Making The Firewall Fit

- IP address
- Domain names
- Protocols
- Ports

What it Protects You From

- Remote login
- SMTP session hijacking
- Operating system bugs
- Spam
- E-mail bombs
- Source routing

❖ Beberapa hal tersebut diatas merupakan point yang harus di jaga

Security Strategies Implemented

- Default Deny
  - Prohibit all communication that is not expressly permitted
- Default Permit
  - Permit all communication that is not explicitly prohibited
- Least Privilege
  - reduces the authorization level at which various actions are performed
- Defense in Depth
  - security approach whereby each system on the network is secured to the greatest possible degree
- Choke Point
  - forces attackers to use a narrow channel to bypass the network

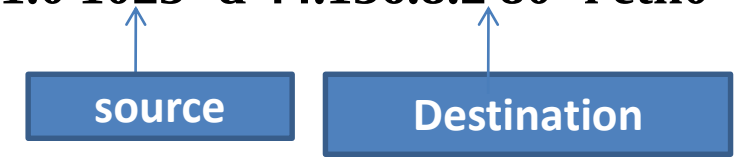
❖ Strategi dalam hal pengamanan

Testing Firewall Configuration

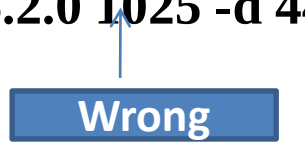
- A faster and easier method is available with the Linux firewall
- Implementation
- Allows you to manually generate tests
- Suppose our local network is 172.16.1.0
- And we allow only TCP connections

Example of Testing Firewall Configuration

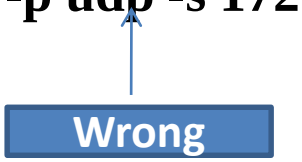
- **# ipchains -C forward -p tcp -s 172.16.1.0 1025 -d 44.136.8.2 80 -i eth0 accepted**



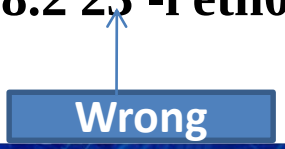
- # **ipchains -C forward -p tcp -s 172.16.2.0 1025 -d 44.136.8.2 80 -i eth0** denied



- **# ipchains -C forward -p udp -s 172.16.1.0 1025 -d 44.136.8.2 80 -i eth0 denied**



- **# ipchains -C forward -p tcp -s 172.16.1.0 1025 -d 44.136.8.2 23 -i eth0 denied**



❖ Contoh testing Firewall Configuration

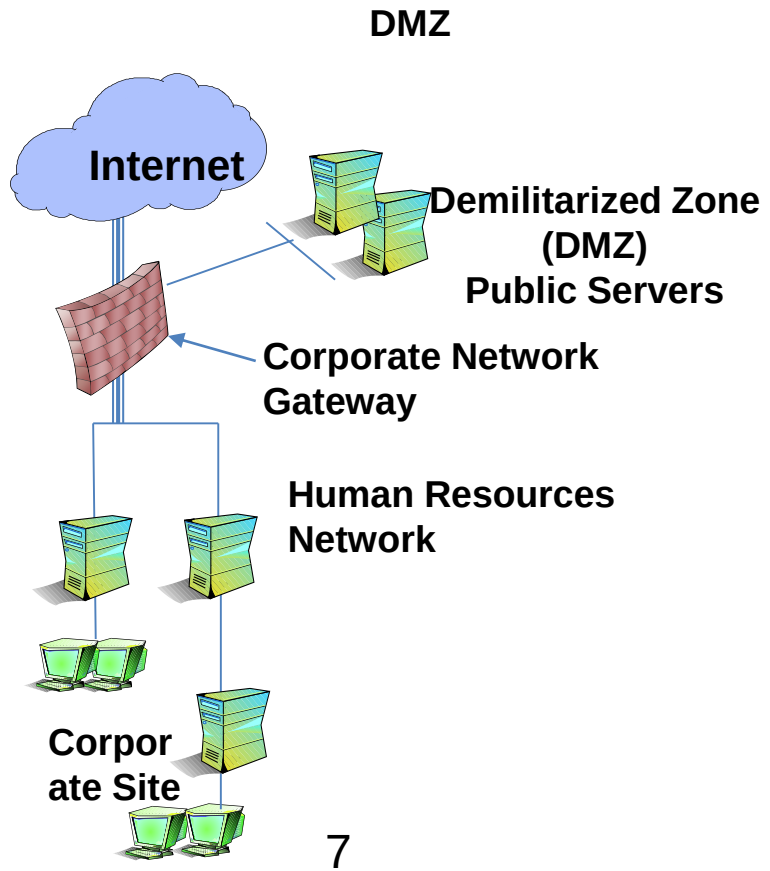
Implementations of FIrewall

- **Software**
  - Devil-Linux
  - Dotdefender
  - ipfirewall
  - PF
  - Symantec …
- **Hardware**
  - Cisco PIX
  - DataPower
  - SofaWare Technologies

❖ Penerapan Firewall dari Software dan Hardware

Firewall Deployment

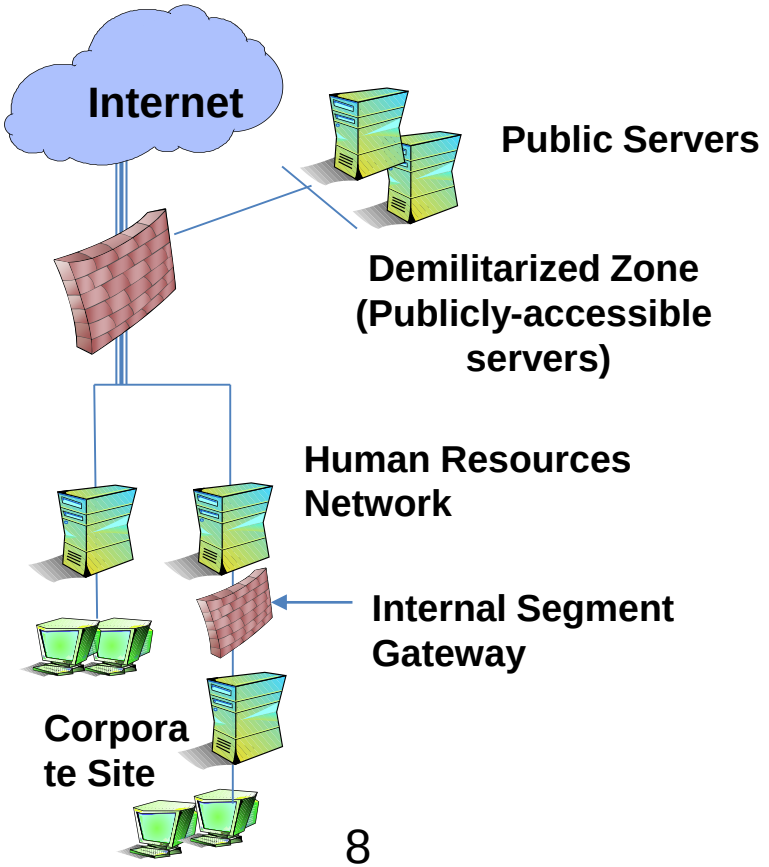
- **Corporate Network Gateway**
  - Protect internal network from attack
  - Most common deployment point



Firewall Deployment : Protect internal network from attack

Firewall Deployment

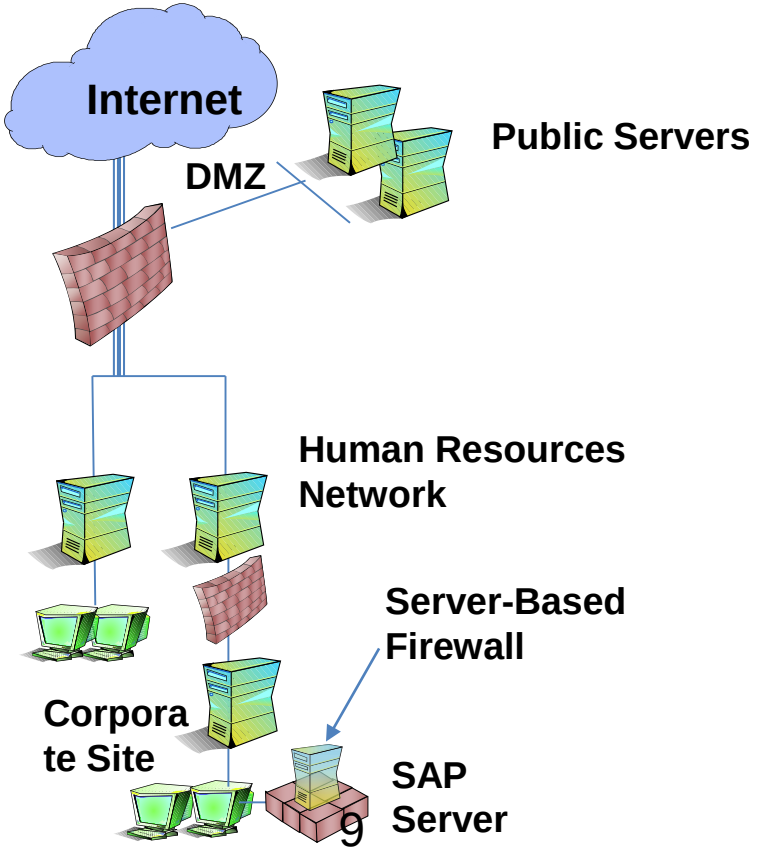
- **Corporate Network Gateway**
- **Internal Segment Gateway**
  - Protect sensitive segments (Finance, HR, Product Development)
  - Provide second layer of defense
  - Ensure protection against internal attacks and misuse



Firewall Deployment : Protect sensitive segments (Finance, HR, Product Development)

Firewall Deployment

- **Corporate Network Gateway**
- **Internal Segment Gateway**
- **Server-Based Firewall**
  - Protect individual application servers
  - Files protect



❖ Firewall Deployment : “Protect individual application servers

Firewall Security Operations

- Administrative Access
- Break Fix Response
- Monitoring and Alarming
- Logging
- Policy/Rule set Administration

❖ Operasi Pengamanan Firewall : Monitoring and Alarming - Logging
“

Firewall Security Operations : Administrative Access

- **What is Administrative access?**

  Administrative Access refers to a group's need to gain control over a system for the purpose of discharging their chartered duties. This access includes, but is not limited to: Monitoring, Log Analysis, Break fix support, User administration, Rule/Policy implementation, OS configuration , software/hardware implementation, and patch/upgrade implementation.

  The need of any group to have this control should be carefully considered. Control rights delegated to teams should be clearly stated in your Corporate Security Policy.

❖ Hak Akses dan Kontrol : Point pentingn dalam Firewall Security Operations

Firewall Security Operations : Administrative Access

- **Who might need access?**
  - Support Staff
  - Implementation staff
  - Design staff
  - Network staff
  - Audit or Review staff
  - Many groups depending on your organizational structure

❖ Terdata dan terpantau dari semua aktifitas : *Administrative Access*

Firewall Security Operations : Administrative Access

Types of access

- Read/View
  - Typical need for design or Network staff
- Add
  - Typical needs for Support and/or Implementation
- Change
  - Typical needs for Support and/or Implementation
- Delete
  - Typical needs for Support and/or Implementation
- Audit/Over-site
  - Typical for Audit or review teams

❖ Type akses, dalam Firewall Security Operations, Administrative Access

Firewall Security Operations : Administrative Access

- **Software Access control**
  - Most systems are restrictive
    - Role based access is often missing
    - Inherent user rights of root/admin cause challenges
      - Root/Admin privilege is required to run firewall app
      - Root privilege is same on OS and firewall
    - Access to view often equals access to change or delete
      - Elevation of privileges
    - Organizational roles add complexity
      - The have and have nots vs. need and function

❖ Software Access Control : *Most System are restrictive*

Firewall Security Operations : Administrative Access

- **Products to help provide control**
  - Many and diverse: sudo
  - All have limitations
    - Control commands
    - Create separate user group from root
    - Privilege can be upgraded inappropriately by user
    - Most provide a patch and not the solution
- **Firewall products need to incorporate the required control**

Firewall Security Operations : Administrative Access

- **Passwords**
  - Strong passwords
  - Centralized administration
    - De-centralized management in a large environment is trouble
  - Two factor authentication
- **Physical access**
  - Access points for administration a must
  - Operation Center with strong physical controls

Firewall Security Operations : Break Fix Response

- Business units must have clear notification path
- Organizations must have clear response plan
  - What teams perform support?
    - What support level is each responsible for
      - 1ST LEVEL
      - 2ND LEVEL
      - 3RD LEVEL
    - What privileges do each of these team have

❖ Break Fix Respon ,Pemahaman masing masing dari para peserta pelatihan

Firewall Security Operations : Break Fix Response

- Talent
  - Each group must be properly trained
    - For every product they support
    - Certifications
    - General security knowledge
      - Running firewalls and running them securely are different
    - Procedurally
      - How they discharge their responsibilities properly
        - i.e. Allowable change
        - Break fix clearly defined from change

❖ Break Fit Response,

Firewall Security Operations : Break Fix Response

- Vendor relationships and support
  - Notification path clear to all team members
    - Internal web site a good communication device
  - Support contracts
    - Up to date
    - Inclusive of all products
    - Repercussions of no support agreement
      - Patch update access
      - Security fix access

❖ Penanganan Break Fix Response : “Vendor relationships and support”!

Firewall Security Operations : Break Fix Response

- Interaction with product owners
  - Business units own application and are experts in the business need which typically conflicts with security policy/process
    - Put in a change when fixing a problem
    - Make changes on the BU side that requires a firewall change that is insecure
    - Without regard implement changes that break service and require firewall changes to restore production
      - Re-IP a dB sever
      - Change the communication protocol

Firewall Security Operations : Break Fix Response

- Oversight
  - Does the fix change security
    - Policies are done slowly with forethought
    - Break fix is done fast and in a vacuum
  - Does the fix change the design
    - Updating designs/risk matrixes
    - Who is responsible
    - How do we ensure it is done?

❖ Break Fix Response : the fix change security, the fix change the design

Firewall Security Operations : Monitoring & Alarming

Firewall Monitoring Problems

- OPSEC
  - Greatly limits a groups ability to perform good monitoring
  - Monitoring and communication fly in the face of “need to know” security concepts
- Products
  - Geared toward functionality—not security
  - Host Agents often open serious security holes
    - Remote login access
    - Random ports
    - Root level access for tools
- Customer disclosure
  - Customer want access to tools to track system performance
  - Good monitoring often discloses sensitive information

Firewall Security Operations : Monitoring & Alarming

- Who performs monitoring?
  - Requires access
  - Discloses information
- Is access being delegated to others for any reason?
  - Who has access?
  - What controls are in place?
  - What rights have they been delegated?
- What product is being used?
  - Check for encryption and transport protocol
  - Check loading and maintenance plans

Firewall Security Operations : Logginng

- **Logging is very important**
  - **Provides history of access**
  - **Provides attack information**
  - **Provides for Policy audit checking**
  - **Provides trending analysis for capacity planning**
  - **Provides evidence for events**

❖ *Logging : History Very Important , Attactk Information,Policy Audit Checking*

Firewall Security Operations : Logginng

- Firewall Logging Problems
  - Many firewalls do not log effectively
  - Extremely large files
  - Difficult to manage and review
  - Products have logs written to different files
  - Access to many logs requires root access to firewalls
  - Log analysis products are add-on and expensive
  - Few organizations log effectively

- Logging :” Firewall Logging Problems - Many firewalls do not log effectively

Firewall Security Operations : Logginng

- Logging Methods
  - Local
    - Directed to files (poor from a security perspective)
  - Remote
    - Syslog
      - Udp protocol is not reliable or secure (new syslog is better)
      - Cannot be used as evidence: not credible
    - Separated management network
      - Some products are managed and logged in an isolated network
      - Logging can be reliable and separate from firewall system
  - Firewall products often account for good logging
    - Ask good questions

❖ Logging Methods : Local, Remote, Firewall

Firewall Security Operations : Policy/Rule set Administration

- General security Policy Guidelines
  - Least Privilege Concept
    - Allow least amount of access to allow someone to complete their duties
  - Government orange and red books
    - Detailed security controls
    - Great reference material

Firewall Security Operations : Policy/Rule set Administration

- General security Policy Guidelines
  - Modems
    - Very insecure
    - Look for them on routers as a backup
    - Remote vendor administration
    - Banned by policy, allowed only by documented exceptions
  - Protocols
    - Tcp is the most easily controlled
      - Session oriented
      - Firewall compatible

Firewall Security Operations : Policy/Rule set Administration

- General security Policy Guidelines
  - Protocols continued
    - UDP
      - Use as little as possible
        - ❑ Needed for some require and some desired functions
        - ❑ Monitoring, logging, snmp management
    - Netbios
      - Easily attacked
      - Bad trust model

Firewall Security Operations : Policy/Rule set Administration

- General security Policy Guidelines
  - Authentication
    - Passwords
    - Two factor
    - Controls
    - CA and digital certificates
  - Encryption
    - Data classification
    - Strength
    - Where/when

Firewall Security Operations : Policy/Rule set Administration

- General security Policy Guidelines
  - Allowed Services
    - Should be known and highly controlled
      - www
      - http://
      - smtp
      - vpn service
      - dns
    - Avoid inherently insecure services where possible
      - Finger
      - Telnet
      - ftp
      - nfs
      - Remote admin tools (some have good controls others do not)

Defining Audit Scope

- Firewall Documentation
- Approval Procedures and Process
- Firewall Rule Base
- VPN
- Layer Seven Switching
- Internal Testing
- External Testing

- Audit Scope : Firewall, VPN, 7 Layers

Firewall Auditing Methodology

Phases

I. Gather Documentation
II. The Firewall
III. The Rule Base
IV. Testing and Scanning
V. Maintenance and Monitoring

Phase I – Gather Documentation

- Security Policy
- Change Control Procedures
- Administrative Controls
- Network Diagrams
- IP Address Scheme
- Firewall Locations
- IPS Capable
- Firewall Vendor
- Software Version and Patch Level
- Hardware Platform
- Operating System Version and Patch Level
- Administrator training and knowledge

- Phase 1, harus dapat dilaksanakan dan dijalankan

Phase II – The Firewall

- Three “A’s”
  - Authentication
    - Local / Remote
  - Access
    - Logical / Physical
  - Auditing (logs)
    - Local / Remote
- OS Hardening

Phase III – The Rule Base

- Based on the Organization's Security Policy
- Review each rule
  - Business reason
  - Owner
  - Host devices
  - Service Ports
- Simplicity is the key
- Most restrictive and least access

- Phase III : The Rule Base : : "Based on the Organization's Security Policy

Phase III – The Rule Base

- Rule order (first out)
  - Administration Rule
  - ICMP Rule
  - Stealth Rule
  - Cleanup Rule
  - Egress Rules
- Logging

Phase IV – Testing & Scanning

- Determine & Set Expectations
- Scan the firewall
  - Nmap
  - Firewalk
- Scan host behind the firewall
  - Nessus
  - ISS
- Ensure results match expectations

Phase V – Maintenance & Monitoring

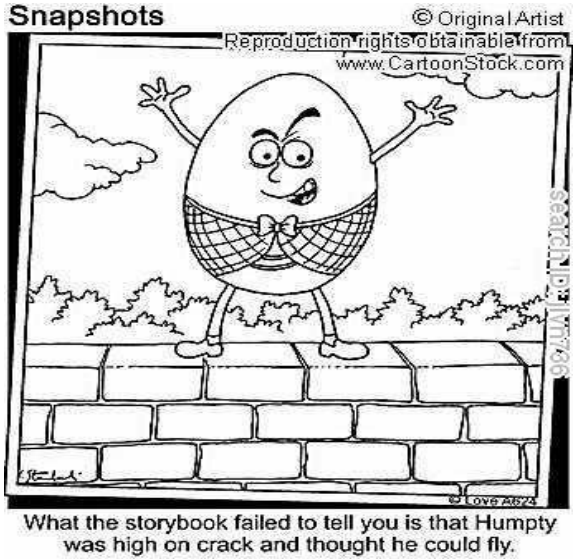
- Change Management and Approval
  - Is the process documented?
  - Is the process being followed?
  - Is there evidence of process?
- Disaster Recovery Plan
  - Formal?
  - Backup and Recovery Procedures
- Firewall Logs
  - Reviews
  - Storage and archival

What a personal Firewall Can Do?

- **Stop hackers** from **accessing** your computer.
- **Protects** your **personal information**.
- Blocks "**pop up**" ads and certain **cookies**.
- Determines which programs can **access** the Internet.
- Block **invalid packets**.

❖ Hal hal yang bisa dilakukan sebagai personal Firewall Can Do ?

What a personal Firewall Cannot Do?



- **Cannot prevent e-mail viruses**
  - Only an antivirus product with updated definitions can prevent e-mail viruses.
- After setting it initially, you cannot forget about it
  - The **firewall** will **require periodic updates** to the rulesets and the software itself.

❖ What a personal Firewall Cannot Do, - Cannot prevent e-mail viruses

Future of Firewalls

- Firewalls will continue to advance as the attacks on IT infrastructure become more and more sophisticated
- More and more client and server applications are coming with native support for proxied environments
- Firewalls that scan for viruses as they enter the network and several firms are currently exploring this idea, but it is not yet in wide use

❖ Masa depan Firewall : ‘More and more ‘

Conclusions

- It is clear that some form of security for private networks connected to the Internet is essential
- A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions.

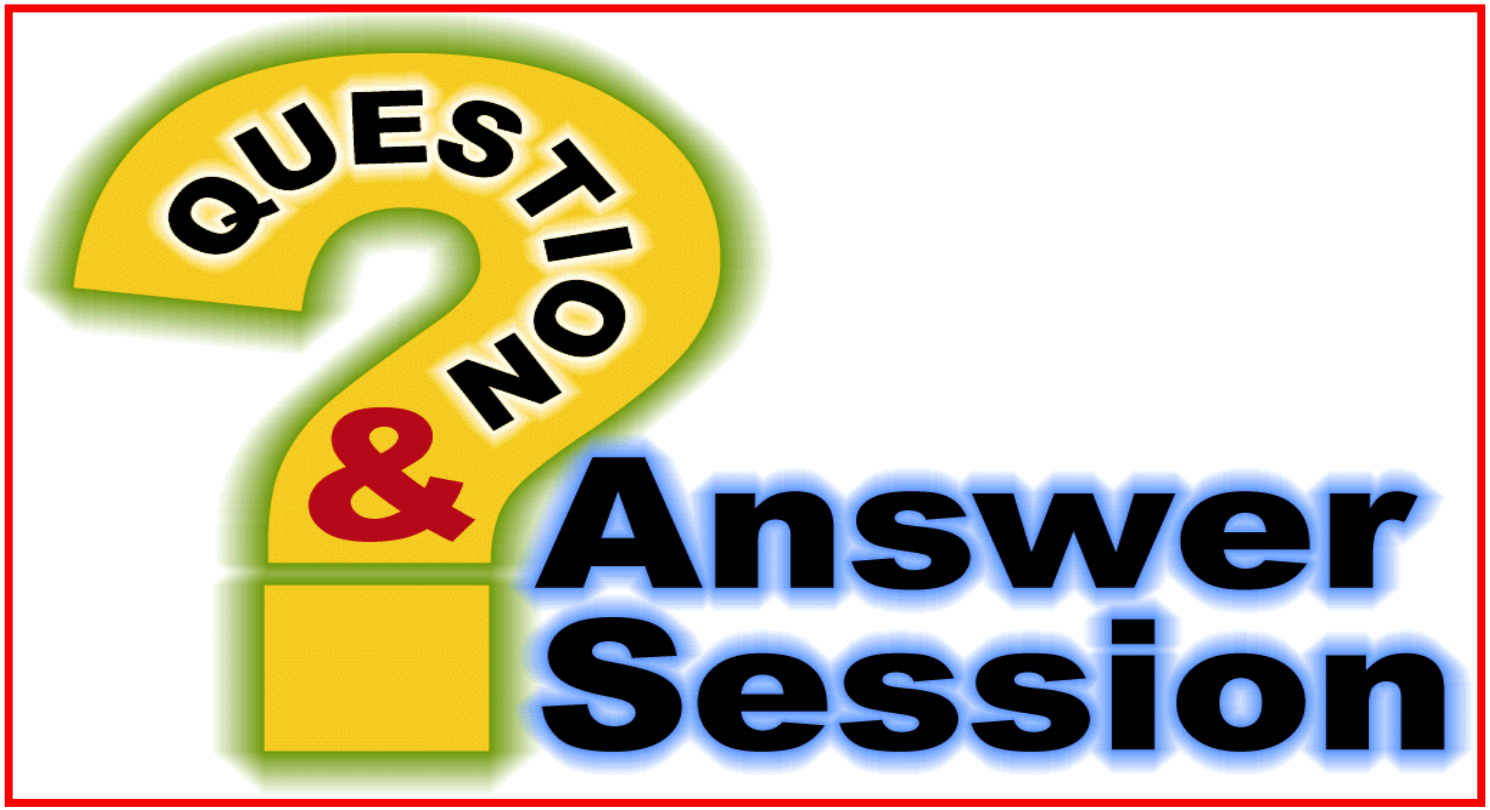
Best Practices

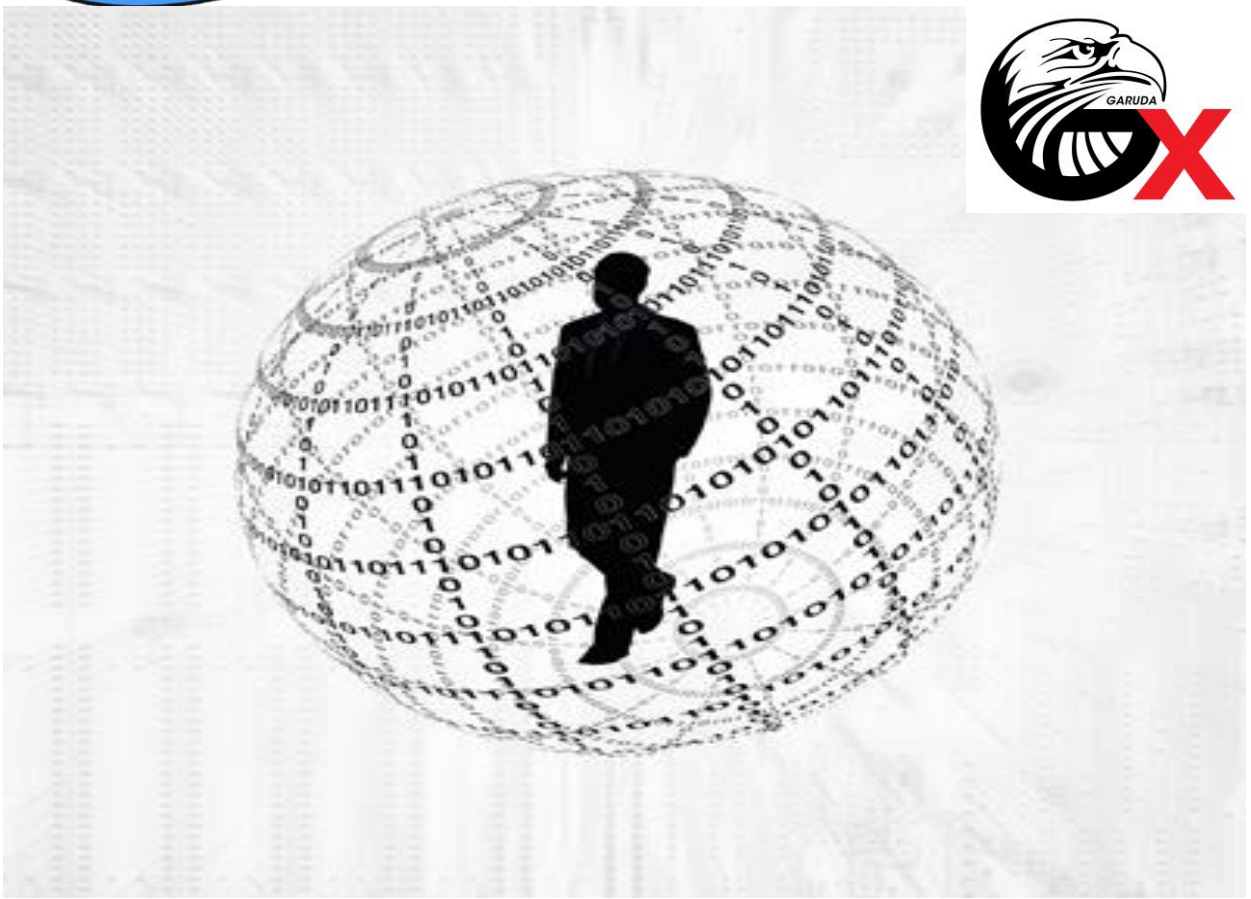
- Create zones of allowable traffic
  - Don’t have one firewall protecting both a publicly accessed system (i.e. email gateway) and an internal system (i.e. email server)
- Get those patches!
- Disable unwanted services
- Set up an IDS

Summary

- http://://www.slideshare.netrubal_9firewall-1985080
- http://www.slideshare.netnetworkingcentralfirewall-powerpoint-presentationqid=416d172b-8227-4034-a12a-03c2a72554df&v=&b=&from_search=7
- http://www.slideshare.netadkpctefirewall-presentationqid=416d172b-8227-4034-a12a-03c2a72554df&v=&b=&from_search=2
- http://www.slideshare.netyogendrasinghchaharfirewall-presentation-16353185qid=416d172b-8227-4034-a12a-03c2a72554df&v=&b=&from_search=3
- http://www.slideshare.netemin_ozfirewall-presentation-m-emin-zgnsrqid=416d172b-8227-4034-a12a-03c2a72554df&v=&b=&from_search=11
- http://www.slideshare.netamuthavallinachiyarfirewall-26050575
- http://swww.google.co.idurlsa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjP-fia8cHNAhVFv48KHV6CD6AQFgg-MAM&url=http://%3A%2F%2Fwww.sfisaca.org%2Fdownload%2Fnetwor
- http://swww.google.co.idurlsa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjCyL6b8sHNAhUVUI8KHRs8CIAQFggtMAI&url=http://%3A%2F%2Fwww.isaca.org%2Fchapters1%2FBat

❖ Referensi ……


QUESTION
&
Answer
Session



- **Hatur Nuhun**
- Matur Nuwun
  Terima Kasih
- **Syukron**
  Merci bien
  ありがとう
  Obrigado
- **Dank**
- **Thanks**
- **Matur se Kelangkong**
- **Kheili Mamnun**
- ευχαριστίες
  Danke
- **Grazias**
- 谢谢