ปกป้องชายขอบ (Network Edge) ของเครือข่ายให้พ้นภัยคุกคาม

แก้ไขปัญหาด้านความไว้วางใจด้วย Border Gateway Protocol

วิธีการเลือกโพรโตคอลในการส่งข้อมูลที่ดีที่สุดสำหรับเครือข่ายในองค์กรมักจะพิจารณาจากความต้องการทางด้านธุรกิจ ซึ่งรวมถึงความรวดเร็วในการตอบรับต่อการเปลี่ยนแปลง การรวบรวมระบบได้สะดวกรวดเร็ว การช่วยให้เกิดความสัมพันธ์ และความไว้วางใจในการสื่อสาร ทำให้การกำหนดค่าคอนฟิกูเรชันมีเพียงเล็กน้อยเท่านั้น

อย่างไรก็ตาม การเชื่อมต่อกับเครือข่ายภายนอกองค์กรจะมีข้อควรพิจารณาที่แตกต่างออกไปอย่างสิ้นเชิง เมื่อคุณเชื่อมต่อไปยังเครือข่ายที่อยู่นอกเหนือการควบคุมของคุณ การรักษาความปลอดภัยและการกำหนดนโยบายยิ่งมีความสำคัญมากยิ่งขึ้น ในขณะที่ความเร็วของเครือข่ายลดลง คุณอาจต้องการเลือกโพรโตคอลในการส่งข้อมูลที่ต่างออกไป (หรือแม้แต่ต้องเปลี่ยนโพรโตคอลในการส่งข้อมูลประเภทอื่นๆ แทน) เพื่อส่งข้อมูล Border Gateway Protocol (BGP) มีเครื่องมืออันหลากหลายสำหรับเครือข่ายองค์กร และเป็นตัวเลือกที่ดีมากสำหรับโพรโตคอลจากภายนอกที่พบบริเวณชายขอบ(Network Edge)ของระบบเครือข่าย โดยมีเหตุผลดังนี้

ประเภทของชายขอบ (Network Edge) เครือข่าย: แบบที่นิยมใช้กับการเชื่อมต่อสู่ภายนอกมากที่สุดคือการต่ออินเทอร์เน็ต ซึ่งทำให้เราท่องไปได้ทั่วโลก แต่ก็ยังมีการเชื่อมต่อสู่ภายนอกแบบอื่นอีกหลายแบบให้พิจารณา ยกตัวอย่างเช่น เอ็กซ์ทราเน็ต ซึ่งสามารถเชื่อมต่อไปยังคู่ค้า ซัพพลายเออร์ ลูกค้า หรือคู่ค้าที่เป็นสถาบันทางการเงินบางประเภทได้

แบบต่อมาเป็นที่นิยมน้อยกว่า เป็นการเชื่อมต่อจากหน่วยงานธุรกิจไปยังเครือข่ายหลักในองค์กรขนาดใหญ่และมีหลากหลายธุรกิจ เครือข่ายหลักดังกล่าวทำหน้าที่เสมือนเป็นผู้ให้บริการภายในองค์กร โดยเชื่อมโยงหน่วยต่างๆ เข้าไว้ด้วยกันและแชร์บริการต่างๆ ให้ใช้งานร่วมกัน

ประเด็นที่ต้องคำนึงถึงในกรณีที่มีการเชื่อมต่อเครือข่ายทั้ง 3 ประเภทก็คือ เมื่อมีการเชื่อมต่อไปยังเครือข่ายที่อยู่นอกเหนือการควบคุมของคุณ คุณจะต้องจัดการกับเรื่องของความไว้วางใจ (Trust) ด้วยว่า คุณจะรู้ได้อย่างไรว่าข้อมูลที่คุณได้รับมาจากการเชื่อมต่อดังกล่าวไว้ใจได้ คุณจำเป็นต้องพิจารณานโยบาย ในขณะที่คุณอาจให้ความสำคัญเป็นพิเศษกับการป้องกันข้อมูล หรือ

เมื่อมีการเชื่อมต่อเครือข่ายออกสู่โลกภายนอก คุณจะต้องจัดการกับเรื่องของความไว้วางใจ

ทราฟฟิก แต่ทว่าคุณอาจไม่ได้คิดถึงเรื่องการป้องกันส่วนควบคุม (Control Plane) หรือระบบการส่งข้อมูลเลยก็เป็นได้

ปัญหาการจัดสรรเส้นทางในการรับส่งข้อมูลที่ชายขอบ (Network Edge) ของเครือข่าย เหตุการณ์ต่อไปนี้เกี่ยวข้องกับข้อมูลการจัดสรรเส้นทาง (Routing) ที่ไม่ถูกต้อง ซึ่งอาจส่งผลเสียหายต่อการส่งข้อมูลภายในบริษัทได้

การจัดสรรเส้นทางในการรับส่งข้อมูลที่ไม่ถูกต้อง

ลองพิจารณาบริษัทตัวอย่าง 2 รายนี้ รายแรกชื่อ BigShoes ซึ่งใช้หมายเลขไอพีเป็น 10.1.0.0/16 และรายที่ 2 ชื่อว่า Medium-Socks ซึ่งใช้หมายเลขไอพี10.2.0.0/16 (ดูภาพประกอบได้ในหน้า 25)

เมื่อเร็วๆ นี้ทั้งสองบริษัทได้ตกลงเป็นคู่ค้ากันเพื่อขายรองเท้าและถุงเท้าภายในร้านเดียวกัน BigShoes เป็นคู่ค้ากับบริษัทอื่นๆ ด้วย อย่างเช่น SmallFeet โดยคู่ค้าทุกรายเชื่อมโยงถึงกันโดยใช้ Redistribution ระหว่าง Interior Gateway Protocols (IGPs) ปัญหาที่อาจเกิดขึ้นในเครือข่ายนี้ มีดังต่อไปนี้:

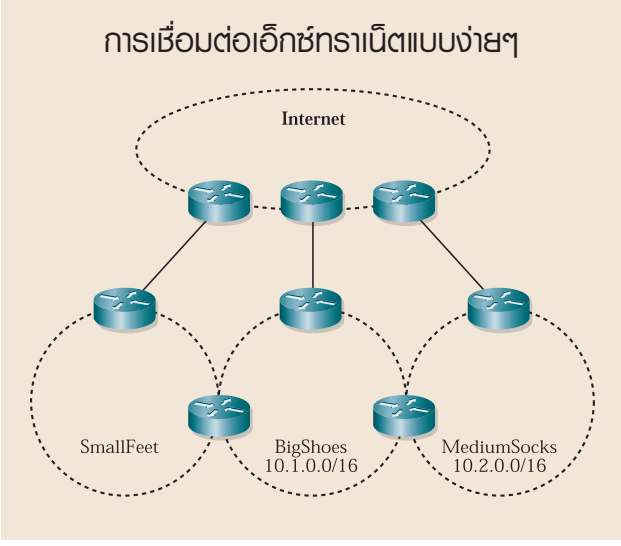
- **SmallFeet** เดิมใช้หมายเลขไอพี กลุ่ม 10.2.1.0/24 ติดต่อกับ Bigshoes ซึ่งเป็นกลุ่มไอพีที่ซ้ำกับทาง MediumSocks Redistribution ระหว่างสามบริษัทนี้อาจจะทำให้เส้นทางของข้อมูลเดินทางผิดพลาดได้
- **BigShoes** รู้จักกลุ่มไอพีของ MediumSocks ผ่านทาง redistribution และประกาศกลุ่มนี้ไปให้ทาง Internet ซึ่ง Edge Router ของ MediumSocks ก็จะได้รับข้อมูลไอพีนี้จาก Internet ด้วย Edge Router ของ MediumSock อาจจะใช้เส้นทางผ่าน Internet และ MediumSocks ซึ่งไม่ใช่เส้นทางที่ดีที่สุด
- **BigShoes** ที่กำหนดค่าอุปกรณ์เราเตอร์ไม่ถูกต้อง กลับส่งตารางการจัดสรรเส้นทางในการรับส่งข้อมูลบนอินเทอร์เน็ต (Internet Routing Table) ไปยัง IGP ของ MediumSocks IGP ซึ่งเกินกำลังที่เราเตอร์ของ MediumSocks จะรับได้ ส่งผลให้เครือข่ายล่ม

สำหรับ MediumSocks แล้ว การป้องกันตนเองจากปัญหาในลักษณะนี้ทำได้ยาก ไม่ว่าจะเป็นเรื่องการโจมตีแบบมุ่งร้าย หรือการกำหนดค่าเพื่อใช้งาน IGP ผิดพลาดโดยไม่ได้ตั้งใจ

Flapping Routing Information

สมมุติว่าวิศวกรเครือข่ายของ MediumSocks ได้วางระบบ Voice over IP (VoIP) ไปทั่วทั้งเครือข่าย และมีการปรับจูนเครือข่ายให้ทำงานได้เร็วที่สุดเท่าที่จะเป็นไปได้ ซึ่งรวมถึง fast timer และ exponential backoff

หาก BigShoes ส่งเส้นทางไปยังเครือข่าย MediumSocks ซึ่งมีการเปลี่ยนแปลงตลอดเวลา เครือข่าย MediumSocks จะเป็นอย่างไรต่อไป? IGP จะตีความการเปลี่ยนแปลงที่เกิดขึ้นตลอดเวลานี้เป็นดัชนีที่บ่งชี้ว่าเครือข่ายไม่เสถียร แล้วยกเลิก Fast Convergence Timer สรุปก็คือการเปลี่ยนแปลงที่เกิดขึ้นตลอดเวลาในเครือข่ายของ BigShoes ส่งผลกระทบต่อ Convergence Time รวมทั้งประสิทธิภาพของเครือข่าย MediumSocks



ชุดของชายขอบระบบเครือข่ายตามปกติจะประกอบด้วยเอ็กซ์ทราเน็ต และการเชื่อมต่อสู่อินเทอร์เน็ตทั่วโลก

MediumSocks จะป้องกันตนเองในปัญหาแบบนี้ได้อย่างไร? คำตอบคือการใช้ BGP

BGP ปะทะ IGP

BGP ได้รับการออกแบบมาให้จัดการกับปัญหาการส่งข้อมูลเส้นทางประเภทนี้โดยเฉพาะ โดยการเชื่อมโยงเครือข่ายทั้งหลายเข้าไว้ด้วยกันก่อให้เกิดเครือข่ายภายใน (Internetwork) ในขณะที่ IGP จะมีชุดเครื่องมือโดยมุ่งไปที่การแลกเปลี่ยนข้อมูลภายใน (Internal Information Exchange) แต่ BGP จัดการแก้ไขปัญหาแบบนี้ได้ดีกว่า เนื่องจากได้รับความเชื่อถือมากกว่า

โซลูชันด้านการจัดสรรเส้นทางเพื่อรักษาความปลอดภัยชายขอบ (Network Edge) ของเครือข่าย

BGP นั้นสามารถกำหนดค่าเพื่อปรับแต่งตามสภาพการใช้งานได้หลากหลาย ช่วยให้เราสามารถสร้างการเชื่อมต่อ (ไปยังเครือข่ายที่นอกเหนือการควบคุมของผู้ดูแลระบบ) ที่ออกแบบไว้อย่างดีและมีความปลอดภัย BGP มีฟังก์ชันหลักๆ ให้คุณใช้งาน อย่างเช่น การกำหนดนโยบาย (Policy) การป้องกัน (Protection) และการจัดการแบบเพียร์ (Peer-based Management)

นโยบาย

การกำหนดนโยบายของ BGP หลายๆ ตัวสามารถป้องกันปัญหาของ MediumSocks ได้ ขอย้อนกลับไปที่ตัวอย่างข้างต้น ตอนที่ 10.1.1.0/24 ถูกส่งจาก SmallFeet ไปยัง BigShoes ทำให้ส่งข้อมูลไปผิดที่ผิดทาง แม้ว่า Prefix Filter ทั่วๆ ไปอาจสามารถแก้ปัญหาเหล่านี้ได้ แต่ทว่า BGP นั้นมีเครื่องมือเสริมอื่นๆ จำนวนมากเพื่อการนี้

- ใช้ Prefix List เพื่อสกัดกั้นการใช้ Prefix Routing Information ที่ยาวเกินไป (เฉพาะเจาะจงมากไป) ในเครือข่าย MediumSocks นโยบายที่กำหนดไว้บน Partner Peering Sessions อาจเปิดโอกาส

ให้ใช้ Prefix ที่มีความยาวของ Maskได้สูงสุดไม่เกิน 17 เท่านั้น เพื่อเป็นการป้องกันไม่ให้รับข้อมูลเส้นทางที่มีรายละเอียดมากเกินไป

- ใช้ AS PATH Filter List ในการป้องกันการส่งข้อมูลซึ่งไม่ได้ส่งมาจากเครือข่ายที่ติดต่ออยู่ไม่ให้ถูกส่งไปยังเครือข่าย MediumSocks ในกรณีนี้ MediumSocks สามารถกรองข้อมูลเส้นทางที่มาจาก BigShoes เท่านั้นที่จะใช้ได้

คุณสามารถแนบ Communities ไปกับ BGP Route ได้ และระบุสิ่งที่คุณต้องการว่า ให้ผู้ดูแลเครือข่ายอื่นทำอย่างไรต่อไป ยกตัวอย่างเช่น หาก MediumSocks ไม่ต้องการให้ SmallFeet มองเห็นเครือข่ายของตนผ่านทาง BigShoes ก็สามารถกำหนดค่า NO_EXPORT community ไว้ตอนส่งข้อมูลเส้นทางที่แจ้งไว้กับ BigShoes เส้นทางใดก็ตามที่ถูกกำหนดค่าเป็น NO_EXPORT ก็จะไม่ถูกประกาศออกไปนอก Routing Domain อีก

ท้ายที่สุด ควรทำจะกรอง Bogon Route ออกไปจากเครือข่ายของคุณ ซึ่ง Bogon Route นั้นหมายถึงเส้นทางที่ใช้ไม่ได้จริงบนอินเทอร์เน็ต ยกตัวอย่างเช่น การกรองเครือข่ายส่วนตัว (Private Network) ทั้งหมดออกจากอินเทอร์เน็ต แม้ว่าเครือข่ายส่วนตัวบางวงอาจได้รับอนุญาตในการกำหนดค่าครั้งก่อน ค่าแอดเดรสที่ได้จองไว้สำหรับโครงการวิจัยหรือเพื่อการใช้มัลติคาสต์ และค่าแอดเดรส ซึ่งไม่สามารถแจกจ่ายให้ใครได้ ก็เป็น Bogon เช่นกัน และโดยทั่วไปก็ไม่ควรที่จะผ่านขอบเขตของโดเมนที่จัดการอยู่

ต่อไปนี้เป็นตัวอย่างการกำหนดค่าคอนฟิกูเรชัน รวมทั้งคำแนะนำเกี่ยวกับวิธีการที่ MediumSocks ใช้ BGP ในการป้องกันโครงสร้างด้านการจัดสรรเส้นทางภายใน (Internal Routing Infrastructure) ที่ cisco.com/packet/183_5a1 ตัวอย่างเหล่านี้สมมติว่า BigShoes ใช้ AS65000 และ MediumSocks ใช้ AS65001

BGP Router Peering with BigShoes

```
router bgp 65001
 neighbor <bigshoes> remote-as 65000
 neighbor <bigshoes> route-map filter-partner-in in
 /* inbound route filter, described below in the
route-map
 /* filter-partner-in configuration
 neighbor <bigshoes> route-map filter-partner-out out
 /* outbound route filter, described below in the
route-
 /* map filter-partner-out configuration
....
route-map filter-partner-in permit 10
 match ip address prefix-list partner-routes-in
 /* any routes permitted by the prefix list partner-
 /* routes-in
 match as-path 1
 /* any routes permitted by the as path access-list 1
will
 /* be accepted
....
route-map filter-partner-out permit 10
 set community no-export
 /* prevents BigShoes from readvertising routes learned
 /* from MediumSocks, and from transiting traffic to
 /* MediumSocks
....
ip prefix-list partner-routes-in seq 10 deny
192.168.0.0/16 ge 15
 /* denies bogon routes in the range 192.168.0.0/16
ip prefix-list partner-routes-in seq 20 deny x.x.x.x/
xx
 /* deny other bogon routes here
ip prefix-list partner-routes-in seq 10 permit
0.0.0.0/0 le 18
 /* permit any routes with a prefix length less than
/17
 /* prevents longer prefix routes from causing local
 /* routing problems
!
ip as-path access-list 1 permit ^65000$
 /* denies any routes originated outside the peering
AS
 /* including BigShoes' partners and routes BigShoes
is
 /* learning from an ISP
```

BGP Router Peering with the Internet Service Provider

```
router bgp 65001
 neighbor <ISP> remote-as <ISP AS>
 neighbor <ISP> prefix-list isp-routes-in in
 neighbor <ISP> route-map filter-isp-out out
....
ip prefix-list isp-routes-in seq 10 permit x.x.x.x/xx
 /* deny bogon routes here
....
route-map filter-isp-out permit 10
 match as-path 2
....
as-path access-list 2 permit ^$
 /* permits only routes originating within
MediumSocks, so
 /* MediumSocks doesn't transit to BigShoes
```

JOIN THE DISCUSSION

ลองถามเพื่อนร่วมงานและผู้เชี่ยวชาญของซิสโก้ หรือแบ่งปันความรู้ของคุณเกี่ยวกับ BGP และโพรโตคอลในการจัดสรรเส้นทางอื่นๆ ได้ที่ Cisco Networking Professionals: forum: cisco.com/discuss/infrastructure

การป้องกัน

BGP ได้เตรียมการป้องกันในกรณีเกิด Flapping Route ในเครือข่าย BigShoes ซึ่งส่งผลกระทบต่อ Convergence Speed และส่งผลต่อเสถียรภาพของเครือข่าย MediumSocks รวมถึงกรณีที่ BigShoes ส่งตารางการจัดสรรเส้นทางทั้งหมดไปยัง Peering Edge ของตน

การป้องกันอย่างแรกทำได้โดยใช้คุณสมบัติของ BGP ที่เรียกว่า Route Flap Dampening ซึ่งใช้วิธีการกำหนดโทษให้แก่เส้นทางทุกครั้งที่เกิด Flap หรือเปลี่ยนแปลง หากเส้นทางใดมีโทษเพิ่มขึ้นจนเกินขีดที่กำหนดไว้ เส้นทางนั้นจะถูกระงับไว้ชั่วคราว Route Flap Dampening นั้นนิยมใช้กันในหมู่ผู้ให้บริการอินเทอร์เน็ตพื่อไว้ป้องกันเส้นทางที่มีการเปลี่ยนแปลงบ่อยๆ

Route Flap Dampening Parameters นั้นจะถือเป็นมาตรการเชิงรุก หรือค่อนข้างรุนแรงมากๆ ในกรณีที่ระงับเส้นทางโดยมีค่าการเปลี่ยนแปลงที่กำหนดไว้ต่ำในช่วงระยะเวลานานๆ แต่ในทางกลับกัน ถ้ากำหนดค่าไว้สูงในช่วงระยะเวลาสั้นๆ

```
router bgp 65000
....
bgp dampening
bgp dampening 1000 2 2000 750 60
```

คุณสามารถจัดการ Flap ด้วย Prefix ที่ต่างกันด้วยอัตราที่ต่างกันได้ โดยใช้ Route-map ยกตัวอย่างเช่น หากการเข้าถึง 10.1.1.0/24 นั้นสำคัญมาก แต่ 10.1.2.0/24 ไม่ใช่ เราสามารถใช้มาตรการเชิงรุก หรือรุนแรงหน่อยกับ 10.1.2.0/24 ได้ ในการแสดงผลว่าเส้นทางใดได้ถูกระงับไปบ้างสามารถใช้คำสั่ง show ip bgp dampened-paths

โดยทั่วไปเรามักต้องการให้ Route Flap Dampening มีระดับที่รุนแรงหน่อยสำหรับ Private Peering Relationship และดูจะไม่ค่อยสมเหตุสมผลเลยถ้าจะยอมให้ค่าการเปลี่ยนแปลงเส้นทางจำนวนสูงๆ ในช่วงระยะเวลาสั้นๆ สำหรับ Private Peering

ในการที่ MediumSocks จะป้องกันตนเองจากการที่ BigShoes ส่งข้อมูลเข้ามาจำนวนมากเกินไปจนล้นเครือข่าย และอาจทำให้การส่งข้อมูลเกิดผิดพลาดไป วิศวกรเครือข่ายของ MediumSocks สามารถจำกัดปริมาณการส่งด้วยคำสั่งต่อไปนี้

```
router bgp 65000
neighbor <bigshoes>
neighbor <big shoes> maximum-prefix 100 restart 30
```

การกำหนดเช่นนี้ช่วยให้ BGP ทำงานเมื่อได้รับการส่งข้อมูลมากกว่า 100 ครั้ง และยอมให้เซสชันรีสตาร์ทได้หลังจากหยุดนิ่งเป็นเวลา 30 วินาที

การป้องกันด้วย BGP อีกอย่างหนึ่งคือการสกัดกั้น Advertising Routes ซึ่งไม่มี AS Number ของเครื่องที่ติดต่อด้วยไม่ให้มารบกวน Peering Router ยกตัวอย่างเช่น หากมีใครที่สามารถเข้าถึงเครือข่าย BigShoes พยายามที่จะส่ง Advertising Routes หมายเลข 10.1.1.0/24 โดยใช้ Originating AS ลวง BGP ของ MediumSocks สามารถปฏิเสธข้อมูลที่แจ้งมากนี้ได้ เนื่องจากไม่มี AS number ของ BigShoes คุณสมบัติที่ว่านี้คือ Enforce the First Autonomous System Path ซึ่งมีให้ใช้กันในซอฟต์แวร์ IOS รุ่นใหม่ๆ ของซิสโก้

คุณสมบัตินี้ช่วยให้เราสามารถควบคุมจำนวนเส้นทางที่เราจะรับใน Peering Session ได้ BGP สามารถตอบสนองต่อเส้นทางที่เพิ่มขึ้นด้วยการออกคำเตือนว่า เราเตอร์กำลังรับงานมากเกินไปแล้ว หรือไม่ก็ปิดเซสชัน BGP ไปเลยเพื่อเป็นการป้องกันอย่างเบ็ดเสร็จเด็ดขาด

นอกเหนือจากการป้องกันประเภทต่างๆ เหล่านี้แล้ว BGP ยังมีระบบป้องกันการโจมตีโดยตรงประเภทอื่นๆ อีกด้วย BGP ได้รับการออกแบบให้สามารถทำงานได้ในสภาพที่มีความเสี่ยงสูง เช่น ลิงก์ออกสู่ภายนอกเครือข่ายอาจไม่ปลอดภัย (หรือไม่สามารถทำให้ปลอดภัยได้) ยกตัวอย่างเช่น BGP สามารถหลีกเลี่ยงไฟร์วอลล์ได้อย่างง่ายดาย เนื่องจากใช้ Unicast TCP Session ในการส่งข้อมูลเส้นทาง วิธีการนี้ช่วยให้เราสามารถใช้ไฟร์วอลล์ในการควบคุมเส้นทางเดินของข้อมูลในเครือข่ายได้ แล้วใช้ BGP ควบคุมการแลกเปลี่ยนข้อมูลเส้นทาง

เราเตอร์ที่ใช้ BGP จะได้รับการปกป้องด้วยกลไกหลายตัวของ BGP ตัวอย่างเช่น Generic Time-to-live Security Mechanism (GTSM) ซึ่งมีคำอธิบายอยู่ใน RFC 3682 at cisco.com/packet/183_5a2

สามารถกำหนดค่าการป้องกันตัวนี้ได้โดยใช้คำสั่งดังนี้

```
router bgp 65000
neighbor <bigshoes> incoming-++1
<minimum ++1 to accept>
```

สรุปได้ว่า เราไม่ควรใช้ IGP ในการรับหรือส่งข้อมูลเส้นทางระหว่างโดเมนในการจัดสรรเส้นทาง 2 ตัว ทางที่ดีควรใช้ BGP ซึ่งเราสามารถเชื่อมั่นในระบบป้องกันที่ดีได้ ■