Reţele VPN cu OpenVPN

Dragoş Acostăchioaie
Facultatea de Informatică Iaşi
<dragos@unixinside.org>

VPN – Retele private virtuale

- VPN = sistem care permite conectarea sigura a mai multor retele, prin intermediul Internetului
- VPN permite comunicatia prin intermediul unor “tunele”, asigurand siguranta acesteia
- “tunelele” = conexiuni punct-la-punct intre doua calculatoare sau doua retele
- sunt cel mai des utilizate pentru interconectarea sediilor companiilor si conectarea agentilor mobili la reteaua interna
- utilizeaza algoritmi criptografici pentru comunicatie

VPN – Scurt istoric

- IPSec – incepand cu 1995: aflat inca in dezvoltare, necesita module ale nucleului, relativ greu de configurat
- SSL – ofera in special servicii pentru aplicatiile Web, ruleaza in “user space”
- Nucleul Linux ofera doua tipuri de interfete virtuale de retea: *tun* si *tap*
- tun – interfata de tip punct-la-punct, trimite pachetele catre “user space”, permitand aplicatiilor sa manipuleze dispozitivul ca un fisier

VPN – Scurt istoric

- tap – similar cu tun, insa interfata de retea este de tip Ethernet
- cu ajutorul interfetei virtuale tun, pot fi create tunele VPN
- pachetele IP provenite de la interfetele tun sau tap sunt criptate si incapsulate printr-o conexiune UDP apoi trimise prin retea
- la receptie, pachetele urmeaza cursul invers
- exemple de VPN-uri in “user space”: OpenVPN, Vtun, Tinc, Cipe si multe altele

Dezavantaje ale IPSec

- IPSec modifica stiva IP: examineaza pachetele, verifica daca exista o legatura sigura cu destinatia acestora, apoi cripteaza/decripteaza informatiile (criptare oportunista)
- datorita limitarilor numarului de adrese IPv4, au aparut o multitudine de retele private care folosesc NAT pentru a accesa Internetul
- datorita acestei limitari s-a raspindit si alocarea dinamica de adrese IP
- IPSec se dovedeste relativ inflexibil la acestea

Securitatea VPN-urilor

- Un VPN trebuie sa ofere protectie impotriva atacurilor pasive si celor active
- atacul pasiv nu poate intrerupe sau modifica pachetele transmise intre doua calculatoare, dar le poate in schimb captura
- criptarea = combaterea atacurilor pasive
- atacul activ poate interveni in canalul de comunicatie si modifica pachetele (“om-in-mijloc”)
- autentificarea = prevenirea atacurilor active

Securitatea VPN-urilor

- autentificarea inseamna semnarea fiecarui pachet printr-o functie hash, pentru ca destinatarul sa poata verifica daca provine dintr-o sursa sigura (HMAC)
- pentru autentificarea initiala si schimbul de chei simetrice poate fi utilizat SSL/TLS
- pot fi folosite si chei statice, predefinite
- pentru certificate si chei private este folosit RSA PKI (biblioteca OpenSSL)

OpenVPN - avantaje

- portabilitate - portat pe numeroase platforme: Linux, *BSD, Windows, MacOS, Solaris etc.
- nu necesita modificari ale nucleului
- rulare de tip “daemon”
- poate fi utilizat impreuna cu NAT si adrese IP alocate dinamic
- daemonul ruleaza sub un utilizator neprivilegiat
- usor de configurat

OpenVPN - facilitati

- in configuratia “clasica”, fiecare daemon OpenVPN suporta un singur tunel peste o interfata tun/tap, utilizand un singur port UDP/TCP (ideal pentru conexiuni de tip “bridge”)
- este permisa conectarea unui numar oarecare de clienti la un singur daemon OpenVPN, care utilizeaza o singura interfata tun/tap respectiv un singur port UDP (ideal pentru agenti mobili)
- poate fi utilizat si ca “gateway” (atunci cand se doreste redirectarea traficului catre Internet prin tunel)