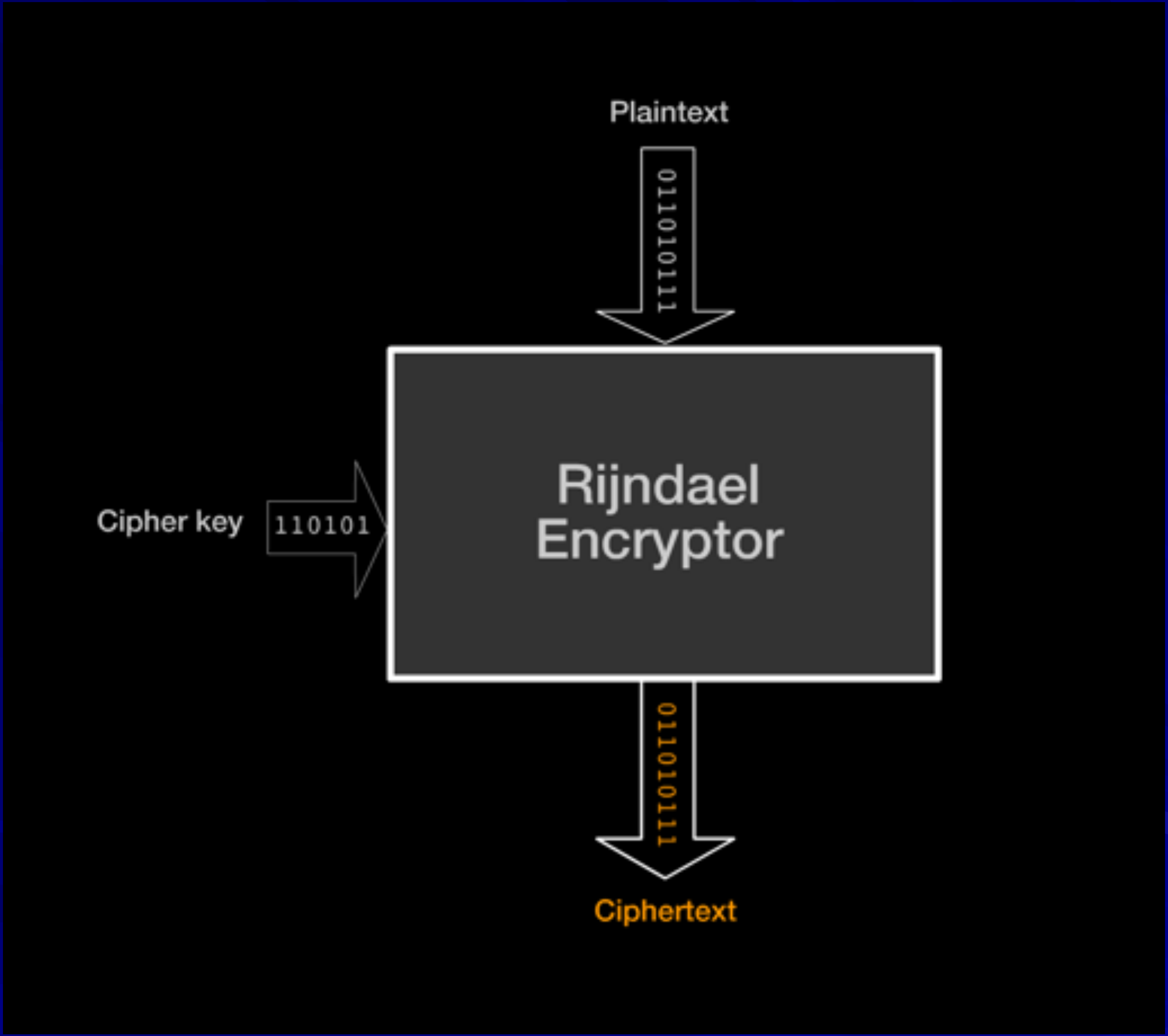
THOMSON

COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense 2nd Edition 57

Chapter 13
Protecting Networks with Security Devices

Last modified 11-10-16


Plaintext
01101010111
Cipher key
110101
Rijndael Encryptor
01101010111
Ciphertext

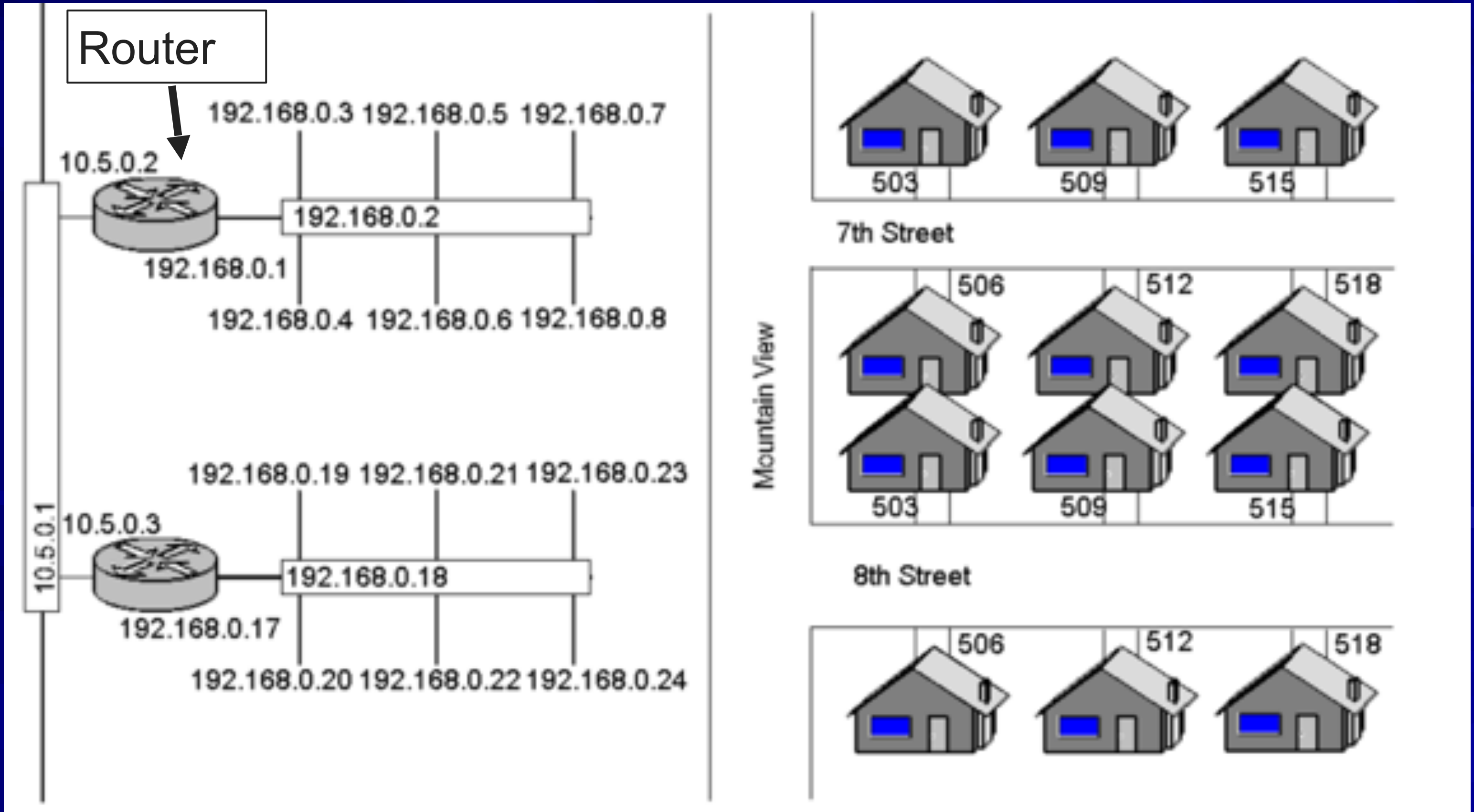
Objectives

- Explain how routers are used to protect networks
- Describe firewall technology
- Describe intrusion detection systems
- Describe honeypots

Understanding Routers

Routers

- Routers are like intersections; switches are like streets
  - Image from Wikipedia (link Ch 13a)



Understanding Routers

- Routers are hardware devices used on a network to send packets to different network segments
  - Operate at the network layer of the OSI model

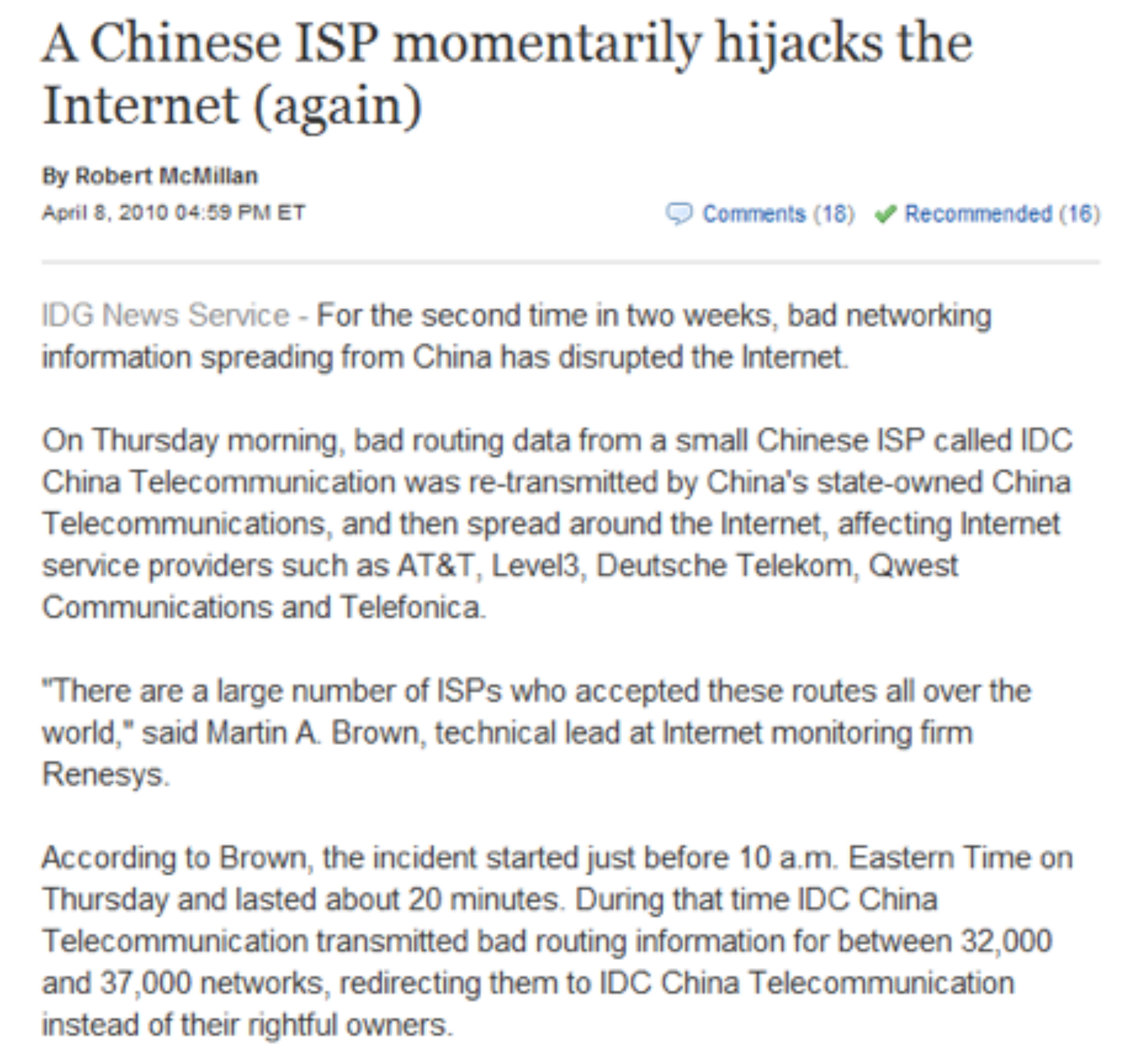
Routing Protocols

- Routers tell one another what paths are available with Routing Protocols
  - Link-state routing protocol
    - Each router has complete information about every network link
    - Example: Open Shortest Path First (OSPF)
  - Distance-vector routing protocol
    - Routers only know which direction to send packets, and how far
    - Example: Routing Information Protocol (RIP)

Routing Protocols

- Path-vector routing protocol
    - Used on the Internet Backbone
    - Example: Border Gateway Patrol (BGP)

China’s BGP Hijacking



A Chinese ISP momentarily hijacks the Internet (again)

By Robert McMillan

April 8, 2010 04:59 PM ET

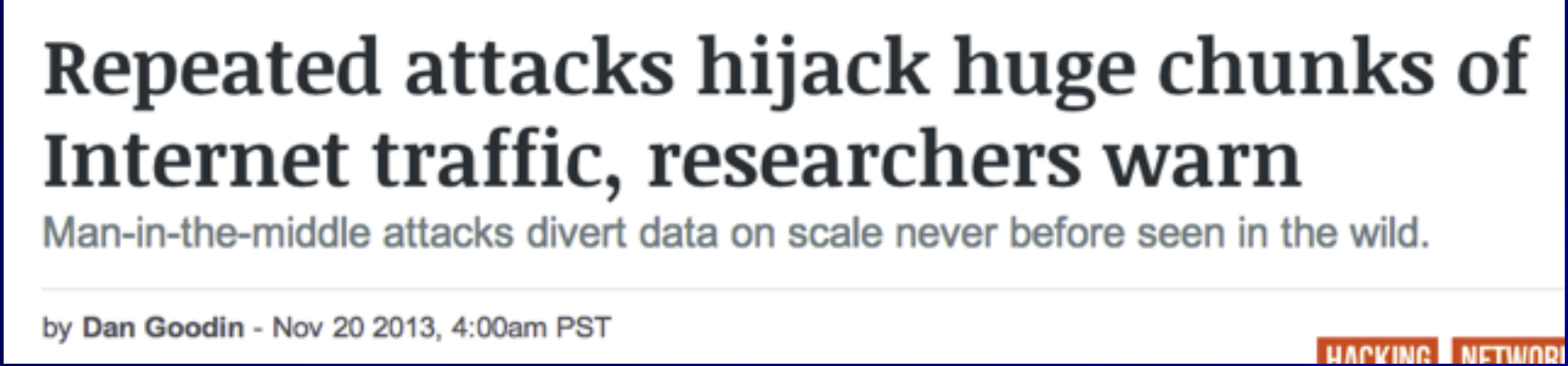
IDG News Service - For the second time in two weeks, bad networking information spreading from China has disrupted the Internet.

On Thursday morning, bad routing data from a small Chinese ISP called IDC China Telecommunication was re-transmitted by China's state-owned China Telecommunications, and then spread around the Internet, affecting Internet service providers such as AT&T, Level3, Deutsche Telekom, Qwest Communications and Telefonica.

"There are a large number of ISPs who accepted these routes all over the world," said Martin A. Brown, technical lead at Internet monitoring firm Renesys.

According to Brown, the incident started just before 10 a.m. Eastern Time on Thursday and lasted about 20 minutes. During that time IDC China Telecommunication transmitted bad routing information for between 32,000 and 37,000 networks, redirecting them to IDC China Telecommunication instead of their rightful owners.

- Link Ch 13v

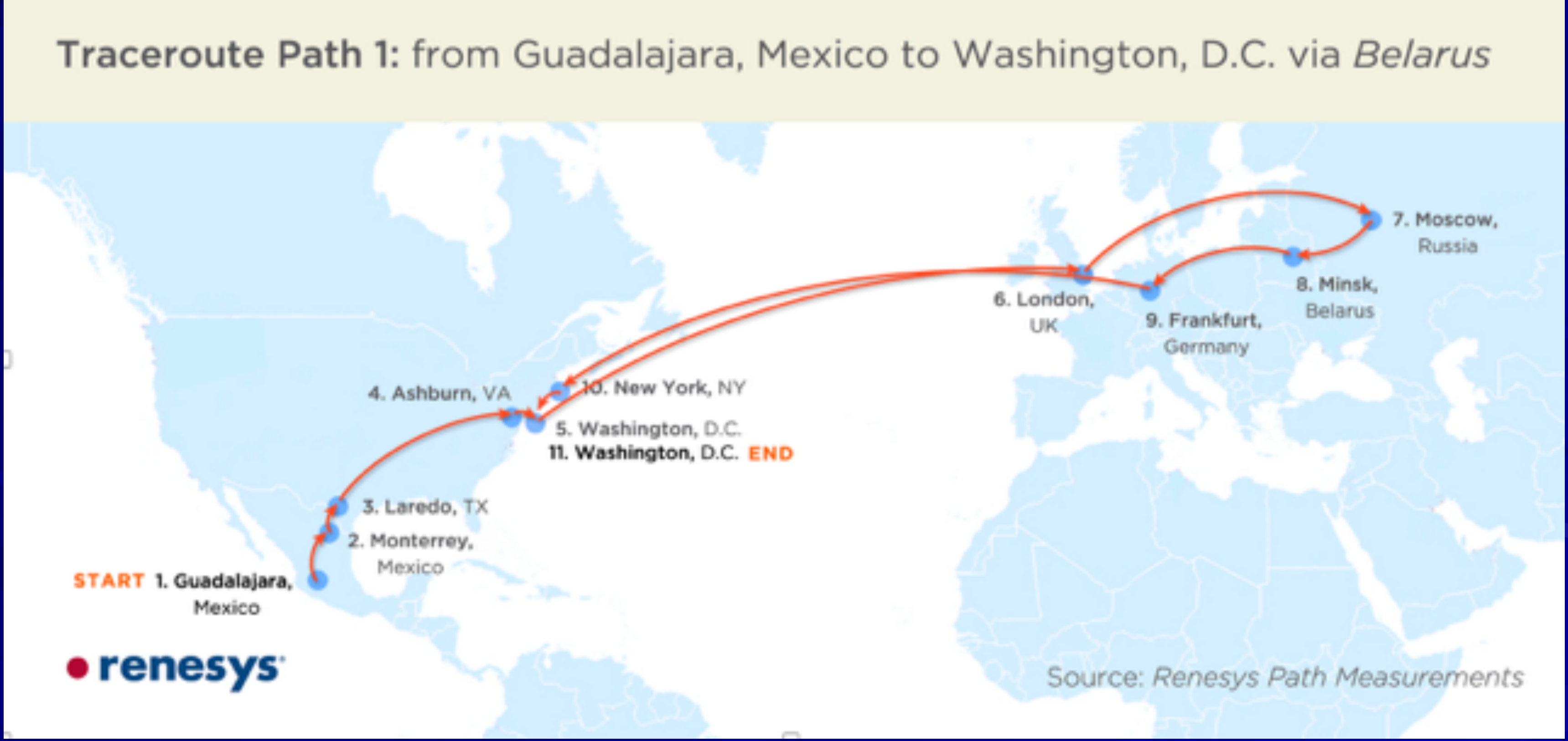


Repeated attacks hijack huge chunks of Internet traffic, researchers warn

Man-in-the-middle attacks divert data on scale never before seen in the wild.

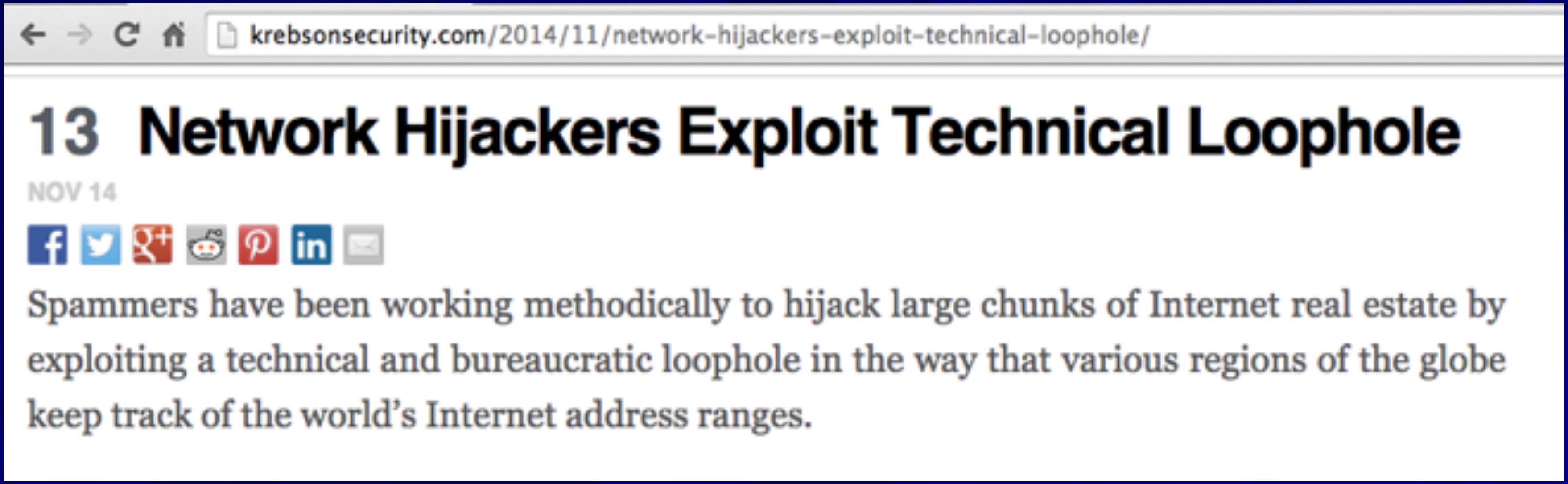
by **Dan Goodin** - Nov 20 2013, 4:00am PST

HACKING NETWOR



Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*

Source: *Renesys Path Measurements*

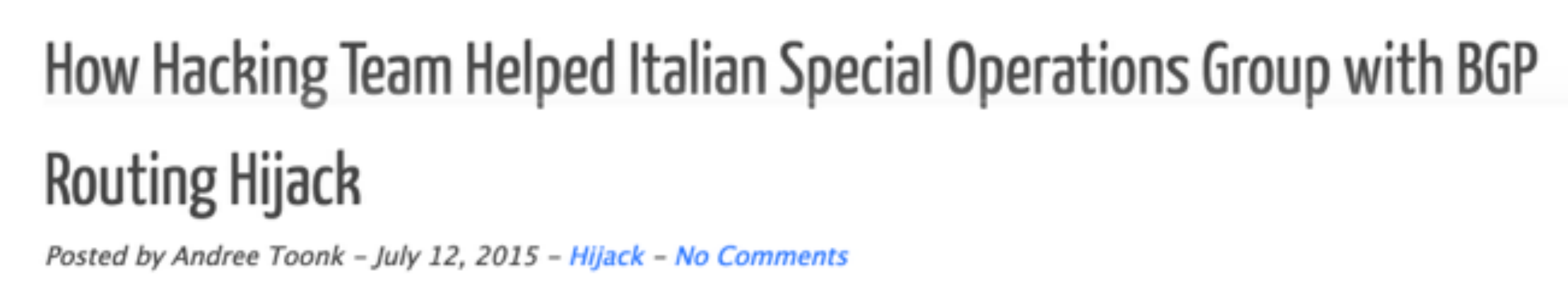

krebsonsecurity.com/2014/11/network-hijackers-exploit-technical-loophole/

13 NOV 14

Network Hijackers Exploit Technical Loophole

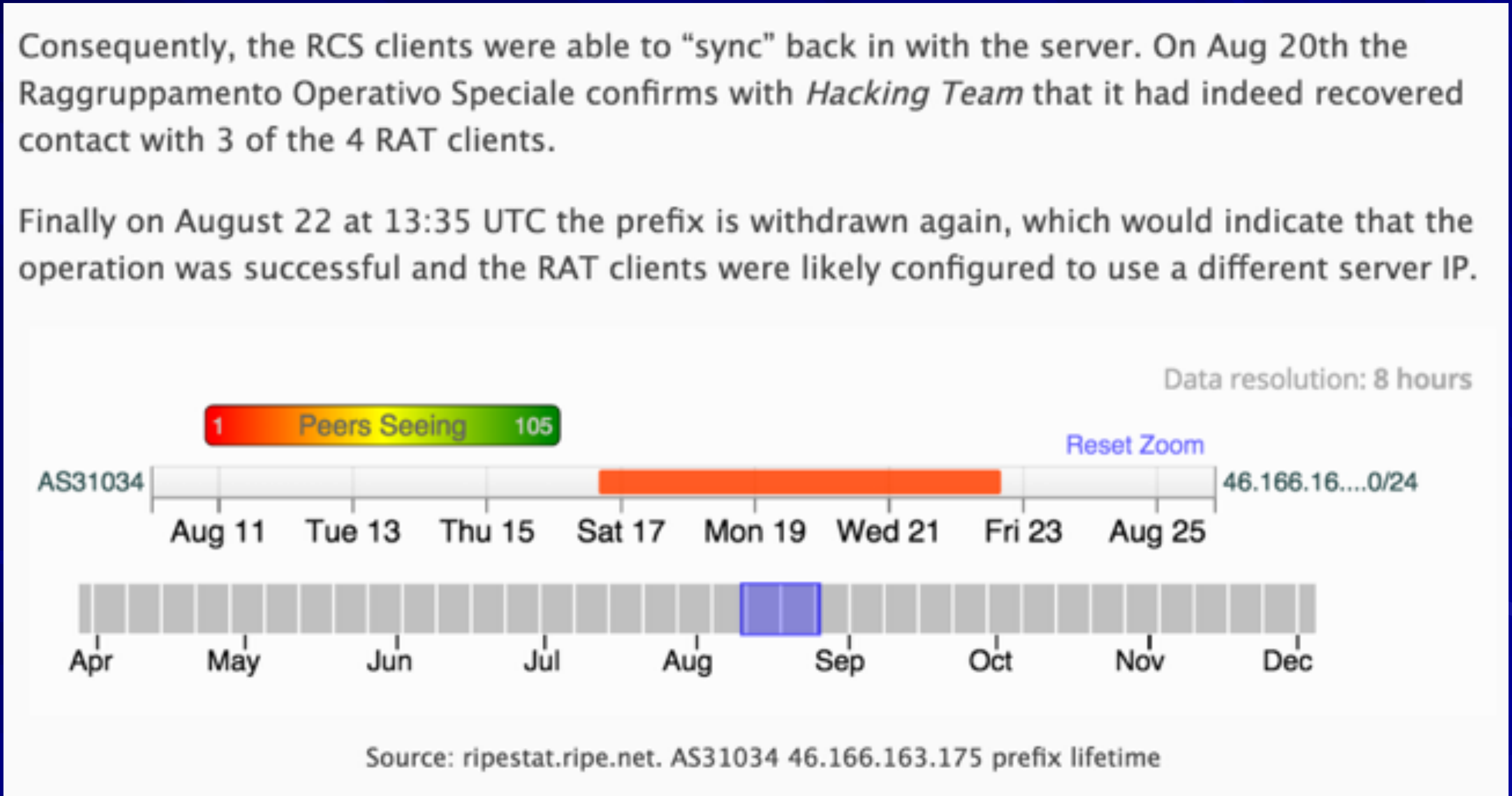
Spammers have been working methodically to hijack large chunks of Internet real estate by exploiting a technical and bureaucratic loophole in the way that various regions of the globe keep track of the world's Internet address ranges.

- IP hijacking via BGP
  - Simply advertise routes to IP addresses assigned to other companies, but unused
  - Like pirate radio
  - Link Ch 13z4; next slide Ch 13z5



How Hacking Team Helped Italian Special Operations Group with BGP Routing Hijack

Posted by Andree Toonk – July 12, 2015 – Hijack – No Comments

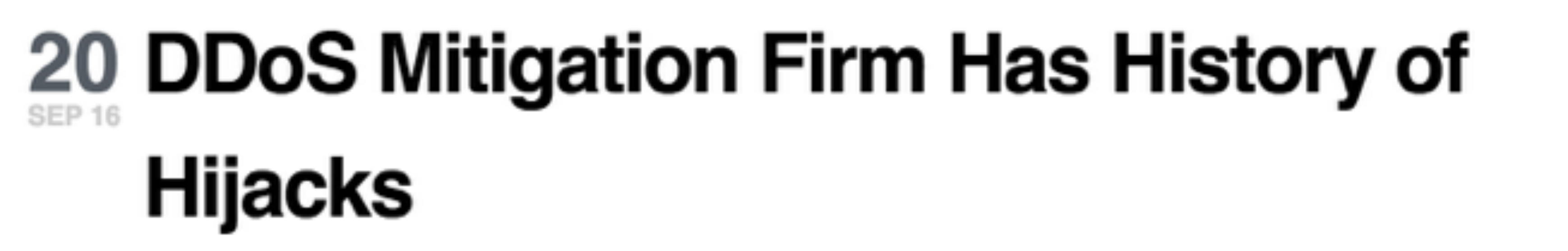


Consequently, the RCS clients were able to "sync" back in with the server. On Aug 20th the Raggruppamento Operativo Speciale confirms with *Hacking Team* that it had indeed recovered contact with 3 of the 4 RAT clients.

Finally on August 22 at 13:35 UTC the prefix is withdrawn again, which would indicate that the operation was successful and the RAT clients were likely configured to use a different server IP.

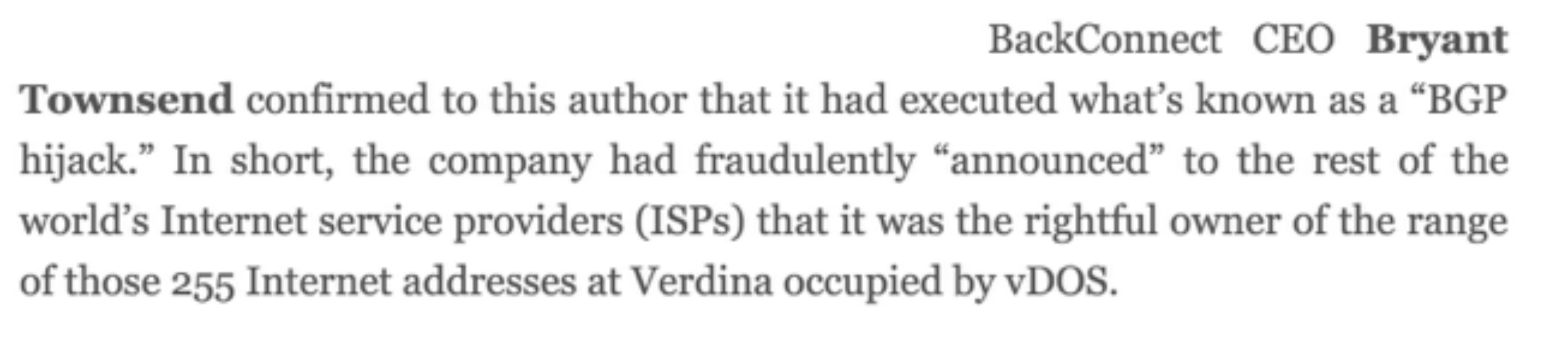
Source: ripestat.ripe.net. AS31034 46.166.163.175 prefix lifetime

- Great investigative reporting
- Follow him on Twitter
  - @briankrebs

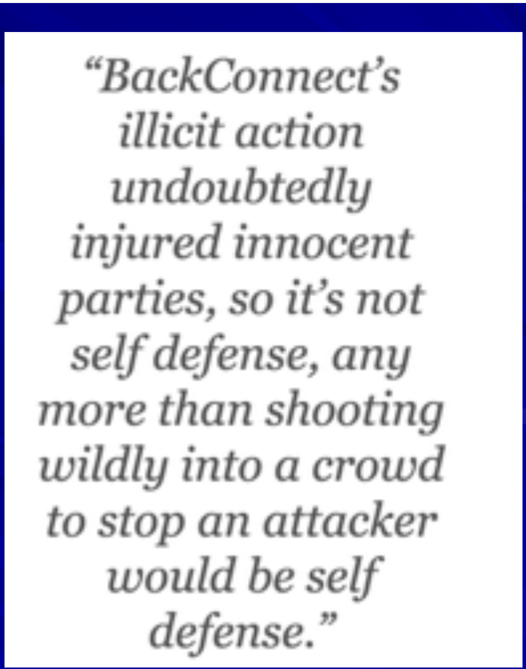


20
SEP 16

DDoS Mitigation Firm Has History of Hijacks

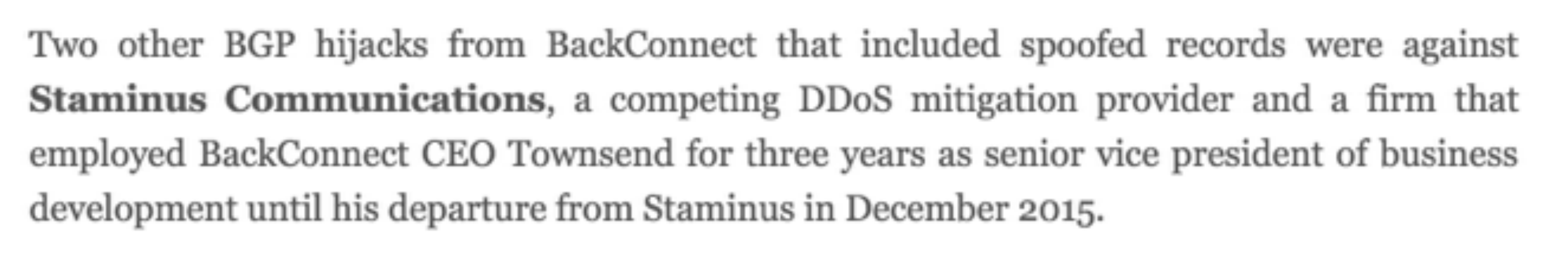


BackConnect CEO **Bryant Townsend** confirmed to this author that it had executed what's known as a "BGP hijack." In short, the company had fraudulently "announced" to the rest of the world's Internet service providers (ISPs) that it was the rightful owner of the range of those 255 Internet addresses at Verdina occupied by vDOS.

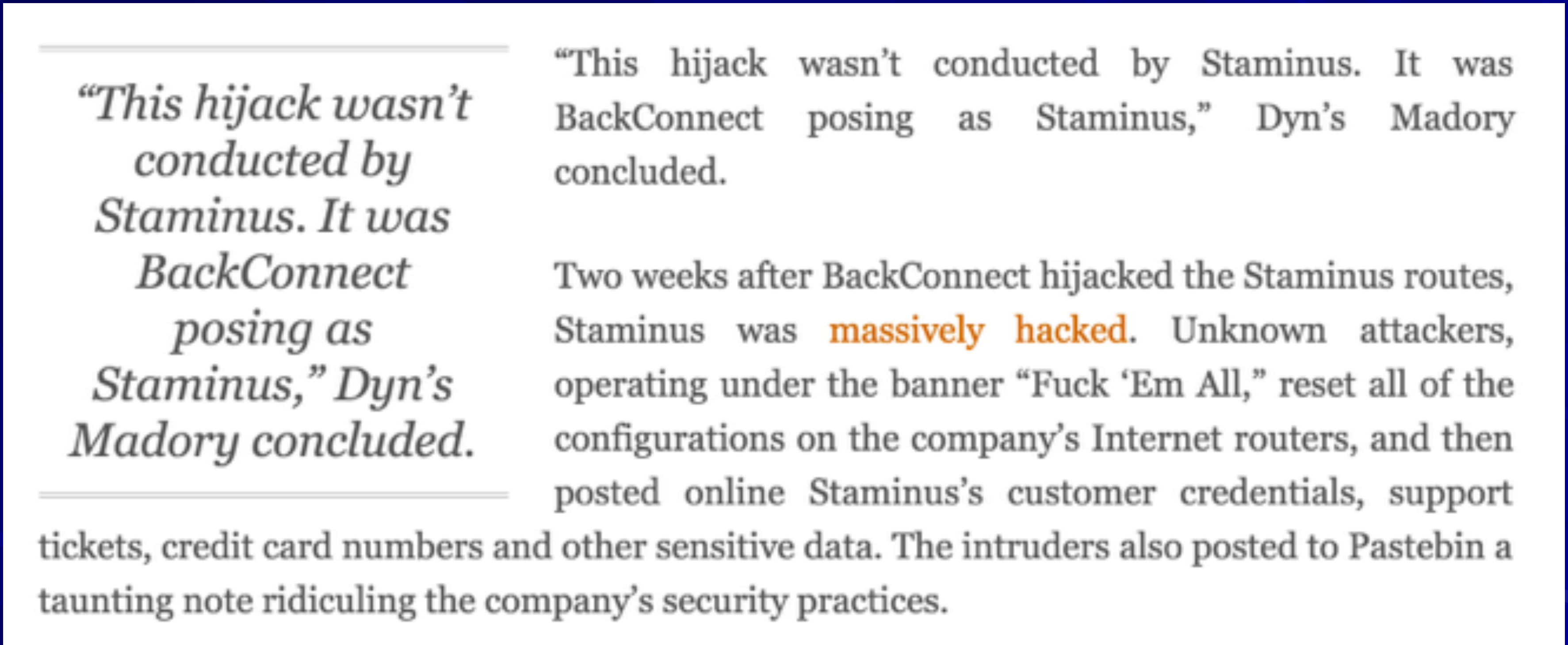


"BackConnect's illicit action undoubtedly injured innocent parties, so it's not self defense, any more than shooting wildly into a crowd to stop an attacker would be self defense."

Link Ch 13z6



Two other BGP hijacks from BackConnect that included spoofed records were against **Staminus Communications**, a competing DDoS mitigation provider and a firm that employed BackConnect CEO Townsend for three years as senior vice president of business development until his departure from Staminus in December 2015.



> *“This hijack wasn’t conducted by Staminus. It was BackConnect posing as Staminus,” Dyn’s Madory concluded.*

“This hijack wasn’t conducted by Staminus. It was BackConnect posing as Staminus,” Dyn’s Madory concluded.

Two weeks after BackConnect hijacked the Staminus routes, Staminus was massively hacked. Unknown attackers, operating under the banner “Fuck ‘Em All,” reset all of the configurations on the company’s Internet routers, and then posted online Staminus’s customer credentials, support tickets, credit card numbers and other sensitive data. The intruders also posted to Pastebin a taunting note ridiculing the company’s security practices.

Cisco Routers

- Image from cisco.com (link Ch 13b)

Understanding Basic Hardware Routers

- Cisco routers are widely used in the networking community
  - More than one million Cisco 2500 series routers are currently being used by companies around the world
- Vulnerabilities exist in Cisco as they do in any operating system
  - See link Ch 13c

Cisco Router Components

- Internetwork Operating System (IOS)
- Random access memory (RAM)
  - Holds the router’s running configuration, routing tables, and buffers
  - If you turn off the router, the contents stored in RAM are wiped out
- Nonvolatile RAM (NVRAM)
  - Holds the router’s configuration file, but the information is not lost if the router is turned off

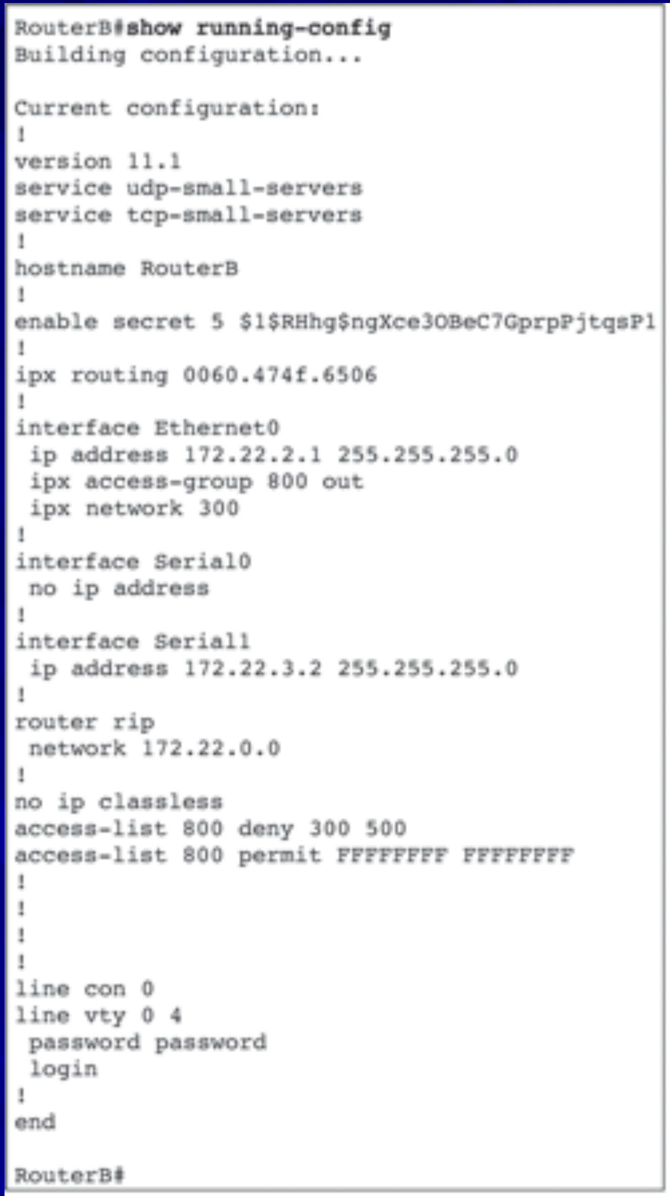
Cisco Router Components

- Flash memory
  - Holds the IOS the router is using
  - Is rewritable memory, so you can upgrade the IOS
- Read-only memory (ROM)
  - Contains a minimal version of the IOS used to boot the router if flash memory gets corrupted

Cisco Router Components

- Interfaces
  - Hardware connectivity points
  - Example: an Ethernet port is an interface that connects to a LAN

- Cisco IOS is controlled from the command line
- The details are not included in this class
- Skip pages 376-378



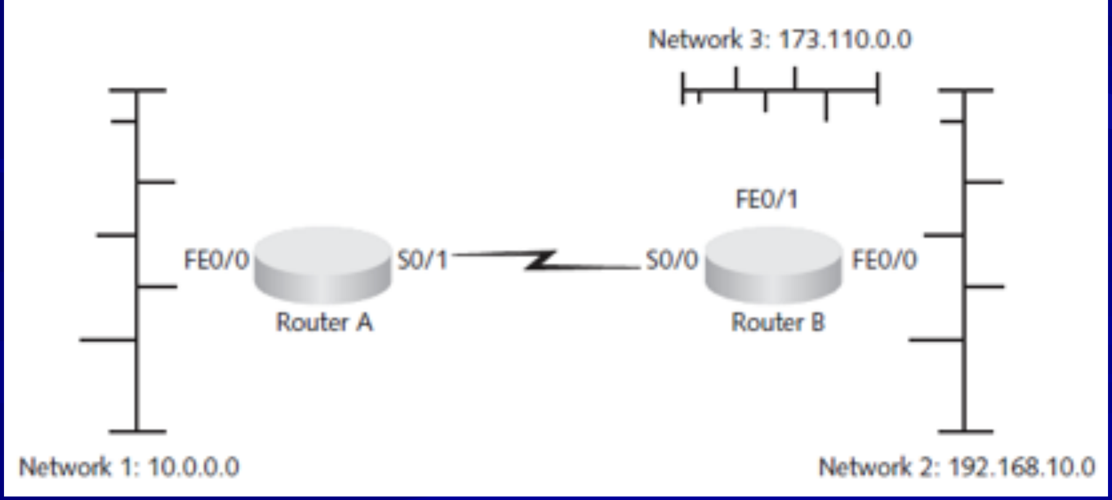
```
RouterB#show running-config
Building configuration...

Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable secret 5 $1$RHhg$ngXce3OBeC7GprpPjtqsP1
!
ipx routing 0060.474f.6506
!
interface Ethernet0
 ip address 172.22.2.1 255.255.255.0
 ipx access-group 800 out
 ipx network 300
!
interface Serial0
 no ip address
!
interface Serial1
 ip address 172.22.3.2 255.255.255.0
!
router rip
 network 172.22.0.0
!
no ip classless
access-list 800 deny 300 500
access-list 800 permit FFFFFFFF FFFFFFFF
!
!
!
!
line con 0
line vty 0 4
 password password
 login
!
end

RouterB#
```

Figure 13-1 Output from the show running-config command

Standard IP Access Lists

- Can restrict IP traffic entering or leaving a router's interface based on source IP address
  - To restrict traffic from Network 3 from entering Network 1, access list looks like:

```
access-list 1 deny 173.110.0.0 0.0.255.255
access-list permit any
```



Extended IP Access Lists

- Restricts IP traffic entering or leaving based on:
  - Source IP address
  - Destination IP address
  - Protocol type
  - Application port number

Michael Lynn

- He presented a major Cisco security vulnerability at the Black Hat security conference in 2005
- He lost his job, was sued, conference materials were confiscated, etc.
  - See links Ch 13 d, e, f, g

Understanding Firewalls

Understanding Firewalls

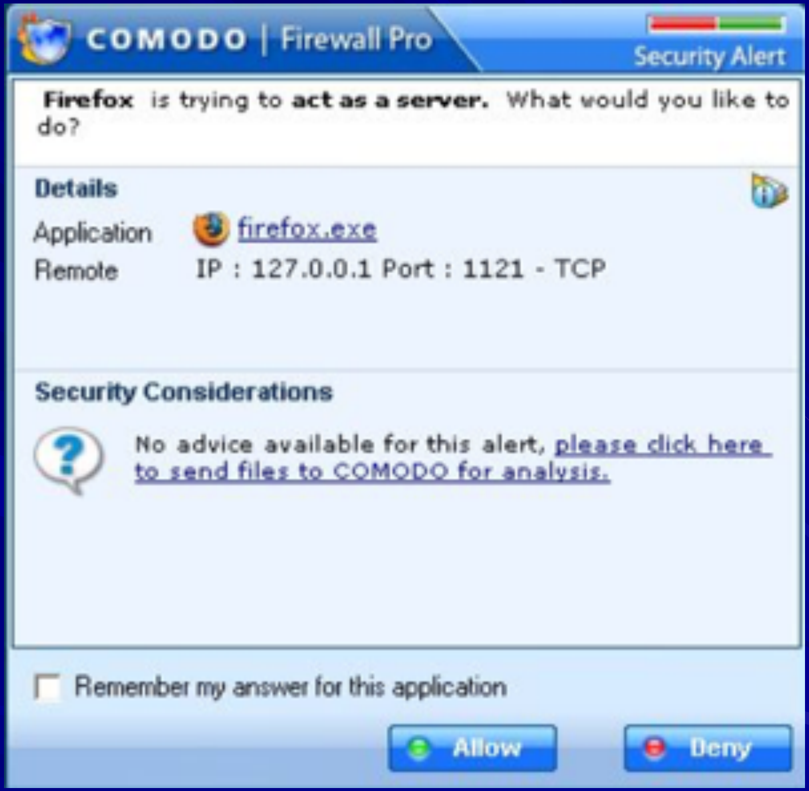
- Firewalls are hardware devices or software installed on a system and have two purposes
  - Controlling access to all traffic that enters an internal network
  - Controlling all traffic that leaves an internal network

Hardware Firewalls

- Advantage of hardware firewalls
  - Faster than software firewalls (more throughput)
- Disadvantages of hardware firewalls
  - You are limited by the firewall’s hardware
    - Number of interfaces, etc.
  - Usually filter incoming traffic only (link Ch 13i)

Software Firewalls

- Advantages of software firewalls
  - Customizable: can interact with the user to provide more protection
  - You can easily add NICs to the server running the firewall software



Firefox is trying to act as a server. What would you like to do?

Details

Application firefox.exe

Remote IP : 127.0.0.1 Port : 1121 - TCP

Security Considerations

No advice available for this alert, please click here to send files to COMODO for analysis.

□ Remember my answer for this application

Software Firewalls

- Disadvantages of software firewalls
  - You might have to worry about configuration problems
  - They rely on the OS on which they are running

Firewall Technologies

- Network Address Translation (NAT)
- Access lists
- Packet filtering
- Stateful packet inspection (SPI)
- Application layer inspection

Network Address Translation (NAT)

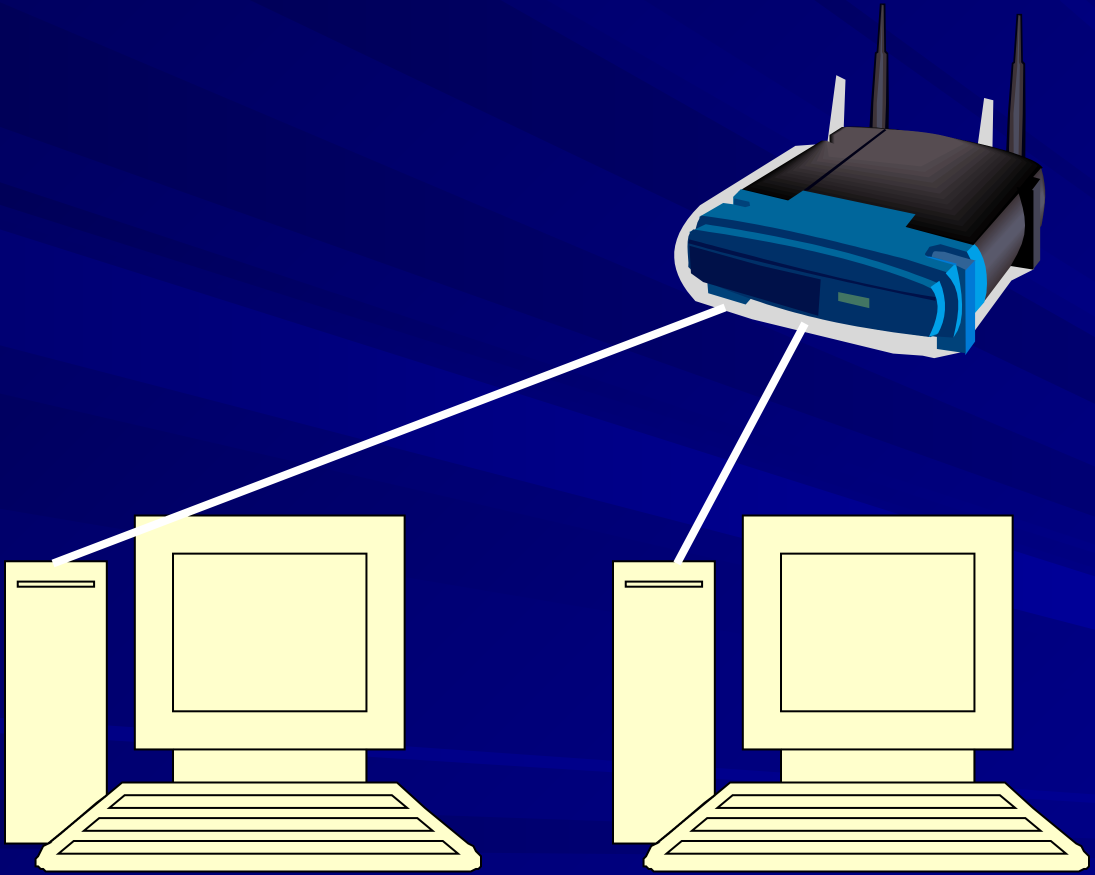
- Internal private IP addresses are mapped to public external IP addresses
  - Hides the internal infrastructure
- Port Address Translation (PAT)
  - This allows thousands of internal IP addresses to be mapped to one external IP address
  - Each connection from the private network is mapped to a different public port

147.144.20.1:1201

147.144.20.1:1202

147.144.20.1:1203

Public Addresses



Router providing
NAT and PAT

192.168.1.101:1100

192.168.1.102:1100

192.168.1.102:1103

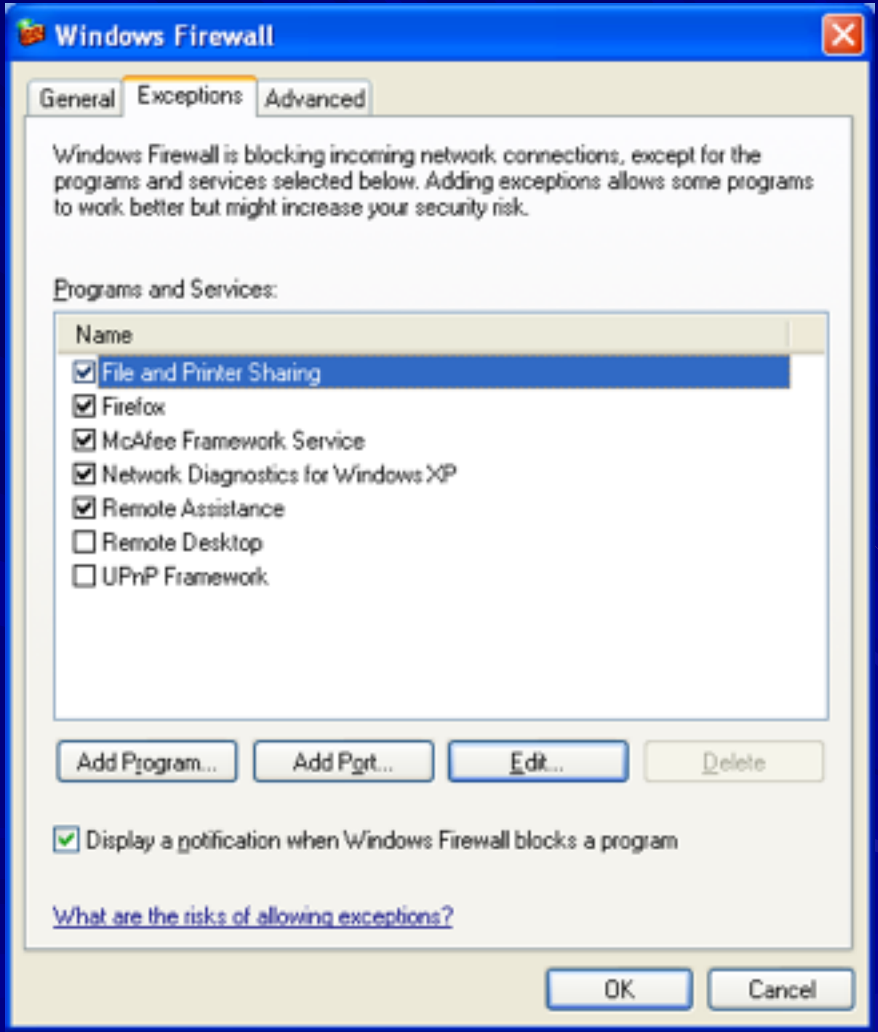
Private
Addresses

Access Lists

- A series of rules to control traffic
- Criteria
  - Source IP address
  - Destination IP address
  - Ports or services
  - Protocol (Usually UDP or TCP)

Packet Filtering

- Packet filters screen traffic based on information in the header, such as
  - Protocol type
  - IP address
  - TCP/UDP Port
  - More possibilities



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name

- ☑ File and Printer Sharing
- ☑ Firefox
- ☑ McAfee Framework Service
- ☑ Network Diagnostics for Windows XP
- ☑ Remote Assistance
- □ Remote Desktop
- □ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Stateful Packet Inspection (SPI)

- Stateful packet filters examine the current state of the network
  - If you have sent a request to a server, packets from that server may be allowed in
  - Packets from the same server might be blocked if no request was sent first

State Table

- Stateful firewalls maintain a *state table* showing the current connections

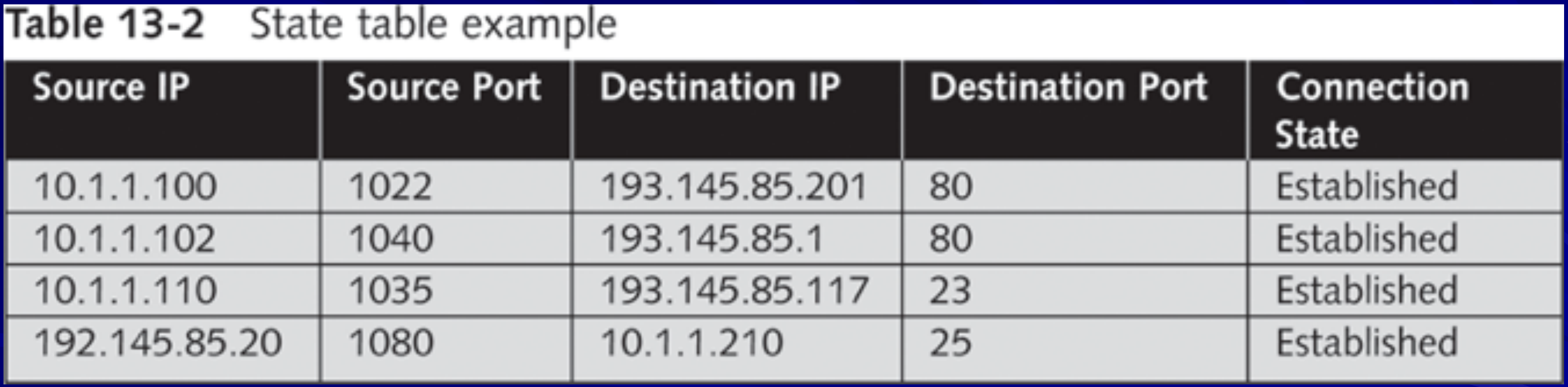


Table 13-2 State table example

Source IP	Source Port	Destination IP	Destination Port	Connection State
10.1.1.100	1022	193.145.85.201	80	Established
10.1.1.102	1040	193.145.85.1	80	Established
10.1.1.110	1035	193.145.85.117	23	Established
192.145.85.20	1080	10.1.1.210	25	Established

ACK Port scan

- Used to get information about a firewall
- Stateful firewalls track connection and block unsolicited ACK packets
- Stateless firewalls only block incoming SYN packets, so you get a RST response
- We covered this in chapter 5

Stateful Packet Inspection (SPI)

- Stateful packet filters recognize types of anomalies that most routers ignore
- Stateless packet filters handle each packet on an individual basis
  - This makes them less effective against some attacks, such as the "reverse shell"

Application Layer Inspection

- Application-layer firewall can detect Telnet or SSH traffic masquerading as HTTP traffic on port 80

Implementing a Firewall

- Using only one firewall between a company's internal network and the Internet is dangerous
  - It leaves the company open to attack if a hacker compromises the firewall
- Use a demilitarized zone instead

Demilitarized Zone (DMZ)

- DMZ is a small network containing resources available to Internet users
  - Helps maintain security on the company’s internal network
- Sits between the Internet and the internal network
- It is sometimes referred to as a “perimeter network”

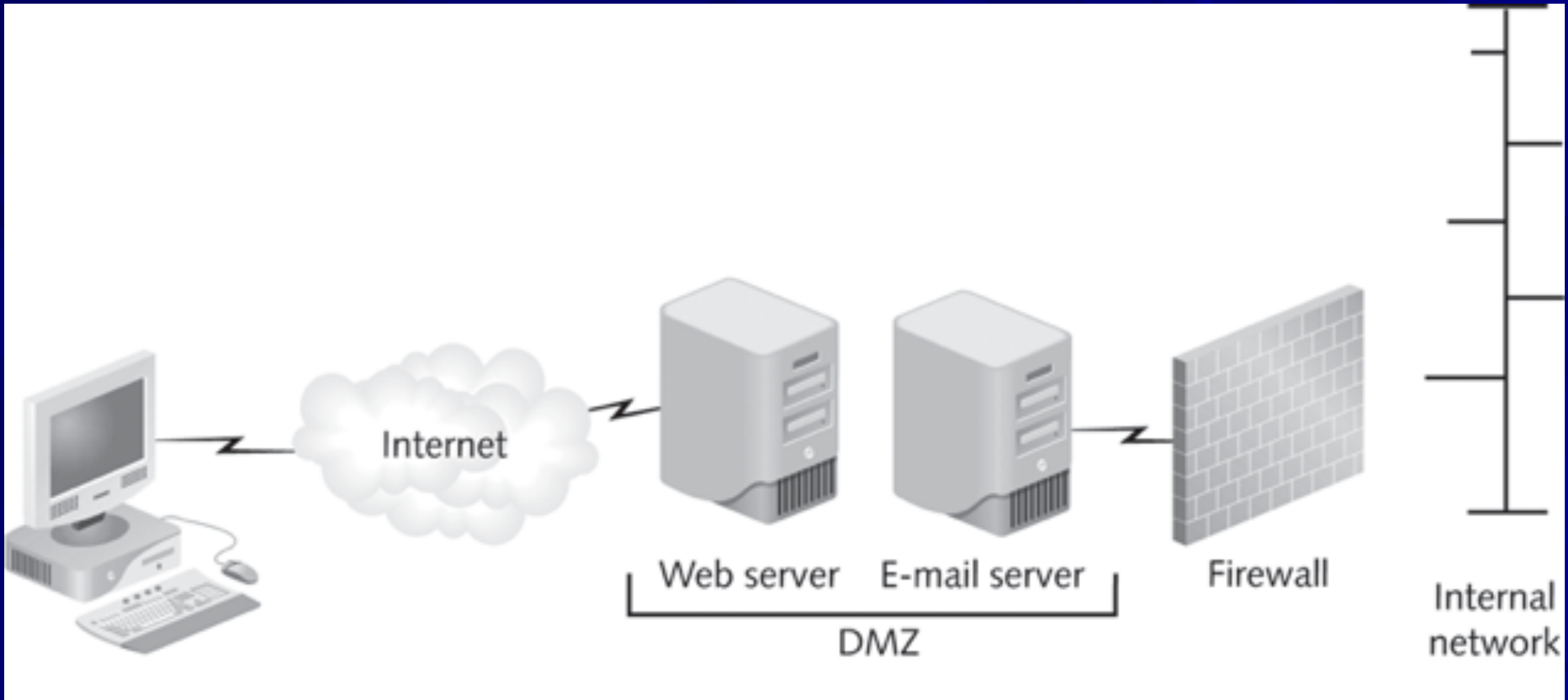


Figure 13-3 A DMZ protecting an internal network.

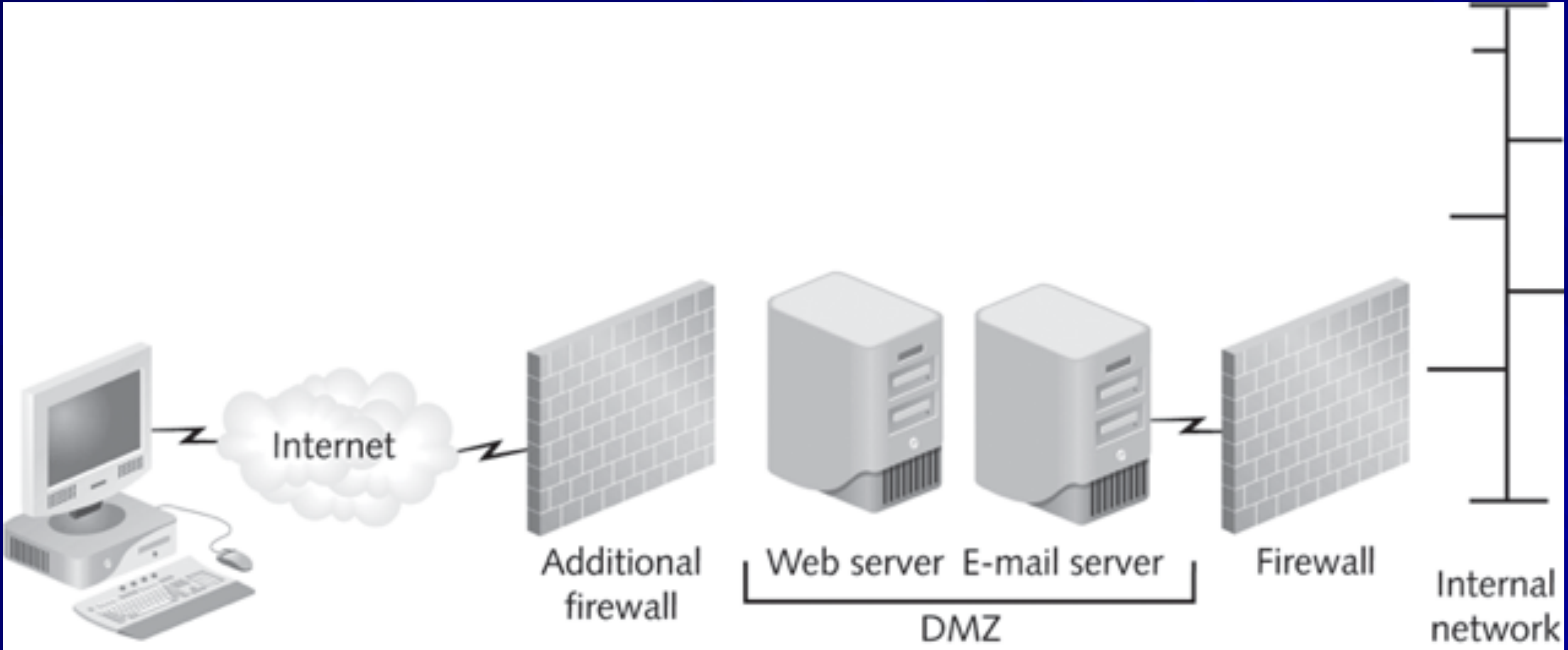


Figure 13-4 An additional firewall used to protect the DMZ

Understanding the Cisco ASA (Adaptive Security Appliance) Firewall

- Replaced the Cisco PIX firewall
  - One of the most popular firewalls on the market

Configuration of the ASA Firewall

- Working with a PIX firewall is similar to working with any other Cisco router
- Login prompt

```
If you are not authorized to be in this XYZ Hawaii
  network device,
log out immediately!
Username: admin
Password: ********
```

  - This banner serves a legal purpose
  - A banner that says “welcome” may prevent prosecution of hackers who enter

Access List

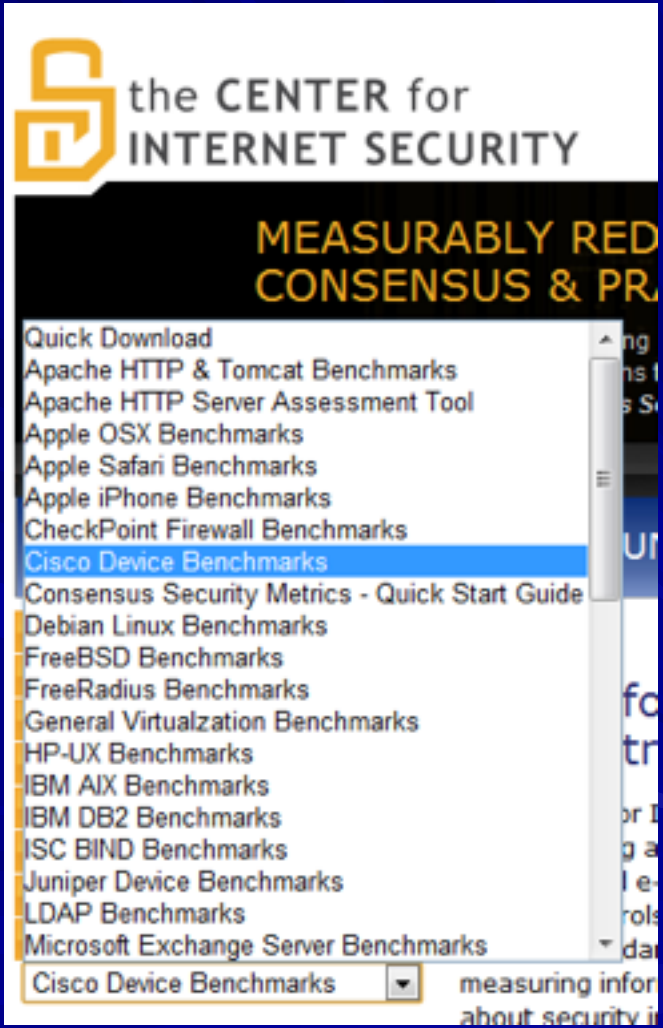
```
ciscoasa( config)# show run access- list
access- list PERMITTED_ TRAFFIC remark VPN- CONC1 TO
TERMINAL CLOSET1B
access- list PERMITTED_ TRAFFIC extended permit ip
host 10.13.61.98 host 10.13.61.18
access- list NONE extended deny ip any any log
access- list CAP- ACL extended permit ip any any
```

ASA Features

- Can group objects, such as terminals and serves, and filter traffic to and from them
- High throughput, and many more features
  - See link Ch 13w

Using Configuration and Risk Analysis Tools for Firewalls and Routers

- Center for Internet Security
  - Cisecurity.org
- Configuration benchmarks and risk assessment tools
- Free "Router Audit Tool" and many other tools
  - Link Ch13x



Red Seal

- Commercial tool to assess network security and compliance
- Diagram shows traffic flow between devices
  - Link Ch 13y

Understanding Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDSs)

- Monitor network devices so that security administrators can identify attacks in progress and stop them
- An IDS looks at the traffic and compares it with known exploits
  - Similar to virus software using a signature file to identify viruses
- Types
  - Network-based IDSs
  - Host-based IDSs

Network-Based and Host-Based IDSs

- Network-based IDSs
  - Monitor activity on network segments
  - They sniff traffic and alert a security administrator when something suspicious occurs
    - See link Ch 13o

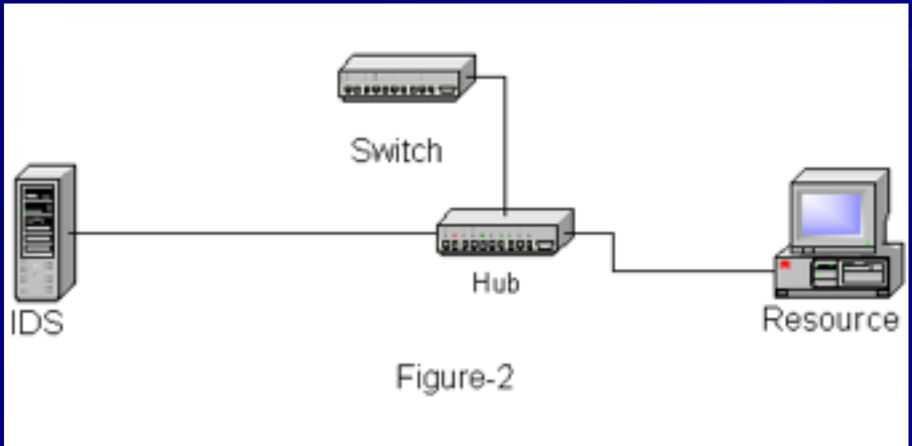


Figure-2

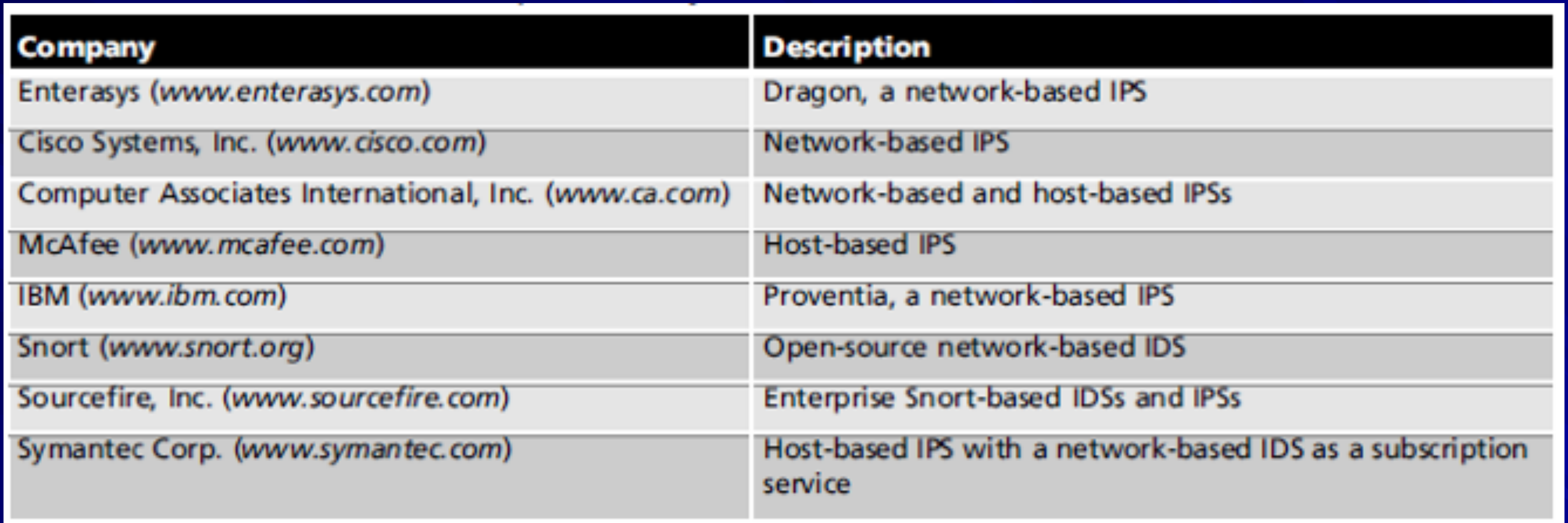
Network-Based and Host-Based IDSs

- Host-based IDSs
  - The software is installed on the server you’re attempting to protect, like antivirus software
  - Used to protect a critical network server or database server

Passive and Active IDSs

- IDSs are categorized by how they react when they detect suspicious behavior
  - Passive systems
    - Send out an alert and log the activity
    - Don't try to stop it
  - Active systems
    - Log events and send out alerts
    - Can also interoperate with routers and firewalls to block the activity automatically

Intrusion Detection and Prevention Systems



Company	Description
Enterasys (*www.enterasys.com*)	Dragon, a network-based IPS
Cisco Systems, Inc. (*www.cisco.com*)	Network-based IPS
Computer Associates International, Inc. (*www.ca.com*)	Network-based and host-based IPSs
McAfee (*www.mcafee.com*)	Host-based IPS
IBM (*www.ibm.com*)	Proventia, a network-based IPS
Snort (*www.snort.org*)	Open-source network-based IDS
Sourcefire, Inc. (*www.sourcefire.com*)	Enterprise Snort-based IDSs and IPSs
Symantec Corp. (*www.symantec.com*)	Host-based IPS with a network-based IDS as a subscription service

Aurora Attack
December 2009

(not in textbook)

"Aurora" Attack on Google

- In December, 2009, Google discovered that confidential materials were being sent out of their network to China
- Google hacked into the Chinese server and stole data back, discovering that dozens of other companies had also been exploited, including Adobe and Intel

Aurora Attack Sequence

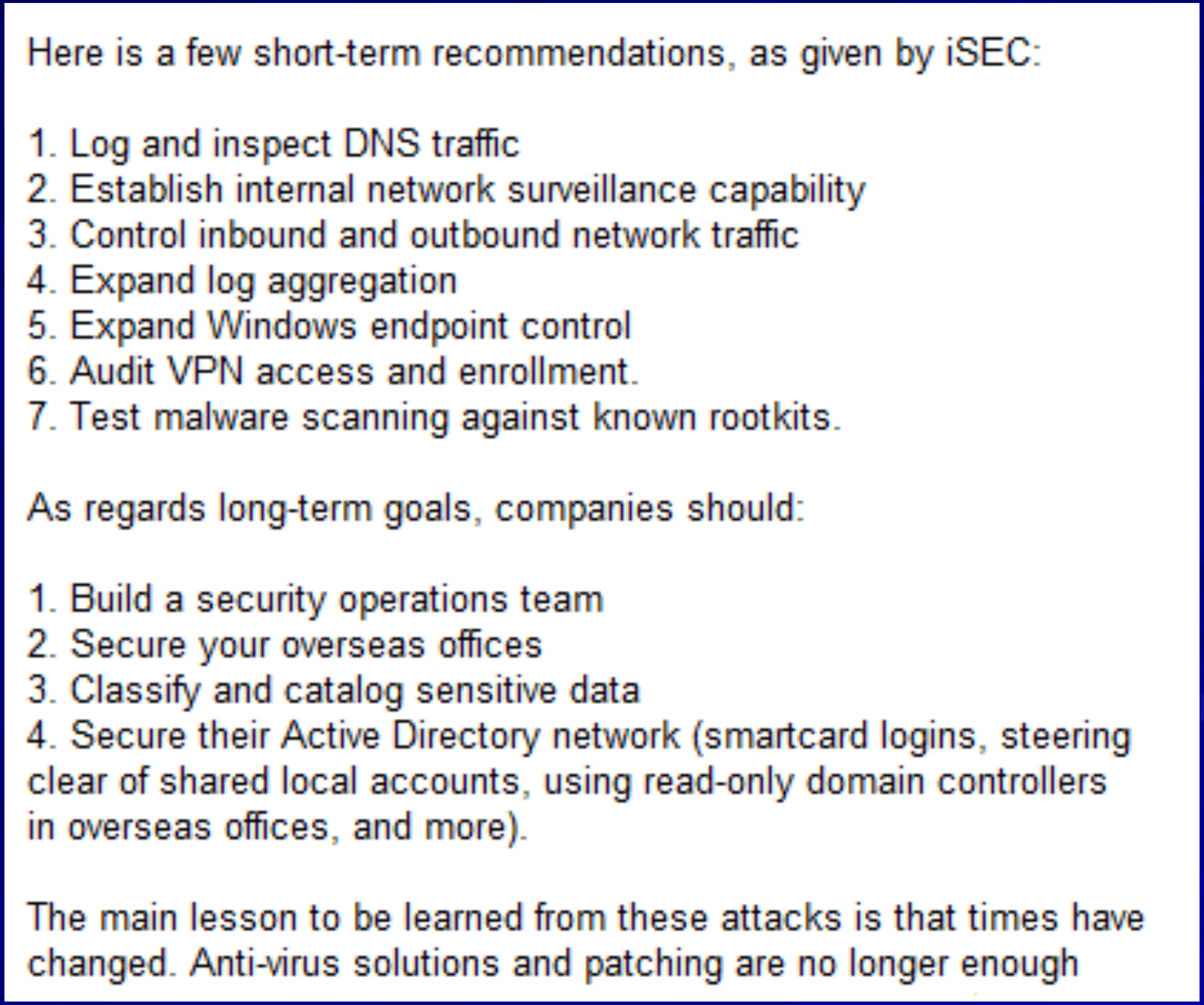
- Attacks were customized for each target based on vulnerable software and antivirus protection
  1. A user is tricked into visiting a malicious website
  2. Browser exploited to load malware on target PC
  3. Malware calls home to a control server
  4. Local privilege escalation

Aurora Attack Sequence

5. Active Directory password database stolen and cracked
6. Cracked credentials used to gain VPN Access
7. Valuable data is sent to China

New Recommendations

- Links Ch 13z1, 13z2



Here is a few short-term recommendations, as given by iSEC:

1. Log and inspect DNS traffic
2. Establish internal network surveillance capability
3. Control inbound and outbound network traffic
4. Expand log aggregation
5. Expand Windows endpoint control
6. Audit VPN access and enrollment.
7. Test malware scanning against known rootkits.

As regards long-term goals, companies should:

1. Build a security operations team
2. Secure your overseas offices
3. Classify and catalog sensitive data
4. Secure their Active Directory network (smartcard logins, steering clear of shared local accounts, using read-only domain controllers in overseas offices, and more).

The main lesson to be learned from these attacks is that times have changed. Anti-virus solutions and patching are no longer enough

CNIT 50: Network Security Monitoring

Proposed for Fall 2017 Sam Bowne

1 unit

THE PRACTICE OF
NETWORK SECURITY MONITORING
UNDERSTANDING INCIDENT DETECTION AND RESPONSE
RICHARD BEJTLICH
WARNING
NETWORK SECURITY MONITORING
IN PROGRESS

Understanding Honeypots

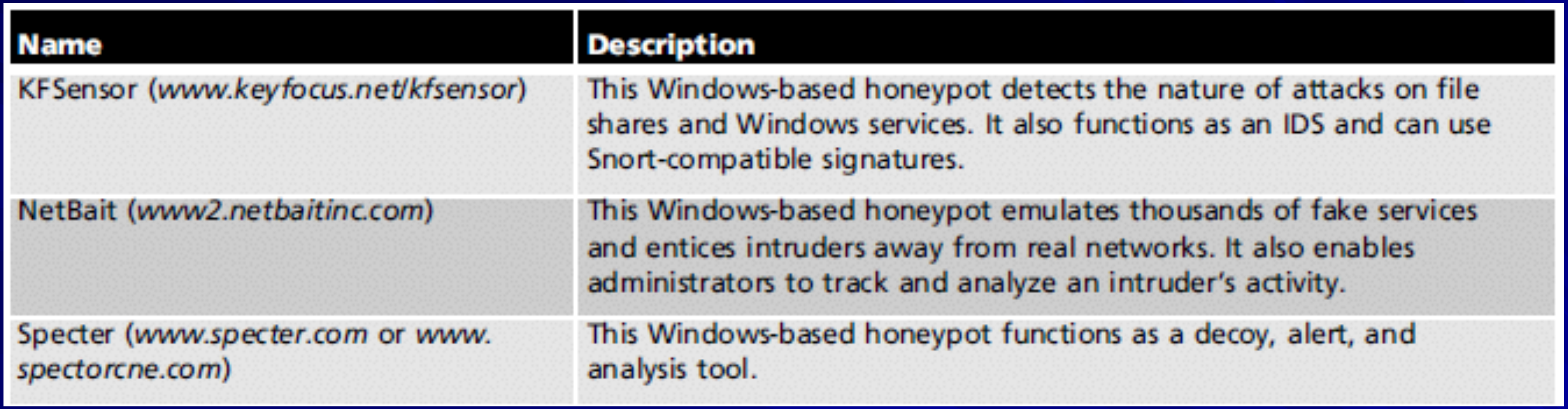
Understanding Honeypots

- Honeypot
  - Computer placed on the perimeter of a network
  - Contains information intended to lure and then trap hackers
- Computer is configured to have vulnerabilities
- Goal
  - Keep hackers connected long enough so they can be traced back

How They Work

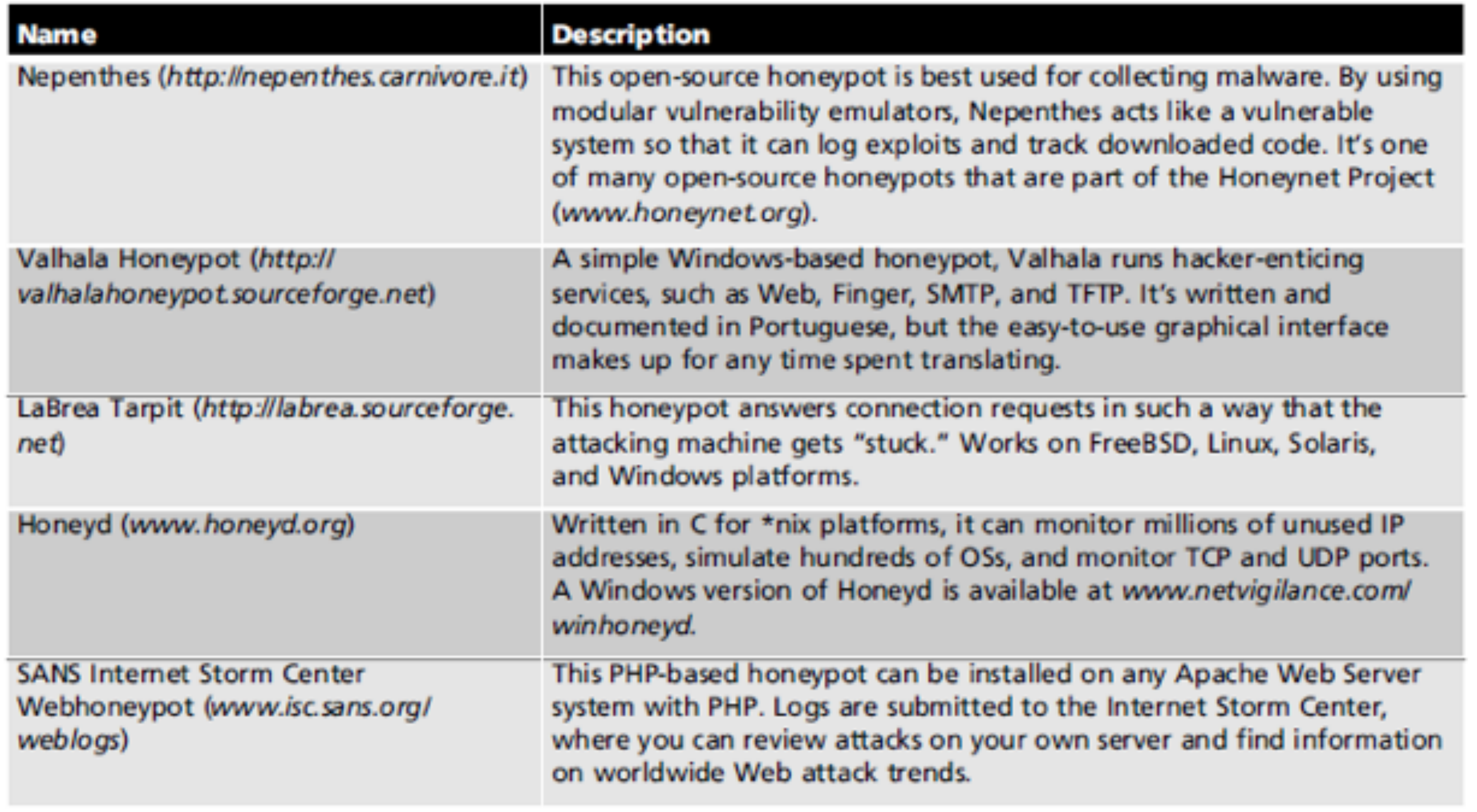
- A honeypot appears to have important data or sensitive information stored on it
    - Could store fake financial data that tempts hackers to attempt browsing through the data
- Hackers will spend time attacking the honeypot
    - And stop looking for real vulnerabilities in the company's network
- Honeypots also enable security professionals to collect data on attackers

Commercial Honeypots



Name	Description
KFSensor (*www.keyfocus.net/kfsensor*)	This Windows-based honeypot detects the nature of attacks on file shares and Windows services. It also functions as an IDS and can use Snort-compatible signatures.
NetBait (*www2.netbaitinc.com*)	This Windows-based honeypot emulates thousands of fake services and entices intruders away from real networks. It also enables administrators to track and analyze an intruder's activity.
Specter (*www.specter.com* or *www. spectorcne.com*)	This Windows-based honeypot functions as a decoy, alert, and analysis tool.

Open-Source Honeypots



Name	Description
Nepenthes (*http://nepenthes.carnivore.it*)	This open-source honeypot is best used for collecting malware. By using modular vulnerability emulators, Nepenthes acts like a vulnerable system so that it can log exploits and track downloaded code. It's one of many open-source honeypots that are part of the Honeynet Project (*www.honeynet.org*).
Valhala Honeypot (*http://valhalahoneypot.sourceforge.net*)	A simple Windows-based honeypot, Valhala runs hacker-enticing services, such as Web, Finger, SMTP, and TFTP. It's written and documented in Portuguese, but the easy-to-use graphical interface makes up for any time spent translating.
LaBrea Tarpit (*http://labrea.sourceforge.net*)	This honeypot answers connection requests in such a way that the attacking machine gets "stuck." Works on FreeBSD, Linux, Solaris, and Windows platforms.
Honeyd (*www.honeyd.org*)	Written in C for *nix platforms, it can monitor millions of unused IP addresses, simulate hundreds of OSs, and monitor TCP and UDP ports. A Windows version of Honeyd is available at *www.netvigilance.com/winhoneyd*.
SANS Internet Storm Center Webhoneypot (*www.isc.sans.org/weblogs*)	This PHP-based honeypot can be installed on any Apache Web Server system with PHP. Logs are submitted to the Internet Storm Center, where you can review attacks on your own server and find information on worldwide Web attack trends.

How They Work (continued)

- Virtual honeypots
  - Honeypots created using software solutions instead of hardware devices
  - Example: Honeyd

Project Honey Pot

- Web masters install software on their websites
- When spammers harvest email addresses from sites, HoneyNet's servers record the IP of the harvester
  - Can help prosecute the spammers and block the spam
    - Link Ch 13p

The NZ Honeynet Alliance - Capture

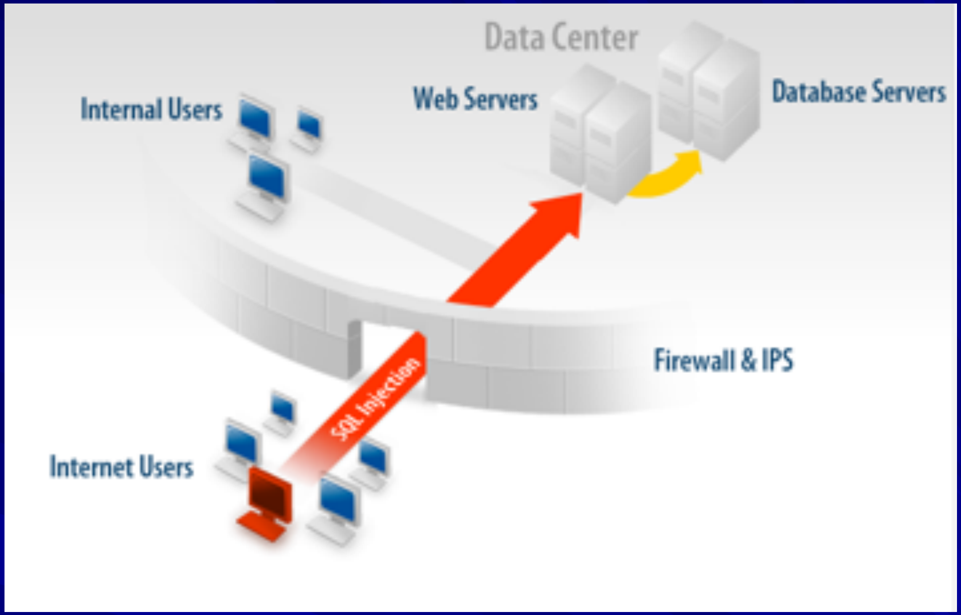
- Uses a Capture Server and one or more Capture Clients
  - The clients run in virtual machines
  - Clients connect to suspect Web servers
  - If the client detects an infection, it alerts the Capture Server and restores itself to a clean state
  - The server gathers data about malicious websites
    - See link Ch 13q

Web Application Firewalls

(not in textbook)

Web Application Attacks

- Normal firewall must allow Web traffic
- Doesn't stop attacks like SQL Injection
- Figure from Imperva, link Ch 13u

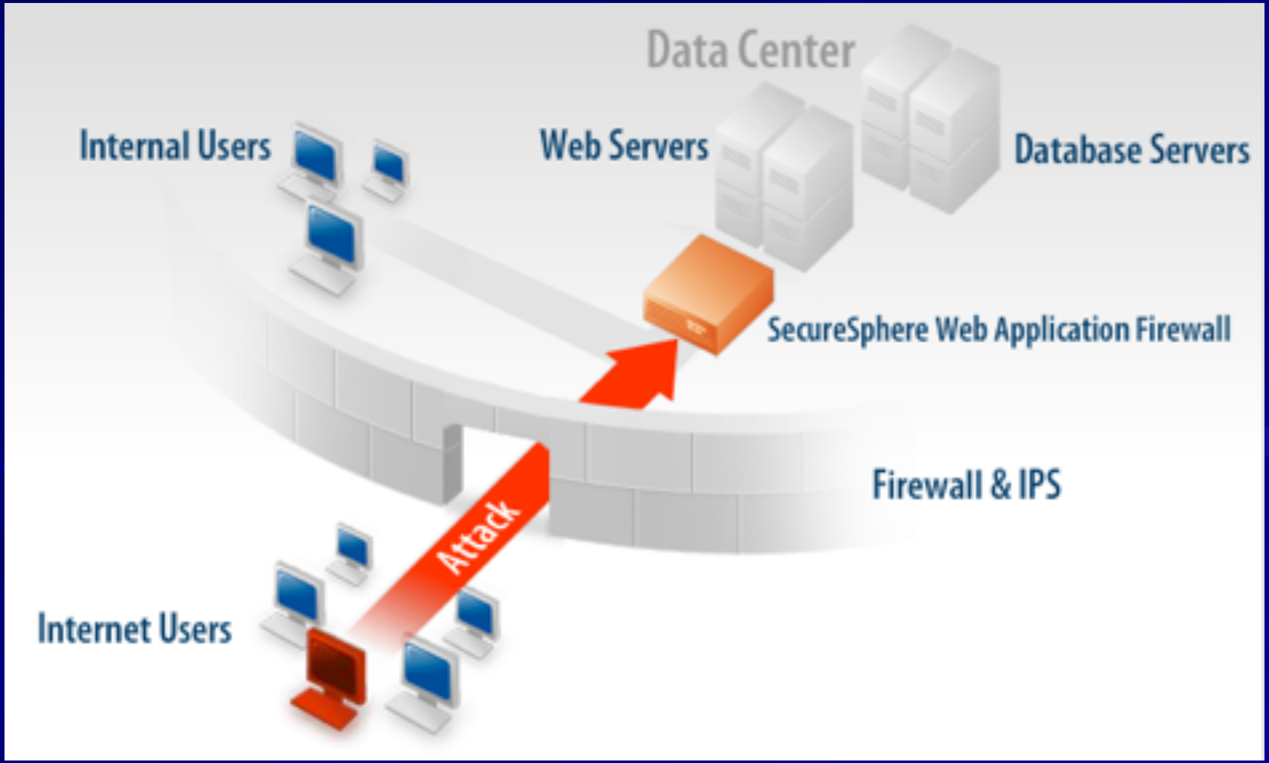


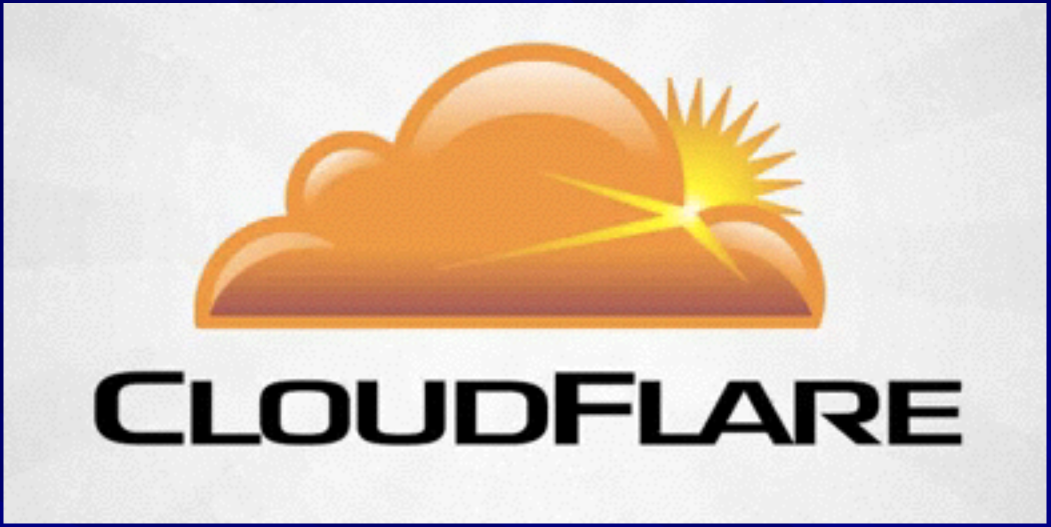
Web Application Firewalls

- There are many WAFs available
- See link Ch 13t

How a WAF Works

- Constantly-updated list of attack signatures
- Protects a vulnerable application





(not in textbook)

Reverse Proxies

- Cloudflare protects Web servers by intercepting requests and caching content
- Makes a Website faster and much more secure
- Used in real combat—LulzSec hid their site behind CloudFlare in Summer 2011 and th3j35t3r could not find them