Information Security Solutions

SANOG 6

July 21, 2005

Thimpu, Bhutan

Ritesh Raj Joshi

Netfiniti

ritesh@netfiniti.com.np

netfiniti

Information Security Challenges

- Managing security has become increasing complex
- Growing external and internal threats
- Internal threats increasingly common than external – much easier too
- Good external security measures in place
- Attackers looking for other means of circumventing/bypassing guards and getting inside
- Social engineering becoming popular
- Methods - personal contact, installing backdoor, key loggers, spyware, phising via email attachments

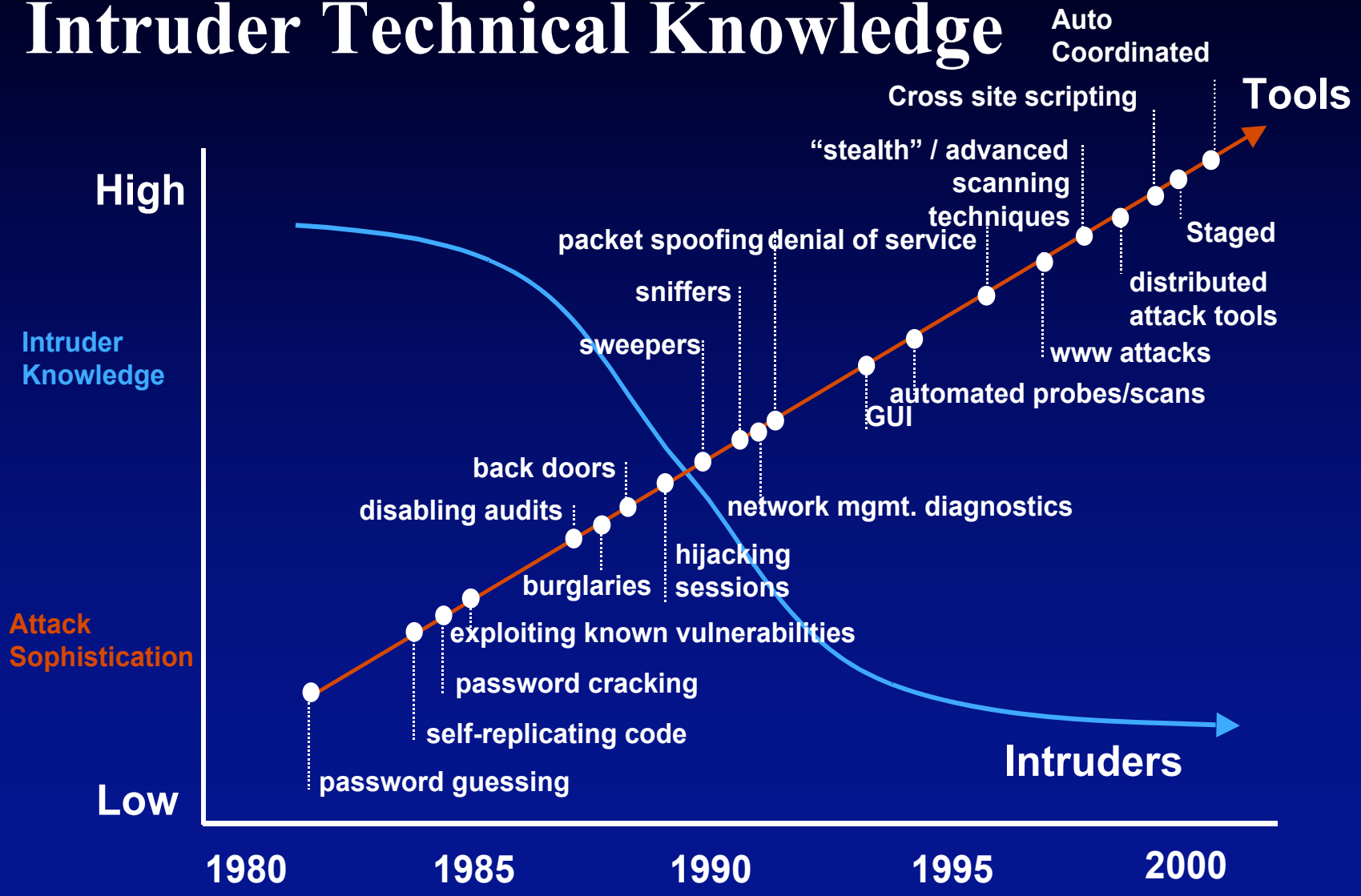
Information Security Solutions

- Nothing is 100% secure!!!
- You can only mitigate the risks.
- Approach should be to apply defense-in-depth
- The most effective way to apply security is in layers
- Place security measures at different points in your network
- Construct a series of obstacles of varying difficulty
- Secure each component in your network (firewalls, routers, servers, desktops)
- If one measure fails the next will protect
- The series of obstacle may finally make the attacker give up!

Present Scenario

- THE MODERN THIEF CAN STEAL MORE WITH A COMPUTER THAN A GUN.
- MORE DAMAGE COULD BE CARRIED OUT WITH A KEYBOARD THAN A BOMB.

Attack Sophistication vs. Intruder Technical Knowledge



netfiniti

Common Security Threats & Vulnerabilties

- Threat:

  Any person, object, or event that, if realized, can potentially cause damage to the network or networked device

- Vulnerability:

  A weakness in a host or network that can be exploited by a threat

Common Threats

- Unauthorized Intrusions
- Denial of Service (DoS) Attacks
- Viruses, Worms, Trojan Horses (Backdoors)
- Website Defacements
- Internal Attacks
- Non-compliance

Unauthorized Intrusions

- Intruders want to gain control of your computer and to use it to launch attacks on other computer systems.
- Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems.
- The damage created depends on the intruder's motives
- Confidential information maybe compromised, altered or damaged

Causes of Intrusion

- Intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software.
- Users fail to obtain and install the latest patches/updates, or correctly configure the software to operate more securely.
- Most of the incidents could prevented if system administrators and users kept their computers up-to-date with patches and security fixes.
- Some default settings that allow other users to access your computer unless you change the settings to be more secure.

Denial of Service

- Interruption of service either because the system is destroyed or is temporarily unavailable

- e.g.
  - Destroying a computer's hard disk
  - Severing the physical infrastructure
  - Using up all available system resource - CPU, memory, disk space
  - Consuming network bandwidth to the server

Denial of Service

- Can be mitigated by applying vendor patches to affected software
- By securing always-on hosts with broadband connectivity – DSL, Cable, etc. that are exploited by attackers for DDOS
- DoS attacks cannot be stopped, but their scope of affected areas can be constrained by secure network design
- Most common – SYN Flood attack, Ping of Death

Viruses & Worms

- A virus requires a user to do something to continue the propagation – harmful, may destroy data
- A worm can propagate by itself - self-propagating malicious code, consumes resources destructively, DoS
  – Blaster, Slammer
- Highly prevalent/common on the Internet
- Common distribution: e-mail, ftp, media sharing, hidden codes

Viruses & Worms

- Some worms include built-in denial-of-service attack payloads (Code Red)
- Creates a DoS in many parts of the Internet because of the huge amounts of scan traffic generated
- Some directed towards specific sites – Microsoft, Yahoo, Ebay, etc.
- Some may install backdoor program for further misuse by attacker

Trojans (Backdoors)

- Trojans (Backdoors) - Executable codes installed that enable entry into the infected host without authorization
- Once installed the back door can be used by the attacker at their leisure
- Launching points for further security attacks (DDOS, SPAM)

Bots (Spyware)

- Modularized root-kits for specific functions.
- What Bots can do:
  - Create Launch pad for DDOS attacks
  - Packet sniffing
  - Key logging
  - File Serving of illegal or malicious code
  - Replicating

Website Defacements

- Intent: To create political propaganda based attacks
- To make a political statement
- Launched primarily at Government Orgs, Media, Religious Groups
- By exploiting known vulnerabilities in websites or servers
- The attacker can plant codes or files to vandalize site

- Examples at: http://www.attrition.org/mirror/attrition

Internal Attacks

- Computer Security Institute/FBI and Ernst & Young say nearly 50% of all network attacks come from the inside
- Often, from unhappy/disgruntled workers
- 76% of the IT executives surveyed by NetVersant said they were concerned about inside attacks from unhappy employees
- Losses associated with insider attacks can be more damaging

Non-compliance

- Security policies and procedures not followed properly by all concerned staff
- Who cares how good your systems are if employees ignore them?
- Highly risky if policies are not followed as stipulated

- NetVersant survey: 82% reported spotty or no compliance with their company's network security policies
- 85% say a properly-implemented firewall would still be at risk from a disgruntled employee
- And 75% say the firewall is at risk from employee incompetence

Other Common Attacks

- Connection (Session) hijacking
- IP source address spoofing
- Smurf attack
- Brute-force/Dictionary attacks (password guessing)

- Humans are often the weakest link = social engg
  "Hi, this is Bob, what's the root password?"

Vulnerabilities

- Insecure protocols/services running on a host
- Exploitable security hole on a host without latest patches or workarounds
- Poorly protected hosts without firewalls, IDSs, etc.
- Use of weak or default passwords
- Insecure configuration of hosts
- Execution of malicious codes – Trojan, Backdoors
- Use of pirated or downloaded software from a public site without verifying checksum (integrity) and authenticity (signature)
- Social engineering

Common Motivations for Attacks

- Greed:
  The intruder is hired by someone to break into a corporate network to steal or alter information for the exchange of large sums of money.

- Prank:
  The intruder is bored and computer savvy and tries to gain access to any interesting sites.

- Notoriety:
  The intruder is very computer savvy and tries to break into known hard-to-penetrate areas to prove his or her competence.
  To gain the respect and acceptance of his or her peers.

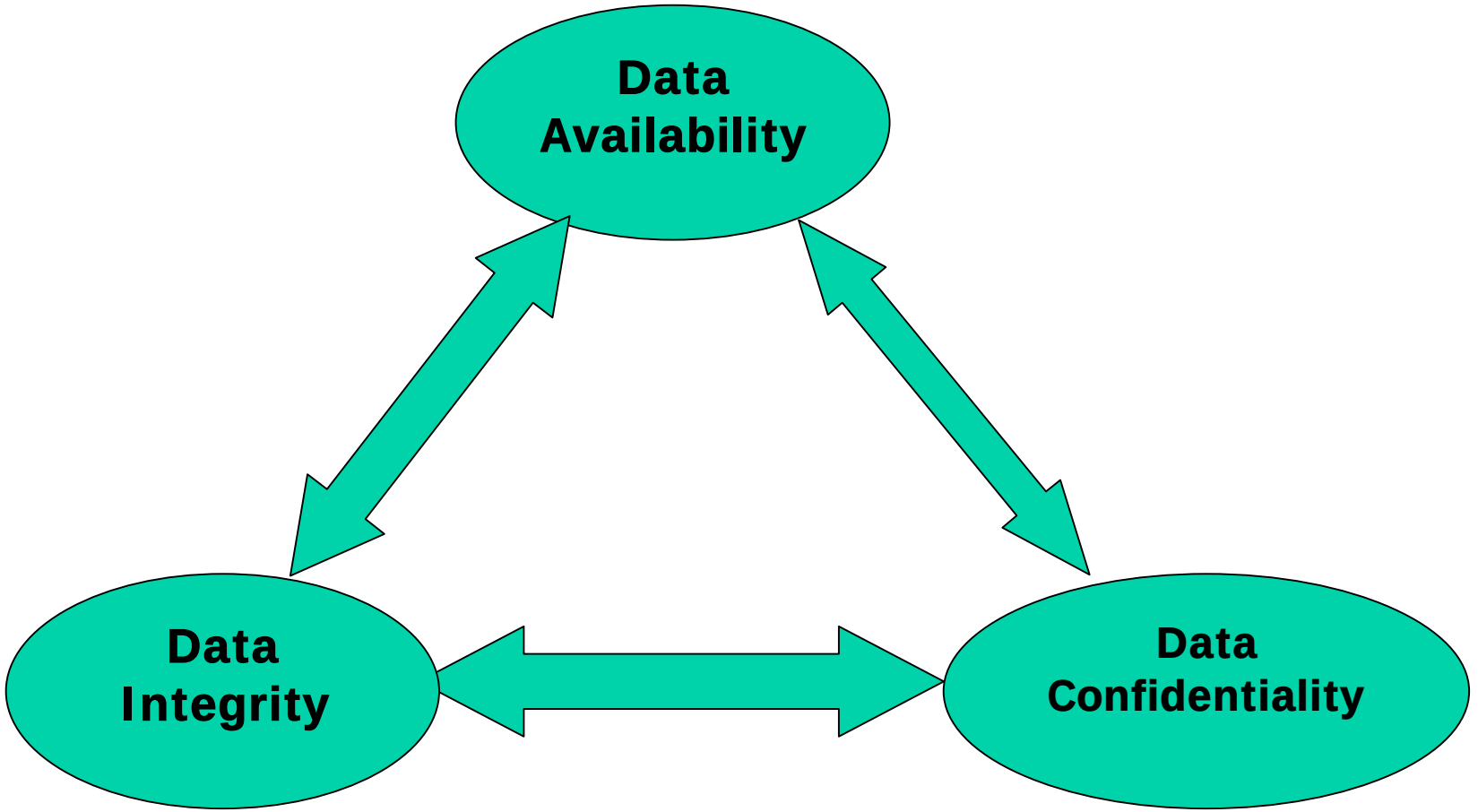
Common Motivations for Attacks

- Revenge:
  The intruder has been laid off, fired, demoted, or in some way treated unfairly. Attacks result in damaging valuable information or causing disruption of services

- Ignorance:
  The intruder is learning about computers and networking and stumbles on some weakness, possibly causing harm by destroying data or performing an illegal act

- There is a large range of motivations for attacks
- Consider all these motivations as possible threats

Goals of NW Security

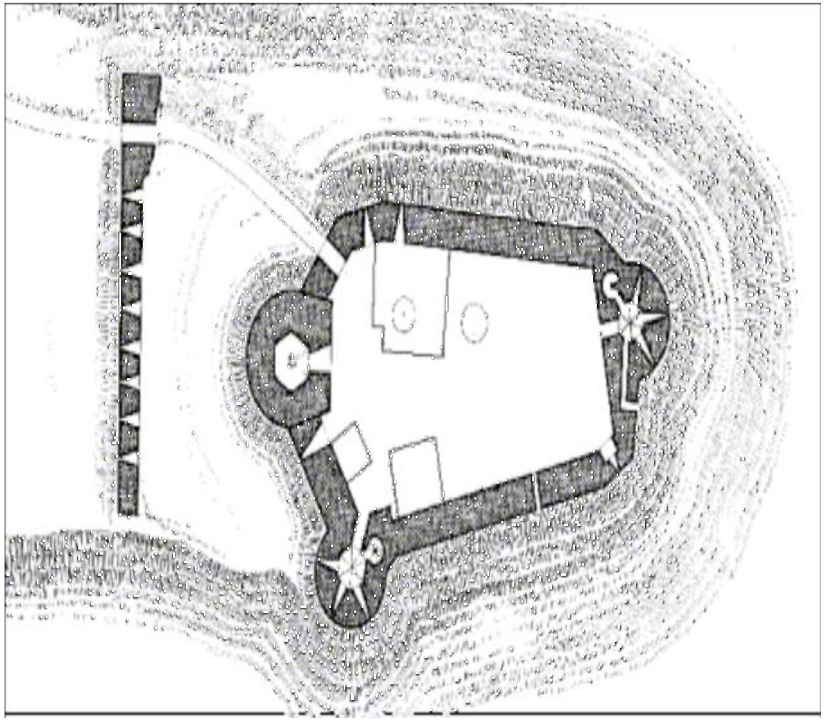


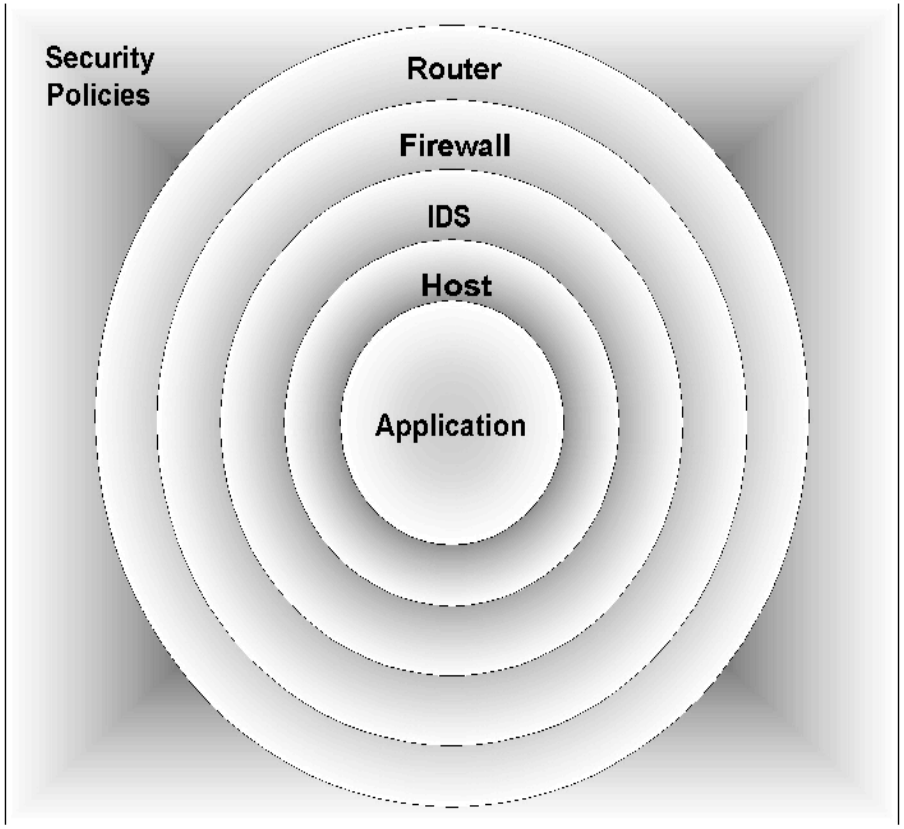
netfiniti

Defence –in- Depth

- Perimeter Defences
- Network Defences
- Host Defences
- Application Defences
- Data & Resources

The Castle Analogy





The Layered Defense Concept

netfiniti

Router Security

- Restrict admin access to console, telnet, SNMP
- Use password encryption methods
- Use TACACS+ for varied levels of access
- Use SSH for remote administration
- Restrict Telnet access
- Use strong SNMP community <password>, RO,RW
- Enable ip accounting and logging, syslog

Router Security

- Enable ip accounting and logging, syslog
- Apply anti-spoofing ACLs on interfaces
- Block all private IP address on the public interface
- Apply route filters for RIP, OSPF, BGP
- Use peer authentication for exchanging routing info
- Use private IP addresses for your backbone routers
- Use out-of-band management if possible
- No management traffic on the primary IP network
- Enable audit features to monitor any anomalies

Router Security

- Enable ip accounting and logging, syslog
- Apply anti-spoofing ACLs on interfaces
- Block all private IP address on the public interface
- Apply route filters for RIP, OSPF, BGP
- Use peer authentication for exchanging routing info
- Use private IP addresses for your backbone routers
- Use out-of-band management if possible
- No management traffic on the primary IP network
- Enable audit features to monitor any anomalies

Firewall

- Protects your internal network from the external world
- Enforces an access control policy between two networks
- Install firewalls also between office departments
- Disallow unauthorized traffic in/out of your network
- Define rules depending on required services/protocol
- Prevent DOS attacks using rate limits

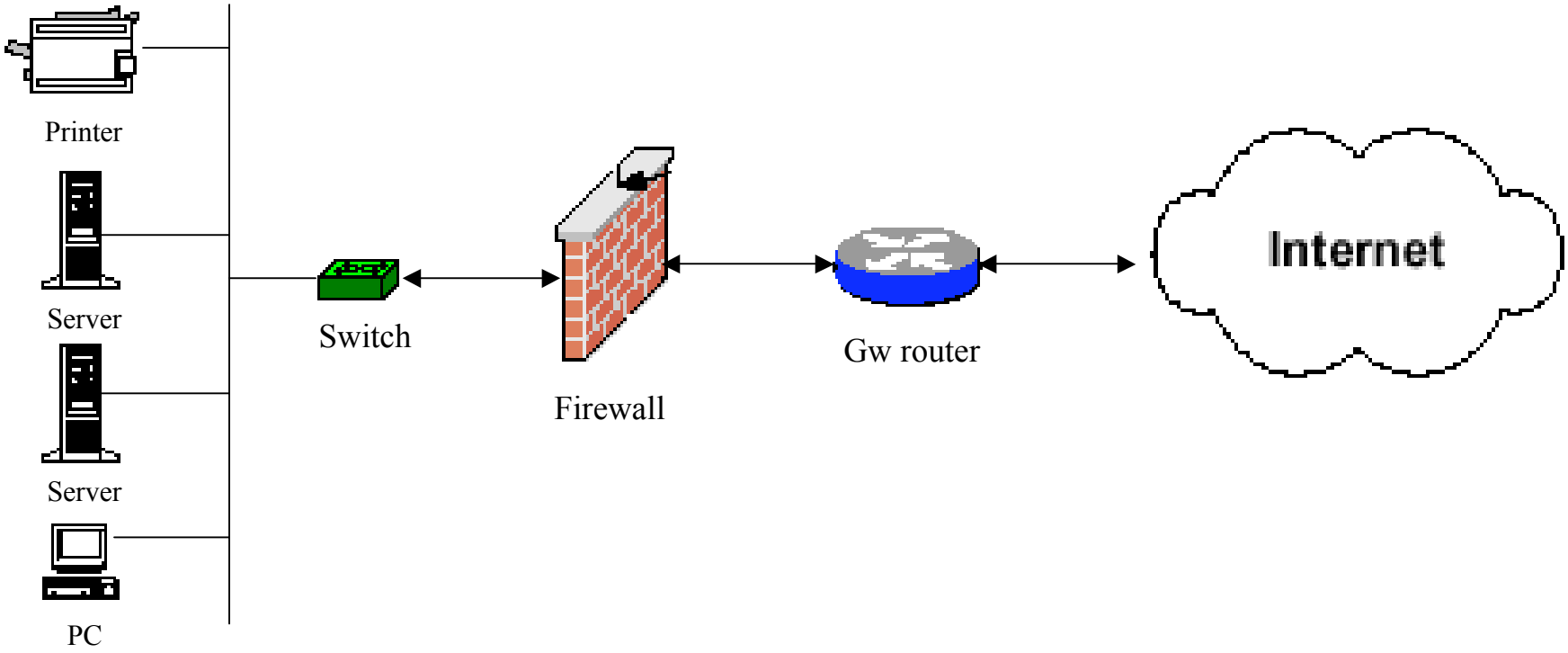
Firewall

- Protects your internal network from the external world
- Enforces an access control policy between two networks
- Install firewalls also between office departments
- Disallow unauthorized traffic in/out of your network
- Define rules depending on required services/protocol
- Prevent DOS attacks using rate limits

Firewall

- Protects your internal network from the external world
- Enforces an access control policy between two networks
- Install firewalls also between office departments
- Disallow unauthorized traffic in/out of your network
- Define rules depending on required services/protocol
- Prevent DOS attacks using rate limits

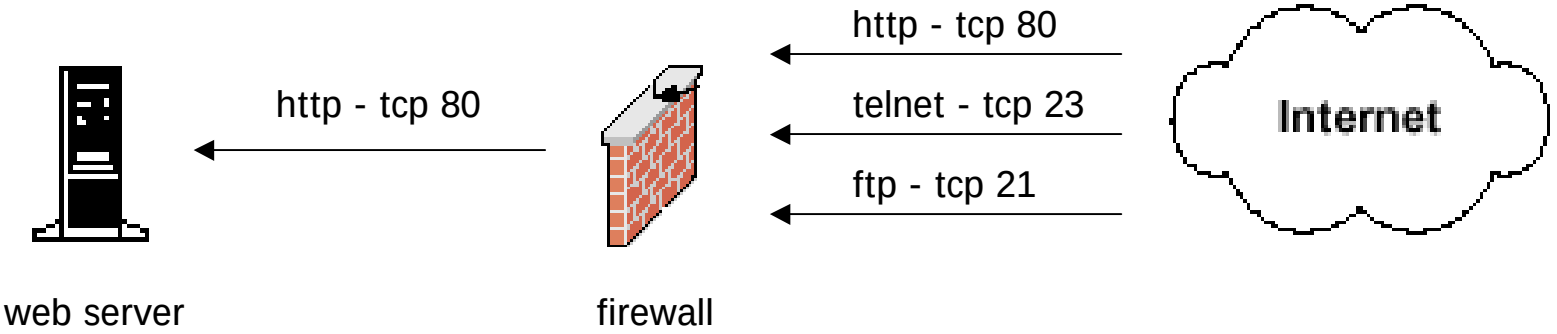
A typical firewall setup



netfiniti

Packet filtering firewalls

- examines the source and destination address of the data packet and either allows or denies the packet from traveling the network
- blocks access through the firewall to any packets, which try to access ports which have been declared "off-limits"

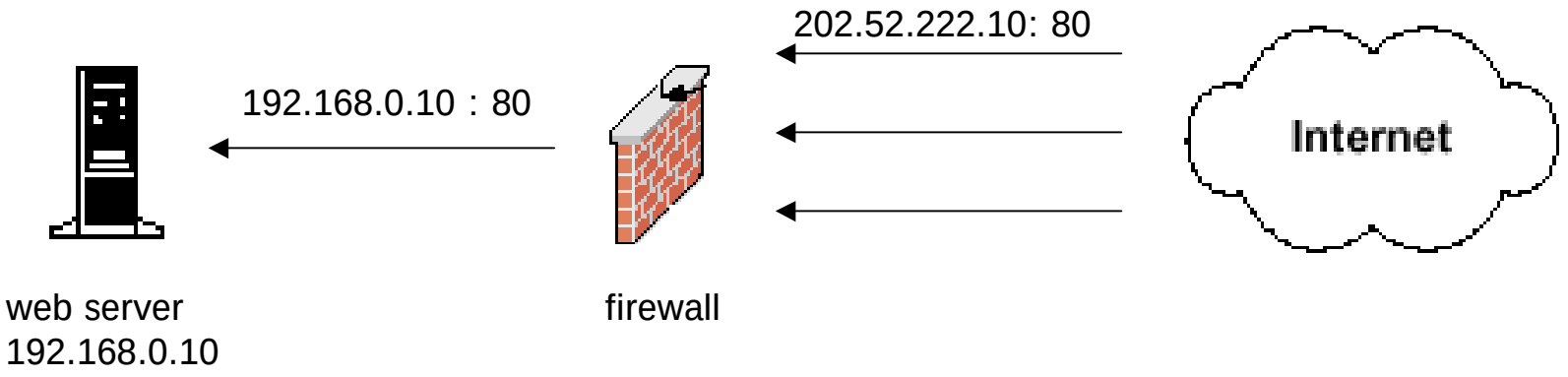


- Allow only http - tcp 80
- Drop ip any

netfiniti

Application layer firewalls

- Also known proxy firewalls, application gateway
- attempts to hide the configuration of the network behind the firewall by acting on behalf of the servers
- All packets are scrutinized for any protocol anomalies before passing on to the server

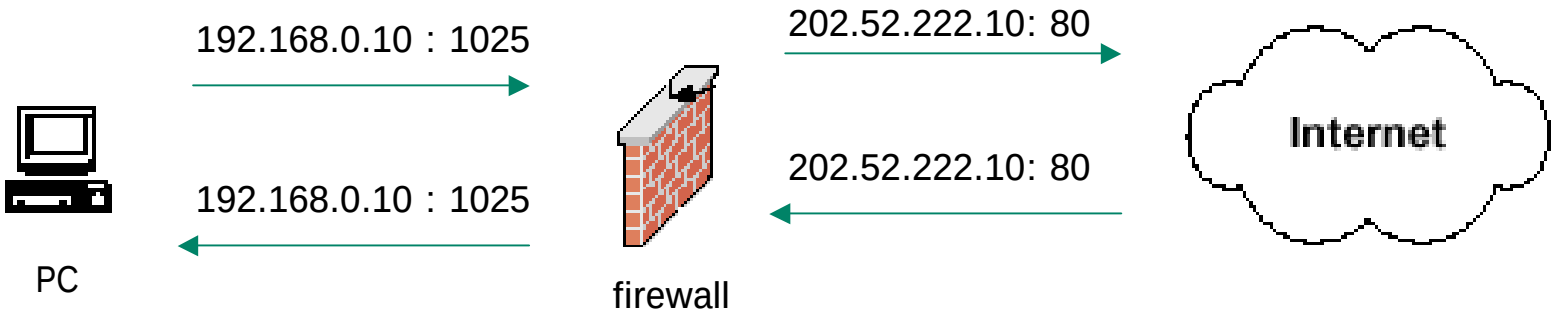


- Translates 202.52.222.10 : 80 to 192.168.0.10 : 80

netfiniti

Stateful Inspection Firewalls

- Examines the state and the context of the packets
- Remembers what outgoing requests have been sent and only allow responses to those requests back through the firewall
- Makes decisions based upon the state information of the packet – SYN, ACK, FIN



- Only allows reply packets for requests made out
- Blocks other unregistered traffic

netfiniti

Firewall Best Practices

- Explicitly deny all traffic except for what you want
- Default policy should be to deny/drop packets
- Make sure all network traffic passes through the firewall
- Disable/uninstall any unnecessary services/software
- Use stateful inspection and application proxies if possible
- Filter packets for illegal/incorrect addresses – ip-spoofing

Firewall Best Practices

- Don't just rely only on your firewall for the protection of your network
- Remember that it's only a device, and devices do fail
- Implement defense in depth - multiple layers of network protection
- Firewalls won't prevent attacks that originate from inside your network

Personal Firewalls

- Protects your PC from intrusions and other network attacks – worms, unauthorized access
- Control of execution of unauthorized applications on your PC
- Disable all incoming server connections to your PC
- Disable file sharing, etc.
- Protects against harmful contents, scripts, codes
- Monitor all activities, traffic to/from your PC
- A must if you are connecting to the public network

Some useful security guidelines…

- Have the latest service packs for the OS of your PC
- Never run any executables or scripts via e-mail
- Have the latest updates for browser and e-mail software
- Use a good Antivirus software
- Make sure to regularly update all software
- Regularly scan your PC with Spybot to detect any malware
- When surfing the Internet, file sharing should be disabled

Some useful security guidelines…

- Have the latest service packs for the OS of your PC
- Never run any executables or scripts via e-mail
- Have the latest updates for browser and e-mail software
- Use a good Antivirus software
- Make sure to regularly update all software
- Regularly scan your PC with Spybot to detect any malware
- When surfing the Internet, file sharing should be disabled

Intrusion Detection System

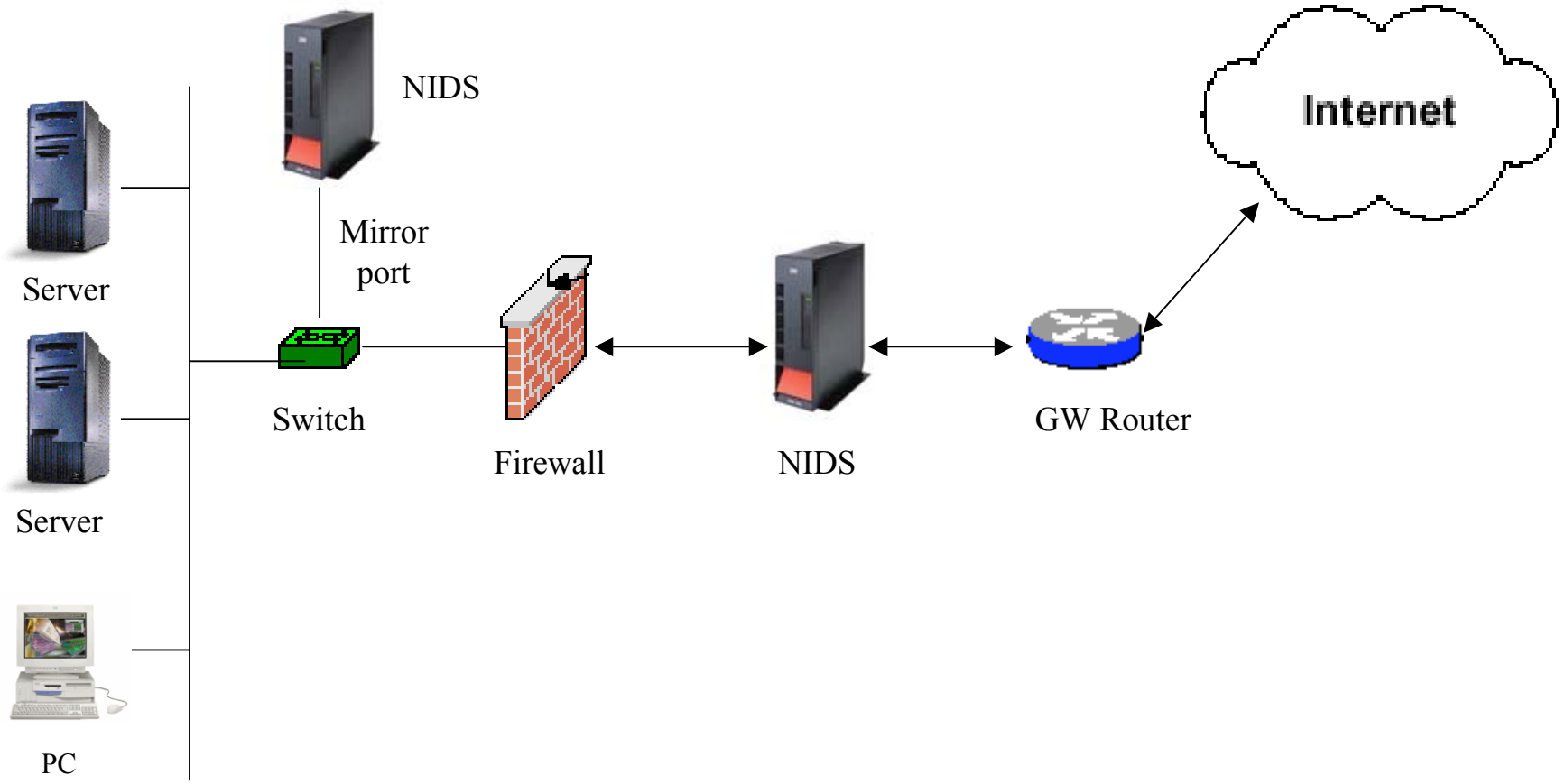
- Firewalls provide limited protection
- Inpects/sniffs all network traffic for any abnormal content
- Has built in signature-base and anomaly detection
- Capability to look for set "patterns" in packets
- String search to look for confidential/offensive data
- Logging of packet information for analysis
- Provides information about malicious network traffic
- Help identify the source of the incoming scans or attacks

- Similar to a security “camera" or a “burglar alarm”
- Alert security personnel that someone is picking the “lock”
- Alerts security personnel that a network invasion maybe in progress

Network based IDS (NIDS)

- Performs an analysis for a passing traffic on the entire subnet
- Alerts admin if an attack is identified, abnormal behavior is sensed
- Place IDS before the firewall to get maximum detection
- In a switched network, place IDS on a mirrored port
- Make sure all network traffic passes the IDS host
- Best to run IDS in bridge mode for transparent network operation

NIDS Placement



netfiniti

Intrusion Detection & Prevention

- Has capability of dynamically blocking attacks on the basis of attack signatures and protocol anomaly detections
- Overcomes limitations of an IDS that just alerts/logs malicious traffic
- Requires less manual intervention to block attacks
- Gaining popularity due to automatic prevention capabilities
- Is placed in-line on the network traffic
- Also known as IPS (Intrusion Prevention System)

WAN Security

- Securing inter-branch office traffic – VPN
- BOVPN – DES/3DES/AES encryption
- IPSec vs. SSL

IPSec vs. SSL

	SSL	IPSec
Layer	Application layer 7 (desired)	Network layer 3 (all traffic)
Overall Security	End to end security, Client to resource encrypted	Edge to client Client to VPN gateway
Accessibility	Anytime anywhere access	Limited to well-defined user base
Cost	Low – no client software	High – managed client software
Installation	Plug n play, no sw/hw install	Difficult, client sw/hw installation
User Simplicity	User-friendly - browser	Challenging for non-tech users
Applications	Web, email, file-sharing	All IP-based services
Users	Customers, partners, remote users, employees	More suited for internal users
Scalability	Easily deployed and scalable	Scalable on server side, Diff to scale clients

Endpoint Security – Network Access Management

Problem:

- Every networked PC is susceptible to variety of threats
- Email-borne attacks, Worms, Trojans, Spyware, etc.
- Hackers perceive the clients as the weakest points in the network
- Reactive, signature based systems not effective/dependent anymore

Requirement:

- Client software to implement and enforce security policies
- Centralized development and deployment of security policies

Endpoint Security – Network Access Management

Solution:

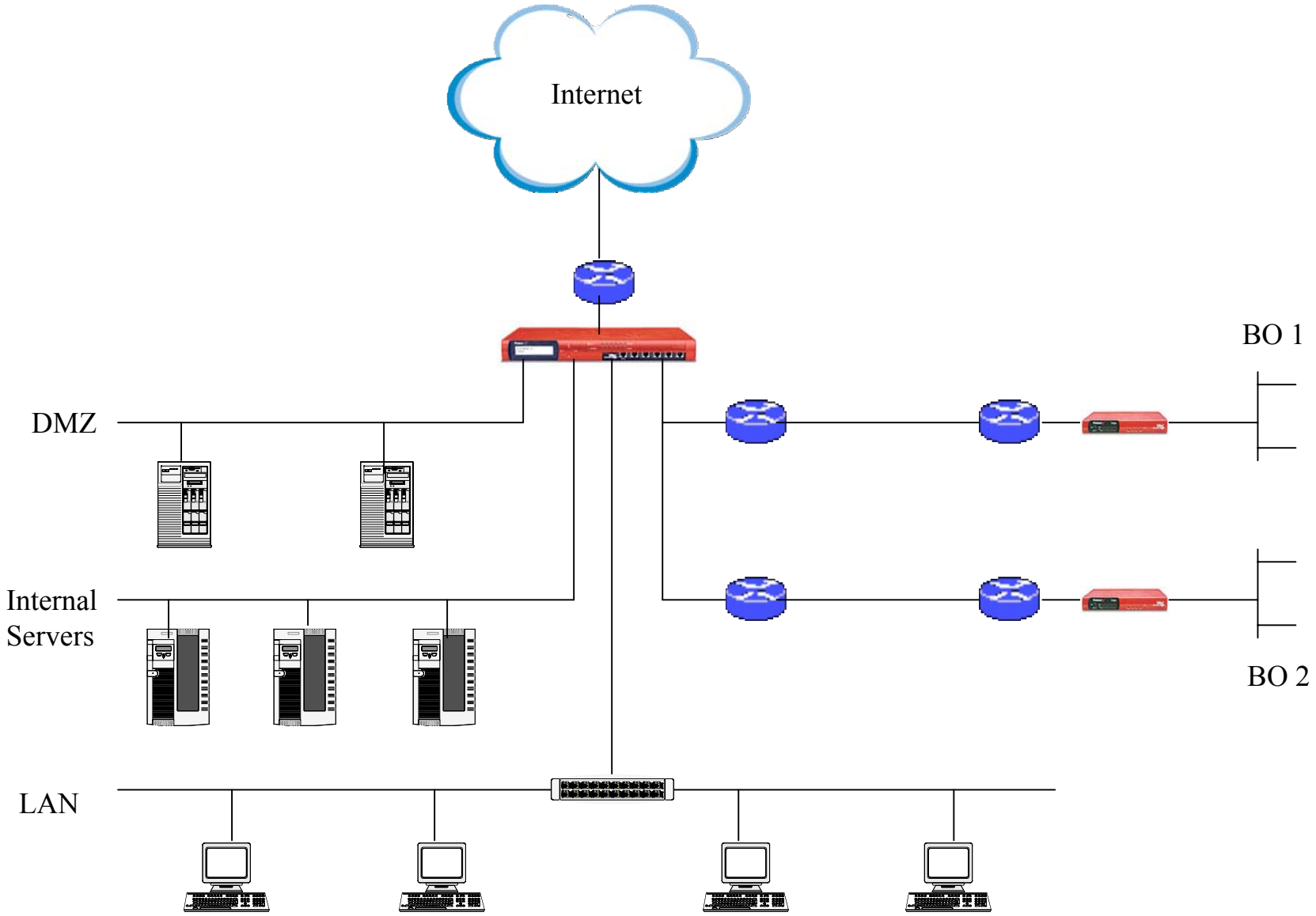
- A system comprised of client and server components that enables organizations to secure and manage endpoints

Features:

- A stateful, stealthing desktop firewall
- Manageable intrusion prevention
- Advanced outbound threat protection (application control)
- Automated policy application (push)
- Assured access policy enforcement

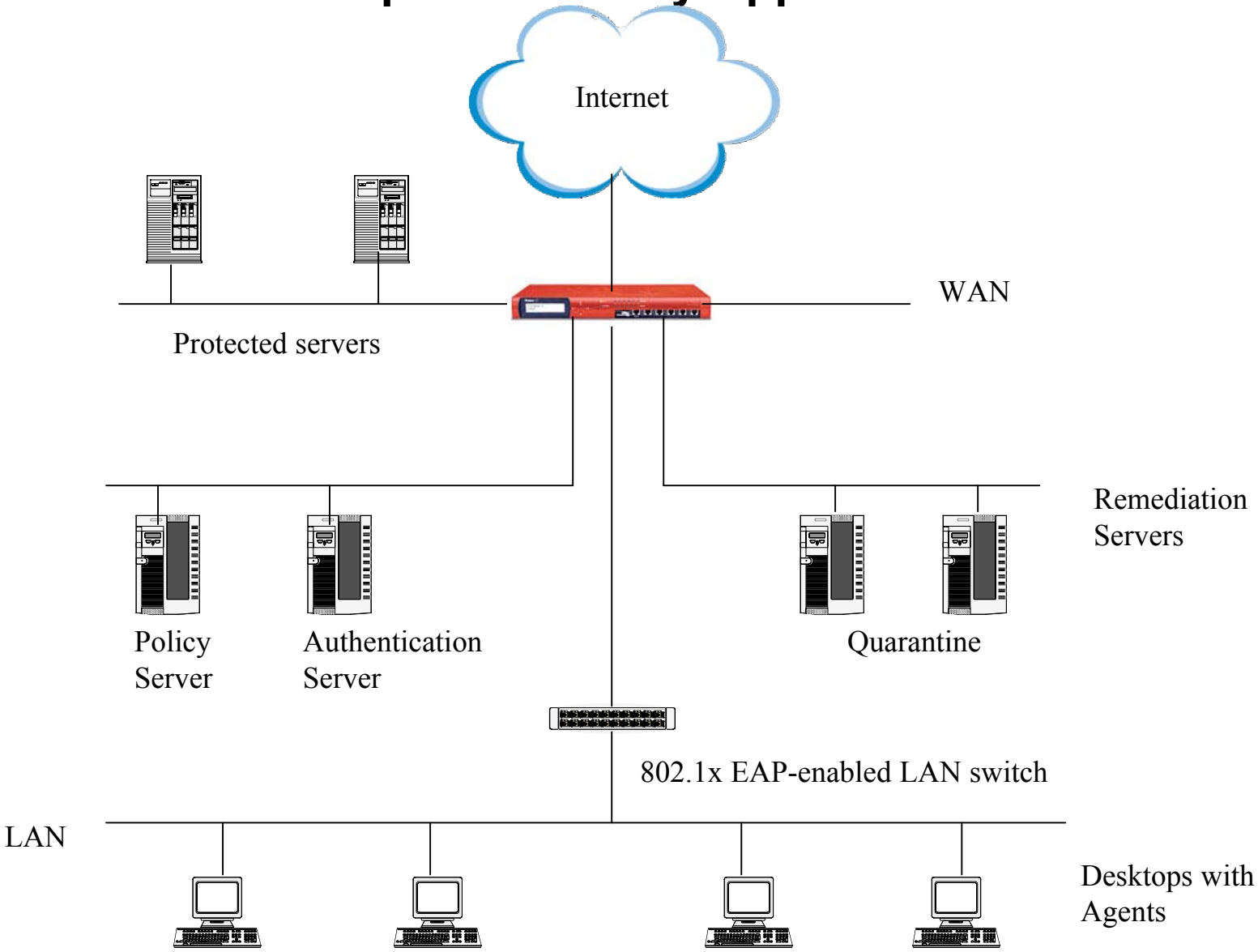
netfiniti

Common Scenario



netfiniti

Endpoint Security Application



netfiniti

Network Access Management

How it works?

1. Desktop client starts up with the machine.
2. The client opens a secure connection to the Policy Enforcement server and passes login information
3. Server retrieves policy for the user
4. Checks whether latest policies are applied on the client
5. An access decision is made
6. Allows network access if the client satisfies all policies
7. Denies and/or quarantines the client for further remediation
8. Allows network access after successful remediation

- Works in conjunction with 802.1x EAP enabled network access devices
- Uses endpoint firewall to enforce compliance on non-EAP networks

netfiniti

Proactive Endpoint Security

- Define and deploy a baseline security policy
- Provides instant desktop firewall protection
- Blocks all unsolicited traffic to/from the PC
- Uses stealth technology to make PCs invisible to hackers
- Control how, when, and which resources PCs can access on the network
- Enables very granular least privilege access of network resources
- Safeguards PCs with intrusion prevention with no rule writing
- Blocks traffic containing malicious codes
- Stops execution of any mal-ware it detects on the PC

netfiniti

Outbound threat protection

- Creates inventory of applications that attempt network access
- Only allow the required apps for network access
- Restrict network access by unrecognized programs
- Prevent malicious code from compromising enterprise data
- Ensures approved programs against spoofing, tampering, hijacking

Host Intrusion Prevention

- Blocks buffer overflow & other attacks on PC apps and OS
- Protects hosts against intrusion attempts, unauthorized access
- Screens all network traffic at app layer for malicious codes
- Requires little admin effort to defend enterprise PCs

Assured Access Policy Enforcement

- Enforce compliance with comprehensive security policy before granting any PC access to the network
- Assures that PC had updated AV, critical patches, latest versions of apps
- Assures a PC is not running any prohibited programs
- Supports 802.1x EAP for policy enforcement with other standard based network access equipment
- Total Client Lockdown prevents end users/hackers from altering/disabling software

Vulnerability Assessment

- Overall network infrastructure is assessed to determine any exploitable vulnerability
- Sophisticated tools are used to identify any potential security weaknesses
- Devices assessed include firewalls, routers, servers, etc.
- Tests are performed to identify system weaknesses from both internal and external threats
- Comprehensive report submitted with vulnerabilities found and corrective actions to be taken
- Should be performed at regular intervals or after any major changes

Penetration Testing

- Attempt to scrutinize the true strength of an organization's security infrastructure against a real attack
- Assume the role of a real intruder and attempts to breach the network in a controlled and safe way not affecting your services
- Launches a series of attacks on the network using commonly used techniques
- Various commercial and open source "hacker" tools will be employed during the tests

Penetration Testing

Benefits:

- Identify weaknesses and exploit the vulnerabilities as an attacker would
- Robustness of entire network against such attacks is thoroughly checked
- Results reveal a realistic view of how the existing infrastructure reacts to actual attacks
- Provides a realistic picture of the state of your organization's security infrastructure

Security Audit

- Audits are conducted to ascertain security status of network infrastructure
- Ensure compliance with current security policies and standards
- Complete audit of security policies, procedures, systems as per BS 7799
- Approach is designed to cover all aspects of security including People, Processes and Technology
- Active testing of system procedures and controls
- Ascertain if procedures are being implemented and followed by all staff
- Both external and internal audit samplings are performed

Security Audit

Report Contents:

- A full technical report of the results of the testing and inspection
- Recommendations for taking remedial corrective actions
- The auditor's statement regarding compliance with prescribed standards
- Executive summary giving a clear understanding of all business risks as per current state of the organization's security

netfiniti

THANK YOU!

ritesh@netfiniti.com.np