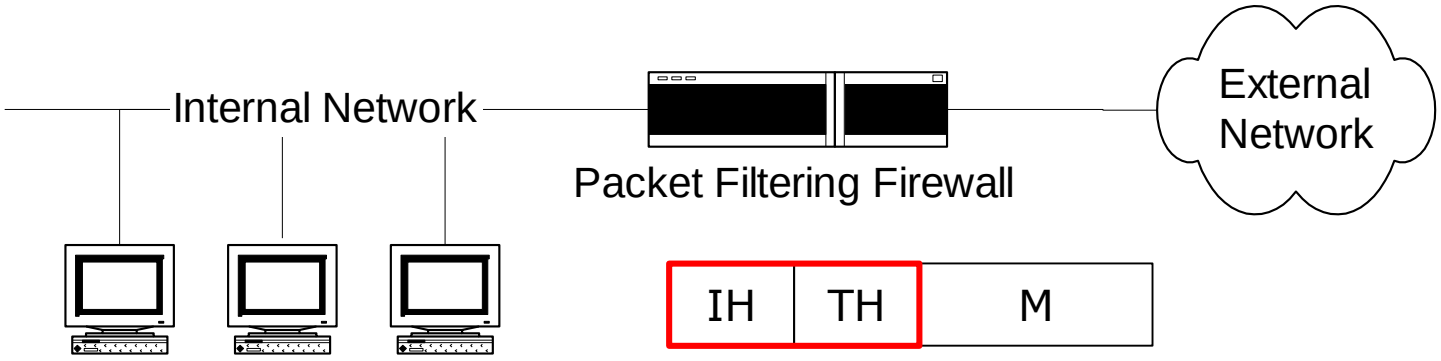
Chap. 12 Firewalls

- Packet Filter
- Application Gateway
- Firewall Architecture

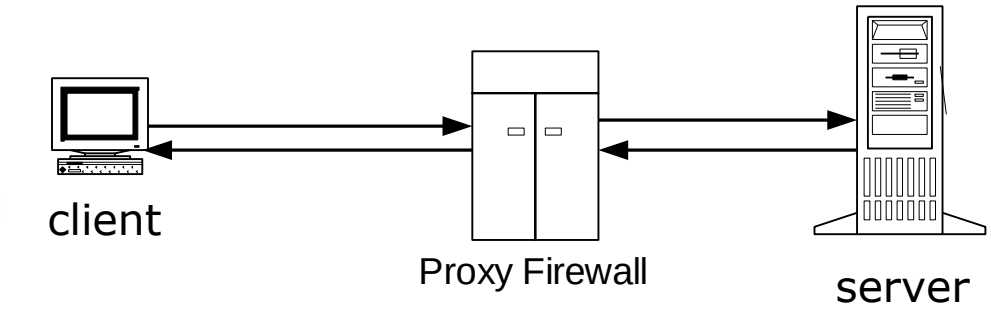
Types of Firewalls

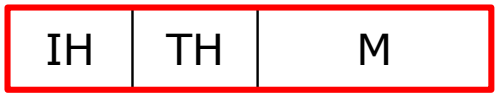
- Packet Filtering firewall
  - Operate on transport and network layers of the TCP/IP stack



Types of Firewalls

- Application Gateways/Proxies
  - Operate on application layers of the TCP/IP stack





Packet Filtering Firewalls

- Operate on transport and network layers of the TCP/IP stack
- Decides what to do based on the transport and network layer information:
  - Protocol type (TCP,UDP,ICMP)
  - Source and destination IP address
  - source and destination ports
  - Flags: (e.g.) SYN, FIN, etc.
  - ICMP message type/code
  - Various IP/TCP options such as packet size, fragmentation etc.

Packet Filtering Firewall: Terminology

- Stateless Firewall:
  - do not maintain state info on a packet stream
  - firewall makes a decision on a packet by packet basis
- Stateful Firewall :
  - firewall keeps state information about transactions (connections)
- NAT - Network Address Translation
  - Translates public IP address to private IP address on a private LAN

Packet Filtering Firewall: Functions

- Forward the packet(s) on to the intended destination
- Reject the packet(s) and notify the sender (ICMP dest. unreach./admin. prohibited)
- Drop the packet(s) without notifying the sender
- Log accepted and/or denied packet information
- NAT - Network Address Translation

Packet Filtering Firewall: Disadvantages

- Filters can be difficult to configure
  - it's not always easy to anticipate traffic patterns and create filtering rules to fit
- Filter rules are sometimes difficult to test
- Packet filtering can degrade router performance
- Attackers can "tunnel" malicious traffic through allowed ports on the filter

Application Gateway (Proxy Server)

- Operate at the application protocol level (http, ftp, smtp, telnet, ...)
- Application gateways understand the appl. protocol and is configured to allow or deny specific protocol operations
- Typically, proxy servers sit between the client and actual server: both the client and server talk to the proxy rather than directly with each other

Application Gateway : Disadvantages

- Requires modification to client software application
- Some protocols aren't supported by proxy servers: (e.g.) smtp, pop3
- Some proxy servers may be difficult to configure and may not provide all the protection you need

Firewall Hardware/Software

- Dedicated hardware/software application which filters traffic passing through the multiple network interfaces

- Firewall functionality in OS
  - a firewall software package which filters incoming and outgoing traffic across the interfaces within kernel
  - Linux: firewall daemon(firewalld) and netfilter kernel firewall module

Packet Filtering Firewall Software for Unix

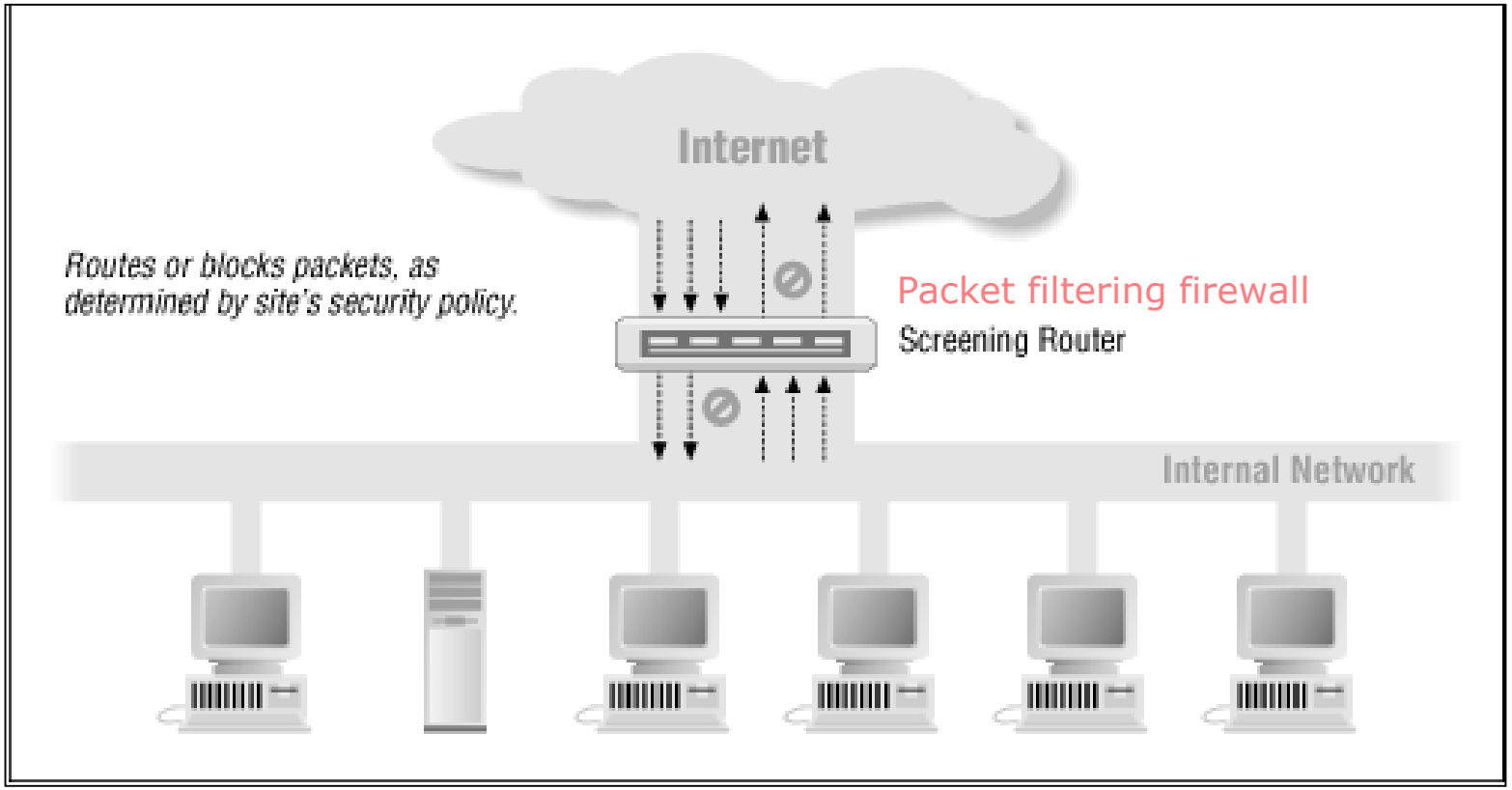
- IPTables (netFilter) - Linux 2.4.x kernels
  - stateful firewall module for Linux
  - http://netfilter.kernelnotes.org
- IPFilter - For Solaris, HP-UX, IRIX, BSD
  - http://coombs.anu.edu.au/ipfilter/

Application Layer (Proxy) Firewalls

- TIS FWTK - Firewall Toolkit
  - http://www.tis.com/
- SOCKS – transport level proxy server
  - http://www.socks.nec.com
- Squid - HTTP, SSL, FTP proxy cache

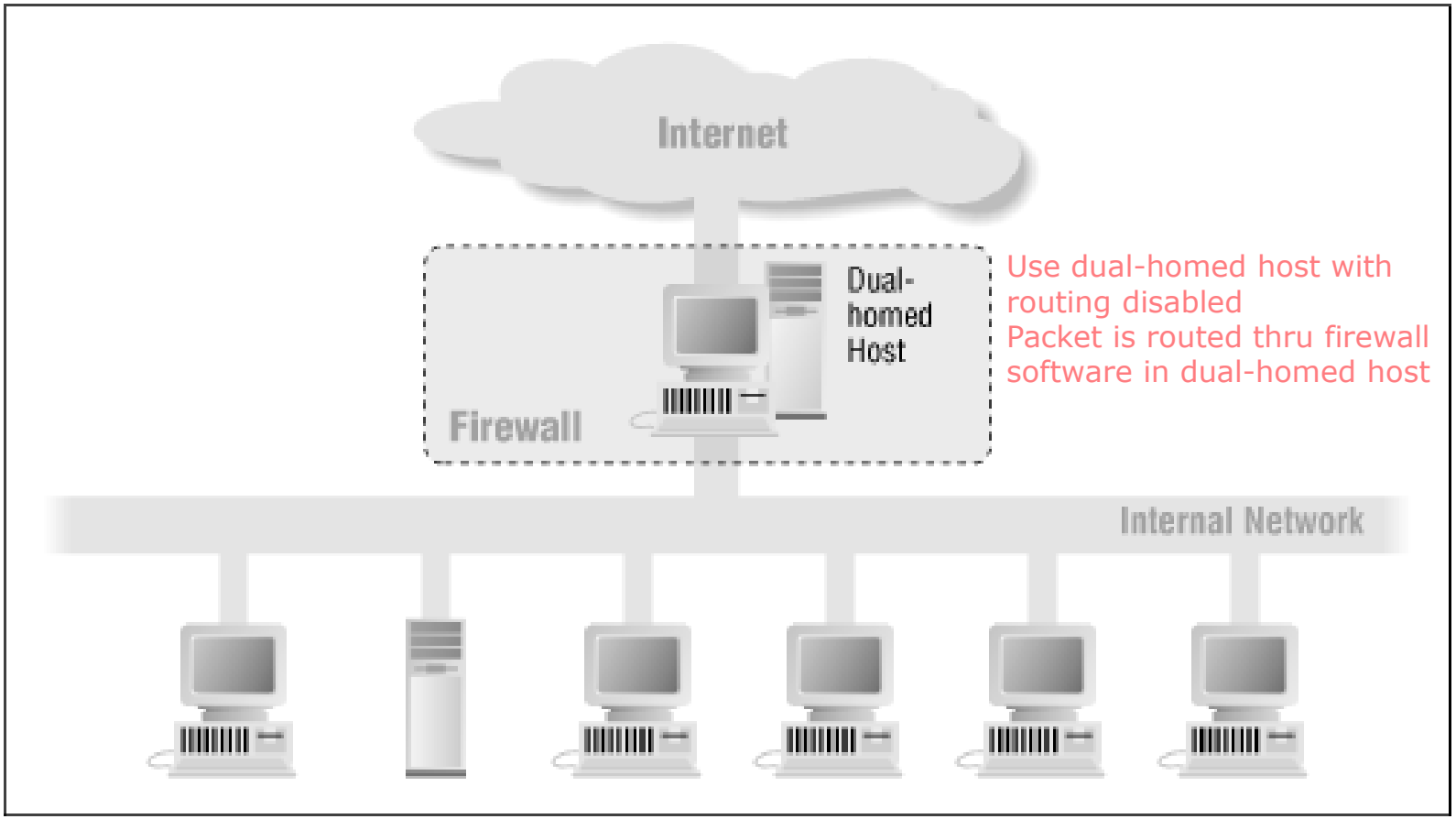
Firewall Architecture

- Firewall using a screening router



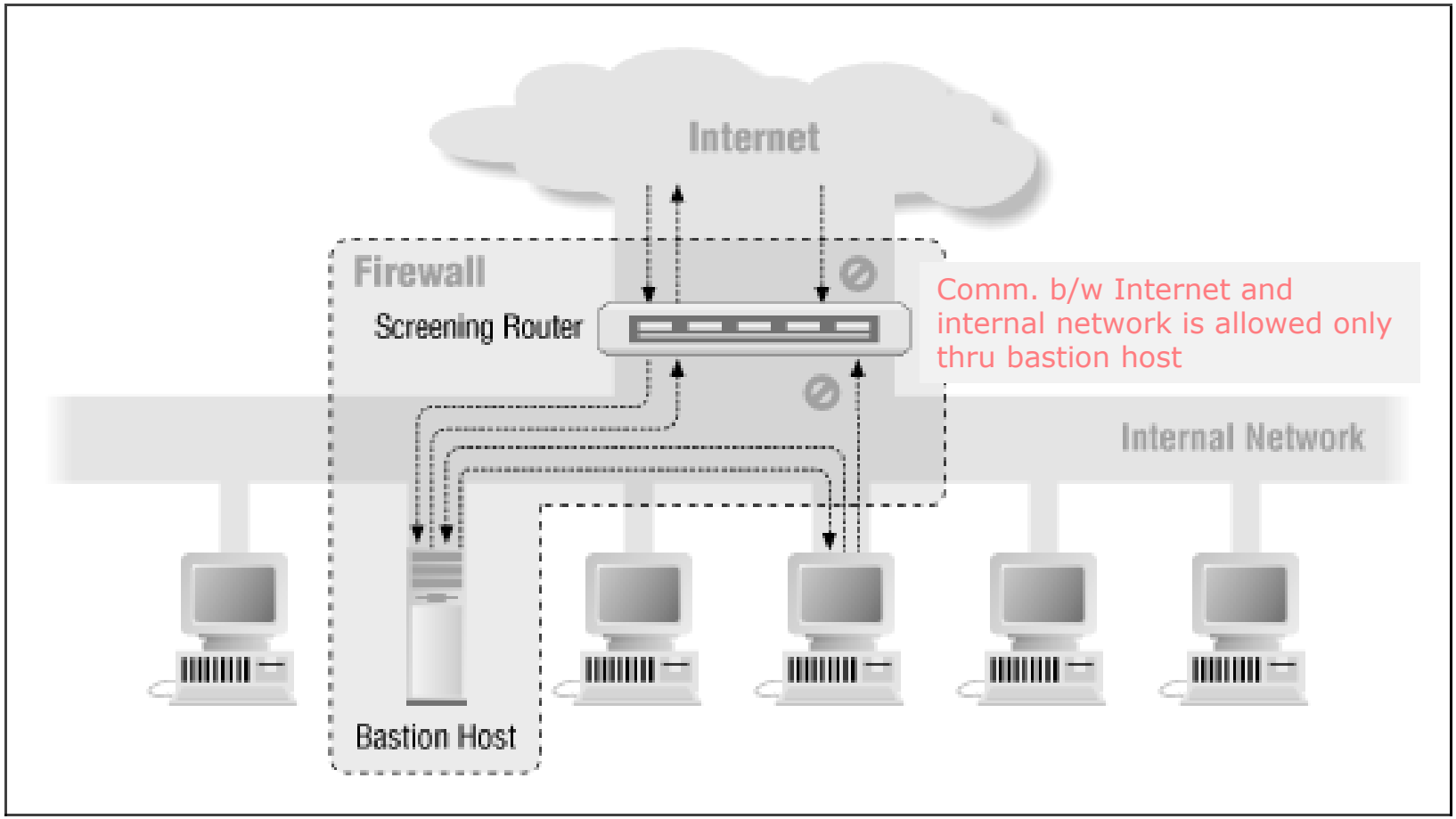
Firewall Architecture

- Dual-homed host architecture



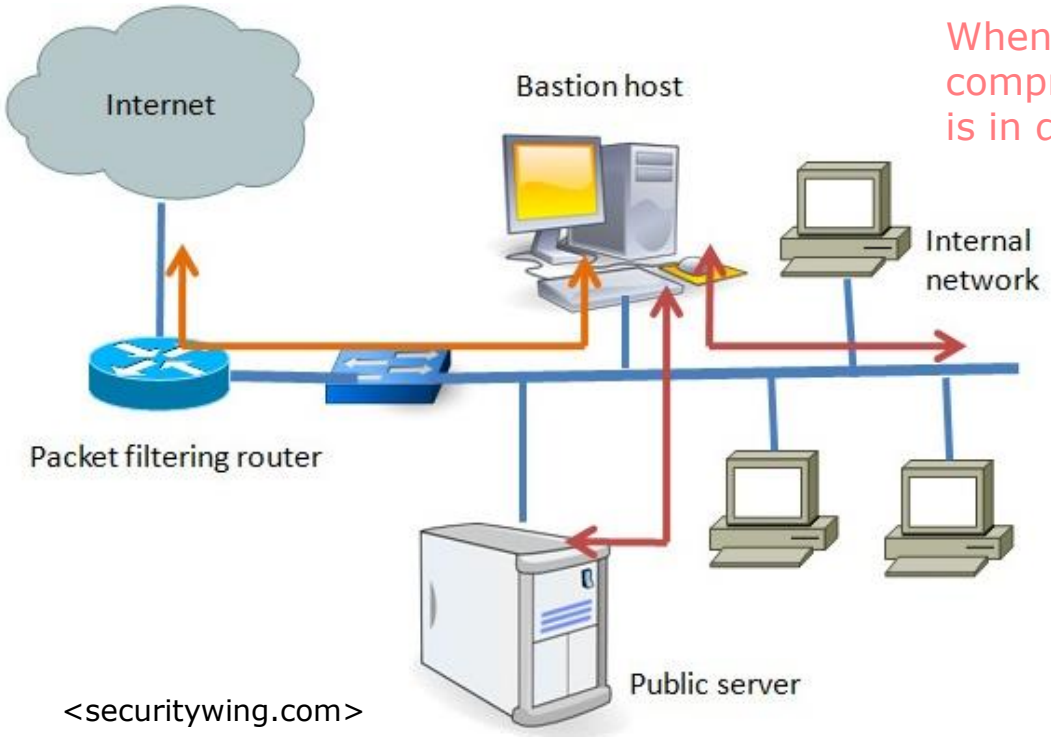
Firewall Architecture

- Screened host architecture



Firewall Architecture

- Screened host architecture
  - Bastion host with single homed host

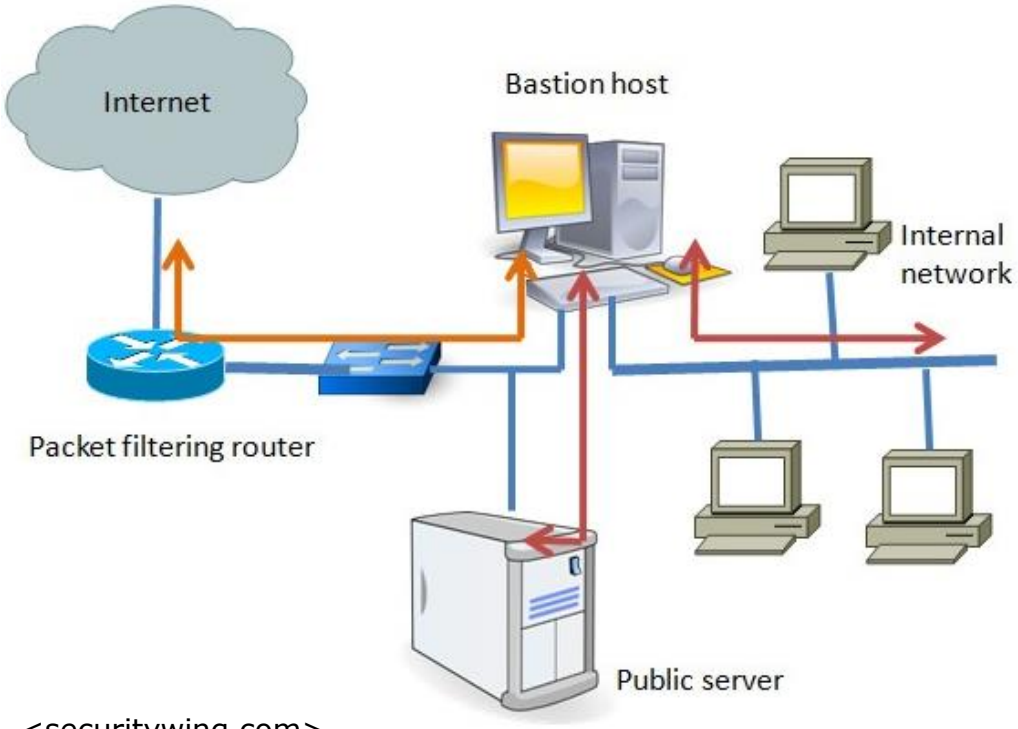


<securitywing.com>

When packet filtering router is compromised, internal network is in danger

Firewall Architecture

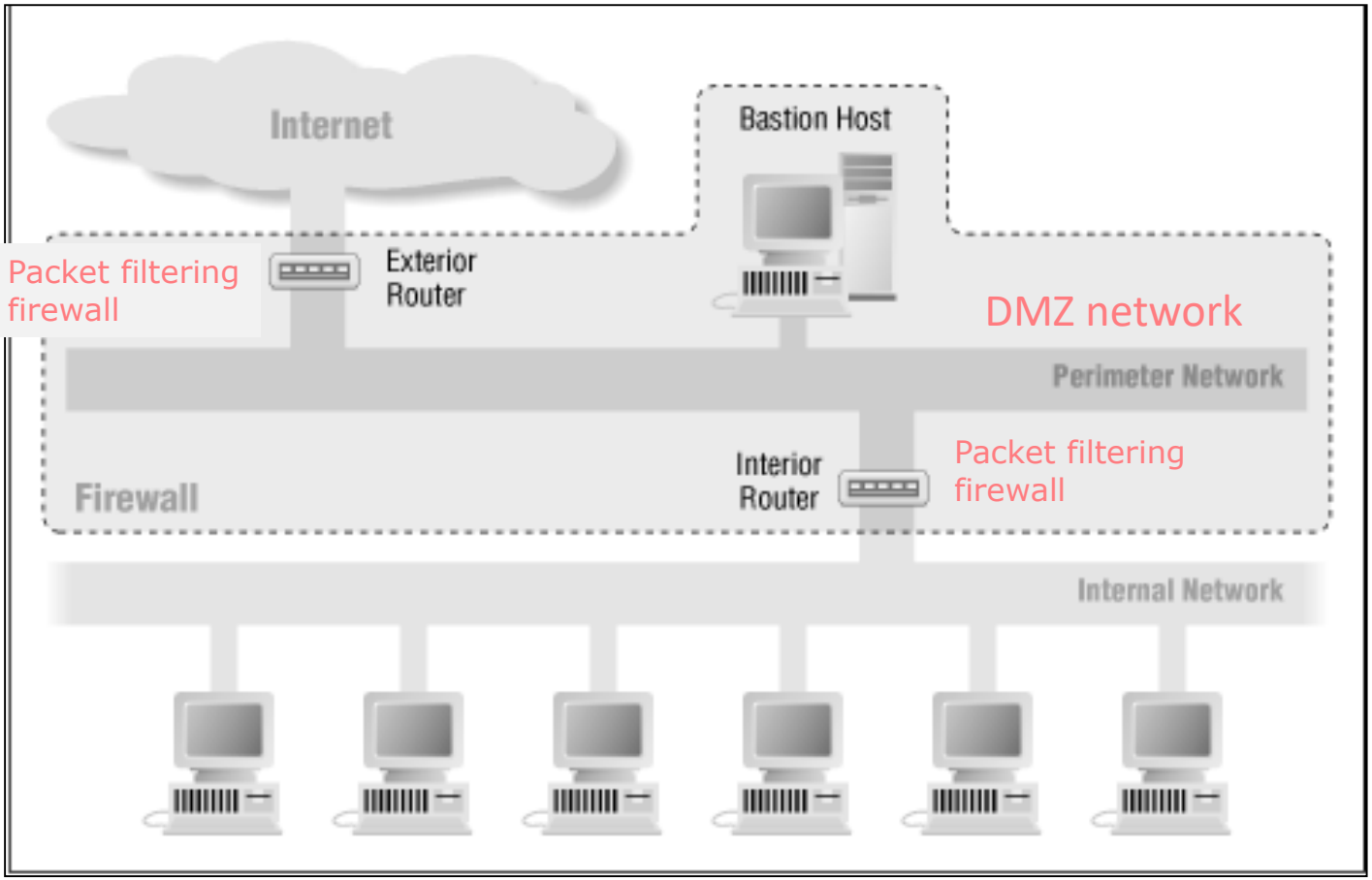
- Screened host architecture
  - Bastion host with dual homed host



<securitywing.com>

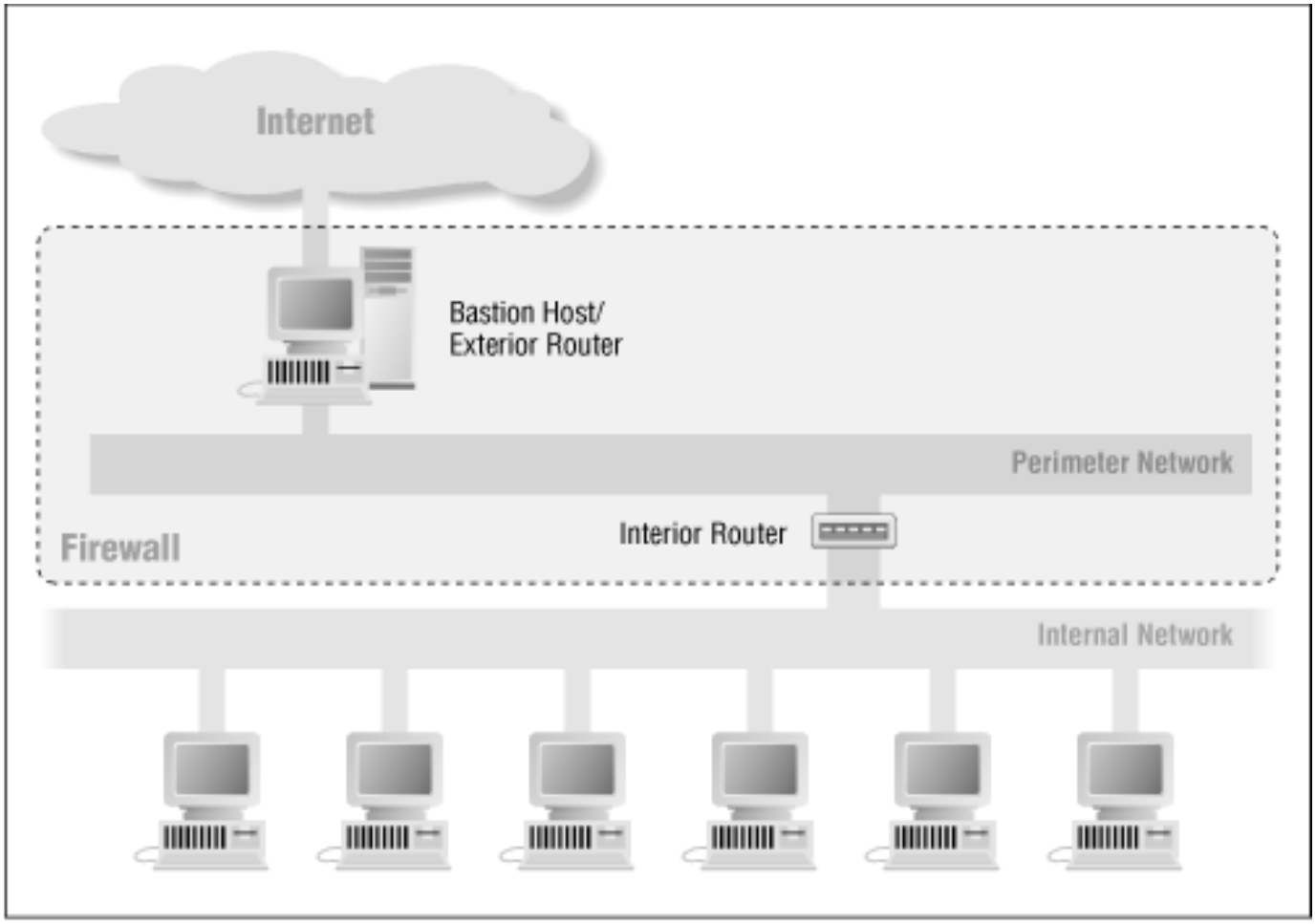
Firewall Architecture

- Screened subnet architecture



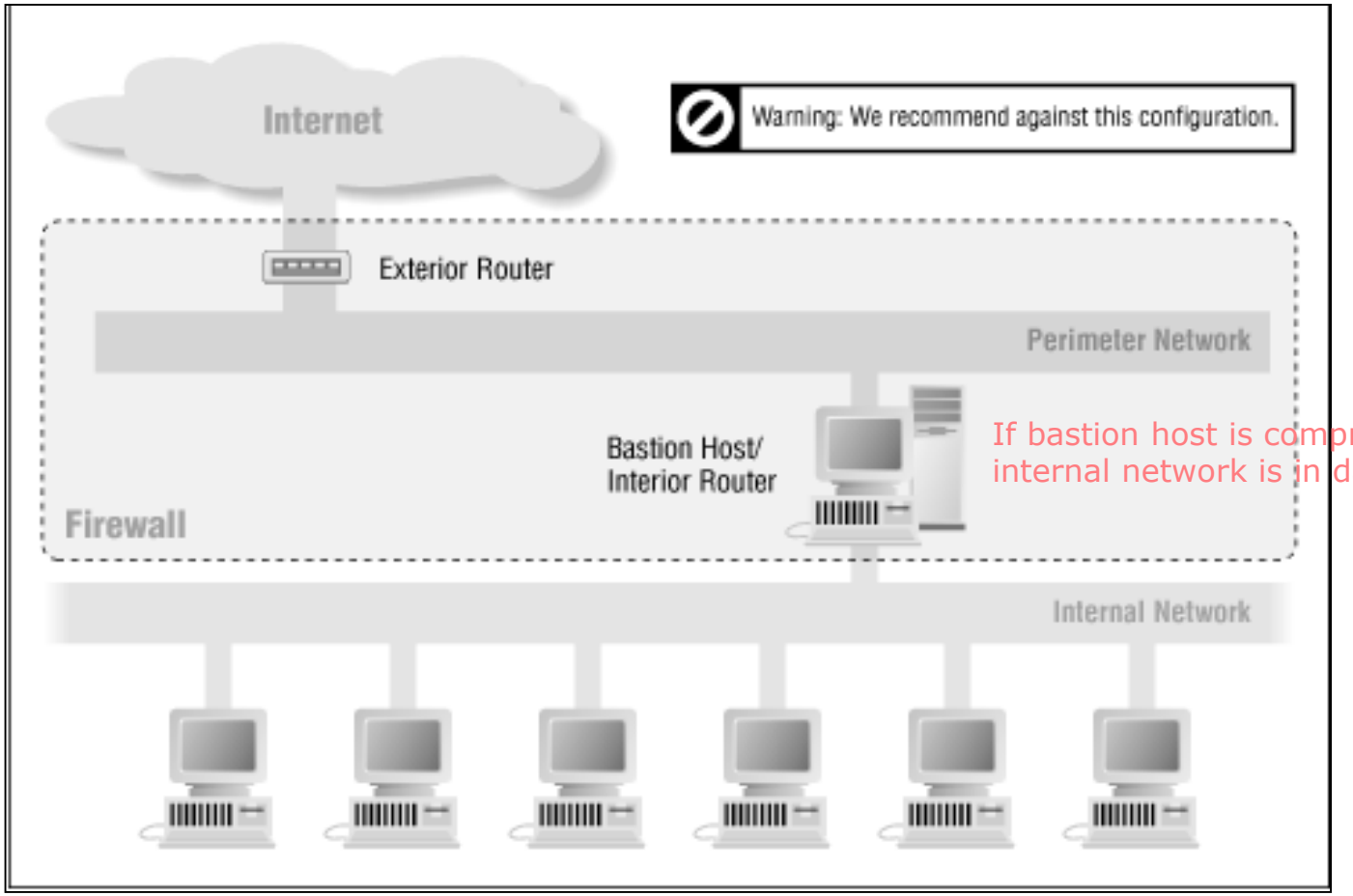
Firewall Architecture

- Firewall using a combined bastion host and exterior router



Firewall Architecture

- Firewall using a combined bastion host and interior router



If bastion host is compromised, internal network is in danger

Firewall Architecture

- Firewalls with multiple internal networks (backbone network)