ภาษาอังกฤษ

APF (Advanced Policy Firewall) - 9.7 [apf@r-fx.org]

1) Introduction:
Advanced Policy Firewall (APF) is an iptables (netfilter) based firewall system designed around the essential needs of today's Internet deployed servers and the unique needs of custom deployed Linux installations. The configuration of APF is designed to be very informative and present the user with an easy to follow process, from top to bottom of the configuration file. The management of APF on a day-to-day basis is conducted from the command line with the 'apf' command, which includes detailed usage information and all the features one would expect from a current and forward thinking firewall solution.

The technical side of APF is such that it embraces the latest stable features put forward by the iptables (netfilter) project to provide a very robust and powerful firewall. The filtering performed by APF is three fold:
1) Static rule based policies (not to be confused with a "static firewall")
2) Connection based stateful policies
3) Sanity based policies

The first, static rule based policies, is the most traditional method of firewalling. This is when the firewall has an unchanging set of instructions (rules) on how traffic should be handled in certain conditions. An example of a static rule based policy would be when you allow/deny an address access to the server with the trust system or open a new port with conf.apf. So the short of it is rules that infrequently or never change while the firewall is running.

ภาษาไทย

APF (นโยบายไฟล์วอลขั้นสูง) - 9.7 [apf@r-fx.org]

1) บทนำ:
นโยบายไฟร์วอลล์ขั้นสูง (APF) คือตารางไอพี (netfilter) ซึ่งมีพื้นฐานอยู่บนระบบไฟร์วอลล์ซึ่งออกแบบด้วยความต้องการที่จำเป็นของเซิฟเวอร์อินเทอร์เน็ตทุกวันนี้ และ ความต้องการเฉพาะของ การติดตั้ง Linux ที่กำหนดเอง การตั้งค่าของ APF นั้นออกแบบมาเพื่อให้ข้อมูลและนำเสนอผู้ใช้ด้วยไฟล์การตั้งค่าจากต้นจนจบที่สามารถทำตามได้ง่ายดาย การจัดการของ APF แบบวันต่อวันถูกสร้างมาจากคำสั่ง 'apf' ซึ่งประกอบด้วยรายละเอียด ข้อมูลการใช้งานและฟังก์ชั่นที่ผู้ใช้พึงคาดหวังจากการจัดการไฟร์วอล์ซึ่งเป็นปัจจุบันและใช้งานได้ในอนาคต

ด้านเทคนิคของ APF นั้น ได้ประกอบไปด้วยความสามารถที่ทันสมัยมีสเถียรภาพซึ่งขับเคลื่อนโดยโปรเจค iptables (netfilter) เพื่อสร้างไฟร์วอลล์ที่ทรงพลังมาก กระบวนการกรองที่ดำเนินการโดย APF มี 3 ขั้นตอน:
1) นโยบายบนพื้นฐานกฎคงที่ (ไม่เกี่ยวข้องกับ "ไฟร์วอลล์คงที่ หรือ static firewall ")
2) นโยบายสเตตฟูลบนพื้นฐานการเชื่อมต่อ
3) นโยบายบนพื้นฐานความบริสุทธิ

ขั้นตอนที่ 1 นโยบายบนฟื้นฐานกฎคงที่ คือวิธีการดั้งเดิมที่สุดในการสร้าง Firewall และนี่คือที่ที่ firewall จะมีชุดกระบวนการที่ไม่เปลี่ยนแปลง (กฎ) ในการจัดการการส่งข้อมูลในแต่ละเงื่อนไข ตัวอย่างของนโยบายบนพื้นฐานกฎคงที่ คือส่วนที่คุณจะ อนุญาต/ปฏิเสธ การเข้าถึง address ไปยังเซิฟเวอร์ ด้วยระบบการเชื่อใจหรือ เปิด port ใหม่ ด้วย conf.apf ดังนั้นมันจึงเป็นกฎที่ไม่เปลี่ยนแปลงบ่อยนักหรือไม่เปลี่ยนแปลงเลยในขณะที่ firewall ทำงานอยู่