Defensive Strategy

Network and Internet Defense

Rangga Firdaus, M.Kom

Identitas Diri

Nama : **Rangga Firdaus, M.Kom**
NIP : 197410102008011015

Pendidikan
S1 Teknik Komputer Univ Gunadarma Jakarta
S2 Ilmu Komputer Univ Gadjah Mada Yogykarta
S3 Teknologi Pendidikan Univ Negeri Jakarta (Progress)

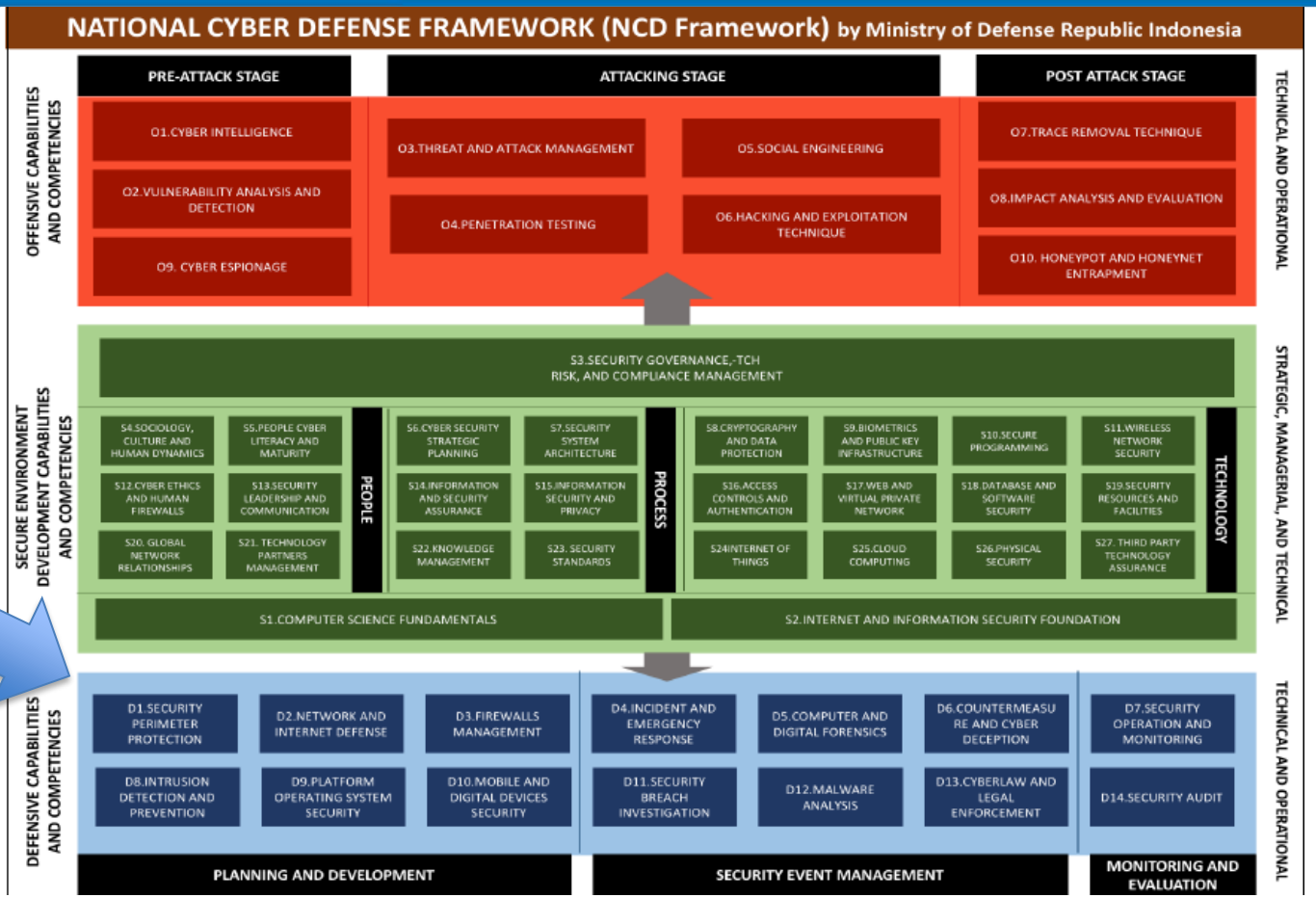
Aktivitas :

- Dosen Ilmu Komputer FMIPA **Universitas Lampung**
- Tim Pembelajaran Daring Indonesi Terbuka dan Terpadu – **Kemenristek Dikti**, Belmawa
- Direktur Pengembangan Wilayah dan Sertifikasi Ikatan Ahli Informatika Indonesia (**IAII**)
- Direktur Konferensi Seminar Asosiasi Pendidikan Tinggi Informatik dan Komputer (**APTIKOM**)
- Koordinator Ikatan Alumni TOT **LEMHANNAS RI** Wilayah Sumatera Bagian Selatan
- Asesor Kompetensi Bidang Informatika , **Lembaga Sertifikasi Profesi Informatika** - BNSP

❖ Pemahaman yang baik, akan menimbulkan aktivitas yang baik, niatkan karena Allah..
❖ Insya allah menjadi amal ibadah , Manjadda Wajadda !!

Cyber Computer Security

NATIONAL CYBER DEFENSE FRAMEWORK



- **3 KOMPETENSI 1.Security Perimeter Protection**
  2. Network and Internet Defense
  3. Firewall Management

HAL PENTING NETWORK AND INTERNET DEFENSE

WHAT(T)

WHY (Y)

WHERE (E)

WHEN (N)

WHO (O)

HOW (W)

DEFENSIVE CAPABILITIES AREA

5.1 (D1) Security Perimeter Protection (D2) Network And Internet Defense (D3) Firewall Management

5.1.1 WHAT(T)

- (D1T-1) Menjelaskan apa yang dimaksud dengan **D1 D2 D3**
- (D1T-2) Mengidentifikasi komponen-komponen pada **D1 D2 D3**

5.1.2 WHY (Y)

- (D1Y-1) Mengemukakan alasan diperlukannya **D1 D2 D3**
- (D1Y-2) Memberikan contoh keuntungan yang diperoleh dari keberadaan **D1 D2 D3**
- (D1Y-3) Memberikan contoh kerugian yang diperoleh jika tidak memiliki **D1 D2 D3**

(D1) Security Perimeter Protection
(D2) Network And Internet Defense
(D3) Firewall Management

DEFENSIVE CAPABILITIES AREA

5.1.3 WHERE (E)

• (D1E-1) Menjelaskan unit organisasi yang bertanggung jawab dalam mengembangkan Security Perimeter Protection

• (D1E-2)Menjelaskan batasan teritori organisasi yang terikat atau harus patuh terhadap Security Perimeter Protection

5.1.4 WHEN (N)

• (D1N-1) Menjelaskan waktu yang tepat bagi sebuah organisasi untuk menyusun Security Perimeter Protection

• (D1N-2) Menyusun jadwal proses penyusunan Security Perimeter Protection

(D1) Security Perimeter Protection
(D2) Network And Internet Defense
(D3) Firewall Management

DEFENSIVE CAPABILITIES AREA

5.1.5 WHO (O)

• (D1O-1) Mengidentifikasi individu atau pihak yang bertanggung jawab dalam menyusun **D1 D2 D3**

• (D1O-2) Menetapkan peranan, tugas, dan tanggung jawab individu dan pihak-pihak yang harus terlibat dalam penyusunan **D1 D2 D3** dalam sebuah organisasi

5.1.6 HOW (W)

• (D1W-1) Menggambarkan metodologi pengembangan **D1 D2 D3**

• (D1W-2) Menjelaskan langkah-langkah yang harus dilakukan dalam menyusun **D1 D2 D3**

• (D1W-3) Menjelaskan rangkaian aktivitas yang harus dilakukan pada setiap langkah pada metodologi penyusunan **D1 D2 D3**

(D1) Security Perimeter Protection
(D2) Network And Internet Defense
(D3) Firewall Management

NETWORK AND INTERNET DEFENSE

PEMBAHASAN

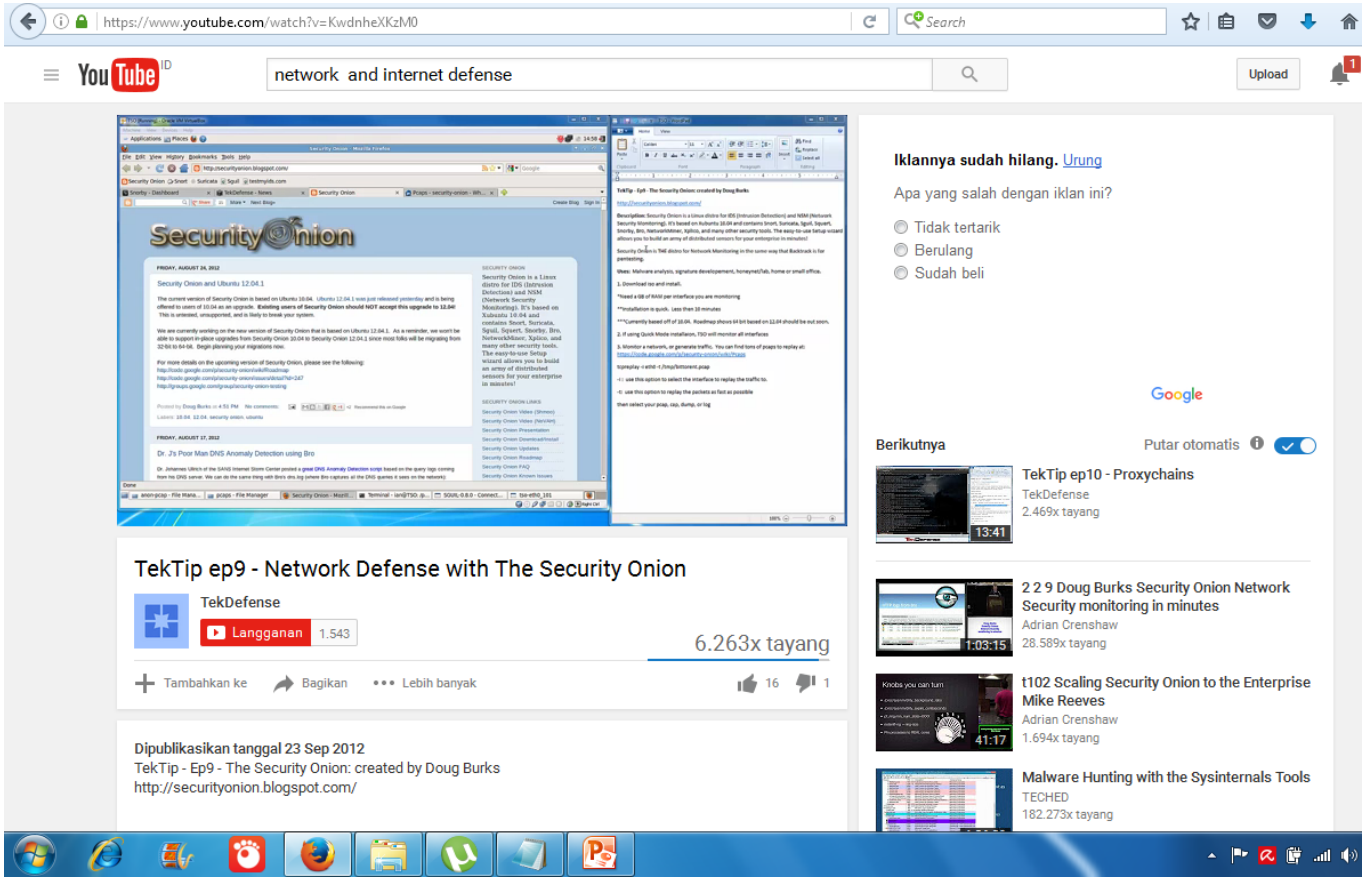
- **INTRODUCTION**
- Using Perimeter Defenses
- Using Microsoft® Internet Security and Acceleration (ISA) Server to Protect Perimeters
- Using Internet Connection Firewall (ICF) to Protect Clients
- Protecting Wireless Networks
- Protecting Communications by Using IPSec

❖ Membahas agenda ke-1 dari 6 agenda yang ada di Network and Internet Defense

CONTOH IMPLEMENTASI NETWORK AND INTERNNET DEFENSE

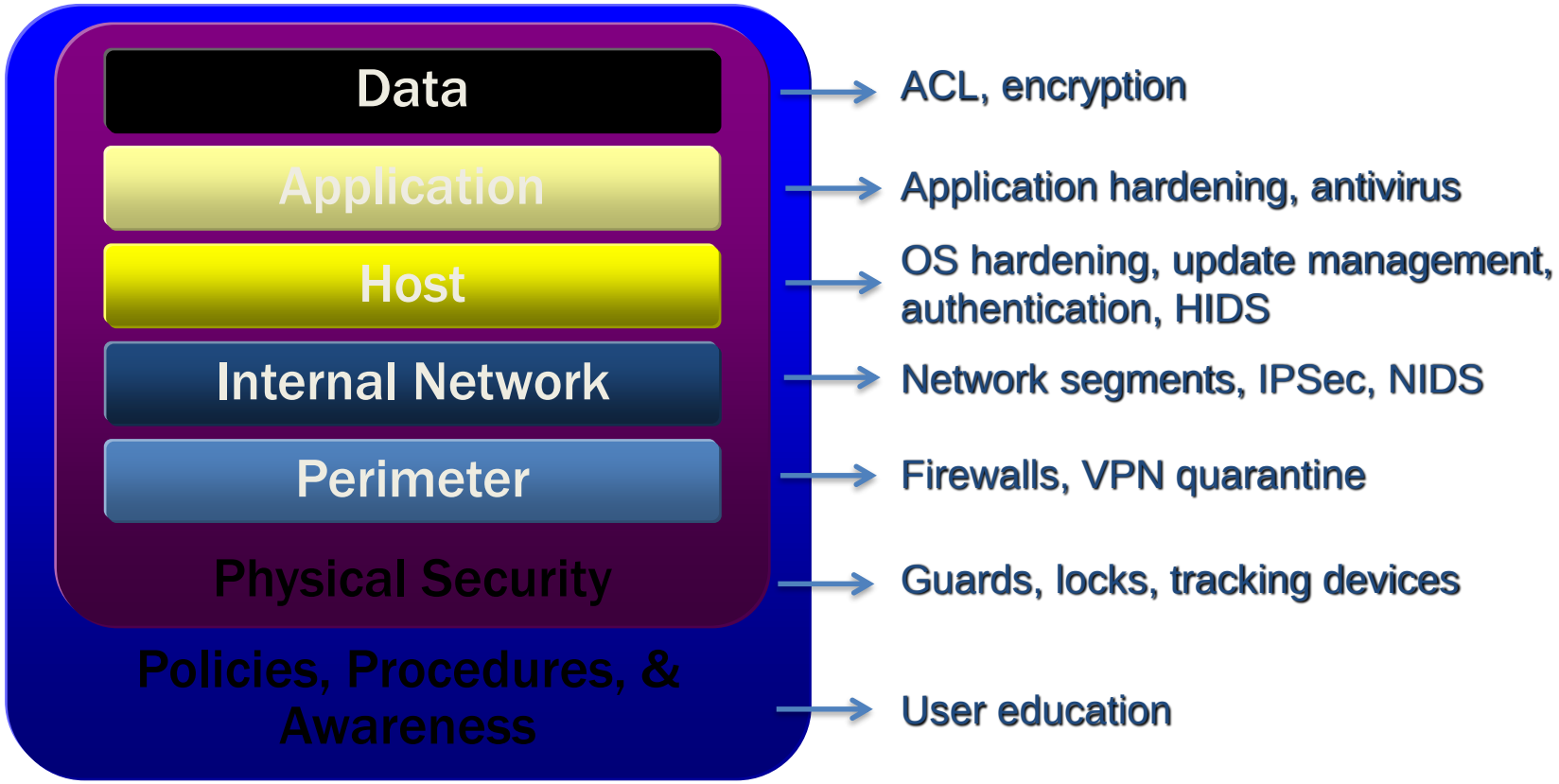
- Berbagai contoh pemahaman dan implementasi dari network and internet defense dapat dilihat dalam bentuk film di youtube maupun yang lainnya.

CONTOH IMPLEMENTASI NETWORK AND INTERNNET DEFENSE



- Berbagai contoh pemahaman dan implementasi dari network and internet defense dapat dilihat dalam bentuk film di youtube maupun yang lainnya.

DEFENSE IN DEPTH



- Memahami lapisan diatas, akan dapat pendeteksian serangan dapat diketeahui dari awal serta mengurangi kesempatan seorang penyerang berhasil dalam kegiatannya

PURPOSE AND LIMITATIONS OF PERIMETER DEFENSES

1. Properly configured firewalls and border routers are the cornerstone for perimeter security
2. The Internet and mobility increase security risks
3. VPNs have softened the perimeter and, along with wireless networking, have essentially caused the disappearance of the traditional concept of network perimeter
4. Traditional packet-filtering firewalls block only network ports and computer addresses
5. Most modern attacks occur at the application layer

❖ 5 Point Penting dari tujuan dan keterbatasan dari perimeter pertahanan

PURPOSE AND LIMITATIONS OF CLIENT DEFENSES

- Client defenses block attacks that bypass perimeter defenses or originate on the internal network
- Client defenses include, among others:
  - Operating system hardening
  - Antivirus software
  - Personal firewalls
- Client defenses require configuring many computers
- In unmanaged environments, users may bypass client defenses

❖ Beberapa Point Penting Perimeter Defense dari sisi Client

PURPOSE AND LIMITATIONS OF INTRUSION DETECTION

1. Detects the pattern of common attacks, records suspicious traffic in event logs, and/or alerts administrators

2. Threats and vulnerabilities are constantly evolving, which leaves systems vulnerable until a new attack is known and a new signature is created and distributed

- Beberapa Point Penting dari tujuan dan keterbatasan Network and Intrusion dari sisi Intrusion Detection

GOALS OF NETWORK SECURITY

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	X		X	X		X
ICF		X				
802.1x / WPA				X	X	
IPSec		X			X	X

- Beberapa hal penting dalam tujuan keamanan jaringan

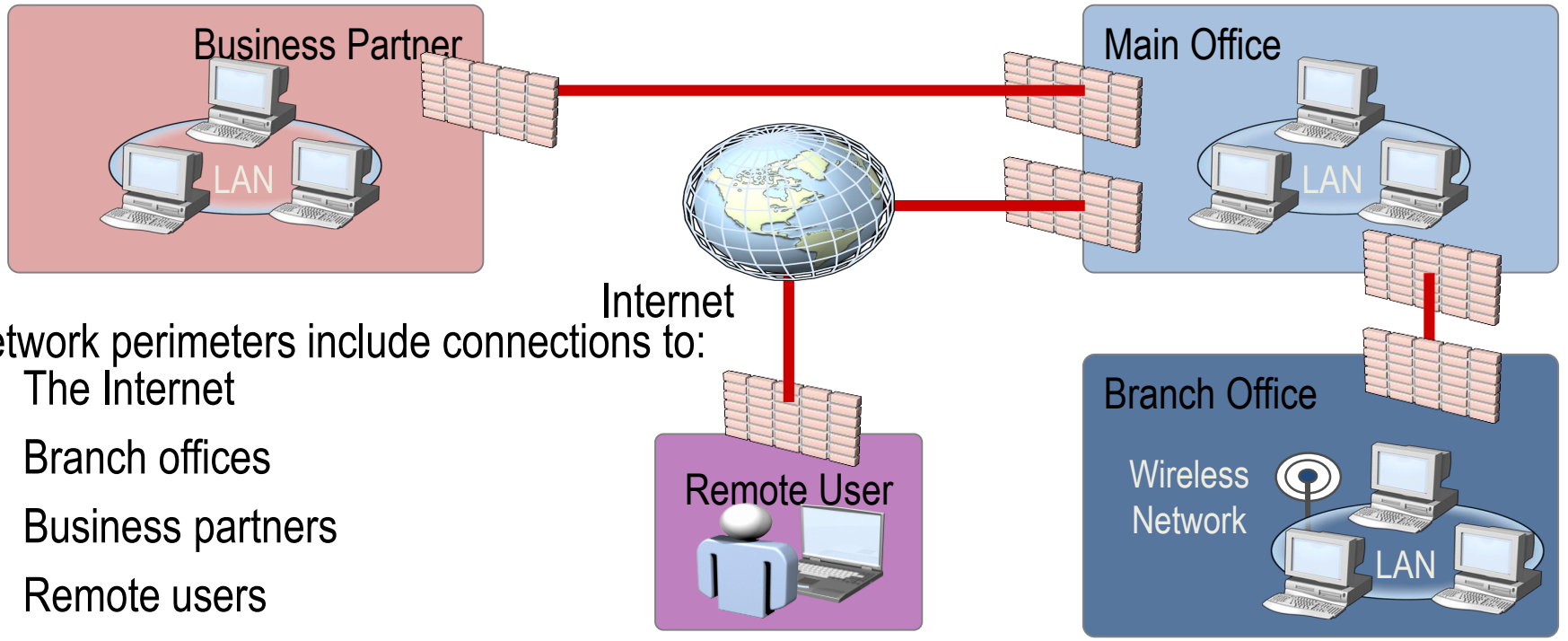
NETWORK AND INTERNET DEFENSE

PEMBAHASAN

1. Introduction
2. **USING PERIMETER DEFENSEs**
3. Using ISA Server to Protect Perimeters
4. Using ICF to Protect Clients
5. Protecting Wireless Networks
6. Protecting Communications by Using IPSec

- Agenda pembahsan ke-2 dari 6 agenda Network And Intenet Defense

PERIMETER CONNECTIONS OVERVIEW

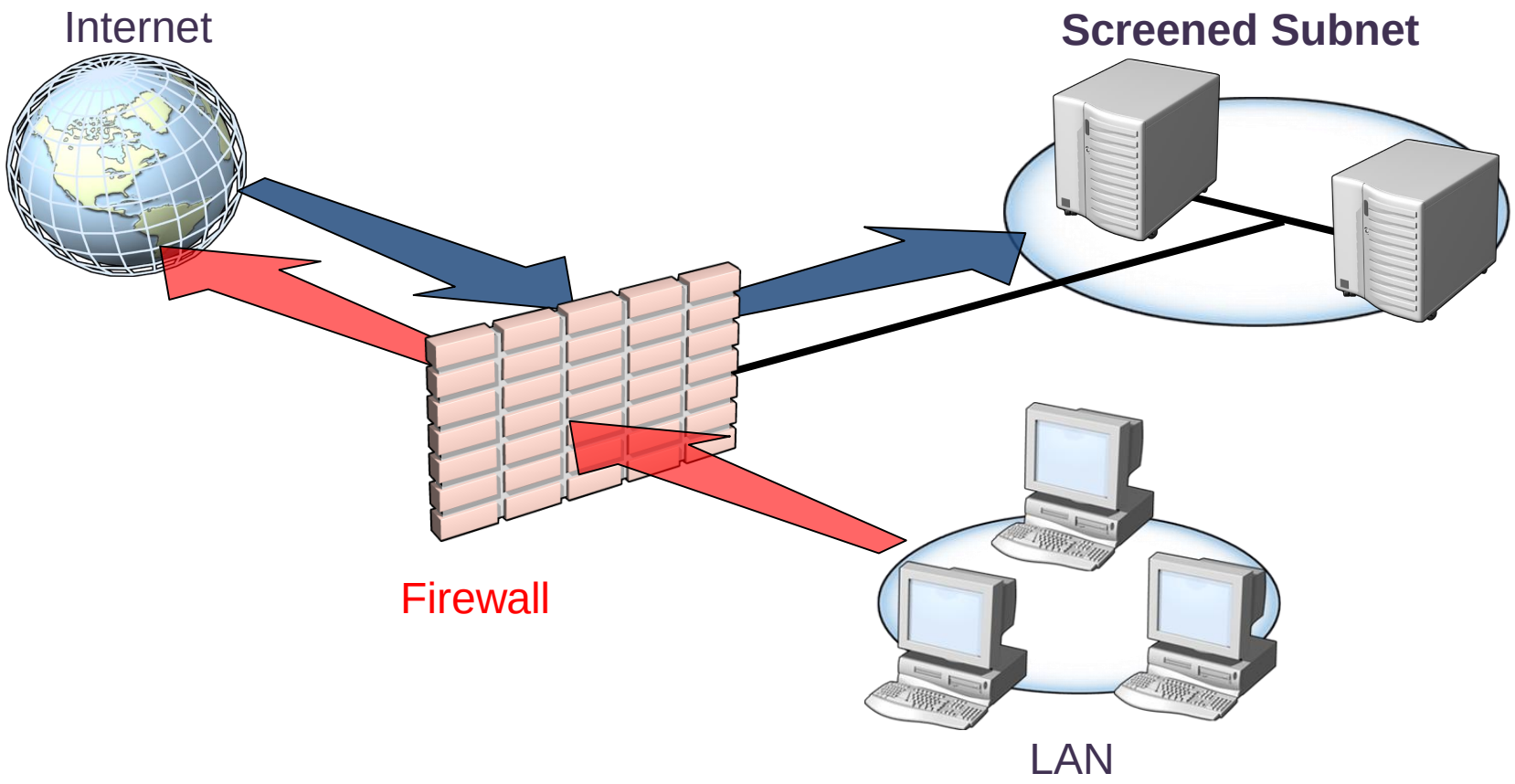


Network perimeters include connections to:

- The Internet
- Branch offices
- Business partners
- Remote users
- Wireless networks
- Internet applications

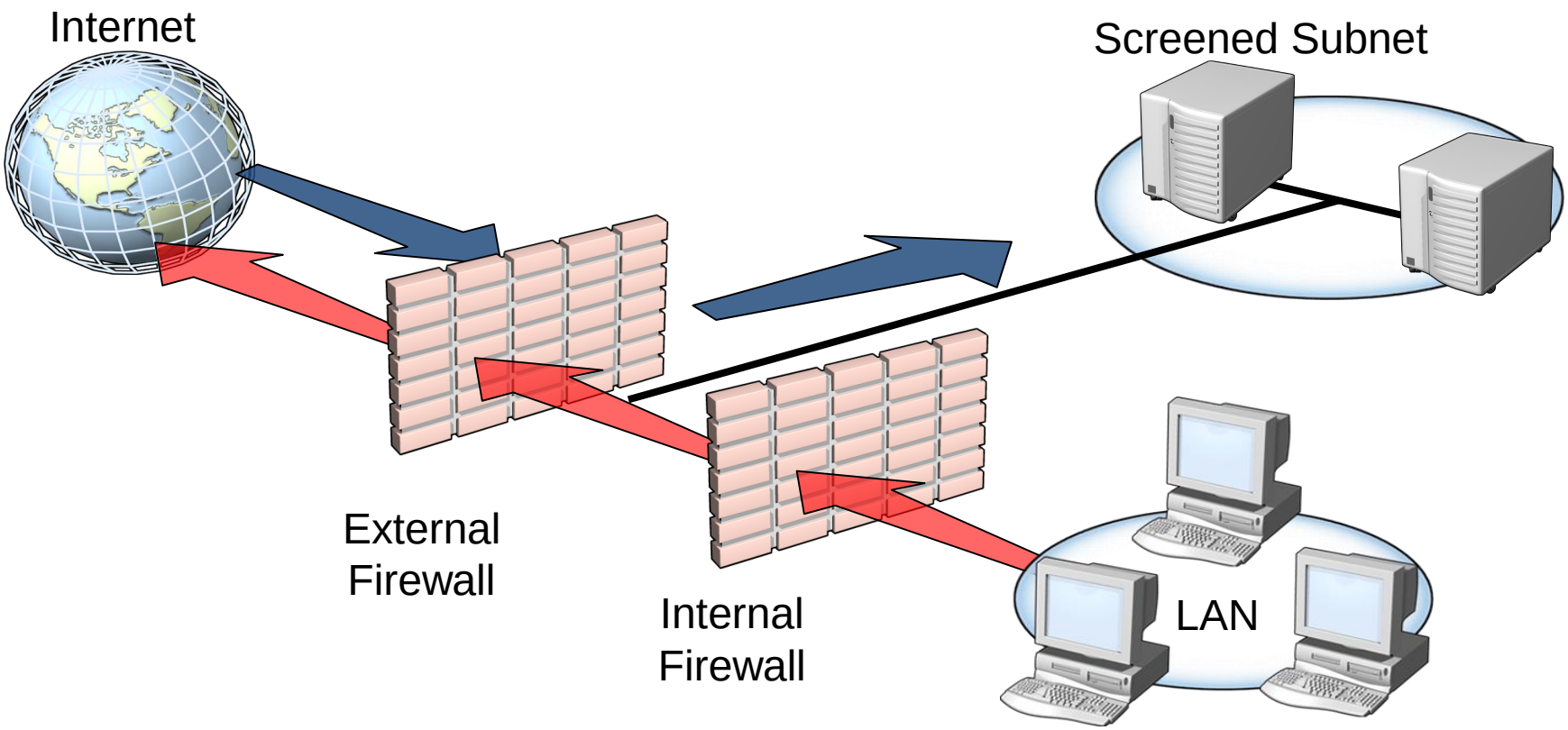
❖ Gambaran Implementasi Perimeter Connection secara umum

FIREWALL DESIGN: THREE-HOMED



- Disain Firewall antara LAN, Internet dan Screened Subnet

FIREWALL DESIGN: BACK-TO-BACK



- Disain Network dan Internet Defense dalam menggunakan Firewall Desain Back to Back

WHAT FIREWALLS DO NOT PROTECT AGAINST

1. Malicious traffic that is passed on open ports and not inspected at the application layer by the firewall
2. Any traffic that passes through an encrypted tunnel or session
3. Attacks after a network has been penetrated
4. Traffic that appears legitimate
5. Users and administrators who intentionally or accidentally install viruses
6. Administrators who use weak passwords

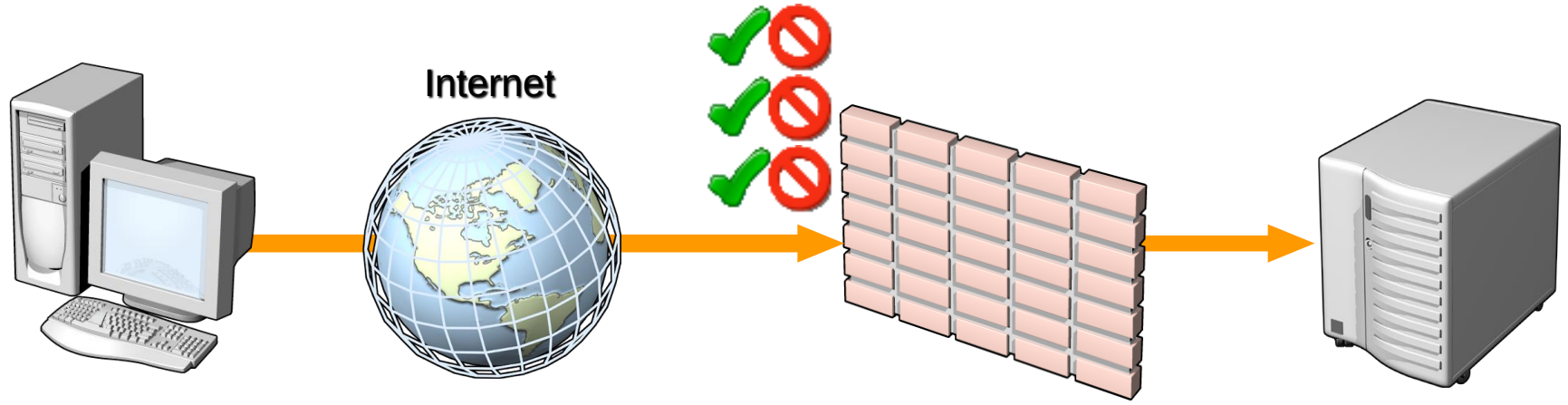
- 5 Point Penting dari tujuan dan keterbatasan dari perimeter pertahanan

SOFTWARE VS. HARDWARE FIREWALLS

Decision Factors	Description
Flexibility	Updating for latest vulnerabilities and patches is often easier with software-based firewalls.
Extensibility	Many hardware firewalls allow only limited customizability.
Choice of Vendors	Software firewalls allow you to choose from hardware for a wide variety of needs, and there is no reliance on single vendor for additional hardware.
Cost	Initial purchase price for hardware firewalls might be less. Software firewalls take advantage of low CPU costs. The hardware can be easily upgraded, and old hardware can be repurposed.
Complexity	Hardware firewalls are often less complex.
Overall Suitability	The most important decision factor is whether a firewall can perform the required tasks. Often the lines between hardware and software firewalls are blurred.

TYPES OF FIREWALL FUNCTIONS

- Packet Filtering
- Stateful Inspection
- Application-Layer Inspection



Multi-layer Inspection
(Including Application-Layer Filtering)

Gambaran umum fungsi dari Firewall dalam penerapan Network and Internet Defense

NETWORK AND INTERNET DEFENSE

AGENDA

- Introduction
- Using Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using ICF to Protect Clients
- Protecting Wireless Networks
- Protecting Communications by Using IPSec

❖ Agenda Pembahsan ke -3 dari 6 Agenda yang dibahas dalam Network And Internet Defense

GOALS OF NETWORK SECURITY

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	X		X	X		X
ICF		X				
802.1x / WPA				X	X	
IPSec		X			X	X

- Beberapa hal penting dalam tujuan keamanan jaringan

PROTECTING PERIMETERS

- ISA Server has full screening capabilities:
  - Packet filtering
  - Stateful inspection
  - Application-level inspection
- ISA Server blocks all network traffic unless you allow it
- ISA Server provides secure VPN connectivity
- ISA Server is ICSA certified and Common Criteria certified

❖ Kemampuan dasar yang harus ada dalam melaksanakan Protecting Perimeter

PROTECTING CLIENTS

Method	Description
Proxy Functions	Processes all requests for clients and never allows direct connections.
Client Support	Support for all clients without special software. Installation of ISA Firewall software on Windows clients allows for greater functionality.
Rules	Protocol Rules, Site and Content Rules, and Publishing Rules determine if access is allowed.
Add-ons	Initial purchase price for hardware firewalls might be less. Software firewalls take advantage of low CPU costs. The hardware can be easily upgraded and old hardware can be repurposed.

- Hal hal yang harus fokus dalam Protecting Clients

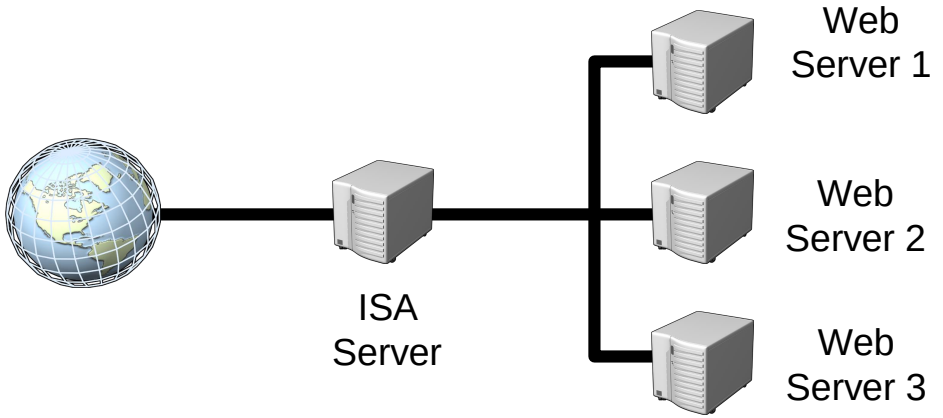
PROTECTING WEB SERVERS

- **Web Publishing Rules**
  - Protect Web servers behind the firewall from external attacks by inspecting HTTP traffic and ensuring that it is properly formatted and complies with standards
- **Inspection of Secure Socket Layer (SSL) traffic**
  - Decrypts and inspects incoming encrypted Web requests for proper formatting and standards compliance
  - Will optionally re-encrypt the traffic before sending them to your Web server

❖ Hal hal yang harus fokus dalam Protecting Web Servers

URL SCAN

- ISA Server Feature Pack 1 includes URLScan 2.5 for ISA Server
- Allows URLScan ISAPI filter to be applied at the network perimeter
  - General blocking for all Web servers behind the firewall
  - Perimeter blocking for known and newly discovered attacks



❖ Url Scan dalam konfigurasi ISA Server ke Web Server sebagai salah satu Implementasi Network and Internet Defense

PROTECTING EXCHANGE SERVER

Method	Description
Mail Publishing Wizard	Configures ISA Server rules to securely publish internal mail services to external users
Message Screener	Screens SMTP e-mail messages that enter the internal network
RPC Publishing	Secures native protocol access for Microsoft Outlook® clients.
OWA Publishing	Provides protection of the OWA front-end for remote Outlook users accessing Microsoft Exchange Server over untrusted networks without a VPN

- Hal penting yang harus diperhatikan dalam Protecting Exchange Server

TRAFFIC THAT BYPASSES FIREWALL INSPECTION

- SSL tunnels through traditional firewalls because it is encrypted, which allows viruses and worms to pass through undetected and infect internal servers
- VPN traffic is encrypted and cannot be inspected
- Instant Messenger (IM) traffic often is not inspected and might be used to transfer files

❖ Hal lain yang perlu dicermati dalam Traffic that bypass firewall instpection

INSPECTING ALL TRAFFIC

- Use intrusion detection and other mechanisms to inspect VPN traffic after it has been decrypted
  - Remember: Defense in Depth
- Use a firewall that can inspect SSL traffic
- Expand inspection capabilities of your firewall
  - Use firewall add-ons to inspect IM traffic

❖ Hal lain yang perlu dicermati dalam inspecting All traffic

SSL INSPECTION

1. SSL tunnels through traditional firewalls because it is encrypted, which allows viruses and worms to pass through undetected and infect internal servers.
2. ISA Server can decrypt and inspect SSL traffic. Inspected traffic can be sent to the internal server re-encrypted or in the clear.

ISA SERVER HARDENING

- Harden the network stack
- Disable unnecessary network protocols on the external network interface:
  - Client for Microsoft Networks
  - File and Printer Sharing for Microsoft Networks
  - NetBIOS over TCP/IP

❖ Hal lain yang perlu dicermati dalam ISA Server Hardening

BEST PRACTICES

1. **Use access rules that only allow requests that are specifically allowed**
2. **Use ISA Server's authentication capabilities to restrict and log Internet access**
3. **Configure Web publishing rules only for specific destination sets**
4. **Use SSL Inspection to inspect encrypted data that is entering your network**

❖ Fokus untuk Best Practis Using ISA Server to Protect Perimeters

AGENDA

- Introduction
- Using Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using ICF to Protect Clients
- Protecting Wireless Networks
- Protecting Communications by Using IPSec

❖ Agenda Pembahasan Ke-4 dari 6 agenda yang dibahas dalam Network And Internet Defense

GOALS OF NETWORK SECURITY

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	X		X	X		X
ICF		X				
802.1x / WPA				X	X	
IPSec		X			X	X

- 5 Point Penting dari tujuan dan keterbatasan dari perimeter pertahanan
- 5 Point Penting dari tujuan dan keterbatasan dari perimeter pertahanan

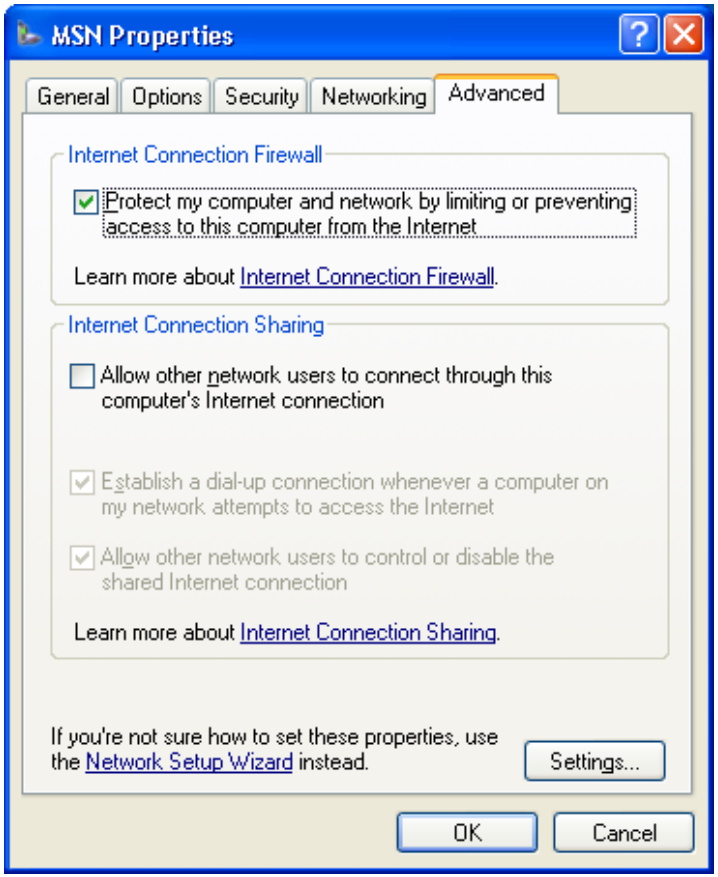
OVERVIEW OF ICF

What It Is	Internet Connection Firewall in Microsoft Windows XP and Microsoft Windows Server 2003
What It Does	Helps stop network-based attacks, such as Blaster, by blocking all unsolicited inbound traffic
Key Features	• **Ports can be opened for services running on the computer** • **Enterprise administration through Group Policy**

❖ Konsesp dasar dari ICF yang dibahas dalam Network And Internet Defense

ENABLING ICF

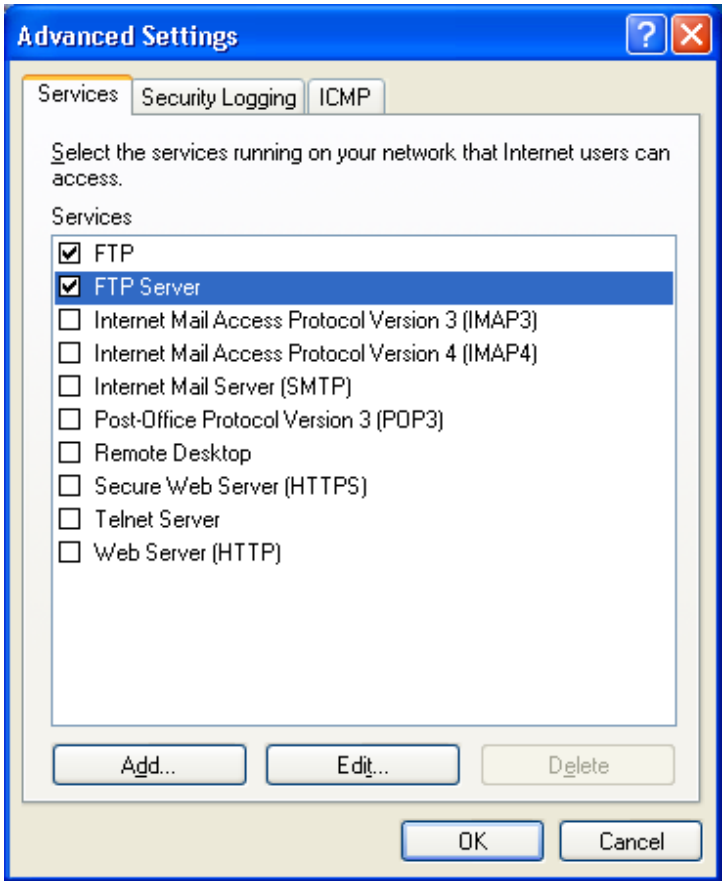
- Enabled by:
  - Selecting one check box
  - Network Setup Wizard
  - New Connection Wizard
- Enabled separately for each network connection



❖ Penjelasan dasar dari Enabling ICF untuk Network and Internet Defense

ICF ADVANCED SETTINGS

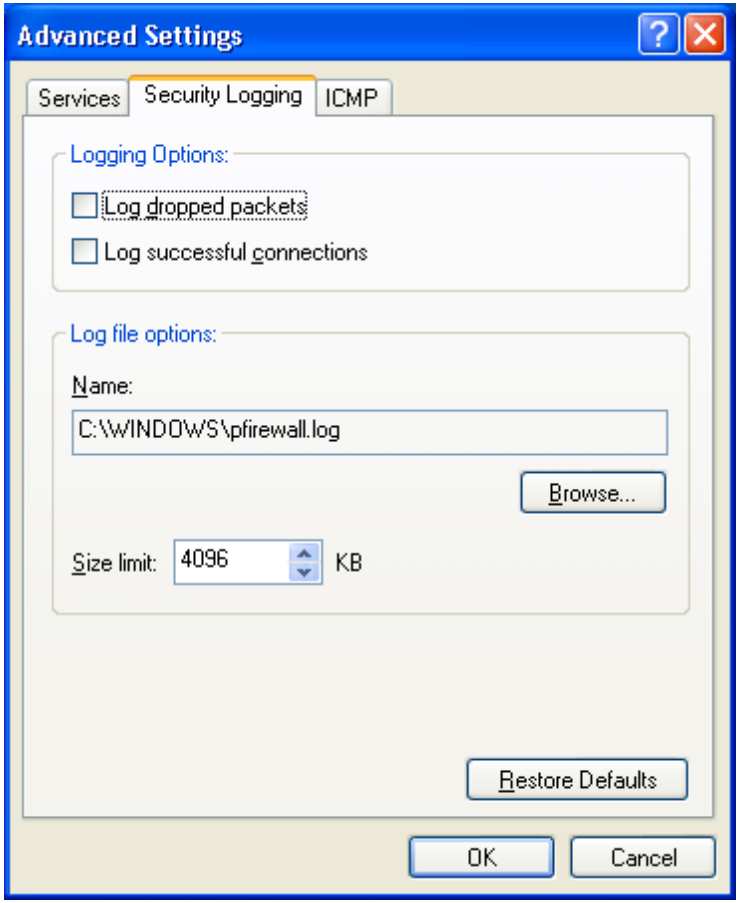
- **Network services**
- **Web-based applications**



❖ Penjelasan dasar dari Enabling ICF Avance Seting untuk Network and Internet Defense

ICF SECURITY LOGGING

- **Logging options**
- **Log file options**



❖ Penjelasan dasar dari ICF Securiiy Logging untuk Network and Internet Defense

ICF IN THE ENTERPRISE

- **Configure ICF by using Group Policy**
- **Combine ICF with Network Access Quarantine Control**

❖ Hal lain dalam ICF in The Enterprise yang harus diketahui.

BEST PRACTICES

1. Use ICF for home offices and small business to provide protection for computers directly connected to the Internet
2. Do not turn on ICF for a VPN connection (but do enable ICF for the underlying LAN or dial-up connection
3. Configure service definitions for each ICF connection through which you want the service to work
4. Set the size of the security log to 16 megabytes to prevent an overflow that might be caused by denial-of-service attacks

- Best Praktis dalam menjalan ICF Network And Internet Defence

AGENDA

- Introduction
- Using Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using ICF to Protect Clients
- Protecting Wireless Networks
- Protecting Communications by Using IPSec

❖ Agenda pembahasan ke-5 dari 6 agenda yang ada di Network And Internet Defense

GOALS OF NETWORK SECURITY

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	X		X	X		X
ICF		X				
802.1x / WPA				X	X	
IPSec		X			X	X

- Beberapa hal, terkait tujuan dari Network Security, dalam 802.1x / WPA

WIRELESS SECURITY ISSUES

- Limitations of Wired Equivalent Privacy (WEP)
  - Static WEP keys are not dynamically changed and therefore are vulnerable to attack.
  - There is no standard method for provisioning static WEP keys to clients.
  - Scalability: Compromise of a static WEP key by anyone exposes everyone.
- Limitations of MAC Address Filtering
  - Attacker could spoof an allowed MAC address.

❖ Pembahasan lebih pada Wireless Security issues

POSSIBLE SOLUTIONS

- Password-based Layer 2 Authentication
  - IEEE 802.1x PEAP/MSCHAP v2
- Certificate-based Layer 2 Authentication
  - IEEE 802.1x EAP-TLS
- Other Options
  - VPN Connectivity
    - L2TP/IPsec (preferred) or PPTP
    - Does not allow for roaming
    - Useful when using public wireless hotspots
    - No computer authentication or processing of computer settings in Group Policy
  - IPSec
    - Interoperability issues

❖ Dalam Penerapannya : “possible solutions” dalam hal Protecting Wireless Networks

WLAN SECURITY COMPARISONS

WLAN Security Type	Security Level	Ease of Deployment	Usability and Integration
Static WEP	Low	High	High
IEEE 802.1X PEAP	High	Medium	High
IEEE 802.1x TLS	High	Low	High
VPN	High (L2TP/IPSec)	Medium	Low
IPSec	High	Low	Low

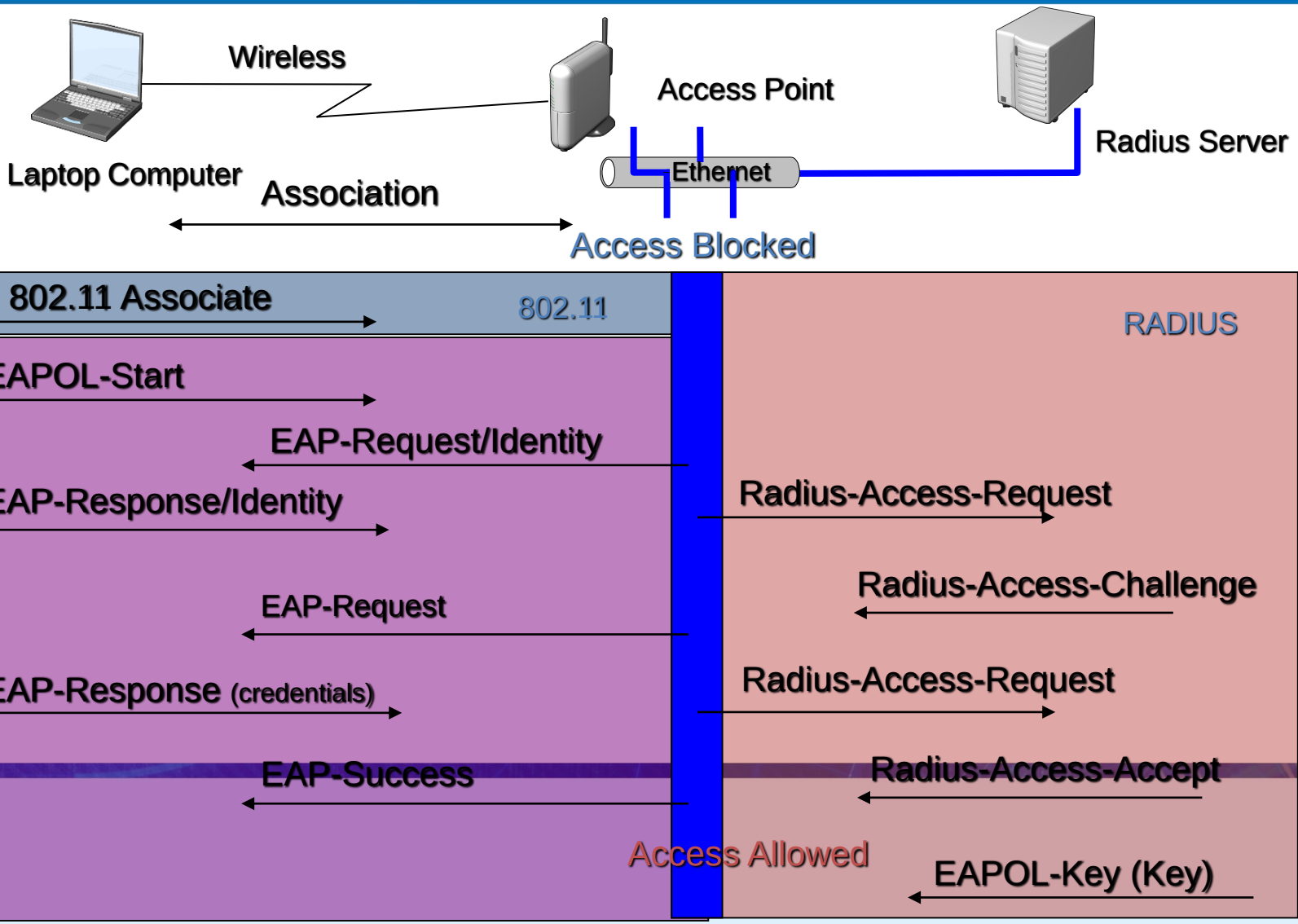
- Data WLAN Security Comparisons

802.1x

- Defines port-based access control mechanism
  - Works on anything, wired or wireless
  - No special encryption key requirements
- Allows choice of authentication methods using Extensible Authentication Protocol (EAP)
  - Chosen by peers at authentication time
  - Access point doesn't care about EAP methods
- Manages keys automatically
  - No need to preprogram wireless encryption keys

❖ Point untuk 802.1X

802.1X ON 802.11



SYSTEM REQUIREMENTS FOR 802.1X

- Client: Windows XP
- Server: Windows Server 2003 IAS
  - Internet Authentication Service—our RADIUS server
  - Certificate on IAS computer
- 802.1x on Windows 2000
  - Client and IAS must have SP3
  - See KB article 313664
  - No zero-configuration support in the client
  - Supports only EAP-TLS and MS-CHAPv2
    - Future EAP methods in Windows XP and Windows Server 2003 might not be backported

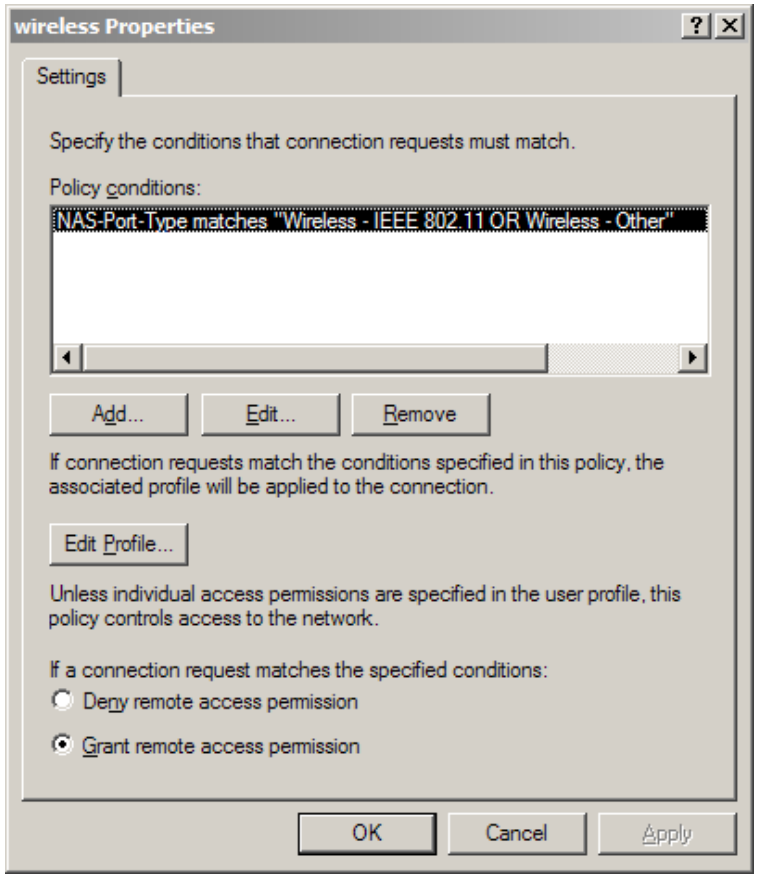
❖ System Requirements untuk 802.1X

802.1x Setup

1. **Configure Windows Server 2003 with IAS**
2. **Join a domain**
3. **Enroll computer certificate**
4. **Register IAS in Active Directory**
5. **Configure RADIUS logging**
6. **Add AP as RADIUS client**
7. **Configure AP for RADIUS and 802.1x**
8. **Create wireless client access policy**
9. **Configure clients**
   - **Don’t forget to import the root certificate**

❖ Tahapan dan konfigurasi dari WLAN : 802.1X

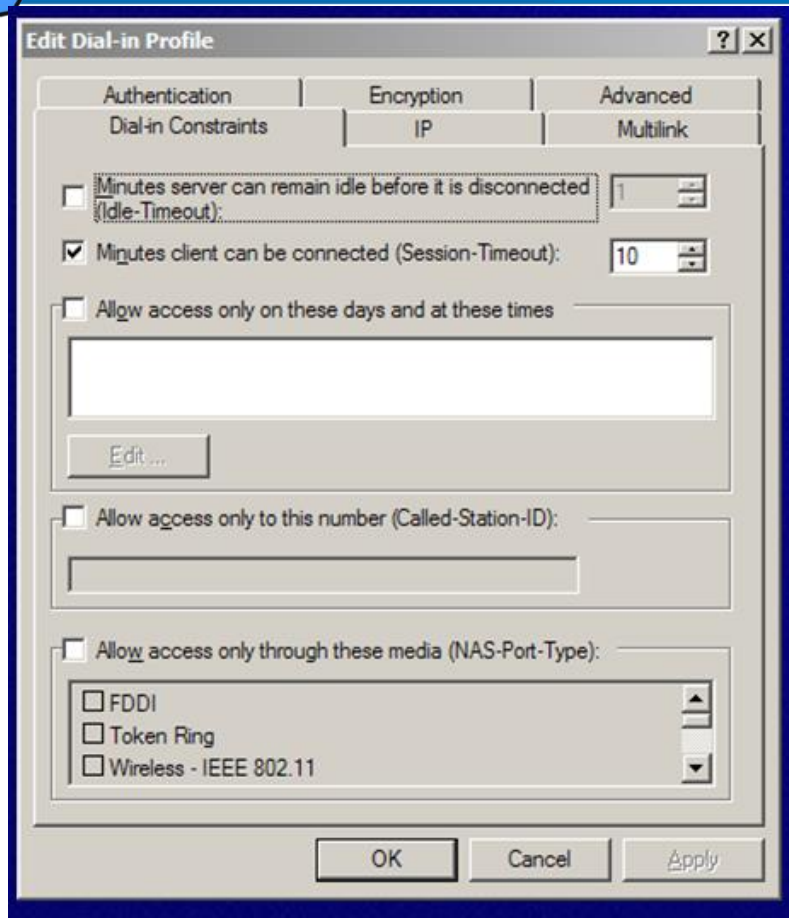
ACCESS POLICY



- Policy condition
  - *NAS-port-type matches Wireless IEEE 802.11 OR Wireless Other*
  - *Windows-group = <some group in AD>*
    - Optional; allows administrative control
    - Should contain user and computer accounts

❖ Access Policy dalam penggunaan WLAN

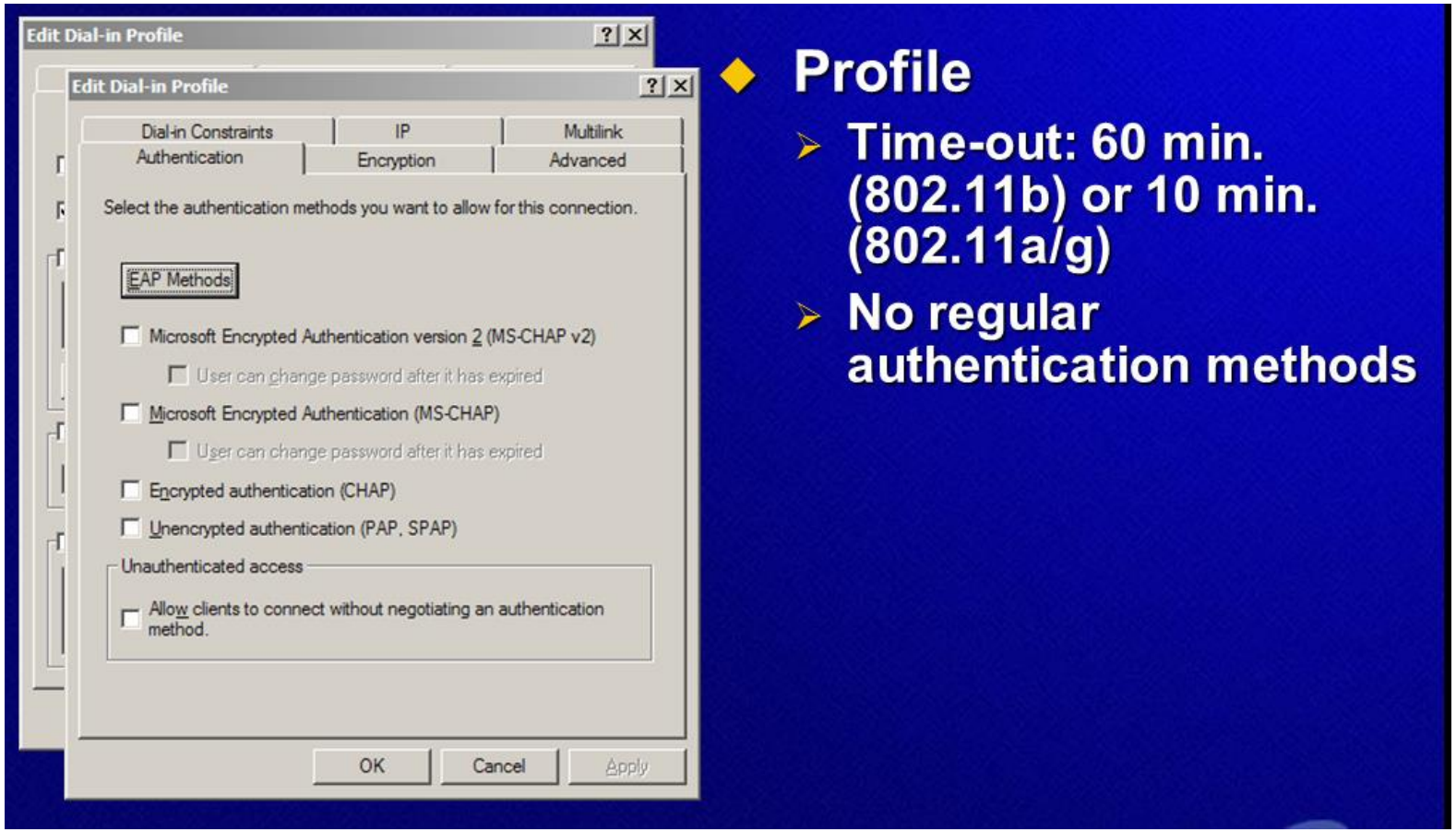
IMPLEMENTASI ACCESS POLICY



- **Profile**
  - **Time-out: 60 min. (802.11b) or 10 min. (802.11a/g)**

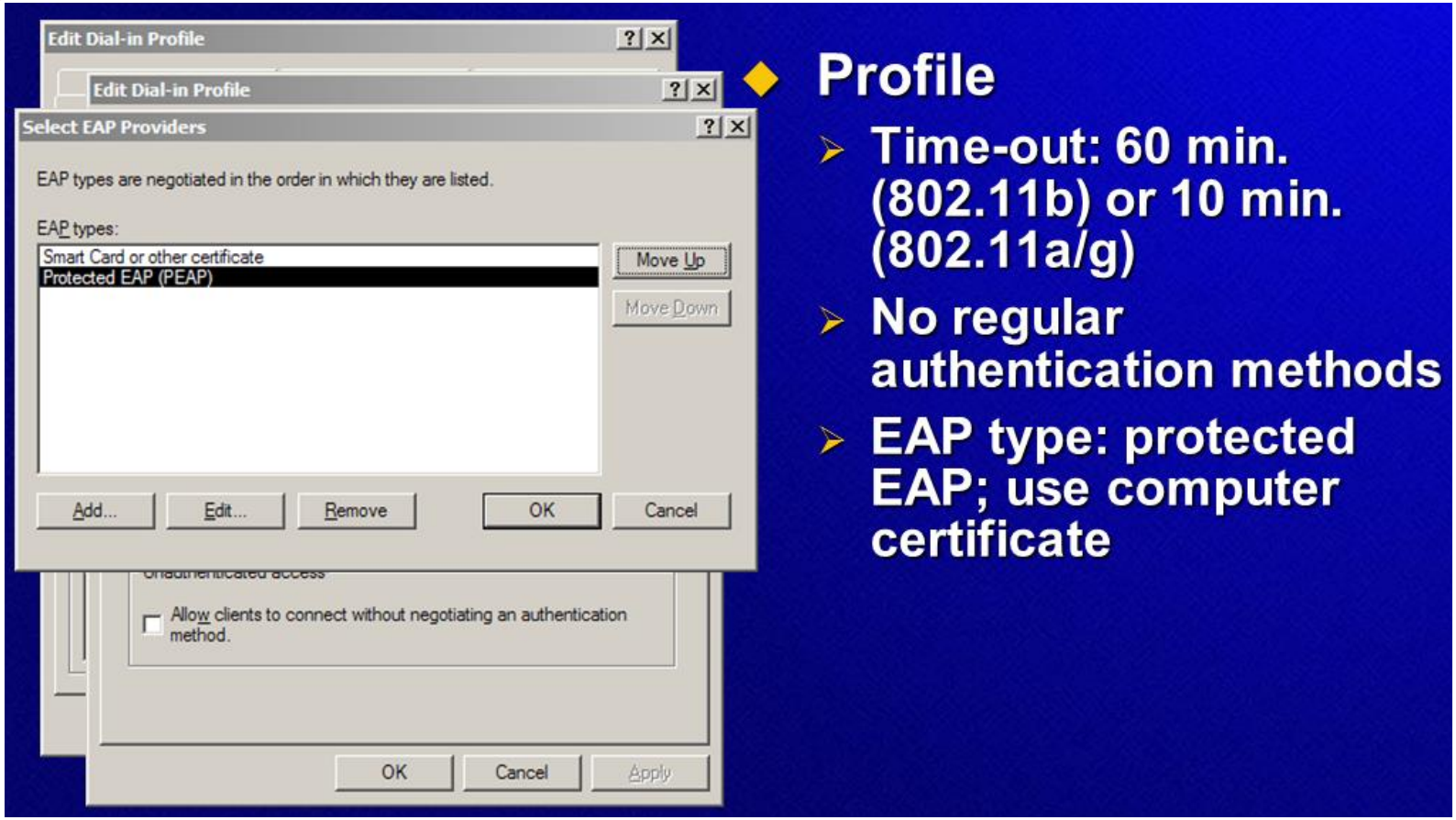
- Tahapan untuk Implementasi Access Policy WLAN

IMPLEMENTASI ACCESS POLICY



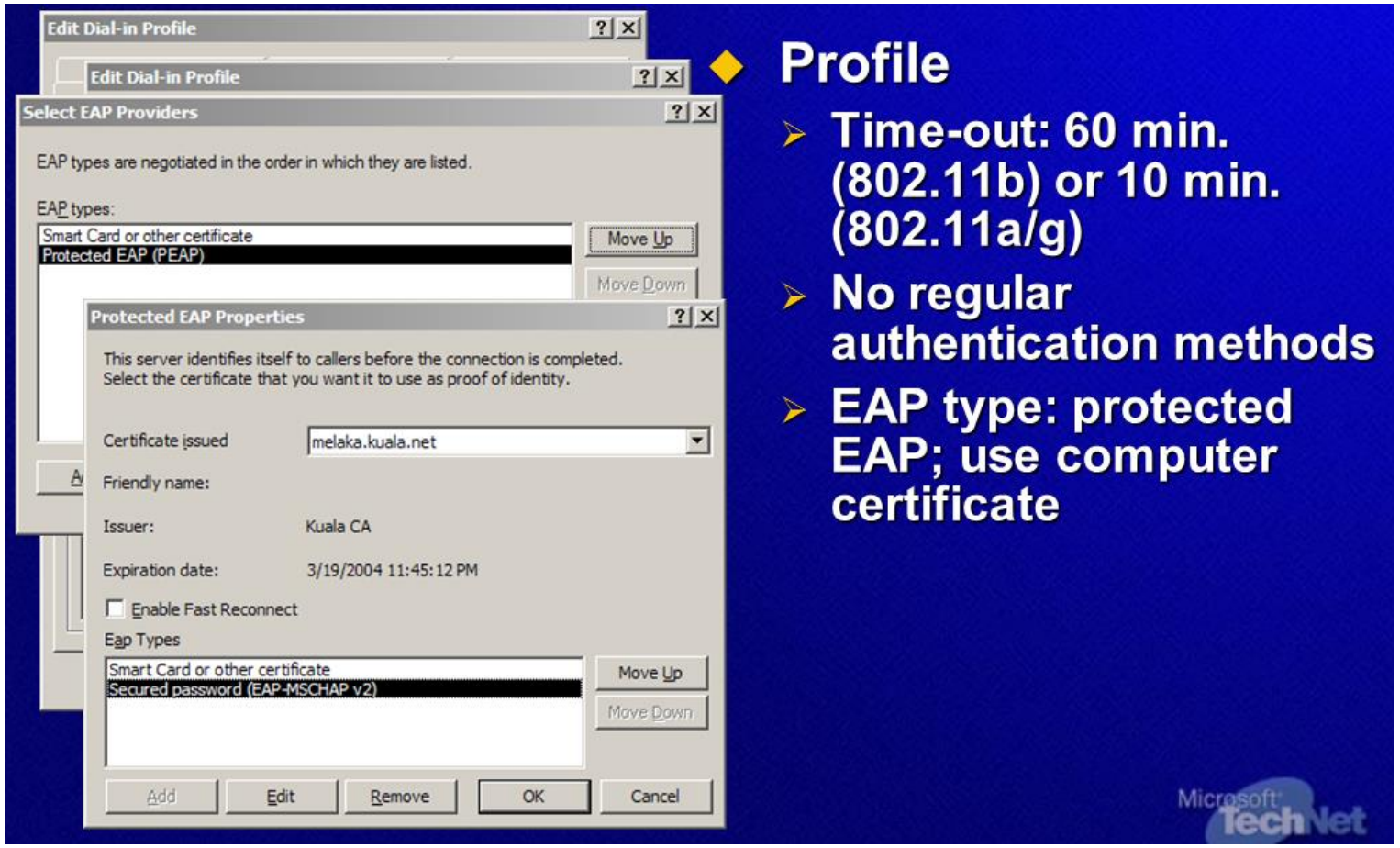
- Tahapan untuk Implementasi Access Policy WLAN

IMPLEMENTASI ACCESS POLICY



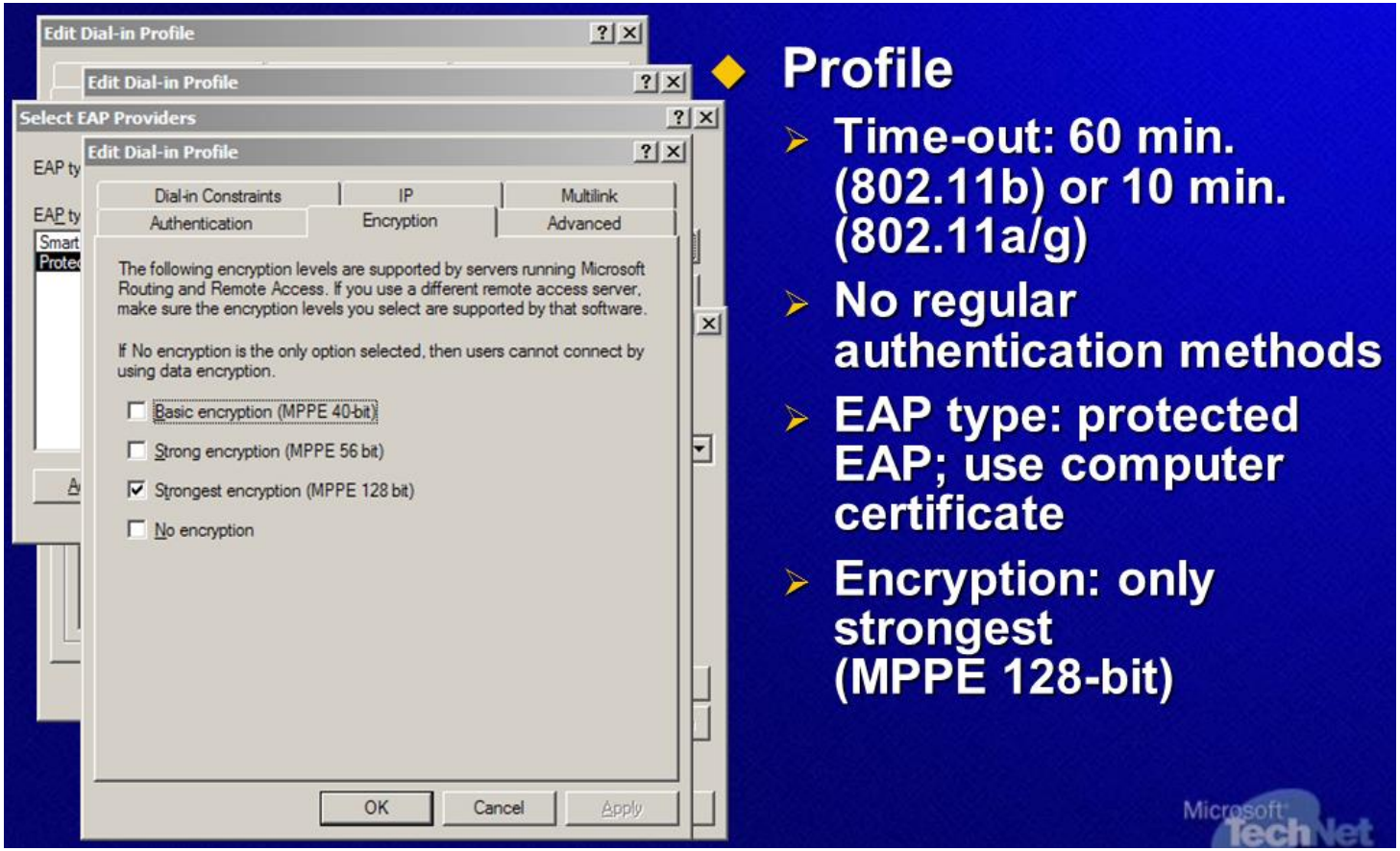
- Tahapan untuk Implementasi Access Policy WLAN

IMPLEMENTASI ACCESS POLICY



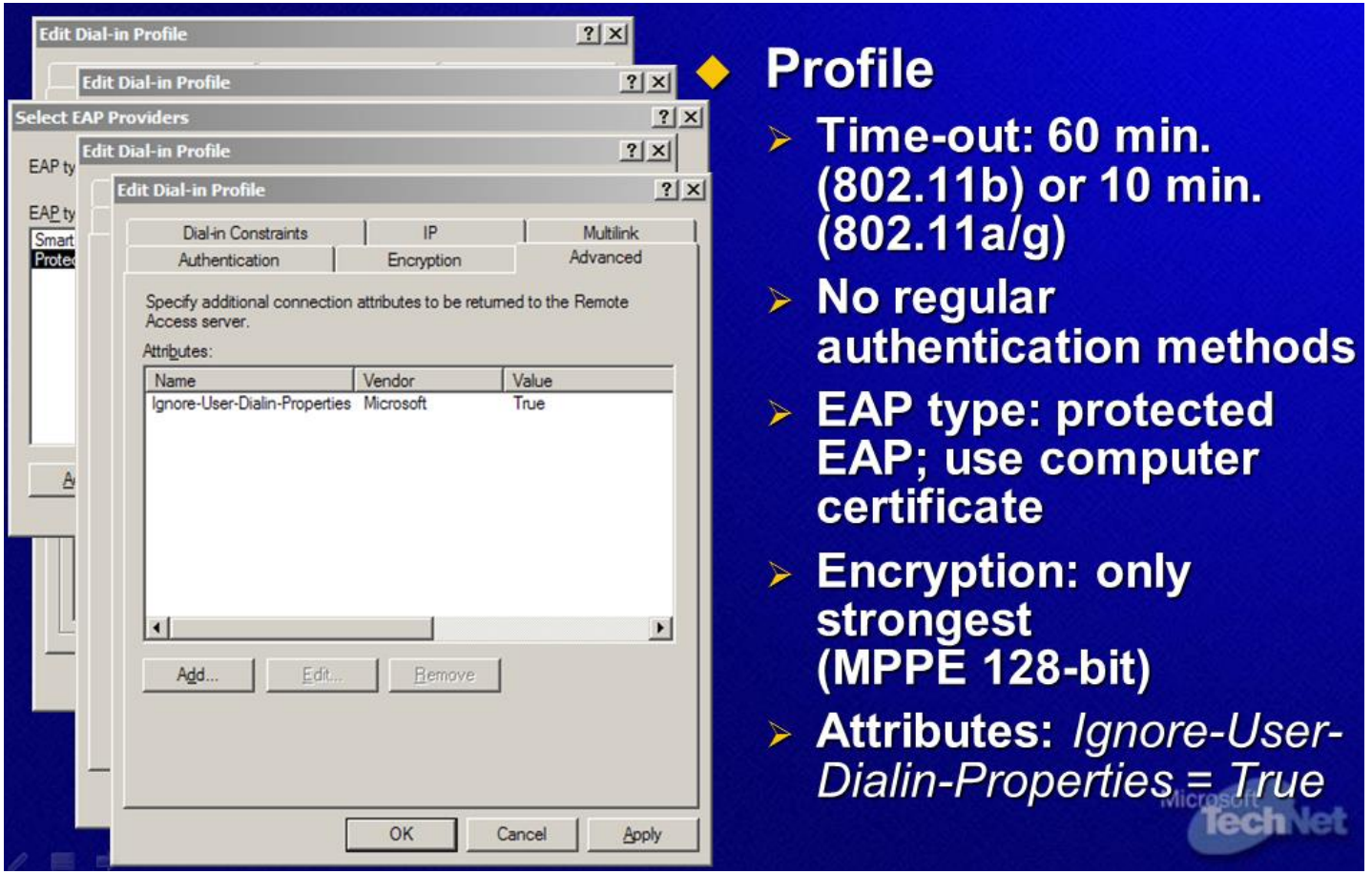
- Tahapan untuk Implementasi Access Policy WLAN

IMPLEMENTASI ACCESS POLICY



- Tahapan untuk Implementasi Access Policy WLAN

IMPLEMENTASI ACCESS POLICY



- Tahapan untuk Implementasi Access Policy WLAN

WIRELESS PROTECTED ACCESS (WPA)

- A specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems
- WPA Requires 802.1x authentication for network access

- Goals
  - Enhanced data encryption
  - Provide user authentication
  - Be forward compatible with 802.11i
  - Provide non-RADIUS solution for Small/Home offices

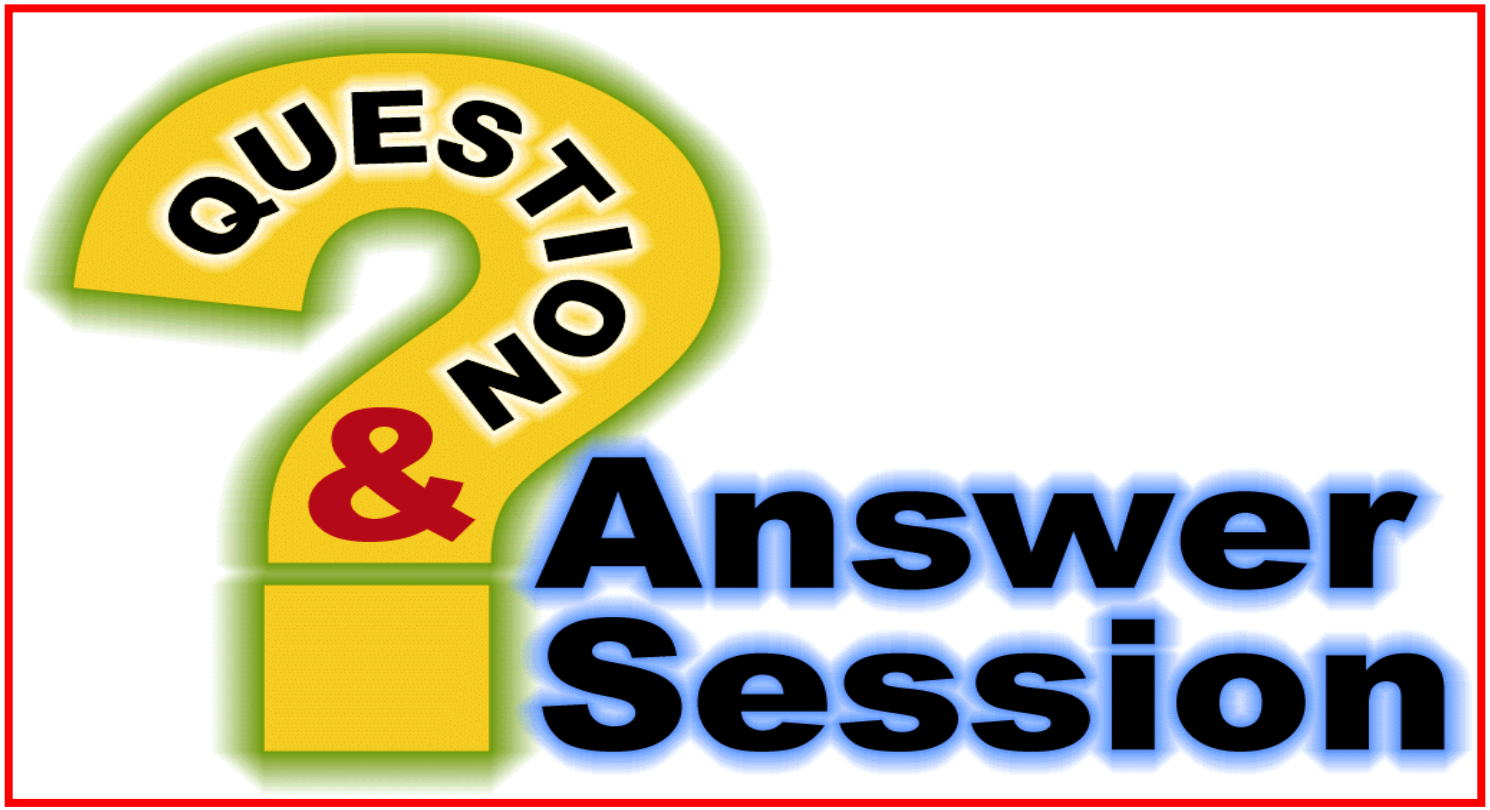
- Wi-Fi Alliance began certification testing for interoperability on WPA products in February 2003

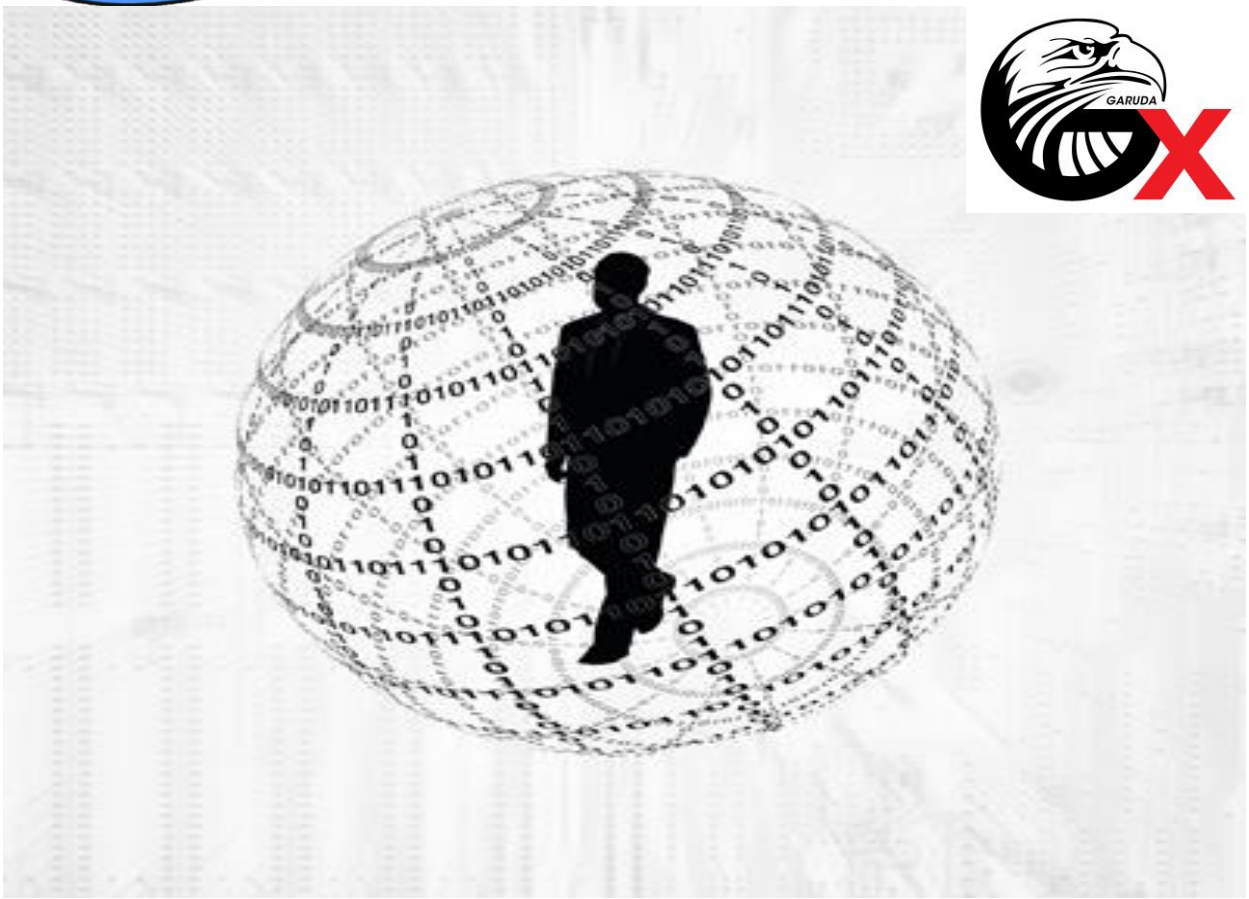
❖ WPA dan seluk beluknya yang harus dipahami

BEST PRACTICES

- Use 802.1x authentication
- Organize wireless users and computers into groups
- Apply wireless access policies using Group Policy
- Use EAP-TLS for certificate-based authentication and PEAP for password-based authentication
- Configure your remote access policy to support user authentication as well as machine authentication
- Develop a method to deal with rogue access points, such as LAN-based 802.1x authentication, site surveys, network monitoring, and user education

❖ Best Praktis dalam menggunakan 802.1x Protecting Wireless Networks


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