Codice Corso: SEC020

Durata: 3 giorni

Obiettivi:

Questo corso è dedicato a personale responsabile della sicurezza delle reti aziendali che stanno prendendo in considerazione le VPN come strumento per garantire connettività.

Nel corso si acquisiscono le conoscenze necessarie a implementare soluzioni VPN. Si studia il protocollo IPSec, PPTP (Point to Point Tunneling Protocol), L2TP (Layer2 Tunneling Protocol) nonché gli standard di Key Management IKE e SKIP e lo standard dei certificati X.509.

Si impara quali sono le soluzioni VPN preferibili per applicazioni differenti, il progetto e l'installazione della migliore soluzione VPN per la propria azienda nonchè il bilanciamento della sicurezza e delle prestazioni.

Prerequisiti: grado di conoscenza equivalente a quella acquisita nel corso di Sicurezza reti (SEC010)

Contenuti:

Definizione di VPN

- Integrità dei dati
- Protezione dei messaggi
- Autenticazione
- Controllo di accesso
- Audit e logging
- Classe e qualità del servizo
- Implementazioni Internet
- Implementazioni Internet con RAS e Dialup
- Intranet
- Extranet
- Riduzione dei costi per linee dedicate
- Aumento della sicurezza
- Integrazione dei dati

Crittografia e VPN

- TCP-IP e la crittografia su rete
- Elementi del protocollo TCP/IP
- Implementazione della crittografia
- Livelli di crittografia
- Implementazioni di VPN
- Origine-Destinazione
- Nodo Intermedio
- Crittografia, codifica, decodifica e chiavi di cifratura
- PRNG, Truly Random Seed Values e chiavi

Integrità dei messaggi

- Funzioni di hash
- Sistemi di chiavi pubbliche e private
- Soluzioni hardware e software

- Lunghezza e volume del messaggio
- Lunghezza della chiave
- Generazione della chiave

Autenticazione

- User id e password
- Certifiacti digitali e X.509
- SHA/SHS e DSA/DSS
- Token card e smart card
- Luogo e biometrica

Controllo di accesso

Sistemi AAA

- RADIUS
- TACACS+