การประยุกต์ใช้งาน IPCop - ฉบับที่ 132 พฤศจิกายน 2006

- อ่าน 11451 ครั้ง

การประยุกต์ใช้งาน IPCop

โดย Barrie Dempster และ James Eaton-Lee

IPCop คือไฟร์วอลล์สำหรับเครือข่ายสำนักงานขนาดเล็ก / สำนักงานที่บ้าน (SOHO), ซึ่งใช้งานง่ายสุด ๆ ทั้งยังให้คุณสมบัติพื้นฐานส่วนใหญ่ที่คุณคาดว่าไฟร์วอลล์สมัยใหม่ต้องมี และ สิ่งที่สำคัญที่สุดก็ คือ มันได้ติดตั้งสิ่งเหล่านี้ให้กับคุณแบบอัตโนมัติ และง่ายดาย. มันง่ายมากที่จะทำให้ระบบ IPCop เริ่มต้นและทำงาน และใช้ได้ดีเกือบจะตลอดเวลา.

ความน่าเชื่อถือของความสัมพันธ์ระหว่างอินเตอร์เฟส

อินเตอร์เฟสเครือข่ายทั้งสี่ชนิด—สีเขียว, สีแดง, สีน้ำเงิน, และสีส้ม —ได้รับการสนับสนุนโดย IPCop ซึ่งระดับความน่าเชื่อถือของแต่ละแบบถูกกำหนดไว้. นี่เป็นเค้าโครงตารางอย่างง่ายแสดงการจราจรที่เข้าออกของแต่ละอินเตอร์เฟส. ตารางนี้และการเรียนรู้ภายใน จะเป็นหลักสำคัญในการวางแผนเมื่อพิจารณาว่ามีอินเตอร์เฟสอะไรที่ใช้ และใช้เพื่ออะไร นี่เป็นแผนภาพการไหลเวียนของการจราจรแบบพื้นฐานจาก การแนะนำการบริหารจัดการ IPCop [1].

อินเตอร์เฟสจาก	อินเตอร์เฟสไปที่	สถานะ	วิธีการเข
สีแดง	ไฟร์วอลล์	ถูกปิด	เข้าถึงจา
สีแดง	สีส้ม	ถูกปิด	การส่งต่อ
สีแดง	สีน้ำเงิน	ถูกปิด	การส่งต่อ
สีแดง	สีเขียว	ถูกปิด	การส่งต่อ
สีส้ม	ไฟร์วอลล์	ถูกปิด	
สีส้ม	สีแดง	เปิด	
สีส้ม	สีน้ำเงิน	ถูกปิด	ช่องทาง
สีส้ม	สีเขียว	ถูกปิด	ช่องทาง
สีน้ำเงิน	ไฟร์วอลล์	ถูกปิด	เข้าถึงแบ
สีน้ำเงิน	สีแดง	ถูกปิด	เข้าถึงแบ
สีน้ำเงิน	สีส้ม	ถูกปิด	เข้าถึงแบ
สีน้ำเงิน	สีเขียว	ถูกปิด	ช่องทาง

สีเขียว	ไฟร์วอลล์	เปิด	
สีเขียว	สีแดง	เปิด	
สีเขียว	สีส้ม	เปิด	
สีเขียว	สีน้ำเงิน	เปิด	

เมื่อหลับตานึกถึงทางซึ่งการจราจรเข้าสู่ IPCop ไฟร์วอลล์ เราสามารถเห็นเป็นชนิดของชุมทางขนาดยักษ์กับการจราจรของ cop (ตัวย่อของ IP Cop นับจากนี้) ในใจกลางของมัน เมื่อรถ (ในแง่ของเครื่อข่ายคือแพ็กเก็ตของข้อมูล) มาถึงทางแยก cop จะตัดสินใจทางที่แพ็กเก็ตควรจะไป (ขึ้นกับตารางเส้นทางที่ IPCop ใช้) และส่งมันไปในทิศทางที่เหมาสม

ในกรณีที่ลูกข่ายสีเขียวเข้าถึงอินเตอร์เน็ต เราจะสามารถเห็นได้จากตารางที่ผ่านมา ว่าการเข้าถึงเปิดอยู่ ดังนั้น cop จะให้การจราจรผ่านไปได้ ในกรณีอื่น ถ้าลูกข่ายสีน้ำเงินพยายามที่จะเข้าถึงลูกข่ายในส่วนสีเขียว ยกตัวอย่างเช่น cop อาจอนุญาตให้การจราจรผ่าน ถ้ามันมาจาก VPN หรือมาจากช่อง DMZ แต่ถ้าหากลูกข่ายบนส่วนสีน้ำเงินไม่ได้เข้าข่ายการอนุญาต มันก็จะถูกหยุดไว้ รถจะถูกดึงออกไป

ควรจำไว้ว่า (โดยทั่วไป) เมื่อเราแสดงการตั้งค่าของ IPCop ตัวประสานสีแดงจะอยู่บนสุด (ทิศเหนือ), สีส้มจะอยู่ทางซ้าย (ทิศตะวันตก), สีน้ำเงินจะอยู่ทางขวา (ทิศตะวันออก) และสีเขียวจะอยู่ด้านล่าง (ทิศใต้)

การดัดแปลงคุณสมบัติของ IP Cop

จากคุณสมบัติที่มากมายของ IPCop ไฟร์วอลล์ มันเป็นไปได้ ที่จะดัดแปลงลักษณะการทำงานของกฎไฟร์วอลล์ ให้ ตรงกับโครงสร้างสีแดงเป็น ภายในสภาวะแวดล้อมของกฎไฟร์วอลล์ IPCop มีไฟล์ตั้งแต่ชุด 1.4 ออกมาก็ได้อนุญาตให้ผู้ใช้ สามารถเจาะจงกฎไฟร์วอลล์ได้ (/etc/rc.d/rc.firewall.local). ตั้งแต่เวอร์ชั่น 1.3 มีสายของ iptables CUSTOMINPUT,CUSTOMFORWARD, เป็นต้น อนุญาตให้เพิ่มกฎ iptables ด้วยมือ การเจาะจงโดยใช้ iptables อยู่นอกเหนือขอบเขตที่นี่ แต่เราแนะนำผู้อ่านที่สนใจให้อ่าน Linux iptables HOWTO [2].

โครงสร้างเครือข่ายที่หนึ่ง : NAT Firewall

โครงสร้างเครือข่ายแรกของเรา จะทำการแทนที่ NAT (Network Address Translation) ไฟร์วอลล์ที่มีและคุ้นเคยกันอยู่ในตลาดอยู่แล้ว ในสำนักงานขนาดเล็กและบ้าน วิธีการแก้ไขปัญหาอย่างเช่น NAT ไฟร์วอลล์ฝังตัวที่ขายโดย D-Link, Linksys และพันธมิตร มักจะถูกนำมาใช้เพื่อที่จะให้บริการเครือข่ายขนาดเล็ก เพื่อความคุ้มค่าของการเข้าถึงเครือข่ายอินเตอร์เน็ต วิธีการแก้ไขปัญหาอย่าง การแบ่งการเชื่อมต่ออินเตอร์เน็ต การรวมตัวกันของ NAT ไฟร์วอลล์, DNS Proxy, และเครื่องแม่ข่าย DHCP ถูกรวมเข้ากับ ฉบับของ Windows ตั้งแต่ Windows 98 เป็นต้นมา ก็สามารถที่จะอนุญาตให้ PC เครื่องหนึ่งที่ต่อกับโมเด็มหรือตัวประสานเครือข่าย ทำหน้าที่เป็นประตูสัญญาณสำหรับลูกข่ายอื่น ๆ สำหรับวัตถุประสงค์ของเรา เราจะมุ่งประเด็นไปที่ ICS (Internet Connection Sharing) ที่โครงสร้างการเชื่อมต่ออยู่เหนือการทำงานดังกล่าว ซึ่งจำเป็นต้องแทนที่อุปกรณ์กำหนดเส้นทางอย่างเช่น Linksys หรือ NETGEAR ตามรูปแบบข้างต้น การอพยพจากอุปกรณ์กำหนดเส้นทางหนึ่ง ๆ เหล่านี้สู่ IPCop ควรที่จะต้องบันทึกโดยตรง สำหรับการใช้งานจากซอฟท์แวร์ ICS ที่ทำงานอยู่ในเครื่องลูกข่าย ถ้าเราลบออกจากอุปกรณ์ค้นหาเส้นทาง ซึ่งเป็นการไม่จำเป็นและอุปกรณ์ค้นหาเส้นทางสามารถปล่อยให้การตั้งค่าให้เป็นอย่างที่เป็นอยู่ (และ/หรือเก็บเป็นข้อมูลสำรอง, หรือนำกลับมาใช้ภายหลัง)(ดู http://www.annoyances.org/exec/show/ics [3] สำหรับข้อมูลการนำไปใช้งาน (และเนื่องจากนั้น, การงานใช้จากสิ่งที่มีอยู่) ICS บนเวอร์ชั่นที่แตกต่างของ Windows) การแก้ปัญหาแบบนั้น, ขณะที่ประหยัดและสะดวกสบาย แต่ก็มักจะไม่สามารถปรับขนาดได้ หรือ น่าเชื่อถือ และให้ความปลอดภัยที่ไม่ดี พวกเขามักจะเปิดเครื่องสถานีงานให้ทำงานบนความเสี่ยงที่ไม่จำเป็น, ให้ปริมาณงานต่ำ และมักไม่น่าเชื่อถือ มักจะต้องเริ่มเครื่องใหม่และปิดบ่อย ๆ

ด้วยซอฟท์แวร์ไฟร์วอลล์, ไฟร์วอลล์เครือข่ายถูกออกแบบมาเพื่อเป็นเกราะป้องกัน ระหว่างเครื่องสถานีงานและเครือข่ายอินเตอร์เน็ต ด้วยการเชื่อมต่อหนึ่งในเครื่องสถานีงาน โดยตรงกับอินเตอร์เน็ต และการใช้การแก้ปัญหาอย่าง ICS แม้ว่าคุณจะลดทรัพยากรที่จำเป็นในการแบ่งปันการเชื่อมต่ออินเตอร์เน็ต คุณจะเปิดเพยให้เครื่องสถานีงานนั้นเสี่ยงโดยไม่จำเป็น มันเป็นการบังคับให้ PC นั้นทำงานตลอดเวลา แต่เทียบกับเครื่อง PC ระดับล่าง ที่ไม่มีอุปกรณ์ที่ไม่จำเป็น และ PSU พลังต่ำที่รัน IPCop, นี่ก็อาจจะรบกวนกว่า และกินทรัพยากรมากกว่า

IPCop เสนอการแทนที่ที่คุ้มค่า ในสถานการณ์นั้น ให้ธุรกิจขนาดเล็กและผู้ใช้ระดับบ้านด้วยไฟร์วอลล์ที่มีประสิทธิภาพ โดยไม่จำเป็นต้องซับซ้อนมากเกินไป

และการเพิ่มคุณสมบัติต่าง ที่ไม่มีในอุปกรณ์ฝังตัวหรือ ICS อย่างเช่น เครื่องแม่ข่าย DHCP ที่ปรับแต่งได้, การตรวจจับการบุกรุก, เครื่องแม่ข่าย Proxy และอื่น ๆ

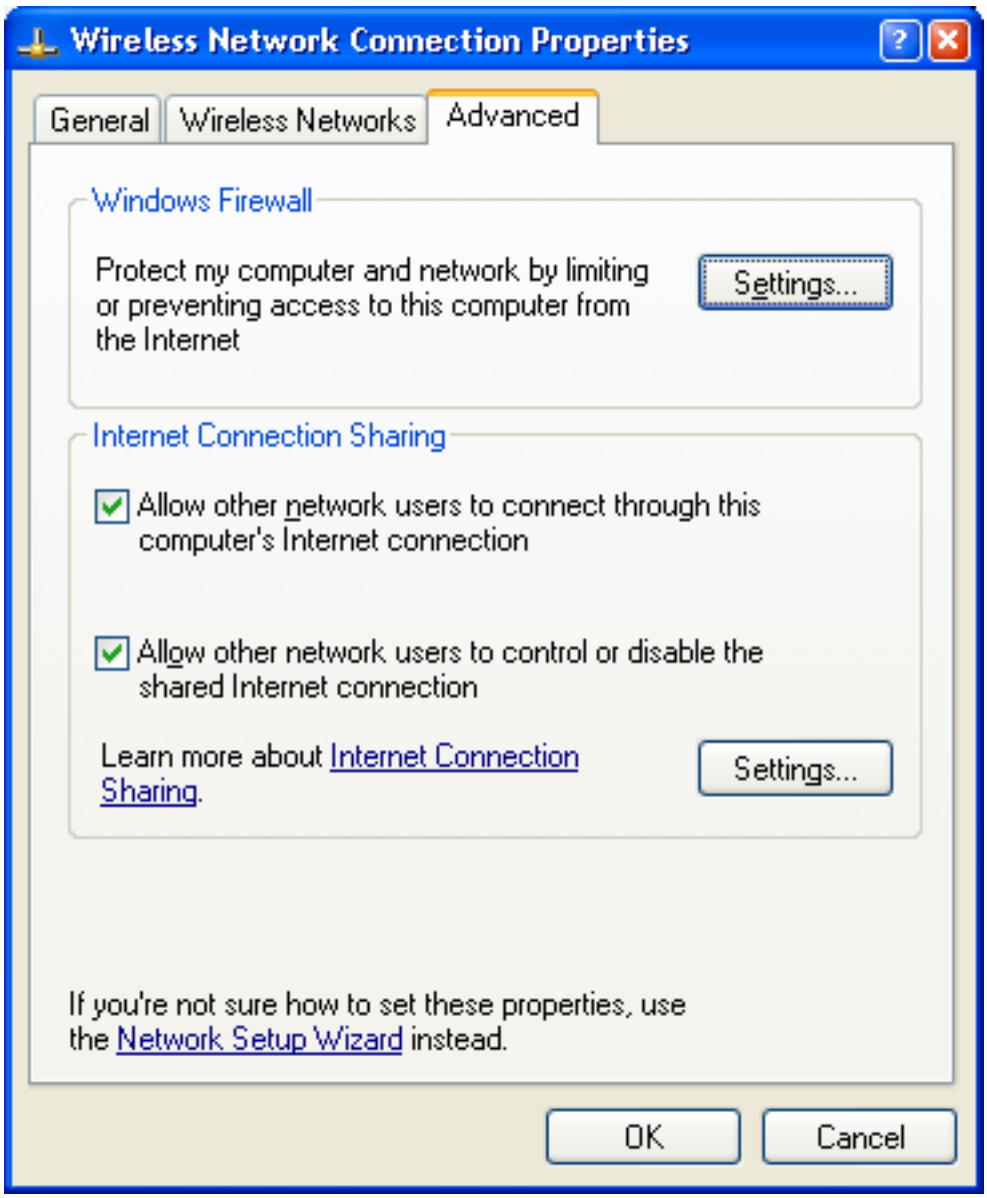
โครงสร้างเครือข่ายตัวอย่างต้องมั่นใจว่า การทำไฟร์วอลล์เรียบร้อยก่อนที่ลูกข่ายจะนำข้อมูลไป การใช้ชุดที่ถูกออกแบบให้ทำหน้าที่เป็นไฟร์วอลล์ของเครือข่าย ช่วยเพิ่มคุณภาพของการบริการให้กับลูกข่ายได้เป็นอย่างดีเท่าที่ความปลอดภัยของเครือข่ายให้ ในสถานการณ์นี้ ชิ้นส่วนต่าง ๆ ของ IPCop ควรจะเป็น :

- เขตสีเขียว/สีแดง
- เครื่องแม่ข่าย DHCP
- เครื่องแม่ข่าย DNS

ในสถานการณ์ดังกล่าว ผู้ดูแลเครือข่าย หรือผู้ให้คำปรึกษาอาจจะต้องเลือก ที่จะเปิดใช้ชิ้นส่วนต่าง ๆ ของคุณสมบัติที่จะเพิ่มคุณภาพของบริการให้กับเครือข่าย : I

- ระบบตรวจจับการบุกรุก
- IPSec เพื่ออนุญาตงานทางไกล หรือการสนับสนุนทางไกล
- การส่งต่อพอร์ต เพื่ออนุญาตการเข้าถึงทางไกลสู่ VNCหรือ บริการเครื่องปลายทาง / หน้าจอทำงานระยะไกล เพื่อความง่าย ของการเข้าถึงสำหรับการสนับสนุนระยะไกล (สะดวกสบายกว่า IPsec แต่ปลอดภัยน้อยกว่า)

การใช้งานจากซอฟท์แวร์ ICS ที่ทำงานอยู่ดังที่สถานการณ์เป็นสิ่งที่ง่าย— เราเพียงแต่ปิดการทำงานของ ICS ดังที่แสดงเป็นภาพตัวอย่างด้านล่าง (นำมาจากคุณสมบัติการเชื่อมต่อเครือข่ายภายนอก ตัวประสานเครือข่าย ICS) การลบ ICS เป็นสิ่งที่ง่ายเพียงแค่ไม่เลือกทางเลือก 'Allow other network users to connect through this computer's Internet connection' หลังจากที่เราทำอย่างนี้ เราก็กด OK แล้วก็เริ่มคอมพิวเตอร์ใหม่ถ้ามีการถาม และเราก็อิสระที่จะเพิ่ม/ลบ ตัวประสานภายนอกบนเครื่องสถานีงาน (ปิดการทำงานถ้าเราต้องการปล่อยให้การ์ดเครือข่ายอันที่สองในเครื่อง หรือถ้ามีเครื่องสองเครื่องบนบอร์ด หรือเอาออกถ้าเรากำลังใช้โมเด็มภายนอก หรือชิ้นส่วนฮาร์ดแวร์ที่เราตั้งใจจะเอาออกหรือเพิ่มเข้าไปสำหรับ เครื่อง IPCop ของเรา)



กฎไฟร์วอลล์สำหรับโครงสร้างเครือข่ายนี้เป็นแบบง่าย โดยที่ส่วนสีเขียวจะอนุญาตในการเข้าถึงทรัพยากรบนตัวประสานสีแดงอย่างอัตโนมัติ ไม่มีการกำหนดโครงสร้างเฉพาะที่จำเป็น เพื่อที่จะติดตั้งให้ทำงาน ข้อดีอย่างอื่นสำหรับการนำ IPCop มาใช้งานกับสถานการณ์สำนักงานขนาดเล็กก็คือ กรณีที่ธุรกิจจำเป็นต้องเติบโตขึ้น หารแก้ปัญหาแบบนี้ก็ยังปรับขนาดได้ เช่นธุรกิจที่ทำงานด้วยสถานีงาน Windows ในกลุ่มงานหนึ่งอาจจะตัดสินว่า กลุ่มงานนั้นไม่เพียงพอต่อความต้องการ และต้องการการจัดการแบบรวมศูนย์, ตัวจัดเก็บไฟล์ และการปรับแต่ง.

IPCop, มีการปรับปรุงขั้นต้นสำหรับเหตุการณ์แบบนี้ ให้เป็นผลอย่างง่ายดาย เพราะว่ามันมีการเปิดทางให้ยกระดับรวมอยู่ด้วย ซึ่งไม่จำเป็นต้องมีการปรับปรุงฮาร์ดแวร์หรือซอฟท์แวร์สำหรับการปรับไปจาก NAT และ DHCP แบบง่าย ๆ ไปยังเครือข่ายที่ประกอบด้วยหลายส่วนย่อย, การส่งต่อพอร์ต และเครื่องแม่ข่ายพร็อกซี่ ถ้าเครื่องแม่ข่ายมีการ์ดประสานเครือข่ายอยู่หลายตัวอยู่แล้ว (และด้วยราคาในปัจจุบันนี้ มันไม่มีเหตุผลที่จะไม่มี ถ้าถูกคาดการขยายไว้ล่วงหน้าแล้ว) นี่สามารถทำได้โดยที่ไม่ขัดจังหวะ การทำงานของบริการเครื่องลูกข่ายที่มีอยู่ หรือเกิดเพียงเล็กน้อยเท่านั้น.

โครงสร้างเครือข่ายที่สอง : NAT Firewall ที่มี DMZ

ในสถาณการณ์สำนักงานขนาดเล็กที่มีการเติบโตของบริษัท ความจำเป็นที่ความจำเป็นสำหรับจดหมายอิเล็กทรอนิกส์ที่เข้ามา อาจจะถูกบังคับกระตุ้นให้ต้องมีการทำงานของเขตสีส้ม การนำไปใช้งาน และการติดตั้งของเครื่องแม่ข่ายจดหมายในส่วนนี้ ดังนั้นบริษัทอาจจะเลือกที่จะเก็บรักษาเครื่องทำงานและเครื่องแม่ข่ายพื้นฐานภายใน ให้อยู่ภายในเขตเครือข่ายสีเขียว และเอาเครื่องแม่ข่ายไว้ใน DMZ (DeMilitarized Zone) บนเครื่องสวิตช์หรือฮับ หรือเพียงติดรวมกับส่วนเชื่อมต่อสีส้มของ เครื่อง IPCop โดยใช้สายสลับ เช่นนั้น ระบบจถถูกปล่อยไปบนอินเตอร์เน็ต ส่วนนี้จะให้ประโยชน์ที่สำคัญ โดยการให้ "เส้นหยุด" ผ่านไป ซึ่งน่าจะยากกว่าสำหรับผู้บุกรุกที่จะขยายการเข้าถึงเขาหรือเธอสู่เครือข่าย เครื่องแม่ข่ายจดหมาย Microsoft's Exchange บางครั้งจะสนับสนุนพวกการตั้งค่าที่จะใช้ การแลกเปลี่ยนหน้าที่ "ส่วนหน้า" และ "ส่วนหลัง"

(แม้ว่าหน้าที่เหล่านี้จะยูกยกเลิกในการออกจำหน่ายของ Exchange ในอนาคต) ด้วยการปรับแต่งค่าเครือข่ายที่แตกต่างกัน แม้ว่าอย่างเครื่องลูกข่ายลินุกซ์จะใช้การจัดการระบบอย่างเช่น Novell's eDirectory หรือ RedHat's Directory Server (RHDS) หรือการกรองที่เป็นประโยชน์อื่น สิ่งที่ระบบเหมือนกันคือการใช้เครื่องแม่ข่ายที่มีส่วนติดต่อภายนอกแบบ SMTP (บางทีก็ทำงานด้วย MTA ที่เป็นโอเพ่นซอร์สอย่าง Exim) ก็จะมีเป็นประโยชน์เช่นเดียวกัน.

ในโครงสร้างนี้ เครื่องลูกข่ายต่างอิสระที่จะติดต่อกับเครื่องแม่ข่ายจดหมาย (อาจจะด้วย POP, IMAP, RPC, หรือ RPC บน HTTP) เพื่อให้เครื่องแม่ข่ายจดหมายที่มีอยู่เป็นส่วนหนึ่งของวงเครือข่ายเพื่อการรับรองกับเครื่องแม่ข่ายรายนาม เราก็จะเป็นที่จะต้องเปิดพอร์ตที่จำเป็น (ซึ่งอาจขึ้นกับผู้ให้บริการเครื่องแม่ข่ายรายนาม) เพื่อให้เครื่องแม่ข่ายรายนามใช้คุณสมบัติของช้องทาง DMZ.

เรามีการติดตั้งกฎการส่งต่อพอร์ตจากหมายเลขเครือข่ายภายนอก ของไฟร์วอลล์ IPCop ไปที่พอร์ต 25 ของเครื่องแม่ข่ายจดหมาย นี่จะอนุญาตให้เครื่องแม่ข่ายจดหมาย สามารถติดต่อกับแม่ข่ายจดหมายภายนอก เพื่อที่จะรับส่งจดหมายได้ สำหรับโครงสร้างนี้ สิ่งที่เป็นอันตรายเครื่องแม่ข่ายจดหมาย (ซึ่งการอยู่ในส่วนสีเขียวควรจะทำให้อยู่ในอันตรายตลอดเครือข่าย) ถูกควบคุม ตามระดับการป้องกันที่ไฟร์วอลล์มีให้.

ตามโรงสร้างเครือข่ายเช่นนี้, เราใช้ความสามารถข้างล่างนี้ของไฟร์วอลล์ IPCop :

- เขตสีแดง, สีส้ม, สีเขียว
- ช่องทาง DMZ
- เครื่องแม่ข่าย DHCP
- เครื่องแม่ข่าย DNS
- การส่งต่อพอร์ตไปยังส่วนสีส้ม

เราอาจจะเลือกที่จะใช้ส่วนประกอบต่าง ๆ ของคุณสมบัติเหล่านี้ด้วยก็ได้ :

- ระบบตรวจจับการบุกรุก
- การส่งต่อพอร์ตไปสู่เครื่องแม่ข่ายเว็บบนเครื่องแม่ข่ายจดหมาย (สำหรับการเข้าถึงภายนอกของ IMAP หรือกล่องจดหมายของ Exchange ด้วยเว็บเมล์ อย่างเช่น Horde, SquirrelMail, หรือ Outlook Web Access) เครื่องแม่ข่ายพร็อกซี่ (สำหรับการเข้าถึงอินเตอร์เน็ตของเครื่องทำงาน)
- IPSec สำหรับการเข้าถึงทางไกลสู่เครื่องแม่ข่ายในส่วนสีเขียว และ สีส้ม สำหรับการเข้าถึงภายนอก
- เครื่องแม่ข่ายจดหมายส่วนหลัง ก้วยกล่องจดหมายในเขตสีเขียว โดยใช้เครื่องแม่ข่ายในส่วนสีส้มส่งต่อ ทำการค้นหา/กรองไวรัส หรือจดหมายขยะ

โครงสร้างเครือข่ายที่สาม: NAT Firewall ที่มี DMZ และ เครือข่ายไร้สาย

ในองค์กรณ์ขนาดใหญ่ หรือถ้าเครือข่ายที่พัฒนาขึ้นมาอีก เราอาจจะเลือกที่จะขยายโครงสร้างเครือข่ายของเราโดยใช้ไฟร์วอลล์ตั้งแต่หนึ่งหรือมากกว่า.

หลายครั้งที่ไฟร์วอลล์ IPCop ถูกใช้เดี่ยว ๆ สำหรับแยกแต่ละที่ตั้ง หรือเพื่อที่จะแยก DMZ หนึ่ง ๆ หรือมากกว่าต่างหากจากไฟร์วอลล์ มันเป็นการพิจารณาที่คุ้มค่าที่ IPCop จะถูกออกแบบพื้นฐานสำหรับเครือข่าย ที่มีเพียงไฟร์วอลล์เครือข่าย ในธุรกิจขนาดเล็กและขนาดกลาง และตลาดบ้าน/สำนักงานที่บ้าน แม่ว่ามันสามารถที่จะตั้งค่าให้ IPCop ใน การใช้งานขนาดใหญ่ มันก็ไม่ถูกต้องซะทีเดียว และมีชุดชิ้นส่วนอื่น ๆ ที่ สนับสนุนและเหมาะสมกับการทำอย่างนั้น กรณีแบบนี้ บังคับให้ส่วนเครือข่ายของ IPCop เริ่มที่จะมีภาระมากกว่าที่เหมาะสม และจำนวนของการทำงาน ทำให้จำเป็นที่จะต้องปรับปรุง IPCop เพื่อตรงกับความต้องการขององค์กร ที่เกินกว่าการทำการติดตั้งชุดชิ้นส่วนอื่นที่เหมาะสมกับโครงสร้างเครือข่ายเดียวกัน.

ในตัวอย่างนี้ เราจะพิจารณาขอบเขตที่กว่างที่สุดที่เครื่อง IPCop หนึ่ง ๆ ควรจะนำไปใช้งาน การใช้ส่วนเชื่อมต่อเครือข่ายทั้งสี่เพื่อป้องกันเครือข่ายด้วยเครือข่ายภายใน (สีเขียว) อินเตอร์เน็ต หรือ การเชื่อมต่อ WAN (สีแดง) DMZ หนึ่งที่ประกอบด้วยเครื่องแม่ข่ายมากกว่าหนึ่ง (สีส้ม), และส่วนของเครือข่ายไร้สาย (สีน้ำเงิน) กับระบบ IPSec VPN. ในกรณีเช่นนี้ เราควรแน่ใจว่าเลือกที่จำใช้งานทั้งหมดของคุณสมบัติระดับสูงที่มีใน IPCop ซึ่งได้แก่ เครื่องแม่ข่ายพร็อกซี่ และระบบตรวจจับการบุกรุก.

ในสถานการณ์นี้ บริการที่เรากำลังให้บริการในแต่ละส่วนเชื่มอต่อเครือข่าย เป็นดังนี้ : ในส่วนเชื่อมต่อสีแดง , ซึ่งหมายถึงนโยบายมาตรฐาน, เราทำการเปอดคุณสมบัติส่งต่อพอร์ต เพื่ออนุญาตให้การเชื่อมต่อไปยังเครื่องแม่ข่ายจดหมาย ที่พอร์ต 25 ใน DMZ และไปที่พอร์ต 443 (https) บนเครื่องแม่ข่ายจดหมาย เพื่อให้การเชื่อมต่อสู่ระบบจดหมายเว็บธุรกิจ เราได้อนุญาต IPSec ที่เข้ามาจาก ไฟร์วอลล์ IPCop

เพื่ออนุญาตการเข้าถึงทางไกลกับผู้ดูแลผู้ที่ทำงานทางไกล และให้การเชื่อมต่อทางไกลสำหรับการสนับสนุน สำหรับ IT Staff และซอฟท์แวร์กับฮาร์ดแวร์ของผู้ขายอื่น ๆ.

บนส่วนเชื่อมต่อสีน้ำเงิน, เราให้การเชื่อมต่อด้วย IPSec VPN สำหรับลูกข่าย เพื่อที่เขาสามารถเข้าถึงบริการที่ทำงานอยู่เครื่องแม่ข่ายภายในส่วนสีเขียว และส่วน DMZ คู่ค้าและผู้มาเยี่ยมก็ได้รับอนุญาตให้เข้าสู่ส่วนสีเขียวผ่านการใช้ WPA โดยใช้รูปแบบกุญแจที่ตั้งค่าที่จุดเชื่อมต่อเครือข่ายไร้สาย.

[เมื่อใช้การเข้ากุญแจต้องแน่ใจว่า คุณใช้ความยาวมากที่สุดของกุญแจที่ประกอบมาจากต้นฉบับแบบสุ่มที่ดี เมื่อ WPA จะไม่สามารถป้องกันการเดารหัสแบบไล่สุ่มไปเรื่อย ๆ ของกุญแจที่บกพร่องได้ นี่ก็เป็นเหตุผลที่ดีสำหรับการเปลี่ยนกุญแจเป็นระยะ ๆ. -- René]

WPA-PSK กับจุดเชื่อมต่อเดี่ยว ป้องกันการเข้าถึงส่วนเครือข่ายไร้สาย และอินเตอร์เน็ตโดยผู้ใช้งานที่ไม่ได้รับสิทธิ์ และนี่เป็นการแก้ปัญหาที่เพียงพอสำหรับเครือข่ายขนาดเล็กและขนาดกลางส่วนมาก การใช้อันที่ใหม่กว่า อย่างคุณสมบัติ จุดเชื่อมต่อที่สามารถใช้ WPA2-PSK ช่วยเพิ่มความปลอดภัยมากขึ้น โดยที่ไม่ต้องมีจุดเชื่อมต่อหรือเครือข่ายพื้นฐานที่สนับสนุน RADIUS หรือ Certificate Services. นโยบายไฟร์วอลล์ และระบบ IPSec ทำให้แน่ใจว่า ผู้มาเยี่ยมและคู่ค้า จะสามารถเข้าถึงส่วนสีแดง (อินเตอร์เน็ต) และไม่สามารถเข้าถึงทรัพยากรใด ๆ ของเครือข่าย.

บนส่วนเชื่อมต่อสีส้ม, ช่องทางเชื่อมต่อของเราอนุญาตให้เครื่องแม่ข่าย DMZ เชื่อมต่อไปยังเครื่องอม่ข่ายรายนาม และ ตัวควบคุมขอบเขต Kerberos ในส่วน สีเขียว เพื่อรับรองผู้ใช้เข้าสู่สิ่งเหล่านั้น ด้วยระบบรายนาม นี่ทำให้มั่นใจว่านโยบายและการตั้งค่าสำหรับเครื่องแม่ข่ายเหล่านี้ ถูกจัดการจากส่วนกลาง และมีล็อกไฟล์เก็บอยู่ที่ส่วนกลางของสิ่งเหล่านั้น แต่ ความเสียหายที่เกิดจากส่วนบริการที่ติดต่อกับภายนอก จะถูกลดจนต่ำสุด และแน่ใจถึงความปลอดภัยของธุรกิจ และเป็นไปตามที่คาดหมายไว้

บนส่วนเชื่อมต่อสีเขียว เราอนุญาตให้เชื่อมต่อไปได้ทุกส่วนเชื่อมต่อ เครื่องสถานีงานและเครื่องแม่ข่ายภายในส่วนสีเขียวถูกจัดการบริการสถานีงาน ซึ่งผู้ใช้ไม่จำเป็นที่ต้องมีระดับการเข้าถึง ที่ทำให้เกิดอันตรายกับทรัพยากรที่พวกเขาเข้าถึง.

[ม้าโทรจันกำลังเป็นที่นิยม นี่เป็นเหตุผลที่ดี ที่มีแนวคิดเกี่ยวกับการจำกัดเครื่องเขที่เข้าถึงเครือข่ายภายในเครือข่ายสีเขียว สู่อุปกรณ์พร็อกซี่ด้วยซอฟท์แวร์ระบบตรวจจับ/ป้องกันการบุกรุก. -- René]

ในกรณีนี้, เราทำการใช้งานคุณสมบัติของ IPCop ดังนี้ :

- เขตสีแดง, สีส้ม, สีเขียว, สีน้ำเงิน
- ช่องทาง DMZ
- เครื่องแม่ข่าย DHCP
- เครื่องแม่ข่าย DNS
- การส่งต่อพอร์ตไปยังเขตสีส้ม
- IPSec สำหรับการเข้าถึงระยะไกลไปยังส่วน สีเขียว, สีส้ม, สีน้ำเงิน
- IPSec สำหรับการเข้าถึงทรัพยากรภายใน โดยผู้ใช้สีน้ำเงิน
- ระบบตรวจจับการบุกรุก
- การส่งต่อพอร์ตไปยังเครื่องแม่ข่ายเว็บบนเครื่องแม่ข่ายจดหมายภายนอก
- เครื่องแม่ข่ายพร็อกซี่ (สำหรับการเข้าถึงอินเตอร์เน็ตของเครื่องทำงาน)

ในองค์กรที่ใหญ่ขึ้น เราอาจจะเลือก IPSec เพื่อที่ใช้ IPSec แบบ site-to-site เพื่อจะเชื่อมต่อสำนักงานนี้กับสาขาอื่น ๆ ในกรณีนี้ ที่เป็นกรณีที่ทำหน้าที่เป็นไฟร์วอลล์เครือข่ายแบบเดี่ยว, IPCop เก่ง.

บทความนี้ดีดแปลงมาจากหนังสือ "Configuring IPCop Firewalls: Closing Borders with Open Source" โดย Packt Publishing [4].

สำหรับรายละเอียดอื่น ๆ กรุณาเยี่ยม http://www.packtpub.com/ipcop/book/ [5].

อภิปรายปัญหา: อภิปรายบทความนี้กับ The Answer Gang [6]

Barrie Dempster

Barrie Dempster ปัจจุบันเป็น Senior Security Consultant ของ NGS Software Ltd ผู้ให้คำปรึกษาที่มีชื่อเสียงของโลก ที่รู้จักกันดีกับการที่พวกเขามุ่งสนใจที่การวิจัยความอ่อนแอของซอฟท์แวร์ประยุกต์ และความปลอดภัยของฐานข้อมูลระดับองค์กร. เขามีพื้นฐานระดับล่าง และความปลอดภัยของข้อมูลในจำนวนของสภาวะแวดล้อมแบบพิเศษ เช่น บริการของสถาบันการเงิน, บริษัทโทรคมนาคม, ศูนย์บริการ, และองค์กรอื่นในหลายทวีป, Barrie มีประสบการณ์ในการรวมเครือข่ายระดับล่างและระบบโทรคมนาคม ที่จำเป็นต้องใช้การออกแบบ, ทดสอบ และการจัดการที่มีความปลอดภัยสูง เขามีส่วนในโครงการหลากหลายจากการออกแบบ และการพัฒนาระบบธนาคารอิเล็กทรอนิกส์ สำหรับการประชุมทางไกลขนาดใหญ่ และระบบโทรศัพท์ระดับล่าง พอ ๆ กับการทดสอบเจาะระบบ และประเมินความปลอดภัยของธุรกิจที่ล่อแหลมในระดับล่าง

James Eaton-Lee

James Eaton-Lee ทำงานเป็นผู้ให้คำปรึกษาเฉพาะความปลอดภัยระดับล่าง ผู้ซึ่งทำงานกับลูกค้าตั้งแต่ธุรกิจขนาดย่อมที่มีพนักงานที่ทำงานด้วยมือ ไปจนถึงธนาคารนานาชาติ เขามีพื้นฐานที่หลากหลาย รวมถึงประสบการณ์ที่ทำงาน IT กับ ISP ห้างหุ้นส่วนผู้ผลิตสินค้า, และศูนย์บริการ Jamesได้มีส่วนร่วมในการรวมระบบตั้งแต่ อนาล็อก และ ระบบโทรศัพท์ VOIP จนถึง NT และ วงเครือข่าย AD ในสภาวะแวดล้อมที่ฉุกเฉิน ที่มีเครื่องนับพัน ไม่ว่าจะเป็น UNIX & เครื่องแม่ LINUX servers ที่ทำหน้าที่ต่าง ๆ. James มีความแม่นยำในการเลือกที่จะใช้เทคโนโลยีที่เหมาะสม และเป็นเทคโนโลยีใกล้เคียงกับความต้องการและยืดหยุ่นที่สุด สำหรับธุรกิจทุกขนาด โดยเฉพาะอย่างยิ่ง ตลาด SME ที่เทคโนโลยีมักจะถูกลืมและถูกมองข้าม. James เป็นคนที่มีความเชื่อมั่นอย่างยิ่งในความสัมพัธ์และความข้อดีของ Open Source และ Free Software เป็นเวลาม่าหลายปีแล้วจะประมาณไม่ได้ ที่ใช้มันสำหรับเขาเอง และลูกค้าของเขา การรวมมันในหลากหลายรูปแบบร่วมกับเทคโนโลยีอื่น ๆ .

สงวนลิขสิทธิ์ ปี 2006, René Pfeiffer and pooz. ออกวางภายใต้สัญญาอนุญาต Open Publication license [7] เว้นแต่บันทึกภายในบทความบอกเป็นอย่างอื่น. Linux Gazette ไม่ได้ถูกสร้างขึ้น, ได้รับการสนับสนุน, หรือได้รับการรับรอง จากผู้ให้ใช้โฮสต์, SSC, Inc.

ตีพิมพ์ในเล่มที่ 132 ของ Linux Gazette, พฤศจิกายน ปี 2006

SiteTags: Linux Gazette [8]
IPCop [9]

Source URL (modified on 2009-08-15 10:39): https://sake.in.th/node/8#comment-0

Links
[1] http://www.ipcop.org/1.4.0/en/admin/html/section-firewall.html
[2] http://www.linuxguruz.com/iptables/howto/
[3] http://www.annoyances.org/exec/show/ics
[4] http://www.packtpub.com/
[5] http://www.packtpub.com/ipcop/book
[6] mailto:tag@lists.linuxgazette.net?subject=Talkback:132/dempster.html
[7] http://linuxgazette.net/copying.html
[8] https://sake.in.th/category/sitetags/linux-gazette
[9] https://sake.in.th/category/sitetags/ipcop