Slide 1

IK1552 Internetworking/Internetteknik

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Electrical Engineering and Computer Science (EECS), KTH Royal Institute of Technology

IK1552 Spring 2019, Period 4 2019.04.07

Slide 2

Module 12: IPSec, VPNs, Firewalls, and NAT

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*.

Slide 3

Outline

- Private networks
- Virtual private Networks (VPNs)
- Security protocols
- IPSec
- Firewalls & Network Address Translation (NAT)
- Demilitarized zone (DMZ)

Slide 4

Private networks

Private Networks are designed to be used by a limited set of users (generally those inside an organization)

Intranet	a private network - access limited to those in an organization
Extranet	intranet + limited access to some resource by additional users from outside the organization

Addresses for Private IP networks

- these should never be routed to outside the private network
- they should never be advertised (outside the private network)
- allocated (**reserved**) addresses:

Range	Total addresses
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

Slide 5

Virtual Private networks (VPNs)

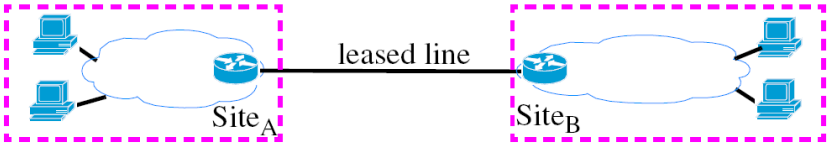


Figure 1: Private network

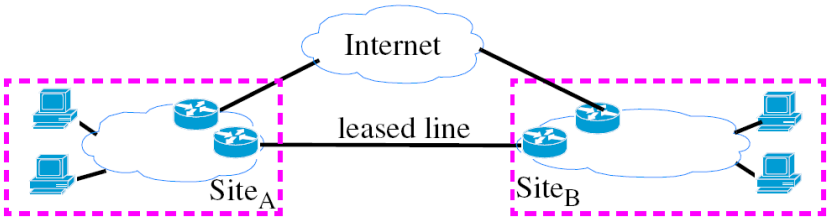


Figure 2: Hybrid network

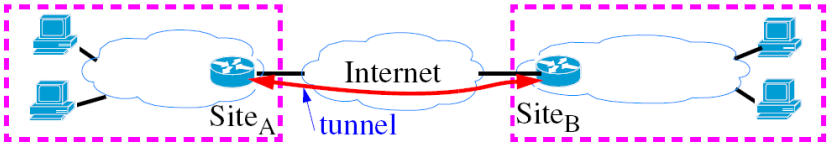


Figure 3: Virtual Private network

Slide 6

Security Protocols, APIs, etc.

- Generic Security Services App. Programming Interface (GSS-API)
- Network layer security
  Internet Protocol Security Protocol (IPSEC)
- Secured Socket Layer (SSL)/Transport Layer Security
  - transport layer security
  - Secured HyperText Transport Protocol (S-HTTP)
- Application layer security
  - Pretty Good Privacy (PGP)
  - Privacy-Enhanced Electronic Mail (PEM), S/MIME (signed MIME), PGP/MIME, and OpenPGP, …
  - MasterCard and Visa's Secured Electronic Transaction (SET)
- Authentication
  - Remote Authentication Dial-In User Services (RADIUS) http://www.gnu.org/software/radius/radius.html, FreeRADIUS, http://www.freeradius.org/ DIAMETER http://www.diameter.org/
- …

IK1552 SPRING 2019 SLIDE 6

S. Garfinkel, PGP: pretty good privacy. Sebastopol, CA: O'Reilly & Associates, 1995, ISBN-10: 1565920988 ISBN-13: 978-1565920989.

Internet Mail Consortium, "S/MIME and OpenPGP", Oct 15, 2004 http://www.imc.org/smime-pgpmime.html

Slide 7

GSS-API

Generic Security Services Application Programming Interface (GSS-API)

- provides an abstract interface which provides security services for use in distributed applications
- but isolates callers from specific security mechanisms and implementations.

GSS-API peers establish a common security mechanism for security context establishment either through administrative action, or through negotiation.

GSS-API is specified in:

- J. Linn, "Generic Security Service API v2", RFC 2078
- J. Wray, "Generic Security Service API v2: C-bindings", RFC 2744.

IK1552 SPRING 2019 SLIDE 7

J. Linn, 'Generic Security Service Application Program Interface', *Internet Request for Comments*, vol. RFC 1508 (Proposed Standard), September 1993, Available at http://www.rfc-editor.org/rfc/rfc1508.txt

J. Linn, 'Generic Security Service Application Program Interface, Version 2', *Internet Request for Comments*, vol. RFC 2078 (Proposed Standard), January 1997, Available at http://www.rfc-editor.org/rfc/rfc2078.txt

J. Wray, 'Generic Security Service API : C-bindings', *Internet Request for Comments*, vol. RFC 1509 (Proposed Standard), September 1993, Available at http://www.rfc-editor.org/rfc/rfc1509.txt

J. Wray, 'Generic Security Service API Version 2 : C-bindings', *Internet Request for Comments*, vol. RFC 2744 (Proposed Standard), January 2000, Available at http://www.rfc-editor.org/rfc/rfc2744.txt

Slide 8

IPSec

IPSec in three parts:

- encapsulating security payload (ESP) defines encryption or IP payloads,
- authentication header (AH) defines authentication method, and
- the IP security association key management protocol (ISAKMP) manages the exchange of secret keys between senders and recipients of ESP or AH packets.

Slide 9

ESP packet

Consists of:

- a control header - contains a Security Parameters Index (SPI) and a sequence number field (the SPI + destination IP address unqiuely identifies the Security Association (SA)).
- a data payload - encrypted version of the user's original packet. It may also contain control information needed by the cryptographic algorithms (for example DES needs an initialization vector (IV)).
- an optional authentication trailer - contains an Integrity Check Value (ICV) - which is used to validate the authenticity of the packet.

ESP could use any one of several algorithms: DES, Triple DES, …

See: RFCs 2406 & 4303: IP Encapsulating Security Payload (ESP)

IK1552 SPRING 2019 SLIDE 9

R. Atkinson, 'IP Encapsulating Security Payload (ESP)', *Internet Request for Comments*, vol. RFC 1827 (Proposed Standard), August 1995, Available at http://www.rfc-editor.org/rfc/rfc1827.txt

S. Kent and R. Atkinson, 'IP Encapsulating Security Payload (ESP)', *Internet Request for Comments*, vol. RFC 2406 (Proposed Standard), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2406.txt

S. Kent, 'IP Encapsulating Security Payload (ESP)', *Internet Request for Comments*, vol. RFC 4303 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4303.txt

Slide 10

AH header

For authentication purposes only contains:

- an SPI,
- a sequence number, and
- an authentication value.

AH uses either:

- Message Digest 5 (MD5) algorithm,
- Secure Hash Algorithm 1 (SHA-1),
- truncated HMAC (hashed message authentication code), or
- …

For further information see:

- IP Authentication Header - RFCs 2402 & 4302

IK1552 SPRING 2019 SLIDE 10

R. Atkinson, 'IP Authentication Header', *Internet Request for Comments*, vol. RFC 1826 (Proposed Standard), August 1995, Available at http://www.rfc-editor.org/rfc/rfc1826.txt

S. Kent and R. Atkinson, 'IP Authentication Header', *Internet Request for Comments*, vol. RFC 2402 (Proposed Standard), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2402.txt

S. Kent, 'IP Authentication Header', *Internet Request for Comments*, vol. RFC 4302 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4302.txt

Slide 11

ISAKMP

ISAKMP is based on the Diffie-Hellman key exchange protocol; it assumes the identities of the two parties are known.

Using ISAKMP you can:

- control the level of trust in the keys,
- force SPIs to be changed at an appropriate frequency,
- identify keyholders via digital certificates [requires using a certificate authority (CA)]

For further information see:

- Internet Security Association and Key Management Protocol (ISAKMP) - RFC 2408
- The Internet IP Security Domain of Interpretation for ISAKMP - RFC 2407
- The OAKLEY Key Determination Protocol - RFC 2412
- The Internet Key Exchange (IKE) - RFC 2409
- Internet Key Exchange (IKEv2) Protocol - RFC 4306
- The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX – RFC 4945
- …

IK1552 SPRING 2019 SLIDE 11

D. Maughan, M. Schertler, M. Schneider, and J. Turner, 'Internet Security Association and Key Management Protocol (ISAKMP)', *Internet Request for Comments*, vol. RFC 2408 (Proposed Standard), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2408.txt

C. Kaufman, 'Internet Key Exchange (IKEv2) Protocol', *Internet Request for Comments*, vol. RFC 4306 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4306.txt

D. Piper, 'The Internet IP Security Domain of Interpretation for ISAKMP', *Internet Request for Comments*, vol. RFC 2407 (Proposed Standard), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2407.txt

C. Kaufman, 'Internet Key Exchange (IKEv2) Protocol', *Internet Request for Comments*, vol. RFC 4306 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4306.txt

H. Orman, 'The OAKLEY Key Determination Protocol', *Internet Request for Comments*, vol. RFC 2412 (Informational), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2412.txt

D. Harkins and D. Carrel, 'The Internet Key Exchange (IKE)', *Internet Request for Comments*, vol. RFC 2409 (Proposed Standard), November 1998, Available at http://www.rfc-editor.org/rfc/rfc2409.txt

S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart, 'On the Use of Stream Control Transmission Protocol (SCTP) with IPsec', *Internet Request for Comments*, vol. RFC 3554 (Proposed Standard), July 2003, Available at http://www.rfc-editor.org/rfc/rfc3554.txt

P. Hoffman, 'Algorithms for Internet Key Exchange version 1 (IKEv1)', *Internet Request for Comments*, vol. RFC 4109 (Proposed Standard), May 2005, Available at http://www.rfc-editor.org/rfc/rfc4109.txt

C. Kaufman, 'Internet Key Exchange (IKEv2) Protocol', *Internet Request for Comments*, vol. RFC 4306 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4306.txt

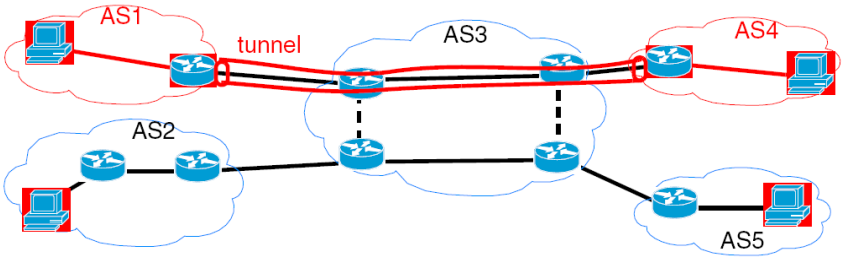
J. Schiller, 'Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)', *Internet Request for Comments*, vol. RFC 4307 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4307.txt

B. Korver, 'The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX', Internet Request for Comments, vol. RFC 4945 (Proposed Standard), Aug. 2007 [Online]. Available: http://www.rfc-editor.org/rfc/rfc4945.txt

Slide 12

Where can you run IPSec?

Mode	Where it runs	Payload
Transport	end-systems	payload data follows the normal IP header
Tunnelling	internetworking device: e.g., router, firewall, or VPN gateway	• end-user's entire packet-IP headers and all-placed within another packet with ESP or AH fields [thus it is encapsulated in another packet] • can hide the original source and destination address information



IPSec usage red = secure, black = unsecure

Slide 13

OpenVPN

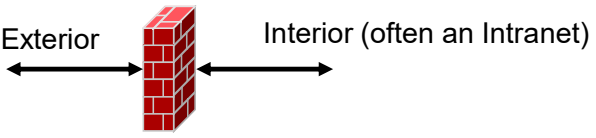
open source VPN package using SSL/TLS
https://openvpn.net/

See the HowTo file at https://openvpn.net/index.php/open-source/documentation/howto.html

- Utilizes UDP or TCP to carry tunneled traffic
- Available for lots of platforms: linux, Windows, MacOS, Android, iOS, …

Slide 14

Firewalls



Firewall an internet gateway

The firewall can provide packet by packet filtering of packets coming into the **intranet** or leaving the intranet. The firewall can decide which packets should be forwarded based on source, destination addresses, and port (or even deeper examination) using an explicitly defined **policy**.

See the books: *Firewalls and Internet Security: Repelling the Wily Hacker; Building Internet Firewalls: Internet and Web security; and* RFCs 2979, 2647, 3511, and 4487

IK1552 SPRING 2019 SLIDE 14

Bill Cheswick and Steve Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison Wesley, 1994,ISBN: 0-201-63357-4

W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, Firewalls and Internet security: repelling the wily hacker, 2nd ed. Boston: Addison-Wesley, 2003, ISBN-10: 020163466X, ISBN-13: 978-0201634662. http://www.amazon.com/Firewalls-Internet-Security-Repelling-Edition/dp/020163466X

D. Brent Chapman and Elizabeth Zwicky, *Building Internet Firewalls*, O'Reilly, 1995,ISBN: 1-56592-124-0
E. D. Zwicky, S. Cooper, and D. B. Chapman, *Building Internet Firewalls: Internet and Web security*, 2nd ed. Beijing ; Cambridge, Mass: O'Reilly, 2000.

D. Newman, 'Benchmarking Terminology for Firewall Performance', Internet Request for Comments, vol. RFC 2647 (Informational), Aug. 1999 [Online]. Available: http://www.rfc-editor.org/rfc/rfc2647.txt

N. Freed, 'Behavior of and Requirements for Internet Firewalls', Internet Request for Comments, vol. RFC 2979 (Informational), Oct. 2000 [Online]. Available: http://www.rfc-editor.org/rfc/rfc2979.txt

B. Hickman, D. Newman, S. Tadjudin, and T. Martin, 'Benchmarking Methodology for Firewall Performance', Internet Request for Comments, vol. RFC 3511 (Informational), Apr. 2003 [Online]. Available: http://www.rfc-editor.org/rfc/rfc3511.txt

F. Le, S. Faccin, B. Patil, and H. Tschofenig, 'Mobile IPv6 and Firewalls: Problem Statement', Internet Request for Comments, vol. RFC 4487 (Informational), May 2006 [Online]. Available: http://www.rfc-editor.org/rfc/rfc4487.txt

Slide 15

Linux firewall

For example, for the software firewall used in Linux systems called “ipfwadm”:

- all ports are typically closed for inbound traffic,
- all outbound traffic is “IP masqueraded”, i.e., appears to come from the gateway machine; and
- For bi-directional services required by the users, “holes” may be punched through the firewall - these holes can reroute traffic to/from particular ports:
  - to specific users or
  - the most recent workstation to request a service.

Slide 16

Firewall Design

Apply basics of security:

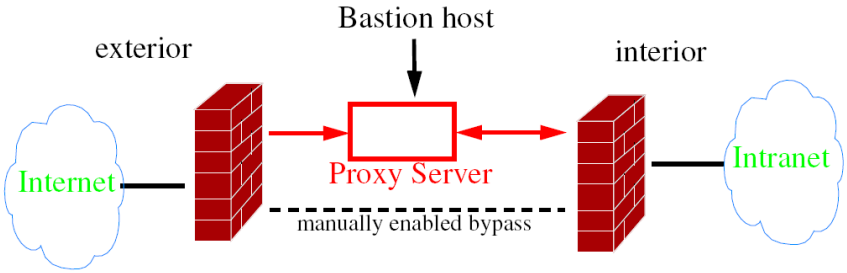
- least privilege:
  - Do not make hosts do more than they have to (implies: specialized servers)
  - use minimum privileges for the task in hand
- fail safe
  - even if things break it should not leave anything open
- defense in depth
  - use several discrete barriers – do not depend on a single firewall for all security
- weakest links
  - know the limitations of your defenses - understand your weakest link

Firewalls should have sufficient performance to keep the pipes full - i.e., a firewall should not limit the amount of traffic flowing across the connection to the external network, only **what** flows across it!

IK1552 SPRING 2019 SLIDE 16

Slide 17

Proxy access through a firewall



Firewall and internet gateway

Often you need application level proxies (i.e., they understand details of the application protocol) -- an example is to proxy RealNetworks' RealAudio's streaming audio.

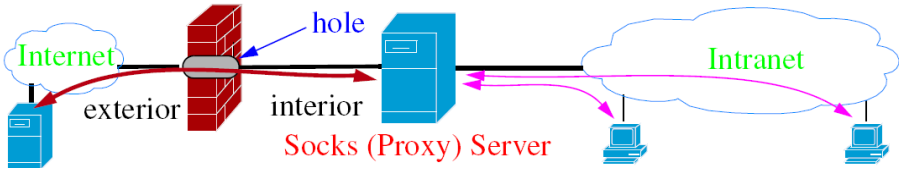
Slide 18

SOCKs v5

In order to bridge a firewall we can use a proxy:

- the proxy will appear to be **all external hosts** to those within the firewall
  - for example, If a user attached to the intranet requests a webpage, the request is sent to the proxy host where the same request is duplicated and sent to the real destination. When data is returned the proxy readdresses (with the user's intranet address) the returned data and sends it to the user.
- widely used to provide proxies for commonly used external services (such as Telnet, FTP, and HTTP).

See: RFC 1928 and RFC 1961



IK1552 SPRING 2019 SLIDE 18

M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, 'SOCKS Protocol Version 5', *Internet Request for Comments*, vol. RFC 1928 (Proposed Standard), March 1996, Available at http://www.rfc-editor.org/rfc/rfc1928.txt

P. McMahon, 'GSS-API Authentication Method for SOCKS Version 5', *Internet Request for Comments*, vol. RFC 1961 (Proposed Standard), June 1996, Available at http://www.rfc-editor.org/rfc/rfc1961.txt

R. Finlayson, 'IP Multicast and Firewalls', *Internet Request for Comments*, vol. RFC 2588 (Informational), May 1999, Available at http://www.rfc-editor.org/rfc/rfc2588.txt

H. Kitamura, 'A SOCKS-based IPv6/IPv4 Gateway Mechanism', *Internet Request for Comments*, vol. RFC 3089 (Informational), April 2001, Available at http://www.rfc-editor.org/rfc/rfc3089.txt

Slide 19

Newping

http://ftp.cerias.purdue.edu/pub/tools/dos/socks.cstc/util/newping.c

- a “ping” for SOCKS
- it depends on the target host **not** blocking the service on the appropriate port (in this case “**time**”).
- This version is primarily for checking “Is it alive?” rather than gathering statistics on the average response time of several echo requests.
- Uses the “**time**” TCP port to verify that a host is up, rather than using ICMP ⇒ usable through a firewall that blocks ICMP.

IK1552 SPRING 2019 SLIDE 19

Slide 20

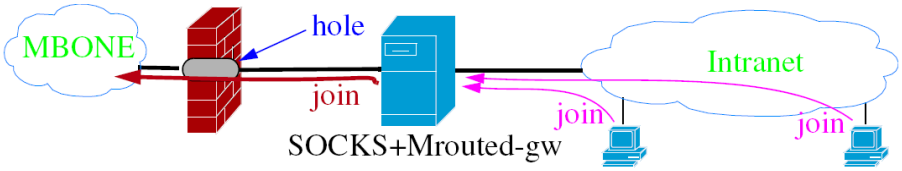
MBONE through firewalls

http://www.cs.virginia.edu/~mngroup/projects/firewalls/

Their firewall features:

- Source host checking (allowing only certain hosts to transmit through the firewall, or denying specific hosts)
- Destination port checking
- Packet contents (unwrapping encapsulated IP)
- Regulating bandwidth allocated to a specific multicast group's traffic

Their Mbone gateway is based on a modified multicast routing daemon.



Firewall and internet gateway

Slide 21

Secure Mailer (aka Postfix)

Wietse Venema's attempt to provide an alternative to the widely-used Sendmail program

70% of all mail sent via the Internet is sent via Sendmail

"Security. Postfix uses multiple layers of defense to protect the local system against intruders. Almost every Postfix daemon can run in a chroot jail with fixed low privileges. There is no direct path from the network to the security-sensitive local delivery programs - an intruder has to break through several other programs first. Postfix does not even trust the contents of its own queue files, or the contents of its own IPC messages. Postfix avoids placing sender-provided information into shell environment variables. Last but not least, no Postfix program is set-uid."

Postfix *http://www.postfix.org*

IK1552 SPRING 2019 SLIDE 21

Slide 22

U.S. DOE CIAC's Network Security Tools

- System Administrator Tool for Analyzing Networks (**SATAN**), network security analyzer designed by Dan Farmer and Wietse Venema; scans systems connected to the network noting the existence of well known, often exploited vulnerabilities. (see also Security Auditor's Research Assistant (SARA))
- **ipacl** - forces all TCP and UDP packets to pass through an access control list facility
- **logdaemon** - modified versions of rshd, rlogind, ftpd, rexecd,login, and telnetd that log significantly more information -- enabling better auditing of problems via the logfiles
- improved versions of: portmap, rpcbind,
- **screend** - a daemon and kernel modifications to allow all packets to be filtered based on source address, destination address, or any other byte or set of bytes in the packet
- **securelib** - new versions of the accept, recvfrom, and recvmsg networking system calls

IK1552 SPRING 2019 SLIDE 22

U.S. DOE's Computer Incident Advisory Capability (formerly at *http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html*)

Lawrence Livermore's COMPUTER SECURITY TECHNOLOGY CENTER (CSTC), Making Information Safe, Science and Technology Review, January/February 1998 https://www.llnl.gov/str/Mansur.html

UNIX Public Tools, US Department of Energy, Accessed on 2014.04.22 http://energy.gov/cio/unix-public-tools

Slide 23

- **TCP Wrappers** - allows monitoring and control over who connects to a host's TFTP, EXEC, FTP, RSH, TELNET, RLOGIN, FINGER, and SYSTAT ports + a library so that other programs can be controlled and monitored in the same fashion
- ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/tcp_wrappers_7.6.BLURB

- **xinetd** - a replacement for inetd which supports access control based on the address of the remote host and the time of access + provides extensive logging capabilities

Slide 24

The Network Mapper (NMAP) Network Mapper (NMAP)

http://nmap.org/

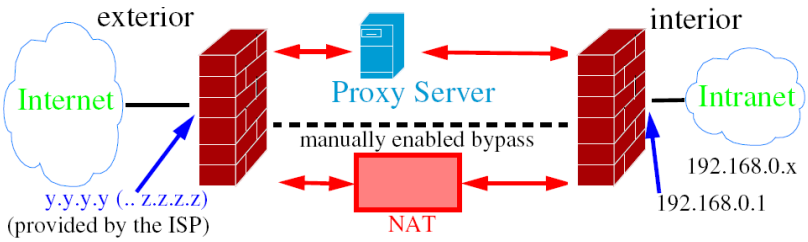
- (cleverly) uses raw IP packets
- determine what hosts are available on the network,
- what services (application name and version) are offered,
- what operating systems (and OS versions) they are running,
- what type of packet filters/firewalls are in use,
- …

http://nmap.org/docs.html

Based upon "*Remote OS detection via TCP/IP Stack FingerPrinting*" by Fyodor (www.insecure.org), October 18, 1998 - a means of identifying which OS the host is running by noting its TCP/IP behavior.

Slide 25

Network Address Translation (NAT)



Example of a Firewall with NAT

NAT maps IP addresses on the inside to one or more addresses on the outside and vice versa. See RFC 3022 and RFC2766. See also RFC 4966 – which describes why RFC 2766 should be historic.

Advantages	Disadvantage
✔ save IPv4 addresses ✔hides internal node structure from outside nodes ✔the intranet does not have to be renumbered when you connect to another ISP	✘ Unfortunately this breaks many services because they use an IP address inside the their data.

IK1552 SPRING 2019 SLIDE 25

P. Srisuresh and K. Egevang, 'Traditional IP Network Address Translator (Traditional NAT)', *Internet Request for Comments*, vol. RFC 3022 (Informational), January 2001, Available at http://www.rfc-editor.org/rfc/rfc3022.txt

G. Tsirtsis and P. Srisuresh, 'Network Address Translation - Protocol Translation (NAT-PT)', *Internet Request for Comments*, vol. RFC 2766 (Historic), February 2000, Available at http://www.rfc-editor.org/rfc/rfc2766.txt

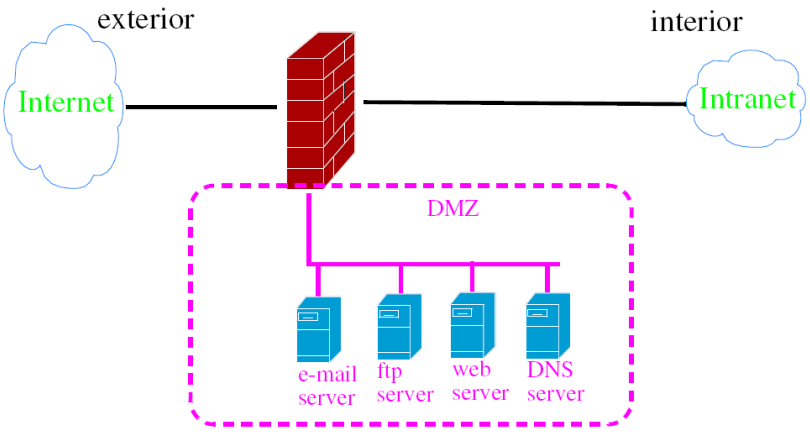
C. Aoun and E. Davies, 'Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status', *Internet Request for Comments*, vol. RFC 4966 (Informational), July 2007, Available at http://www.rfc-editor.org/rfc/rfc4966.txt

D. Thaler, L. Zhang, and G. Lebovitz, 'IAB Thoughts on IPv6 Network Address Translation', Internet Request for Comments, vol. RFC 5902 (Informational), Jul. 2010 [Online]. Available: http://www.rfc-editor.org/rfc/rfc5902.txt

M. Bagnulo, P. Matthews, and I. van Beijnum, 'Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers', Internet Request for Comments, vol. RFC 6146 (Proposed Standard), Apr. 2011 [Online]. Available: http://www.rfc-editor.org/rfc/rfc6146.txt

Slide 26

Demilitarized zone (DMZ)



Example of a Firewall with a DMZ

Note that the various services may also be in different DMZs (see for example figure 4 page 90 of [Malmgren 2003]

IK1552 SPRING 2019 SLIDE 26

Robert Malmgren, *Praktisk nätsäkerhet*, Internet Academy Press, Stockholm, Sweden, 2003, ISBN 91-85035-02-5

Will Schmied, Victor Chang, Damiano Imperatore, Drew Simonis, Thomas W. Shindler, and Robert J. Shimonski (Technical Editor), Building DMZs For Enterprise Networks. Syngress, 2003, ISBN 1931836884, 978-1931836883.

Slide 27

Security Organizations and Companies

Computer Emergency Response Team (CERT ®) Coordination Center
http://www.cert.org/

- 1988 - Computer Emergency **Response** Team
- 2003 - Computer Emergency **Readiness** Team

Additionally, there are numerous other CERTs:

- CanCERT™, GOVCERT.NL, Sveriges IT-incidentcentrum (SITIC) http://www.sitic.se/, Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA), CNCERT/CC [Crochemore 2005], …
- The European CSIRT Network http://www.ecsirt.net/

Forum of Incident Response and Security Teams (FIRST),
as of 2014.04.23: 298 members in 64 countries

NIST Computer Security Resource Center; Swedish Defense Material Administration, Electronics Systems Directorate; …

IK1552 SPRING 2019 SLIDE 27

Computer Emergency Response Team http://www.cert.org/

David Crochemore, "Response/Readiness: What R the new CERTS?", National Computer network Emergency Response technical Team/Coordination Center of China (CNCERT/CC) 2005 Annual Conference, Guilin, P.R.China, 30 March 2005
http://www.cert.org.cn/upload/2005AnnualConferenceCNCERT/1MainConference/10.DavidCrochemore-NGCERTOI.pdf

Forum of Incident Response and Security Teams http://www.first.org/

U. S. National Institute of Standards and Technology (NIST), Computer Security Division, Computer Security Resource Center http://csrc.nist.gov/

Swedish Defense Material Administration http://www.fmv.se/

Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA) http://www.cert.ssi.gouv.fr/

Slide 28

Summary

This module has discussed:

- VPNs
- IPSec
- Firewalls
- NATs
- DMZ

Slide 29

Further reading

C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*, 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2002, ISBN-10: 0130460192 ISBN-13: 978-0130460196.

Slide 30

¿Questions?