E-Module

Class : MSc (IT) Semester 4th

Subject: Network Security

Gurmeet Singh

Associate Professor,

PG Department of Computer Science & IT

Hans Raj Mahila Maha Vidyalaya, Jalandhar.

Chapter 1: Defense in Depth

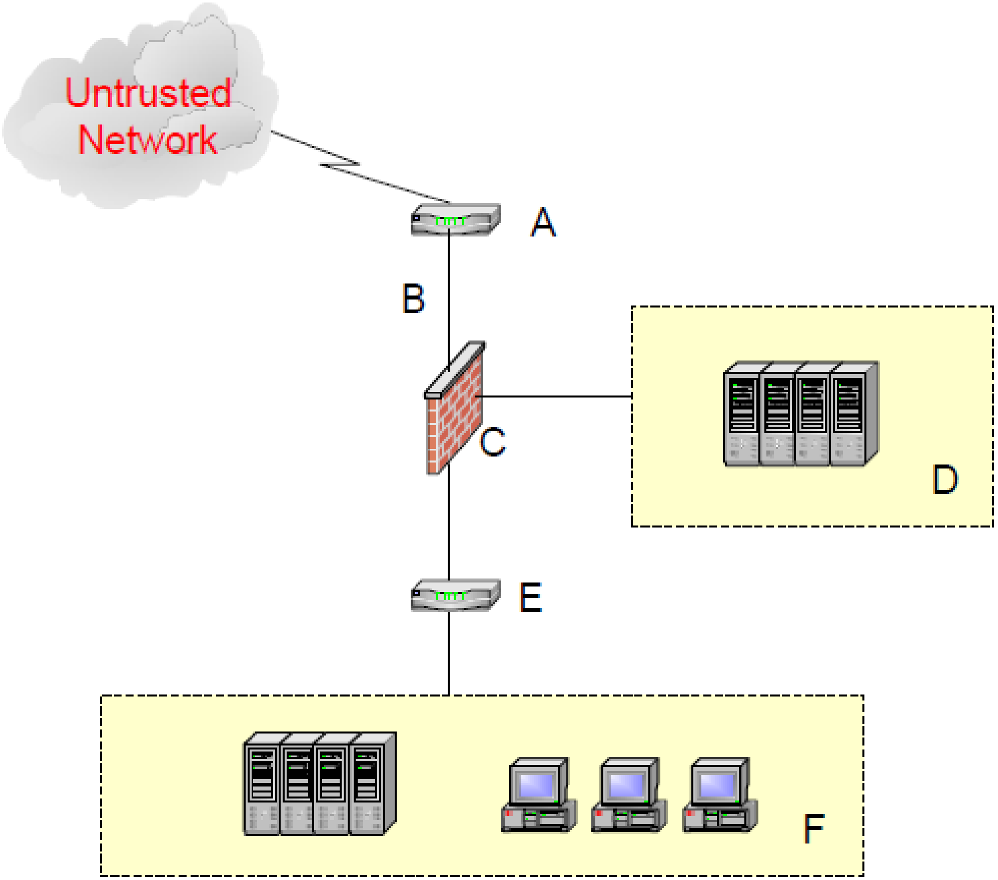
Terms of the Trade

- The Perimeter
- Border Router
- Firewall
- Interior Router
- Intrusion Detection System(IDS)

Terms of the Trade (contd..)

- Virtual Private Network (VPN)
- Demilitarized Zone (DMZ)
- Screened Subnets
- Defense in Depth

The Perimeter



Chapter 2: Static Packet Filtering

- It can be used along with defense in Depth
- It can be implemented on

(a) Hosts

(b) Servers

(c) Firewalls

(d) Routers

Static Packet Filtering (contd..)

- Ingress Filtering & Egress Filtering
- It simply blocks the 90% unwanted traffic
- The job of Firewall gets reduced
- Speed of filtering is quite fast
- One must try to implement it on Border Router.

Cisco ACLs for Packet Filtering

- By default, deny rule applies
- Always list specific rules at the upper end while general rules at the bottom.

The Cisco ACL can be

(a) Standard ACL

(b) Extended ACL

(c) Reflexive ACL

What is Ingress Filtering?

- Always deny reserved IPs
- Always deny your internal IPs
- Deny loopback address
- Deny Broadcast address
- Deny Multicast Address
- Permit only which is required.

What is Egress Filtering?

- Permit only your own IPs.
- Always deny critical local use IPs

Try to use “***deny any log***” at the end of CISCO ACL to store the information in log file.

Comparison of different types of ACLs

Standard ACL	Extended ACL	Reflexive ACL
Standard ACL filters on the basis of Source IP address.	It filters traffic on the basis of source Address, Destination Address, Protocol type, Port Number, Flags etc.	It being the dynamic in nature gets generated and deleted. It does not support TCP flags. However, it is the only one by which UDP and ICMP (connectionless) traffic is filtered.
It can be numbered or named list	It can also be numbered as well as named.	It can only be a named ACl

Standard ACL

Advantages

- Fast
- Use for Blacklisting of single IP or network.
- Supports Ingress/Egress Filtering

Disadvantage

- Filtering only on the basis of source IP
- Vulnerable to source spoofing/ source routing
- Although “deny” is correct but “permit” using standard ACL is like opening a big hole.

Extended ACL

Advantages

- Provides more control than standard ACL
- Allow the use of “state” of protocol.

Disadvantage

- Vulnerable to source spoofing/ source routing
- Problems in filtering in case of “fragmented” data

Advantages/Disadvantages of Static Packet Filtering

- Does not affect the performance of the network.
- Already a part of many Operating Systems
- Simple and best method for filtering majority of unwanted traffic.

- While filtering, examine only network and lower layers.
- No information about payload of the packet data.
- No information about “state” of the protocol.
- Order of rules become cumbersome after a number of rules.

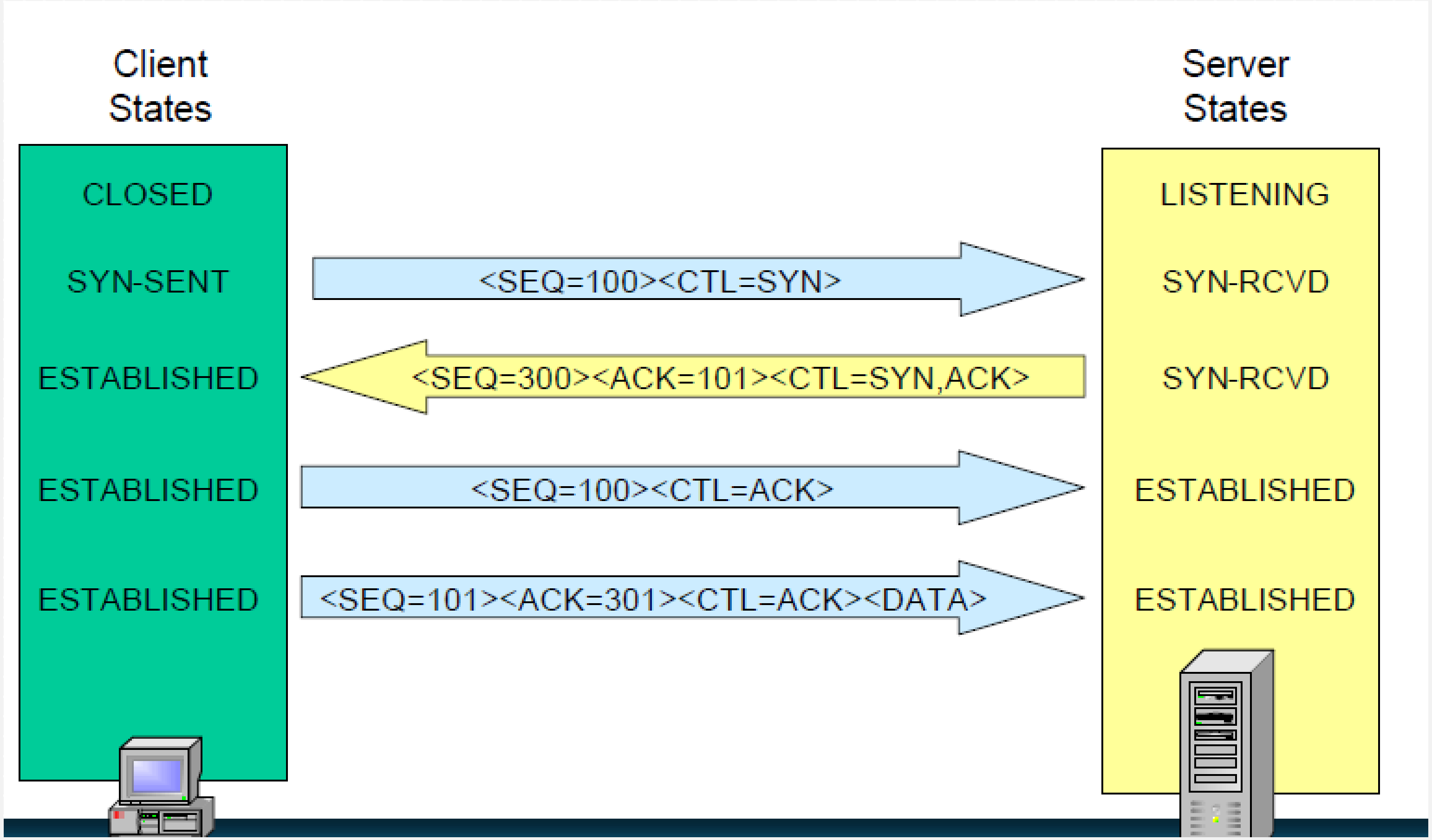
Reflexive ACL

- Aware about “state” of the protocol thereby enhancing performance.
- Already included in so many Operating Systems
- Fully SMP compliant.
- Examine only network and lower layer headers.
- No information about packet payload.
- IP spoofing possible.
- Ordering of rules is difficult to maintain.
- Poses risk in case of connection establishment without 3-way handshaking.

Chapter 3: Stateful firewalls

- Filters traffic based on layer 4 and below.
- Uses Application layer packet inspection
- Use of “state table” to keep track information about established communications (TCP).
- Provides faster filtering than proxy firewalls.
- Comparatively less secure than proxy firewall as only application level connection establishment information is used.

TCP 3-way handshaking



Concept of “state” in UDP

- UDP being the connectionless protocol, it has no visible concept of state.
- State is maintained in pseudo manner.
- Table entries are deleted on time out.
- ICMP is used fro error correction.

Concept of “state ” in ICMP

- ICMP being a connectionless, no :state”
- It is used by both the TCP and UDP
- For layer 4 protocols, it is one way response.
- Ping type request/response is easier to track
- Table entries are deleted on time out basis.

Special Multimedia Protocols

- Multimedia protocols create two or more channels to communicate.
- These mutiple channels are controlled by TCP
- Support in firewall is always on per-protocol basis
- Not application aware

Stateful Firewall Review

- Fast
- More secure than static packet filtering
- Less secure than proxy firewall
- Stateful inspection is application specific
- May need to open holes in case application not supported
- Susceptible to covert channels on open ports

Various Stateful Firewall in market

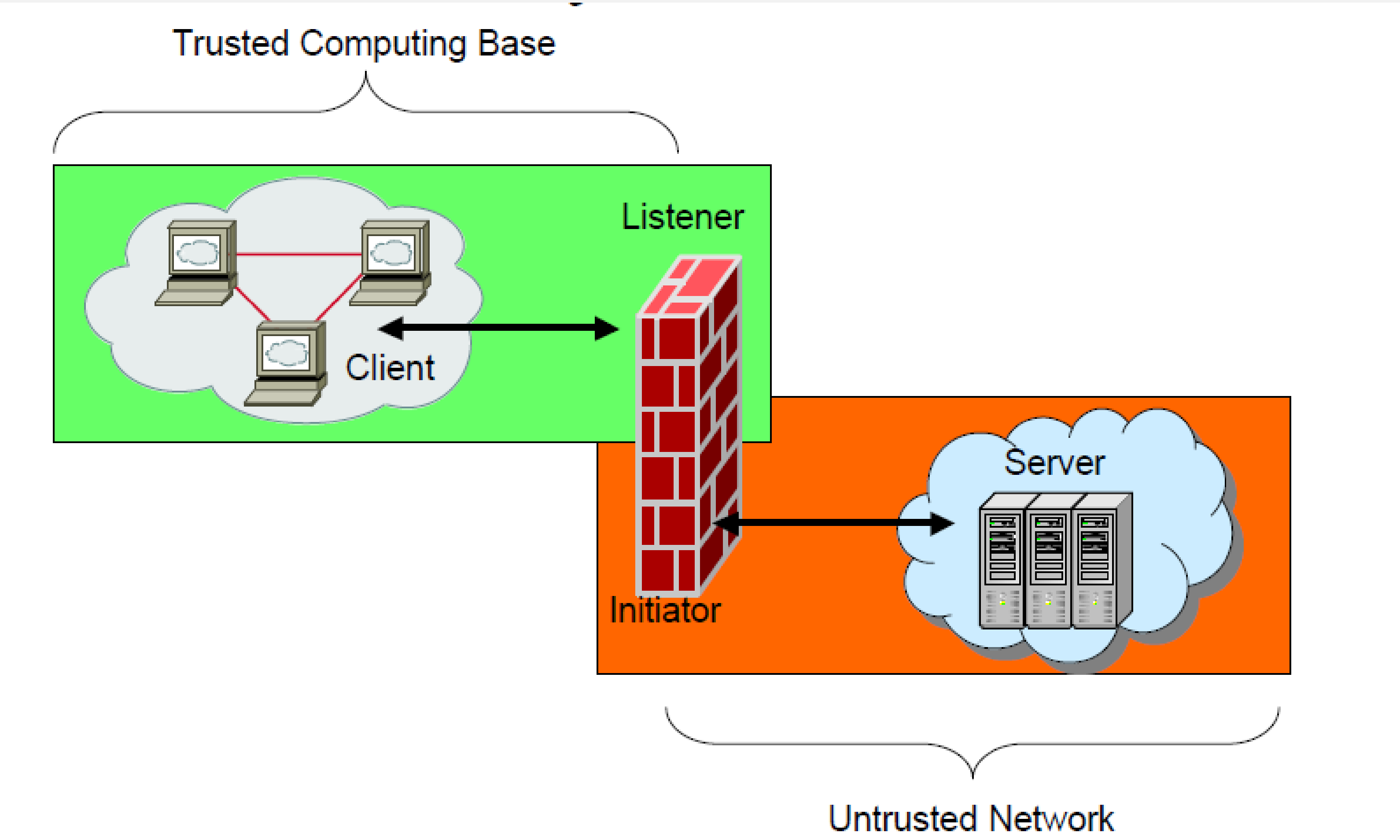
- Cisco Reflexive ACLs
- Netfilter/IPTables
- Checkpoint firewall-1
- CISCO PIX Firewall
- NetScreen

Chapter 4: Proxy Firewall

What is Proxy?

- An application designed to act as the go-between
- Accepts request from client (may filter)
- If allowed, pass request to server
- Receive response from server
- If allowed, pass response back to the client.
- It acts as both client and server with reference to initiator and listener.
- No end to end direct communication.

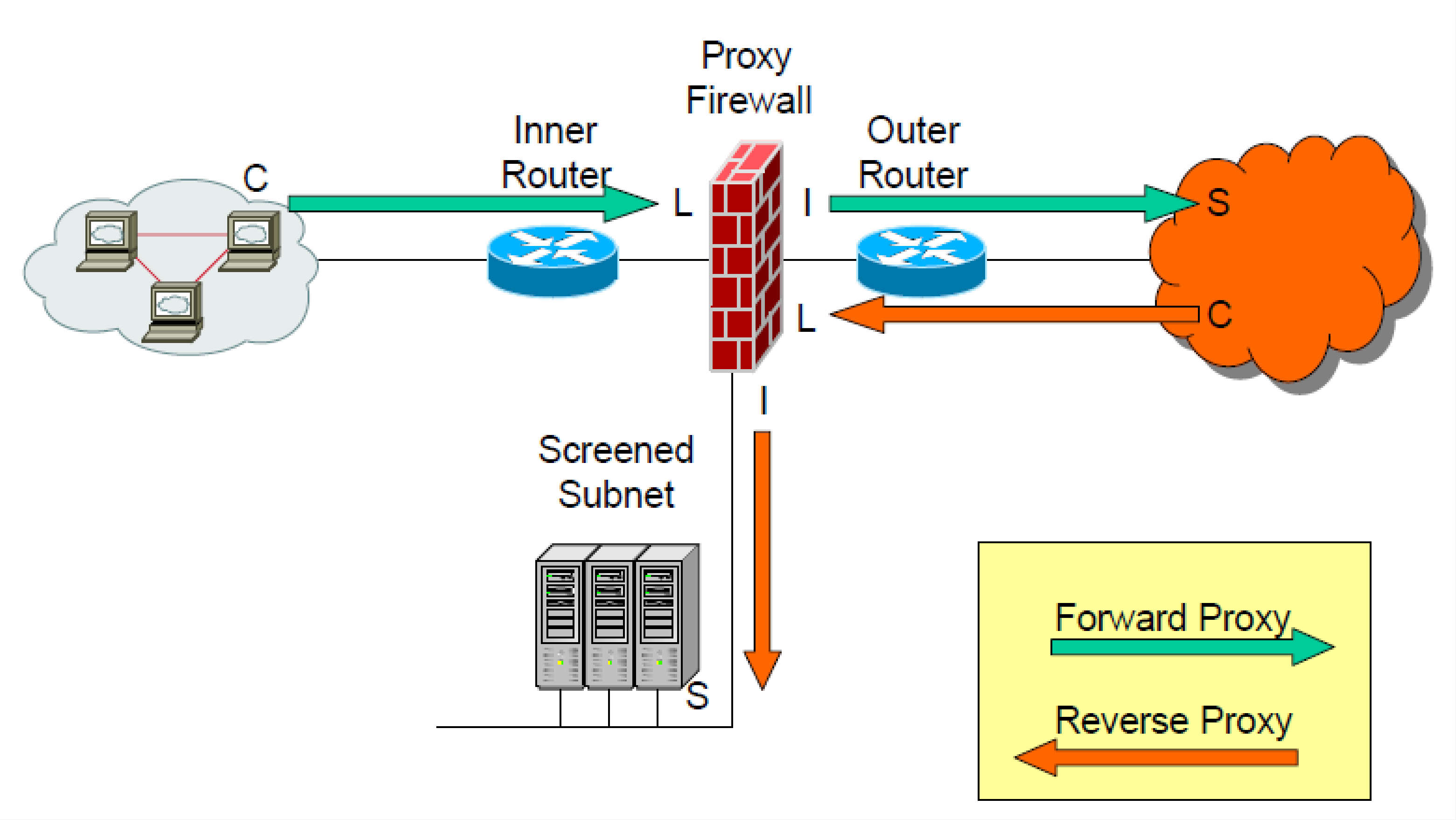
Proxy Firewall



Proxy Types?

- Forward Proxy
- Reverse Proxy
- Circuit level Proxy
- Application level Proxy
- Cutoff Proxy

Forward/Reverse Proxy



Circuit Level Proxy Firewall

- Validates and monitors sessions (Layer 5)
- Verifies proper RFC 3-way handshake
- Verify legitimacy of sequence numbers in establishing connection
- Expand capabilities over SI/Packet Filter (Port No, Ips, protocols, userID, Time of the day)

Application Level Proxy Firewall

- Application specifies proxies
- Prevent direct connection between trusted and untrusted
- Proxies examine entire packet – can filter at application layer.
- Implemented for each service to be analyzed

Cutoff Proxy

- Verifies RFC 3-way handshake
- Limited application based authentication
- Switches to dynamic packet filter mode after connection/authentication complete
- Does not break client/server model for duration of connection

Advantages of Proxy Firewall

- Shielding of Internal addresses.
- Robust logging support
- Enforcement of User policies (supports authentication)
- Application awareness
- Strong application proxy check fields before forwarding.

Disadvantages of Proxy Firewall

- Slower than static packet filtering
- Proxy required for every application or protocol.
- Vulnerable to OS and bugs in applications
- More complex to install, operate and maintain

Summary of Firewalls

- Network Security is the right balance between trust performance
- As you move higher in OSI model, more processing required.
- As you move higher in OSI model, more protection required.
- Newer computing technologies are narrowing gap in the performance.

Chapter 5: Security Policy

Security Policy is the blueprint of effective security.

- It provides means by which effective Defense in Depth is achieved.
- Provides authority for executing CND
- Requires support and commitment of senior officials
- Must be enforceable

How to develop Security Policy?

Obtain senior management buy-in

Assessment if external laws and regulations

Assessment of external and internal strategic plans

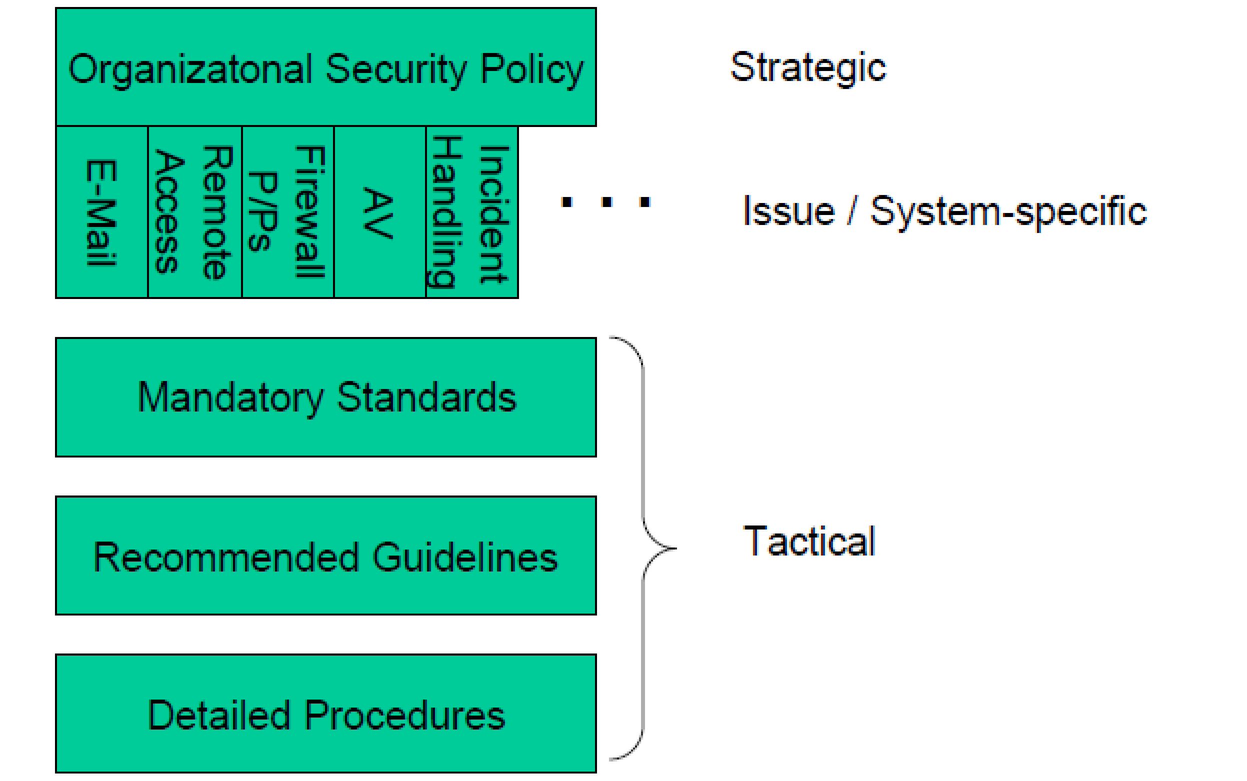
Assessment of internal policies, standards, guidelines and procedures

Identify policy gaps

Draft necessary policy

Publication of policy by senior management

Recommended structure of developing Policy at Enterprise level



Developing Policy

- Identify Risk involved
- Communicate your findings
- Create/update policy as required
- Determine Policy Compliance
- Sound out the organizations’ rules and culture.

Key elements of Policy

- Authority
  - from where the policy draw
    - Signature of individual that have authority
- Scope of policy
  - who, what , where
- Expiration of policy
  - when

Hallmarks of Good Policy

- It should be unambigous, specific and clear

There should not be any ambiguity in the statements of written policy. It must be clear that upon whom the policy is going to be implemented.

- Concise
- Realistic

The policy should be the realistic one so that it should not become *unenforceable*

Perimeter Considerations

Presumption of Privacy

Know organizational expectations

Know applicable laws and regulations

Get the lawyers involved

Capture in your policy and procedures

Publicize the policy

Involve law enforcement

Perimeter Considerations (contd..)

Incident Handling

Policy and procedures need to be clearly spelled

Immediate action drill

Appropriate notifications

Roles and responsibilities

A detailed process flow, that is practiced and refined.

After action review and adjustment.

Chapter 6: Network Intrusion Detection

Basis of Intrusion Detection System

There are two types of Intrusion Detection Systems.

1. Host based Intrusion Detection System
2. Network Intrusion Detection System

Host based IDS

- Monitors specific system and interfaces
- Log analyzers
- File integrity software

Network based IDS

- Monitors network segment
- Examines network traffic
- Detects scans, probes and attacks

Two basic IDS methods:

Signature based ID

Statistical anomaly based ID

NIDS (Signature Matching)

Network based IDS signature

- A pattern of network traffic to be matched.
- Generated a response (Alert, Log, Defensive Action)
- Signatures adapted to your environment (Running DNS, IIS, UNIX)
- Vendor specific depth of analysis
- Updating signatures

NIDS (Tuning your system)

- Specific signatures

  More accurate in positive,

  Resource Intensive

  More likely to miss a morphed attack [false negative]

- General signatures

  More likely to catch morphed attack

  Less resource intensive

  More likely to generate false positives

NIDS (Tuning your system) contd..

- Tuning and IDS system is critical
- Finding the balance is the art

NIDS (Alert, Logging and Reporting)

- Signature Matched or Anomaly Detected
  - Alert (Analyst Console, Email, SNMP trap)
  - Logging and Reporting

    Recommended centralized database/repository

    Allows cross sensor correlation

    Helps identify low an slow attacks

  __ Active Response

  - Log analysis and event correlation

NIDS (Outsourcing)

- Many organizations turning to outsourcing
  - Real world example (NMCI)
  - NMCI only a segment of enterprise
  - Correlation of all sensor data required
  - USMC must retain response control

    Faster, more surgical response is goal

    Operational awareness is a critical element

Role of IDS in Perimeter Defense

- Identifying Weaknesses/Vulnerabilities
  - Identify denied activity, policy violations
- Detecting the Insider Attack
  - Unauthorized outbound traffic
- Incident Handling and Forensics
  - Tracking an attack, tuning to a focussed investigation
- Complementing other Components
  - Correlation of network activities

IDS Sensor Placement

- Deploy multiple network sensors
- Placing sensors near filtering devices an on internal network
- Working with Encryption
- Processing in High Traffic Situations
- Configuring Switches
- Using and IDS Management Network
- Maintaining Sensor Security
- Hybrid Firewall/IDS solutions

Thanks