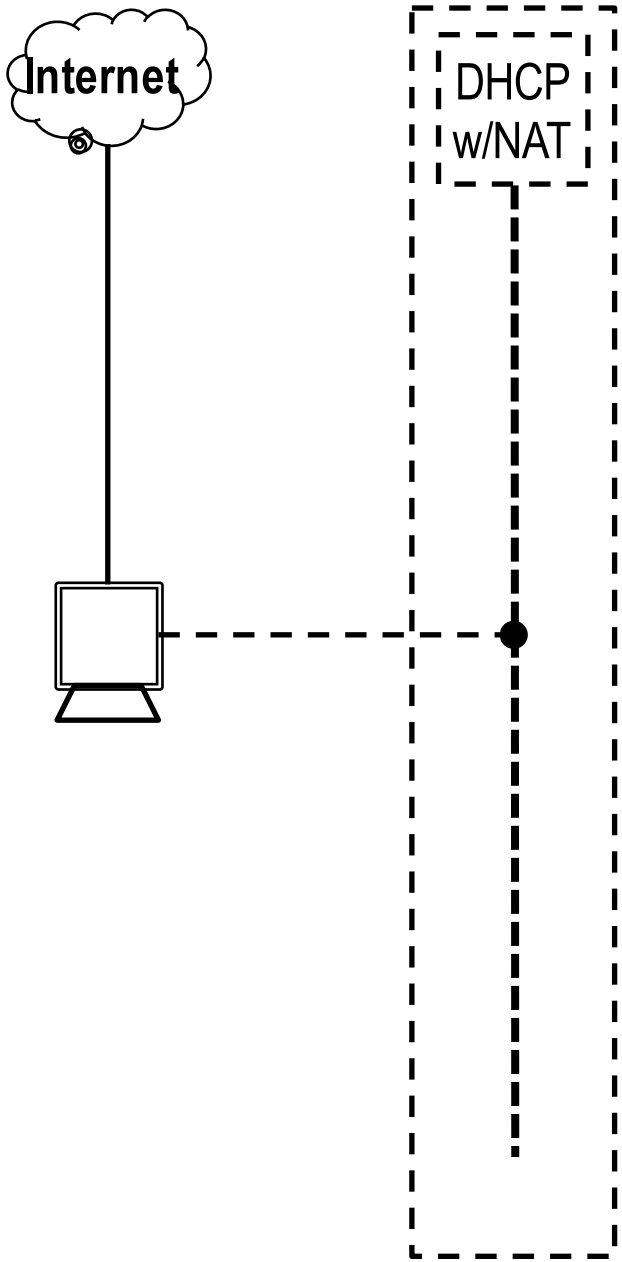
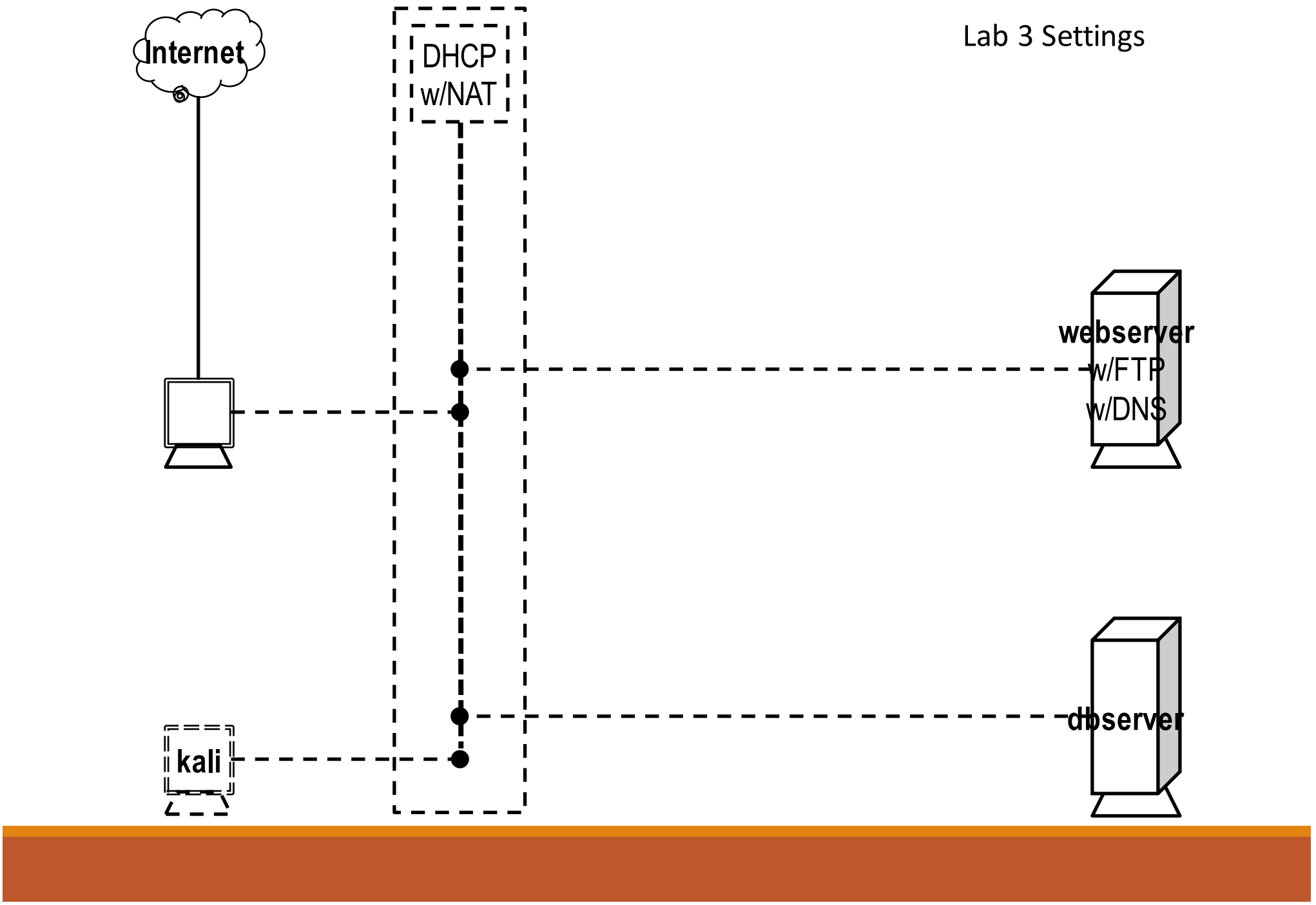
Week 4 – Network Infrastructure Security



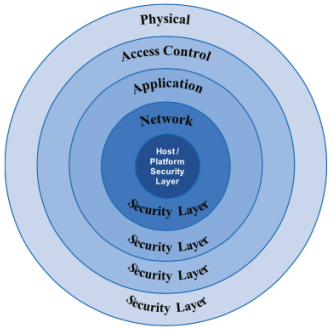
Lab 3 Settings


Lab 3 Settings
Internet
DHCP
w/NAT
webserver
w/FTP
w/DNS
dbserver
kali

Network Security Defense Mechanisms

Network Security Defense Mechanisms

Types of Network Security Defense Mechanisms



2nd or 3rd layer of defense

First layer of defense

Defense = Filtering

Example of multi-tier application infrastructure from "Information Security The Complete Reference, 2nd Edition"

Firewall

Hardware/software used to implement security policies governing the network traffic between networks. (alike a router)

- Stop unwanted network traffic
- Protect information

Types

- Bastion Host
- Packet-filtering
  - Stateful inspection firewall
- Application Proxies
- Transparent Proxies

Firewall – Packet Filtering

Specify packets to filter (discard/reject) during the routing process

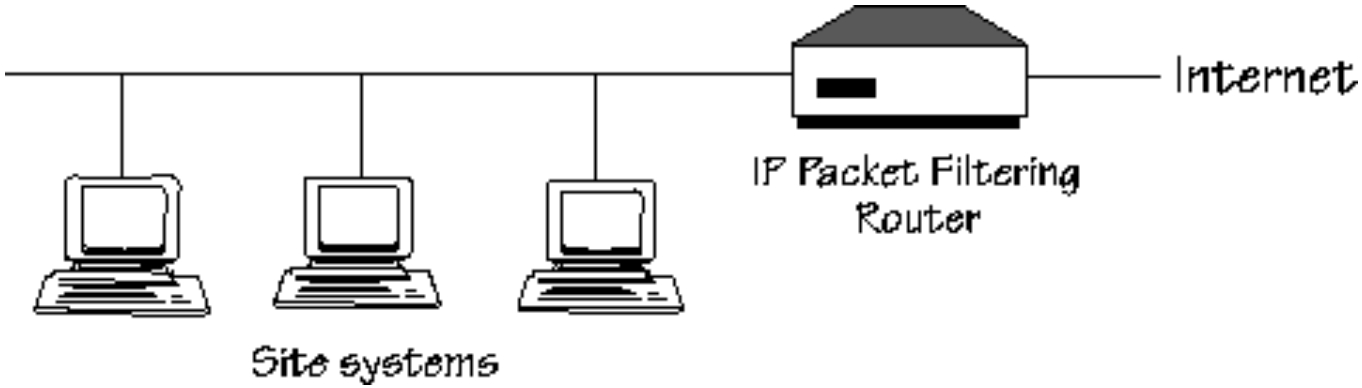
- source/destination ip address
- protocol
- port
- time
- length

Not efficient for dynamic protocol:

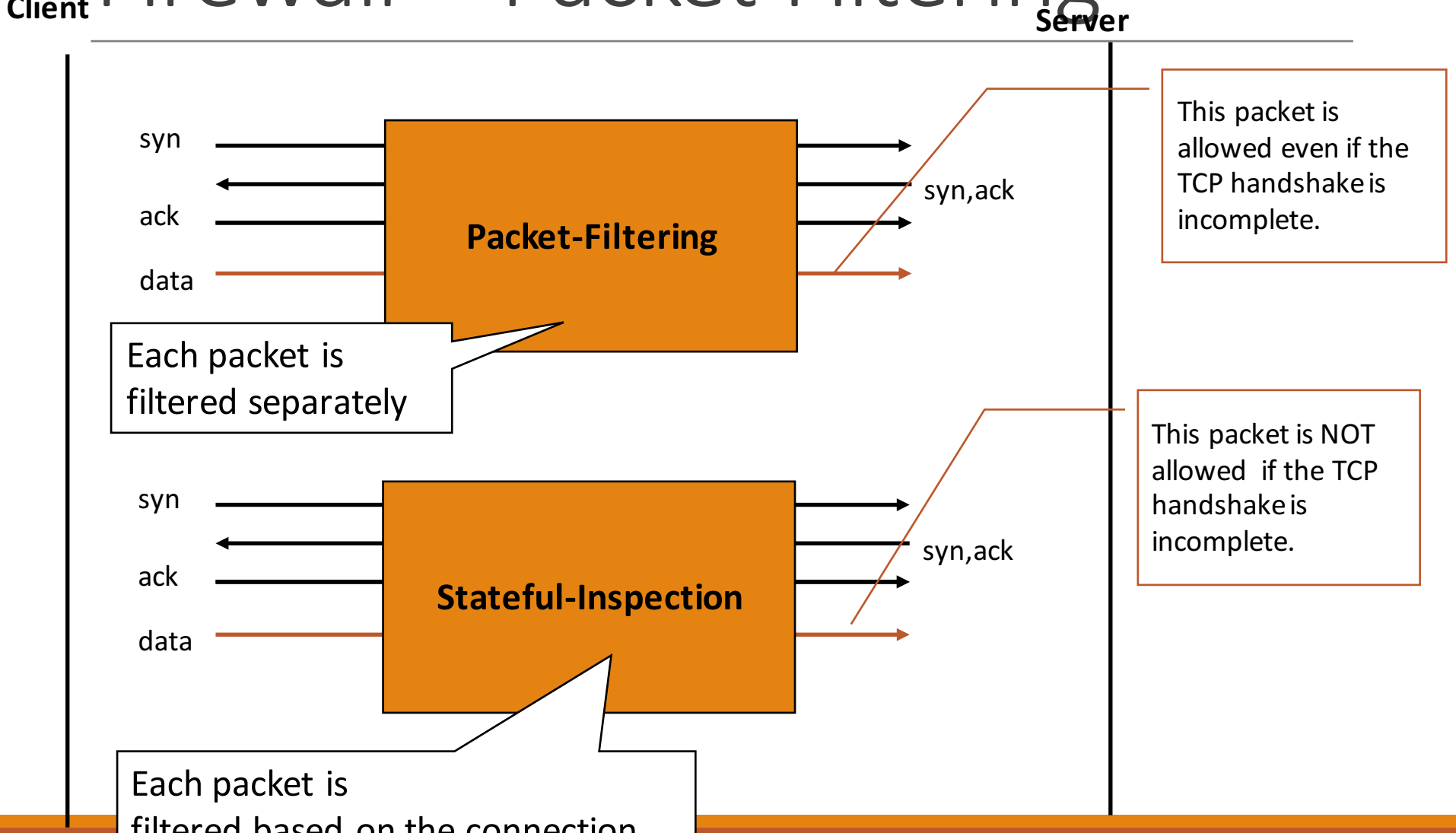
- RPC, FTP, Streaming, etc.

Packet Filter

Using filtering of packets on network level

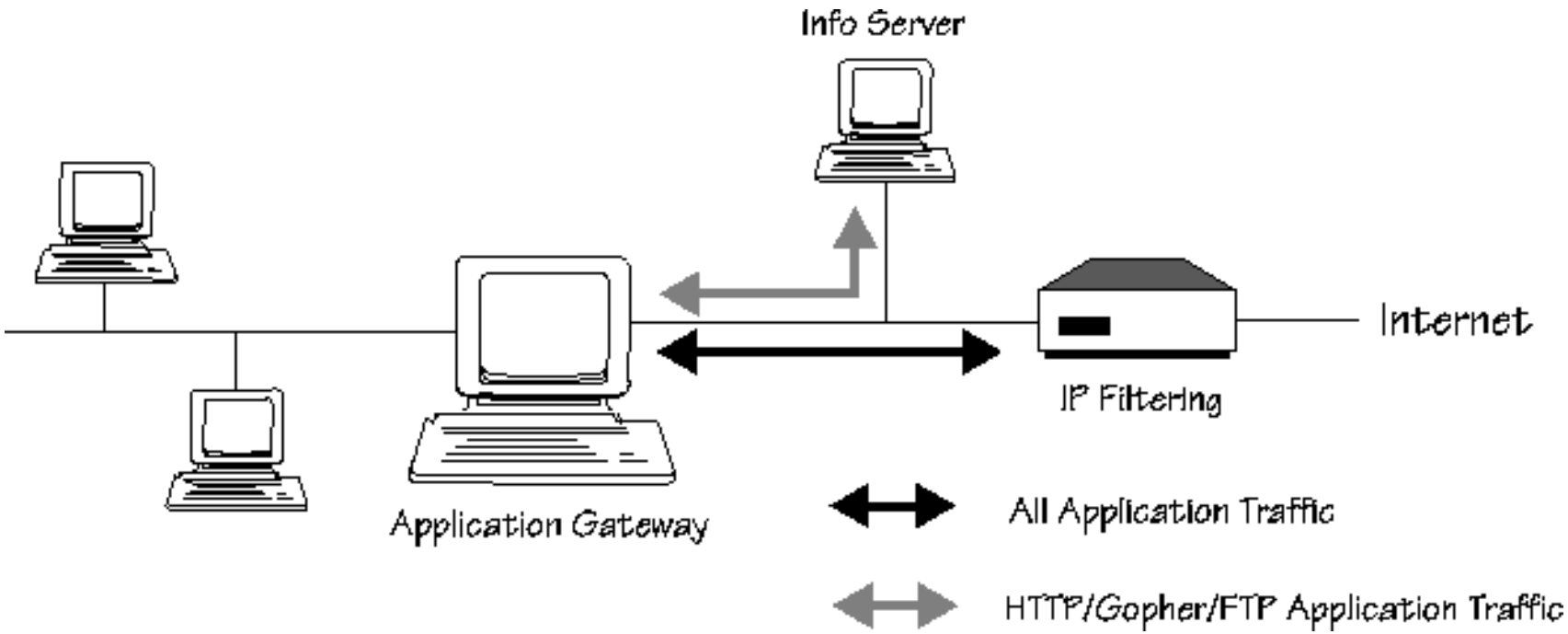


Firewall – Packet Filtering



Bastion Host

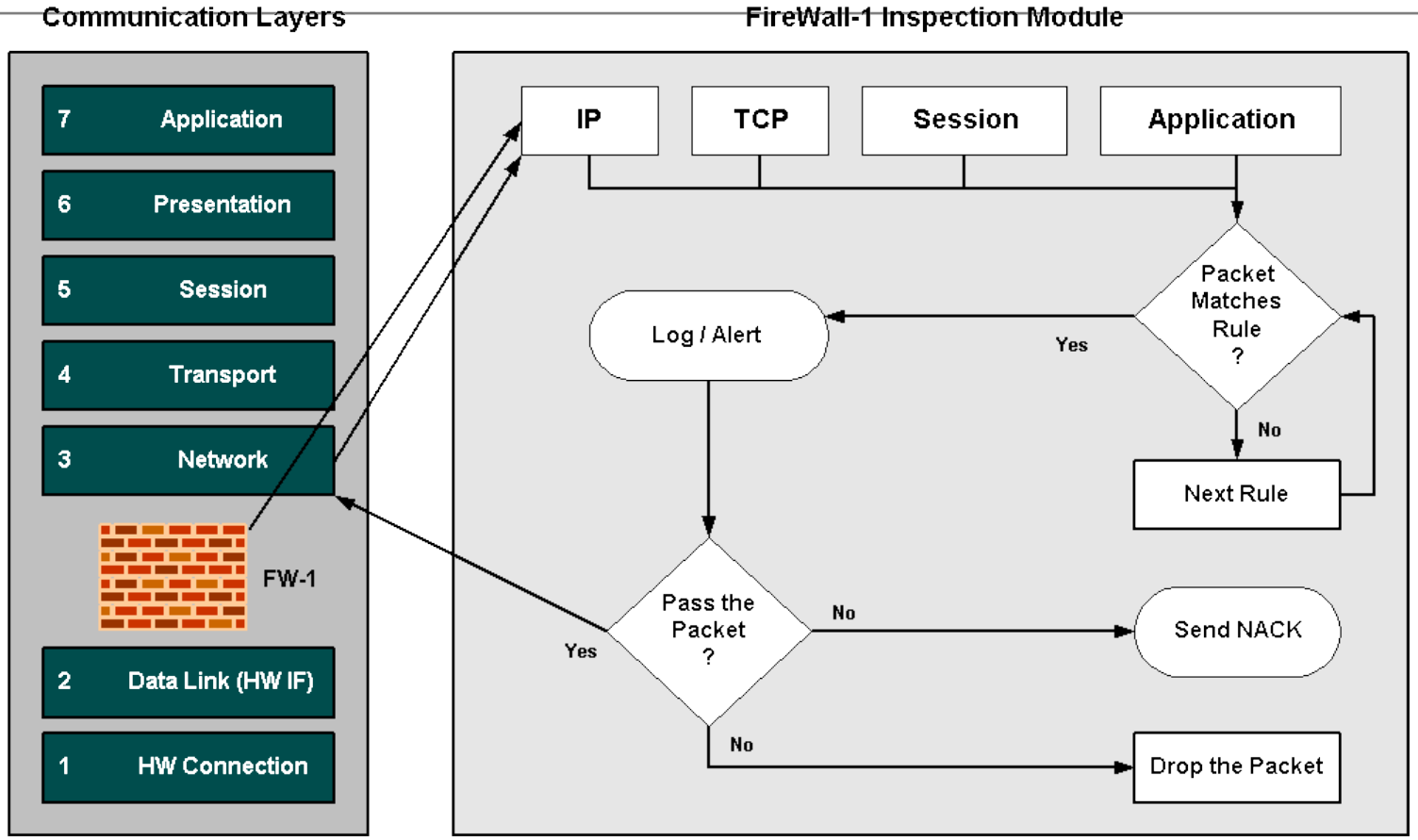
Using a machine as a gateway controlling the packets entrance



Stateful packet filters

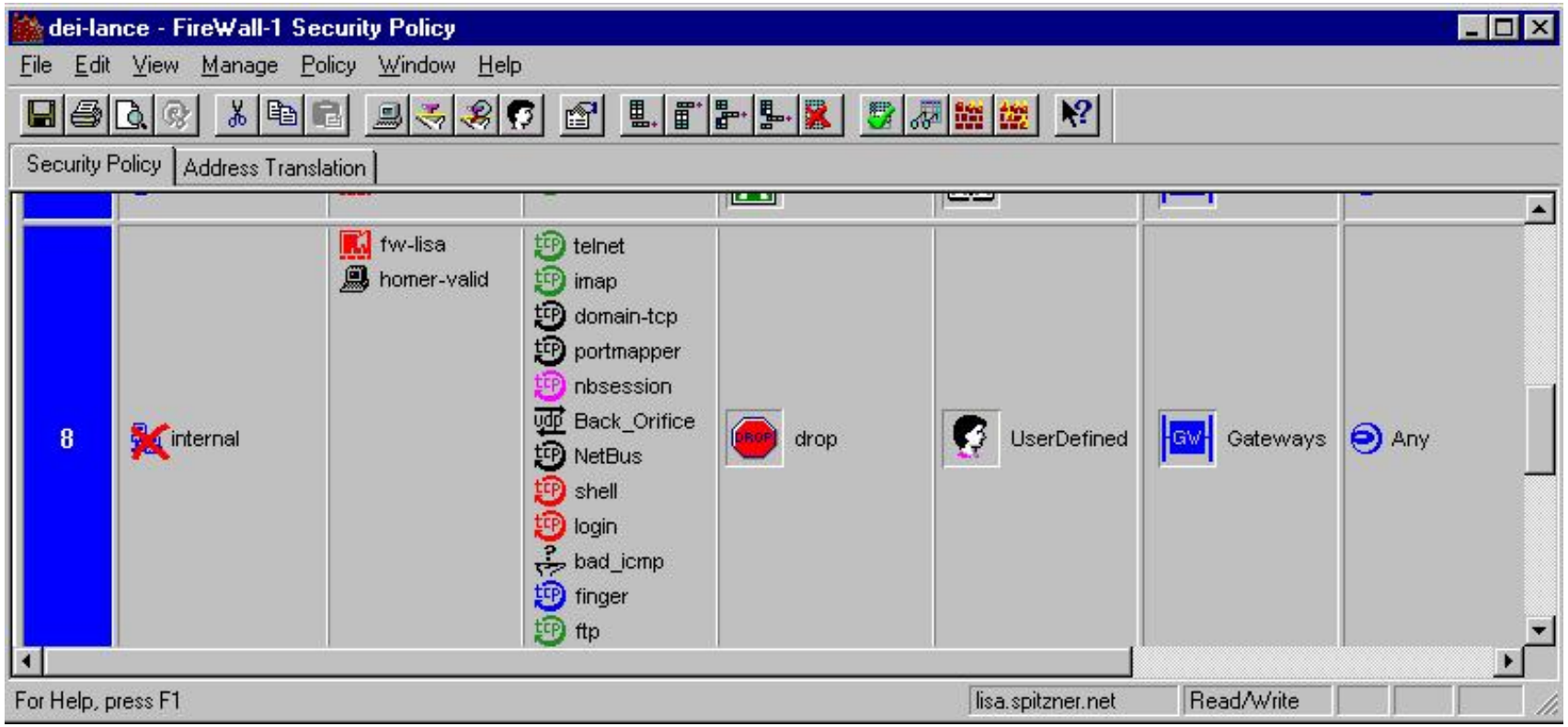
- SPFs track the last few minutes of network activity. If a packet doesn't fit in, they drop it.
- Stronger inspection engines can search for information inside the packet's data.
- SPFs have to collect and assemble packets in order to have enough data.
- Examples: Checkpoint, Cisco PIX, Juniper, ipfilter

Flow of Packets through Inspect Engine



The Inspection Module is located inside the Operating System Kernel - between the device driver and the IP stack.

Firewall



Application proxy

- FW transfers only acceptable information between the two connections.
- The proxy can understand the protocol and filter the data within.
- Examples: Palo Alto Firewall

Firewall – Application Proxy

Connect to the protected servers on behalf of the client

- Service is provided by processes that maintain complete TCP connection state and sequencing
- Often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Firewall – Application Proxy

Benefits

- No direct connections between client and server
- Support user-level authentication
- Analyze application commands inside the payload portion of data packets (WHY?)
- Have comprehensive logs of traffic and specific activities.

Drawbacks

- Perform slower
- Is resource-demanding
- Requires client configuration

Firewall - Circuit level Proxy

The idea of circuit level gateway is fundamentally different from packet filtering.

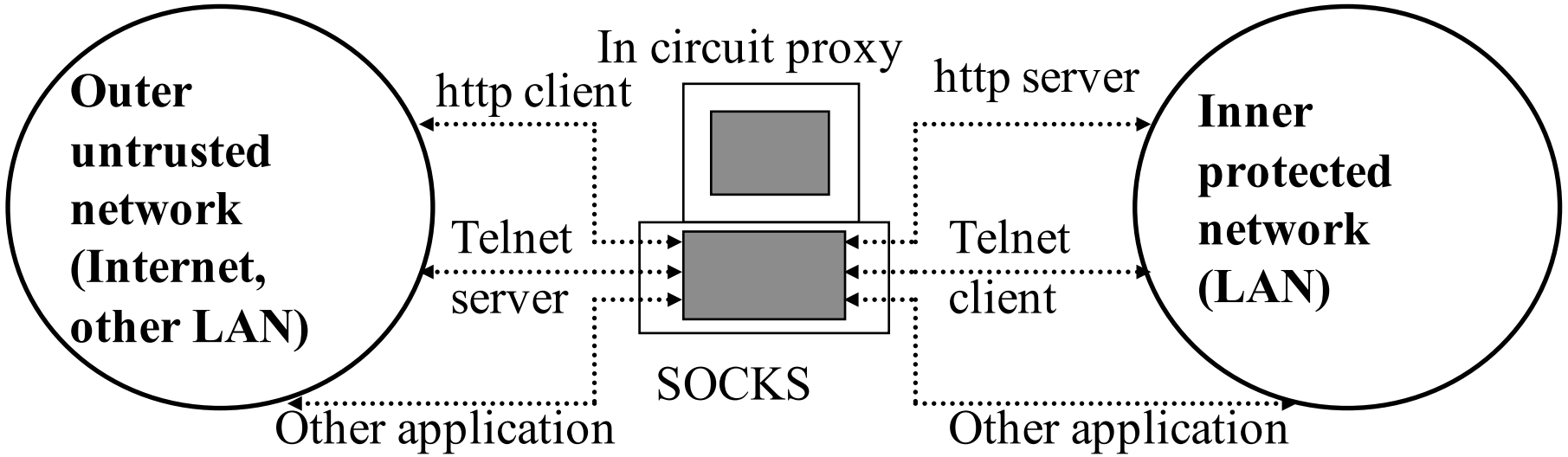
Operates at Transport Layer

- it takes a TCP connection request from the client, authenticates and authorizes the client, and establishes a second TCP connection to the origin server on the client's behalf
- after having successfully established this second TCP connection, gateway simply relays data forth and back between the two connections

Implementation by SOCKS

- SOCKS follows a customized client approach (it requires customization and modification to client software, no change is usually required to user procedures)

Firewall - Circuit level gateway (in circuit proxy)



Firewall Architecture

Firewall Architecture

Dual-homed screening router

Dual-homed host

Screened host

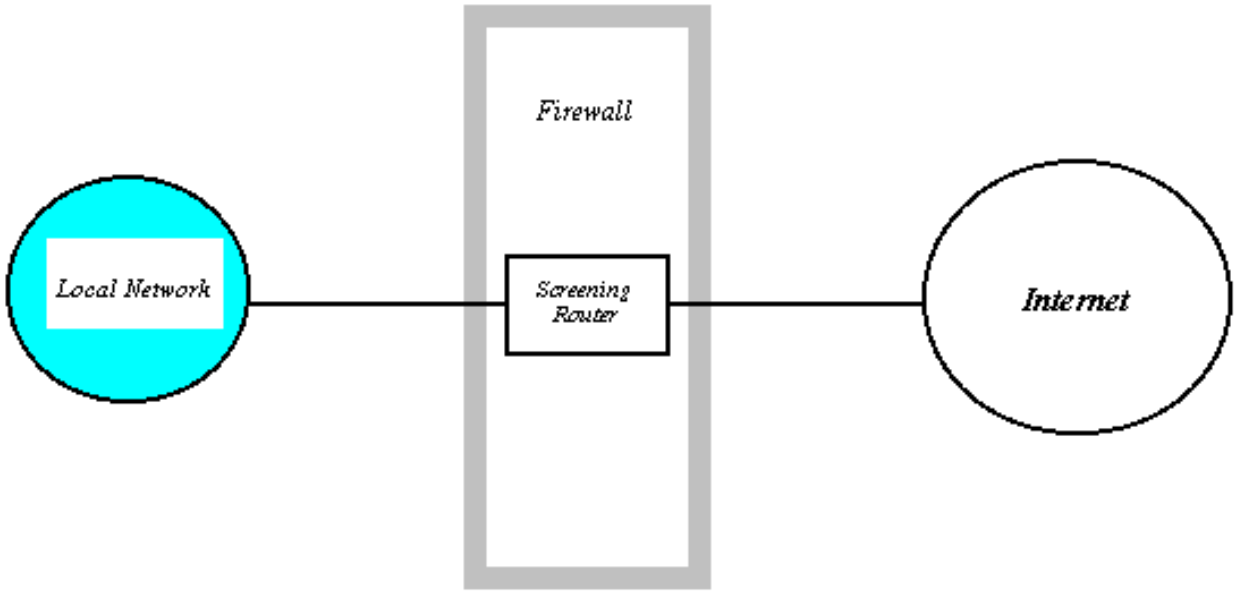
Screened subnet

Multi-homed

Dual-homed screening router

Direct connection to internet

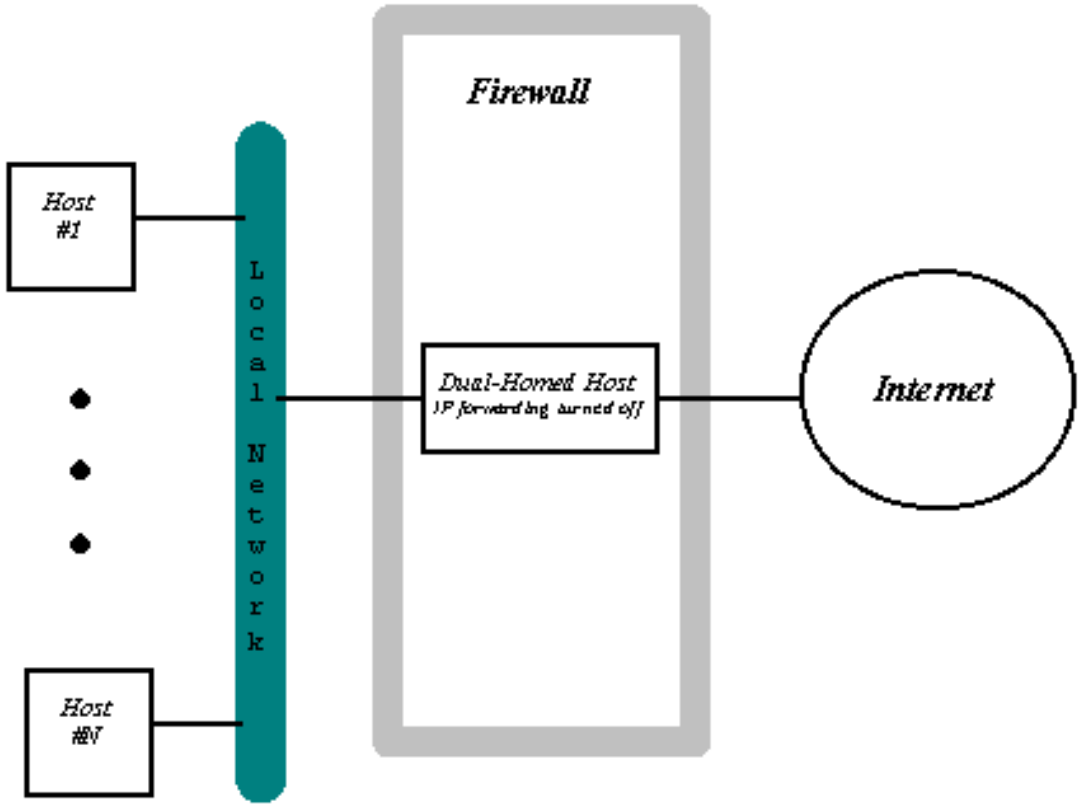
Only network level filter



Dual-homed Host

Indirect connection t
internet (IP forward
off)

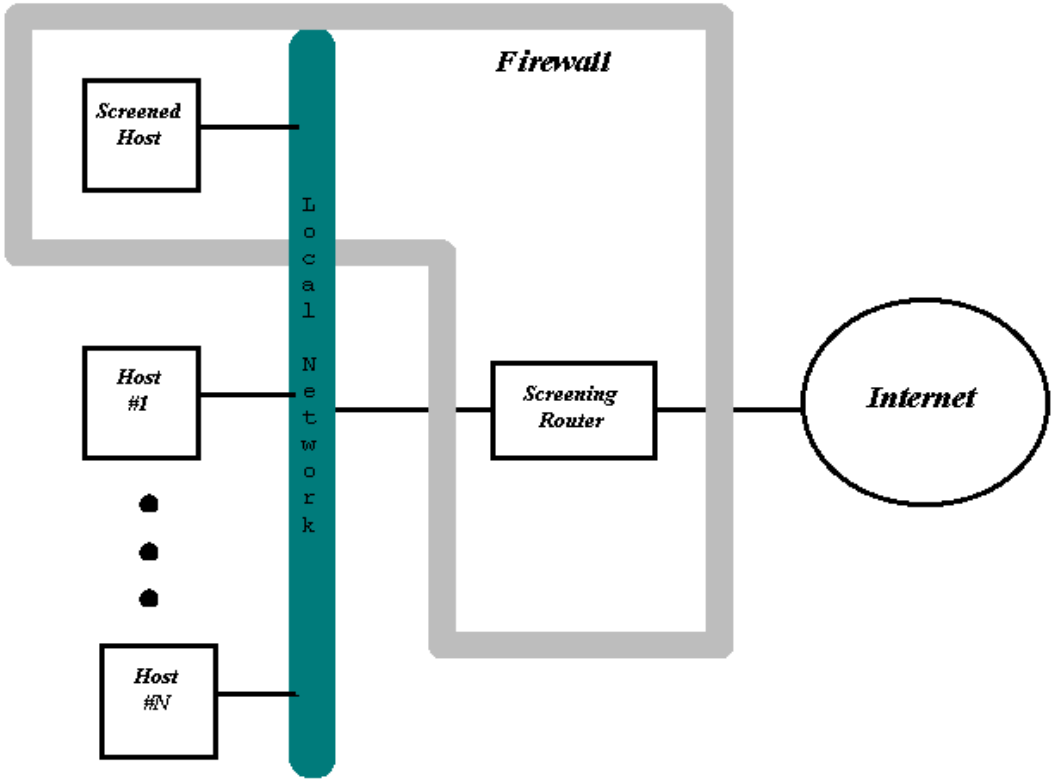
Application Proxy



Screened-Host

Only the screened host is allowed to go outside

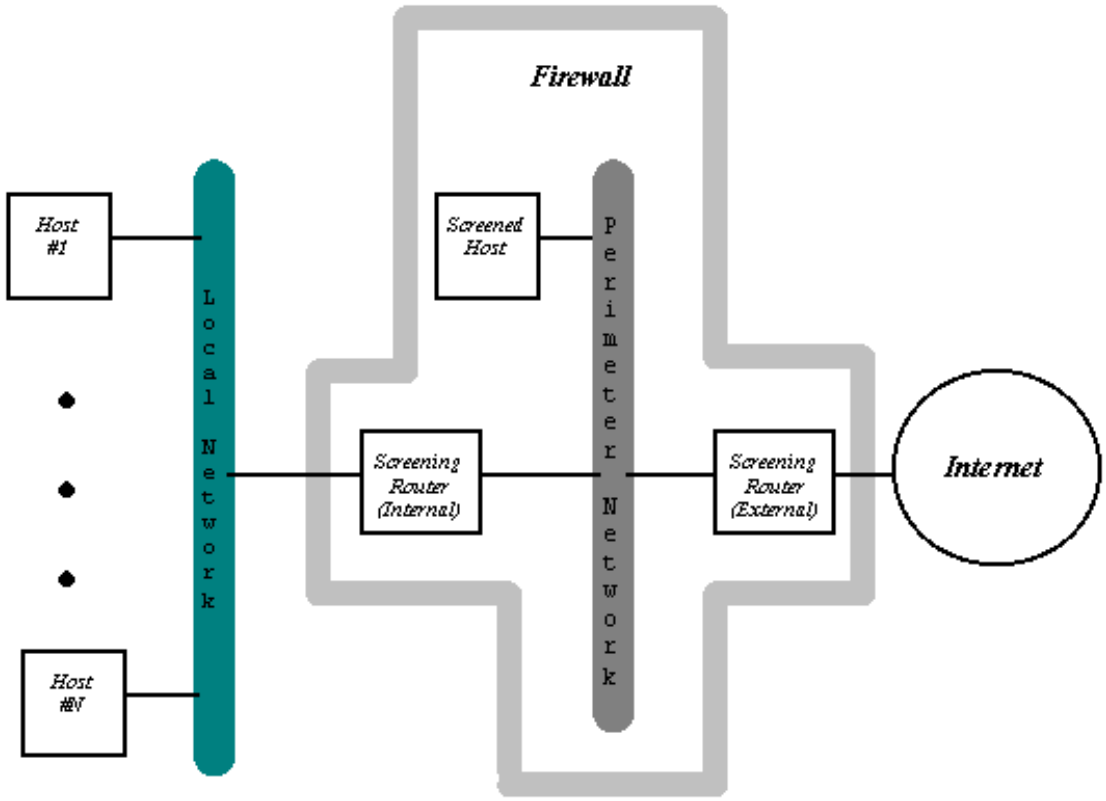
Application Proxy



Screened Sub-net

A zone is created

Additional filtering

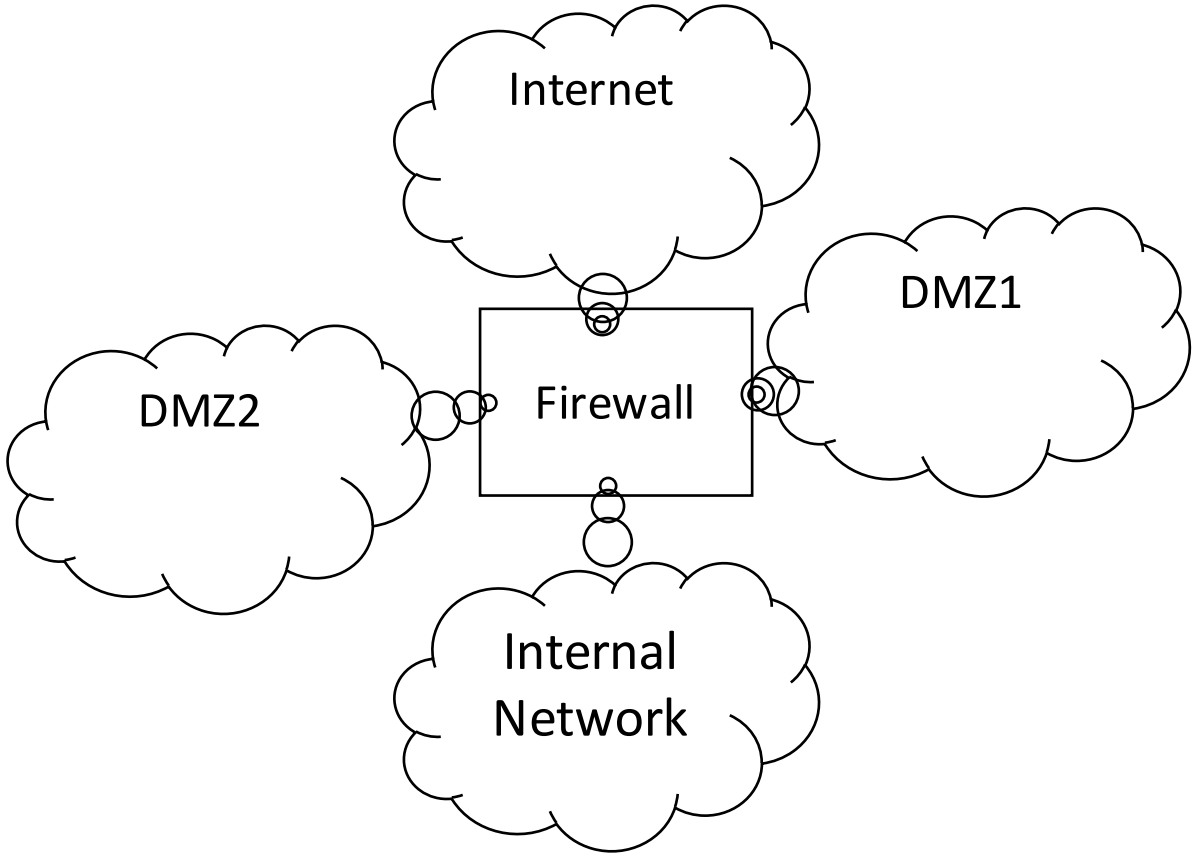


Multi-homed

Multiple DMZs

Performance

Cost saving



Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

Intrusion Detection Systems

What is IDS and IPS?

- IDS monitors system or network for attacks.
- IPS monitors and prevents attacks.

IDS/IPS engine has a library and set of signatures that identify an attack

Adds Defence in depth

Could be used in conjunction with a system scanner for maximum security

WHY IDS/IPS?

To detect attacks and other security violations that are not prevented by other security measures,

To document the existing threat to an organization

To act as quality control for security design and administration

To provide useful information about intrusions that do take place

To compel users to security requirements

To deterrent attackers

IDS/IPS Types

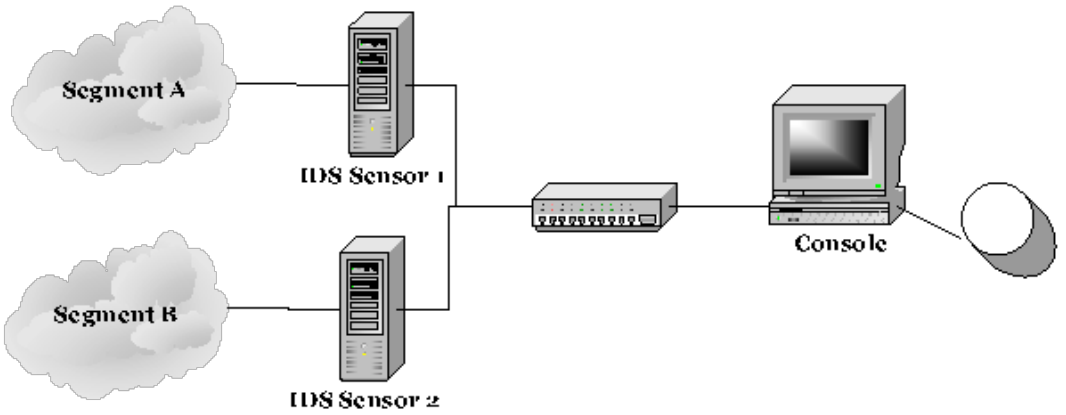
Knowledge-based/Signature-based
- Rules/Patterns

Behaviour-based/Statistical
- Anomalies

Network-based

Host-based

Application-based



Intrusion Detection Systems/IPS

Detect intruders and hackers' activity using anomaly detection/ pattern matching method to compare intruders action

Under the scope of IDS/IPS

- Network based IDS/IPS
- Host based IDS/IPS
- File Integrity checker

Network based IDS/IPS

Consists of sensor and management station

Used for monitoring network

Based on the promiscuous mode of the network card

Analyze by the management station

Network based IDS/IPS

Advantages

- Can detect network attack traffic
- Does not require modification of production servers or hosts
- More self contained

Network based IDS/IPS

Disadvantages

- Cannot detect attack from other not directly connected segment
- Inadequate to detect more complex threats especially for the signature analysis scheme
- Large amount of data will be generated
- Cannot handle encrypted attack

Host based IDS/IPS

Looks for signs of intrusion on local host system

Based on hosts' audit and logging mechanism

Using rule-based engines for analyzing activity

Host based IDS/IPS

Advantages

- Extremely powerful tool for analyzing a possible attack
- Network bandwidth will not be affecting the sensor analysis
- Less risky to configure with active response
- Lower false positive rates

Host based IDS/IPS

Disadvantages

- Require installation
- Rely on the innate logging and monitoring capabilities
- Relatively more expensive

File Integrity Checkers

Examine the files on the computer

Determine whether files have been modified

Recalculates the hash value and compares with the stored value

Based on calculating the two collision value

E.g. Tripwire

File Integrity Checkers

Advantages

- Almost infeasible to defeat the integrity checker
- Proper configuration can ensure the integrity of the files, directories and programs
- Can be configured to watch everything on the system
- Extremely flexible

File Integrity Checkers

Disadvantages

- Rely on data stored on the local computers which can also be modified
- Need to be configured individually for each system
- Depending on operating system
- Required considerable resources

IDS/IPS Planning

Location to place the IDS agent

- Agent on high risk machines
- Agent on firewall
- Network agent inside the DMZ
- Network agent in Internal segment

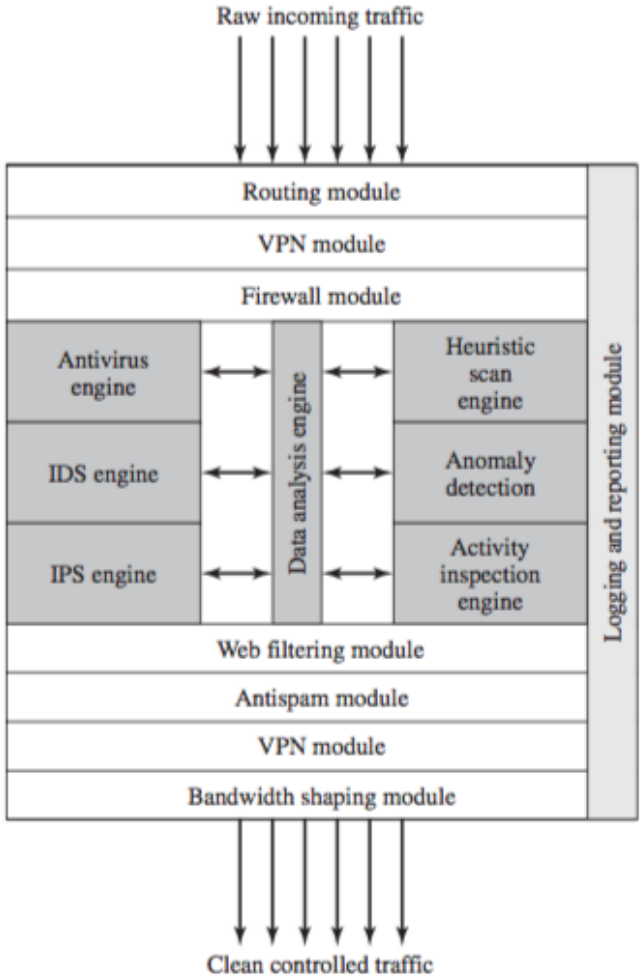
IDS monitoring console

- Construct an independent network for IDS management
- Protect the console from being attacked

Unified Threat Management

Security solutions or appliance with the following functions

- Firewalls
- Anti-virus, Anti-malware, Anti-spam
- IDS/IPS
- Content filtering
- Data Leak prevention
- VPN
- Continuous monitoring and reporting



From Computer Security – Principles and Practice

EndPoint Security

Security vendors are focusing more on developing endpoint security products.

Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, anti-spam, anti-bots and personal firewalls.

These system are usually applied at host/server level directly. The goal is to make it harder to compromise systems and to improve the effectiveness of detection and investigation of breaches when they do occur

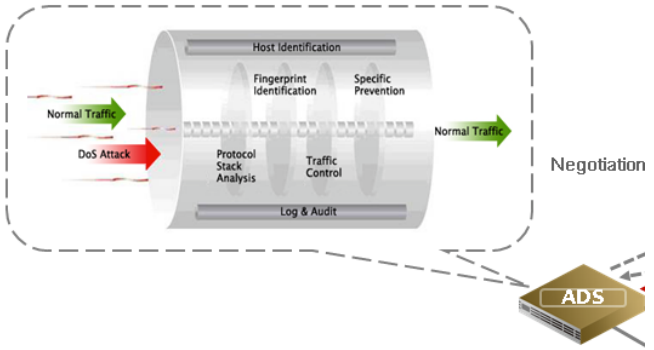
Can be considered as “host version” of UTM

Anti-DDoS

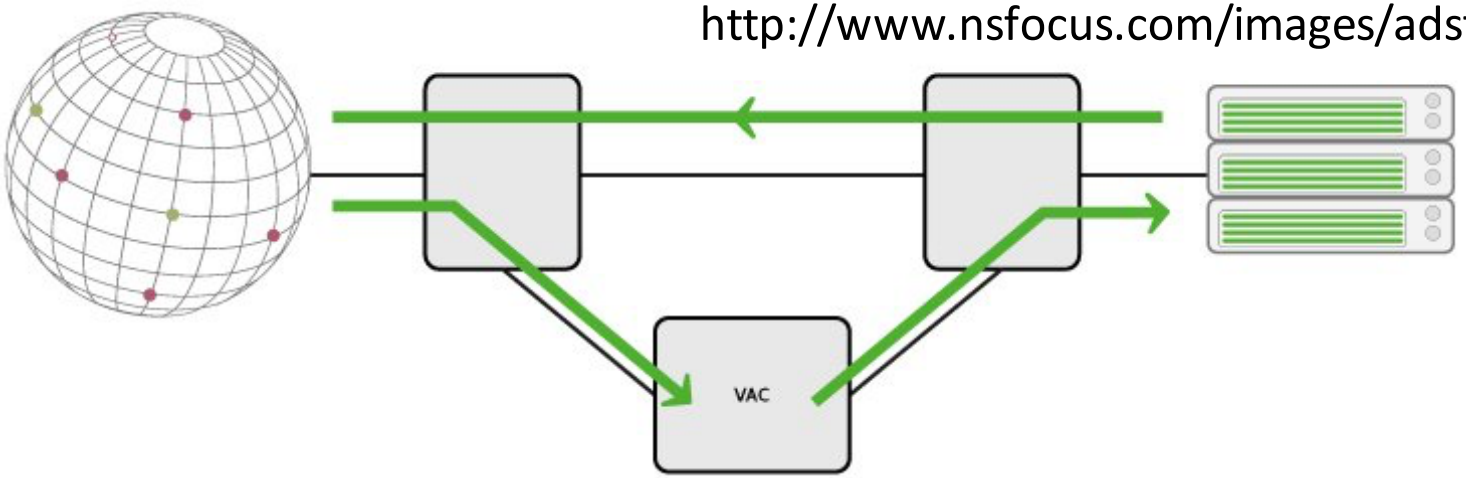
Anti-DDoS solution

Solution against bandwidth/resources type DDoS attack

- Black-hole
- Behavioral IDS detection
- Clean pipe



http://www.nsfocus.com/images/adsfa04.png



http://www.vilayer.com/sec-layer-anti-ddos.html

Other Additional network security controls

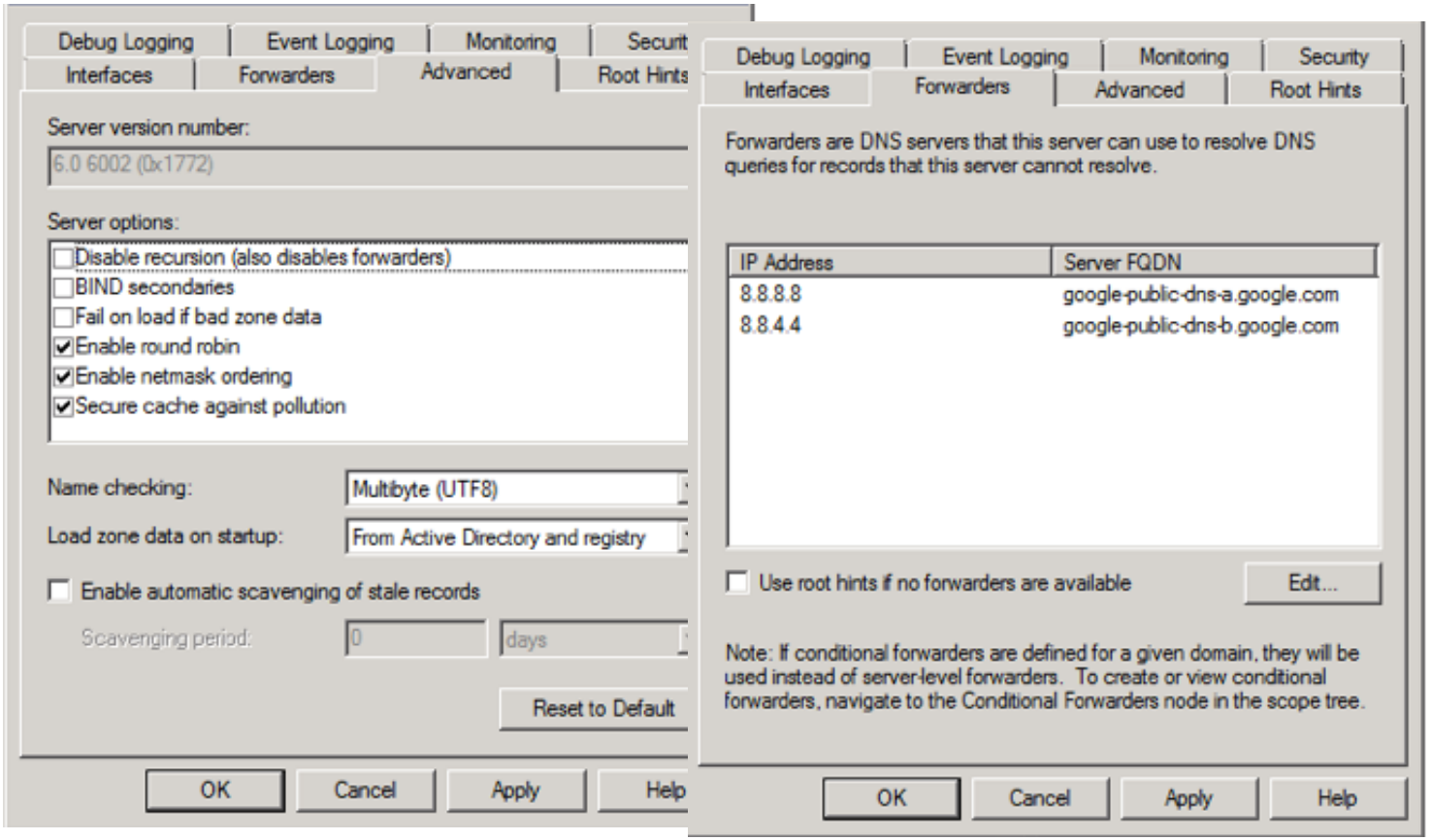
DNS Security

DNS Attacks

DNS Attacks

- DNS Spoofing
- DNS Response Flooding
- DNS ID hacking
- DNS cache poisoning
- Information Leakage
- DNS Server Exploitation

DNS settings in Windows



DNSSEC

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

It is a set of extensions to DNS which provide to

- DNS clients (resolvers) origin authentication of DNS data,
- authenticated denial of existence, and data integrity
- but not availability or confidentiality
- DNSSEC works by digitally signing records for DNS lookup using public-key cryptography.

DNSCurve

DNSCurve

- designed by Daniel J. Bernstein
- uses Curve25519 Elliptic curve cryptography (256-bit ECC) to establish keys used by Salsa20
- paired with the MAC function Poly1305
- used in CurveCP, a UDP-based protocol which is similar to TCP but uses elliptic-curve cryptography to encrypt and authenticate data
- to encrypt and authenticate DNS packets between resolvers and authoritative servers.
- Public keys for remote authoritative servers are placed in NS records, so recursive resolvers know whether the server supports DNSCurve

OpenDNS

OpenDNS offers DNS resolution as an alternative to using Internet service providers' DNS servers or locally installed DNS servers. OpenDNS has adopted and supports DNSCurve

IPv4

- 208.67.222.222
- 208.67.220.220

IPv6

- 2620:0:ccc::2
- 2620:0:ccd::2

Other DNS related functions

Phishing filter, OpenDNS also run a service called PhishTank for users to submit and review suspected phishing sites.

FamilyShield parental controls which block pornography, proxy servers, and phishing sites

OpenDNS supports the DNSCrypt protocol, which authenticates DNS traffic between the user's computer and the name servers

OpenDNS Enterprise, a first foray into enterprise-grade network security.

OpenDNS Insights. This new service featured integration with Microsoft Active Directory, which allowed admins granular control over creating policies on a per-user, per-device, and per-group basis

WLAN Defense

802.1x Authentication Standards

New standard for wired and wireless authentication

With strong and mutual authentication between client and authentication server

Rely on Extensible Authentication Protocol (EAP)

Support EAP Cisco Wireless (or LEAP)

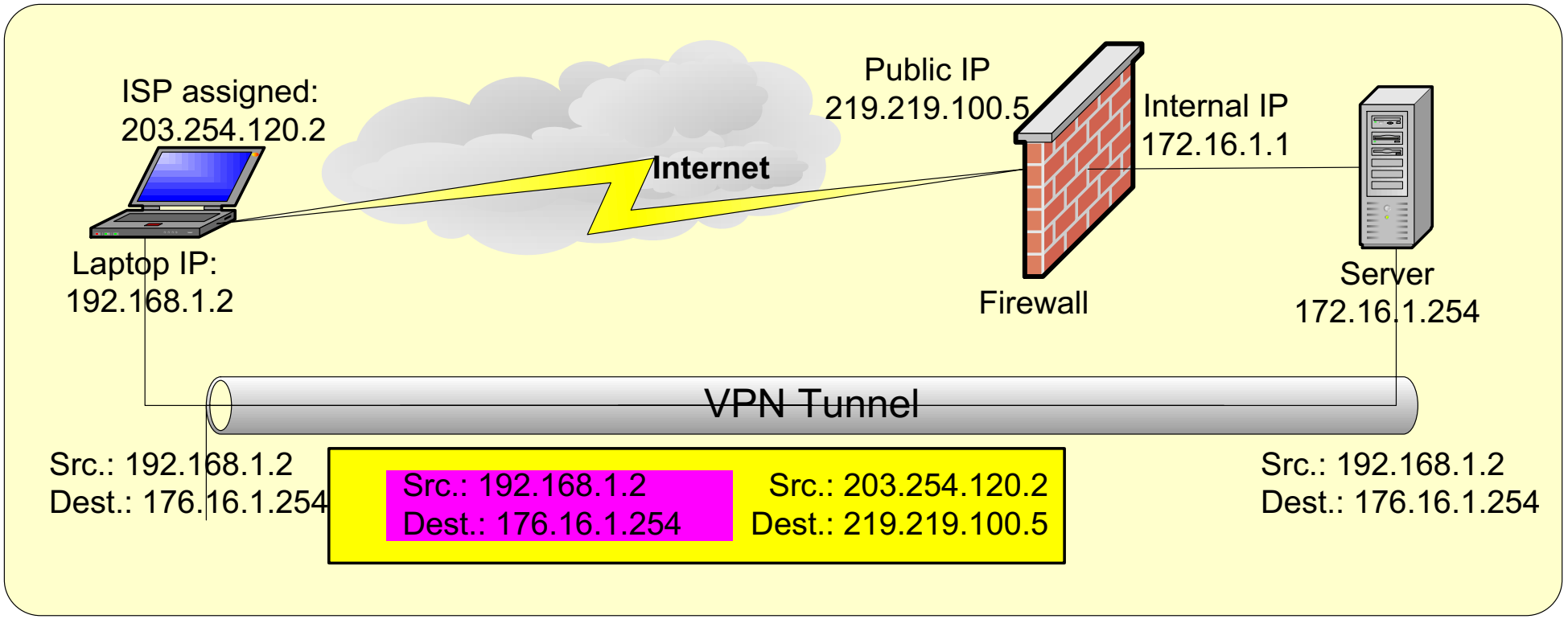
Possible WLAN defense mechanism

Authentication
- Shared key
- Open system

Authentication
- SSID - Set Service ID
- MAC - Media Access Control

Privacy
- WEP – Wired Equivalent Privacy
- 802.1x - IEEE 802.1x standard
- VPNs - Virtual Private Networks
- VLANs - Virtual Local Area Networks
- WSA (WAP Security Protocol) and WTLS (Wireless Transport Layer Security)

How VPNs Works



NAP and End Point Security

Network Access Protection

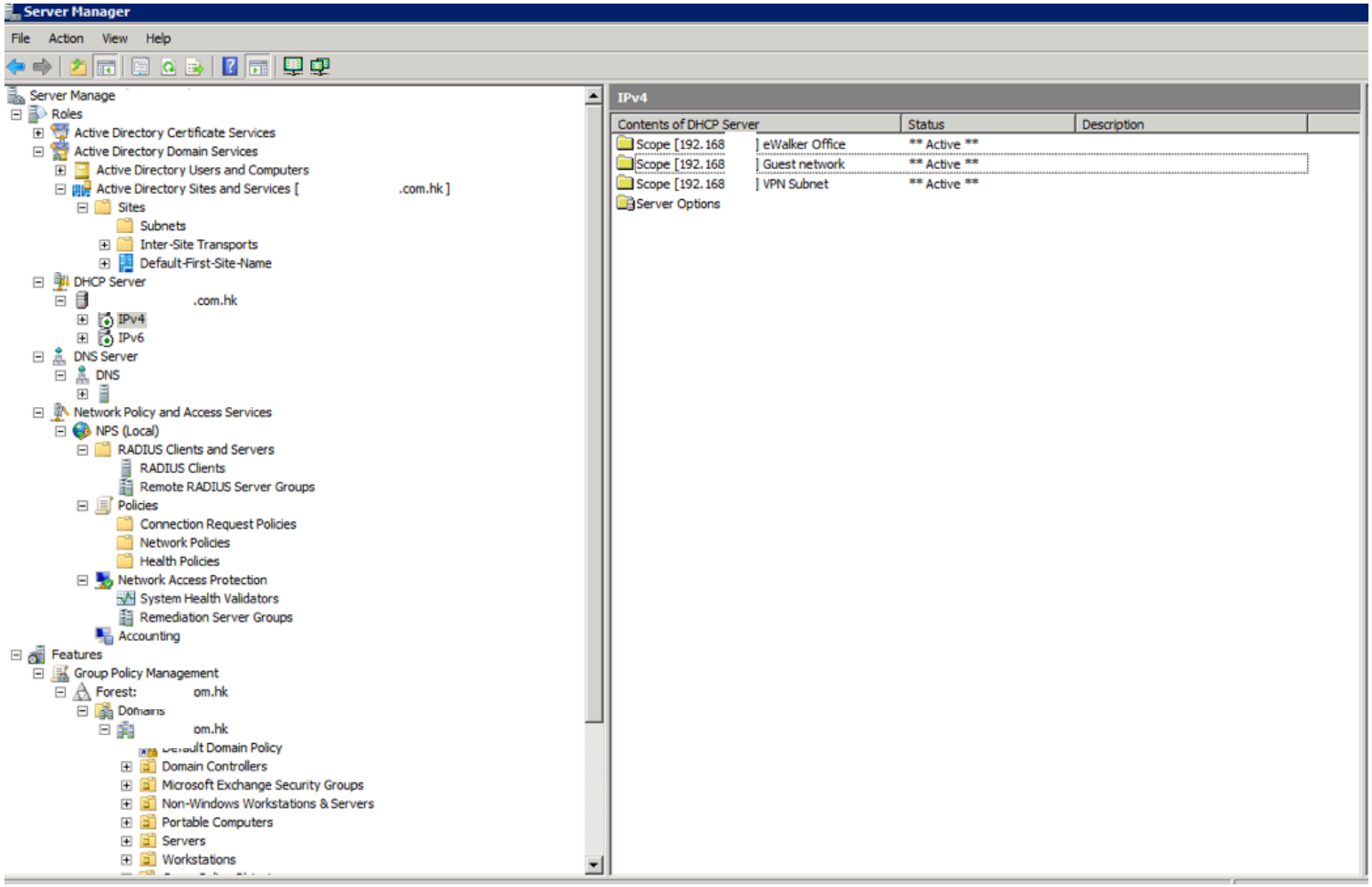
Network Access Protection (NAP) is a set of operating system components that provide a platform for protected access to private networks.

The NAP platform provides an integrated way of evaluating the system health state of a network client that is attempting to connect to or communicate on a network and restricting the access of the network client until health policy requirements have been met.

Combined functions of:

- Authentication Server IEEE 802.1X for wireless and wired network
- DHCP
- DNS
- VPN

NAP



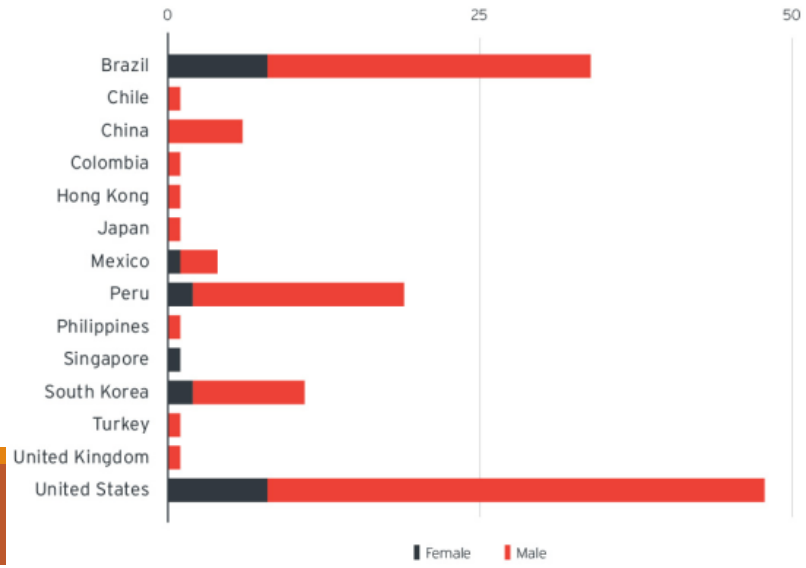
Ashley Madison, Why Do Our Honeypots Have Accounts On Your Website? (2015)

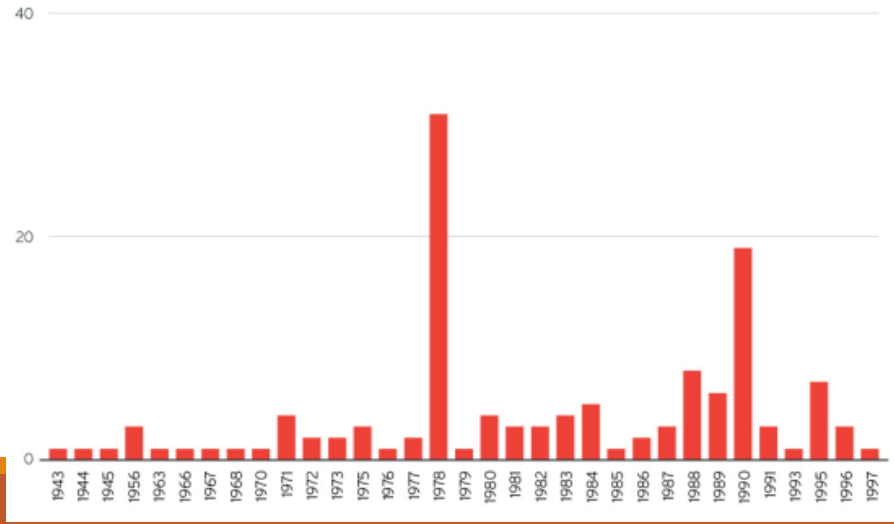
Sep 8

Ashley Madison, Why Do Our Honeypots Have Accounts On Your Website?

5:00 am (UTC-7) | by Ryan Flores (Threat Research Manager)

She is 33 years old, from Los Angeles, 6 feet tall, sexy, aggressive, and a "woman who knows what she wants", according to her profile. She is intriguing. However, her intrigue doesn't end there: her email address is one of Trend Micro's email honeypots. Wait… what?



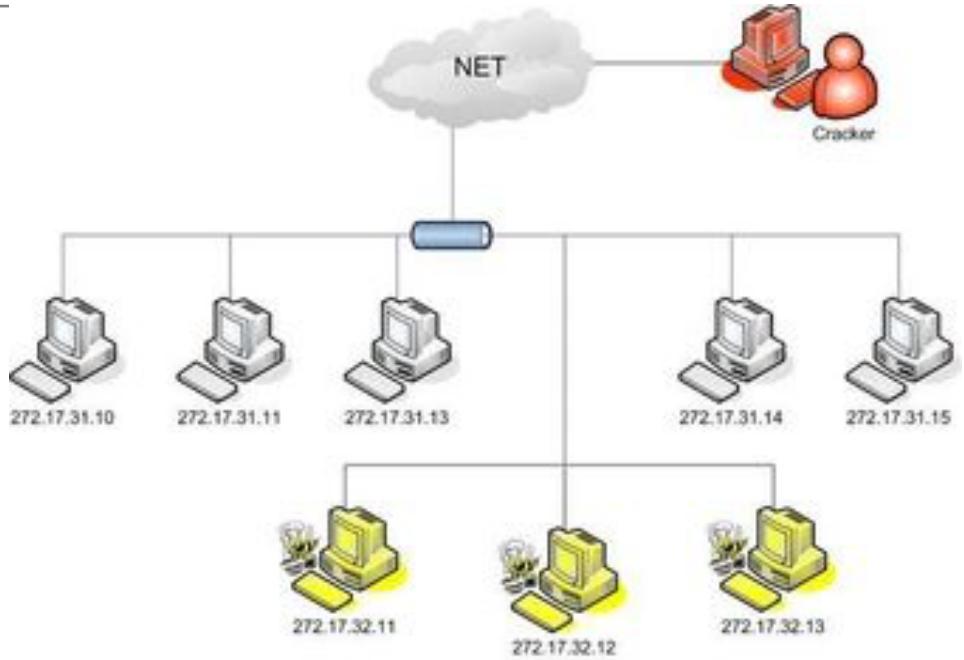


What is Honeypot

Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Consists of 3 types

- Pure honeypots
- High-interaction honeypots (imitate most services)
- Low-interaction honeypots (imitate frequently used services)



http://honeypots-the-trap-of-computing.wikia.com/wiki/Honeypots:_The_Trap_of_Computing_Wiki

https://en.wikipedia.org/wiki/Honeypot_(computing)

Reference Books

Related content	Book	Chapter
W4: Firewall	Cryptography and Network Security (2011)	Chapter 22: Firewalls
W4: Firewall, IDS	Guide to Computer Network Security (2015)	Chapter 12: Firewall Chapter 13: System Intrusion Detection and Prevention
W4: Antivirus	Guide to Computer Network Security (2015)	Chapter 15: Virus and Content Filtering
W4: Network Security	The InfoSec Handbook (2014)	Chapter 9: Understanding Networks and Network Security
W4: Firewall	The InfoSec Handbook (2014)	Chapter 10: Firewalls
W4: IDS and IPS	The InfoSec Handbook (2014)	Chapter 11: Intrusion Detection and Prevention Systems
W4: Firewall and IPS	Computer Security Principles and Practice (2012)	Chapter 9: Firewalls and Intrusion Prevention Systems