Chapter 12:
Anatomy of an Attack

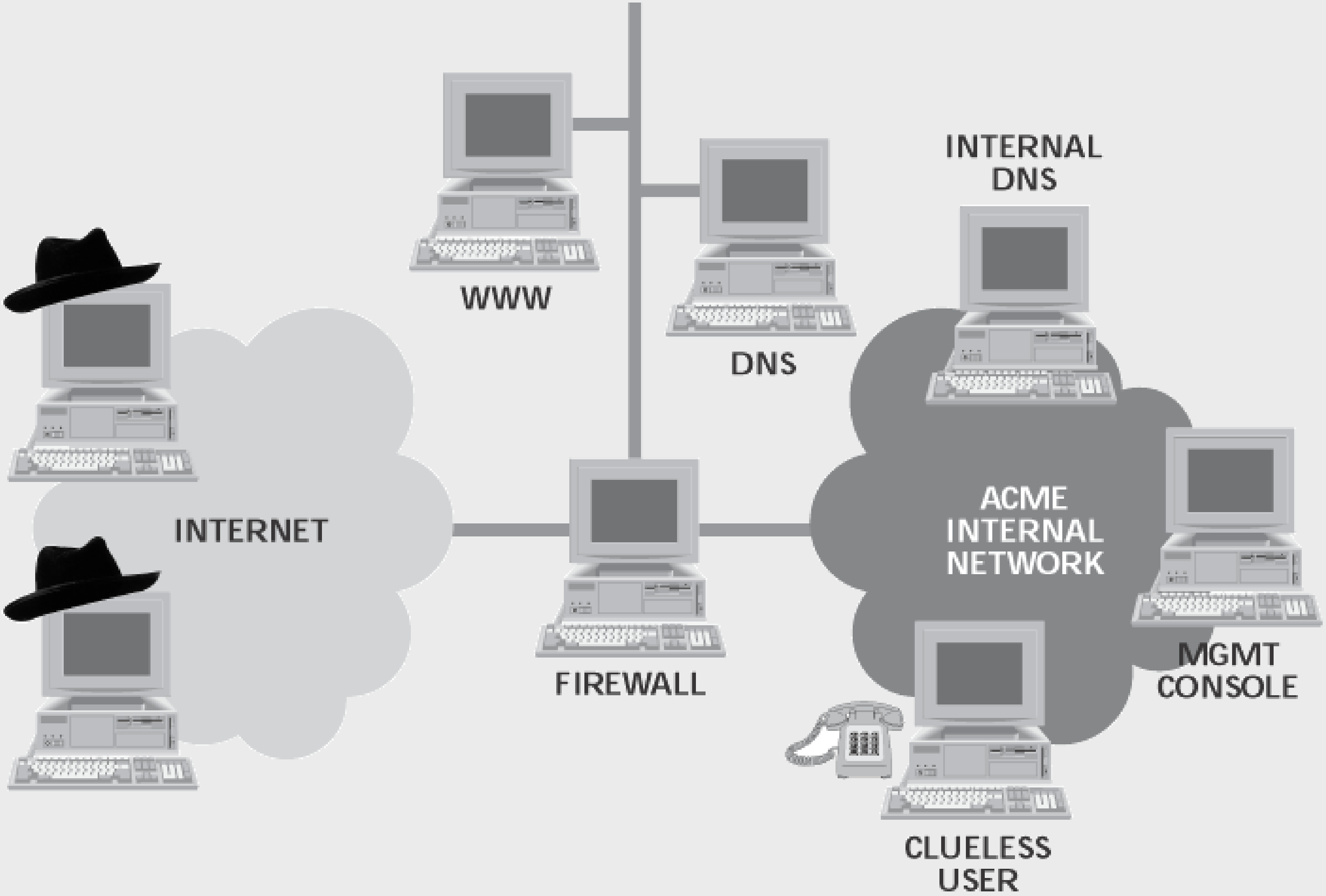


Figure 12.1
Network Architecture of Acme Widgets

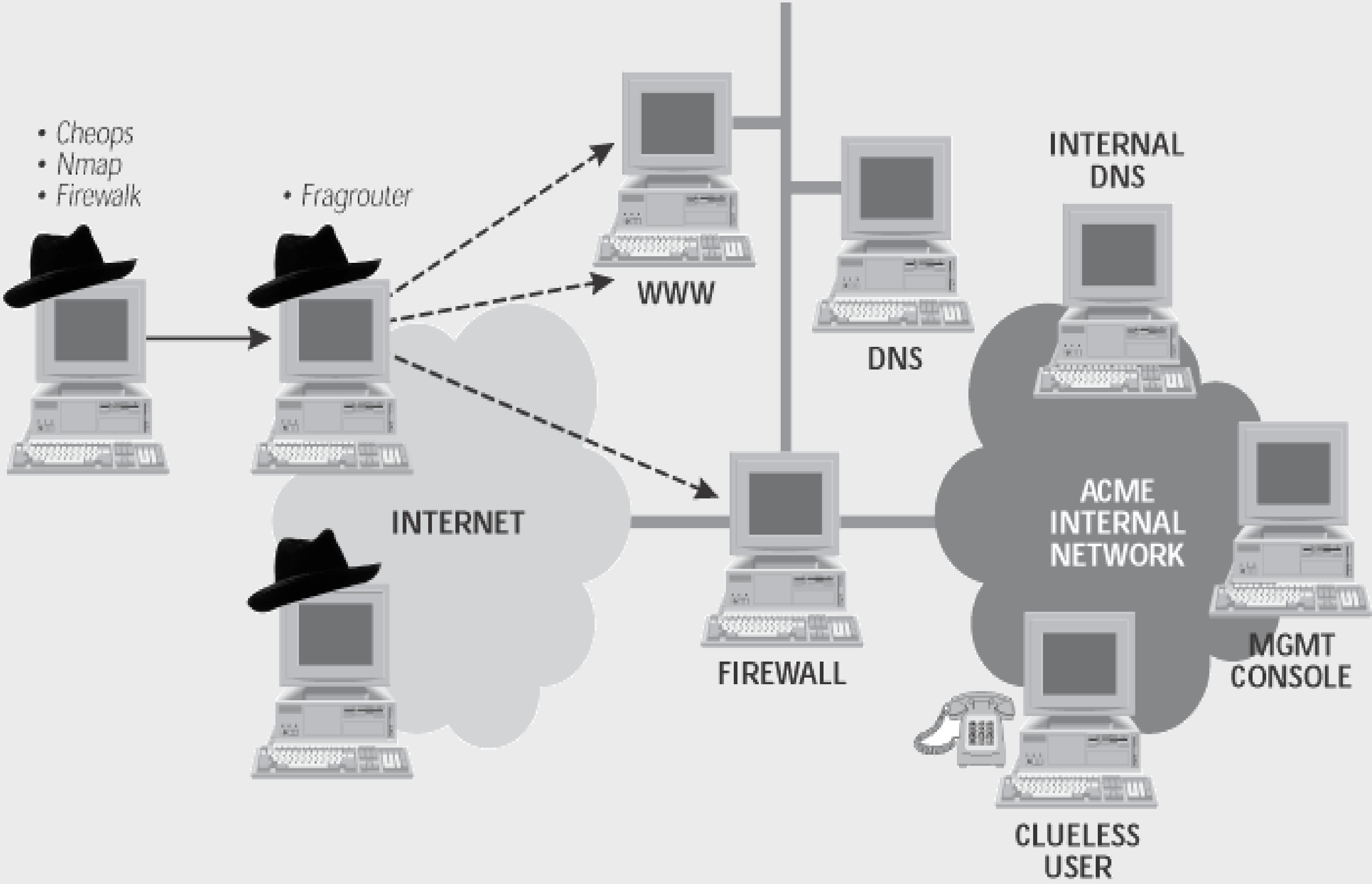


Figure 12.2
Let the scanning begin!

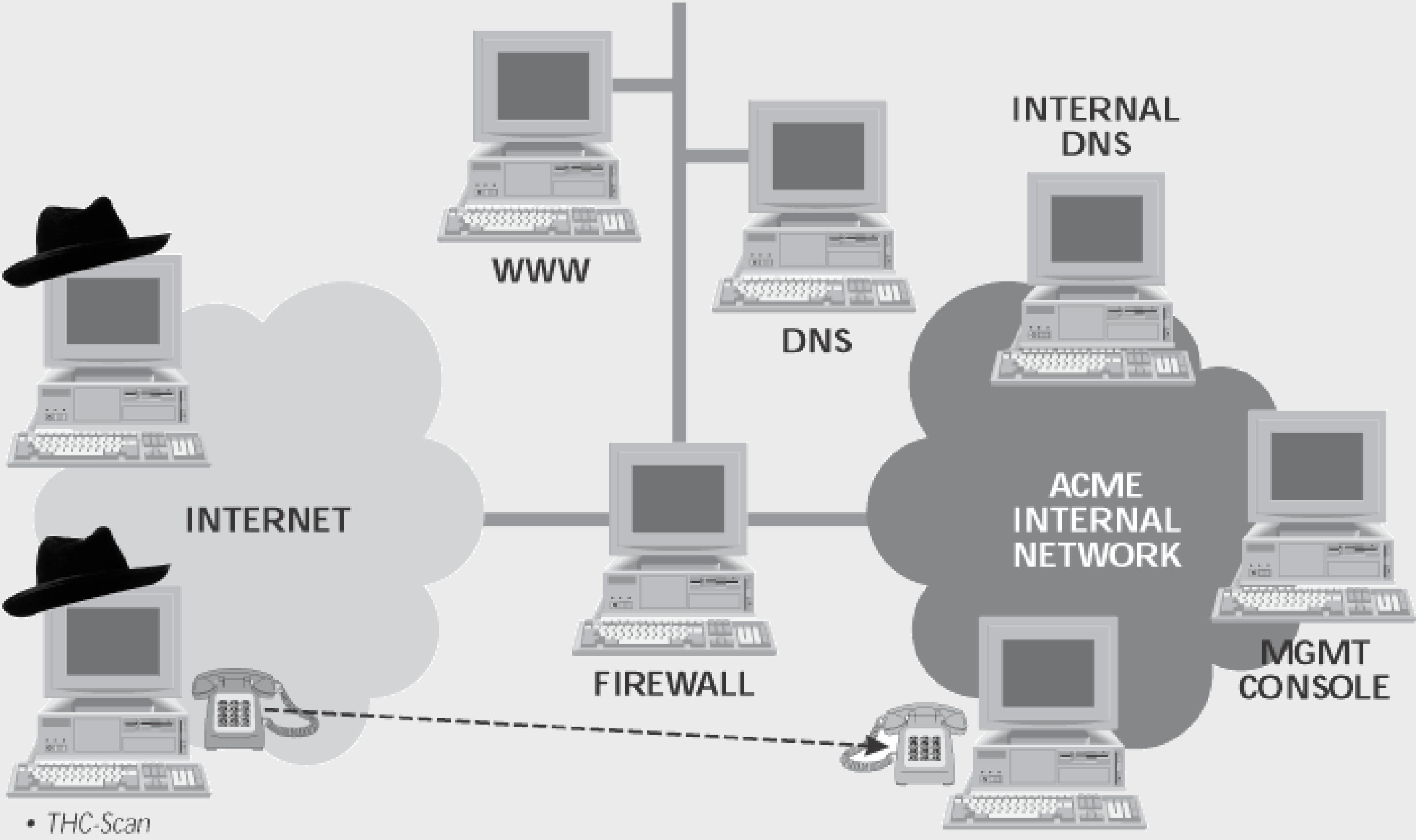


Figure 12.3
War dialing success

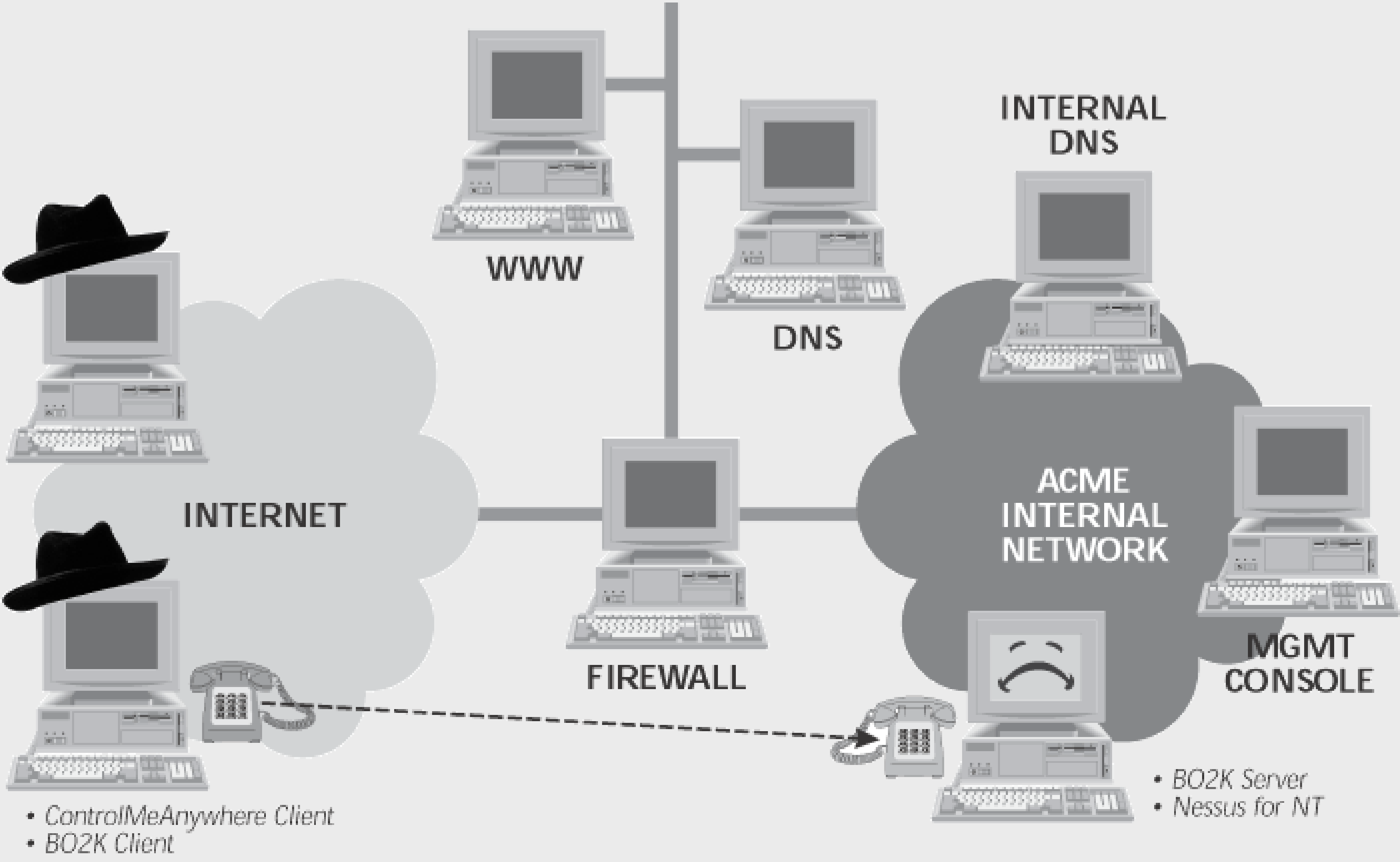


Figure 12.4
Darth installs a B02K backdoor and Nessus

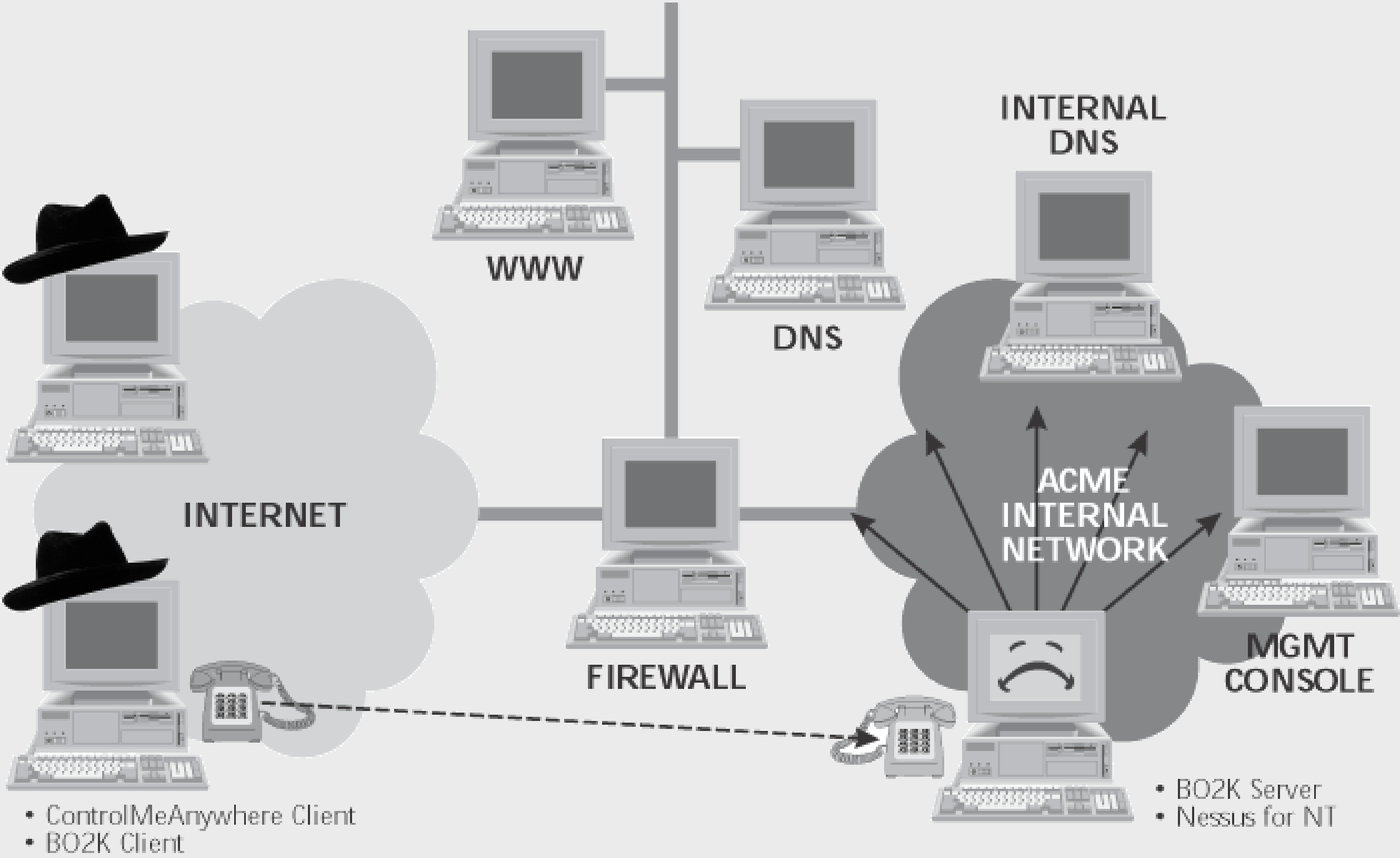


Figure 12.5
Scanning the internal network using Nessus

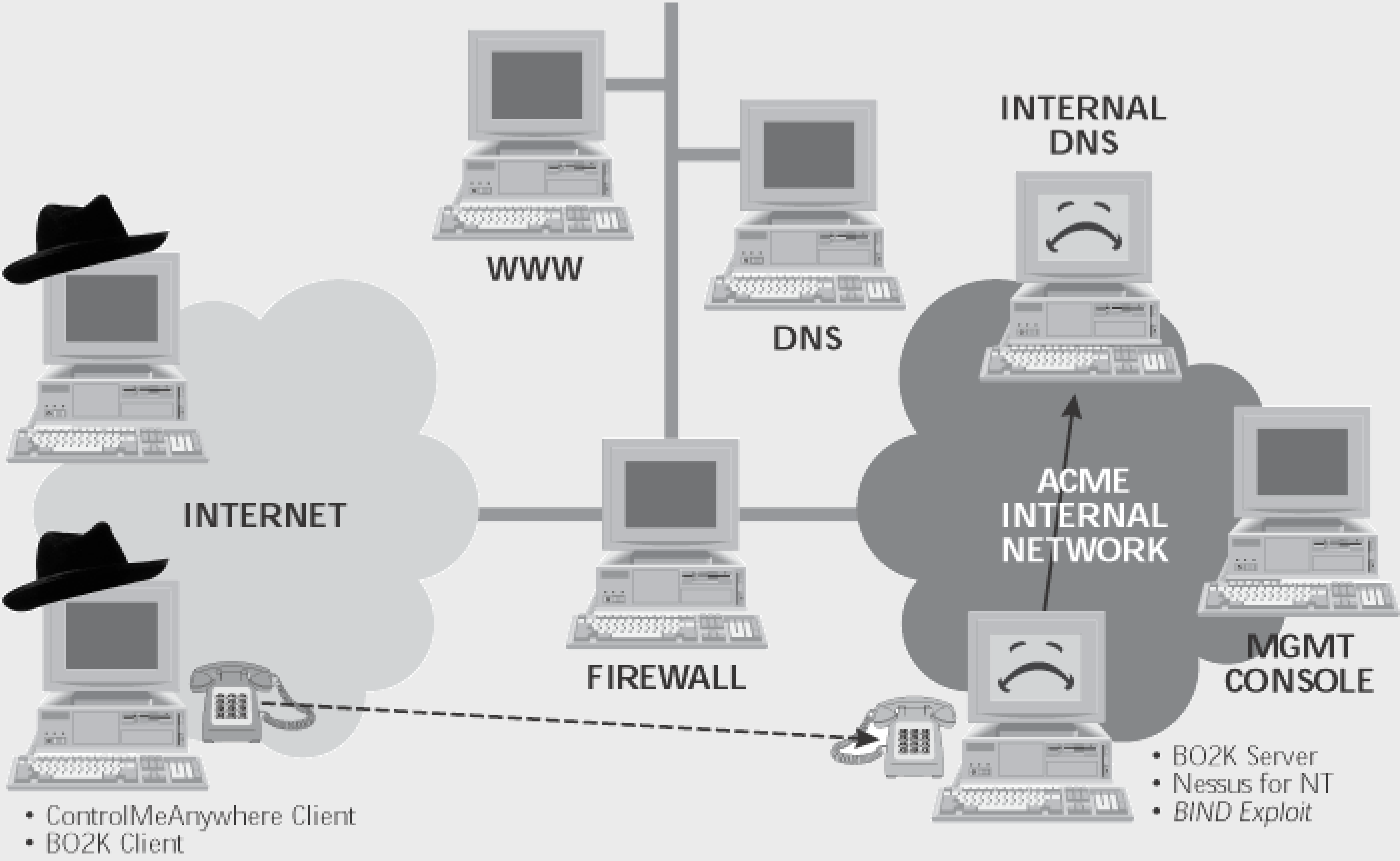


Figure 12.6
Taking over the internal DNS server

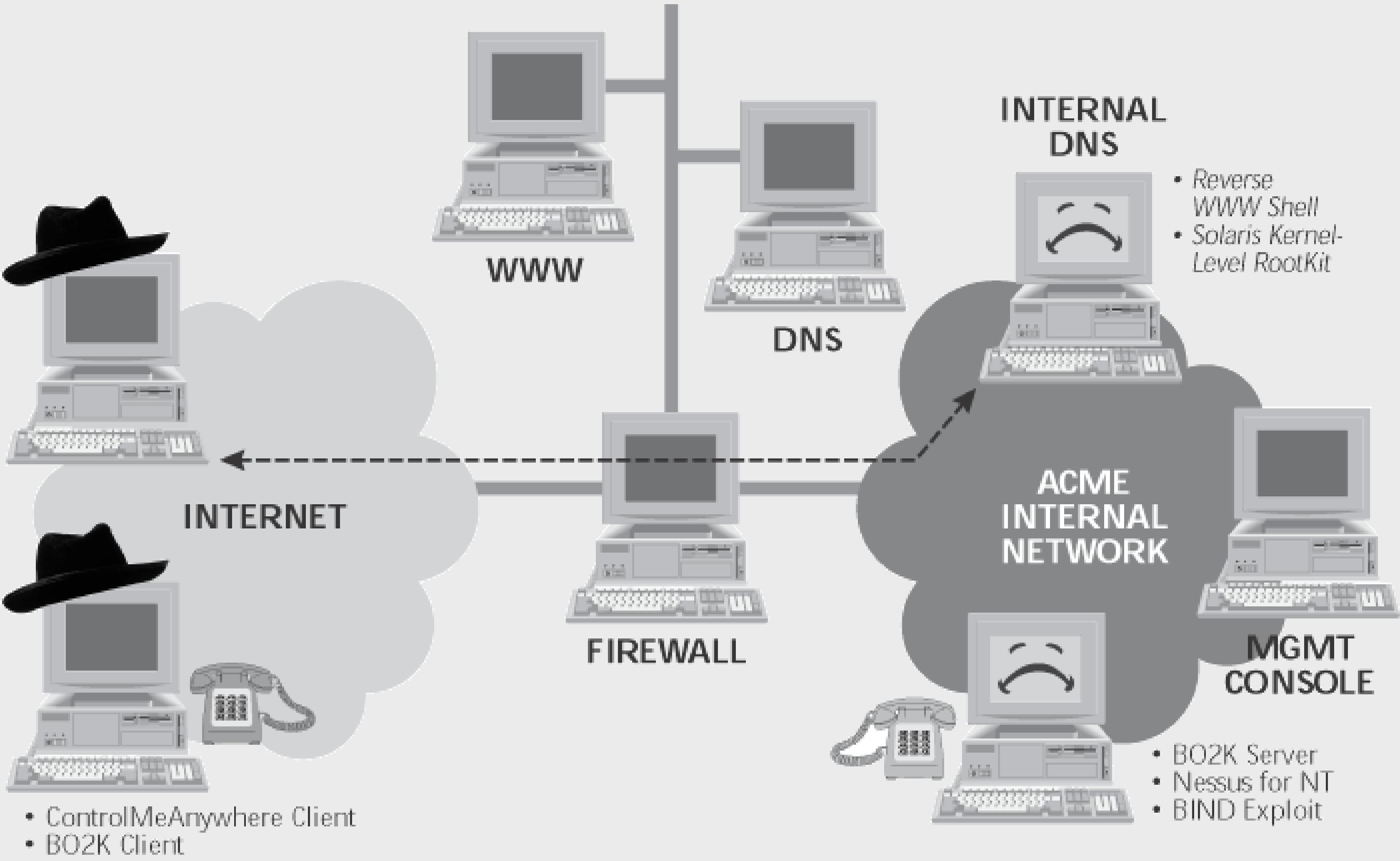


Figure 12.7
Using Reverse WWW Shell for access

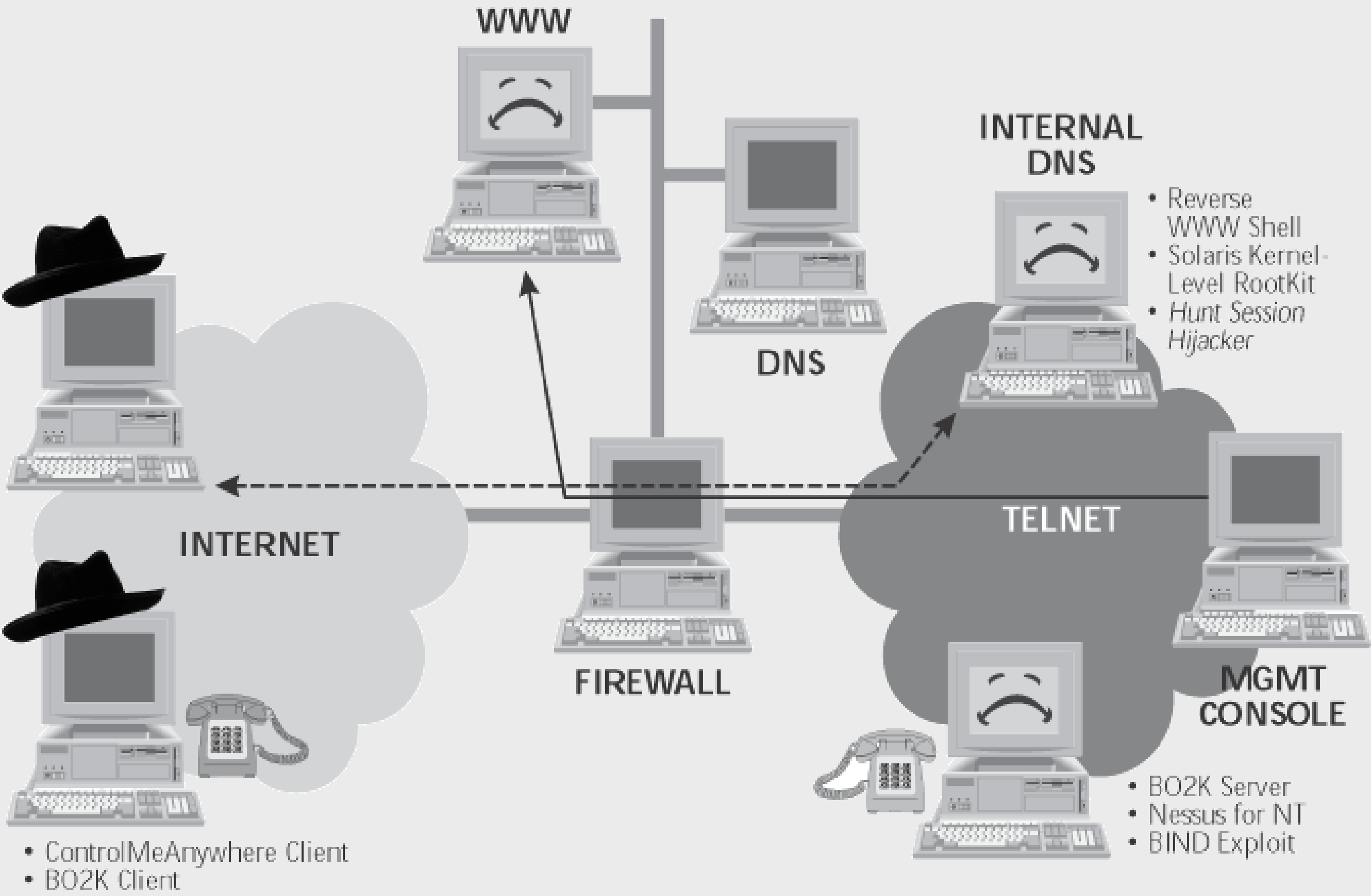


Figure 12.8 Hijacking a telnet session to the Web server with root privileges

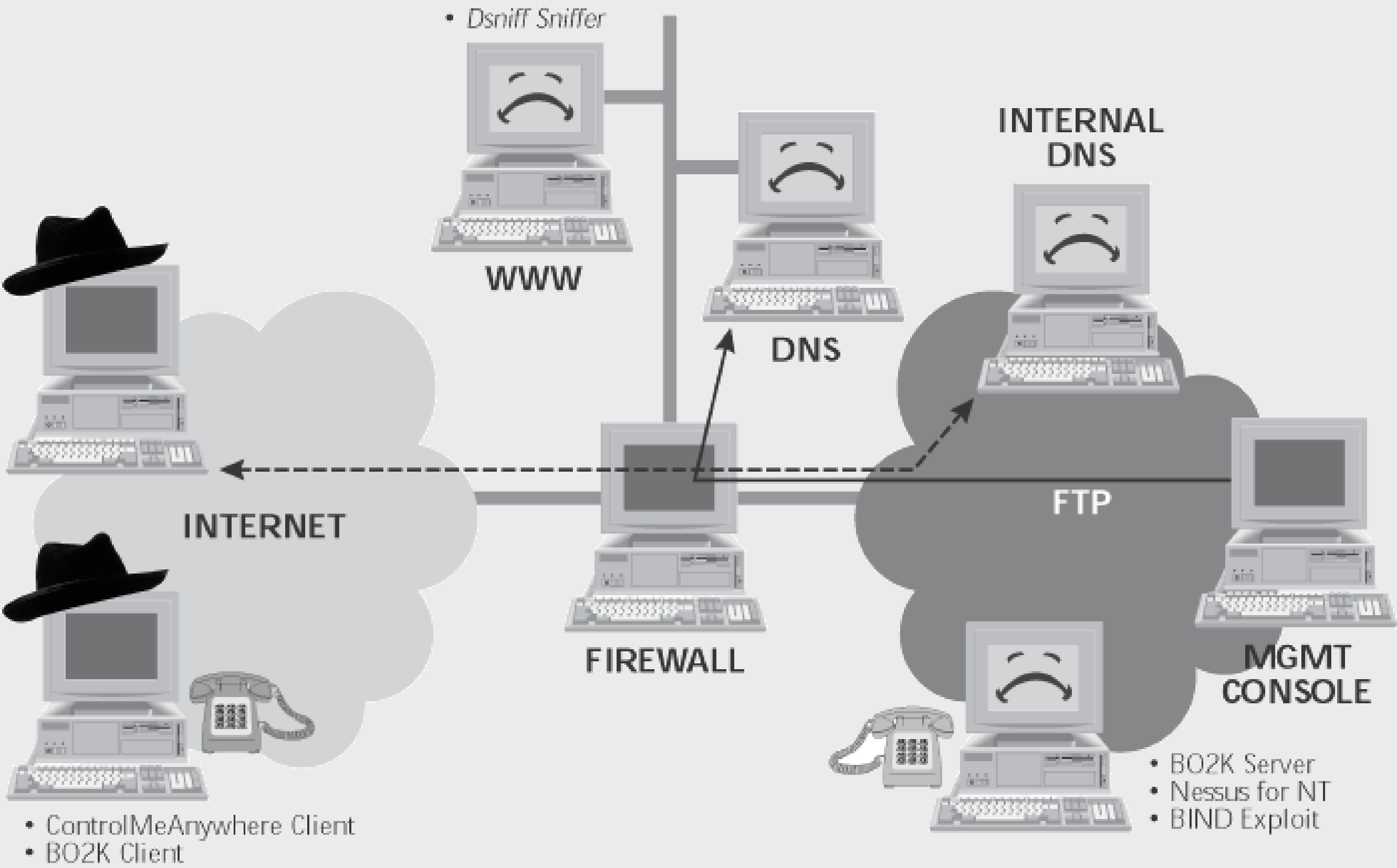


Figure 12.9 Sniffing the external DNS server's password via Dsniff

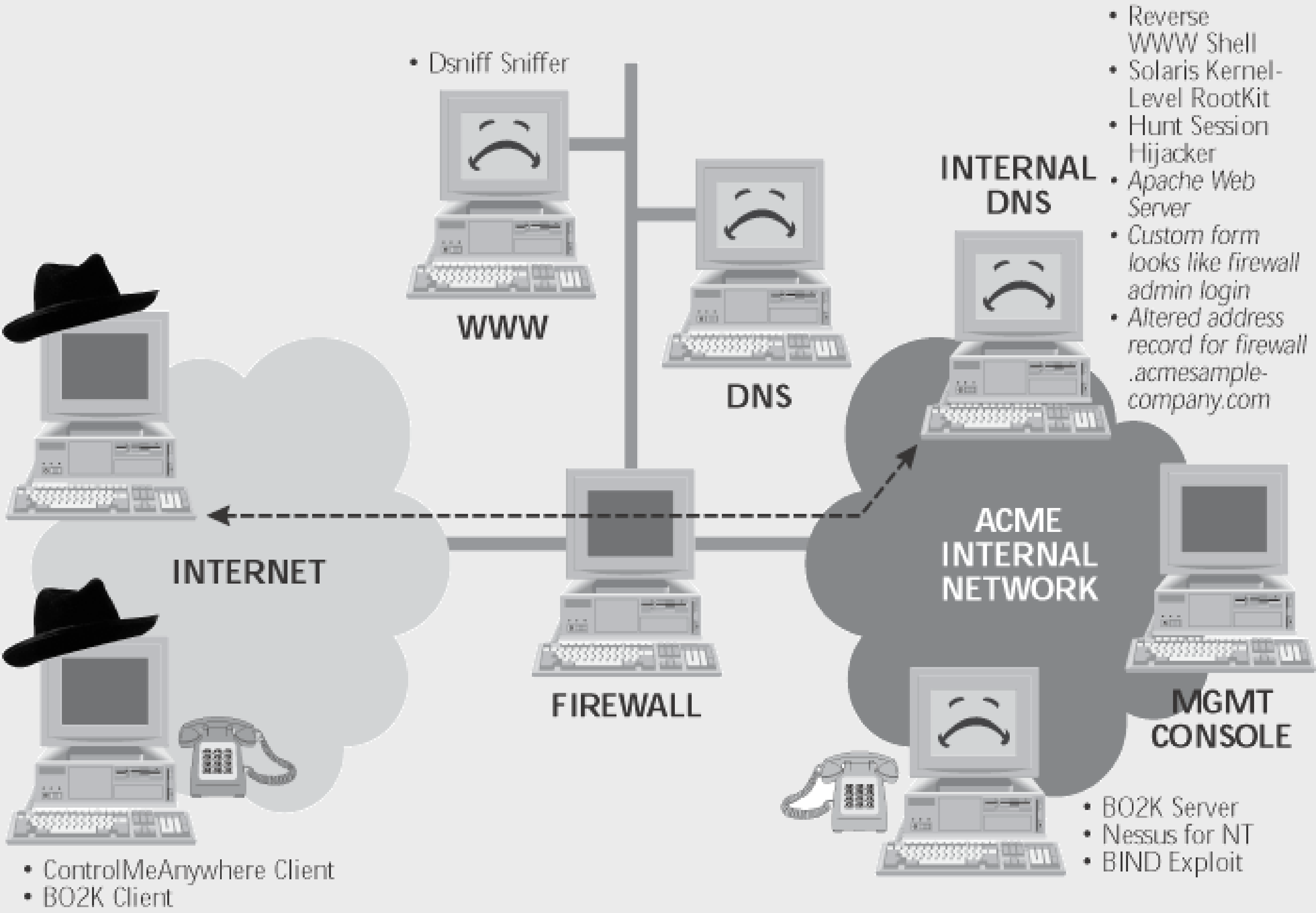


Figure 12.10 Darth’s trap

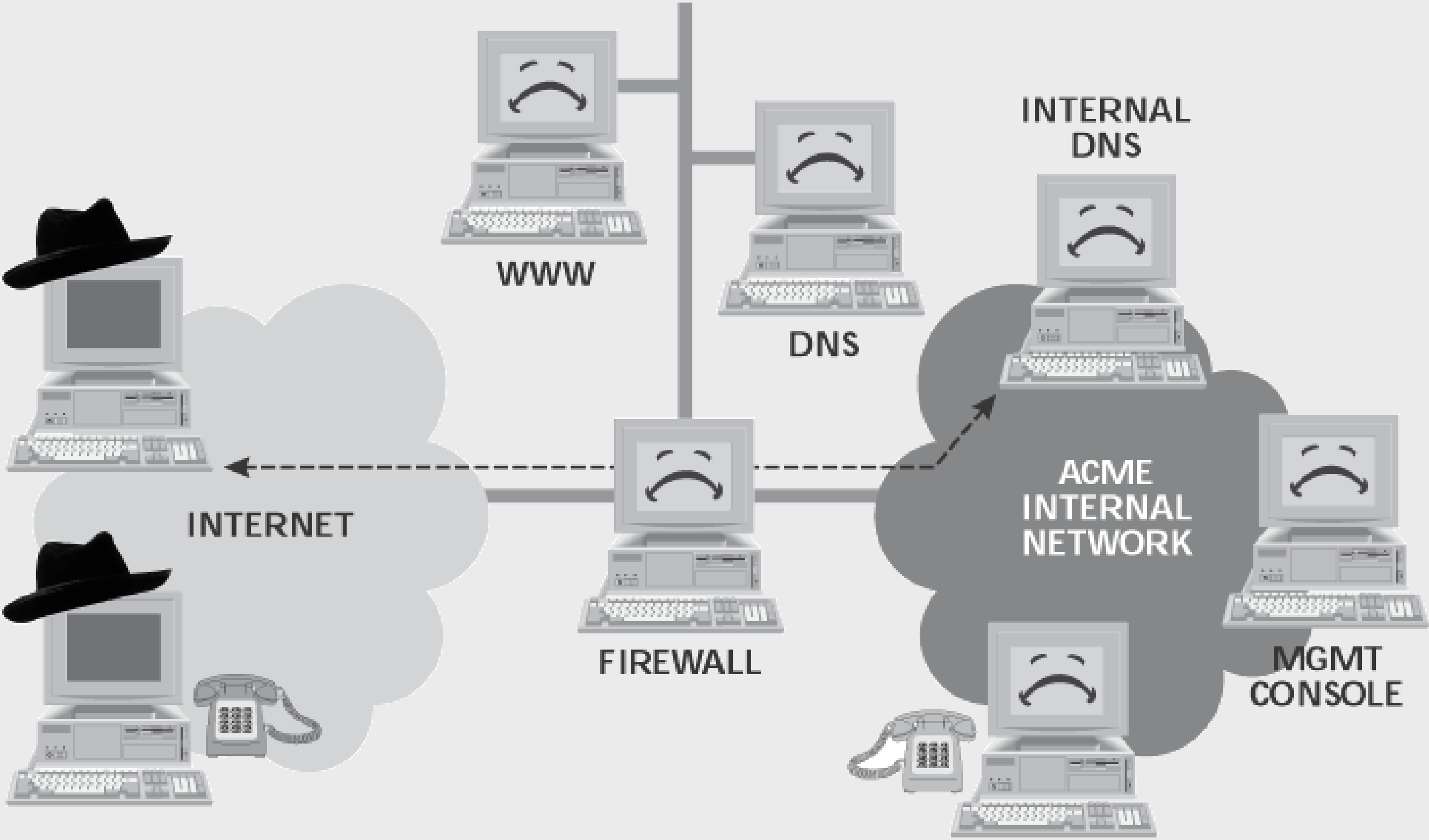


Figure 12.11 Game over!

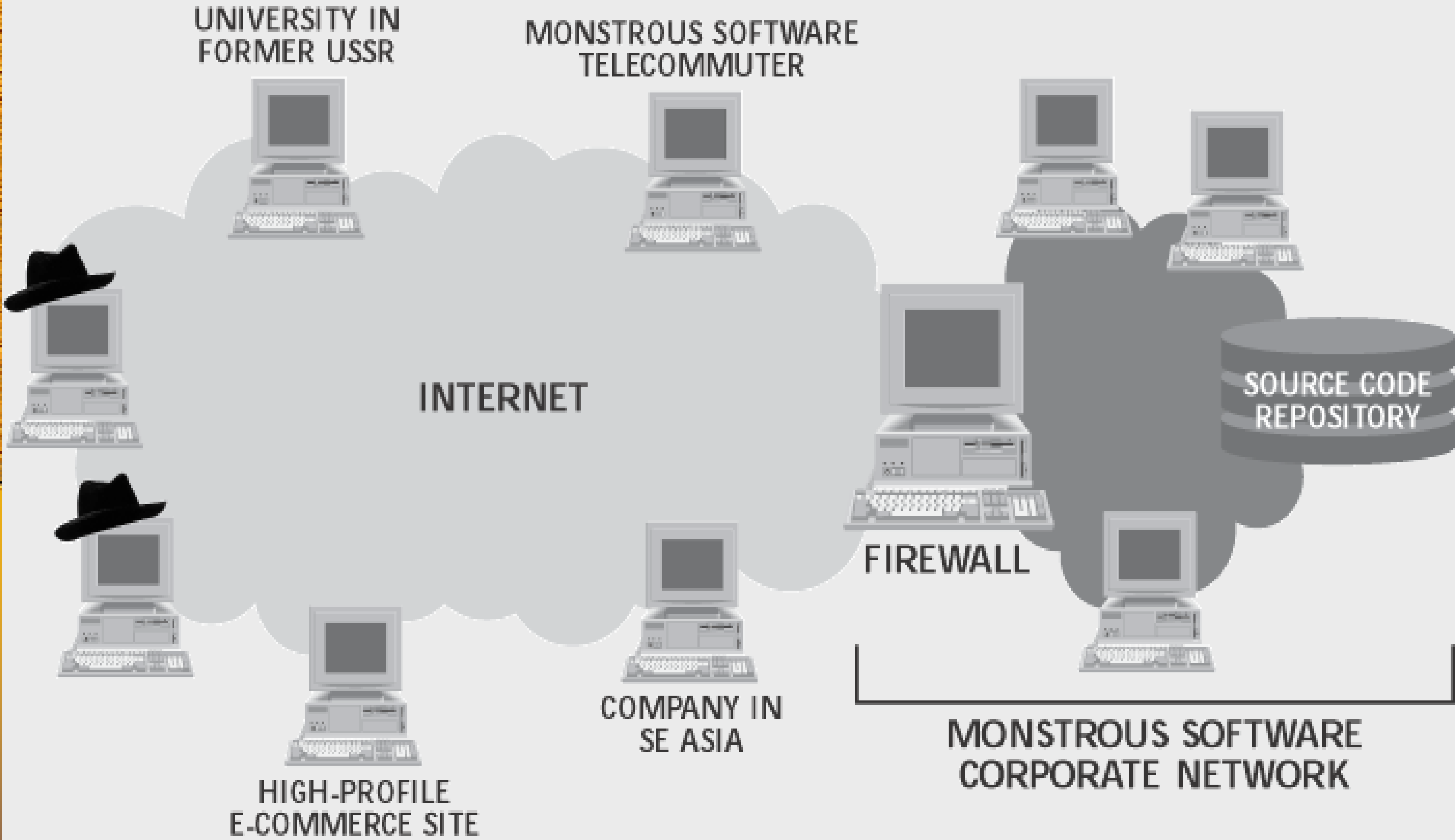

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
HIGH-PROFILE E-COMMERCE SITE
COMPANY IN SE ASIA
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.12 An attack against Monstrous Software to obtain Foobar source code

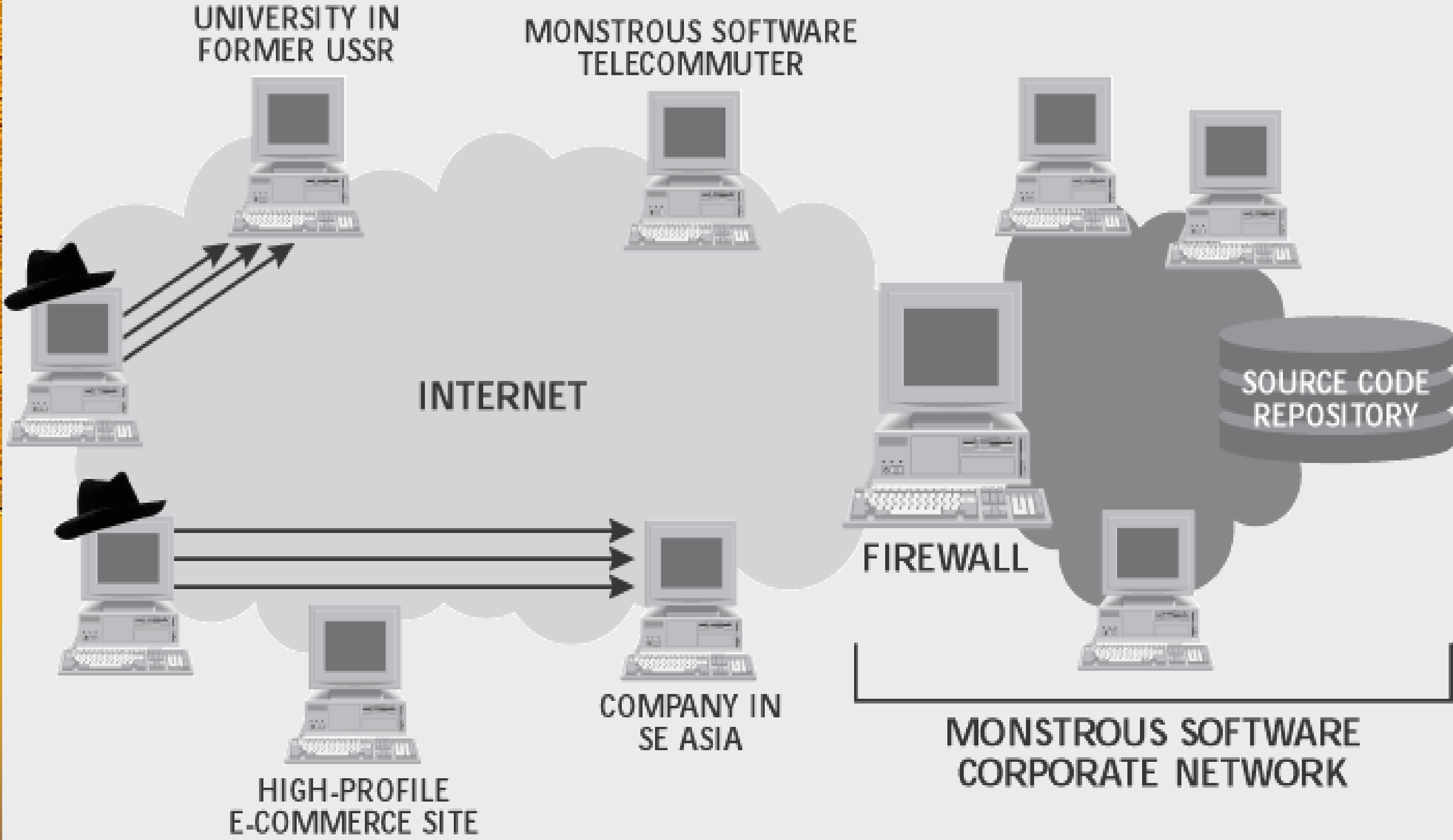
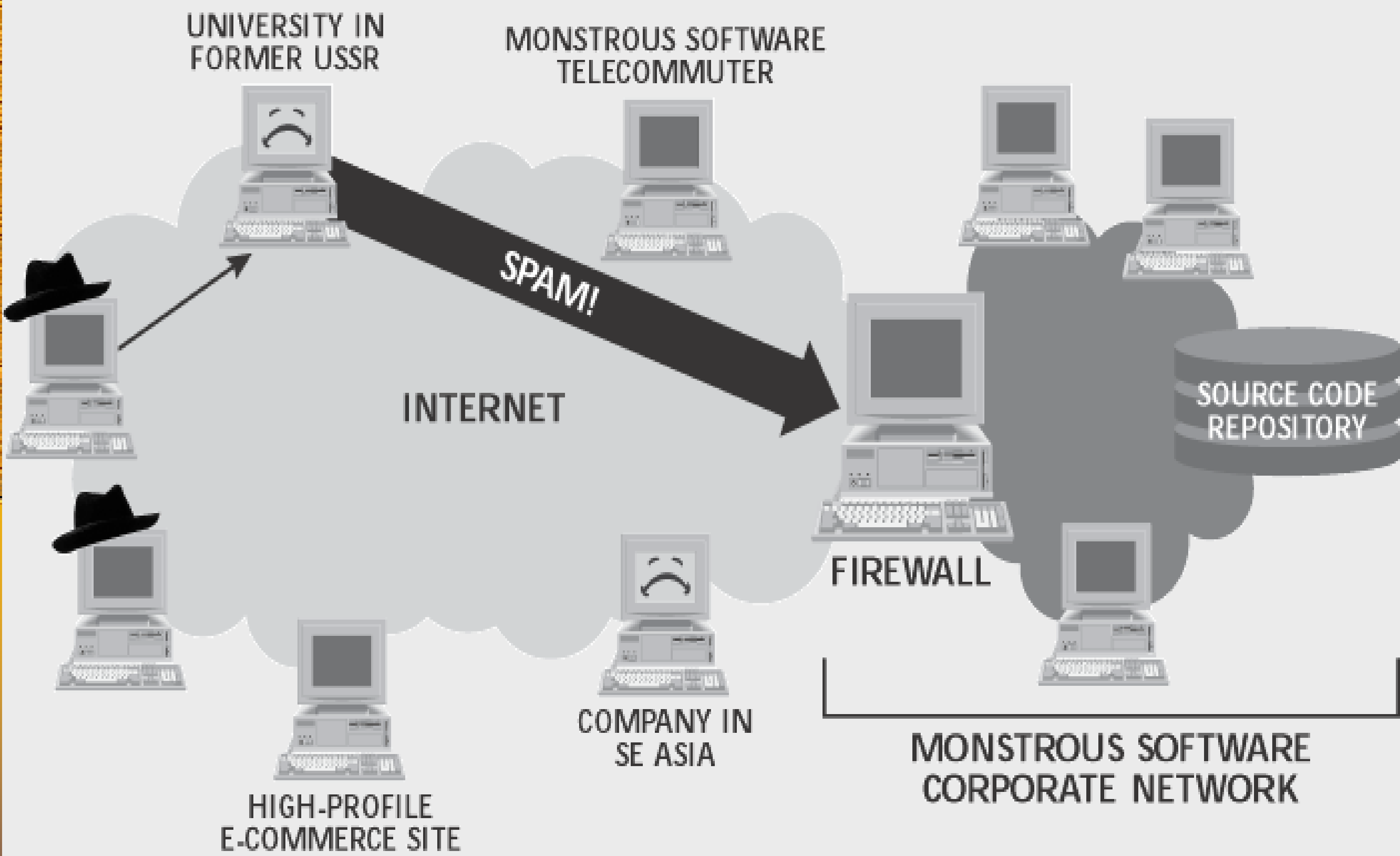

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
COMPANY IN SE ASIA
HIGH-PROFILE E-COMMERCE SITE
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.13 Nessus Scanning for some weak jump-off points around the world



UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
SPAM!
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
HIGH-PROFILE E-COMMERCE SITE
COMPANY IN SE ASIA
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.14 Sending email spam with an enticing offer (game with trojan horse backdoor program created via wrapper)

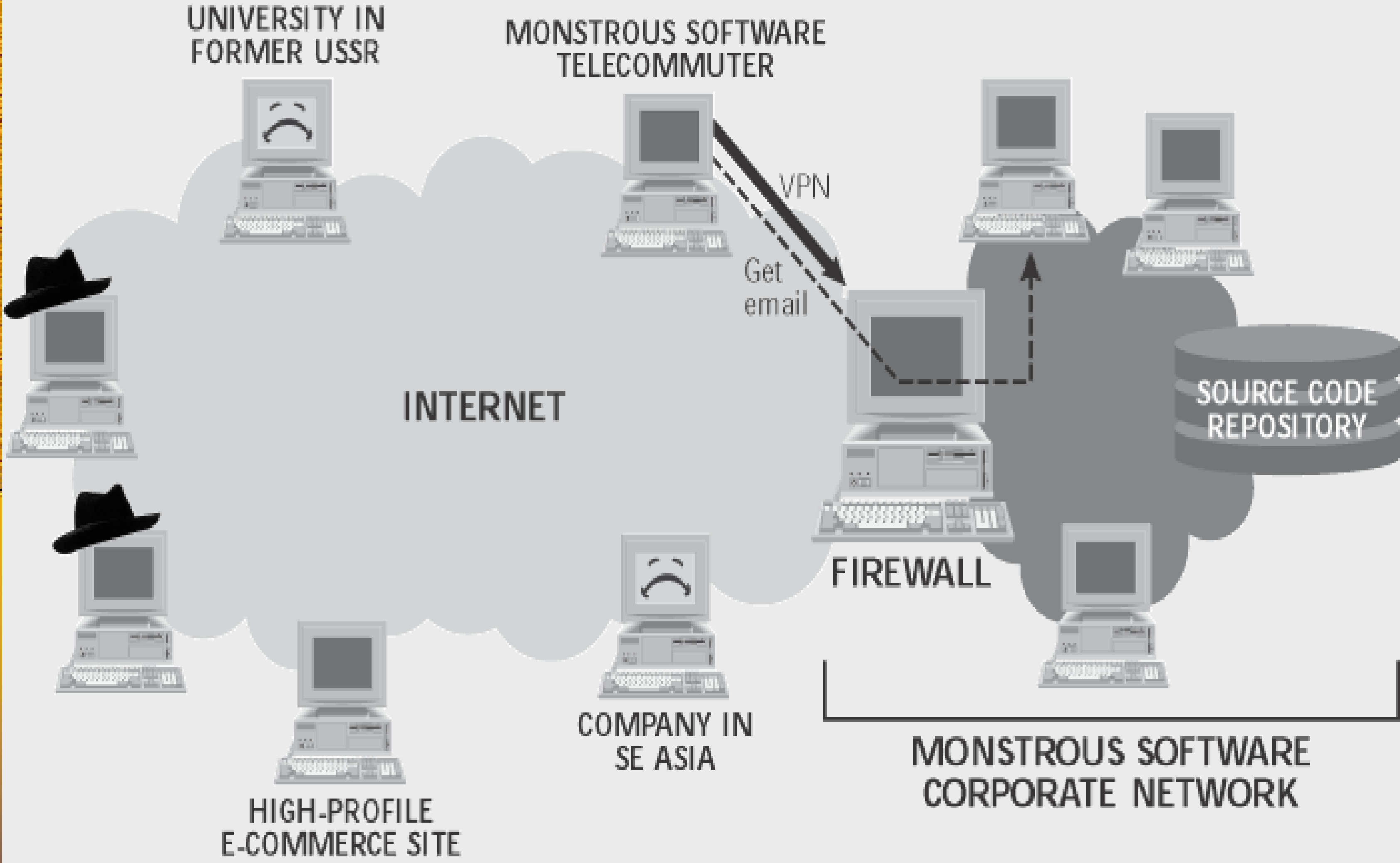

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
VPN
Get email
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
COMPANY IN SE ASIA
HIGH-PROFILE E-COMMERCE SITE
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.15 Telecommuter downloads her email

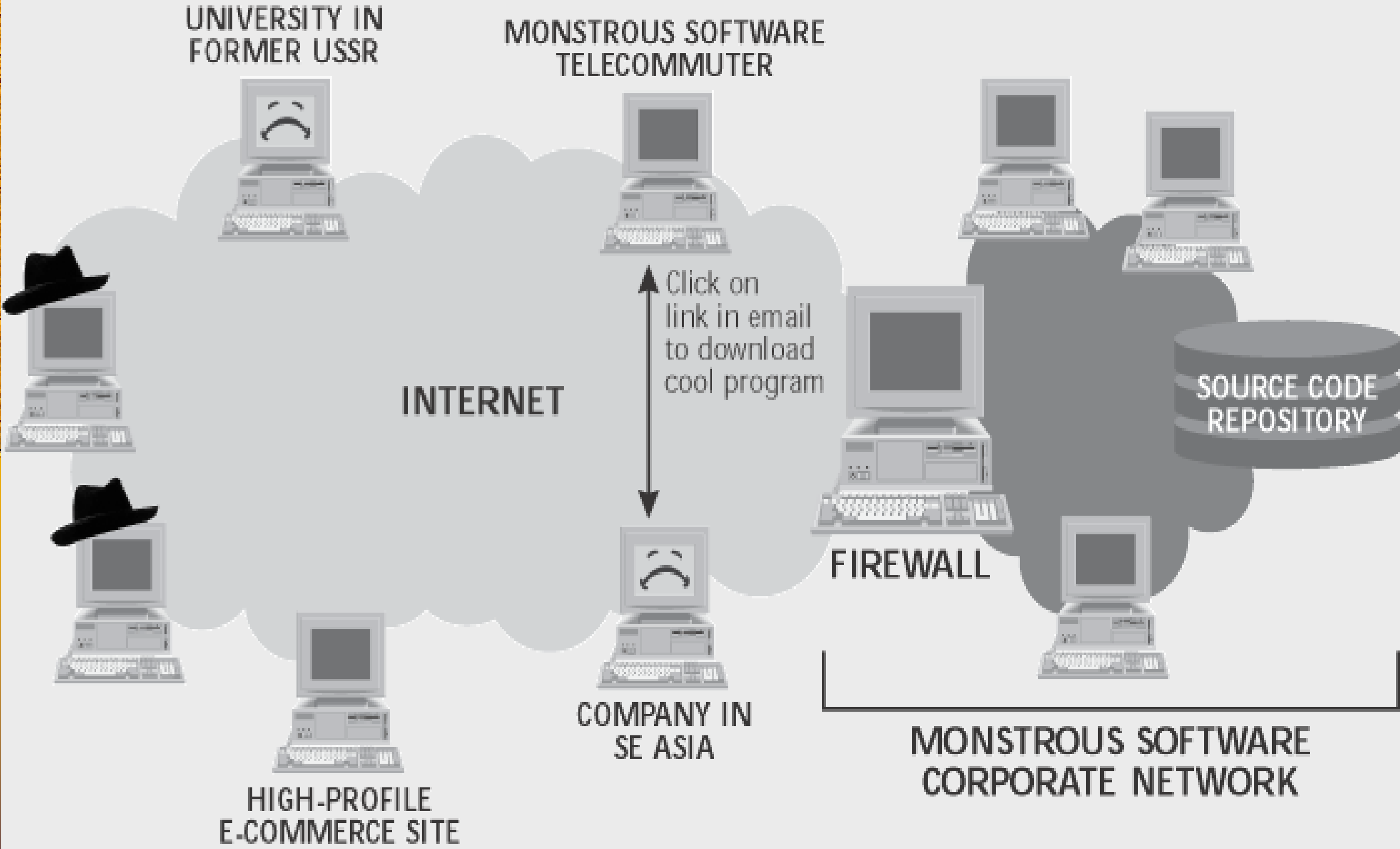

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
INTERNET
Click on link in email to download cool program
FIREWALL
SOURCE CODE REPOSITORY
HIGH-PROFILE E-COMMERCE SITE
COMPANY IN SE ASIA
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.16 Telecommuter takes the bait

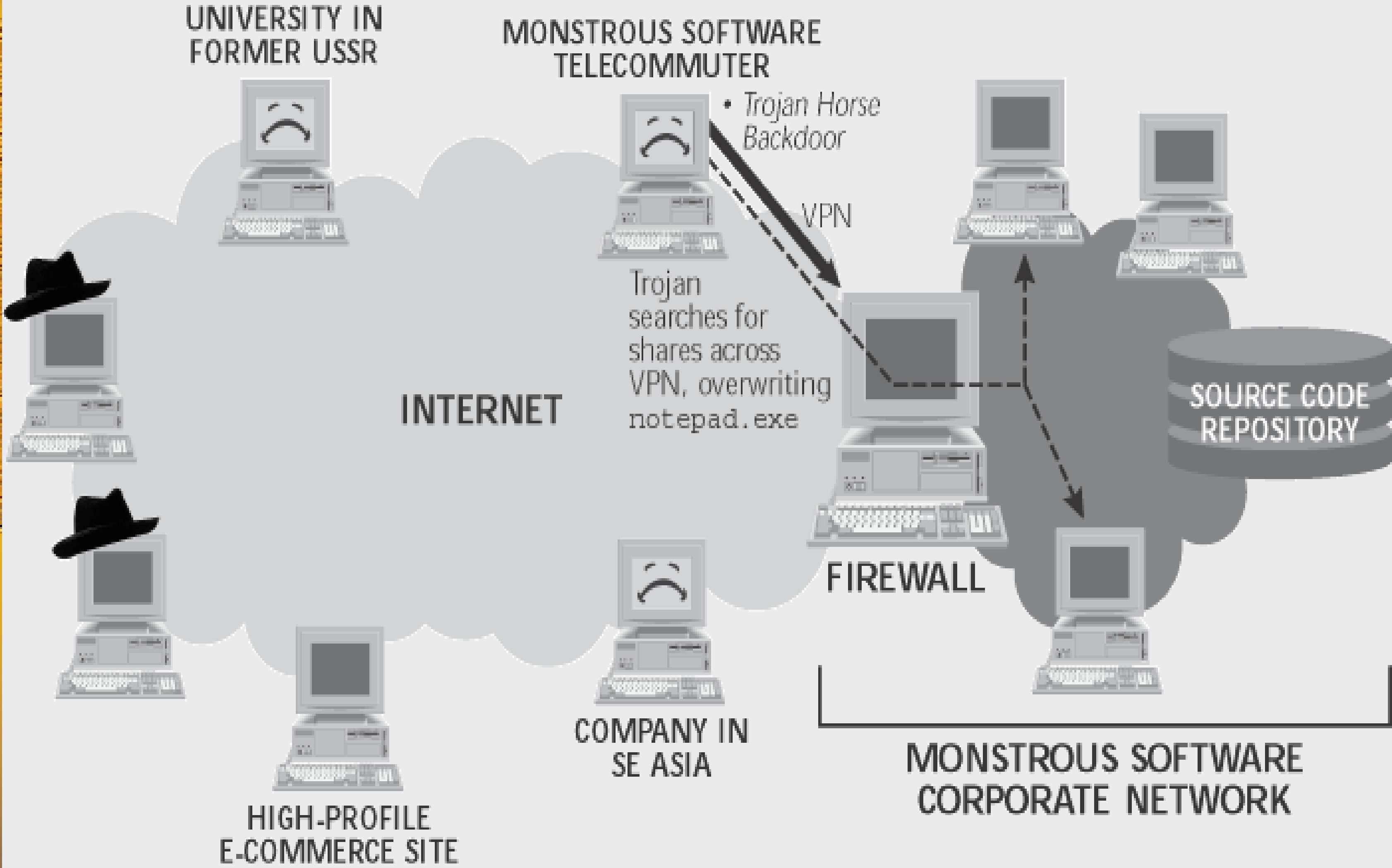

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
• Trojan Horse Backdoor
VPN
Trojan searches for shares across VPN, overwriting notepad.exe
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
COMPANY IN SE ASIA
HIGH-PROFILE E-COMMERCE SITE
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.17 When the telecommuter uses the VPN again, the Trojan horse backdoor searches for mountable shares on the Monstrous corporate network

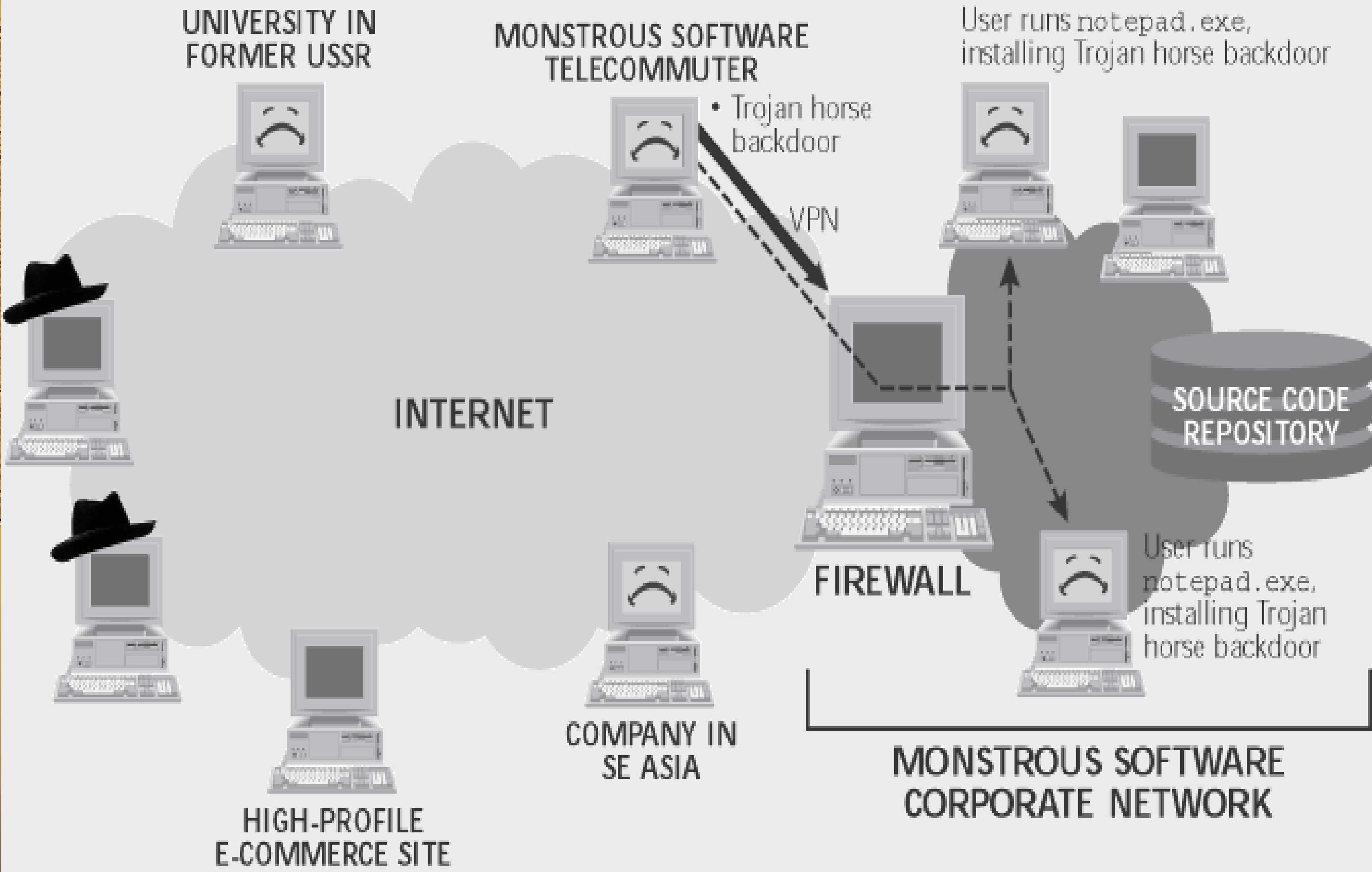

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
• Trojan horse backdoor
VPN
User runs notepad.exe, installing Trojan horse backdoor
INTERNET
FIREWALL
SOURCE CODE REPOSITORY
User runs notepad.exe, installing Trojan horse backdoor
COMPANY IN SE ASIA
HIGH-PROFILE E-COMMERCE SITE
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.18 When users on the corporate network run notepad.exe, the Trojan horse is installed

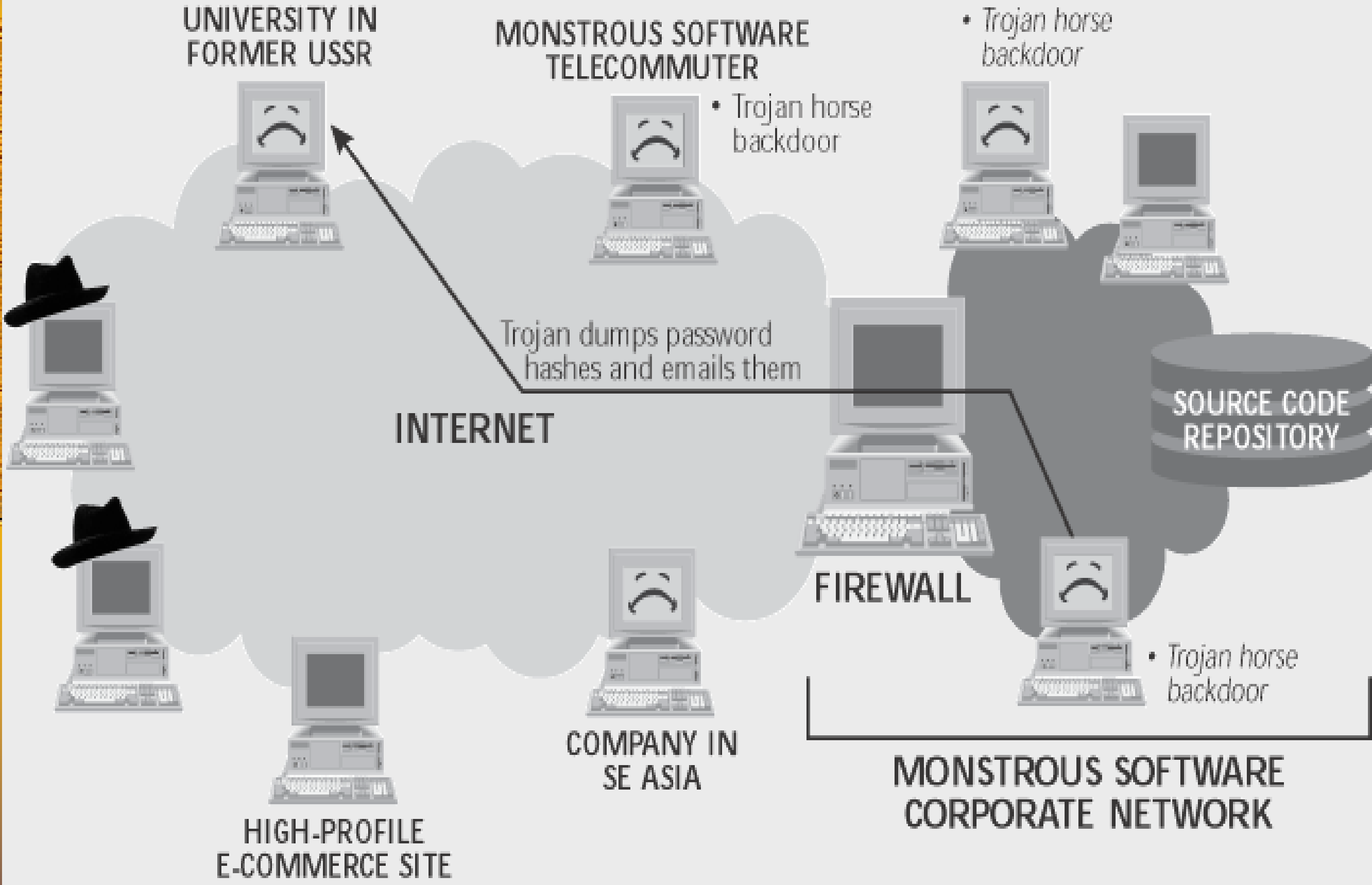

UNIVERSITY IN FORMER USSR
MONSTROUS SOFTWARE TELECOMMUTER
• Trojan horse backdoor
• Trojan horse backdoor
Trojan dumps password hashes and emails them
INTERNET
SOURCE CODE REPOSITORY
FIREWALL
• Trojan horse backdoor
COMPANY IN SE ASIA
HIGH-PROFILE E-COMMERCE SITE
MONSTROUS SOFTWARE CORPORATE NETWORK

Figure 12.19 The Trojan horse dumps password hashes and emails them across the Internet

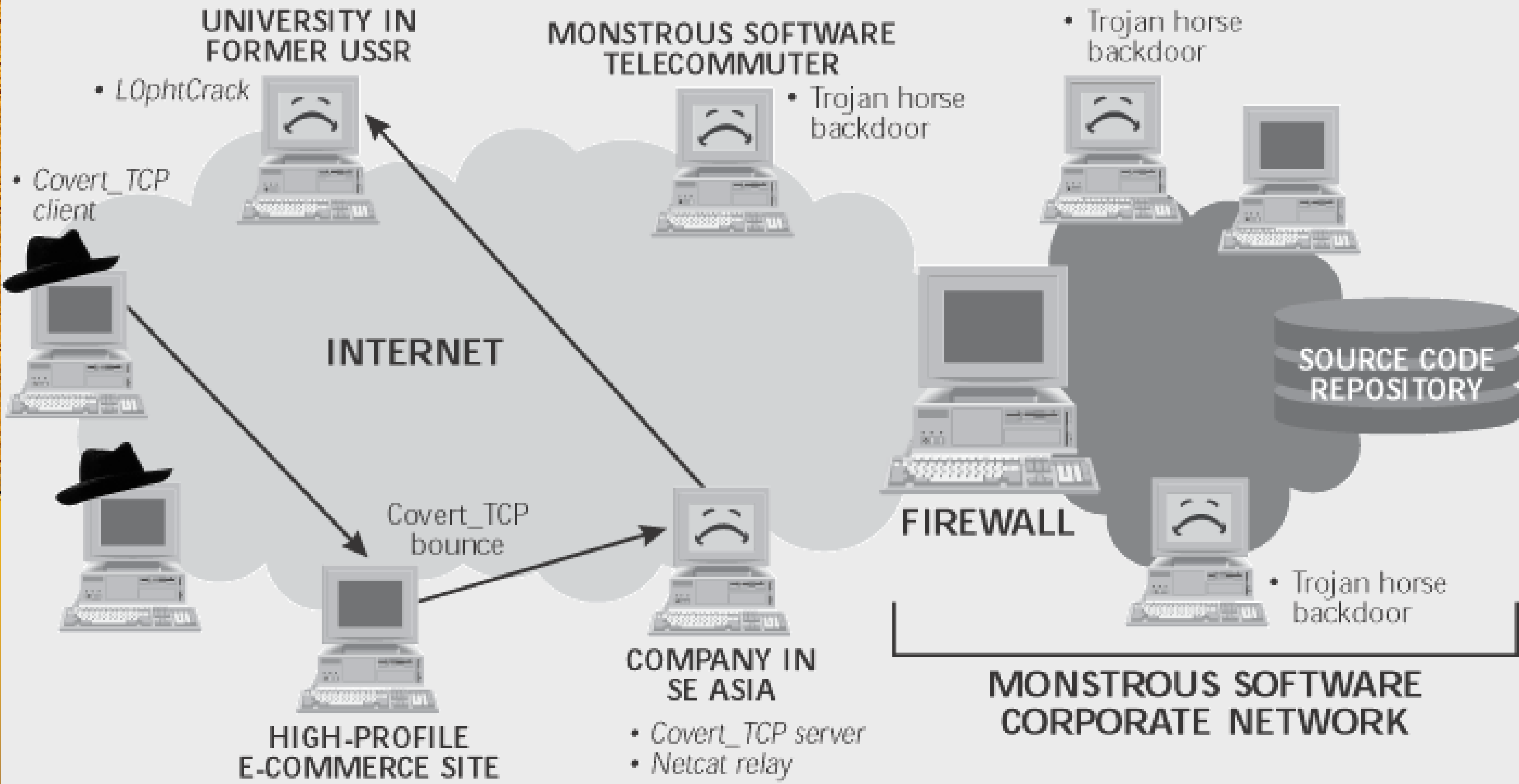


Figure 12.20 The attackers crack the passwords through three levels of indirection

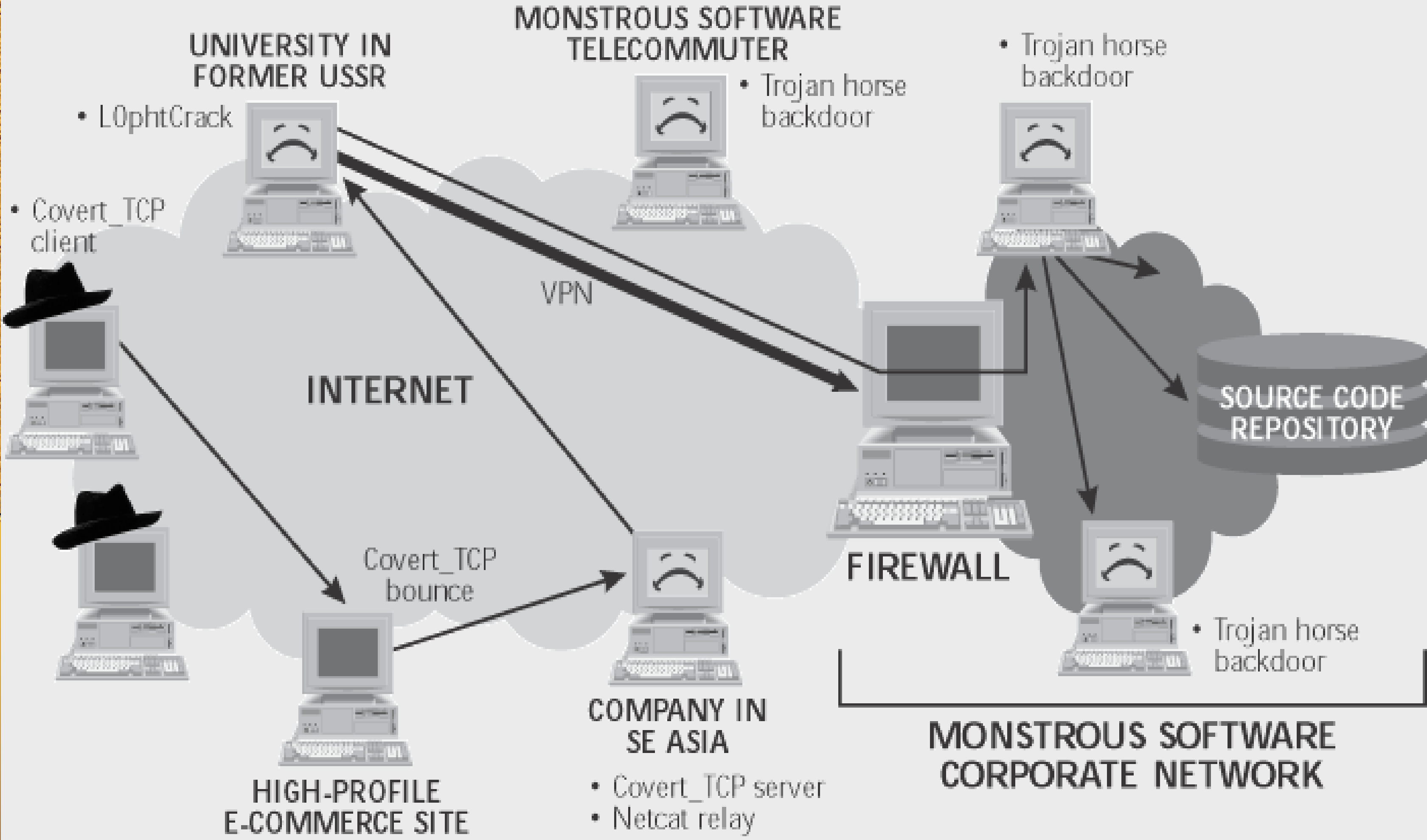


Figure 12.21 The attackers set up a VPN connection using the stolen passwords, and remotely control the Trojan horse on the internal network

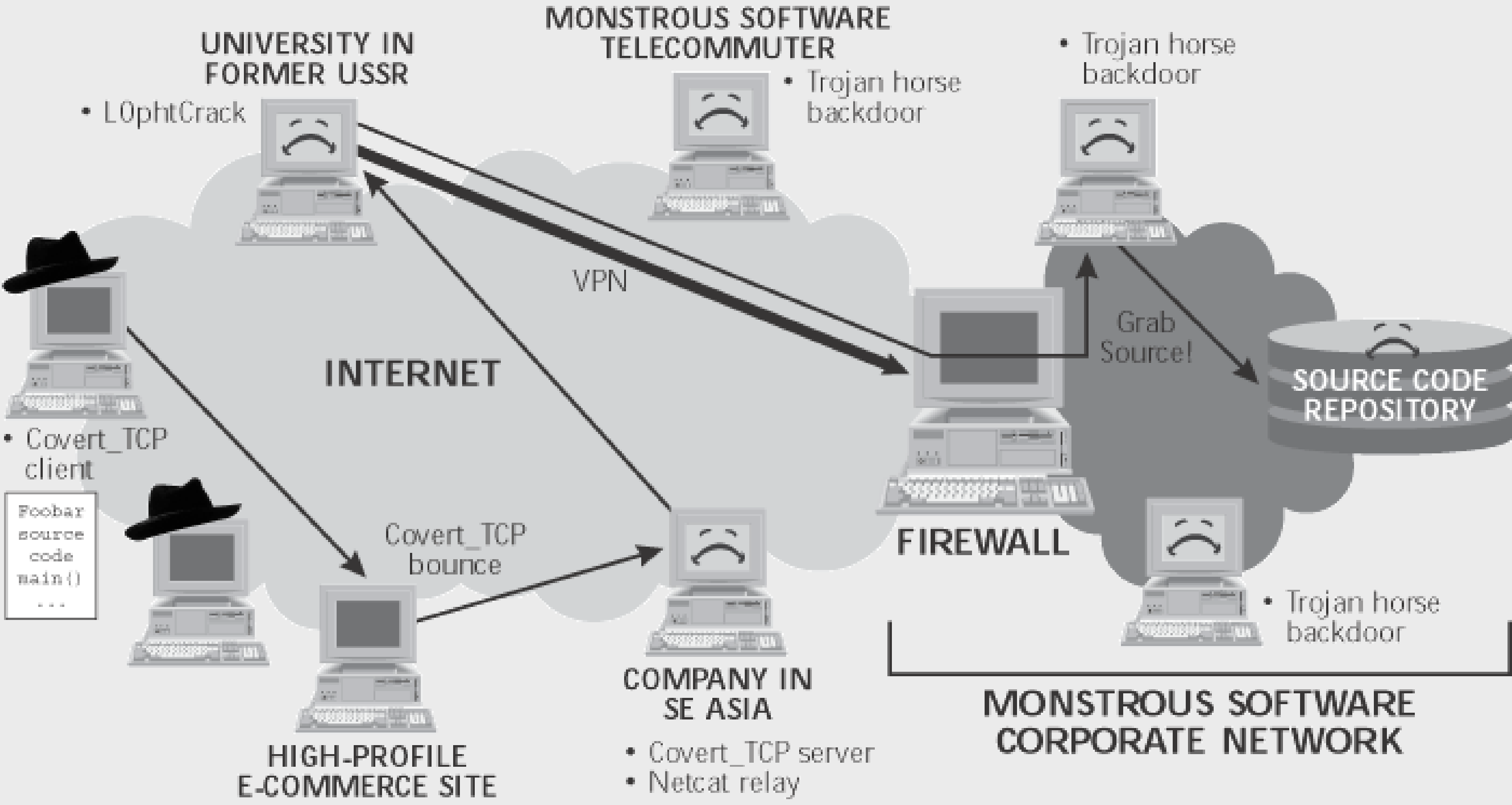


Figure 12.22 Bonnie and Clyde get the Foobar source code