IK1350 Protocols in Computer Networks/ Protokoll i datornätverk Spring 2008, Period 3

Module 13: IPSec, VPNs, Firewalls, and NAT

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *TCP/IP Protocol Suite*, by Behrouz A. Forouzan, 3rd Edition, McGraw-Hill, 2006.

For this lecture: Chapters 26 and 28

Last modified: 2008.02.07:09:56

Outline

- IPSec, VPN, …
- Firewalls & NAT
- Private networks

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}

Virtual Private networks (VPNs)

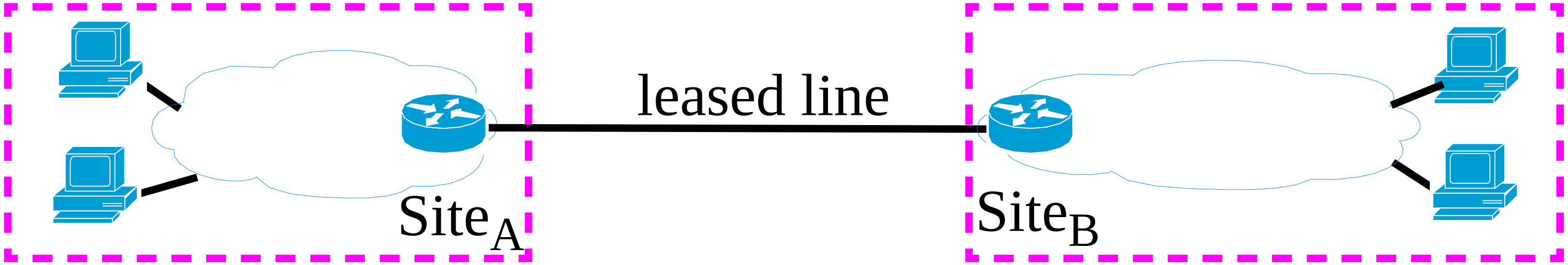


Figure 128: Private network

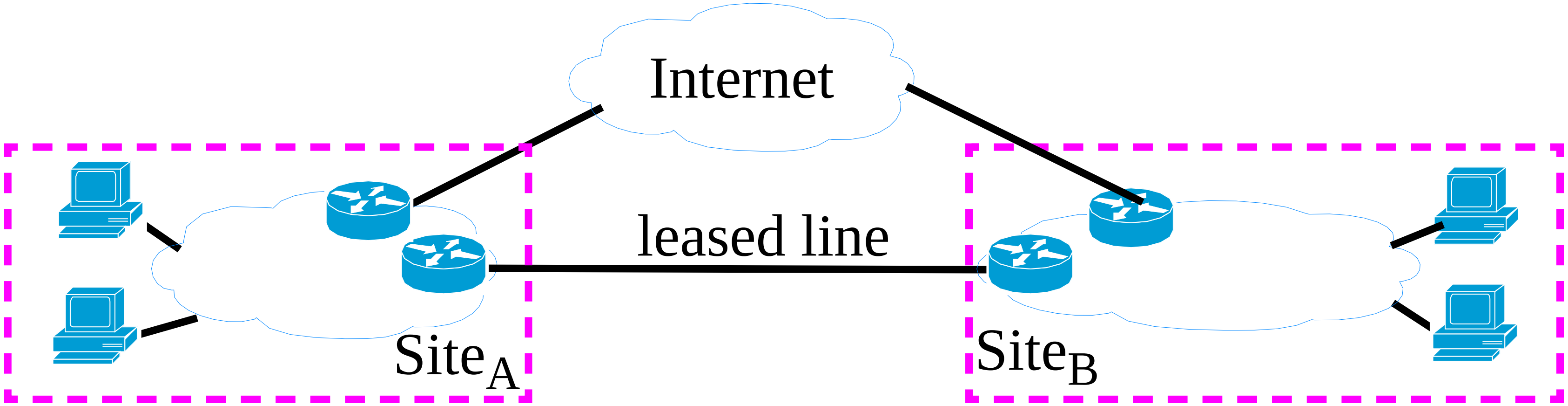


Figure 129: Hybrid network

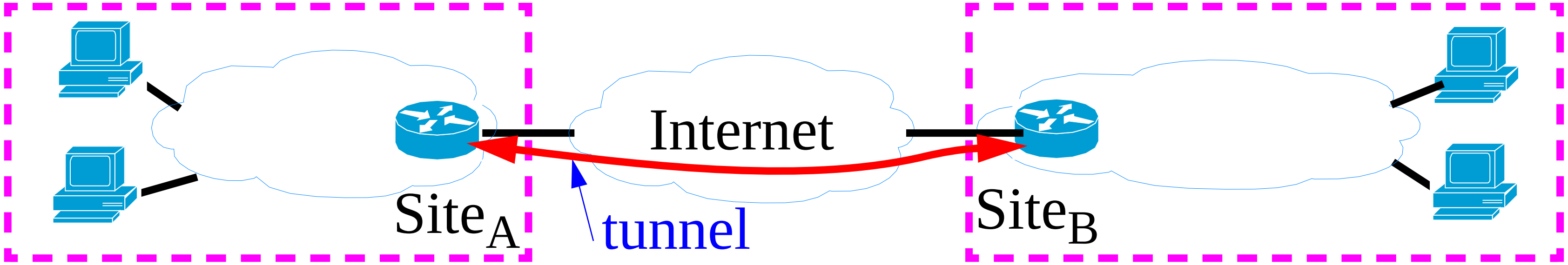


Figure 130: Virtual Private network

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) [139]
  - Privacy-Enhanced Electronic Mail (PEM), S/MIME (signed MIME), PGP/MIME, and OpenPGP, … [140]
  - 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/`
- …

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 [125]
- J. Wray, "Generic Security Service API v2: C-bindings", RFC 2744 [126].

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.

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: RFC 2406: IP Encapsulating Security Payload (ESP)[119]

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 - RFC 2402 [120]

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 [121]
- The Internet IP Security Domain of Interpretation for ISAKMP - RFC 2407 [122]
- The OAKLEY Key Determination Protocol - RFC 2412 [123]
- The Internet Key Exchange (IKE) - RFC 2409 [124]

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

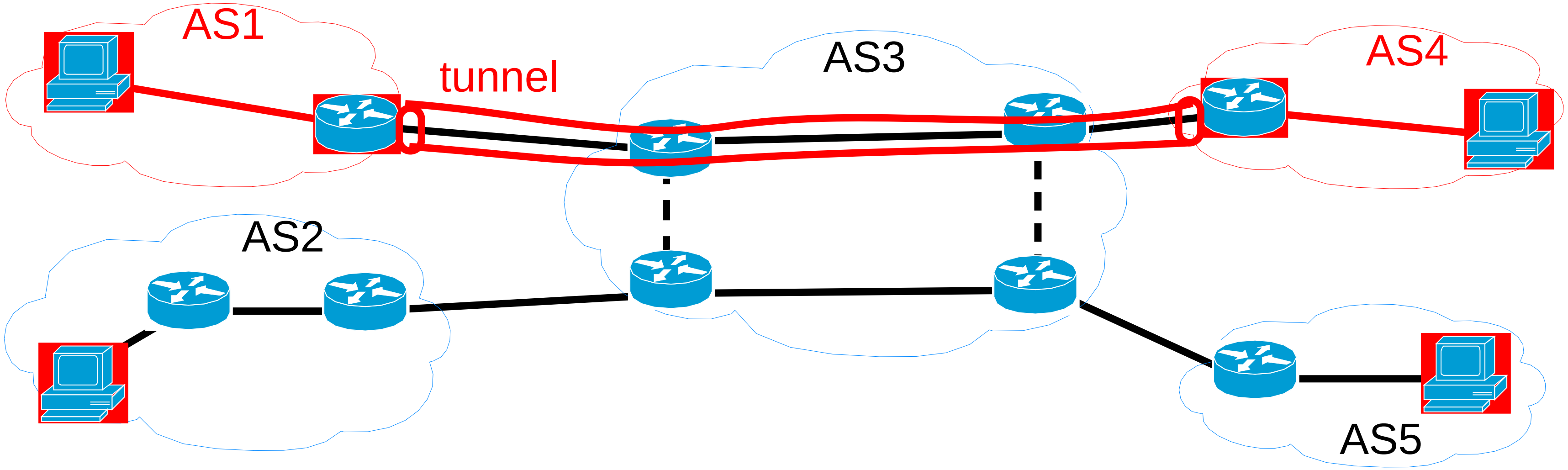
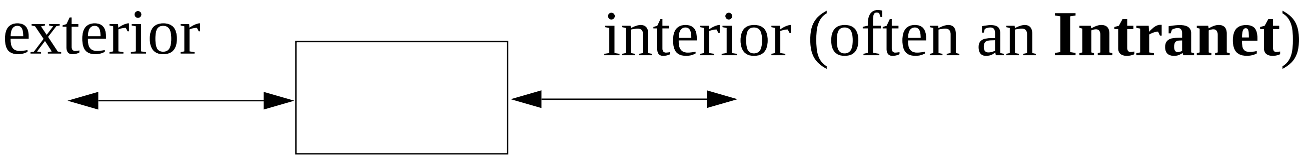


Figure 131: IPSec usage
red = secure, black = unsecure

Firewalls



exterior

interior (often an **Intranet**)

Figure 132: 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**.

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.

Firewall Design

apply basics of security:

- least privilege:
  - don’t make hosts do more than they have to (implies: specialize servers)
  - use minimum privileges for the task in hand
- fail safe
  - even if things break it should not leave anything open
- defence in depth
  - use several discrete barriers - don’t depend on a single firewall for all security
- weakest links
  - know the limitations of your defences - 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!

Proxy Access Through A Firewall

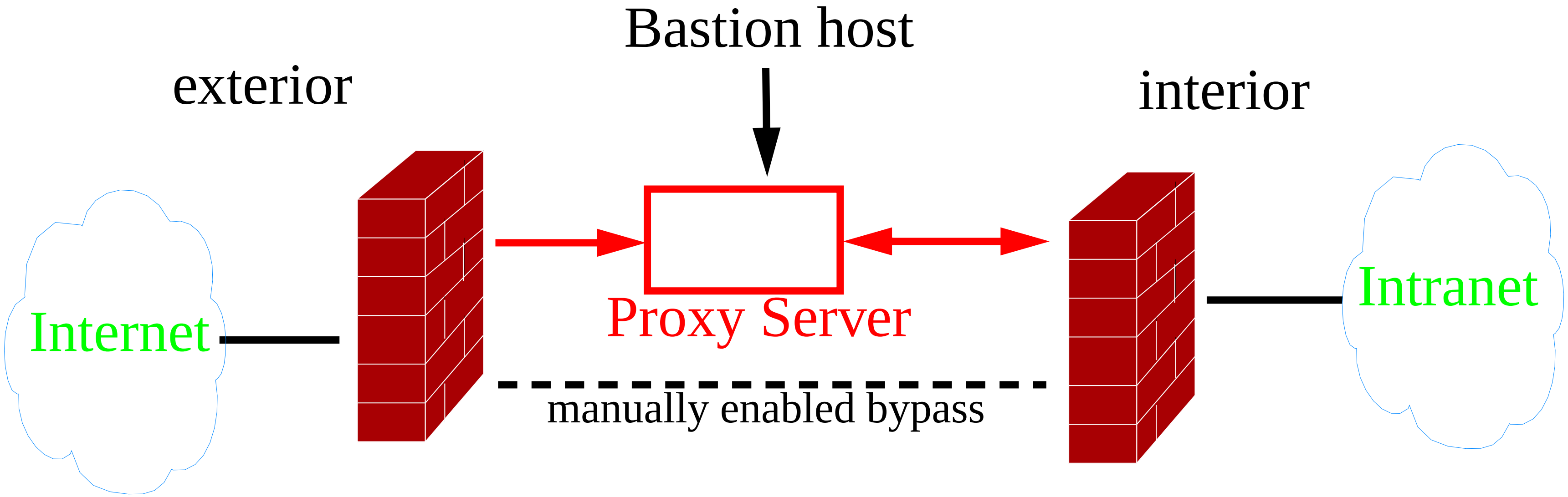


Figure 133: Firewall and internet gateway

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

SOCKs

Permeo Technologies, Inc.’s SOCKS *http://www.socks.nec.com/*

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: [133] and [134]

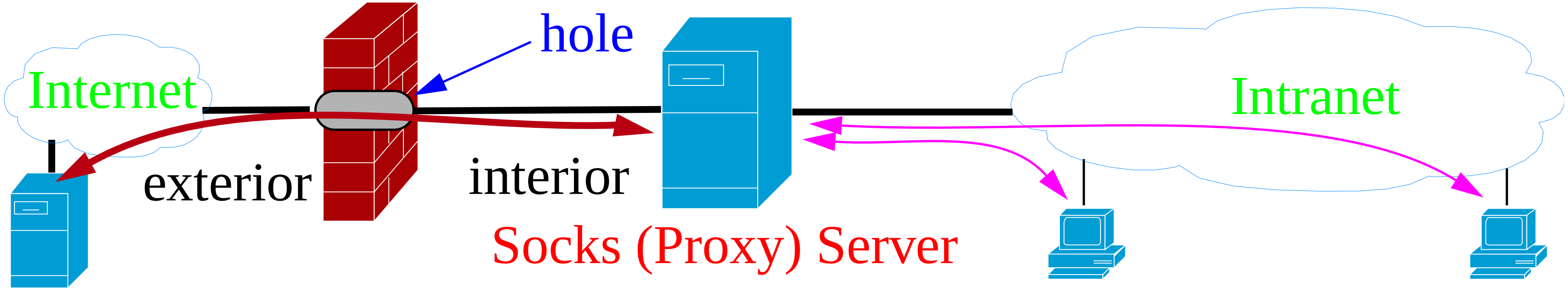


Figure 134: Firewall and internet gateway

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.

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.

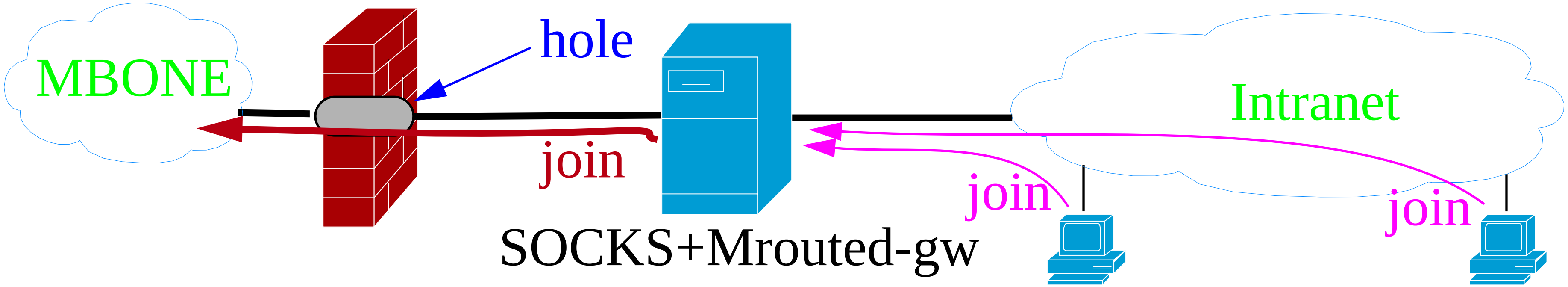


Figure 135: Firewall and internet gateway

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." [135]

U.S. DOE CIAC’s Network Security Tools [136]

- 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

- **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
- **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

The Network Mapper (NMAP)

Network Mapper (NMAP) http://www.insecure.org/nmap/

- (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://www.insecure.org/nmap/nmap_documentation.html also has a link to "Remote OS detection via TCP/IP Stack FingerPrinting" by Fyodor <fyodor@dhp.com> (www.insecure.org), October 18, 1998 - a means of identifying which OS the host is running by noting its TCP/IP behavior.

Network Address Translation

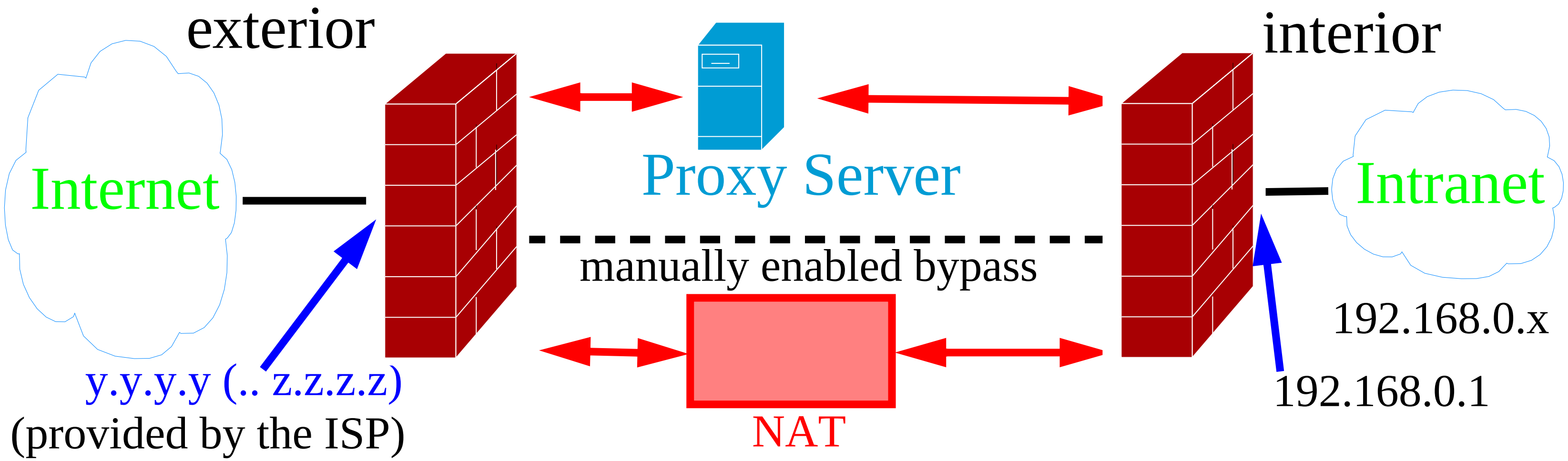


Figure 136: Example of a Firewall with NAT

NAT maps IP addresses on the inside to one or more addresses on the outside and vice versa. See RFC 3022 [146] and RFC2766 [147]

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.

Demilitarized zone (DMZ)

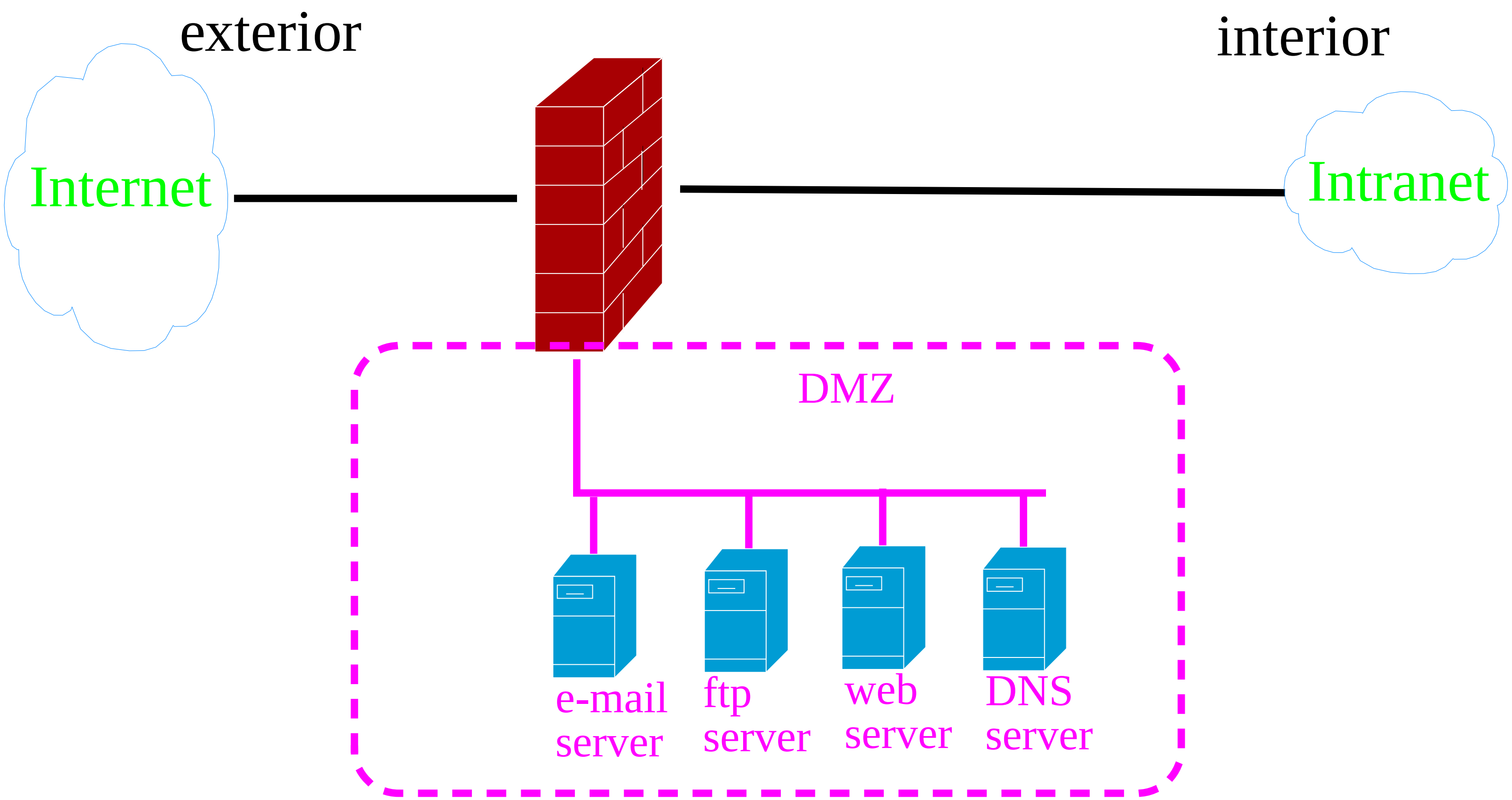


Figure 137: Example of a Firewall with a DMZ

Note that the various services may also be in different DMZ (see for example fogure 4 page 90 of [137]

Network Security Exercises

You will find a nice set of exercises by Ramesh Govindan at USC’s ISI for Kerberos, S/Key, and firewalls at: *http://www.isi.edu/~govindan/cs558/netsec/index.html*

Note that you should **not** use their machines for these exercises, but I think you will find this useful reading.

Security Organizations and Companies

Computer Emergency Response Team (CERT ®) Coordination Center [127]

- 1988 - Computer Emergency **Response** Team
- 2003 - Computer Emergency **Readiness** Team [131]

Addionally, 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 [131], …
- The European Computer Security Incident Response Team Network http://www.ecsirt.net/

Forum of Incident Response and Security Teams (FIRST), now: 170 members[128]

NIST Computer Security Resource Center [129], Swedish Defense Material Administration, Electronics Systems Directorate [130], …

Summary

This lecture we have discussed:

- Private networks
- IPSec
- Firewalls

Further information

[118]IETF Security Area http://sec.ietf.org/

[119]S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406, November 1998 http://www.ietf.org/rfc/rfc2406.txt

[120]S. Kent and R. Atkinson, "IP Authentication Header", IETF RFC 2402, November 1998 http://www.ietf.org/rfc/rfc2402.txt

[121]D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 2408, November 1998 http://www.ietf.org/rfc/rfc2408.txt

[122] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", IETF RFC 2407, November 1998 http://www.ietf.org/rfc/rfc2407.txt

[123] H. Orman, "The OAKLEY Key Determination Protocol", IETF RFC 2412, November 1998 http://www.ietf.org/rfc/rfc2412.txt

[124]D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)", IETF

RFC 2409,November 1998 *http://www.ietf.org/rfc/rfc2409.txt*

[125]J. Linn, “Generic Security Service Application Program Interface, Version 2”, IETF RFC 2078, January 1997, *http://www.ietf.org/rfc/rfc2078.txt*

[126]J. Wray, “Generic Security Service API Version 2 : C-bindings”, IETF RFC 2744, January 2000 *http://www.ietf.org/rfc/rfc2744.txt*

[127] Computer Emergency Response Team *http://www.cert.org/*

[128]Forum of Incident Response and Security Teams *http://www.first.org/*

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

[130]Swedish Defense Material Administration *http://www.fmv.se/*

[131]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

[132]Centre d’Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA) *http://www.certa.ssi.gouv.fr/*

[133]M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, “SOCKS Protocol Version 5”, IETF RFC 1928, March 1996

http://www.ietf.org/rfc/rfc1928.txt

[134]P. McMahon, “GSS-API Authentication Method for SOCKS Version 5”, IETF RFC 1961, June 1996 *http://www.ietf.org/rfc/rfc1961.txt*

[135] Postfix *http://www.postfix.org*

[136]U.S. DOE’s Computer Incident Advisory Capability

http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html

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

[138]Charlier Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a PUBLIC World*, Prentice-Hall, 1995, ISBN 0-13-061466-1

[139]Simson Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, 1995 ISBN 1-56592-098-8

[140]Internet Mail Consortium, "S/MIME and OpenPGP", Oct 15, 2004

http://www.imc.org/smime-pgpmime.html

Firewalls

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

[142]D. Brent Chapman and Elizabeth Zwicky, *Building Internet Firewalls*, O'Reilly, 1995,ISBN: 1-56592-124-0

[143]Tony Mancill, *Linux Routers: A Primer for Network Administrators* Prentice-Hall, 2001, ISBN 0-13-086113-8.

[144]Firewalls mailing list *http://www.isc.org/index.pl?/ops/lists/firewalls/*

[145]Computer Security Institute (CSI) at *http://www.gocsi.com/*

NAT

[146] P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator (Traditional NAT)”, IETF RFC 3022, January 2001

http://www.ietf.org/rfc/rfc3022.txt

[147]G. Tsirtsis and P. Srisuresh, “Network Address Translation - Protocol Translation (NAT-PT)”, IETF RFC 2766, February 2000

http://www.ietf.org/rfc/rfc2766.txt