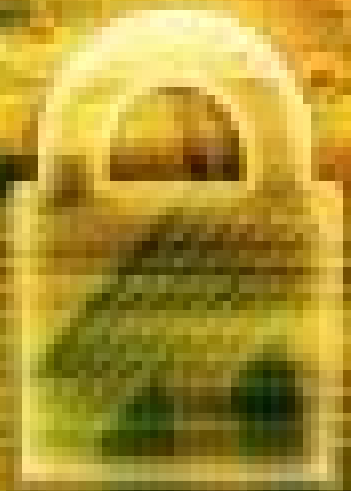
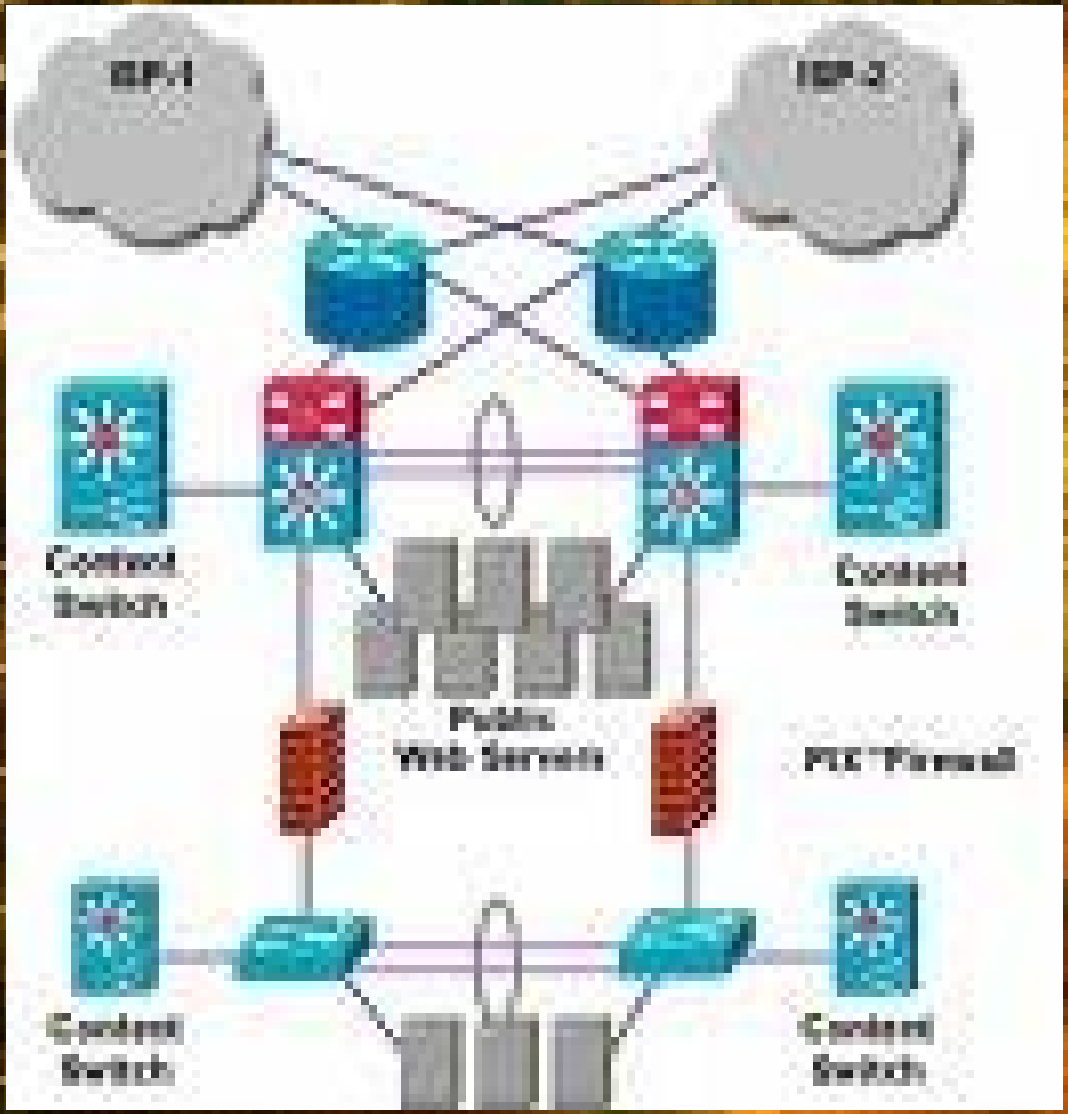
การป้องกันการโจมตีแบบ
Denial of Service



จัดทำโดย น.ส. ภัทรา รุ่งศิริศิลป์

การป้องกันการโจมตีแบบ
Denial of Service

การโจมตีแบบ Distributed Denial of Service (DDoS) เป็นการโจมตีที่มักจะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานได้ตามปกติ หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ธรรมดาได้



Denial of Service

เกริ่นนำ

การป้องกันการโจมตีแบบ DoS นั้น จะสามารถทำได้ก็ต่อเมื่อทราบวิธีของการโจมตีก่อน และการป้องกันการโจมตีในบางครั้งก็ไม่สามารถทำได้ในครั้งเดียว ขึ้นอยู่กับรูปแบบการโจมตี และสถาปัตยกรรมของเป้าหมายที่ถูกโจมตี

Back

การป้องกันอาจจะได้ผลหรือล้มเหลวก็ขึ้นอยู่กับ

- การมีคู่มือหรือเอกสารการใช้งานของระบบเป้าหมายที่ถูกโจมตี
- การตรวจจับการโจมตีสามารถทำได้อย่างรวดเร็วและสามารถค้นหาต้นตอที่แท้จริงได้
- มีวิธีดำเนินการสนองตอบเหตุการณ์ละเมิดความปลอดภัยอย่างเป็นขั้นตอน (incident response)
- และการป้องกันรูปแบบอื่นที่สามารถทำได้

Back

รูปแบบการโจมตี และ การป้องกัน

เครื่องมือที่ใช้โจมตีแบบ DDoS มีใช้กันอย่างแพร่หลายมานานหลายปีแล้ว และบรรดาผู้ผลิตเองต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่าง SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น ซึ่งจะได้ศึกษาในรายละเอียดและวิธีป้องกันกันต่อไป

Back

SYN Flood

เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYNบิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบTCPตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source addressได้)

Back

SYN Flood

เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายังsource ip address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source ip address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-openขึ้นที่เครื่องเป้าหมาย หากมีการส่งSYN flood จำนวนมากก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม

Back

SYN Flood

ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปเป็นจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

Back

SYN Flood

การป้องกัน

1.1Cisco Router

เราเตอร์ของ Cisco มีฟังก์ชันการทำงานชื่อ TCP Intercept ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood

Back

SYN Flood

โดย TCP intercept software จะพยายามสร้างการเชื่อมต่อกับ client หากสำเร็จการเชื่อมต่อดังกล่าวก็จะถูกส่งไปให้กับเครื่องให้บริการต่อไป ดังนั้นการโจมตีแบบ SYN flood จะไม่สามารถเข้าไปถึงเครื่องเป้าหมายจริงๆได้ และเราเตอร์ที่ถูกออกแบบให้รองรับการเชื่อมต่อได้มากกว่าเครื่องให้บริการ(surver) อีกด้วย แต่ก็มีข้อเสียคือจะทำให้เราเตอร์ใช้ทรัพยากรมากกว่าปกติ

Back

SYN Flood

นอกจากนี้ เราเตอร์ของ Cisco ยังมีฟังก์ชันชื่อ Committed Access Rate (CAR) ซึ่งใช้ในการจำกัดแบนด์วิดธ์ที่ใช้สำหรับแต่ละบริการได้ (แก้ไขได้ผ่านทางextended access control list) ซึ่งไม่เพียงแต่ป้องกันการโจมตีแบบ SYN flood ยังป้องกันการเชื่อมต่อที่ถูกต้องไม่ให้ใช้แบนด์วิดธ์มากเกินไป ซึ่งข้อเสียในการนำไปใช้งาน

Back

SYN Flood

คือ ในขณะที่เครื่องเป้าหมายถูกโจมตีจะทำให้การเชื่อมต่อจากผู้ใช้ธรรมดาไม่สามารถทำได้

เทคนิคหนึ่งในการนำ CAR ไปใช้งาน คือ การจำกัดการเข้าถึงโดยระบุเป็นจำนวน client ที่สามารถเข้าใช้งานได้

Back

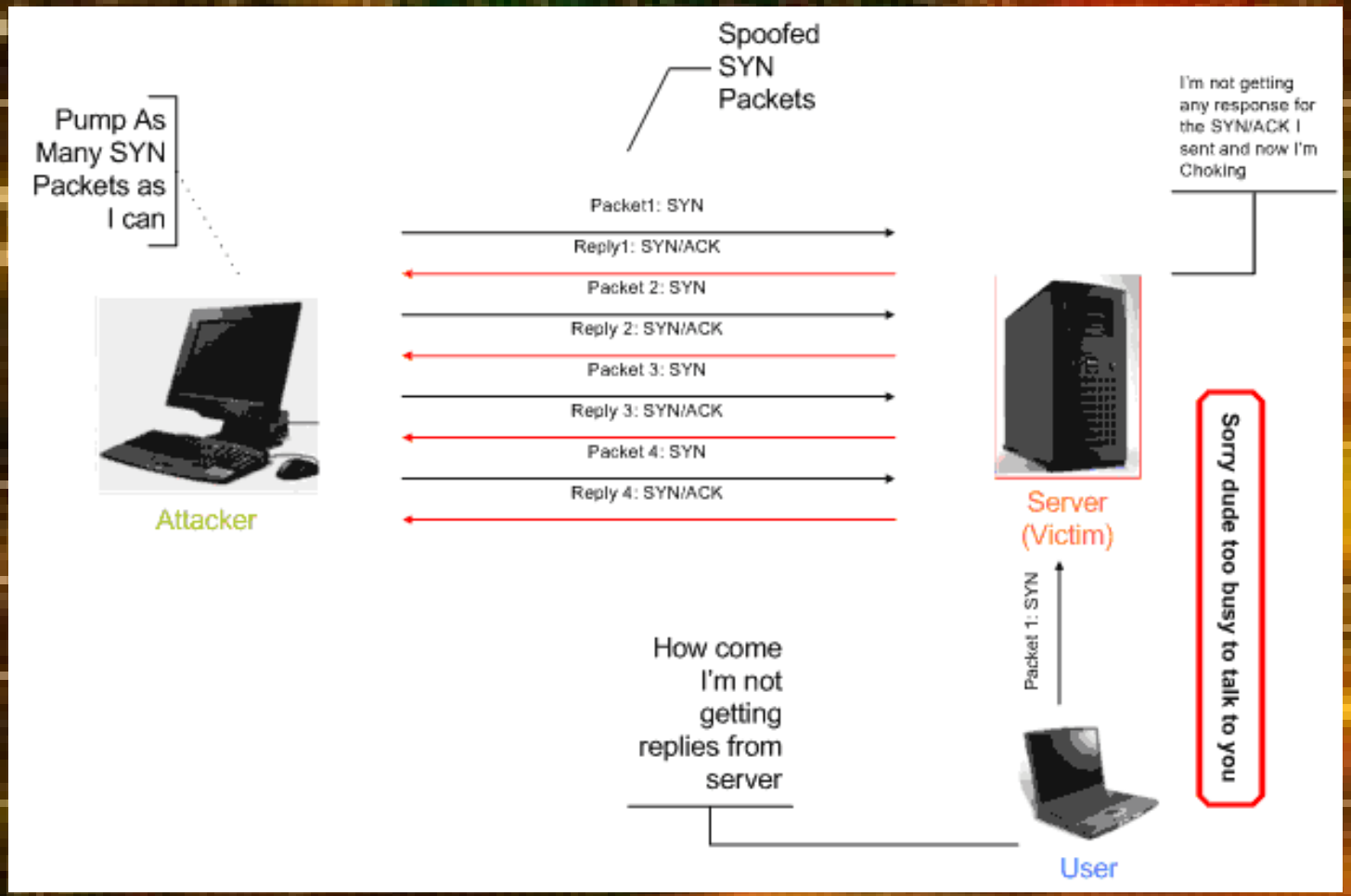
SYN Flood

1.2Checkpoint FW-1

FW-1 มีฟังก์ชันชื่อ SYN Defender ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดยใช้หลักการเช่นเดียวกันกับ Cisco's TCP Intercept ซึ่งจะทำให้ SYN packet ถูกหยุดยั้งไว้ที่FW-1 เช่นเดียวกันกับCisco's TCP Intercept ตัว FW-1 เองก็จะใช้ทรัพยากรมากกว่าปกติ ในการทำงานลักษณะดังกล่าว

Back

SYN Flood



Back

ICMP Flood

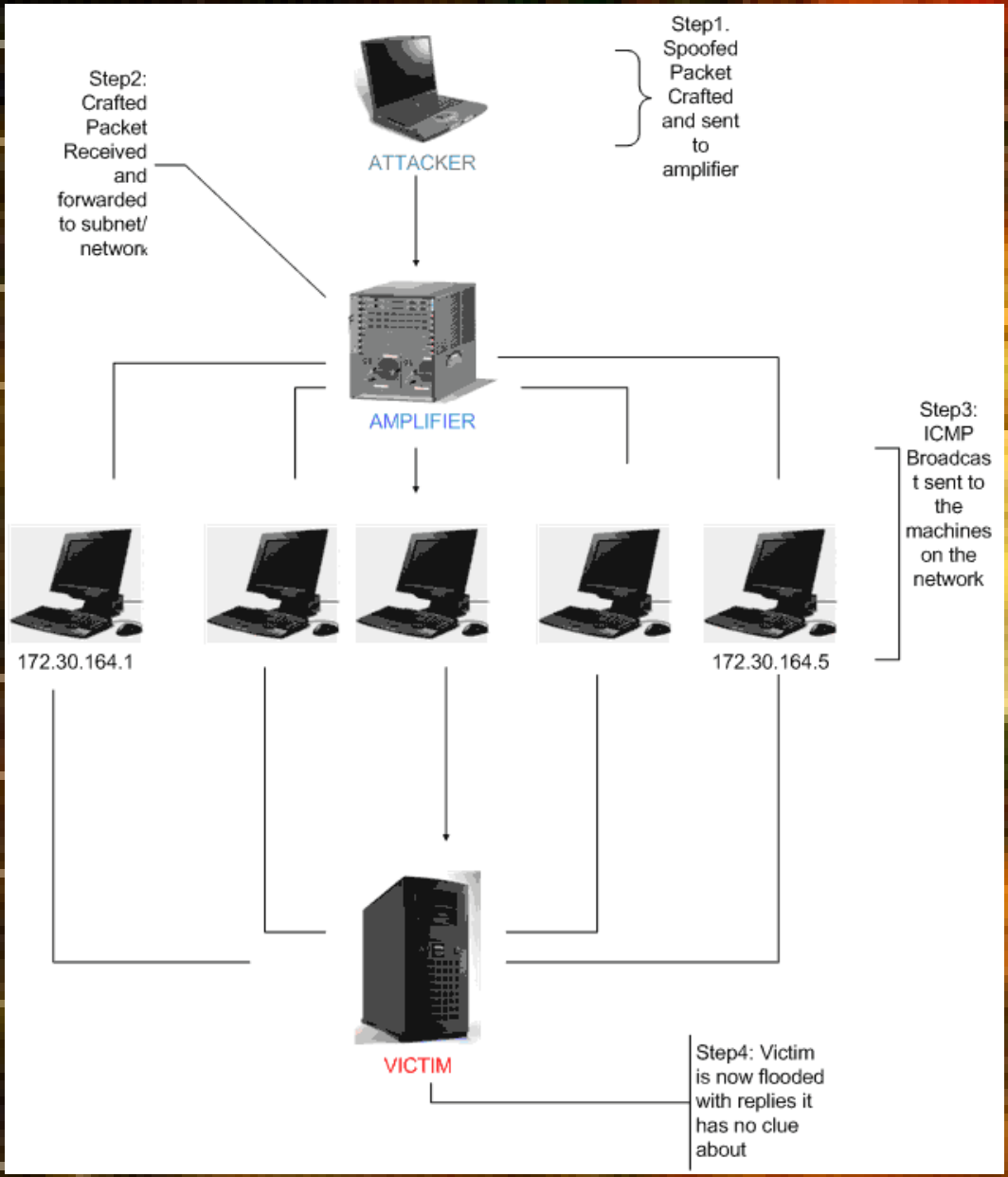
เป็นการส่งแพ็คเก็ต ICMP จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

การป้องกัน

ระบบสามารถทำงานได้โดยไม่ต้องใช้ ICMP EchoRequest ซึ่งสามารถป้องกันการใช้งานได้โดยใช้คำสั่งที่เราเตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ

Back

ICMP Flood



Back

UDP Flood

เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่และ/หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด

โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53(DNS)

Back

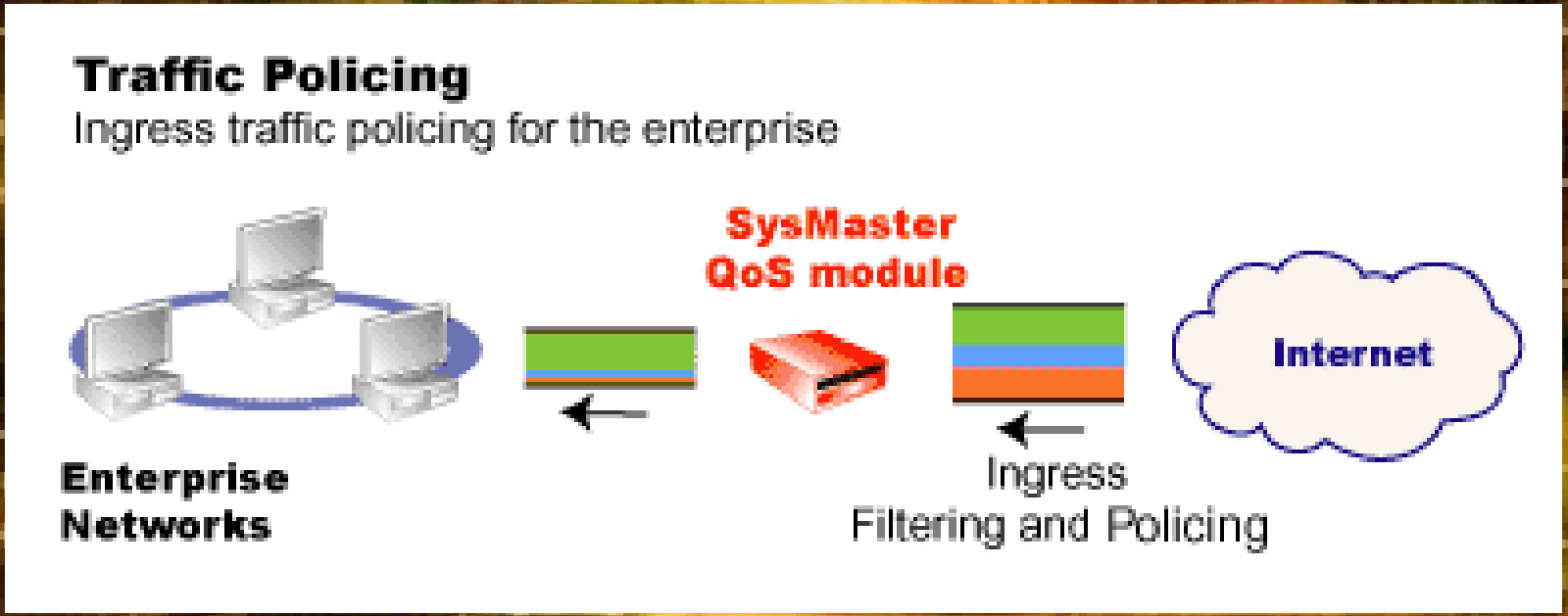
UDP Flood

การป้องกัน

เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop แพ็คเก็ตที่มุ่งโจมตีมายัง port ที่ไม่เป็นที่ต้องการได้ เช่น โจมตีมายัง port ที่ไม่ได้ให้บริการในportดังกล่าว ในกรณีที่เป็นการโจมตีเฉพาะ port ที่เปิดให้บริการ เช่น port 53 ก็สามารถป้องกันระบบเป้าหมายได้ โดยใช้ CAR เพื่อจำกัดจำนวนข้อมูล

Back

UDP Flood



Back

Smurf

ผู้โจมตีจะส่ง ICMP Echo Requestไปยัง broadcast addressในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอมsource ip address เป็น ip address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลาง ส่ง ICMP Echo Reply กลับไปยัง ip addressของเป้าหมายทันที

Back

Smurf

การป้องกัน

เช่นเดียวกันกับการโจมตีแบบ ICMP flood

เราเตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop ICMP Echo Reply ซึ่งในกรณีนี้ควร drop ICMP Echo Replyที่ส่งเข้ามา โดยไม่ได้มีการส่ง ICMP Echo Requestออกไปก่อน

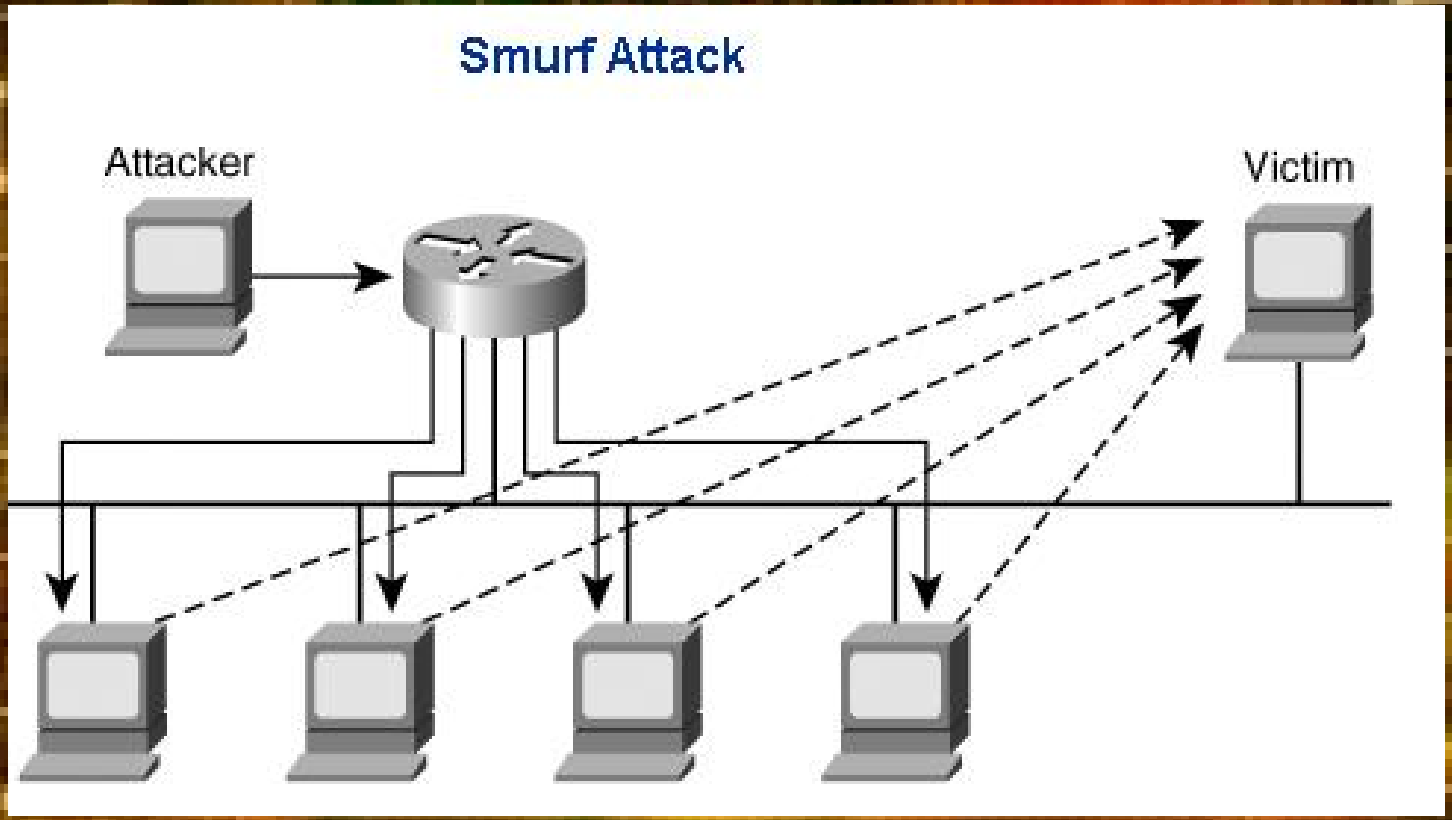
Back

Smurf

ซึ่งการทำงานลักษณะนี้อาจจะทำให้อุปกรณ์packet filtering ใช้ทรัพยากรเพิ่มขึ้น และในกรณีที่เกิดการโจมตีขึ้นแล้วยังสามารถบล็อก source ip address ของ ICMP Echo Reply ได้ เพราะผู้โจมตีไม่สามารถเปลี่ยนแปลงข้อมูลส่วนนี้ได้

Back

Smurf



Back

Fraggle

เป็นอีกรูปแบบหนึ่งของการโจมตีแบบ Smurf
โดยผู้โจมตีจะส่ง UDP Echo Request (UDP port 7)
ไปยัง broadcast address ของamplifier network
โดยปลอมsource ip addressไปเป็น
ip address ของเป้าหมาย

Back

Fraggle

ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่และ/หรือทำให้มีการใช้ทรัพยากรของเป้าหมายจนหมดไป ซึ่งการโจมตียังสามารถใช้ได้กับ UDP, TCP services อื่น เช่น Chargen อีกด้วย

Back

Fraggle

การป้องกัน

สามารถป้องกันได้คล้ายๆ กับการป้องกันการโจมตีแบบ Smurf attack โดยใช้เราเตอร์ หรือ อุปกรณ์กรองอื่น drop แพ็คเก็ต UDP/TCP ที่ใช้โจมตีเข้ามา หรืออาจจะใช้วิธีบล็อก source ip addressได้เช่นกัน

อย่างไรก็ตามผู้ดูแลระบบควรยกเลิกการใช้งาน UDP, TCP service บางตัวเช่น Echo, Chargen, Discard ซึ่งไม่มีความจำเป็นในการใช้งานอีกแล้วซึ่งสำหรับเราเตอร์ของ Cisco แล้ว สามารถใช้คำสั่ง

no service udp-small-servers
no service tcp-small-servers เพื่อยกเลิก

Back

Fraggle

จะทำอย่างไรเมื่อถูกโจมตี

- การโจมตีที่เกิดขึ้นมักจะทำให้เกิดการใช้งานแบนด์วิดธ์จนเต็มที่ เช่น SYN flood ถ้าหากทำการกรองแพ็คเก็ตที่ ISP ได้ ก็จะสามารถลดผลกระทบที่จะเกิดขึ้นได้
- ติดตั้ง hardware ที่มีขีดความสามารถสูงไว้ระหว่างเครือข่ายของISP กับของระบบที่ต้องการป้องกัน เช่น การติดตั้งเราเตอร์ประสิทธิภาพสูง ที่สามารถทำ filtering ได้

Back

Fraggle

- โดยปกติการโจมตีแบบ DoS ผู้โจมตีมักจะโจมตีไปยังเป้าหมายโดยระบุเป็น ip addressโดยตรง ไม่ได้ผ่านการทำ DNS lookup มาก่อน ดังนั้น เมื่อเกิดการโจมตีก็ยังสามารถหาหนทางหลบหลีกการโจมตีดังกล่าวได้ 2 วิธีคือ

1. เปลี่ยน ip address เมื่อเกิดการโจมตี
2. เปลี่ยน ip address ไปเรื่อยๆแม้จะไม่มีการโจมตี

ซึ่งการกระทำทั้งสองรูปแบบก็มีข้อดีข้อเสียต่างกัน

Back

Fraggle

ในรูปแบบแรกจะต้องมีระบบตรวจจับที่ดี สามารถแจ้งเตือนผู้ดูแลระบบ ให้สามารถปรับเปลี่ยน ip address ได้อย่างรวดเร็ว จะเห็นว่ามีช่องว่างระหว่างการดำเนินงานอยู่ แต่ยังมีข้อดีที่ผู้โจมตีจะไม่สามารถรู้แทกติกนี้ จนกว่าจะเริ่มโจมตี ในขณะที่วิธีที่สองจะมีความยากลำบากในการเริ่มโจมตีมากกว่า

Back

วิธีปฏิบัติที่ใช้ได้จริง

ซึ่งต้องการการแก้ไขเพียงเล็กน้อยและพยายามลดผลกระทบที่จะเกิดขึ้นกับผู้ใช้ให้น้อยที่สุด ดังนี้

1. การแก้ไข DNS

   การแก้ไข DNS entries โดยเปลี่ยน ip addressของ ระบบที่กำลังถูกโจมตีไปเป็น ip address ใหม่

2. Network Address Translation

   หากระบบที่ถูกโจมตีสามารถใช้งาน NAT ได้ ก็จะทำให้ง่ายในการเปลี่ยน ip address

Back

วิธีปฏิบัติที่ใช้ได้จริง

3. filter ค่า ip address เดิม

หากไม่ต้องการให้ traffic ของ ip addressชุดเดิม เข้ามาภายในระบบก็สามารถทำได้โดยการยกเลิก routing สำหรับ ip address เดิมเสีย

4. ใช้ ip address ชุดใหม่และลิ้งค์ที่แตกต่าง

5. การป้องกันการโจมตี DNS server มีวิธีป้องกันดังต่อไปนี้

Back

วิธีปฏิบัติที่ใช้ได้จริง

- วางเครื่อง primary DNS server ไว้ในลิ้งค์ที่แยกต่างหาก
- สำรองข้อมูลของ primary DNS server ไปยังที่ตั้งแห่งใหม่
- สร้าง secondary DNS server ไว้ในหลายๆ จุดบนลิ้งค์ที่แตกต่างกัน
- ใช้ primary DNS server ที่ผู้อื่นมองไม่เห็นและเชื่อมโยงไปยัง secondary DNS server โดยลิ้งค์ที่แยกต่างหาก

Back

วิธีปฏิบัติที่ใช้ได้จริง

- สร้าง non-advertised secondary DNS server ที่สามารถพร้อม advertise ได้ตลอดเวลา

6. ผู้โจมตี

หากผู้โจมตีเปลี่ยนเป้าหมายมาเป็น ip address ใหม่ตามที่กำหนด จะทำให้สามารถประมาณการณ์การตั้งรับได้ เช่น

- เมื่อผู้โจมตีซึ่งควบคุมการโจมตีเปลี่ยนแปลงคำสั่ง ก็จะทำให้เพิ่มโอกาสในการตามจับตัวได้ง่ายขึ้น

Back