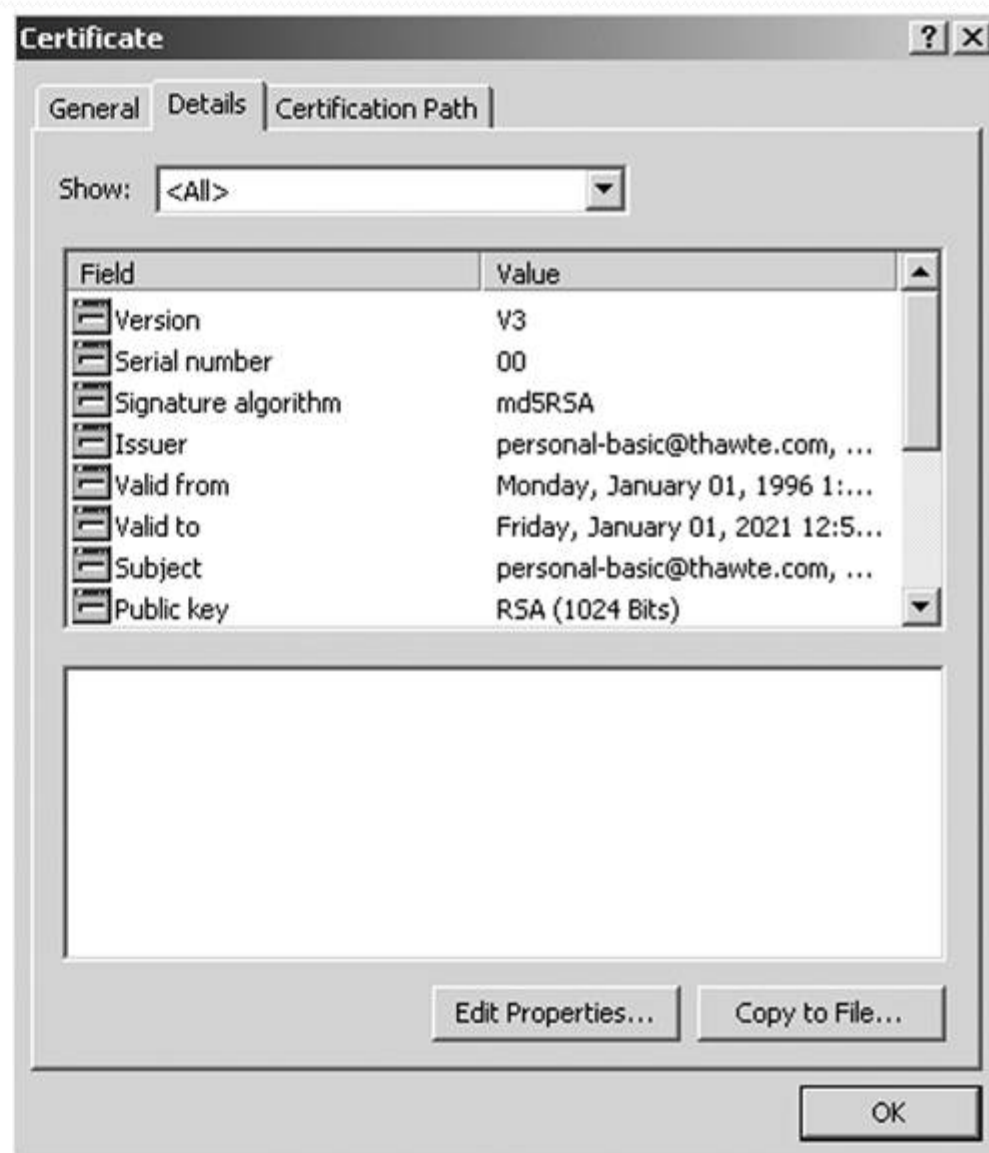
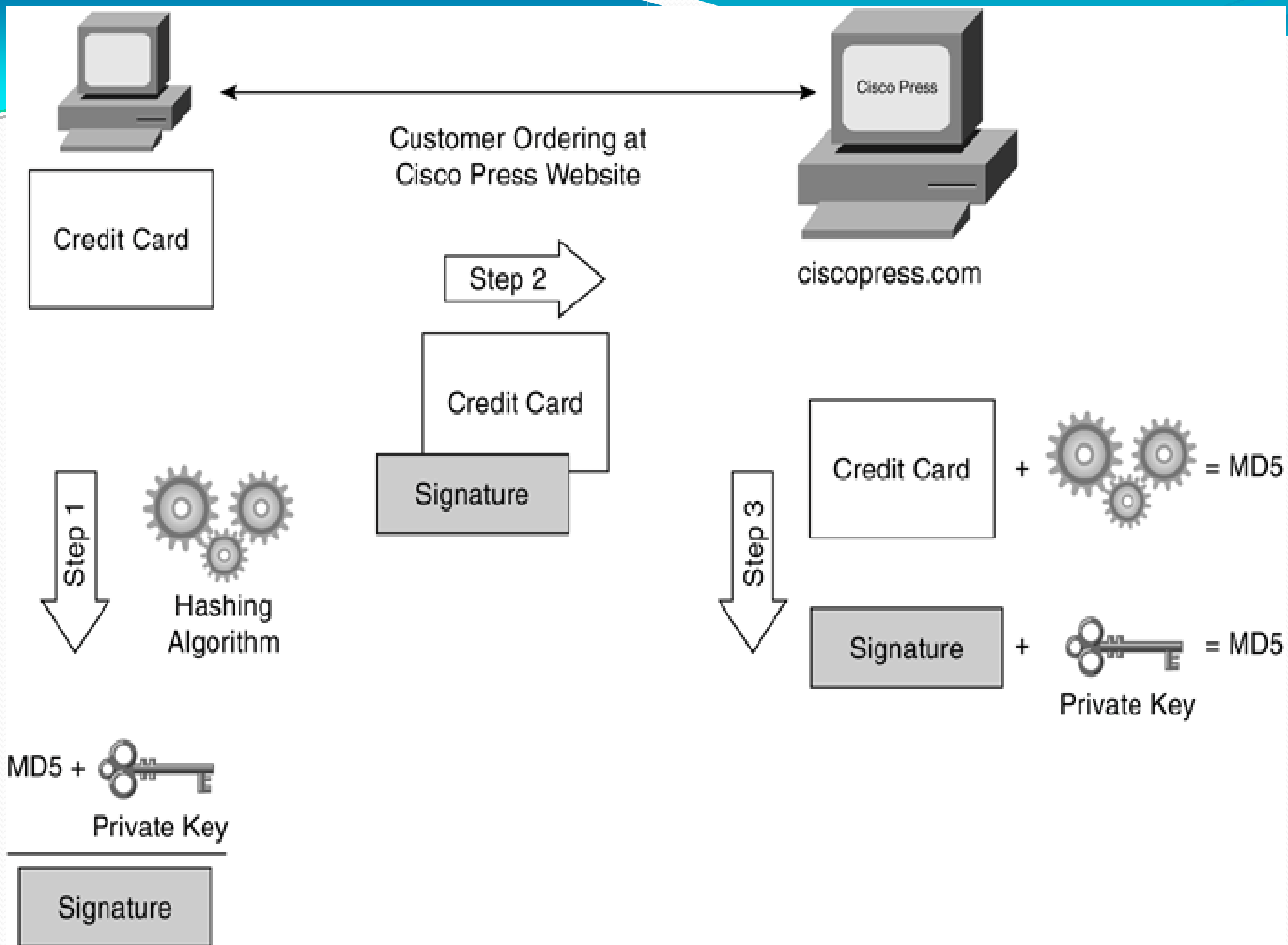



# Digital ID's

- Identitas digital, atau digital ID, adalah sarana untuk membuktikan identitas Anda atau bahwa Anda telah mendapat izin untuk mengakses informasi tentang perangkat jaringan atau jasa. Sistem atau metode digital di balik ID ini mirip dengan kartu identifikasi.
- Menggunakan ID foto pada kartu mencegah orang lain dari menyalahgunakan kartu dan berlaku meniru anggota klub.



- Version number: V3
- Serial number: 00
- Signature algorithm: MD5RSA
- Name of the issuer: Thawte Personal Basic CA
- Expiration date: Friday, January 01, 2021
- Owner's name: Thawte Personal Basic CA
- Owner's public key: RSA (1024 bits)




- 
- Hanya kunci publik yang dipertukarkan antara pengirim dan penerima. Sebelum transmisi sebenarnya dimulai antara dua host, host pengirim mengirimkan sertifikatnya, yang memberitahukan kunci publik, sehingga penerima dapat mengirim data atau informasi yang dienkripsi kembali.


- Informasi yang diterima kembali dapat didekripsi dengan menggunakan kunci privat. Kunci privat memiliki dua fungsi utama. Pertama, adalah membuat ID atau tanda tangan digital yang unik, dan kedua, melakukan decrypts informasi dalam kombinasi yang sesuai dengan kunci publik.

# Intrusion Detection System

- sistem deteksi intrusi (IDSs) mendeteksi dan mencegah intrusi ke dalam sistem.
- Intrusion adalah ketika seseorang mencoba untuk menembus, penyalahgunaan, atau memanfaatkan sistem yang ada.

- 
- IDSs telah terbukti menjadi solusi efektif baik serangan dari dalam dan luar.
  - Sistem ini berjalan terus-menerus di jaringan dan memberitahu personel keamanan jaringan ketika mendeteksi sebuah usaha yang dianggap mencurigakan.



- 
- IDSs memiliki dua komponen utama:
    - IDS sensor dan
    - IDS manajemen.

# • IDS sensor

- IDS sensor adalah software dan hardware yang digunakan untuk mengumpulkan dan menganalisis lalu lintas jaringan.
- Sensor ini tersedia dalam dua jenis,
  - network IDS dan
  - host IDS.

# Host IDS

- adalah agen khusus yang berjalan pada server dengan minimum overhead untuk memonitor sistem operasi dan aplikasi yang berada di server, seperti HTTP, SMTP, dan FTP.

# Network IDS

- dapat ditanamkan dalam sebuah perangkat jaringan, peralatan mandiri, atau modul untuk memonitor lalu lintas jaringan.

# IDS management

- bertindak sebagai titik pengumpulan peringatan dan melakukan konfigurasi dan penyebaran layanan dalam jaringan.

# PC CardBased Solutions

- PC CardBased Solutions memungkinkan administrator jaringan untuk menambah keamanan untuk mengendalikan akses, identitas, perangkat lunak, penyimpanan file, e-mail, dan sebagainya.
- Security cards atau smart cards, hardware keys dan PC card encryption cards yang paling umum digunakan.

# Security cards

- Security cards (sering disebut sebagai smart card) adalah kartu seukuran kartu kredit yang didalamnya terdapat chip.
- Smart card dapat digunakan untuk berbagai aplikasi dan tujuan yang membutuhkan perlindungan keamanan dan otentikasi karena semua informasi disimpan pada kartu itu sendiri. Setelah kartu diprogram, tidak lagi tergantung pada sumber daya eksternal.

# Contoh Smart Card

- Identification cards (including biometrics)
- Medical cards
- Credit and debit cards
- Access control cards (authentication)

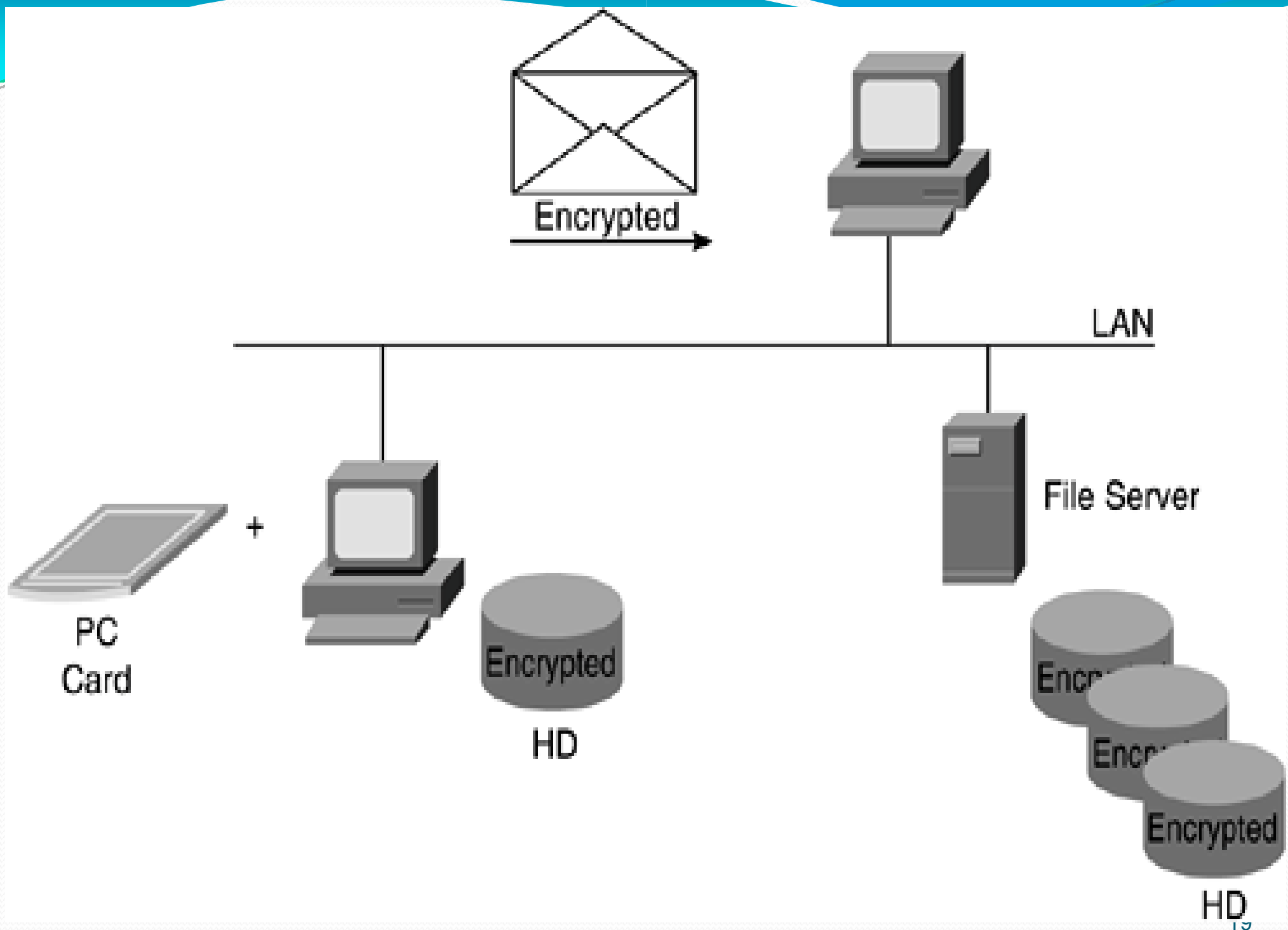


# Hardware Keys

- Hardware Keys yang dikenal sebagai pelindung dari perangkat lunak.
- Hardware Keys adalah solusi berbasis USB.

# PC Encryption Cards

- PC Encryption Cards tersedia untuk USB, LPT, COM, RS232, PCMCIA, dan (E) ISA.
- Kartu ini dapat ditambahkan sebagai peripheral atau terintegrasi dalam hampir semua perangkat komputer.



# Physical Security

- Outside and External Security
  - Electronic fence
  - Electromagnetic IDS
  - Camera systems
  - Entrance security (smart cards, PIN code)
  - Permanent guards

# Physical Security

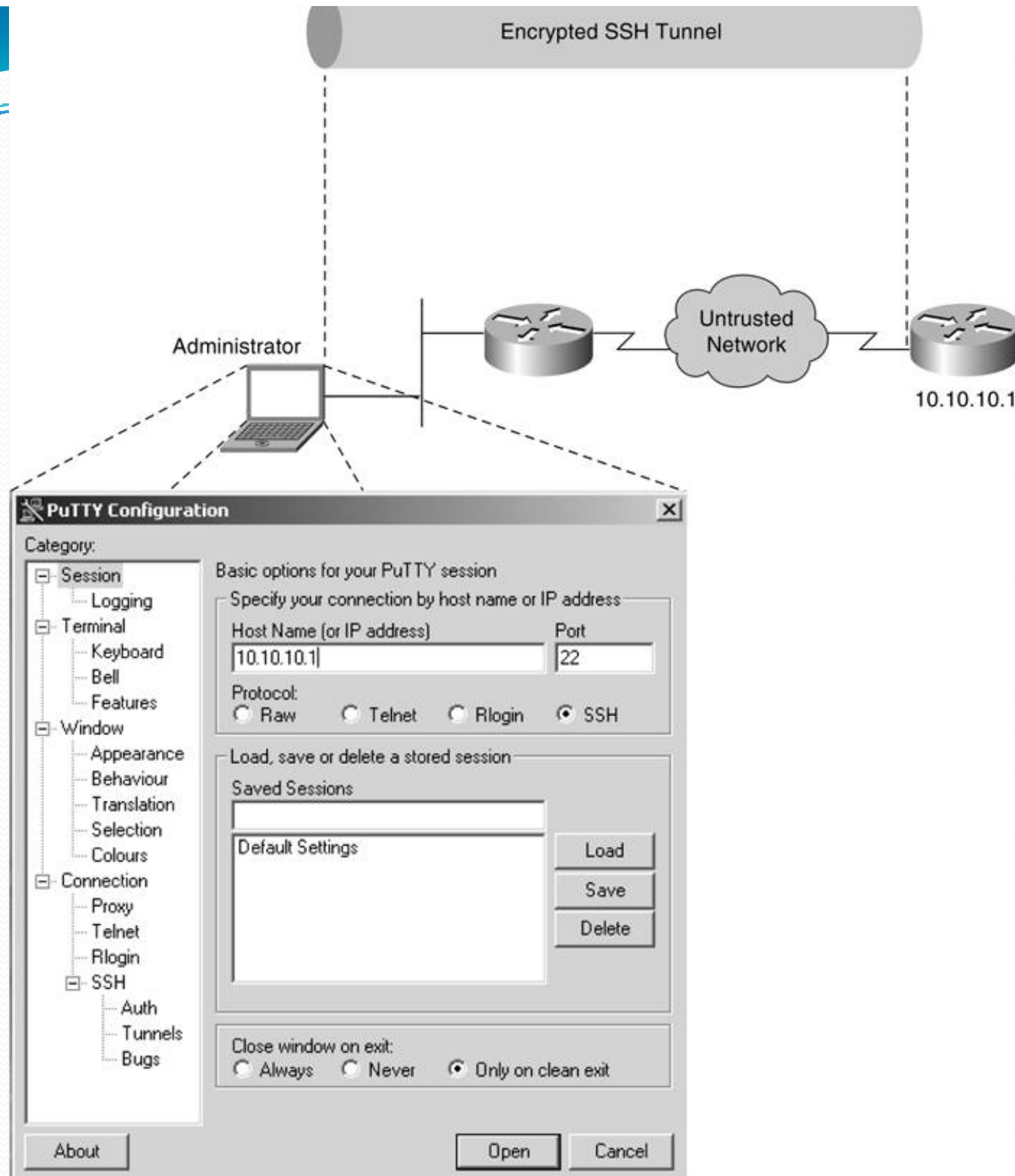
- Disaster-Recovery Plans
  - Hot site
  - Warm site
  - Cold site

# Physical Security

- Personnel Awareness
  - Mengembangkan kebijakan keamanan yang kuat membantu melindungi sumber daya Anda hanya jika semua anggota staff mengikuti seluruh kebijakan dengan benar

# Encrypted Login

- Secure Shell Protocol login session dapat digunakan untuk mengamankan remote Telnet session dan remote login.
- Protokol SSH digunakan untuk koneksi yang aman dengan mengenkripsi data seperti password, perintah-baris entri, debug output, atau bahkan file biner.





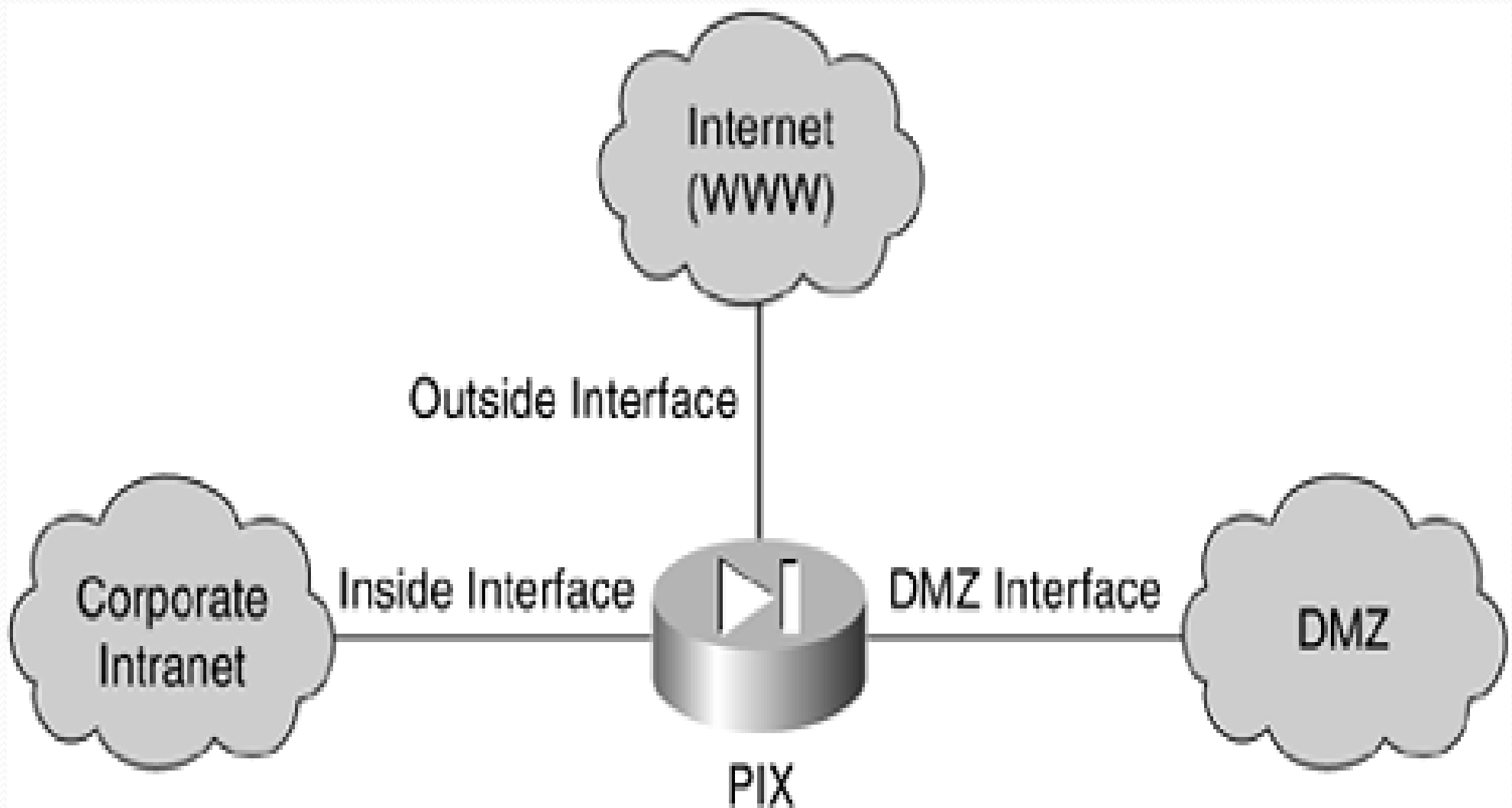
# Kerberos Encrypted Login Sessions

- Kerberos Encrypted Login Sessions menyediakan pendekatan alternatif SSH-encrypted login, di mana pihak ketiga yang terpercaya melakukan mekanisme otentikasi dan memverifikasi identitas pengguna. Kerberos dirancang untuk menjamin otentikasi kuat dalam skenario client-server dengan menggunakan kriptografi kunci rahasia.
- SSH menyediakan otentikasi dan transmisi data yang dienkripsi sedangkan Kerberos hanya menyediakan otentikasi terenkripsi.

# Secure Socket Layer (HTTP versus HTTPS)

- Digital ID menggunakan HTTPS, dimana data yang dikirim dienkripsi dan tidak dapat didekripsi tanpa kunci pribadi.
- Dalam HTTP, informasi tersebut dikirim dalam teks biasa dan tidak aman.
- Perbedaan utama adalah ini: HTTP tidak memiliki enkripsi, dan HTTPS menggunakan publik / sistem kunci pribadi untuk otentikasi.

# Firewall



# Reusable Passwords

- Otentikasi pengguna untuk akses sistem kontrol dicapai dengan menggunakan kombinasi username dan password atau kode PIN.

# Kelemahan Password

- Memilih password yang mudah ditebak.
- Panjang password yang tidak sesuai dengan ketentuan.
- Jarang mengganti password.
- Tidak menggunakan kombinasi karakter yang dianjurkan.

# Sample Password Policy

- Password length Eight characters or more
- Character classes Upper- and lowercase letters
- Characters Mix of numbers, symbols, and letters
- Grammar check No dictionary or jargon words
- Recurrence No use of the same character more than twice