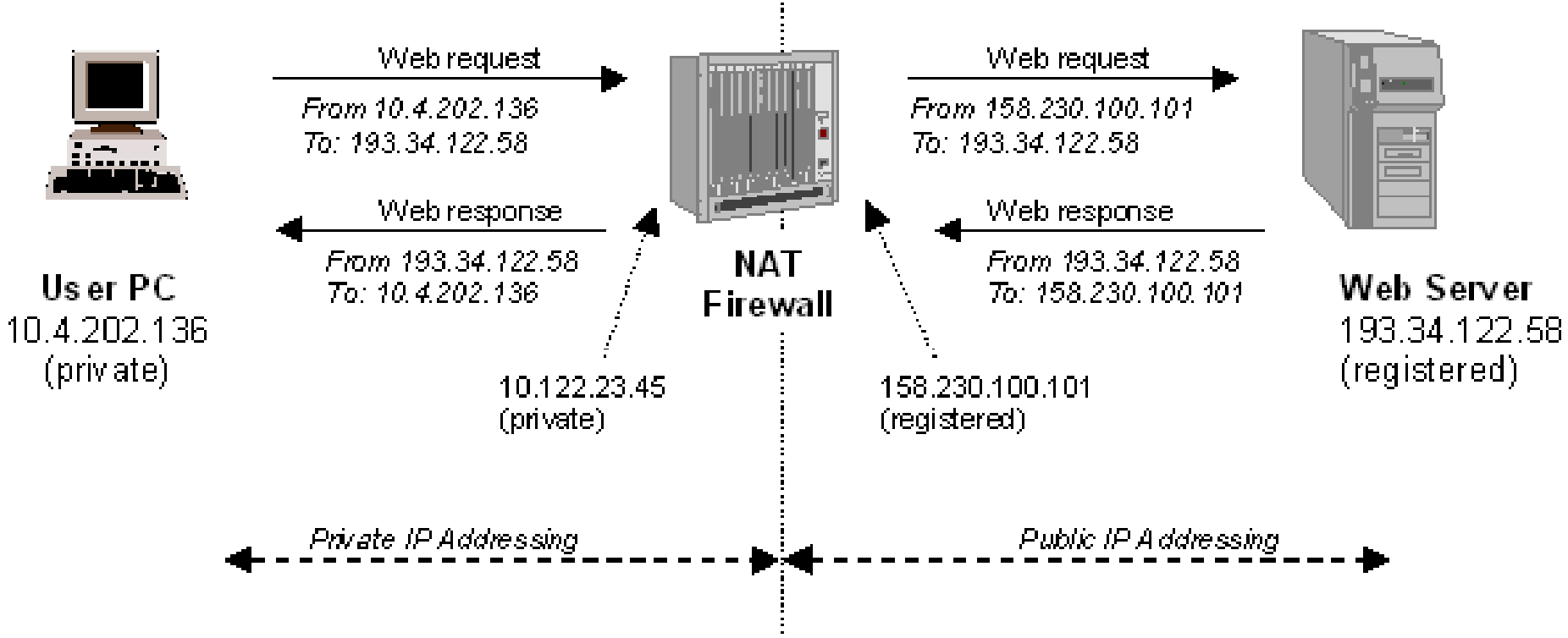
Fourth Generation Firewall จะเป็นแบบ Dynamic Packet Filtering Firewall

Fifth Generation Firewall จะเป็นแบบ Kernel Firewall ซึ่งเป็น Firewall ที่ทำงานกับระบบปฏิบัติการที่เป็น Kernel สามารถตรวจสอบได้หลาย Layer



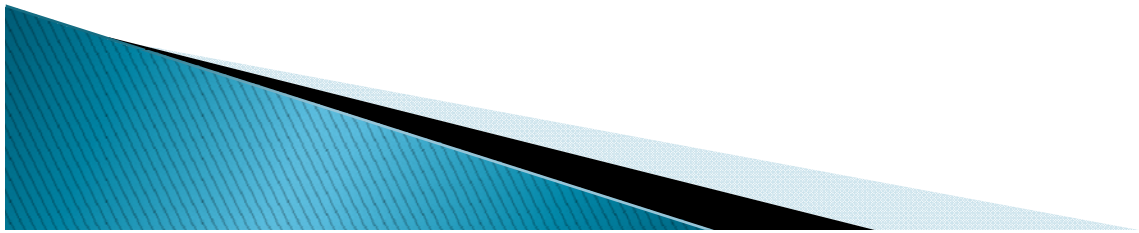
Network Address Translation : NAT Firewall

เป็น Firewall ที่ป้องกันการลักลอบนำ IP Address ไปใช้งาน โดยจะซ่อน IP ที่แท้จริงไว้ และแสดงให้ภายนอกเห็นเฉพาะ IP NAT เท่านั้น

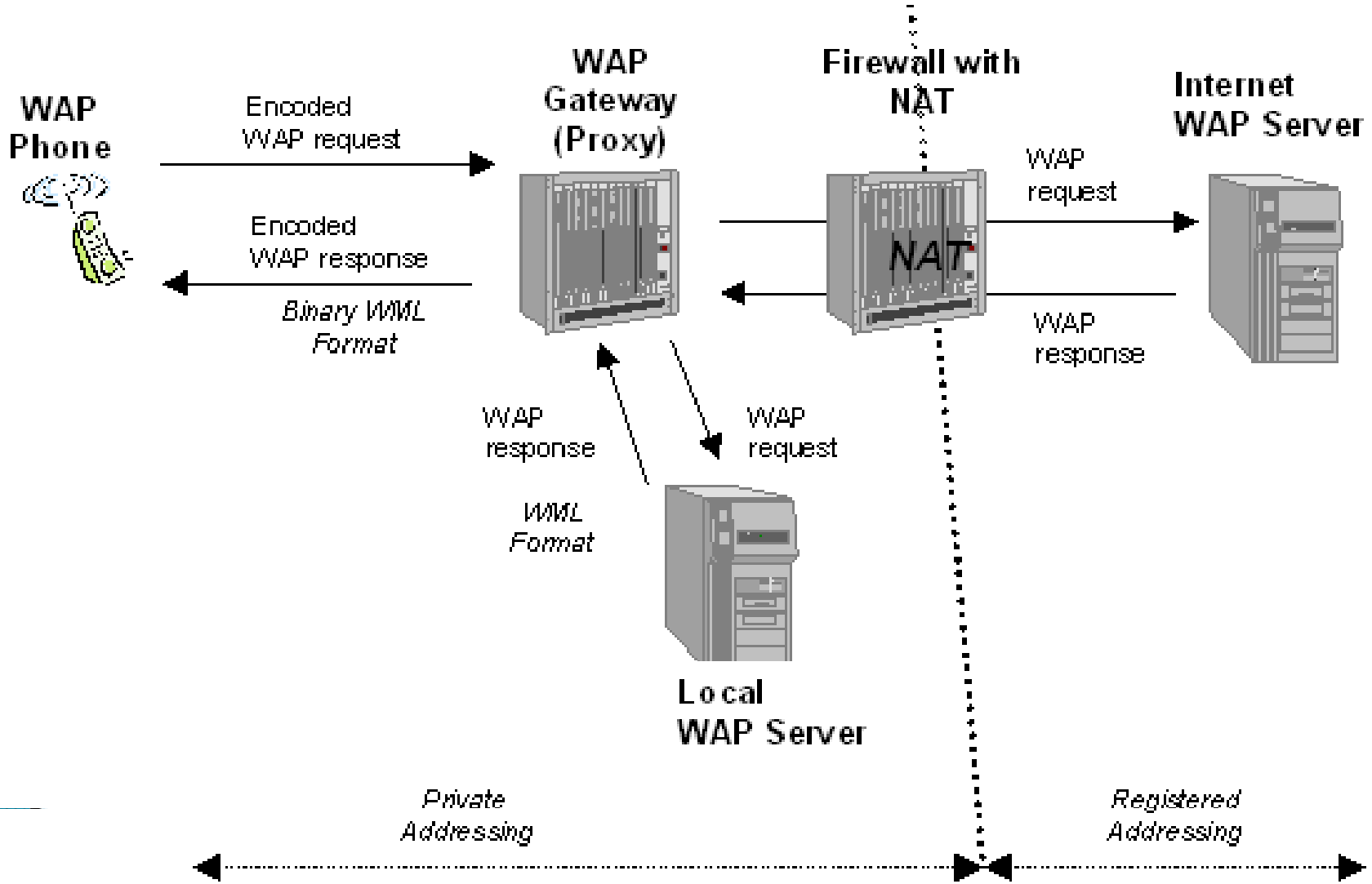


Network Address Translation : NAT Firewall

เป็น Firewall ที่เหมาะกับ Small Office/Home Office : SOHO ปัจจุบันได้นำมาใช้กับ DSL/ADSL จะทำการติดตั้งไว้กับอุปกรณ์ DSL/ADSL Router เรียกว่า SOHO Firewall เริ่มแรกจะเป็นแบบ Statefule Inspection Firewall ได้อย่างเดียว ปัจจุบันมีการพัฒนาความสามารถ Packet Filtering ร่วมกับ WAP และให้บริการ NAT Firewall และตรวจสอบ MAC Address ให้ด้วย



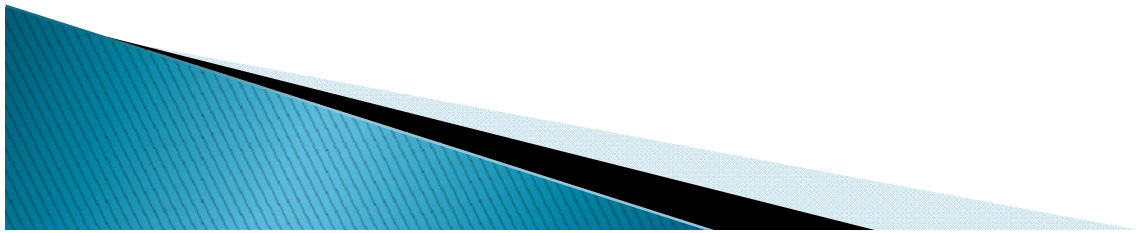
Network Address Translation : NAT Firewall



Firewall Architecture

มีทั้งหมด 4 รูปแบบ คือ

1. Packet Filtering Router
2. Screened Host Firewall
3. Dual-homed Host Firewall
4. Screened Subnet Firewall



Firewall Architecture → Packet Filtering Router

จะใช้ Router ทำหน้าที่เป็น Firewall กั้นระหว่างเครือข่ายในองค์กรกับภายนอกองค์กร ซึ่งจะกรอง Packet ที่ตรงกันกับตาราง ACL เท่านั้นที่จะสามารถเข้ามาในเครือข่ายภายในองค์กรได้

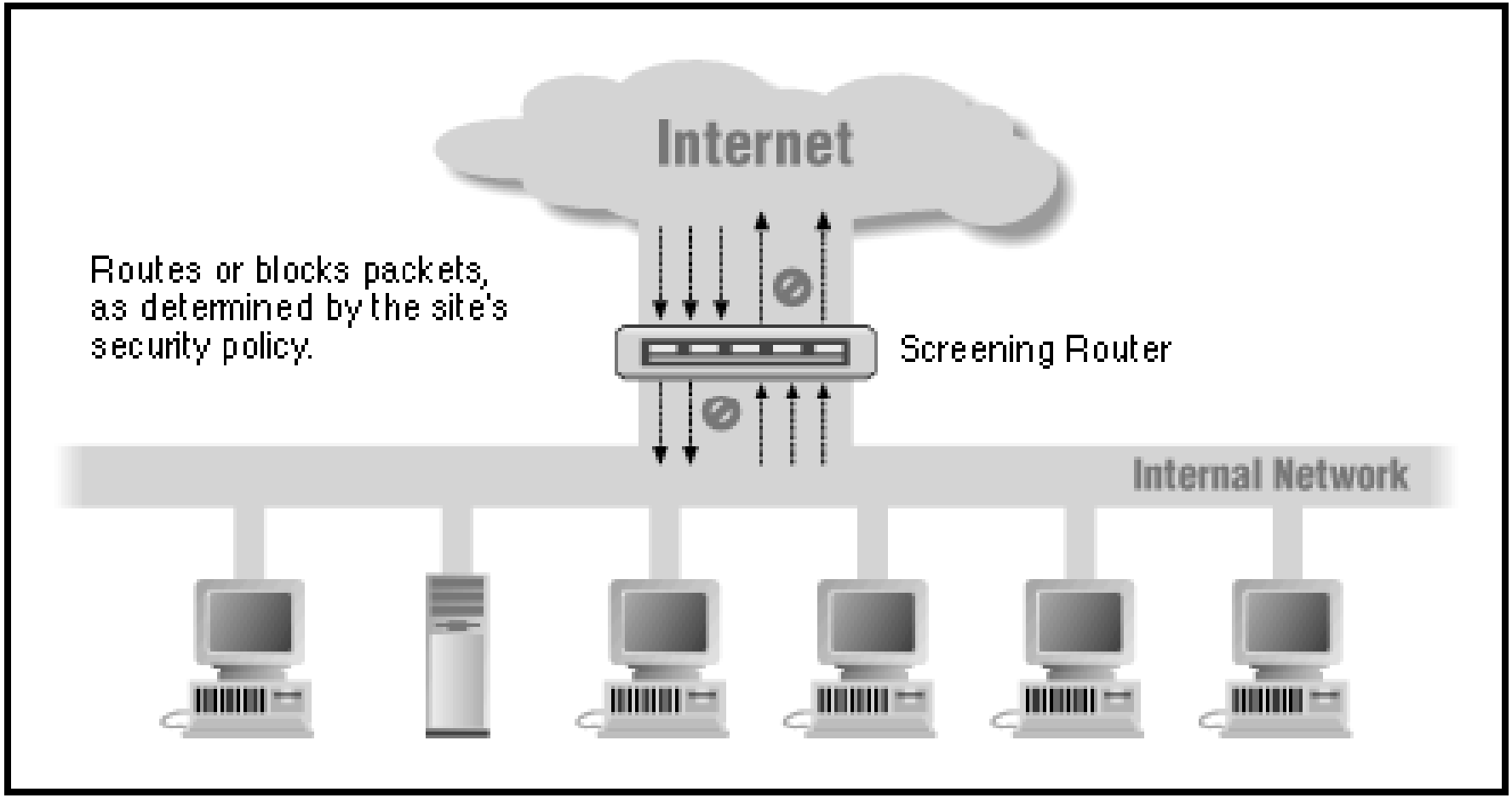
ข้อดี

- Implement ง่าย
- มีความเร็วสูง
- ประหยัดค่าใช้จ่าย

ข้อเสีย

- ไม่มีระบบการตรวจสอบและตรวจจับที่เข็มงวด
- ยิ่งเพิ่มกฎเกณฑ์ในตาราง ACL มาก จะทำให้ระบบช้าลง

Firewall Architecture → Packet Filtering Router



Firewall Architecture → Screened Host Firewall

ใช้ Router เป็น Packet Filtering Firewall ทำการกรอง Packet และใช้ Server เป็น Proxy Server เรียกว่า Bastion Host ตรวจสอบการบริการ Application ที่เข้ามา เพื่อทำการบันทึกก่อนส่งให้ User ที่ร้องขอ ในการส่งคำร้องขอข้อมูลภายนอกเครือข่ายจะต้องผ่าน Bastion Host ก่อนเสมอ Client Internal Network จะไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายภายนอกโดยตรง

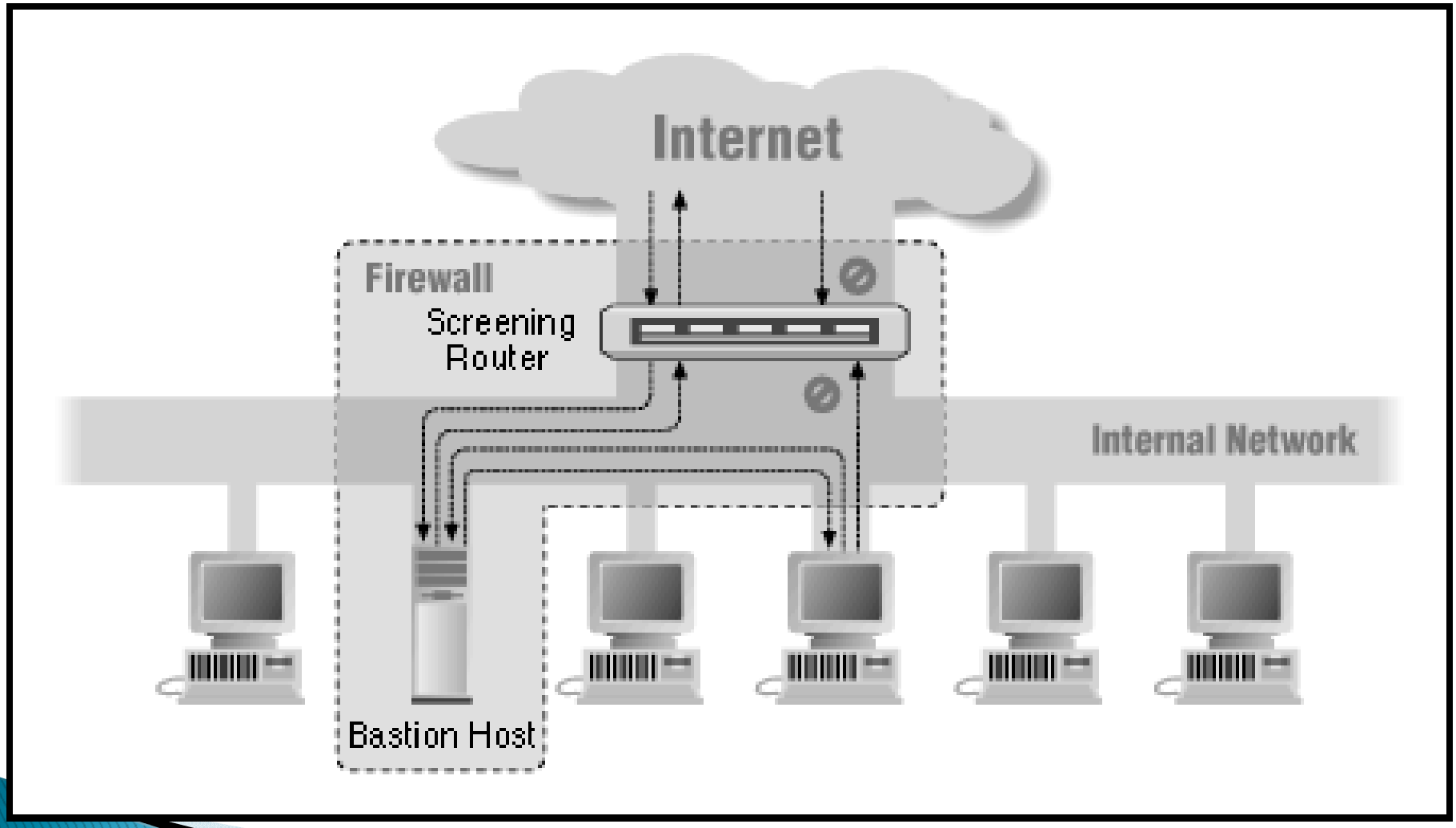
ข้อดี

- ประหยัดค่าใช้จ่าย

ข้อเสีย

- ถ้ามีการโจมตี Bastion Host สำเร็จ ก็จะได้ข้อมูล Client ทั้งหมด

Firewall Architecture → Screened Host Firewall



Firewall Architecture → Dual-homed Host Firewall

Bastion Host มี NIC 2 Card เพื่อเชื่อมต่อกับ Private Network and Public Network ทุกเส้นทางเข้าออกของข้อมูลจะผ่าน Firewall

การ Implement Firewall ส่วนใหญ่จะใช้ NAT Firewall จะเรียกว่า NAT Server

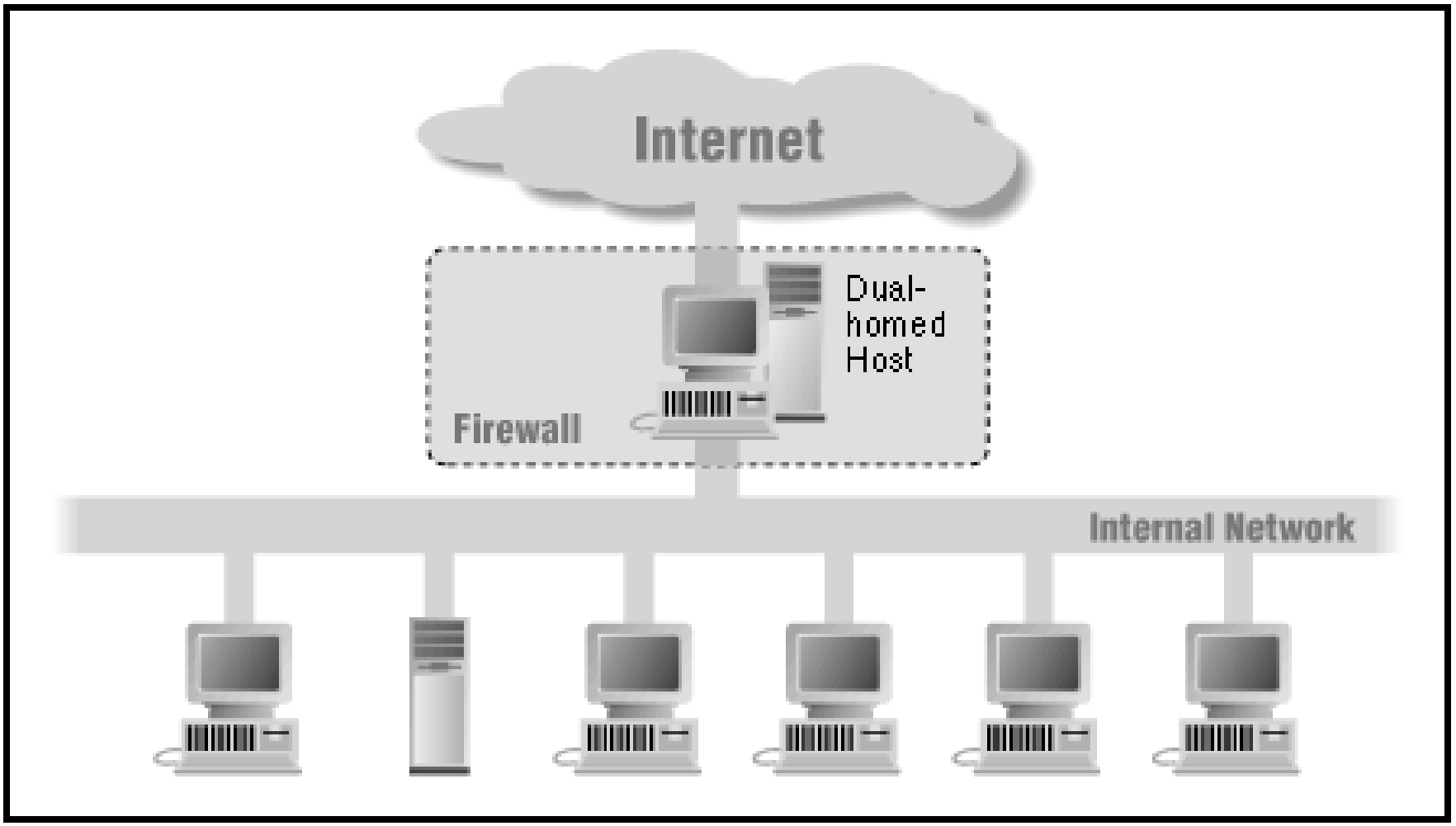
ข้อดี

- ป้องกันการโจมตีได้ 2 ระดับ
- ป้องกันการสแกน IP Address Private Network
- ประหยัดค่าใช้จ่าย

ข้อเสีย

- ซับซ้อน ทำงานช้า
- รองรับ Traffic ได้น้อยกว่า Packet Filtering Firewall
- ต้องการทรัพยากรมากกว่ารูปแบบอื่น

Firewall Architecture → Dual-homed Host Firewall



Firewall Architecture → Screened Subnet Firewall

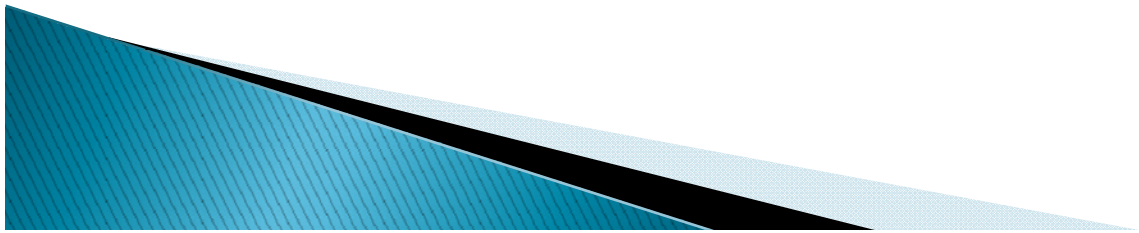
จะใช้ Packet Filtering Router 2 ตัววางไว้ทั้ง Internal and External Network โดยมี Bastion Host ตั้งแต่ 1 เครื่องขึ้นไป ทำหน้าที่ป้องกัน Private Network โดยแยกมาอยู่ในเขตที่เรียกว่า Demilitarized Zone : DMZ อยู่ระหว่าง Internal and External Network

ข้อดี

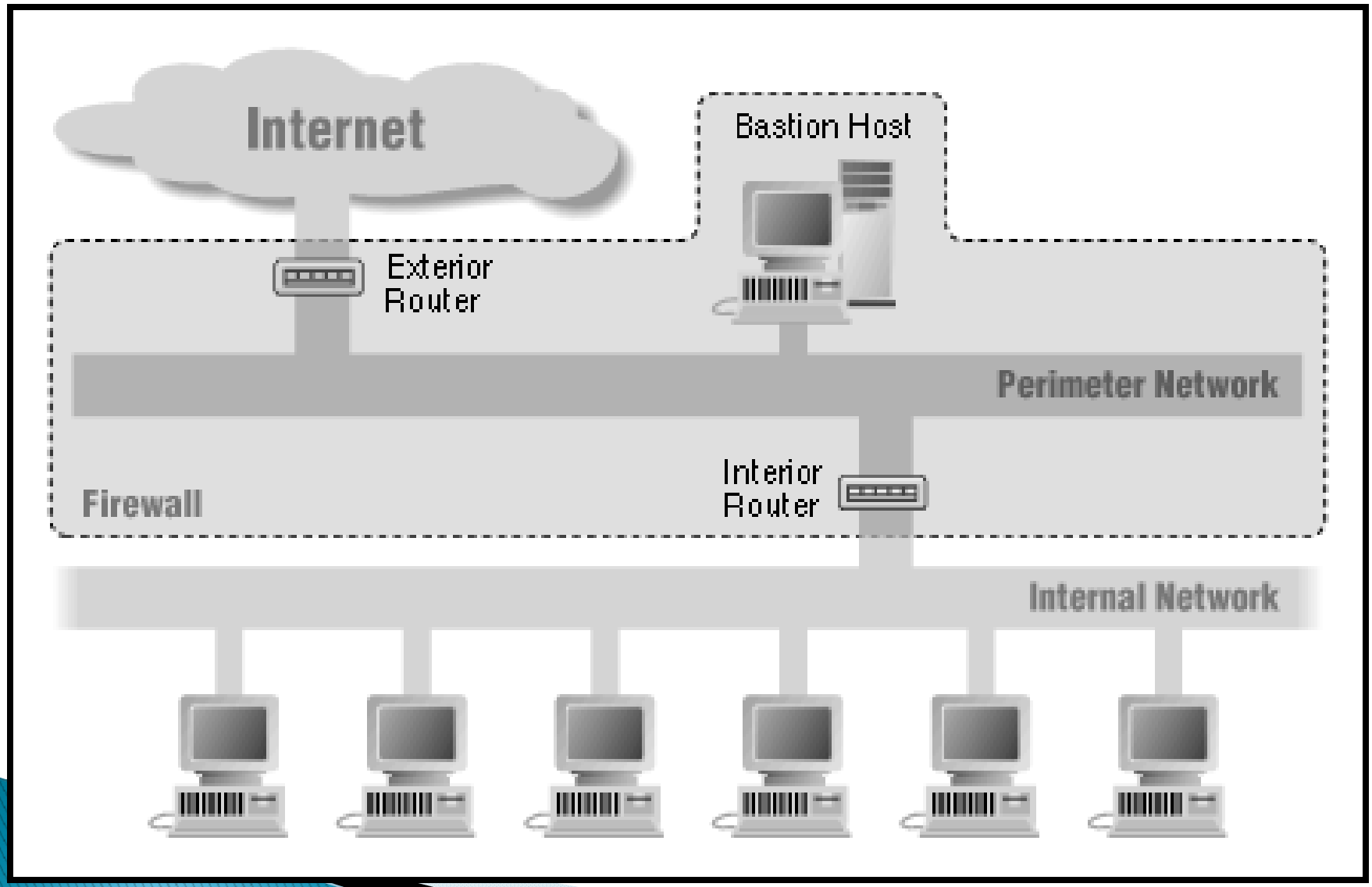
- มีความปลอดภัยสูง

ข้อเสีย

- ค่าใช้จ่ายสูง
- ระบบมีความซับซ้อน จัดการยาก



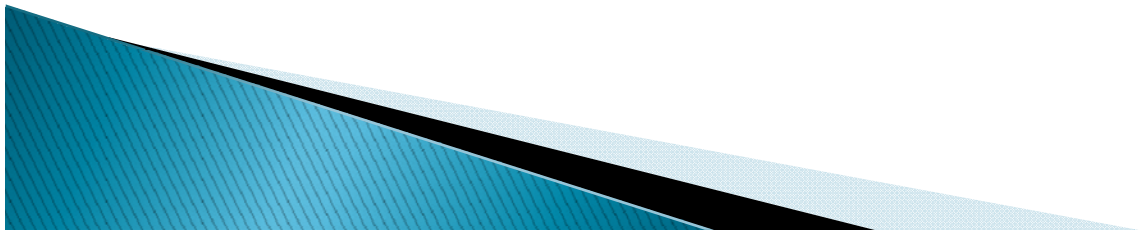
Firewall Architecture → Screened Subnet Firewall



การปรับแต่งคุณสมบัติของ Firewall

เพื่อให้สอดคล้องกับ Security and Business Policy จำเป็นต้องมีการกำหนดกฎเกณฑ์ เพื่อใช้เป็นข้อบังคับให้ User ปฏิบัติเหมือนกัน ตัวอย่างเช่น

1. Traffic จะอนุญาตเฉพาะ Trusted Network
2. Device ไม่สามารถเข้าถึงได้โดยตรงจาก Public Network
3. SMTP จะต้องผ่านการตรวจสอบจาก Gateway เพื่อกรอง Message
4. ICMP or Ping Service จะต้องปฏิเสธ
5. Block Telnet ถ้าต้องการเข้าถึงให้ผ่าน VPN



Load Balancing Firewall

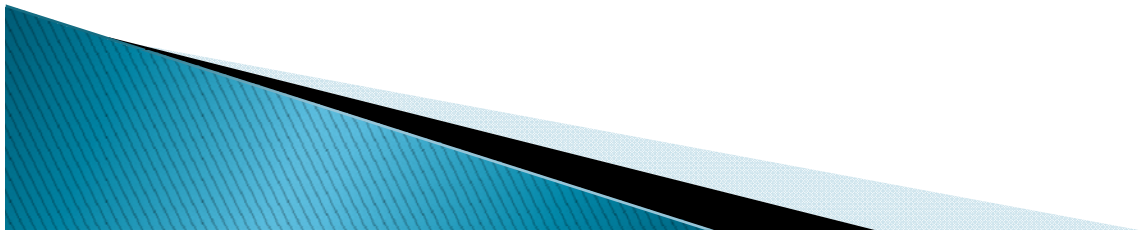
เพื่อเพิ่มขีดความสามารถให้กับ Firewall รองรับระบบเครือข่ายที่มีความเร็วในการรับ-ส่งข้อมูลสูง โดยกลุ่ม Firewall Array ทำหน้าที่ประมวล Data Packet แบบ Parallel

ข้อดี

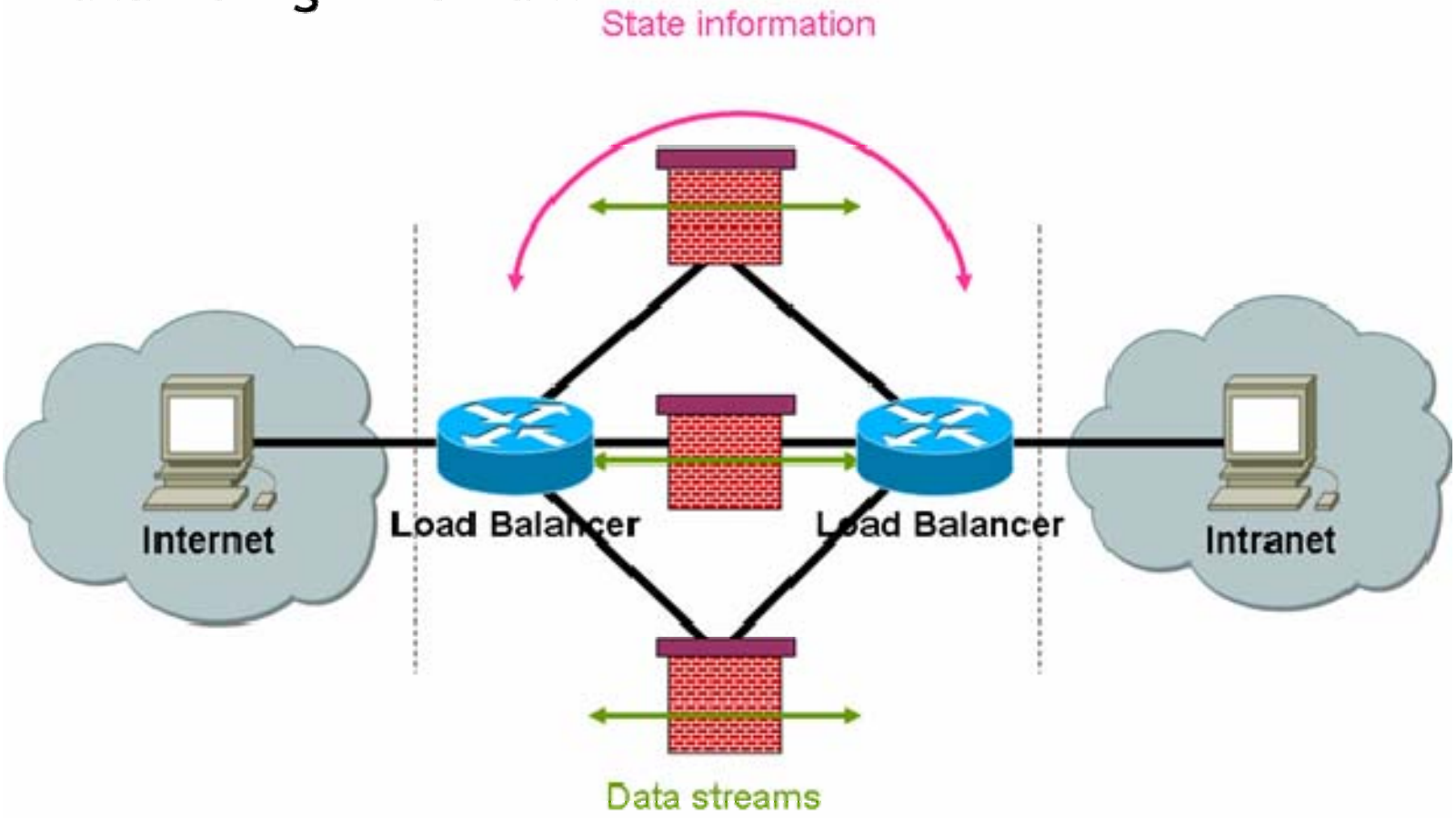
- มีประสิทธิภาพสูงสุดกับระบบที่ต้องการผลผลิตจากการประมวลผลมาก
- ถ้า Firewall ตัวใดตัวหนึ่งไม่ทำงาน จะไม่ส่งผลกระทบต่อระบบโดยรวม
- บริหารจัดการกฎเกณฑ์ของ Firewall ได้ง่าย

ข้อเสีย

- ต้องรักษาสถานการณ์เชื่อมต่อไว้จนกว่า Firewall จะประมวลผล Data Packet แล้วเสร็จ



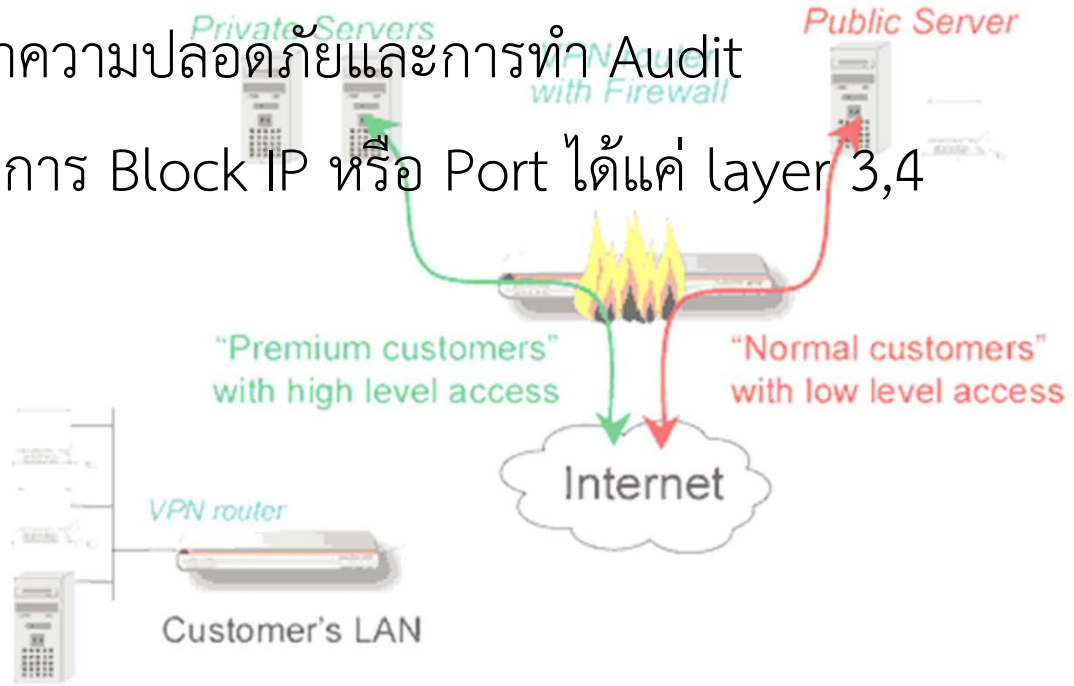
Load Balancing Firewall



ขีดความสามารถของ Firewall

ขีดความสามารถของ firewall ทั่วๆ ไปนั้นมีดังต่อไปนี้

- ป้องกันการ Login ที่ไม่ได้รับอนุญาตที่มาจากภายนอกเครือข่าย
- ปิดกั้นไม่ให้ Traffic จากนอกเครือข่ายเข้ามาภายในเครือข่ายแต่ก็ยอมให้ผู้ที่อยู่ภายในเครือข่ายสามารถติดต่อกับโลกภายนอกได้
- เป็นจุดรวมสำหรับการรักษาความปลอดภัยและการทำ Audit
- Firewall จะตรวจสอบดูแค่การ Block IP หรือ Port ได้แค่ layer 3,4



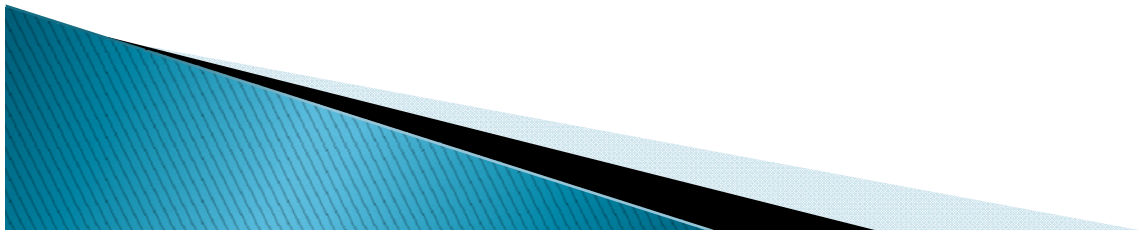
ข้อจำกัดของ Firewall

- Firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน Firewall เช่น การโจมตีจากภายในเครือข่ายเอง
- ไม่สามารถป้องกันการโจมตีที่เข้ามากับ Application Protocols ต่างๆ ที่เรียกว่าการ Tunneling หรือกับโปรแกรม Client ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ หรือโปรแกรมที่ถูกทำให้เป็น Trojan horse
- ไม่สามารถป้องกัน Virus ได้อย่างมีประสิทธิภาพเนื่องจากจำนวน Virus มีอยู่มากมาย จึงจะเป็นการยากมากที่ Firewall จะสามารถตรวจจับ Pattern ของ Virus ทั้งหมดได้ถึงแม้ว่า Firewall จะเป็นเครื่องมือที่สามารถนำมาใช้ป้องกันการโจมตีจากภายนอกเครือข่ายได้อย่างมีประสิทธิภาพ การที่จะใช้ Firewall ให้ได้ประโยชน์สูงสุดนั้นจะขึ้นอยู่กับนโยบายความปลอดภัยโดยรวมขององค์กรด้วย นอกจากนี้ แม้แต่ Firewall ที่ดีที่สุดก็ไม่สามารถนำมาใช้แทนการมีจิตสำนึกในการที่จะรักษาความปลอดภัยภายในเครือข่ายของผู้ที่อยู่ในเครือข่ายนั้นเอง

Content Filter

คือ Software กรองเนื้อหาที่ช่วยให้ Admin สามารถจำกัดการเข้าถึง Website ต่าง ๆ ของ User ภายในเครือข่ายได้ หรือสามารถจำกัดการรับเนื้อหาที่ไม่เหมาะสมจาก Website ใดๆ ได้ นอกจากนั้นยังสามารถจำกัดชนิดของ Protocol ซึ่งบางครั้งเรียกว่า Content Filter or Reverse Firewall กลุ่ม User ที่จำเป็นต้องใช้ Content Filter ดังนี้

1. School
2. General business organization
3. Financial institution
4. Institutes of Health
5. ISP
6. Government
7. Library
8. Parent



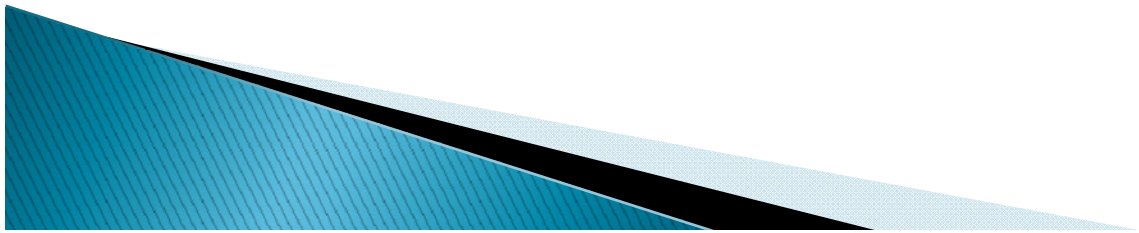
Content Filter Algorithm

1. Banned Word List เป็นวิธีที่บล็อกเฉพาะคำหรือวลีที่ไม่ต้องการ อาจจะสร้างเป็น Blacklist Dictionary

2. **URL** เป็นวิธีการกำหนดชื่อ Website ไว้ใน Blacklist แทนคำหรือวลี

3. Category Block วิธีนี้อาศัยบริการจัดหมวดหมู่ Website จาก Server ของ ISP และติดตั้งอุปกรณ์บล็อกตามกลุ่ม และจะบันทึกการเปลี่ยนแปลงทุกครั้ง ทำให้ Admin ไม่จำเป็นต้องเพิ่มด้วยตัวเอง

4. Bayesian Filter เป็นการกรองเนื้อหาตามค่าที่เป็นไปได้ของคำต้องห้ามที่นิยมใช้ในการเข้าถึง Web ต้องห้าม เช่น คำว่า XXX



Content Filter Algorithm

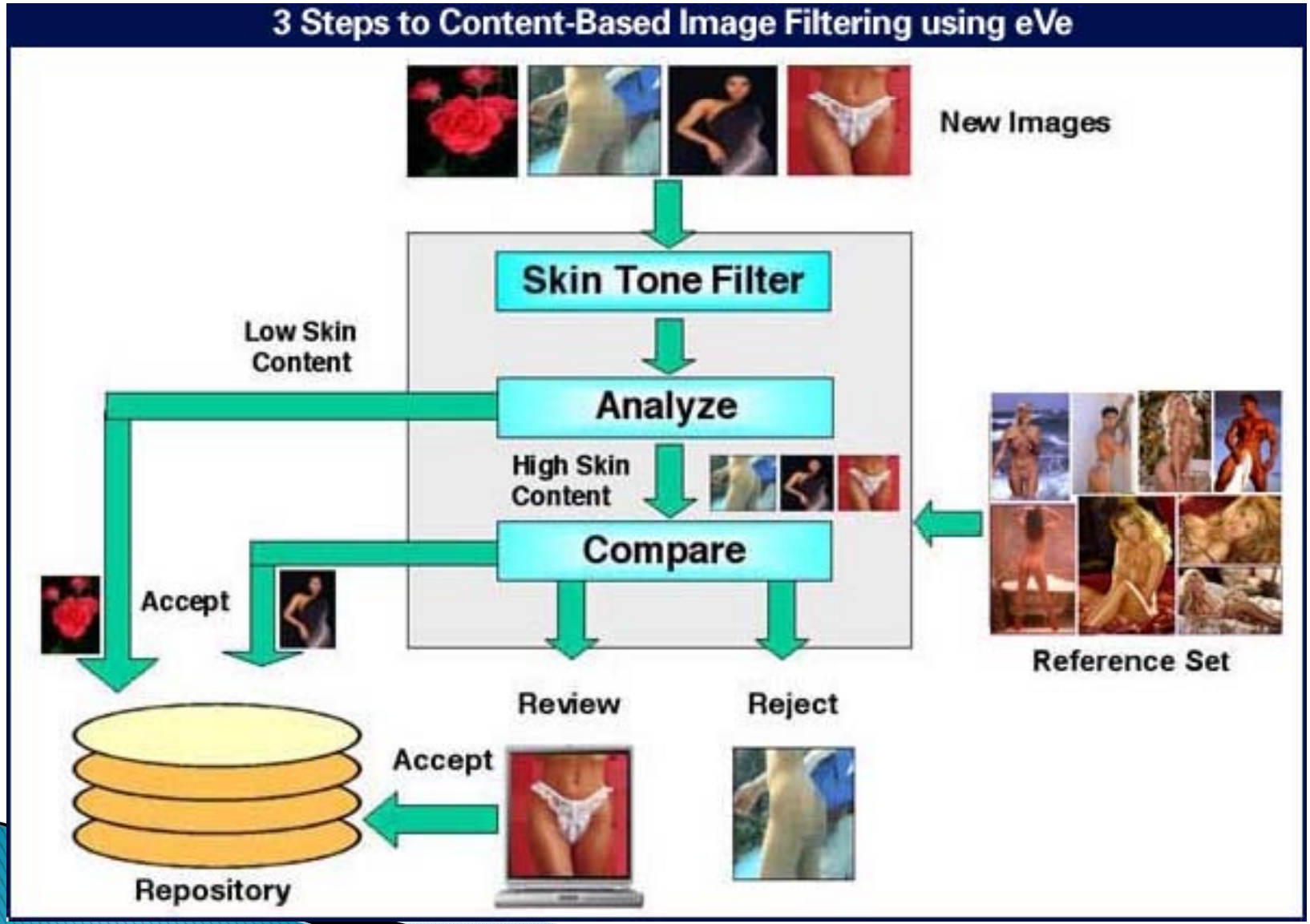
5. Content-based Image Filtering เป็นการกรองภาพ มีขั้นตอนการทำงาน 3 ขั้นตอน ดังนี้

1. Skin Tone Filter เป็นขั้นตอนแยกสีผิวของคนออกจากวัตถุอื่น โดยใช้ทฤษฎีสีจาก สีแดง เหลือง และน้ำตาล

2. Analyze เป็นการวิเคราะห์หาพื้นที่ผิวของคน เพื่อคำนวณหาพื้นที่ผิว ถ้าเป็น Low Skin Content จะบันทึกลงในฐานข้อมูล ถ้าเป็น High Skin Content จะนำไปแบ่งส่วนรูปพรรณสัณฐาน และสร้างเป็น Visual Signature

4. Compare ระบบจะนำ Visual Signature มาเปรียบเทียบแล้วจัดระดับความน่าเชื่อถือเข้าข่ายเป็นภาพลามกหรือไม่

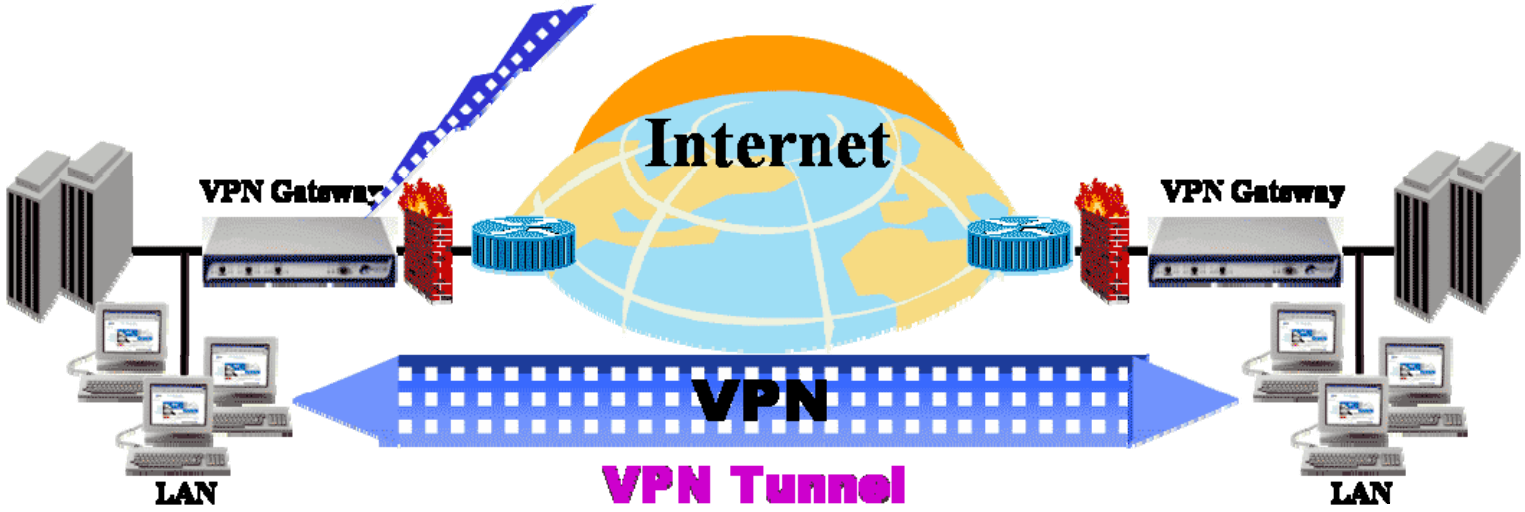
Content Filter Algorithm



http://www.evisionglobal.com/business/cf.html

Virtual Private Network : VPN

เป็น Private Network แต่ใช้ใช้โครงสร้างพื้นฐานของ Public Network และ มีความเป็น Private โดยใช้ Protocol Tunnel and Security Procedure องค์กรต่าง ๆ จึงนิยมนำ VPN มาใช้ในการเข้าถึงระยะไกลจาก Public Network



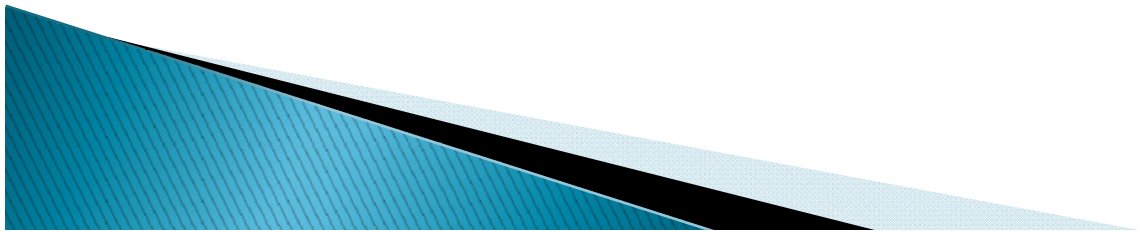
Virtual Private Network : VPN

Virtual Private Network Consortium : VPNC define type of VPN Technology 3 type.

1. Trusted VPN or Legacy VPN Use Least line Circuit form ISP and Packet Switching Network.

2. Secure VPN Use Security Protocol and Data Encryption when sent through Public Network.

3. Hybrid VPN Use both VPN Network in other words use Data Encryption when sent through Least line Circuit.



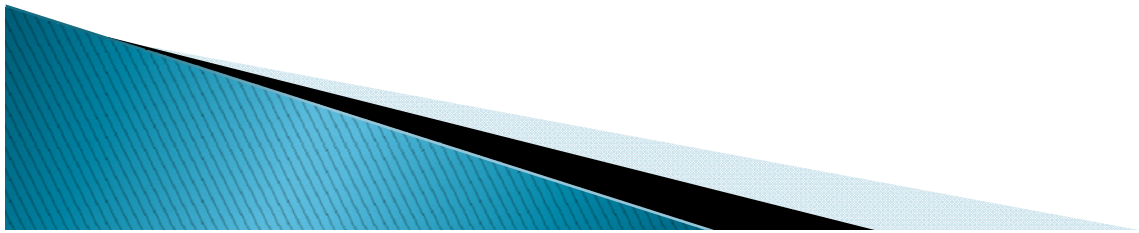
Virtual Private Network : VPN

VPN Network to maintain the privacy of the information in Public Network requires the third section.

1. Encapsulation เป็นกาห่อหุ้มข้อมูลที่เข้าและออกจากเครือข่าย

2. Encryption เป็นการเข้ารหัสข้อมูลที่เข้าและออกเครือข่าย เพื่อเก็บข้อมูลไว้เป็นส่วนตัวในขณะที่ส่งผ่าน Public Network

3. Authentication เป็นการพิสูจน์ตัวตนของ User and VPN



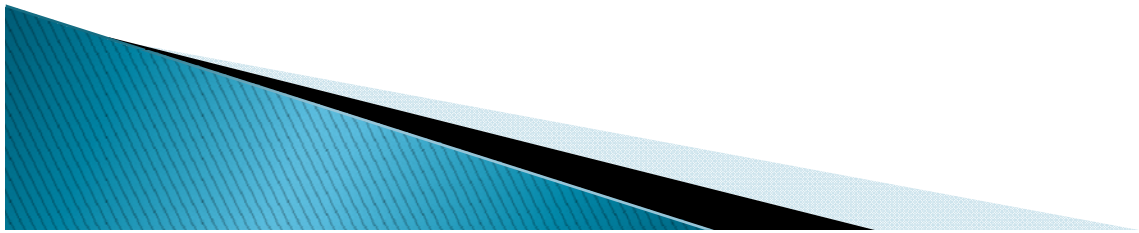
Virtual Private Network : VPN

Implementation VPN divided into two working modes.

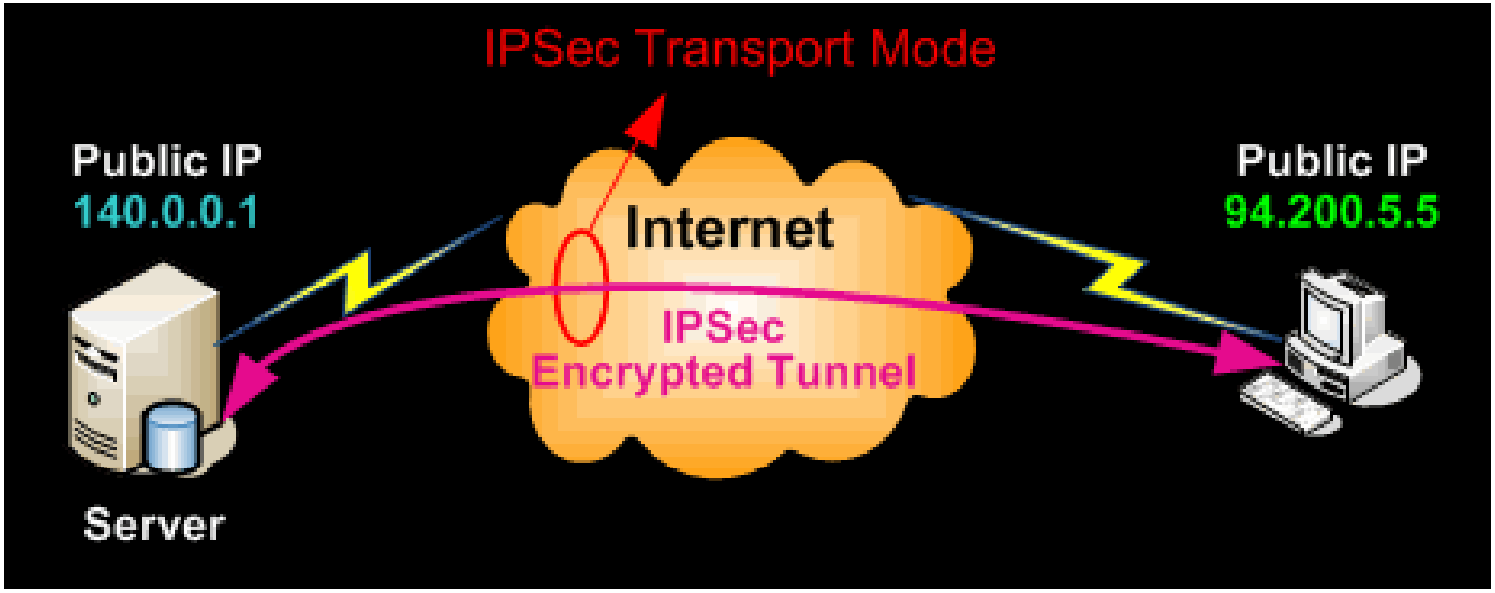
1. Transport Mode data in IP Packet be Encrypted ยกเว้นส่วน Header of Packet จะทำให้ User สามารถเชื่อมต่อโดยตรงกับ Remote Host ได้อย่างปลอดภัย

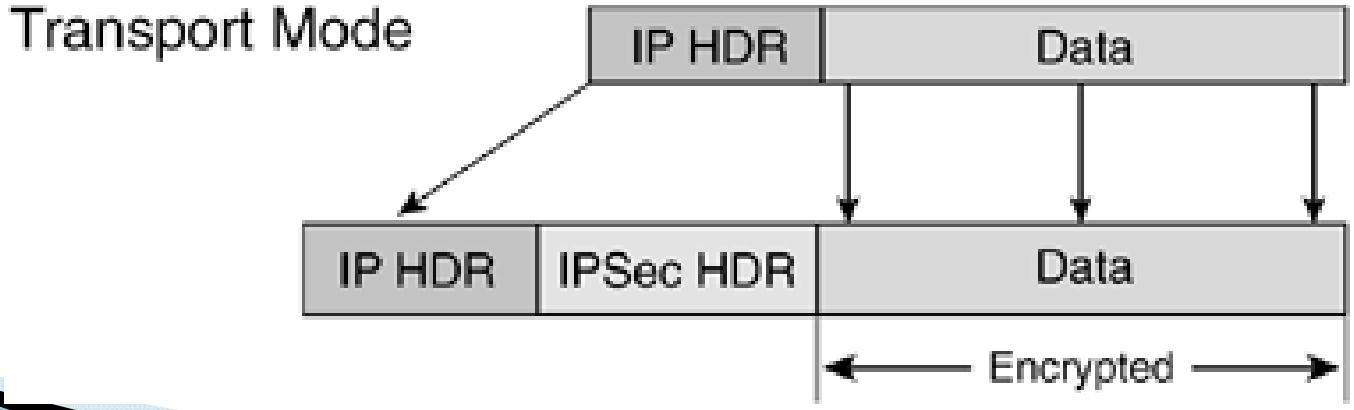
ข้อเสีย คือ ถ้าดักจับ Packet ได้จะทราบตำแหน่งที่อยู่ปลายทาง และสามารถดึงข้อมูลมาได้

ข้อดี คือ ไม่จำเป็นต้องมี Server and Software และอนุญาตให้ User เข้าถึงระบบได้ทุกแห่ง



Virtual Private Network : VPN → Transport Mode



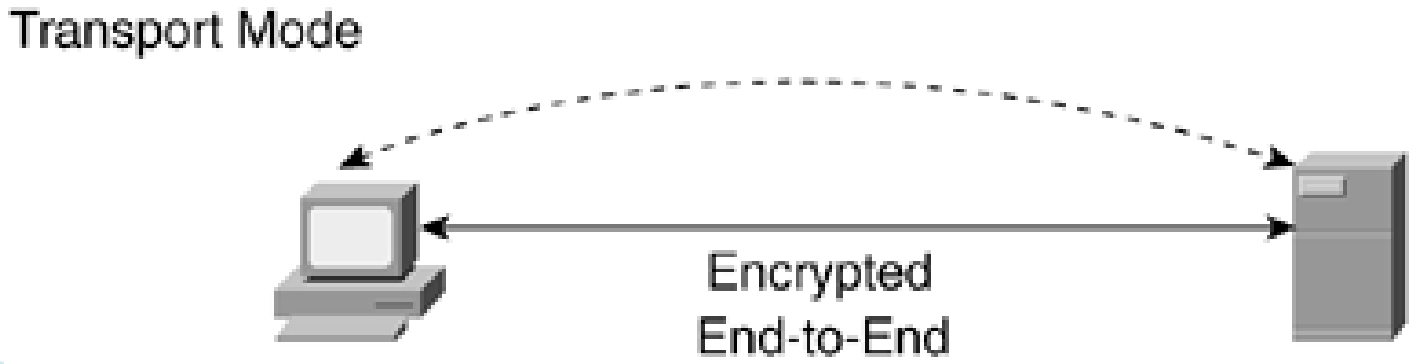


http://www.[illegible]cx/networking-topics/protocols/870-ipsec-modes.html

Virtual Private Network : VPN → Transport Mode

Transport Mode VPN แบ่งการทำงานได้ 2 ลักษณะ ดังนี้

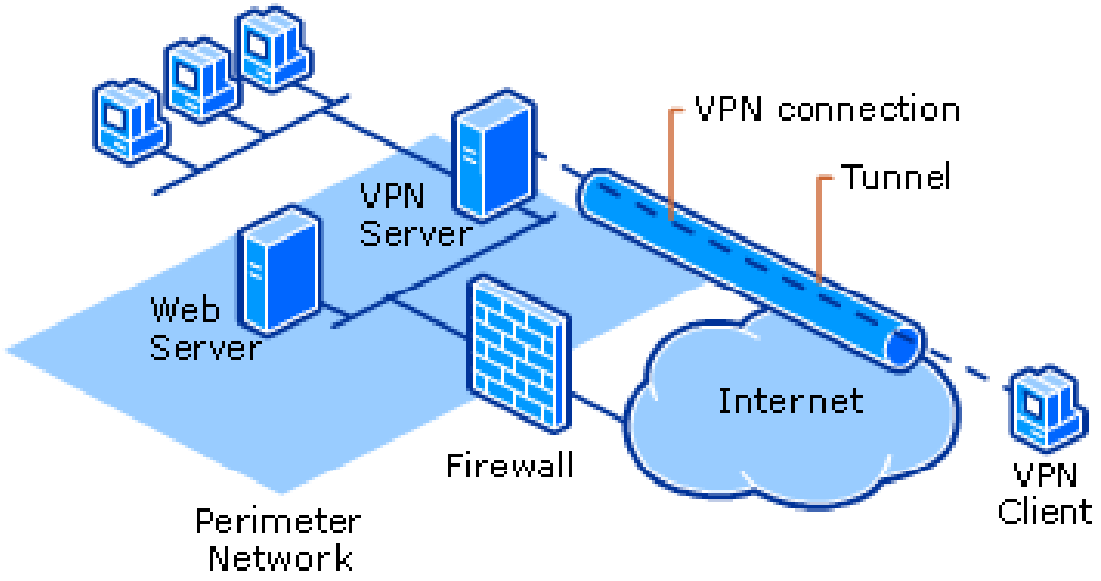
1. **End-to-End** การทำงานในลักษณะนี้ End User ทั้งฝ่ายรับและฝ่ายส่ง สามารถติดต่อสื่อสารข้อมูลได้โดยตรงและสามารถเข้าและถอดรหัสได้ตามต้องการ ในกรณีนี้ เครื่องคอมพิวเตอร์ของแต่ละ End User จะทำหน้าที่เป็นทั้ง Client and End Node VPN Server



Virtual Private Network : VPN → Transport Mode

Transport Mode VPN แบ่งการทำงานได้ 2 ลักษณะ ดังนี้

2. VPN Server Working in this manner Remote Host form User connect to VPN Server in DMZ before into Private Network VPN Server acts as an intermediary between users to encrypt and decrypt both.



Virtual Private Network : VPN

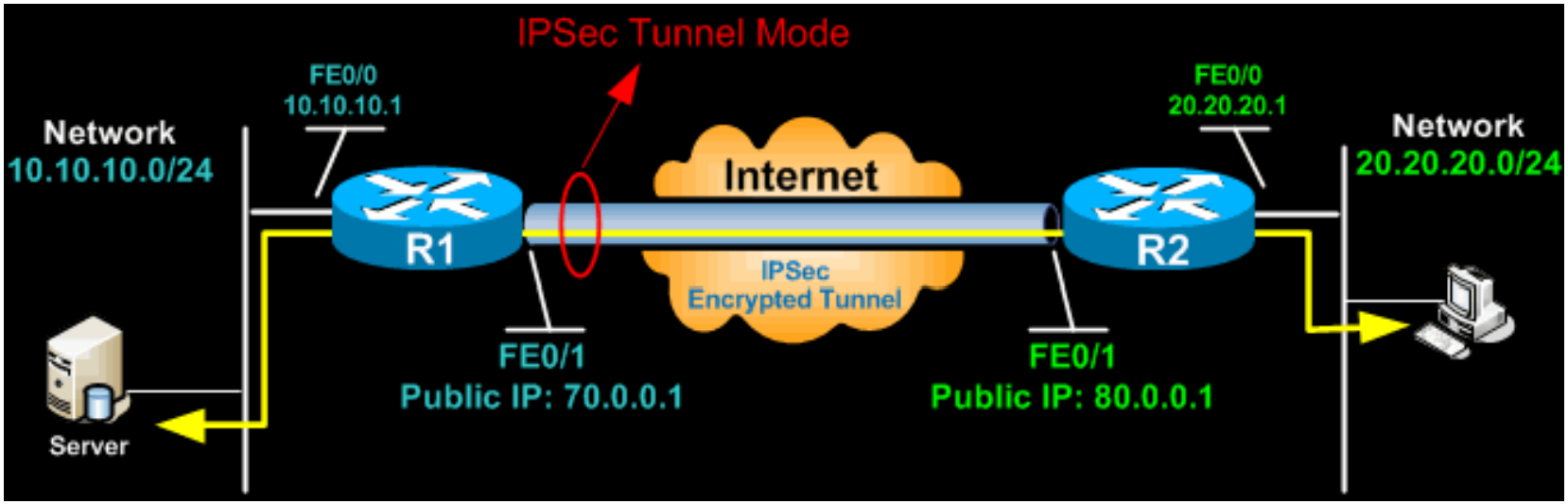
Implementation VPN divided into two working modes.

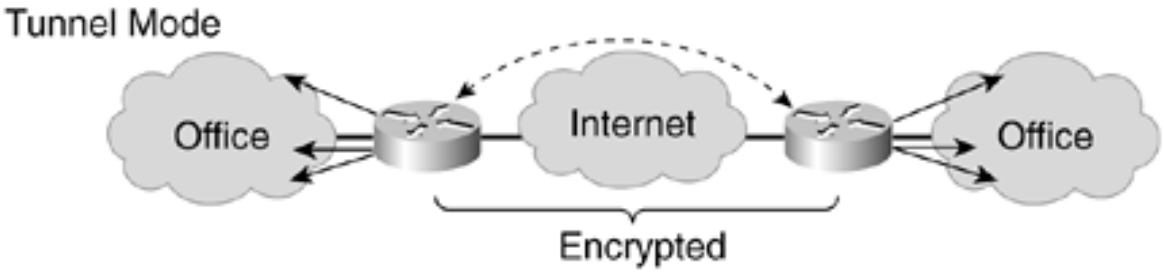
2. Tunnel Mode จะมี VPN Server 2 เครื่องเรียกว่า Tunnel Server ทำหน้าที่เป็นศูนย์กลางการเข้ารหัสข้อมูลที่จะไปยังทุกเส้นทางของเครือข่ายที่ไม่น่าเชื่อถือ

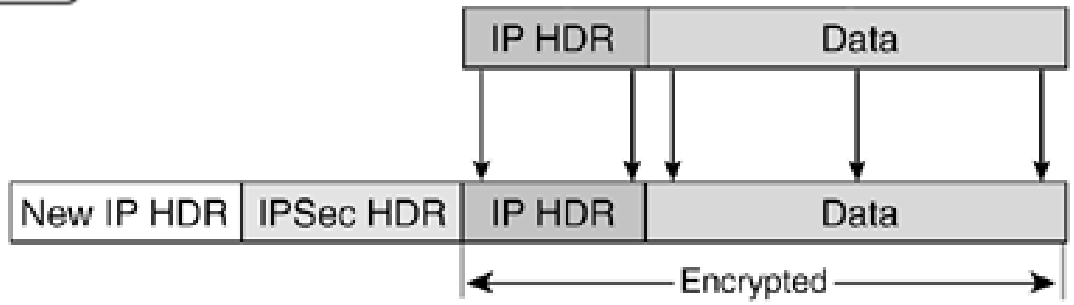
IP Packet ของ User ต้นทางจะถูกเข้ารหัสไว้ทั้งหมด และนำไปเก็บไว้ใน Packet อีกชั้นหนึ่งเพื่อส่งไปให้ Source Tunnel Server into Destination Tunnel Server เพื่อถอดรหัสและส่งไปให้ User ปลายทาง

ข้อดี คือ ไม่แสดงตำแหน่งที่แท้จริงของระบบปลายทาง เปรียบเสมือนว่ามีอุโมงค์ซ่อนข้อมูลไว้ระหว่างเคลื่อนย้ายอยู่ใน Public Network

Virtual Private Network : VPN







http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

Questions and Answers

MS1 Thanin Muangpool

Thank you